RESEARCH NOTE

NC-167 Thomas J. Watson Research Center, Yorktown Heights

ON AN ABSTRACT MACHINE PROPERTY PRESERVED UNDER THE SATISFACTION RELATION

by

M. P. Schützenberger *

11/12/62

ABSTRACT: Application of classical results on finite monoids to the Elgot-Rutledge theory gives a new property of machines that is preserved under the satisfaction relation.

---

* Presently at the University of Poitier in Poitier, France.

IBM

I. INTRODUCTION

The present note is a straightforward application to the theory of C. C. Elgot and J. D. Rutledge of basic results of D. D. Miller and A. H. Clifford. We refer to these two papers for further motivation and bibliography. I gladly acknowledge my indebtedness to C. C. Elgot for most of my notions on this topic.

For simplicity it will be assumed once for all that all the machines considered here are finite, that all their transitions are defined and that all their states are accessible from the initial state. The input alphabet X and the output set $Y = \{y_j\}$ $(1 \leq j \leq n)$ are fixed finite sets. Thus a machine $\mathcal{M}$ can be identified with a triple $(S, \sigma, \bar{\beta})$ where:

i) S is a finite set of states;

ii) σ is a right regular mapping onto S of the free monoid F generated by X;

iii) $\bar{\beta}$ is a mapping of S into the set $\{0, 1, \ldots, n\}$ of integers.

We recall that σ is a right regular mapping iff for all $f, f', f'' \in F$, $\sigma f f'' \neq \sigma f' f''$ only if $\sigma f \neq \sigma f'$. With this notation the initial state is σe (e = the neutral element of F); the transition function $S \times X \to S$ is defined for all $s \in S$ and $x \in X$ by $s \cdot x = \sigma((\sigma^{-1} s) x)$ (and, more generally, for all $f \in F$, $s \cdot f = \sigma((\sigma^{-1} s) f)$); the behavior of $\mathcal{M}$ is the set of all pairs (f, y_i) where $f \in F$, $y_i \in Y$ are such that $i = \bar{\beta}\sigma f$.

Thus another machine $\mathfrak{M}' = (T, \tau, \bar{\delta})$ satisfies $\mathfrak{M}$ iff, for all $f \in F$, $(\bar{\beta}\sigma f - \bar{\delta}\tau f) \cdot \bar{\beta}\sigma f = 0$.

Finally, a subset S' of states of $\mathfrak{M}$ is compatible in the sense of C. C. Elgot and J. D. Rutledge iff, for all $s_1, s_2 \in S'$, $f \in F$, $s_3 = s_1 \cdot f$, $s_4 = s_2 \cdot f$, one has $(\bar{\beta}s_3 - \bar{\beta}s_4)\bar{\beta}s_3\bar{\beta}s_4 = 0$.

We shall associate to $\mathfrak{M}$ a finite collection Gp $\mathfrak{M}$ of finite groups and to each $G \in$ Gp $\mathfrak{M}$ a finite collection Comp G of quotient groups G/N such that the following relation holds:

Main Property. If $\mathfrak{M}'$ satisfies $\mathfrak{M}$ there corresponds to each $G \in$ Gp $\mathfrak{M}$ at least one $K \in$ Gp $\mathfrak{M}'$ and at least one $G' \in$ Comp G such that G' is a homomorphic image of a subgroup of K.

It is not claimed that this property is useful for solving algorithmically the state minimization problem. On the other hand, it is vacuous only if there exists a natural number p such that for all f, the set $\sigma f^p F f^p$ is compatible.

It has been pointed out by C. C. Elgot that the property could be part of a proof showing that if the monoid of $\mathfrak{M}$ is a group (cf. below), the same is true for any minimal machine satisfying $\mathfrak{M}$.

Clearly the main property could be formulated without recourse to machine terminology in terms of two partitions

$\{R_i\}_{0 \le i \le n}$ and $\{R'_i\}_{0 \le i \le n}$ of F into regular events such that, for all positive i, $R_i \subset R'_i$.

II. VERIFICATION OF THE MAIN PROPERTY

Let $\mathfrak{M} = (S, \sigma, \bar{\beta})$ be a fixed machine and define as usual a homomorphism μ of F onto quotient monoid $M = \mu F$ by setting for all $f, f' \in F$

$\mu f = \mu f'$ iff, for all $s \in S$, $s \cdot f = s \cdot f'$.

Definition 1. Gp $\mathfrak{M}$ is the family of all subsets G of M that have the following properties:

i) G is isomorphic to a group;

ii) G is not properly contained in another subset of $\mathfrak{M}$ isomorphic to a group.

Definition 2. For each $G \in$ Gp $\mathfrak{M}$, Comp G is the set of all quotient groups $G' = G/N$ for which the normal subgroup N of G is such that $\sigma\mu^{-1}N$ is a compatible subset of S in the sense of C. C. Elgot and J. D. Rutledge.

We reformulate in the following terms a fundamental result of A. A. Miller and A. H. Clifford.

Theorem 1. If the subset G of M is isomorphic to a group, it contains one and only one idempotent u; then the set $G_u = \{m \in M: m \in uMu;\ u \in Mmu \cap umM\}$ belongs to Gp $\mathfrak{M}$ and it admits G as a subgroup.

It follows that we can attach to each $f \in F$ a well defined group $G_f \in \underline{Gp}\ \mathcal{M}$ by the following construction based upon the remark that for all $f, f', f'' \in F$, one has $S.f'f \subset S.f$ and $\underline{Card}\ S\cdot f'ff'' \leq \underline{Card}\ S\cdot f$.

Let k be the least natural number such that $S.f^{k+1} = S.f^k$ ($k < \infty$ since $\underline{Card}\ S < \infty$); let $\bar{k}$ be the least natural number such that, for all $s \in S$, $s.f^{k+\bar{k}} = s.f^k$ ($\bar{k} < \infty$ since f determines a permutation of $S.f^k$); let $\bar{f} = f^{k+k'}$ where k' is the least natural number congruent to $-k$ modulo $\bar{k}$.

By construction, for all $s \in S$, $s.\bar{f}\bar{f} = s.\bar{f}$ and, thus, $u = \mu\bar{f}$ is an idempotent of M.

Consider any $m \in G_u$; since $umu = m$, the set $\mu^{-1}m \cap \bar{f}F\bar{f}$ is not empty. Hence $G_u \subset \mu(\bar{f}F\bar{f})$.

Now let $H_f = \{f' \in F: f' \in \bar{f}F\bar{f}, \underline{Card}\ S.f' = \underline{Card}\ S.\bar{f}\}$ and verify that $G_u = \mu H_f$ and that G_u is isomorphic to a group. Indeed, if $m_1 \in G_u$ and $f_1 \in \mu^{-1}m_1 \cap \bar{f}F\bar{f}$, the existence of $m_2 \in G_u$ such that $m_1 m_2 = u$ implies the existence of at least one $f' \in F$ such that $S.\bar{f} = S.f_1 f'$. However, since $f_1 \in \bar{f}F\bar{f}$ implies $S.f_1 \subset S.\bar{f}$, this gives $S.f_1 = S.\bar{f}$, proving $G_u \subset \mu H_f$.

Reciprocally, $f' \in H_f$ implies $S.f' = S.\bar{f}f' = S.\bar{f}$. Thus $\{\mu f'^p: p \geq 0\}$ is contained in H_f and it is isomorphic to a group having $u = \mu\bar{f}$ as its neutral element. Hence, setting $m' = \mu f'$

there exists a natural number p' such that $m'' = \mu f'^{p'}$ satisfies $m'm'' = m''m' = u$. Thus $m', m'' \in uMu$; $u \in Mmu \cap umM$ (since $m'' \in M$) proving $m = \mu f' \in G_u$ and concluding the verification.

Now let $\mathcal{M}' = (T, \tau, \bar{\delta})$ be another machine; the homomorphism π of F onto a quotient monoid P is defined for all $f, f' \in F$ by $\pi f = \pi f'$ iff, for all $t \in T$, $t.f = t.f'$.

We shall use repeatedly the fact that $\mu\pi^{-1}$ is a mapping of the family of all subsets of P into the family of all subsets of M such that for all $P', P'' \subset P$, one has $(\mu\pi^{-1}P')(\mu\pi^{-1}P'') \subset \mu\pi^{-1}P'P''$. Thus, particularly if P' is <u>stable</u> (i.e., if $P'^2 \subset P'$), its image $\mu\pi^{-1}P'$ is also a stable subset of M.

Similar properties hold for $\pi\mu^{-1}$.

<u>Remark 1.</u> For each $G \in \underline{Gp}\,\mathcal{M}$, there exists at least one $K \in \underline{Gp}\,\mathcal{M}'$ and a subgroup $\bar{K}$ of K such that $\bar{K} = K \cap \pi\mu^{-1}G$ and $G \subset \mu\pi^{-1}\bar{K}$.

<u>Proof.</u> By construction $\pi\mu^{-1}G$ is a finite stable subset of P. Hence we can find at least one element $\bar{f} \in \mu^{-1}G$ having the following properties:

i) $\mu\bar{f} = u$, the idempotent of G;

ii) $\pi\bar{f} = v$, an idempotent of P;

iii) For all $f' \in \mu^{-1}G$, $\underline{\text{Card}}\ T.\bar{f} \leq \underline{\text{Card}}\ T.f'$.

Thus by the construction recalled above, $G = G_u$; $K = K_v \in \underline{Gp}\,\mathcal{M}'$, and $K = \pi L_{\bar{f}}$ where $L_{\bar{f}} = \{f' \in F\colon f' \in \bar{f}F\bar{f}$, Card $T.f' =$ Card $T.\bar{f}\}$. Because of iii, $H_{\bar{f}} \subset L_{\bar{f}}$; $\mu H_{\bar{f}} = G$; $\pi\mu^{-1}G \cap K = \pi H_{\bar{f}} = \bar{K} \subset K$. Since K is finite and $\bar{K}$ is stable, we have verified that $\bar{K}$ is a subgroup of K.

Let us now define a mapping ρ of $\bar{K}$ into the family of all subsets of G by setting for all $k \in \bar{K}$, $\rho k = G \cap \mu\pi^{-1}k$.

Remark 2. The mapping ρ is a homomorphism of $\bar{K}$ onto the quotient group G/N where $N = \rho v$ $(= G \cap \mu\pi^{-1}\bar{f})$.

Proof. This is a well-known computation: since G is a stable subset of M, ρ maps every stable subset of $\bar{K}$ (and in particular $\{v\}$) onto a stable subset of G, hence onto a subgroup since G is finite and $\rho k \neq \emptyset$ for all $k \in \bar{K}$.

Let k be any element of $\bar{K}$ and take $k' \in \bar{K}$; $q, q' \in G$ such that $kk' = v$, $g \in \rho k$; $g' \in \rho k'$. Since $k'k = v$, we have the relations:

$$(\rho k)g'g \subset (\rho kk')g = Ng \subset \rho kk'k = \rho k;$$

$$gg'\rho k \subset g\rho k'k = gN \subset \rho kk'k = \rho k.$$

Because G is a group, however, $(\rho k)g'g \subset \rho k$ implies $(\rho k)g'g = \rho k$ and, similarly, $gg'\rho k = \rho k$. Thus $\rho k = gN = Ng$, proving that N is a normal subgroup and ρ an epimorphism $\bar{K} \to G/N$.

This essentially concludes the verification of the main property. Indeed, if $\mathfrak{M}'$ satisfies $\mathfrak{M}$, the element $t = \tau\bar{f} \in T$ is a state of $\mathcal{M}'$ and, by a special case of Theorem 2 of C. C. Elgot and J. D. Rutledge, we know that the set $\sigma\tau^{-1}t$ (which contains $\sigma\mu^{-1}N$) is a compatible set of states.

Example. Let $X = \{x\}$, a single letter, i.e., let $\mathcal{M}$ be an input-free machine. (cf. C. C. Elgot and J. D. Rutledge.) Then taking $f = x$ in the construction described after Th. 1, Gp $\mathcal{M}$ consists of a single cyclic group with $\bar{k}$ elements. Our main property asserts that any input-free machine which satisfies $\mathcal{M}$ has a loop with $\bar{k}'$ states where $\bar{k}'$ is some multiple of a divisor d' of $\bar{k}$ such that if $dd' = \bar{k}$ the set $\{\sigma f^{\bar{k}+i} : 0 \leq i < d\}$ of states of $\mathcal{M}$ is compatible.

Remark. Let us recall that $\mathcal{M}$ is minimal iff, for all $f, f' \in F$, the relation $\sigma f \neq \sigma f'$ implies that, for at least one $f'' \in F$, one has $\bar{\beta}\sigma ff'' \neq \bar{\beta}\sigma f'f''$. Under the hypothesis that both $\mathcal{M}$ and $\mathcal{M}'$ are minimal, the homomorphisms μ and π depend only upon the partitions $\{R_i\}$ and $\{R_i'\}$ of F where $R_i = (\bar{\beta}\sigma)^{-1}i$ and $R_i' = (\bar{\delta}\tau)^{-1}i$ for $0 \leq i \leq n$. Then, by an argument symmetric to the one used by C. C. Elgot and J. D. Rutledge, it is easily seen that the condition "$\sigma\mu^{-1}N$ is compatible" can be replaced by the two-sided condition: for all $f, f' \in \mu^{-1}N$ and $f_1, f_2 \in F$, the elements $f_3 = f_1 ff_2$ and $f_4 = f_1 f' f_2$ satisfy $(\bar{\beta}\sigma f_3 - \bar{\beta}\sigma f_4)\,\bar{\beta}\sigma f_3\,\bar{\beta}\sigma f_4 = 0$.

REFERENCES

C. C. Elgot and J. D. Rutledge, "Machine properties preserved under state minimization," Switching Circuit Theory and Logical Design, Proceedings of the Third Annual AIEE Symposium, 61-70 (September 1962).

D. D. Miller and A. H. Clifford, "On regular D-classes in semigroups," Trans. Am. Math. Soc., 82, 270-280 (1956).