On equational classes of unoids

By F. GÉCSEG and S. SZÉKELY in Szeged

To Professor B. Sz.-Nagy on his 60th birthday

In this paper we present an algorithm to decide for a given finite unoid $\mathfrak{A}$ and an equational class K generated by finitely many finite unoids whether or not $\mathfrak{A}$ is contained by K. This problem has an automata theoretical background. Using this algorithm one can decide for a finite automaton whether it can be given as a homomorphic image of a subautomaton of an A-direct product of smaller automata. (For an automata theoretical terminology, see [1].)

Before stating our theorem, we introduce some notions and notations.

A universal algebra $\mathfrak{A}=\langle A; F\rangle$ is called *unoid* if each operation in F is unary (see А. И. Мальцев [2]). $\mathfrak{A}$ is *finite* if both A and F are finite. Take an arbitrary polynomial xp over F. We say that xp is of *length n* if it has the form $xp=xf_1\dots f_n(=(\dots(xf_1)\dots)f_n)$ $(f_1,\dots,f_n\in F)$. A polynomial $xp=xf_1\dots f_n$ is a *subpolynomial* of xq if $xp=xq$ or $xq=xf_1\dots f_n f_{n+1}\dots f_m(=xpf_{n+1}\dots f_m)$ holds, in notation: $xp\subseteqq xq$.

Let X be an arbitrary set and $\mathfrak{X}=\langle X^{(\infty)}; F\rangle$ the free unoid generated by X. By $X^{(n}$ $(n=0,1,\dots)$ we denote the subset of $X^{(\infty)}$ consisting of all polynomials with length not exceeding n. (Here $X^{(0)}=X$.)

A partition π of $X^{(n)}$ into disjoint subsets is called an *n-congruent partition* of $\mathfrak{X}$ if

(I) for any $x,y\in X^{(n-1)}$ and $f\in F$, $x\equiv y(\pi)$ implies $xf\equiv yf(\pi)$ and
(II) for each $x\in X^{(n)}$ there exists a $y\in X^{(n-1)}$ such that $x\equiv y(\pi)$.

It should be noted that if π is an n-congruent partition of $\mathfrak{X}$ then it can be extended uniquely to a congruent (m-congruent, $m\geqq n$) partition of $\mathfrak{X}$. For the congruent extension of an n-congruent partition π we use the notation π^*. Furthermore, $\mathfrak{X}/\pi^*$ denotes the factor unoid induced by π^*.

Now we are ready to state our

Theorem. *Let $\mathfrak{A}_i=\langle A_i; F\rangle$ $(i=1,\dots,k)$ and $\mathfrak{A}=\langle A; F\rangle$ be finite unoids. Moreover, let $\langle a_1,\dots,a_l\rangle$ be a generating system of $\mathfrak{A}$, $X=\langle x_1,\dots,x_l\rangle$ a set of symbols* *and* $m = \max \langle \bar{\bar{A}}, \bar{\bar{A}}_1, \ldots, \bar{\bar{A}}_k \rangle$. *Then* $\mathfrak{A}$ *is contained in the equational class generated by* $\langle \mathfrak{A}_i | i = 1, \ldots, k \rangle$ *if and only if there exist m-congruent partitions* $\pi_1^{(m)}, \ldots, \pi_r^{(m)}$ *and* $\pi^{(m)}$ *of* $\mathfrak{X} = \langle X^{(\infty)}; F \rangle$ *such that for their extentions* $\pi_1^{(m^r)}, \ldots, \pi_r^{(m^r)}$ *and* $\pi^{(m^r)}$ *to* m^r*-congruent partitions the following hold:*

(1) $\pi_1^{(m^r)} \cap \cdots \cap \pi_r^{(m^r)} \subseteq \pi^{(m^r)}$,

(2) $\mathfrak{X}/\pi^{(m)*} \cong \mathfrak{A}$ *and each* $\mathfrak{X}/\pi_j^{(m)*}$ $(1 \leqq j \leqq r)$ *is isomorphic to a subunoid of the unoids* $\mathfrak{A}_i$ $(i = 1, \ldots, k)$.

Proof. Let us suppose that $\mathfrak{A}$ is contained in the equational class generated by $\langle \mathfrak{A}_i | i = 1, \ldots, k \rangle$. Denote by $S(\langle \mathfrak{A}_i | i = 1, \ldots, k \rangle)$ the class of all unoids isomorphic to a subunoid of the unoids $\mathfrak{A}_i$ $(i = 1, \ldots, k)$. Then there exists a subdirect product $\mathfrak{B} = \langle B; F \rangle$ of unoids from $S(\langle \mathfrak{A}_i | i = 1, \ldots, k \rangle)$ such that $\mathfrak{A}$ is a homomorphic image of $\mathfrak{B}$ under a suitable homomorphism φ. Let $\langle b_1, \ldots, b_l \rangle$ be a subset of B for which $b_j \varphi = a_j$ $(j = 1, \ldots, l)$ hold. It is obvious that the subunoid $\mathfrak{B}'$ of $\mathfrak{B}$ generated by $\langle b_1, \ldots, b_l \rangle$ can be given in the subdirect form $\mathfrak{B}' = \mathfrak{B}_1 \times \cdots \times \mathfrak{B}_s \times \cdots (\mathfrak{B}_1, \ldots, \mathfrak{B}_s, \ldots \in S(\langle \mathfrak{A}_i | i = 1, \ldots, k \rangle))$ and the restriction of φ to $\mathfrak{B}'$ (which is denoted by the same φ) is a homomorphism of $\mathfrak{B}'$ onto $\mathfrak{A}$.

Now take the homomorphism ψ of $\mathfrak{X}$ onto $\mathfrak{B}'$ for which $x_j \psi = b_j$ $(j = 1, \ldots, l)$ hold. Then $\psi\varphi$ is a homomorphism of $\mathfrak{X}$ onto $\mathfrak{A}$ such that $x_j(\psi\varphi) = a_j$ $(j = 1, \ldots, l)$.

Let us define partitions ϱ_t $(t = 1, \ldots, s, \ldots)$ on $\mathfrak{B}'$ in the following way:

$$(c_1, \ldots, c_t, \ldots) \equiv (c_1', \ldots, c_t', \ldots)(\varrho_t)$$

$((c_1, \ldots, c_t, \ldots), (c_1', \ldots, c_t', \ldots) \in B')$ if and only if $c_t = c_t'$. Moreover, take the partition ϱ on $\mathfrak{B}'$ given as follows: $b \equiv b'(\varrho)$ $(b, b' \in B')$ if and only if $b\varphi = b'\varphi$. It can easily be seen that the number of all classes of ϱ_t is equal to the cardinality of B_t. A similar statement is valid for ϱ and A. It is also clear that the intersection of the partitions ϱ_t is the trivial partition ι on $\mathfrak{B}'$.

Now take the following partitions π_t $(t = 1, \ldots, s, \ldots)$ and π on $X^{(m)}: x \equiv y(\pi_t)$ and $x \equiv y(\pi)$ $(x, y \in X^{(m)})$ if and only if $x\psi \equiv y\psi(\varrho_t)$ and $x\psi \equiv y\psi(\varrho)$, respectively. We show that π_t and π are m-congruent partitions of $\mathfrak{X}$. It can be proved by an easy computation that condition (I) of m-congruence holds for π_t $(t = 1, \ldots, s, \ldots)$ and π. It remains to be shown that condition (II) is also satisfied by these partitions.

Take an arbitrary polynomial xp from $X^{(m)} \setminus X^{(m-1)}$. Since the number of classes of π_t is less than or equal to m, there are two different subpolynomials xp' and xp'' of xp such that $xp' \subset xp''$ and $xp' \equiv xp''(\pi_t)$. (Here xp' can be x.) Therefore, there exists a polynomial $x'w$ with $xp = xp''w$. Thus $xp \equiv xp'w(\pi_t)$ and the length of $xp'w$ is less than m. The statement concerning π can be proved similarly. But the number of elements of $X^{(m)}$ is finite. Therefore, among the m-congruent partitions π_t $(t = 1, \ldots, s, \ldots)$ we have only finitely many different. Let us denote them by $\pi_1^{(m)}, \ldots, \pi_r^{(m)}$. Thus we got that the number of all classes of $x_1^{(m)*} \cap \cdots \cap x_r^{(m)*}$ is less than or equal to m^r. Since the restrictions of $x_1^{(m)*}, \ldots, x_r^{(m)*}$ to $X^{(m^r)}$ are the same as the extensions $\pi_1^{(m^r)}, \ldots, \pi_r^{(m^r)}$ of $\pi_1^{(m)}, \ldots, \pi_r^{(m)}$ to $X^{(m^r)}$, we got that $\pi_1^{(m^r)} \cap \cdots \cap x_r^{(m^r)}$ is an m^r-congruent partition. It is obvious that $\pi_1^{(m^r)} \cap \cdots \cap \pi_r^{(m^r)} \subseteqq \pi^{(m^r)}$, $\mathfrak{X}/\pi^{(m)*} \cong \mathfrak{A}$, and $\mathfrak{X}/\pi_h^{(m)*}$ $(h=1, \ldots, r)$ is isomorphic to a unoid in $S(\langle \mathfrak{A}_i | i=1, \ldots, k \rangle)$.

Conversely, let us suppose that the conditions of our theorem are satisfied. Then, as is well known, $\mathfrak{A}\, (\cong \mathfrak{X}/\pi^{(m)*})$ is a homomorphic image of a subdirect product of $\mathfrak{X}/\pi_1^{(m)*}, \ldots, \mathfrak{X}/\pi_r^{(m)*}$ because $\pi_1^{(m)*} \cap \cdots \cap \pi_r^{(m)*} \subseteqq \pi^{(m)*}$. Therefore, $\mathfrak{A}$ is contained in the equational class generated by $\langle \mathfrak{A}_i | i=1, \ldots, k \rangle$. This ends the proof of the theorem.

We remark that the algorithm given by the theorem above can easily be generalized for equational classes generated by finitely many finite universal algebras of finite type.

References

[1] F. Gécseg and I. Peák, *Algebraic Theory of Automata* (Budapest, 1972).
[2] А. И. Мальцев, *Алгебраические системы* (Москва, 1970).

(Received September 1, 1972)