On ν_1-products of commutative automata

By F. GÉCSEG

The aim of this paper is to show the existence of commutative automata such that each of them forms a homomorphically complete system with respect to the ν_1-product in the class of all commutative automata.

By an *automaton* we mean a system $\mathbf{A}=(X, A, \delta)$, where X is a nonvoid finite set of *input signals, A* is a nonvoid finite set of *states,* and $\delta\colon A\times X\to A$ is the *transition function.* The automaton $\mathbf{A}$ is *commutative* if $\delta(a, xy)=\delta(a, yx)$ holds for arbitrary $a\in A$ and $x, y\in X$. (The transition $\delta(a,p)$ $(a\in A, p\in X^*)$ is defined by $\delta(a, e)=a$ and $\delta(a, qx)=\delta(\delta(a, q), x)$ $(a\in A,\ q\in X^*,\ x\in X)$, where X^* is the set of all finite words over X and e denotes the empty word.)

Since automata can be considered unary algebras (cf. for instance [5]) the concept of a subautomaton of an automaton, and those of isomorphism and homomorphism of automata can be defined in a natural way.

Let $\mathbf{A}_i=(X_i, A_i, \delta_i)$ $(i=1, \ldots, k)$ be a system of automata, X a nonvoid finite set and $\varphi\colon A_1\times\ldots\times A_k\times X\to X_1\times\ldots\times X_k$ a function. Take the automaton $\mathbf{A}=(X, A, \delta)$ given by $A=A_1\times\ldots\times A_k$ and $\delta((a_1, \ldots, a_k), x)=(\delta_1(a_1, x_1), \ldots, \delta_k(a_k, x_k))$ $((a_1, \ldots, a_k)\in A, x\in X)$, where $(x_1, \ldots, x_k)=\varphi(a_1, \ldots, a_k, x)=(\varphi_1(a_1, \ldots, a_k, x), \ldots, \varphi_k(a_1, \ldots, a_k, x))$. Then $\mathbf{A}$ is called the *product* of $\mathbf{A}_1, \ldots, \mathbf{A}_k$ *with respect to* X and φ, and we denote it by

$$\prod_{i=1}^{k} \mathbf{A}_i[X, \varphi].$$

Consider the above product $\mathbf{A}$, and take a non-negative integer i. We say that $\mathbf{A}$ is an *α_i-product* if for every t $(1\leqq t\leqq k)$, φ_t is independent of its j^{th} component $(1\leqq j\leqq k)$ whenever $t\geqq j+i$. Moreover, if for all t $(=1, \ldots, k)$, $(a_1, \ldots, a_k)\in A$ and $x\in X$, $\varphi_t(a_1, \ldots, a_k, x)$ may depend on x only then $\mathbf{A}$ is a *quasi-direct product.*

Again take the product $\mathbf{A}$ above. Moreover, let $\nu\colon N_k\to\mathfrak{P}(N_k)$ be a mapping, where N_k is the set of the first k positive integers and $\mathfrak{P}$ is the powerset-operator. If i is a non-negative integer such that for every $t\in N_k$, $|\nu(t)|\leqq i$ and φ_t is independent of its j^{th} component $(1\leqq j\leqq k)$ whenever $j\notin\nu(t)$ then $\mathbf{A}$ is called a *ν_i-product* (see [1]). If $\mathbf{A}_1=\ldots=\mathbf{A}_k=\mathbf{B}$ then $\mathbf{A}$ is a *ν_i-power* of $\mathbf{B}$. Moreover, in φ_t we shall indicate only those variables on which it may depend. Finally, for the ν_i-product $\mathbf{A}$ we shall use the notation

$$\mathbf{A} = \prod_{t=1}^{k} \mathbf{A}_t[X, \varphi, \nu].$$

Let $\mathscr{K}$ be a class of automata. Then
$\mathbf{H}(\mathscr{K})$: homomorphic images of automata from $\mathscr{K}$.
$\mathbf{S}(\mathscr{K})$: subautomata of automata from $\mathscr{K}$.
$\mathbf{Q}(\mathscr{K})$: quasi-direct products of automata from $\mathscr{K}$.
$\mathbf{P}_{\nu_i}(\mathscr{K})$: ν_i-products of automata from $\mathscr{K}$.

For every prime number p consider the automata $\mathbf{A}_p=(X_p, A_p, \delta_p)$, where $X_p=\{x_0, x_1, \ldots, x_{p-1}\}$, $A_p=\{0, 1, \ldots, p-1\}$ and $\delta_p(i, x_j)=i\oplus_p j$, where $0\leqq i, j<p$ and $\oplus_p$ denotes the modulo p addition. Obviously, each $\mathbf{A}_p$ is a commutative automaton.

We are now ready to state and prove the following

Theorem. For an arbitrary commutative automaton $\mathbf{A}$ and for every prime number p the inclusion $\mathbf{A}\in\mathbf{HSP}_{\nu_1}(\{\mathbf{A}_p\})$ holds.

Proof. For every prime number p and every positive integer n take the automaton $\mathbf{B}_{(p,n)}=(X, B_{(p,n)}, \delta_{(p,n)})$ with $X=\{x, y\}$, $B_{(p,n)}=\{0, 1, \ldots, p^n-1\}$, $\delta_{(p,n)}(i, x)=i\oplus_{p^n} 1$ and $\delta_{(p,n)}(i, y)=i$ $(i=0, 1, \ldots, p^n-1)$. Moreover, for every natural number n let $\mathbf{E}_n=(\{x, y\}, \{0, 1, \ldots, n\}, \delta_n)$ be the $n+1$ state *elevator*, that is the automaton with $\delta_n(i, y)=i$ $(i=0, \ldots, n)$ and

$$\delta_n(i, x) = \begin{cases} i+1 & \text{if } 0\leqq i<n, \\ n & \text{if } i=n. \end{cases}$$

Denote by $\mathscr{K}$ the class of all $\mathbf{B}_{(p,n)}$ and $\mathbf{E}_n$. In [3] it is shown that $\mathbf{HSQ}(\mathscr{K})$ is the class of all commutative automata. Since every quasi-direct product of ν_i-products of automata is isomorphic to a ν_i-product of the same automata in order to prove our theorem it is enough to show that for arbitrary prime numbers p, q and positive integer n the inclusions $\mathbf{B}_{(q,n)}\in\mathbf{HSP}_{\nu_1}(\{\mathbf{A}_p\})$ and $\mathbf{E}_n\in\mathbf{HSP}_{\nu_1}(\{\mathbf{A}_p\})$ hold. We start with the proof of $\mathbf{B}_{(q,n)}\in\mathbf{HSP}_{\nu_1}(\{\mathbf{A}_p\})$. Let us fix p, q and n. We distinguish the following two cases.

Case 1. $p\neq q$. Then q^n divides p^m-1 for some $m>0$. (We may also assume that $m>1$.) Therefore, it is sufficient to show the existence of a ν_1-power $\mathbf{B}=(X, B, \delta)$ of $\mathbf{A}_p$ such that $\mathbf{B}$ contains a subautomaton which is a cycle of length p^m-1 under x, and y induces the identity mapping of this subautomaton.

Let $\mathbf{B}=(X, B, \delta)=(\underbrace{\mathbf{A}_p\times\ldots\times\mathbf{A}_p}_{p^m-1 \text{ times}})[X, \varphi, \nu]$ be the ν_1-product, where for every $i\in\{1, \ldots, p^m-1\}$

$$\nu(i) = \begin{cases} i-1 & \text{if } i>1, \\ p^m-1 & \text{if } i=1, \end{cases}$$

and for arbitrary $i\in\{1, \ldots, p^m-1\}$ and $j\in\{0, \ldots, p-1\}$

$$\varphi_i(j, z) = \begin{cases} x_j & \text{if } z=x, \\ x_0 & \text{if } z=y. \end{cases}$$

Take a $b=(b_1, b_2, \ldots, b_{p^m-1})$ from B. Then, by the definition of $\mathbf{B}$, we obviously have $\delta(b, x)=(b_1\oplus_p b_{p^m-1}, b_2\oplus_p b_1, \ldots, b_{p^m-1}\oplus_p b_{p^m-2})$.

In the rest of the paper all multiplications of integers, and all the binomial coefficients $\binom{k}{l}\left(=\frac{k!}{l!(k-l)!}\right)$ are taken modulo p. Moreover, $\oplus$ and $\ominus$ will stand for the modulo p addition and modulo p substraction, respectivelly. Finally, we denote p^m-1 by t.

One can easily show, by induction on k, that

$$\delta(b, x^k) = \left(\binom{k}{0} b_1 \oplus \binom{k}{1} b_t \oplus \binom{k}{2} b_{t-1} \oplus \dots \oplus \binom{k}{k} b_{t-k+1},\right.$$

$$\binom{k}{0} b_2 \oplus \binom{k}{1} b_1 \oplus \binom{k}{2} b_t \oplus \binom{k}{3} b_{t-1} \oplus \dots \oplus \binom{k}{k} b_{t-k+2}, \dots$$

$$\left. \dots, \binom{k}{0} b_t \oplus \binom{k}{1} b_{t-1} \oplus \dots \oplus \binom{k}{k} b_{t-k}\right)$$

if $1 \leqq k < t$, and

$$\delta(b, x^t) = \left(\left(\binom{t}{0} \oplus \binom{t}{t}\right) b_1 \oplus \binom{t}{1} b_t \oplus \binom{t}{2} b_{t-1} \oplus \dots \oplus \binom{t}{t-1} b_2,\right.$$

$$\left(\binom{t}{0} \oplus \binom{t}{t}\right) b_2 \oplus \binom{t}{1} b_1 \oplus \binom{t}{2} b_t \oplus \binom{t}{3} b_{t-1} \oplus \dots \oplus \binom{t}{t-1} b_3, \dots$$

$$\left. \dots, \left(\binom{t}{0} \oplus \binom{t}{t}\right) b_t \oplus \binom{t}{1} b_{t-1} \oplus \dots \oplus \binom{t}{t-1} b_1\right).$$

We would like to find a b such that $\delta(b, x^t) = b$ holds, i.e.,

$$\left(\binom{t}{0} \oplus \binom{t}{t}\right) b_1 \oplus \binom{t}{1} b_t \oplus \binom{t}{2} b_{t-1} \oplus \dots \oplus \binom{t}{t-1} b_2 = b_1,$$

$$\left(\binom{t}{0} \oplus \binom{t}{t}\right) b_2 \oplus \binom{t}{1} b_1 \oplus \binom{t}{2} b_t \oplus \dots \oplus \binom{t}{t-1} b_3 = b_2$$

(*) $\quad\vdots$

$$\left(\binom{t}{0} + \binom{t}{t}\right) b_t \oplus \binom{t}{1} b_{t-1} \oplus \binom{t}{2} b_{t-2} \oplus \dots \oplus \binom{t}{t-1} b_1 = b_t$$

holds. Let us consider (*) a system of equations over the prime field $\{0, 1, \dots, p-1\}$ with modulo p addition and modulo p multiplication, where $b_1, b_2, \dots, b_t$ are unknowns. Add (modulo p) $(p-1)b_i$ to both sides of the i^{th} equation in (*) for every i $(=1, \dots, t)$. Then we get the linear homogeneous system of equations

$$\binom{t}{0} b_1 \oplus \binom{t}{1} b_t \oplus \binom{t}{2} b_{t-1} \oplus \dots \oplus \binom{t}{t-1} b_2 = 0,$$

$$\binom{t}{0} b_2 \oplus \binom{t}{1} b_1 \oplus \binom{t}{2} b_t \oplus \dots \oplus \binom{t}{t-1} b_3 = 0,$$

(**) $\quad\vdots$

$$\binom{t}{0} b_t \oplus \binom{t}{1} b_{t-1} \oplus \binom{t}{2} b_{t-2} \oplus \dots \oplus \binom{t}{t-1} b_1 = 0.$$

Using the congruence $\binom{t+1}{l} \equiv 0 \pmod{p}$ $(1 \leqq l \leqq t)$, one can easily show that for every l $(=0, 1, \ldots, t-1)$, $\binom{t}{l} \equiv 1 \pmod{p}$ if l is even, and $\binom{t}{l} \equiv p-1 \pmod{p}$ if l is odd. (Therefore, the determinant of (**) is 0, consequently (**) has a nontrivial solution.) It can be seen immediately that $b_1=1$, $b_2=1$, $b_3=0, \ldots, b_t=0$ is a solution of (**). Moreover, by the construction of **B**, the states $b, \delta(b, x), \ldots, \delta(b, x^{t-1})$ are pairwise distinct, that is they form a cycle of length t $(=p^m-1)$ under x.

Case 2. $p=q$. We now show the existence of a ν_1-power $\mathbf{B}=(X, B, \delta)$ of $\mathbf{A}_p$ such that **B** contains a subautomaton which is a cycle of length p^n under x, and y induces the identity mapping on this subautomaton.

Let $\mathbf{B}=(X, B, \delta)=(\underbrace{\mathbf{A}_p \times \ldots \times \mathbf{A}_p}_{p^n \text{ times}})[X, \varphi, \nu]$ be the ν_1-product given in the following way. For every $i \in \{1, \ldots, p^n\}$

$$\nu(i) = \begin{cases} i-1 & \text{if } i > 1, \\ \emptyset & \text{if } i = 1, \end{cases}$$

and for arbitrary $i \in \{2, \ldots, p^n\}$ and $j \in \{0, \ldots, p-1\}$

$$\varphi_i(j, z) = \begin{cases} x_j & \text{if } z = x, \\ x_0 & \text{if } z = y, \end{cases}$$

moreover, $\varphi_1(x)=\varphi_1(y)=x_0$.

Take the state $b=(1, 0, \ldots, 0)$ of **B**. One can prove easily, by induction on k, that for every k $(=1, \ldots, p^n-1)$

$$\delta(b, x^k) = \left(\binom{k}{0}, \binom{k}{1}, \ldots, \binom{k}{k}, 0, \ldots, 0\right).$$

Therefore

$$\delta(b, x^{p^n}) = \left(\binom{p^n}{0}, \binom{p^n}{1}, \ldots, \binom{p^n}{p^n-1}\right).$$

As it has been noted, for every k $(=1, \ldots, p^n-1)$, $\binom{p^n}{k} \equiv 0 \pmod{p}$. Thus $\delta(b, x^{p^n})=b$ showing that the states $b, \delta(b, x), \ldots, \delta(b, x^{p^n-1})$ form a desired cycle.

To prove that for arbitrary natural number n and prime number p the inclusion $\mathbf{E}_n \in \mathbf{HSP}_{\nu_1}(\{\mathbf{A}_p\})$ holds take the automaton

$$\mathbf{B} = (X, B, \delta) = (\underbrace{\mathbf{A}_p \times \ldots \times \mathbf{A}_p}_{p^n \text{ times}})[X, \varphi, \nu]$$

defined in the same way as in Case 2 with the following exceptions: $\nu(1)=p^n$ and $\varphi_1(j, x)=x_p \ominus_j$ $(j=0, \ldots, p-1)$. Again take $b=(1, 0, \ldots, 0)$. Then, like in Case 2, for every k $(=1, \ldots, p^n-1)$

$$\delta(b, x^k) = \left(\binom{k}{0}, \binom{k}{1}, \ldots, \binom{k}{k}, 0, \ldots, 0\right).$$

Therefore

$$\delta(b, x^{p^n}) = (0, 0, \ldots, 0)$$

showing that the states $b, \delta(b, x), \ldots, \delta(b, x^{p^n})$ form a p^n+1 state elevator. Since $p^n > n$ this ends the proof of the Theorem.

Remark. It follows from Theorem 3 in [4] that there exists no finite system of automata which is homomorphically complete with respect to the α_1-product in the class of all commutative automata. Thus, by the Theorem above, in this respect the ν_1-product is more powerful than the α_1-product. (By the Theorem in [2], the ν_1-product is not stronger than any of the α_i-products if $i > 1$.)

Acknowledgements

The author wants to thank Dr. B. Imreh for detecting a gap in the first version of the proof of the Theorem.

DEPT. OF COMPUTER SCIENCE
A. JÓZSEF UNIVERSITY
ARADI VÉRTANÚK TERE 1.
SZEGED, HUNGARY
H-6720

References

[1] Dömösi, P., Imreh, B., On ν_i-products of automata, Acta Cybernet., v. VI. 2, 1983, pp. 149—162.
[2] Ésik, Z., Horváth, Gy., The α_2-product is homomorphically general, Papers on Automata Theory, v. V. 1983, pp. 49—62.
[3] Gécseg, F., On subdirect representations of finite commutative unoids, Acta Sci. Math. (Szeged), v. 36, 1974, pp. 33—38.
[4] Gécseg, F., On products of abstract automata, Acta Sci. Math. (Szeged), v. 38, 1976, pp. 21—43.
[5] Gécseg, F., Steinby, M., Tree automata, Akadémiai Kiadó, Budapest, 1984.

(Received Febr. 1, 1984)