Reprinted from INFORMATION AND CONTROL, Volume 8, No. 2, April 1965

INFORMATION AND CONTROL **8,** 190–194 (1965)

On Finite Monoids Having Only Trivial Subgroups

M. P. SCHÜTZENBERGER

An alternative definition is given for a family of subsets of a free monoid that has been considered by Trahtenbrot and by McNaughton.

I. INTRODUCTION

Let X^* be the free monoid generated by a fixed set X and let $\mathbf{Q}$ be the least family of subsets of X^* that satisfies the following conditions (K1) and (K2):

(K1). $X^* \in \mathbf{Q}$; $\{e\} \in \mathbf{Q}$ (e is the neutral element of X^*); $X' \in \mathbf{Q}$ for any $X' \subset X$.

(K2). If A_1 and A_2 belong to $\mathbf{Q}$, then $A_1 \cup A_2$,

$$A_1 \backslash A_2 \ (= \{f \in A_1 : f \notin A_2\})$$

and $A_1 \cdot A_2$ $(= \{ff' \in X^* : f \in A_1 ; f' \in A_2\})$ belong to $\mathbf{Q}$.

With different notations, $\mathbf{Q}$ has been studied in Trahtenbrot (1958) and, within a wider context, in McNaughton (1960). According to Eggan (1963), $\mathbf{Q}$ contains, for suitable X, sets of arbitrarily large star-height (cf. Section IV below).

For each natural number n, let $\Gamma(n)$ denote the family of all epimorphisms γ of X^* such that $\mathbf{Card}\ \gamma X^* \leqq n$ and that γX^* has only trivial subgroups (i.e., $\gamma f^n = \gamma f^{n+1}$ for all $f \in X^*$, cf. Miller and Clifford (1956)).

MAIN PROPERTY. $\mathbf{Q}$ *is identical with the union* $\mathbf{Q}'$ *over all* n *of the families*

$$\mathbf{Q}'(n) = \{A \subset X^* : \gamma^{-1}\gamma A = A ; \gamma \in \Gamma(n)\}$$
$$(= \{\gamma^{-1}M' : M' \subset \gamma X^*; \gamma \in \Gamma(n)\}).$$

As an application, if $A, A' \subset X^*$ are such that for at least one triple $f, f', f'' \in X^*$, both $\{n \in \mathbf{N} : f'f^nf'' \in A\}$ and $\{n \in \mathbf{N} : f'f^nf'' \in A'\}$ are infinite sets of integers, we can conclude that no $B \in \mathbf{Q}$ satisfies $A \subset B$ and $A' \subset X^*\backslash B$.

II. VERIFICATION OF $\mathbf{Q} \subset \mathbf{Q}'$

The next two remarks are reproduced from Petrone and Schützenberger (1963) for the sake of completeness.

REMARK 1. $\mathbf{Q}'$ *satisfies* (K1).

Verification. Let the monoid $M = \{e', x', 0\}$ and the map $\gamma : X^* \to M$ be defined as follows: $\gamma e = e' = e'^2$; for each $x \in X'$, $\gamma x = x' = e'x' = x'e'$; for each $f \in X^* \backslash (\{e\} \cup X')$, $\gamma f = 0 = e'0 = 0e' = x'^2 = x'0 = 0x' = 0^2$.

It is clear that $\gamma \in \Gamma(3)$ and, since $X^* = \gamma^{-1}M$; $\{e\} = \gamma^{-1}e'$; $X' = \gamma^{-1}x'$, the remark is verified.

REMARK 2. $\mathbf{Q}'$ *satisfies* (K2).

Verification. For $j = 1, 2$ let $\gamma_j : X^* \to M_j$ and $M_j' \subset M_j$ satisfy $\gamma_j \in \Gamma(n_j)$ and $A_j = \gamma_j^{-1}M_j'$. We consider the family R of all sets of pairs $(m_1, m_2) \in M_1 \times M_2$ and for $m_1 \in M_1$, $m_2 \in M_2$, $r = \{(m_{1,i}, m_{2,i}) : i \in I_r\}$, we let $m_1r = \{(m_1m_{1,i}, m_{2,i}) : i \in I_r\}$ and $rm_2 = \{(m_{1,i}, m_{2,i}m_2) : i \in I_r\}$. Finally, letting $\bar{M}$ denote the direct product of sets $M_1 \times R \times M_2$, we define an associative product on $\bar{M}$ and an epimorphism γ of X^* onto a subset M of $\bar{M}$ by setting for all (m_1, r, m_2), $(m_1', r', m_2') \in \bar{M}$ and $f \in X^*$:

$$(n_1, r, m_2)(m_1', r', m_2') = (m_1m_1', m_1r' \cup rm_2', m_2m_2');$$

$$\gamma f = (\gamma_1 f, \{(\gamma_1 f', \gamma_2 f'') : f', f'' \in X^*; f'f'' = f\}, \gamma_2 f).$$

It is clear that $A_1 \cup A_2$, $A_1 \backslash A_2$ and $A_1 \cdot A_2$ are images by γ^{-1} of suitable subsets of M. Since $\bar{M}$ is finite, the remark will follow from the fact that any subgroup $G = \{(m_{1,i}, r_i, m_{2,i}) : i \in I_G\}$ of $\bar{M}$ is isomorphic to a direct product $G_1 \times G_2$ where G_j is a suitable subgroup of M_j $(j = 1, 2)$.

Indeed, by construction $\{m_{j,i} : i \in I_G\}$ is a homomorphic image of G, hence a subgroup G_j of M_j. Let e_j denote the neutral element of G_j $(j = 1, 2)$ and let N be the intersection of G with the subset $\{(e_1, r, e_2) : r \in R\}$ of $\bar{M}$. Since G is finite N is a normal subgroup of G and G/N is isomorphic to a subgroup of $G_1 \times G_2$. Therefore it suffices to show that N reduces to the neutral element $e' = (e_1, r, e_2)$ of G. To see this, let $g = (e_1, s, e_2)$ and $h = (e_1, t, e_2)$ be elements of N inverse of each other. The relations $e' = e'^2$, $e' = gh$, and $g = e'ge'$ give, respectively, $r = e_1r \cup re_2$, $r = e_1t \cup se_2$, and $s = e_1r \cup e_1se_2 \cup re_2$. From the second and the first of these equations we get $e_1t \cup e_1se_2 = e_1r \subset r$. Thus, using the third equation, $s = r \cup e_1se_2$ where, as we have just seen, $e_1se_2 \subset r$. This gives $s = r$; hence $e' = g = h$, concluding the verification of the Remark and of $\mathbf{Q} \subset \mathbf{Q}'$ since $\mathbf{Q}$ is defined as the least family to satisfy (K1) and (K2).

III. VERIFICATION OF $\mathbf{Q}' \subset \mathbf{Q}$

The family $\mathbf{Q}'(1)$ consists of X^* and of the empty set. Thus $\mathbf{Q}'(1) \subset \mathbf{Q}$ and it will suffice to consider an arbitrary fixed $\gamma \in \Gamma(n)$ and to show $\gamma^{-1}M' \in \mathbf{Q}$ for all $M' \subset M = \gamma X^*$ under the induction hypothesis $\mathbf{Q}'(n-1) \subset Q$.

Remark 3. *If $W_{M'} = \{m \in M : MmM \cap M' = \emptyset\}$ contains two elements or more, then $\gamma^{-1}M' \in \mathbf{Q}$.*

Verification. Let β be a map of M onto a set $\bar{M}$ that has the following two properties: β sends $W_{M'}$ on a distinguished element 0 of $\bar{M}$; the restriction of β to $M \backslash W_{M'}$ is a bijection onto $\bar{M} \backslash \{0\}$.

Taking into account that, by definition, $W_{M'} = M \cdot W_{M'} \cdot M$, a structure of monoid is defined on $\bar{M}$ by letting $(\beta m)(\beta m') = \beta(mm')$ for all $m, m' \in M$. Then, if $\mathbf{Card}\ W_{M'} \geqq 2$, we have $\beta\gamma \in \Gamma(n-1)$ and, since $\gamma^{-1}M' = (\beta\gamma)^{-1}\beta M'$, the Remark is verified.

Remark 4. *If M' is an ideal (i.e., if $M' = M'M$ or $= MM'$), then $\gamma^{-1}M' \in \mathbf{Q}$.*

Verification. Because of left-right symmetry and of the finiteness of M, it suffices to consider the two cases of $M' = mM \neq MmM$ and of $M' = MmM \neq M$ where m is an arbitrary fixed element of M.

Let $A = \gamma^{-1}(mM)$ (resp. $= \gamma^{-1}(MmM)$) and $B = A \backslash A \cdot X \cdot X^*$ (resp. $= A \backslash (X^* \cdot X \cdot A \cup A \cdot X \cdot X^* \cup X^* \cdot X \cdot A \cdot X \cdot X^*)$). By construction B is the least subset of X^* such that $A = B \cdot X^*$ (resp. $= X^* \cdot B \cdot X^*$) and the hypothesis $M' \neq M$ is equivalent to $e \notin B$. Further, let $M'' = \{m' \in M : \gamma^{-1}m' \cdot X \cap B \neq \emptyset\}$ (resp. $= \{m' \in M : X \cdot \gamma^{-1}m' \cdot X \cap B \neq \emptyset\}$). Since $\gamma B \subset M' = M'M$ (resp. $= MM'M$) and $e \notin B$, we can find $X_0 \subset X$ and, for each $m' \in M''$, one subset $X_{m'}$ of X (resp. two subsets $X_{m'}$ and $X'_{m'}$ of X) in such a way that $A = X_0 \cdot X^* \cup \{\gamma^{-1}m' \cdot X_{m'} \cdot X^* : m' \in M''\}$ (resp. $= X^* \cdot X_0 \cdot X^* \cup \{X^* \cdot X'_{m'} \cdot \gamma^{-1}m' \cdot X_{m'} \cdot X^* : m' \in M''\}$) and we have only to check $\mathbf{Card}\ W_{\{m'\}} \geqq 2$ for all $m' \in M''$.

First, let us recall the following consequence of Green (1951). *If P is a finite monoid and if $u, u' \in P$ satisfy $u' \in uP$ and either $u'P \neq uP$ or $Pu'P \neq PuP$, then $Pu'P \subset W_{\{u\}}$.*

Indeed, assume $u' \in uP$ and $Pu'P \not\subset W_{\{u\}}$, that is, assume $u' = ua''$ and $u = au'a'$ for some $a, a', a'' \in P$. We have $u = a^n u(a''a')^n$ for $n = 1$, hence for all $n \geqq 1$. Since P is finite there exist two positive integers r and

q such that $a^{rq} = a^q a^{rq}$. It follows that $u = a^{rq}u(a''a')^{rq} = a^q a^{rq} u \cdot (a''a')^{rq} = a^q u$ from which we deduce $u = a^{rq}u(a''a')^{rq} = u(a''a')^{rq} = u'a'(a''a')^{rq-1}$ showing $u \in u'P$, i.e., $uP \subset u'P$. Since by hypothesis $u'P \subset uP$ this gives the desired relations $u'P = uP$ and $Pu'P = PuP$. (For later reference we note that if P has only trivial subgroups, i.e., if $q = 1$, the same hypothesis give $u = au$ hence $au' = aua'' = ua'' = u'$ and, finally, $u = au'a' = u'a'$).

Consider now $m' \in M''$ and take $f \in \gamma^{-1}m'$ and $x \in X$ such that $fx \in B$ (resp. $x'fx \in B$ for some $x' \in X$). We have $\gamma fx = m'\gamma x \in m'M \cdot$ (resp. $\gamma fx \in m'M$ and $\gamma x'fx \in (\gamma x' \cdot m') \cdot M$). Because of the minimal character of B, $\gamma fx \cdot M$ $(= M' = M' \cdot M)$ is not equal to $m'M$ (resp. $M \cdot \gamma x'fx \cdot M$ $(= M' = M \cdot M' \cdot M)$ is not equal to $M \cdot \gamma x'f \cdot M$, a fact which implies that, also, $\gamma fx \cdot M \neq m'M$). Thus $M \cdot M' \cdot M \subset W_{\{m'\}}$ and **Card** $W_{\{m'\}} \geqq 2$ because of the hypothesis $M' \neq M \cdot M' \cdot M$ (resp $M \cdot \gamma fx \cdot M \subset W_{\{m'\}}$ and $M \cdot \gamma x'fx \cdot M \subset W_{\{\gamma x'f\}}$, hence, using symmetry, $\gamma x'fx, \gamma x'f, \gamma fx \in W_{\{m'\}}$ with $\gamma x'fx \neq \gamma x'f$).

REMARK 5. *For all $m \in M$, the set $(mM \cap Mm) \backslash W_{\{m\}}$ reduces to $\{m\}$.*

Verification. The hypothesis $m' \notin W_{\{m\}}$, $m' \in mM \cap Mm$ is equivalent to the existence of $a, a', a_1'', a_2'' \in M$ such that $m = am'a'$; $m' = ma_1''$; $m' = a_2''m$. As mentioned above the first two relations imply $m = m'a'$ and $m' = am'$. Thus, by symmetry, $m = am'$ and $m' = m'a'$ showing $m = m'$. This concludes the verification of Remark 5 and, in view of Remark 4, it also concludes the verification of $\mathbf{Q} = \mathbf{Q}'$.

IV. AN EXAMPLE OF EGGAN

Let $X = \{x_n\}_{n \in \mathbf{N}}$ and for each $k \in \mathbf{N}$ let λ_k be the endomorphism of X^* that sends each $x_n \in X$ onto $x_{n+n'}$ where $n' = 2^k - 1$ if $n < 2^k$ and $n' = 0$, otherwise. Setting $B_1 = \{x_1\}$, we define inductively for $k > 1$, $B_k = B_{k-1}^* \cdot (\lambda_k B_{k-1})^* \cdot \lambda_k x_0$ where for any $A \subset X^*$, A^* denotes the submonoid generated by A. In Eggan (1963), p. 389, it is shown that B_k^* (denoted by $|\beta_k^*|$) has exactly star-height k.

It is clear that $B_1 \in \mathbf{Q}$ and, to verify $B_{k+1} \in \mathbf{Q}$, it suffices to verify $B_k^* \in \mathbf{Q}$ under the induction hypothesis that $\gamma^{-1}\gamma B_k = B_k$ for some epimorphism γ of X^* onto a finite monoid having only trivial subgroups. Consider any element $f \in X^* \cdot B_k$. Induction on the number of times $\lambda_k x_0$ appears in f shows that either $f \in B_k^* \cdot B_k$ or $f \in V_k = \{f' \in X^* : f'X^* \cap B_k^* = \emptyset\}$. Thus $B_k^* = \{e\} \cup X^* \cdot B_k \backslash V_k$ and since $V_k = \gamma^{-1}M'$ where $M' = \{m \in \gamma X^* : m \cdot \gamma X^* \cap \gamma B_k = \emptyset\}$ the result follows from the induction hypothesis.

It may not be too irrelevant to recall the following example which shows that sets of star-height one can have associated arbitrarily complex groups. Let x and y be two distinct elements of X and, for $n > 3$, let $C_n = \{x^n, x^{n-1}yx, x^{n-2}y, yx^{n-1}\} \cup \{x^i yx^{n-i-1} : 1 \leqq i \leqq n - 3\}$. Applying the theorem of Teissier (1951) shows that if ρ is a homomorphism of X^* into a finite monoid such that the sets ρC_n^* and $\rho C_n^* \cdot \rho x$ are disjoint, then ρX^* contains at least one subgroup which admits the symmetric group $\mathfrak{S}_n$ as a quotient group.

RECEIVED: March 20, 1964

REFERENCES

EGGAN, L. C. (1963), Transition graphs and the star-height of regular events. *Michigan Math. J.* **10**, 385–397.

GREEN, J. A. (1951), On the structure of semi-groups. *Ann. Math.* **54**, 163–172.

MCNAUGHTON, R. (1960), Symbolic logic and automata. WADC Tech. Rept. 60–244.

MILLER, D. D., AND CLIFFORD, A. H. (1956), Regular D-classes in semigroups. *Trans. Am. Math. Soc.* **82**, 270–280.

PETRONE, L., AND SCHÜTZENBERGER, M. P. (1963), Sur un problème de McNaughton. Rapport CETIS·EURATOM.

TEISSIER, M. (1951), Sur les équivalences régulières dans les demi-groupes. *Compt. Rend. Acad. Sci. Paris* **232**, 1987–1989.

TRAHTENBROT, B. A. (1958), Sintes logiceskikh setei .... *Dokl. Akad. Nauk SSSR* **118**, 646–649.