Denkpatronen

Hoe wiskunde en logica werken

Johan van Benthem
Robbert Dijkgraaf

Hoe Wiskunde en Logica werken

Wiskundig denken is een van de meest kenmerkende componenten van onze cultuur. Electronische gebruiksvoorwerpen zijn stukjes gestolde wiskunde, de veiligheid op uw dagelijkse treinstation berust op wiskundige analyse, maar ook de klassieke schilderijen die u dit weekeinde bewondert in het museum berusten op de wiskundige perspectiefleer. Minder tastbaar, maar nog meer algemeen, staat de wiskunde model voor precisie, helderheid, en publieke controleerbaarheid van denken en communiceren, en ze geeft daarmee een norm voor intellectueel gedrag . Het uitgangspunt van dit boekje is deze brede rol van de wiskunde, in natuur, taal, cognitie, en interactie tussen mensen. Onze thema's doorlopen dan ook het hele spectrum van beta tot alfa- en gamma-vakken.

Om dit werkingsterrein in kaart te brengen heeft de traditionele indeling in algebra, meetkunde, en andere 'subdisciplines' van de wiskunde weinig zin. In plaats daarvan hebben we gekozen voor een aantal hoofdthema's die op velerlei gebieden spelen. Het loutere feit dat een wiskundig fysicus en een wiskundig logicus zich in deze cursus moeiteloos op dergelijke thema's konden vinden illusteert op zichzelf al de eenheid van de wiskunde! In deel I van het boek zien we een aantal centrale thema's, Tellen, Oneindigheid, en Symmetrie, telkens belicht vanuit twee gezichtspunten. We beginnen elk thema vanuit de natuur en de klassieke wiskunde, en maken vervolgens een wending naar een meer taal- en redeneren-gerichte kijk op dezelfde verschijnselen. Op deze manier wordt tegelijkertijd het zelf-reflecterende vermogen van de wiskunde duidelijk. We beschrijven een wiskundige realiteit, maar zijn ons tegelijk bewust van de logische middelen waarmee we dat doen. Overigens besteden we niet alleen aandacht aan de logische structuur van taal en redeneren, maar ook – waar dat zo uitkomt aan de bevindingen over feitelijk menselijk taal — en redeneer-gedrag die momenteel beginnen op te komen in de cognitiewetenschappen.

Een ander aspect van levende wiskunde is de veelheid aan legitieme gezichtspunten. In deel II bespreken we thema's als Waarschijnlijkheid, Spel, en Voorspellen, waar de vorming van ideeën en technieken nog steeds in volle gang is. Er is bijvoorbeeld niet één definitieve wiskundige analyse van het begrip waarschijnlijkheid, of van het begrip spel. En misschien komt er ook nooit zo'n definitief dogma dat de discussie sluit. Wiskundige analyse stimuleert juist de creativiteit, ook in het verzinnen van alternatieven! Overigens loopt ook hier de toepassing vanaf objectieve frequenties in de natuur en observeerbaar gedrag van populaties in de biologie tot subjectieve waarschijnlijkheden, weddenschappen, en de – al dan niet logische – manieren waarop mensen hun meningen vormen, en herzien in interactie met elkaar. Soms kan een technisch onderwerp dan ineens weer verrassende filosofische repercussies hebben, zoals we zullen zien in het theorie van 'dynamische systemen'.

In deel III, tenslotte, kiezen we een hoger abstractie-niveau, en analyseren noties die de hele wiskundige activiteit doordrenken, te weten Bewijs, Rekenen, en Paradoxen. Deze noties werden object van wiskundig onderzoek in het grondslagenonderzoek in de eerste helft van de twintigste eeuw. Beroemde resultaten van Gödel en Turing brachten hierbij zowel mogelijkheden als grenzen aan het licht: niet elk probleem is effectief oplosbaar, niet elk waar inzicht is te bewijzen. Het logische grondslagenonderzoek geldt als één van de meest abstracte takken van de moderne wiskunde. Maar tegelijkertijd heeft het geleid tot de meest concrete consequenties, zoals het ontstaan van computers en de moderne informatica. En daarmee zien we hoe wiskundige zelf-reflectie de wereld kan transformeren. Wij leven anno 2005 in een wereld van mensen, machines, fysische en virtual reality, met velerlei vormen van informatie en communicatie die vroeger niet denkbaar waren. De wiskunde heeft een cruciale rol gespeeld in het scheppen van die diverse wereld van vandaag. Zij blijft ook een van onze beste bondgenoten in het begrijpen van die wereld, en het bewaren van een intellectueel evenwicht en overzicht.

Johan van Benthem
Robbert Dijkgraaf

Inhoudsopgave

Deel I

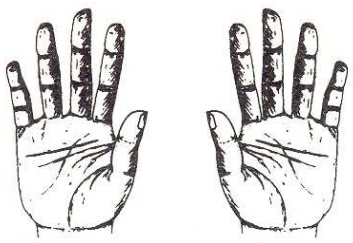
Tellen en taal

Hoofdstuk 1

Tellen

1.1 Telbaarheid óf hoe ver kun je tellen?

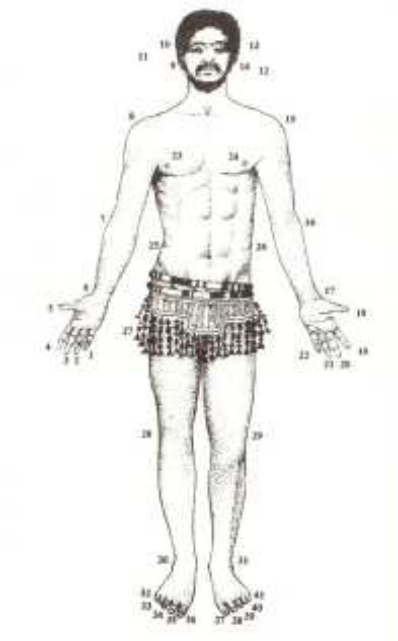
Leren tellen is een moeizaam proces. Dat kan iedereen die kleine kinderen heeft vaststellen. Het duurt een aantal jaar voordat een kind met één blik kan zien dat er drie knikkers op tafel liggen. Welk gedachtestappen zijn daarvoor nodig en hoe wordt de vaardigheid om te tellen vertaald in de wiskunde, waar de natuurlijke getallen aan de basis van alles liggen?



Primitieve culturen hebben in het algemeen een zeer eenvoudig telsysteem. Soms telt men niet verder dan vier. Men begint het tellen met de begrippen ‘één’ en ‘twee’ te onderscheiden: alleen of samen. Vervolgens ontstaat ‘drie’, vaak gerepresenteerd als de som $1 + 2$, en eindigt men bij ‘vier’, veelal benoemd en soms ook geschreven als $2 + 2$. Daarna wordt er geen onderscheid gemaakt tussen de aantallen groter dan vier. Het is allemaal ‘veel’. In deze karikatuur van ons getallensysteem verliezen we de belangrijkste eigenschap van tellen, namelijk dat het nooit ophoudt, dat er oneindig veel natuurlijke getallen zijn. In zo’n ‘primitief’ systeem gaat tellen eenvoudig van

1, 2, 3, 4, veel.

Toch is men zelfs met zo’n elementair getalbegrip in staat om in de dagelijkse praktijk met veel grotere getallen om te gaan. Dat kan bijvoorbeeld door handig gebruik te maken van lichaamsdelen zoals vingers, tenen, ellebogen en knieën. Door creatief genoeg te zijn in het vinden van te onderscheiden lichaamsonderdelen telt men zo in sommige Polynesische culturen gemakkelijk tot over de veertig.



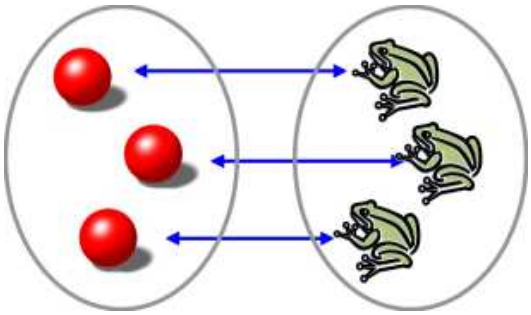
Ook al is er geen apart woord voor ‘vijf’, je kan op deze wijze toch vaststellen dat bijvoorbeeld het aantal gezinsleden precies op de vingers van één hand te tellen is. Preciezer gezegd, er kan worden vastgesteld dat twee verzamelingen, namelijk enerzijds de vingers aan een hand en anderzijds het aantal leden van het gezin, één op één met elkaar in verband kunnen worden gebracht. Beide bevatten precies evenveel elementen. Dat is een belangrijke les. In veel praktische gevallen is het van groter belang te weten of twee aantallen gelijk zijn, dan het precieze aantal te weten of te kunnen benoemen.

Nog een praktijkvoorbeeld. Zeg men leeft in een clan van zesentwintig mensen. Maar er bestaat in de gesproken taal geen woord ‘zesentwintig’ voor dit aantal, het is gewoon ‘veel’. Als het er zeventwintig waren geweest, had dit precies hetzelfde aangevoeld. Misschien zoals wij ons nu voelen in een voetbalstadion, waar het totale aantal toeschouwers ons ook ontgaat. Toch kan men nagaan of ’s avonds iedereen weer veilig terug in de groep is. ’s Ochtends legt iedereen een balletje in een kom en ’s avonds neemt men dat balletje er weer uit. Het aantal balletjes dat overblijft is dan het aantal missende personen. Als alle balletjes uit de kom zijn genomen is vastgesteld dat alle zesentwintig personen weer aanwezig zijn, zonder dat het getal 26 ooit expliciet is gemaakt. Er is alleen vastgesteld dat er precies evenveel balletjes als veilig teruggekeerde groepsleden zijn.

Een ander voorbeeld, meer uit onze alledaagse ervaring. Je stapt in de bus en kijkt of er een plaats is. Als je geen vrije stoel ziet heb je vastgesteld dat er precies evenveel passagiers in de bus zitten als er stoelen zijn. Maar het aantal stoelen of passagiers weet je niet precies. Wederom is het voldoende een correspondentie gevonden te hebben tussen het aantal stoelen en het aantal reizigers.

We zijn hier bij het kernbegrip van dit hoofdstuk aangeland: de correspondentie tussen de elementen van twee even grote verzamelingen, bijvoorbeeld ‘groepsleden’ en ‘balletjes’, of ‘buspassagiers’ en ‘stoelen’. Technisch spreken we dan van een *bijectie*.

Hier is bijvoorbeeld een bijectie tussen een verzameling knikkers en een verzameling kikkers.



Als we praten over eindige verzamelingen is het duidelijk dat er alleen zo’n bijectie kan bestaan als het aantal elementen in X en Y hetzelfde is. Dat wil zeggen, voor het bestaan van een bijectie is het noodzakelijk dat X en Y even groot zijn.

We kunnen de redenering ook omdraaien en beweren dat uit deze bijecties van concrete verzamelingen de abstracte getallen ontstaan. Er zijn allerlei verzamelingen om ons heen en deze vallen uiteen in categorieën van verzamelingen waarvan we kunnen vaststellen dat ze even groot zijn. We kunnen nu afspreken dat we twee verzamelingen, vanuit een bepaald perspectief, als identiek beschouwen als ze evenveel elementen hebben. Dat wil zeggen, we kijken door een zeer grove bril waarbij we alleen oog hebben voor het aantal elementen en verder niet geïnteresseerd zijn in het wat en hoe van de elementen. Daarmee vallen allerlei verzamelingen samen, zeg de verzameling van ‘drie knikkers’, ‘drie kikkers’, ‘drie appels’ etc. Al deze verzamelingen hebben ‘drie’ als een gemeenschappelijke factor.

Dit leidt tot een abstractie, ‘de verzameling met drie elementen’. Deze ‘equivalentieklasse’ van verzamelingen kunnen we nu met een abstract symbool weergeven. Hiertoe kiezen we het symbool

TECHNIEK 1.

Functies

- *Een* functie *of* afbeelding f *met* domein A *en* bereik B*, kort opgeschreven als* $f : A \to B$*. is wat met elk element* x *van* A *een uniek element* $f(x)$ *van* B *associeert. We spreken van de* toepassing *van* f *op* x*, en het resultaat* $f(x)$ *noemen we het* f*-*beeld *van* x*.*
- *Het* beeld $f[A]$ *van* f *is de verzameling van alle* f*-beelden. Dit is natuurlijk een deelverzameling van* B*.*
- *Als geldt dat* $f[A] = B$ *dan noemen we* f *een* surjectie *of een* surjectieve functie*.*
- *Als elk tweetal verschillende elementen van het domein van een functie* f *een verschillend* f*-beeld heeft dan noemen we* f *een* injectie *of een* injectieve *functie.*
- *Een* bijectie *is een functie die surjectief en injectief is.*
- *Als* $f : A \to B$ *een bijectie is dan kunnen we* f *ook omkeren en een krijgen we een nieuwe bijectie van* B *naar* A*. Deze omkering van* f *heet de* inverse *van* f *en wordt kort genoteerd als* f^{-1}*.*

  $$f^{-1} : B \to A \text{ met } f^{-1}(y) = x \text{ als } f(x) = y \text{ voor alle } y \text{ in } B$$

  Dit is inderdaad een juist functie-voorschrift: voor elke $y \in B$ *is* f^{-1} *gedefinieerd want* f *is surjectief, en* f^{-1} *geeft ook steeds voor elke* y *een uniek beeld want* f *is injectief. Verder geldt er* $f(f^{-1}(y)) = y$ *voor alle* y *in* B*,* $f^{-1}(f(x)) = x$ *voor alle* x *in* A *en* $(f^{-1})^{-1} = f$*.*
- *Als er een bijectie bestaat dan schrijven we* $A \leftrightarrow B$*, wat het bestaan van de inverse mede verbeeldt.*

Functies en de omvang van eindige verzamelingen

Voor een verzameling A *schrijven we* $|A|$ *voor zijn omvang of* cardinaliteit*.*

Als A *en* B *eindige verzamelingen zijn en* $f : A \to B$ *is een functie dan geldt dat het aantal* f*-beelden niet groter is dan* A*:* $|f[A]| \leq |A|$*. Als* f *een* surjectie *is weet je dat* $|B| \leq |A|$*. Als* f *een injectie is dan geldt* $|f[A]| = A$*. In dit laatste geval krijgt elk element van* A *een uniek* f*-beeld in* B*. Je zou kunnen spreken van een 'herbenoeming' van de elementen van* A *in* B*.*

Als $|B| < |A|$ *dan kan* f *dus nooit een injectie zijn. Dit is het duiventilprincipe uit de tekst. Er moet een paar* x_1, x_2 *in* A *te vinden zijn met* $x_1 \neq x_2$ *maar wel* $f(x_1) = f(x_2)$*.*

Als f *een bijectie is dan moet gelden dat* $|B| = |A|$*. Dit is een 'herbenoeming' van* A*-elementen in* B *waarbij alle elementen van* B *gebruikt worden.*

Als f *een injectie is dan geldt natuurlijk dat de functie* $f' : A \to f[A]$ *met* $f'(x) = f(x)$ *voor alle* $x \in A$ *een bijectie is.*

3 en we spreken dit uit als ‘drie’! Een blik op een telboek voor kleuters leert ons dat dit inderdaad de manier is hoe we een getal leren, namelijk als het gemeenschappelijke van allerlei verzamelingen. Door het kind genoeg te laten oefenen met concrete voorbeelden ontstaat langzamerhand het abstracte en overkoepelende getalsbegrip.

De duiventil

Er zijn altijd minstens twee Amsterdammers met evenveel haren op hun hoofd. Dit volgt uit het duiventil of *pidgeon hole* principe dat is gebaseerd op de kennis dat een verzameling groter is dan een ander, zonder precies te weten hoeveel groter.

Als er vijf duiven zijn, maar slecht drie hokjes in de duiventil, en alle duiven moeten een slaapplaatsje in de til zoeken, dan weten we zeker dat er minstens twee duiven een hokje moeten delen. Er zijn immers meer duiven dan hokjes. Dit eenvoudige inzicht van de stoelendans geeft aanleiding tot het volgende algemene principe.

> DUIVENTILPRINCIPE. *Als we p objecten in q dozen doen met $p > q$, dan is er minstens één doos met twee objecten.*

Oneindig

We vinden de mens die ‘1, 2, 3, 4, veel’ telt primitief. Maar hoe tellen wij dan? Wij tellen 1, 2, 3, 4, 5, ... Hier staan de ... voor een oneindige reeks getallen. Er komt immers geen eind aan de verzameling $\mathbb{N}_+$ van positieve gehele getallen. Als n het laatste en grootste getal zou zijn dan kunnen we altijd een groter getal $n+1$ vinden door er één aan toe te voegen. Misschien moeten we dan tellen als

$$1, 2, 3, 4, 5, \ldots, \text{ oneindig}.$$

Daarmee neemt het begrip ‘oneindig’ in zekere zin dezelfde plaats in als het begrip ‘veel’ bij het eenvoudige telsysteem, waar alle getallen boven de vier op een hoop verder geveegd. Op dezelfde wijze noemen we alles wat niet uit een eindig aantal bestaat oneindig.

Er is een rijke ideeëngeschiedenis van het begrip oneindig, zowel in de vorm van oneindig groot als oneindig klein. Denk aan de beroemde paradoxen van Zeno van Elea, zoals Achilles en de schildpad die hij nooit kan inhalen, en de vliegende pijl, die nooit vooruit kan komen omdat deze op ieder tijdstip stilstaat. Het is erg gemakkelijk om in de knoop te draaien als je niet voorzichtig met een oneindigheid omgaat.

Inderdaad, zoals we nog uitgebreid zullen zien, de kenmerkende, paradoxale eigenschap van oneindige verzamelingen is dat zo’n verzameling een (eigenlijke) deelverzameling toestaat die ‘even groot’ als de oorspronkelijke verzameling.

Andere wiskundigen die belangrijke bijdragen hebben geleverd zijn Aristoteles en veel later in de negentiende eeuw de Tsjechische wiskundige Bernard Bolzano (1781–1848). Deze laatste compileerde een groots overzicht van allerlei paradoxale aspecten van het begrip ‘oneindig’, *Paradoxien des Unendlichen* (1851). In dit boek werd het begrip ‘verzameling’ voor het eerst gebruikt (een begrip dat wij hier stilzwijgend als, op z’n minst intuïtief, bekend veronderstellen). Ook was hij de eerste die de methode van de bijecties uitbreidde naar oneindige verzamelingen.

Maar de werkelijke bedwinger van dit lastige onderwerp en de grote held van dit hoofdstuk is de Duitse wiskundige Georg Cantor. Cantor was een onomstreden genie. Hij heeft als geen ander onze blik op de wereld van het oneindige vergroot. Hij heeft in wezen de lont in het kruitvat van de moderne wiskunde gestoken, zoals we later zullen zien.

$\xrightarrow{\text{P. 1}}$ 15

Oneindige verzamelingen getallen

- *De verzameling van de* natuurlijke getallen *is de verzameling van alle niet negatieve gehele getallen:* $\{0, 1, 2, \ldots\}$. *Voor deze verzameling gebruiken we de naam* $\mathbb{N}$. $\mathbb{N}_+$ *staat voor alle positieve gehele getallen. We schrijven verder* $12 \in \mathbb{N}, \sqrt{2} \notin \mathbb{N}$ *om aan te geven dat* 12 *een element van de verzameling van de natuurlijke getallen is en* $\sqrt{2}$ *niet.*
- *De verzameling van alle* gehele getallen, $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$, *wordt* $\mathbb{Z}$ *genoemd. We schrijven* $\mathbb{N} \subseteq \mathbb{Z}$ *en* $\mathbb{Z} \nsubseteq \mathbb{N}$ *om aan te geven dat* $\mathbb{N}$ *een deelverzameling van* $\mathbb{Z}$ *maar niet andersom.*
- *De verzameling van de* gebroken getallen *of* breuken *wordt* $\mathbb{Q}$ *genoemd. De breuken worden in de wiskunde ook* rationale getallen *genoemd. Elke breuk heeft de vorm* $\frac{a}{b}$ *waarbij* a *en* b *gehele getallen zijn.*

Reële getallen

Zijn alle getallen te schrijven als een breuk*? Dat blijkt* niet *zo te zijn. Een duidelijk tegenvoorbeeld is* $\sqrt{2}$. *Stel dat* $\sqrt{2} = \frac{n}{m}$ *met* n *en* m *gehele getallen. Neem nu de kleinste getallen* a *en* b *zodanig dat* $\frac{a}{b} = \frac{n}{m}$. *Zo'n paar is te krijgen door* n *en* m *te delen door hun grootste gemeenschappelijke deler. Er moet voor* a *en* b *gelden dat*

$$\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2 \text{ en dus } a^2 = 2b^2$$

Hieruit volgt dat a^2 *een even getal is, en dus* a *zelf ook:* $a = 2c$ *voor zeker geheel getal* c. *Hiermee geldt weer*

$$a^2 = (2c)^2 = 4c^2 = 2b^2 \text{ en dus } b^2 = 2c^2$$

Hieruit volgt dat b *ook even is, wat in tegenspraak is met dat* a *en* b *geen gemeenschappelijke delers groter dan* 1 *hebben.* $\sqrt{2}$ *kan dus geen breuk zijn.*

- *Een getal dat niet te schrijven is in een verhouding (ratio) tussen gehele getallen noemen we* irrationaal.
- *De verzameling van* rationale *en* irrationale *getallen tezamen is* $\mathbb{R}$*: de verzameling van de* reële *getallen. Omdat in deze verzameling geen 'gaten' zitten spreken we ook over de* reële rechte *of* reële lijn.
- *Een* interval *van reële getallen is een continu deel van de reële rechte. Intervallen kunnen de volgende vormen aannemen:*

  $\langle \leftarrow, a \rangle$ *Alle reële getallen kleiner dan* a

  $\langle \leftarrow, a]$ *Alle reële getallen kleiner dan of gelijk aan* a

  $\langle a, b]$ *Alle reële getallen groter dan* a *en kleiner dan of gelijk aan* b

  Het moge duidelijk zijn wat $\langle a, b \rangle, [a, b], [a, b \rangle, \langle a, \rightarrow \rangle$ *en* $[a, \rightarrow \rangle$ *beduiden.*

P 1.

GEORG CANTOR

1845 — 1918

Grondlegger van de verzamelingentheorie.

Verschillende soorten oneindig?

Er zijn veel verzamelingen met oneindig veel elementen. Denk aan $\mathbb{N}_+$, of het aantal punten van een lijn of een vlak, of het aantal mogelijke manieren waarop we een kromme in een vlak kunnen tekenen. Moeten we die allemaal als even groot beschouwen, allemaal even oneindig? Of zijn we dan als de primitieve cultuur die beweert dat $5 = 6 = 7 =$ *veel*.

Uiteindelijk is het Cantor geweest die inzag dat dit laatste inderdaad het geval is. Er zijn vele verschillende soorten oneindig zijn die we allemaal kunnen onderscheiden. Het is zelfs zo dat er oneindig veel verschillende soorten oneindig zijn, waarbij men zich weer kan afvragen: “Hoe oneindig veel dan?”

We zijn dus op een punt aangeland dat we het veel preciezere begrippen apparaat van de wiskunde moeten gaan gebruiken omdat ons gezond verstand ons hier in de steek laat. Cruciaal daarbij is weer het begrip bijectie, een afbeelding tussen twee verzamelingen die de elementen één aan één relateert. Bijecties kunnen ook bestaan tussen oneindig grote verzamelingen. Ook al kunnen we het aantal elementen niet meer tellen, het bestaan van een bijectie tussen twee verzameling legt wel vast dat ze evenveel elementen bevatten. We spreken dan van gelijke *cardinaliteit*.

TECHNIEK 3.

Cardinaliteit

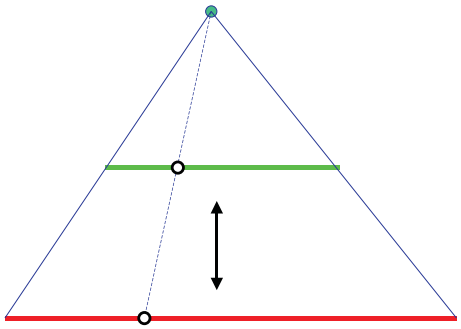
- *Als er tussen twee verzamelingen A en B een bi-jectie bestaat noemen we die twee verzamelingen* gelijkmachtig *, of zeggen dat ze* gelijke cardinaliteit *hebben. We schrijven ook $A \leftrightarrow B$ en concluderen $|A| = |B|$.*
- *We schrijven $|A| \leq |B|$ indien er een injectie $f : A \to B$ bestaat, en $|A| < |B|$ betekent dan dat $|A| \leq |B|$ en tegelijkertijd $|A| \neq |B|$. In het laatste geval heeft A kleinere cardinaliteit dan B.*

Laten we eerst nog wat concrete voorbeelden geven van oneindige verzamelingen. Ons eerste voorbeeld was de verzameling $\mathbb{N}_+ = \{1, 2, 3, \ldots\}$ van positieve gehele getallen. Dit is in ieder opzicht het eenvoudigste en belangrijkste voorbeeld. Een gerelateerd voorbeeld is $\mathbb{N}_+^2$, de verzameling van paren positieve gehele getallen zoals $(1, 1)$, $(1, 2)$, $(35, 276)$ etc. Andere bekende oneindige verzamelingen zijn $\mathbb{Z}$, bestaande uit alle positieve en negatieve gehele getallen inclusief nul, en $\mathbb{Q}$, de verzameling van alle breuken.

T. 2 ⟸ 14

Een belangrijke oneindig grote verzameling met een geheel ander karakter dan de vorige voorbeelden is de reële getallenlijn $\mathbb{R}$. De oneindig lange lijn bestaat uit alle reële getallen en we kunnen ons afvragen hoeveel punten deze lijn bevat. Hier komen we al direct voor een verrassing te staan. Stel we bekijken een eindig lijnstukje, zeg het interval $\langle 0, 1\rangle$ dat alle punten x bevat met $0 < x < 1$. Stel dat we dit interval in tweeën knippen en alleen de onderste helft $\langle 0, \frac{1}{2}\rangle$ behouden. Liggen er minder punten op het halve interval $\langle 0, \frac{1}{2}\rangle$ dan op het hele interval $\langle 0, 1\rangle$? Hiertoe moeten we twee oneindige verzamelingen vergelijken. Intuïtief zijn er tweemaal zoveel punten op het lange interval dan het korte interval, maar hoeveel is tweemaal oneindig?

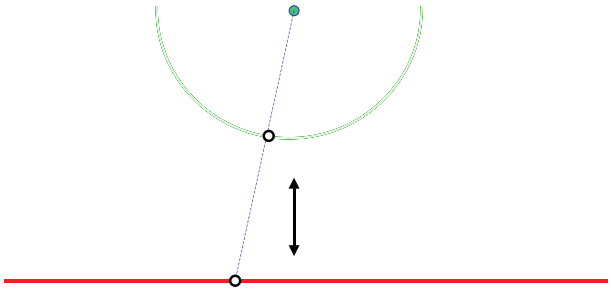
Als we bovenstaande definitie gebruiken komen we tot de onherroepelijke conclusie dat het aantal punten op beide intervallen gelijk moet zijn. Het is niet moeilijk de gevraagde bijectie te maken. We geven de constructie in een figuur weer:



Hier projecteren we de punten van het korte interval één op één op die van het lange interval en stellen vast dat er daarom evenveel punten liggen op het korte als het lange interval. Het is duidelijk dat we deze constructie kunnen herhalen voor intervallen van willekeurige lengte. We komen daarmee tot de conclusie dat alle intervallen dezelfde cardinaliteit hebben. De projectie is niks anders dan een bijectie tussen de punten op de twee lijnstukken.

Maar hoe zit het met de oneindig lange rechte $\mathbb{R}$ zelf? Verrassend genoeg bevat deze evenveel punten als een interval. Ook dit kan het beste grafisch worden uitgelegd met een kleine variatie van de bovenstaande projectie. We buigen het interval tot een halve cirkel en projecteren nu vanuit het

middelpunt de punten van deze cirkelboog op de lijn.[1]



We hebben hier te maken met een verzameling waarvan onderdelen ‘even groot’ kunnen zijn als het geheel. Dit kan duidelijk alleen als de verzameling oneindig is, en dat is een verschijnsel dat we nog vaker zullen tegenkomen.

Er zijn nog ‘wildere’ voorbeelden van oneindig grote verzamelingen te bedenken. Bijvoorbeeld de verzamelingen van alle deelverzamelingen van het vlak. Als we de punten die in de deelverzameling zitten zwart kleuren en de andere punten wit, dan kunnen we hierover nadenken als de verzameling van alle mogelijke tekeningen op een vel papier. We komen hier nog op terug.

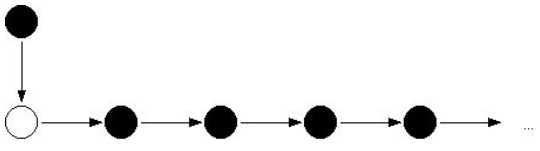
Hilbert’s hotel

Wat gebeurt er met een oneindig grote verzameling als we daar één extra element aan toevoegen? Is dit de beroemde druppel op de gloeiende plaat?

Deze vraag wordt beantwoord in het befaamde voorbeeld van Hilbert’s hotel. Om de merkwaardige eigenschappen van het begrip oneindig duidelijk te maken kwam Hilbert met het elegante voorbeeld van een hotel met oneindig veel kamers, ieder genummerd met een natuurlijk getal $n \in \mathbb{N}_+ = \{1, 2, 3, \ldots\}$. $\overset{\text{P. 2}}{\Longrightarrow}$ 18

Stel het hotel is volledig volgeboekt. Alle kamers zijn bezet. Wiskundig gesteld: er is een bijectie tussen de verzameling kamers en de verzameling gasten. Nu verschijnt er een extra gast. Kunnen we nog plaats vinden voor deze vreemdeling?

De gast beweert van wel. Er is altijd nog een plaats vrij te maken, en wel als volgt. De gast van kamer 1 verhuist naar kamer 2, de gast van kamer 2 verhuist naar kamer 3, enzovoort. Er is dus een simpel algoritme: de gast van kamer n verhuist naar kamer $n + 1$, en dat voor alle n. Als deze boodschap duidelijk gecommuniceerd wordt en alle gasten tegelijkertijd en gedisciplineerd verkassen, dan kan de hele verhuisoperatie snel geschieden. Zo komt kamer 1 vrij waar de extra gast rustig zijn intrek in kan nemen.



Het moge duidelijk zijn dat dit proces nog een flink aantal keren herhaald kan worden. Kan het hotel ooit echt vol zijn? Is er een reisgezelschap dat we niet kunnen plaatsen?

[1] Let wel, het ombuigen van het lijnstuk is ook bijectie. We hebben hier dus eigenlijk de samenstelling van twee bijecties gebruikt, wat gegarandeerd altijd weer een nieuwe bijectie oplevert (zie T.1).

P 2.

David Hilbert *was in zijn tijd absoluut de leidende wiskundige in de wereld. Vanuit het slaperige Duitse universiteitsstadje Göttingen, toen het centrum van het wiskundig universum, bestreek hij alle gebieden van de wiskunde. We zullen hem nog uitvoerig tegenkomen als we komen te spreken over de problematiek rond de fundamenten van de wiskunde. Hij voerde hierin de formalistische school aan die een streng axiomatische aanpak voorstond.*
In 1900 formuleerde Hilbert, tijdens een belangrijk wiskundig congres in Parijs, drieëntwintig richtinggevende problemen waar de wiskunde zich in de twintigste eeuw mee bezig zou moeten houden. Sommige problemen werden tegen zijn verwachting in heel snel opgelost. Eén daarvan is de 'volledigheidskwestie' die we in hoofdstuk 4 uitvoerig zullen bespreken. Kurt Gödel bewees in de dertiger jaren van de vorige eeuw dat, tegengesteld aan Hilbert's verwachtingen, dat een volledige axiomatisering van de wiskunde niet mogelijk is.
Andere problemen kostten meer tijd, en er zijn ook problemen uit Hilbert's lijst die nog open staan. Sommige zijn zelfs zo breed geformuleerd dat getwijfeld kan worden of er ooit wel een oplossing gegeven zal worden.

DAVID HILBERT

1862 — 1943

Via de verhuisoperatie vinden we dat de verzamelingen $\{1, 2, 3, \ldots\}$ en $\{2, 3, 4, \ldots\}$ dezelfde cardinaliteit hebben. De bijectie die de elementen op elkaar afbeeldt is eenvoudig

$$n \mapsto n + 1.$$

Als we ∞ (Romeins symbool voor 1000) schrijven voor de cardinaliteit van $\mathbb{N}$ dan hebben we symbolisch de formule

$$\infty + 1 = \infty.$$

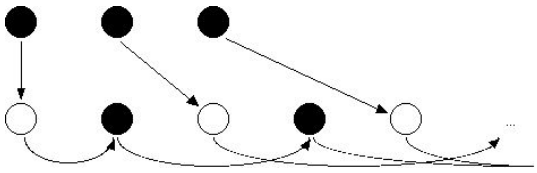
Als een verzameling dezelfde cardinaliteit heeft als $\mathbb{N}$ noemen we deze *aftelbaar oneindig*.

Hilbert breidt uit

Hilbert's hotel is een groot succes, en hij besluit een tweede hotel als dependance te bouwen, ook met aftelbaar oneindig veel kamers. Het is hoogseizoen en beide hotels zijn volledig vol geboekt. Helaas is het tweede hotel door een onbetrouwbare aannemer gebouwd en de inspectie sluit de bouwval met onmiddellijke ingang. Kunnen alle gasten die nu in eens op straat komen te staan geplaatst worden in het eerste hotel, ook al is dat volledig vol?

Jawel, we kunnen genoeg ruimte maken door de gasten als volgt te laten verhuizen. De gast van kamer 1 gaat naar kamer 2, de gast van kamer 2 naar kamer 4, en in het algemeen gaat de gast van kamer n naar kamer $2n$. Na deze actie zijn alleen de even kamers bezet, en zijn alle oneven kamernummers leeg. In deze lege kamers met oneven nummers kunnen nu de gasten van het tweede hotel gehuisvest worden: gast 1 gaat naar kamer 1, gast 2 naar kamer 3, en gast m verhuist naar kamer

$2m - 1$.



Hierboven staat de het integratie-procédé van de nieuwe gasten nog eens verbeeld voor de eerste drie nieuwe binnenkomers.

Daarmee is de inhoud van twee hotels in één hotel geplaatst en Hilbert realiseert zich dat de uitbreiding helemaal niet nodig was geweest. Alle verdere expansieplannen gaan dan ook in de ijskast want het is niet moeilijk in te zien dat op soortgelijke wijze de inhoud van 3, 4, of meer hotels ook in een enkel hotel geplaatst kan worden.

Wat we in dit voorbeeld gezien hebben is dat er in het bijzonder evenveel (positieve) getallen zijn als even getallen. De twee verzamelingen $\{1, 2, 3, \ldots\}$ en $\{2, 4, 6, \ldots\}$ worden op elkaar afgebeeld via de bijectie

$$n \mapsto 2n.$$

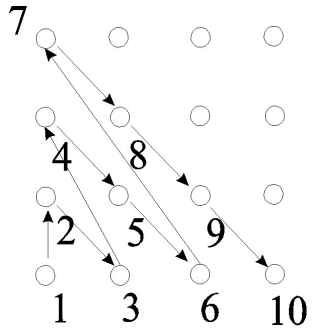
Dit is enigszins tegennatuurlijk omdat intuïtief de even getallen de helft vormen van alle getallen. Het lijkt erop dat we toch over oneindigheid als een of ander groot getal denken, analoog aan de kwantiteit *veel* in het primitieve telsysteem. Elke bovengrens voor de gehele getallen, hoe duizelingwekkend groot gekozen ook, had de verhuisoperatie van hierboven niet toegelaten. Symbolisch kunnen we na de bevindingen van hierboven de volgende gelijkheid noteren

$$2 \cdot \infty = \infty.$$

Maar Hilbert laat het er niet bij zitten. Hij is er nu van overtuigd dat uitbreiding met een *eindig* aantal hotels niet zinvol is, maar hij heeft nu een *oneindige* keten van hotels laten bouwen. Om precies te zijn een aftelbaar oneindig lange keten van hotels, genummerd $1, 2, 3, \ldots$. Al deze hotels zijn volledig volgeboekt. De gasten worden nu genummerd door twee natuurlijke getallen. Het paar (n, m) geeft de gast aan in kamer n van hotel m. De verzameling kamers is dus nu $\mathbb{N}_+^2$.

Is het mogelijk dat ook deze expansie een zinloze verspilling van beton is geweest? Kunnen alle gasten van alle hotels weer in één hotel geplaatst kunnen worden? Hiertoe moeten we aantonen dat de verzamelingen $\mathbb{N}_+$ en $\mathbb{N}_+^2$ even groot zijn.

De methode kan het beste in een figuur worden weergegeven. Hfet is een pad dat langs de diagonalen stelselmatig alle paren afloopt.



Op deze wijze tellen we de paren getallen systematisch af als[2]

$$(1,1),\ (1,2),\ (2,1),\ (1,3),\ (2,2),\ (3,1), \ldots$$

[2]Voor de lifehebber: laat zien dat gast (n, m) gaat naar kamer $\frac{1}{2}(n + m - 1)(n + m - 2) + n$.

Op deze wijze hebben we gevonden dat

$$\infty \cdot \infty = \infty.$$

Een zelfde soort truc kunnen we uithalen voor alle drietallen van positieve gehele getallen, en we leren dan dat ook $\infty^3 = \infty$ en $|\mathbb{N}_+^3| = |\mathbb{N}_+|$. En weer generaliserend geldt dit ook voor alle n-tallen, en dus

$$\infty^n = \infty \text{ voor elke } n.$$

Het voorbeeld voor paren hierboven leert ons tussendoor ook nog dat de verzameling van breuken even groot is als $\mathbb{N}_+$. Tenslotte zijn breuken niks anders als paren gehele getallen van deler en noemer.

Cantor's diagonaalargument

T. 4 ⟹ 22

We kunnen ons nu aanvragen of iedere oneindige verzameling altijd *aftelbaar* — even groot als $\mathbb{N}_+$ — is. Zou er voor elke oneindige verzameling een bijectie naar $\mathbb{N}_+$ bestaan? Dit blijkt *niet* het geval en het belangrijkste tegenvoorbeeld wordt gegeven door het volgende bijzondere resultaat van Cantor

$$|\mathbb{N}_+| \neq |\mathbb{R}|$$

Dat wil zeggen: het aantal punten op een lijn is wezenlijk meer oneindig dan het aantal natuurlijke getallen. De lijn is daarmee niet aftelbaar, we zeggen overaftelbaar oneindig.

Eerst is het handig via een bijectie de reële rechte $\mathbb{R}$ af te beelden op het open interval $\langle 0, 1\rangle$. We hebben al gezien dat dit gemakkelijk kan.

Hoe moeten we nadenken over een reëel getal in het interval $\langle 0, 1\rangle$? Voor ons bewijs is het nuttig zo'n getal voor te stellen als een (mogelijkerwijs oneindig lange) decimale ontwikkeling, bijvoorbeeld

$$\pi/4 = 0,78539816339744830961566084581987572104929234984378\ldots$$

Alle mogelijke decimale ontwikkelingen met een nul voor de komma vormen de elementen van het interval $\langle 0, 1\rangle$.

Stel nu dat we een bijectie f kunnen vinden tussen het interval $\langle 0, 1\rangle$ en de verzameling $\mathbb{N}_+$. Daarmee kunnen de elementen in $\langle 0, 1\rangle$ geordend worden als

$$r_1, r_2, r_3, \ldots$$

waarbij r_1 gepaard is met het getal 1, r_2 gepaard is met het getal 2, enzovoorts. Ofwel, $f(1) = r_1$, $f(2) = r_2$, etcetera. Bijvoorbeeld, we zouden kunnen hebben dat de uitkomst van dat hypothetische algoritme gegeven is door

$$\begin{aligned}
r_1 &= 0,57659671367455070696 8\ldots \\
r_2 &= 0,13209466182037656084 3\ldots \\
r_3 &= 0,00354610099918544237 8\ldots \\
r_4 &= 0,22431917717165651781 1\ldots \\
r_5 &= 0,17444376915454100101 1\ldots \\
&\ldots
\end{aligned}$$

Laat nu $(x)_m$ onze notatie zijn voor de m-de term in de ontwikkeling van het getal x, dat wil zeggen het cijfer op de m-de plaats achter de komma. In deze notatie zal dus $(r_n)_m$ de m-de decimaal van het

n-de getal r_n aangeven. Als we bijvoorbeeld naar bovenstaande ontwikkeling van het getal r_3 kijken dan zien we dat $(r_3)_5 = 4$ omdat er een 4 staat op de vijfde plaats achter de komma.

Als we al de getallen $r_1, r_2, r_3, \ldots$ onder elkaar zetten krijgen we een oneindig keer oneindige matrix, waar de decimaal $(r_n)_m$ op de n-de rij en de m-de kolom staat. Het eerste stukje van die matrix ziet er als volgt uit, waarbij we alleen de cijfers achter de noteren:

5	7	6	5	9
1	3	2	0	9
0	0	3	5	4
2	2	4	3	1
1	7	4	4	4

Nu komt de geniale inval van Cantor. Definieer een reëel getal s met de eigenschap dat n-de decimaal van s alles mag zijn behalve de n-de decimaal van het getal r_n in onze lijst,

$$(s)_n \neq (r_n)_n$$

Zo'n getal s is eenvoudig te maken, er zijn er zelfs (oneindig) veel. Bijvoorbeeld we kunnen s definiëren door eerst de diagonaal te nemen van de tabel

5	7	6	5	9
1	3	2	0	9
0	0	3	5	4
2	2	4	3	1
1	7	4	4	4

In dit voorbeeld wordt dan het beoogde diagonaalgetal $0,53334\ldots$. Nu kunnen vervolgens ieder decimaal van dit getal met 1 te verhogen waar we modulo 10 werken, zodat $9 + 1 = 0$. Bijvoorbeeld, krijgen we zo

$$s = 0,64445\ldots$$

We kunnen nu beweren dat het getal s een nieuw reëel getal is dat zeker niet op de lijst $r_1, r_2, r_3, \ldots$ staat. Waarom? Hoe dan ook is s niet gelijk aan r_1, want het verschilt in ieder geval in de eerste decimaal met r_1. In ons voorbeeld heeft r_1 daar een 5 staan en in s hebben we daar een 6 van gemaakt. Verder kan s ook niet gelijk zijn aan r_2, want daar verschilt het mee in de tweede decimaal. Meer in het algemeen is Cantors constructie zodanig dat getal s in ieder geval op de n-de plaats met het getal r_n verschilt en het is daarmee ongelijk aan r_n voor alle $n \in \mathbb{N}$.

Het getal van Cantor staat dus niet in de lijst. Maar aangezien het wel een element is van het interval $\langle 0, 1\rangle$, hebben we aangetoond dat het niet mogelijk is een bijectie $\mathbb{N}_+ \to \langle 0, 1\rangle$ te vinden. Iedere mogelijke lijst, hoe compleet die ook geprobeerde is te maken, zal oneindig veel lacunes vertonen. Q.E.D.

Aftelbaar en overaftelbaar

- *Als $A \leftrightarrow \mathbb{N}$ dan is A* aftelbaar oneindig. *We kunnen A 'herbenoemen' met behulp van natuurlijke getallen. Dit wordt ook wel* tellen *genoemd. Deze cardinaliteit is de kleinste vorm van oneindigheid en werd door Cantor $\aleph_0$ gedoopt (zeg 'aleph nul', $\aleph$ is de eerste letter in het hebreeuwse alfabet).*
- *Een* aftelling *van een verzameling A is een rij $x_0, x_1, \ldots$ met $x_i \in A$ voor alle i en als voor elke $x \in A$ geldt dat $x = x_k$ voor zekere k.*
- *Een oneindige verzameling A waarvoor geen bi-jectieve afbeelding naar de natuurlijke getallen bestaat heet* overaftelbaar *(niet te tellen). Er geldt dan $|A| > \aleph_0$.*

Aftelbaar oneindige verzameling zijn bijvoorbeeld de verzamelingen van de priemgetallen, de even getallen, de gehele getallen $\mathbb{Z}$ en ook de rationale getallen $\mathbb{Q}$.
In het algemeen is elke oneindige deelverzameling A van $\mathbb{N}$ aftelbaar oneindig. We kunnen A zelfs aftelling door ze op volgorde te leggen. De passende bi-jectie is dan de functie $f : A \to \mathbb{N}$ met $f(x_i) = i$ voor alle i waarbij x_i het i-de getal is in de genoemde aftelling.
Een aftelling voor een oneindige verzameling A legt direct een injectie $f : A \to \mathbb{N}$ vast. Definieer $f(x) = n$ als n het kleinste getal met $x = x_n$. Het beeld $f[A]$ is oneindig omdat f injectief is. Omdat $f[A] \subseteq \mathbb{N}$ moet volgens het bovenstaande gelden dat $f[A] \leftrightarrow \mathbb{N}$ en aangezien $A \leftrightarrow f[A]$ ook $A \leftrightarrow \mathbb{N}$.

To infinity and beyond?

Met Cantors briljante inval hebben we gezien dat er op z'n minst twee soorten oneindig zijn: het aftelbaar oneindige van de gehele getallen en de overaftelbaarheid van de reële lijn. Is het mogelijk om nog grotere verzamelingen te maken?

Een eerste idee zou kunnen zijn om nu het vlak te bekijken, de ruimte $\mathbb{R}^2$ van paren (x, y) van reële getallen. Intuïtief lijkt het vlak veel meer punten te bevatten dan een lijn. Dit is echter bedrieglijk. Als we praten over een lijn of een vlak dan bedoelen we veel meer dan zomaar een collectie losse punten. De punten hebben ook allerlei interessante relaties tot elkaar. Ze zijn naaste buren, of juist niet. Al deze relaties worden collectief de *topologie* genoemd, en in onze nogal primitieve vraag van 'hoeveel' laten we dit soort aspecten volledig varen.

Het is dan ook zo dat de cardinaliteit van het vlak en de lijn gelijk is. Hoe bizar dat ook mag klinken, we kunnen een bijectie maken tussen de punten van het vlak en de lijn. De afbeelding is niet moeilijk. Laten we voor het gemak een bijectie maken tussen het vierkant en een lijnstuk. Neem een punt in het vierkant. Dit wordt gegeven door een paar getallen (x, y) met $0 < x, y < 1$. Deze getallen hebben ieder een decimale ontwikkeling, bijvoorbeeld

$$\begin{aligned} x &= 0,1171661719919911\ldots \\ y &= 0,9465729565873022\ldots \end{aligned}$$

Aan dit paar getallen (x, y) gaan we nu één reëel getal z toevoegen. We doen dat door de decimale expansie van x te gebruiken voor de oneven decimalen van z en soortgelijk de expansie van y te gebruiken voor de even decimalen van z. De twee reeksen van x en y worden dus in elkaar geritst, zoals op de autobaan we van twee rijbanen naar één rijbaan overgaan[3]. In ons voorbeeld vinden we

[3]In formules: $(z)_{2n-1} = (x)_n$ en $(z)_{2n} = (y)_n$.

dus dat

$$z = 0,191476156762197516\ldots$$

Omgekeerd kunnen we een getal zoals z splitsen in twee reële getallen door alleen de even of oneven decimalen te lezen. Het moet wel duidelijk zijn dat deze afbeelding de getallen van de lijn op een volledig willekeurige manier verstrooit over het vlak. Uiteindelijk zullen de punten van de lijn het vlak overdekken, maar de natuurlijke ordening op de lijn (groter en kleiner) is helemaal verwoest. Twee getallen die dicht bij elkaar liggen op de lijn kunnen zeer ver van elkaar af komen te liggen in het vlak.

Op dezelfde manier vinden dat ook het aantal punten in de drie- of hogerdimensionale ruimte[4] de cardinaliteit van $\mathbb{R}$ blijft houden. Hoe komen we daar voorbij? Niet door naar hogere dimensies te gaan, maar wat dan?

Cantors schilderijententoonstelling

In het diagonaalargument van Cantor zit een prachtige logica die we nog niet goed hebben duidelijk gemaakt. Laten we die nu naar boven brengen, zeker omdat we Cantors argument nogmaals, nauwelijks verhuld, tegen zullen komen als we Turings werk over de onbeslisbaarheid van de wiskunde gaan bespreken in hoofdstuk 4.

Hiervoor is het beter in het binair stelsel te werken, dat wil zeggen een getallenstelsel met alleen de cijfers 0 en 1. Het is geen enkel probleem getallen in dit stelsel op te schrijven. Zo is bijvoorbeeld

$$1/4 = 0,01.$$

en ons favoriete voorbeeld van een reëel getal in het interval $\langle 0, 1\rangle$ ziet er nu uit als

$$\pi/4 = 0,11001001000011111101101010100 0\ldots$$

We kunnen nu iedere stap van Cantors bewijs herhalen in dit nieuwe stelsel. Het enige verschil is dat de matrix waarvan we uiteindelijk de diagonaal beschouwen opgebouwd is uit alleen 0-en en 1-en.

Maar deze nieuwe notatie brengt een conceptueel voordeeltje. Er is nu een andere manier om naar een reëel getal x te kijken. De n-de 'decimaal' $(x)_n$ is nu of 0 of 1. Dat wil zeggen voor ieder natuurlijk getal n moeten we een binaire keuze maken. We krijgen een 0 of een 1 op de n-de plaats in de binaire ontwikkeling. Bekijk nu die posities n waarvoor dit cijfer een 1 is. In het bovenstaand voorbeeld van $x = \pi/4$ vinden we zo de volgende verzameling van waarden van n

$$\{1, 2, 5, 8, 13, 14, 15, 16, \ldots\}$$

omdat er 1-en staan op de eerste, tweede, vijfde, achtste, etc. plaats. Dit geeft een deelverzameling van $\mathbb{N}_+$. Omgekeerd kunnen we met iedere deelverzameling van $\mathbb{N}_+$ een reëel getal x construeren. Het heeft alleen een 1 op de n-de plaats als n een element van de deelverzameling is. Op alle andere plaatsen staat een nul. Daarmee hebben we een volstrekt nieuwe interpretatie gevonden van een reëel getal. We kunnen dat ook opvatten als een deelverzamelingen van $\mathbb{N}_+$. Daarmee is de verzameling $\mathbb{R}$ van reële getallen geïnterpreteerd als de verzameling van deelverzamelingen van $\mathbb{N}_+$. Dit heet technisch gesproken de *machtsverzameling* van $\mathbb{N}_+$, notatie $\wp(\mathbb{N}_+)$.

We kunnen daarmee de stap van $\mathbb{N}_+$ naar $\mathbb{R}$, waarmee we ons van het kleinste niveau van oneindig naar de overtreffende trap hebben getild, opvatten als de overgang van de verzameling $\mathbb{N}_+$ naar zijn machtsverzameling.

[4] Voor de fijnproevers, zelfs een ruimte van (aftelbaar) oneindig veel dimensies heeft de cardinalieit van $\mathbb{R}$.

Een machtsverzameling is niet zo'n vreemd object. Stel dat we met een eindige groep mensen te maken hebben. Dan bestaat de machtsverzameling uit alle mogelijke ensembles die we uit die groep kunnen samenstellen, alle mogelijke combinaties die een team kunnen vormen. Dat kan variëren van niemand (de lege verzameling) tot iedereen (de verzameling zelf), en ieder ander mogelijke combinatie daartussen in. Als de groep uit n personen bestaat dan zijn er 2^n mogelijke deelverzamelingen. Namelijk, voor ieder persoon moeten we beslissen of die wel of niet onderdeel van de groep zal zijn. Dat geeft

$$\underbrace{2 \times 2 \times 2 \cdots \times 2}_{n} = 2^n$$

mogelijkheden. We kunnen dus nu abstract de cardinaliteit van de reële lijn schrijven als

$$|\mathbb{R}| = 2^{\infty}.$$

Nu we Cantors argument in deze ruimte zin hebben geformuleerd en begrepen, kunnen we de truc gaan herhalen en grotere en grotere verzamelingen maken door de steeds de machtsverzameling te nemen van de voorafgaande stap. Op deze wijze kunnen we voorbij de cardinaliteit van $\mathbb{R}$ komen. De volgende stap is namelijk de verzameling van alle deelverzamelingen van de reële lijn. Om zo'n deelverzameling te geven moeten we van ieder punt x in $\mathbb{R}$ aangeven of deze 'in' of 'uit' is. Dat kunnen we doen met een functie $f(x)$ die de waarde 0 of 1 aanneemt. De deelverzameling bestaat dan uit alle punten x met $f(x) = 1$. Anders gezegd, de verzameling van alle afbeeldingen $\mathbb{R} \to \{0, 1\}$ heeft een cardinaliteit groter dan $\mathbb{R}$.

We kunnen ons dit nog wat plastischer voorstellen als we in plaats van de lijn het vlak nemen. Een deelverzameling kan nu opgevat worden als een voorschrift op de punten van het vlak wit of zwart te kleuren. Daarmee krijgen we een (oneindig verfijnde) tekening. De volgende stap in onze reeks oneindigheden is dus de verzameling van alle schilderijen, met oneindig fijne details[5].

Wat moeten we ons bij de volgende stap voorstellen? Wel, nu hebben we te maken met een deelverzameling van alle mogelijke schilderijen. Dat wil zeggen een tentoonstelling. De verzameling van alle mogelijke mathematische schilderijententoonstellingen is een mooie metafoor voor de volgende trap van oneindigheid!

[5] Bijna al deze schilderijen zullen zeer abstract zijn!

TECHNIEK 5.

Machtsverheffing

We kunnen blijven 'machtsverheffen' en steeds zal de cardinaliteit van nieuwe machtsverzamelingen toenemen. We eindigen met de stelling die dit formuleert. De formalisering van van bijectie en cardinaliteit stelt ons in staat dit in een paar regels te bewijzen.

Stelling *Voor elke verzameling A geldt dat $|A| < |\wp A|$.*
Bewijs. Voor eindige verzamelingen is dit triviaal. We weten verder al dat $|A| \leq |\wp A|$ dankzij de eenvoudige injectie $a \mapsto \{a\}$. We hoeven dus alleen aan te tonen dat $|A| \neq |\wp A|$, ofwel dat er geen bijectie $f : A \to \wp A$ bestaat.

Stel dat zo'n bijectie f wel zou bestaan. We definiëren dan

$$D_f = \{a \in A \mid a \notin f(a)\}.$$

D_f is de verzameling van alle A-elementen a die niet in hun f-beeld $f(a)$ voorkomen. Omdat aangenomen is dat f een bijectie is moet er een $d \in A$ te vinden zijn zodanig dat

$$f(d) = D_f \quad \textit{want} \quad D_f \in \wp A.$$

Maar nu geldt dat als $d \notin f(d) = D_f$ dan juist wel $d \in D_f$ vanwege D_f's definitie. Maar als $d \in D_f = f(d)$ dan moet weer gelden $d \notin D_f$. Kortom, zo'n d kan niet bestaan en f kan dus onmogelijk een bijectie zijn: $A \not\leftrightarrow \wp A$ ófwel $|A| \neq |\wp A|$. QED

N.B. *De definitie van de verzameling D_f is natuurlijk de crux van het bewijs. Deze komt overeen met de diagonaal-zet in het bewijs dat $|\mathbb{N}| < |\wp\mathbb{N}| = |\mathbb{R}|$ en $|\mathbb{R}| < |\wp\mathbb{R}|$.*

De kleinste vorm van oneindigheid hebben we $\aleph_0$ gedoopt. Met de machtsverzamelingconstructie kunnen we de opvolgers als volgt definiëren:

$$\aleph_{n+1} = 2^{\aleph_n},$$

en er geldt vanwege Stelling 5 dat $\aleph_n < \aleph_{n+1}$ voor alle n. Een geordende oneindige ruimte van oneindigheden!

1.2 Tellen in taal: de vorm van rekenen en redeneren

Dit hoofdstuk begon met een activiteit uit het dagelijkse leven. We tellen onze boodschappen, de postzegels in een album, en soms schaapjes 's avonds in bed. Zelfs kinderen doen dit alles met speels gemak. Maar vanuit deze vertrouwde omgeving abstraheert een wiskundige tot getallen, abstracte objecten met soms buitengewoon verrassende eigenschappen. We arriveerden daarmee in contreien die de alledaagse ervaring ver overstijgen, zoals oneindige verzamelingen en de vele gradaties daarin. In het tweede gedeelte van het onderwerp 'Tellen' volgt zelfs nog een verdere abstractiestap. We gaan nadenken over de manier waarop een wiskundige met getallen omgaat, en ermee rekent en redeneert. Om dat goed in het vizier te krijgen moeten we kijken naar de taal van de wiskunde, de symbolen en de regels voor hun gebruik. Dat lijkt nog veel 'formeler' en geheimzinniger dan gewoon rekenen met getallen. Maar juist de aandacht voor de wiskundige taal brengt ons ook weer terug bij het begin in ons gewone leven. De alledaagse natuurlijke taal die wij gebruiken: Nederlands, Engels, Turks, doordrenkt al onze activiteiten. Sommige geleerden menen zelfs dat taalgebruik de meest kenmerkende eigenschap is van de homo sapiens!

De opzet van dit tweede deel volgt een stramien dat door dit hele boek zal terugkomen. Eerst analyseren we de werkwijze van het voorafgaande wiskundige hoofdstuk, met behulp van technieken uit de logica, de exacte studie van geldig redeneren en andere vormen van informatieverwerking. Daarbij vinden we allerlei begrippen met een bredere strekking, die ook later in dit boek blijven terugkeren. Maar vervolgens leggen we onze bevindingen over de wiskunde naast bekende feiten over natuurlijke taal, alledaags redeneren, en andere cognitieve vermogens van ieder mens. Deze feiten worden doorgaans bestudeerd door taalkundigen, filosofen, of psychologen. Maar ze hebben nog steeds van alles te maken met onze wiskundige vermogens. Deze totale bandbreedte 'van natuur tot cognitie' is de strekking van de titel van dit boek.

Wiskunde beschrijft een wereld van wiskundige objecten, zoals getallen, functies, ruimtes, en andere patronen. Dit is het beeld van de werkende wiskundige, en ook van de meesten van ons als we op school met wiskunde kennismaken. Maar die wiskundige objecten zijn abstract, en niet voor ons zichtbaar zoals mensen, gebouwen, of sterren. Heel veel van de wiskunde zit eigenlijk ook in een manier van doen: werken volgens bepaalde regels, heel precies omgaan met taal en definities. Sommige heel radicale filosofen menen zelfs dat wiskunde in wezen een 'taalspel' is, zonder dat we ook nog gelovige hoeven te zijn in het bestaan van een diepere wereld daarachter. Dat taalspel blijkt het nuttige met het aangename te verenigen, want het werkt in de praktijk en het is elegant en zorgvuldig, en daarom blijven we het doen. Hoe dit ook zij, wiskunde heeft essentieel te maken met werken met symbolen, en een beter begrip daarvan is noodzakelijk om een dieper inzicht te krijgen in wiskundig bewijzen, wiskundige theorievorming, en tegenwoordig ook rekenen en bewijzen op computers. In dit hoofdstuk gaan we daarom kijken naar de taal van de wiskunde. Niet veel mensen houden van grammatica, maar we moeten er toch even doorheen. Dat duurt maar één hoofdstuk, dus in elk geval steekt het gunstig af bij het leren van andere vreemde talen.

Getallen en hun namen

Als we 5 en 4 optellen en 9 verkrijgen dan lijkt het alsof we die drie getallen werkelijk manipuleren. Maar eigenlijk weet niemand hoe getallen er *echt* uit zien. Wat we in werkelijkheid in het geval van zo'n berekening doen is niets meer dan het manipuleren van symbolen. We herschrijven namen tot andere namen voor hetzelfde object. Zulke namen voor het getal 9 zijn bijvoorbeeld:

$$9,\ 5+4,\ 3^2,\ \text{ de unieke } x \text{ zodat } x+1=10,\ \text{IX}$$

De eerste hiervan is een enkelvoudig symbool, de andere vier zijn samengesteld, en benoemen datzelfde getal op verschillende manieren. De meeste bekende namen voor wiskundige objecten zijn doorgaans samengesteld, zoals bij

$$\sqrt{2},\ 12 \text{ of een verzamelingsnotatie als } \{1,5\}$$

Enkelvoudige namen in de wiskunde lijken op grammaticale eigennamen in gewone taal zoals 'Ed van den Heuvel', 'Beatrix van Oranje-Nassau', terwijl samengestelde namen lijken op omschrijvingen als 'de eerste Spinoza-premie winnaar aan de UvA' of 'de koningin van Nederland'. Soms kennen we niet eens een eigennaam voor een object, zoals bij $\sqrt{2}$ of 'de volgende president van de VS'. We hebben de getallen zelf ook helemaal niet nodig om te rekenen, want dat kunnen we heel goed doen met dit soort namen, getuige een algebraïsche omvorming als

$$2 \times (3 + x) = 2 \times 3 + 2 \times x = 2x + 6$$

Je zou notatie een noodzakelijk kwaad kunnen noemen. Om over iets te spreken hebben we namen nu eenmaal nodig om de realiteit om ons heen te benoemen. Maar het is natuurlijk juist de grote kracht van taal dat we over van alles onder de zon kunnen denken en spreken zonder al die voorwerpen er letterlijk bij te hoeven slepen.

Overigens heeft niet elk object een naam. Het lijkt niet zinvol om alle blaadjes in een boom, of de tegels in een straat, aparte eigennamen te geven, en dat doen we dan ook niet. Een wiskundig voorbeeld van anonimiteit zijn de reële getallen. Een gewone taal heeft op zijn best aftelbaar oneindig veel namen en beschrijvingen beschikbaar, en dat zijn er, zoals we in 1.1 hebben aangetoond, te weinig om elk reëel getal te benoemen.[6] Om over anonieme objecten toch te kunnen spreken hebben we andere middelen dan namen nodig. Een zeer sprekend voorbeeld hiervan is de 'kwantificatie' die in dit hoofdstuk uitgebreid aan bod zal komen.

Het nut van goed gekozen wiskundige notatie kan niet overschat worden. Het dient de precisie in het rekenen en bewijzen, en evenzo het overzicht. Eén enkele notatie kan heel compact een algemeen feit weergeven, zoals de formule

$$x + y = y + x$$

die de zogenaamde 'commutativiteit' van de optelling van getallen uitdrukt: in beide volgordes levert optellen hetzelfde resultaat. Hierbij gebruikten we variabelen om een algemeen principe te stellen. De introductie van de variabelen in de wiskundige taal heeft de wiskunde en natuurwetenschappen indertijd in een enorme versnelling gebracht. De wiskunde handelt over abstracte ontastbare, en vaak ook niet aanwijsbare, objecten. De intellectuele lenigheid en vindingrijkheid in de wiskunde zit hem dan ook vaak in de wiskundige taalvaardigheid.

We gaan in het vervolg van dit hoofdstuk nader in op twee onderwerpen: de structuur van die wiskundige taal, en een vergelijking met onze eigen *natuurlijke* taal.

Taal, betekenis en abstractie

In de taalkunde maakt men een fundamenteel onderscheid tussen taalvorm en betekenis. De vorm is de constructie, waarover we dingen kunnen zeggen als

'Haarlem' heeft zeven letters,

'Niemand' is onderwerp in "Niemand weet de oorzaak van de ramp".

[6] Een prachtig literair effect van ontbreken van een naam zien we in Umberto Eco's roman 'De Naam van de Roos'. Nooit komt de monnik Adson achter de ware naam van zijn geliefde.

De betekenis heeft te maken met de objecten, of meer algemeen, de werkelijkheid die wordt aangeduid door de taalvorm. Men spreekt in de taalkunde over *syntaxis*, de vormleer, en *semantiek*, de betekenisleer. Met zuivere syntaxis hebben we in het gewone leven zelden te maken omdat we de betekenis van onze taal als kind al geleerd hebben. We krijgen de werkelijkheid die aan de taal zit vastgehecht al met de paplepel ingegoten. We herinneren het ons nauwelijks, maar die betekenis moest eerst wel worden geleerd. In het geval van talen die ons minder eigen zijn is dit onderscheid veelal duidelijker. We komen dan wel betekenisloze taalvormen tegen, zoals een krant in een vreemde taal bij de krantenkiosk op het Centraal Station of een wiskundige notatie die nieuw voor ons is. Wiskunde is juist vaak sterk syntactisch gericht, vooral omdat er vaak ook een omgekeerd proces van betekenis leren plaats vindt. Beginnend met een vorm met een vaste betekenis vindt 'onthechting' plaats, waarbij we steeds abstracter denken over hetgeen wordt uitgedrukt. Neem eens dit specifieke feitje over twee specifieke getallen:

$$3 + 4 = 4 + 3$$

We kunnen hier steeds meer elementen variabel maken en we krijgen dan bijvoorbeeld

$3 + y = y + 3$	commutativiteit van 3 bijtellen
$x + y = y + x$	commutativiteit van de optelling
$fxy = fyx$	commutativiteit van willekeurige functie f
$t_1 = t_2$	gelijkheid tussen twee willekeurige namen
$R(fxy, fyx)$	relatie tussen functiewaarden met verwisselde argumenten

Steeds verdergaande abstractie laat ons nadenken over steeds algemenere begrippen. Dit raakt steeds verder verwijderd van de oorspronkelijke concrete situatie, maar in ruil daarvoor geldt de regel:

Hoe abstracter, hoe meer toepassingen!

Immers, één enkele taalvorm kan vele concrete betekenissen hebben, afhankelijk van hoe we de symbolen in die vorm interpreteren als concrete objecten in concrete situaties. Zo kan $x + y = y + x$ ook gelezen worden met x, y als verzamelingen, en $+$ als de zogenaamde vereniging: het bij elkaar nemen van alle objecten in twee verzamelingen tot één nieuwe. In dat geval wordt door $x + y = y + x$ de commutativiteit van vereniging uitgedrukt, dat wil zeggen, het doet er niet toe in welke volgorde we die operatie van samennemen van twee verzamelingen uitvoeren. Soms zijn die andere lezingen heel verrassend. Bekijk bijvoorbeeld de bekende formule die de distributiviteit weergeeft van vermenigvuldiging over optelling:

$$x \times (y + z) = (x \times y) + (x \times z)$$

Als we x, y en z hier als verzamelingen lezen, $+$ als de operatie van vereniging, en $\times$ als doorsnede, dan staat hier een wet van de verzamelingenleer.[7] Maar ook heel andere interpretaties zijn denkbaar. Lees bijvoorbeeld $x \times y$ als het minimum van getallen x, y en $x + y$ als het maximum van x en y. Ook dan is de vergelijking van hierboven weer een waar feit over getallen:

$$\max\{x, \min\{y, z\}\} = \min\{\max\{x, y\}, \max\{x, z\}\}.$$

Overigens, laten we het maar eerlijk toegeven, al deze overwegingen zijn voor veel zuiver wiskundigen ondergeschikt aan hun streven naar esthetiek. Het echte motief is vaak "hoe abstracter, hoe

[7] Zie T. 9 op pag. 40 voor een rechtvaardiging van deze vergelijking.

mooier!". Dit is een belangrijk cultuurverschil en ook vaak een bron van onenigheid tussen wiskundigen en experimentele wetenschappers. Toch is vaak gebleken dat abstracte theorieën, die aanvankelijk door wiskundigen opgezet werden ter harmonisering van hun bevindingen en door buitenstaanders gezien werden als abstracte zweverigheid, uiteindelijk zeer toepasbaar waren. Een heel sterk voorbeeld is de groepentheorie die in het volgende hoofdstuk aan bod komt.

Formele symbolische talen komen ook elders in de wetenschap voor. Hedendaagse prominente voorbeelden zijn natuurlijk de programmeertalen in de informatica. Maar de taal van de wiskunde is wel de rijkste. Hieronder bekijken we de *structuur* van die taal nader: de grammatica. De grammatica van de wiskunde past op één pagina! Desnoods kunt u hem opvouwen om hem voor altijd op zak te hebben.

Grammatica van de wiskundige taal

Er bestaat geen officieel grammaticaboek van de wiskunde. Maar we kunnen wel kijken naar wat met name de logici hebben ontworpen aan taalvormen in hun studies van de structuur van wiskundige theorieën en bewijzen. Dan komen met name de volgende patronen naar voren, die in veel logische formalismen centraal staan. In T. 6 vindt u de formele definitie van deze taal, die in de logica bekend staat als de *predicaatlogische* taal.

Namen van wiskundige objecten Om te beginnen hebben we namen nodig voor wiskundige objecten. Zoals we al zagen vallen die uiteen in enkelvoudige en samengestelde namen. Het precieze vocabulaire werkt als volgt:

eigennamen	$0, 1, \pi, \ldots$
variabelen	$x, y, z, \ldots$
functiesymbolen	$+, \times, \ldots f, g, \ldots$
samengestelde termen	$3^2, \sqrt{(x+2y)}, \ldots, f(x, g(y)), \ldots$

In de praktijk gebruiken we de zogenaamde *infix*-notatie (ertussen) in plaats van de *prefix*-notatie (ervoor) voor functie-symbolen. In plaats van $+(x, y)$ of $+xy$ schrijven we $x + y$. Soms wordt zelfs expliciete referentie naar de functie weggelaten zoals in $2y$ en 3^2.

Basisbeweringen Als we eenmaal namen van objecten hebben, dan kunnen we beweringen doen. Typische eenvoudige wiskundige beweringen zijn

$t_1 = t_2$	gelijkheid
$t_1 < t_2$	kleiner dan
$x \in y$	element van

allemaal binaire relaties met twee objecten, of

x ligt tussen y en z

een ternaire relatie tussen drie meetkundige objecten. Vergelijk in natuurlijke taal de transitieve werkwoorden in "Marie zingt de Marseillaise" (binair) en "Marie geeft een stuk van Rolland aan Jan" (ternair). De algemene vorm van dergelijke basisbeweringen is een relatie-symbool plus een passend aantal namen van objecten:

$$R(t_1, \ldots, t_k)$$

met k het aantal argumenten van de relatie. In de praktijk gebruiken we voor binaire relaties weer vaak de infix-variant. Bijvoorbeeld:

$$x + 2y < y^2 \times z$$

In dit voorbeeld is $<$ de relatie in standaard infix-notatie (er tussen in) en zijn $x + 2y$ en $y^2 \times z$ de samengestelde termen waartussen de relatie wordt vastgesteld.

Dit werkt net zo voor verzamelingen en andere objecten:

$$x^2 \in A \cup B$$

Hier is $\in$ de relatie en x^2 en $A \cup B$ samengestelde termen.

Connectieven Echte wiskundige taal ontstaat pas doordat we met deze eenvoudigste beweringen samengestelde uitdrukkingen maken. Een heel bekende manier is zinscombinatie met ontkenningen, conjuncties, implicaties, en andere 'Boolese operatoren' die positieve of negatieve verbanden leggen:

$\neg$	niet	negatie
$\wedge$	en	conjunctie
$\vee$	of	disjunctie
$\rightarrow$	als... dan...	implicatie
$\leftrightarrow$	dan en slechts dan als	equivalentie

Dit zijn als het ware de voegwoorden — de technische term is connectieven — van de wiskunde.

Een voorbeeld van Boolese structuur zien we als we een ambigue uitdrukking uit onze gewone taal eenduidig wiskundig willen schrijven. Hier zijn twee verschillende betekenissen voor "geen oude mannen of vrouwen":

$$\neg((O \wedge M) \vee V) \quad \neg(O \wedge M) \vee V$$

Overigens er zijn nog meer van zulke lezingen. Probeert u zelf eens de alle betekenissen te achterhalen van de zin "Ik zag geen oude mannen of vrouwen".

Kwantoren Wiskundigen willen spreken over alle objecten in een bepaald domein, zoals getallen, zelfs als die niet alle een naam hebben! Hiertoe dienen de volgende uitdrukkingen van hoeveelheid:

Alle	$\forall x\, \varphi(x)$	Alle x voldoen aan φ
Een	$\exists x\, \varphi(x)$	Minstens één x voldoet aan φ

Hiermee kunnen we weer andere verwante uitdrukkingen definiëren, zoals

Geen	$\neg\exists x\, \varphi(x)$	Geen enkele x voldoet aan φ

De kracht van deze notatie schuilt met name in herhaalde kwantoren, zoals

$\forall x\, \exists y\, x < y$	Bij elk getal is er een groter getal
$\exists x\, \neg\exists y\, y < x$	Er is een kleinste getal

Omgekeerd kunnen we nu allerlei belangrijke wiskundige eigenschappen heel precies opschrijven. Een voorbeeld is de *dichte* ordening van de reële getallen die inhoudt dat tussen elk tweetal verschillende reële getallen een derde getal te vinden is:

$$\forall x\, \forall y\, (x < y \rightarrow \exists z(x < z \wedge z < y))$$

Lezen en schrijven Net als bij gewone talen moet je voor wiskundige taal woordjes leren en een paar grammaticaregels. Gelukkig zijn er maar heel weinig van die regels. Daarna kunt u al aan de slag. Een voorbeeld van 'schrijven' is definiëren van rekenkundige begrippen. Bijvoorbeeld, in een rekenkundige taal met vermenigvuldiging $\times$ kunnen we "x is een priemgetal" als volgt definiëren, waarbij de logische structuur van getalsnamen, basisbeweringen, Boolese operaties en kwantoren in zo'n begrip stapsgewijs duidelijk wordt. Eerst een tweetal hulpbegrippen

$$\begin{array}{ll} x \text{ deelt } y & \exists z\, x \times z = y \\ x = 1 & \forall z\, x \times z = z \end{array}$$

Dan nu de gevraagde definitie zelf:

$$x \text{ is een priemgetal} \quad \forall u\,(u \text{ deelt } x \to (u = x \vee u = 1)) \wedge x \neq 1,$$

of helemaal uitgeschreven:

$$\forall u\,(\exists z\, u \times z = x \to (u = x \vee \forall z\, u \times z = z)) \wedge \neg \forall z\,(x \times z = z).$$

Omgekeerd is het nuttig om gegeven abstracte formules vlot te leren lezen. Hier is een voorbeeld uit de abstracte taal van de verzamelingen. De volgende formule drukt het principe uit van de zogenaamde extensionaliteit: twee verzamelingen met dezelfde elementen zijn gelijk:

$$\forall x\, \forall y\, (\forall z\, (z \in x \leftrightarrow z \in y) \to x = y)$$

Hoe lezen we zo'n formule? We zoeken eerst naar deelformules die we makkelijker kunnen begrijpen. Zo zegt $z \in x \leftrightarrow z \in y$ dat iets (z) in x zit dan en slechts dan als het in y zit. De $\forall z$ hieraan voorafgaand stelt dat deze eigenschap geldt voor alle mogelijke elementen. Dit is een wiskundige formulering van de zin "x en y hebben de zelfde elementen". Nu is de formule deels 'genaturaliseerd':

$$\forall x\, \forall y\ (x \text{ en } y \text{ hebben dezelfde elementen} \to x = y)$$

Maar dan spreekt de bewering verder vanzelf. Het is een implicatie over alle verzamelingen, die zegt dat alle verzamelingen die dezelfde elementen hebben gelijk zijn.

Nog zo'n typische formule is het zogenaamde 'machtsverzamelingsaxioma' uit de verzamelingenleer:

$$\forall\, x \exists\, y (\forall z\, (z \in y \leftrightarrow \forall u\, (u \in z \to u \in x))$$

Het deel achter de dubbele pijl zegt dat z een deelverzameling van x is. De hele formule zegt dat er voor elke verzameling (x) een verzameling (y) is die bestaat uit alle deelverzamelingen van de eerstgenoemde.

TECHNIEK 6.

Formele grammatica van de logische taal

We definiëren hier de predicaatlogische taal*, die in onze tekst wordt gebruikt. Zo'n taal heeft een kernrepertoire van vaste logische symbolen, en verder een woordenboek van 'niet-logische symbolen' voor objecten, functies, en predikaten die door de gebruiker zelf kunnen worden gekozen. Tezamen vormen deze* formules *die logisch goed gestructureerde beweringen uitdrukken.*

Niet-logische symbolen

Constanten en variabelen

Functiesymbolen Functiesymbolen dienen om namen van objecten samen te stellen. Elk functiesymbool heeft een positief geheel getal als bijbehorende plaatsigheid*: het aantal argumenten. Constanten vat men vaak op als het grensgeval van 0-plaatsige functiesymbolen.*

Predicaten Elk predicaat heeft een niet-negatief getal als bijbehorende plaatsigheid. Veelal wordt het twee-plaatsige gelijkheidspredicaat $=$ *standaard standaard opgenomen in de logische taal.*

Termen en formules

Termen

Enkelvoudige termen Elke constante en elke variabele is een term*.*

Samengestelde termen Als $t_1, \ldots, t_n$ een n-tal termen zijn en f is een n-plaatsig functiesymbool dan is $f(t_1, \ldots, t_n)$ een (samengestelde) term*.*

Formules

Atomaire formules Een atomaire formule *of kortweg* atoom *ontstaat als volgt. Als $t_1, \ldots, t_n$ termen zijn en P is een n-plaatsig predicaat P, dan is $P(t_1, \ldots, t_n)$ een atomaire formule. Deze formule zegt dat de objecten $t_1, \ldots, t_n$ in die volgorde voldoen aan de relatie aangeduid door P.*

Samengestelde formules

Connectieven Als φ en ψ formules zijn, dan zijn $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ en $(\varphi \leftrightarrow \psi)$ eveneens formules.

Kwantoren Als φ een formule is en x een variabele, dan zijn $\forall x\, \varphi$ en $\exists x\, \varphi$ eveneens formules.

Conventies

De hier genoemde clausules werken 'recursief': men kan ze telkens herhalen om steeds meer complexe termen en formules te schrijven. Doorgaans worden daarbij zo weinig mogelijk haakjes geschreven. In termen en atomaire formules worden vaak alle haakjes weggelaten. Voorts worden twee-plaatsige functie- en predikaat-symbolen vaak tussen hun argumenten ingeschreven (infix), denk aan $+$ en $<$ bij het rekenen, of $\subseteq$ tussen verzamelingen. Verder gebruiken we een voorrangsregel voor negaties en kwantoren. Zij binden sterker dan de binaire connectieven. Bijvoorbeeld, $\forall x\, Px \vee Qx$ staat voor $((\forall x\, Px) \vee Qx)$ en niet voor $(\forall x\, (Px \vee Qx))$.

TECHNIEK 7.

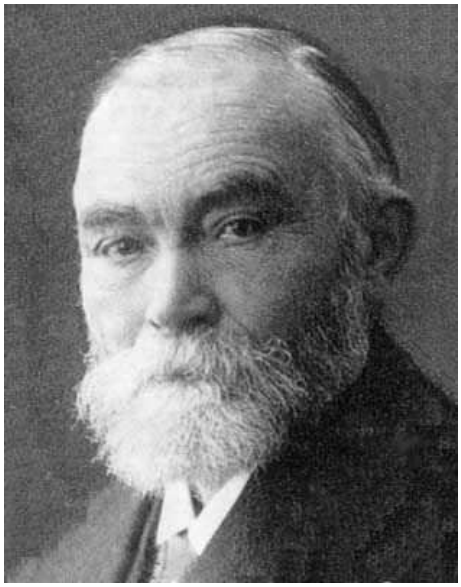
De taal van de natuurlijke getallen

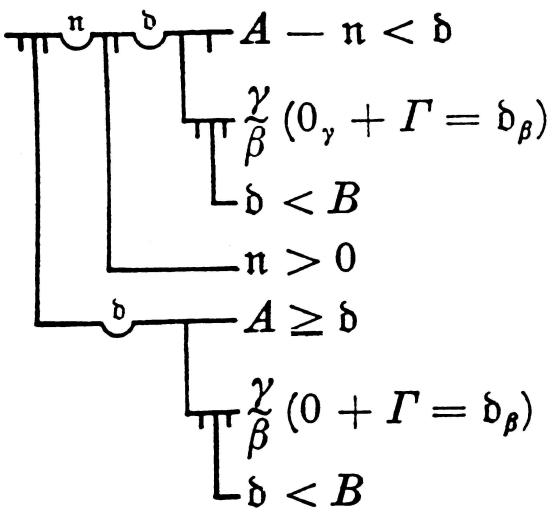
Een veel gebruikte predicaatlogische taal, ook in dit boek, is die van de natuurlijke getallen*. In het niet-logisch vocabulaire kiezen we een beginconstante* 0*, en een één plaatsige opvolgersfunctie* S*, zodat we kunnen tellen. Zo kunnen we elk getal benoemen:* 1 *heet nu* $S(0)$*,* 2 *heet* $S(S(0))$ *etc. Verder gebruiken we twee twee-plaatsige functies: optelling* $+$ *en vermenigvuldiging* $\cdot$ *die we met infix-notatie schrijven tussen hun argumenten in. Predicaten in deze taal zijn gelijkheid* $=$ *en de ordening* $<$ *eveneens met infix-notatie. Haakjes worden onderdrukt met enkele speciale conventies. We schrijven* Sx *in plaats van* $S(x)$ *en gebruiken de schoolrekenregel dat vermenigvuldigen voorrang heeft ten opzichte van optellen:* $x \cdot y + z$ *staat voor* $(x \cdot y) + z$ *en niet voor* $x \cdot (y + z)$*. Tenslotte heeft de opvolgerfunctie voorrang ten opzichte van vermenigvuldiging:* $Sx \cdot y + z$ *staat voor* $((S(x)) \cdot y) + z$*.*
Guiseppe Peano, Italiaans logicus en wiskundige, gebruikte deze taal voor het axiomatiseren van de rekenkunde. Hiervoor hebben we dus slechts vijf woordjes nodig, de niet-logische symbolen $0, S, +$ *en* $\cdot$*, tezamen met onze vaste logische symbolen. Hier is alvast een voorbeeld van één van Peano's axioma's:*

$$\forall x \forall y \, (x + Sy = S(x + y))$$

In 'gewoon' Nederlands zegt dit dat, voor elk tweetal getallen x *en* y *is de som van* x *en de opvolger van* y *gelijk aan de opvolger van de som van* x *en* y*. Het axioma-systeem van Peano komen we later nog tegen in hoofdstuk 7 (*T. *27) wanneer we de logische grondslagen van de wiskunde bespreken.*

P 3.





GOTTLOB FREGE

1848 — 1925

Gottlob Frege *is de ontwerper geweest van de predicatenlogica. Hij beschreef het formalisme in zijn eerste belangrijke boek 'Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens' (1879). In het rechterplaatje hierboven staat een voorbeeld van Frege's originele notatie.*
In zijn eigen tijd kreeg hij maar weinig waardering. Zelfs een wiskundige als Cantor die we vandaag de dag als geestverwant zouden opvoeren, stond bijzonder onverschillig tegenover Frege's werk. Vandaag de dag is de predicatenlogica het meest gebruikte logische formalisme, niet alleen maar in de wiskunde maar ook in de informatica, de filosofie en de linguïstiek.
Frege was ervan overtuigd dat de wiskunde teruggebracht kon worden tot pure logica (logicisme). In twee delen 'Die Grundlagen der Arithmetik' doet hij ook een werkelijke poging. Toen door anderen (o.a. door Bertrand Russell met zijn beroemde paradox, zie ook hoofdstuk 3) tot tweemaal toe werd aangetoond dat zijn axiomatisering inconsistent was gaf hij het mismoedig op, en het derde deel wat hij voornemens was te schrijven, is dan ook nooit gepubliceerd.

Mathematische linguïstiek Misschien zijn inmiddels excuses wel op hun plaats. U dacht een boek over wiskunde te lezen, en u lijkt nu verzeild geraakt te zijn in een dictaat over taalkunde. Wellicht strekt het tot troost dat de taalkunde van formele talen zelf weer een onderwerp is van wiskundige studie. Er bestaat zelfs een heel vakgebied van de *mathematische linguïstiek* waar theorieën ontwikkeld worden over grammatica's en talen. Daarnaast vindt in de informatica ook nog eens wiskundige theorievorming plaats over nieuw ontworpen programmeertalen. En ook logici hebben de nodige interessante feiten ontdekt over formele notatie. Maar veel belangrijker nog dan die taalvormen op zich is de studie van formele patronen van het taalgebruik. Voor de wiskunde betreft dat met name het bewijzen van wiskundige feiten. Daarmee komen we op het gebied van de logica, een thema dat in latere hoofdstukken nog vaak zal terugkeren.

Logica: patronen in bewijzen Intuïtief onderscheiden we geldige en ongeldige gevolgtrekkingen in bewijzen. Geldig zijn bijvoorbeeld de volgende patronen, met de gegevens ('premissen') gescheiden van de 'conclusie' door de pijl $\Rightarrow$:[8]

$$\begin{aligned} A \to B, A &\Rightarrow B \\ A \to B, \neg B &\Rightarrow \neg A \\ \exists x\, \forall y\, Rxy &\Rightarrow \forall y\, \exists x\, Rxy \end{aligned}$$

Dankzij de abstractie van de niet-logische symbolen blijven deze redeneerprincipes altijd van kracht. We kunnen voor A en B een willekeurig tweetal uitspraken nemen: steeds moet de conclusie waar zijn als de premissen dat zijn. Dit geldt ook voor de twee beweringen in de laatste redenering, wat de relatie R ook is. Neem bijvoorbeeld de menselijke relatie 'houden van' over een gespreksdomein van personen, dan staat hier het volgende:

> Aangenomen dat er iemand bestaat waarvan iedereen houdt, dan mogen we concluderen dat iedereen van iemand houdt.

Ongeldig daarentegen zijn redeneringen als de volgende:

$$\begin{aligned} A \to B, \neg A &\not\Rightarrow \neg B \\ \forall y\, \exists x\, Rxy &\not\Rightarrow \exists x\, \forall y\, Rxy \end{aligned}$$

Bijvoorbeeld, in een groep van egoïsten houdt iedereen van iemand, te weten zichzelf, maar niemand houdt van iedereen. We laten het aan de lezer over zelf een dergelijk tegenvoorbeeld te bedenken voor de eerste gevolgtrekking. In hoofdstuk 6 zullen we een nadere logische uitleg geven van de geldigheid en ongeldigheid van de redeneringen.

Lof der notatie Precisie in wiskundige taal heeft geleid tot het ontdekken van alle geldige patronen voor Boolese operaties en kwantoren. Vervolgens kunnen we die patronen tegenwoordig zelfs in een computer stoppen, en daarmee dan zuiver symbolisch rekenen en redeneren. Machines kunnen op die manier wiskundige bewijzen mechanisch controleren, en soms zelfs ontdekken. Toch blijft het bestuderen van pure symbolen en formele bewijzen op zich voor veel mensen moeilijk. Misschien is het goed om de vele goede redenen hiervoor nog eens samen te vatten. Symbolische notatie verhoogt precisie waar dat nodig is. Ze brengt wiskunde daarmee in een vorm die geschikt is voor 'grondslagenonderzoek' naar haar algemene eigenschappen, iets waarvan we nog diepzinnige voorbeelden zullen zien in latere hoofdstukken. Maar notatie brengt wiskunde ook in een praktische vorm die voor computers begrijpelijk is, zodat we hun rekenkracht kunnen inzetten om ons te helpen met allerlei wetenschappelijke taken.

We zijn nu aan het eind gekomen van onze grammatica van de wiskundige taal. De belangrijke Boolese operaties en kwantoren kent u nu. Deze waren ook niet moeilijk te begrijpen, want ze komen voort uit gewone uitdrukkingen die u vanzelf al kent en gebruikt, zij het dat ze veel preciezer werden gemaakt, zonder allerlei uitzonderingen en ambiguïteiten. Maar dan hebben we meteen ook een probleem. Gezien al die prachtige voordelen van het gebruik van formele wiskundige taal, waarom heeft deze dan in de loop van de tijd niet gewonnen als medium voor communicatie en redeneren? Wat moeten we eigenlijk nog met al dat Nederlands?

[8] Let wel, de dubbel gelijnde pijl $\Rightarrow$ is een andere dan de implicatie $\to$. De laatste is een binair connectief waarmee we twee logische beweringen kunnen aaneenvoegen tot één nieuwe bewering. De dubbele pijl is een 'meta'-symbool. Het stelt de geldigheidsrelatie tussen een aantal aannames en een conclusie, die allen afzonderlijke logische beweringen zijn.

Gewone taal, rekenen en menselijke cognitie

Ondanks eeuwen van symbolische notatie, gebruiken wij nog steeds onze natuurlijke taal, zelfs in een wiskunde colloquium! Deze taal is ontstaan in een lange cognitieve evolutie, hetgeen we onder meer merken aan een mengsel van efficiëntie en allerlei rariteiten, zoals de beroemde 'uitzonderingen' op regels. Onze gewone taal is dus een natuurverschijnsel, en niet ontworpen in de studeerkamers van geleerden, ook al kunnen individuen wel degelijk de taal beïnvloeden. Bovendien heeft die taal vele functies, zoals overdracht van informatie, sociale communicatie, tonen van emotie, enzovoort. Bestuderen van die functies geeft inzicht in ons cognitief functioneren. In de filosofie heeft lang een scherpe tegenstelling bestaan tussen formele 'versus' natuurlijke taal, waarbij de laatste 'misleidend' zou zijn. Het gebrek aan precisie en het onlosmakelijk ambigue karakter van natuurlijke taal maakt dat mensen elkaar gemakkelijk kunnen misverstaan. Het was de droom van Leibniz, de grote zeventiende eeuwse wiskundige en universeel geleerde, om onze taal te formaliseren zodat in het geval van onenigheid een berekening ("Calculemus!") uitsluitsel zou kunnen geven. Zijn streven was een belangrijke inspiratie in de ontwikkeling van de moderne logica, en ook die van de hedendaagse techniek van 'redenerende machines'.

Tegenwoordig is men juist meer geïnteresseerd in de verbanden over en weer tussen natuurlijke en formele talen. We houden vast aan onze 'misleidende' gewone taal omdat we er zo handig en efficiënt mee zijn. Deze intelligentie staat juist in het huidige computertijdperk in het middelpunt van de belangstelling. Het lukt voorlopig nog maar heel beperkt om formeel redenerende machines natuurlijke taal te laten begrijpen.

Laten we eens kijken naar één aspect hiervan, en wel het thema van dit hoofdstuk: tellen. Hoe gaan gewone stervelingen om met hoeveelheden in natuurlijke taal? En wat voor soort wiskunde steekt daar achter?

Uitdrukkingen van hoeveelheid Onze gewone taal heeft een rijk repertoire aan teluitdrukkingen. Enkele voorbeelden zijn:

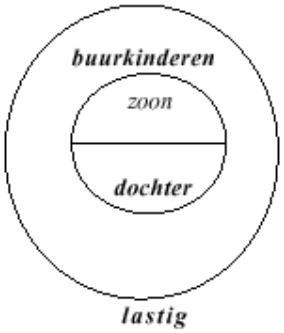
> "Dit meisje kent drie talen",
>
> "Weinig mensen kennen meer dan twee talen",
>
> "De meeste mensen zijn rechtshandig",
>
> "Alle vogels zingen een lied".

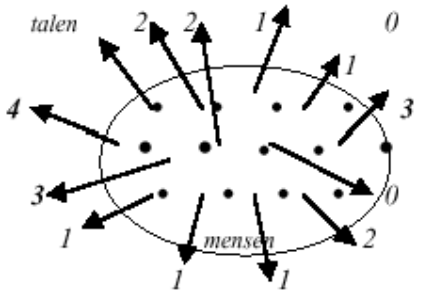
Hiermee kunnen aantallen worden uitgedrukt en onderling gecommuniceerd, maar in ons gebruik van dit soort uitdrukkingen wordt in wezen ook gerekend!

Alledaags redeneren codeert rekenen Hele gewone gevolgtrekkingen die we moeiteloos gebruiken zijn tegelijkertijd rekenstappen. Bijvoorbeeld,

> Uit het feit dat alle kinderen van uw buurman lastig zijn
>
> volgt dat alle dochters van uw buurman lastig zijn.
>
> Uit het feit dat weinig mensen meer dan twee talen kennen
>
> volgt dat weinig mensen meer dan drie talen kennen.

De volgende plaatjes illustreren dit nog eens op een andere manier:





Als we dit telvocabulaire en dit soort gevolgtrekkingen nader bestuderen, dan leren we meteen iets over het 'natuurlijke tellen' dat we vanzelf doen.

Determinatoren en kwantoren

Determinatoren *Kwantoruitdrukkingen* zijn woorden als 'twee, alle, weinig, geen, de meeste'. Deze komen op allerlei plaatsen in zinnen voor. Bijvoorbeeld:

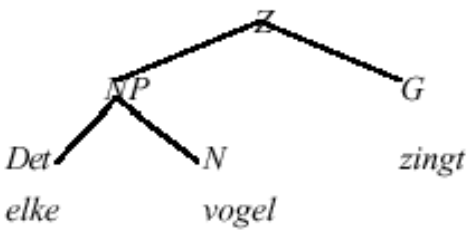
"Drie boeken worden veel verkocht"	(onderwerp)
"Ik kocht drie boeken"	(lijdend voorwerp)
"Zij kwam binnen met drie boeken onder de arm"	(bijwoordelijke bepaling)

De centrale uitdrukkingen hier zijn NP's ('nominal phrases'), vaak gevormd door een eigenschap zoals 'boek' plus een zogenaamde *determinator*, waarmee geheel of gedeeltelijk wordt vastgelegd over welke van de dragers van deze eigenschap we het hebben. Kwantoren zijn voorbeelden van determinatoren, waarbij specifiek wordt verwezen naar de omvang van de groep. Voorbeelden van andersoortige determinatoren zijn uitdrukkingen als "Napoleon's' of 'Marie's mooiste', als in "Napoleon's generaals bleven trouw", of "Marie's mooiste jurk draagt ze alleen op zondag".

Hieronder staan twee grammaticaregels gegeven voor de zinsconstructie met determinatoren zoals die in heel veel bekende talen voorkomen:

$$Z \Rightarrow NP + G$$
$$NP \Rightarrow Det + N$$

De eerste regel zegt dat een zin (categorie *Z*) mag worden gevormd door combinatie van een onderwerp (*NP*) met een gezegde (*G*). Dat onderwerp mag zelf weer worden geschreven als een determinator (*Det*) plus naamwoord (*N*). Taalkundigen schrijven dit vaak in een boomvorm, die er bijvoorbeeld voor "Elke vogel zingt" als volgt uitziet:



TECHNIEK 8.

Naïeve verzamelingenleer

In T. 2 (pag. 14) hebben we al verzamelingen getallen geïntroduceerd. Maar algemener beschouwen we een verzameling als een ongeordend stel van willekeurige objecten: de elementen *van de verzameling. Als a een element is van verzameling A dan schrijven we $a \in A$; en evenzo $a \notin A$ als a geen element is van A. De 'lege verzameling' zonder elementen wordt geschreven als $\emptyset$. Aftelbare verzamelingen (T. 4, pag. 22) worden ook vaak elementsgewijs geschreven in een lijst-notatie met accolades:*

$$\{x_0, x_1, \ldots x_n\} \text{ , of in het oneindige geval } \{x_0, x_1, \ldots\}.$$

Verzamelingen zijn gelijk als ze dezelfde elementen hebben. Het maakt dus niet uit in welke volgorde we die elementen schrijven, en ook niet hoe vaak. Bijvoorbeeld, $\{a, b, c\}$ is dezelfde verzameling als $\{c, a, b, b, a\}$. Als verzamelingen bestaan uit elementen die aan een bepaalde definierende conditie voldoen dan wordt dit als volgt genoteerd:

$$\{x \mid x \text{ voldoet aan eigenschap } {}_1, x \text{ voldoet aan eigenschap } {}_2, \ldots\}$$

Dit beschrijft de verzameling van alle objecten x die aan de eigenschappen $1, 2, \ldots$ voldoen. Vaak worden deze elementen weer uit een eerder gekozen verzameling A genomen en schrijven we

$$\{x \in A \mid x \text{ voldoet aan } \ldots \text{ etc.}\}$$

Belangrijke operaties op verzamelingen zijn nu te definiëren met behulp van de bovenstaande notatie:

doorsnede	$A \cap B$	$=$	$\{x \mid x \in A \text{ en } x \in B\}$
vereniging	$A \cup B$	$=$	$\{x \mid x \in A \text{ of } x \in B \text{ (of beide)}\}$
verschil	$A - B$	$=$	$\{x \mid x \in A \text{ en } x \notin B\}$
complement	$\overline{A}$	$=$	$\{x \mid x \notin A\}$

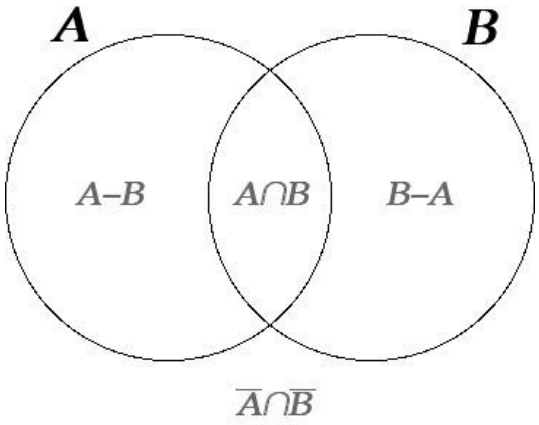
Veelal worden deze operaties in een bepaald universum *of* domein U *van alle 'mogelijke' elementen uitgevoerd. In plaats van $\{x \mid \ldots\}$ wordt dan vaak $\{x \in U \mid \ldots\}$ in de definities hierboven geschreven.*
Als alle elementen van een verzameling A ook element zijn van een verzameling B dan heet A een deelverzameling *van B, en schrijven we $A \subseteq B$. $A \not\subseteq B$ betekent dat A geen deelverzameling van B is. In dat laatste geval moet er dus een $x \in A$ te vinden zijn zodat $x \notin B$.*
Tenslotte, waar we in het eerste deel van dit hoofdstuk mee eindigden was de z.g. 'machtsverzameling':

$$\wp A = \{B \mid B \subseteq A\}$$

Deze verzameling bestaat precies uit alle deelverzamelingen van A.

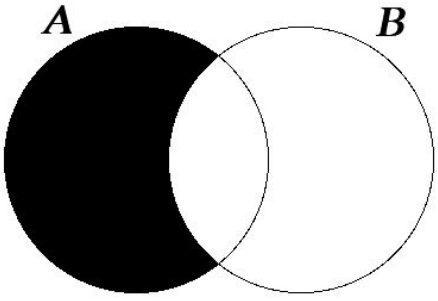
Natuurlijk zijn er nog veel meer van dit soort regels in een echte grammatica. Maar wat betekenen deze uitdrukkingen nu in concrete situaties? We stellen ons dit wiskundig voor in termen van verzamelingen van objecten. We beperken ons nu verder tot de betekenis van kwantoruitdrukkingen. $\stackrel{\text{T. 8}}{\Longrightarrow}$ 38

Kwantoren Uitspraken als "*alle* A zijn B", "*drie* A zijn B", "*de meeste* A zijn B" kunnen we abstract beschrijven als een formule $\mathsf{Q}\,AB$ waarbij het symbool Q voor de *kwantor* staat, en letters A, B voor de twee eigenschappen die Q relateert in de zinsvorm $(\mathsf{Q}\,A)B$. Eigenschappen A en B vatten we hierbij op als verzamelingen, en wel als die objecten binnen het totale gespreksdomein die de eigenschap hebben. In een plaatje, een zogenaamd *Venn-diagram*, tekenen we dit als volgt: $\stackrel{\text{T. 9}}{\Longrightarrow}$ 40



We zien hier vier zones waar een object zich kan bevinden: de doorsnede $A \cap B$, de verschilverzamelingen $A - B$ en $B - A$, en het buitengebied $\overline{A} \cap \overline{B}$. Als het gespreksdomein alleen mensen bevat en A staat voor Amsterdammers en B voor roodharigen, dan is het overlappende gebied $A \cap B$ de roodharige Amsterdammers. De twee verschilverzamelingen zijn de niet-roodharige Amsterdammers ($A - B$) en de roodharige niet-Amsterdammers ($B - A$). Het buitengebied zijn de mensen die beide eigenschappen missen, en dus noch Amsterdams noch roodharig zijn.

Een kwantor eist nu een bepaald verband tussen de verzamelingen A en B. Zo zegt "Alle A zijn B" dat A een deelverzameling is van B, in verzamelingtheoretische notatie $A \subseteq B$. Dit zegt dat er geen A is zonder de eigenschap B, ofwel, de verzameling $A - B$ is leeg. In het plaatje hierboven kunnen we dat intekenen door het $A-B$ gebied zwart te kleuren. Dat gebied heeft dan geen elementen.



De kwantor 'Geen' legt ook zo'n relatie tussen twee verzamelingen. "Geen A is B" zegt dat $A \subseteq \overline{B}$, ofwel, $A \cap B$ is leeg. Ook dit kan ingekleurd worden, door de overlap van A en B zwart te maken.

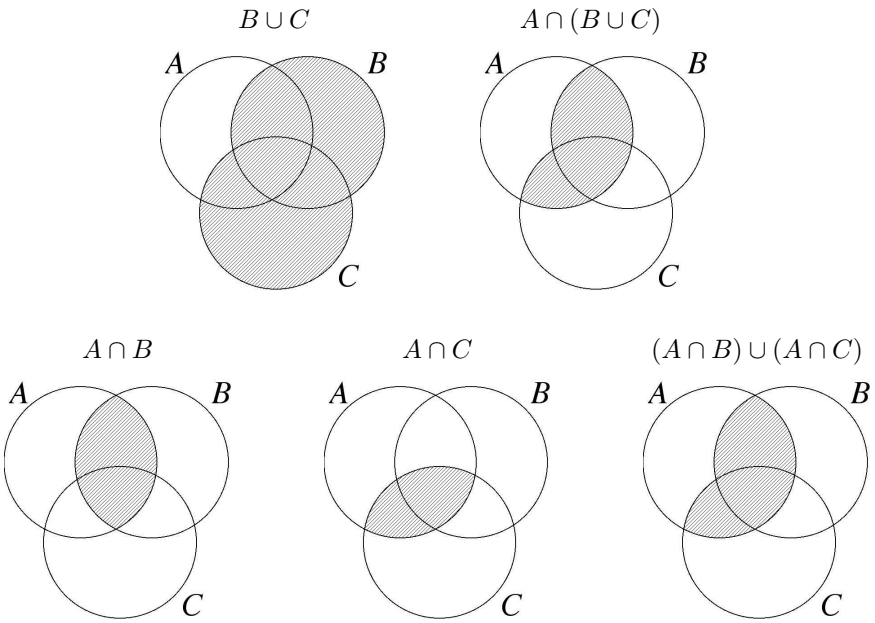
In ditzelfde rijtje horen nog twee kwantoren, die ditmaal zeggen dat bepaalde gebieden in het diagram juist niet leeg zijn. "Niet alle A zijn B" zegt dat $A - B \neq \emptyset$, en 'Een A is B' (we lezen dit

TECHNIEK 9.

Venn-diagrammen

Eenvoudige algemene berekeningen op verzamelingen worden vaak grafisch verbeeld met een 'Venn-diagram' (naar de 19de eeuwse wiskundige John Venn). In zo'n diagram tekent men verzamelingen als cirkels en laat deze zodanig overlappen zodat alle mogelijke Boolese combinaties van objecten voorkomen. Vervolgens arceert men gedeelten van plaatjes die bij bepaalde verzamelingtheoretische expressie horen. Hieronder zien we zo'n grafische berekening, die aantoont dat:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$



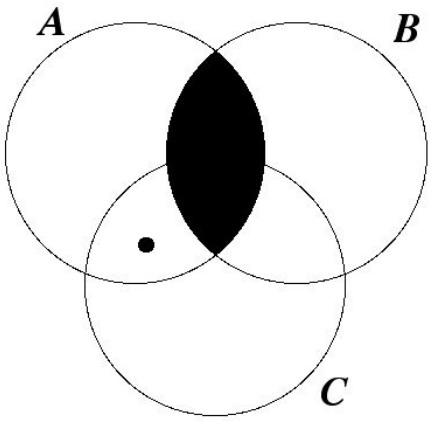
Met behulp van Venn-diagrammen is ook snel in te zien of belangrijke andere relaties gelden tussen gegeven verzamelingen. Een voorbeeld dat we aan de lezer ter grafische verificatie overlaten:

$$A \cap (B \cup C) \subseteq (A \cap B) \cup C$$

als ‘minstens één’) zegt dat $A \cap B \neq \emptyset$. De geldigheid van een redenering als de volgende kunnen we nu met een diagram als hierboven grafisch bewijzen.

$$\text{Geen } A \text{ is } B, \ \text{Een } A \text{ is } C \Rightarrow \ \text{Niet alle } C \text{ zijn } B \tag{1.1}$$

Om aan te geven dat een bepaalde verzameling niet leeg is plaatsen we een stip, met dien verstande dat in zwarte gebieden geen stip meer gezet kan worden. Om de eerste aanname waar te maken kleuren we het $A \cap B$-gedeelte zwart. Om de tweede aanname waar te maken moeten we nu een stip zetten in het $A \cap C$ gedeelte. Dit kan alleen maar in $A \cap C \cap \overline{B}$, omdat $A \cap C \cap B = \emptyset$ vanwege het zwarte gebied in het midden van het diagram.



Daarmee zien we in een oogopslag dat $C \cap \overline{B} = C - B \neq \emptyset$, en daarmee moet de conclusie “Niet alle C zijn B” waar zijn in het geval dat de beide premissen “Alle A zijn B” en “Een C is B” waar zijn.

Redeneringen met deze vier zogenaamde *klassieke* kwantoren werden al door Aristoteles rond 300 voor Christus systematisch in kaart gebracht. Dit systeem heet de *syllogistiek*, en het heeft tot aan de Renaissance de symbolische logica gedomineerd.

P 4.

Aristoteles, *hier afgebeeld op een fragment van een fresco van Giotto (de Atheense school), is de bedenker van de syllogistiek, het eerste formele logische rekensysteem.*

ARISTOTELES

384 — 322 v. Chr.

Bijecties en invariantie Natuurlijke taal bevat veel meer kwantoren dan de vier klassieke. Deze zijn vaak niet in simpele diagrammen te vatten. Toch kunnen we ze wel degelijk beschrijven als kwantitatieve relaties tussen verzamelingen. Zo betekent bijvoorbeeld "De meeste A zijn B" dat

$$|A - B| < |A \cap B|,$$

ofwel, het aantal A's die de eigenschap B missen is kleiner dan het aantal A's die de eigenschap B wel hebben. Zulke betekenissen staan in nauw verband met een begrip uit het eerste deel van dit hoofdstuk 1.1. Ze hangen alleen af van de aantallen objecten in de zones van bovenstaande plaatjes, ofwel, hun kardinaliteit. De klassieke kwantoren drukken slechts een simpel 'tel'-verband uit:

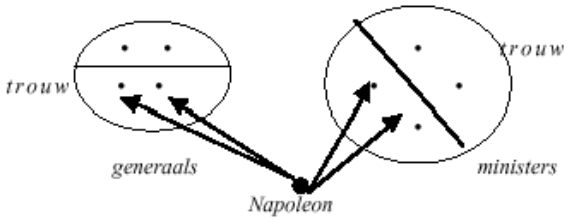
$$\begin{array}{rcl@{\qquad\qquad}rcl} \text{Alle } AB & \Leftrightarrow & |A - B| = 0 & \text{Geen } AB & \Leftrightarrow & |A \cap B| = 0 \\ \text{Niet alle } AB & \Leftrightarrow & |A - B| > 0 & \text{Een } AB & \Leftrightarrow & |A \cap B| > 0 \end{array}$$

Andere kwantoren, zoals 'De meeste' of 'weinig' stellen meer ingewikkelde eisen. Maar allemaal zijn ze 'invariant voor bijecties', waarmee we het volgende bedoelen. Als Q een willekeurige kwantor
$\overset{\text{T. 1}}{\Longleftarrow}$ 12 is en f is een bijectie tussen twee verzamelingen E en E', de objecten waarover we spreken in twee verschillende situaties, dan geldt toch steeds de volgende equivalentie

$$\mathsf{Q}\, AB \Leftrightarrow \mathsf{Q}\, f[A] f[B], \text{ voor alle } A \subseteq E \text{ en } B \subseteq E$$

Deze invariantie noemt men ook wel 'individu-neutraliteit'. Een kwantor is niet geïnteresseerd in specifieke kenmerken van objecten in de verzamelingen die hij relateert. Bij een één-op-één transformatie, of herbenoeming, van het gespreksdomein van objecten, blijven dezelfde gekwantificeerde uitdrukkingen waar. Dit weerspiegelt precies het wiskundige tellen dat we al hebben leren kennen.

Voor determinatoren in het algemeen geldt dit invariantie-principe overigens niet. Hieronder staat een simpel voorbeeld getekend:



We hebben hier twee verzamelingen E en E', een van generaals en een van ministers. Laat deze twee verzamelingen even groot zijn. De pijlen staan voor de relatie 'bij Napoleon horen'. Laat nu eens $f : E \to E'$ een bijectie zijn met $f[\text{Generaals}] = \text{Ministers}$. Laten daarbij nu juist de twee trouwe generaals en de twee ontrouwe ministers worden gekoppeld. De uitspraak "Napoleon's (Q) generaals (A) zijn trouw (B)" is waar in de linker figuur, maar niet meer na de afbeelding f. Want "Napoleon's (Q) ministers ($f[A]$) zijn trouw ($f[B]$)" is niet waar in de rechterfiguur.

Invariantie voor bijecties ligt iets ingewikkelder als we kwantoren bekijken in oneindige situaties, zoals een bewering "De meeste natuurlijke getallen zijn geen priemgetallen". In dit geval kan ordening een rol spelen, of een waarschijnlijkheidsmaat. We kunnen dan overgaan op transformaties tussen verzamelingen die meer structuur van objecten bewaren dan alleen zuivere aantallen, zoals zal gebeuren in (6.1). In het algemeen blijkt dat als we invariantie van uitspraken in gewone taal willen garanderen extra eisen een rol spelen naast het zuivere tellen dat wordt verricht door bijecties.

Redeneren over hoeveelheid

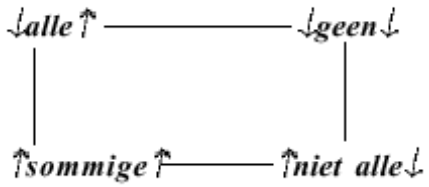
Ondanks de verschillen, blijken we dus toch wiskunde te kunnen gebruiken om het natuurlijke 'tellen in taal' exact te beschrijven! Hiertoe gebruikten we al verzamelingsdiagrammen. Maar dit is een zeer beperkte methode die alleen werkt voor klassieke kwantoren met combinatie van hoogstens drie verzamelingen. Een meer algemene methode gebruikt *inferentie-regels*. Dat zijn belangrijke eigenschappen van kwantoren die we kunnen gebruiken als een soort sjablonen. Een belangrijke voorbeeld zijn zogenaamde *monotonie-principes*. Dit zijn vervangingsregels voor eigenschappen in kwantoruitdrukkingen door kleinere of grotere verzamelingen zodat de uitdrukking waar blijft. Bijvoorbeeld, in een uitdrukking "Alle AB" kunnen we A vervangen door een willekeurige deelverzameling. Als "Alle AB" waar is dan blijft "Alle CB" waar indien $C \subseteq A$. Men noemt dit wel 'links-daling'. Hier is een concrete illustratie:

Alle Nederlanders zijn Europeanen	$\mathsf{Q}\ AB$
Limburgers zijn Nederlanders	$C \subseteq A$
Alle Limburgers zijn Europeanen	$\mathsf{Q}\ CA$

Links-daling geldt ook voor de kwantoren 'Geen' en 'Weinig', maar bijvoorbeeld niet voor 'Een' of 'De meeste'. Zo zijn de meeste Nederlanders geen Amsterdammers, maar daar volgt niet uit dat de meeste Amsterdammers geen Amsterdammers zijn. Een kwantor als 'Een' heeft juist een eigenschap van links-stijging: we mogen de linker verzameling vervangen door een grotere. Als er een Europeaan gestorven is, dan is er een mens gestorven. En evenzo hebben we mogelijke stijging of daling in het rechter argument. De kwantor 'Een' is rechts-stijgend. Als er een Europeaan is die danst, dan is er een Europeaan die beweegt. Eveneens rechts-stijgend is de kwantor 'De meeste': als de meeste gasten dansen, dan bewegen de meeste gasten. Overigens hebben niet alle kwantoren monotonie-gedrag aan beide kanten. Zo is 'De meeste' geen linker daler, maar evenmin een linker stijger: de meeste vogels kunnen vliegen, maar daaruit volgt niet dat de meeste dieren kunnen vliegen. We sommen de mogelijke patronen nog eens op:

$$\mathsf{Q}\,AB, C \subseteq A \Rightarrow \mathsf{Q}\,CB \quad \text{links-daling}$$
$$\mathsf{Q}\,AB, A \subseteq C \Rightarrow \mathsf{Q}\,CB \quad \text{links-stijging}$$
$$\mathsf{Q}\,AB, C \subseteq B \Rightarrow \mathsf{Q}\,AC \quad \text{rechts-daling}$$
$$\mathsf{Q}\,AB, B \subseteq C \Rightarrow \mathsf{Q}\,AC \quad \text{rechts-stijging}$$

Kwantoren die monotonie-gedrag hebben in beide argumenten zijn wel heel belangrijk. We illustreren dit in het zogenaamde 'Vierkant van Oppositie' uit de Middeleeuwen dat de klassieke kwantoren met hun monotoniciteits-kenmerken afbeeldt.



Deze monotoniciteits-kenmerken volstaan nog niet om de klassieke kwantoren uniek te beschrijven. Zo is de kwantor "Minstens twee" een dubbele stijger, net zoals de klassieke 'Een'. Maar we kunnen wel het wiskundige surplus bedenken dat de klassieke kwantoren uniek vastlegt. Om te beginnen

hebben ze alle vier een eigenschap die ze delen met alle bekende determinatoren in natuurlijke talen, en wel *conservativiteit*:

$$\mathsf{Q}\,AB \leftrightarrow \mathsf{Q}\,A(B \cap A) \text{ voor alle } A \text{ en } B \tag{1.2}$$

Dit zegt dat een kwantor in de vergelijking van A en B een voorkeursrol geeft aan het linker argument A. Alleen dat gedeelte van B doet ertoe dat binnen A ligt. Dit is eenvoudig te zien aan talloze voorbeelden. Zo zegt 'Geen geld is verdiend' hetzelfde als 'Geen geld is verdiend geld', of 'De meeste mannen zijn kleinzerig' hetzelfde als 'De meeste mannen zijn kleinzerige mannen'. Maar ook "Minstens tweeïs conservatief, dus we hebben nog een verdere kenmerkende eigenschap nodig! Deze vinden we in het sterke 'onderscheidend vermogen' van klassieke kwantoren', hetgeen wiskundig is te formuleren als hun *variëteit*:

$$\text{Als } \mathsf{Q}\,AB \text{ en } A \neq \emptyset \text{ dan } gelden\mathsf{Q}\,AC \wedge maarook\neg\mathsf{Q}\,AD \text{ voor zekere } C \text{ en } D \tag{1.3}$$

Het is makkelijk na te gaan dat de klassieke kwantoren voldoen aan alle genoemde eisen: dubbele monotonie, conservativiteit en variëteit. [9]

Ter afsluiting van dit hoofdstuk wordt in T. 10 een bewijs gegeven dat deze eenvoudige eigenschappen de klassieke kwantoren ook precies vastleggen. De strekking van zo'n resultaat is intrigerend in het algemeen. We kunnen de expressieve kracht van belangrijke delen van onze natuurlijke taal vastleggen met wiskundige eigenschappen!

Verschillen met tellen in natuurlijke taal

Ondanks de bruikbaarheid van wiskundige technieken, houdt natuurlijke taal allerlei eigenschappen die afwijken van wiskundige talen. We noemden reeds de veel voorkomende ambiguïteit: het verschijnsel van meer betekenissen voor één enkele uitdrukking. Ook ons telvermogen in taal, hoe systematisch ook, wijkt af van de gewone wiskunde. Een belangrijk onderscheid is de voorkeur in natuurlijke taal voor eindige verzamelingen. Zelfs kwantorbetekenissen liggen ineens niet eenduidig meer als we spreken over oneindige verzamelingen. Er bestaan natuurlijk wel uitdrukkingen als 'oneindig veel', maar deze lijken import vanuit de wetenschap en geen eigen kweek. Zelfs kwantoren als 'veel' en 'heel erg veel' lijken in hun standaard betekenis steeds te slaan op eindige situaties.

Een tweede opmerkelijke eigenschap van natuurlijke taal die verschilt van wetenschappelijke taal is haar context-afhankelijkheid. Zo kunnen 'Veel UvA studenten' heel goed 'weinig Nederlanders' zijn, omdat de kwalificatie 'veel/weinig' afhangt van een referentie-groep waaraan we de norm ontlenen. "Veel Nederlanders zitten in de WAO" zou bijvoorbeeld kunnen slaan op een drempelwaarde $N = 3$ miljoen, hetgeen dan 'veel' is op een bevolking van 16 miljoen. Maar de context kan ook de verzameling E zijn van alle objecten waarover we spreken. Zo kan de zin over 'veel' WAO-ers ook gelezen worden als 'qua percentage meer dan het Europees gemiddelde'. Context-afhankelijkheid geldt ook voor bijvoeglijke naamwoorden:

> Een grote muis is een klein dier, een kleine olifant is een groot dier.

Taalgebruikers wisselen moeiteloos van context en dat omschakelen werkt zelfs goed bij gewone communicatie. Toch blijft de betekenis van 'veel' wat vaag, omdat we het criterium doorgaans niet helemaal kennen. Ook vaagheid is een typisch kenmerk van taal!

Tenslotte noemen we nog een derde eigenaardigheid. Het kwantorsysteem van natuurlijke talen lijkt altijd dubbel voor te komen: soms 'discreet' om te tellen, en dan weer 'continu' om te meten.

[9] Het is hier van belang dat we $A \neq \emptyset$ kiezen. "Een $\emptyset B$" is onwaar voor elke eigenschap B.

TECHNIEK 10.

Karakterisering van de klassieke kwantoren

We kunnen het in de tekst genoemde resultaat voor de kwantor 'Een' als volgt formuleren.

Stelling *Als een kwantor* Q *links- en rechts-stijgend, conservatief en onderscheidend is dan moet* Q AB *zeggen dat "Een* A *is* B*".*

$$\mathsf{Q}\, AB \Leftrightarrow A \cap B \neq \emptyset, \text{ voor alle verzamelingen } A \text{ en } B$$

Bewijs $\Leftarrow$*: Stel dat* $A \cap B \neq \emptyset$*. Nu geldt dankzij het onderscheidingsprincipe dat er een verzameling* C *moet zijn zodanig dat* Q $(A \cap B)C$ *geldt. Dankzij het conservativiteitsprincipe volgt dan dat* Q $(A \cap B)(C \cap A \cap B)$*. Dankzij links-stijging krijgen we ook* Q $A(C \cap A \cap B)$ *en vervolgens met behulp van rechts-stijging ook* Q AB*.*
$\Rightarrow$*: Stel nu omgekeerd dat* Q AB *het geval is. We moeten bewijzen dat nu* $A \cap B \neq \emptyset$*. Stel dat dit laatste niet het geval zou zijn. Omdat* Q $A(B \cap A)$ *wegens conservativiteit, moet ook gelden dat* Q $A\emptyset$*. Dat zou betekenen, dankzij links-stijging, dat we* A *kunnen vervangen door een willekeurige niet-lege grotere verzameling* A'*:* Q $A'\emptyset$*. Dankzij rechts-stijging geldt dan dat* Q $A'C$ *voor willekeurige verzamelingen* C*, omdat* $\emptyset \subseteq C$ *voor alle* C*. Vanwege het onderscheidings-principe zou dat echter alleen kunnen als* $A' = \emptyset$*. Maar dit laatste was nu juist niet het geval, en dus kan de veronderstelling dat* $A \cap B = \emptyset$ *niet kloppen.* QED

De stelling dekt ook de overige drie klassieke kwantoren als we de juiste monotoniciteitskenmerken invullen. Bijvoorbeeld, in het geval van 'Alle' wordt dit:

Als Q *links-dalend en rechts-stijgend is, alsmede conservatief en onderscheidend, dan*

$$\mathsf{Q}\, AB \Leftrightarrow A - B = \emptyset, \text{ voor alle vrezamelingen } A \text{ en } B$$

De bewijzen voor deze karakteriseringen volgen hetzelfde stramien als boven. □

Het contrast, en de analogie, ziet men bij zinnen met enerzijds telbare naamwoorden zoals ‘appel’, en anderzijds stofnamen zoals ‘wijn’:

hij at alle appels (’telbaar’)	zij dronk alle wijn (’meetbaar’)
hij at de meeste appels	zij dronk de meeste wijn
hij at geen appels	zij dronk geen wijn

Kennelijk beschrijft de gewone taal de wereld in discrete telbare termen, maar ook in continue meetbare, twee domeinen die de wiskunde zorgvuldig uit elkaar houdt.

Cognitie Een balans van overeenkomsten en verschillen tussen wiskundige en natuurlijke taal is niet alleen een kwestie van boekhouden. De genoemde bijzonderheden van natuurlijke taal, zoals ambiguïteit en context-afhankelijkheid, zijn zo hardnekkig en veel voorkomend dat ze ongetwijfeld een belangrijke positieve rol spelen in ons cognitief functioneren. Maar wat die rol precies is, daar is het laatste woord nog lang niet over gezegd, in natuurlijke of in formele taal.

Hoofdstuk 2

Symmetrie

2.1 Symmetrie

Structuren

De wiskunde bestudeert structuren die vaak onze eigen omgeving ontstijgen die alleen in onze verbeelding, in het mathematisch universum bestaan. Dat deze patronen niet willekeurig zijn maar aan hun eigen systematiek zijn onderworpen, dat er wetmatigheden zijn binnen de wetmatigheden, dat is het wonderlijke inzicht dat de wiskunde ons te bieden heeft.

De wiskunde is op zoek naar universele patronen die uit de veelheid aan ervaringen kunnen worden geabstraheerd en waarvan we zeker kunnen zijn dat we ze keer op keer in concrete situaties zullen blijven tegenkomen en kunnen toepassen. Het is een groot wonder dat deze abstracte wiskundige patronen bedacht kunnen worden en aan de basis van zoveel verschillende (natuurlijke) verschijnselen blijken te staan. De Hongaars-Amerikaans mathematisch-fysicus Eugene Wigner (1902-1995) sprak in dit verband in een bekend artikel van de *unreasonable effectiveness of mathematics in the natural sciences.* En we kunnen er aan toevoegen dat die effectiviteit ook in de mens- en maatschappijwetenschappen terug te vinden is.

Om die abstracte structuren te vinden en te begrijpen moet men voorzichtig te werk gaan. Het is daarbij vaak nodig om bepaalde aspecten voorlopig over het hoofd te zien en de wereld eerst aanzienlijk te vereenvoudigen.

We kunnen dan langzamerhand meer en meer details toevoegen. De wiskundige bouwt daarmee de wereld in laagjes op, als een schilder. Bij het opzetten van de grondlaag wordt er weinig onderscheid gemaakt, maar uiteindelijk worden alle fijne details verwerkt. De cruciale vraag daarbij is vaak: wanneer beschouwen we twee objecten als 'hetzelfde '. Technisch noemt men twee objecten dan *equivalent* of *isomorf*. Kortom, als we een wiskundige formule schrijven van het type

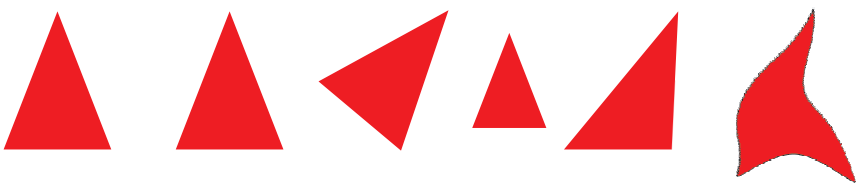
$$x = y$$

wat bedoelen we dan precies met het symbool '='? De gelijkheid tussen objecten kan de wiskundige — zich daarbij wel houdende aan een aantal minimale criteria — zelf 'instellen'. In het eerstgenoemde stadium van abstractie wordt een grove versie van gelijkheid gebruikt om de essentiële structuur te achterhalen. Hierbij wordt weinig onderscheid tussen objecten gemaakt. In het latere stadium van verfijning en toepassing zal juist een meer gedetaileerde notie van gelijkheid gebruikt worden om meer onderscheid tussen objecten te maken.

T. 11 ⟹ 50

Een driehoek is een driehoek is een driehoek

Laten we proberen met een eenvoudig voorbeeld deze abstracte discussie concrete vorm te geven. Stel we zien twee driehoeken. Wanneer vinden we dat deze twee driehoeken hetzelfde zijn. We hebben hierbij vele keuzes, en het zal geheel van de omstandigheden afhangen welke mate van flexibiliteit we in de identificatie willen toelaten. Neem bijvoorbeeld de volgende reeks 'driehoeken'



(a) (b) (c) (d) (e) (f)

We kunnen de ‘oerdriehoek’ (a) met de andere versies identificeren als we bepaalde transformaties of bewegingen toestaan. Bijvoorbeeld driehoek (b) wordt verkregen uit (a) door een verschuiving of een translatie. In de praktijk zullen we meestal geen onderscheid maken tussen (a) en (b). In het geval (c) hebben we de driehoek gedraaid. Ook dat geval komt veel voor. U houdt bijvoorbeeld deze bladzijde gedraaid vast en beschouwt dan de driehoek die op het papier staat afgedrukt nog steeds als dezelfde.

Op soortgelijke wijze zal in veel gevallen versie (d), die verkregen door een schaaltransformatie, of versie (e), verkregen door een algemene lineaire transformatie, ervaren worden als ‘dezelfde’ driehoek. U hoeft bij wijze van spreken deze bladzijde alleen maar wat verder weg of onder een hoek te houden om zo het geprojecteerde beeld op uw netvlies te veranderen en deze transformaties in de praktijk toe te passen. Als we onszelf toestaan om een driehoek van type (a) in type (e) om te zetten dan hebben we alles wat we in het algemeen een driehoek noemen (drie punten verbonden door lijnstukjes) geïdentificeerd. Er is dan nog maar één driehoek.

We kunnen zelfs veel wilder te werk gaan. Als we willekeurige deformaties van het vlak toestaan zonder het papier te scheuren, is een driehoek zelfs equivalent met bijvoorbeeld figuur (f). Denk aan de reflectie in een rustig kabbelend wateroppervlak. Op deze manier verliest de driehoek natuurlijk veel van zijn karakteristieke eigenschappen, en kan zelfs equivalent met een vierkant of een cirkel worden. Kortom, naarmate we royaler worden in wat we wel en niet toestaan met onze oorspronkelijke driehoek wordt het aantal verschillende types minder en minder en de wereld overzichtelijker. Uiteindelijk reduceert ieder figuur tot een onduidelijke ‘blob’.

Topologie

Een ander voorbeeld van hoe de wiskunde dingen kan versimpelen en de onderliggende structuur kan bloot leggen is de topologie van oppervlakken. Hier zijn een aantal voorbeelden van oppervlakken zoals we die in de praktijk tegen kunnen komen — een bril, een schaar, een krakeling. Als we doen alsof deze oppervlakken gemaakt zijn van zeer flexibel rubber dat we willekeurig kunnen uitrekken en deformeren zonder te scheuren (topologie wordt dan ook wel ‘rubbermeetkunde’ genoemd) dan zijn al deze oppervlakken te herleiden tot één oervorm — een oppervlak van geslacht twee, een bol met twee gaten.

Ieder oppervlak is zo te zien als een bol met een gegeven aantal gaten, het zogenaamde geslacht $g = 0, 1, 2, \ldots$. De eindeloze variatie aan oppervlakken reduceert daarmee tot een eenvoudige lijst

TECHNIEK 11.

Equivalentie

Een equivalentierelatie, of kortweg een equivalentie*,* $\equiv$ *over een verzameling* V *wordt gebruikt om elementen van* V *die we voor ononderscheidbaar willen houden op één hoop te vegen. Zo'n relatie hanteren we als een pseudo-gelijkheid om bepaalde verschillen tussen bepaalde elementen van* V *te veronachtzamen. Deze verschillen doen er dan niet meer toe, en de complexiteit en omvang van de originele verzameling* V *kunnen we met zo'n grovere gelijkheidsnotie verkleinen. Dit is een standaardtechniek van het wiskundig bedrijf. Als er gerekend moet worden proberen we de structuur waarop gerekend wordt zo simpel mogelijk te houden en willen we niet lastig gevallen worden door irrelevante details.*
We moeten wel een aantal eisen opleggen aan equivalenties om ze ook te kunnen hanteren als een 'tijdelijke' vorm van gelijkheid. Een relatie $\equiv$ *is een equivalentie als aan de volgende drie eisen voldaan is.*

1. *Alles is equivalent met zichzelf:*
$$\forall x\, x \equiv x$$
2. *Als iets equivalent is met een tweede object dan moet het andersom ook zo zijn:*
$$\forall x \forall y\, (x \equiv y \to y \equiv x)$$
3. *Als een object equivalent is met een tweede, en deze laatste weer equivalent is met een derde object, dan is de eerstgenoemde ook weer equivalent met de laatstgenoemde*
$$\forall x \forall y \forall z\, ((x \equiv y \wedge y \equiv z) \to x \equiv z)$$

De eerste eis heet reflexiviteit*, de tweede* symmetrie *en de derde* transitiviteit*.*
Gegeven een equivalentie $\equiv$ *over een verzameling* V *dan kan* V *opgedeeld worden in zogenaamde* equivalentie-klassen*. Dit zijn niets anders als de bijeengeveegde deelverzamelingen van — gegeven de equivalentie — niet langer te onderscheiden objecten. Elke equivalentie-klasse kan door een enkel object gereprenteerd worden. Gegeven een element* $a \in V$ *dan is de* equivalentie-klasse waartoe a behoort *de verzameling* $\{b \in V \mid a \equiv b\}$*. Deze wordt geschreven als* $\overline{a}$*. Het maakt niet uit welk element we uit zo'n klasse als representant kiezen:*
$$\forall x \forall y\, (x \in \overline{y} \leftrightarrow \overline{x} = \overline{y})$$
Dit volgt uit de eisen die we hierboven opgelegd hebben aan equivalenties. Het laat ook zien dat equivalentie-klassen altijd netjes van elkaar gescheiden zijn:
$$\forall x \forall y \forall z\, ((x \in \overline{y} \wedge x \in \overline{z}) \to \overline{x} = \overline{y} = \overline{z})$$
De opdeling — in wiskundeteksten meestal uitdeling genoemd — van V *in* $\equiv$*-equivalentie-klassen wordt geschreven als* $V/\equiv$*:*
$$V/\equiv = \{\overline{a} \mid a \in V\}$$
Een belangrijke equivalentie is de relatie $\leftrightarrow$ *van gelijke cardinaliteit. Als we verzamelingen alleen op hun grootte beschouwen, en andere eigenschappen vergeten, dan zijn* $\mathbb{N}$*,* $\mathbb{Z}$ *en* $\mathbb{Q}$ *equivalent en ook* $\mathbb{R}$ *en* $\wp(\mathbb{N})$*. Natuurlijk is dit een zeer grove gelijkheidsnotie.*

genummerd door het geslacht g. We kunnen nu in stapjes verder informatie over het oppervlak toevoegen zoals vorm, grootte etc. De topologische classificatie is dus de basisvorm waaruit ieder oppervlak wordt opgebouwd.

We moeten hier wel oppassen. Niet altijd is er zo'n elegante en eenvoudige classificatie mogelijk. Soms zijn er stellingen in de wiskunde die ons vertellen dat het zelfs in principe niet mogelijk is zo'n lijst te maken. Zo is het bijvoorbeeld niet mogelijk hogerdimensionale (hyper)oppervlakken te rubriceren. In 7.1 komen we te spreken over dergelijke 'onbeslisbaarheden' in de wiskunde. Het is natuurlijk wel weer prachtig dat men wiskundig kan bewijzen dat het maken van zo'n lijst weer wiskundig onmogelijk is.

Transformaties en symmetrieën

We zullen veel gebruik maken van de begrippen transformaties en symmetrieën. Laten we dit iets preciezer uitleggen. Bekijk nogmaals de volgende twee driehoeken

De linker driehoek wordt overgevoerd in de rechter driehoek onder een translatie. Laten we die operatie aangeven met het abstracte symbool T. We hebben daarmee een vergelijking van het type

$$\textit{driehoek 2} = \mathsf{T}(\textit{driehoek 1}).$$

De translatie T is een goed voorbeeld van een transformatie. Hij kan gebruikt worden om twee verschillende objecten in elkaar over te voeren.

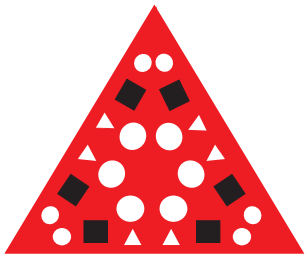
Stel nu dat we een enkele gelijkzijdige driehoek beschouwen

en deze roteren over $120°$. Laten we deze rotatie aangeven met het symbool R. Dit is een bijzondere transformatie omdat de transformatie de driehoek *invariant* laat. Er is geen manier waarop we kunnen uitvinden dat de driehoek onder deze hoek gedraaid is. We hebben dus de symbolische vergelijking

$$\textit{driehoek} = \mathsf{R}(\textit{driehoek}).$$

Let wel, nu staat hetzelfde object links en rechts van het isgelijkteken. In dit geval spreken we van een *symmetrie*. Symmetrieën zijn dus transformaties die een object hetzelfde of invariant laten, we spreken ook wel van een automorfisme. Daarmee zijn symmetrische objecten altijd 'simpeler', omdat er sprake is van een zekere redundantie van informatie. In dit concrete geval zijn de drie hoeken van de driehoek precies identiek. Als we al weten dat ons object invariant is onder de rotatie over $120°$ dan hoeven we maar een derde van de figuur te zien om het totale beeld samen te kunnen stellen. Dit

is het principe van een kaleidoscoop



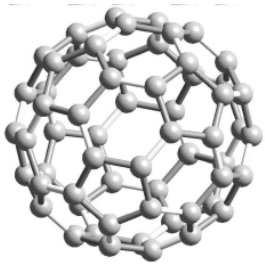
Symmetrie in de natuur

Laten we beginnen met wat voorbeelden van symmetrieën zoals we die in de natuur tegenkomen.

Een sneeuwvlok. Deze is invariant onder rotaties over veelvouden van 60° en onder spiegelingen. Hoewel er ontelbaar verschillende sneeuwvlokken zijn, dragen zij alle deze zesvoudige symmetrie, die een weerspiegeling is van de microscopische moleculaire structuur van het ijskristal. De symmetrie is het ordenende principe achter de oneindige variatie op het thema 'sneeuwvlok'.

Een veel abstracter maar verwand voorbeeld uit de fysica is de symmetrie van elementaire deeltjes. Hier is het veel minder intuïtief duidelijk in welke 'richting' we draaien. Het is een volledige abstracte symmetrie, maar wel een zeer krachtig leidend principe dat de patronen van ladingen en interacties vastlegt.

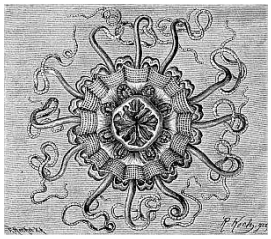
Ook in de scheikunde bepaalt de symmetrie van chemische verbindingen voor een groot gedeelte hun eigenschappen. Dit wordt weerspiegelt in de grote regelmaat van het Periodiek Systeem. Een mooi recent voorbeeld zijn de wonderbaarlijke *buckyballs* of fullerenen (bekroond met de Nobelprijs 1996).



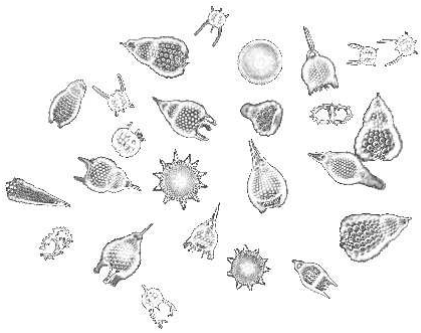
Dit zijn kooivormige C_{60} moleculen genoemd naar de radicale Britse architect R. Buckminster Fuller in wiens werk veel geometrische koepels voorkomen. De geometrische vorm is een afgeknotte icosaeder, opgebouwd uit regelmatige vijfhoeken en zeshoeken, al bekend bij Archimedes en vandaag de dag gebruikt als favoriet model voor een voetbal.

In de biologie vinden we vele organismes met een bij benadering symmetrische lichaamsbouw. Naast de gebruikelijke bilaterale spiegelsymmetrie, de links-rechts symmetrie die ook het menselijk

lichaam deelt, komen vooral bij lagere diersoorten allerlei draaiinggroepen van bijvoorbeeld orde 5, 8 of 12 voor.



Denk ook aan de prachtig symmetrische radiolaria of virussen, die een organische afspiegeling zijn van de Platonische wereld van regelmatige veelvlakken (waarover later meer).



Symmetrie in cultuur

Ook in de kunsten, bijvoorbeeld de beeldende kunst of de architectuur, speelt symmetrie een belangrijke rol in de vorm van de thema's herhaling en variatie. Zie de vele voorbeelden van ornamentiek, de classicistische bouwstijl of het grafisch werk van Escher.

In de muziek vinden we ook veel symmetrieën: herhalen van frasen, inversies van thema's, transposities. Interessant is dat hier de transformaties in de *tijd* in plaats van de ruimte plaatsvinden. Een partituur legt deze tijdsordening weer op papier vast. Zo kunnen we repeterende muzikale frasen direct vergelijken met betegelingen in de ornamentiek.

In voorbeelden uit de kunst vinden we natuurlijk een belangrijke esthetische component. Een symmetrische bouwstijl wordt als prettig en elegant ervaren. Ook voor de mens is symmetrie is een typisch schoonheidsideaal, zie bijvoorbeeld de inspanningen van de plastische chirurgie die de bilaterale invariantie van het menselijk gelaat zo perfect mogelijk proberen te benaderen.

Deze ervaring blijft niet alleen tot het uiterlijke beperkt. Van symmetrie gaat ook een sterke innerlijke suggestieve werking uit. Daarvan wordt bijvoorbeeld slim gebruikgemaakt in de psychologie bij

de Rorschachtest, die net als de kaleidoscoop de symmetrie gebruikt om van een willekeurige figuur, in dit geval een inktvlek, iets betekensivol te maken.

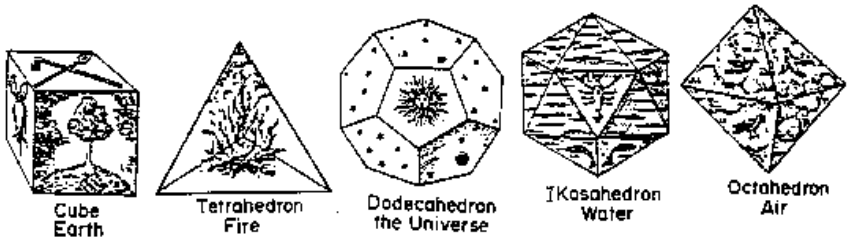
Tenslotte een voorbeeld van een symmetrie die we in allerlei gedaanten voorkomt maar die van een compleet ander karakter is. Bekijk een verzameling objecten, zeg een groep mensen. Iedereen in de groep is in principe uniek en verschillend van de overige leden. Maar als we de persoonlijke identiteit (even) vergeten en alle leden van de groep als identiek beschouwen, kunnen we mensen uitwisselen. Er ontstaat nu een symmetrie: de permutaties of verwisselingen van personen. In dit perspectief van de democratie (‘iedereen is gelijk’) of van de bestuurder (‘iedereen is vervangbaar’) kan ieder lid van de groep op willekeurige wijze verwisseld worden. Deze inwisselbaarheid is een fundamentele eigenschap van atomen en moleculen of elementaire deeltjes. In deze wereld is er werkelijk geen verschil te maken tussen twee elektronen. We kunnen niet stiekem er eentje markeren. Deze symmetrie staat bekend als Bose- of Fermi-statistiek.

Korte geschiedenis

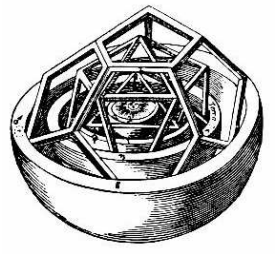
De mensheid is altijd gefascineerd geweest met symmetrische objecten. Voor Plato was het bestaan van de vijf regelmatige veelvlakken een hoogtepunt.

Deze vijf objecten — de tetraëder, kubus, octaëder, dodecaëder en icosaëder — worden verkregen door veelhoeken aan elkaar te plakken, zodanig dat in ieder hoekpunt even veel zijden bij elkaar komen. Hoewel er vijf bekend waren ten tijde van Plato, wordt eindelijk pas in in *De Elementen* van Euclides van Alexandrië (325–265 v.Ch.) bewezen dat er precies vijf zulke symmetrische veelvlakken zijn.

Plato geeft een diepe mystieke betekenis aan dit aantal vijf: het staat voor de vier elementen (aarde, water, lucht en vuur) plus de kosmos zelf (weergegeven door de dodecaëder).



Deze metafysische ideeënwereld dringt nog door tot de 16de eeuw. Zo was zelfs Johannes Kepler (1571–1630) gegrepen door de dwingende regelmaat. Kepler gebruikte de regelmatige veelvlakken om in 1595 een model van het zonnestelsel af te leiden. De banen van de op dat moment bekende planeten (in volgorde vanaf de zon: Mercurius, Venus, Aarde, Mars, Jupiter, Saturnus) kon hij benaderen door de binnen en buiten omschreven bollen van de regelmatige veelvlakken in elkaar te passen.



Helaas werden later de planeten Uranus (1781), Neptunus (1846) en Pluto (1930) ontdekt, terwijl er geen nieuwe veelvlakken gevonden zijn. Sindsdien staat Keplers poging bekend als een klassiek geval van een overenthousiaste toepassing van de voorliefde voor symmetrie in de fysica. We weten nu dat het aantal van negen planeten (min of meer — er gaan de laatste tijd stemmen op om Pluto te demoveren tot een astroïde) en de specifieke stralen van de planeetbanen min of meer willekeurig zijn. Sterker nog er zijn nu aanwijzingen dat om veel van de ontelbare vele sterren in het heelal planeetstelsels te vinden zijn, ieder met een specifiek aantal banen van een bepaalde steeds andere grootte. De werkelijke, verborgen symmetrie van het probleem bestaat niet uit de afmetingen van de zes planeetbanen die Kepler kende, maar is bevat in de eigenschappen van de wet van Newton, die de gravitationele interactie beschrijft. Newtons wetten waren gebaseerd op de uiteindelijke wetten van Kepler, die in een latere poging wel een waarachtige regelmaat in de planeetbanen wist te vinden. De symmetrie van het Keplerprobleem blijkt trouwens te bestaan uit rotaties in een abstracte ruimte met *vier* dimensies en is daarmee eigenlijk nog wonderlijker dan Kepler kon vermoeden.

Toch is de relevante wiskunde die nodig is om symmetrieën te beschrijven en te begrijpen, de *groepentheorie*, niet door de oude Grieken ontwikkeld, maar pas in de negentiende eeuw bedacht door het Franse genie Évariste Galois . Hij probeerde te begrijpen waarom het niet mogelijk was een algemene formule te vinden voor de nulpunten van een vijfdegraads polynoom: P. 5 ⟹ 56

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

Er waren wel eerder oplossingen gegeven, zij het met veel pijn en moeite, voor tweede-, derde- en vierdegraads vergelijkingen. De lezer zal vast de oplossing voor de tweedegraads vergelijking op de middelbare school hebben moeten leren:

$$ax^2 + bx + c = 0 \Leftrightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \text{ als } b^2 - 4ac \geq 0.$$

De Noorse wiskundige Niels Hendrik Abel (1802–1829) bewees een aantal jaren voor Galois dat voor de vijfdegraads versie inderdaad geen algemene formule gegeven kon worden.

Om de systematiek hierachter bloot te leggen heeft Galois de belangrijkste ingrediënten van de groepentheorie moeten introduceren. Galois was geen academicus en zijn geschriften werden dan ook maar nauwelijks begrepen. Bij een eerst poging tot publicatie werd aangedrongen zijn artikel later in te zenden, en uiteindelijk werd het werk afgewezen omdat definities ontbraken en de tekst daardoor niet goed begrepen werd.

Uiteindelijk kwam hij op twintig-jarige leeftijd al op tragische wijze om, in een duel zoals wel meer gebeurde in die tijd. Galois had zelf aan de vooravond van dit duel ook geen vertrouwen op een goede afloop en hij heeft op die avond alles wat hij wist proberen op te schrijven. Natuurlijk door het tijdgebrek werd dit geen volledig verslag, waarvan de volgend beroemd geworden notitie in de kantlijn nog getuigt:

Il y a quelque chose à completer sur cette demonstration. Je n'ai pas le temps.

De broer van Galois heeft de wiskundige nalatenschap nog proberen te slijten bij beroemdheden uit zijn tijd als Gauss en Jacobi. Pas dertien jaar na de dood van Galois komt het werk in handen van Liouville die het werk op zijn waarde weet te schatten en het uiteindelijk publiceert.

P 5.

ÉVARISTE GALOIS

1811 — 1832

NIELS HENDRIK ABEL

1802 — 1829

Nogmaals transformaties

We hebben gezien dat symmetrieën opgevat kunnen worden als transformaties die een object invariant laat. Neem bijvoorbeeld een kubus. Die kunnen we ronddraaien. Maar niet iedere draaiing brengt de kubus weer terug in de oorspronkelijke oriëntatie. Er zijn precies 24 rotaties die een kubus invariant laten. Als we de kubus voorstellen als een dobbelsteen zodat we de zes zijden kunnen onderscheiden,

breken we deze symmetrie. Zo zien we de 24 verschillende posities die de kubus kan innemen.

De symmetriegroep van een kubus bevat daarmee 24 transformaties: 9 rotaties over $90°$, 8 rotaties over $120°$, 6 rotaties over $180°$, en tenslotte 'niets doen', de identiteit — ook een belangrijk voorbeeld van een transformatie[1].

Wiskundig stellen we een transformatie voor met een abstract symbool, bijvoorbeeld T. Een transformatie voert een configuratie over in een andere, symbolisch geschreven als

$$\mathsf{T}\colon x \to y$$

Stel dat we nu een tweede transformatie S hebben, dan kunnen we de twee transformaties na elkaar laten werken, bijvoorbeeld eerst T dan S. Dit wordt geschreven als $\mathsf{S} \cdot \mathsf{T}$. Let op dat we de uitdrukking $\mathsf{S} \cdot \mathsf{T}$ dus van *rechts naar links* moeten lezen.[2]

Belangrijk is dat we op deze wijze weer een symmetrie verkrijgen. We kunnen de symmetrieën S en T 'vermenigvuldigen' en verkrijgen zo een nieuwe transformatie U. Symbolisch hebben we daarmee

$$\mathsf{S} \cdot \mathsf{T} = \mathsf{U}$$

Dit lijkt op de vermenigvuldiging van getallen, maar is het (meestal) niet. Zoals we direct zullen zien maakt het in het algemeen uit in welke volgorde we de vermenigvuldiging uitvoeren

$$\mathsf{S} \cdot \mathsf{T} \neq \mathsf{T} \cdot \mathsf{S}$$

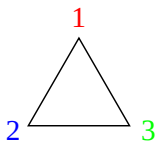
We zeggen dat de vermenigvuldiging van transformaties in het algemeen *niet commutatief* is.

[1] We sluiten altijd voor compleetheid de triviale transformatie in. In de wiskunde heeft dus ieder object dus op z'n minst één symmetrie, namelijk de transformatie die alles op z'n plaats laat! Het serieus nemen van het triviale is een veelvoorkomend en diep thema in de wiskunde: nul is ook een getal, de lege verzameling is ook een verzameling, geen relatie is ook een relatie, etc. Vergelijk het met het belang van het vacuüm in de fysica.

[2] Deze vermenigvuldiging van komt overeen met de compositie van twee functie als gedefinieerd in T. 1 op pagina 12.

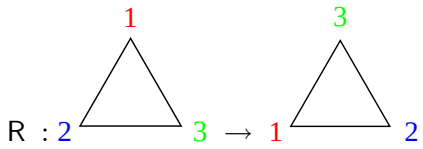
Symmetrieën van de driehoek

Laten we om ons te oriënteren een heel eenvoudig concreet voorbeeld bekijken — de gelijkzijdige driehoek. Om de transformaties goed te kunnen aangeven nummeren we de hoekpunten 1, 2, 3.

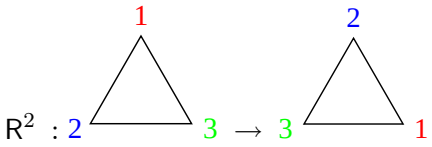


Wat zijn de transformaties van het vlak die deze driehoek op zichzelf afbeelden?

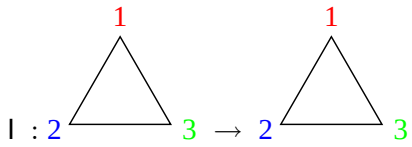
Een duidelijke kandidaat is een rotatie (tegen de klok in) over 120 graden. Laten we deze rotatie R noemen.



Wat gebeurt er als we tweemaal de operatie R uitvoeren? In dat geval draaien we over 240 graden en dit is weer een symmetrie van onze driehoek. We noteren deze transformatie als $\mathsf{R} \cdot \mathsf{R}$ of ook als R^2.



Het is duidelijk dat als we de operatie R driemaal uitvoeren, het figuur op zijn plaats blijft, omdat we over 360 graden draaien. Dat wil zeggen, de transformatie R^3 is gelijk aan de *triviale* transformatie, de identiteit, waarbij alles op z'n plaats blijft. We schrijven deze transformatie als I.

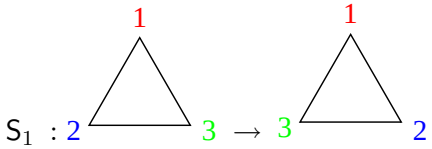


Symbolisch geldt dus de relatie

$$\mathsf{R}^3 = \mathsf{I}.$$

We lezen deze relatie als: driemaal R toegepast geeft de identiteit.

Er zijn nog meer symmetrieën van onze driehoek. Ook een spiegeling in een as door een hoekpunt, loodrecht op een zijde, is een invariantie van het figuur. We noteren de spiegeling door het hoekpunt 1 als S_1, de spiegeling door het hoekpunt 2 als S_2, en de spiegeling door het hoekpunt 3 als S_3. Concreet hebben we



en soortgelijk voor S_2 en S_3. Het is goed nu een lijst te maken van alle symmetrieën die we tot nu toe gevonden hebben:

$$\mathsf{I},\ \mathsf{R},\ \mathsf{R}^2,\ \mathsf{S}_1,\ \mathsf{S}_2,\ \mathsf{S}_3.$$

Omdat de symmetrie volledig vastligt door de actie op de drie hoekpunten die op $3! = 6$ verschillende manieren gepermuteerd kunnen worden, vinden we dus dat ons lijstje noodzakelijkerwijs compleet is. Er zijn precies 6 symmetrieën van de driehoek.

We kunnen ons nu afvragen wat er gebeurt als we twee symmetrieën na elkaar uitvoeren. Als we bijvoorbeeld tweemaal spiegelen vinden we de identiteit, zodat

$$S_1 \cdot S_1 = I.$$

Een interessante vraag is wat er gebeurt als we spiegelingen met rotaties combineren. Laten we eerst spiegelen met S_1 en daarna roteren met R. Onze notatie hiervoor is $R \cdot S_1$. Maar als we deze transformatie uitvoeren vinden we dat dit precies het resultaat geeft van de spiegeling S_3! We schrijven daarom

$$R \cdot S_1 = S_3.$$

We kunnen ons ook afvragen of het uitmaakt of we eerst spiegelen en dan roteren of de operaties in de omgekeerde volgorde uitvoeren. Controleer zelf dat

$$S_1 \cdot R = S_2,$$

zodat we concluderen dat

$$R \cdot S_1 \neq S_1 \cdot R$$

Op dit moment is het handig een zogeheten *vermenigvuldigingstabel* te maken. Verticaal zetten we de transformatie T en horizontaal de transformatie T'. In de tabel zetten we dan de samenstellingen $T \cdot T'$. Voor het geval van de symmetrieën van de driehoek vinden we zo

	I	R	R^2	S_1	S_2	S_3
I	I	R	R^2	S_1	S_2	S_3
R	R	R^2	I	S_3	S_1	S_2
R^2	R^2	I	R	S_2	S_3	S_1
S_1	S_1	S_2	S_3	I	R	R^2
S_2	S_2	S_3	S_1	R^2	I	R
S_3	S_3	S_1	S_2	R	R^2	I

Probeer zelf deze vermenigvuldigingsregels uit op de webpagina.

Definitie van een groep

We hebben nu in voorbeelden genoeg gezien om de abstracte definitie van een groep te geven. Een groep bestaat uit een aantal objecten, zoals bijvoorbeeld het soort transformaties wat we hierboven bespraken, S, T, $U \ldots$. Verder is er een regel gegeven die twee transformaties kan samenstellen, $\xrightarrow{\text{T. 12}}$ 64 bijvoorbeeld $S \cdot T = U$. Het resultaat van zo'n samenstelling moet weer een element van de groep zijn. We zeggen ook wel dat de groep *gesloten* moet zijn voor vermenigvuldiging.

Verder is er een *eenheids-* of *neutraal element* I in zo'n groep. In het geval van de hierboven gegeven transformaties is dat de identieke transformatie. Formeel moet zo'n element zich gedragen als 1 bij gewone vermenigvuldiging:

$$T \cdot I = I \cdot T = T$$

voor elk groepselement T.

Daarnaast moet elk element geneutraliseerd of 'ongedaan gemaakt' kunnen worden. Daarvoor is voor elk groepselement een *inverse element* nodig. Denk aan $\frac{1}{x}$ voor elk getal x in het geval gewone vermenigvuldiging. In het algemeen schrijven we T^{-1} voor de inverse van een groepselement T, en de regel voor inverse elementen zegt dan dat

$$\mathsf{T}^{-1} \cdot \mathsf{T} = \mathsf{T} \cdot \mathsf{T}^{-1} = \mathsf{I}$$

voor elk zo'n groepselement T.

Tenslotte, als we drie transformaties $\mathsf{S}, \mathsf{T}, \mathsf{U}$ samenstellen waarbij we tweemaal moeten vermenigvuldigen, maakt het niet uit welke vermenigvuldiging we eerst doen (waar de haakjes staan)

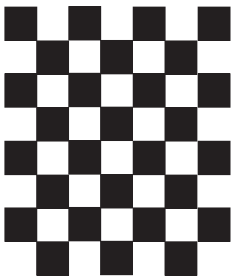
$$\mathsf{S} \cdot (\mathsf{T} \cdot \mathsf{U}) = (\mathsf{S} \cdot \mathsf{T}) \cdot \mathsf{U}$$

voor elk drietal $\mathsf{S}, \mathsf{T}, \mathsf{U}$. Deze eigenschap wordt *associativiteit* genoemd. Het betekent dat we zonder bezwaren de haakjes in een vermenigvuldiging van drie elementen kunnen weglaten: $\mathsf{S} \cdot \mathsf{T} \cdot \mathsf{U}$. De volgorde van paring doet er niet toe.

Iedere verzameling met een vermenigvuldiging die aan de bovenstaande drie eisen voldoet is een groep. Laat bijvoorbeeld zien dat de verzameling $\{\mathsf{I}, \mathsf{T}\}$ met $\mathsf{T}^2 = \mathsf{I}$ een goed voorbeeld van een groep is. Was is in dit geval de inverse van T?

Gebroken symmetrie

Wat voor symmetriegroepen komen we tegen in de natuur? Het voor de hand liggende antwoord is 'geen een'. Als we zo om ons heen kijken ziet de wereld er namelijk niet erg symmetrisch uit. Er zijn natuurlijk wel objecten met een grote symmetrie, zoals bijvoorbeeld een schaakbord.



Als we dit patroon oneindig voortzetten dat heeft het allerlei symmetrieën waarbij we het bord een aantal vakjes opzij of naar boven schuiven. Zo'n translatie laat het patroon invariant. We kunnen dit symbolisch schrijven als

$$\textit{schaakbord} = \mathsf{T}(\textit{schaakbord}).$$

Maar als in het bos lopen en in het rond kijken is het waarschijnlijker dat we eerder iets zien zoals

dit

Zo'n bladerendek heeft geen in het oog springende symmetrische eigenschappen. Als we het plaatje opzij schuiven krijgen we iets compleet anders. Alhoewel, krijgen we wel iets dat wezenlijk anders is?

Eigenlijk is het verschoven plaatje een net zo'n overtuigend beeld van een met bladeren bedekt bospaadje. In zekere zin verandert er niet veel. Het enige wat de translatie doet is dat het een bladerenpatroon verandert in een ander, even waarschijnlijk in de natuur voorkomend, bladerenpatroon. We moeten hier dus schrijven

$$\textit{bospaadje 2} = \mathsf{T}(\textit{bospaadje 1}).$$

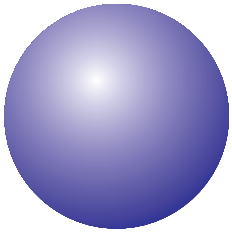
Waarom noemen we de translatie T nog een symmetrie ook al is het bladerenpatroon er niet invariant onder?

Wel, voordat de bladeren op het pad vielen en er een perfect leeg vlak bestond, was de situatie nog volledig translatie-invariant. Op het moment dat de bladeren gingen vallen moest er een keus gemaakt worden. Zo'n blad moet ergens op het pad terecht komen. Ieder punt is a-priori even waarschijnlijk, maar vanwege het elementaire feit dat een blad dat hier valt ook niet daar kan vallen wordt de oorspronkelijke symmetrie niet langer gerespecteerd. We zeggen dat de symmetrie *gebroken* wordt. Een symmetrie heet gebroken als onze beschrijving, zeg de natuurwetten, invariant zijn onder de transformatie in kwestie, maar de concrete realisatie, de oplossing van de wetten, niet. Vele van de symmetrieën 'in het vrije veld' zijn gebroken.

Een gebroken symmetrie zal altijd een configuratie relateren aan een andere, even goede, realisatie van onze wereld. Aan alle natuurwetten wordt voldaan. Dit is gerelateerd aan een relativistisch principe: er is geen absoluut centrum van de wereld, maar als je afstand wil meten moet je ergens beginnen, ergens een oorsprong, een nul kiezen.

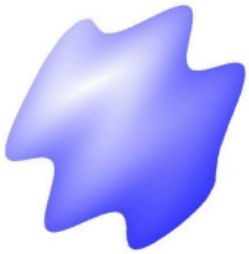
Perfecte bollen en aardappelen

Laten we een tweede voorbeeld bekijken van een (gebroken) symmetrie. We beginnen met een perfecte bol

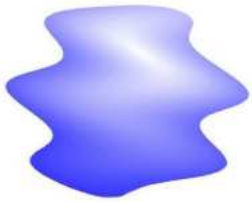


Deze is duidelijk invariant onder alle rotaties rond het middelpunt. Maar is het mogelijk in de praktijk zo'n perfecte, Platonische bol te maken? Zullen er niet altijd, microscopisch kleine bobbeltjes en

krasjes in zitten. Maar in dat geval hebben we eerder te maken met wat je karikaturaal een aardappel kan noemen, een misbaksel van een bol.



Zo'n pokdalig geval is onder geen enkele beweging invariant. Maar, als we hem roteren krijgen we een net zo'n representatief voorbeeld van een aardappel!



Een ander voorbeeld: de roulette. Voordat we het balletje laten vallen zijn alle vakjes even waarschijnlijk (als het goed is). Toch valt het balletje maar in één vakje. Ook al waren in principe alle vakjes gelijk, de uiteindelijke situatie dwingt tot een keuze — het balletje moet gewoon ergens blijven liggen. De symmetrie wordt gebroken, en misschien ook de bankrekening.

We kunnen de symmetriebreking zo als een actieve handeling opvatten: het vallen van de bladeren, het indeuken van een bal, het gooien van het rouletteballetje. Een ander favoriet voorbeeld is de keuze die men moet maken tussen het linker of rechter broodbordje bij een symmetrische tafelschikking. Als de eerste kiest voor het linker of rechterbordje moet de rest van de tafel volgen. Daarmee is de links-rechts symmetrie definitief gebroken.

Breking en ondergroepen

Laten we dit alles nu proberen te formaliseren. Als een symmetriegroep G gebroken wordt kan er nog een kleinere symmetriegroep H overblijven (de *ongebroken* symmetrie). Welke paren G en H kunnen zo voorkomen. Hier is een mooie stelling voor.

Bij symmetriebreking wordt de symmetrie G altijd gebroken tot een ondergroep $H \subset G$.

Een ondergroep is een deelverzameling die zelf weer een groep is. Bijvoorbeeld in het geval van de symmetriegroep van de gelijkzijdige driehoek

kunnen we alleen de rotaties beschouwen en geen spiegelingen. Deze groep bestaat dan uit drie elementen

$$H = \{\mathsf{I}, \mathsf{R}, \mathsf{R}^2\}$$

Deze sluiten in zichzelf: de samenstelling van twee rotaties is weer een rotatie. Deze kleinere ondergroep treedt op als symmetrie van de volgende deformatie van de driehoek

We kunnen ook een vaste spiegeling S nemen en de ondergroep

$$H = \{\mathsf{I}, \mathsf{S}\}$$

beschouwen. Dit is de symmetrie van een andere deformatie van onze driehoek.

Het monster

We hebben al gezegd dat de wiskunde probeert 'structuren van structuren' te vinden. In het geval van de bestudering van symmetrieën komt dit neer op een classificatie van alle mogelijke symmetriegroepen. Het is een prachtig resultaat dat dit inderdaad mogelijk is. Het is gelukt een complete beschrijving te geven van alle (enkelvoudige, eindige) groepen. Dit was een megaproject waar vele wiskundigen bij betrokken waren en dat pas rond 1990 beëindigd is.

Toen de mist was opgetrokken bleek het antwoord redelijk eenvoudig. Er zijn een aantal regelmatige oneindige reeksen, zoals bijvoorbeeld permutaties van n objecten met $n = 1, 2, 3, \ldots$. Verder zijn er 24 zogenaamde sporadische groepen. Dit zijn groepen die volledig op zichzelf staan en niet in een of ander patroon vallen. De grootste en laatste die gevonden werd heet 'het monster'.

De wiskunde kent geen Nobelprijs. Het ontbreken van een Nobelprijs voor de wiskunde wordt meestal toegeschreven aan een affaire tussen mevrouw Nobel en de bekende 19de-eeuwse Zweedse wiskundige Mittag-Leffler. Maar dit is historisch onjuist, zo is Nobel nooit getrouwd geweest. De Fieldsmedaille wordt slecht eens in de vier jaar uitgereikt en alleen aan kandidaten onder de veertig. Net als een Olympisch topsporter kan een wiskundige dus ongelukkig pieken, zoals Andrew Wiles overkwam die net na zijn veertigste verjaardag de Laatste Stelling van Fermat wist te bewijzen.

In 1998 werd de Fieldsmedaille toegekend aan Richard Borcherds voor zijn werk aan de monstergroep. Het monster is de grootste sporadische groep, met

$$808017424794512875886459904961710757005754368000000000$$

verschillende symmetrieën. Het monster treedt op als symmetriegroep van een hele bijzondere algebraïsche structuur afkomstig uit de snaartheorie uit de hoge-energiefysica. De kleinste ruimte waarin deze groep kan werken bestaat uit 196884 dimensies!

TECHNIEK 12.

Groepen

Een groep G *is een verzameling tezamen met een* operatie *waarmee elk paar van elementen van* G *gecombineeerd kunnen worden. Zo'n combinatie levert dan altijd weer een element van* G *op. De combinatie van twee objecten* a, b *in* G *schrijven we als* $a * b$ *of kortweg* ab*. De volgorde van combineren kan een verschillend resultaat opleveren, en dus geldt niet in het algemeen dat* $ba = ab$*. Waar wel aan voldoen moet worden*

1. *Er is een* neutraal *of* eenheids*element in* G*. Dat wil zeggen dat er een* $e \in G$ *moet zijn zodanig dat*

$$\forall x \, ex = xe = x$$

2. *Voor elk element moet er een* neutraliserend *of* inverse *element in* G *zijn:*

$$\forall x \, \exists y \, xy = yx = e$$

3. *De combinatie van een geordend drietal levert een uniek resultaat.*

$$\forall x \, \forall y \, \forall z \, (xy)z = x(yz)$$

Een ondergroep H *van een groep* G *is een groep waarvan alle elementen ook in* G *voorkomen en de elementen gecombineerd worden precies als in* G*.*
Een heel vertrouwde oneindige groep wordt gevormd door de gehele getallen $\mathbb{Z}$ *met optelling als operatie. Het eenheidselement is* 0 *en voor elk getal* x *is er een inverse* $-x$*. Een ondergroep is bijvoorbeeld* $2\mathbb{Z}$ *de verzameling van alle even gehele getallen. Elke optelling van twee even getallen is weer even.*
De gehele getallen met gewone vermenigvuldiging vormen geen groep. Er is niet voorzien in inverse elementen. De breuken zonder 0*,* $\mathbb{Q} - \{0\}$ *vormen wel een groep onder vermenigvuldiging. Het eenheidselement is* 1 *en voor elke breuk* x *is er een inverse* $1/x$*.*
Bekende eindige groepen komen uit de 'modulaire' rekenkunde uitgebreid bestudeerd in de achttiende eeuw door Euler en Gauss. Voorbeelden hiervan zijn de groepen $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$ *met optelling modulo* n*. Deze groep komt overeen met* $\mathbb{Z}$ *waarbij we getallen gelijk (equivalent) beschouwen als ze de zelfde 'rest' opleveren na deling door* n*. Bijvoorbeeld* $3 + 3 = 1$ *in* $\mathbb{Z}/5\mathbb{Z}$*. Het eenheidselement is* 0 *en voor elke* x *is er een inverse* $n - x$*.*
Met vermenigvuldiging vormt $\mathbb{Z}/n\mathbb{Z}$ *weer geen groep, wederom door het ontbreken inversen. In het geval dat* n *een priemgetal is vormt* $\mathbb{Z}/n\mathbb{Z} - \{0\}$ *wel een groep!*
De voorbeelden hier zijn allemaal commutatieve of Abelse *groepen. Voorbeelden van niet-commutatieve groepen zijn de permutatie-groepen zoals de transformaties die hier in dit hoofdstuk besproken zijn. Het kan natuurlijk wel zijn dat deze groepen wel commutatieve ondergroepen hebben, zoals de rotatie-ondergroep van de driehoekstransformaties.*

2.2 Structuurgelijkenis, invariantie en taal

Symmetrie wil zeggen dat een structuur hetzelfde blijft als we zijn objecten verplaatsen met een transformatie. We hebben in het vorige hoofdstuk al vele mooie wiskundige symmetrieën gezien, die vaak een afspiegeling vormen van symmetrieën in de natuur om ons heen. Zoals steeds in de opzet van dit boek maken we nu een verdere stap naar logica, taal en cognitie. Maar eigenlijk is die stap al lang voor ons gezet, en wel in de negentiende eeuw! Het was de bekende geleerde Hermann von Helmholtz die opmerkte dat de fundamentele meetkundige transformaties van translatie en rotatie overeenkomen met de *natuurlijke bewegingen* van het menselijk lichaam. Hij formuleerde vervolgens de baanbrekende hypothese dat ons denken dus speciaal gericht zal zijn op *invariante patronen* die we herkennen dwars door zulke bewegingen heen. Een goed voorbeeld is de relatie "tussen". Als een punt P zich bevindt tussen twee andere punten Q, R (eventueel samenvallend met een van deze twee punten), dan kunnen we dit nooit anders 'zien', hoe we ons ook bewegen. Altijd blijven ze op een lijn liggen, nooit ligt plotseling Q echt tussen P en R. En inderdaad is het begrip 'liggen op een lijnstuk' essentieel in de meetkunde. Maar dit inzicht valt natuurlijk nog verder door te trekken. Niet toevallig heeft onze natuurlijke taal ook een basiswoord voor de relatie "tussen"die ons helpt te beschrijven wat we om ons heen zien. Mensen zijn van nature al 'afgestemd' op de symmetrieën en invarianties in hun omgeving, en hun taal benoemt daarvan de meest voorkomende en nuttige. In het vervolg van dit hoofdstuk maken we deze inzichten wat preciezer, waarbij de formele talen van het vorige hoofdstuk een nuttige rol spelen.

P 6.

HERMANN VON HELMHOLTZ

1821 — 1894

Transformaties en structuurniveaus Transformaties en symmetrie komen in de wiskunde op allerlei niveaus voor. Er is niet één beste beschrijvingswijze die voor alle gevallen moet worden gebruikt. Zo bekijkt een wiskundige de ruimte heel gedetailleerd in de Euclidische meetkunde, met een kleine klasse van toegestane 'starre transformaties' (translatie, rotatie, spiegeling). Zoals eerder gesteld, ligt dit veel grover in de topologie, die werkt met een veel grotere klasse van transformaties die figuren

mogen deformeren, zodat driehoeken kunnen overgaan in andere gesloten figuren zoals vierkanten of cirkels. Heel in het algemeen beschrijft een wiskundige theorie altijd een klasse van structuren (meetkundige ruimten, groepen, grafen, enzovoort) met daarbij expliciet aangegeven welke transformaties geacht worden die structuur te bewaren. In feite gaf ons vorige hoofdstuk al een mooi eenvoudig voorbeeld van deze werkwijze. We lopen dit nog eens langs.

Van tellen naar ordenen In het vorige hoofdstuk classificeerden we verzamelingen naar hun zuivere omvang. In wiskundige zin wilde dat zeggen dat we voor doeleinden van tellen twee verzamelingen als gelijk beschouwen als er een *bijectie* tussen bestaat. Met andere woorden, de relevante transformaties zijn in dit geval bijecties. Dit is natuurlijk een heel ruwe manier van 'gelijkschakelen'. Bijvoorbeeld, elk object mag worden verwisseld met een ander: hun individuele eigenaardigheden doen er niet toe. Dit is het interesse-niveau van een toer-gids die bij een excursie op een wetenschappelijk congres alleen de aantallen telt bij in- en uitstappen van de bus, in willekeurige volgorde: of het nu gaat om grote gevestigde genieën, of aankomende studenten. Op zichzelf is dit natuurlijk een onschatbare les in bescheidenheid. Maar het enige typisch invariante patroon onder al deze transformaties is het aantal objecten, ofwel de kardinaliteit van de verzameling.

T. 3 ⟸ 16

Een ander voorbeeld van een transformatie die dwars door aanwezige structuur heen walst is de bijectie die Cantor construeerde tussen de gehele getallen $\mathbb{Z}$ en de breuken $\mathbb{Q}$. Beide zijn aftelbaar, maar het is zonneklaar dat deze twee wiskundige structuren drastisch verschillen in hun *ordening*. De gehele getallen liggen 'discreet': bij elk getal n is er een onmiddellijke opvolger $n+1$ en een onmiddellijke voorganger $n-1$. Maar de breuken liggen juist 'dicht': tussen elke twee verschillende breuken ligt steeds een derde, en er zijn helemaal geen onmiddellijke opvolgers of voorgangers. Als we dit soort verschillen willen verantwoorden, bijvoorbeeld omdat we niet louter willen tellen, maar *ordenen*, dan moeten we deze ordeningsstructuur expliciet maken, en hiermee gepaard, de klasse toegestane transformaties inperken. We staan dan alleen nog bijecties toe die de ordeningsstructuur respecteren. Ook dergelijke transformaties komen in de wiskunde veel voor.

Ordening en isomorfisme Als we ook de ordening $<$ willen respecteren in onze vergelijking van wiskundige structuren, dan werken we voortaan alleen met orde-bewarende bijecties, ofwel *orde-isomorfismen*. Het mooie woord 'isomorfisme' betekent letterlijk 'vormgelijkheid'. In T. 13 staat een precieze definitie. Om dit begrip te illustreren kiezen we hele eenvoudige wiskundige structuren, en wel *geordende grafen* bestaande uit een stel punten met een ordeningsrelatie aangeduid met pijlen. Als er een pijl loopt van een punt a naar een punt b, dan staat het paar $\langle a, b\rangle$ in de relatie. Grafen geven wiskundige relaties weer, zoals beschreven in hoofdstuk 1, maar ze worden ook veel gebruikt voor beschrijven van sociale relaties zoals "a is een kind van b" of "a kent b". Hier is een concrete illustratie. Tussen de volgende driehoeken, opgevat als grafen, loopt kennelijk een bijectie, want ze zijn even groot.

Maar er bestaat geen orde-isomorfisme dat de ene driehoek in de andere overvoert. Neem bijvoorbeeld het punt rechtsonder in de linkergraaf. Dit heeft twee ‘opvolgers’ in de relatie. Elke bijectie zal dit punt naar een punt in de tweede figuur sturen en de twee opvolgers naar verschillende punten. Tenminste één ervan moet dan echter zijn opvolgersrol verloren hebben, want in de rechterfiguur is er geen punt met twee verschillende opvolgers. Elke bijectie verstoort dus het patroon. Als we ons beperken tot de linkerdriehoek, dan valt het verschil tussen orde-bewarende en orde-verstorende isomorfismen ook nog eens anders te beschrijven. Er zijn zes bijecties van de driehoek op zichzelf: de permutaties van de drie hoekpunten. Hiervan zijn er echter slechts drie orde-isomorfismen. Als we namelijk een punt x naar een ander punt $f(x)$ sturen, dan liggen in het geval van een orde-isomorfisme f de andere twee waarden al vast: de directe opvolger van x moet gaan naar de directe opvolger van $f(x)$, en evenzo met de directe voorganger. Hiermee ligt de hele functie vast.

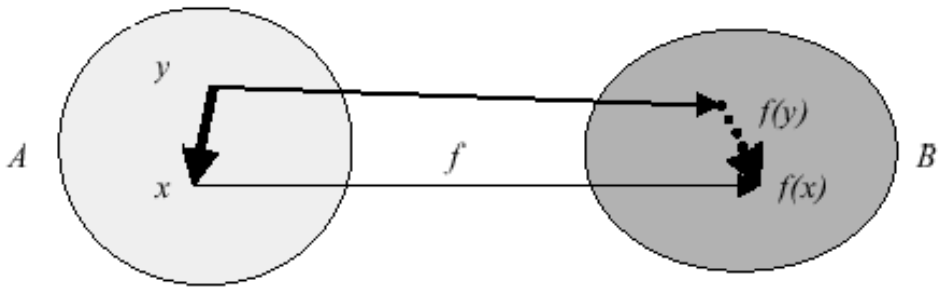
TECHNIEK 13.

Orde-isomorfisme

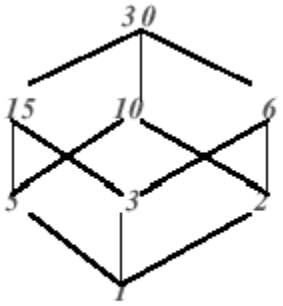
Laat A en B twee verzamelingen zijn, en $<_A$ en $<_B$ twee ordeningen (twee-plaatsige relaties) op A en B respectievelijk. Een orde-isomorfie *$f : A \to B$ is een bijectie waarvoor geldt dat*

$$\forall x \in A \, \forall y \in A \, (x <_A y \to f(x) <_B f(y))$$

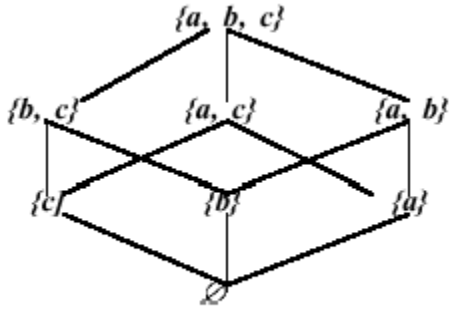
De structuren $\langle A, <_A \rangle$ en $\langle B, <_B \rangle$ heten dan orde-isomorf*. Dit is een equivalentie tussen structuren.*
Deze definitie wordt niet alleen gebruikt voor de bekende ordeningsstructuren in onze tekst, maar ook voor structuren met relaties in het algemeen. In het plaatje hieronder is dat nog eens abstract getekend: de relatie tussen objecten moet behouden blijven na het overvoeren in de andere verzameling.



Orde-isomorfismen kunnen verrassend zijn, en nuttige analogieën aan het licht brengen tussen structuren die we op het eerste gezicht niet met elkaar in verband zouden brengen. Het plaatje hieronder laat zien hoe soms verzamelingstructuur en getalstructuur overeenkomen. In de linker figuur staan de delers van 30 aangegeven, en in de tweede alle deelverzamelingen van een verzameling van drie elementen $\{a, b, c\}$. De ordening links is de relatie ‘deler van’, en rechts de deelverzamelingsrelatie $\subseteq$.



Delers van 30



P({a, b, c})

In de plaatjes loopt de ordening naar boven toe. Bijvoorbeeld, 1 is deler van alle getallen, terwijl $\emptyset$ deelverzameling is van alle verzamelingen. Het getal 3 is deler van 3, 6, 15 en 30. De verzameling $\{b\}$ is deelverzameling van $\{b\}$, $\{a, b\}$, $\{b, c\}$ en $\{a, b, c\}$. Het orde-isomorfisme zal duidelijk zijn.

Een typisch gevolg van een dergelijk isomorfisme is dat niet alleen de basis-ordening wordt bewaard, maar ook verder noties die we in termen van die ordening kunnen *definiëren*. Zo worden ook operaties binnen de ene structuur overgevoerd op de andere. Een mooi voorbeeld is de getalsconstructie van de *grootste gemene deler*: het grootste getal dat twee gegeven getallen deelt. Als we deze definitie letterlijk transporteren naar de andere structuur via het orde-isomorfie, dan krijgen we in de verzamelingenstructuur precies een andere bekende constructie, en wel de *doorsnede* van twee gegeven verzamelingen. In een formule:

$$f(\text{ggd}(x, y)) = f(x) \cap f(y).$$

Eenzelfde verband geldt voor het kleinste gemene veelvoud van twee getallen en de vereniging van de corresponderende verzamelingen. Isomorfismen helpen ons om eenheid te zien in de wiskunde: onder geschikte transformaties doen we soms op verschillende gebieden 'hetzelfde'. Er zijn vele beroemde verrassende isomorfismen.

Invarianten voor transformaties Transformaties gaan altijd gepaard met *invariante eigenschappen*, of kortweg 'invarianten'. Zo bewaarden bijecties de kardinaliteit $|A|$ van een verzameling A, maar niet altijd diens ordening. Orde-isomorfismen bewaren die laatste wél. Invarianten kunnen eigenschappen van verzamelingen zijn, relaties tussen objecten, of wiskundige operaties. Nog eens de regel bij dit alles: hoe kleiner de klasse van transformaties (vanwege sterkere eisen van 'structuurbewaring'), hoe meer invariante eigenschappen!

Deze manier van denken is wijd verbreid in de moderne wetenschap. Helmholtz' oorspronkelijke observaties zijn gaandeweg ver doorgedrongen. Zo volgt onze beschrijving van de wiskunde het 'Erlanger Programma' van Felix Klein, een bekend wiskundige in de tweede helft van de negentiende eeuw, die stelde dat elke bona fide wiskundige theorie een klasse transformaties kiest over haar structuren, en vervolgens de invarianten tot de centrale objecten van haar studie maakt. Soortgelijke ideeën zijn inmiddels ver doorgedrongen in de natuurkunde (denk aan de beroemde 'Lorentz transformaties' in de relativistische mechanica), informatica, en andere exacte disciplines, maar ook in de sociale wetenschappen, zoals de psychologie.

We merken nogmaals op dat bij dit alles geen uniek optimaal beschrijvingsniveau bestaat! Diverse niveaus kunnen natuurlijk zijn voor theorievorming, en noch de wiskunde, noch andere wetenschappen vertellen ons waar we de lat moeten leggen. Dit belangrijke inzicht werd nog eens treffend

verwoord tijdens de impeachment procedure voor de vorige Amerikaanse president, die tijdens de Lewinsky hearings de volgende behartigenswaardige woorden sprak:

Clinton's principe

"It all depends on what you mean by 'is'."...

Overigens kunnen we het verschijnsel invariantie ook heel goed andersom benaderen. Als er *geen* transformatie is te vinden in de gegeven klasse die een verzameling A overvoert in een verzameling B, dan ligt dit aan een klaarblijkelijk *structuur-verschil* op het niveau van die transformaties. Een voorbeeld hiervan zijn de eerdere gehele getallen $\mathbb{Z}$ versus de breuken $\mathbb{Q}$. Er is eenvoudig in te zien dat er geen orde-bewarende bijectie tussen deze twee verzamelingen kan bestaan. Maar dat konden we ook concreet benoemen in de dichtheid van de breuken versus de discreetheid van de gehele getallen. Met deze opmerking komen we toe aan de volgende stap in onze analyse van transformaties en invarianten.

Invarianties genereren taal! Helmholtz suggereerde reeds dat invarianties worden 'verwoord' in een *taal*. En inderdaad zijn de patronen die we bewaren onder transformaties vaak juist de wiskundige begrippen die we eerder expliciet beschreven in de taal van Hoofdstuk 1. In het geval van onze eerdere grafen zijn dat relaties als 'x deelt y' of 'y is een onmiddellijke opvolger van x':

$$x < y \wedge \neg\exists z\,(x < z \wedge z < y)$$

Nog een voorbeeld was 'x is de grootste gemene deler van y en z'.

Een rijke structuur vraagt om een rijke taal, die nodig is om alle eigenschappen weer te geven die invariant blijven onder de toegestane transformaties. Een arme structuur, met veel transformaties die ruw kunnen omspringen met objecten, heeft slechts een arme taal nodig, omdat maar weinig eigenschappen deze 'mishandeling' overleven. Een invariant voor gewone meetkundige transformaties was, zoals we reeds zagen, het begrip "x ligt tussen y en z", omdat rechte lijnen steeds in rechte lijnen overgaan. Maar zogenaamde 'continue transformaties' in de topologie laten dit begrip niet langer invariant. Een lijn kan dan heel goed overgaan in een kromme. Topologische begrippen die zelfs alle continue transformaties overleven zijn de wiskundige tegenhangers van voorzetsels als 'binnen' en 'buiten', maar ook meer verfijnde begrippen van 'benadering' van punten door rijen van punten.

Samenvattend, voor de wiskunde, en vele andere wetenschappen, geldt:

Waar invarianties zijn ontstaat taal!

Een transformatie kunnen we zien als een *analogie*. Definieerbare eigenschappen van objecten in de ene structuur worden overgedragen naar hun tegenhangers in de andere. Maar we kunnen deze rol van taal ook nog eens anders, hoewel equivalent, illustreren. Als er geen transformatie is, dan is er kennelijk een wezenlijk *verschil*, en het is juist de rol van taal om dergelijke verschillen te *benoemen*. Ook deze rol van taal zagen we reeds enkele keren in het voorgaande. In de eerdere twee driehoekjes gold bijvoorbeeld dat rechts elk punt een opvolger heeft via een vertrekkende pijl, en links niet. Dit verschil is simpel in onze ordeningstaal te definiëren via de structuur-eigenschap:

$$\forall x\,\exists y\,x < y.$$

Evenzo verschilden de gehele getallen en de breuken echt qua ordening, en dit kunnen we expliciet uitdrukken in onze wiskundige taal als een eigenschap die wel opgaat voor $\mathbb{Q}$ en niet voor $\mathbb{Z}$:

$$\forall x\,\forall y\,(x < y \rightarrow \exists z\,(x < z \wedge z < y))$$

Structuren

Een structuur A *voor een wiskundetaal met basispredicaten* $P1, P2, \ldots$ *en constanten* $c1, c2, \ldots$[a] *bestaat uit*

- *een* domein $\mathcal{D}_A$ *van individuen (ook wel objecten genoemd),*
- *voor elke constante* c *een individu* $c_A \in \mathcal{D}_A$*, en*
- *voor elk* n*-plaatsig basispredicaat* P *een verzameling* P_A *van* n*-tallen in* $\mathcal{D}_A$*:* $P_A \subseteq \mathcal{D}_A^n$*.*

Het element c_A *en de verzameling* P_A *zijn de* interpretaties *van* c *en van* P *in* A*. Een atomaire bewering (zonder variabelen)* $P(a1, .., an)$ *is* waar *in* A *als geldt dat het tupel*

$$\langle a1_A, \ldots, an_A \rangle \in P_A.$$

Op basis van deze definitie kan nu elke formule uit de taal geëvalueerd worden. We laten details hier achterwege omdat de variabelen in predikaatlogische formules deze definitie enigszins gecompliceerd maken. Elke goede logica-inleiding verschaft nadere informatie.
In de tekst zijn wel enkele eenvoudige concrete voorbeelden gegeven, met ongelabelde grafen als de structuren. De taal heeft dan een enkel twee-plaatsig basispredicaat dat naar de pijlen in het diagram verwijst, en het uitverkoren predicaat $=$ *van gelijkheid.*

Structuur-isomorfisme

Om gelijkheid van structuren te definiëren moeten we het begrip orde-isomorfie in T. 13 generaliseren. Als A *en* B *structuren zijn voor dezelfde predicatenlogische taal, met een gegeven lexicon van constanten en basispredicaten, dan is* $f : \mathcal{D}_A \to \mathcal{D}_B$ *een* stuctuur-isomorfisme *indien* $f(c_A) = c_B$ *voor elke constante* c*, en voor elk* n*-plaatsig basispredicaat* P *geldt dat*

$$\langle d_1, \ldots, d_k \rangle \in P_A \Leftrightarrow \langle f(d_1), \ldots, f(d_k) \rangle \in P_B.$$

Deze eis verwoordt dat elk predicaat P invariant *is onder* f*. Omdat de wiskundetaal het predicaat* $=$ *van stricte identiteit bevat, zegt dit meteen ook dat* f *een bijectie moet zijn. Als zo'n isomorfisme bestaat, heten de structuren* A *en* B isomorf*.*

Invariantie

Deze algemene definitie van structuur-isomorfie volstaat voor het vaststellen van ononderscheidbaarheid in de wiskundige taal.
Stelling *De wiskundige taal is invariant voor structuur-isomorfismen. Preciezer: als* f *een structuur-isomorfismeis van structuur* A *naar structuur* B*, dan is elke bewering die in de wiskundetaal gedaan kan worden over objecten* $d, \ldots$ A *ook waar voor* $f(d), \ldots$ *in* B*.*

[a] We laten hier functiesymbolen hier voor het gemak buiten beschouwing.

Excursie: expressieve volledigheid van een taal De slogan dat invarianties te maken hebben met taal kan heel precies worden gemaakt met technieken uit de logica. We willen iets hiervan laten zien, eerst abstract geformuleerd, maar vervolgens met een heel concrete spel-techniek. Om te beginnen merken we op dat het begrip orde-isomorfisme valt te generaliseren tot het geval van willekeurige verzamelingen objecten met willekeurige relaties. Vervolgens kunnen we de volledige wiskundige taal bekijken, zoals gedefinieerd in Hoofdstuk 1, die deze relaties kiest als zijn atomaire predicaten. Vervolgens kunnen we dan bewijzen dat *elke bewering* $\varphi(x, y...)$ *uit deze taal*, atomair of logisch complex gedefinieerd met Boolese operaties en kwantoren, invariant blijft voor isomorfismen f tussen verzamelingen A, B in de volgende zin:

$$\varphi(a, b, ...) \text{ geldt in A } \Leftrightarrow \varphi(f(a), f(b)...) \text{ geldt in } B.$$

Meer details hiervan staan uitgespeld in T. 14.

Deze observatie drukt de *expressieve correctheid* uit van ónze wiskundige taal. Maar geldt ook het omgekeerde: kan de taal elke invariant benoemen? Deze omgekeerde vraagstelling van *expressieve volledigheid* is veel abstracter, maar typerend voor de denkwijze van een logicus. Normaal nemen we een taal als gegeven aan. Maar een logicus vraagt of de taal wel geschikt is voor zijn doel, of dat het ontwerp wellicht valt te verbeteren. In het bijzonder, kan de wiskundige predicaatlogische taal iedere eigenschap van objecten definiëren die invariant is voor isomorfismen? Het technische antwoord luidt: "In het algemeen niet, maar soms wel". Hier is een klein positief resultaat:

> Als twee *eindige* grafen A, B dezelfde eigenschappen hebben die uit te drukken zijn in de predicaatlogische taal dan bestaat er een structuur-isomorfisme tussen A en B.

Dit zegt dat althans voor veel voorkomende structuren als eindige grafen invariantie en gelijkheid qua definieerbare eigenschappen in onze wiskundige taal op hetzelfde neerkomen. Maar in het algemeen hoeft expressieve volledigheid niet op te gaan, en kunnen er heel goed allerlei invarianten om ons heen zijn die niet in onze taal worden benoemd.

Vergelijkingsspelen voor structuren Dat analogie en onderscheid slechts keerzijden zijn van dezelfde medaille wordt bijzonder duidelijk in de volgende *speltheoretische* analyse van het beschrijven van structuren. Spelen zijn wiskundig en logisch een belangrijk thema, dat we in hoofdstuk 4 apart gaan bestuderen. Maar voor het moment geven we slechts een intuïtief scenario.

Laten we eens aannemen dat twee personen het niet eens zijn over de mate van gelijkenis tussen twee gegeven structuren, zeg twee grafen. Hoe zouden ze hierover precies van gedachten kunnen wisselen op een manier die tot eenduidige antwoorden leidt? Voor dit doel werd in de vijftiger jaren van de twintigste eeuw door de wiskundigen Fraïssé en Ehrenfeucht het volgende spel bedacht.

Twee grafen A en B zijn gegeven. Dit zijn structuren voor de predicaatlogische taal met een basispredikaat R dat verwijst naar de eerdere pijl-ordening in de grafen, en het predicaat $=$ voor gelijkheid tussen objecten. Het spel plaatst een *gelijkenis-speler* G tegenover een *verschil-speler* V. Een spelstadium bestaat uit twee even lange eindige rijtjes objecten a uit A, en b uit B. We stellen ons voor dat objecten in die rijtjes uniek gekoppeld zijn aan een object op dezelfde plaats in het andere rijtje. Dit codeert op voor de hand liggende wijze een *partiële functie* f van A naar B tussen objecten uit de twee grafen, in tegenstelling tot een gewone functie niet noodzakelijk gedefinieerd voor elk element van A. Een ronde van het spel verloopt nu als volgt:

> In spelstadium (a, b) kiest V een graaf, A of B, en een willekeurig object c erin; G kiest vervolgens een 'corresponderend' object d in de andere graaf. Het nieuwe stadium dat dan ontstaat is: a, b aangevuld met de nieuwe link $c - d$.

De verschilspeler V wint nu in een stadium als f geen *partieel isomorfisme* is: d.w.z. een of andere instantie van de relatie (pijl) in het ene rijtje wordt geschonden door de corresponderende objecten in het andere: zie de voorbeelden beneden. De gelijkenisspeler G hoeft dit alleen maar te vermijden, en het spel kan aldus in principe oneindig doorgaan. We kiezen echter meestal vooraf een eindig aantal rondes, waarmee we de zwaarte van de vergelijking instellen. G wint als hij die rondes allemaal heeft doorstaan, anders wint V.

Voorbeelden

Met één ronde wint G dit spel altijd, want er kan hoogstens een punt zonder pijl gekoppeld worden aan een partieel isomorf punt zonder pijl. Maar er is natuurlijk wel een verschil tussen deze grafen, en dit blijkt als volgt:

> V kan het spel altijd winnen in twee rondes: bijvoorbeeld door eerst 1 te kiezen, waarna G in A bijvoorbeeld b kiest, en in een tweede ronde kan V dan de opvolger a kiezen waarvoor in A voor G geen passende keuze bestaat, omdat 1 geen opvolgers heeft.

Het gaat in dit spel echt om *kunnen* winnen, via een zogenaamde 'winnende strategie'. Een strategie voor speler V is een voorschrift dat bij elke beurt van V in het spel, na elke eerdere reeks zetten van G, een specifieke vervolgzet voorschrijft. En evenzo voor speler G. Een speler kan ook domme zetten doen die van zijn winnende strategie afwijken, en alsnog verliezen!

Nu weten we uit de wiskundige speltheorie dat in een dergelijk spel over eindig veel rondes altijd een van de twee spelers een winnende strategie moet hebben. Dit volgt uit de zogenaamde 'Stelling van Zermelo', een fundamenteel resultaat dat we in Hoofdstuk 4 zullen bewijzen. En die winnende strategieën zijn nu heel mooi te koppelen aan taal! Een winnende strategie voor V (als die bestaat) exploiteert een *definieerbaar verschil* tussen de twee grafen. Dit wordt gegeven door een 'verschilformule' in de predicaatlogische taal die waar is de ene graaf en onwaar in de andere. In het bovenstaande geval is zo'n verschilformule bijvoorbeeld $\forall x \exists y\, x < y$: elk punt heeft een opvolger. V kan nu al zijn zetten laten bepalen door deze formule, en met name door de kwantoren die hierin voorkomen:

- $\forall$ Kies voor de structuur waar de formule onwaar is.
- $\exists$ Kies voor de structuur waar de formule waar is.

Hier is een tabel voor het eerdere spel over twee rondes die de methode meer in detail illustreert:

	STRUCTUUR 1		STRUCTUUR 2	
Ronde	Speler	Formule	Speler	Formule
		$\forall x \exists y\, x < y$		$\forall x \exists y\, x < y$
1	V	$\exists y\, v_1 < y$	G	$\exists y\, g_1 < y$
2	G	$v_1 < g_2$	V	$g_1 < v_2$

Het spel begint met een verschil dat wordt uitgedrukt door een formule met twee geneste kwantoren. Volgens het voorschrift begint V in de graaf waar de buitenste kwantor $\forall$ onwaar is, en dat is links. Hij kiest een object v_1, bijvoorbeeld 1, en G antwoordt met g_1 rechts, bijvoorbeeld a (ze kan elk van de drie objecten kiezen). Na deze eerste ronde fungeert nu $\exists y\, x < y$ als nieuwe verschilformule: deze is onwaar voor $x = 1$ in de linker graaf, maar waar voor elke $x = g_1$ rechts, omdat elk object daar opvolgers heeft. De eerste ronde heeft dus een kwantor van de oorspronkelijke formule 'afgepeld'. Maar er is nog één over, en dat is net genoeg voor V's strategische zet in de resterende ronde. Hij gaat nu naar de graaf waar de existentiële verschilformule waar is, dat wil zeggen rechts, en kiest een object v_2 dat voldoet aan $g_1 < v_2$. Omdat v_1 geen opvolgers heeft in de linkergraaf weten we dat de corresponderende atomaire formule $v_1 < g_2$ altijd onwaar moet zijn voor elke keuze van G. Dit verschil betekent dat V het spel heeft gewonnen.

We zien dus dat de winnende strategie van de verschilspeler precies is gecorreleerd met het handhaven van een definieerbaar verschil. We illustreren ditzelfde verschijnsel nog eens, nu aan het eerdere voorbeeld van twee oneindige structuren, en wel $\mathbb{Z}$ versus $\mathbb{Q}$. Het is niet moeilijk om te zien dat in een spel over ene of twee ronden, de gelijkenis speler G altijd kan winnen. Maar dat verandert zodra we over drie rondes spelen. Alvorens verder te lezen is het werkelijk de moeite waard om dit eerst eens zelf te proberen. Wat moet V doen om G in een val te lokken? De eerste zet van beide is willekeurig, maar daarna is het van groot belang welke zet V doet in relatie tot de gekoppelde objecten van de eerste ronde... De taalkant van de winnende strategie zien we als volgt. De benodigde drie ronden hangen precies samen met de drie kwantoren van de eerdere verschilformule van *dichtheid* $\forall x\, \forall y\, \exists z\, (x < y \rightarrow (x < z \wedge z < y))$. De winst voor V volgt nu het procédé:

	$\mathbb{Z}$		$\mathbb{Q}$	
		$\forall x\, \forall y\, \exists z\, (x < y \rightarrow (x < z \wedge z < y))$		$\forall x\, \forall y\, \exists z\, (x < y \rightarrow (x < z \wedge z < y))$
1	V	$\forall y\, \exists z\, (v_1 < y \rightarrow (v_1 < z \wedge z < y))$	G	$\forall y\, \exists z\, (g_1 < y \rightarrow (g_1 < z \wedge z < y))$
2	V	$\exists z\, (v_1 < v_2 \rightarrow (v_1 < z \wedge z < v_2))$	G	$\exists z\, (g_1 < g_2 \rightarrow (g_1 < z \wedge z < g_2))$
3	G	$v_1 < v_2 \rightarrow (v_1 < g_3 \wedge g_3 < v_2)$	V	$g_1 < g_2 \rightarrow (g_1 < v_3 \wedge v_3 < g_2)$

De clou van het spel is dat de verschilspeler in de tweede beurt $v_2 = v_1 + 1$, de *directe opvolger* van v_1, kiest. Als v_1 en g_1 eenmaal gekoppeld zijn, dan moet G na V's tweede keuze $v_1 + 1$ een opvolger g_2 van g_1 kiezen, anders verliest zij sowieso, omdat er anders geen partieel isomorfisme zou zijn. Maar vanwege de dichtheid van $\mathbb{Q}$ kan V dan in de derde ronde v_3 *tussen* g_1 en g_2 in kiezen, en G is niet in staat een daarmee overeenkomende keuze te doen tussen v_1 en $v_1 + 1$ in $\mathbb{Z}$. Wat zij ook kiest dus, het verstoort het partiële isomorfisme, en ze verliest.

Nu komt weer de taal-connectie. De verschilspeler heeft weer goed de kwantorregels toegepast. Twee keer kiezen in $\mathbb{Z}$ vanwege de twee universele kwantoren (en de onwaarheid van dichtheid voor de gehele getallen), met daarna een 'oversteek' voor de derde keuze in $\mathbb{Q}$. Verdere details van handhaven van steeds eenvoudiger verschilformules laten we aan de lezer over.

Overigens kan men zich afvragen wat het betekent als de *gelijkenisspeler* G de winnende strategie heeft in het spel over k rondes. In dat geval stemmen de gegeven grafen overeen in logische eigenschappen die zijn te definiëren met hoogstens k geneste kwantoren. Voor verder details verwijzen we naar T. 15. In principe zouden we het spel ook over oneindig veel rondes kunnen spelen. In het geval dat G dan nog steeds kan winnen moet deze winnende strategie berusten op een globale *analogie* tussen de gegeven structuren, bijvoorbeeld een orde-isomorfisme, of een andere sterke wiskundige overeenkomst.

TECHNIEK 15.

Spel-invariantie en taal

De volgende stelling zegt het allemaal nog eens kort en bondig. Met behulp van de spel-invariantie hebben we een exacte *structurele beschrijving van talige equivalentie, in tegenstelling tot het 'halve' resultaat wat we voor structuur-isomorfie verkregen in Stelling 14.*
Stelling *De volgende twee condities zijn equivalent voor structuren A en B:*

1. *G heeft een winnende strategie in het AB-spel over k rondes*
2. *A en B maken dezelfde beweringen waar in de wiskundige taal die hoogstens k geneste kwantoren bevatten.*

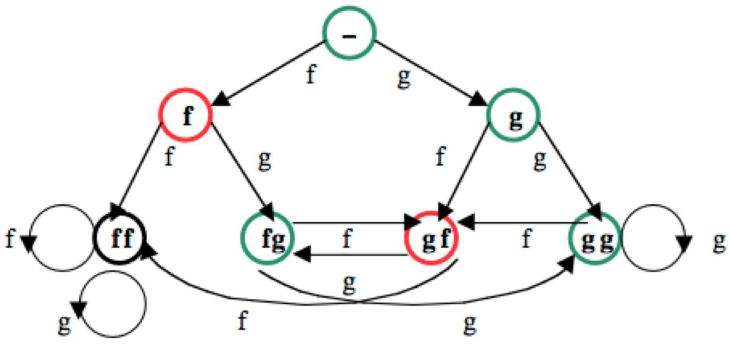
Het bewijs van deze stelling is niet moeilijk, maar het valt buiten het bereik van dit hoofdstuk.

Nieuwe genres invariantie: processen in informatica In onze bespreking van transformaties en invarianties benadrukten we 'Clinton's Principe': er kunnen allerlei verschillende niveaus zijn van 'gelijkheid' voor structuren. Gezien de spelanalyse die we zojuist hebben gegeven voor de standaard predicaatlogische taal betekent dit dat er ook andere vergelijkingsspelen moeten bestaan, die spelers andere rechten of plichten geven. Dat is inderdaad het geval. En daarmee corresponderen dan ook nieuwe beschrijvingstalen voor grafen. Om de brede strekking van dit hoofdstuk te onderstrepen, gaan we daarom nog eens heel anders naar grafen kijken, en wel als diagrammen voor *processen* in de informatica! In de laatste decennia zijn in de theorie van rekenprocessen heel nieuwe noties van invariantie ontstaan, die interessant zijn op zich. En uiteindelijk zullen we ook zien hoe deze invarianties tot een nieuwe taal leiden, en wel de 'modale logica' van processen.

Lezers die al genoeg menen te weten kunnen hier overigens dt hoofdstuk afsluiten: we gaan nu iets verder de diepte in.

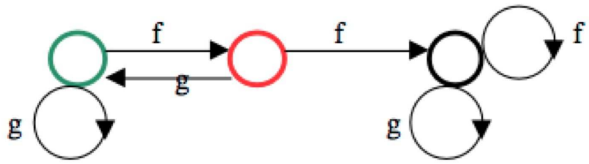
Wanneer zijn twee processen gelijk?

Grafen worden vaak gebruikt als diagram of stroomschema van een proces. De punten staan dan voor mogelijke toestanden waarin het proces zich kan bevinden, en de pijlen geven mogelijke overgangen aan, waarbij het proces verspringt van de ene toestand naar de andere. Ook is nog mogelijk dat bij de punten lokale eigenschappen staan aangegeven die opgaan voor die toestand: bijvoorbeeld dat een rood of groen lichtje brandt, of dat een of andere interne conditie opgaat voor het geheugen van een computer in die toestand. Een voorbeeld maakt dit duidelijker. In een fabricageproces in het zuiden des lands werkt een controleur die op een lopende band objecten binnenkrijgt. Deze kunnen zowel correct ('g') als defect ('f') zijn. De controleur kan een arriverend fout object repareren, en tegelijkertijd het volgende object laten binnenkomen. Maar als er twee foute objecten achter elkaar arriveren, dan wordt het hem gewoon te veel, en blokkeert hij. Hier is een procesgraaf die dit kort weergeeft.

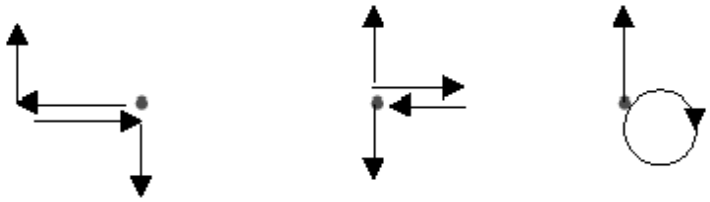


De start-toestand begint met een leeg 'geheugen'. De pijlen geven aan wat het volgende arriverende object is: 'goed' of 'fout', en lopen dan naar de volgende geheugen-toestand. Deze houdt ten hoogste de twee laatst gelezen objecten bij. De mogelijke toestanden van onze controleur vallen in drie categorieën die worden aangegeven door de kleuren: 'veilig' (groen), 'gevaarlijk' (rood) en 'hopeloos' (zwart).

Maar is dit wel de beste weergave van ons fabricageproces? Kan het ook anders, misschien eenvoudiger? Dat blijkt inderdaad mogelijk. Hieronder is een equivalente procesgraaf met slechts drie toestanden.



Het moge duidelijk zijn dat hier geen sprake is van isomorfie. De twee procesgrafen hebben niet eens hetzelfde aantal toestanden en er is dus geen bijectie of orde-isomorfisme die ze verbindt. Toch lijken de twee processen 'hetzelfde' te doen. Rond 1980 is een alternatieve wiskundige equivalentie-notie bedacht — onafhankelijk van elkaar in de logica en de informatica — die dit nieuwe begrip gelijkheid precies omschrijft. Alvorens de definitie te geven volgen hier eerst nog een drietal uiterst simpele procesgrafen om onze intuïtie te scherpen. Er is maar één soort handeling (de pijlen) en de toestanden bevatten verder geen informatie.



Hier is wat een informaticus waarschijnlijk zou zeggen over deze drie processen. De linkerfiguur beschrijft hetzelfde proces als de rechterfiguur: het proces kan rondcirkelen maar ook telkens in één stap naar een eindpunt gaan waar het stopt. Maar de middelste figuur laat ook ander gedrag toe. Vanuit de beginpositie kan het proces gaan naar het punt rechts ernaast vanwaar geen stap naar een eindpunt mogelijk is. De notie die we gaan definiëren moet dit soort overeenkomsten en verschillen

verantwoorden. Het idee is daarbij als volgt. Gelijkheid van processen heeft te maken met de vraag of het ene proces het andere getrouw kan *simuleren*. Deze intuïtie gaan we nu precies omschrijven.

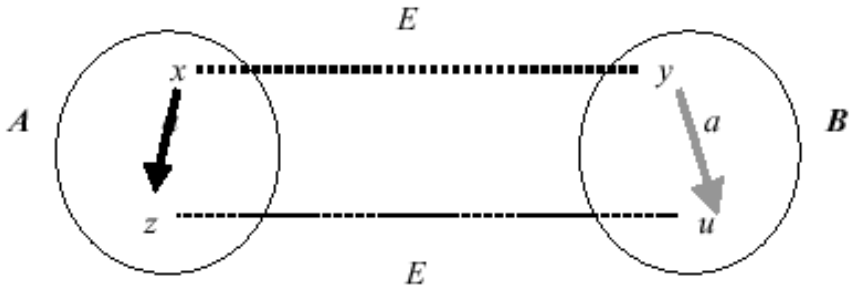
TECHNIEK 16.

Bisimulatie

Een bisimulatie *tussen twee structuren A, B is een binaire relatie E die begintoestanden verbindt, en telkens als Exy, voldoet aan de volgende drie eisen:*

1. *x en y hebben dezelfde lokale eigenschappen*
2. *als $x \xrightarrow{a} z$ dan $\exists u\,(y \xrightarrow{a} u \wedge Ezu)$,*
3. *als $y \xrightarrow{a} u$ dan $\exists z\,(x \xrightarrow{a} z \wedge Ezu)$.*

Deze laatste twee 'zigzag eigenschappen' geven de proces-simulatie weer. Ze moeten gelden voor alle transities a. In een plaatje:



In de laatste figuur is er een bisimulatie tussen de eerste en de derde procesgraaf die hun begintoestanden verbindt, en wel als volgt:

Er is ook makkelijk te zien dat er geen bisimulatie bestaat die hetzelfde doet tussen de eerste en tweede procesgraaf. Een typische vorm van bisimulatie neemt toestanden samen in een procesgraaf en verkleint aldus de structuur terwijl het proces toch gelijk blijft. Bisimulaties worden dan ook vaak gebruikt om eenvoudigste processen of computerprogramma's te vinden voor een gegeven doel. Dit zien we ook in ons fabricageproces: de lezer kan makkelijk een bisimulatie geven die het eerste proces met zes toestanden koppelt aan het tweede met slechts drie. Dit is overigens slechts een van diverse nuttige eigenschappen:

> Elke graaf opgevat als proces heeft een kleinste 'bisimilair' proces, de zogenaamde 'bisimulatiecontractie'. Elke graaf heeft ook een grootste bisimilair proces, en wel de uitrolling tot een vertakkend netwerk van alle mogelijke proces-verlopen.

Dit soort wiskundige feiten worden gebruikt in de theorie van rekenprocessen en ook in de informatica-praktijk.

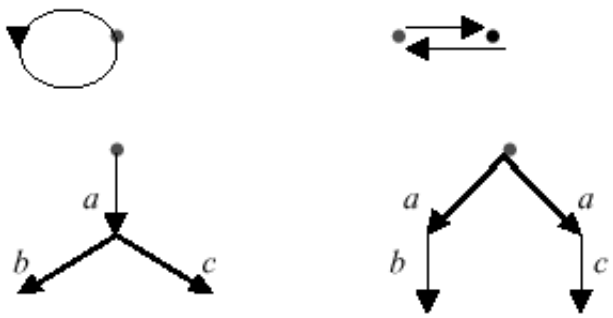
Tenslotte ligt voor de hand dat bisimulatie ook te maken heeft met een vergelijkingsspel voor processen. In feite suggereert de definitie van de 'zigzag clausules' van de simulatie al hoe zo'n spel zal verlopen, getuige het plaatje in 16. Spelers testen of de processen werkelijk overeenkomstige mogelijke verlopen toestaan. In ieder stadium wordt een paar toestanden x, y vergeleken, één uit elke graaf. Als die twee verschillen qua lokale eigenschappen (deze lezen we ter plaatse af), dan heeft de verschil-speler V meteen gewonnen. Zo niet, dan gaat de ronde verder. V kiest een opvolger z via een gelabelde pijl vanuit hetzij x, hetzij y. De gelijkenis-speler G moet nu een soortgelijke opvolger u kiezen (met hetzelfde actielabel) voor de resterende toestand uit x, y in de andere graaf. Als zij dit niet kan, dan verliest ze: er is dan immers een overduidelijk verschil in gedrag van de twee processen. Het spel gaat dan verder met als startpunt de nieuwe link $\langle z, u\rangle$. Gelijkenis van procesgrafen kunnen we weer precies meten aan het aantal rondes dat de verschilspeler nodig heeft voor een winnende strategie, als hij die überhaupt heeft. Maar het kan ook zo zijn dat dit nooit gebeurt. Zelfs is mogelijk dat de gelijkenisspeler zonder verlies kan blijven doorgaan in een spel over oneindig veel ronden. Dat gebeurt in feite precies als er een bisimulatie bestaat tussen de twee processen.

Ontstaan van een nieuwe taal: modale logica Waar invarianties zijn is taal. Deze voorspelling van Helmholtz moet ook hier opgaan. En we kunnen een preciezere voorspelling doen. Bisimulaties zijn veel 'ruwere' transformaties dan orde-isomorfismen: ze trekken zich veel minder aan van de precieze structuur van punten en pijlen. Navenant verwachten we dus een *armere* taal voor procesbeschrijving dan de volledige predicaatlogica die we tot nu toe gebruikten. De proces-eigenschappen van die invariant zijn voor bisimulatie blijken allemaal definieerbaar in een logische taal die alleen 'lokale' eigenschappen van toestanden kan weergeven. Om te beginnen heeft deze *modale logica* alleen unaire eigenschappen van toestanden, die we kunnen weergeven met propositieletters $p, q, ...$ Maar nog belangrijker: kwantoren blijven nu beperkt tot opvolgers van de huidige toestand:

$\langle a\rangle\varphi$ φ geldt in minstens één a-opvolger

$[a]\varphi$ φ geldt in alle a-opvolgers

Hieronder is een simpel tweetal niet-bisimilaire grafen gegeven. De verschil-speler in een bisimulatiespel als boven moet dus kunnen winnen.



Hij kan dat doen door gebruik te maken van een verschilformule in deze eenvoudige modale taal. Een voorbeeld is $\langle a\rangle(\langle b\rangle\top \wedge \langle c\rangle\top)$, met $\top$ een formule die altijd waar is. Deze modale formule zegt dan

dat actie a is uit te voeren en leidt naar een toestand waar zowel b als c zijn uit te voeren. Al deze modale operatoren zijn existentieel, en V kan dus in de linker graaf spelen. In de eerste stap doen beide spelers een a-stap: de verschil-speler links, de gelijkenis-speler rechts. Dan komen ze in een toestand waar het in feite nog gaat om de resterende formule $\langle b\rangle\top \wedge \langle c\rangle\top$. Deze is waar in de middelste toestand links, maar in geen enkele middentoestand rechts. Dus wat G ook heeft gekozen, ze zit fout. Afhankelijk van wat ze gekozen heeft gaat V nu links naar een opvolger met een actie dat G niet tot haar beschikking heeft, en wint. Overigens kan eenzelfde spel meerdere winnende strategieën hebben voor een speler. Dat correspondeert dan in ons geval met meerder verschillen die in de modale taal zijn uit te drukken. Een voorbeeld is de alternatieve verschilformule $[a]\langle b\rangle\top$, die zegt dat altijd na uitvoeren van actie a actie b daarna nog uitvoerbaar is. Dit is links waar en rechts niet. In dit geval van twee verschillende modale kwantoren moet de verschilspeler in de rechter-figuur beginnen en voor de rechterkant kiezen. Daarna steekt hij over naar de linker graaf, en kiest daar een b-opvolger vanuit het midden.

In T.17 staat een simpel wiskundig bewijs dat de modale taal inderdaad invariant is onder bisimulatie. Net als in het geval van de volledige predicaatlogische taal een orde-isomorfie ligt de omgekeerde bewering, en daarmee de expressieve volledigheid van de modale logica iets subtieler.

Invariantie, natuurlijke taal en cognitie De transformaties en invarianten in dit hoofdstuk lijken een zuiver wiskundige techniek. Maar we hebben ook al opgemerkt dat deze denkwijze ook veel voorkomt in andere wetenschappen. Ze is ook heel goed toe te passen op natuurlijke taal en cognitie. Invarianten zijn van belang voor succesvolle regelmaat in gedrag, en het vermogen kennis over een situatie over te dragen op analoge situaties is essentieel voor elk succesvol bestaan. De taal levert ons een rijk vocabulaire aan invariante begrippen waarmee we elkaar mededelingen kunnen doen die overdraagbaar zijn naar nieuwe situaties. Anderzijds is echter beschrijven van verschillen tussen situaties evenzeer een wezenlijk kenmerk van intelligent gedrag. Het medium waarin we beide functies uitvoeren is weer de *natuurlijke taal*, die ook al in Hoofdstuk 1 werd benadrukt. Sommige psychologen en taalkundigen menen zelfs dat onze menselijke talen hun basisvocabulaire kiezen als weerspiegeling van invarianties in onze fysieke omgeving, of beter, hoe wij met onze beperkte bewegingsvrijheid en zintuigen die fysieke wereld waarnemen. We zagen reeds hoe kwantoruitdrukkingen te maken hadden met invariantie voor bijecties, hele ruwe teltransformaties. Maar ook andere veel gebruikte uitdrukkingen in onze gewone taal, zoals comparatieven (‘groter dan’) of tijdsuitdrukkingen (‘nu’, ‘toen’ of ‘later’) vallen goed met bijpassende transformaties te beschrijven.

TECHNIEK 17.

Modale logica en bisimulatie

De taal van de modale logica bestaat uit propositieletters $p, q, r, \ldots$, een soort nul-plaatsige predicaten. Daarnaast worden de Boolese connectieven gebruikt, en twee modale operatoren $[a]$ *en* $\langle a \rangle$ *voor gegeven* atomaire processen a.
Een procesgraaf P bestaat uit een verzameling van toestanden S, met voor elk atomair proces a een binaire relatie $\rightarrow_a$ over S, en een lokale informatiefunctie V die in elke toestand een waarheidswaarde toekent aan elke propositieletter. Een formule φ uit de taal van de modale logica wordt nu per toestand geëvalueerd volgens de volgende recursieve procedure:

- *Als φ een prositieletter p is, dan is deze waar in een toestand s indien de lokale informatiefunctie V de waarde 1 toekent aan p in s.*
- *Een negatie $\neg\psi$ is waar in s alleen dan als ψ niet waar is in s. Een conjunctie $\psi \wedge \chi$ is alleen waar in s als ψ en χ beide waar zijn in s. Voor de overige connectieven verloopt deze evaluatie analoog.*
- *Een modale formule van de vorm $[a]\psi$ is deze waar in s als ψ waar is in alle t waarvoor $s \rightarrow_a t$. Een modale formule van de vorm $\langle a \rangle \psi$ is waar in s als er tenminste één toestand t bestaat met $s \rightarrow_a t$ die ψ waar maakt.*

Nu kunnen we de genoemde bisimulatie-invariantieprecies formuleren.

Stelling *Als E een bisimulatie is tussen twee proces-grafen P en P', dan maakt voor elk paar $\langle s, s' \rangle$ met Ess', s in P dezelfde modale formules waar als s' in P'.*

Bewijs *Laat P en P' twee grafen zijn met een bisimulatie E daartussen. Stel dat er een een paar bisimilaire toestanden in E te vinden is die verschillen in hun modale informatie. We gaan laten zien dat dit tot een tegenspraak leidt.*
Laat φ een 'verschilformule' zijn van minimale lengte *(= het aantal symbolen in φ). Er is dan geen kortere formule die verschil maakt tussen twee bisimilaire toestanden in de twee grafen. Nu kan de verschilformule geen minimale lengte 1 hebben. Want, de lokale informatie van bisimilaire toestanden is per definitie gelijk: (zie T. 16, pag. 76).*
Als φ een negatie is, $\neg\psi$, dan is ψ ook een verschilformule, en dat is in tegenspraak met de minimale lengte van φ. Als φ een conjunctie is, $\psi \wedge \chi$, dan moet tenminste één van de twee conjuncten ψ of χ ook een verschilformule zijn: wederom in tegenspraak met de minimale lengte van φ. Voor de overige connectieven loopt de bewijsvoering analoog.
Nu de modale operatoren! Als φ van de vorm $[a]\psi$ is, dan is er dus een paar $\langle s, s' \rangle$ in E met $[a]\psi$ waar in s en onwaar in s', of omgekeerd. In het eerste geval geldt dat ψ waar is voor alle a-opvolgers t van s, maar ψ is onwaar in tenminste één van de a-opvolgers van s'. Maar alle opvolgers van s' bisimuleren met een a-opvolger van s, volgens de derde eis in T. 16, en dus is ψ reeds een verschilformule. Dit weerspreekt opnieuw de minimale lengte van φ. Het tweede geval gaat evenzo, op basis van de tweede eis in T. 16. In het laatste geval, $\varphi = \langle a \rangle \psi$ voor zekere ψ, krijgen we weer dezelfde tegenspraken als zojuist.
De minimale verschilformule kan echter geen andere vorm aannemen dan de hier genoemde, en dus moeten we concluderen dat zo'n verschilformule helemaal niet kan bestaan in het geval van bisimilaire grafen.

Deel II

Wiskunde en cognitie

Hoofdstuk 3

Onzekerheid

3.1 Waarschijnlijkheid

Er zijn maar weinig situaties in het dagelijkse leven waar de volledig waterdichte redeneringen van de wiskunde direct kunnen worden toegepast. Vaak zijn er gewoon te veel onzekerheden in het spel om een alledaags probleem om te zetten in een wiskundige formule. Met name bij het gebruik van wiskunde in de sociale wetenschappen is het niet eenvoudig allerlei onbeheersbare variabelen weg te 'cijferen'. Toch kan wiskunde ons ook in deze situaties helpen met deze intrinsieke onzekerheid om te gaan. Wiskunde stelt ons namelijk in staat met onzekerheden te rekenen en te combineren met zekere kennis. Met name bij het afsluiten van belangrijke contracten kan dit bijzonder lonend zijn. Historisch gezien zijn het juist het afsluiten van weddenschappen en het opstellen van levensverzekeringen en lijfrenterekeningen geweest waar de economische belangen hebben geleid tot het ontwikkelen van de relevante wiskunde.

Grote getallen, kleine kansen: ongecijferdheid

Bij het wiskundig modelleren van onzekerheid moeten de woorden van Benjamin Disraeli[1] ter harte worden genomen

> *There are three kinds of lies: lies, damned lies, and statistics.*

Het nieuws staat vol met incorrect of op z'n minst onduidelijk gebruik van kansrekening. Hier volgen een paar pregnante voorbeelden.

> *Vrouw wint loterij tweemaal: kans van één op een biljoen.*

Wat is hieraan mis? Het lijkt inderdaad zeer onwaarschijnlijk dat je tweemaal de loterij wint. Maar pas op. De extreem kleine kans $1/1000000000000$ is de kans dat een gegeven persoon (de vrouw in kwestie) bij twee gegeven trekkingen van de loterij de hoofdprijs wint, waar we uitgaan dat er per keer zo'n miljoen loten in omloop zijn. Dan heb je inderdaad een kans van een miljoen om de eerste keer te winnen, en de kans om tweemaal achterelkaar te winnen is een miljoenste maal een miljoenste.

Waarom is deze redenering op z'n minst verwarrend? Er is natuurlijk altijd iemand die de eerste keer wint. (We nemen aan dat alle loten verkocht zijn.) De vraag is nu zal deze persoon, die door het lot is aangewezen, ook de tweede loterij zal winnen. De kans daarop is 'slechts' één op een miljoen. Maar dit is nog niet het einde. Het mag natuurlijk ook een andere trekking of een andere loterij zijn. Wat is de kans dat iemand van alle miljoenen personen die loterijkaarten kopen ergens in zijn of haar leven twee keer wint? Uiteindelijk blijkt dat (voor bijvoorbeeld de Verenigde Staten) de kans groter dan 50% dat dit binnen zeven jaar gebeurt. De kans is nog steeds beter dan één op dertig voor een periode van vier maanden zoals in het geval van de vrouw waarvan de krantenkop spreekt. Daarmee zijn we van een kans van $0,00000000001\%$ naar een kans van meer dan 3% gegaan.

Een ander zeer vermaard voorbeeld van oneigenlijk gebruik van statistiek dook op in de verdediging van O.J. Simpson, aangeklaagd voor de moord op zijn vrouw en met een voorgeschiedenis van mishandelingen. De bekende Harvard jurist Alan Dershovitz voerde aan dat de statistieken laten zien dat de kans dat een man die zijn vrouw slaat haar uiteindelijk vermoord maar één op een paar miljoen is. Daarmee probeerde hij de verdachte voorgeschiedenis tot een statistische onbenulligheid te reduceren. Deze kans is natuurlijk zo klein omdat de kans om überhaupt vermoord te worden erg klein is. Dershovitz liet na te vermelden dat in de gevallen dat de vrouw ook daadwerkelijk vermoord wordt, in één op de vier gevallen de echtgenoot de dader is! Het was absoluut verbijsterend dat de openbare aanklager de redenering van de verdediging ongemoeid liet.

[1] Of was het Mark Twain, zelfs de oorsprong van het citaat is niet met exacte zekerheid vast te stellen.

Het onbegrip van onzekerheid is trouwens maar een van de symptomen van ongecijferdheid. Getallen, en dan vooral heel grote getallen en de daarbij behorende zeer kleine waarschijnlijkheden, worden vaak slecht gehanteerd. Hier zijn een paar directe voorbeelden die ons ongemak en onbekendheid met grote getallen illustreren.

- *Hoeveel pianostemmers zijn er in Amsterdam?*. De bekende Italiaans-Amerikaanse fysicus Enrico Fermi begon zijn colleges steevast met de vraag: "Hoeveel pianostemmers zijn er in Chicago?" Kan men dit getal bij benadering bepalen zonder de pianostemmers expliciet te gaan tellen? Een ruwe schatting voor Amsterdam zou als volgt kunnen gaan: één miljoen inwoners, driehonderdduizend gezinnen, tien procent heeft een piano, die één keer per tien jaar gestemd wordt. Dit geeft drieduizend te stemmen piano's per jaar. Een stemmer kan ruwweg twee piano's per dag of driehonderd piano's per jaar stemmen. Dus ongeveer tien fulltime stemmers in Amsterdam. Een blik in de Gouden Gids bevestigt deze schatting. Alle getallen kunnen met een flinke korrel zout genomen worden, maar de orde van grootte is correct.

- *Hoeveel letters zijn er in een boekhandel te vinden?* We geven weer een ruwe schatting. Zeg tienduizend boeken met ieder tweehonderd bladzijden met duizend letters per bladzijde: totaal zo'n twee miljard letters. Dit geeft een goed beeld om bij een miljard voor ogen te houden.

- *Hoe lang duurt het om met traditionele methoden de heilige berg Fuji af te graven?* Dit is een klassieker. Een middelgrote berg geeft ongeveer 10^{11} kubieke meter steen. Een vrachtauto kan zo'n vijftig kubieke meter per keer vervoeren, zeg tien ritten per dag, dat geeft honderdduizend kubieke meter per jaar. Vijfhonderd vrachtauto's — dat is een hoge schatting — doen er dan zo'n tweeduizend jaar over.

- *Hoeveel deeltjes passen er maximaal in het Heelal?* Het voor ons zichtbare heelal is nu zo'n vijftien miljard lichtjaar of 10^{25} meter groot. Het totale volume op dit moment is dus 10^{75} kubieke meter. Een proton heeft een afmeting van ongeveer 10^{-15} meter. We kunnen dus 10^{40} protonen zij aan zij in het heelal op een rijtje zetten. Al met al passen er dus zo'n $10^{40} \cdot 10^{40} \cdot 10^{40} = 10^{120}$ protonen in het heelal. Dit getal vormt een bovengrens voor ieder mogelijk materiaal of apparaat dat we zouden willen bouwen. Stel we willen de allergrootste denkbare computer bouwen en stel dat we op de een of andere manier er in geslaagd zijn de onderdelen daarvan te reduceren tot een proton. Dan kan zo'n computer nooit bestaan uit meer dan 10^{120} onderdelen.

- *Wat is de kans dat je een luchtmolecuul inademt dat ook Julius Caesar heeft ingeademd, bijvoorbeeld toen hij "Tu quoque, fili" zei?* De aardatmosfeer bestaat uit zo'n 10^{18} kubieke meter lucht. Er zijn daarmee ongeveer 10^{44} moleculen in de atmosfeer. Een hap adem van zeg twee liter bevat ongeveer 10^{22} moleculen. Als we aannemen dat deze een ademteug zich gedurende de afgelopen tweeduizend jaar goed door de atmosfeer heeft gemengd, dan zal daarmee één op iedere 10^{22} luchtmoleculen uit deze laatste adem afkomstig zijn. Als we dus zelf een teug lucht inademen is er een zeer grote kans dat er een molecuul van Caesar bijzit (de kans is ongeveer 99%).

  Als we trouwens alleen vragen dat de luchtmolecuul ooit eens door Ceasar is in- of uitgeademd, dan zit in iedere adem zo'n tien miljoen 'Caesarmoleculen'.

- Een ander voorbeeld van ons ongemak met cijfers wordt veroorzaakt door het oneigenlijk gebruik van percentages om winst en verlies uit de drukken. Als een aandeel van honderd gulden

vandaag 90% verliest maar morgen weer 90% wint is het toch nog maar negentien gulden waard!

- Zijn er oninteressante getallen? De bekende getaltheoreticus Ramanujan werd verteld dat zijn gast een taxi met nummer 1729 had gereden, wat ogenschijnlijk een oninteressant getal is. Integendeel zei Ramanujan, het is het kleinste getal dat op twee manieren geschreven kan worden als de som van twee derde machten

$$1729 = 1^3 + 12^3 = 9^3 + 10^3$$

Stel dat er evenwel oninteressante getallen bestaan. Wat is dan het kleinste oninteressante getal? Is het daarmee eigenlijk niet een heel interessant getal?

Coïncidenties en synchroniciteit

We leven te midden van een enorme hoeveelheid aan gebeurtenissen en ervaringen, en vaak zijn de onderlinge verbanden tussen die gebeurtenissen van een subtiele aard. Er is niet altijd een eenvoudige oorzakelijk verband te geven. Eén van onze verbluffende cognitieve vermogens is om uit 'ruwe data' patronen te distilleren en te interpreteren, bijvoorbeeld een afbeelding van een persoon te herkennen in een wazige foto. Maar hoe weten we dat de relaties die we zien — het patroon van zwarte en witte stipjes in de foto — daadwerkelijk betekenis dragen en niet door een toevallige samenloop van omstandigheden veroorzaakt zijn. Vooral als het gaat om betekenisvolle relaties te onderscheiden van willekeurige patronen is het belangrijk om het kansbegrip wiskundig precies te maken. Zeker omdat onze intuïtie ons hierbij niet zelden in de steek laat.

Een goed voorbeeld zijn coïncidenties, gewoonlijk gedefinieerd als een verrassende samenloop van gebeurtenissen die als betekenisvol wordt ervaren zonder dat er een schijnbaar causaal verband tussen de gebeurtenissen bestaat. We kennen dit verschijnsel allemaal uit de dagelijkse praktijk. Soms lijken gebeurtenissen te onwaarschijnlijk om toeval genoemd te kunnen worden.

Twee beroemde wetenschappers van het begin van de twintigste eeuw, de psychiater Carl Gustav Jung en de bioloog Paul Kammerer, stelden de notie van coïncidentie centraal in hun onderzoekingen. Ruwweg kwamen zij tot de conclusie dat coïncidenties veel vaker gebeuren dan in een gewoon kansproces. Daartoe poneerde Jung het begrip 'synchroniciteit' als een soort kracht die gebeurtenissen als het ware bijeen drijft. Er zijn vele treffende voorbeelden door Jung en Kammerer verzameld.

Hier is een typisch voorbeeld van Kammerer

> Op 5 mei 1917 bezoek ik het artiestencafé tegenover de Universiteit van Wenen. Ik merk voor het eerst het portret van Dr. Tyvolt op aan de muur. De ober brengt me mijn krant waarin me meteen een artikel over de crisis in het Duitse Volkstheater opvalt van de hand van Dr. Tyvolt.

Een beroemd voorbeeld van Jung

> Een jonge vrouw vertelt me van haar droom waar een gouden scarabee voorkomt. Op dat moment hoor ik getik tegen het raam. Het is een kever die een grote gelijkenis vertoont met een gouden scarabee. De kever wil, tegen zijn natuur in, de donkere kamer binnen vliegen.

Gemotiveerd door dit soort ervaringen is er een diffuse beweging ontstaan die dit soort verschijnselen een grote betekenis toekent, en onder andere raakt aan de astrologie, paranormaliteit en andere spirituele verschijnselen.

Hoe kunnen we bepalen of dit soort gebeurtenissen meer dan toeval zijn? Wanneer spreken we van een coïncidentie. Het moet duidelijk zijn dat de kansen afhangen van het aantal mogelijkheden in een bepaalde categorie (bijvoorbeeld, hoeveel Weense toneelrecensenten waren er) en vervolgens van het aantal categorieën. Misschien heeft Jung een duidelijk geval gevonden waar ons *waargenomen* begrip van kans niet aansluit bij het *wiskundig* begrip?

Principes van kansrekening

Stel we gooien een dobbelsteen. Er zijn zes mogelijke uitkomsten: 1, 2, 3, 4, 5 en 6. Wat is de kans dat we een cijfer gooien dat 3 of hoger is?

We redeneren als volgt. Er zijn zes mogelijke uitkomsten, alle zes a-priori even waarschijnlijk. De kans om dan een bepaalde uitkomst te gooien, bijvoorbeeld een 4, is dan $1/6$. De uitkomsten die we willen beschouwen zijn er vier van de zes, namelijk 3, 4, 5 en 6. De kans op deze uitkomsten is dan vier uit zes of

$$P = \frac{4}{6} = \frac{2}{3}$$

We kunnen dit eenvoudige voorbeeld formaliseren. Allereerst is er een verzameling Ω van alle uitkomsten. In het geval van de dobbelsteen hebben we

$$\Omega = \{1, 2, 3, 4, 5, 6\}.$$

Laten we voor het gemak eerst aannemen dat het aantal elementen in de uitkomstenruimte Ω eindig is. Aan iedere uitkomst $\omega \in \Omega$ kennen we vervolgens een getal $P(\omega)$ toe, de kans op de uitkomst ω. Deze getallen moeten voldoen aan

$$0 \leq P(\omega) \leq 1$$

Immers iedere kans ligt ergens tussen 0 (gebeurt nooit) en 1 (gebeurt met absolute zekerheid). Verder moet gelden dat de som van alle kansen 1 is

$$\sum_{\omega \in \Omega} P(\omega) = 1$$

Het is zeker dat één van de uitkomsten gebeurt.

Achter deze definitie schuilt de veronderstelling dat in de praktijk de kansverdeling $P(\omega)$ bepaald kan worden door het experiment maar vaak genoeg te herhalen, waarna $P(\omega)$ benaderd kan worden

door de relatieve frequentie van de uitkomst ω, dat wil zeggen de ratio van het aantal keer dat ω plaats vindt op het totaal aantal keren dat we het experiment herhaald hebben. In geval van een perfecte dobbelsteen zijn al deze kansen gelijk, dus hebben we voor al de zes uitkomsten $\omega = 1, 2, \ldots, 6$ dat $P(\omega) = 1/6$.

Laat $A \subset \Omega$ nu een deelverzameling van uitkomsten zijn. Vaak wordt zo'n deelverzameling een *gebeurtenis* genoemd. Wat is de kans dat er een gebeurtenis A plaats vindt. Per definitie is dit de som van alle kansen van alle elementen in A

$$P(A) = \sum_{\omega \in A} P(\omega)$$

Op deze wijze kunnen we een waarschijnlijkheid toekennen aan alle deelverzamelingen van Ω. In het bijzonder is $P(\Omega) = 1$ en voor de lege verzameling is $P() = 0$.

Abstract gezegd: er is een functie P die aan alle deelverzamelingen $A \subset \Omega$ een getal $0 \leq P(A) \leq 1$ toekent.

Elementaire operaties

Er zijn drie elementaire operaties die we op verzamelingen kunnen toepassen die zowel een logische als een kansrekening interpretatie hebben.

1. Allereerst kunnen we de vereniging $A \cup B$ van twee deelverzamelingen van Ω beschouwen. Dit zijn alle elementen die in A *of* B liggen.

2. Vervolgens is er de doorsnede $A \cap B$. Dit zijn de elementen die in A *en* B liggen.

3. Tenslotte is er het complement A^c. Dit zijn alle elementen van Ω die *niet* in A liggen.

De definitie van $P(A)$ impliceert de volgende belangrijke relatie: Laten A en B disjunct zijn, d.w.z. de doorsnede $A \cap B$ is leeg, dan geldt

$$P(A \cup B) = P(A) + P(B)$$

De kans op A of B is in dit geval eenvoudig de som van de twee kansen. We kunnen weer de dobbelsteen als voorbeeld nemen. De kans dat we een 3 of een 4 gooien is de som van de kans op een 3 en de kans op een 4

$$P = \frac{1}{6} + \frac{1}{6} = \frac{1}{3}.$$

Deze bovenstaande eigenschappen worden vaak als startpunt gekozen voor een formele definitie van een kansruimte. Deze wordt gedefinieerd met behulp van de volgende ingrediënten:

1. De uitkomstenruimte Ω, een verzameling van elementen ω (de uitkomsten).

2. Een klasse van deelverzamelingen A van Ω die we gebeurtenissen noemen. Als A en B gebeurtenissen zijn, dan geldt dat ook van $A \cup B$, $A \cap B$ en A^c (respectievelijk "A of B", "A en B" en "niet A").

3. Een toekenning van een getal $P(A)$ aan iedere gebeurtenis A die voldoet aan de volgende regels
   – $P(A) \in [0, 1]$,
   – $P(\Omega) = 1$,
   – de eigenschap: als $A \cap B = \emptyset$ dan is $P(A \cup B) = P(A) + P(B)$.

In het geval van oneindig grote kansruimten wordt deze definitie een stuk subtieler. In dat geval hebben we een kansmaat. Het is heel goed mogelijk dat voor alle elementen $\omega \in \Omega$ de kans $P(\omega) = 0$ is. Denk bijvoorbeeld aan een uniforme maat op het interval $[0, 1]$. De toegestane deelverzamelingen moeten dan een goedgedefinieerde maat hebben.

Verjaardagsprobleem

Laten we de kansrekening toepassen op een klassiek probleem. Wat is de kans dat op een bijeenkomst van n personen (op z'n minst) twee personen op dezelfde dag jarig zijn? Wanneer moeten we verbaasd zijn als deze coïncidentie plaats vindt, en wanneer was dit min of meer te verwachten?

In dit geval bestaat de uitkomstenruimte Ω uit 365^n elementen. Immers iedere aanwezige heeft 365 mogelijke verjaardagen, waarbij we de 29ste februari even buiten beschouwing laten. Het totaal aantal mogelijkheden is daarmee

$$\underbrace{365 \times 365 \times \cdots \times 365}_{n} = 365^n$$

Voor het gemak zullen we alle dagen van het jaar als even waarschijnlijke geboortedagen beschouwen. De kansfunctie is dus

$$P(\omega) = \frac{1}{(365)^n}$$

voor alle uitkomsten ω. Pas op, een uitkomst is hier een n-tupel van verjaardagen.

Hoe berekenen we de kans van de gebeurtenis A dat er minstens twee van de n verjaardagen op dezelfde dag vallen?

In dit geval is het gemakkelijker om eerst de kans uit te rekenen dat dit *niet* gebeurt. A^c staat voor gebeurtenissen waarbij alle n personen een verschillende verjaardag hebben. Hoeveel mogelijkheden zijn dat? De eerste persoon kan een willekeurige dag kiezen, dat zijn er 365. De volgende persoon heeft maar 364 mogelijkheden etc. De laatste persoon heeft nog maar $365 - (n - 1)$ mogelijkheden. Zo vinden we dat de kans p dat er geen gelijke verjaardagen voorkomen gegeven is door

$$p = P(A^c) = \frac{365}{365} \cdot \frac{364}{365} \cdots \frac{365 - (n-1)}{365} = \prod_{k=1}^{n-1} \left(1 - \frac{k}{365}\right)$$

De kans op A, d.w.z. wel minstens twee gelijke verjaardagen, is dan

$$P(A) = 1 - P(A^c) = 1 - p$$

We hebben weliswaar een formeel antwoord gevonden, maar hoe groot is de kans nu in de praktijk? Als we het gewoon (laten) uitrekenen vinden we dat voor n gelijk aan 23 de kans ongeveer 50% is. Dus voor een groep van 23 personen is er een 50% kans dat er twee personen op dezelfde dag jarig zijn. Willen we 95% zekerheid dan moeten we $n = 48$ kiezen. Deze aantallen zijn verrassend klein.

Het is evenwel een compleet andere zaak als we honderd procent zekerheid willen hebben dat de coïncidentie plaatsvindt. Daarvoor moeten we minstens 366 personen hebben. Alleen in dat geval weten we zeker dat de verjaardag van de 366ste persoon zeker al een keer eerder is voorgekomen.

Maar hoe verandert dit getal als we in plaats van verjaardagen hadden gekeken of mensen op hetzelfde huisnummer wonen, of in hetzelfde jaar naar dezelfde plaats op vakantie zijn gegaan, of in dezelfde stad geboren zijn. En wat is de kans als maar één van de bovenstaande reeks van mogelijke coïncidenties hoeft plaats te vinden. Hier komen we in het vaarwater van Jung.

Een algemene formule

Laten we het probleem eerst eens wat algemener formuleren. Stel we hebben n balletjes en die moeten we willekeurig verdelen over c categorieën (met $n \leq c$). Deze categorieën zijn de abstracte versies van de verjaardagen. In het verjaardag voorbeeld was c dus 365. De kans dat er niet meer dan één balletje per categorie is wordt gegeven door

$$p = \prod_{k=0}^{n-1} \left(1 - \frac{k}{c}\right)$$

Deze formule kunnen we benaderen — aannemende dat n relatief klein is ten opzichte van het aantal categorieën c — door de natuurlijke logaritme te nemen en te gebruiken dat

$$\ln(1-x) \approx -x$$

We vinden dan dat

$$\ln p = \sum_{k=0}^{n-1} \ln\left(1 - \frac{k}{c}\right) \approx \sum_{k=0}^{n-1} -\frac{k}{c} \approx -\frac{n^2}{2c}$$

zodat

$$p \approx e^{-n^2/2c}$$

Wat leren we van deze formule? Ten eerste kunnen we nu eenvoudig berekenen wat er voor nodig is om een coïncidentie te verwachten. Voor een 50% kans willen we dat $p = \frac{1}{2}$. Daaruit volgt dat

$$n \approx 1.2\sqrt{c}$$

Dus $n \approx 12$ voor een categorie met 100 elementen. Soortgelijk vinden dat voor een 95% kans op een coïncidentie dat

$$n \approx 2.5\sqrt{c}$$

Dus $n \approx 25$ voor een categorie met 100 elementen.

Dit zijn interessante formules. We zien dat het aantal personen voor een waarschijnlijke coïncidentie groeit met de wortel van het aantal categorieën. Hadden we twaalf mensen nodig voor een 50% kans op een coïncidentie met een keuze uit 100 mogelijkheden, als we het aantal mogelijkheden verhonderdvoudigen tot 10.000, dan hoeft het aantal personen slecht met een factor tien toe te nemen tot 120. Soortgelijk als we 1200 mensen ieder een getal laten kiezen onder de miljoen, dan is er weer een 50% kans dat twee hetzelfde getal hebben gekozen.

Stel dat we nu m categorieën gaan introduceren, zeg met een aantal mogelijkheden $c_1, c_2, \ldots, c_m$. Wat is de kans dat we met n personen ergens in deze categorieën een coïncidentietreffer scoren? We kunnen weer eerst kijken naar de kans dat er geen coïncidenties zijn in alle categorieën. Laat p_1 de kans zijn dat er *geen* coïncidenties zijn in categorie c_1, p_2 de kans zijn dat er *geen* coïncidenties zijn in categorie c_2, etc. Dan is de totale kans op *geen* coïncidenties

$$p = p_1 \cdot p_2 \cdots p_m$$

Maar dat kan berekend worden als

$$p \approx e^{\left(-\sum_{j=1}^{m} \frac{n^2}{2c_j}\right)} = e^{\left(-\frac{n^2}{2\bar{c}}\right)}$$

met

$$\frac{1}{\bar{c}} = \frac{1}{c_1} + \ldots + \frac{1}{c_m}$$

Nu kunnen we weer n oplossen en vinden met deze nieuwe 'effectieve' waarde van c

$$n \approx 1.2\sqrt{\bar{c}}$$

In het bijzonder als we m categorieën hebben die allen dezelfde grootte c hebben, dan is $\bar{c} = c/m$ zodat voor een 50% kans

$$n \approx 1.2\sqrt{c/m}$$

Stel we houden $c = 100$ maar laten nu $m = 25$ categorieën toe, dan zijn twee á drie personen al genoeg voor een coïncidentie met 50% kans.

3.2 Redeneren met onzekerheid

Het samenspel van fysische en cognitieve gezichtspunten komt wel bijzonder natuurlijk naar voren bij het thema waarschijnlijkheid. Anders dan in de meeste gebieden van de wiskunde zijn hier na het ontstaan van de theorie duidelijk verschillende interpretaties in omloop, die beiden een legitieme uitleg geven van wat de waarschijnlijkheidsrekening nu eigenlijk beschrijft. Dat wil niet zeggen dat er elkaar bestrijdende 'waarschijnlijkheidsleren' bestaan, maar wel dat de twee lijnen van dit boek elkaar hier op natuurlijke wijze snijden. We zullen dit thema weer uitwerken vanuit logisch perspectief, want redeneren met onzekerheid is een typisch menselijke bezigheid waaraan niemand ontkomt in het gewone leven.

Twee gezichten van waarschijnlijkheid

Waarschijnlijkheid is een begrip met twee gezichten, die al spelen sinds de eerste wiskundige theorievorming op dit gebied. Aan de ene kant is er *objectieve waarschijnlijkheid* in de natuur, met kansen gebaseerd op feitelijke frequenties. Dat we het getal 3 een kans van $\frac{1}{6}$ geven om geworpen te worden met een dobbelsteen berust op deze interpretatie - uiteraard mits we een perfect symmetrische dobbelsteen beschouwen. En bij radio-actieve processen komen deeltjes volgens een objectief natuurkundig toevalsproces vrij. Algemener gezegd, op deze manier zegt het meest elementaire waarschijnlijkheidsoordeel ons dat

$P_{obj}(A) = k\%$

De gebeurtenis A doet zich voor in $k\%$ van de gevallen in de totale ruimte van alle mogelijke uitkomsten.

In de wiskundige theorie, maar ook in de statistische praktijk, worden naast dergelijke percentages ook andere waarschijnlijkheidsmaten dan percentages gehanteerd voor gebeurtenissen. Maar ook deze weerspiegelen reële verschijnselen, bijvoorbeeld de verdeling van de aankomsttijden van auto's bij een stoplicht, of de spreiding van geboorten door het jaar heen. Objectieve waarschijnlijkheden weerspiegelen gebeurtenissen die zich echt voordoen in een proces met vele herhalingen.

Toch zijn er ook veel situaties waar dit begrip niet werkt, bijvoorbeeld bij unieke gebeurtenissen waar geen grotere ruimte omheen zit van soortgelijke gevallen. Wat is de kans dat een kerncentrale explodeert? Wat is het percentage leugentjes om bestwil onder alle beweringen die Nederlanders in een jaar doen? In zulke situaties werkt men vaak met *subjectieve waarschijnlijkheid*, waarbij de formule $P(A) = k$ gerelateerd wordt aan een persoon, en dan meer zoiets betekent als:

$P_{subj}(i, A) = k$

De graad van geloof van een zekere persoon i dat gebeurtenis A optreedt is k.

Met andere woorden, hoeveel kans geeft iemand aan een bewering A? Uiteraard kan deze subjectieve verwachting per persoon verschillen. Het is ook goed mogelijk dat er wel degelijk een onderliggende objectieve kans is, maar dat personen toch hun eigen subjectieve schattingen volgen wanneer ze redeneren en plannen maken. Subjectieve waarschijnlijkheid ligt dichter tegen de logica aan, vanwege het verband met beweringen en het geloof van personen die over hun meningen nadenken. We nemen dit tweede begrip in dit hoofdstuk nu verder onder de loep.

Overigens duurt het filosofisch debat over de interpretatie van waarschijnlijkheid voort. Er is nog een derde alternatieve wiskundige uitleg van waarschijnlijkheid door Von Mises in termen van 'randomness', de mate van willekeurigheid van reeksen uitkomsten. En zelfs de beroemde Russische

P 7.

BLAISE PASCAL

1623 — 1662

JOHAN DE WITT

1625 — 1672

wiskundige Kolmogorov, in de jaren 1930 bedenker van de gangbare waarschijnlijkheidsaxioma's uit het vorige hoofdstuk, was niet tevreden met zijn eigen theorie. In zijn latere jaren prefereerde hij een uitleg van kansprocessen via een beschrijvingen van uitkomsten door hun kortste coderingen in Turing machines! Deze wiskundige discussie weerspiegelt een meer algemene cognitieve kwestie. Ons vermogen tot redeneren is doordrongen van waarschijnlijkheidsbegrip en het inschatten van kansen. Gewone taal bevat allerlei kansuitdrukkingen als 'mogelijk', 'vast wel', 'doorgaans', 'bijna zeker', en 'waarschijnlijk'. Niettemin is het een ervaringsfeit dat mensen minder goed kunnen omgaan met dit soort redeneren dan met strikte informatie van het meer klassiek logische soort. Vergissingen zijn frequent, en zelfs professionele cognitiewetenschappers twisten erover hoe mensen nu echt redeneren met onzekerheid.

Wedden en verwachte waarde

Ondanks de wat softe klank van het begrip is het wel degelijk mogelijk subjectieve kansen preciezer te meten, en wel in observeerbaar menselijk gedrag. De oorsprong van de wiskundige waarschijnlijkheidsleer ligt zelfs in de analyse van ons gedrag in kansspelen. In het werk van zeventiende eeuwse geleerden als Blaise Pascal en Johan de Witt worden een weddenschap of een contract gebruikt om een concrete numerieke uiting van een subjectieve kans te geven. Beschouw hiertoe het volgende scenario:

> Ik wed met u 2 tegen 1 dat A het geval is.

Dit wil het volgende zeggen. Ik betaal aan u twee maal de inzet als A niet het geval is, maar ik krijg van u één maal de inzet als A wel het geval is. Mijn bereidheid tegen u te wedden op A met k tegen n wordt doorgaans gezien als een objectieve maat van de subjectieve waarschijnlijkheid die ik aan A toeken, en wel als volgt:

$$P(A) = \frac{k}{k+n}.$$

De kans die ik aan A toeken blijkens bovenstaande weddenschap is dan $2/3$. De reden van deze gelijkstelling is de volgende. Een weddenschap heet 'eerlijk' als de *verwachte waarde* voor beide spelers 0 is. Niemand heeft dan op de lange duur, als er vaak zou worden gespeeld, een systematisch voordeel.

Alleen al de formulering van het centrale begrip 'verwachte waarde' was een doorbraak in de zeventiende eeuw. Deze notie werd pas goed uitgelegd in het eerste leerboekje over waarschijnlijkheid, geschreven door Christiaan Huygens, ooit studiegenoot te Leiden van Johan de Witt:

> Gegeven zijn elkaar uitlsuitende uitkomsten $A_1, ..., A_n$, die tezamen alle mogelijkheden uitputten. De verwachte waarde is nu de som
>
> $$\sum_{i=1}^{k} P(A) \cdot \text{waarde}(i).$$

Bijvoorbeeld, bij de bovenstaande weddenschap is mijn verwachte waarde:

$$(P(A) \cdot 1) + (P(\neg A) \cdot (-2)) = (\frac{2}{3} \cdot 1) - (\frac{1}{3} \cdot 2) = 0$$

Meer in het algemeen zien we hetzelfde met wedden met k tegen n:

$$\left(\frac{k}{k+n} \cdot n\right) + \left(\frac{n}{k+n} \cdot (-k)\right) = 0$$

Overigens zijn niet alle weddenschappen waarmee wij ons uit vrije wil inlaten eerlijk. Neem de roulette in het Holland Casino. Er zijn 37 vakjes. Als ik 'rouge' speel, dan krijg ik mijn inleg als het balletje op rood valt, en anders verlies ik mijn inleg. Maar dit betreft alleen de vakjes 1 tot en met 36. Valt het balletje op de 0 dan wordt nog een keer gedraaid, en ik verlies mijn inzet als het dan niet op rood komt. Mijn verwachte waarde in dit spel bij een inzet van één euro is als volgt:

$$\left[\frac{18}{37} \cdot 1 + \frac{18}{37} \cdot (-1)\right] + \left[\frac{1}{74} \cdot 0 + \frac{1}{74} \cdot (-1) = -\frac{1}{74}\right]$$

Op den duur ga ik hier dus geld op verliezen. Men spreekt wel van systematische oneerlijkheid in een dergelijke aangeboden weddenschap. Dit voordeel ten opzichte van de klant is de reden waarom entrepreneurs casino's starten. Ze worden er met grote waarschijnlijkheid beter van!

Dutch books

Een stelsel weddenschappen dat tegelijk wordt afgesloten heet een 'boek' (vandaar het Engelse woord 'bookmaker'). Mensen op de renbaan sluiten vaak boeken af: ze 'wedden op meerdere paarden'. Bekijk nu eens het volgende, wellicht wat bizarre, boek dat ik u voorstel:

> Ik wil met u wedden 1 tegen 2 dat A, en tegelijkertijd ook 1 tegen 2 dat $\neg A$.

Wat is uw verwachte waarde als u hierop in gaat? Hier is een tabel:

	A	$\neg A$
	ik krijg 2 euro	u krijgt 1 euro
	u krijgt 1 euro	ik krijg 2 euro
Totaal	ik krijg 1 euro	ik krijg 1 euro

Onder alle omstandigheden krijg ik dus geld van u. Een dergelijk stel weddenschappen heet een 'Dutch Book', een terminologie die wel iets zegt over hoe onze westerburen vroeger dachten over Nederlandse handelspraktijken. Uiteraard is dit een situatie om te vermijden. De manier waarop staat aangegeven in het volgende wiskundige resultaat van Kemeny en Shimony uit 1953.[2] U moet ten allen tijde uw wedgedrag laten beheersen door de axioma's van de waarschijnlijkheidsleer!

Stelling *Dutch Book Stelling*

De enige interpretatie voor de waarschijnlijkheden $P(\neg A)$ en $P(A \vee B)$ die gegarandeerd oneerlijke boeken verhindert, is wedden volgens de gangbare wiskundige axioma's: $P(\neg A) = 1 - P(A)$ en $P(A \vee B) = P(A) + P(B)$ indien $P(A \wedge B) = 0$.

Beslissen onder onzekerheid

Verwachte waarden, vaak gebaseerd op subjectieve waarschijnlijkheden, liggen met name ten grondslag aan *beslissingen*. In dat geval gaat het niet meer om weddenschappen op zich, maar om handelen in het algemeen. Moet ik bijvoorbeeld een reisverzekering kopen? Er zijn twee scenario's. Een ongeval doet zich voor, of mijn reis verloopt veilig. Om te kunnen beslissen moet ik wel de waarden kennen die ik hecht aan die uitkomsten, afhankelijk van het al dan niet aanschaffen van de verzekering. Zeg dat die als volgt liggen:

	Ongeval	Veilig
Kopen	10	5
Laten	-20	9

Laat nu de kans die ik toeken aan een ongeval 1/10 zijn. We berekenen eerst de verwachte waardes voor beide handelwijzen apart, om ze daarna te vergelijken:

$$\begin{aligned} VW(Kopen) &= 0.1 \cdot 10 + 0.9 \cdot 5 = 5.5 \\ VW(Laten) &= 0.1 \cdot (-20) + 0.9 \cdot 9 = 6.1 \end{aligned}$$

De aanbeveling van de rationele beslissingstheorie luidt in het algemeen:

> Kies de handelwijze met de grootste verwachte waarde.

In dit geval zou dat zijn: "Laten!", en op reis gaan zonder verzekering. Uiteraard hangt zo'n conclusie per persoon af van diens subjectieve waarschijnlijkheden, plus de *nutswaarden* die iemand toekent aan de uitkomsten onder beide scenario's. Met andere nutswaarden kan de bovenstaande aanbeveling bijvoorbeeld gemakkelijk veranderen. Overigens is het kopen van verzekeringen, op deze manier beschouwd, vaak in ons nadeel. Maar we doen het doorgaans toch. Kennelijk hebben we toch zo onze aanvullende redenen, zoals de behoefte ons extra in te dekken tegen het ergste geval.

[2] Kemeny was assistent van Einstein in Princeton, maar hij werd uiteindelijk pionier in wiskunde en computers.

Zeer duidelijk zien we dit indekken voor het slechtste geval als we dezelfde situatie analyseren in de *speltheorie*, die we nader zullen bespreken in het volgende hoofdstuk. In een speltheoretisch scenario kennen we vaak geen waarschijnlijkheden voor de mogelijke uitkomsten, of we negeren ze. We volgen in zo'n situatie meer globale aanbevelingen als:

Kies de handelwijze die in het ergste geval de hoogste uitkomst garandeert.

In het bovenstaande geval zou dat dan juist 'Kopen' zijn van de reisverzekering, omdat het ergste wat ons daar kan overkomen (5) veel minder erg is dan de -20 die de optie 'Laten' ons kan aandoen.

Rekenen met waarschijnlijkheid

De rekenregels voor waarschijnlijkheid, objectief of subjectief opgevat, zijn reeds besproken in 3.1. We zagen onder meer regels voor een negatie $P(\neg A)$ en een disjunctie $P(A \vee B)$ met disjuncte uitkomstenverzamelingen A en B, zoals ook nog eens gememoreerd in de Dutch Book Stelling. De regel voor conjunctie van gebeurtenissen is lastiger: met name was $P(A \wedge B)$ in het algemeen niet gelijk aan het product $P(A) \cdot P(B)$, zoals men eenvoudig ziet bij proberen van wat concrete percentages. De gelijkheid $P(A \wedge B) = P(A) \cdot P(B)$ geldt alleen als de betrokken gebeurtenissen A en B 'onafhankelijk' zijn van elkaar. Voorbeelden daarvan zijn het gooien van een ideale dobbelsteen, of het uitvoeren van achtereenvolgende trekkingen voor de Champion's League. De juiste algemene regel voor de kans op een conjunctie van gebeurtenissen is de volgende:

$$P(A \wedge B) = P(A) \cdot P(B|A)$$

Maar wat betekent die laatste formule met de rechtopstaande streep?

Nieuwe informatie: nieuwe kansen

De mate waarin wij iets geloven is niet eens en voor altijd gegeven. Zij wordt beïnvloed door binnenkomende nieuwe informatie. Als uw vliegtuig eenmaal veilig is geland, dan is de kans die u in het bovenstaande aan de gebeurtenis 'Veilig' toekent natuurlijk van 0.9 naar 1 omhoog gegaan. Dit mechanisme van *update* van waarschijnlijkheidswaarden $P(A)$ op grond van nieuwe informatie is essentiëel om te begrijpen hoe wij met kansen redeneren. Hoe werkt het systematisch?

Voorbeeld Verkiezingskandidaat A heeft kans $0,4$ om te winnen, B heeft $0,3$, C $0,2$, en D $0,1$. Nu trekt kandidaat C zich plotseling terug na een onthullende publikatie in het weekblad Panorama. Wat zijn de nieuwe kansen voor de resterende kandidaten? We berekenen de

conditionele waarschijnlijkheid $P(A|B)$ de kans op A na nieuwe informatie dat B

Deze wordt gedefinieerd als een quotiënt:

$$P(A|B) = \frac{P(A \wedge B)}{P(B)}$$

Dit is de simpelste manier van 'herschalen' der oude waarschijnlijkheden, gegeven het feit dat de B-verzameling van uitkomsten nu het hele universum is geworden. Bijvoorbeeld, na het terugtrekken van C ligt de nieuwe kans voor A als volgt:

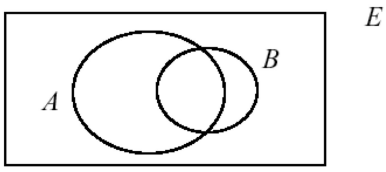
$$P(A|\neg C) = \frac{P(A \wedge \neg C)}{P(\neg C)} = \frac{P(A)}{P(\neg C)} = \frac{0,4}{0,8} = 0,5.$$

P 8.

THOMAS BAYES

1702 — 1761

In een plaatje is dit heel concreet voor te stellen. Laat de rechthoek E de verzameling zijn van alle mogelijke uitkomsten, de cirkel A de uitkomsten die aan A voldoen, en evenzo voor B. Denk nu aan $P(A)$ als het percentage van de A's in E. Zodra we B weten, beperken we ons tot de getekende B-cirkel. Het percentage der A's daarbinnen: dat wil zeggen, de doorsnede $A \cap B$, kan natuurlijk heel anders liggen dan voorheen:



Dit is hetzelfde soort plaatje als de Venn-diagrammen die we tekenden voor natuurlijke taal in het eerste hoofdstuk, en de beperking tot B bij conditionele waarschijnlijkheid lijkt inderdaad wel wat op het daar besproken principe van Conservativiteit. $\overset{\text{P. 9}}{\Longrightarrow}$ 40

Hier is een handige regel om conditionele waarschijnlijkheden uit te rekenen, mits we enkele andere al kennen. Ze werd bedacht door de Engelse dominee Bayes rond 1720.

Stelling

$$P(A|B) = P(B|A) \cdot \frac{P(A)}{P(B)}$$

Het bewijs van deze nuttige regel is heel simpel. We weten op grond van de eerdere definitie dat

$$P(A|B) = \frac{P(A \wedge B)}{P(B)} \quad \text{en evenzo dat} \quad P(B|A) = \frac{P(B \wedge A)}{P(A)}.$$

Maar nu geldt overduidelijk dat $P(A \wedge B) = P(B \wedge A)$, zodat we voor de $P(A \wedge B)$ in de eerste regel op grond van de tweede regel kunnen invullen: $P(B|A) \cdot P(A)$. Q.E.D.

Een soortgelijke redenering geeft uitvoeriger versies van Bayes' Regel:

$$P(A|B) = P(B|A) \cdot \frac{P(A)}{P(B|A) \cdot P(A) + P(B|\neg A) \cdot P(\neg A)}$$

$$P(A_i|B) = P(B|A_i) \cdot \frac{P(A_i)}{\sum_i P(B|A_i) \cdot P(A_i)}$$

Met dit soort regels kan men voor personen nieuwe verwachtingen uitrekenen. Bijvoorbeeld, u bent een geregeld drinker, en de kans dat u een glas wijn drinkt is $0,1$. Stel dat ik verder weet dat uw kans op hoofdpijn na het drinken van een glas wijn $0,8$ is. U heeft nu hoofdpijn, maar die kwaal is wel iets waaraan u al zo'n 20% van uw leven lijdt. Hoe groot acht ik dan de de kans dat deze hoofdpijn komt doordat u een glas wijn heeft gedronken?

$$P(W|H) = P(H|W) \cdot \frac{P(W)}{P(H)} = 0,8 \cdot \frac{0,1}{0,2} = 0,4$$

Overigens kunnen deze kansen voor mij weer anders gaan liggen als ik meer over de situatie te weten kom. Bijvoorbeeld dat u kort geleden bij uw hotelkamer bent gesignaleerd met een dame en een fles Chateau Migraine. Meer algemeen speelt hier een proces van update van waarschijnlijkheden op grond van nieuwe informatie. Update van informatie is een heel algemeen verschijnsel, dat we al meerdere malen hebben ontmoet in dit boek. Het werkt evengoed voor processen zonder intrinsiek kanselement, zoals communicatie. Dit laatste thema zal nog terugkeren in ons volgende hoofdstuk.

Nogmaals redeneerproblemen

Redeneren met conditionele waarschijnlijkheden leiden vaak tot allerlei misrekeningen. Zo worden dikwijls conditionele waarschijnlijkheden $P(A|B)$ en $P(B|A)$ omgekeerd:

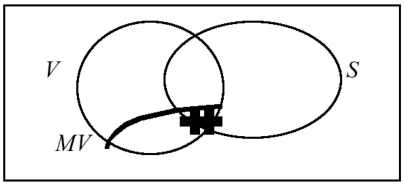
> Amsterdamse reizigers zijn vaak zwartrijders ($P(Z|A)$). Want kijk maar, als je mensen in Holland ziet zwart rijden, dan zijn dat wel heel erg vaak Amsterdammers ($P(A|Z)$).

Een ander voorbeeld van onduidelijke intuïties betreft de mate waarin beweringen elkaar qua waarschijnlijkheid beïnvloeden:

> een nieuwe bewering B bevestigt A als $P(A|B) > P(A|\neg B)$.

Hier raakt de waarschijnlijkheid aan de juridische praktijk, waar het essentiële rechtsbegrip 'redelijke twijfel' eveneens berust op het schatten van kansen. Een goede illustratie is de roemruchte rechtzaak tegen O.J. Simpson wiens vrouw was vermoord (V). Ook werd tijdens het proces bekend dat O.J. zijn vrouw sloeg (S). Nu wist men op grond van misdaadstatistieken dat de kans dat iemand die zijn vrouw slaat haar ook nog eens vermoordt ($M \wedge V$) zo'n één promille bedraagt. Dat wil zeggen de conditionele kans $P(M \wedge V|S) = 0,001$. Bevestigde het nieuwe feit S tijdens het proces nu het vermoeden dat O.J. Simpson zijn vrouw vermoordde? O.J. Simpson's advocaten beweerden dat het die kans juist verminderde, omdat slaanders kennelijk zo zelden doders zijn! Het correcte antwoord is dat het niet valt te zeggen op grond van deze gegevens, want we kennen de kans niet dat mannen die hun vrouw *niet* slaan haar wel vermoorden. Misschien ligt die hoger, omdat het slaan als uitlaatklep ontbreekt ... maar misschien ook niet.

Overigens is de echte kans waarin we geïnteresseerd zijn in een dergelijke situatie eerder wat we schatten op grond van *alle* relevante gegevens. Dat zou dan eerder $P(MV|(V \wedge S))$ zijn. Ook deze situatie is weer concreet voor te stellen met een plaatje. We hebben te maken met drie gebieden van mogelijke gebeurtenissen V, S, en MV waarover we slechts partiële informatie hebben. En we weten in deze rechtszaak met name niet genoeg om te bepalen wat het percentage is van het zwarte deelgebied van de doorsnede $V \cap S$:[3]

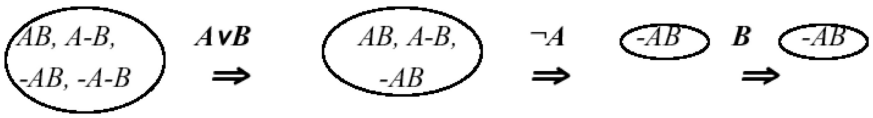


Waarschijnlijkheid en logica

De regels van de waarschijnlijkheidsrekening voor negatie en disjunctie lijken wel wat op de rekenregels voor propositielogica in eerdere hoofdstukken. Bekende auteurs als Carnap hebben in de jaren vijftig van de vorige eeuw dan ook gezocht naar een zogenaamde 'inductieve logica', die logica en waarschijnlijkheidsrekening zou moeten combineren. De logica doet dan het skelet van kwalitatieve deductief geldige redeneringen, terwijl waarschijnlijkheden hier meer kwantitatieve structuur aan verlenen. Op zo'n manier wordt de diepe kloof tussen 'geldig' en 'ongeldig' wat kleiner, omdat ongeldige redeneringen soms toch een zekere mate van plausibiliteit hebben. Hier is nog eens een eerder voorbeeld van een geldige gevolgtrekking:

$$A \vee B, \neg A \Rightarrow B$$

Een serie updates van informatie voor de premissen ziet er als volgt uit, beginnend met vier mogelijke uitkomsten waarvan we niet weten welke de juiste is:



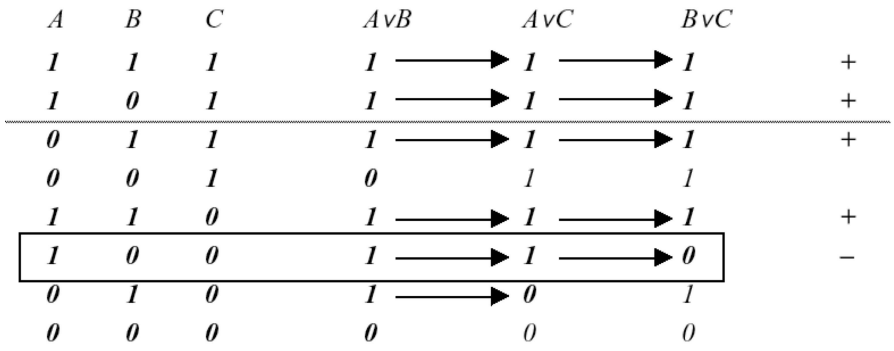
Het feit dat de update met bewering B aan het eind geen informatie meer toevoegt weerspiegelt het feit dat B geldig volgt als conclusie uit de twee gegevens $A \vee B, \neg A$. Maar het plaatje geeft ook waarschijnlijkheden. De kans op B is aan het begin $\frac{1}{2}$, als de vier mogelijkheden gelijke waarschijnlijkheid hebben. Maar na de update met de eerste premisse is ze toegenomen tot $\frac{2}{3}$, en na update met de tweede premisse is ze zelfs 1, en dat blijft ze. De conclusie is 100% zeker.

Laten we nu eens een ander geval bekijken, weer met de updates getekend. Ongeldig was bijvoorbeeld de gevolgtrekking

$$A \vee B, A \vee C \Rightarrow B \vee C.$$

In dit geval zijn de updates als volgt, dit keer in een volledige waarheidstabel opgeschreven:

[3] Er is overigens meer te zeggen over de rol van waarschijnlijkheid in de O.J. Simpson zaak, en er is daarover ook gepubliceerd in de statistische vakliteratuur.



We lezen enkele relevante conditionele waarschijnlijkheden af voor de updates:

$$P(B \vee C) = \frac{3}{4}, P(B \vee C | A \vee B) = \frac{5}{6}, P(B \vee C | (A \vee B) \wedge (B \vee C)) = \frac{4}{5}$$

Hier is dus meer drama. De conclusie won aan plausibiliteit na de eerste premisse, en zakte weer iets na de tweede, maar blijft aan het eind toch plausibeler dan aan het begin. Dit soort eenvoudige logische modellen zijn nog verder te verfijnen als we ook nog eens verschillende kansen toekennen aan verschillende uitkomsten in de totale logische ruimte.

Moderne inductieve logica gaat veel verder dan dit soort simpele rekenregels. Men bepaalt doorgaans conditionele waarschijnlijkheden van beweringen A met gewogen mengsels van twee ingrediënten: (i) een beginschatting van de kans op A, maar ook (ii) de tot nu toe geconstateerde frequentie van A. Aldus komen zowel subjectieve als objectieve waarschijnlijkheid tot hun recht! Een weegfactor geeft daarbij aan hoe snel wij leren van ervaringen dan wel vasthouden aan onze vooroordelen. Deze combinatie van factoren, en de mogelijke variatie in hoe ze worden gewogen, lijkt sterk op feitelijk gedrag bij mensen, en de mogelijke diversiteit daarin.

Overigens heeft het thema logica en waarschijnlijkheid ook heel andere kanten. Bijvoorbeeld, spelen statistische aspecten ook een rol in de metamathematica? Kunnen we zinvol praten over kansen op bewijzen of op waarheid in een wiskundige theorie? In elk geval is de laatste jaren ontdekt dat logische bewijssystemen soms verrassende, en van te voren niet vermoede, statistische eigenschappen hebben wanneer men kijkt naar de bewijslengte en bewijsduur voor grote aantallen formules.

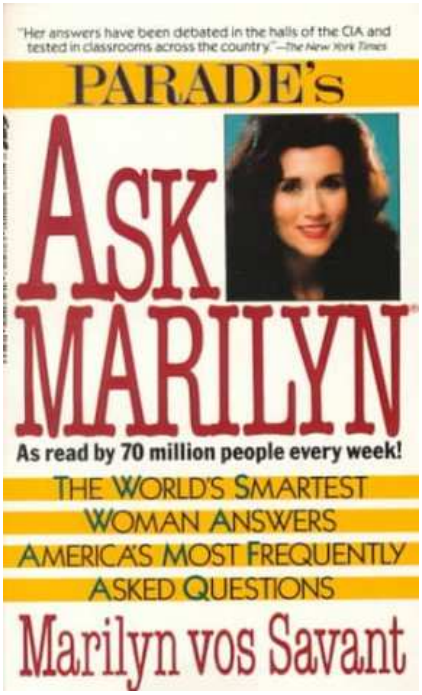
Problemen: modelleren gaat vooraf aan redeneren

Zelfs als we alle rekenregels op orde hebben, en helder voor de geest, dan blijft redeneren met onzekerheid toch moeilijk. Dit komt door een prealabele stap, die bij logisch redeneren meestal eenvoudig is: wat is de *correcte beschrijving* van de situatie? Men noemt dit de keuze van het 'statistisch model'. Geschikte modelkeuze is essentieel voor goede resultaten in toegepaste wiskunde. Veel puzzels in statistisch redeneren — en die zijn er te over — illustreren deze moeilijkheid. We bespreken hier een beroemd geval.

Het Quizmaster Dilemma, versie 1

Een quizmaster toont drie deuren. Achter één van deze deuren staat een auto, en de quizmaster weet achter welke. U mag nu één van de deuren kiezen. Als daarachter een auto blijkt te staan mag u die houden. Vervolgens opent de quizmaster een andere deur dan uw keuze, waarachter geen auto blijkt te staan. Hij staat u nu toe om uw keuze te veranderen. Wat moet u doen? Bij de oude keuze blijven?

Veranderen? Dit probleem werd in de jaren zeventig gepubliceerd in de Amerikaanse puzzelcolumn van Marilyn Vos Savant.[4] Het leidde meteen tot verhitte discussie in kranten en vaktijdschriften, zelfs tussen professionals. Hier is een eerste redenering.



Stel u kiest deur 1. Schrijf D_i voor 'de auto staat achter deur i'. Eerst is de kans $P(D_1) = \frac{1}{3}$, want er zijn drie mogelijheden, en u heeft geen speciale informatie ten gunste van een van deze. Laat de quizmaster nu bijvoorbeeld de deur 2 openen. U leert dan dat $\neg D_2$, en dus lijkt het nu te gaan om de nieuwe kans $P(D_1|\neg D_2)$. Deze kunt u uitrekenen met Bayes' Regel, en u vindt $P(D_1|\neg D_2) = \frac{1}{2}$. Het heeft dus geen zin om te switchen naar deur 3.

Dit klinkt wellicht plausibel, maar het hier gekozen model geeft de nieuwe informatie niet goed weer! Wat u geleerd heeft is namelijk niet alleen dat de auto niet achter deur 2 staat, maar dat

de quizmaster deur 2 opende ('QD_2').

En dit bevat meer informatie dan alleen $\neg D_2$. Want in het gegeven scenario moet hij als volgt te werk zijn gegaan. Als de auto achter deur 1 staat kiest hij een willekeurige andere deur, als de auto achter deur 2 of 3 staat, dan opent hij de andere van die twee. Nu rekenen we nog eens de conditionele kans uit:

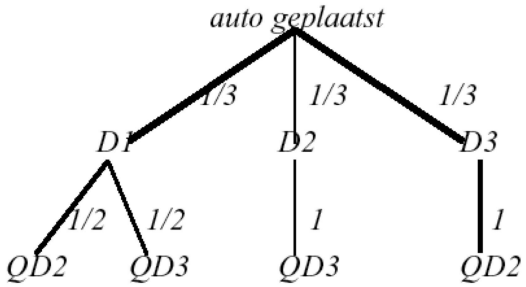
$$P(D_1|QD_2) = P(QD_2|D_1) \cdot \frac{P(D_1)}{\sum_i P(QD_2|D_i) \cdot P(D_i)} =$$

$$\frac{1/2 \cdot 1/3}{(1/2 \cdot 1/3 + 0 \cdot 1/3 + 1 \cdot 1/3} = \frac{1/6}{1/2} = \frac{1}{3}$$

Met andere woorden, gegeven dat QD_2, is de kans juist kleiner dat de auto achter deur 1 staat dan achter de resterende deur 3, en u moet dus switchen! Dit laatste is inderdaad de correcte uitkomst.

We illustreren dit nog eens anders. Hier is een boom waarin alle mogelijke gebeurtenissen staan getekend:

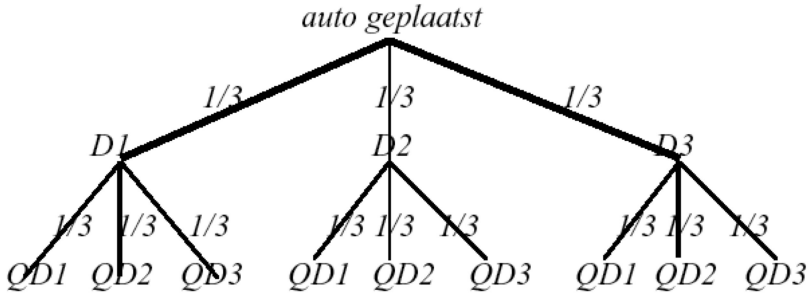
[4] In het Guiness book of records staat Marilyn Vos Savant te boek als de persoon met het hoogst gemeten IQ ooit: 228.



QD_2 gebeurt op de twee zwarte takken, één met totale kans $1/3 \cdot 1/2 = 1/6$, de ander met $1/3 \cdot 1 = 1/3$. U ziet nu grafisch dat de kans op D_1 binnen dat zwarte bereik $1/3$ is!

Quizmaster Dilemma, versie 2

Statistische aanbevelingen luisteren nauw naar het scenario. Stel nu eens dat de quizmaster een deur opent, maar dit keer zonder zelf te weten waar de auto staat. Weer blijkt er nu geen auto te staan achter de geopende deur. Verandert dit uw analyse? Het antwoord is "Ja". De kans op D_1 is nu $1/2$, en wisselen heeft geen zin. Dit is weer uit te rekenen met Bayes' regel, en in wezen is de oorspronkelijke redenering nu correct. De eerdere boom wordt in dit nieuwe scenario:



Gegeven dat deur 2 is geopend, en er staat geen auto achter, zitten we op een der zwarte takken, beide met kans $1/9$, en de kans op D_1 daarbinnen is inderdaad $1/2$.

Er is veel meer te zeggen over de logica die schuilt achter dit soort redeneerprocessen. Maar als gebruikelijk aan het eind van onze hoofdstukken nemen we liever een kort kijkje in de realiteit, en stellen onze gebruikelijke vraag. Hoe manifesteert waarschijnlijkheid zich eigenlijk in onze gewone taal, en in ons alledaagse redeneren?

Waarschijnlijkheid in natuurlijke taal

Zoals we reeds opmerkten is het vocabulaire aan kansuitdrukkingen in onze gewone taal zeer rijk, met woorden als 'waarschijnlijk', 'zeker', 'gewoonlijk', 'doorgaans', etc. En zelfs gewone bijvoeglijke naamwoorden als 'breekbaar' of 'hulpvaardig' lijken al een ingebouwd kansaspect te hebben. Zo zijn 'breekbare' objecten diegene met een zekere kans om in bepaalde omstandigheden te breken. Overigens is niet gezegd dat achter deze alledaagse woorden nu juist standaard wiskunde steekt. In feite concurreren in de literatuur allerlei theorieën over waarschijnlijkheidsaspecten van natuurlijke taal,

van officiële waarschijnlijkheidsrekening tot de ook in bredere kring bekend geraakte 'fuzzy logic'. Misschien zijn er zelfs meerdere cognitieve mechanismen die dit soort redeneren in taal bepalen.

Bekijk om die diversiteit te begrijpen eens de kwalitatieve kansuitdrukking

als A dan doorgaans ook B Notatie: WAB.

Hier volgen twee bekende, maar verschillende visies op de betekenis van deze uitdrukking in de taalkunde. De eerste uitleg zegt dat B kans $> 1/2$ heeft, gegeven dat A:

Doorgaans-1 W_1AB

In de meeste gevallen met A gaat ook B op.

Een 'test' op zo'n formele uitleg is bijvoorbeeld de vraag welke gevolgtrekkingen nu geldig zouden worden. Die kunnen we dan vergelijken met onze intuïtieve oordelen als taalgebruikers. Ter illustratie kiezen we als test-set we de volgende redeneerpatronen met 'doorgaans':

$$\begin{aligned} WAB &\Rightarrow W(A \wedge C)B \\ WAB &\Rightarrow WA(B \vee C) \\ WAB, WAC &\Rightarrow WA(B \wedge C) \\ WAB, WCB &\Rightarrow W(A \vee C)B \\ WAB, WBC &\Rightarrow WAC \end{aligned}$$

De antwoorden die W_1 hiervoor geeft volgen hier. Deze weerspiegelen de gevolgtrekkingseigenschappen van de kwantor 'de meeste' uit hoofdstuk 1:

ongeldig, geldig, ongeldig, ongeldig, ongeldig.

Deze antwoorden zijn gemakkelijk te controleren. Bekijk bijvoorbeeld de laatste redeneervorm. Deze is wel geldig voor de wiskundige standaard kwantor 'alle', of 'altijd'. Uit "Alle A zijn B" en "Alle B zijn C" volgt immers "Alle A zijn C". Maar voor 'doorgaans' is makkelijk een concreet tegenvoorbeeld te bedenken:

> De meeste getallen in de verzameling $\{1, 2, 3, 4, 5\}$ zijn in $\{1, 3, 5\}$, de meeste getallen in $\{1, 3, 5\}$ zijn in $\{1, 5\}$, maar de meeste getallen in $\{1, 2, 3, 4, 5\}$ zijn niet in $\{1, 5\}$.

Twee ware 'doorgaans' beweringen zijn dus niet geldig aan elkaar te schakelen. Anders dan bij 'Alle' kan in een langere keten van waarschijnlijkheidsoordelen de plausibiliteit onderweg weglekken. Deze lekkage is een welbekend verschijnsel in de praktijk.

Maar er is ook een bekende alternatieve uitleg van plausibiliteit, die een ander, veel minder kansgericht beeld geeft van onze activiteit. We nemen dan aan dat de mogelijke gevallen die zich kunnen voordoen door ons zelf geordend zijn naar hun mate van 'plausibiliteit'. Het volgende alledaagse voorbeeld illustreert de gangbaarheid daarvan:

> Als ik de trein neem (T), kom ik *doorgaans* in Amsterdam (A). Ik neem de trein. Dus ik kom in Amsterdam.

Strikt genomen zijn er nog extra gegevens vereist zoals dat 'de NS functioneert' om de conclusie te legitimeren. Men kan de acceptatie van een zeer redelijke conclusie als hierboven modelleren door situaties te rangschikken naar plausibiliteit. Er zijn situaties waarin de NS niet functioneert, maar ik beschouw die als minder plausibel dan situaties waar zij wel functioneert, en ze zijn dus minder relevant voor mijn directe gevolgtrekkingen. In de meest plausibele gevallen volgt voor mij dan inderdaad 'Amsterdam bereiken' uit 'de trein nemen'. Het achterliggende idee kunnen we als volgt algemeen definiëren:

Doorgaans-2 W_2AB

In alle meest-plausibele gevallen met A gaat ook B op.

Het verschil met de eerdere kans-uitleg merkt u onder meer in de lijst van geldige redeneervormen. De antwoorden op de gegeven testbatterij van gevolgtrekkingen worden nu:

ongeldig, geldig, geldig, geldig, ongeldig.

Kennelijk staat redeneren over alle meest plausibele situaties meer logische gevolgtrekkingen toe dan redeneren over de meeste situaties zonder meer. Een verifikatie van de gegeven geldigheids-antwoorden is overigens niet moeilijk, en scherpt het logisch begrip.

Waarschijnlijkheid in informatica en AI

Maar eigenlijk hebben we met het laatste voorbeeld ook een overstap gemaakt naar een ander wetenschapsgebied. Er bestaat een grote interesse voor redeneren met conditionele beweringen en plausibiliteit in gebieden als de Kunstmatige Intelligentie, waar men om efficiëntie-redenen graag redeneert met kwalitatieve waarschijnlijkheid, zonder ingewikkelde numerieke berekeningen van $P(A)$'s en $P(A|B)$'s te hoeven maken.

Overigens heeft dat trekken van plausibele conclusies wel zijn prijs. Te optimistische conclusies op grond van redeneren met onzekerheid blijken soms onterecht, en moeten dan worden herzien. Een bekend voorbeeld uit de AI-literatuur is het volgende. Neem de volgende twee gegevens aan:

Vogels vliegen (doorgaans). Tweetie is een vogel.

Het ligt voor de hand om dan te concluderen dat 'Tweetie kan vliegen'. Maar nu hoort u vervolgens dat

Tweetie is een pinguin.

Dan ligt het voor de hand de zojuist bereikte conclusie weer in te trekken, omdat pinguins doorgaans juist níet vliegen. Maar als u nu weer hoort dat pinguin Tweetie al jaren woont in een beroemd aeronautisch laboratorium, dan kan ze misschien toch vliegen, en zo kan de conclusie blijven 'flip-floppen'.

Men spreekt hier wel van 'niet-monotone logica'. Gevolgtrekkingen staan niet eens en voor goed vast, maar kunnen opkomen en weer worden ingetrokken naarmate onze informatie toeneemt. Hierbij spelen weer twee kwesties door elkaar: redeneren en modelleren. We moeten eerst besluiten hoe we nieuwe gegevens, conditioneel of niet, weergeven, en welke rol we open laten voor uitzonderingen. Pas na deze modelkeuze kunnen we overgaan tot toepassen van bewijsregels, in wat voor soort logica dan ook. Niet-monotone logica is een intrigerend gebied. Zo bevat het naast logische gevolgtrekkingen ook procedures voor geloofsherziening. Kennelijk passen wij onze meningen over de werkelijkheid aan naarmate meer informatie beschikbaar komt, waarbij we soms weer afstappen

van eerdere meningen. De subtiele mechanismen van meningsverandering die hierbij spelen worden langzamerhand zelf tot onderwerp van logische en wiskundige theorievorming. Dit onderwerp zal nog aan bod komen in het laatste deel van dit boek over logische 'grondslagen'.

De psychologische realiteit

Maar hoe gedragen mensen zich nu echt in redeneren met onzekerheid of conditionele waarschijnlijkheid? We hebben al een voorbeeld gezien in de Wason kaart-test van aan het eind van Hoofdstuk 3, die een ander gedrag laat zien dat propositielogica volgens het boekje. Analoog, wat is de empirische status van de elementaire waarschijnlijkheidsrekening? Een beroemd experiment dat zelfs basiswetten van dit soort in twijfel trekt werd bedacht door de psychologen Tversky en Kahneman 1982.[5] Proefpersonen kregen de volgende tekst voorgelegd:

> Bill is thirty four years old. He is intelligent, but unimaginative, compulsive and generally lifeless. He likes jazz. In school, he was strong in mathematics, but weak in social studies and humanities.

Daarna moesten zij de volgende beweringen ordenen naar waarschijnlijkheid:

A Bill is a physician playing poker for a hobby.

B Bill is an accountant.

C Bill plays jazz for a hobby.

D Bill surfs for a hobby.

E Bill is an accountant playing jazz for a hobby.

Hier is de opmerkelijke uitslag die werd geconstateerd. Mensen zetten B boven C, maar vervolgens E er *tussenin*! Deze uitkomst is in strijd met de kansrekening, omdat de conjunctie van accountant en jazz altijd minder waarschijnlijk is dan jazz alleen.

Zijn mensen dus gewoon dom, en redeneren ze 'fout'? Dat is nog maar de vraag. Er zijn vele interessante verklaringen voor deze afwijkingen van de wiskundige waarschijnlijkheidstheorie, zoals de rol van 'associatie' van begrippen, of het oproepen van 'proto-types' door de plaatsing van de beweringen in een gegeven tekst. Recent onderzoek aan de Universiteit van Amsterdam, gebaseerd op uit de AI bekende technieken voor niet-monotoon redeneren en geloofsherziening, heeft onlangs resultaten opgeleverd waarbij het geobserveerde gedrag van de proefpersonen eigenlijk toch als 'heel logisch' op te vatten was! Wiskundige analyse is dus bepaald niet in strijd met alledaags cognitief gedrag, maar helpt juist om het beter in het vizier te krijgen. Bovendien begint de laatste tijd het idee terrein te winnen dat deze nieuwere wiskundige theorieën uit de logica en informatica een correlaat kunnen hebben in neurale netwerken, en daarmee op onbewust hersenniveau.

Met dat laatste dwarsverband zijn we overigens wel op een ander onderdeel van de wiskunde aanbeland, en wel de zogenaamde 'dynamische systemen'. Dit onderwerp zal nog nader aan bod komen in hoofdstuk 5.

[5] De tweede auteur ontving onlangs een Nobelprijs voor zijn cognitiewetenschappelijk oeuvre.

Hoofdstuk 4

Spelen

4.1 Spelen: zetten en strategieën

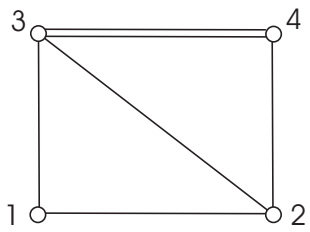
Spelen zijn een typisch menselijke activiteit, lopend vanaf kaartspelen of voetbal tot spelpatronen in algemeen economisch en sociaal gedrag. Wiskundigen zijn reeds diverse malen in de geschiedenis door spelen genspireerd tot het opstellen van belangrijke theorien. Zo komt het begrip waarschijnlijkheid uit de zestiende-eeuwse studie van kansspelen en weddenschappen. In de 20ste eeuw ontstond de 'speltheorie' als algemene analyse van rationeel gedrag van personen in interactie.

Winnende strategieën

Het Blokkadespel Gegeven is een netwerk met plaatsen (aangegeven door punten) en paden (verbindingen tussen punten), met een of andere startplaats. Er zijn twee spelers. 'Loper' is eerst aan zet, en moet proberen alle plaatsen in het netwerk te bezoeken langs openstaande wegen, waarbij hij telkens een pad kiest vanuit zijn laatste plaats. 'Remmer' mag na elke stap van Loper een willekeurig pad verwijderen uit het netwerk. En zo verder, om en om. Het spel stopt als een speler geen zet meer kan doen. In dat geval heeft Loper gewonnen als elke plaats is bezocht, anders wint Remmer.

U kunt zich voorstellen dat Loper de gemiddelde NS-gebruiker is, die probeert van reis langs verschillende stations te maken, en dat Remmer de NS-bedrijfsvoering voorstelt, die probeert zo efficiënt mogelijk verbindingen buiten werking te stellen.

Laten we eens zo'n spel bekijken:



Hier is een mogelijk spelverloop:

Loper loopt van	*Remmer verwijdert een lijn van*
1 – 3	3 – 2
3 – 4	4 – 2
4 – 3	1 – 2

enzovoorts. Het is duidelijk dat Loper verliest, want 2 is onbereikbaar. Maar bekijk nu eens het volgende verloop:

Loper loopt van	*Remmer verwijdert een lijn van*
1 – 2	2 – 3
2 – 4	4 – 3
4 – 3	

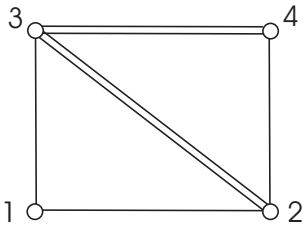
In dit geval heeft Loper gewonnen! In de meeste spelen kunnen beide spelers winnen of verliezen, afhankelijk van hoe ze spelen. Maar dit is niet alles. Want in dit spel is alles welbeschouwd essentieel in het voordeel van Remmer. We beweren dan ook

Remmer kan altijd winnen, hoe Loper ook speelt!

Immers, als Loper naar 3 gaat, dan heeft Remmer genoeg tijd om in drie beurten punt 2 te 'isoleren'. Maar als Loper eerst naar punt 2 gaat, dan werkt het volgende. Laat Remmer in zijn eerste twee

beurten de verbindingen tussen 3 en 4 weghalen. Dit dwingt Loper terug te keren op weg naar 3 of 4, en Remmer heeft dan tijd om één van deze twee plaatsen te isoleren. Een dergelijke handelwijze, die op elk mogelijk gedrag van de tegenpartij een passend antwoord geeft, heet een *strategie*. Een strategie die garandeert dat een speler altijd wint (hoe de ander ook speelt) heet een *winstrategie*.

Om dit begrip nader te begrijpen kunt u nagaan welke speler een winnende strategie heeft in het volgende spel:

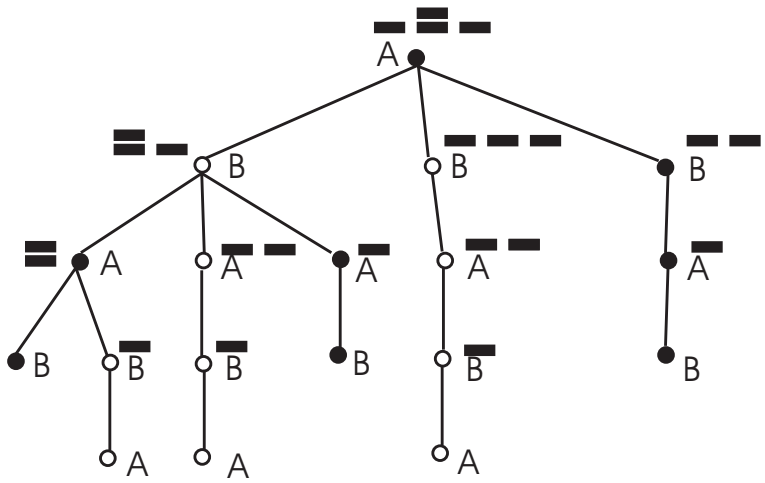


Het antwoord is nu juist: Loper! Schets van de redenering. Loper moet eerst naar 2 gaan. Aldaar afkappen van een 2–3 of 2–4 helpt Remmer niet: Loper kan toch naar 3 en 4 komen. Weghalen van de twee 3–4 paden boven, zoals eerder, helpt dit keer echter ook niet — want dit laat Loper net genoeg tijd om eerst naar 4 te gaan en dan via 2 ook nog naar 3 te komen.

Is dit iets algemeens? Volgens een stelling van de wiskundige Zermelo is elk eindig spel van het zogenaamde type ‘nul-som’ — en elke versie van Blokkade is zo’n spelsoort — is er één speler met een winnende strategie. Een *nulsom*-spel is een spel waarvoor elke eindtoestand geen twee verliezers of twee winnaars zijn. Er is één winnaar en één verliezer.

Deze verrassend sterke stelling valt redelijk eenvoudig te bewijzen met een volledige inductie naar het aantal tussentoestanden van het spel. In T.18 is het volledig uitgewerkt. Om het bewijs intuïtief snel te begrijpen kunnen we het gemakkelijkst illustreren aan de hand waarvan we de toestanden makkelijk in een zogenaamde *spelboom* kunnen intekenen: het Nim-spel.

Het Nim-spel Het spel begint met een aantal stapeltjes lucifers. De speler die de beurt heeft kiest één van de stapeltjes uit, waarna er minstens één lucifer van dat stapeltje moet worden weggenomen. De laatste speler die een lucifer wegneemt is de winnaar. De algemene manier om de winnende strategie te bepalen is de volledige spelboom langs te gaan. Hier is bijvoorbeeld de spelboom van de beginsituatie 1–2–1.



In elke toestand is aangegeven wie aan de beurt is, en dus wordt in elke eindtoestand de beurtspeler ook de verliezer. De eindtoestanden die voor A gewonnen zijn kleuren we zwart en die voor B kleuren we

Spelen en strategieën

Een spel *of* spelboom G *is een eindige procesgraaf in de volgende specifieke vorm* $\langle S, T, t_0, Z, B, W\rangle$*, met*

S*: de verzameling* spelers.

T*: een verzameling van* spel-toestanden.

t_0*: de* begintoestand *met* $t_0 \in T$.

Z*: is de verzameling van* zetten. *Een zet* z *is een partiële functie van* T *naar* T. *Dat wil zeggen dat voor elke* $t \in T$ *elke* $z \in Z$ *ofwel* z *niet toepasbaar is of er is een uniek bepaalde opvolger* $z(t) \in T$ *van* t*: de nieuwe toestand die ontstaat na het zetten van* z *in toestand* t.

B*: dit is de* beurtfunctie. *Het bepaalt wie aan de beurt is in een gegeven toestand:* $B : T \to S$.

W*: deze bepaalt voor elke toestand waarvoor geen* $z \in Z$ *toepasbaar is — dit zijn de* eindtoestanden *— wie de winnaar is.*

Een spel is eindig als er geen cyclus van zetten is te geven waardoor we weer in een oude toestand terechtkomen:

Voor geen enkele $t \in T$ *is er een rijtje* $z_1, ..., z_n$ *van zetten zodanig dat* $z_n(z_{n-1}(..z_1(t)...)) = t$.

Een spel is nulsom *als* W *voor elke eindtoestand een unieke winnaar aanwijst.*
Een strategie σ *voor speler* s *in een eindig nulsom-spel* G *is een functie die voor elke toestand waar* s *aan de beurt is een in die toestand uitvoerbare zet voorschrijft. De opbrengst van een strategie is de verzameling van alle eindtoestanden die kunnen optreden als* s *speelt volgens* σ *tegen elk denkbaar tegenspel van de andere spelers. Een winstrategie voor* s *is een strategie voor* s *waarvan de opbrengst alleen maar bestaat uit gewonnen toestanden voor* s*. Een spel heet gedetermineerd als een van de spelers een winstrategie heeft.*

Stelling *Elk eindig nulsom-spel is gedetermineerd.*
Bewijs*: Laat* $G = \langle S, T, t_0, Z, B, W\rangle$ *een spel van het voorgeschreven type. Het bewijs loopt met inductie naar* $|T|$ *(zie ook T.21). Als geldt dat* $|T| = 1$ *dan* $|T| = t_0$*. Volgens de eis van eindigheid van het spel is* t_0 *tevens een eindtoestand.* $W(t_0)$ *is de winnaar (de strategie is "doe niks").*
Als $|T| = n + 1 > 1$ *beschouwen we alle vervolg-toestanden* T_1 *van* t_0*:*

$$T_1 = \{t \mid \exists z \in Z : z(t_0) = t\}$$

Voor elk zo'n vervolg-toestand t *is er weer een spel* G_t *te definiëren:*

$$G_t = \langle S, T - \{t_0\}, t, Z_t, B_t, W_t\rangle$$

waarbij Z_t*,* B_t *en* W_t *de eenvoudige beperkingen tot* $T - \{t_0\}$ *zijn van hun corresponderende versies in* G*. Er geldt natuurlijk* $|T - \{t_0\}| = n$ *en we kunnen dus de inductie-hypothese toepassen voor de spelen* G_t*. Voor elk zo'n spel moet er dus een speler* s_t *met win-strategie* σ_t *zijn. Er zijn nu twee mogelijkheden die tot een verschillende speler met winstrategie voor* G *leiden:*

1. $B(t_0) \neq s_t$ *voor alle vervolg-toestanden* $t \in T_1$*. De begin-speler heeft voor geen van de vervolgspelen* G_t *een winnende strategie. De speler met winnende strategie voor* G *is de tegenspeler van de beginspeler. Hij heeft voor alle* G_t *een winnende strategie* σ_t*. Zijn strategie is:*

   Laat de beginspeler $B(t_0)$ *zijn zet* z *doen en voer vervolgens strategie* $\sigma_{z(t_0)}$ *toe.*

2. $B(t_0) = s_t$ *voor zekere* $t \in T_1$*. Nu heeft de beginspeler een winnende strategie. Deze luidt:*

   Kies een zet $z \in Z$ *zodanig dat* $s_{z(t_0)} = B(t_0)$ *en pas daarna* $\sigma_{z(t_0)}$ *toe.*

In beide gevallen is er dus een speler met een winnende strategie. Q.E.D.

wit. Nu kunnen we ook de toestanden voor de eindtoestanden inkleuren als indicator van de speler die kan winnen: de speler met de winstrategie. Als er voor de beurtspeler in de voorlaatste toestand een winnende eindtoestand is dan heeft hij als winstrategie de specifieke zet die tot die eindtoestand leidt. We kleuren die toestand overeenkomstig. Mocht er voor hem geen enkele winnende eindtoestand zijn dan kleuren we de gegeven voorlaatste toestand als wintoestand voor de tegenspeler. Met deze kleuring kunnen we nu deze voorlaatste toestand in feite opvatten als een eindtoestand: een winnaar en een verliezer (gegeven dat ze geen domme zetten doen). Zo kunnen we vervolgen en de gehele spelboom inkleuren door volgens hetzelfde procedé stap voor stap naar boven toe de toestanden in te kleuren. De kleur van de begintoestand geeft dan de speler aan die een winnende strategie heeft. De strategie voor de winnende speler, na kleuring van de spelboom, is te kiezen voor een vervolg-toestand met zijn eigen kleur als hij aan de beurt is. Het Zermelo-bewijs geeft construeert dus ook nog een keer de winstrategie.

Net als in ons eerdere inductievoorbeeld in T.21 in 6.1 op pagina 170 heeft de stelling van Zermelo, en ook zijn kleurings-algoritme, maar weinig praktische betekenis. Het probleem is natuurlijk de omvang van de spelboom, en het terugrekenen vanuit de eindtoestanden is doorgaans ondoenlijk.

Zermelo was zelf voornamelijk geïnteresseerd in spelen als schaken waarbij ook remise mogelijk is. In deze spelen garandeert zijn stelling dan één van beide spelers een strategie heeft om niet te verliezen. Het verschil tussen theorie en praktijk voor het schaakspel is immens. Een eeuw na het oorspronkelijke resultaat is nog steedss niet bekend welke speler deze niet-verliezende strategie heeft. Er zijn ruwweg twintig mogelijkheden per zet, en het totaal aantal mogelijk toegestane posities van de schaakstukken op het schaakbord is ongeveer 10^{120}. Zoals we eerder in 3.1 vermeldden komt dit getal ongeveer overeen met het aantal elementaire deeltjes in het zichtbare heelal!

In het geval van het Nim-spel is evenwel een elegante short-cut te geven om te bepalen wie er zal winnen. Laat $n_1, n_2, \ldots$ de aantallen lucifers zijn in stapeltjes. Het idee is nu deze getallen binair te schrijven en wel onder elkaar. Hier is een voorbeeld. Stel we beginnen met drie stapels met $n_1 = 5$, $n_2 = 9$ en $n_3 = 4$ lucifers. Of, in binaire notatie $n_1 = 101$, $n_2 = 1001$ en $n_3 = 100$. We tellen nu het totaal aantal enen op de n-de plaats van deze getallen. In het voorbeeld geeft dit

n_1		1	0	1
n_2	1	0	0	1
n_3		1	0	0
	1	2	0	2

1, 2, 0 en 2 enen. Een spel heet *gebalanceerd* als voor iedere positie in de binaire notatie het totaal aantal enen even is. Anders noemen we het spel ongebalanceerd. In het gegeven geval is het spel ongebalanceerd omdat er maar één 1 staat op de vierde plaats. Nu zijn er de volgende twee belangrijke feiten:

(1) Een gebalanceerd spel zal na iedere toegestane zet veranderen in een ongebalanceerd spel. Immers het aantal lucifers in één stapel zal gewijzigd worden, zodat in één rij sommigen enen in nullen veranderen en vice versa. Als in iedere kolom het aantal enen even was zal dat na de zet niet langer het geval kunnen zijn.

(2) Een speler die aan zet is in een gebalanceerd spel zal nooit met die zet kunnen winnen, omdat er voor een gebalanceerd spel altijd minstens twee stapels moeten zijn.

De winnende strategie is dus om van een ongebalanceerd spel altijd een gebalanceerd spel te maken. Daarna kan de tegenstander het spel niet uitmaken.

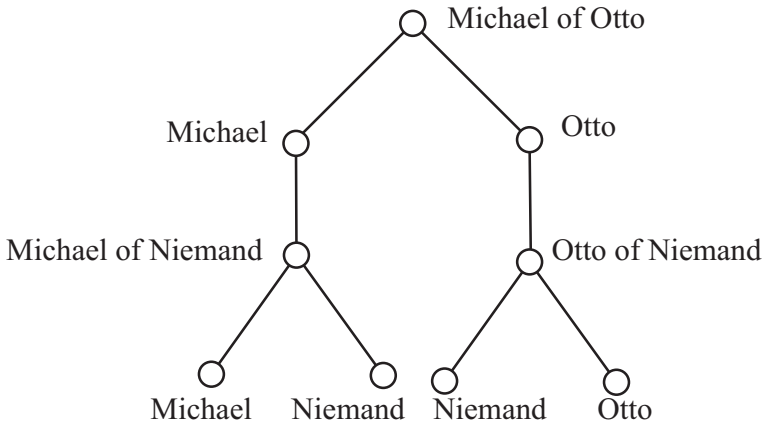
Spelen met voorkeuren

In toepassingen van speltheorie op echte situaties, volstaan deze 'kale' spelen niet langer. Mensen hebben in het algemeen veel ingewikkelder voorkeuren tussen uitkomsten dan 'winnen' versus 'verliezen'.

Voorbeeld: verkiezingen Marie, Natasha en Ofelia hebben een vrijkaartje over voor het Toonloos Ensemble. Ze kunnen stemmen over een keuze tussen Michael, Niemand en Otto om mee te nemen. Hun voorkeuren liggen als volgt:

	Marie	Natasha	Ofelia
1	Michael	Niemand	Otto
2	Niemand	Michael	Michael
3	Otto	Otto	Niemand

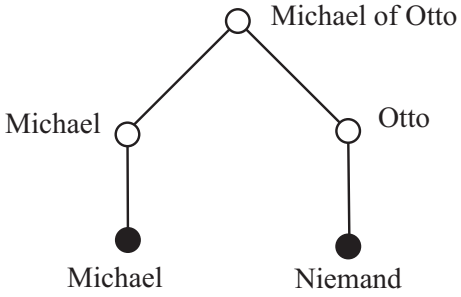
Eerst wordt gestemd over 'Michael of Otto', daarna over de resterende mogelijkheid hieruit of Niemand. Hoe moeten de dames stemmen? De volgende boom geeft de mogelijkheden weer.



Als iedereen stemt volgens zijn voorkeur, dan wint Michael in de eerste ronde, en vervolgens wint Michael ook tegen Niemand. Maar als Natasha dit voorziet, dan kan ze beter haar stemgedrag in de eerste ronde veranderen — en tegen haar eigen voorkeur in stemmen! Immers, als ze in die ronde stemt voor Otto boven Michael, dan wordt in die ronde Otto gekozen, waarna bij meerderheidsstemming daarna Niemand wint, hetgeen haar eerste voorkeur was. Maar de andere spelers kunnen deze redenering zelf weer van te voren bedenken, en kunnen dus ook hun stemgedrag daarop aanpassen. Is hier een beste oplossing te vinden?

Als we denken op dezelfde manier als in ons bewijs van Zermelo's Stelling, dan beginnen we achterin de spelboom, en redeneren terug. (Dit proces heet 'backwards induction'.) In het laatste stadium weet elke speler wat er is gebeurd, en resteert slechts één eindkeuze. Afwijken van de eigen voorkeur heeft dan geen zin, dus bijv. bij een keuze tussen Niemand en Otto komt Niemand uit de bus, en bij Niemand versus Michael juist Michael. Maar dan kunnen spelers in het stadium daarvoor

van dit gedrag uitgaan:



In dat geval stemmen verstandige spelers aan het begin als volgt:

Marie	Michael
Natasha	Otto
Ofelia	Michael

en Michael mag mee naar het concert.

Strategisch evenwicht

We bekijken een spel met twee personen. Voor ieder paar van strategieën (σ, τ) van de twee spelers zal er een unieke uitkomst zijn die verkregen wordt door de twee strategieën tegen elkaar te laten spelen. Deze uitkomst kan door beide spelers geëvalueerd worden.

Een tweetal strategieën, voor beide spelers één, is in *Nash-evenwicht* als geen van beide spelers de uitkomst kan verbeteren, aangenomen dat de andere speler niet van strategie verandert. Het sluit daarmee niet uit dat de uitkomst verbetert als *beide* spelers tegelijk van strategie veranderen.

Idealiter correspondeert zo'n evenwicht met stabiel gedrag voor rationele spelers. Met meer spelers is de definitie van strategisch evenwicht in wezen hetzelfde. In het bovenstaande verkiezingsspel gaat men eenvoudig na dat het zojuist gegeven stemgedrag voor de drie spelers een Nash-evenwicht vormt.

Spelen met onvolmaakte informatie Het verkiezing-voorbeeld was ander soort spel dan het eerdere Blokkade, of het schaakspel. Spelers moesten namelijk in elke ronde tegelijk zetten, zonder te weten wat de anderen doen in dezelfde beurt. Veel voorbeelden in de speltheorie zijn van deze aard, met name zogenaamde 'strategische spelen'.

Strategische spelen worden vaak gegeven door een matrix van uitkomsten, waarbij de rijen de strategie van de eerste speler geven en de kolommen de strategie van de tweede speler. Een paar getallen (i, j) in de matrix geeft de uitkomsten die de rijspeler en kolomspeler (in die volgorde) aan de relevante uitkomst toekennen. Hier zijn een aantal beroemde 2×2 voorbeelden: twee spelers en dus ook twee strategieën.

Prisoners' Dilemma Een onvervalste evergreen. In de klassieke opzet betreft het twee arrestanten. Er is niet genoeg bewijsmateriaal voor een zware veroordeling. Als beiden blijven zwijgen krijgen ze maar één jaar gevangenisstraf. Als echter (precies) één van beide bekent, dan gaat deze vrijuit en de andere gaat voor tien jaar de gevangenis is. Als beiden bekennen krijgen ze vijf jaar straf. Hier is de matrix die het probleem weergeeft

	zwijg	beken
zwijg	$(-1,-1)$	$(-10,0)$
beken	$(0,-10)$	$(-5,-5)$

In dit geval is er een duidelijk Nashevenwicht, namelijk (beken,beken). Namelijk ongeacht wat verdachte 2 doet, is het voor verdachte 1 gunstiger te bekennen. We spreken in dit geval van een *dominante strategie*. Het zelfde geldt voor verdachte 2 en het zal er dus op uitdraaien dat ze vijf jaar gevangenisstraf oplopen. De twee spelers worden dus niet geleid tot coöperatief gedrag, terwijl dat ze tot collectief zwijgen had kunnen aanzetten wat maar één jaar gevangenisstraf voor beide verdachten had betekend.

Dit voorbeeld kan in verschillende andere vormen geformuleerd worden. Een typisch voorbeeld daarvan is niet coöperatief gedrag tussen concurrerende bedrijven. Stel Coca Cola en Pepsi hebben een afspraak gemaakt om frisdrank tegen een hoge prijs te verkopen. De winst is dan (in een bepaalde eenheid) zes voor iedere fabrikant. Maar ieder van beide heeft de mogelijkheid deze afspraak te schenden en tegen een lagere prijs te verkopen. In dat geval zal degene met de lage prijs acht eenheden verdienen, tegen twee voor de fabrikant van het hooggeprijste product. Als beide partijen de afspraak schenden blijft slechts een winst van drie over. In een tabel

	hoog	laag
hoog	$(6,6)$	$(2,8)$
laag	$(8,2)$	$(3,3)$

Ook hier is de niet-coöperatieve versie (laag,laag) de evenwichtssituatie. Rationaal gedrag voorspelt dus dat beide partijen de afspraak zullen schenden. Kartelvorming had hier voor een veel beter resultaat voor beide partijen gezorgd.

In een derde variant bekijken we de samenwerking tussen twee wetenschappers 'Johan' en 'Robbert' die een lezing moeten voorbereiden. Er zijn twee mogelijkheden: hard werken en alles op tijd afmaken, of lui zijn en zien waar het schip strandt. Als beiden hard werken is de winst $(6,6)$. Als beiden lui zijn is het resultaat $(3,3)$. De grootste uitkomst is voor (bijvoorbeeld) Robbert het grootst (8) als hij niets doet en Johan zijn lezing laat uitschrijven (voor een magere beloning van 2), en vice versa. Dit geeft exact de bovenstaande tabel. Het Nashevenwicht voorspelt dus dat we beiden het werk zouden laten zitten en geen lezing geven!

Een andere bekende vorm van het Prisoners' Dilemma is de wapenwedloop, met als strategieën 'ontwapen' en 'bewapen'. Bijvoorbeeld in onderstaande vorm

	ontwapenen	bewapenen
ontwapenen	$(3,3)$	$(0,4)$
bewapenen	$(4,0)$	$(1,1)$

Hier worden de partijen naar het Nash-evenwicht 'bewapenen' gedreven, ook al is het in ieders belang te ontwapenen.

In al deze gevallen is communicatie een duidelijke manier om tot coöperatief gedrag te komen. Als de twee arrestanten informatie kunnen uitwisselen en elkaar genoeg vertrouwen kunnen ze afspreken

beiden te zwijgen. In het geval van kartelvorming zijn dit soort (geheime) prijsafspraken verboden en aan inspectie onderhevig.

Battle of the Sexes Een ander klassiek voorbeeld is die waarin man en vrouw moeten beslissen tussen een avondje voetbal of opera. De uitkomstentabel is

	voetbal	opera
voetbal	$(2,1)$	$(0,0)$
opera	$(0,0)$	$(1,2)$

In dit geval zijn er twee evenwichten: (voetbal,voetbal) en (opera,opera). Dit laat zien dat hier de beste strategie voor alle betrokken partijen is om het eens te zijn over de uitkomst.

We kunnen het voorbeeld van de wapenwedloop enigszins aanpassen om ook dit tweede evenwicht mogelijk te maken. Als we de uitkomsten als volgt vervangen

	ontwapenen	bewapenen
ontwapenen	$(3,3)$	$(0,2)$
bewapenen	$(2,0)$	$(1,1)$

is het voordeel van bewapenen terwijl de andere partij een ontwapenstrategie volgt niet langer dominant. Daarom ontstaat er nu een tweede evenwicht waar beide partijen het eens zijn over ontwapenen.

Gemende strategieën

Matching Pennies In dit voorbeeld kiezen beide partijen een (euro)cent te laten zien met kop of munt boven. De eerste speler 'Even' wint als er twee koppen of twee munten zijn. De tweede speler 'Oneven' wint als er een kop en een munt te zien is. Dit is een nulsomspel: de winst van de ene speler is het verlies van de andere. De uitkomstenmatrix is

	kop	munt
kop	$(1,-1)$	$(-1,1)$
munt	$(-1,1)$	$(1,-1)$

In dit geval zijn er geen Nash-evenwichten. Stel dat Even voor kop kiest, dan is het onmiddellijk duidelijk dat Oneven voor munt moet kiezen. Maar gegeven deze strategie voor Oneven, zal Even de strategie moet wijzigen in munt, etcetera, etcetera.

De oplossing is dat we ons begrip van strategie moeten wijzigen tot een probabilistisch begrip. We moeten toestaan dat bepaalde strategieën met een bepaalde waarschijnlijkheid worden gespeeld. Dit idee van het introduceren van een toevalsfactor is natuurlijk wel bekend, denk bijvoorbeeld aan poker waar het zeer nuttig is zo nu en dan te bluffen.

Wat is de juiste strategie in dit spel? Stel dat Even speelt met kans p op kop en kans $1-p$ op munt. Voor een evenwichtsituatie mag de verwachte uitkomst niet afhangen van de strategie van Oneven. Daarmee vinden we dat

$$1 \cdot p + (-1) \cdot (1-p) = (-1) \cdot p + 1 \cdot (1-p)$$

zodat $p = 0,5$. Het Nashevenwicht krijgen we nu als beide spelers met deze strategie van 50% kans op kop en 50% kans op munt gaan spelen. Deze 'gemengde strategie' garandeert voor beiden de optimale verwachte uitkomst van 0. Natuurlijk wordt zo'n kansproces betekenisvoller als de spelers het spel meerdere keren kunnen spelen. Dit zal aan de orde komen in het college *Voorspelbaarheid*.

Uiteindelijk leidt deze kijk tot een van de parels van de speltheorie, de stelling van Nash, die direct voortbouwt op de befaamde Minimax Stelling van von Neumann

> NASH. *Alle strategische spelen met een eindig aantal spelers hebben minsten één evenwichtsoplossing, als we gemengde strategieën toestaan.*

Hert en Haas Er kunnen ook pure en probabilistische evenwichtsituaties naast elkaar bestaan. Bekijk bijvoorbeeld het volgende spel, ontleent aan een verhaal van de Franse filosoof Jean Jacques Rousseau. Een tweetal jagers staat klaar om een hert te vangen. Plotseling doet zich voor ieder van de jagers de kans voor een haas te vangen. Als een jager dit doet ontsnapt het hert en blijft de andere jager met lege handen. De uitkomsten zijn

	hert	haas
hert	$(2,2)$	$(0,1)$
haas	$(1,0)$	$(1,1)$

In dit geval zijn er weer twee pure Nash-evenwichten: (hert,hert) en (haas,haas), met een uitkomst van respectievelijk 2 en 1 voor beide jagers. Maar er is ook een probabilistische strategie, waar iedere jager met kans p voor het hert gaat. (Bereken de waarde van p.)

Het ultimatumspel

Er zijn ook grenzen aan de toepassingen van de speltheorie. In het bijzonder is het niet duidelijk dat mensen in alle omstandigheden zich uitsluitend door rationele overwegingen laten leiden. Een goed voorbeeld is het *ultimatumspel* dat recent veel in de belangstelling heeft gestaan.

In dit spel met twee spelers wordt een aanzienlijke som, zeg 100.000 euro aan speler 1 gegeven. Speler 1 mag dit bedrag over de twee spelers verdelen. Vervolgens mag speler 2 besluiten of beide spelers de toegekende bedragen mogen houden of niet. Dat wil zeggen, als speler 2 akkoord is krijgt hij het percentage dat speler 1 hem heeft toegedacht en mag speler 1 de rest houden. Als speler 2 niet akkoord is krijgen beide spelers helemaal niets. Het spel wordt slechts één keer gespeeld en de spelers zijn onbekenden en zullen elkaar ook niet opnieuw ontmoeten.

De rationele keuzetheorie zegt dat speler 2 altijd moet accepteren zolang hij maar iets krijgt toegewezen, ongeacht hoe klein het bedrag is. Zelfs als speler 1 maar één euro 'fooi' geeft en zelf de resterende 99.999 houdt kan speler 2 toch een winst van één boeken. Het alternatief is namelijk helemaal niets. Toch zal in de praktijk speler 2 geneigd zijn nee te zeggen als het toegewezen bedrag laag is. Een percentage van minstens 30% wordt als redelijk ervaren.

Eén van de mogelijke verklaringen is dat wij mensen toch zo geprogrammeerd zijn dat we rekening houden met het lange termijn effect van de beslissing. het zou wel eens zo kunnen zijn dat onze reputatie een deuk oploopt als we een belachelijk lage fooi accepteren. We zouden de naam krijgen 'goedkoop' te zijn, en dat zou ons later duur komen te staan.

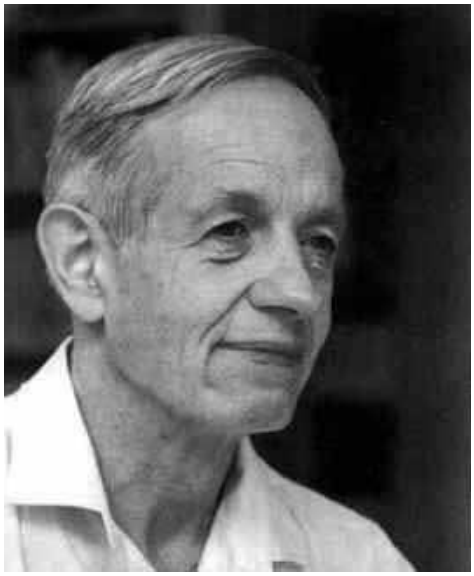
P 9.

JOHN VON NEUMANN

1903 — 1957

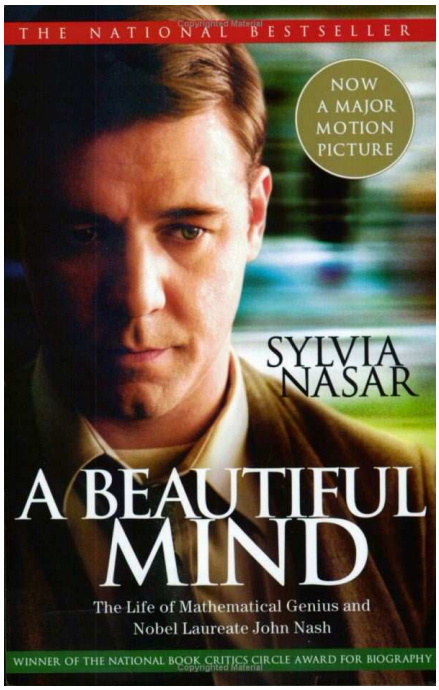
John von Neumann *was een wonderkind die op zesjarige leeftijd al met zijn vader in Oudgrieks grapjes maakte en na een minuut een bladzijde uit het telefoonboek uit z'n hoofd wist. Zijn eerste wiskundige artikel schreef hij toen hij 19 was. In 1928 leidde hij de beroemde minimaxstelling af. Er is gezegd dat hij als puur wiskundige genoeg gedaan heeft voor drie belangrijke carrières. Zijn eerste werk was trouwens voornamelijk in de logica en verzamelingenleer. Daarna wijdde hij zich aan de kwantummechanica en operatoralgebra. Hij schreef het standaardwerk Mathematische Grundlagen der Quantenmechanik in 1932. In 1944 verscheen het standaardwerk over de speltheorie en economie Theory of Games and Economic Behavior met co-auteur Morgenstern. Von Neumann heeft ook aan de wieg gestaan van de waterstofbom en de eerste computer.*

P 10.



JOHN NASH

1928 —



John Nash *was een ander wonderkind. Hij promoveerde op 22-jarige leeftijd op een proefschrift in de speltheorie waar hij het begrip Nash-evenwicht introduceerde en liet zien dat zo'n evenwicht altijd bestaat. Daartoe gebruikte hij trouwens de dekpuntstelling van Brouwer (in een gegeneraliseerde vorm van Kakutani) die we op het college Bewijzen al gezien hebben. Na dit werk is hij actief geworden in de topologie en differentiaalmeetkunde. Hij bewees een van de diepste resultaten en liep maar net de Fieldsmedaille mis. Hij is ook bekend geworden doordat hij midden jaren vijftig in een ernstige psychose terecht kwam, waar hij op wonderbaarlijke wijze begin jaren 90 weer uit 'ontwaakte'. Dit alles is in een prachtig boek (A Beautiful Mind van Sylvia Nadar) beschreven, en is ook te zien in een sterk afgewaterde versie als Hollywood blockbuster met Russel Crowe in de hoofdrol (in 2001 de oscar voor beste film). Uiteindelijk was zijn speltheoretisch werk goed voor de 1994 Nobelprijs in de economie.*

4.2 Spelen, informatie en communicatie

De wiskundige speltheorie beschrijft strategieën en evenwichten voor spelers in een breed scala van interactieve situaties. Nu is een strategie een globaal gedragspatroon dat voor elke spelbeurt vertelt wat een speler moet doen. Maar in feite lopen wij stapsgewijs door een spel heen. Daarbij delibereren we over de beste zet om te doen in een gegeven situatie, die ons slechts een deel heeft onthuld van de spelwijze van de tegenstander. Naast de globale theorie van evenwicht is er dus ruimte voor een lokale analyse van stapsgewijs redeneren door spelers op grond van hun kennis tot nu toe. Deze fijnstructuur is weer het terrein van de logica!

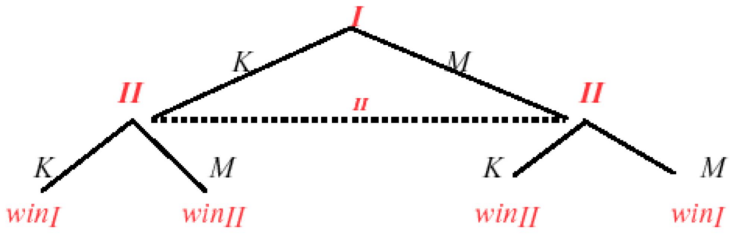
Spelen zijn dus kennelijk een werkterrein voor meer dan één discipline, en hun belang gaat ver uit boven het winnen van een potje, of het de loef afsteken van een concurrent. Spelen zijn een soort miniatuur van rationeel handelen, met een klein repertoire aan welomschreven zetten en een hoeveelheid informatie die binnen hanteerbare perken blijft. In het gedrag van schaakspelers, kaarters in de kantine, concurrerende firma's, of zelfs oorlogvoerende partijen zien we belangrijke cognitieve verschijnselen in klein bestek in actie. Spel gaat om logisch redeneren in een situatie met onzekerheid, doelbewust handelen om de wereld in een gewenste richting te beïnvloeden, en sociale interactie met anderen die tegelijkertijd hun eigen doelen nastreven, niet noodzakelijk de onze. Het is dan ook niet toevallig dat spelen in de geschiedenis telkens weer de aandacht hebben getrokken van wiskundigen, en dan aanleiding gaven tot nieuwe begrippen. We zagen dit al met het begrip waarschijnlijkheid en kansspelen, maar evenzo met strategisch evenwicht in de moderne speltheorie. En deze bron van inspiratie is ook de laatste jaren nog steeds springlevend. Speltheoretici uit de economie en wiskundigen treffen elkaar in de studie van spelen, maar evenzo taalkundigen of informatici die zich interesseren voor taalspelen, of transacties tussen commerciële partijen op het internet.

In dit hoofdstuk bespreken we van deze contacten één belangrijk logisch aspect: redeneren met kennis, en de dynamische overdracht van informatie tijdens een spel, en meer in het algemeen, tijdens communicatie.

Onvolmaakte informatie

In het Blokkadespel uit 4.1 beschikken de spelers over *volmaakte informatie*. Dat wil zeggen, op ieder moment van het spel weten spelers hun positie in de spelboom. Dit zien we ook bij dammen of schaken, maar evenzeer in een activiteit als argumentatie, wanneer we dat opvatten als een spel. In een vergadering weet men precies wat er gezegd is, wat er aan de orde is, en hoe de procedure verder loopt. Maar veel andere spelen hebben *onvolmaakte informatie*. Bijvoorbeeld, als spelers onafhankelijk van elkaar tegelijk hun zet moeten doen, zoals in het Prisoner's Dilemma, dan weten ze niet wat de ander in deze zelfde ronde doet. Ook een kaartspel als bridge heeft typisch onvolmaakte informatie, omdat u de hand van uw tegenspelers niet volledig kent. Gezelschapsspelen worden juist vaak ontworpen met een balans van kennis en onwetendheid om het spel interessant te maken, maar net niet te moeilijk om bij te houden. Een voorbeeld is het populaire spel Cluedo, dat sinds zijn ontstaan in de VS in de tweede wereldoorlog de wereld heeft veroverd.

Onvolmaakte informatie verandert de wiskundige eigenschappen van spelen drastisch. Hier is een eenvoudig voorbeeld, en wel een variant op het bekende spelletje Kruis of Munt. Speler 1 kiest eerst K of M, maar deze zet blijft geheim. (Zeg, de zet wordt afgegeven in een envelop.) Daarna kiest speler 2 een zet. Diens onzekerheid over 1's keuze geven we nu weer met een stippellijn in de spelboom:



Dit spel valt niet langer onder Zermelo's Stelling. Speler 1 heeft in principe vier mogelijke strategieën (twee keuzen per beurt), die we kunnen noteren als

(K,K), (K,M), (M,K) en (M,M).

De Zermelo winststrategie zou zijn "Kies het omgekeerde van wat 1 zojuist koos". Maar deze is nu onbruikbaar geworden, omdat 2 immers niet wéét wat I koos! De enige bruikbare strategieën zijn de twee vaste keuzen: "Kies K" of "Kies M", omdat deze niet vereisen dat speler 2 weet waar hij is in de spelboom. Bijgevolg is dit spel niet gedetermineerd, geen van beide spelers heeft een winnende strategie. Overigens is er wel een oplossing van dit spel in gemengde strategieën: elke speler moet dan met kans 1/2 K en M spelen. Maar in de analyse van wat te doen in een enkel spel helpt dat niet veel!

Dit ontbreken van gegarandeerd beste strategieën heeft ook een positieve kant. Spelen met onvolmaakte informatie vragen om meer dan alleen slim nadenken vooraf. Het gaat daarnaast ook om verdere manieren om de ontbrekende informatie alsnog te verwerven. De manier bij uitstek om dat te doen is het observeren van nieuwe feiten, of het bedrijven van communicatie, bijvoorbeeld door stellen van vragen en geven van antwoorden. Het mechanisme van vragen en antwoorden zal in de rest van dit hoofdstuk nog een aantal malen aan de orde komen. Maar misschien wilt u uw krachten eens beproeven op een iets ander scenario van informatieoverdracht dat later een rol zal spelen:

> We hebben beide een gesloten enveloppe gekregen. De een bevat een uitnodiging voor een wiskundecollege, de ander een kaartje voor een geavanceerde nachtclub op het Rembrandtsplein. Kennelijk weten we niet welk lot ons wacht. Nu open ik mijn enveloppe, en lees de inhoud zonder een spier te vertrekken. De uwe blijft dicht. Welke informatie is hier over tafel gegaan? Wie weet nu wat?

En daarmee zijn we aangekomen bij een heel algemeen cognitief verschijnsel. Wij zijn tamelijk vaardig in dit soort analyse, omdat ons hele leven berust op dit opnemen van informatie uit dagelijkse interacties. Dit hoofdstuk is gewijd aan enkele logische structuren in communicatie.

Informatie en communicatie

Een typisch voorbeeld van onvolmaakte informatie zijn kaartspelen, waar we de kaarten van de andere spelers onvolledig kennen. Hier zien we de zojuist beschreven dynamiek aan het werk: aanvankelijk weten we weinig over de kaarten in ieders hand, maar gaandeweg raken we beter geïnformeerd! Een gezelschapsspel als Cluedo heeft hiervoor een repertoire van toegestane vragen tussen spelers, waarvan de antwoorden uiteindelijk tot totale kennis leiden van wie de moord heeft begaan, met welk voorwerp, en op welke plek. Deze informatiestroom gedurende een spel valt concreet wiskundig te modelleren. Kaartspelen zijn om zo te zeggen een gratis, zonder overheidssubsidie, door de natuur al

voor ons gemaakt cognitief laboratorium om te zien hoe mensen met informatie omgaan en vervolgens strategisch handelen.

Om deze verschijnselen wiskundig te bestuderen is een modellering nodig van twee fundamentele aspecten van een proces van informatie-overdracht:

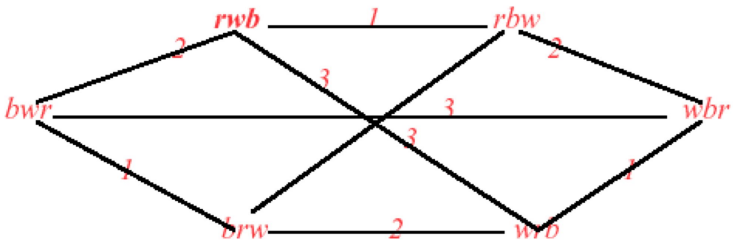
(a) informatietoestanden voor groepen personen

(b) updates die zulke toestanden veranderen

We introduceren nu zo'n model vanuit het volgende eenvoudige scenario.

Hoe de kaarten liggen: een logisch model

Drie kaarten rood, wit blauw worden verdeeld over spelers 1, 2, 3. Elke speler krijgt er één. Ieder kan zijn eigen kaart zien, maar niet die van de anderen. De echte verdeling is $\langle 1 : \text{rood}, 2 : \text{wit}, 3 : \text{blauw}\rangle$. Het volgende diagram is nu het informatiemodel:



De genummerde lijntjes representeren de individuele onzekerheden. Zij verbinden de toestanden die de desbetreffende speler niet kan onderscheiden. De echte verdeling rwb kent niemand. Nadenkend over wat anderen weten — over de kaarten, en over elkaar — moet elke speler rekening houden met alle zes mogelijke verdelingen.

Nu vraagt speler 2 aan speler 1: "Heb jij de blauwe kaart?"

Het antwoord, naar waarheid, luidt: "Nee"

Welke informatie wordt hier overgebracht? Iedereen leert door deze publieke mededeling dat 1 de blauwe kaart niet heeft. Maar verder verschillen de effecten per persoon. Het is erg nuttig om, alvorens deze tekst verder te lezen, zelf eens te beredeneren dat Speler 2 na het gegeven antwoord weet hoe de kaarten liggen.

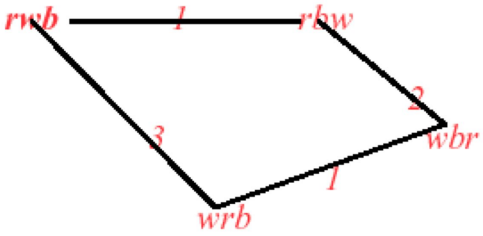
Speler 3 weet dat 2 erachter is gekomen.

Speler 1 weet alleen dat 2 of 3 het weet.

Speler 3 had bijvoorbeeld blauw, en wist dus dat het antwoord "Nee" zou zijn. Maar hij begrijpt dat dit voor 2 de kwestie beslecht, of die nu rood of wit heeft. Misschien bent u het niet met deze analyse eens, omdat u vindt dat 2's vraag zelf al informatie bevatte voor spelers 1 en 3, en wel dat 2 het antwoord niet weet. Daar valt zelf al iets uit op te maken over 2's kaart. Wij denken hier echter aan een mogelijk retorische vraag (het is immers een spel), maar lees door naar de volgende paragraaf!

Het kan toch lastig zijn hier goed in woorden uit te drukken wat er is gebeurd, en mensen maken soms fouten in het onder woorden brengen van wat ze weten. Maar plaatjes zeggen veel meer dan woorden! Onze communicatie-episode bewerkstelligt een update van het eerste informatiediagram:

1's antwoord elimineert alle toestanden met als eerste positie een 'b' :

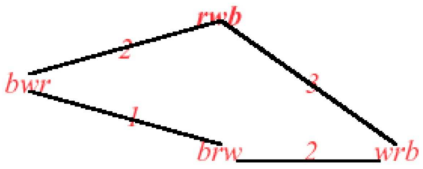


Dit diagram laat alle eerdere beweringen meteen aflezen. Bijvoorbeeld, vanuit rwb gezien heeft speler 2 geen onzekerheidslijntjes: hij kent dus de ware situatie. Maar speler 3 is wel onzeker tussen twee situaties (rwb en wrb). Wat hij wel kan zien is echter dat in elk daarvan 2 niet onzeker is (geen uitgaande 2-lijntjes), hetgeen betekent dat 3 wél weet dat 2 weet hoe het zit.

We kunnen nu ook verdere acties plannen, en hun effecten voorspellen. Zo kan alleen speler 2 de toestand der kaarten tot gemeenschappelijke kennis maken door zijn eigen kaart te noemen. Als hij dat doet wordt ondergaat het informatiemodel een update tot één punt: rwb. We kunnen dit lezen als een informatiemodel waar de feitelijke toestand rwb tot 'gemeenschappelijke kennis' is geworden van de hele groep, een begrip dat we nog zullen preciseren.

Variaties op conversatie

Dit model kan diverse genres van communicatie aan! In het vorige scenario hadden vragen op zich geen informatieve waarde. Maar stel nu dat 2's vraag onkundigheid van het antwoord impliceert. Dan produceert de vraag zelf al een update, en wel tot:



1's antwoord geeft dan een veel informatiever diagram, waarin 1 en 2 alles weten:

3 weet alleen dat zij beide alles weten, en zij weten weer dat 3 dat weet, enzovoorts. Het einddiagram is kleiner: dat wil zeggen dat in dit tweede scenario meer informatie over tafel is gegaan. 'Gewone' vragen helpen dus om communicatie te bespoedigen.

Groepskennis

In het voorgaande spraken we losjes over kennis of informatie van individuen in een groep, bijvoorbeeld over kaarten of over elkaars informatie. We gaan dit straks nader preciseren. Maar van belang

is ook dat communicatie een sociaal verschijnsel is, waarbij een groep als zodanig informatie kan hebben. Zo weet de spelersgroep in het bovenstaande impliciet al hoe de kaarten liggen, want de leden kunnen door hun informatie bij elkaar te leggen tot volledige kennis geraken van de feitelijke toestand. Als dat eenmaal gebeurd is ontstaat expliciete kennis. Maar bij nadere beschouwing speelt hier een interessant onderscheid, dat typerend is voor de sociale subtiliteiten van communicatie.

> *Scenario 1* Iedere collega weet van mijn misstap, maar ze weten niet van elkaar dat ze het weten. Deze algemene kennis is vervelend, maar ik kan er mee leven.
>
> *Scenario 2* Iedere collega weet het, maar ze weten ook van elkaar dat ze het weten, enzovoorts. Deze gemeenschappelijke kennis is een publieke schande van een veel ernstiger aard, met mogelijk heel andere praktische consequenties voor mij.

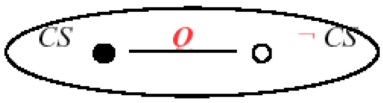
Het verschil is ook als volgt te begrijpen. Stel dat iedereen in de zaal al weet hoe hoog uw salaris is, en een spreker zegt dit nu ook nog eens publiekelijk. Is dit nutteloos, en voegt het niets toe? Nee, want met die mededeling maakt de spreker de bewering A over uw salaris van algemene kennis tot gemeenschappelijke kennis: ieder weet nu van elkaar dat ze het weten, enzovoorts. Zulk soort groepsinformatie over elkaar is niet zomaar een 'bijproduct' van communicatie. Het kan essentieel zijn voor praktisch handelen. Bijvoorbeeld, als we elkaar willen ontmoeten, dan moet ieder van ons de plaats en tijd weten. Maar dan nog gaan we niet als we niet weten dat de ander het ook weet, en zelfs dan zouden we nog niet gaan als we niet wisten dat de ander weet dat wij het weten, enzovoorts. Al deze niveaus zijn bevat in het begrip gemeenschappelijke kennis.

Vraag en antwoord

Misschien het eenvoudigste voorbeeld van een communicatiestap wordt geïllustreerd door het volgende voorval:

Q vraagt:	"Is dit de weg naar het Centraal Station?"(CS)
A antwoordt:	"Ja"

We weten natuurlijk niet precies welke informatie deze twee personen nu bezitten. Maar hier is een plausibel informatiemodel aan het begin:



Intuïtief weet A hier in de feitelijke situatie (aangegeven door de zwarte stip links) dat CS het geval is. In de andere situatie, waar $\neg CS$ opgaat weet hij dat laatste: blijkens het ook daar ontbreken van onzekerheidslijntjes met label A. Onze Q weet daarentegen niet hoe het zit met CS, want hij heeft een onzekerheidslijntje. Maar hij weet wel dat A weet hoe het staat met CS: en wel, omdat dit in beide situaties het geval is die hij kan zien. Dit is dus een hele goede reden om een vraag te stellen. De update naar volledige informatie voor beide spreekt dan voor zich:

TECHNIEK 19.

Epistemische logica

De epistemische of kennislogica wordt gebruikt voor het modelleren van de informatie en de uitwisseling daarvan zoals in de tekst besproken wordt. Deze logica is geïnspireerd op de eerder in 2.2 besproken modale logica (zie T.17 op pagina 79).

Epistemische taal

Laat A een verzameling van agenten. Voor elke individuele agent a is er een modale operator K_a. $K_a\varphi$ betekent dat de desbetreffende agent weet dat φ het geval is. Verder wordt gebruik gemaakt van twee groepsoperatoren E_G en C_G voor elke niet-lege deelverzameling van A. $E_G\varphi$ betekent dat elk van de agenten in G weet dat φ het geval is. $C_G\varphi$ zegt dat φ gemeenschappelijke kennis van de groep G is. Naast deze modale operatoren hanteren we de Boolese connectieven uit de propositielogica.

Informatiemodellen

De modellen zijn identiek aan die voor modale logica, gelabelde grafen met een lokale informatiefunctie voor de atomaire proposities, met die beperking dat de relaties tussen toestanden equivalentierelaties zijn (zie T.11). Elke relatie is gekoppeld aan een agent en verbeeldt zijn onzekerheidsrelatie. Hij weet niet welk van de gerelateerde werelden de werkelijke wereld is. Voor zo'n model $M = \langle S, \{R_a\}_{a\in A}, V\rangle$ en gegeven toestand $s \in S$ is de waarheid van formules gegeven als in T.17, en voor epistemische formules als volgt bepaald:

- *$K_a\varphi$ is waar in toestand s in M als geldt dat φ waar is in elke t met R_ast.*
- *$E_G\varphi$ is waar in toestand s in M als geldt dat φ waar is in elke t met R_gst voor willekeurige $g \in G$.*
- *$C_G\varphi$ is waar in toestand s in M als geldt dat voor elke niet lege rij van agenten $g_1, ..., g_n$ (niet noodzakelijk verschillend) uit G en elke rij $t_1, ..., t_n$ met $R_{g_1}st_1, R_{g_2}t_1t_2, ..., Rg_nt_{n-1}t_n$ geldt dat φ waar is in t_n.*

TECHNIEK 20.

Epistemische wetgeving

Een axiomatisering van de kennislogica vereist een aantal specieke kennisaxioma's naast de gewone klassieke propositielogica zoals in de Boolese algebra (zie T.26).
Als eerste hebben we een algemeen inferentieprincipe dat zegt dat de agenten zelf de kennislogica moeten kennen.

> *Als φ afleidbaar is in de kennislogica dan ook $K_a\varphi$, $E_G\varphi$ en ook zelfs $C_G\varphi$ voor alle agenten a en groepen G.*

Het tweede axioma is een algemeen axioma van de modale logica. Iedere agent kent de gevolgen van zijn kennis:

$$(K_a(\varphi \to \psi) \wedge K_a\varphi) \to K_a\psi$$

Specifieke epistemische axioma's zijn de volgende drie:

$$K_a\varphi \to \varphi$$
$$K_a\varphi \to K_aK_a\varphi$$
$$\neg K_a\varphi \to K_a\neg K_a\varphi$$

Het eerste zegt dat kennis altijd waar moet zijn. Onware zaken kunnen immers niet geweten worden. De tweede heet ook wel positieve introspectie*: als een agent iets weet, dan weet hijzelf ook dat hij het weet. Het derde axioma is de* negatieve *variant hiervan: als een agent iets niet weet dan weet hij dat het niet weet. Dit laatste principe is erg sterk. In de oorspronkelijke epistemische logica — een ontwerp van de Finse logicus Jaakko Hintikka in 1962, die een ruimere klasse van informatiemodellen hanteerde — werd dit principe verworpen. In de modernere varianten waarbij agenten vaak met een beperkt domein van propositionele informatie werken — bijvoorbeeld de kaartspelers uit de tekst — lijkt het wel acceptabel.*
Het principe van positieve introspectie is hier overigens overbodig. Het kan afgeleid worden uit de overige principes.
Deze axiomatisering is een volledige axiomatisering van universele waarheden over de genoemde informatiemodellen voor individuele agenten. Voor de groepsoperatoren moeten we nog toevoegen:

$$E_G\varphi \leftrightarrow (K_{a_1}\varphi \wedge ... \wedge K_{a_n}\varphi) \text{ indien } G = \{a_1, ..., a_n\}$$
$$C_G\varphi \leftrightarrow (E_G\varphi \wedge E_GC_G\varphi$$
$$(E_G\varphi \wedge C_G(\varphi \to E_G\varphi)) \to C_G\varphi$$

Het eerste principe zegt dat iedereen weet dat φ als een ieder afzonderlijk weet dat φ. Het tweede zegt dat φ gemeenschappelijke kennis als iedereen het weet en tevens iedereen ook weet dat het gemeenschappelijke kennis is. Het laatste lastiger te lezen principe is in feite een inductief axioma. Het zegt dat als iedereen weet dat φ (basis) en het is gemeenschappelijke kennis dat als φ geldt dat iedereen het dan ook weet (inductiestap) dan moet het gemeenschappelijke kennis zijn.
De volledigheidsstelling van deze logica stamt van eind jaren tachtig, een bekend resultaat van een vooraanstaande Californische groep van logici en informatici onder leiding van Joseph Halpern. Het bewijs is gebaseerd op eerdere volledigheidsbewijzen voor de in Hoofdstuk 2 genoemde proceslogica's (eind jaren zeventig).

We lezen een informatie model dus als volgt. Het diagram is publiek bekend aan alle personen. De onzekerheid voor individuele personen komt door hun lijntjes, maar de structuur van al die lijntjes is zelf weer aan iedereen gelijkelijk bekend.

Zodra we eenmaal dit soort modellen hebben, kunnen we ook een logisch systeem ontwerpen dat de kennis van spelers in detail beschrijft.

Geldig redeneren met kennis

Wij lezen niet alleen informatie af: we redeneren ook over onze eigen kennis, of die van anderen, en verbinden daaraan nieuwe consequenties. Dat redeneren kan worden beschreven met een logische taal en bewijsregels, net als we dat deden voor 'hardere' wiskundige bewijsvormen in eerdere hoofdstukken. Deze gebruikt notaties als

$K_a\varphi$ persoon a weet dat φ

waarmee allerlei feiten uit het voorgaande compact kunnen worden uitgedrukt. Zo brengt een vraag-antwoord episode

"Q: φ?" A: "Ja."

onder meer de volgende beweringen met zich mee:

Vooraf weet niet Q niet ofdat φ: $\neg(K_Q\varphi \vee K_Q\neg\varphi$, of logisch equivalent daarmee, $\neg K_Q\varphi\wedge\neg K_Q\neg\varphi$. Maar anderzijds houdt Q wel voor mogelijk dat A weet of φ: $\langle Q\rangle(K_A\varphi\vee K_A\neg\varphi)$.

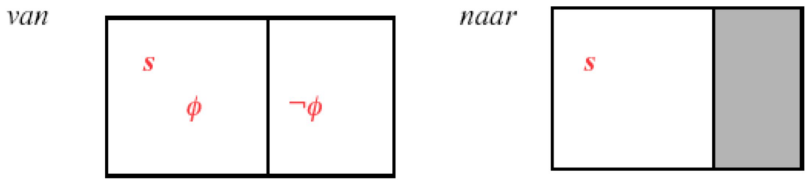
In T.19 worden wiskundige informatiemodellen gegeven, in analogie met de modellen voor proceslogica's uit Hoofdstuk 2 (zie ook T.17 op pagina 79). Deze modelleren individuele kennis en groepskennis. Hierbij aansluitend zijn ook weer volledige afleidingsystemen ontworpen voor 'kennis-
T. 20 $\Longrightarrow$ 125 logica'. Enkele voorbeelden van zulke kennislogische wetten zijn:

$K_a\varphi \to \varphi$ wat iemand weet is waar
$K_a\varphi \to K_aK_a\varphi$ we weten dat we iets weten

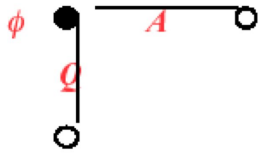
De winst van dit soort korte formules ten opzichte van lange formuleringen in natuurlijke taal zal duidelijk zijn. Met kennislogica's wordt tegenwoordig veel gewerkt in de informatica voor de analyse van zogenaamde 'multi-agent systems'. Met dit soort systemen kunnen we over onze kennis en informatie even exact redeneren als met Boolese operaties en kwantoren. Aldus komen steeds verdere vormen van intelligent handelen binnen het bereik van logische bewijsanalyse. En daarbij komen dan weer allerlei interessante verschijnselen aan het licht die verborgen blijven zolang we slechts informeel filosofisch of taalkundig naar communicatie kijken.

Wiskunde van publieke communicatie

Openbaar naar waarheid aankondigen dat φ verandert het huidige informatiemodel $\langle M, s\rangle$, waarbij s de feitelijk toestand is. De toestandsruimte is nu op te delen in toestanden waar φ waar is en die waar dat niet het geval is. Naar waarheid aankondigen dat φ het geval is, betekent dus dat alle werelden waar φ niet geldt *geëlimineerd* worden. s zelf blijft echter staan, want de aankondiging betrof ware informatie.



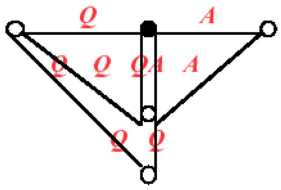
Dit eliminatiemechanisme lijkt heel eenvoudig, maar het kan subtiel liggen. We geven ter illustratie nog eens een vraag-antwoord episode "φ"?, maar nu beginnend in het volgende informatie-model met 3 toestanden waarbij φ alleen waar is in de werkelijke toestand (zwart).



Q stelt de vraag of φ geldt. A weet het antwoord niet. Maar de vraag zelf vertelt haar dat Q het ook niet weet, hetgeen haar juist de informatie oplevert dat de zwarte toestand de ware toestand is. Dus kan zij nu correct antwoorden! Wij kunnen dus wiskundig zelfs door onzekerheid uit te wisselen tot zekere kennis komen. Maar hiermee rijst ook een technische vraag.

> "Wat is de maximale correcte informatie die wij kunnen overdragen via updates van een gegeven beginmodel, en wat is het resulterende eindmodel?"

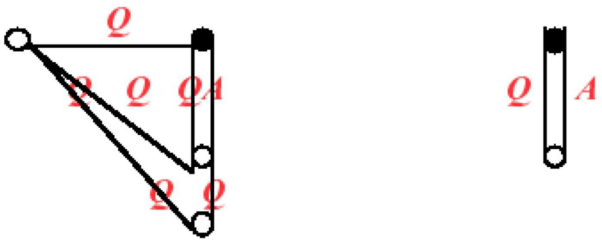
Bijvoorbeeld wat kunnen Q en A in het volgende model bereiken?



Het antwoord is in dit geval dat alleen een soort symmetrische kern van het diagram overblijft. Denk maar aan de volgende wat existentiële conversatie.

Q verzucht:	"Ik weet het niet",
en A verzucht dan:	"Ik weet het ook niet"

De bijbehorende updates staan hieronder:



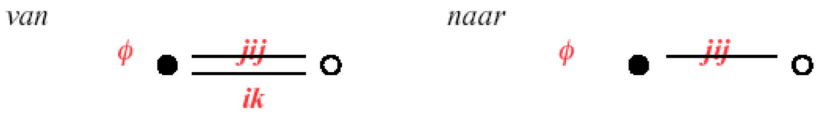
Hierachter schuilt een meer algemeen wiskundig bewijsbaar resultaat.

> Maximale publieke communicatie tussen twee personen levert een informatiediagram bestaande uit de feitelijke toestand plus alle toestanden die daaraan vast zitten met onzekerheidslijnen voor elke persoon; en dit kan altijd in twee rondes worden bereikt.

Wiskundige analyse helpt ons dus algemene eigenschappen van communicatie te achterhalen.

Updates met privacy

Onze voorbeelden tot nu toe betreffen slechts het eenvoudigste soort communicatie. Heel veel situaties in het leven vragen echter om *verbergen* van informatie. Spelen met onvolmaakte informatie waren een voorbeeld: als ik een kaart trek van de stapel leert u wel iets, maar niet precies wat ik trek. Iets soortgelijks speelde in ons scenario met de 'Twee Enveloppen', en verbergen is natuurlijk ook de essentie van algemeen beschaafde omgangsvormen waar we niet alles zeggen wat ons voor de mond komt. We geven alleen een kleine illustratie. De uitgangssituatie voor het Enveloppe voorbeeld is weer een eerder informatie-model, maar de update is dit keer dat we lijntjes weghalen in plaats van toestanden:



Dergelijke lijn-eliminatie is de juiste update procedure wanneer een vraag publiek wordt gesteld, maar het antwoord alleen wordt gegeven aan een deelgroep van de totale groep. Een spel als Cluedo kent episodes van dit soort.

Nog meer ingewikkelde updates, die informatiemodellen zelfs kunnen vergroten, zijn nodig voor de juiste analyse van meer complexe communicatieve handelingen die kunnen misleiden. Stel bijvoorbeeld dat in het eerdere kaartvoorbeeld, speler 1 een *email* stuurt aan speler 2 met de mededeling "ik heb niet de blauwe kaart". Maar hij stuurt die email ook aan speler 3 zonder dit aan 2 te laten merken, door middel van de speciale email adresseerknop bcc. Dan weet 2 niet dat 3 deze informatie heeft, en wat hij meent te weten loopt dus niet langer synchroon met de feiten. Het is niet moeilijk in te zien dat het nieuwe informatiemodel voor een handeling als e-mailen met bcc wezenlijk ingewikkelder zal moeten zijn dan alle diagrammen die we tot nu toe tekenden. Mocht dit u te technologisch lijken, dan kunt u denken aan meer alledaagse communicatievormen als 'afluisteren': deze leveren informatie op, maar door de meerpersoons complicaties kunnen ze informatie-modellen wezenlijk vergroten.

Meer praktisch worden dergelijke complicaties nodig in de analyse van 'veiligheid' van bijvoorbeeld internet-protocollen, waar personen enerzijds onderling vrijuit willen communiceren, maar anderzijds naar andere gebruikers toe maximaal afgeschermd willen zijn. Nog verdere niveaus van complexiteit ontstaan als we ons buigen over de logische studie van wijd verbreide cognitieve verschijnselen als liegen en bedriegen.

Kennislogica en informatica

Moderne logische systemen voor communicatie zijn overigens nog iets rijker dan wat we tot nu toe hebben gezien. Tot nu toe hebben we alleen beweringen over kennis en onwetendheid beschouwd per informatiemodel. Maar de essentie van update is dat zulke modellen *veranderen* wanneer communicatieve handelingen plaats vinden. Ook dit soort toestandsverandering kan logisch worden beschreven,

zoals we reeds zagen met de procesgrafen van Hoofdstuk 2, en de bijbehorende modale taal voor programma's. Maar dan moeten we de structuur van 'communicatieprogramma's' zichtbaar maken. Een modale proceslogica voor communicatie heeft typische formules van de vorm

$[A!]\varphi$ na een publieke mededeling van A geldt in het nieuwe informatiemodel de kennislogische bewering φ.

Ook voor dergelijke logica's bestaan interessante algemene wetten, die kennislogica mengen met programmalogica. We geven hier een voorbeeld, enkel en alleen om het genre typografisch te illustreren:

$$[A!]K_a\varphi \rightarrow K_a[A!]\varphi.$$

Dit relateert kennis na een mededeling aan kennis die iemand al voor die mededeling had, of wiskundig gesproken: het laat zien hoe kennis en handelingen commuteren — althans voor personen met een perfect geheugen, en perfecte observatievermogens. Formele wetten van dit soort maken het mogelijk om welbekende technieken van programma-analyse uit de informatica toe te passen op communicatieprocessen.

Discussie: taal en cognitie

Het informatiemodel van dit hoofdstuk is zeer algemeen. Het wordt bijvoorbeeld ook toegepast op gewoon taalgebruik. In de moderne 'dynamische semantiek' wordt de betekenis van uitdrukkingen in natuurlijke taal uitgelegd in termen van de bijdrage die zij leveren als communicatieve updates. Elke bewering is een 'zet' in een gesprek. Taalhandelingen nemen aldus het primaat over van de taalstructuur. Zoals steeds rijst dan de vraag of het dynamische model van informatie-update ook empirisch cognitief plausibel is. Wij laten dat voor wat het is, omdat nog weinig cognitief-psychologisch onderzoek is gedaan naar de aansluiting tussen communicatie-logica's en feitelijk communicatiegedrag van mensen.

Wel is er de laatste tijd een andere onderzoeksrichting van theorie naar praktijk, en wel de 'social software'. Deze leuze beoogt het systematisch ontwerp van sociale procedures, zoals stemprocedures, verdelingsmethoden, juridische regels, en dergelijke. Veelal worden deze beschouwd als natuurgegevens, maar in feite zijn het constructies, die voor analyse en verbetering vatbaar zijn. Zo is er een interessante literatuur over verbeterde regels voor echtscheiding, om maar eens een bloeiende miljoenen-industrie te noemen. De logische modellen van dit hoofdstuk kunnen hierbij worden gebruikt, naast speltheorie, en andere wiskundige technieken. Een aardig huiselijk voorbeeld van social software is het volgende trekkings-probleem, dat in 2000 werd opgeworpen door een studente van deze cursus die voorafging aan dit boek.

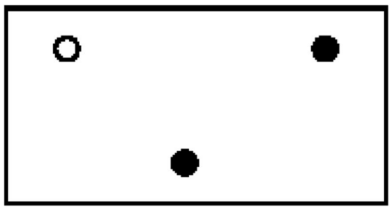
> Een familie wil met Sint Nicolaas lootjes trekken voor het maken van de surprises zodat (a) niemand van een ander weet welke persoon hij heeft, en (b) niemand zichzelf krijgt toegewezen. De procedure moet plaats vinden met allen aanwezig in de kamer, gebruik van kaartjes en dergelijke is toegestaan — maar waarschijnlijkheidsmechanismen niet. Kunt u een manier vinden om dit te bereiken?

Dit vergt een koppeling tussen een gewone programmeertaak (toewijzen van objecten aan objecten), uitvoerbaar door een Turing machine, en een voorgeschreven dosering aan kennis en onwetendheid, die het ontwerp compliceert. Dit soort software wordt steeds belangrijker, bijvoorbeeld bij het ontwerp van elektronische transacties, en van algemene nieuwe 'omgangsvormen' op het Internet.

Toegift: 'Modderige Kinderen'

Een belangrijke bron van inzichten over communicatie en informatie is te vinden in puzzels. Hier is een bekend voorbeeld, waarvan de origine ver in de geschiedenis terug gaat (sommige puzzels zijn traceerbaar tot in de Klassieke Oudheid):

> Drie kinderen spelen in de tuin, en twee van hen hebben modder op hun voorhoofd gekregen. Ze zien elkaar, maar niet zichzelf. Ieder kind ziet dus minstens één modderig kind. Nu komt hun vader langs, en vertelt ze iets wat allen al weten: "Minstens één van jullie heeft modder op zijn voorhoofd." (Ouders zeggen wel vaker van die dingen die je allang weet.) Nu vraagt de vader: "Weet iemand van jullie of hij modderig is?" Alle kinderen antwoorden naar waarheid. Hij blijft dit vragen. Wat gebeurt er?

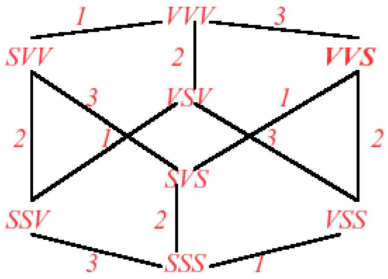


Één mogelijk antwoord is: "Er gebeurt niets." De vader voegde immers geen informatie toe aan wat iedereen al wist. Maar dit kunnen we terzijde schuiven, gescherpt door wat we in het voorgaande al leerden. In feite zal iedereen zeggen dat ze het niet weten in de eerste vraagronde. Daarna kennen beide modderige kinderen hun status in de tweede ronde, omdat beide als volgt kunnen redeneren:

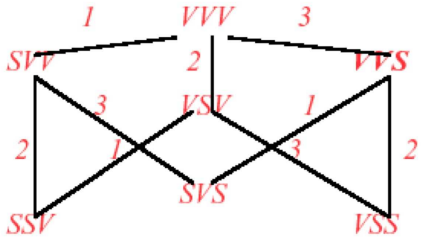
> Stel eens dat ik schoon was. Dan had het modderige kind dat ik zie alleen schone kinderen om zich heen, zodat vader's mededeling hem meteen zei dat hij modderig was. Maar dat is niet gebeurd — want hij wist het niet. Dus ben ik modderig.

Het schone kind weet zijn status nog niet in de tweede ronde, maar wel in de derde. Wat is er hier precies gebeurd? Om te beginnen heeft Vader's mededeling de aanwezigheid van een modderig kind verheven van algemene kennis naar *gemeenschappelijke kennis* in de groep. En in de daarop volgende communicatie blijkt dat zelfs leren over andermans onwetendheid positieve informatie kan opleveren.

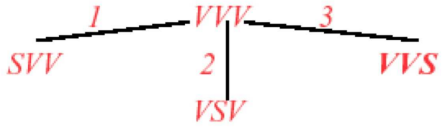
Een overzichtelijke manier om dit proces te beschrijven zijn weer informatiediagrammen en updates. Een toestand van de wereld kent eigenschappen V (vies) of S (schoon) toe aan elk kind: acht mogelijkheden totaal. De feitelijke toestand is VVS. In elke toestand heeft een kind maar één onzekerheid: hij kan die toestand niet onderscheiden van een waar zijn eigen V/S-waarde verschilt.



De update voor vader's mededeling elimineert allereerst de toestand SSS:



Dit nieuwe informatiemodel heeft drie toestanden waar minstens een kind zijn status kent: te weten SSV, SVS en VSS. De eerste ronde elimineert deze dus:



Nu weten kinderen 2 en 3 hun status in toestand VVS en dat zeggen ze ook. Dat elimineert nog eens de toestanden SVV, VSV en VVV en we belanden bij het model met alleen VVS nog over. Nu is ieder's status gemeenschappelijke kennis geworden.

Tot zover is deze analyse een toepassing van wat we al hebben gezien. Maar er schuilen ook diepere kwesties achter deze bekende puzzel.

Programmastructuur en complexiteit van communicatie

Vader's instructies bevatten alle bekende programma-structuren uit de informatica. Zo is er een conditionele instructie: *Als* je het weet, *dan* moet je "JA"zeggen, *anders* "NEE". Maar er is met name ook een in principe onbeperkte *herhaling*: "Blijf antwoorden op mijn vraag, *zolang* je je status niet kent". Zulke herhalingen zijn kenmerkend voor programmeren. Ze wijzen erop dat 'social software' wel eens subtiele informatica-aspecten zou kunnen hebben. Met name komt hiermee de *complexiteit* van sociale mechanismen in het vizier. In 2003 werd bewezen dat de gecombineerde kennis/actie-logica van herhaalde aankondigingen *onbeslisbaar* is![1]

Het precieze betekeniseffect van conversatie

Maar minstens zo intrigerend is de volgende betekeniskwestie, die ons terug brengt naar een basale vraag in taalkunde en filosofie. We hebben in het voorgaande nergens duidelijk gezegd wat nu eigenlijk het algemene informatieve effect van een publieke mededeling is. Nu lijkt dat voor de meeste mensen duidelijk:

> Publiek aankondigen van φ maakt φ tot gemeenschappelijke kennis.

En dat is ook zo in simpele gevallen. Een meegedeeld feit – zeg dat de Romeinse keizers in Rome een Germaanse garde hadden, lang voor onze huidige UN missies - wordt gemeenschappelijke kennis in

[1] In hoofdstuk 7 wordt de notie van onbeslisbaarheid gedefinieerd en uitgebreid besproken.

de groep. Maar de puzzel van de Modderige Kinderen weerlegt dit principe in het algemeen! Immers, in de eerste ronde van ons voorbeeld delen de modderige kinderen mee dat ze hun status niet kennen. Maar het effect van de bijbehorende update is helemaal niet dat iedereen nu weet dat ze hun status niet kennen. Dat effect is juist dat zij hun status *wel* kennen.

We zien hier een eigenaardigheid van de dynamiek van toestandsverandering. Een handeling kan juist de condities aantasten die hem in eerste instantie mogelijk maakten. De mededeling betreft de situatie zoals hij was, en is daarvoor waar. Maar zij verandert nu juist die situatie, en in de nieuwe situatie kunnen andere beweringen gelden. Sommige mededelingen zagen de tak af waarop zij zitten (’zaten’...). Er ligt hier zelfs een nog niet opgeloste wiskundige vraag. Wanneer gaat het wel goed?

> *Leerprobleem* Wat is de precieze klasse van ware publieke mededelingen die automatisch tot gemeenschappelijke kennis leiden?

En dit zijn alleen nog maar vragen over het eenvoudigste soort ’open’ communicatie dat we kennen:, de publieke mededeling. De meer verfijnde wiskunde van communicatie met verbergen van informatie, en vervolgens de kunst van misleiden en bedriegen, staat nog maar in de kinderschoenen.

Hoofdstuk 5

Voorspellen

5.1 Dynamische systemen

Teleologie versus causaliteit

Vele filosofen hebben zich bezig gehouden met de vraag hoe veranderingen in de natuur plaatsvinden. Bij Aristoteles en de andere Griekse filosofen was dat voornamelijk een teleologische of doelgerichte kijk, waarin veranderingen in eerste instantie een duidelijk vooropgezet doel hadden. Deze visie was vooral geïnspireerd door de levende natuur; een zaadje heeft het *in zich* om uit te groeien tot een plant. Alle gebeurtenissen in het groeiproces moeten gezien worden in het licht van het uiteindelijke resultaat van de volgroeide plant.

Deze kijk werd ook overgedragen naar materiële zaken, zoals de valbeweging van een zware massa naar de aarde toe. Voor de Griekse filosofen bestond alles uit vier elementen: vuur, lucht, water en aarde. Ieder van die element had een 'natuurlijke' beweging. Zo ligt het in de natuur van het element 'aarde' om in een rechte lijn te bewegen naar het centrum van de aarde. Dat is de natuurlijke plaats voor zware objecten. Op eenzelfde wijze gaan vuurvlammen die uit een brandend stuk hout ontsnappen omhoog, omdat voor het element 'vuur' de hemel de natuurlijke plaats is. In wezen werd met deze kijk materie 'bezield' en van een eigen wil voorzien.

De teleologische visie werd volledig onderuit gehaald in de mechanische natuurwetenschappelijke revolutie van de 16de en 17de eeuw. Van de Engelse filosoof Thomas Hobbes (1588-1679) is de volgende bekende uitspraak over de filosofie van Aristoteles, waarin dingen vallen omdat ze zwaar zijn.

> *But if you ask what they mean by heaviness, they will define it to be an endeavour to go to the center of the earth. So that the cause why things sink downward, is an endeavour to be below; which is as much to say that bodies descend, or ascend, because they do. It is as if stones and metals had a desire, or could discern the place they would be at, as man does.*

In de oudheid werd ook al naast het teleologische verband het oorzakelijke, of causale, verband onderscheiden. Bepaalde gebeurtenissen kunnen nu eenmaal andere gebeurtenissen tot gevolg hebben. Zo zijn het de hamerslagen van de beeldhouwer die een stuk marmer tot een standbeeld maakt. Het ligt niet in de natuur van het marmer zelf om tot de Venus van Milo te transformeren. In de moderne natuurwetenschappelijke kijk is deze causale kijk volledig dominant geworden. Zelfs het uitgroeien van een cel tot een volledig organisme zullen we beschrijven als een serie zeer complexe chemische reacties die een duidelijk oorzakelijk verloop hebben.

De teleologische kijk is natuurlijk niet helemaal verdwenen. Het is vaak een goede beschrijving voor het gedrag van mensen of andere levende organismen. De beste verklaring waarom rond acht uur 's avonds honderden mensen bij de ingang van het Concertgebouw verzamelen is natuurlijk gelegen in het feit dat weldra een concert begint. Het zal zeer moeilijk zijn het collectief gedrag van al deze mensen te beschrijven uitgaande van hun fysieke en geestelijke toestand bij het ontbijt diezelfde ochtend.

Dynamische systemen

De oorzakelijke kijk op hoe veranderingen plaatsvinden, houdt in dat een volledige beschrijving op een gegeven moment genoeg is om de toestand een tijdje later te kennen. In de wiskunde heeft dit zijn plaats gevonden in de theorie van de *dynamische systemen.*

Startpunt is een bepaald (abstract) systeem of model waarvan we de veranderingen in de tijd willen beschrijven. Daartoe moeten we eerst een volledige karakterisering van het systeem geven. We

veronderstellen dat dit gebeurt met een *toestandenruimte* of *faseruimte* Ω. In voorbeelden zullen we vaak voor de faseruimte een deelruimte van $\mathbb{R}^n$ nemen. Maar soms zal Ω ook een eindige verzameling kunnen zijn.

Per definitie legt een punt $x \in \Omega$ het systeem volledig vast. Daarmee bedoelen we dat iedere eigenschap van het systeem door het punt x gekarakteriseerd wordt. De vraag is nu hoe een punt x in de tijd zal gaan lopen. Als de toestand voor latere tijd volledig bepaald is door de begintoestand spreken van een *deterministisch systeem.* Het tijdsbegrip dat we daarbij gebruiken zal dat van Newton zijn. Newton stelde

> *Absolute, true and mathematical time, of itself, and by its own nature, flows uniformly on, without regard to anything external.*

Dit idee van tijd als een eeuwigdurende klok is later door Einsteins relativiteitstheorie vervangen door een veel flexibeler tijdsbegrip. Einstein liet zien dat tijd niet los van ruimte beschouwd kan worden. In de moderne fysica is tijd een relatief begrip dat voor iedere waarnemer verschillend kan zijn en alleen lokaal, in een kleine ruimtelijke omgeving van de waarnemer, betekenis heeft. Tijd kan ook eindigen (bijvoorbeeld in het binnenste van een zwart gat), beginnen (zoals bij de Big Bang) of zelfs in zichzelf terugkeren (wormgaten).

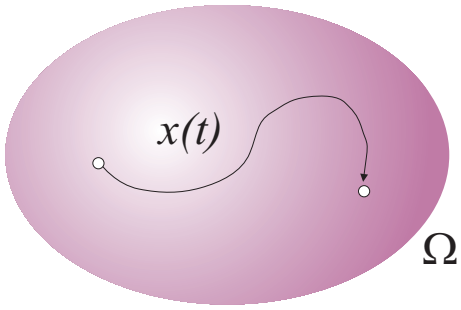
Hier zullen we ons niet met dit soort 'subtiliteiten' bezig houden. Tijd zal voor ons een parameter t zijn, die we vaak zullen opvatten als een element in de reële rechte $\mathbb{R}$ of een interval daarvan. In dat geval spreken van een continu tijdsbegrip. Omdat we de tijd als een continue variabele beschouwen, kunnen we tijdsverschuivingen $t \to t + \delta t$ beschouwen, waarbij δt zo klein gekozen kan worden als we maar willen. Door de limiet $\delta t \to 0$ van oneindig kleine tijdsontwikkeling te nemen, komen we vanzelfsprekend uit op het begrip tijdsafgeleide of snelheid. Dit was natuurlijk het grote inzicht van de pioniers van de mechanica (Newton, Leibniz, Huygens).

In een algemeen dynamisch systeem zal de toestandsvariabele $x \in \Omega$ dan ook aan een relatie voldoen van de vorm

$$x(t + \delta t) \approx x(t) + f(x, t)\delta t$$

Hier is de infinitesimale verandering van x gegeven door een functie f van zowel de toestand x als het tijdstip t. We kunnen bijvoorbeeld denken aan de beweging van een deeltje in een krachtenveld dat expliciet in de tijd verandert. In veel voorbeelden zullen we aannemen dat deze extra tijdsafhankelijkheid niet bestaat, zodat we gewoon kunnen schrijven $f(x)$.

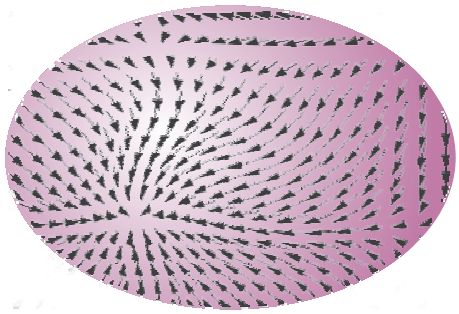
Wat betekent dit? Als we een punt $x \in \Omega$ nemen, dan zal deze toestand in een tijdspanne δt evolueren van een toestand x naar een toestand $x + f(x)\delta t$. Het punt x gaat 'stromen' over de faseruimte Ω, de variable x wordt een functie van de tijd t. We schrijven $x(t)$ voor de positie op tijdstip t. Hier is $x(0)$ de beginpositie. Het volledige traject is een kromme in de faseruimte Ω die we de *baan* noemen.



Door de limiet $\delta t \to 0$ te beschouwen verkrijgen we de eerste-orde differentiaalvergelijking

$$\frac{dx}{dt} = f(x).$$

We schrijven ook vaak Newton's originele notatie $\dot{x}$ voor dx/dt.[1] De functie f is een vectorveld op de faseruimte Ω. Het geeft in ieder punt weer in welke richting de beweging gaat stromen.



De harmonische oscillator

Het is misschien goed om eerst een eenvoudig voorbeeld uit de mechanica te bekijken. Stel, we hebben een (punt)deeltje dat vastgemaakt zit aan een veer. Het deeltje kan alleen maar in één richting bewegen. Deze positie zullen we beschrijven met de coördinaat $q \in \mathbb{R}$.

$\longleftarrow q \longrightarrow$

Nu ligt de toestand van dit systeem niet vast als we alleen de variabele q geven op tijdstip t. We moeten ook de snelheid $v = \dot{q}$ geven. Samen geven de variabelen (q, v) de toestand van het deeltje volledig weer. De ruimte $\mathbb{R}^2$ van alle paren $x = (q, v)$ is dan de faseruimte. De variabele x is dus in dit geval gegeven door twee reële getallen q en v.

De differentiaalvergelijking die dit systeem in z'n eenvoudigste vorm beschrijft is de zogeheten harmonische oscillator, geven door de vergelijkingen

$$\dot{q} = v, \qquad \dot{v} = -q.$$

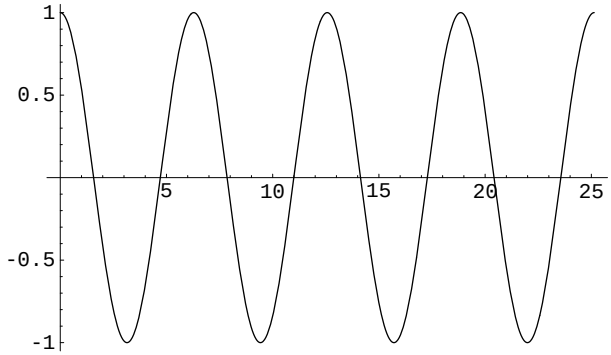
Stel op tijdstip $t = 0$ kiezen we het punt $x = (1, 0)$. Dat wil zeggen, de variabele $q = 1$ (de veer is uitgerekt over een afstand 1), en de variabele $v = 0$ (het deeltje staat stil). De algemene oplossing van bovenstaande vergelijkingen met deze beginconditie is

$$q(t) = \cos t, \qquad v(t) = \sin t$$

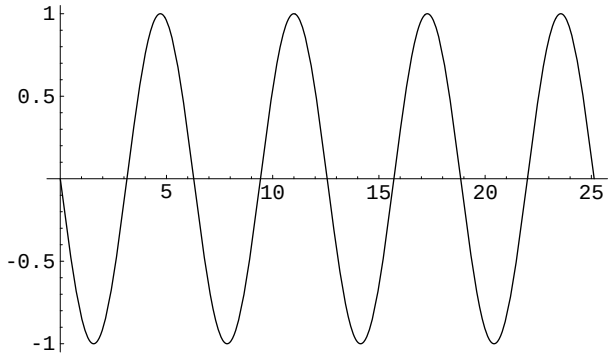
Het deeltje gaat dus inderdaad een trilling uitvoeren. Na een tijdspanne $t = 2\pi$ is het deeltje weer op

[1] De laatste gebruikelijkere notatie werd geïntroduceerd door Leibniz.

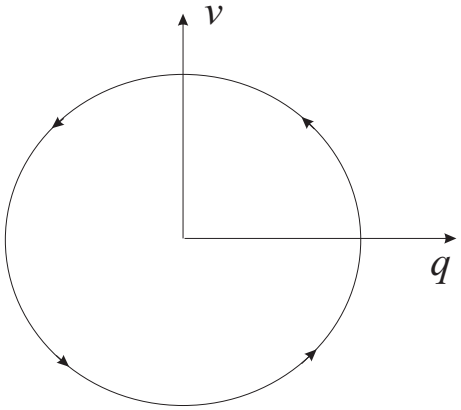
de beginpositie teruggekeerd. De tijdsontwikkeling van $q(t)$ is gegeven door



Soortgelijk kunnen we de veranderingen in de snelheid weergeven



Het is nu zeer instructief om deze twee bewegingen uit te zetten als een beweging van een punt in de faseruimte $\mathbb{R}^2$. Omdat we eenvoudig zien dat de grootheid $q^2 + v^2$ behouden is — dat wil zeggen dat deze niet verandert in de tijd — is het traject in de faseruimte gegeven door een cirkel die tegen de klok in wordt doorlopen.



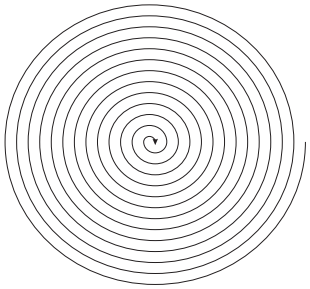
Dekpunten en stabiliteit

In het eenvoudige voorbeeld van de harmonische oscillator zien we één heel bijzonder gedrag, namelijk de beginsituatie $q = 0$ en $v = 0$. In dat geval zal de oplossing eenvoudig constant zijn: het deeltje

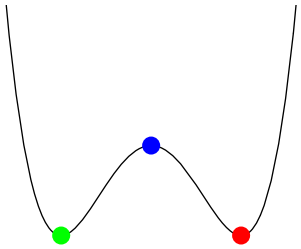
blijft in het punt $q = 0$ liggen. Zo'n oplossing, waarbij de variabelen niet veranderen noemen we een *dekpunt* van het dynamische systeem. Een dekpunt voldoet voor alle t aan

$$x(t) = x(0).$$

In het algemeen zijn dekpunten belangrijk omdat vaak in een dynamisch systeem banen zullen convergeren tot een dekpunt. Je kunt bijvoorbeeld denken aan een trilling met wrijving. Uiteindelijk zal de beweging stoppen in de configuratie $q = v = 0$. In dit geval zijn de bewegingen geen cirkels in de faseruimte, maar spiralen die langzaam naar de oorsprong toe convergeren.



In het bovenstaande geval is er maar één dekpunt, maar in het algemeen kunnen er natuurlijk meer zijn. Denk bijvoorbeeld aan een deeltje dat kan bewegen op onderstaande 'glijbaan'



Hier kan het deeltje stil komen te liggen in het linker of in het rechter putje. Deze posities hebben een belangrijke eigenschap. Als we het deeltje een klein beetje verstoren, door het een kleine snelheid te geven of lichtjes van zijn plaats af te halen, zal het (met de invloed van wrijving) uiteindelijk naar de beginpositie terugkeren. In dit geval spreken we van een *stabiel* dekpunt.

In het voorbeeld is er ook een instabiel dekpunt. Namelijk de positie waarin het deeltje precies in het midden ligt, op het middelste bergje. In dit geval zal de kleinste verstoring de oplossing laten verdwijnen.

Periodieke en quasi-periodieke beweging

In het algemeen zijn de oplossingen van de harmonische oscillator allemaal gegeven door periodieke bewegingen. Deze oplossingen zijn van de vorm

$$q(t) = A\cos(t + B)$$

en hebben de eigenschap dat

$$q(t + 2\pi) = q(t)$$

Na een tijdsperiode van 2π zijn we dus weer in hetzelfde punt van de faseruimte aangeland. Omdat de beweging volledig deterministisch is, zal de beweging zichzelf vervolgens moeten herhalen.

Immers, we zijn in hetzelfde beginpunt aangekomen en per definitie ligt de baan vast gegeven het beginpunt. Periodieke bewegingen zijn een van de meest karakteristieke oplossingen van dynamische systemen. Na dekpunten zijn het ook de eenvoudigste. Een periodieke baan in de faseruimte waar andere bewegingen naar convergeren heet een *limietcykel*.

Periodieke bewegingen zijn overal om ons heen, in slingers, veren, maar ook in het zonnestelsel, de banen van de planeten, manen en astroïden, als wel in de (klassieke) banen van elektronen om de atoomkern. Maar vele andere verschijnselen in de natuur, cultuur en economie zijn cyclisch. Een eenvoudig voorbeeld is te vinden in de populatiedynamica.

Prooi-roofdier systemen

Stel we bekijken een populatie van herten en tijgers. Laat H het totaal aantal herten zijn en T het aantal tijgers. Een simpel populatiemodel (het Lotka-Volterra model) beschrijft hoe deze aantallen in de tijd veranderen. In de afwezigheid van roofdieren verwachten we een simpel proportioneel groei gedrag voor de herten. De verandering $\dot{H}$ in het aantal herten is evenredig met het aantal H zelf. In een formule

$$\dot{H} = A \cdot H$$

met $A > 0$ een maat voor het succes van reproductie. De oplossing van dit eenvoudige systeem is

$$H(t) = H(0)e^{At}$$

De populatie verdubbelt in een tijd $t = \log 2/A$.

We kunnen nu het effect van de tijgers toevoegen. Ten eerste zullen de tijgers een zeker percentage van de herten gaan jagen. Deze bijdrage is proportioneel met zowel het aantal herten als het aantal tijgers, dus met $H \cdot T$. Dit geeft een extra term in de vergelijking voor $\dot{H}$, namelijk

$$\dot{H} = A \cdot H - B \cdot H \cdot T$$

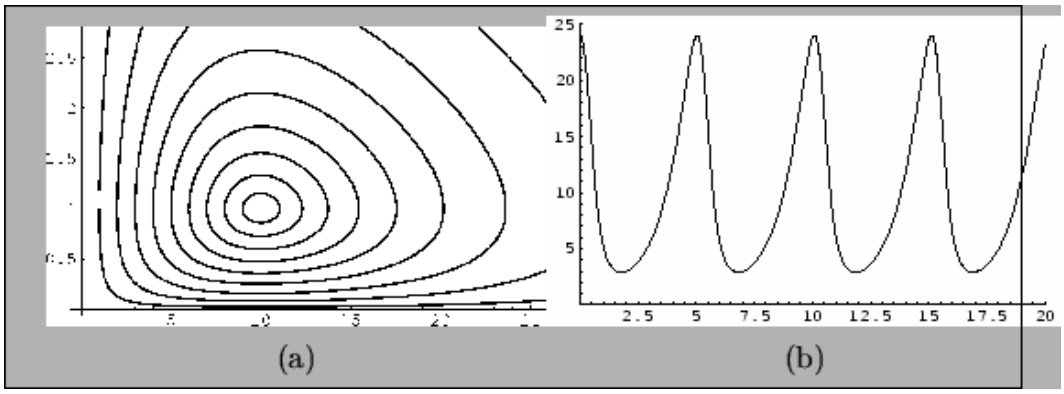
De constante $B > 0$ geeft aan hoe succesvol de tijgers zijn in hun jacht.

Vervolgens zal ook de populatie van tijgers veranderen, en wel door twee effecten. Er zal groei zijn door het eten van herten — een effect weer evenredig met $H \cdot T$ — en er zal natuurlijke sterfte zijn, evenredig met T. Dit geeft de vergelijking

$$\dot{T} = C \cdot H \cdot T - D \cdot T$$

voor constantes $C, D > 0$.

In onderstaande figuren is in (a) het typische gedrag in de faseruimte van punten (H, T) geschetst tezamen met in (b) een typische tijdsontwikkeling van H.



Duidelijk zichtbaar zijn de periodieke banen. Er is een intuïtieve reden voor dit cyclisch gedrag. Stel we beginnen met veel herten en weinig tijgers. Dan zullen de tijgers zeker in het begin zeer succesvol zijn, er is immers genoeg prooi. In de vergelijking voor $\dot{T}$ zal de eerste positieve term domineren. Dit groeigedrag van de tijgerpopulatie zal na enige tijd ten koste gaan van de hertenpopulatie. H zal gaan afnemen totdat uiteindelijk er zo weinig herten zijn dat de natuurlijke sterfte van de tijgers de sterk verminderde groei door het jagen op een kleinere populatie van herten zal gaan domineren. Nu zal de tijgerpopulatie gaan afnemen en de hertenpopulatie gaan groeien. Na enige tijd is deze cyclus voltooid en begint het proces van vooraf aan.

Discrete systemen

Vaak wordt een *discreet* beeld van de tijd gehanteerd. In dat geval zijn we slechts geïnteresseerd in de toestand van het systeem op tijdstippen $t_0, t_1, t_2, \ldots$. We zullen deze tijdstippen uniform kiezen, dat wil zeggen

$$t_n = n \cdot \delta t,$$

waarbij δt de tijdstap is.

We krijgen op deze wijze ook een serie elementen $x_0, x_1, x_2, \ldots \in \Omega$. De tijdsevolutie wordt nu beschreven door een systeem van de vorm

$$x_{n+1} - x_n = f(x_n)$$

Hier beschrijft $f(x_n)$ de verandering van de toestand x_n in het discrete tijdsinterval δt. We kunnen deze vergelijking trouwens ook schrijven als

$$x_{n+1} = g(x_n)$$

met $g(x) = x + f(x)$.

Een simpel voorbeeld is exponentiële groei. In dat geval hebben we te maken met de vergelijking

$$x_{n+1} = (1 + \lambda)x_n$$

Dit is een eenvoudig model van populatiegroei, waarin de populatie in een tijdsinterval toeneemt met een factor $1 + \lambda$. Als bijvoorbeeld $\lambda = 0,1$ dan is er sprake van 10% groei in ieder tijsinterval δt. De oplossing is dan

$$x_n = (1 + \lambda)^n x_0.$$

Vele van de eerdere voorbeelden met een continu tijdsverloop kunnen ook met een discrete versie van tijd bestudeerd worden.

Stochastische beweging

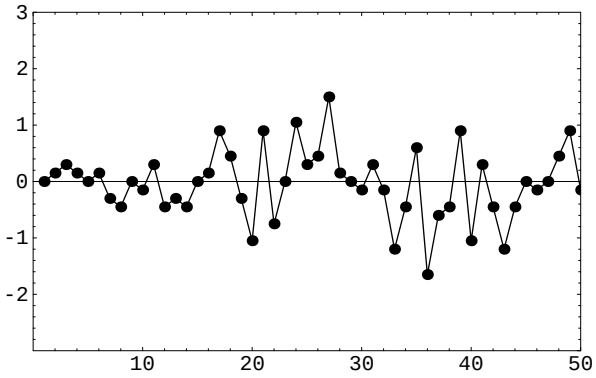
We hebben tot nu toe twee eenvoudige soorten van beweging gezien, vaste punten en periodieke banen. Beide bewegingen hebben de eigenschap dat het systeem uitstekend voorspelbaar is.

Er is een ander soort beweging dat in wezen heel eenvoudig is, maar dat absoluut niet voorspelbaar is, namelijk stochastische processen. In een stochastisch systeem wordt de positie x_{n+1} bepaald door een kansproces. De loop van de veranderingen wordt (gedeeltelijk of volledig) door het toeval bepaald.

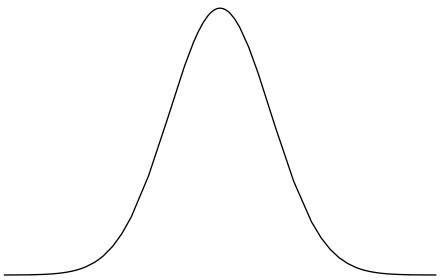
Een standaardvoorbeeld is de Brownse beweging die ook de *dronkemansloop* wordt genoemd. In dit model wordt de verandering van de positie x bepaald door een munt op te gooien en afhankelijk van de uitkomst ofwel een stap δx naar links of naar rechts uit te voeren

$$x_{n+1} = x_n + \epsilon_n \delta x$$

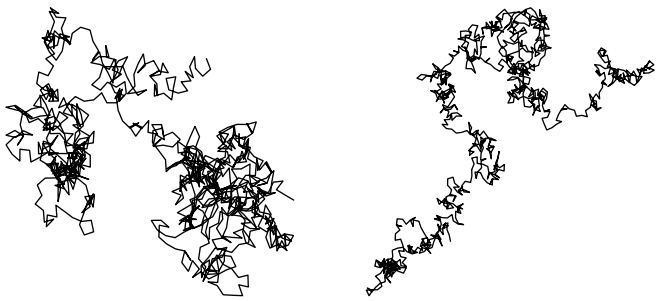
Hier is ϵ_n een toevalsvariabele die met een kans van 50% de waarde $+1$ aanneemt en met kans 50% de waarde -1. Een typisch verloop van een één-dimensionale Brownse beweging is bijvoorbeeld

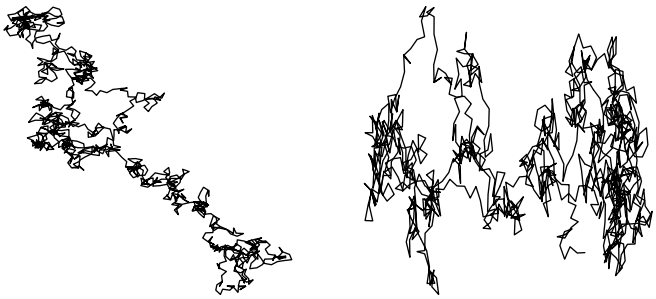


In principe hebben we bij stochastische bewegingen het determinisme volledig opgegeven. Als we met een gegeven beginpositie de tijdsontwikkeling nogmaals doorlopen, krijgen we een volledig andere uitkomst. Toch is er 'orde in de willekeur.' Namelijk, allerlei statistische grootheden hebben weer een eenvoudige vorm. Zo kunnen we bijvoorbeeld voor een groot aantal paden de gemiddelde lengte van het Brownse pad bepalen. We krijgen dan weer een mooi regelmatig beeld, in dit geval een normaalverdeling van de vorm e^{-x^2}.



Brownse beweging kan ook in hogere dimensies beschouwd worden, Hier zijn wat voorbeelden van een tweedimensionale Brownse beweging





De logistieke vergelijking

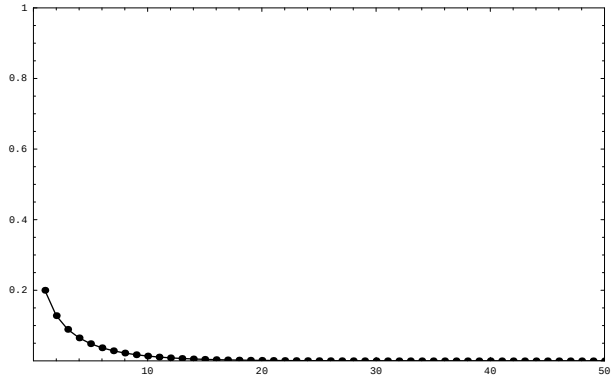
De *logistieke vergelijking* is zonder meer een van de beroemdste discrete dynamische systemen. Het betreft de volgende eenvoudige vergelijking

$$x_{n+1} = f(x_n), \qquad f(x) = bx(1-x)$$

De variabele x neemt hierbij waarden in in het interval $[0,1]$. Het kan gezien worden als een populatie model, waarbij $x = 1$ de maximale populatie is. Er zijn twee termen. Voor kleine waarde van x domineert de sterfte/groei term met factor bx. Voor $b > 1$ geeft dit (exponentiële) groei, voor $b < 1$ geeft het (exponentiële) afname. Er is echter ook een ingebouwde rem. Als de variabele x namelijk in de buurt van 1 komt, is er de remmende factor $1 - x$. Deze zorgt ervoor dat de verandering klein wordt als x in de buurt van het punt $x = 1$ komt.

De parameter b wordt gekozen in het interval $[0,4]$. (Voor grotere waarden van b blijft x niet langer tussen 0 en 1. Ga na dat het maximum van de functie $bx(1-x)$ aangenomen wordt voor $x = 1/2$ en dat het maximum $b/4$ is.) Dit simpele systeem vertoont een groot aantal verschillende soorten gedrag afhankelijk van de waarde van de parameter b.

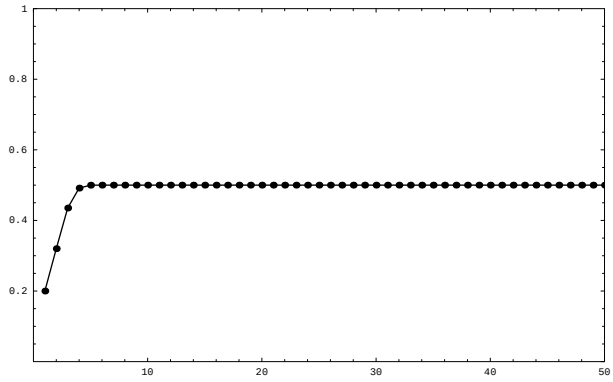
- Uitsterven. Als $b < 1$ dan zal voor iedere beginvoorwaarde $x \in [0,1]$ de oplossing uiteindelijk naar $x = 0$ gaan.



- Dekpunt. In het regiem $1 < b < 3$ zal iedere reeks x_n uiteindelijk convergeren naar het dekpunt x_*, gegeven door

$$x_* = bx_*(1-x_*).$$

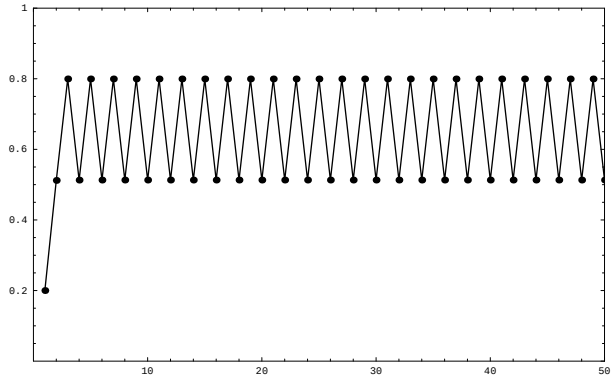
Hier is bijvoorbeeld het gedrag voor $x_0 = 0,2$ en $b = 2$



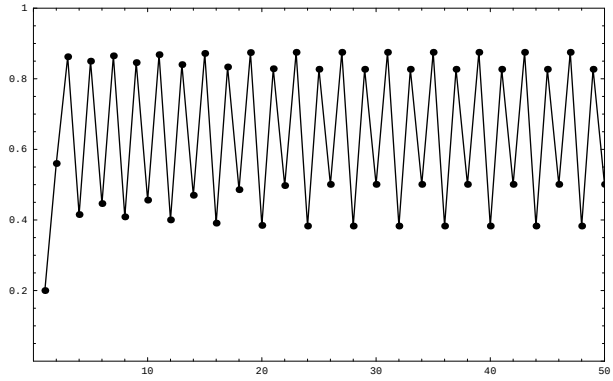
- Periodieke beweging met periode 2. In het regiem $3 < b < 1 + \sqrt{6}$ zijn er geen stabiele dekpunten meer, maar zal de beweging typisch convergeren naar een periodieke beweging met periode 2. Dat wil zeggen, er zijn twee punten x_* en x_{**} die voldoen aan

$$x_{**} = f(x_*) \qquad en \qquad x_* = f(x_{**}).$$

Zie het gedrag voor $x_0 = 0,2$ en $b = 3,2$



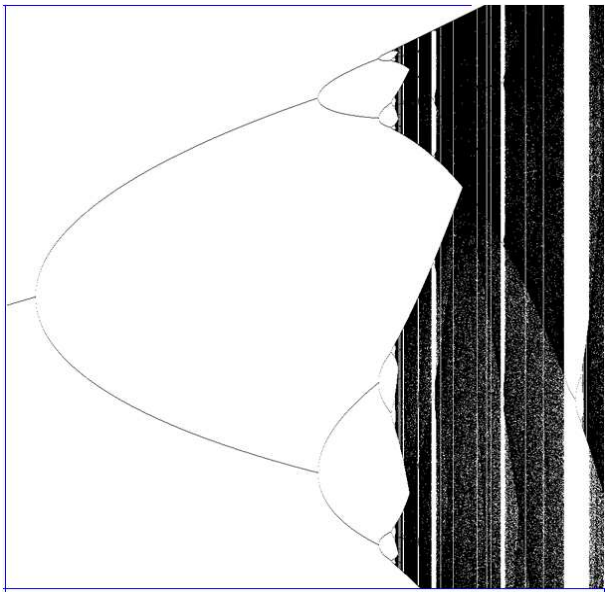
- Periodeverdubbeling. Als we b nog verder verhogen krijgen we baan met periode 4.



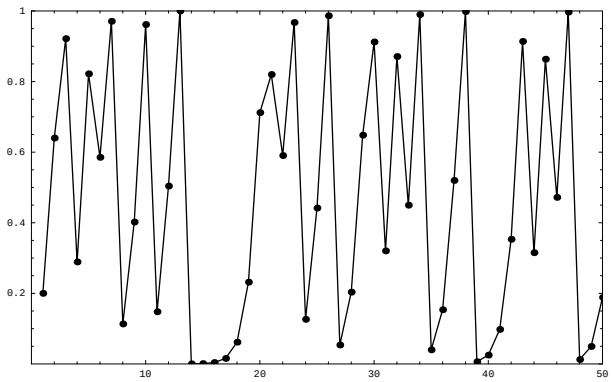
Er zelfs een oneindige cascade. Naarmate we b verhogen krijgen we banen met periode

$$2 \to 4 \to 8 \to 16 \to \ldots$$

Dit verschijnsel heet *periodeverdubbeling*. Hieronder zijn de waarden de periodieke baan als een functie van b in een grafiek uitgezet. Na $b = 3.56994\ldots$ wordt stopt de periodeverdubbeling en vertoont de vergelijking volledig *chaotische gedrag*.



Voor $b > 3.56994$ verlopen de waarden vergelijking grillig. Het verloop kan overigens zeer gevoelig af van de beginvoorwaarde. Hier is een voorbeeld met $b = 4$.



Chaos

We hebben in het voorbeeld van de logistieke vergelijking een goed voorbeeld gezien van een chaotisch systeem. Kort gezegd voldoen chaotische systemen aan de volgende voorwaarden

- Determinisme.
- Gevoeligheid voor beginvoorwaarden.
- Ergodiciteit.

Laten we deze punten kort doorlopen.

Determinisme Chaos is een eigenschap van een deterministisch dynamisch systeem, een systeem dus waar een gegeven begintoestand tot een unieke eindtoestand leidt. Ook al lijkt het verloop grillig en willekeurig, het systeem is zeker niet stochastisch. De positie x_{n+1} wordt met een volledig bepaald algoritme berekend uitgaande van x_n. De meeste natuurlijk voorkomende systemen zijn deterministisch, althans op microscopisch niveau. De aardatmosfeer bijvoorbeeld is deterministisch in theorie. Als we van alle luchtmoleculen de beginposities en snelheden kennen kunnen we in principe met de wetten van de mechanica deze posities een week later berekenen.

Beginvoorwaarden Extreme gevoeligheid voor begincondities is de meest in het oog springende eigenschap van chaos. Twee begintoestanden x en y die 'dicht bij elkaar liggen' leiden na een eindige tijdsevolutie tot toestanden x' en y' die 'ver van elkaar kunnen liggen'. Dit is de bekende slag van de vlindervleugel in Brazilië die het weerpatroon in Nederland beïnvloedt.[2] Een kleine verandering in de beginpositie wordt dus zeer snel vergroot in de tijd. In het algemeen groeit de verandering exponentieel.

Er zijn vele voorbeelden te vinden waarbij extreme gevoeligheid voor begincondities aanwezig is. U kunt denken aan een balletje geplaatst vlakbij de top van de berg. Afhankelijk of het balletje iets naar links of iets naar rechts plaatsen zal het balletje naar links of naar rechts de berg afrollen. De uitkomsten verschillen dus aanzienlijk. Toch willen we in dit geval niet over chaos spreken.

Ergodiciteit Het cruciale extra ingrediënt is *ergodiciteit*. Deze technische eigenschap kunnen informeel als volgt beschrijven. Stel we beginnen in een punt x in de faseruimte. Ergodiciteit wil zeggen dat we na een eindige tijd weer in de buurt van x komen. Dat wil zeggen, voor iedere omgeving $U \subset \Omega$ die x bevat is er een tijd t zodat $x(t)$ weer in U komt.

Complexe systemen

We hebben tot nu toe verschillende soorten gedrag onderscheiden: dekpunten, periodiek, chaos, stochastisch. In al deze processen was in zekere zin sprake van een eenvoudige beweging. Vele processen in de natuur vertonen een veel rijker patroon met structuren op allerlei afmetingen. Denk bijvoorbeeld aan een organisme als een chemisch proces, of de economie als een aaneenschakeling van microscopische handelingen. Hoe moeten dit soort processen goed begrepen worden?

Een eenvoudig model voor dit soort complexe systemen zijn zogenaamde cellulaire automaten. We volstaan hier met een, zeer beroemd voorbeeld, het zogeheten *Game of Life*. Dit spel werd bedacht door de Britse wiskundige John Horton Conway. Het wordt gespeeld op een oneindig schaakbord. De vakjes noemen we *cellen*. Iedere cel heeft acht buren. Een cel kent twee toestanden: levend of dood (vol of leeg). De regels zijn als volgt.

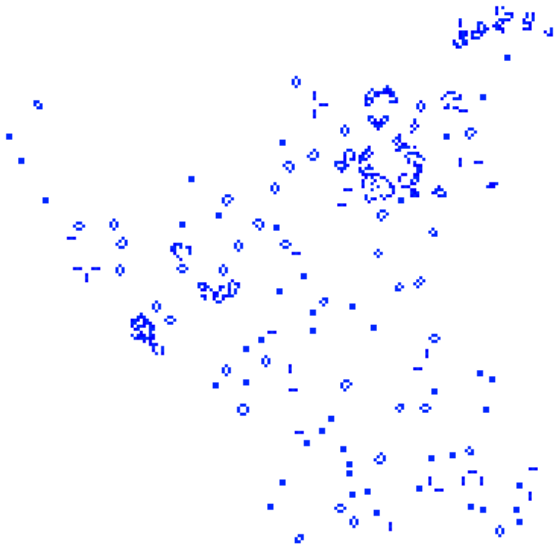
1. Een levende cel sterft als het aantal buren kleiner is dan twee (eenzaamheid) of groter is dan drie (overbevolking).

2. Een dode cel wordt geboren als er precies drie buren zijn (reproductie).

3. Bij precies twee buren blijft een levende cel bestaan.

[2] Inderdaad doet een kleine verplaatsing in de luchtstroom er zo'n zeven dagen over om zich over de aardatmosfeer te verspreiden. Dit is dus een fundamentele beperking in iedere poging om het weer op lange termijn met enige precisie te voorspellen.

Life kan zeer complexe patronen genereren. Het kan zelfs een universele Turingmachine simuleren! Als afsluiting een typische snapshot van krioelend leven volgens de regels van het spel.



P 11.

JOHN CONWAY

1937 —

5.2 Het voorspellen van gedrag

Dynamische systemen beschrijven wat gebeurt op de lange duur, waarbij een systeem met talloze kleine interacties globale regelmatigheden in zijn gedrag kan gaan vertonen. Dit langetermijn gedrag lijkt ver verwijderd van de situatie in de logica waar we redeneringen beschrijven die na een betrekkelijk kort aantal stappen ten einde lopen, of episodes van communicatie die zich binnen een beperkt bestek afspelen. Toch is de laatste tijd de interesse groeiende in langetermijn verschijnselen binnen de logica en taalkunde. Een taal is immers niet alleen een verzameling uitdrukkingen, maar ook een stabiel stelsel van regels en gewoonten door vele generaties gebruikers heen — en hetzelfde zou men kunnen zeggen over redeneren en argumentatie. Eenzelfde interesse in deze langere duur vindt men binnen de informatica. Veel programma's worden gebruikt voor taken die snel moeten aflopen, zoals het uitrekenen van kolommen in een spreadsheet. Maar er zijn ook juist programma's die liefst onbeperkt moeten doorgaan, zoals het operating system van uw computer thuis, of nog belangrijker, die van de Sociale Dienst. Weer gaat het hier om gedrag van systemen met vele actoren over langere tijd.

De stap van de 'logische dynamiek' in het vorige hoofdstuk naar dynamische systemen is dan ook een natuurlijke uitbreiding op vele terreinen van onderzoek. In dit laatste hoofdstuk bespreken we wat er gebeurt wanneer we een overgang maken in perspectief van 'lokaal' naar 'oneindig' bij het voorspellen van gedrag. Heel pregnant is deze thematiek aanwezig in de moderne speltheorie.

Voorspellen van toekomstig gedrag

Redeneren gaat vaak over de toekomst, bijvoorbeeld om een plan te maken voor de dag van morgen, of gewoon om te weten wat onze vooruitzichten zijn. Maar eigenlijk kennen we alleen het verleden, en zelfs dat maar in beperkte mate. Hoe kunnen we op een rationele manier in de toekomst kijken, en voorspellen wat er gaat gebeuren? De logische route van dit college zoekt in dit geval een *dwingende argumentatie*. Bijvoorbeeld, ik kan er vanuit gaan dat mijn tegenspeler iets zal doen omdat hij het beloofd heeft, of omdat het zijn plicht is, of omdat het in zijn eigen beste belang is. Met andere woorden, we zoeken een onontkoombare redenering over de toekomst die tot een zeker gedrag zal leiden. Vaak heeft deze de vorm van een beste beslissing, zoals bij het maximaliseren van verwachtingswaarden door de beslissingstheorie in 3.2, of het kiezen van een Nash evenwichts-strategie door spelers in hoofdstuk 4.1. Met andere woorden, onze redeneringen over onze eigen toekomst mengen statistische verwachtingen over de loop van de natuur met hypothesen over rationeel gedrag van andere personen. Vergelijkbare beschouwingen werken voor de maatschappij als zodanig. Een variant van de logische route is de verklaring die soms wordt gegeven voor het voortbestaan van onze samenleving volgens gedragsregels waaraan iedereen zich blijft houden. Dit is de bekende historische fictie van het 'sociaal contract' die we vinden bij de filosoof Rousseau, ook al de bedenker van het 'haas versus hert' scenario uit 4.1. Ooit zijn onze sociale regels om goede redenen afgesproken en die goede redenen gelden nog steeds. Iedereen die erover nadenkt komt weer op de conclusie uit dat het rechtvaardig is om je aan de regels te houden. Kortom, redelijke redenaties houden ons vast in voorspelbaar gedrag.

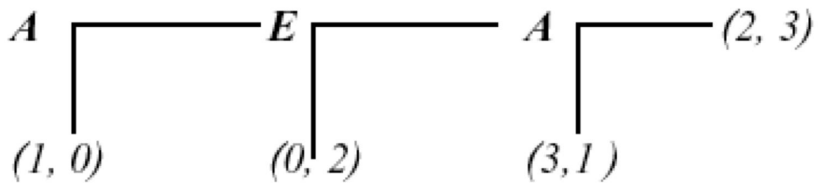
Toch zijn er redenen om te twijfelen aan het realiteitsgehalte van deze analyses. Natuurlijk zijn mensen in staat tot rationeel delibereren, en argumenten spelen een rol in onze visie op de toekomst. Maar het blijft de vraag of we ons steeds rationeel gedragen. We doen vaak maar wat, domweg gedachteloos, of gestuurd door emotie. En zelfs in een laboratoriumsituatie van feitelijke speltheoretische experimenten wordt het 'rationele' Nash evenwicht door proefpersonen vaak niet bereikt. En ook als we dat wel doen, is maar de vraag of we dat gedrag baseren op vernuftige redeneringen over maximalisering en evenwicht, die we misschien niet eens kennen.

Aan de andere kant blijft er het onmiskenbare feit dat menselijk gedrag tot op zekere hoogte voor-

spelbaar is, anders zou onze maatschappij niet kunnen functioneren. Als manier van verklaren van die regelmaat staat tegenover de logische route van herhaalbare dwingende argumenten echter een alternatief, en wel een meer 'blinde' statistische route. Deze kijkt naar herhaalde kleinschalige gedragspatronen die 'vanzelf' regelmaat opleveren, met een globale uitkomst onafhankelijk van bewuste redeneringen, beslissingen, en bedoelingen van individuen. Aldus ontstaat regelmaat in gedrag niet door een redenering die ons telkens weer doet inzien dat dit het beste is, maar zijn het vanzelf ontstaande, blinde hogere-orde eigenschappen van grote verzamelingen handelingen van mensen, opgebouwd uit heel veel eenvoudige basisacties. We komen dan op het wiskundige terrein van de dynamische systemen uit het vorige deel van dit hoofdstuk. In dit laatste deel kijken we naar deze tweede weg van voorspellen van de toekomst, die de laatste tijd steeds meer opgang doet, bijvoorbeeld in de evolutionaire speltheorie, maar ook in de sociale filosofie, en zelfs de taalkunde en cognitiewetenschap. We gaan hiertoe terug naar de speltheorie, en met name de groeiende rol daarin van de wiskundige begrippen waarschijnlijkheid en oneindigheid.

Rationaliteit en problemen daarmee

In ons vorige logische hoofdstuk beschreven we de traditionele wiskundig-logische analyse van spelen. Spelers zoeken een evenwicht tussen strategieën — en mocht het spel onvolledige informatie bevatten, dan pakken ze onderweg zoveel mogelijk informatie op uit afgespeelde kaarten en andere observaties, die helpen om hun situatie nader te begrijpen. Door de tijd heen zien we dan een samenspel van twee logische processen. Het eerste is informatie-update zoals uitgelegd in ons hoofdstuk over kennismodellen, en het tweede is bijhouden van verwachtingen over wat nog gaat gebeuren, bijv. met een analyse van rationeel gedrag voor iedereen in de spelboom vanaf het stadium waar we nu zijn. Maar zulke redeneringen hebben hun beperkingen. Kiest ieder steeds de zet met het meeste gegarandeerde eigen gewin? Een beroemd probleem dat reeds in de vijftiger jaren werd opgemerkt is het *Duizendpootspel*. We tekenen hier voor het gemak een vierpoot:



De regels zijn als volgt. De speler die aan de beurt is kan het spel beëindigen of de beurt overgeven. Als hij eindigt worden de bij die eindtoestand horende waarden uitgekeerd. Na een van te voren bepaald aantal beurtwisselingen moet de beurtspeler eindigen. Hierboven in de figuur staan de horizontale verbindingslijnen voor het overgeven van de beurt. Helemaal rechts. waar A in dit geval de beurtspeler is, geeft de horizontale lijn ook een eindzet aan. De cijfer-paren geven de uitkeringen aan: de linkercoördinaat is de waarde voor A, zeg in Euros. de rechter die voor E.

Het enige Nash evenwicht in dit spel is makkelijk te vinden met achterwaartse inductie op de 'Zermelo-manier' — zelfs al is dit natuurlijk geen nulsom-spel. Vergelijk hiertoe bijvoorbeeld het verkiezingspel uit 4.1. Het blijkt dan te voorspellen dat speler A meteen aan het begin omlaag gaat en het spel beëindigt. U kunt dit makkelijk zelf van rechts naar links beredeneren. Maar dit zou betekenen dat de spelers nooit uitkomen bij de tweede A-beurt rechts, van waaruit *beide* spelers duidelijk beter af zouden zijn dan in (1, 0). Met echte duizendpoten met lange reeksen zetten wordt dit verschil nog

veel dramatischer. Het spel loopt aan het begin af, terwijl beide spelers elk rond de duizend euro hadden kunnen verdienen aan het eind.

In de experimentele speltheorie is veel gekeken naar het werkelijke gedrag van mensen in dit soort spelsituaties. We zien dan wel degelijk eerst bewegen naar rechts, tegen de Nash voorspelling in, en pas 'uitstappen' met een zet naar beneden dicht tegen de rechterkant aan. Overigens is dit niet-Nash gedrag niet zo makkelijk eenduidig te interpreteren. Het kan zijn dat mensen een nutswaarde toekennen aan uitkomsten die niet gelijk is aan de financiële uitbetaling, bijvoorbeeld omdat ze risico's willen belonen die de andere speler heeft genomen om ieder een betere uitkomst te bezorgen ('repaying favours'). Maar ook houden mensen vaak rekening met mogelijke herhalingen van het gegeven spel, waarbij hun gedrag nu latere repercussies heeft ('je moet toch verder met elkaar'). In dat geval moeten de nutswaarden anders berekenend worden, zoals we later zullen zien. Maar hoe dan ook, het blijkt dat simplistische evenwichten niet werken in geobserveerd spelgedrag.

Spelevenwicht als voorspelling

Een strategisch evenwicht in een spel is in wezen een algemene voorspelling. Een strategie beschrijft immers gedrag onder allerlei varianten van spelverloop, afhankelijk van wat de anderen doen. Herhaald gedrag, in plaats van één enkel spelverloop, speelt zelfs nog sterker bij evenwichten met gemengde strategieën zoals in hoofdstuk 4. De standaard interpretatie van gemengde strategieën als het kiezen van zetten afhankelijk van waarschijnlijkheden, bijvoorbeeld door het werpen van een dobbelsteen, lijkt gekunsteld. Zulk gedrag komt in de praktijk zelden of nooit voor. Veel realistischer lijkt een interpretatie als evenwicht op den duur bij herhaling van het gegeven spel. In zo'n langere termijn situatie kunnen we een gemengde strategie als

$$q \cdot A + (1 - q) \cdot B$$

dan op allerlei verschillende manieren lezen. De eerste sluit aan bij de *objectieve waarschijnlijkheid* die we in hoofdstuk 3 tegenkwamen. De coëfficiënten q en $1 - q$ staan dan voor uiteindelijke frequenties van werkelijk gedrag. Maar we kunnen deze getallen ook lezen met *subjectieve waarschijnlijkheden*, als verwachtingen van spelers over elkaars gedrag. En er is zelfs nog een derde interpretatie! De gewichten q en $1 - q$ hoeven helemaal niet te staan voor iets wat een individuele speler doet of gelooft, maar eerder in biologische zin voor *percentages van een stabiele bevolking* waarvan de individuele leden alleen zuivere strategieën spelen! Dit alles is aanleiding eens nader te kijken naar langdurig herhaalde spelen.

Eindig herhaalde spelen

We herhalen eerst de formulering van Prisoner's Dilemma, dat vaak gebruikt wordt om herhaalde spelen te illustreren. Eén enkel spel illustreert een episode van het sociale probleem dat hier aan de orde is: samenwerking in afwezigheid van communicatie. Herhalingen modelleren het langere termijn functioneren van een maatschappij waar individuen telkens weer in dit soort situaties belanden.

	C	D
C	$3, 3$	$0, 5$
D	$5, 0$	$1, 1$

Het enige Nash evenwicht in dit spel was (D, D). Bekijk nu eens een aantal van deze spelen achter elkaar. Alle oude strategieën blijven uiteraard bestaan, in dit geval: ‘

‘speel altijd C”, “speel altijd D”.

Maar in een herhaald spel ontstaan ook nieuwe strategieën — want we kunnen onze keuzen afhankelijk maken van wat de tegenstander in de vorige ronde heeft gedaan, net als in de meer gedetailleerde spelbomen van 4.1. Een bekend voorbeeld is de strategie

> *Lik op Stuk* (LoS)
>
> Begin met C. Speel C als de tegenstander in de vorige ronde C heeft gespeeld, maar speel D als hij daar D heeft gespeeld.

Dit begint vriendelijk, maar straft tegenwerking meteen af in de volgende ronde — en vergeeft ook weer na een ronde. Toch helpt dit niet meteen:

> *Feit* (D, D) is het enige Nash evenwicht in een herhaald Prisoner’s Dilemma.

De reden is weer een Zermelo-analyse van de spelboom met achterwaartse inductie. In de op één na laatste ronde is de situatie der spelers net als in het enkele spel en dus spelen ze het evenwicht (D, D). Maar dat begrijpen ze de ronde daarvoor al, dus kunnen ze daar net zo goed maar (D, D) spelen. En zo terugwerkend zien we dat steeds (D, D) wordt gespeeld. Het precieze bewijs is overigens iets ingewikkelder, maar dit geeft wel het idee.

Oneindig herhaalde spelen

Deze situatie verandert drastisch als we een oneindige herhaling toestaan van het spel. We moeten dan wel een betekenis geven aan uitkomsten in zo’n situatie: oneindige uitbetalingen zijn immers niet zinvol. We gebruiken voor dit doel de manier waarop men in de financiële wereld oneindige geldstromen *verdisconteert*. We kiezen een disconto-factor r tussen 0 en 1, en definiëren de uitkomst voor een speler van oneindige rij spelen als volgt:

$$\sum_{i=1}^{\infty} r^i \cdot u_i \quad \text{met } u_i \text{ de uitkomst in het } i\text{-de spel.}$$

Een andere mogelijke lezing voor de discontofactor r is als de kans dat je weer zo’n spel zal spelen. Dan geeft de macht r^i de kans dat je aan het i-de spel toekomt.

Voorbeeld Oneindig Prisoner’s Dilemma met $r = 3/4$.

Hier is een aantal soorten gedrag. Spelers die D tegen elkaar spelen krijgen beide:

$$\sum_i (3/4)^i \cdot 1 = \frac{1}{1 - 3/4} \cdot 1 = 4$$

Steeds C spelen geeft aan beide spelers:

$$\sum_i (3/4)^i \cdot 3 = 12$$

Een speler die tegen LoS, de speler die consequent het ‘lik-op-stuk’-stramien volgt, altijd D speelt:

$$5 + (3/4) \cdot 4 = 8$$

Een speler tegen LoS met één keer D en daarna C:

$$5 + 0 + (3/4)^2 \cdot 12 = 11\frac{3}{4}$$

Een speler tegen LoS met D, C, D, C,...:

$$\sum_i (9/16)^i \cdot 5 = \frac{1}{1 - 9/16} \cdot 5 = 11\frac{3}{7}$$

Spelers met LoS tegen elkaar krijgen natuurlijk hetzelfde als eeuwige C-spelers, namelijk 12. Maar iets anders dan LoS tegen LoS geeft net niet 12!

Achter deze observaties steekt een al eerder genoemd algemeen feit. Oneindige spelen hebben veel meer strategische evenwichten dan eindig herhaalde! Enerzijds blijven de oude evenwichten uit het enkele spel op een voor de hand liggende wijze bewaard. Zo is (D, D) nog steeds een Nash evenwicht. Maar ook geldt:

Feit

$(\mathrm{LoS}, \mathrm{LoS})$ is een Nash evenwicht in oneindig Prisoner's Dilemma.

We geven alleen een schets van het bewijs. Afwijken verbetert je uitkomst van 12 niet tegen een LoS tegenstander. Je wint 5 bij je eerste keer D waar LoS nog C speelt, maar of je keert eens terug naar C, en verliest dan 5, en we staan weer op gelijke voet — of je blijft D spelen, en krijgt totaal minder dan als je steeds C had gespeeld. Het precieze wiskundige argument is iets ingewikkelder. Bovendien hangen dit soort berekeningen natuurlijk af van de getallen in de matrix en de disconto-factor r.

Wel is het zo dat er heel erg veel Nash evenwichten zijn in oneindige spelen. De zogenaamde 'folk theorems' van de speltheorie zeggen bijvoorbeeld voor ons oneindig Prisoner's Dilemma dat elk paar numerieke uitkomsten in de verzameling

$$\{(x, y) \mid x, y \in \mathbb{Q}, x \geq 1, y \geq 1, x + y \leq 5\}$$

een mogelijke uitkomst van een of ander Nash-evenwicht is. [3] In de speltheorie is dus veel gezocht naar restricties op zinvolle strategieën die in deze grote ruimte meer voor de hand liggende gedragsvormen scheiden van meer buitenissige. [4]

Lik op Stuk: how the good guys win?

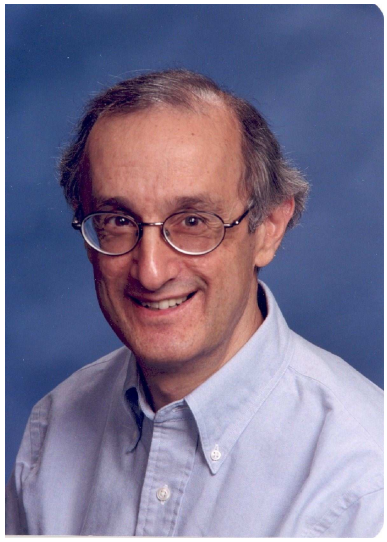
De strategie Lik-op-Stuk is beroemd geworden door een boek van Robert Axelrod uit 1984, 'The Evolution of Cooperation' (Pelican books, Harmondsworth) waarin lange termijn gedrag in maatschappijen wiskundig wordt geanalyseerd. Axelrod's titel verwoordt een ruimere ambitie van voorspellen. Het Nash-evenwicht zegt alleen maar dat LoS, indien eenmaal aanwezig, een zekere stabiliteit heeft. Samenwerking loont! Maar het zegt niet dat LoS ook in een groep zal *ontstaan*. Immers, het 'slechte' gedrag D was ook in evenwicht met zichzelf. Toch zijn er wel praktische aanwijzingen dat samenwerking een goede kans heeft op ontstaan. Om dit te demonstreren organiseerde Axelrod een toernooi

[3] Deze evenwichten in een oneindig spel hebben vaak nog wel iets te maken met het eenmalige spel. Ze correleren met zogenaamde 'afdwingbare' strategie-paren, die je tot evenwicht kunt maken in het eenmalige geval door afspraken of door manipulatie van de uitkomsten met boetes, c.q. straffen.

[4] Één bekend soort restrictie gaat uit van 'beperkte rationaliteit'. Dat wil zeggen dat we aannemen dat een strategie computationeel eenvoudig moet zijn, zonder excessief geheugengebruik en buitenissige instructies voor handelen.

tussen concurrerende computerprogramma's, ingezonden vanuit de hele wereld, die herhaald Prisoner's Dilemma tegen elkaar speelden. LoS ('Tit for Tat' in het Engels) won op den duur tegen alle andere programma's in een volledige competitie waarin alle deelnemers een keer tegen elkaar speelden.

P 12.



ROBERT AXELROD

Een precieze verklaring van deze hoopgevende uitkomst is niet gemakkelijk. Axelrod suggereert twee dingen, zonder ze helemaal precies te bewijzen. LoS, eenmaal aanwezig, is stabiel tegen invasie door anderen, en nog sterker: samenwerking heeft ook meer kans op ontstaan in een bevolking dan tegenwerking. Deze laatste bewering is echter omstreden.

We geven een voorbeeld van Axelrod's redenering over 'invasies', die hij ontleende aan het bekende werk van de bioloog Maynard-Smith over 'evolutionaire stabiliteit' van populaties:

Feit

Een bevolking die alleen LoS speelt kan niet worden geïnfiltreerd door een groepje slechteriken dat D speelt.

Bewijs De indringers kunnen zich niet handhaven, op grond van onze eerdere berekeningen. Ze krijgen namelijk gemiddeld 4 onderling, en in ontmoeting met een 'inboorling' 8. Een inboorling met een soortgenoot krijgt 12, met een slechterik 3. Nu berekenen we heel eenvoudig de kansen op zulke ontmoetingen, en daarmee weer een verwachte waarde voor beide soorten gedrag. Bijvoorbeeld bij 10% indringers zijn de verwachte waarden:

inboorling		indringer
$9/10 \cdot 12 + 1/10 \cdot 3 = 11.1$	$>$	$9/10 \cdot 8 + 1/10 \cdot 4 = 7.6$

De inboorlingen zijn dus beter af, en de indringers sterven uit.

Feit

Een niet-samenwerkende bevolking met D kan wel worden geïnfiltreerd door 'LoS-goedzakken'.

Bewijs De indringers kunnen zich dank zij een verkregen voordeel uitbreiden, mits ze in voldoende getale zijn, en samenwerking genoeg meerwaarde geeft in het spel. Bijvoorbeeld, met 25% indringers krijgen we de volgende verwachte waarden:

inboorling		indringer
$3/4 \cdot 4 + 1/4 \cdot 8 = 5$	$<$	$3/4 \cdot 3 + 1/4 \cdot 12 = 51/4$

Wat deze wiskundige gedachte-experimenten zeggen over feitelijk gedrag is voor discussie vatbaar. Zo zijn de uitkomsten sterk afhankelijk van de nutswaarden in de spelmatrix, de gekozen discontofactor, en groepspercentages voor de indringers. Aan de andere kant gaat het doorgaans alleen om kwalitatieve voorspellingen over gedrag op de lange termijn. Die kunnen we technisch vaak al aflezen uit de manier waarop de genoemde relevante variabelen in de bovenstaande formules voorkomen. We illustreren hoe dit werkt voor het beschreven geval.

Evolutionaire stabiliteit

Het volgende scenario om gedrag te analyseren komt uit de evolutionaire biologie. Stel dat 'mutanten' binnenkomen die strategie F spelen tegen een bevolking die in evenwicht strategie G speelt. Stel de kans dat een mutant een andere mutant tegenkomt op ϵ. Hier is de verwachte waarde van een ontmoeting voor een mutant:

$\epsilon \cdot u(G,G)$	$+$	$(1-\epsilon) \cdot u(G,F)$
mutant, mutant		*mutant, normaal*

Voor de oude bevolking ligt dit symmetrisch:

$$\textit{Normaal} \quad \epsilon \cdot u(F,G) + (1-\epsilon) \cdot u(F,F)$$

Evolutionaire stabiliteit van G eist nu de volgende betrekking:

$$\textit{Mutant} < \textit{Normaal} \text{ voor elke strategie } F \neq G$$

Deze eis is een versterking van het Nash evenwicht uit het vorige hoofdstuk— en de volgende herbeschrijving is makkelijk te bewijzen:

Feit

G is evolutionair stabiel dan en slechts dan als de volgende twee condities gelden:

(a) (G,G) is een Nash evenwicht, en

(b) als $u(G,G) = u(F,G)$ dan $u(F,F) < U(G,F)$

Spelen waar deze versterking er toe doet zijn makkelijk te vinden. In het oneindig herhaalde Prisoner's Dilemma was (D,D) wel een Nash evenwicht, maar het is niet evolutionair stabiel. LoS is dat overigens evenmin: een succesvolle invasie door 'altijd-C'-spelers volgens het bovenstaande scenario is wel degelijk mogelijk: maar wat betreft het observeerbaar gedrag maakt dat niet uit. Invasies door mutanten zijn een geliefkoosd scenario van speltheoretici in de uitleg van stabiel gedrag in allerlei situaties, en er bestaan mooie stellingen over evolutionair stabiele coöperatieve evenwichten.

Spelen als dynamische systemen

Maar gaandeweg is in de speltheorie een iets andere, zij het verwante, wiskundige kijk op herhaalde spelen opgekomen, meer in de lijn van het vorige hoofdstuk. We nemen daarbij aan dat spelers in een bevolking strategieën hebben die vaststaan: er wordt niet gereageerd op wat in eerdere ontmoetingen is gebeurd. Geen LoS-ers dus! Denk bijvoorbeeld aan genetisch bepaald gedrag, dat van te voren is ingebouwd: je bent of een slechterik of een goedzak. De dynamiek zit dan niet in adaptief gedrag door individuen die kunnen leren van ervaring en anticiperen op nieuwe spelen, maar in percentages van de bevolking met biologische genen voor de diverse strategieën. We illustreren deze zogenaamde *replicator-dynamiek* van een populatie voor een bekend spel dat ontmoetingen beschrijft tussen agressieve en niet-agressieve dieren, of mensen:

	Duif	Havik
Duif	$1, 1$	$0, 2$
Havik	$2, 0$	$-1, -1$

Op de manier van het vorige hoofdstuk is makkelijk uit te rekenen dat er hier twee zuivere Nash evenwichten zijn en één gemengd:

(Duif, Havik) (Havik, Duif) (50/50 Duif/Havik, 50/50 Duif/Havik)

Interpreteer nu de uitkomsten in de spelmatrix niet economisch als nutswaarde, maar biologisch als *extra fitness*. Stel in de bevolking van Duiven en Haviken een p-deel Havik is, en $1 - p$ Duiven. Een Duif verwerft in een ronde van het spel dan gemiddeld als extra fitness:

$$f_D(p) = (1 - p) \cdot 1 + p \cdot 0 = 1 - p$$

Een Havik krijgt gemiddeld als extra fitness:

$$f_H(p) = (1 - p) \cdot 2 + p \cdot (-1) = 2 - 3p$$

De gemiddelde fitness winst f_{gem} berekenen we dan als volgt:

$$p \cdot f_H(p) + (1 - p) \cdot f_D(p) = 1 - 2p^2$$

Het systeem wordt nu 'aangedreven' door de volgende *replicator-vergelijking* voor de verandering van het percentage $p(t)$ als functie van de tijd:

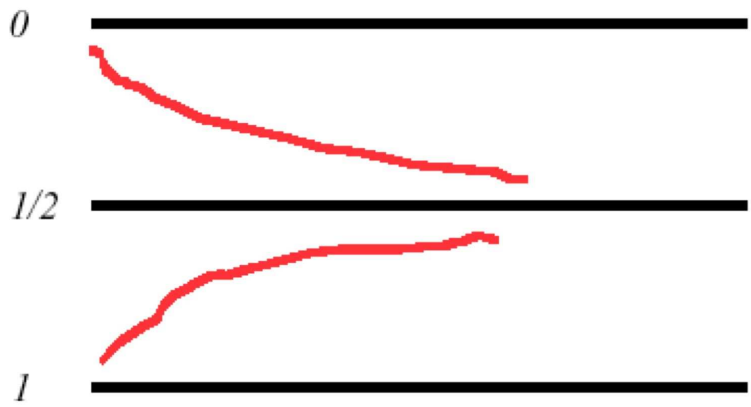
$$dp/dt = p \cdot (f_H(p) - f_{\text{gem}})$$

Voor het Havik/Duif spel luidt deze differentiaalvergelijking als volgt:

$$p' = p \cdot (2p^2 - 3p + 1) = p \cdot (p - 1) \cdot (2p - 1)$$

Merk op dat we nu zijn overgeschakeld van discrete matrices op een systeembeschrijving met 'continue wiskunde': differentiaalvergelijkingen en continue functies door de tijd heen. Met heel grote aantallen herhaalde spelen is dit een verantwoorde abstractie.

Het resulterende dynamische systeem gedraagt zich als volgt:



Er zijn hier drie rustpunten $p = 0$, $p = 1$, $p = 1/2$. Maar er vindt asymptotische convergentie plaats naar $p = 1/2$! De lange termijn voorspelling is dus dat de bevolking zich qua percentages instelt op de gemengde evenwichtsstrategie '50/50 Duif/Havik'. Dit is een algemeen verschijnsel. Populaties convergeren naar Nash evenwichten uit het enkele spel, eventueel naar gemengde strategieën.

Het gedrag van zo'n dynamisch systeem hangt uiteraard af van het type 'basisontmoeting'. Zo levert eenzelfde analyse voor Prisoner's Dilemma het volgende. Met onze eerdere matrixwaarden wordt de replicator vergelijking

$$p' = p \cdot (p - 2) \cdot (p - 1)$$

en er vindt asymptotische convergentie plaats naar $p = 1$: de D's winnen in dat geval, dat wil zeggen, de bad guys! Met meer complexe scenario's voor een dynamisch systeem kunnen ook gemengde populaties voorkomen, inclusief good guys - maar het ontstaan van samenwerking lijkt ook biologisch geen vanzelfsprekendheid. De discussie over het ontstaan van sociale samenwerking gaat dan ook nog steeds met verve voort.

We kunnen overigens de algemene replicator-formule als volgt schrijven:

$$p' = p \cdot (1 - p) \cdot (p \cdot (u_{H,H} - u_{D,H}) + (1 - p) \cdot (u_{H,D} - u_{D,D}))$$

Voorspellingen voor specifieke spelen zijn dan direct afleesbaar uit hun spel-matrix. Met name vertoont dit schema geen continuïteit. Kleine verschillen in begincondities kunnen beslissend zijn voor het soort dynamisch systeem dat ontstaat. Van de bestaande wiskundige analyse op dit gebied vermelden we alleen het volgende

> *Feit* In eenstaps 2-persoon spelen zijn de asymptotische attractoren in de replicator dynamiek juist de de symmetrische evolutionair stabiele strategieën.

Axelrod's eerder genoemde computer-toernooi past overigens goed binnen deze biologische aanpak met dynamische systemen. Na elke ronde paste hij de percentages kopieën van de mededingende programma's aan op grond van hun scores tot nu toe, hetgeen neerkomt op een populatiedynamica met verschillende mengsels. De jongste stand van zaken op dit gebied is te vinden in zijn boek uit 1997 met als titel 'The complexity of cooperation'. Om toch maar tot de conclusie te komen dat samenwerking wel degelijk ontstaat komen daar nog andere mechanismen de dynamiek beïnvloeden, zoals *leermethoden* die op den duur de genetische aanleg kunnen overstemmen. Kortom, de variatie in wiskundige methodiek weerspiegelt zo'n beetje alle posities die men cognitiewetenschappelijk, of zelfs politiek, zou kunnen innemen.

Oneindige spelen in de informatica

Oneindige spelen komen ook voor in andere gebieden. Zo bestuderen informatici computer systemen die oneindig moeten doorgaan. Er bestaat dan evenzeer een terrein van logische studie van oneindige rekenprocessen, waarbij gestreefd wordt naar een gegarandeerd verloop van gebeurtenissen dat voldoet aan gewenste eigenschappen, zoals het correct afhandelen van elk binnenkomend verzoek. Moderne rekensystemen bestaan uit vele parallelle samenwerkende procesoren, en daarom zijn deze ook vaak op te vatten als oneindige spelen. Vandaar dat speltheorie, zowel klassiek als evolutionair, momenteel ook binnendringt in de informatica. Sommige informatici menen zelfs dat heel complexe computersystemen alleen nog maar als dynamische systemen te begrijpen zijn, met emergent gedrag dat ver af kan staan van wat ontwerpers van de componenten voor ogen hadden.

Spelen in taal

Speltheoretische scenario's als de bovenstaande komen ook voor in de studie van natuurlijke taal. Zo kan men het kiezen van een formulering door een spreker, en het kiezen van een bijbehorende interpretatie van wat wordt gezegd door de hoorder, begrijpen als een tweepersoons spel. De spreker zegt iets, maar houdt rekening met hoe de luisteraar het gaat opvatten. De luisteraar interpreteert wat de spreker zegt, maar houdt rekening met het feit dat de spreker zich tot hem richt, enzovoorts. Het gaat in dergelijke conversatiespelen dan weer om strategische evenwichten die stabiele betekenissen en communicatie garanderen. Evolutionaire speltheorie wordt in dit verband met name gebruikt om het ontstaan en voortbestaan van algemene taalregels te verklaren. Voorbeelden zijn het principe dat frequente betekenissen korte woorden hebben, of de regel dat we antwoorden op een vraag begrijpen als precies de juiste informatie voor de doeleinden van de vraagsteller. In de dialoog

> "Wie komen vanavond?" "Jan en Marie!"

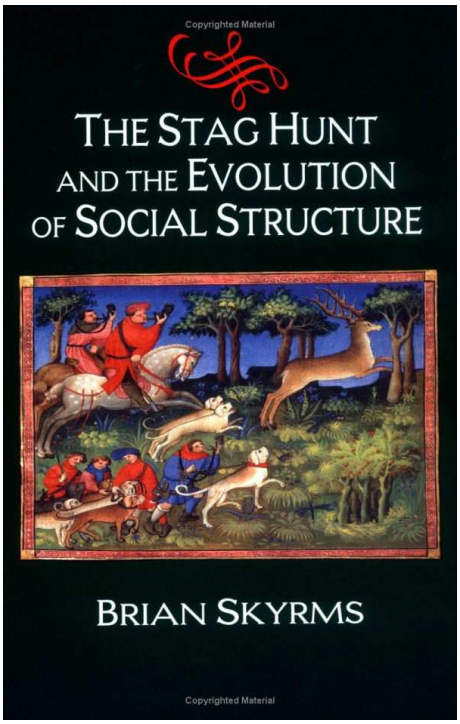
zult u het antwoord lezen als "Jan en Marie zijn de enige die komen". Dit is weer een voorbeeld van een coperatief evenwicht, en taalkundigen zouden graag weten waarom deze gedragsvorm is ontstaan, en stabiel werkzaam blijft. Ook bekende economen wagen zich aan de analyse van taal, en zelfs logica. Ariel Rubinstein's boek 'Economics and Language' uit 2000 past het eerdere mutanten-scenario toe op natuurlijke taal. De stabiliteit van betekenissen en gesprekconventies zou hierin liggen dat groepen met afwijkende taalgebruik het op den duur afleggen tegen de bestaande versies. Evenzo analyseert hij argumentatiegewoonten als speciale speltheoretische evenwichten.

Discussie

Voorspellen of verklaren van toekomstig gedrag is kennelijk mogelijk met oneindig herhaalde spelen en dynamische systemen. Niettemin blijven veel van deze analyses speculatief. Uitkomsten hangen sterk af van het gekozen model en de aannamen bij het begin. Ook is het goed mogelijk dat wezenlijke aspecten van sociale interactie tot nu toe buiten de wiskundige modellering zijn gebleven. Bijvoorbeeld, 'goodies' overleven soms niet qua strikte evolutionaire stabiliteit, maar wel in een geschikte geografische of sociale structuur. Deze structuur kan ervoor zorgen dat ze aanvankelijk een grotere kans hebben aan het begin om elkaar te ontmoeten dan de bevolkingspercentages in onze eerdere formules aangeven, bijvoorbeeld door hun ongelijke distributie over het totale territorium. Ook vastberaden indringers in een populatie werken vaak op die manier, door 'klitten'.

Ook zegt de bovenstaande theorie niets over het *leren* van nieuwe strategieën op grond van ervaring, of het ontstaan van een sociale *hiërarchie* die interacties beïnvloedt, en daarmee juist weer tot gedragsveranderingen kan leiden. Dergelijke scenario's zijn vaak nog te ingewikkeld voor analytische

oplossingen als dynamisch systeem. Er wordt daarom veel geëxperimenteerd met computersimulaties van zulke rijkere beschrijvingen. Een mooi voorbeeld is recente boek ‘The Stag Hunt: Evolution of Social Structure’ (2002) van de filosoof Brian Skyrms, dat allerlei varianten van Rousseau’s ‘Haas versus Hert’ in simulatie gebruikt voor een studie van het ontstaan van sociale normen en hiërarchiën.



De keuze tussen meer logische en meer statistische modellen in gedrag weerspiegelt een mogelijke meer algemene wisseling van perspectief in sociale en zelfs morele kwesties. In dat laatste geval gaat het om een tegenstelling tussen bewuste moraliteit, op grond van principes of ons geweten, versus blinde, in grote aantallen vanzelf ontstaande gedragspatronen. Veel mensen vinden de gedachte stuitend dat veel van wat wij als ‘goed’ beschouwen wel eens een statistisch systeem-effect zou kunnen zijn, in plaats van een goed beredeneerde keuze. Maar vruchtbaarder lijkt eerder de *relatie* tussen logische en statistische modellen van gedrag. De eerste kijken naar individuele beslissingen en redeneringen, de tweede naar het totale effect van heel veel, wellicht buitengewoon simpele individuele stappen. Er is een vloeiende overgang van het een naar het ander. Het geheim dat ik u nu vertel is inhoudelijk, welbewust, en ’logisch’. Maar als het gerucht nu langdurig gaat rondzingen, dan wordt statistiek van belang. Een aardig voorbeeld van dat laatste is Kees Mouwen’s zuiver natuurkundige model voor meningsverandering in ‘The Dynamics of Opinion Change’, 1998, Tilburg University Press. En inderdaad, als we kijken naar publieke opinie op grote schaal, dan lijkt de inhoud van communicatie van minder belang dan puur statistische mechanismen van voortplanting van een bewering. Maar nogmaals, de logische en de statistische zienswijze kunnen uitstekend samenleven. Zo zijn er tegenwoordig interessante modellen voor cognitief gedrag die ons gewone taalgebruik, maar ook onze wiskundige bewijsvermogens, beschrijven als een mengsel van twee activiteiten: patroonherkenning in een geheugen vol eerder meegemaakte gevallen, en logisch afleiden via een regelsysteem dat wordt aangeroepen als patroonherkenning niet volstaat.

Deel III

Wiskunde over wiskunde

Hoofdstuk 6

Bewijzen

6.1 Bewijzen

Wiskunde gebruikt een precisie in redeneringen die bij weinig andere menselijke activiteiten gevonden wordt. Eén van de rode draden in onze beschouwingen is de vraag waar en wanneer zo'n exacte redeneertrant wenselijk of noodzakelijk is. Deze precisie culmineert in het wiskundige bewijs.

Wat is een bewijs, hoe vind je een bewijs, en waarvoor dient het? Deze vragen raken aan de kern van de vraag wat wiskunde is, en we komen daarmee aan een gevoelig punt voor vele wiskundigen. Sommigen zien het als het enige wezenlijke van de wiskunde, de arbiter van wat wel en wat niet tot de wiskunde gerekend moet worden: de scheiding van de mannen van de jongens. Anderen beweren juist dat de relatie van bewijzen tot de wiskunde is als die van de spelling tot de poëzie. Vanuit dit gezichtspunt ligt de uiteindelijke kracht van de wiskunde juist lin de verbeelding en creativiteit die voorafgaat aan het uiteindelijke bewijs. Een bewijs is dan slechts de laatste, evenwel noodzakelijke, stap in het precies maken en het overbrengen van de intuïtie.

Eén ding is duidelijk, er is geen ander wetenschapsgebied waar het 'harde bewijs' zo'n belangrijke rol speelt. Van de juridische tot de natuurwetenschappelijke wereld, nergens zal een redenering werkelijk honderd procent waterdicht hoeven te zijn, nergens is een bewijs zo absoluut. De zekerheid waarmee we weten dat er geen oplossing van louter positieve gehele getallen van de vergelijking $x^3 + y^3 = z^3$ is van een geheel andere orde dan de zekerheid die we bijvoorbeeld hebben dat een proton een stabiel deeltje is, of dat vogels van dinosauriërs afstammen.

In dit hoofdstuk zullen we aan de hand van eenvoudige voorbeelden proberen te illustreren hoe bewijzen werken in de praktijk, en wat zo al de verschillende stijlvormen zijn die door de jaren ontwikkeld zijn. In het volgende hoofdstukdeel 6.2 zal dieper worden ingegaan op de formele structuren achter de bewijsvoering. Vergelijk het met een verhandeling over muziek. In dit deel laten we wat muziekstukken en frases horen, terwijl in het volgende hoofdstuk de compositieleer wordt behandeld.

Wiskunde versus mens en natuur

Het geven van een wiskundig bewijs is in de eerste plaats een typisch menselijke handeling.[1] Via logische redeneringen lopen we een pad van gevolgtrekkingen af om uiteindelijk bij de conclusie aan te komen. Daar beleven we het 'aha' of 'eureka' gevoel, de moeilijk te beschrijven emotie die we ondergaan als het laatste puzzelstukje op zijn plaats valt en het patroon zichtbaar wordt. We hebben het gevoel dat ergens iets in ons brein 'klik' zegt en het spreekwoordelijke lampje gaat branden. Er gaat een schakelaar over in ons neurale stelsel en ineens 'zien' we dat de bewering waar is.

Een bewijs is daarmee een 'alles of niets' proces. Of de redenering is correct, óf deze is niet correct, er is geen middenweg. In het eerste geval hebben we een universele waarheid gevonden, die hier en nu waar is, maar ook in de Andromedanevel en ook nog over een biljoen jaar. Daarbij doet het er niet toe hoe we aan de overkant zijn gekomen, misschien kan het eleganter, korter, dieper, maar het resultaat is er en blijft voor altijd staan. Daarentegen, als de redenering niet klopt is het resultaat absoluut nihil. We staan met lege handen. De bewering kan nog steeds goed of fout zijn. We weten het eenvoudig niet.

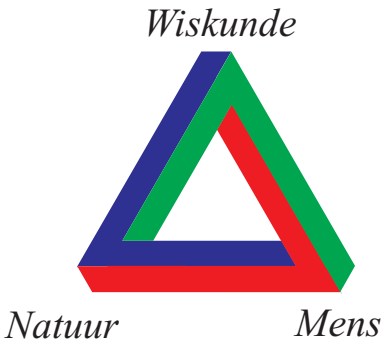
Dit is natuurlijk wel heel erg grof gesteld. Een mislukt bewijs is zelden tevergeefs. We kunnen veel leren van onze fouten. Onderweg kunnen we een goed beeld gekregen hebben van de context en meer inspiratie opgedaan hebben voor een nieuwe poging. Maar toch, het blijft natuurlijk een troostprijs.

[1] In 6.2 zullen we zien hoe bewijsmethoden zover geformaliseerd kunnen worden zodat ze in principe ook door een computer uitgevoerd kunnen worden. Dit levert vaak, juist door de formele precisie waarmee machines aangestuurd moeten worden, zeer steriele bewijzen waarvan het heel veel moeite kost om het nog als bewijs te herkennen. Het vereist dan meestal toch weer heel veel 'mensenwerk' om het tot een verteerbaar bewijs te transformeren.

Een bewijs kan uiteindelijk niet voor 99% correct zijn. Als er een klein foutje in is geslopen, een detail is overzien, dan stort het bouwwerk volledig in. Iemand die een bewijs wil leveren gaat altijd voor goud. Er zijn geen andere medailles te verdienen.

Dit laatste overkwam de Engelse wiskundige Andrew Wiles die, na zeven jaar kluizenaarsarbeid, uiteindelijk zijn bewijs van de Laatste Stelling van Fermat (waarover later meer) wereldkundig maakte. Uiteindelijk bleek één van de vele stappen niet correct bewezen te zijn en moest hij, onder het ongedurig oog van zijn collega's die allen popelden om zelf de laatste en beslissende slag te slaan, helemaal terug naar af en in wezen een volledig nieuw bewijs uit zijn tenen trekken. Dat is hem uiteindelijk gelukt, maar in de tussentijd had iemand anders de missende stap in het oude bewijs kunnen afmaken. Wie had dan de stelling van Fermat bewezen?

Het 'klik' gevoel dat zo bepalend is voor onze ervaring van een bewijs, raakt aan de merkwaardige relatie tussen de drie hoofdrolspelers in dit boek: de wiskunde, de natuur en de mens (geest, cognitie). Hierbij past een mooi beeld dat bedacht werd door de Britse mathematisch fysicus Roger Penrose. Penrose heeft een imposante staat van dienst. Hij is onder andere in samenwerking met Stephen Hawking verantwoordelijk voor vele diepe resultaten over het bestaan van singulariteiten (zoals de *big bang* en zwarte gaten) in Einsteins algemene relativiteitstheorie. Verder is hij de bedenker van een aantal bekende onmogelijke figuren. Nadat hij in 1954 op het Amsterdamse internationale wiskundig congres kennis had gemaakt met de Nederlandse graficus Maurits Escher en zijn werk, publiceerde hij met zijn vader, de bekende geneticus Lionel Penrose, een artikel over de onmogelijke driehoek, die uiteindelijk door Escher weer in vele vormen beroemd gemaakt zou worden. We gebruiken hem hier om het thema van ons boek te illustreren.



Deze driehoek staat symbolisch voor de cyclische relatie tussen de drie ingrediënten van dit boek: mens (cognitie), natuur en wiskunde. Laten we de driehoek met de klok mee aflopen, te beginnen met de top.

Wiskunde is bedacht door mensen. Wiskundige formules zijn hersenspinsels. De definities en bewijzen worden gegeven door wiskundigen. Wiskunde is het kennisgebied dat door wiskundigen wordt uitgebreid. Daarmee is de wiskunde een onderdeel van het totaal van cognitieve processen dat de mens kan ondernemen. Maar de mens op zijn beurt is een onderdeel van de natuur. Wij zijn zeer complexe fysische en chemische systemen. Onze gedachten zijn 'slechts' *Phosphorreactionen*. Ons brein vormt een onderdeel van de overkoepelende natuur, het geheel van alle processen die in onze fysische werkelijkheid afspelen. En daarmee is de wiskunde ook een onderdeel van de natuur geworden. Daarmee zijn we twee zijden van de driehoek afgelopen. Laten we nu de laatste afleggen.

Tot onze verbazing kunnen de natuurwetten, die de complexe reacties waaruit onze denkprocessen bestaan beschrijven, zelf weer met akelige precisie beschreven worden met wiskundige formules. Dit inzicht werd mooi verwoord door Galileo Galilei, die zei dat het boek van de natuur geschreven is in de taal van de wiskunde. Dezelfde natuur, die de mens en daarmee de wiskunde bevat, is zelf

slechts een onderdeel van de wiskunde! Maar de wiskunde omvat op haar beurt veel meer dan alleen onze werkelijkheid. We kunnen ons ook andere, wiskundig consistente, realiteiten voorstellen, met meer of minder dimensies bijvoorbeeld of met andere getalsystemen. Onze wereld, de natuur, is dus slechts één van de vele imaginaire werelden die de wiskunde bevat. Deze vreemde kringloop wordt symbolisch weergegeven door Eschers onmogelijke trap, die hij geïnspireerd door het werk van vader en zoon Penrose, later maakte

Het Boek van Erdös

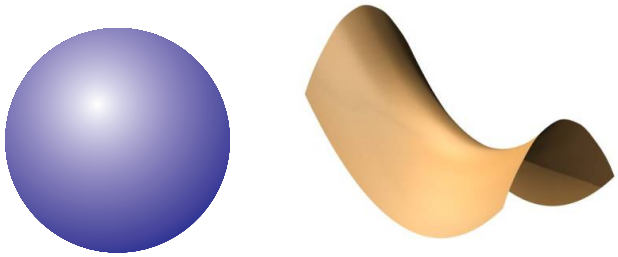
Er is voor wiskundigen ook een belangrijk esthetisch aspect aan een bewijs. De legendarische wiskundige Paul Erdös (1913–1996) hield zich graag voor dat er ergens het Boek is, waarin van ieder probleem het ultieme, elegantste bewijs wordt opgeschreven en bijgehouden. Vele wiskundige ervaren het vinden van zo'n bewijs dan ook als een ontdekking veeleer dan een uitvinding. Alsof weer een pagina van het Boek is blootgelegd.

Leren van negatieve resultaten

Ook al is het vinden van een bewijs voor een groot openstaand probleem een hoog ideaal, in de geschiedenis zien we ook vele voorbeelden waar het *niet* vinden van een bewijs uiteindelijk een belangrijke ontwikkeling heeft geleid. In 2.1 noemden we al hoe de onmogelijkheid van het vinden van een oplossing van de algemene vijfdegraads vergelijking via Abel en Galois tot de geboorte van de groepentheorie heeft geleid.

Een andere belangrijke open vraag in die tijd (begin 19de eeuw) was of het zogenaamde parallellenpostulaat van Euclides — de uitspraak dat door een punt dat niet op een lijn ligt precies een lijn gaat die de eerste lijn niet snijdt — volgt uit de vier andere postulaten van de Euclidische meetkunde. Men dacht eerst van wél, en er waren zelfs, later natuurlijk verworpen, bewijzen gegeven. Gauss probeerde ook al op vroege leeftijd een bewijs te leveren en kwam mede met zijn Hongaarse college Farkas Bolyai tot het inzicht dat er een meetkunde denkbaar moest zijn die aan de vier overige postulaten voldeed maar waar het parallellenpostulaat niet opgaat. In Rusland ontwikkelt tegelijkertijd Nicolai Lobatsjevski een niet-Euclidische meetkunde waarin het parallellenpostulaat vervangen wordt

door een variant. Rond 1870 geeft de Italiaanse wiskundige Eugenio Beltrami uiteindelijk een concreet voorbeeld van een meetkundig stelsel dat zich gedraagt volgens Lobatsjevski's postulaat maar dat niet gehoorzaamt aan het vijfde postulaat van Euclides.[2] Een nieuwe wereld ging open, en een hele nieuwe tak van de wiskunde was daarmee geboren.



Een tweede belangrijk voorbeeld in de ontwikkeling van de wiskunde was de paradox van Bertrand Russell (begin 20ste eeuw), vaak ook bekend als de kappersparadox:

> *In een stad wordt iedere man geschoren door de kapper tenzij hij zichzelf scheert. Wie scheert de kapper?*

Iedereen die door de kapper wordt geschoren scheert dus niet zichzelf, en iedereen die zichzelf scheert wordt niet door de kapper geschoren. Dit plaats de kapper in een onmogelijke situatie.

Russell beschouwde trouwens meer abstract de verzameling V van alle verzamelingen.[3] Dit is een vreemde verzameling, omdat V een element is van V zelf

$$V \in V.$$

Een toendertijd gehanteerde axiomatisering van de verzamelingenleer liet dit soort verzamelingen domweg toe.

Het bestaan van V leidt al snel tot grote problemen. Laten we alle verzamelingen verdelen in twee categorieën: verzamelingen X met de eigenschap dat ze element van zichzelf, $X \in X$, en verzamelingen die de eigenschap niet hebben, $X \notin X$. Vele alledaagse voorbeelden van verzamelingen vallen natuurlijk in de laatste categorie. Laat W nu de verzameling zijn van alle 'fatsoenlijke' verzamelingen zijn, de verzamelingen die *niet* in zichzelf zitten. In welke van de twee categorieen valt W nu zelf? Als we aannemen dat $W \in W$ dan voldoet hij niet aan zijn eigen voorschrift en moet je concluderen dat $W \notin W$. Vice versa, als we aannemen dat $W \notin W$ dan voldoet hij wél aan zijn eigen voorschrift en moet dus $W \in W$ het geval zijn. We concluderen dus

$$W \notin W \Leftrightarrow W \in W.$$

Maar in de wiskunde kunnen niet tegelijkertijd een bewering en de negatie waar zijn. In dat geval kunnen we namelijk alles concluderen. Als zowel A als $\neg A$ ('niet A') waar zijn dan volgt iedere andere uitspraak B volgens de regels van de logica. Immers, ten eerste volgt uit A dat ook $A \vee B$ ('A of B') waar is. Symbolisch

$$A \Rightarrow A \vee B.$$

[2] Een andere bekende niet-Euclidische meetkunde uit die tijd is Riemann's elliptische meetkunde waarin twee lijnen nooit parallel lopen.

[3] Cantor was er zelf al van doordrongen dat dit geen verzameling kon zijn. Zijn machtsverzamelingstelling (T.5) geeft ook voor deze V dat $|\wp V| > |V|$. $\wp V$ is natuurlijk een verzamelling van verzamelingen en er moet dus ook gelden $\wp V \subseteq V$ en dus $|\wp V| \leq |V|$.

In een concreet voorbeeld: als ik thuis ben, dan geldt ook dat ik thuis ben of op college ben. Ten tweede volgt uit $A \vee B$ gecombineerd met het feit dat $\neg A$ waar is, dat B waar moet zijn.

$$(A \vee B) \wedge \neg A \Rightarrow B.$$

In hetzelfde concrete voorbeeld: als ik gezegd heb dat ik thuis ben of op college ben, en het is tevens waar dat ik niet thuis ben, dan moet ik op college zijn. Als we dus weten dat ik thuis ben en dat ik niet thuis ben, kunnen we concluderen dat ik op college ben, of op de maan, of wat u maar wilt! Iedere conclusie is even waar. In de redenering deed het er absoluut niet toe wat de uitspraak B was, en uiteindelijk kunnen we dus uit A en $\neg A$ alles concluderen.

In de verzamelingenleer zelf is de paradox uiteindelijk (redelijk flauw) opgelost door de verzamelingen van het type V of W eenvoudig niet langer in deze onversneden vorm toe te staan. De kapper van Sevilla wordt dus zijn bestaansrecht ontnomen. Het is dan vervolgens wel weer een opdracht om een toch weer zo sterk mogelijke verzamelingentheorie op te zetten.

Russell's paradox had echter binnen de wiskundige gemeenschap een veel grotere impact dan enkel deze technische reparatie van de verzamelingenleer. Het gaf zelfs de aanzet tot een verwoede grondslagenstrijd. De angst voor een inconsistente wiskunde — geheel passende bij de de algehele sombere gemoedstoestand van het fin de siecle — zat er plotseling goed in. Stond het wiskundig huis, steen voor steen geconstrueerd door generaties van de meest geniale wetenschappers, uiteindelijk op drijfzand? Deze crisis heeft er voor gezorgd dat de logica de wiskunde binnengehaald werd. Onder aanvoering van Hilbert en zijn volgelingen gingen wiskundigen zich bezighouden met metawiskunde: de wiskundige structuur van bewijzen zelf. Hieraan zullen we in het tweede deel van dit hoofdstuk ruim aandacht besteden. In hoofdstuk 4 zullen we zien dat al deze logische werkijver in eerste instantie slechts negatieve resultaten leek op te leveren, in het bijzonder de roemruchte onvolledigheidsstelling van Gödel en de onbeslisbaarheidsstelling van Church en Turing in de jaren dertig van de vorige eeuw. Tegelijkertijd heeft al deze wiskundige wedijver zeer belangrijke wiskundige en ook technische vooruitgang opgeleverd. Het belangrijkste voorbeeld van het laatstgenoemde is ongetwijfeld de uitvinding van de moderne digitale computer.

Pythagoras, Fermat en Euler

De wiskunde is de Koningin van de wetenschap, de getaltheorie de Koningin van de wiskunde. Dit waren de woorden van één der allergrootsten, Carl Friedrich Gauss, die vaak in analogie van zijn uitspraak de 'Prins der wiskundigen' wordt genoemd. De getaltheorie toont als geen andere richting in de wiskunde de kracht en impotentie van de vraag naar een bewijs. De subtiele patronen van de natuurlijke getallen kunnen eenvoudig aanleiding geven tot diepe vermoedens die in vele voorbeelden gecontroleerd kunnen worden maar die soms zeer moeilijk op te lossen zijn. Er lijkt geen enkele a-priori aanwijzing te zijn of een getaltheoretische uitspraak gemakkelijk of moeilijk te bewijzen is, of het een leuk sommetje is voor scholieren of dat het eeuwige roem en glorie zal brengen aan degene die het probleem kan kraken.

Een voorbeeld van een relatief gemakkelijk te bewijzen stelling is de bewering dat er oneindig veel gehele getallen x, y, z zijn die aan de relatie van Pythagoras voldoen

$$x^2 + y^2 = z^2.$$

In dit geval zijn x, y en z de zijden van een rechthoekige driehoek. Zulke tripels zijn al bekend sinds de tijd van de Babyloniërs. Zo vinden we op een kleitablet uit zo'n 200 jaar v. Ch. naast de bekende oplossing $3^2 + 4^2 = 5^2$ ook de formidabele oplossing

$$12709^2 + 13500^2 = 18541^2.$$

Een manier om zo'n oneindige reeks oplossingen te genereren is bijvoorbeeld

$$x = 2n, \qquad y = n^2 - 1, \qquad z = n^2 + 1,$$

wat voor elke $n \geq 1$ een gewenst drietal geeft.

Een goed voorbeeld van een notoir moeilijk resultaat is de befaamde Laatste Stelling van Fermat (1630), die zegt dat de Pythagoreïsche tripels niet langer bestaan als we hogere machten dan de tweede macht beschouwen.

FERMAT. De vergelijking $x^n + y^n = z^n$ heeft voor $n > 2$ geen oplossingen in $\mathbb{N}_+$.

Het bewijs voor deze stelling heeft zeer lang op zich laten wachten. Pas in 1994 heeft Andrew Wiles uiteindelijk het bewijs gegeven. Zijn bewijs maakte gebruik van de allermodernste technieken (arithmetische meetkunde, Galoistheorie, elliptische krommen, modulaire vormen) en is zeker niet het bewijs waarvan Pierre de Fermat in de kantlijn beweerde het gevonden te hebben maar volgens hem niet vermeldenswaardig genoeg was. Hij schreef dat het hem aan papierruimte in zijn schrift ontbrak.

Zulke vermoedens kunnen ook anders beslecht worden. In 1769 generaliseerde Euler de stelling van Fermat, door in plaats van drie getallen, vier of meer getallen te nemen. Een eenvoudige specialisatie van zijn vermoeden is bijvoorbeeld

EULER. *De vergelijking $x^4 + y^4 + z^4 = w^4$ heeft geen niet-triviale oplossingen.*

Ook dit resultaat bleef lange tijd staan totdat de Amerikaanse wiskundige Noam Elkies in 1988 op tweeëntwintigjarige leeftijd liet zien dat de volgende relatie geldt

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Dit tegenvoorbeeld was het einde van het vermoeden van Euler! Wat zorgt ervoor dat het vermoeden van Fermat wel waar is en dat het vermoeden van Euler niet geldt? Is hier een diepere achtergrond? Doorgronden doen we het vandaag de dag in ieder geval nog zeker niet.

Priemgetallen

Nog een ander gemakkelijk te bewijzen voorbeeld uit de getaltheorie.

Er zijn oneindig veel priemgetallen.

Hier is het bewijs uit het ongerijmde. Stel er zijn een *eindig* aantal priemgetallen

$$p_1, \ldots, p_n$$

Vorm nu het getal

$$p_1 p_2 \cdots p_n + 1$$

Dit getal heeft de eigenschap dat bij deling door het priemgetal p_1 de rest 1 is, idem voor deling door p_2, p_3 tot en met p_n. Het is dus slechts alleen deelbaar door 1 en zichzelf, en dus of een nieuw priemgetal wat niet in de oorspronkelijke lijst stond of het het is deelbaar door zo'n nieuw priemgetal. Daarmee is het uitgangspunt tot een tegenspraak geleid.

Maar laten we deze eenvoudige eigenschap van de priemgetallen contrasteren met het vooralsnog onbewezen vermoeden van Goldbach (1742).

P 13.

PIERRE DE FERMAT

1601 — 1665

LEONHARD EULER

1707 — 1783

P 14.

CARL FRIEDRICH GAUSS

1777 — 1855

GOLDBACH. *Ieder even getal is te schrijven als de som van twee priemgetallen.*

Bijvoorbeeld $8 = 3 + 5$ of $12 = 5 + 7$. Dit vermoeden staat nog steeds wijd open. In een publiciteitsstunt van de uitgever van de roman *Uncle Petros and Goldbach's Conjecture* van Apostolos Doxiadis werd zelfs een miljoen dollar uitgeloofd aan degeen die het vermoeden kon bewijzen dan wel een tegenvoorbeeld zou geven. Voorlopig is er nog niemand die de prijs heeft mogen komen incasseren.[4]

Stijlfiguren

Een bekende anekdote over Gauss vertelt dat hij op zevenjarige op school aan het werk werd gezet met de opgave alle getallen van 1 tot en met 100 op te tellen. Gauss zag onmiddellijk dat het antwoord 5050 was. Wat was zijn redenering? Wel, hij telde de eerste bij de laatste sommant op

$$1 + 100 = 101,$$

en vervolgde met het paar van de tweede en de op één na laatste

$$2 + 99 = 101,$$

en uiteindelijk tot aan $50 + 51 = 101$. In totaal vond hij zo 50 gelijke sommanten van 101, ofwel, $50 \cdot 101 = 5050$. Dit resultaat laat zich formaliseren tot de volgende stelling voor de som van eerste n natuurlijke getallen

$$\sum_{k=0}^{n} k = \frac{1}{2} n(n+1).$$

Deze formule klopt overigens ook voor oneven n aangezien de het getal in het midden wat je overhoudt na de methode van Gauss is gelijk aan $n+1/2$. Dit bewijs kan op vele verschillende manieren bewezen worden. Laten we een aantal van deze wiskundige stijlfiguren aflopen.

Volledige inductie Laten we de bovenstaande uitspraak $\mathsf{p}(n)$ noemen. Volledige inductie stelt ons in staat de uitspraak $\mathsf{p}(n)$ te bewijzen voor alle $n \in \mathbb{N}$ uitgaande van twee stappen.

1. Toon aan dat $\mathsf{p}(0)$ waar is.

2. Leidt $\mathsf{p}(n+1)$ af, uitgaande dat $\mathsf{p}(n)$ waar is.

In dit geval reduceert stap 1 tot de uitspraak $0 = 0$. In stap 2 moeten we bewijzen dat

$$\frac{1}{2} n(n+1) + (n+1) = \frac{1}{2}(n+1)(n+2)$$

hetgeen eenvoudig volgt.

Volledige inductie is een bijzonder krachtige bewijsmethode die veel gebruikt wordt in alle mogelijke takken van de wiskunde. Ook in dit boek zullen we er nog veelvuldig gebruik van maken.

[4]Dit miljoen op het hoofd van Goldbach moet niet verward worden met de bekendere Clayprijzen die te verdienen zijn met de oplossing van zeven (nog diepere) wiskundige problemen zoals bijvoorbeeld de Riemann hypothese en het vermoeden van Birch en Swinnerton-Dyer dat in wezen het Goldbachvermoeden omvat.

Inductie

De formele logische formulering van inductie luidt als volgt:

$$(\varphi(0) \wedge \forall n\,(\varphi(n) \rightarrow \varphi(n+1))) \rightarrow \forall n\,\varphi(n)$$

Dat ziet er flink cryptisch uit. Een prettige metafoor om inductie goed te begrijpen is het 'domino-effect' voor eeen oneindige rij stenen. Het inductie-axioma zegt nu dat

> *Als de eerste, of liever nulde, dominosteen omvalt ($\varphi(0)$) en als elke dominosteen omvalt indien zijn voorganger ($\forall n\,(\varphi(n) \rightarrow \varphi(n+1))$) omvalt dan vallen alle dominostenen om ($\forall n\,\varphi(n)$).*

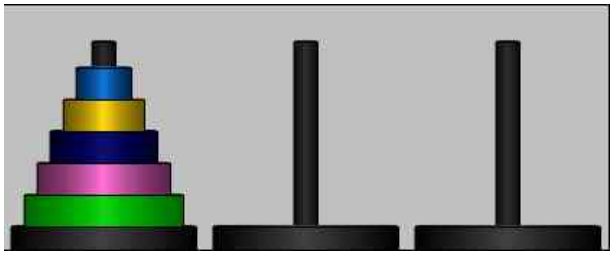
Het eerste geval, de eerste dominosteen, heet ook wel de basis *van de inductie. Dit is meestal een triviale stap. Daarna veronderstel je dat je het bewijs gevonden hebt voor een zekere n, de zogenaamde* inductiehypothese*, en daarna moet dan aangetoond worden dat op basis van deze veronderstelling de eigenschap ook geldt voor $n+1$.*
Een variant van het inductie-axioma, ook wel sterke inductie *genoemd, luidt als volgt:*

$$\forall n\,(\forall m\,((m < n \wedge \varphi(m))) \rightarrow \varphi(n)) \rightarrow \forall n\,\varphi(n)$$

Met de vertaling naar de dominostenen-metafoor:

> *Als geldt dat elke dominosteen omvalt indien al zijn voorgangers omvallen dan vallen alle dominostenen om.*

Let op dat de conditie altijd $\varphi(0)$ impliceert want deze heeft geen voorgangers. Deze versie van inductie wordt vaak gebruikt bij inductie over de lengte van andere structuren als getallen zoals formules (zie bijvoorbeeld T.16, dit bewijs kan eenvoudig opnieuw gedaan worden met een inductieve argumentatie).
Om de kracht te illustreren van inductieve bewijzen nemen we het volgende alom bekende puzzeltje: de torens van Hanoi. De bedoeling is de schijven één voor één te verschuiven en een nieuwe stapel op één van de andere stokken te krijgen. De spelregel is dat nooit een schijf op een schijf van kleinere omvang geplaatst mag worden.

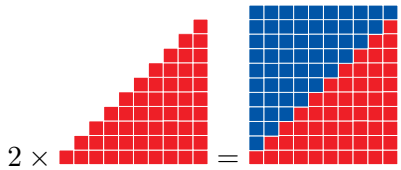


Als men zo aan de gang gaat zal het niet meevallen een oplossing te vinden. De verkoper van de puzzel kan de klant daarentegen een heel eenvoudig inductief argument geven dat hij wel opgelost kan worden, ongeacht op welke stok je de stapel zou willen plaatsen en vanaf welke stok je begint.

> Basis. *Voor de puzzel met één schijf is er een oplossing.*
>
> Inductie. *We veronderstellen dat we de puzzel kunnen oplossen (voor beide stokken) voor n stenen. De oplossing voor $n+1$ is nu makkelijk te beschrijven want we kunnen de oplossing voor n stenen direct gebruiken omdat elke schijf op de grootste $n+1$-ste schijf geplaatst kan worden. Schuif volgens de oplossing waarover we beschikken voor n stenen de stapel zonder de grootste schijf naar de stok waar we niet op uit willen komen. Schuif nu de vrijgekomen grootste steen naar naar de beoogde stok en gebruik weer de oplossing voor n stenen om die stapel nu naar de bedoelde stok boven op de grootste schijf te krijgen.*

We hebben nu het domino-effect bestendigd. Het eerste geval klopt, en als het n-de geval werkt dan ook de $n+1$-ste. Kortom de Hanoi-puzzel is voor alle n op te lossen. Om de daadwerkelijke oplossing uit te rekenen is vervolgens weer veel werk.

Grafisch of ruimtelijk Er zijn ook andere bewijzen mogelijk die meer een 'aha' gevoel geven. Bijvoorbeeld het onderstaande grafisch bewijs.



De eerste figuur is duidelijk de som $1 + 2 + \ldots + n$. De tweede figuur heeft oppervlak $n(n + 1)$.

Een stapje hoger We kunnen het resultaat ook bewijzen door eerst iets moeilijkers te bekijken, namelijk de som van de eerste n kwadraten

$$\sum_{k=0}^{n} k^2$$

In plaats van de variabele k te laten lopen van 0 tot n, kunnen we de som natuurlijk ook laten lopen van n tot 0. Dit maakt voor het uiteindelijke antwoord niets uit. Maar daarmee hebben we de volgende formule

$$\sum_{k=0}^{n}(n-k)^2 - \sum_{k=0}^{n} k^2 = 0.$$

Nu kunnen we gebruikmaken van de identiteit

$$(n-k)^2 = n^2 - 2nk + k^2$$

Als we dit invullen dan valt de term met k^2 weg en blijven we over met de relatie

$$\sum_{k=0}^{n}(n^2 - 2nk) = 0$$

en vervolgen na deling door n:

$$\sum_{k=0}^{n}(n - 2k) = 0.$$

Dit geeft dan weer

$$(n+1)n - 2\sum_{k=0}^{n} k = 0,$$

en hieruit concluderen we eenvoudig het gevraagde resultaat. De moraal van dit bewijs is dat je soms een stapje hoger moet reiken om te vinden wat je zoekt!

Verandering van blik

Soms wordt een bewijs ineens duidelijk als we van perspectief veranderen. Een voorbeeld wat dit duidelijk illustreert is het volgende.

Het getal 12 heeft zes delers, te weten 1, 2, 3, 4, 6 en 12. Laten we het aantal delers van n schrijven als $d(n)$. Dus we schrijven $d(12) = 6$. Als we n variëren zal het getal $d(n)$ zeer onregelmatig

springen. Zo is $d(13) = 2$ omdat 13 een priemgetal is met delers 1 en 13 als enige delers. We vragen ons vervolgens af wat het gemiddelde is van het aantal delers van de eerste n getallen? In een formule wordt dit gemiddelde gegeven door

$$\frac{1}{n}\sum_{k=1}^{n} d(k)$$

Als we dit gaan uitproberen lijkt het getal $d(n)$ zich zeer grillig te gedragen. Het gemiddelde lijkt daarmee geen mooi patroon te kunnen hebben, totdat we het in een tabel weergeven:

	1	2	3	4	5	6	7	8	9	10	11	12
1	•	•	•	•	•	•	•	•	•	•	•	•
2		•		•		•		•		•		•
3			•			•			•			•
4				•				•				•
5					•					•		
6						•						•
7							•					
8								•				
9									•			
10										•		
11											•	
12												•

Om het gemiddelde aantal delers van de eerste 12 getallen te berekenen tellen we gewoon het aantal zwarte bolletjes • en delen door 12. De kolommen zijn inderdaad niet regelmatig, maar de rijen zijn perfect regelmatig. In de n-de rij herhalen de delers zich precies na n plaatsen. We moeten het plaatje dus over negentig graden draaien. Door nu over de rijen te sommeren in plaats van de kolommen krijgen we

$$\frac{1}{n}\sum_{k=1}^{n} d(k) = \frac{1}{n}\sum_{k=1}^{n} \lfloor \frac{n}{k} \rfloor$$

waarbij $\lfloor \frac{n}{k} \rfloor$ afronden naar een geheel getal voorstelt. Voor grote n kunnen we dit benaderen als

$$\frac{1}{n}\sum_{k=1}^{n} \lfloor \frac{n}{k} \rfloor = \sum_{k=1}^{n} \frac{1}{k} \approx \int_{1}^{n} \frac{dx}{x} = \ln n$$

Het gemiddelde aantal delers van de eerste n getallen zal dus bij benadering (voor grote n) gegeven worden door $\ln n$. Voor de eerste miljard getallen is dat dus ongeveer 21.

Het nut van bewijzen en definities

De Amerikaanse wiskundige Bill Thurston, winnaar van de Fieldsmedaille in 1984 en bekend door zijn werk aan de klassificatie van driedimensionale ruimtes, heeft een zeer interessant en tegendraadse analyse gegeven van het nut van bewijzen in de wiskunde[5]. Hij voert daarin aan dat een exacte oplossing in de wiskunde niet altijd het enige doel is. Om verdere vooruitgang te stimuleren is het ook van belang dat de context en de nieuwe ideeën goed worden uitgedragen. Hij illustreert deze gedachte

[5] W.P. Thurston, *On proof and progress in mathematics*, Bull. Amer. Math. Soc. (NS) 30 (1994), 161–177.

met het begrip definitie. In de wiskunde worden objecten precies gedefinieerd. Maar vaak mist zo'n definitie vele andere inzichtelijke aspecten en associaties.

Een goed voorbeeld is het begrip *afgeleide* van een functie $f(x)$, zeg van $\mathbb{R}$ naar $\mathbb{R}$. De technische definitie, zoals je die in een standaard college analyse leert is niet erg verhelderend op eerste gezicht

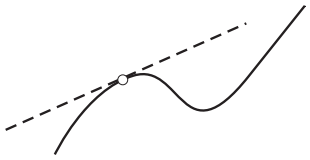
Formeel De afgeleide $f'(x)$ in x voldoet aan:

$$\forall \epsilon > 0 \, \exists \delta > 0 \left[0 < |\Delta x| \delta \Rightarrow \left| \frac{f(x + \Delta x) - f(x)}{\Delta x} - f'(x) \right| < \epsilon \right].$$

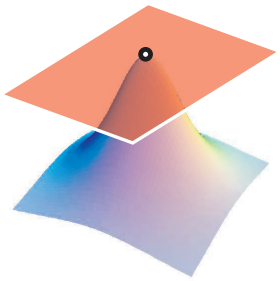
Maar er zijn nog andere vele andere gezichtspunten die enerzijds het begrip groter maken en anderzijds nieuwe generalisaties suggereren.

Snelheid De afgeleide $f'(t)$ is de instantane snelheid van $f(t)$ waarbij t nu de tijd is. Dit geeft direct een goede intuïtie wat te verwachten als we een functie $f : \mathbb{R} \to \mathbb{R}^n$ differentiëren. De afgeleide is dan een snelheidsvector.

Meetkundig De afgeleide als tangens van de hoek die de raaklijn van de grafiek van de functie maakt.



Dit suggereert hoe de afgeleide te definiëren als we een functie over meerdere veranderlijken hebben. In het geval van twee variabelen krijgen we bijvoorbeeld een raakvlak in plaats van een raaklijn



Infinitesimaal De afgeleide is de infinitesimale verandering in de functiewaarde $f(x)$ als we de variabele x infinitesimaal veranderen. Dit is natuurlijk dicht bij de oorspronkelijke definitie van Leibnitz en Newton. De afgeleide als ratio

$$f' = \frac{df}{dx}$$

van de infinitesimalen df en dx. In dit geval wordt het duidelijk dat als we een discrete functie $f(n)$ hebben (met n een geheel getal) de discrete variant van de afgeleide het verschil $f(n+1) - f(n)$ is.

Symbolisch Van speciale functies is de afgeleide gemakkelijk. Bijvoorbeeld als $f(x) = x^n$ dan is $f'(x) = nx^{n-1}$. De afgeleide nemen is dus de symbolische operatie op veeltermen

$$x^n \to nx^{n-1}$$

Dit stelt ons in staat om de afgeleide ook te definiëren als x helemaal geen getal is, maar wel een vermenigvuldiging heeft. Deze kijk heeft geleid tot bijvoorbeeld een goede definitie van de afgeleide van een knoop!

Benadering In de buurt van het punt x kunnen we de functie $y = f(x)$ benaderen door een lineaire functie $y = ax + b$ met $a = f'(x)$.

$$f(x + z) \approx f(x) + f'(x)z.$$

Microscopisch Als we onbeperkt inzoomen op het punt x dan kunnen we $f(x)$ door de lineaire benadering vervangen. Alles wordt lineair in deze limiet. Daarom neemt lineaire algebra een voorname plaats binnen veel wiskundeopleidingen.

Zo gaat de rij nog een lange tijd door. Ieder perspectief geeft een nieuwe benadering. Uiteindelijk moest Thurston zelf wel eens de volgende definitie — de zevenendertigste! — gebruiken.

Thurston De afgeleide is de Lagrangiaanse sectie van de co-raakbundel welke aanleiding geeft tot de connectievorm voor de unieke vlakke connectie op de triviale $\mathbb{R}$-bundel waarvoor de grafiek van f parallel is.

Tegen de intuïtie in

Onze aangeboren ruimtelijke en getalsmatige intuïtie, opgedaan door jarenlang in de dagelijkse praktijk te oefenen, geeft ons vaak een indruk wat we wel en wat we niet van de wiskunde kunnen verwachten. Maar soms bevinden we ons in zo'n onbekend terrein dat we werkelijk geen flauw idee hebben wat mogelijkerwijs waar is. Zo'n onvoorstelbaar fenomeen troffen we voorbij de horizon van onze gewone eindige wereld in het eerste hoofdstuk. Eenmaal wiskundig over oneindigheid nadenkend troffen we een oneindige variatie aan oneindigheden aan.

Juist als we deze vreemde wereld binnentreden kan de precieze redeneertrant van de wiskunde ons houvast geven. Een goed voorbeeld is de volgende stelling[6]

> BANACH-TARSKI *Het is mogelijk een bal in vijf stukken te snijden die, na ze te draaien en te verschuiven, in elkaar geplakt kunnen worden tot twee ballen van dezelfde grootte als de oorspronkelijke bal.*

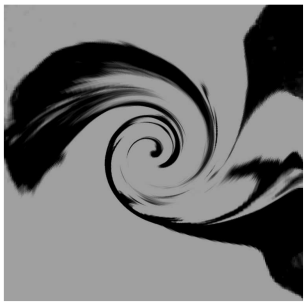
Dit resultaat lijkt in tegenspraak met alle intuïtie van een stoffelijk object. Immers als we de vijf stukken op de weegschaal zouden leggen wegen ze toch tezamen evenveel als de oorspronkelijke bal. En daarmee moet iedere van de twee gereconstrueerde ballen toch de helft wegen? Maar hier raken we aan de bizarre mogelijkheden die de wiskunde toestaat. Geen van de onderdelen heeft een gewicht. Dat wil zeggen, de stukken zijn zo vreemd van vorm — u kunt denken aan een fractal — dat het gewoon niet mogelijk is een gewicht of een volume toe te kennen.

Nog een parel uit de topologie, nu van de bekende Nederlandse wiskundige Luitzen Brouwer

[6] Hierbij wordt met een wiskundige 'bal' een opgevulde bol in de ruimte $\mathbb{R}^3$ bedoeld, zeg, de deelverzameling van punten met coördinaten x, y en z zodanig dat $x^2 + y^2 + z^2 \leq 1$ (de eenheidsbol).

BROUWER *Een continue*[7] *afbeelding van een bal naar een bal laat op zijn minst een punt vast.*

Deze zogenaamde dekpuntstelling kan als volgt worden toegepast. Als u (voorzichtig) in een geïdealiseerd kopje koffie roert, zal uiteindelijk op zijn minst één koffiemolecuul op zijn oorspronkelijke plaats terugkeren, hoe hard u ook uw best doet alle moleculen van plaats te laten veranderen. Dat zo'n punt kan bestaan zien we al als we bijvoorbeeld het kopje over een slag rond draaien. Dan verandert ieder punt van plaats behalve het centrum waarom heen we draaien.



Een ander voorbeeld van dezelfde stelling: neem twee identieke vellen papier. Verfrommel de eerste en leg deze boven op de tweede. Er is nu minstens een punt op het eerste vel dat precies boven het corresponderende punt op het tweede vel ligt.

Laten we proberen een schets van een bewijs te geven van de dekpuntstelling voor het eendimensionale geval. Een eendimensionale bal is gewoon een gesloten interval zoals bijvoorbeeld $[0, 1]$. Stel we hebben nu een afbeelding $f : [0, 1] \to [0, 1]$ van het interval naar zichzelf. Bijvoorbeeld door een kopie te verfrommelen en de projectie te beschouwen.

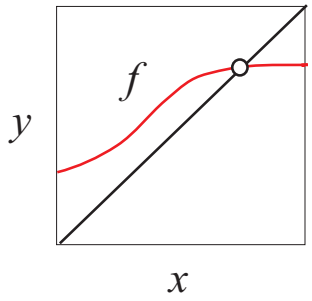
We kunnen dit ook in een grafiek uitzetten. Het beginpunt 0 komt terecht in $f(0)$, en het eindpunt komt terecht in $f(1)$. De twee punten $f(0)$ en $f(1)$ liggen op het interval $[0, 1]$ en we kunnen aannemen dat $f(0) > 0$ en $f(1) < 1$, anders zijn we direct klaar want dan hebben we al een dekpunt gevonden. Een dekpunt voldoet aan de vergelijking

$$f(x) = x$$

Laten we nu naar de grafieken van de functies $y = f(x)$ en $y = x$ kijken. Een blik op onderstaand

[7] Een afbeelding heet *continu* als ruwweg twee punten die dicht bij elkaar liggen ook na de afbeelding weer dicht bij elkaar liggen. We mogen dus niet 'scheuren'.

figuur leert ons dat deze twee grafieken elkaar hoe dan ook moeten snijden.



Immers voor $x = 0$ ligt de ene kromme boven de andere, en voor $x = 1$ is de volgorde omgedraaid. Gezond verstand zegt ons dat ergens onderweg de twee daarom moeten snijden. Eureka!

6.2 Bewijzen, redeneren en logica

Beroemde wiskundige bewijzen lijken vaak geniale flitsen van grote geesten. Maar een opgeschreven bewijs heeft ook een structuur die voor gewone stervelingen is te begrijpen. Het vormt als het ware een protocol van die oorspronkelijke creatieve gedachtengang. Bewijzen worden door velen ervaren als het meest ontoegankelijke en abstracte aspect van de wiskunde. Maar men zou even goed kunnen zeggen dat ze juist de 'democratie' dienen: een bewijs maakt een creatieve gedachtengang van een eenling tot een publiek goed, dat ook door anderen is te gebruiken, en aan te passen aan nieuwe omstandigheden. Het wordt op deze manier dus juist makkelijker om wetenschappelijke innovaties te begrijpen, en er zelf aan bij te dragen. Bovendien zijn bewijzen geen geïsoleerde stukjes wiskundig vuurwerk: ze vormen een samenhangend bouwsel, dat we kunnen onderzoeken op zijn eigenschappen, en soms zelfs praktisch exploiteren. In dit hoofdstuk geven we een idee van dat systeem in bewijzen, door een logische analyse van enkele veel voorkomende patronen. Logische bewijssystemen spelen een belangrijke rol in het grondslagenonderzoek van de wiskunde, dat in het derde deel aan de orde komt. Maar ze worden ook praktisch gebruikt in computers die automatisch 'intelligente' taken moeten verrichten waarbij een of andere vorm van precies redeneren nodig is. Nu zijn noch computers noch professionele wiskundigen 'gewone' denkers, zoals we dat zijn in het dagelijks leven wanneer we proberen te bedenken hoe de kaarten liggen in een spel, of hoe we de route naar een vergadering moeten plannen, of hoe we ons staande houden in een gesprek. Daarvoor gebruiken we alledaagse argumentaties. Toch lijken wiskundige bewijsvormen veel meer op zulke gewone cognitieve vaardigheden van gewone mensen dan men pleegt te denken. We bespreken enkele overeenkomsten en verschillen aan het eind van dit hoofdstuk. Er bestaat geen wetenschappelijke consensus over de precieze relatie tussen logisch bewijzen — al dan niet door computers — en menselijk redeneren. Maar ze lijken zeker niet met elkaar in strijd.

Bewijspatronen

Om bewijspatronen te vinden hoeven we alleen maar terug te gaan naar eerdere hoofdstukken, en nog eens met een iets meer afstandelijk oog te kijken naar wat daar gebeurde. Bijvoorbeeld, om te bewijzen dat de reële getallen niet aftelbaar zijn, namen we in 1.1 aan dat er juist wel een aftelling bestaat, en lieten vervolgens met een diagonaalconstructie zien dat in die aftelling minstens één reëel getal moest ontbreken. Achter deze bewijsvoering zit een algemeen, en veel gebruikt patroon. We willen laten zien dat een zekere bewering A niet geldt, of kort genoteerd: $\neg A$. Maar dat doen we door juist A aan te nemen, 'for the sake of argument', en dan te laten zien dat $\neg A$ daaruit volgt, en dus de contradictie: we hebben dan immers zowel A als $\neg A$. Dit is een versie van het zogenaamde

Bewijs uit het Ongerijmde

uit $A \rightarrow (B \wedge \neg B)$ volgt dat $\neg A$.

De rechtvaardiging voor deze gevolgtrekking is duidelijk. Er geldt altijd A of $\neg A$. In het tweede geval zijn we klaar, en het eerste geval kan zich niet voordoen, omdat dan een contradictie waar zou zijn, hetgeen nooit gebeurt. Het Bewijs uit het Ongerijmde komt heel vaak voor in de wiskunde als men een negatieve conclusie wil bewijzen. Maar het is evenzeer een principe van gewoon redeneren. Als u in een gesprek wilt aantonen dat iemand ongelijk heeft met een gedane bewering A, dan probeert u vaak uit A een of andere tegenspraak $B \wedge \neg B$ af te leiden. Want iemand die betrapt wordt op tegenspraken verliest het debat!

Zodra we eenmaal dit soort patronen zien kunnen we er verder mee spelen. Zo hanteren wiskundigen ook wel de volgende variant op Bewijs uit het Ongerijmde. Ze tonen aan dat een bewering A geldt door te weerleggen dat de ontkenning $\neg A$ geldt! Op deze manier kan men bijvoorbeeld laten zien dat elke verzameling natuurlijke getallen een kleinste element heeft. Immers, als dat niet zo was, dan kon je in die verzameling steeds maar weer een kleiner getal kiezen, en daarmee een oneindig dalende rij natuurlijke getallen maken: wat niet mogelijk is. Is dit nu letterlijk het voorgaande bewijspatroon? Eigenlijk niet, want dat zou slechts zeggen dat: uit $\neg A \rightarrow (B \wedge \neg B)$ volgt dat $\neg\neg A$. Het nieuwe patroon zegt net iets anders, en wel: uit $\neg A \rightarrow (B \wedge \neg B)$ volgt dat A. Hierin zit nog een extra bewijsprincipe verstopt, en wel de equivalentie van de dubbele ontkenning $\neg\neg A$ en de bewering A zelf. Ook dit is weer een veel voorkomend principe.

Als we op deze abstracte manier kijken naar wiskundig bewijzen, of naar redeneren in het algemeen, dan zien we een systeem waarin steeds meer patronen zijn te ontdekken. Zo kan u in een gesprek ook als volgt attaqueren. Iemand zegt dat A; maar u laat zien dat daar een bewering B uit volgt waarvan al bekend is dat die onwaar is. In dat geval hanteert u een gevolgtrekking met twee gegevens en een conclusie die al sinds Middeleeuwen de naam 'Modus Tollens' draagt:

$$\text{uit } A \rightarrow B \text{ en } \neg B \text{ volgt dat } \neg A.$$

Wie houdt van argumenteren begrijpt dit soort bewijspatronen impliciet, en soms zelfs expliciet. Nu is natuurlijk niet alle redeneren correct, en soms zelfs even interessant zijn *ongeldige* bewijspatronen. Een favoriet van veel personen is de volgende variant op Modus Tollens:

$$\text{uit } A \rightarrow B \text{ en } \neg A \text{ volgt dat } \neg B.$$

Dit zou de drogreden kunnen zijn van een dokter die dreigend tegen u zegt:

> "Als u mijn medicijn slikt (A), dan wordt u beter (B). Maar u slikt mijn medicijn niet ($\neg A$). Dus u wordt niet beter ($\neg B$)."

Deze conclusie volgt helemaal niet. Zoals bekend worden we immers vaak beter van gewoon wachten, één van de beste breedspectrum medicijnen die ooit zijn uitgevonden. Een dergelijke situatie die de uitgangspunten van een gevolgtrekking waar maakt, maar de conclusie onwaar, noemt men wel een *tegenvoorbeeld*. Nu vindt u zulke huis-tuin-en-keuken scenario's misschien niet serieus genoeg. Hier is dan ook nog een wiskundig tegenvoorbeeld:

> "Als $x > 5$, dan geldt $x > 3$, voor alle getallen x." In het bijzonder is de implicatie waar dat, als $4 > 5(A)$, dan $4 > 3(B)$. Nu geldt $4 > 5$ niet, en is $\neg A$ dus waar. Maar $\neg B$ is onwaar, aangezien $4 > 3$.

Wel geldig zou het overigens zijn als de dokter zich bij een later consult zou beroepen op het correcte bewijspatroon van Modus Tollens:

> "Als u mijn medicijn slikt, dan wordt u beter. Maar u bent niet beter. Dus u slikt mijn medicijn niet."

Dit alles is nog maar een tipje van de sluier. Achter de praktijk van bewijzen en redeneren die we zo spontaan beoefenen zit een wiskundige wereld van vaste patronen. Het inzicht dat die wereld op zichzelf bestudeerd kan worden heeft al in de Griekse en de Indiase Oudheid geleid tot het ontstaan van het vakgebied van de logica. In dit hoofdstuk geven we een nadere indruk van logische systemen en hun rol in de wiskunde en daarbuiten.

Bewijspatronen en logische formules

Hoe beschrijven we bewijspatronen? Het prettige is dat we voor dit doel geen nieuwe notatie hoeven uit te vinden, want die hebben we al! De formele taal van het eerste hoofdstuk diende om de structuur van wiskundige beweringen optimaal doorzichtig te maken. Dat ging met atomaire formules die relaties uitdrukten tussen objecten, en vervolgens logische operaties die uit zulke atomaire formules complexe beweringen maakten:

Basisbeweringen	$s = t$, $s < t$, $s \in t$, ... etc.
Boolese operaties	$\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
Kwantoren	$\forall$, $\exists$

Maar deze taal is ook precies wat we nodig hebben om bewijspatronen in het vizier te krijgen. Een eerste belangrijk genre is het redeneren met alleen Boolese operaties. Zo draait een bewijs uit het ongerijmde alleen om het gedrag van negatie en implicatie. Andere gevallen hebben ook te maken met conjunctie, disjunctie en equivalentie. Er zijn talloze bekende bewijsvormen in dit genre, zowel geldige als ongeldige. Hier is een kort lijstje van veel voorkomende geldige gevolgtrekkingen:

$$\begin{aligned} A \vee B, \neg A &\Rightarrow B \\ \neg(A \wedge B), A &\Rightarrow \neg B \\ A \rightarrow B, A &\Rightarrow B \\ A \rightarrow B, B \rightarrow C &\Rightarrow A \rightarrow C \\ A \rightarrow B, C \rightarrow B &\Rightarrow (A \vee C) \rightarrow B \end{aligned}$$

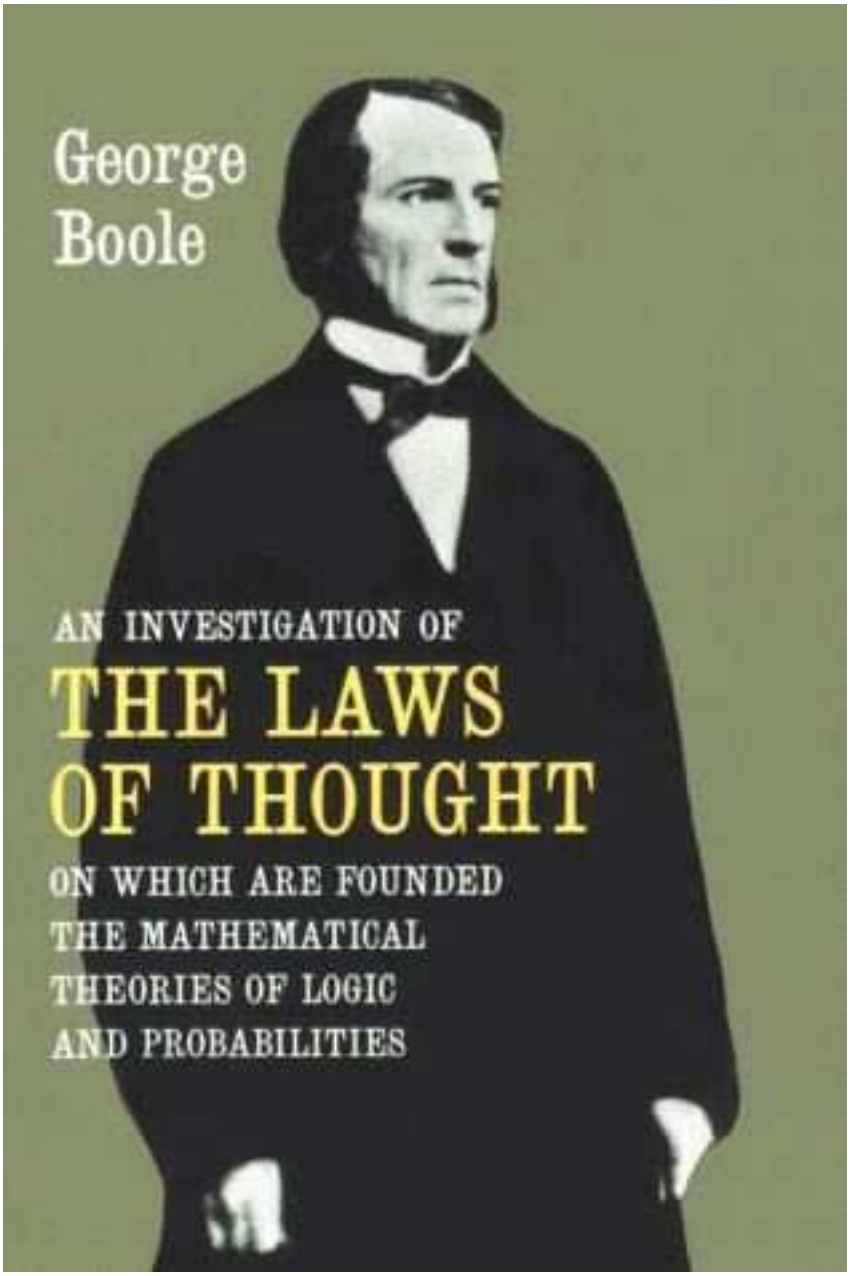
Bij wijze van contrast zijn hier enkele ongeldige patronen:

$$\begin{aligned} A \rightarrow B &\Rightarrow B \rightarrow A \\ \neg(A \wedge B) &\Rightarrow \neg A \wedge \neg B \\ (A \wedge B) \rightarrow C &\Rightarrow A \rightarrow C \end{aligned}$$

Door variëren met dit soort vormen met steeds complexer formules kunnen we zelfs oneindig veel geldige, en niet geldige, bewijspatronen maken! Natuurlijk zal slechts een deel daarvan corresponderen met wat er gebeurt in de praktijk. Dergelijk redeneren met alleen Boolese operaties noemt men wel *propositielogica*. Dit systeem draait om waarheid en onwaarheid van gehele beweringen en hun samenstellingen. De meest voorkomende patronen in dit genre zijn al ontdekt door de Stoïcijnse filosofen in de Klassieke Oudheid, maar de echte wiskundige doorbraak kwam pas in de negentiende eeuw met de Britse wiskundige George Boole in zijn boek "The Laws of Thought" (1847) (zie hiervoor ook T.26 in het volgende hoofdstuk op pagina 218). Ook moderne computers hebben een innige relatie met propositielogica, omdat machinaal binair rekenen met waarden 1 en 0 kan worden opgevat als manipuleren van 'waarheidswaarden' waar en onwaar. Over dit rekenkundig verband komen we in het volgende hoofdstuk nog nader te spreken, maar we concentreren ons nu op bewijsprincipes.

Naast de propositielogica zijn er nog veel meer genres bewijspatronen. Veel belangrijke wiskundige gevolgtrekkingen hebben bijvoorbeeld te maken met de *kwantoren* $\exists, \forall$ van hoofdstuk 1, zoals we later in dit hoofdstuk nog zullen zien. Kwantorlogica is veel rijker dan propositielogica. Maar voor het beschrijven van eigenschappen van bewijssystemen gebruiken we dit laatste als prettig vehikel.

P 15.



GEORGE BOOLE

1815 — 1864

George Boole *op de voorkant van zijn boek in een editie van 1973. Zijn werk is nog steeds in de Engelse boekhandels te verkrijgen voor een luttel bedrag.*

Geldig en ongeldig redeneren

Ook hier zien we weer het belang van wiskundige abstractie, met formules als beweringsvormen. Een bewijspatroon is niet gekoppeld aan een enkele concrete situatie: het is juist bruikbaar voor redeneren in verschillende situaties. Met het oog daarop wordt het begrip *logische geldigheid* van zo'n patroon als volgt gedefinieerd. De waarheid van de gegevens ('premissen') $P_1, \ldots, P_k$ moet algemeen de waarheid garanderen van de conclusie C, hoe we de schematische formules ook precies lezen. Geldigheid van een patroon wordt dan uitgedrukt door de volgende bewering:

> $P_1, ..., P_k \Rightarrow C$, in woorden: "$C$ volgt uit $P_1, ..., P_k$", wil zeggen dat
> in elke situatie die $P_1, ..., P_k$ waar maakt, is ook C waar.

Deze definitie spoort met onze eerdere intuïtieve geldigheidsoordelen. Bijvoorbeeld, in een situatie waarin $A \vee B$ en $\neg A$ allebei waar zijn kunnen we slechts twee gevallen hebben: (a) A geldt — maar dit is in strijd met het tweede gegeven A, en dus vervalt deze mogelijkheid — of (b) B is waar, en dit is inderdaad wat de gevolgtrekking beweerde.

Geldigheid is een begrip waarover u wel even goed moet nadenken. Het is met name niet voldoende dat de conclusie in een enkele *gegeven* situatie waar is om de gevolgtrekking geldig te maken. Uit $x < 2$ volgt bijvoorbeeld niet dat $x < 2 \wedge x > 0$ (denk aan $x = 0$, hoewel zowel $x < 2$ als $x < 2 \wedge x > 0$ voor sommige keuzen van x wel waar zijn (bijv. $x = 1$). Evenmin is onwaarheid van de conclusie in een gegeven geval altijd fataal voor geldigheid van een gevolgtrekking. Uit $x < 2 \wedge x > 0$ volgt wel degelijk dat $x < 2$, zelfs al bestaan er getallen als $x = 3$ die de conclusie onwaar maken. Een gevolgtrekking is volgens de zojuist gegeven definitie pas niet geldig (meestal zegt men: *ongeldig*) als er een situatie bestaat waarin de premissen wel waar zijn, maar de conclusie niet: een zogenaamd *tegenvoorbeeld* voor de gevolgtrekking. We zagen al dat het eerdere doktersscenario een tegenvoorbeeld was voor de gevolgtrekking van $A \rightarrow B, \neg A \Rightarrow \neg B$. Een geldige gevolgtrekking heeft geen tegenvoorbeelden: als de conclusie in een gegeven situatie onwaar is, dan moet ook minstens een van de premissen onwaar zijn.

De volledige propositielogica van Boolese operaties is een fraai systeem. Het bevat naast veel voorkomende patronen ook wiskundige principes die u niet zo gauw uit de dagelijkse praktijk zou opmaken. Zulke principes hebben vaak de vorm van een enkele formule, die waar is in elke situatie, een z.g. *logische wet*. Twee bekende logische wetten zijn:

$(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$	Distributiviteit
$\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$	De Morgan's Wet

Boole's cruciale inzicht rond 1847 was dat dergelijke wetten voor het bewijzen in de propositielogica neerkomen op de geldigheid van een klein aantal elementaire algebraïsche regels voor binair rekenen met de getallen 0 en 1. Zo lijkt Distributiviteit op de rekenregel $x * (y + z) = (x * y) + (x * z)$ – al moet men met de precieze analogie wel even oppassen. $\overset{\text{T. 26}}{\Longrightarrow}$ 218

Propositielogica in de praktijk

Propositielogisch redeneren is een basismodule in wiskundig bewijzen, maar ook van gewoon praktisch denken, zoals bij het oplossen van een puzzel, of een meer serieus probleem. Stel we plannen een klein feestje, maar moeten rekening houden met de 'compabilités des humeurs' van een drietal potentiële gasten:

1	Jan komt als Marie of Anne komt	$(M \vee A) \rightarrow J$
2	Anne komt als Marie niet komt	$\neg M \rightarrow A$
3	Als Anne komt, dan komt Jan niet	$A \rightarrow \neg J$

We lezen het woordje 'of' als 'en/of'. Hier is een beredeneerde oplossing in simpele stappen. (i) Stel dat Anne komt. Dan komt Marie of Anne, dus komt Jan (vanwege 1). Maar vanwege 3 komt Anne dan juist niet. Tegenspraak. Dus, onze aanname is onhoudbaar, en Anne komt niet. (ii) Maar dan volgt met 2 (vanwege de eenvoudige consequentie dat $\neg M \rightarrow A \Rightarrow \neg A \rightarrow M$) dat Marie wel komt. (iii) Dan komt dus ook Marie of Anne, en weer met 1 concluderen we dat Jan komt. Ons uitnodigingsplan moet dus zijn:

$$\neg A, M, J$$

Ook puzzels berusten vaak op dit soort redeneren. Hier is een illustratie uit de Nationale Wetenschapsquiz van het jaar 2001:

> Jantje zegt dat Pietje liegt. En Pietje zegt dat Klaasje liegt. Maar Klaasje zegt dat Jantje en Pietje liegen. Wie liegt er wel, en wie niet?

We kunnen dit als volgt weergeven in formules:

$$J \leftrightarrow \neg P, P \leftrightarrow \neg K, K \leftrightarrow (\neg J \wedge \neg P)$$

waarbij een propositieletter aangeeft dat de betreffende persoon de waarheid spreekt. De correcte oplossing luidt:

J en K zijn onwaar, P is waar.

U vindt dit makkelijk met een klein aantal propositionele bewijsstappen.

Maar strikt redeneren speelt zich natuurlijk op elk serieus terrein van het leven af. Ons laatste voorbeeld komt uit de sfeer van het Recht. Drie personen worden verdacht bij een moord, en het volgende bewijsmateriaal ligt ter tafel - zeg op grond van getuigenverklaringen:

1	A was aanwezig of B	$A \vee B$
2	A was aanwezig of C	$A \vee C$
3	C is een maatje van A	$A \rightarrow C$
4	er zijn hoogstens twee daders	$\neg(A \wedge B \wedge C)$

De aanklager beweert nu: "A was aanwezig!" De advocaat zegt daarentegen: "Nee, dat hoeft niet." Let op het verschil in *bewijslast*. De aanklager moet een bewijs geven van de bewering A uit de gegevens. Dit is een geldigheidsprobleem in onze eerdere zin. De advocaat hoeft daarentegen alleen maar aan te tonen dat de vier gegevens die ter tafel liggen compatibel zijn met de onschuld van zijn cliënt, d.w.z. de negatie van de conclusie: $\neg A$. Logisch gezien heet dit laatste een

> *Consistentie- of vervulbaarheidsprobleem*
>
> Gegeven een stel beweringen, geef een situatie waarin ze allemaal waar zijn.

Dit verschil in bewijslast voor de twee partijen is de logische zin van het Romeinse rechtsprincipe van 'onschuldig zijn tot het tegendeel is bewezen'. De advocaat hoeft niets te bewijzen: hij kan volstaan met verzinnen van een scenario waarin zijn cliënt A het niet gedaan heeft. (Met name kan de beklaagde de misdaad wel degelijk begaan hebben in de echte situatie!) In het hier gegeven geval kan de advocaat inderdaad zo'n consistent scenario geven, en wel door zich vast te leggen op de feiten combinatie

$$\neg A, B, C.$$

Hij moet daartoe dus wel de schuld van anderen opperen... Het opmerkelijke van een juridisch voorbeeld is dat precisie in redeneren soms een zaak van leven of dood kan zijn!

Dit samenleven van twee tegenovergestelde, maar nauw verwante logische taken: 'vind een bewijs' en 'blijf consistent' is heel algemeen, zowel in de dagelijkse praktijk als in de wiskunde. Denk aan de historische discussie over het vijfde postulaat van Euclides ($P5$) in 6.1. Eerst dacht men te kunnen bewijzen dat $P5$ uit de overige vier te bewijzen was. Maar Lobatsjevski liet zien dat dit niet het geval was, door een situatie te geven van een 'alternatieve meetkunde' waarin de eerste vier postulaten gelden tezamen met de negatie van het vijfde. In een gesprek gaat het vaak zelfs primair om handhaven van consistentie. De spreker doet allerlei beweringen, zeg over een exotische vakantiebelevenis, en zolang die consistent zijn (d.w.z., ze zouden allemaal samen waar kunnen zijn) kan hij doorgaan – hoewel het natuurlijk wel gaandeweg een 'sterk verhaal' kan worden. Bewijzen worden ook wel gebruikt in conversatie, maar dan eerder door een kritische toehoorder, die met kleine gevolgtrekkingen uit wat de spreker zo allemaal beweert probeert om onware consequenties leiden.

Geldigheid testen: semantische tableaus

In het bovenstaande deden we een beroep op intuïties van de lezer als we beweerden dat een gevolgtrekking al dan niet geldig was. Maar er bestaan diverse methoden om logische geldigheid meer exact te testen. Een veel voorkomende algemene manier is het zoeken van een formeel bewijs, een keten van kleine inzichtelijke stapjes die de conclusie uit de premissen te voorschijn tovert. Dit volgt het Euclidische model van meetkundig bewijzen. Maar voor speciale logische systemen zijn er vaak meer bijzondere methoden die met andere principes werken. Een voorbeeld is de rekenmethode der waarheidstafels voor propositielogica in het volgende hoofdstuk. In het vervolg hier bespreken we kort een elegante methode, die werkt voor zowel propositielogica als kwantorlogica, bedacht door de Amsterdamse logicus Evert Beth in de jaren vijftig van de vorige eeuw. Beth's methode richt het zoeklicht op *ongeldigheid*:

> We zoeken een tegenvoorbeeld voor een gegeven gevolgtrekking $P_1, ..., P_k \Rightarrow C$: een situatie die alle premissen waar maakt, doch de conclusie onwaar.

Anders gezegd, tableaus onderzoeken een consistentieprobleem in de bovenstaande zin, en wel voor $P_1, ..., P_k, \neg C$. We zullen deze methode hier uitleggen, om een concrete indruk te geven van een formeel wiskundig systeem dat een genre redeneren expliciet en volledig analyseert. Als opstapje bespreken we een simpel voorbeeld uit het voorgaande. De gevolgtrekking $A \vee B, \neg A \Rightarrow B$ was intuïtief geldig. Dit testen we nu preciezer als volgt. Stel eens dat er een tegenvoorbeeld was. Dan moet er een situatie zijn met de twee premissen waar, en de conclusie onwaar. We schrijven dit als een topknoop, met de premissen links, en de conclusie rechts.

$$A \vee B, \neg A \bullet B$$

P 16.

EVERT WILLEM BETH

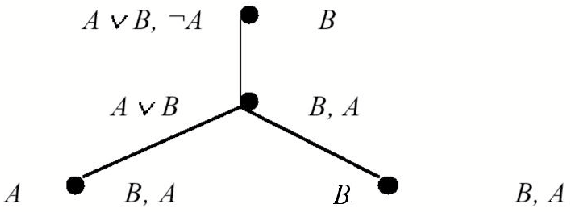
1909 — 1964

Een dergelijke formulering noemen we een *sequent*. Links van de stip staan de uitspraken die *waar* moeten worden, en rechts de uitspraken die *onwaar* moeten worden. Kan zo'n situatie bestaan? Om dit te onderzoeken gaan we *reductieregels* toepassen, die de sequent omzetten in één of meer gereduceerde vormen van het probleem. Aldus ontstaat gaandeweg een boom van alle mogelijkheden om aan een tegenvoorbeeld te komen: een z.g. *semantisch tableau*. Reductieregels werken op de aanwezige logische operaties. De eerste luidt als volgt. Een negatie $\neg A$ links zegt dat $\neg A$ waar moet worden, hetgeen equivalent is met zeggen dat A onwaar moet worden. Dus kunnen we de $\neg A$ links weghalen en vervangen door een A rechts:

$$A \vee B,\ \neg A \quad\bullet\quad B$$

$$A \vee B \quad\bullet\quad B,\ A$$

Merk op dat de complexiteit van ons probleem in deze stap is gedaald: er is één logische operatie verdwenen. Nu moeten we de disjunctie links analyseren. Deze is waar in twee gevallen: A is waar, of B is waar. Er ontstaan dus twee mogelijkheden om te onderzoeken, hetgeen we aangeven door een *splitsing* van het tableau:

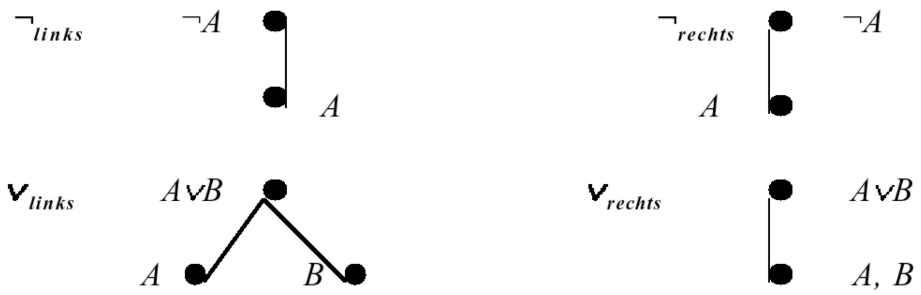


Beide takken staan dus voor een mogelijk tegenvoorbeeld tegen de oorspronkelijke gevolgtrekking. In de eindknopen kunnen we nu geen logische operatoren meer analyseren. In dat geval is rechtstreeks te zien of hier een vervulbare taak staat. Bijvoorbeeld links moet A waar worden, maar A en B ook allebei onwaar. Dit is een tegenspraak! En eenzelfde probleem geldt rechts. Het algemene principe luidt als volgt:

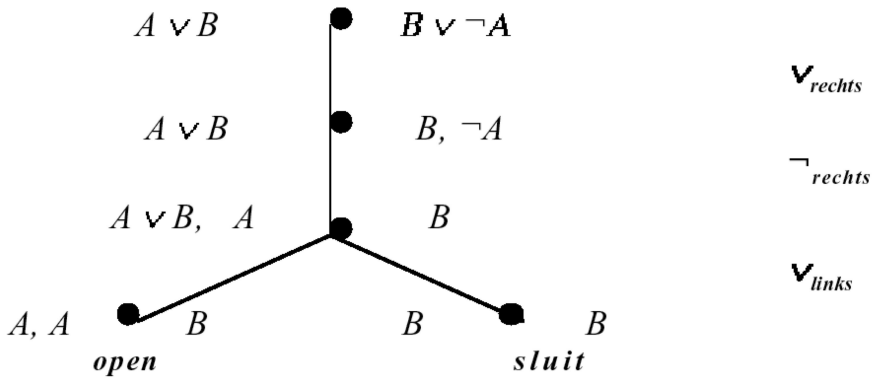
> Een knoop zonder logische operaties levert een tegenvoorbeeld als geen bewering zowel links als rechts staat. De knoop heet in dat geval *open*. In het andere geval kan de knoop geen tegenvoorbeeld representeren, en zeggen we dat de knoop *sluit*.

We zien dat in de gegeven boom beide takken sluiten in hun eindknoop. Als alle takken gesloten zijn, dan heet het hele tableau gesloten. Er bestaat dan geen tegenvoorbeeld voor de oorspronkelijke gevolgtrekking, en deze is dus geldig. Dat $A \rightarrow B, \neg A \Rightarrow B$ geldig was hadden we natuurlijk al eerder gezien, maar het tableau maakt de reden heel inzichtelijk.

Een echt bruikbaar tableau-systeem ontstaat door een volledig stel reductieregels vast te leggen voor de Boolese operaties. Hier zijn die regels voor negatie en disjunctie:



Met name splitst een disjunctie rechts het tableau niet, want een inclusieve disjunctie $A \vee B$ is alleen onwaar als zowel A als B onwaar zijn. Met deze regels kunnen we alle gevolgtrekkingen testen die berusten op negatie en disjunctie. Hier is nog een voorbeeld. Geldt $A \vee B \Rightarrow B \vee \neg A$? De lezer kan misschien even zelf een vermoeden formuleren alvorens het formele tableau te lezen.

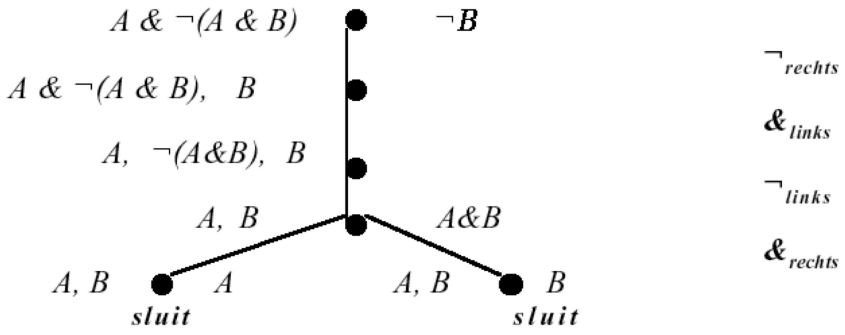


Kennelijk sluit in dit tableau de rechtertak. Maar de linkertak blijft open. We kunnen namelijk tegelijkertijd A waar maken en B onwaar. Dit levert een tegenvoorbeeld, want in deze situatie is $A \vee B$ waar, maar $B \vee \neg A$ juist onwaar.

Door herhaalde toepassing van reductieregels ontstaat uiteindelijk een boom van alle potentiële tegenvoorbeelden, die mechanisch een antwoord geeft. Als er een tak open blijft, dan lezen we een tegenvoorbeeld af; als alle takken sluiten, dan hebben we geldigheid voor de gegeven gevolgtrekking. We zien hier dat tableaus geen voorkeur hebben voor 'positieve' of 'negatieve' antwoorden. Beide gevallen bevatten interessante informatie. Een tableau dat sluit is een soort bewijs voor de gegeven gevolgtrekking; maar open takken zijn ook informatief, als recept om een gegeven stel beweringen tegelijkertijd waar te maken. Tableaus zijn daarmee ook een testmethode voor consistentieproblemen.

Om de methode te completeren hebben we ook regels nodig voor de andere Boolese operaties uit de propositielogica. We geven hier alleen de regels voor de conjunctie, die lijken op die voor de disjunctie.

Het volgende gesloten tableau laat zien dat $A \wedge \neg(A \wedge B) \Rightarrow \neg B$ geldig is.



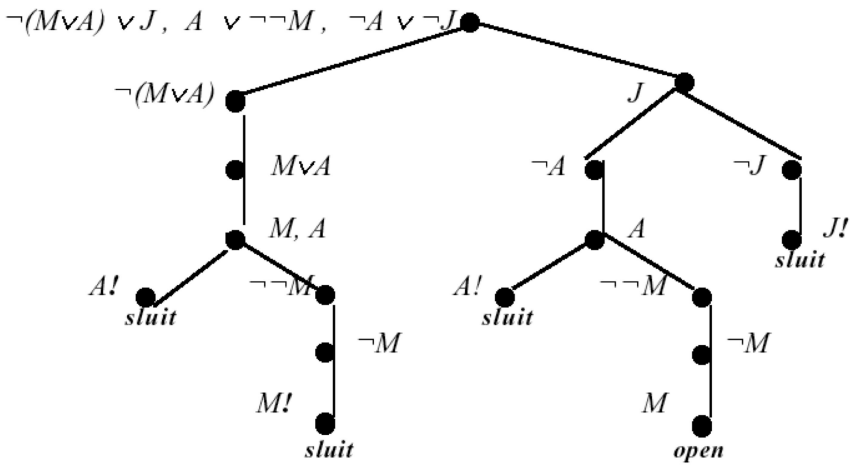
De mooie harmonie tussen disjunctie en conjunctie weerspiegelt zich in het hele verdere systeem van geldigheden van de propositielogica. Zo hebben bijv. de twee eerder genoemde logische wetten van Distributiviteit en De Morgan ook geldige tegenhangers die disjunctie en conjunctie verwisselen:

$(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$ Tweede Distributiviteitswet

$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$ Tweede De Morgan Wet

Tableauregels voor de resterende operaties van implicatie en equivalentie zijn net zo eenvoudig te geven. Al onze eerdere voorbeelden van propositioneel redeneren zijn dan met tableaus te behandelen. $\overset{\text{T. 22}}{\Longrightarrow}$ 188
Zuiver als grafische illustratie laten we een tableau zien voor het eerdere Feestje. Daarbij hebben we alle formules eerst voor het gemak even omgeschreven naar een equivalente vorm met alleen disjuncties en negaties, volgens het geldige propositielogische principe

$$A \rightarrow B \Leftrightarrow \neg A \vee B:$$



Alleen de essentiële formules staan aangegeven. De enige open tak correspondeert met de eerdere unieke consistente oplossing: links op de 'ware kant' staan J, M, en rechts op de 'onware kant' staat A. Het zal duidelijk zijn dat dit tableau meer werk kost dan de korte redenering die we eerder gaven als oplossing. Maar een voordeel van deze systematische machinerie is wel dat een rekenmachine deze tableau-oplossing mechanisch kan vinden, en niet alleen in dit speciale geval, maar ook voor alle mogelijke varianten. $\overset{\text{T. 23}}{\Longrightarrow}$ 189

Eigenschappen van bewijssystemen

Semantische tableaus zijn een overzichtelijke grafische methode om logisch geldigheidsvragen te analyseren. Studenten leren deze methode met gemak in de praktijk, en ook een computer kan worden geprogrammeerd om tableaus te maken. Er bestaan diverse werkende 'tableau provers' in de wereld van de automatische deductie. Maar een dergelijke rekenmethode werpt ook een aantal vragen op. $\overset{\text{T. 23}}{\Longrightarrow}$ 189
We geven enkele formules als input, en krijgen op een gegeven moment een antwoord "Ja" of "Nee" inzake geldigheid. Als we dit niet zomaar als orakel willen accepteren, dan moeten we die methode zelf nader bestuderen. Om te beginnen, zijn de antwoorden die we krijgen betrouwbaar? Men noemt dit wel de *correctheid* (Engels: 'soundness') van de methode. En inderdaad geldt volgens de eerdere definitie van geldigheid dat:

> *Correctheid van de tableaumethode*:
> Gesloten tableaus corresponderen met een geldige gevolgtrekking, open tableaus corresponderen met een ongeldige gevolgtrekking.

Tableaus

Om het tableau-systeem voor het propositie-logische deel te vervolmaken hebben we nog vier regels nodig voor implicaties en equivalenties. Voor beide connectieven definiëren we een linker- en een rechterregel.

$$\frac{\varphi \to \psi \bullet}{\psi \bullet \quad \bullet \varphi} \qquad \frac{\bullet \varphi \to \psi}{\varphi \bullet \psi} \qquad \frac{\varphi \leftrightarrow \psi \bullet}{\varphi, \psi \bullet \quad \bullet \varphi, \psi} \qquad \frac{\bullet \varphi \leftrightarrow \psi}{\varphi \bullet \psi \quad \psi \bullet \varphi}$$

Het is niet lastig om met de waarheidstabellen bij de hand de correctheid van de regels te verifiëren.
De regels voor kwantoren zijn wat lastiger. In dit geval moet een te construeren tegenmodel ook individuen bevatten. Deze worden tijdens de ontwikkeling van het tableau geïntroduceerd.

$$\frac{\forall x\, \varphi \bullet}{\varphi[a_1/x], ..., \varphi[a_n/x] \bullet} \qquad \frac{\bullet \forall x\, \varphi}{\bullet \varphi[a_{n+1}/x]} \qquad \frac{\exists x\, \varphi \bullet}{\varphi[a_{n+1}/x] \bullet} \qquad \frac{\bullet \exists x\, \varphi}{\bullet \varphi[a_1/x], ..., \varphi[a_n/x]}$$

In deze regels gaan we er van uit dat er al n individuen, $a_1, ...a_n$ geïntroduceerd zijn. De rechterregel voor $\forall$ en de linkerregel $\exists$ introduceren een nieuw individu die we a_{n+1} noemen om hem te onderscheiden van de reeds geïntroduceerde individuen. Deze nieuweling wordt gesubstitueerd voor alle vrije voorkomens van de variabele x in het gekwantificeerde deel φ. Het resultaat schrijven we als $\varphi[a_{n+1}/x]$: "a_{n+1} is een φ". In de linker-regel wordt a_{n+1} opgevoerd als een getuige van φ-heid omdat $\exists x\, \varphi$ bewaarheid moet worden. In de rechter-regel komt de zelfde formule rechts te staan waarmee getracht wordt $\forall x\, \varphi$ te falsifiëren. a_{n+1} wordt in de volgende zet opgevoerd als een tegenvoorbeeld van φ-heid om de universele formule onwaar te krijgen. De overige twee regels, de eerste en de laatste, leggen een universele eis op het tegenmodel. Dit manifesteert zich in de regel door de gekwantificeerde eigenschap toe te passen op alle tot dan toe geïntroduceerde individuen. Als die er nog niet waren dan nemen we a_1 omdat een model nooit leeg mag zijn. In het geval van $\forall$-links wordt φ waar gemaakt voor alle instanties, en in het geval van $\exists$-rechts wordt φ voor alle mogelijke instanties ontkend.
Het probleem met de laatste twee regels is dat de formule niet echt 'weggewerkt' hoeft te zijn. Als er een nieuw individu wordt geïntroduceerd door een van de andere twee regels dan worden de originele formules weer actief: ze moeten bevestigd dan wel ontkend worden voor mogelijk nieuwe individuen. Om het één ander te illustreren twee voorbeelden die we al eerder tegenkwamen.

$\exists y \forall x\, Rxy$	$\bullet$	$\forall x \exists y\, Rxy$
$\forall x\, Rxa_1$	$\bullet$	
	$\bullet$	$\exists y\, Ra_2y$
Ra_1a_2, Ra_2a_2	$\bullet$	
	$\bullet$	Ra_2a_1, Ra_2a_2

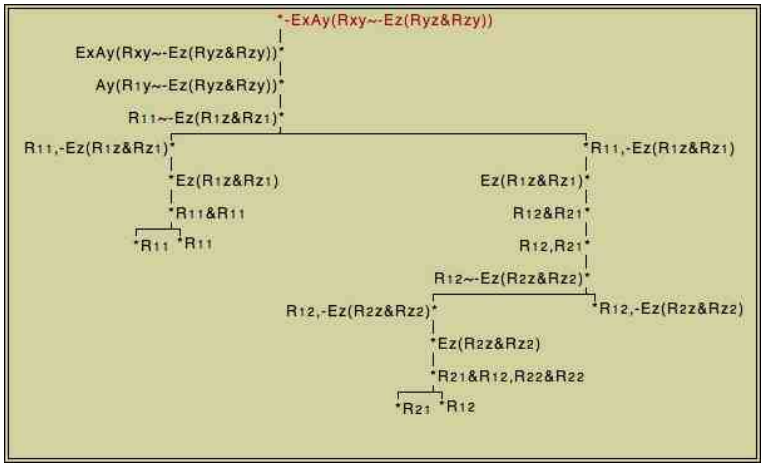
$$\begin{array}{c} \forall x \exists y\, Rxy \bullet \exists y \forall x\, Rxy \\ \hline \exists y\, Ra_1y \bullet \\ \hline \bullet \forall x\, Rxa_1 \\ \hline Ra_1a_2 \bullet \\ \hline \bullet\, Ra_3a_1 \\ \hline \vdots \end{array}$$

Het linker tableau sluit. Het gevonden tegenmodel wat nu onstaat is een model wat Ra_2a_2 waar maakt en tegelijkertijd onwaar. We hebben daarmee onze verlangde tegenspraak. De tableau-methode is nu zo sterk dat dit direct elk tegenmodel uitsluit en dus is $\exists y \forall x\, Rxy \Rightarrow \forall x \exists y\, Rxy$ een geldige redenering. M.a.w., de tableau-methode is correct*. Sterker nog, de methode is ook* volledig*, hetgeen wil zeggen dat er voor elke geldige redenering een sluitend tableau is te geven!*
Moeilijker ligt het met ongeldige redeneringen. Een voorbeeld daarvan is het rechter-tableau. In de laatste twee stappen zijn er nieuwe individuen opgevoerd. Dit maakt dat de tak (nog) niet open is. De beginformules zijn opnieuw actief geworden en moeten weer geïnstantieerd worden voor de nieuwelingen. In dit geval blijft de geboorte van nieuwe individuen doorgaan en we krijgen een oneindige tak. Het tableau is een oneindig tegenmodel aan het maken. Het volledigheidsresultaat voor tableaus zegt ons dat de redenering dan ongeldig moet zijn, maar het is helaas niet altijd mogelijk vast te stellen dat er een oneindige tak bezig is zich te ontwikkelen.
Er zijn alternatieve regels voor $\forall$-links en $\exists$-rechts te geven met hergebruik van 'oude' individuen, waarmee eindige tegenmodellen voorrang gegeven kunnen worden. Zo'n methode zal werken voor het specifieke geval hierboven, maar er blijft een probleem. Er zijn redeneringen met slechts oneindige tegenmodellen!

Machinale deductie

Zowel de tableau-methode als het in de tekst besproken resolutie-mechanisme lenen zich uitstekend voor het automatiseren van deductie. Resolutie is het inferentie-principe wat achter 'logisch programmeren' steekt, waarbij de predicatenlogica zelf als programmeertaal wordt gebruikt. Het leent zich echter minder voor presentatie alhier omdat de lijn van deductie die gevolgd wordt ver verwijderd is van onze eigen redeneertrant. Bij gebruik van tableau's kan vaak wel een analogie met menselijk redeneren getrokken worden. Hieronder ziet u de uitdraai van een computer die volgens de regels als uitgelegd in T.22 de onvervulbaarheid van de zogenaamde Quine paradox — naar de filosoof en logicus Willard Van Orman Quine — aantoont.

$$\exists x \, \forall y \, (Rxy \leftrightarrow \neg \exists z \, (Ryz \wedge Rzy))$$



De formule is een tweelingbroertje van de Russell-paradox. Hij laat zich wat minder makkelijk uitleggen met behulp van verzameling of knippende kappers als in 6.1, maar met een andere relatie: R is 'kent' in een domein van personen. Het tweede gedeelte van de formule $\exists z \, (Ryz \wedge Rzy)$ zegt dan dat y iemand kent die y weer kent: 'een kennis'. De formule zegt dus dat er een persoon (x) bestaat, de Quine persoon — noem hem q — die een persoon y kent dan en slecht dan als y zonder kennissen is. Er zijn twee mogelijkheden q kent zichzelf, of niet. In het eerste geval hebben we direct een tegenspraak want als q zichzelf kent dan heeft hij een kennis: zichzelf. Als q zichzelf niet kent dan moet volgens de formule q een kennis hebben — noem haar r. Maar dan kent q iemand met een kennis. Wederom een tegenspraak.
De tableau-machine heeft dezelfde argumentatie gevonden, met dat verschil dat q 1 heet en r 2. Verder zijn de logische tekens door symbolen van het toetsenbord gebruikt. ($\sim$ staat hier voor $\leftrightarrow$). Voor de splitsing heeft hij gevonden dat 1 zichzelf kent dan en slechts dan als hij geen kennissen heeft. De equivalentie geeft twee mogelijkheden (zie ook T.22): "1 kent zichzelf en heeft geen kennis" en "1 kent zichzelf niet en heeft wel kennissen". De eerste mogelijkheid geeft, net zoals hierboven, het snelst aanleiding tot een tegenspraak. De tweede tak is een stuk langer wat veroorzaakt wordt door de introductie van het tweede individu in de derde stap na de splitsing als kennis van 1: $R12 \wedge R21$. Hierdoor wordt de universeel gekwantificeerde formule $\forall y \, (R1y \leftrightarrow \neg \exists z \, (Ryz \wedge Ryz))$ opnieuw geactiveerd. Hij moet ook op 2 toegepast worden om hem opnieuw weg te krijgen. Het resultaat: "1 kent 2 dan en slechts dan als 2 geen kennissen heeft". 2 was opgevoerd als kennis van 1, wat er voor zorgt dat deze keer de tak aan de rechterkant direct sluit. Er wordt in de resterende "1 kent 2"-tak geconcludeerd dat 2 geen kennissen heeft en dus kent 1 2 niet of 2 kent 1 niet wat in beide gevallen sluiting geeft met 2 als kennis van 1 vlak voor de splitsing afgeleid.

We zullen deze bewering hier niet bewijzen: de details vergen wiskundige inducties op het aantal knopen in tableaus, en op de lengte van formules die op takken voorkomen. Merk alleen op dat we hier verschillende niveaus van 'bewijzen' combineren. Immers, we zijn nu geïnteresseerd in aantonen van beweringen over een bewijssysteem: men noemt deze laatste wel 'meta-beweringen'.

Maar correctheid is slechts de helft van wat we wensen. Liefst hebben we ook *volledigheid* (Engels: "completeness"): de methode moet elk correct antwoord ook werkelijk vinden. Ook dit is voor onze methode te bewijzen:

> *Volledigheid van de tableaumethode*:
> Elke geldige gevolgtrekking is af te lezen uit een gesloten tableau, elke ongeldige gevolgtrekking heeft een tegenvoorbeeld in een open tableau.

Dit is een werkelijk een extra eigenschap. Correctheid impliceert in het algemeen niet volledigheid. Er kunnen best correcte deelmethoden zijn voor een probleem die niet alle antwoorden opleveren. Een extreem voorbeeld van zo'n veilige maar onvolledige methode is om helemaal nooit enig antwoord te geven! De twee desiderata van correctheid en volledigheid komen ook buiten de logica vaak voor. Denk aan het gedrag van programma's in de informatica: u wilt dat bij gegeven invoer het antwoord dat op het scherm van uw computer verschijnt betrouwbaar is, en verder ook dat, als er een antwoord is, dat dan ook op het scherm te zien komt. Of in termen van een eerder scenario, in de rechtspraak geldt het adagium "The truth: the whole truth, and nothing but the truth". Het eerste vraagt om volledigheid, het tweede om correctheid.

Maar naast correctheid en volledigheid zijn we ook genteresseerd in de 'rekenkosten' van het verkrijgen van gewenste antwoorden. Nu is makkelijk in te zien dat Beth's methode althans voor de propositielogica een computationeel zeer gewenste eigenschap heeft. De constructie van een tableau loopt altijd na eindig veel stappen af, daar de reductieregels het aantal logische operaties in een probleem steeds verminderen. In computertermen: de methode loopt nooit vast, en draait nooit oneindig dol. We zeggen dit als volgt:

> Geldigheid in de propositielogica is *beslisbaar*.

Dat wil zeggen, er is een mechanische methode die geldigheid test voor alle gegeven gevolgtrekkingen, en die na eindig veel stappen met een antwoord komt.

Voor de propositielogica hebben we dus een universele 'logische machine'. Beroemde logici en wiskundigen hebben lang gemeend dat dergelijke machines moeten bestaan voor alle logische taken. Zo ontwierp Leibniz een project voor een 'Calculus Ratiocinator' die alle menselijke meningsverschillen objectief door rekenwerk moest beslechten. In het volgende hoofdstuk zullen we echter zien dat beslisbaarheid een uitzonderlijke situatie is in de wiskunde, en zelfs binnen de logica. En zelfs wanneer beslisbaarheid optreedt, liggen er toch nog serieuze drempels van computationele complexiteit, die een methode onbruikbaar kunnen maken. Als voorproefje geeft T.22 een tableau-versie voor de predicatenlogica, waar de boom oneindige takken kan bevatten, zodat beslisbaarheid in gevaar komt– en in feite verdwijnt. Dit brengt ons bij de vraag hoe logische bewijssystemen er eigenlijk uitzien voor andere wiskundig wezenlijke operaties, zoals met name de kwantoren.

Andere bewijssystemen: kwantoren

Reeds uit de Oudheid bekend zijn de 'syllogismen' van Aristoteles, die telkens uit twee kwantorbeweringen een derde afleiden. Ze werden in de Middeleeuwen aan alle universiteiten onderwezen, en in diverse landen krijgen adolescenten ze zelfs op middelbare scholen. Misschien wel het beroemdste syllogisme is het volgende bewijspatroon, 'Barbara' geheten naar een middeleeuwse terminologie:

Alle A zijn B Alle B zijn C: dus Alle A zijn C

Bijvoorbeeld, alle Nederlanders zijn mensen, alle mensen zijn zoogdieren, en dus zijn alle Nederlanders zoogdieren. Iets ingewikkelder syllogismen gebruiken verschillende kwantor-uitdrukkingen. Uit het feit dat sommige Nederlanders piano spelen, en het feit dat geen haai piano speelt, volgt dat niet alle Nederlanders haaien zijn:

Sommige A zijn B Geen C is B: dus Niet alle A zijn C

Deze overzichtelijke notatie doet niet toevallig denken aan de kwantoren in natuurlijke taal, die we in hoofdstuk 1 nader hebben bekeken. Weer zal de lezer snel allerlei andere patronen zien. Zo spelen in de achtergrond van syllogismen ook veel gebruikte logische equivalenties tussen kwantor-beweringen, zoals

"Niet alle A zijn B" is equivalent met "Sommige A zijn niet B",
"Alle A zijn niet-B" is equivalent met "Geen A is B".

In hun tijd waren syllogismen al heel formeel, en de notatie met variabele letters was een grote vernieuwing. Maar wij kunnen natuurlijk ook onze moderne formules schrijven voor kwantor-patronen. Hier is een lijstje met voorbeelden:

$$\begin{array}{rcll} \forall x\,(Px \wedge Qx) & \Rightarrow & \forall x\,Px \wedge \forall x\,Qx & \text{geldig} \\ \forall x\,Px \wedge \forall x\,Qx & \Rightarrow & \forall x\,(Px \wedge Qx) & \text{geldig} \\ \forall x\,(Px \vee Qx) & \Rightarrow & \forall x\,Px \vee \forall x\,Qx & \text{ongeldig} \\ \forall x\,Px \vee \forall x\,Qx) & \Rightarrow & \forall x\,(Px \vee Qx) & \text{geldig} \end{array}$$

Vier soortgelijke observaties zijn te maken voor de existentiële kwantor. Deze kunnen we juist wel geldig 'distribueren' over een disjunctie, maar niet over een conjunctie.

Syllogismen gaan steeds over enkelvoudige kwantoren. Maar in de analyse van wiskundig bewijzen stuit men al gauw op patronen met herhaalde kwantoren, omdat veel wiskundige begrippen een structuur hebben met meerdere herhaalde kwantoren: twee, of zelfs meer– zoals we in Hoofdstuk 1 op diverse plaatsen zagen. Ook dit kennen we al uit onze gewone taal. We concluderen moeiteloos uit het gegeven dat er iemand is die iedereen bemint – zeg Moeder Theresa — dat iedereen door iemand wordt bemind.

$$\exists x\,\forall\, y Rxy \Rightarrow \forall\, y \exists x\, Rxy \text{ is geldig.}$$

Als er iemand is die van iedereen houdt — zeg Moeder Theresa — dan wordt iedereen door iemand bemind. Als een graaf een rood punt heeft vanwaaruit elk ander punt is te bereiken, dan is elk punt vanuit een rood punt te bereiken. Maar we weten ook dat het omgekeerde patroon juist gevaarlijk is:

$$\forall y\, \exists x\, Rxy \Rightarrow \exists x\, \forall y\, Rxy \text{ is ongeldig.}$$

Ieder mens wordt bemind door zijn moeder (laten we maar hopen), maar dat betekent nog niet dat er iemand is die ieder mens bemint. Of een getallentegenvoorbeeld: voor elk natuurlijk getal is er een groter getal, maar er is zeker geen getal dat groter is dan ieder getal.

De kwantoren $\forall$ en $\exists$ zijn bijzonder krachtig, en volstaan, zoals we in het eerste hoofdstuk zagen, voor het formuleren van de verzamelingenleer. Bewijssystemen voor predicatenlogica zijn dan ook in principe geschikt voor het formaliseren van de gehele wiskunde — al hebben logici hiervoor ook nog wel andere systemen ontwikkeld. Niettemin kunnen we ook praktisch heel goed redeneren met $\forall$, $\exists$, en andere kwantor-uitdrukkingen, al vergt dat laatste soms wat meer nadenken. Hier is een kleine oefening voor de lezer. We schrijven

$\exists!x\,\varphi(x)$ voor 'er is precies één object x met de eigenschap φ '

Nu gelden voor de gewone kwantoren twee simpele omwisselingsprincipes van volgorde: $\forall x\,\forall y\,Rxy \Leftrightarrow \forall y\,\forall x\,Rxy$ en $\exists x\,\exists\,yRxy \Leftrightarrow \exists y\,\exists x\,Rxy$. Maar geldt nu ook $\exists!x\,\exists!\,yRxy \Leftrightarrow \exists!y\,\exists!x\,Rxy$? Stel dat er precies één zee is die door één zeeman is bevaren. Volgt dan dat er precies één zeeman is die precies één zee heeft bevaren? We laten het antwoord aan de lezer.

Logici bestuderen nog vele verdere genres bewijzen die van belang zijn in de wiskunde. Voorbeelden zijn redeneren met kennis en met waarschijnlijkheid, die in eerdere hoofdstukken werden besproken.

Logische systemen: tussen beslisbaar en onbeslisbaar

De enkele impressionistische voorbeelden tot nu toe vormen zeker niet het volledige systeem van geldige principes in de predicatenlogica. Een dergelijk systeem is wel te vinden, maar het vergt bijvoorbeeld een niet-triviale uitbreiding van de methode der semantische tableaus, die weer veilig en
T. 22 ⟸ 188
volledig blijkt. De details van zo'n methode zijn voor ons doel echter niet van belang. In plaats daarvan besluiten we met een algemene opmerking over de *complexiteit* van de predicatenlogica, als contrapunt bij onze propositielogische voorbeelden. De taal van de kwantoren is wezenlijk rijker dan die van de Boolese operaties. Immers, we kunnen nu rechtstreeks verzamelingen objecten beschrijven met hun eigenschappen en relaties, zoals getallenruimten, grafen, meetkundige ruimtes, of groepen — en evengoed allerlei praktische gespreksdomeinen, zoals het Nederlands Elftal, of de polder-structuur van Noord-Holland. Maar juist door die rijkdom speelt weer de kwestie 'eindig' versus 'oneindig' uit ons eerste hoofdstuk. Om te beginnen kan de predicaatlogische taal oneindig veel verschillende situaties onderscheiden. Denk alleen al aan eindige lineaire ordeningen, die iedere eindige grootte kunnen hebben. En bovendien kunnen de beschreven situaties zelf ook nog eens oneindig veel objecten bevatten, zoals getalstructuren, of het aantal ruimtelijke punten dat u kunt omvatten met uw hand.

Nu spreekt geldigheid van een predicaatlogische logische gevolgtrekking volgens de eerder gegeven definitie over al deze oneindig veel situaties: overal waar de premissen waar zijn, moet ook de conclusie waar zijn. Dit is dus principieel niet na te rekenen door alle mogelijkheden op te sommen, zoals dat in de propositielogica wel kan. Hier is een iets meer concrete illustratie van deze complexiteit.

Redeneren over communicatienetwerken Laat een eindige graaf gegeven zijn met punten opgevat als personen, en pijlen als de richting van mogelijke communicatie. Neem nu aan dat een graaf veel communicatie heeft, en wel als volgt: tussen elk tweetal verschillende objecten x, y loopt een pijl : d.w.z. van x naar y, of omgekeerd, om misschien in beide richtingen. Als u nu plaatjes probeert te tekenen van zulk soort netwerken, dan zal u een patroon opvallen. Er is altijd iemand die alle anderen in hoogstens twee communicatiestappen kan bereiken, een 'Great Communicator'. Dat dit ook altijd zo moet zijn is in te zien met inductie naar de grootte van de graaf. We geven het bewijs omdat het simpel is, en toch verrassend.

In een graaf met 1 object is de bewering zeker waar. Stel nu dat een graaf $n + 1$ objecten heeft, en neem er een punt uit, zeg x. Volgens de inductiehypothese heeft de resterende subgraaf met n objecten op zichzelf beschouwd een Great Communicator y. We vergelijken nu x en y.

Geval 1 y kan via 1 of 2 pijlen x bereiken. Dan is y ook een Great Communicator in de hele groep.

Geval 2 y kan niet via 1 of 2 pijlen x bereiken. Dan moet x een Grote Communicator zijn! Merk om te beginnen op dat er een pijl moet lopen van x naar y, vanwege het gegeven. Laat nu z een willekeurig object zijn verschillend van x.

Geval 2.1 y bereikt z met 1 pijl. Dan doet x dat met twee pijlen, en klaar.

Geval 2.2 y bereikt z met 2 pijlen, maar niet met een enkele. Laat de tussenstap object v zijn. We weten dat er geen pijl loopt van v naar x, want anders was x toch in twee stappen vanuit y bereikbaar. Dus geldt het omgekeerde: er loopt een pijl van x naar v, en dus kan x z via twee pijlen bereiken.

Mogen we nu dus concluderen dat uit de formule $\forall x \forall y ((Rxy \vee Ryz)$ voor de 'communicatie-dichtheid' logisch volgt dat er een Great Communicator is, d.w.z. $\exists x \forall y ((Rxy \vee \exists z (Rxz \wedge Rzy))$? Op eindige verzamelingen is dit inderdaad een gewettigde conclusie, blijkens ons argument. Maar, de gevolgtrekking is toch ongeldig, omdat er *oneindige* tegenvoorbeelden bestaan. Neem bijv. als domein de gehele getallen, en als relatie R 'kleiner dan of gelijk' . Geen enkel getal n is een Great Communicator, omdat de kleinere getallen nooit zijn te bereiken.

Deze noodzaak van oneindige tegenvoorbeelden blijkt ook bij semantische tableaus voor predicatenlogica. De tableau-boom zal, om deze te vinden, oneindige takken moeten bevatten. Hiermee vervalt de eenvoud van de eindige tableau-bomen voor alleen Boolese operaties, en we hebben niet langer een beslissingsmethode. In hoofdstuk 7 zullen we zelfs zien dat dit falen onvermijdelijk is. Een van de vele ontnuchterende gevolgen van Gödel's beroemde Onvolledigheidsstellingen is dat de kwantor-logica 'onbeslisbaar' is. Geen enkele eindige methode kan de geldigheid correct en volledig testen! Anders gezegd, een rijk logisch systeem als de predicatenlogica bekoopt haar grotere uitdrukkingskracht, vergeleken bij de propositielogica, met een veel hogere complexiteit van geldig redeneren. Deze balans tussen de uitdrukkingskracht van een taal en de complexiteit van haar logisch redeneren is een algemeen verschijnsel door de hele wiskunde en informatica heen.

In dit perspectief laat ons eerdere hoofdstuk 2 dan nog een vraag open. We vonden daar, in de studie van bisimulatie-invariantie op procesgrafen, een intermediaire taal tussen propositie- en kwantor-logica, en wel de *modale logica*. Deze was rijker dan de propositielogica, en kon tot op zekere hoogte met modaliteiten $\langle a \rangle, [b]$ het bestaan van acties beschrijven tussen toestanden. Maar ze was wel beperkter in haar uitdrukkingskracht dan predicatenlogica in het algemeen. Hier ligt de balans inderdaad anders. Geldigheid voor redeneren in modale logica blijft beslisbaar, net als in de propositielogica. Maar het is wel computationeel complexer dan dat laatste systeem. Preciezer kunnen we dit onderscheid pas maken in hoofdstuk 7, waar we wiskundige definities geven van het begrip complexiteit van berekeningen.

Bewijssystemen in de wiskunde

Hiermee zijn we aan het eind gekomen van onze algemene inleiding in logische geldigheid en bewijssystemen. Om deze begrippen in hun juiste context te plaatsen, moeten we echter iets breder in de wetenschap kijken. Allereerst zijn moderne logische systemen eindpunt van een lange historische ontwikkeling. Systematische bewijzen in een samenhangend systeem ontstonden voor het eerst in de Griekse wiskunde vanaf 500 voor Christus. Zo heeft Euclides' "Elementen"vele eeuwen het onderwijs bepaald, met een strakke opzet van 'gegeven, stelling, bewijs' voor meetkundig redeneren. Dat redeneren vindt plaats vanuit een vast repertoire van toegestane stappen, met een vooraf expliciet door de auteur gegeven stelsel van uitgangspunten. Deze komen in een drietal genres. Om te beginnen hebben we

Definities, zoals

Een lijn is lengte zonder breedte.
Lijnen zijn evenwijdig als ze elkaar ook bij verlenging nooit snijden.

Axioma's, zoals

Tussen elk tweetal punten loopt een lijn.

Om elk punt met gegeven lijnstuk loopt een cirkel met dat lijnstuk als straal.

Door elk punt niet op een lijn loopt één lijn parallel aan de gegeven lijn.

Dit laatste axioma is het beroemde 'Vijfde Parallellen-postulaat' dat we al eerder in 6.1 bespraken. Daarnaast bevatten de 'Elementen' ook een aantal zogenaamde

Algemene Begrippen , zoals

Optellen van gelijken bij gelijken levert gelijken.

Twee dingen die gelijk zijn aan een derde zijn gelijk aan elkaar.

Dit zijn meer 'logische' principes, die in elke wiskundige context bruikbaar zijn: meetkundig, maar ook algebraïsch. Door deze drie groepen van simpele principes nu maar steeds verder te combineren worden door Euclides uiteindelijk gecompliceerde stellingen afgeleid, zoals de Stelling van Pythagoras, of de classificatie der Platonische regelmatige veelvlakken, die we al noemden in Hoofdstuk 2. Maar de 'Elementen' bevatten ook reeds belangrijke rekenkundige methoden, zoals het bewijs met natuurlijke inductie, vaak toegeschreven aan Jacob Bernoulli rond 1700.

De invloed van de 'Elementen' is immens geweest. Bewijzen bleken velerlei nut te hebben. Ze leveren precisie, en daarmee een dwingende rechtvaardiging voor een wiskundig inzicht. Maar bewijzen zorgen ook voor systematiek; ze brengen allerlei wiskundige beweringen met elkaar in verband, en suggereren door variatie weer nieuwe inzichten. Verder zorgt de abstractie van bewijzen voor ruime toepasbaarheid, net zoals bij de formele talen van Hoofdstuk 1. En er zijn nog vele andere belangrijke aspecten. Zo zijn Euclides' bewijzen vaak ook constructies om een meetkundig object te maken. In de moderne informatica vindt men evenzo bewijssystemen die automatisch programma's maken om wiskundige objecten te berekenen of te construeren.

Toch is Euclides' 'Elementen' niet het laatste woord gebleken. Met name in de achttiende en negentiende eeuw werd de bewijsvoering in de meetkunde steeds verder aangescherpt. Dit had verschillende redenen, waaronder de vele pogingen het minder evident geachte 'Parallellen-postulaat' af te leiden uit de resterende axioma's. Men trachtte dit postulaat uit de overige te bewijzen door zijn negatie $\neg P5$ aan te nemen en dan een contradictie af te leiden, een Bewijs uit het Ongerijmde dus. Dit is uiteindelijk niet gelukt, en men ontdekte op deze manier het bestaan van de zogenaamde 'niet-Euclidische meetkundes' die andere genres van ruimte beschrijven. Deze nieuwe meetkundes zijn zeer abstracte theorieën waarbij gewone ruimtelijke intuïtie met plaatjes minder helpt, zodat strenge bewijsvoering belangrijker wordt als garantie voor correctheid. Met deze toegenomen aandacht voor precisie bleken ook de 'Elementen' zelf niet waterdicht. Nieuwe axioma's bleken nodig om gaten te dichten in Euclides' bewijzen. Een soortgelijke wending naar abstracte theorievorming kenmerkt de hele wiskunde van de negentiende en twintigste eeuw. Hierbij 'kantelde' langzamerhand het beeld van een wiskundige theorie, en wel van de beschrijving van één concrete structuur naar de beschrijving van een klasse abstracte structuren die zich overal kunnen voordoen. Zo bevat Hilbert's 'Grundlagen der Geometrie' (1899) een beroemde beginpassage waarin de auteur zegt dat

> 'met punten, lijnen en vlakken bedoel ik elke willekeurige verzameling objecten die aan de gegeven axioma's voldoen'.

Was het woord 'ruimte' tot 1800 een eigennaam voor een uniek object, tegenwoordig spreken wiskundigen van talloze 'ruimten'. De eigennaam is dus een zelfstandig naamwoord geworden met een meervoud.

Formele theorieën en grondslagenonderzoek

Ondanks de groeiende precisie van de negentiende eeuwse wiskunde doken rond 1900 toch tegenspraken op in zulke fundamentele theorieën als de verzamelingenleer. Een bekend probleem is de *Russell Paradox* over de plausibel klinkende verzameling van alle verzamelingen die zichzelf niet als element hebben:

$$r = \{x \mid x \notin x\}$$

Het lijkt dat een dergelijke verzameling moet bestaan, maar het bestaan ervan leidt tot een tegenspraak! In minder virulente vorm troffen we deze tegenspraak reeds als de Kapperspuzzel — onlangs nog op televisie te zien, toen in Afghanistan na het vertrek van de Talibaan veel baarden eraf gingen. Er is niemand die alleen die mensen scheert die zichzelf niet scheren! Een bewijs hiervoor is heel inzichtelijk te geven in de kwantor-logica.

Laat Sxy staan voor "x scheert y". We zullen laten zien dat

$$\neg\exists x\,\forall y\,(Sxy \leftrightarrow \neg Syy).$$

Een bewijs werkt weer uit het ongerijmde. Stel dat $\exists x\,\forall y\,(Sxy \leftrightarrow \neg Syy)$ (*). Zij r zo'n object x. Daarvoor geldt dan $\forall y\,(Sry \leftrightarrow Syy)$. De universele kwantor zegt dat dit geldt voor elk object, en dus zeker *ook voor r zelf*: $Srr \leftrightarrow \neg Srr$. Deze laatste formule is echter altijd onwaar, en de veronderstelling (*) moet dus ook onwaar zijn.

Met deze precieze analyse van de kleinste predicaatlogische redeneerstappen werd totale formalisering van de wiskunde mogelijk. Rond 1900 ontstonden zo volledig exacte theorieën, met een precies gedefinieerde formele taal, een expliciet logisch bewijssysteem, en een complete specificatie van alle toegestane wiskundige axioma's. Zo formaliseerde Peano in dit formaat de formele rekenkunde, waarin het al enkele malen gebruikte principe van natuurlijke inductie voorkomt als een wiskundig axioma

$$(\varphi(0) \wedge \forall x\,(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \forall x\,\varphi(x)).$$

Evenzo werd de verzamelingenleer geformaliseerd door Zermelo en Fraenkel, waarbij centrale axioma's precies vastleggen wanneer verzamelingen $\{x|\varphi(x)\}$ bestaan voor geschikte condities φ. Formele bewijzen voor stellingen in zulke theorieën zijn dan eindige ketens van logische bewijsstappen, met hier en daar een beroep op een axioma uit de vooraf gegeven lijst. De eerste formele versie van de Euclidische meetkunde werd overigens pas gegeven door Alfred Tarski in de jaren veertig. De bestudering van dat bewijssysteem leverde ook nog een bonus op, naast loutere precisie. Zo bleek althans de elementaire schoolmeetkunde *beslisbaar*: er bestaan mechanische procedures, inmiddels ook geautomatiseerd, gevonden om de correctheid van elementaire meetkundige stellingen te beslissen. Deze wiskundige studie van wiskundige theorieën was de centrale gedachte van de 'metamathematica' van Hilbert, die beoogde de consistentie van de wiskunde eens en voor goed aan te tonen. Deze heroïsche periode van de geschiedenis van de wiskunde zullen we weer opnemen in hoofdstuk 7.

Automatisch bewijzen op de computer

Logische bewijssystemen spellen elk stapje expliciet uit, en zijn dus in principe bruikbaar voor een rekenmachine. Dit nuttige effect was niet voorzien door de grondslagenonderzoekers van de wiskunde; maar de wetenschapsgeschiedenis vertoont wel vaker verrassende wendingen. Er bestaan inmiddels vele genres programma's die automatisch wiskundige stellingen bewijzen uit formele theorieën. Met name meetkundige stellingbewijzers hebben reeds allerlei nieuwe resultaten ontdekt, en concurreren dus met de mens. Maar geautomatiseerde logische deductie is veel ruimer bruikbaar, omdat heel veel taken zijn op te vatten als een afleidingsproces. Voorbeelden zijn het ontleden van natuurlijke taal, 'logisch programmeren' in computertalen als LISP of PROLOG, of expert-systemen in de Kunstmatige Intelligentie die het redeneren van artsen of rechters nabootsen, dan wel ondersteunen.

Overigens zien bewijsstappen in zo'n computersysteem er vaak anders uit dan wat mensen hanteren. Een voorbeeld is de volgende veel gebruikte regel in bewijsmachines voor propositielogica:

Resolutie

$\stackrel{\text{T. 24}}{\Longrightarrow}$ 197 Concludeer uit $A \vee B$ en $\neg B \vee C$ dat $A \vee C$.

Dit is inderdaad een geldige gevolgtrekking, hetgeen makkelijk is te zien met een semantisch tableau. De kracht ervan wordt echter slechts gaandeweg duidelijk. Om Resolutie te kunnen gebruiken wordt elke propositielogische formule eerst equivalent herschreven tot een conjunctie van een verzameling 'clausules' van de vorm $(\neg)A_1 \vee ... \vee (\neg)A_k$, een disjunctie van atomaire beweringen A_i of negaties daarvan. Dit is mogelijk met eenvoudige toepassing van de wetten der Boolese Algebra (T.26). Vervolgens wordt elke conclusie, hoe ingewikkeld ook, gevonden door de machine mogelijke resolutiestappen te laten maken vanuit de gegeven premissen. Voor mensen zou dit zoekproces moordend saai zijn, maar een computer doet miljoenen van dit soort stappen zonder klagen, waarbij het werken met slechts één regel een voordeel is. Ons eerdere Feestvoorbeeld is een eenvoudige illustratie. In clausule vorm veranderen de drie gegevens in vier clausules:

$$\neg M \vee J, \neg A \vee J, M \vee A, \neg A \vee \neg J$$

Met achtereenvolgende resolutiestappen vindt een machine dan bijvoorbeeld:

$$\dfrac{\dfrac{\neg A \vee J \qquad \neg A \vee \neg J}{\neg A \vee \neg A:\ \text{dwz}\ \neg A} \qquad \dfrac{M \vee A \qquad \neg M \vee J}{M}}{J}$$

In dit bewijs komt de hele eerder gegeven oplossing naar voren. Voor redeneren met kwantoren gebruiken computers overigens meer complexe varianten van resolutie, die ook pattern matching uitvoeren op samengestelde termen die objecten aanduiden.

Andere automatische deductiesystemen zijn de al eerder genoemde tableau-bewijzers. Weer andere veel gebruikte systemen maken gebruik van analogieën met algebraïsch rekenen, zoals de 'equationele logica' die soms uiterst verrassende conclusies bereikt door aaneenschakeling van miljoenen op zichzelf triviale bewijsstapjes als

Transitiviteit $\quad x = y, y = z \Rightarrow x = z$

Congruentie $\quad x = y, z = u \Rightarrow f(x, z) = f(y, u)$

Resolutie

De algemene resolutie-regel luidt:

$$\varphi_1 \vee A \vee \varphi_2, \psi_1 \vee \neg A \vee \psi_2 \Rightarrow \varphi_1 \vee \varphi_2 \vee \psi_1 \vee \psi_2$$

In principe is deze enkele regel voldoende om elke geldige redenering te staven. Maar dan moet wel heel veel voorwerk gedaan worden. We nemen hier weer de Quine formule van T.22 ter illustratie. Deze formule moet tot een tegenspraak leiden. Allereerst herschrijven de formule tot een zogenaamde prenex-normaalvorm. *Dat wil zeggen dat de kwantoren bereik over de hele formule hebben, de conjuncties over de disjuncties en die weer over de negaties. De laatste mogen alleen voorkomen voor atomaire formules. Elke formule kan herschreven worden tot een logisch equivalente formule van deze speciale vorm. Het resultaat voor de Quine formule is dan de volgende*

$$\exists x \, \forall y \, \exists w \, \forall z \, ((Rxy \vee Ryw) \wedge (Rxy \vee Rwy) \wedge (\neg Rxy \vee \neg Ryz \vee \neg Rzy))$$

Vervolgens herschrijven we het Boolese deel van de formule verder zodat alleen disjuncties en de negaties overblijven. We beginnen met het wegwerken van de existentiële kwantoren.
De eerste existentiële kwantor kwijtraken is niet lastig. Er wordt gesteld dat een individu bestaat met de Quine-eigenschap. In de nieuwe formule kiezen we een neutrale 'verse' naam a, waarover we verder geen informatie hebben. De tweede existentiële kwantor is wat lastiger weg te werken omdat hij in het bereik staat van een universele kwantor. De formule heeft de vorm $\forall y \, \exists w \, \varphi$, ofwel, alle individuen (y) onderhouden een of andere relatie φ met w: "Alles φ-t iets". We kunnen niet simpelweg een naam b kiezen voor w, want dan zou er iets zijn dat door alles ge-φ-d wordt. De juiste lezing zonder existentiële kwantor vergt introductie van een één-plaatsige functie f die voor elk individu (y) een uitverkoren φ-instantie aanwijst. Dit levert de volgende herformulering:

$$\forall y \, \forall z \, ((Ray \vee Ryfy) \wedge (Ray \vee Rfyy) \wedge (\neg Ray \vee \neg Ryz \vee \neg Rzy))$$

Als we de relatie R weer met 'kent' lezen, dan wijst de functie voor elke individu die niet door het Quine-individu a gekend wordt een kennis aan, en voor de overigen een niet-kennis.
Een dergelijke herformulering zonder existentiële kwantoren heet wel een Skolem-vorm, *naar de Noorse logicus Thoralf Skolem. Een Skolem-vorm is logisch gesproken een versterking van de originele formule. Maar als de Skolem-vorm onvervulbaar (inconsistent) is, dan moet het origineel ook onvervulbaar zijn, en dat laatste wilden we nu juist aantonen voor de Quine formule.*
Vervolgens laten we de kwantoren en de conjuncties weg, en houden drie 'clausules': disjuncties van literals, over, die allemaal waar moeten zijn volgens de veronderstelde waarheid van de Quine formule.

$$(1)\, Ray \vee Ryfy \quad (2)\, Ray \vee Rfyy \quad (3)\, \neg Ray \vee \neg Ryz \vee \neg Rzy$$

Nu komt de resolutieregel in het spel. Wat we nu moeten doen is geschikt gekozen speciale gevallen van deze drie formules met resolutie combineren om een tegenspraak af te leiden. Hier is een mogelijke route in drie stappen:

$$\dfrac{\dfrac{\dfrac{1'\; Raa \vee Rafa \quad 3'\; \neg Raa}{Rafa} \qquad 3''\; \neg Rafa \vee Rfaa}{\neg Rfaa} \qquad 2'\; Raa \vee Rfaa}{Raa}$$

De gebruikte clausules verschijnen in verschillende gedaanten, door verschillende substitituties voor de variabelen. De eerste stap combineert 1 en 3 door voor alle variaben a te kiezen. De tweede stap combineert dit resultaat met een andere versie van 3: met fa voor y en a voor z. In de laatste stap gebruikten we 2 met a voor y.
De tegenspraak die aldus wordt afgeleid is identiek aan die in T.22. De Quine persoon a moet zich zelf kennen volgens de laatste stap (Raa). In de eerste stap hebben we echter, door in de derde clausule voor beide variabelen a te kiezen, al afgeleid dat a zichzelf niet kent ($\neg Raa$).

Redeneren en natuurlijke taal

Tot nu toe ging dit hoofdstuk over formele talen, zoals notatiesystemen in de wiskunde, of programmeertalen in de informatica, en bijbehorende abstracte bewijssystemen. Maar in Hoofdstuk 1 hebben we ook een lans gebroken voor onze gewone natuurlijke taal als respectabel communicatiemedium met wiskundige structuur. Hoe staat het met bewijzen en redeneren rechtstreeks in natuurlijke taal? Voor een deel sporen de twee werelden aardig. Taalkundig is welbekend dat natuurlijke talen Boolese operaties bezitten waarvan het gedrag redelijk lijkt op de propositielogica. En ook kenmerkende talige redeneervormen voor kwantoren als de monotonie van Hoofdstuk 1 zijn abstract logisch te verklaren. Zo is — om maar iets te noemen — de stijgende linker monotonie van de kwantor '(minstens) een' niets anders dan de geldige gevolgtrekking

$$\exists y\,(Py \wedge Ry), \forall x\,(Px \rightarrow Qx) \models \exists\, y(Qy \wedge Ry)$$

Ons dagelijkse redeneren lijkt dus niet ver af te staan van wiskundig bewijzen. En ook omgekeerd: wiskundig bewijzen is op te vatten als gewoon redeneren met gezond verstand, wat langer volgehouden dan we normaal plegen te doen.

Maar bij nader inzien zijn er toch ook aanzienlijke verschillen tussen formeel bewijzen en alledaags redeneren. Deze zijn met name aan het licht getreden in de Kunstmatige Intelligentie, toen men rond 1980 systematisch ging proberen intelligent menselijk redeneren 'in de computer te brengen', bijvoorbeeld in de beschrijving van planningstaken. En zodra we dat doen valt een opmerkelijk verschijnsel op. Mensen maken frequent gebruik van veel meer conclusies dan strikt logisch mag, en wel door het hanteren van zogenaamde *'default' aannamen*. Hier is nogmaals het eenvoudige voorbeeld van een UvA employee, dat we eerder in hoofdstuk 3 bespraken:

> Als ik de trein neem (T), kom ik *doorgaans* in Amsterdam (A). Ik neem de trein. Dus ik kom in Amsterdam.

De verzwegen aanname bij dat 'doorgaans' is dat de NS functioneert, dat er geen aardbeving optreedt, of dat andere uitzonderlijke omstandigheden zich niet voordoen. We zouden dit kunnen zien als een extra conditie $\neg U$, waarvan de precieze aard verzwegen blijft. Maar nu is duidelijk dat de conclusie A niet geldig volgt uit de twee premissen $(T \wedge \neg U) \rightarrow A$ en T. We moeten ook nog aannemen dat $\neg U$, maar we *weten* dat strikt genomen niet! Vaak wordt dit verschijnsel geherformuleerd in termen van zogenaamde *minimale modellen*. In principe zijn er 3 situaties die de gegevens $(T \wedge \neg U) \rightarrow A$ en T waar maken, en wel $T, \neg U, A$,T, U, A, $T, U, \neg A$. Kennelijk hebben wij een voorkeur voor de minimale situatie daaronder, met de minste ware feiten, te weten $T, \neg U, A$, en redeneren we verder daarover. Anders gezegd, in logisch geldige gevolgtrekkingen moeten we rekening houden met *alle* situaties die de premissen waar maken, in het dagelijks leven kijken we alleen naar de *minimale* situaties die dat doen.

Stilzwijgend aannemen dat uitzonderlijke omstandigheden zich niet voordoen zolang we niet beter weten, werkt snel, en is ook meestal gerechtvaardigd bij oplossen van problemen, of plannen van activiteiten. Maar er is wel een prijs te betalen. Als onverhoopt de NS toch niet functioneert, of de Nederlandse bodem slaat ineens op tilt, dan moeten we de conclusie A alsnog intrekken, en onze hele informatie heroverwegen. Naast 'gretig' redeneren voorbij wat strikt logisch is toegestaan, hebben we dus een compenserend mechanisme nodig. Dit is de systematische *herziening* van eerdere conclusies als we te maken krijgen met recalcitrante feiten. Ons alledaagse redeneren is dus veel dynamischer dan stapelen van correcte conclusies op correcte conclusies!

Psychologie van redeneren

Maar de meest concrete informatie over hoe mensen nu werkelijk redeneren krijgen we niet van wiskundigen, logici, taalkundigen, of zelfs informatici werkzaam in de AI. Daarvoor moeten we eerder te rade bij de cognitieve psychologen. Er is een lange, en vaak moeizame geschiedenis van contacten tussen de meer theoretisch denkende logici en empirische cognitiewetenschappers. Psychologen beweren vaak dat echt redeneren heel anders gaat dan de logica beweert! Beroemd is de Wason Kaart Test uit 1970, die beoogt aan te tonen dat conditionele beweringen $A \rightarrow B$ zich anders gedragen dan in de logica, en meer algemeen, dat redeneren helemaal niet draait om bewijspatronen, maar afhankelijk is van inhoud en concrete situatie. Dit experiment loopt als volgt.

Beschouw de volgende regel over een aantal kaarten, die aan de ene kant een letter hebben, en aan de andere kant een cijfer:

> "Als er een klinker op de ene kant staat, dan staat er een oneven getal op de andere kant: $K \rightarrow O$".

U krijgt nu de volgende rij kaarten te zien.

$$A \quad K \quad 4 \quad 7$$

De vraag is nu:

> Welke kaarten *moet* u omdraaien en aan de achterkant inspecteren om na te gaan of de genoemde regel opgaat?

Proefpersonen doen dit doorgaans 'fout', en noemen niet de *twee* kaarten die volgens de logica moeten worden omgekeerd, namelijk de A én de 4. Doorgaans kiest men alleen kaart A, of kaarten A en 7. Een citaat uit het oorspronkelijke artikel: "Even professional logicians have been known to fail in an embarrassing manner..." Een tweede belangrijke observatie was dat het 'logisch correcte antwoord' wel veel vaker wordt gegeven als de test een concrete inhoud krijgt, bijvoorbeeld met kaarten die aan de ene kant leeftijden vermelden, en aan de andere al dan niet drinken. De regel zegt dan dat je alleen mag drinken als je ouder bent dan 18. Dit beschrijft een herkenbare sociale situatie van eventueel drankgebruik door minderjarigen, en proefpersonen draaien nu veel vaker de juiste kaarten om.

Er is dus een verschil tussen de logisch correcte uitkomst en geobserveerd gedrag. Maar wat dat betekent blijft een kwestie van interpretatie. Redeneren mensen 'fout'? Hebben ze misschien een vooroordeel tegen 'moeilijke' negatieve noties als weerleggen, waardoor een implicatie $\neg B \rightarrow \neg A$ lastiger wordt gevonden dan het logisch equivalente $A \rightarrow B$? Of moeten we beter kijken naar de manier waarop proefpersonen het concrete scenario omzetten in premissen? Heeft de concrete drank-situatie bijvoorbeeld wel dezelfde logische structuur als het abstracte kaartvoorbeeld? Als de premissen in de twee scenario's verschillen, dan is 'de logica' niet meer direct in het geding. Over deze kwesties vindt een levendig debat plaats tussen logici en psychologen.

De laatste jaren wordt vaak gesuggereerd dat feitelijk redeneren wel eens meer zou kunnen lijken op de eerder genoemde default logica's voor probleem-oplossing in de artificiële intelligentie. Zo wijzen experimenten van Byrne rond 1980 erop dat conclusies kunnen worden herzien door eventuele extra premissen, iets wat kenmerkend was voor revisie. Stel dat we proefpersonen de volgende twee dingen vertellen over een studente:

> Als ze examen moet doen, dan zal ze naar de bibliotheek gaan ($E \rightarrow B$).
>
> Ze moet examen doen (E)

dan concludeert men in grote meerderheid “Ze gaat naar de bibliotheek”. Maar die conclusie wordt weer ingetrokken als we nog een extra gegeven toevoegen:

Als de bibliotheek open is, dan zal ze ernaar toe gaan ($O \rightarrow B$).

Geven we echter als extra een andere implicatie, te weten “Als ze een boek nodig heeft, dan gaat ze naar de bibliotheek”, dan blijft de conclusie B weer wél staan. Kennelijk spelen in de weergave die mensen kiezen voor dergelijke scenario’s verzwegen condities een rol, die door verdere informatie kunnen worden geactiveerd. Zo is de verzwegen conditie bij de eerste implicatie dat de bibliotheek open is, en juist deze wordt door de toegevoegde implicatie tot kwestie gemaakt.

Een interessante logische analyse van dit soort default redeneren en de bijbehorende revisiemechanismen is onlangs gegeven door van Lambalgen en Stenning. In hun analyse draait alles weer om het vinden, en waar nodig aanpassen, van ’minimale modellen’ voor de gegevens. Het proces dat dergelijke minimale situaties opspoort wordt uiteindelijk zelfs in verband gebracht met de tegenwoordig veel gebruikte ’neurale netten’ voor hersenwerking. Maar met die laatste connectie komen we op een heel ander wiskundig terrein, en wel de studie van dynamische systemen zoals die in hoofdstuk 5 werden besproken. Ons feitelijk redeneergedrag is wellicht niet zuiver logisch in de klassieke zin des woords, maar daarmee ontsnapt het bepaald nog niet aan wiskundig-logische analyse!

Hoofdstuk 7

Berekenbaarheid

7.1 Turingmachines

In het geval van een vraag naar de fundamenten van een bepaald vakgebied, kan bijna iedere wetenschap refereren aan een aanpalend terrein dat uiteindelijk deze grondslagen voor z'n rekening neemt. Zo zal uiteindelijk een vraag naar de microscopische basis van de biologie beantwoord moeten worden door de scheikunde. Op zijn plaats geeft de natuurkunde de fundamentele wetten (de Schrödingervergelijking) waarop de scheikunde gebaseerd is. Etcetera, etcetera. Een scheikundige hoeft niet bang te zijn dat het bouwwerk van de chemie instort omdat de hoge mate van interne consistentie van de kwantumfysica, zoals ontwikkeld door de collega theoretisch fysici, waarborgt dat de grondbeginselen consistent zijn.

Voor de wiskunde en logica is er echter geen hogere macht. Er is geen vakgebied dat als het ware de metamathematica bestudeert en waaruit de axioma's en methoden van de wiskunde kunnen worden afgeleid. De wiskunde is dus in laatste instantie zelf verantwoordelijk voor de eigen consistentie en deze verantwoordelijkheid is een zware last gebleken.

Hilberts programma

Het wiskundige grondslagenonderzoek heeft een sterke stimulans verkregen door David Hilbert die in 1928 ter gelegenheid van een van de befaamde Internationale Congressen de volgende vragen stelde:

- Is de wiskunde compleet?
- Is de wiskunde consistent?
- Is de wiskunde beslisbaar?

Hilbert heeft waarschijnlijk gedacht dat uiteindelijk het antwoord op al deze drie vragen ja zou zijn. Zijn lijfspreuk was immers *Wir müssen wissen. Wir werden wissen.* Hij werd hierin lelijk teleurgesteld! Maar laten we eerst wat verder ingaan op deze drie vragen.

Volledigheid Dit is de vraag of van iedere wiskundige bewering A bewezen kan worden dat deze waar is of niet-waar is. We kunnen ons deze vraag als volgt voorstellen. Beschouw de verzameling van alle mogelijke wiskundige uitspraken. Deze bevat uitspraken die manifest waar zijn, zoals '$1+2=3$'. Dit zijn uitspraken die met weinig moeite uit de axioma's van de rekenkunde kunnen worden afgeleid. Door wiskundige bewerkingen op zo'n ware bewering toe te passen volgen eenvoudig nieuwe ware beweringen. Bijvoorbeeld de commutativiteit van optellen van gehele getallen

$$a + b = b + a$$

impliceert dat als '$1 + 2 = 3$' waar is, dat ook '$2 + 1 = 3$' waar is. Omgekeerd geldt ook dat bijvoorbeeld de uitspraak '$1+2=4$' niet waar is. Dit impliceert dan op zijn beurt dat ook '$2+1=4$' niet waar is.

We kunnen ons dit grafisch proberen voor te stellen uitgaande van een abstract universum van wiskundige uitspraken. Ieder punt in dit universum stelt een mogelijke wiskundige uitspraak voor. Stel dat we iedere ware bewering in dit universum wit kleuren en iedere niet-ware bewering zwart. Naar mate de wiskunde voortschrijdt worden dus steeds meer vakjes wit of zwart gekleurd. (Als we de uitspraak A wit kleuren, dan kunnen we natuurlijk direct de uitspraak $\neg A$ zwart kleuren.) Er zijn op dit moment natuurlijk grote gebieden nog niet ingekleurd. Bijvoorbeeld het Goldbachvermoeden

(iedere even getal is de som van twee priemgetallen) staat nog open. Het is nog niet bekend of dit vakje wit of zwart zal worden.

Hilbert vroeg zich nu af of uiteindelijk iedere bewering in het universum òf wit òf zwart is. Dat wil zeggen, hij maakte zich zorgen of er ook stukken fundamenteel niet ingekleurd konden worden. Dit zijn dan uitspraken waarvan niet met de gebruikelijke wiskundige technieken kan worden bewezen of ze waar of niet-waar zijn.

Consistentie Is het mogelijk dat we zowel A als *niet* A zouden kunnen bewijzen? In de vorige beeldspraak, is het mogelijk dat uiteindelijk een wiskundige bewering zowel wit als zwart moeten worden ingekleurd? In dat geval zou er een reeks valide wiskundige redeneerstappen bestaan die, zeg, vertrekkend van '$1+2=3$' bij A uitkomt, en tegelijkertijd een complementaire reeks stappen waaruit *niet* A zou kunnen worden afgeleid.

We hebben al gezien dat in dat geval de wiskunde inconsistent is. Als zowel A als $\neg A$ waar zijn, dan is iedere uitspraak B waar. (En daarmee ook iedere uitspraak $\neg B$.) Het wiskundig universum is dan èn helemaal wit èn helemaal zwart gekleurd.

Het uiteindelijke antwoord op deze eerste twee vragen van Hilbert was negatief. In 1931 liet Kurt Gödel zien dat de wiskunde of onvolledig of inconsistent is. Aan het einde van dit hoofdstuk wordt daar veel dieper op ingegaan. Omdat inconsistentie de doodsteek voor de wiskunde zou betekenen, kiezen we voor incompleetheid. Er zijn dus uitspraken die wel waar zijn (in de zin dat er geen tegenvoorbeelden gevonden kunnen worden), maar waarvan nooit zal worden aangetoond via een wiskundig bewijs dat deze ook waar is.[1]

Beslisbaarheid De laatste vraag, het zogeheten *Entscheidingsproblem*, betreft een meer praktische zaak. Hilbert vroeg zich af of er een 'machine' bestaat die in een eindig aantal stappen kan bepalen of een uitspraak A waar is of niet. In dat geval zouden we in principe een machine kunnen bouwen die, als we maar lang genoeg wachten, op iedere wiskundige vraag een antwoord zou geven — een waar orakel!

Deze laatste vraag werd door Alan Turing (1912–1954), gelijktijdig ook door Alonso Church,[2] in 1936 negatief beantwoord.

Turing machines

Turing stelde zich de vraag wat nu eigenlijk wiskunde is vanuit een strikt operationeel standpunt. Als we een formeel standpunt innemen kunnen we wiskunde zien al een serie symbolen, volgens een bepaalde grammatica opgeschreven, die gemanipuleerd worden. Bijvoorbeeld, de definitie van een afgeleide van een functie f zal geschreven worden als

$$f'(x) = \frac{df}{dx}(x) \Leftrightarrow \forall\epsilon > 0\, \exists\delta > 0 \left[0 < |\Delta x| < \delta \Rightarrow \left|\frac{f(x+\Delta x) - f(x)}{\Delta x} - f'(x)\right| < \epsilon\right]$$

Turing eerste inzicht was dat zo'n uitdrukking uiteindelijk gecodeerd kan worden in een serie `0`-en en `1`-en. Dat wil zeggen een grammaticaal correcte wiskundige bewering A kan gezien worden als een eindige reeks

$$A = \texttt{0100100111010010100010}\ldots\texttt{1010}$$

[1] Zo werd soms wel gevreesd dat de Laatste Stelling van Fermat zo'n onbewijsbare bewering was!

[2] Church gebruikte hiervoor een veel minder toegankelijk model voor de notie van algoritme: de recursie functies.

In het huidige digitale tijdperk hebben we natuurlijk geen enkele moeite zo'n 'streepjes'-codering voor te stellen. In feite is de bovenstaande uitspraak, zoals ik die nu in mijn tekstverwerker invoer, al digitaal opgeslagen.

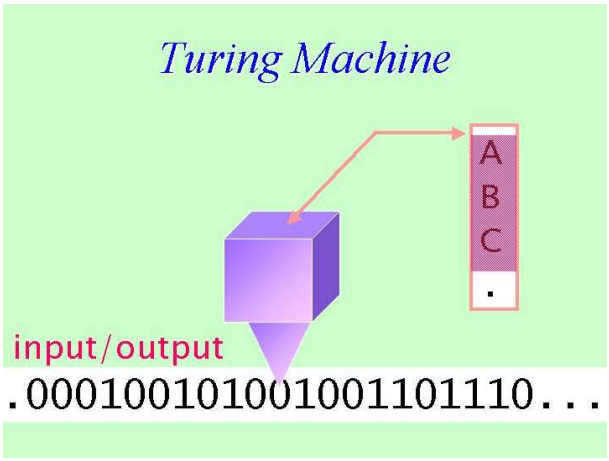
Het *Entscheidungsproblem* kan nu geformuleerd worden als de vraag naar de existentie van een *bewijsmachine*. Dit is een machine waar de uitspraak A kunnen invoeren, en waarvan de uitkomst zal zijn 'waar' of 'niet-waar'. Als zo'n machine bestaat, kunnen we eenvoudig bijvoorbeeld het Goldbach-vermoed oplossen en het uitgeloofde miljoen (zie 6.1) opstrijken.[3] Zo'n orakel zou alleen al daarom zeer welkom zijn!

Om de onmogelijkheid van de constructie van een bewijsmachine in te zien, moeten we eerst het begrip *Turingmachine* introduceren. Dit is in wezen een vereenvoudigde vorm van een moderne computer.

Een Turingmachine bestaat uit verschillende onderdelen. Allereerst is er de tape. Dit is een oneindig lange band, bestaande uit vakjes, cellen genoemd, die of leeg zijn of gevuld. De lege cellen zullen we weergeven met een `0`, de volle cellen met een `1`. Een typische tape ziet er dus uit als een oneindig lange reeks

$$\ldots \texttt{00001110100100111110010101000} \ldots$$

De machine heeft de mogelijkheid zich in een (eindig aantal) configuraties $A, B, C, \ldots$ te bevinden. De akties van de machine worden volledig bepaald door de toestand waarin de machine zich bevindt.



Verder bestaat de machine uit een kop die verschillende dingen kan doen.

- Als de kop van de machine boven een cel van de band staat, kan deze een cel lezen, dat wil zeggen een `0` van een `1` onderscheiden.
- Vervolgens kan de machine in de desbetreffende cel schrijven, en zodoende eventueel het binaire cijfer, `0` of `1`, in de cel wijzigen.
- De machine kan daarna eventueel één stap naar links of naar rechts uitvoeren. In die positie kan de aangrenzende cel gelezen worden. De machine mag ook besluiten te stoppen.
- Tenslotte kan de machine van interne toestand veranderen, bijvoorbeeld als de oorspronkelijke toestand A is, kan deze nu overgaan in B.

[3] Sterker nog, de zeven open problemen als opgesteld door het Clay Institute for Mathematics kunnen we in gedigitaliseerde vorm invoeren en wachten wat de machine ons vertelt en zodoende de zeven miljoen dollar incasseren.

Al deze acties zullen afhangen van (1) wat er in de betreffende cel gelezen is en (2) de toestand waarin de machine zich op dat moment bevindt. Alle handelingen kunnen weergegeven worden in een instructietabel. In deze tabel kan de machine 'opzoeken' wat hij verwacht wordt te doen bij een gegeven toestand en celinhoud.

We kunnen nu een gegeven Turingmachine een band aanbieden, de invoer, en daar zal de machine mee aan het werk gaan. Uiteindelijk, als de machine stopt, zal er een nieuw resultaat op de band staan: de uitvoer.

Een eenvoudig voorbeeld

Stel we willen een machine maken die kan optellen, bijvoorbeeld $5 + 7 = 12$. We beginnen met de getallen 'unair' weer te geven. Dat wil zeggen, het getal 5 wordt geschreven als vijf gevulde cellen (we geven de lege cellen niet weer)

$$5 = \texttt{11111}$$

en op dezelfde manier is

$$7 = \texttt{1111111}$$

De invoer voor de opgave $5 + 7$ is eenvoudig: vijf en zeven gevulde cellen, gescheiden door één lege cel

$$5 + 7 = \texttt{1111101111111}$$

De machine moet nu de gevraagde uitvoer

$$12 = \texttt{111111111111}$$

geven. Hier is een instructietabel die dat doet. Er zijn drie configuraties $\{A, B, C\}$ en twee verschillende invoers $\{\texttt{0}, \texttt{1}\}$.

	`1`	`0`
toestand A	rechts, blijf in toestand A	schrijf `1`, rechts, $\rightarrow$ toestand B
toestand B	rechts, blijf in toestand B	links, $\rightarrow$ toestand C
toestand C	schrijf `0`, STOP	STOP

Laten we eens kijken hoe de machine opereert op onze invoer. De machine begint in toestand A en leest de meest linkse `1`. Nu doet de machine een stap naar rechts, en blijft daarbij in toestand A. Als in de volgende cel weer een `1` staat, herhaalt zich het proces. Uiteindelijk komt de machine een `0` tegen. De instructies vertellen de machine dat dan een `1` geschreven moet worden. De machine beweegt vervolgens weer een stap naar rechts, maar is nu overgegaan in toestand B. De machine blijft in deze toestand totdat het weer een lege cel tegenkomt. Nu heeft het de opdracht een stap naar links uit te voeren, naar toestand C te gaan, de daar aanwezige `1` te vervangen door een `0` en vervolgens te stoppen.

In dit proces is de string

`1111101111111`

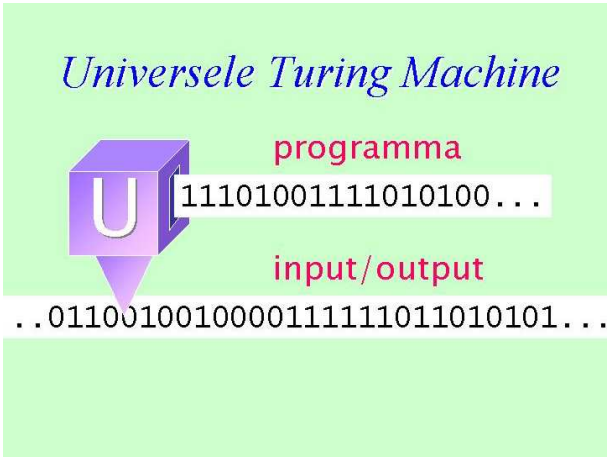
vervangen door

`1111111111110`

hetgeen de symbolische weergave van de som $5 + 7 = 12$ is.

De universele Turingmachine

Is het nodig om voor iedere opdracht een nieuwe Turingmachine te bouwen? Het is duidelijk dat de instructietabel van de machine, de code, ook in binaire vorm kan worden weergegeven. Kunnen we niet een machine bouwen die twee invoers heeft: (1) de code die vertelt wat de precieze instructies zijn, en (2) de tape waarop de machine moet werken. Turing liet al zelf zien dat zo'n *universele Turingmachine* inderdaad bestaat. Wederom, met onze huidige programmeerbare computers is dit een minder verbazingwekkend feit, dan in de tijd van Turing, begin jaren dertig, toen typmachines de modernste technologie vertegenwoordigden.



Deze notie van universele Turingmachine geeft Turingmachines een meer realistische status. Bij een eerste kennismaking van het fenomeen denkt men wellicht wat een primitieve apparatuur. Het was Turing erom te doen om juist het model zo simpel mogelijk te houden om het te kunnen hanteren voor wiskundige bewijzen over de mechaniseerbaarheid van de wiskunde. Zijn model is echter zo algemeen dat elk ingewikkeld rekenapparaat door een, wellicht erg grote en ook inefficiëntere, Turingmachine vervangen kan worden. De vervangbaarheid bedoelen wil hier zeggen dat de machines dezelfde uitkomsten geven.

Dit laatste heet ook wel de zogenaamde Church-Turing-these: "Voor elke algoritme, ofwel mechanisch uitvoerbare rekenmethode, is er een Turingmachine die hem uitvoert". Het is maar een these — een werkhypothese — maar tot op de dag van vandaag houdt hij stand. En het is common sense dat deze these ook wel stand zal blijven houden. Al die gecompliceerde rekenapparatuur waarover we nu beschikken had Turing al in principe beschreven. Om onbeslisbaarheid voor een probleem te bewijzen hoeven we 'alleen maar' aan te tonen dat er geen Turingmachine bestaat die de uitkomst berekent.

Het Halting Problem

We kunnen nu het belangrijkste voorbeeld van een onbeslisbaar probleem formuleren. Beschouw een programma P en invoer A. Wat zal de machine met instructie P doen als we de tape A aanbieden. Er zijn twee mogelijkheden: (1) òf de machine komt in een eindtoestand waarbij de procedure stopt, (2) òf de machine blijft altijd doorwerken. In het eerste geval hebben we een duidelijk gedefinieerde uitvoer B. In het tweede geval is er geen sprake van een eenduidige uitvoer. De machine stopt eenvoudig niet. Het blijft eeuwig 'werk in uitvoering'.

Men zal in het algemeen deze tweede mogelijkheid als negatief ervaren. We willen graag dat programma's na eindige tijd stoppen. Als u een programma op uw PC draait, bijvoorbeeld een tekstverwerker, en dit programma blijft niet meer in een rusttoestand komt na een toetsaanslag, dan zal dat zeer frustrerend zijn. Maar aan de andere kant zijn er ook programma's waarvan we juist willen dat deze absoluut niet stoppen, bijvoorbeeld het besturingssysteem van uw PC. De moderne informatica is dan ook 'neutraal' wat betreft het wel of niet stoppen van programma's. Er is geen gevoelsmatige voorkeur.

Het Haltingprobleem kan nu als volgt geformuleerd worden:

> *Is het mogelijk met een eindige procedure vast te stellen of het programma P stopt met invoer A?*

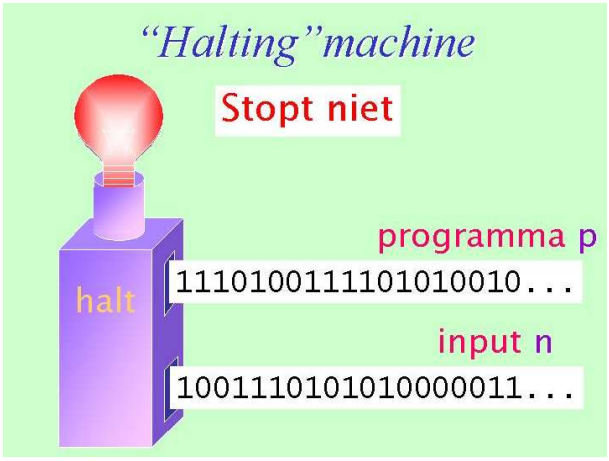
Om deze vraag te beantwoorden moeten we dus een tweede machine construeren, een 'Haltingmachine', die gegeven de invoers P en A eenvoudig antwoordt 'halt' of 'niet halt'. Laten we dit symbolisch weergeven. Hier staat

$$\texttt{halt}(P, A)$$

voor de bewering dat programma P stopt met invoer A, en

$$\neg\, \texttt{halt}(P, A)$$

staat voor de bewering dat het programma P *niet* stopt met invoer A.



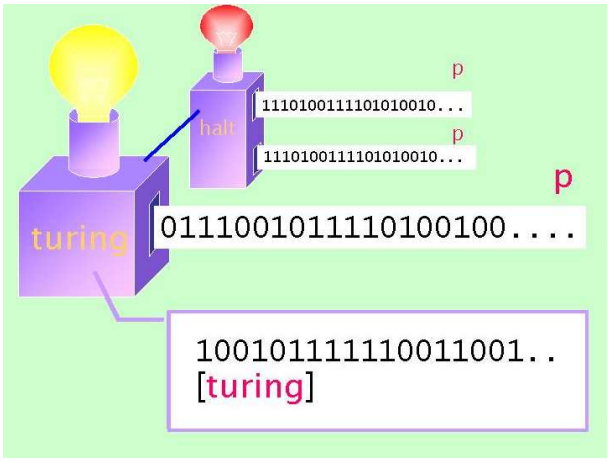
Stel dat we de Haltingmachine hebben geconstrueerd. We kunnen nu iets 'pervers' doen. Merk op dat zowel het programma P als de invoer A gegeven zijn als een (eindig) binair getal. In het bijzonder kunnen we code van het programma P ook opvatten als een mogelijke invoer. Uiteindelijk verwachten we van het programma P dat deze met iedere willekeurige invoer wat doet (in het bijzonder zal stoppen of niet zal stoppen). Er is dus geen principieel bezwaar om in een soort kannibalisme de (code van) P als invoer aan P zelf aan te bieden.

Er rijst nu de vraag: "zal programma P stoppen als deze invoer P krijgt aangeboden?" Met andere woorden, is

$$\texttt{halt}(P, P)$$

waar? Als de Haltingmachine daadwerkelijk bestaat, kan deze vraag eenvoudig beantwoord worden. Maar Turing beargumenteerde dat dit tot een tegenspraak leidt.

Veronderstel dat de machine `halt` bestaat. Dan kunnen we een kleine variant daarop construeren. Laten we deze machine `turing` noemen. Deze machine vraagt om één invoer, een code P. De instructies zijn als volgt.



- Als `halt`(P, P) waar is, dat wil zeggen als P met invoer P stopt, dan stopt `turing` juist niet. (Maar gaat wat anders doen, het doet er eenvoudig niet toe wat, zolang de machine maar niet stopt.)
- Als `halt`(P, P) waar is, d.w.z. als P met invoer P stopt, dan stopt `turing`.

In een formule hebben we dus eenvoudig

$$\texttt{halt}(\texttt{turing}, P) = \neg\, \texttt{halt}(P, P) \tag{7.1}$$

Als we aangenomen hebben dat de machine `halt` bestaat, dan zal de machine `turing` ook bestaan.

We zijn nu toe aan het pièce de résistance van het argument. Omdat `turing` een machine is, zal deze ook door de universele Turingmachine geëmuleerd kunnen worden. Er is dus een code die de machine beschrijft. Laten we deze code ook gewoon met `turing` aangeven.

Het zal u nu duidelijk zijn wat we willen gaan doen. In een laatste act van gedwongen kannibalisme zullen we de machine `turing` de code `turing` voeren. Zal de machine stoppen of niet? Maar hier komen we een echte paradox tegen. Dit is al direct duidelijk als we $P =$ `turing` invullen in vergelijking (7.1). We krijgen immers

$$\texttt{halt}(\texttt{turing}, \texttt{turing}) = \neg\, \texttt{halt}(\texttt{turing}, \texttt{turing})$$

Dit is een uitspraak van de vorm

$$A = \neg\, A$$

waarvan de wiskundige stoppen doorslaan!

Wat langzamer: Stel dat `turing` stopt met invoer `turing`. Gegeven de definitie betekent dat dat

$$\neg\, \texttt{halt}(\texttt{turing}, \texttt{turing})$$

waar is. Dat wil zeggen, `turing` stopt *niet* met invoer `turing`. Dit is precies de tegengestelde bewering! Omgekeerd vinden we dat de machine niet stopt dan en slechts dan als deze wel stopt. We hebben dus een echte tegenspraak gevonden. ‘Modus Tollens’ brengt ons de kortsluiting:

Als `halt` bestaat, dan bestaat `turing`

`turing` bestaat niet.

Ergo `halt` bestaat niet.

Berekenbare getallen

In Turings oorspronkelijke artikel werd de bovenstaande redenering gegeven in het kader van een ander probleem, namelijk welke getallen de uitkomst kunnen zijn van een wiskundige berekening. Dit lijkt in eerste instantie een vreemde vraag. Is niet ieder getal een mogelijke uitkomst?

Om de vraag preciezer te maken, bekijk het volgende getal. Voor het gemak is het in binaire notatie geschreven, en ook voor het gemak bekijken we alleen getallen tussen 0 en 1. Het getal is

$$\texttt{0,1111111111111111111111111111111}\ldots$$

In dit geval is het niet moeilijk de volgende 'decimaal' te raden. het is simpelweg een oneindige reeks `1`-en. Deze oneindige reeks staat voor het getal 1. (De binaire variant op 0,99999999999...) Ook al bevat de ontwikkeling een oneindig aantal cijfers, er is niet oneindig veel informatie voor nodig om deze reeks te coderen. In woorden kunnen we gewoon zeggen 'schrijf een oneindige reeks `1`-en.' We kunnen ook een instructiecode schrijven voor een computer, bijvoorbeeld een universele Turingmachine. Deze code zal zeer kort zijn, in ieder geval veel korter dan het uiteindelijke getal.

Soortgelijk kan het getal

$$\texttt{0,0000000000000000000000000000000}\ldots$$

ook veel korter worden samengevat.

Maar wat kunnen we zeggen over het volgende getal

$$\texttt{0,1100100100001111110110101010000}\ldots$$

Hoe moeilijk is het hier het volgende cijfer te raden? De puzzel wordt opgelost als we erbij vermeld krijgen dat dit de ontwikkeling is van $\pi/4$. In dat geval is er een eenvoudige formule die ons de volgende cijfers in de binaire ontwikkeling geven. Bijvoorbeeld de formule van Leibniz[4]

$$\frac{\pi}{4} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$$

Een beter convergerende serie is trouwens

$$\frac{\pi}{4} = \frac{3}{4} + \frac{1}{2 \cdot 3 \cdot 4} - \frac{1}{4 \cdot 5 \cdot 6} + \frac{1}{6 \cdot 7 \cdot 8} + \ldots$$

Voor de echte liefhebbers: in 1995 werd de volgende magische formule voor π gevonden door Bailey, Borwein en Plouffe:

$$\pi = \sum_{n=0}^{\infty} \left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6} \right) \left(\frac{1}{16} \right)^n$$

[4] Ook reeds voor Leibniz bekend.

Met deze formule kan direct de $n$de bit in de hexadecimale (zestientallige) en dus ook binaire expansie van π berekend worden, zonder alle tussenliggende cijfers eerst te hoeven berekenen! Het wereldrecord is nu voor de 10^{15}-ste binaire bit (ja, de duizend biljoenste bit). Deze is `0`. Om precies te zijn de ontwikkeling gaat verder als

$$\texttt{0011000100001011010110000011010011100}\ldots$$

In ieder geval kunnen we computer programmeren met een eindige code die deze oneindige reeks cijfers genereert.

Maar dit terzijde. Het gaat erom dat in het algemeen kunnen we nu kunnen vragen: "Is er een code P die het getal $x \in [0,1]$ geeft als uitvoer?" Preciezer geformuleerd: "Kunnen we de universele Turingmachine een code P aanbieden, zodat de invoer `0000000.....` (de lege tape) wordt omgezet in de binaire ontwikkeling van het getal x?" In dat geval noemen we x *berekenbaar*. Deze machinevertaling betekent eenvoudig dat er een bepaald wiskundige procedure is, die uiteindelijk het getal x kan geven (zoals in het voorbeeld van $\pi/4$).

Deze definitie geeft ook aan dat er een natuurlijke maat is voor de *algoritmische complexiteit* van het getal x, namelijk de lengte van het kleinste programma P dat x geeft als uitvoer. Op deze wijze zullen de getallen 0 en 1 een kleine complexiteit hebben, en $\pi/4$ een, maar uiteindelijk niet veel, grotere. Er zijn natuurlijk vele voorbeelden te vinden van getallen met een veel grotere complexiteit.

Is er een lijst van alle berekenbare getallen? Kunnen we vaststellen van een getal x of het berekenbaar is of niet? Wel, we hebben al gezien dat de berekenbare getallen overeenkomen met programmacodes. Deze codes P hebben allemaal een eindige lengte, en kunnen dus alfabetisch gerangschikt worden, met het kortste programma bovenaan. Zo krijgen we een lijst van programma's $P_1, P_2, P_3, \ldots$. Bij deze reeks programma's hoort een reeks getallen $x_1, x_2, x_3, \ldots$. Iedere zo'n getal is een (oneindige reeks) `0`-en en `1`-en. We krijgen dus een reeks van de vorm

$$\begin{aligned}
x_1 &= \texttt{100101000101010}\\
x_2 &= \texttt{011110100100110}\\
x_3 &= \texttt{110001010010011}\\
x_4 &= \texttt{000100101101010}\\
x_5 &= \texttt{001001100101111}\\
\ldots &\quad \ldots
\end{aligned}$$

Maar op deze reeks kunnen we weer de truc van Cantor toepassen. Neem de diagonaal. Dat wil zeggen, het eerste cijfer van x_1, het tweede cijfer van x_2 etc. Dan krijgen we in ons voorbeeld

$$\texttt{11010}\ldots$$

Verander nu iedere `0` in een `1` en omgekeerd. We krijgen nu een getal

$$y = \texttt{00101}\ldots$$

Dit getal y staat niet in de lijst, en is dus niet berekenbaar.

Dit argument leert ons dus dat er onberekenbare getallen zijn. Maar er zit een adder onder het gras. Hebben we niet net een procedure gegeven hoe het getal y berekend kan worden? Moeten we daarom

niet y toevoegen aan de lijst van berkenbare getallen? Maar dan geeft Cantors diagonaalmethode een nieuw getal y', etcetera, etcetera.

Waar zit hier de 'catch'? Onze premisse was dat we een lijst konden opstellen van alle programma's P_n die een berekenbaar getal gaven. Hoe herkennen we die programma's? Ten eerste moeten we controleren of een code P de code van een grammaticaal correcte instructie is. Anders verslikt de universele Turingmachine zich in P. Dat is eenvoudig, want de regels waaraan een consistent programma moet voldoen zijn duidelijk te controleren. Maar nu rijst de vraag: "Wat gaat het programma P doen als de lege tape wordt aangeboden? Gaat het een uitvoer x geven?"

Hier botsen we wederom op het haltingprobleem. Om zeker te weten dat programma P, zeg, het 312ste cijfer van de uitvoer x definitief heeft geschreven, moeten we zeker weten dat het programma niet terugkeert en alsnog een 0 in een 1 verandert (of omgekeerd). Maar die vraag is een variant op het haltingprobleem waarvan we nu net hebben aangetoond dat het niet oplosbaar is! Het is dus niet mogelijk de lijst van programma's $P_1, P_2, P_3, \ldots$ te maken, en dus ook niet de lijst van berekenbare getallen.

TECHNIEK 25.

Post's correspondentieprobleem

Het onbeslisbaarheidsbewijs voor het haltingprobleem konden we weer geven door een zelfreferentie. Omdat het veronderstelde programma ook moet werken op zichzelf en zijn tweelingbroertjes komen we tot een tegenspraak. Het lijkt erop dat we naar dergelijke 'hogere orde' probleemgevallen moeten zoeken om zo'n negatief resultaat als onbeslisbaarheid te kunnen bewerkstelligen.
Er zijn echter ook veel op het eerste gezicht veel meer onschuldige problemen te geven die uiteindelijk ook onberekenbaar blijken te zijn. Een bekend voorbeeld, al aan het begin van de 20ste eeuw bedacht door de Amerikaanse wiskundige en logicus Emile Post, is het volgende correspondentieprobleem.
Stel we hebben twee verschillende manieren om een eindig aantal symbolen binair — met nullen en enen — te coderen. Bijvoorbeeld:

	a	b	c	d
codering 1	*11*	*01*	*01110*	*1001*
codering 2	*101*	*011*	*1010*	*01*

De vraag die het correspondentieprobleem stelt is of er een rijtje te geven is wat na codering volgens de verschillende methoden toch dezelfde rij van nullen en enen oplevert. In het geval hierboven kunnen we een positief antwoord geven: `babcd` *geeft na codering in beide gevallen* `011101011101001`*. De vraag is nu of er een Turingmachine te geven is die dit voor elk mogelijk tweetal coderingen beantwoord. Het antwoord is "Nee!" Het correspondentieprobleem is onbeslisbaar.*

Berry's paradox

Dit is misschien een goed moment om kort even een andere paradox (ook voor het eerst gemeld door Russell) te vermelden. We zeggen dat een getal x complexiteit 13 heeft als het kleinste programma dat x kan geven lengte 13 heeft. Dat wil zeggen dat programma heeft 13 'woorden'. We kunnen nu het volgende getal definiëren (paradox van Berry)

Het kleinste getal dat niet in dertien of minder woorden beschreven kan worden.

Op het oog is er hier niets mis mee. We hebben vele getallen die meer dan 13 woorden of symbolen nodig hebben voor hun definitie, en er zal wel een de kleinste zijn. De paradox verschijnt pas als we het aantal woorden in bovenstaande zin tellen, dat zijn er namelijk dertien! We hebben het getal dus net in precies dertien woorden gedefinieerd!

P 17.

ALAN TURING

1912 — 1954

Alan Turing *speelde buiten de wiskunde een minstens zo grote heldenrol. Hij werkte in WOII voor de Britse geheim dienst bij de cryptografische dienst, en leverde een zeer groot aandeel in het ontcijferen van de Duitse enigma-code. Dit was het versleutelingsmechanisme achter de geheime communicatie tussen de Duitse eenheden. Op basis van het indrukwekkende ontcijferingswerk van Turing en zijn collega's zijn belangrijke slagen beslist in het voordeel van de geallieerden.*
Uiteindelijk blijkt zijn rol vervuld van tragiek. Turing pleegde in 1954 zelfmoord, waarvan sommigen beweren dat zijn oude werkgever, de Britse geheime dienst, hem ertoe heeft aangezet. Turing leidde een tamelijk openlijk homosexueel leven, en zou daarom gemakkelijk te chanteren zijn geweest. Dat zou te gevaarlijk zijn voor een man die zoveel wist. Een absolute aanrader waarin deze heldentragiek is opgetekend is Turing's biografie, geschreven door Andrew Hodges: 'Alan Turing: The Enigma' (ook in het Nederlands).

7.2 Redeneren, Rekenen en Complexiteit

Tot dusver in dit hoofdstuk werd de operationele kant van de wiskunde benadrukt, waarbij rekenen en rekenmachines centraal stonden. Zo langzamerhand hebben we in dit boek nu al heel wat kenmerkende aspecten gezien van wiskundige activiteiten. Eerst stond manipuleren van symbolen in formele talen centraal, vervolgens het geven van bewijzen in formele axiomatische theorieën, en nu dan weer het rekenen volgens bepaalde regels die ook gehanteerd kunnen worden door automaten. Toch vormen al deze gezichtspunten een eenheid vanuit logisch perspectief. Deze eenheid is historisch langzamerhand gegroeid, en ze culmineerde theoretisch in de inzichten van het grondslagenonderzoek van de wiskunde, waarvan Gödel's Stellingen uit 1931 de beroemdste zijn. Sinds die tijd is de eenheid van rekenen, bewijzen en symbolische taken ook praktisch gemeengoed geworden. Een moderne computer doet niet anders: uw tekstverwerker rekent 'achter de schermen', achter diverse programmeertalen die berekeningen uitvoeren schuilt een bewijssysteem, maar hetzelfde geldt ook voor een expertsysteem dat wordt gebruikt om bijvoorbeeld medische beslissingen te ondersteunen.

We willen nu nader illustreren door in te gaan op drie thema's. Eerst kijken we naar verbanden tussen logische taken en rekentaken, die vaak heel verrassend liggen. Vervolgens gaan we verder in op de *fijnstructuur* van rekenen, en wel de complexiteit van rekenmethoden. Deze ligt heel verschillend, vanaf snel en makkelijk op een computer uitvoerbaar tot buitengewoon complex, met als bekend voorbeeld de 'exponentiële groei' waarvoor diverse scenario's inzake milieuproblemen, bevolkingsgroei, en informatieoverdaad op het internet waarschuwen. Tenslotte leggen we weer ons gebruikelijke verband naar menselijke cognitie, met de vraag wat deze noties betekenen voor het begrip van de manier waarop wijzelf met rekentaken omgaan.

Daarnaast willen we in dit boek ook aandacht besteden aan de grondslagenresultaten van Gödel en anderen, maar dit doen we in een toegevoegde afsluiting (7.3) dat apart gelezen kan worden, zowel vanwege het belang als de hogere moeilijkheidsgraad.

Redeneren is rekenen is redeneren

In de logica zijn gevolgtrekkingen in wezen slechts taalvormen. Eén of meer rijtjes symbolen staan voor de gegevens, gevolgd door eens nog zo'n rijtje voor de conclusie. Sommige van zulke symboolrijtjes, zoals '$A \to B, \neg B \Rightarrow \neg A$', hebben dan de eigenschap van logische geldigheid; andere, zoals '$A \to B, \neg A \Rightarrow \neg B$', hebben die eigenschap juist niet. Om te bepalen of een gegeven gevolgtrekking geldig is kan men in principe dus werken met een rekenmethode op symbolen! Dit idee heeft een lange geschiedenis, zoals we reeds eerder aanstipten.

Reeds de beroemde zeventiende eeuwse wiskundige Leibniz vatte redeneren op als een speciale vorm van rekenen. Hiertoe zocht hij naar een algemene symbolentaal, de 'Characteristica Universalis', waarin beweringen exact kunnen worden geformuleerd. Daarna zou geldigheid van gevolgtrekkingen worden berekend via een 'Calculus Ratiocinator', een soort algemene logische machine. Leibniz is niet geheel toevallig ook de bedenker van het binair rekenen met grondtal 2, hetgeen de basis vormt van symbolische manipulatie door moderne computers. Leibniz' project is overigens nooit gerealiseerd, tenzij in zijn volumineuze archieven nog een gouden sleutel wordt ontdekt... Ook Boole, de ontdekker van de moderne propositielogica, analyseerde rond 1850 redeneren weer als rekenen, gebruik makend van de analogieën tussen Boolese operaties als $\wedge$, $\vee$ en numerieke optelling en vermenigvuldiging op de getallen $\{0, 1\}$, de moderne 'Boolese Algebra'. De negentiende eeuw is ook de tijd waarin de eerste concrete rekenmachines werden geconstrueerd, zoals het rekenapparaat van Babbage, of Stanley Jevons' 'logische piano'. Vanaf deze ideeën loopt een rechte lijn naar de moderne informatica, met Turing's analyse van rekenmachines uit het voorgaande hoofdstuk als mijlpaal in de

jaren 1930. Voor het eerst werd toen mechanische berekenbaarheid wiskundig gedefinieerd, en op zijn grenzen onderzocht, terwijl ook de ontwikkeling van echte rekenmachines een stimulans kreeg, waarbij logisch geïnspireerde wiskundigen als Turing en Von Neuman een grote rol speelden. Turing's werk laat tevens concreet zien dat manipuleren van symbolen door geschikte codering in getallen neerkomt op een vorm van rekenen. Destijds waren dit verrassende inzichten, die vaak als enigszins kabbalistisch werden ervaren. Tegenwoordig is dit alles praktisch gemeengoed. Een computer die taal verwerkt staat in feite te rekenen.

Nog iets ruimer, alle processen die symbolen manipuleren, zoals logisch bewijzen, of grammaticale ontleding voor natuurlijke taal, zijn op te vatten als een vorm van rekenen. Maar dit verband ligt net zo goed omgekeerd! We kunnen elke vorm van rekenen opvatten als een vorm van bewijzen: elke valide rekenstap is immers een soort geldige gevolgtrekking. Ook dit tweede, omgekeerde gezichtspunt heeft groot praktisch belang. Zo reduceren diverse programmeertalen, zoals PROLOG, rekenproblemen op uw computerscherm tot een vorm van bewijzen in een onderliggend logisch systeem, dat de gebruiker verder niet te zien krijgt. We bespreken nu verder, zoals boven aangekondigd, enkele raakpunten tussen redeneren en rekenen, zonder voorkeursrichting, met speciale aandacht voor niveaus van complexiteit van rekentaken. Sommige Turingmachines voeren hun taken snel uit, andere nemen een hoog tijd- en ruimtebeslag. Het blijkt dat hierover precieze uitspraken zijn te doen. Rekencomplexiteit is een onderwerp van groot belang in de informatica, dat sinds het ontstaan in de jaren zeventig een geheel nieuwe wiskundige theorie heeft opgeleverd.

Propositielogica als rekenen

Geldigheid van een gevolgtrekking in de propositielogica werd in een eerder hoofdstuk getest met semantische tableaus, een symbolische, en half-grafische methode. Maar we kunnen deze geldigheid ook uitrekenen met zogenaamde *waarheidstabellen*. Deze welbekende methode berust op de volgende observatie. De Boolese taal beschrijft heel simpele situaties, namelijk hoe het staat met waarheid en onwaarheid van de basisbeweringen. Bekijk bijvoorbeeld weer eens onze geldige gevolgtrekking uit 6.2

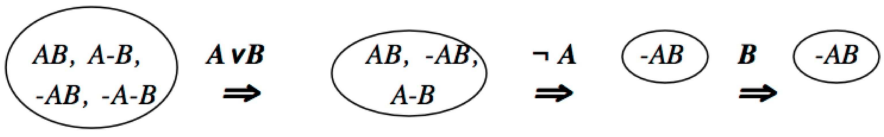
van premissen $A \vee B, \neg A$ naar conclusie B.

Er zijn voor de beoordeling hiervan vier relevante situaties, te weten de vier verdelingen van 'waar' en 'onwaar' over de twee basisbeweringen A en B. Deze kunnen we weergeven als

$$AB, A\text{–}B, \text{–}AB, \text{–}A\text{–}B.$$

Elk van die situaties leidt tot uniek bepaalde waarheidswaarden voor alle samengestelde beweringen met Boolese operaties. Zo geldt de disjunctie $A \vee B$ alleen in de eerste drie hier genoemde situaties, en de negatie $\neg A$ alleen in de laatste twee. Intuïtief kunnen we nu als volgt denken over de geldigheid van de bovenstaande gevolgtrekking. Het begin is een toestand waar we nog niets weten. Alle vier genoemde situaties zijn dan nog mogelijk. De eerste premisse $A \vee B$ vertelt ons dan dat we zitten in een van de eerste drie situaties, en de tweede premisse $\neg A$ sluit daarvan nog eens de eerste twee uit. We zitten derhalve in de situatie $\text{–}AB$ en daar is de conclusie B inderdaad waar!

Dit idee is makkelijk te visualiseren. Hier is een video-strip van de opeenvolgende 'informatietoestanden' en de bijbehorende 'updates' die we in de voorgaande passage hebben beschreven:



Om hiermee nu gewoon te rekenen introduceren we waarheidswaarden 1 ('waar') en 0 ('onwaar'). Bijvoorbeeld, de situatie A–B geeft aan A de waarde 1 en aan B de waarde 0. De Boolese operaties in samengestelde beweringen corresponderen dan met eenvoudige rekenvoorschriften voor verdere waarheidswaarden. Om te beginnen keert een negatie de waarheidswaarde om:

$$\text{waarde}(\neg A) = 1 - \text{waarde}(A)$$

Een conjunctie $A \wedge B$ is alleen waar als zowel A als B waar zijn. Dit effect krijgen we precies met vermenigvuldiging van waarheidswaarden:

$$\text{waarde}(A \wedge B) = \text{waarde}(A) \cdot \text{waarde}(B)$$

Een disjunctie $A \vee B$ (als steeds gelezen als de 'inclusieve of') is alleen dan waar als minstens één van A en B waar is. Dit wordt bereikt door te stellen:

$$\text{waarde}(A \vee B) = \text{ het maximum van waarde}(A) \text{ en waarde}(B)$$

Compacter genoteerd staan hier de bijbehorende waarheidstabellen:

A	$\neg A$
1	**0**
0	**1**

$A \wedge B$	1	0
1	**1**	**0**
0	**0**	**0**

$A \vee B$	1	0
1	**1**	**1**
0	**1**	**0**

De dun gedrukte getallen verticaal geven de waarden voor argument A aan, horizontale die voor B. De vet gedrukte getallen geven de waarden van de Boolese operatie voor de vier mogelijke combinaties voor de argumenten. Tabellen voor andere logische operaties, met name implicatie en equivalentie, zijn ook eenvoudig op te stellen, maar we zullen ze hier niet gebruiken.

Nu wordt het controleren van geldig gevolg een kwestie van eenvoudig rekenen. We maken een volledige tabel van de vier situaties voor de eerdere gevolgtrekking, en berekenen de waarheidswaarden van alle betrokken beweringen:

A	B	$A \vee B$	$\neg A$	B
1	1	1	0	1
1	0	1	0	0
0	1	1	1	1
0	0	0	1	0

Om te testen of B volgt uit $A \vee B, \neg A$ zoeken we dan alle lijnen (d.w.z., mogelijke situaties) waar alle premissen 1 krijgen — hier is dat alleen de derde lijn — en gaan na of daar ook de conclusie een 1 krijgt. Dat klopt in dit geval. De bovenstaande gevolgtrekking is dus geldig.

Deze methode werkt voor alle propositielogische gevolgtrekkingsproblemen. In het bijzonder komt op deze manier ook *ongeldigheid* concreet aan het licht. Ter vergelijking is hier een ongeldig geval:

$$\neg A \vee B, A \not\models \neg B$$

A	B	$\neg A$	$\neg A \vee B$	A	$\neg B$
1	1	0	1	1	0
1	0	0	0	1	1
0	1	1	1	0	0
0	0	1	1	0	1

De eerste lijn is een tegenvoorbeeld. In de situatie AB gelden de beweringen $\neg A \vee B$ en A allebei, maar toch is de conclusie $\neg B$ hier niet waar. Overigens kunnen we op eenzelfde manier ook andere vragen beantwoorden uit eerdere hoofdstukken. Stel dat we een aantal beweringen krijgen met de vraag of deze *consistent* zijn. Dan schrijven we weer de volledige waarheidstabel op en zoeken naar een lijn die aan elke gegeven bewering de waarde 1 toekent.

Het zal duidelijk zijn dat deze eenvoudige methode altijd toepasbaar is voor wie secuur kan tabuleren en rekenen met eenvoudige operaties. De moeilijkheid zit hem eigenlijk meer in de *hoeveelheid* van die simpele rekenhandelingen. Met meer basisbeweringen in een gevolgtrekking wordt de tabel namelijk snel groter. Neem bijvoorbeeld de Resolutieregel van PROLOG, genoemd in hoofdstuk 6 over automatisch bewijzen:

$$\text{uit } A \vee B, \neg A \vee C \text{ volgt } B \vee C \tag{7.2}$$

Om na te gaan dat Resolutie geldig is heeft u al een waarheidstabel nodig met acht lijnen, voor alle combinaties van de drie relevante beweringen A, B en C. De groei in het aantal rekenstappen is in het algemeen exponentiëel in de grootte van de invoerformules. In principe is dit uiterst complex, zelfs al blijkt de praktijk vaak mee te vallen. We gaan hier later in dit hoofdstuk nader op in.

Het rekenkarakter van geldigheid komt bijzonder sprekend tot uiting in het verschijnsel van geldige equivalenties, dat wil zeggen, formules van de vorm $A \leftrightarrow B$ die op elke lijn van hun waarheidstabel de waarde 1 krijgen. Het is bijzonder instructief om een aantal van dergelijke principes na te rekenen, en te zien hoe uiteindelijk overal enen verschijnen. Hier zijn een aantal geldige principes van de zogenaamde 'Boolese Algebra':

T. 26 ⟹ 218

Dubbele negatiewet	$\neg\neg A \leftrightarrow A$
De Morganwetten	$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$
	$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
Distributiewetten	$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$
	$A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$

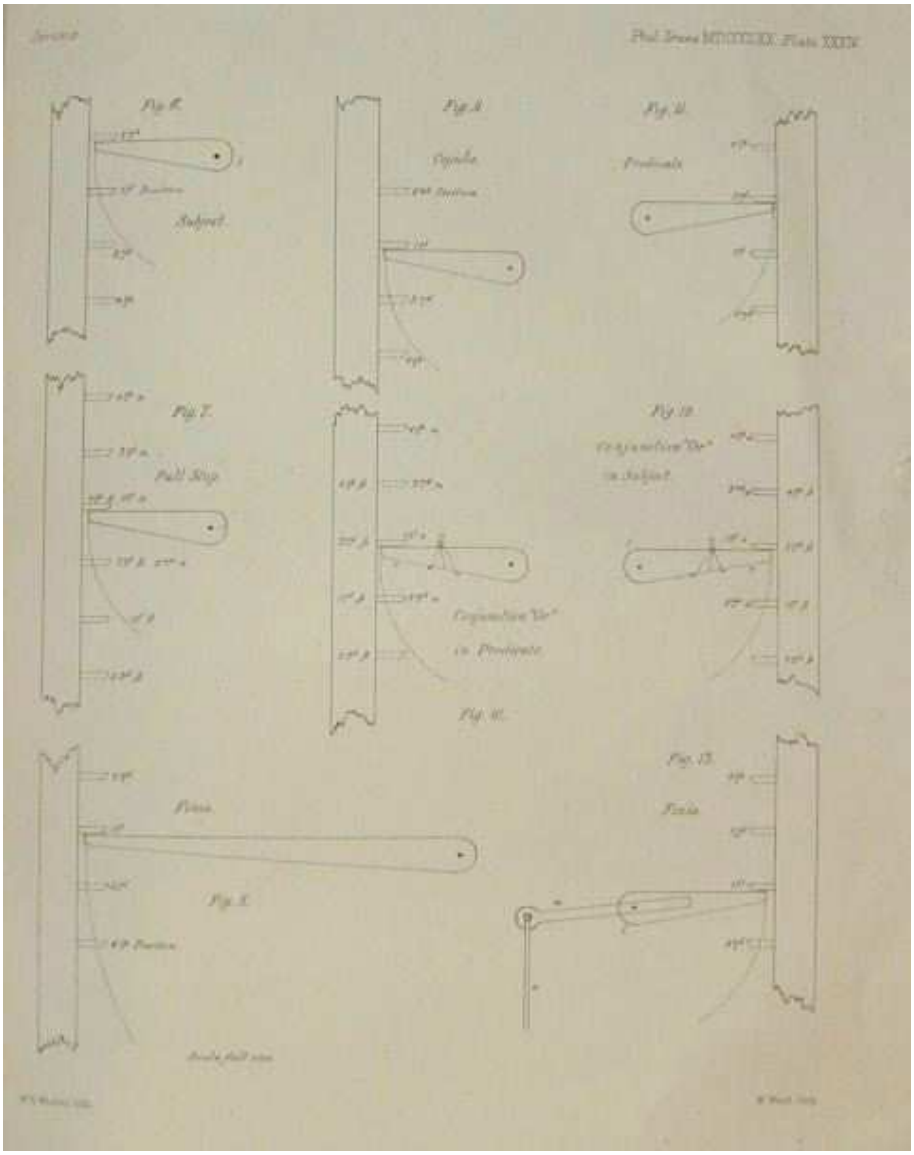
Zoals we ook al kort aanduidden in hoofdstuk 6, zijn dit in feite algebraïsche rekenregels voor de logische operaties. Deze zijn zelfs mooier dan die voor gewone getallen. Zo hebben we voor de natuurlijke getallen wel de distributiewet

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

maar niet:

$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

Voor conjunctie en disjunctie mag het echter allebei! Waarheidstabellen en Boolese algebra liggen ten grondslag aan de digitale circuits die nog steeds al onze computers sturen.



Een originele ontwerp-plaat van William Stanley Jevons' logische piano in een artikel van zijn hand uit 1870. Dit is de eerste logische machine die op basis van 'Boolese rekenen' syllogistische redeneringen aankon. Het apparaat was geheel van hout. Op internet wordt de bundel met Jevons' piano-ontwerp erin voor $ 3200 aangeboden.

Kwantor-logische taken als rekentaken

De volle taal van de wiskunde maakt naast Boolese operaties ook essentieel gebruik van kwantoren $\forall$, $\exists$. Deze grotere uitdrukkingskracht leidt tot een rijker repertoire aan logische taken. We bespreken een drietal voorbeelden, die alle in eerdere hoofdstukken al aan de orde kwamen. Om te beginnen is er weer het analoog van uitrekenen van een waarheidswaarde:

Modelcontrole

Gegeven een structuur M en een formule φ, bepaal of die formule waar is.

Boolese algebra

George Boole introduceerde zijn algebra voor propositielogica in 1847 in het boek 'The Laws Of Thought: Investigations in the Theory of Logic and Probability'. Hier zijn onze denkwetten:

⊥⊤-WETTEN

$$\begin{array}{lll} \bot \wedge \varphi = \bot & \top \wedge \varphi = \varphi & \varphi \wedge \neg\varphi = \bot \\ \bot \vee \varphi = \varphi & \top \vee \varphi = \top & \varphi \vee \neg\varphi = \top \end{array}$$

DUBBELE NEGATIE

$$\neg\neg\varphi = \varphi$$

IDEMPOTENTIE

$$\begin{array}{l} \varphi \wedge \varphi = \varphi \\ \varphi \vee \varphi = \varphi \end{array}$$

COMMUTATIVITEIT

$$\begin{array}{l} \varphi \wedge \psi = \psi \wedge \varphi \\ \varphi \vee \psi = \psi \vee \varphi \end{array}$$

ABSORPTIE

$$\begin{array}{l} \varphi \wedge (\varphi \vee \psi) = \varphi \\ \varphi \vee (\varphi \wedge \psi) = \varphi \end{array}$$

DE MORGANWETTEN

$$\begin{array}{l} \neg(\varphi \wedge \psi) = \neg\varphi \vee \neg\psi \\ \neg(\varphi \vee \psi) = \neg\varphi \wedge \neg\psi \end{array}$$

DISTRIBUTIVITEIT

$$\begin{array}{l} \varphi \wedge (\psi \vee \chi) = (\varphi \wedge \psi) \vee (\varphi \wedge \chi) \\ \varphi \vee (\psi \wedge \chi) = (\varphi \vee \psi) \wedge (\varphi \vee \chi) \end{array}$$

ASSOCIATIVITEIT

$$\begin{array}{l} \varphi \wedge (\psi \wedge \chi) = (\varphi \wedge \psi) \wedge \chi \\ \varphi \vee (\psi \vee \chi) = (\varphi \vee \psi) \vee \chi \end{array}$$

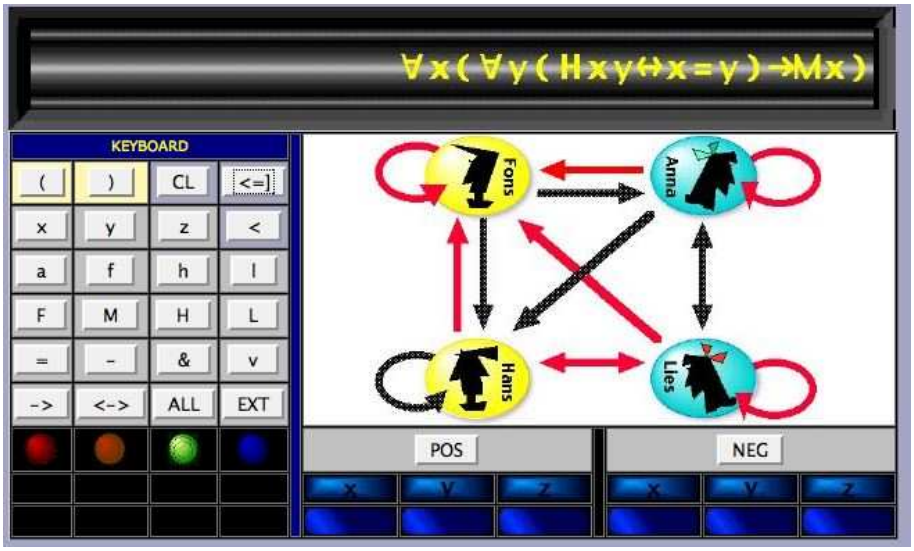
De symbolen $\top$ en $\bot$ zijn nul*-plaatsige connectieven. $\bot$ is de uitspraak die altijd onwaar is, het* falsum*. Het* verum $\top$ *is zijn tegenhanger, de altijd ware uitspraak.*
Boole gebruikte geen implicaties en equivalenties. Ze zijn makkelijk te definiëren: $\varphi \rightarrow \psi = \neg\varphi \vee \psi$ en $\varphi \leftrightarrow \psi = (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$.
Het zal de lezer niet al te lastig vallen na te gaan dat dit een correct stelsel axioma's is. Het is ook een volledig systeem: elke logische equivalentie in equationele Boolese vorm valt af te leiden met gebruikmaking van de wetten hierboven.
Om ook over geldigheid van gevolgtrekkingen te kunnen spreken gebruikte Boole de volgende gedefinieerde relatie:

$$\varphi \leq \psi \quad \Leftrightarrow \quad \varphi \wedge \psi = \varphi$$

De relatie $\leq$ komt overeen met onze eerdere notie $\Rightarrow$ van geldig gevolgtrekking voor het geval de propositielogica. De rechterkant van de equivalentie hierboven kan gelezen worden als "ψ volgt uit φ als ψ geen informatie toevoegt als de informatie φ al gegeven is".

Bijvoorbeeld, gegeven is een graaf M met punten en pijlen, en een formule $\forall x\, \exists y\, Rxy$ die zegt dat elk punt een opvolger heeft in de relatie. Modelcontrole van deze formule betekent dan systematisch nagaan of de relatie in de graaf (zoals gegeven door een plaatje met pijlen, of een tabel in een database) voldoet aan de eigenschap dat vanuit elk punt een pijl vertrekt. Meer ingewikkelde predicaatlogische formules drukken weer andere controleerbare eigenschappen van grafen uit, zoals het bestaan van een Great Communicator in hoofdstuk 6. Het zal duidelijk zijn dat al dit soort vragen systematisch zijn na te gaan wanneer we maar punt voor punt de graaf afwerken. Dit proces is dan ook te programmeren.

Hieronder staat een heel eenvoudige automatische 'model-checker'. Er wordt hier gevraagd: "Als iemand alleen van zichzelf houdt dan moet het een man zijn". Het groene lampje gaat branden!



Modelcontrole-taken komen veel voor in de informatica. Een graaf kan bijvoorbeeld een concrete blauwdruk zijn voor een nieuw ontworpen proces of een organisatie. Belangrijke eigenschappen van dat proces of die organisatie kunnen vaak overzichtelijk worden uitgedrukt in logische formules, en modelcontrole gaat dan na of het gegeven ontwerp voldoet aan de specificaties van de gewenste eigenschappen. Nadat in de negentiger jaren een fout ontwerp voor chips de firma Intel bijna een half miljard dollar kostte, werkt daar tegenwoordig een groep informatici die automatische model-checkers maken om dit soort bugs voortijdig op te sporen. Het probleem is wel vaak dat die modellen weer erg groot worden, zodat het verificatieproces zelf veel tijd neemt. Maar er zijn ook technieken ontwikkeld die dit effect weer kunnen minimaliseren.

Vervolgens komen we weer bij de centrale logische vraag, te weten of een gegeven gevolgtrekking geldig is. Heel vaak komen we deze in de rekenpraktijk tegen als een verwante vraag van

Vervulbaarheid

Heeft een gegeven formule φ een model M dat φ waar maakt?

In dat geval vragen we bijvoorbeeld niet rechtstreeks of een conclusie C geldig volgt uit P, maar equivalent, of $P \wedge \neg C$ vervulbaar is. Zo werkten bijvoorbeeld de semantische tableaus van 6.2, die zochten naar tegenvoorbeelden, en alleen tot geldigheid besloten als er geen enkel tegenvoorbeeld is te vinden. Consistentievragen doen zich ook voor als we een 'verlanglijstje' opschrijven van allerlei eigenschappen waaraan een proces zou moeten voldoen, en ons dan afvragen of überhaupt wel een situatie te vinden is die aan al die eisen tegelijk voldoet. In de informatica noemt men dit soms wel de 'synthese' of 'design' vraag.

Er is een groot verschil in complexiteit tussen Modelcontrole en Vervulbaarheid. Dat moet ook wel, want in hoofdstuk 6 zagen we al dat predicaatlogische geldigheid een uiterst complex begrip was, dat essentieel verwijst naar een oneindige klasse van modellen, die ieder op zich ook nog eens oneindig veel objecten kunnen bevatten. Een eenvoudige eindige opsomming, zoals in de methode van de waarheidstabellen, zal hier zeker niet werken. Bij Modelcontrole ligt dat anders: gegeven worden zowel een specifieke eindige situatie M als een formule φ, en we berekenen alleen voor dat geval een waarheidswaarde. Bij Vervulbaarheid is alleen de formule φ gegeven en we zoeken een M in een oneindige collectie van mogelijke kandidaten die φ waar maakt. Dit is meer open-ended. In feite is het verschil dramatisch. Uit Turing's werk en dat van Gödel, dat we in het volgende hoofdstuk zullen bespreken, volgt zelfs een opmerkelijke negatieve conclusie:

> *Onbeslisbaarheid van de predicatenlogica*
>
> Er bestaat geen mechanische methode voor het volledig en correct testen van geldigheid of vervulbaarheid in de predicatenlogica.

Leibniz' droom van een universele logische machine is dus onuitvoerbaar! Soms zijn eenvoudig te definiëren taken dus helemaal niet voor mechanische rekenoplossingen vatbaar. Als een totale verrassing komt dit overigens niet meer voor ons, want we zagen hetzelfde al in het voorgaande hoofdstuk met het Halting Problem voor Turingmachines, en voor computers in het algemeen. Dat dit verdrietige inzicht kennelijk toch nog ruimte laat voor meer positieve resultaten blijkt uit het feit dat het vak logica na de dertiger jaren bepaald niet is opgeheven, en dat de informatica juist is opgebloeid...

Tenslotte suggereert de predicaatlogische taal ook nieuwe vragen, die in de propositielogica nog niet op de voorgrond traden. Een belangrijk voorbeeld zagen we al in hoofdstuk 2, waar verschillende wiskundige structuren M en N systematisch vergeleken werden met een spel voor twee spelers G en V. Dat spel onderzocht de mate van structurele invariantie tussen M en N, die kon worden gemeten met logische formules die een verschil detecteren. Hier is een derde en laatste bekende taak voor logische systemen:

> *Modelvergelijking*
>
> Gegeven twee eindige structuren (bijv. grafen) M en N, kunnen we ze onderscheiden met een expliciete predicaatlogische eigenschap?

Positief gesteld is dit de vraag wanneer twee eindige structuren dezelfde formules waar maken. Dit laatste bleek in hoofdstuk 2 weer equivalent met een taal-vrije bewering, en wel dat er een *isomorfisme* bestaat tussen de ordeningen van M en N. In die laatste vorm staat modelvergelijking ook wel bekend als het probleem van 'graaf-isomorfie'. In zijn algemeenheid kunnen we Modelvergelijking dus beschouwen als de computationele pendant van de invariantiekwesties in hoofdstuk 2. Dit is ook praktisch nuttig in de informatica, bijvoorbeeld wanneer we willen weten of twee gegeven processen hetzelfde zijn, of althans hetzelfde gedrag vertonen. Nog een andere manier om dit probleem te stellen is vragen welke speler in het vergelijkingsspel de winnende strategie heeft. Daarmee komen we op het gebied van de speltheorie uit hoofdstuk 4, waar eveneens rekenmethoden bestaan voor dit soort taken.

Maar nu dan de complexiteit! Het zal duidelijk zijn dat, als de gegeven structuren eindig zijn, de vergelijkingstaak altijd na een eindig aantal stappen is te beslissen. Maar hoeveel stappen? Met name, is dit probleem nu makkelijker of moeilijker dan Modelcontrole voor predicatenlogica, of het werken met waarheidstabellen in propositielogica? Om dit soort vragen te beantwoorden moeten we preciezer worden over het wiskundige begrip complexiteit.

Complexiteit van algoritmen

We nemen nu een kijkje in de informatica, en de daar ontwikkelde complexiteits-analyse van rekenmethoden, of zoals ze ook vaak genoemd worden *algoritmen*, naar de Perzische wiskundige Al-Kwaraizhmi. In principe kan men bij algoritmen denken aan programma's voor rekentaken op een Turingmachine. Maar in feite is een Turingmachine een tekstverwerker die symbolen verplaatst, afdrukt, verwisselt, en nog veel meer. Dit weerspiegelt de realiteit van de informatica, waar de belangrijkste genres problemen van niet-numerieke aard zijn, zoals sorteren van rijen symbolen, of *zoeken* in een ruimte van mogelijke oplossingen. Om te beginnen bespreken we eerst een veel voorkomende en typisch 'doenlijke' rekentaak in de informatica, die zich leent voor snelle algoritmen c.q. programma's:

> *Bereikbaarheid*
>
> Gegeven is een eindige graaf bestaande uit punten en pijlen, met twee speciale punten s, t ('begin', 'eind'). Bestaat er een pad van opeenvolgende pijlen van s naar t?

Deze vraag is typerend voor zoekproblemen, zoals: "Kan ik een reisroute vinden van Bloemendaal naar Singapore?", of "Is er een reeks zetten vanuit de begintoestand van een spel naar een door mij gewenste eindtoestand?". In de kunstmatige intelligentie zijn zoekproblemen essentiëel, maar ook in het zakelijke gebruik van gegevensbestanden. We meten nu de complexiteit van beantwoording van de Bereikbaarheidsvraag als volgt:

> Wat is het aantal tijdstappen, gemeten in de grootte van de invoergraaf, dat een optimaal algoritme nodig heeft om de taak te verrichten?

Antwoorden zullen hier geen vast getal geven, maar een schatting van een orde van grootte van het aantal rekenstappen, afhankelijk van de grootte van de invoer. Wat we werkelijk willen begrijpen is hoe die rekentijd verloopt als we de invoer groter maken. Loopt ze langzaam op, of snel? Het antwoord dat we krijgen voor zoeken kent hetzelfde soort groei als een cirkeloppervlak met de straal (πR^2), of een afgelegde afstand met een valtijd ($\frac{1}{2}gt^2$):

> *Feit* Bereikbaarheid is oplosbaar met een algoritme dat werkt in kwadratische tijd.

Om dit aan te tonen geven we een kwadratisch algoritme. Hiervoor gebruiken we twee verzameling A en M, respectievelijk van *actieve punten* en *gemarkeerde* punten in de graaf. Deze twee verzamelingen veranderen stapsgewijs tot ofwel de verzameling van actieve toestanden leeg is of de eindtoestand t is gemarkeerd. We beginnen met het activeren en markeren van de begintoestand s:

$$A_0 = M_0 = \{s\}.$$

Als $s = t$ zijn we dus gelijk klaar: het vertrekpunt is gelijk aan het eindpunt. Zo niet, dan gaan we de vervolgende lus herhalen tot we ons doel bereikt hebben:

$$\begin{array}{l} \text{Als } A_n \neq \emptyset \wedge t \notin M_n \text{ dan} \\ \quad \text{Kies een } a \in A_n \\ \quad A_{n+1} \;=\; (A_n \cup \{b \mid b \notin M_n \wedge Rab\}) - \{a\} \\ \quad M_{n+1} \;=\; M_n \cup \{b \mid b \notin M_n \wedge Rab\} \end{array}$$

Met andere woorden, als aan de genoemde eindvoorwaarde niet voldaan is dan nemen we een actieve toestand, deactiveren hem en activeren al zijn opvolgers in de relatie R van de graaf die niet gemarkeerd zijn. Verder markeren we de zojuist geactiveerde toestanden. Als t aan het einde gemarkeerd is

dan is t bereikbaar vanuit de begintoestand s. De actieve toestanden zijn de punten van waaruit we op het gegeven moment naar het eindpunt zoeken. De gemarkeerde toestanden zijn de in onze zoektocht reeds bereikte punten.

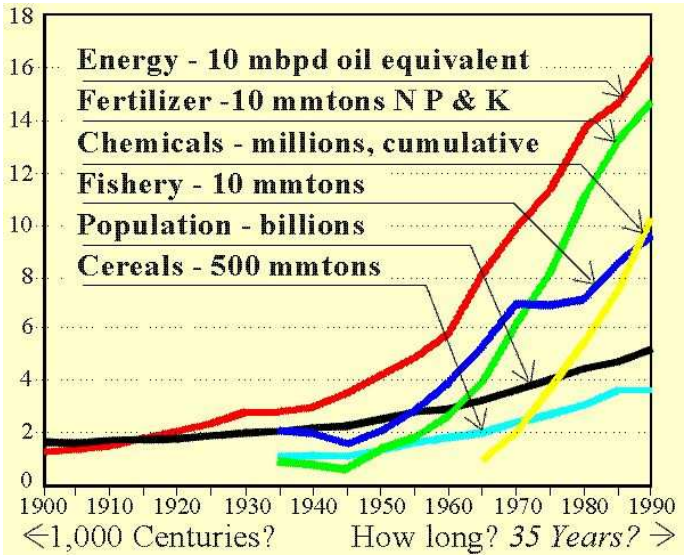
Om in te zien dat het algoritme doet wat het moet doen toont een eenvoudige inductie naar n aan dat

$$(i) \forall t \, \forall n \, (t \in M_n \rightarrow t \text{ is bereikbaar vanuit } s)$$

$$(ii) \forall t \, \forall n \, ((t \notin M_n \wedge A_n = \emptyset) \rightarrow t \text{ is niet bereikbaar vanuit } s)$$

Dit algoritme gebruikt maximaal kwadratische tijd. Elke pijl in de graaf tussen twee punten wordt hoogstens één keer gebruikt, en er zijn maximaal n^2 pijlen.

Kwadratische tijd zegt dat het aantal rekenstappen wordt begrensd door een functie $ax^2 + b$ voor geschikte constante coëfficiënten a en b. Dit is voor computers snel te doen, maar het kan soms nog makkelijker. Een probleem als omzetten van elk symboolrijtje 'je' in een uitdrukking door 'u' vergt slechts één maal door de gegeven uitdrukking lopen, en onderweg symbolen vervangen. Dat kost slechts lineaire tijd in de lengte van de invoer x, begrensd door een nog eenvoudiger uitdrukking $ax + b$, waarbij a en b constanten zijn. Het kan ook lastiger zijn. Zo gebruiken ontledingsalgoritmen, veel gebruikt in natuurlijke taalverwerking op computers, vaak *kubische* rekentijd: het aantal rekenstappen is dan slechts af te schatten met een uitdrukking van de vorm $ax^3 + b$. Men kan bij deze schattingen denken aan plaatjes voor genres van groei zoals we die kennen van de Club van Rome uit de jaren zeventig over milieuproblemen en vervuilingsprocessen: hoe krommer de lijn naar boven, hoe onstuimiger de groei!



Complexiteitsklassen

Meer in het algemeen liggen alle tot nu toe genoemde voorbeelden van taken in de complexiteitsklasse **P** ('polynomiale tijd') van die rekenproblemen waarvoor een algoritme bestaat dat het correcte antwoord geeft in een aantal rekenstappen dat naar boven wordt begrensd door een polynoom (lineair, kwadratisch, kubisch, ...) met als variabele de invoerlengte. Deze worden algemeen gezien als 'doenlijke' taken voor een moderne computer. De groei van de rekentijd met de invoergrootte blijft binnen redelijke grenzen. Maar het kan erger!

Het volgende probleem uit de informatica komt eveneens in talloze varianten voor. De vraag is deze. Een handelsreiziger wil een gegeven netwerk van steden, weergegeven als een graaf, zo doorlopen via een keuze van aanwezige verbindingen dat hij elke stad precies één keer aandoet. Dit heet ook wel het 'Hamilton-probleem' naar de negentiende eeuwse Ierse wiskundige William Rowan Hamilton.

Hamilton-probleem

Is er een rondreis door een gegeven graaf die alle knopen één keer aandoet?

Een methode met grof geweld somt alle verschillende mogelijke routes door de graaf op, en kijkt of daar een rondreis bij zit. Deze methode vergt een *exponentiëel* aantal tijdstappen omdat er exponentiëel veel van dit soort routes kunnen zijn, gemeten in de grootte van de graaf. Maar we kunnen de analyse iets verfijnen, waarbij een patroon aan het licht komt dat in de informatica en logica heel veel voorkomt. Een positief antwoord op de gestelde vraag naar een rondreis heeft namelijk de volgende vorm:

(a) 'Geef een certificaat voor het antwoord', d.w.z. een object dat in korte tijd is op te schrijven gegeven de invoergrootte.

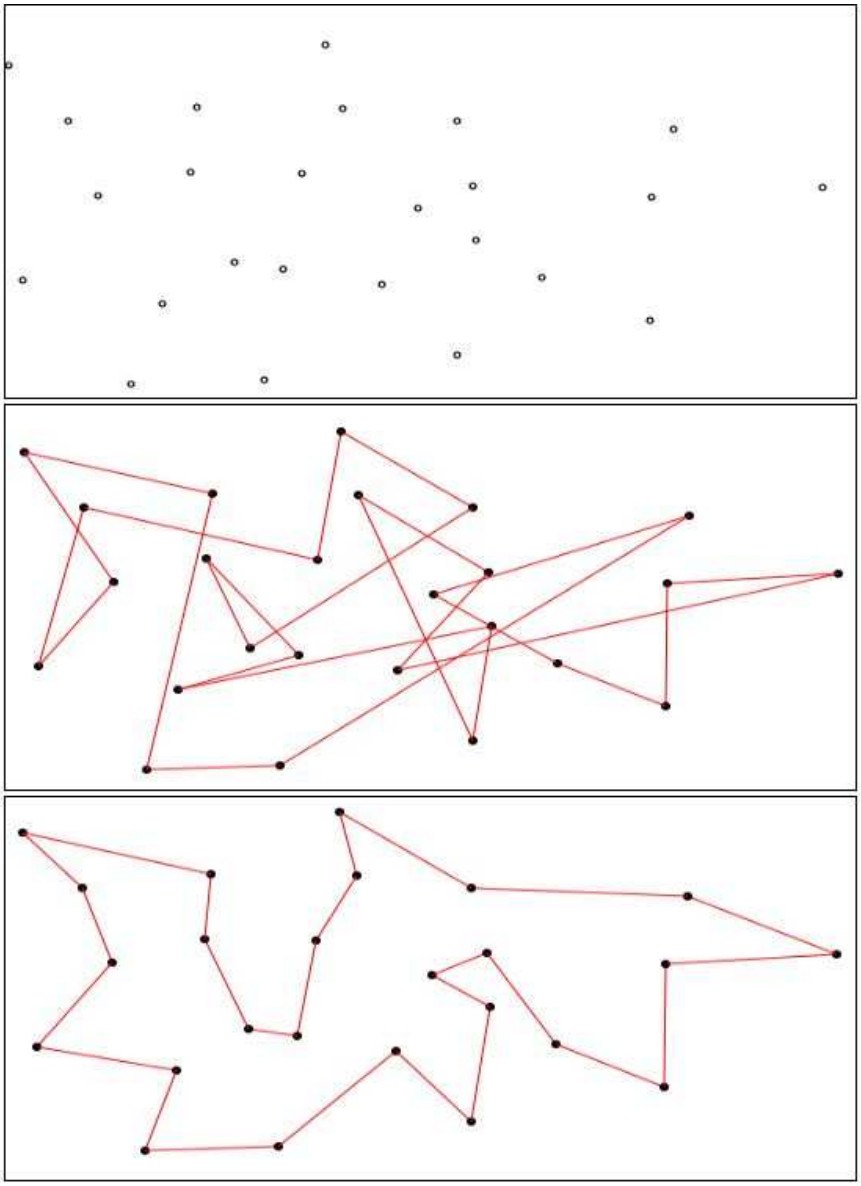
Dat geldt voor elke route op zich: opschrijven kost slechts de grootte van de graaf.

(b) 'Test dat het certificaat voldoet' in korte tijd.

In ons geval is testen dat een voorgestelde route elk punt van de graaf inderdaad precies éń keer bezoekt eveneens snel uit te voeren. Algoritmen die aan de condities (a) en (b) voldoen liggen in de volgende grote familie van rekenproblemen na **P**, te weten de complexiteitsklasse **NP** ('niet-deterministische polynomiale tijd'). Deze bestaat uit alle rekenproblemen waarvoor een JA-antwoord bestaat in het opschrijven van een certificaat in polynomiale tijd in de invoergrootte, gevolgd door verificatie van het certificaat, eveneens in polynomiale tijd in de invoer.

Feit Het Hamilton-probleem ligt in $\mathbf{NP}$.

Het Hamilton-probleem wordt ook wel eens gesteld als het vinden van een *kortste rondreis* voor n steden op een landkaart met wegen. Maar dat is weer complexer qua rekencomplexiteit. Deze versie staat bekend onder de naam *Traveling Salesman*. Hieronder is een landkaart met steden getekend, daaronder de oplossing van een goedkoop maar helaas incorrect algoritme, en daaronder weer de oplossing gegeven door een exponentiëel maar correct algoritme.



P en **NP** zijn slechts het begin van een veel groter landschap van rekenproblemen, en daarmee van soorten van complexiteit. Het kan bepaald nog moeilijker! Een volgend niveau vinden we door te kijken naar het al eerder genoemde probleem oplossen van spelen, dat wil zeggen, het bepalen welke van de spelers een winnende strategie heeft. Meer in het algemeen is dit de speltheoretische vraag naar bepalen van strategische evenwichten uit hoofdstuk 4. Spelen zijn ingewikkelder dan gewone rekenprocessen, omdat we nu de interactie van meerdere personen moeten verdisconteren. Veel problemen in de moderne informatica hebben overigens zo'n interactief spelkarakter: denk maar aan 'e-commerce', of de concurrentie tussen gedistribueerde systemen om schaarse ruimte in processorgeheugen.

Soms is het oplossen van een spel overigens nog eenvoudig. Een bekend genre zijn spelen op een graaf G, startend vanuit een of ander beginpunt.

Graafspel

De eerste speler I kiest een pijl, en we gaan naar het eindpunt daarvan. Nu moet de tweede

speler II vanuit het nieuwe punt een pijl kiezen: enzovoorts, om en om. Als een speler geen pijl kan kiezen vanuit het huidige punt, en het is haar beurt, dan verliest zij. Als het spel oneindig doorgaat, dan wint speler II.

Het is een aardige opgave om te zien hoe we kunnen bepalen wie dit spel kan winnen op een gegeven eindige graaf G vanuit zeker punt s. Dit probleem blijkt oplosbaar in polynomiale tijd gemeten in de grootte van G, en het ligt dus in de klasse $\mathbf{P}$. Maar het graafspel wordt al snel ingewikkelder. Hier is een realistische variatie. In een bekend plaatsnamenspel moeten spelers steden noemen, waarbij de volgende stad moet beginnen met de laatste letter van de vorige, en we verliezen als we geen stadsnaam kunnen noemen, dan wel de eerste herhaling begaan van een eerdere stadsnaam. Dit heet het

Aardrijkskundespel

Dit is het eerdere Graafspel; maar wie terugkeert op een reeds bezocht punt verliest!

Nu wordt het echt lastig. Er valt te bewijzen dat Aardrijkskunde in een echt hogere complexiteitsklasse zit dan $\mathbf{P}$ of $\mathbf{NP}$. De beste omschrijving daarvoor gebruikt echter een nieuwe manier van meten, en wel een ruimtemaat eerder dan een tijdsmaat. We meten het aantal geheugencellen ('rekenplaatsen') dat het algoritme moet gebruiken. Aardrijkskunde blijkt te liggen in de klasse $\mathbf{Pspace}$ ('polynomiale ruimte'). Algoritmen in deze klasse hebben een aantal geheugencellen nodig om in te lezen en schrijven dat wordt begrensd door een polynoom in de invoerlengte. Ter controle, de tijdsmaat $\mathbf{P}$ is bevat in de ruimtemaat $\mathbf{Pspace}$, omdat een algoritme in polynomiale tijd slechts polynomiaal veel geheugencellen kan bezoeken. Het omgekeerde geldt echter niet, daar we eenzelfde geheugenlocatie vele malen kunnen bezoeken. Ergens houdt het nut hiervan overigens op: er kan worden bewezen dat een **Pspace**-probleem ten hoogste exponentiële tijd neemt, omdat al te vaak herhaalde bezoekgewoontes geen zin hebben. Problemen met polynomiale ruimte komen vaak voor in de analyse van bordspelen, zoals het Schaakspel of 'Go'.

Weer moeilijker problemen vragen exponentiële tijd ($\mathbf{Exptime}$), en het groeitempo kan zelfs nog dramatischer zijn. Testen van geldigheid voor logische talen met moeilijke operatoren of ingewikkelde oneindige modellen vergt soms zelfs hyper-exponentiële tijd — 2^{2^x} — of nog veel hoger! Eveneens zeer complex is de beslissingsmethode voor de elementaire schoolmeetkunde waarvan we het bestaan in hoofdstuk 6 hoofdstukvermeldden. In de limiet krijgen we dan genres problemen waarvoor helemaal geen algoritme meer valt te geven. Voorbeelden hiervan zijn het eerder genoemde onbeslisbare Haltingprobleem voor Turingmachines, of het probleem van Geldigheid voor predicatenlogica.

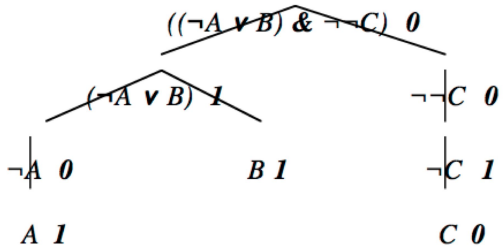
Complexiteit van logische taken

Met deze wiskundige begrippen kunnen we nu terugkeren naar de eerder genoemde drie logische taken, en meer gedetailleerde vragen stellen over de computationele aspecten van de logische begrippen uit de voorafgaande hoofdstukken. Hoe moeilijk waren die taken nu eigenlijk?

Feit

Evaluatie van propositielogische formules is in $\mathbf{P}$, en neemt slechts lineaire tijd.

Neem bijvoorbeeld een situatie waar A en B de waarde 1 krijgen, en C de waarde 0. Dan kunnen we voor een complexe formule als $((\neg A \vee B) \wedge C)$ de waarheidswaarde stapsgewijs van binnenuit berekenen, met de constructie van die formule mee:



Voor een willekeurige bewering φ met lengte $|\varphi|$ kost zo'n proces $c \cdot |\varphi|$ stappen, waar c een of andere constante is. De reden is simpel. Het aantal subformules is gelijk aan de lengte van de formule. Dit is natuurlijk wel een ruwe schatting, die afhangt van wat we tellen als stappen in het proces. Bijv. als we het opschrijven van de waarheidswaarde voor een A zelf zien als proces van opzoeken in de gegeven lijst van waarden voor basisbeweringen, dan kost dat nog een lineaire factor extra in de lengte van φ. Geheel exact kunnen we dit maken door een Turingmachine te programmeren om de taak te doen, en dan het aantal rekenstappen daarvan te tellen. Maar onafhankelijk van de precieze implementatie blijken dit soort analyses qua orde van grootte stabiel, in elk geval tot op een polynomiale factor.

Maar nu de volgende propositielogische taak, waarvoor waarheidstabellen eigenlijk waren bedacht! Stel dat we geldigheid of consistentie willen uitrekenen voor een gegeven formule. Evaluatie van formules op elke lijn van de waarheidstafel is snel, zoals we net zagen. Maar er is een probleem: het aantal lijnen. Voor formules met n basisbeweringen moeten we 2^n lijnen opschrijven, en daarmee hebben we exponentiële groei voor het totale rekenproces, gemeten in de lengte der invoerformules. Preciezer nadenkend zien we dat consistentie vraagt om een certificaat (een valuatie) dat moet worden getest of het de gegeven formule waar maakt, en we concluderen:

Feit

Consistentie van propositielogische formules is in $\mathbf{NP}$.

De semantische tableaus van hoofdstuk 6 veranderen dit oordeel niet wezenlijk, al besparen ze soms wel op het volledige uitschrijven van een waarheidstabel. Maar hun splitsende regels voor disjunctie en conjunctie zorgen in principe nog steeds voor exponentiële groei... De beide hoofdklassen van de complexiteitstheorie doen zich dus al voor in het eenvoudigste logische systeem. Als we nu kijken naar de rijkere predicatenlogica, dan gaan de drie eerder genoemde kerntaken omhoog in complexiteit. We geven hier alleen de uitkomsten, zonder nadere toelichting:

Feiten

Modelcontrole voor predicatenlogica neemt polynomiale ruimte ($\mathbf{Pspace}$).

Vervulbaarheid voor predicatenlogica is onbeslisbaar.

Modelvergelijking voor predicatenlogica is in $\mathbf{NP}$.

Dit laatste feit komt omdat testen voor isomorfisme tussen twee grafen weer het typische $\mathbf{NP}$-karakter heeft van: 'geef een certificaat (een kandidaat functie), en voer een controle uit of de functie aan de isomorfie-eisen voldoet'.

Wat we hier zien is de eerdere kwestie van *balans* in het functioneren van logische systemen. Wanneer we de uitdrukkingskracht van een taal uitbreiden om meer wiskundige structuur te beschrijven betalen we een prijs. De rekencomplexiteit van de kerntaken voor een rijkere taal gaat doorgaans

omhoog. Maar elk nadeel heeft zijn voordeel. Omgekeerd zal, als we uitdrukkingskracht verkleinen, complexiteit ook weer verminderen. De kunst is nu om zoveel mogelijk te zeggen met een taal, maar niettemin wezenlijke 'tijdwinst' te boeken. Een voorbeeld van dit verschijnsel is de modale logica uit hoofdstuk 2. Dit was een taal om te spreken over procesgrafen die qua uitdrukkingskracht in ligt tussen de propositielogica en predicatenlogica. Deze bescheidenheid wordt beloond. Modelcontrole voor modale formules ligt in $\mathbf{P}$, vervulbaarheid van modale formules is te testen in $\mathbf{Pspace}$, en is dus beslisbaar), en modelvergelijking (d.w.z. testen op bisimulatie) ligt in $\mathbf{P}$. Een goed begrip van de delicate balans tussen uitdrukkingskracht en complexiteit is essentieel bij het ontwerpen van nieuwe formele talen in wiskunde en informatica.

Complexiteitstheorie

Complexiteit is een belangrijke wiskundige manier van denken over rekenproblemen. Sinds het begin van de jaren zeventig is een heel nieuw gebied ontstaan van Complexiteitstheorie, die de fijnstructuur bestudeert van berekeningen. Een belangrijk hulpmiddel hierbij is de zogenaamde Hiërarchie van Complexiteitsklassen

P NP Pspace Exptime ... **Onbeslisbaar** ...

die nog veel meer stadia kent dan wat we zojuist hebben gezien. Dit is misschien de plaats om te bekennen dat we in het voorgaande niet helemaal nauwkeurig zijn geweest. Wat we werkelijk bedoelden als we zeiden dat een probleem in zo'n complexiteitsklasse lag was dat het daarin ligt, *en in geen lagere*! Aantonen van zo'n 'ondergrens' van moeilijkheid is vaak veel lastiger dan het aangeven van een intutieve 'bovengrens', waartoe wij ons hebben beperkt.

Bewijstechnieken in de complexiteitstheorie gebruiken vaak combinatorische methoden samen met ideeën uit de logica, inclusief variaties op diagonaalargumenten. Met name is daarbij gebleken dat redeneerproblemen en rekentaken nog veel inniger samenhangen dan reeds bekend was uit het werk van Turing en Gödel. Zo is het mogelijk om met geschikte vertalingen in logische formules alle centrale rekentaken van de informatica, zoals Bereikbaarheid, Handelsreiziger, of Speloplossing, efficiënt te reduceren tot logische taken van Evaluatie of Consistentie in propositielogica, of Modelcontrole in predicatenlogica. Dit illustreert weer het opmerkelijk hechte verband tussen redeneren en rekenen. Met name kan iemand die complete waarheidstabellen kan maken, in wezen elke $\mathbf{NP}$ rekentaak aan! Of iets beeldender gesteld: iemand die correct redeneert lost *tegelijkertijd* interessante rekenproblemen op! In het licht van de complexiteitstheorie is iedere oplossing van een enkel probleem meteen ook een oplossing van een hele familie van verwante problemen.

Maar de complexiteitstheorie heeft ook een spectaculaire niet-opgeloste wiskundige vraag in petto. Zijn de rekenproblemen in de klasse $\mathbf{NP}$ nu werkelijk moeilijker dan die in $\mathbf{P}$? Het voelt zo aan, en niemand heeft nog ooit een handelsreiziger probleem omgetoverd in een gewoon zoekprobleem. Maar een onvermogen is geen bewijs, en dus kennen we al sinds het begin van de jaren zeventig het roemruchte open

P = **NP**-*probleem*:

Zijn de complexiteitsklassen $\mathbf{P}$ en $\mathbf{NP}$ verschillend, of gelijk?

Anders gezegd, is de complexiteitshiërarchie wel 'echt'? En nog anders gezegd, kan de propositielogica beslist worden in polynomiale tijd, en dus 'slimmer' dan met waarheidstafels of tableaus? Vele jaren zoeken door logici heeft bijvoorbeeld nooit wezenlijk snellere methoden opgeleverd voor Consistentie. Maar anderzijds is ook nog nooit een afdoend bewijs gevonden dat het echt complexer is

dan evaluatie van formules. Onlangs werd het **P** = **NP**-probleem opgenomen in de lijst van centrale open wiskundige problemen van deze tijd van het Clay Institute. Algemeen wordt verwacht dat het antwoord ontkennend luidt, maar wellicht zijn bestaande combinatorische methoden onvoldoende om dit te bewijzen. Het is verbazend dat dit probleem zich reeds voordoet in een logisch systeem als de propositielogica, dat inmiddels al zo'n tweeduizend jaar is bestudeerd.

Overigens is complexiteitstheorie in de praktijk vaak slechts 'onweer in de verte'. Het schrijven van snelle programma's voor rekentaken is ook een vorm van schone kunst, waarbij getalenteerde programmeurs zich weinig aantrekken van theoretische barrières.

Complexiteit en cognitie

Dit hoofdstuk heeft laten zien dat redeneren en rekenen nauw verbonden zijn langs diverse lijnen, waarbij we speciaal aandacht hebben besteed aan de complexiteit van rekenprocedures en verwante redeneertaken. Dit samenspel komt in de wiskunde al voor vanaf Euclides' "Elementen"waar meetkundige bewijzen vaak samen gingen met constructieprocedures voor objecten. En het is in de moderne tijd evenzeer gemeengoed in de informatica, waar bewijsregels vaak tegelijk programmeerregels zijn om objecten te construeren. Overigens is het resulterende inzicht in complexiteit bepaald geen wondermethode om praktische problemen op te lossen. In feite stuiten we op vele plaatsen op *complexiteitsbarrières*, waar onze methoden vastlopen - zoals de beruchte informatieoverdaad op het Internet, of in de gegevensbanken van grote nationale inlichtingendiensten. Beheersing van die complexiteit, voorzover mogelijk, lijkt te vragen om intelligentie naast brute rekenkracht. Mat dat laatste aspect komen we weer bij ons gebruikelijke slotthema: de cognitie.

Het is verleidelijk om aan te nemen dat de verstrengeling van redeneren en rekenen, en de diverse complexiteitsniveaus van logische taken, ook een belangrijke rol spelen in onze praktische cognitieve vermogens. Heel pregnant ziet men dit in de klassieke AI, waar universele computers zoals Turingmachines worden gebruikt als modellen voor de studie van menselijke cognitieve vermogens. En ook allerlei verdere met dat machinemodel samenhangende logische thema's lijken cognitief relevant, zoals de balans tussen uitdrukkingskracht en complexiteit. Hoe rijker onze taal, hoe moeilijker het uitvoeren van daarmee samenhangende taken: hoe zou de natuur hier omheen kunnen? Niettemin is het machinemodel van menselijke cognitie bepaald niet onomstreden. De neurologische feiten over hersenwerking wijzen niet in de richting van een stapsgewijs werkende rekenautomaat van een gangbaar soort, maar eerder naar een parallel taken uitvoerend netwerk van neuronen. En ook de precieze architectuur van onze redeneer- en rekenvermogens is niet bekend – en introspectie levert daarover slechts beperkte informatie. Omzetten van wiskundig-logische ideeën, hoe elegant en aannemelijk ook, in toetsbare cognitieve hypothesen is bepaald geen simpele kwestie. Iets dergelijks geldt voor complexiteit. Ongetwijfeld is ons cognitief functioneren ook onderhevig aan dit verschijnsel. Sommige taken zijn boven onze macht. Maar de cruciale factoren die hierbij een rol spelen hoeven niet altijd dezelfde zijn voor mensen en machines. Computers voelen wiskundige complexiteit, mensen voelen *moeilijkheid*. De twee begrippen zijn niet noodzakelijk hetzelfde. Uit experimenteel onderzoek in speltheorie is bijvoorbeeld bekend dat moeilijkheid van een taak voor mensen in eerste instantie niet wordt bepaald door wiskundige complexiteit, maar door het verwachte nut, intenties, en zelfs door emotie. Een winnende strategie zien in een spel gaat beslist sneller als u een sterke behoefte voelt om een arrogante tegenstander te verslaan!

7.3 Paradoxen en onbewijsbaarheid

Logische analyse vestigt de aandacht op de taal van de wiskunde, de bewijspatronen die daarin zijn te schrijven, en de structuur van axiomatische theorieën. Deze abstracte structuur is zo geheel formeel dat zelfs machines ermee kunnen omgaan, zoals we in dit hoofdstuk al hebben gezien. Maar formalisering is meer een oefening in abstractie dan een doel op zich. In feite werd het formaliseringsprogramma aan het begin van de twintigste eeuw gedreven door echte brandende vragen. Het had ten doel de wiskunde van veilige grondslagen te voorzien, zodat consistentie en andere plezierige eigenschappen eens en voor goed zouden zijn gegarandeerd. In deze toegevoegde paragraaf geven we een indruk van de belangrijkste kwesties die destijds speelden, en de verrassende ontknoping. Het onderzoek naar formele grondslagen van de wiskunde legde juist fundamentele beperkingen bloot aan wat met wiskunde valt te bereiken!

Gödel's Onvolledigheidstellingen

Veel mensen hebben wel eens gehoord van Gödel's Onvolledigheidsstelling, die, populair gesproken, zoiets zeggen als 'dat men niet alles wiskundig kan bewijzen'. Een bekende uiteenzetting is het boek 'Gödel, Escher, Bach' van Douglas Hofstadter, dat Gödel koppelt aan de kunstmatige intelligentie en biologie, en hem meteen ook maar in een artistieke context plaatst rond het thema 'zelf-referentie'. Ook in de lijst van twintig meest vooraanstaande intellectuelen van de twintigste eeuw die TIME magazine rond de eeuwwisseling opstelde, stond Kurt Gödel opgenomen, naast Einstein en andere groten uit wetenschap en cultuur. Overigens bevatte die lijst van twintig ook Alan Turing en Ludwig Wittgenstein. In dit aparte hoofdstuk proberen we een indruk te geven van de strekking van Gödel's resultaat, en de gedachten erachter. Maar veel van de intellectuele prestatie schuilt juist in formele details die we hier niet behandelen. Zelfs een kleine eeuw later vergen Gödel's resultaten en hun repercussies aan de universiteit nog steeds een wiskunde cursus op zich!

P 18.

KURT GÖDEL

1906 — 1978

We beginnen met een kleine aanloop uit eerdere colleges.

Paradoxen, grondslagenonderzoek, en Hilbert's Programma

In eerdere hoofdstukken zagen we reeds de historische tendens naar steeds grotere precisie in wiskundige bewijzen. Dit resulteerde in steeds scherpere stelsels van axioma's en bewijsregels, bijvoorbeeld in de meetkunde en algebra. Niettemin werden aan het eind van de negentiende eeuw toch tegenspraken gevonden in een belangrijke wiskundige theorie die toen juist was voorgesteld als basis voor de opbouw van het wiskundig universum: te weten, de verzamelingenleer. De Russell Paradox over het niet bestaan van de verzameling van alle verzamelingen die zichzelf niet als element bevatten was zo'n tegenspraak, die aantoonde dat de verzamelingenleer geen veilig gebied was. Zolang een dergelijke verrassing ons nog kan overkomen lopen we het gevaar dat het hele bouwwerk van de wiskunde ooit nog eens 'als een kaartenhuis ineenstort' zoals de logicus Frege, de uitvinder van de moderne predicatenlogica die we voortdurend gebruiken, het rond die tijd formuleerde.

Tegen deze dreigende achtergrond stelde David Hilbert op het grote wiskunde congres in Parijs van 1900 voor om de wiskunde eens en voor goed van dit soort twijfels te zuiveren. *Hilbert's Programma* houdt het volgende in:

> *Formalisering*
>
> Alle wiskundige theorieën geheel expliciet definiëren met een formele taal, axioma's en bewijsregels.

Dit voorwerk werd rond deze tijd begonnen door Giuseppe Peano, en later ook Bertrand Russell tezamen met Alfred Whitehead in hun monumentale werk "Principia Mathematica". Gaandeweg is aldus het vertrouwen ontstaan dat formalisering altijd mogelijk is. Wat moet men zich voorstellen bij een formele theorie? Om althans de sfeer van het grondslagenonderzoek te laten zien, geven we een formalisering van de rekenkunde zoals beschreven door Giuseppe Peano in T.27 op pagina 231.

Maar precieze formalisering is slechts een middel voor een doel! Hilbert's vernuftige idee was nu dat zelfs zeer ingewikkelde wiskundige theorieën T, zoals de verzamelingenleer of de analyse, op dit syntactische taalniveau toch een simpele concrete vorm hebben. Immers, we kijken nu alleen naar de manier van opschrijven, niet naar de inhoud. Bovendien is de bewering dat zo'n theorie T consistent is zelf een eenvoudige typografische eigenschap van die syntaxis. Zij zegt dat onder de rijtjes symbolen die afleidbaar zijn uit de axioma's met de bewijsregels zich nooit een rijtje φ bevind tezamen met zijn negatie $\neg\varphi$. Deze bewering CONS-T kan men dan zelf streng wiskundig onderzoeken, want het onderzoek van de taal en bewijssystemen van wiskundige theorieën is zelf wiskundig uit te voeren. Hilbert sprak hier van 'meta-mathematica', en in deze context kwam een tweede ambitie in het vizier:

> *Consistentiebewijzen*
>
> Van die geaxiomatiseerde theorieën door simpele wiskundige analyse van hun 'grammaticale bewijs-structuur' de consistentie aantonen.

Metamathematica is het bestuderen van wiskunde met wiskunde. Op zich is dit een wonderbaarlijk idee, abstract door zijn concreetheid: de taal en theorie-structuur van de wiskunde zelf vormen een legitiem onderwerp van wiskundige studie!

Natuurlijk ligt dit alles enigszins delicaat. Als we om de consistentie van een theorie T te bewijzen een metamathematische theorie T' nodig hebben die sterker is dan T, dan zitten we in een cirkel - en zal ons vertrouwen in de consistentie van T niet bepaald zijn toegenomen. Maar Hilbert's verwachting was dat een klein stukje elementaire wiskunde voldoende zou zijn voor de syntactische bewijsanalyse van de meest complexe wiskundige theorieën. Te denken valt aan een klein stukje middelbare school rekenkunde, of een klein stukje wiskunde van formele talen. En de consistentie van die laatste kleine 'werk-theorieën' zal toch niemand serieus in twijfel trekken?

Peano Axioma's

Rond 1900 introduceert Guiseppe Peano een axiomatisering van de natuurlijke getallen met binaire operaties optelling en vermenigvuldiging. Hieronder staat een versie in onze kwantor-logische taal voor de natuurlijke getallen. Hiervan maakt ook een één-plaatsig functie-symbool deel uit: de opvolger-functie S.

1. $\forall x \neg(0 = Sx)$
2. $\forall x \neg(x = y) \rightarrow \neg(Sx = Sy)$
3. $\forall x\,(x + 0 = x)$
4. $\forall x \forall y\,(x + Sy = S(x + y))$
5. $\forall x\,(x \cdot 0 = 0)$
6. $\forall x\,(x \cdot Sy = (x \cdot y) + x)$
7. $(\varphi[0/x] \wedge \forall x\,(\varphi \rightarrow \varphi[Sx/x])) \rightarrow \forall x\,\varphi$

Het laatste axioma is het eerder besproken axioma van inductie (zie ook T.21).
Vaak worden naast de functie-symbolon ook bekende relaties gebruikt door ze te definëren in termen van de hierboven gebruikte functies. Bijvoorbeeld:

$$s < t \stackrel{\text{def}}{=} \exists x\,(s + Sx = t)$$

Om met deze axiomatisering te redeneren hebben we ook een bewijsmethode voor algemene kwantor-logische geldigheden nodig. We zouden daartoe het tableau-systeem T.22 kunnen gebruiken. Zo'n systeem past echter minder bij de gangbare stijl van axiomatische deductie. Hier is een voorbeeld van een geldig kwantor-logisch principe in axiomatische stijl:

$$\forall x\,\varphi \rightarrow \varphi[t/x]$$

Het zegt dat we in de formule φ elke willekeurige term voor de vrije variabelen x in φ mogen invullen (substitueren). Met behulp hiervan kunnen we ons geheel formeel bewijs geven voor een wiskundig feit als "Een plus een is twee".

$\forall x \forall y\,(x + Sy = S(x + y))$	*Axioma 4*	$S0 + 0 = S0$	*Subsitutie* $S0/x$
$\forall y\,(S0 + Sy) = S(S0 + y)$	*Substitutie* $S0/x$	$S(S0 + 0) = SS0$	
$S0 + S0 = S(S0 + 0)$	*Substitutie* $0/y$	$S0 + S0 = SS0$	
$\forall x\,(x + 0) = x$	*Axioma 3*		

De laatste twee stappen hebben we nog niet expliciet gerechtvaardigd. Hier spelen weer andere axioma's van de kwantor-logica. De laatste stap volgt uit de transitiviteit van gelijkheid, en de stap ervoor dankzij het axioma van congruentie. Dit zegt dat als als twee termen gelijk zijn, dan blijven ze gelijk nadat ze ingevoerd zijn in één en dezelfde functie.
Hieronder, ter illustratie van het inductie-axioma 7 van hierboven, een algemenisering van de rekenkundige stelling van hierboven: $\forall x\, S0 + x = Sx$: als je 1 optelt bij x dan krijg je de opvolger van x.

$$\begin{array}{l} S0 + 0 = S0 \\ \forall x\,(S0 + Sx = S(S0 + x) \\ \forall x\,(S0 + x = Sx \rightarrow S0 + Sx = SSx) \\ \forall x\, S0 + x = Sx \end{array}$$

Hier hebben we gemakshalve de bureaucratische stappen achterwege gelaten. We hebben afgeleid dat het gestelde voor 0 geldt, en dat als het voor x geldt dan ook voor zijn opvolger Sx. Het inductie-axioma zegt dan dat het vervolgens voor alle x moet gelden.

Achter dit programma schuilt een groot vertrouwen in het probleemoplossend vermogen van wiskundige theorieën. In deze zelfde geest kan men wel zeggen dat Hilbert ook iets sterkers vermoedde dan formalisering alleen, en wel

> *Volledigheid*
>
> Voor het domein van wiskundige objecten zijn overzichtelijke *volledige* theorieën op te stellen, die alle waarheden van dat domein als stellingen produceren.

Het optimisme dat uit dit alles spreekt, wordt samengevat in twee fameuze citaten:

> [Hilbert's credo:] *Wir müssen wissen, wir werden wissen.*
>
> [Hilbert's doel:] *Die Grundlagenfragen eins für allemal aus der Welt zu schaffen.*

Dit programma kende aanvankelijke successen — zelfs de beroemde wiskundige John von Neumann werkte mee om consistentiebewijzen te leveren voor diverse theorieën. Maar in 1931 werd Hilbert's algemene ideaal weerlegd door Gödel's Stellingen, bewezen toen de auteur slechts 26 jaar oud was. De situatie met consistentie en volledigheid bleek veel complexer dan vermoed, en heel vaak 'kunnen we niet weten', zelfs als zouden we dat willen of moeten. Bijvoorbeeld,

> Er bestaan geen volledige axiomatische theorieën voor de rekenkunde, de verzamelingenleer, of andere significante wiskundige theorieën waarvan we de consistentie op Hilbert's manier zouden willen bewijzen.

De intellectuele fall-out van Gödel's ontdekkingen heeft de hele twintigste eeuw voortgeduurd. Met name bleek de onvolledigheid ook op diepe wijze samen te hangen met het al eerder genoemde verschijnsel van *onbeslisbaarheid*, en dus weer een onmogelijkheid die eerdere verwachtingen de bodem insloeg:

> Voor veel significante wiskundige vragen, zoals rekenkundige waarheid of logische geldigheid, bestaan geen mechanische beslissingsmethoden.

Voorbeelden zagen we reeds in de bespreking van Turing machines, en de onbeslisbaarheid van het Halting probleem.

In onze verdere bespreking bouwen we de ideeën achter Gödel's bewijs in stadia op, vanaf de oorspronkelijke filosofische achtergrond tot de uiteindelijke wiskundige vormgeving. Daarna gaan we nog iets nader in op de verdere repercussies.

De Leugenaarsparadox

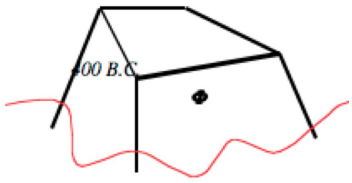
Hoe vinden we significante algemene eigenschappen van formele theorieën en bewijzen? Hiervoor greep Gödel terug op een oude filosofische traditie in de logica. De volgende paradox wordt toegeschreven aan Philites van Cos – de 'Brief aan de Kretenzers' van de apostel Paulus bevat een ietwat verwaterde versie. De leugenaar doet de volgende bewering L:

> Deze zin (d.w.z. L zelf) is onwaar.

In deze schijnbaar onschuldige bewering schuilt een probleem:

> Als L waar is, dan gaat wat hij zegt op, dus was L niet waar. Ergo: L is onwaar. Maar dat zei L nu juist, en dus is L toch waar! Tegenspraak...

In wezen ziet u hier wéér de truc van Cantor's diagonaalargument, maar dan al 2000 jaar eerder geformuleerd. Maar wat betekent deze tegenspraak nu? Is het een kleine curiositeit die we kunnen negeren, of is ons gewone denken misschien 'lek'? De legende zegt dat de arme Philites inderdaad zelf is overleden aan excessief nadenken over deze schier onontwarbare knoop:



Over de Leugenaarsparadox is veel geschreven, en nieuwe oplossingen voor dit staaltje van logisch vernuft worden nog steeds voorgesteld. In elk geval spelen in bovenstaande paradoxale redenering de volgende drie ingrediënten een rol:

(a) vormen van logisch geldig redeneren

(b) het begrip 'waarheid'

(c) 'zelf-referentie': de mogelijkheid dat beweringen op zichzelf slaan.

Men kan de redenering trachten te blokkeren op elk van deze punten, en alle drie zijn in de vele eeuwen sinds de Oudheid al eens door filosofen geprobeerd — en er verschijnen nog steeds nieuwe gezichtspunten. Gödel's vernieuwing was echter anders. Hij liet de Leugenaarsparadox voor wat ze was op het niveau van gewone taal en redeneren, maar merkte op dat de bovenstaande paradoxale redenering met haar drie ingrediënten ook optreedt binnen een wiskundige context met precies gedefinieerde talen en bewijssystemen. Maar dan raakt de paradox wel 'getemd'!

Van taal naar getallen: coderen

Om te beginnen treedt zelfreferentie in de wiskunde op zodra we beweringen B coderen als getallen $\lceil B \rceil$. De kracht van coderen was destijds natuurlijk al bekend vanwege allerlei geheimschriften. Zoals reeds eerder is opgemerkt, kan codering op vele manieren worden bewerkstelligd. Gödel zelf werkte bijvoorbeeld in eerste instantie als volgt. Hij kende achtereenvolgende priemgetallen $2, 3, 5, 7, ..$ toe aan basissymbolen van de taal. Een formule als $\neg x = 3$ correspondeert dan met een rijtje getallen

code($\neg$), code (x), code(=), code (3)

en een dergelijk rijtje codeerde hij dan weer uniek als één getal met de macht

$$2^{\mathrm{code}(\neg)} \cdot 3^{\mathrm{code}(x)} \cdot 5^{\mathrm{code}(=)} \cdot 7^{\mathrm{code}(3)}$$

Maar zodra we een dergelijke functie hebben van beweringen naar getallen, ontstaat de mogelijkheid van zelfreferentie. Bijvoorbeeld, een rekenkundige bewering $\forall x\, \varphi(x)$ in onze gewone predicaatlogische taal zegt dat alle getallen de eigenschap φ hebben. Maar dat is dan inclusief het getal dat het codenummer is van $\forall x\, \varphi(x)$ zelf! In die zin spreekt een universele rekenkundige formule dus over zichzelf. En er zijn nog vele andere meer subtiele manieren waarop een rekenkundige bewering iets kan zeggen over zijn eigen codenummer. Dit klonk destijds geheimzinnig en enigszins 'kabbalistisch', maar het verschijnsel is tegenwoordig natuurlijk welbekend - omdat codering precies de manier is waarop computers tekst verwerken. Beweringen worden omgezet in getallen, daarmee wordt gerekend, en de resultaten worden terugvertaald als voor ons leesbare beweringen.

Ondefinieerbaarheid van waarheid

Alleen al deze eerste observatie leidt tot een interessant resultaat, dat soms apart wordt toegeschreven aan Alfred Tarski. Laten we de drie ingrediënten in de redenering van de Leugenaarsparadox nu eens bekijken in een rekenkundige setting. Met de logica is niets mis (a), zelfreferentie (c) is kennelijk ook mogelijk, dus moet er iets haperen in punt (b) hierboven. Onze conclusie luidt dan:

Stelling Het rekenkundig waarheidsbegrip is zelf niet rekenkundig definieerbaar.
Iets preciezer gezegd:

> Het begrip "φ is waar in $\mathbb{N}$", voor formules φ uit Peano's rekenkundige taal, is op te vatten als rekenkundige eigenschap van natuurlijke getallen, te weten, de codenummers $\lceil\varphi\rceil$. Met name geldt het precies voor de codes van de ware formules φ. Tarski's Stelling zegt nu dat Peano's predicaatlogische taal te arm is om deze eigenschap van 'waarheid' zelf met één van zijn eigen formules te definiëren.

Tarski trok overigens eenzelfde les voor onze gewone natuurlijke taal. Ook daar is het waarheidsbegrip niet precies te definiëren! Om dan toch systematisch te kunnen werken met de begrippen waarheid en onwaarheid, zoals we nu eenmaal plegen te doen, introduceerde hij zijn vermaarde onderscheid tussen *object-taal* versus *meta-taal*. De object-taal is het medium waarmee we een bepaald gebied van objecten beschrijven. De meta-taal is het medium waarmee we over de object-taal praten. Kennelijk zijn er begrippen, zoals waarheid van object-formules, die essentieel op het tweede niveau van de meta-taal thuishoren. Op deze manier beschouwd berust de Leugenaar Paradox dus op een niveau-verwarring: de cruciale bewering L wordt in het argument door elkaar heen als object-taal en meta-taal gebruikt. Dit 'object/meta' onderscheid is buitengewoon populair geworden, en het voorvoegsel 'meta' beleeft nog steeds een grote bloei. Toch lost dit het probleem van de Leugenaarsparadox in wezen slechts op door zelf-referentie te *verbieden*, een historisch welbekende, maar intellectueel niet bijzonder aansprekende manier om problemen van tafel te krijgen. Het zal u dus niet verbazen dat dit niet het laatste woord is geweest in deze discussie.

Principiële onbewijsbaarheid: een mini-versie van Gödel's Stellingen

Maar Gödel's eigen analyse ging veel verder dan deze eerste stap, en betrok ook het begrip *bewijsbaarheid* in de leugenaarsredenering. Dit omzeilt allerlei mogelijke problemen met het begrip waarheid, omdat aan de concrete wiskundige aard van de notie 'bewijs' niet kan worden getwijfeld. Wat zegt de Leugenaarsparadox ons dan? We formuleren, ruwweg, wat Gödel bewees:

> *Eerste Onvolledigheidsstelling*
>
> Voor elke consistente geaxiomatiseerde wiskundige theorie T die de rekenkunde bevat bestaat er een zin φ_T in de taal van T zodat
>
> (a) φ_T is niet in T bewijsbaar
>
> (b) $\neg\varphi_T$ is evenmin in T bewijsbaar
>
> (c) φ_T is waar.

Dit zegt dat formele wiskundige theorieën onvolledig zijn zodra hun uitdrukkingskracht een zeker rekenkundig minimum overschrijdt. Vervolgens komt een tweede observatie, die de doodsteek toebrengt aan Hilbert's Programma:

P 19.

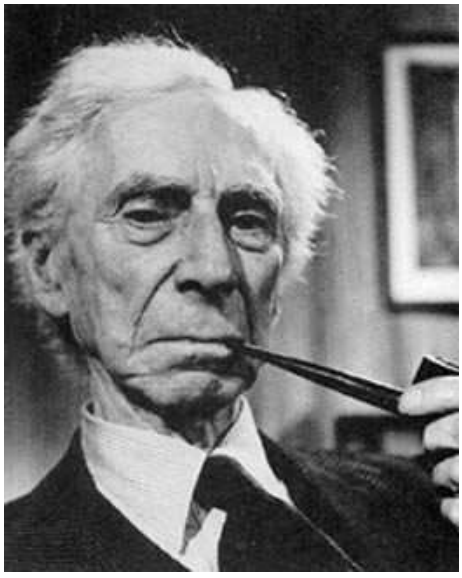
GUISEPPE PEANO

1858 — 1932

ALFRED TARSKI

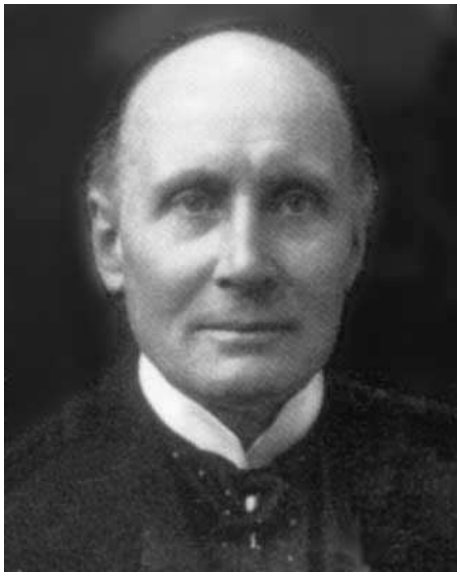
1902 — 1983

P 20.



BERTRAND RUSSELL

1878 — 1970



ALFRED WHITEHEAD

1861 — 1947

Tweede Onvolledigheidsstelling

Geen enkele consistente wiskundige theorie die de rekenkunde bevat kan zijn eigen consistentie bewijzen.

In het bijzonder zal dus Hilbert's 'elementaire rekenkunde', die de motor moest zijn van de metamathematica, niet de consistentie kunnen bewijzen van meer ambitieuze wiskundige theorieën.

We bespreken globaal de belangrijkste ideeën achter deze twee beroemde resultaten, in een soort eerste bewijsronde. Daarop volgend werken we een aantal essentiële details iets nader uit.

Bewijsschets van de Eerste Onvolledigheidsstelling Gezien de eenvoud van syntactische bewerkingen in expliciet geaxiomatiseerde formele theorieën zoals de Peano rekenkunde bestaat er een eenvoudig rekenkundig predikaat

$\text{BEW}_T(n)$ getal n codeert een bewijs in theorie T.

Met gebruik van dit rekenkundige bewijspredikaat geeft een 'diagonaal-constructie', waarover later meer, dan de volgende rekenkundige 'leugenaarzin':

G: deze zin (G zelf) is niet T-bewijsbaar

Preciezer gezegd,

T bewijst $G \Leftrightarrow \neg\text{BEW}_T(\ulcorner G \urcorner)$, met $\ulcorner G \urcorner$ de getalscode van formule G. (*)

Nu bootsen we de Leugenaar redenering na. Dat blijkt te kunnen zonder op enige tegenspraak te stuiten, maar we moeten wel de moed hebben de consequenties te 'nemen'!
Stel dat G bewijsbaar is in T. Dan is het bestaan van dat bewijs zelf een simpel feit dat in T bewijsbaar is: ofwel, theorie T bewijst $\text{BEW}_T(\ulcorner\ulcorner G \urcorner\urcorner)$. Maar vanwege de equivalentie (*) met een scheutje propositielogica bewijst T dan ook $\neg G$. In dat geval hebben we een inconsistentie onder de stellingen. Maar we namen nu juist aan dat T consistent is, en dus moeten we concluderen dat

(a) *G is niet bewijsbaar in T.*

Maar dat beweerde G nu juist al (weer volgens (*)), en deze formule heeft dus gelijk:

(c) G is waar!

Dat de negatie $\neg G$ evenmin in T bewijsbaar is (b) vergt een iets meer technische redenering, die we hier achterwege laten. Met een excursie naar het waarheidsbegrip kan het echter heel snel. Als u gelooft dat theorie T correct is, en dus alleen ware stellingen produceert, dan is deze derde bewering onmiddellijk, aangezien G waar was. Q.E.D.

Bewijsschets van de Tweede Onvolledigheidsstelling Nadere inspectie leert dat het bewijs van de Eerste Stelling, hoe subtiel ook, toch zo eenvoudig is qua stappen dat het zelf geheel valt te formaliseren binnen de rekenkunde. In onze eerdere notatie kunnen we dan schrijven:

T bewijst $\text{CONS}_T \rightarrow \neg\text{BEW}_T(\ulcorner G \urcorner)$

Maar ook de eerdere equivalentie (*) is nog steeds tot onze beschikking! Als we die toepassen dan volgt dat, als T CONS_T bewijst, dan bewijst T ook de leugenaarsformule G, wat nu juist niet zo was! We moeten dus concluderen dat CONS_T niet in T bewijsbaar is, als de theorie T tenminste consistent is. Q.E.D.

Waarom staat er eigenlijk telkens die laatste conditie 'als T consistent is'? De reden is heel eenvoudig. Als een theorie inconsistent is, dan kan hij - zoals we reeds in een eerder college zagen - om logische redenen elke bewering bewijzen ('uit een contradictie volgt alles'). In het bijzonder bewijst een inconsistente theorie dus ook de (onware!) rekenkundige bewering van zijn eigen consistentie...

Algemene wiskundige strekking

De brede strekking van deze resultaten werd in de jaren na 1931 snel duidelijk. Gödel's stellingen gelden niet alleen voor de rekenkunde. Ze treffen alle centrale wiskundige theorieën, zoals de verzamelingenleer, omdat die altijd genoeg rekenkunde bevatten om de genoemde coderings-argumenten te kunnen uitvoeren.

Verder helpen allerlei vaak gesuggereerde uitwegen niet. Je zou kunnen proberen de leugenaarzin G toe te voegen aan de theorie T om de onvolledigheid op te heffen. Maar dan ontstaat gewoon een nieuwe rekenkundige theorie $T + G$, met weer zijn eigen leugenaarzin, die dus ook weer onvolledig is, enzovoorts. Ook oneindig doorgaan met zulk toevoegingen helpt niet, omdat in de limiet dan een theorie ontstaat die hetzij nog steeds onvolledig is, hetzij niet langer 'effectief geaxiomatiseerd'. In het laatste geval zijn de axioma's geen simpele lijst meer, zoals in het voorgaande steeds werd verondersteld - en de notie geaxiomatiseerde theorie en rekenkundig definieerbaar bewijspredikaat verliest daarmee zijn zin. We kunnen dus de strekking van Gödel's resultaat samenvatten als:

> Exact gedefinieerde wiskundige theorieën beschrijven nooit de volledige waarheid omtrent hun domein, zodra dit laatste de natuurlijke getallen omvat.

In wat volgt bespreken we twee belangrijke aspecten van het bewijs nog iets nader, om u een indruk te geven van de volgende laag van ideeën.

Arithmetisering van de syntaxis en zelf-referentie

De eerste vraag die we moeten oplossen luidt als volgt:

> Hoe kunnen we de rekenkunde precies laten spreken over de rekenkunde zelf?

Zoals we reeds opmerkten, was Gödel's cruciale inzicht hier het volgende. Onder geschikte codering wordt de syntaxis van een wiskundige theorie een vorm van eenvoudige rekenkunde op codenummers. Men noemt dit *arithmetisering van de syntaxis*: de rekenkunde formuleert alle feiten over de rekenkunde. Gödel gaf zelfs twee specifieke codes voor dit doel. Eén werkte als gezegd met machten van priemgetallen, en gebruikte de unieke priemfactor-ontbinding van natuurlijke getallen. De ander werkte met rekenen modulo n, en gebruikte de zogenaamde 'Chinese Reststelling'. De resulterende arithmetisering stelt ons in staat belangrijke aspecten van het bovenstaande bewijs wiskundig precies te maken.

Beschouw voor het gemak alleen rekenkundige formules $\varphi(x)$ waar één vrije variabele x los in voorkomt (denk aan het al vaak aangehaalde voorbeeld van "x is priem"). Met name bestaat er dan een eenvoudig definieerbare rekenkundige *substitutie-functie* 'sub' met

sub(n, m) is het codenummer van de formule $\varphi_n(m)$ die het resultaat is van invullen van het getal m voor de vrije variabele x in de formule φ_n met codenummer n.

Nog iets formeler:

$\ulcorner\varphi_n\urcorner) = n$ en $\ulcorner\varphi_n(m)\urcorner = \text{sub}(n, m)$.

En dit levert ons nu een middel voor een exacte *diagonaliserings-methode*. Bekijk om te beginnen eens de uitdrukking

sub(n, n).

Volgens de bovenstaande afspraak geeft deze de code aan van het resultaat van invullen in de formule met codenummer n van *zijn eigen code*! Nu kunnen we zelf-referentie bewerkstelligen voor een geheel willekeurige rekenkundige bewering $A(x)$. Daartoe vormen we de uitdrukking

$A(\text{sub}(x, x))$.

Dit is zelf weer een formule met één vrije variabele x, en heeft dus een codenummer, zeg k. Dan geldt in het bijzonder, vanwege de bovenstaande definitie van de substitutie-functie:

$\text{sub}(k, k) = \ulcorner A(\text{sub}(k, k))\urcorner$.

Maar dit levert meteen de volgende equivalentie:

$A(\text{sub}(k, k)) \leftrightarrow A(\ulcorner A(\text{sub}(k, k))\urcorner)$.

Deze notatie is ingewikkeld, maar veel lezen heeft ook iets esthetisch aantrekkelijks. We zien hier hoe dan ook een heel algemeen feit:

$A(\text{sub}(k, k))$ zegt van zichzelf: "Ik heb eigenschap A"!

Wat we dus hebben aangetoond is dat elke rekenkundige bewering A een 'dekpunt' heeft: d.w.z. een bewering die precies van zichzelf zegt dat zijn codenummer de eigenschap A heeft.

Dekpuntslemma Voor elke rekenkundige bewering A met één vrije variabele is er een rekenkundige bewering B zodat $B \Leftrightarrow A((\ulcorner B\urcorner)$.

Dit resultaat geldt wat voor eigenschap A we ook nemen: 'groter dan een miljoen', 'priem', 'code van een stelling', enzovoorts. Ondanks deze kracht zijn de hier gegeven constructie en redenering zo eenvoudig dat het Dekpuntslemma met enige zorg zelf binnen de elementaire rekenkunde is te bewijzen.

Nu is Gödel's leugenaarzin G voor het eerdere bewijs heel eenvoudig te vinden. Pas het Dekpuntslemma simpelweg toe op de volgende rekenkundige formule:

$A(x)$: "de door x gecodeerde bewering heeft geen bewijs in T" ($\neg\text{BEW}_T(x)$).

De centrale equivalentie (*) in het eerdere bewijs komt dan vanzelf te voorschijn. Het Dekpuntslemma creëert op een wiskundig onberispelijke manier zelf-referentie binnen de rekenkunde. Deze methode heeft inmiddels vele verdere toepassingen gevonden. Het is bijvoorbeeld ook bruikbaar als een manier om 'zelf-reproducerende' programma's te maken, en andere curieuze objecten in de informatica.

Intermezzo: nieuwe paradoxen

Misschien wilt u weer even wat blauwe lucht zien in plaats van een dichte jungle van formules. Terugvertaald naar een meer informele context leveren abstracte resultaten uit de metamathematica soms weer nieuwe filosofische puzzels op, die in de geschiedenis nog niet waren ontdekt. Een mooi voorbeeld staat bekend als 'Löb's Paradox' (1955):

> Elke bewering φ is waar!

Laat daartoe φ eens een volmaakt willekeurige bewering zijn, bijvoorbeeld dat (in een iets andere loop van de vaderlandse geschiedenis na 1810) Lodewijk Napoleon VII de huidige koning van Nederland is. We maken nu een 'zelf-referente' bewering N die van zichzelf het volgende zegt[5]

> Als ik (d.w.z. N) waar ben, dan is φ waar: $\quad N \leftrightarrow (N \rightarrow \varphi))$ (*)

Als we eenmaal zo'n hulpbewering N hebben gemaakt, dan ontspint zich de volgende welhaast 'magische' redenering:

(i)	Stel dat N	Aanname
(ii)	Dan ook $N \rightarrow \varphi$	(i) en (*)
(iii)	Dan ook φ	(i) en (ii)
(iv)	Dus $N \rightarrow \varphi$	(iii) volgde uit veronderstelling (i)
(v)	En dus ook N	(iv) en (*)
(vi)	Maar dan: φ	(iv) en (v)

Propositielogisch is de clou hier de geldige gevolgtrekking $B \leftrightarrow (B \rightarrow A) \models B \wedge A$. Deze laatste is ook rechtstreeks na te gaan met waarheidstafels of semantische tableaus. Overigens was Martin Löb de opvolger van Evert Beth, de ontdekker van de semantische tableaus uit hoofdstuk 6, in Amsterdam. Dus onze lokale 'petite histoire' loopt parallel met de grote geschiedenis.

Representatie en berekenbaarheid

Een tweede technische aspect van het Gödel's bewijs heeft juist te maken met wat wél bewijsbaar is in de rekenkunde. Immers, in de redenering die aantoonde dat de Leugenaarzin niet bewijsbaar was, speelde een rol dat bepaalde feiten uit de gearithmetiseerde syntaxis bewijsbaar waren. De equivalentie (*) was daarvan een essentieel voorbeeld. En in feite heeft de Peano Rekenkunde ook wel degelijk veel in haar mars qua bewijskracht. Heel wat bekende rekenkundige stellingen zijn erin afleidbaar. Dat dit afleiden rond 1900 zo goed lukte leek in feite zelfs evidentie voor Hilbert's Programma. Hiermee is een algemene 'positieve' vraag aan de orde:

> Wat voor ware beweringen zijn eigenlijk binnen de rekenkunde weer te geven, en wel degelijk formeel te bewijzen?

Een tweede baanbrekend inzicht van Gödel, naast zijn codering en het rekenkundig maken van de syntaxis, was de opmerking dat hier een verband ligt met onze eerdere notie van effectieve mechanische berekenbaarheid:

[5] Technisch kan dat ook weer binnen de rekenkunde met het Dekpuntslemma: maar we krijgen dan weer een versie in termen van bewijsbaarheid i.p.v. waarheid.

Effectief mechanisch berekenbare feiten zijn rekenkundig te formuleren, en dan in de Peano Rekenkunde bewijsbaar.

Bijvoorbeeld alle concrete rekenfeiten zijn bewijsbaar, zoals $7 + 5 = 12$, en meer algemeen de standaard rekenregels van de middelbare school. Na codering geldt hetzelfde ook voor alle basisfeiten over syntaxis, zoals het gedrag van de eerdere substitutie-functie, en weer een ander voorbeeld zijn de basisfeiten over het rekengedrag van Turingmachines.

Deze observaties berusten op enkele meer algemene inzichten, uitgewerkt in Gödel's bewijs, die we hier alleen formuleren - maar niet nader toelichten:

- Voor elke mechanisch berekenbare functie f bestaat een rekenkundig predikaat $\mathrm{VALUE}{-}f$ zodat de volgende formule bewijsbaar is voor alle getallen k, n met $f(k) = n$:

$$\forall y \ \mathrm{VALUE}{-}f(k, y) \leftrightarrow y = n.$$

- Voor elke mechanisch berekenbare eigenschap P van natuurlijke getallen bestaat er een rekenkundig predikaat $\mathrm{HOLDS}{-}P$ zodat voor alle getallen k geldt:

  als $P(k)$ waar is, dan is $\mathrm{HOLDS}{-}P(k)$ bewijsbaar, anders is $\neg\,\mathrm{HOLDS}{-}P(k)$ bewijsbaar.

Gödel bewees zelfs dat de effectief berekenbare functies precies diegene zijn waarvan het gehele gedrag op deze manier binnen de formele rekenkunde valt te bewijzen. Dit is een alternatieve karakterisering van mechanische berekenbaarheid, nu niet in termen van Turing machines, maar via bewijsbaarheid van gedrag in een formeel systeem. Inmiddels zijn veel van deze inzichten ook praktisch verwezenlijkt in de moderne informatica, bijvoorbeeld in logische stellingbewijzers die rekenen door te bewijzen.

Wiskundig-logische gevolgen

De details van Gödel's bewijzen vergen, zoals gezegd, een hele cursus op zich. Het begrijpen van de bredere spin-off duurde nog veel langer, en wel vele decennia. Als u een modern standaardwerk raadpleegt als het 'Handbook of Mathematical Logic' (J. Barwise ed., Elsevier, Amsterdam, 1977, en volgende drukken), dan vindt u hele onderzoeksgebieden die zijn ontstaan vanuit diverse draden in het bewijs van de onvolledigheidsstellingen. Voorbeelden zijn de *bewijstheorie* die zich bezig houdt met de formele structuur van bewijzen, de *modeltheorie* die alle wiskundige structuren bestudeert die voldoen aan een gegeven formele axioma's (bijv. alle modellen van de Peano rekenkunde), en de *recursietheorie*: de abstracte theorie van effectieve berekenbaarheid in het algemeen. Verdere spin-off thema's zijn de analyse van concrete gevallen van onvolledigheid in de wiskunde (zie de Paris-Harrington Stelling in het genoemde Handboek), en de wiskundige beschrijving van alle eigenschappen van het bewijsbaarheidspredikaat BEW_T in de formele rekenkunde, die pas midden jaren 1970 volledig is afgerond.

Deze ontwikkeling illustreert een algemeen verschijnsel in de wiskunde. Negatieve resultaten die de onmogelijkheid van iets aantonen zijn zelden het einde van een ontwikkeling, maar eerder een begin! Om zijn resultaten te bewijzen moest Gödel vele positieve begrippen voor de eerste keer precies uitleggen, zoals codering, zelf-referentie, en bewijsbaarheid, en dat was het begin van vele nieuwe ontwikkelingen. Iets dergelijks zagen we al bij de 'negatieve' oplossing van de oplosbaarheid van vijfdegraads vergelijkingen, die leidde tot het ontstaan van de groepentheorie. Maar hoe zit het dan met Frege's Kaartenhuis? Moeten we maar steeds in angst leven dat de wiskunde inconsistent is?

Logici bestuderen ondanks alles nog steeds consistentie van wiskundige theorieën. Maar tegenwoordig gaat het daarbij niet meer om absolute fundering in Hilbert's zin, maar eerder om verbanden in bewijstheoretische sterkte van verschillende systemen, en manieren om nieuwe axioma's te bedenken.

Onbeslisbaarheid en onberekenbaarheid

Metamathematica leidde ook tot informatica! We zagen dit al bij het verband tussen mechanisch berekenbare functies en gedrag dat bewijsbaar is in de rekenkunde. Maar ook Gödel's Stellingen zelf hebben rechtstreekse consequenties voor onbeslisbaarheid, zelfs al wordt dit begrip niet direct genoemd in hun formulering. Zo volgt uit het bovenstaande dat er geen mechanische methode is om rekenkundige waarheid te testen - er is dus geen wondermachine om alle rekenkundige vragen op te lossen:

Stelling Rekenkundige waarheid is onbeslisbaar.

U kunt dit als volgt begrijpen. Stel dat rekenkundige waarheid wél beslisbaar was. Dan zou er een mechanische berekenbaar predikaat WAAR(n) bestaan zodat

> φ is waar in de natuurlijke getallen dan en slechts dan als WAAR$(\lceil\varphi\rceil)$ geldt, voor elke rekenkundige formule φ.

Nu hebben we al gezien dat mechanisch berekenbare predikaten zelf binnen de rekenkunde door rekenkundige formules representeerbaar zijn. Maar dan zouden we alsnog een rekenkundige definitie voor rekenkundige waarheid hebben, hetgeen volgens Tarski's Stelling onmogelijk is.

Deze schets hier onderdrukt details van het exacte bewijs, maar geeft toch een eerste indruk. Door nadere analyse van het bewijs voor de onbeslisbaarheid van de rekenkunde kan men ook een volgend resultaat aantonen dat reeds in vorige colleges over logisch bewijzen en rekenen werd genoemd als eigenschap van de predicatenlogica in het algemeen:

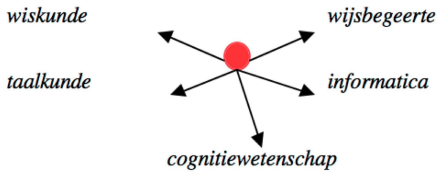
Stelling (Church-Turing) Logisch geldig gevolg is onbeslisbaar.

Ook dit negatieve resultaat heeft weer tot positieve spin-off geleid. Zo is grote aandacht ontstaan voor het ontwerp *deelsystemen* van de predicatenlogica die nog wel beslisbaar zijn. De propositielogica en ook de modale logica uit Hoofdstuk 6 zijn bekende voorbeelden. In feite worden nog steeds krachtige logische deelsystemen gevonden die beslisbaar zijn, zij het vaak wel met veel hogere rekencomplexiteit dan **NP** of **Pspace**.

We besluiten met een interessant feit over de rekenkunde zelf. De volledige theorie van $\mathbb{N}$ is, zoals Gödel aantoont, niet axiomatiseerbaar en ook niet beslisbaar. Nu betreft dit de natuurlijke getallen met nul, opvolger, optelling, en vermenigvuldiging. Wat gebeurt als we kijken naar het deelsysteem zonder vermenigvuldiging? Deze 'additieve rekenkunde' volstaat voor belangrijke deeltaken als oplossen van lineaire vergelijkingen. Reeds rond 1930 werd aangetoond dat de additieve rekenkunde wel volledig axiomatiseerbaar is, en zelfs beslisbaar! Waarom lukt hier wel wat voor de gehele $\mathbb{N}$ misloopt? Eén reden betreft codering. De codes die in Gödel's bewijs formules en bewijzen correct in getallen omzetten gebruiken naast optelling ook vermenigvuldiging. En kennelijk is dat essentiëel.

Discussie: filosofie, AI, en cognitie

De onvolledigheidsstellingen zijn zo intrigerend omdat ze op het grensvlak liggen van een aantal disciplines:



In onze uiteenzetting speelden reeds de wiskunde, informatica, wijsbegeerte, en taalkunde. Maar ook nu nog spelen Gödel's resultaten een richtinggevende rol in de kunstmatige intelligentie en cognitiewetenschap. Ze zeggen dat er onvermijdelijke begrenzingen zijn aan wat is te bewijzen binnen één enkel gegeven formeel systeem. Aangenomen dat wij zelf in staat zijn dergelijke beperkingen te signaleren en te overstijgen, kan er bijvoorbeeld niet één vast computerprogramma zijn dat onze redeneervermogens eens en voor goed vastlegt. Aan de andere kant laten Gödel's resultaten wel degelijk de mogelijkheid open dat we iedere eenmaal aangetoonde begrenzing kunnen overstijgen door uitbreiding van onze huidige theorie... Hiermee verschuift de aandacht, net als in eerdere hoofdstukken, naar *cognitieve dynamiek*: manieren waarop we onze kennis aanpassen, en soms zelfs hele begripskaders veranderen.

Bij een dergelijk gezichtspunt lijkt de centrale interesse verschoven. De oorspronkelijke dramatiek van de 'grondslagencrisis' rond 1900 bestaat niet meer. De onvolledigheidsstellingen maken duidelijk dat garanties voor consistentie niet bestaan, evenmin als gegarandeerde 'quick fixes' voor inconsistente theorieën. Maar er is ook geen kaartenhuis ingestort... In feite kan men ook heel anders denken over de kracht van de wiskunde. Voorgoed uitbannen van tegenspraken is niet mogelijk, maar het is wellicht ook niet nodig. Eén van de meest opmerkelijke eigenschappen van menselijke intelligentie is veeleer ons vermogen om bij gebleken tegenspraken in te grijpen, en de bestaande theorieën op interessante wijze te *herzien*. Cantor's verzamelingenleer is een goed voorbeeld. Deze theorie is helemaal niet ingestort na de ontdekking van de Russell-paradox. Ze is juist meteen herzien, met Russell's argument als 'test' voor zwakke plekken, en daarna op een meer verfijnde manier gereconstrueerd. En de wetenschapsgeschiedenis kent veel meer van zulke gevallen.

Het interessante verschijnsel is hier dan vanuit logisch gezichtspunt die dynamiek zelf van nieuwe informatie! Hoe veranderen wij onze theorieën, en hoe repareren wij eventuele inconsistenties als we iets leren dat in strijd is met wat we tot nu toe dachten? Moderne logische systemen van informatie-update en geloofsherziening proberen juist dergelijke mechanismen te beschrijven. In hoofdstuk 3 zagen we hier al enkele voorbeelden van.

Het zal duidelijk zijn dat met deze wending ook algemene cognitieve kwesties aan de orde zijn. Zijn mensen op consistentie gerichte, kalm kennis cumulerende bewijsmachines, of eerder springerige hypothesen-vormers die telkens via 'trial and error' hun informatie en verwachtingen aanpassen? Het laatste ligt meer in de lijn van wat we eerder gezegd hebben over feitelijk redeneren aan het eind van voorgaande hoofdstukken. In dat licht berust onze grootste kracht niet op eeuwige garanties voor correctheid, maar op ons voortdurende aanpassingsvermogen.