On subdirect representations of finite commutative unoids

By F. GÉCSEG in Szeged

In this paper we give a representation of finite commutative unoids as homomorphic images of subdirect products of very simple finite commutative unoids. Furthermore, using this representation, we present a full characterization of those finite commutative unoids $\mathfrak{A}$ which have the following property: if $\mathfrak{A}$ can be given as a homomorphic image of a subdirect product of two finite commutative unoids $\mathfrak{B}$ and $\mathfrak{C}$ then there exists a subunoid of $\mathfrak{B}$ or $\mathfrak{C}$ which can be mapped homomorphically onto $\mathfrak{A}$.

Let $\mathfrak{A}=\langle A; F\rangle$ be a unoid. (For the terminology, see [1].) We say that $\mathfrak{A}$ is commutative if $af_1f_2=af_2f_1$ for any $a\in A$ and $f_1, f_2\in F$. In this paper by a unoid we always mean a finite commutative unoid.

Take an arbitrary unoid $\mathfrak{A}=\langle A; F\rangle$, an element $a\in A$ and an operation $f\in F$. Then by the *cycle generated by* (a, f) in $\mathfrak{A}$ we mean the set of elements $af^0, af, \dots$ $\dots, af^k, \dots,$ where $af^0=a$ and $af^k=(af^{k-1})f$ for any positive integer k. For this cycle we use the short notation (a, f). If $af^0, \dots, af^u$ are all different and u is the least exponent for which there exists a $w>u$ such that $af^w=af^u$ then $af^0, \dots, af^{u-1}$ is the *preperiod* of this cycle and u is the *length of this preperiod*. (When the preperiod is empty its length equals 0.) Furthermore, if $u+v$ is the minimal number for which $af^{u+v}=af^u$ holds then $af^u, af^{u+1}, \dots, af^{u+v-1}$ is the *period* of the cycle under question and v is the *length of this period*. In this case we say that (a, f) *is a cycle of type* (u, v).

A unoid $\mathfrak{A}=\langle A; F\rangle$ is called *f-cyclic* $(f\in F)$ of type (k, l) if for some $a\in A$, the set A coincides with the cycle (a, f) in $\mathfrak{A}$ and this cycle is of type (k, l), while the operations different from f are identical mappings of A.

$\mathfrak{A}$ is called *prime-power unoid* (with respect to $f\in F$) if it is f-cyclic of type $(0, r^n)$ where r is a prime number. $\mathfrak{A}$ is an *elevator* (regarding $f\in F$) if it is f-cyclic of type $(k, 1)$. We say that $\mathfrak{A}$ is a prime-power unoid (resp. elevator) if it is prime-power unoid (resp. elevator) regarding one of its operations.

Now we are ready to state our

Theorem 1. *Every commutative unoid can be given as a homomorphic image of a subdirect product of finitely many elevators and prime-power unoids.*

Proof. Let $\mathfrak{A}=\langle A; F\rangle$ be an arbitrary commutative unoid. Denote by F^* the unoid of all polynomials over F of the form xp under a fixed variable x. We shall write $xp\equiv xq(\varrho)$ if and only if $xp=xq$ holds identically in $\mathfrak{A}$. It is obvious that the relation ϱ is a congruence on F^* (we say that $\mathfrak{A}$ induces ϱ), and the factor unoid $F^*/\varrho=\mathfrak{B}(=\langle B; F\rangle)$ is commutative. For elements of $\mathfrak{B}$ we shall apply the following notation: $C_\varrho(xp)$ means the class of the partition of F^* induced by ϱ containing xp.

Let us suppose that $F=\langle f_1, \ldots, f_k\rangle$, and define the unoids $\mathfrak{B}_i=\langle B_i; F\rangle$ $(i=1, \ldots, k)$ as follows: B_i is the cycle $(C_\varrho(x), f_i)$ in $\mathfrak{B}$ and f_i is the restriction of f_i (on B) to B_i, while the operations f_j are identical mappings of B_i for $j\neq i$.

Now take the mapping φ of the direct product $\mathfrak{B}_1\times\ldots\times\mathfrak{B}_k$ into $\mathfrak{B}$ defined in the following way:

$$\varphi\big((C_\varrho(xf_1^{n_1}), \ldots, C_\varrho(xf_i^{n_i}), \ldots, C_\varrho(xf_k^{n_k}))\big) = C_\varrho(xf_1^{n_1}\ldots f_i^{n_i}\ldots f_k^{n_k})$$
$$(n_1, \ldots, n_i, \ldots, n_k = 0, 1, \ldots).$$

Using commutativity of $\mathfrak{B}$ it can immediately be verified that φ is a homomorphism *onto* $\mathfrak{B}$.

Let us denote by ϱ_1 the relation induced by $\mathfrak{B}_1\times\ldots\times\mathfrak{B}_k$ on F^*. Then $\varrho_1\leqq\varrho$ because $\mathfrak{B}$ is a homomorphic image of $\mathfrak{B}_1\times\ldots\times\mathfrak{B}_k$. Observe that $\mathfrak{B}_i$ is f_i-cyclic for every i $(1\leqq i\leqq k)$. Let $\mathfrak{B}_i$ be of type (u_i, v_i). In the case $v_i=1$ let $\mathfrak{B}_i'$ be an f_i-cyclic unoid of type $(u_i, 2)$ and let $\mathfrak{B}_i'=\mathfrak{B}_i$ in the other case. It is obvious that $\mathfrak{B}_i'$ can be mapped homomorphically onto $\mathfrak{B}_i$. Therefore, $\mathfrak{B}_1\times\ldots\times\mathfrak{B}_k$ is a homomorphic image of $\mathfrak{B}_1'\times\ldots\times\mathfrak{B}_k'$. Denote by ϱ_2 the relation of F^* induced by $\mathfrak{B}_1'\times\ldots\times\mathfrak{B}_k'$. Then we get that $\varrho_2\leqq\varrho_1$.

As it can be seen in [2], every equation of an equational class of commutative unoids can have one of the following two forms:

$$(1)\qquad xf_1^{m_1}\ldots f_k^{m_k} = xf_1^{n_1}\ldots f_k^{n_k}$$
$$(2)\qquad xf_1^{m_1}\ldots f_k^{m_k} \doteq yf_1^{n_1}\ldots f_k^{n_k}$$
$$(m_1, \ldots, m_k, n_1, \ldots, n_k \geqq 0).$$

Equation (2) implies $xf_1^{m_1}\ldots f_k^{m_k}=yf_1^{m_1}\ldots f_k^{m_k}$. Choose an element b_i from every B_i' $(i=1, \ldots, k)$. Then $(b_1, b_2, \ldots, b_k)f_1^{m_1}\ldots f_k^{m_k}\neq(b_1f_1, b_2, \ldots, b_k)f_1^{m_1}\ldots f_k^{m_k}$ showing that (2) fails to hold on $\mathfrak{B}_1'\times\ldots\times\mathfrak{B}_k'$.

Therefore, we have got that every equation which holds on $\mathfrak{B}_1'\times\ldots\times\mathfrak{B}_k'$ is of the form (1). Since $\varrho_2\leqq\varrho$ thus all equations holding on $\mathfrak{B}_1'\times\ldots\times\mathfrak{B}_k'$ hold on $\mathfrak{A}$, too, i.e., $\mathfrak{A}$ is contained in the equational class generated by $\mathfrak{B}_1'\times\ldots\times\mathfrak{B}_k'$. This means that $\mathfrak{A}$ can be given as a homomorphic image of a subunoid of a finite direct power of $\mathfrak{B}_1'\times\ldots\times\mathfrak{B}_k'$ (see, e.g., the proof of the Theorem in [1]).

In order to end the proof of Theorem 1, it is enough to show that every $\mathfrak{B}_i'$ can be given as a subdirect product of finitely many elevators and prime-power unoids. Let $B_i' = \langle b_0, \ldots, b_{u_i}, \ldots, b_{u_i+v_i-1}\rangle$ and $v_i = r_1^{w_1} \ldots r_t^{w_t}$ where r_i are different prime numbers. Define the relations $\sigma_0, \sigma_1, \ldots, \sigma_t$ on B_i' as follows: $b_j \equiv b_k(\sigma_0)$ if and only if $j=k$ or $j, k \geqq u_i$, and for every l $(l=1, \ldots, t)$, $b_j \equiv b_k(\sigma_l)$ if and only if $j \equiv k \pmod{r_l^{w_l}}$. It is clear that $\sigma_0, \ldots, \sigma_t$ are congruences of $\mathfrak{B}_i'$; moreover, their intersection is the identity relation. Indeed, from $b_j \equiv b_k(\sigma_0 \cap \ldots \cap \sigma_t)$ it follows that $j=k$ or $j, k \geqq u_i$ and (by the Chinese Remainder Theorem) $j \equiv k \pmod{v_i}$. In both cases we have $b_j = b_k$. Thus $\mathfrak{B}_i'$ can be given as a subdirect product of $\mathfrak{B}_i'/\sigma_0, \ldots, \mathfrak{B}_i'/\sigma_t$. Moreover, $\mathfrak{B}_i'/\sigma_0$ is an elevator and each of $\mathfrak{B}_i'/\sigma_1, \ldots, \mathfrak{B}_i'/\sigma_t$ is a prime-power unoid. This ends the proof of Theorem 1.

A unoid $\mathfrak{A} = \langle A; F\rangle$ is called *homomorphically prime* if $|A|>1$ and the fact $\mathfrak{A}$ is a homomorphic image of a subdirect product of two unoids $\mathfrak{A}_1$ and $\mathfrak{A}_2$ implies that there exists a subunoid in $\mathfrak{A}_1$ or $\mathfrak{A}_2$ which can be mapped homomorphically onto $\mathfrak{A}$.

First we state the following simple

Theorem 2. *If $|F|=1$ then $\mathfrak{A} = \langle A; F\rangle$ is homomorphically prime if and only if $\mathfrak{A}$ is an elevator or prime-power unoid.*

Proof. The subunoids and homomorphic images of elevators are elevators, too. Similar statement is valid for prime-power unoids. Therefore, by Theorem 1, every homomorphically prime unoid should be either elevator or prime-power unoid. It can be shown, by an easy computation, that in the case $|F|=1$ all elevators and prime-power unoids are homomorphically prime.

This Theorem 2 and Theorem 1 of Yoeli in [3] show that the class of all homomorphically prime unary algebras and that of all connected subdirectly irreducible unary algebras coincide.

We now prove

Theorem 3. *If $|F| \geqq 2$ then a commutative unoid $\mathfrak{A} = \langle A; F\rangle$ is homomorphically prime if and only if $\mathfrak{A}$ is an elevator.*

Proof. The subunoids and homomorphic images of an elevator are elevators. Prime-power unoids have similar property. Thus, by Theorem 1, homomorphically prime unoids should be either elevators or prime-power unoids.

First we show that none of the prime-power unoids is homomorphically prime. Before proving this statement, let us introduce the notation $k \pmod n$ for the least non-negative residue of k modulo n.

For the sake of simplicity, let $\mathfrak{A} = \langle A; F\rangle$ be a prime-power unoid with respect to f_1 such that $A = \langle a_0, \ldots, a_{m^n-1}\rangle$ and

$$a_i f_1 = a_{i+1 \pmod{m^n}}$$

where m is a prime number. Take two different prime numbers $m_1(\neq m)$, $m_2(\neq m)$ such that $m^2 \nmid (m_1-m_2)$, and let r be an integer with $r>n$. Let us define the unoids $\mathfrak{A}_i=\langle A_i; F\rangle$ $(i=1, 2)$ in the following way:

$$A_i = \langle a_{i0}, \dots, a_{im^r}\rangle, \quad a_{ij}f_1 = a_{i(j+1)(\mathrm{mod}\, m^r)},$$

$$a_{ij}f_2 = a_{i(j+m_i)(\mathrm{mod}\, m^r)}$$

and $a_{ij}f_l=a_{ij}$ if $l>2$, where $i=1, 2$ and $j=0, \dots, m^r-1$. It is obvious that $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are commutative.

Consider the subdirect product $\mathfrak{A}_1 \dot{\times} \mathfrak{A}_2$ of $\mathfrak{A}_1$ and $\mathfrak{A}_2$ consisting of all elements (a_{1j}, a_{2j}) and $(a_{1j}, a_{2j})f_2^k$ $(j=0, \dots, m^r-1;\ k=1, 2, \dots)$. We show that the mapping φ defined by

$$\varphi((a_{10}, a_{20})f_1^t) = a_0 f_1^t \quad \text{and} \quad \varphi((a_{10}, a_{20})f_1^t f_2^k) = a_0 f_1^t \quad (t, k = 1, 2, \dots)$$

is a homomorphism of $\mathfrak{A}_1 \dot{\times} \mathfrak{A}_2$ onto $\mathfrak{A}$.

It is enough to prove that φ is well defined. Let t_1, k_1 and t_2, k_2 be natural numbers such that

$$(3) \qquad (a_{10}, a_{20})f_1^{t_1}f_2^{k_1} = (a_{10}, a_{20})f_1^{t_2}f_2^{k_2}.$$

We show that this implies $a_0f_1^{t_1}=a_0f_1^{t_2}$, i.e., $t_1\equiv t_2 \pmod{m^n}$. The equality (3) means that

$$(4) \qquad t_1+m_ik_1 \equiv t_2+m_ik_2 \pmod{m^r} \quad (i = 1, 2),$$

whence we get $m^r|(m_1-m_2)(k_1-k_2)$. But $m^2 \nmid (m_1-m_2)$, thus $m^n|(k_1-k_2)$ because $r>n$. From this, using anyone of the congruences (4) we have $t_1\equiv t_2 \pmod{m^n}$. Thus we have shown that φ is well defined. Therefore, by definition, it is a homomorphism.

It remains to be shown that $\mathfrak{A}$ cannot be given as a homomorphic image of a subunoid of $\mathfrak{A}_1$ or $\mathfrak{A}_2$. Neither $\mathfrak{A}_1$ nor $\mathfrak{A}_2$ have any subunoid different from themself. Thus take a mapping φ_i of $\mathfrak{A}_i$ onto $\mathfrak{A}$ $(i=1, 2)$ such that $\varphi_i(a_{ij})=a_u$. If φ_i is a homomorphism then

$$\varphi_i(a_{ij}f_2) = \varphi(a_{ij}f_1^{m_i}) = a_{(u+m_i)(\mathrm{mod}\, m^n)} = a_u.$$

But $a_{(u+m_i)(\mathrm{mod}\, m^n)} \neq a_u$ because $m^n \nmid m_i$. Therefore, φ_i cannot be a homomorphism.

We now show that every elevator is homomorphically prime. Let $\mathfrak{A}_k=\langle A_k; F\rangle$ denote the elevator with

$$A_k = \langle a_0, \dots, a_k\rangle \quad (k > 0), \quad a_if_j = a_i \quad (a_i\in A_k, f_j\in F) \quad \text{if} \quad j > 1$$

and

$$a_i f_1 = \begin{cases} a_{i+1} & \text{if} \quad i < k, \\ a_k & \text{if} \quad i = k. \end{cases}$$

In the sequel by p and q with or without indices we denote polynomials in which f_1 does not occur.

Let us assume that $\mathfrak{A}_k$ can be given as a homomorphic image of a subdirect product of two unoids $\mathfrak{B}_1$ and $\mathfrak{B}_2$ under a homomorphism φ for which $\varphi((b_1, b_2)) = a_0$ $((b_1, b_2) \in B_1 \times B_2)$ holds. First we show that at least one of the unoids $\mathfrak{B}_i$ $(i=1, 2)$ has the following property P: for every p, the elements $b_i p, b_i pf_1, \dots, b_i pf_1^{k-1}$ are all different and there exists no $b_i pf_1^u$ with $u \geqq k$ which is equal to one of them. Indeed, in the opposite case there exist polynomials p_1 and p_2, non-negative integers u_1, t_1 and u_2, t_2 such that $b_1 p_1 f_1^{u_1} = b_1 p_1 f_1^{t_1}$, $b_2 p_2 f_1^{u_2} = b_2 p_2 f_1^{t_2}$; $u_1, u_2 < k$; $t_1 > u_1$ and $t_2 > u_2$. By the commutativity of $\mathfrak{B}_1$ and $\mathfrak{B}_2$, $b_1 p_1 p_2 f_1^{u_1} = b_1 p_1 p_2 f_1^{t_1}$ and $b_2 p_1 p_2 f_1^{u_2} = b_2 p_1 p_2 f_1^{t_2}$. Now let us suppose that $u_2 \geqq u_1$. Then

$$b_1 p_1 p_2 f_1^{u_2} = b_1 p_1 p_2 f_1^{u_2 + (t_1 - u_1)(t_2 - u_2)}$$

and

$$b_2 p_1 p_2 f_1^{u_2} = b_2 p_1 p_2 f_1^{u_2 + (t_1 - u_1)(t_2 - u_2)}.$$

Therefore,

$$(b_1, b_2) p_1 p_2 f_1^{u_2} = (b_1, b_2) p_1 p_2 f_1^{u_2 + (t_1 - u_1)(t_2 - u_2)}.$$

Since φ is a homomorphism thus we get

$$a_0 f_1^{u_2} = a_0 f_1^{u_2 + (t_1 - u_1)(t_2 - u_2)}$$

which is impossible.

In the sequel we write simply $\mathfrak{B}$ instead of $\mathfrak{B}_i$ having the above property and b instead of b_i. Consider the cycle (bp, f_1) in $\mathfrak{B}$ with minimal preperiod d among all cycles generated by pairs of the form (bq, f_1). Then property P implies $d \geqq k$. Take the subunoid $\mathfrak{B}'$ of $\mathfrak{B}$ generated by bp. We show that $\mathfrak{B}'$ can be mapped homomorphically onto $\mathfrak{A}_k$, namely, the mapping φ defined by $\varphi(bpqf_1^l) = a_0 f_1^l$ for all q and non-negative integer l will be such a homomorphism.

To prove that φ is well defined let us assume that $bpq_1 f_1^{l_1} = bpq_2 f_1^{l_2}$. We must have $a_0 f_1^{l_1} = a_0 f_1^{l_2}$, or, equivalently, $l_1 = l_2$ provided $l_1, l_2 \geqq k$ does not hold. Suppose $l_1 < l_2, k$. Observe that, for any q, the preperiod of the cycle (bpq, f_1) cannot be longer than d and in fact, in view of the minimum property of bp, it coincides with d. Indeed, by the commutativity of $\mathfrak{B}$, $bpf_1^u = bpf_1^v$ implies $bpqf_1^u = bpqf_1^v$. Now we distinguish two cases:

1) $l_2 < d$. If c is the length of the period of the cycle (bpq_2, f_1) then $bpq_1 f_1^{l_1 + d - l_2} = bpq_1 f_1^{l_1 + d - l_2 + c}$. But this is incompatible with property P because $l_1 + d - l_2 < d$.

2) $l_2 \geqq d$. Then we get similarly $bpq_1 f_1^{l_1} = bpq_1 f_1^{l_1+c}$, which is again a contradiction.

Finally, a short computation shows that $\varphi(bpqf_1^l)f = \varphi(bpqf_1^l f)$ holds for any $f \in F$. This completes the proof of Theorem 3.

Acknowledgements. The author is grateful to B. CSÁKÁNY for his useful comments which helped to make the paper more concise.

References

[1] F. GÉCSEG—S. SZÉKELY, On equational classes of unoids, *Acta Sci. Math.*, **34** (1973), 99—101.
[2] А. И. Мальцев, *Алгебраические системы* (Москва, 1970).
[3] M. YOELI, Subdirectly irreducible unary algebras, *Amer. Math. Monthly*, **74** (1967), 957—960.

(Received May 30, 1973)