On minimal and maximal clones II

László Szabó *†

Abstract

Two minimal clones which generate all operations, and two maximal clones with trivial intersection are given on $2p$–element sets where $p \geq 5$ is a prime number.

1 Introduction

Let A be a fixed universe with $|A| \geq 2$ and let $\mathbf{O}_A$ denote the set of all finitary operations on A. For $1 \leq i \leq n$ let e_i^n denote the n-ary i-th projection (trivial operation). Further let $\mathbf{J}_A = \{e_i^n | 1 \leq i \leq n < \infty\}$. The operations in $\mathbf{O}_A \setminus \mathbf{J}_A$ are called *nontrivial operations.* By a *clone* we mean a subset of $\mathbf{O}_A$ which is closed under superpositions and contains all projections. The set of clones, ordered by inclusion, forms an algebraic lattice $\mathbf{L}_A$ with least element $\mathbf{J}_A$ and greatest element $\mathbf{O}_A$. For A finite $\mathbf{L}_A$ is an atomic and dually atomic lattice with finitely many atoms and coatoms. The atoms and the coatoms of $\mathbf{L}_A$ are called *minimal clones* and *maximal clones*, respectively.

In [4] we showed that for an at least three element finite set A there are three maximal clones with intersection $\mathbf{J}_A$, and there are three minimal clones with join $\mathbf{O}_A$. If $|A|$ is a prime number then there are two maximal clones and two minimal clones with the above properties. Moreover, we formulated the following two problems:

Problem 1 *Find all natural numbers k for which there exist two maximal clones on a k-element set A such that their intersection is $\mathbf{J}_A$.*

Problem 2 *Find all natural numbers k for which there exist two minimal clones on a k-element set A such that their join is $\mathbf{O}_A$.*

This short note is a modest step to answer these problems. Namely, we give two maximal clones with intersection $\mathbf{J}_A$ and two minimal clones with join $\mathbf{O}_A$ on a $2p$-element set A where p is a prime number with $p \geq 5$.

*Research partially supported by Hungarian National Foundation for Scientific Research grants no. OTKA T022876, OTKA T026243 and Scientific Research grant of the Hungarian Education Ministry no. FKFP 0877/1997.

†Bolyai Institute, H-6720 Szeged, Aradi vértanúk tere 1, Hungary

2 Results

We need some more notions. A ternary operation f on A is a *majority operation* if for all $x, y \in A$ we have $f(x,x,y) = f(x,y,x) = f(y,x,x) = x$; f is a *Mal'cev operation* if $f(x,y,y) = f(y,y,x) = x$ for all $x, y \in A$. An n-ary operation t on A is said to be an i-th *semi-projection* ($n \geq 3$, $1 \leq i \leq n$) if for all $x_1, \ldots, x_n \in A$ we have $t(x_1, \ldots, x_n) = x_i$ whenever at least two elements among $x_1, \ldots, x_n$ are equal.

For a finitary relation ρ on A the set of operations preserving ρ forms a clone, and is denoted by $\operatorname{Pol}\rho$.

Theorem 1 *Let $A = \{0, 1, \ldots, 2p-1\}$ where p is a prime number with $p \geq 5$ and put $C = \{0, 1, p, p+2\}$. Let us define a binary relation ρ and a permutation π on A as follows:*

$$\rho = \{(a,a): a \in A\} \cup (C \times A) \cup (A \times C)$$

and

$$\pi = (0\ 1\ \ldots\ p-1)(p\ p+1\ \ldots\ 2p-1).$$

Then $\operatorname{Pol}\rho$ and $\operatorname{Pol}\pi$ are maximal clones and $\operatorname{Pol}\rho \cap \operatorname{Pol}\pi = \operatorname{Pol}\{\rho, \pi\} = \mathbf{J}_A$.

Proof: Taking into consideration the list of maximal clones given by I. G. Rosenberg (see e.g. [3]) we have that $\operatorname{Pol}\rho$ and $\operatorname{Pol}\pi$ are maximal clones. We need the following fact which follows immediately from the definitions of C and π: (*)

For any $x, y \in A$, $x \neq y$, there is a $k \in \{0, \ldots, p-1\}$ such that $x\pi^k \in C$ and $y\pi^k \notin C$. First we establish some properties of the operations in $\operatorname{Pol}\{\rho, \pi\}$. Let

$f \in \operatorname{Pol}\{\rho, \pi\}$ be an arbitrary n-ary operation, $n \geq 1$.

Claim 1 $f(A^n) \supseteq \{0, 1 \ldots, p-1\}$ *or* $f(A^n) \supseteq \{p, p+1 \ldots, 2p-1\}$.

This claim follows immediately from the fact that $f \in \operatorname{Pol}\pi$.

Claim 2 $f(C^n) \subseteq C$.

Let $c_1, \ldots, c_n \in C$. By Claim 1, there are $a_1, \ldots, a_n \in A$ such that

$$f(a_1, \ldots, a_n) \notin C \cup \{f(c_1, \ldots, c_n)\}.$$

Then $(c_1, a_1), \ldots, (c_n, a_n) \in \rho$, and therefore $(f(c_1, \ldots, c_n), f(a_1 \ldots, a_n)) \in \rho$. From this, taking into consideration the definition of ρ, it follows that $f(c_1, \ldots, c_n) \in C$.

Claim 3 *f is an idempotent operation.*

Consider the unary operation $g(x) = f(x, \ldots, x)$. If $g(0) = 0$ and $g(p) = p$ then $g(x) = x$ for all $x \in A$ and f is an idempotent operation. Indeed, in this case for $k = 0, \ldots, p-1$ we get that

$$g(k) = g(0\pi^k) = g(0)\pi^k = 0\pi^k = k$$

and

$$g(p+k) = g(p\pi^k) = g(p)\pi^k = p\pi^k = p+k.$$

Therefore we have to show that $g(0) = 0$ and $g(p) = p$. By Claim 2,

$$g(0), g(1) \in C = \{0, 1, p, p+2\}.$$

It follows that

$$g(0) = g(1\pi^{-1}) = g(1)\pi^{-1} \in C\pi^{-1} = \{p-1, 0, 2p-1, p+1\}$$

and $g(0) = 0$. Similarly,

$$g(p), g(p+2) \in C = \{0, 1, p, p+2\}$$

implies that

$$g(p) = g((p+2)\pi^{-2}) = g(p+2)\pi^{-2} \in C\pi^{-2} = \{p-2, p-1, 2p-2, p\}$$

and $g(p) = p$, completing the proof of Claim 3.

Claim 4 *If f is binary then $f(x, y) \in \{x, y\}$ for all $x, y \in A$.*

Let f be binary and suppose that $f(a, b) = c \notin \{a, b\}$ for some $a, b \in A$. Then, by (*), $a\pi^k \in C$ and $c\pi^k \notin C$ for some k. Put $u = a\pi^k$, $w = c\pi^k$ and $v = b\pi^k$. Then

$$f(u, v) = f(a\pi^k, b\pi^k) = f(a, b)\pi^k = c\pi^k = w \notin C,$$

and therefore, by Claim 2, we have that $v \notin C$. Now $c \neq b$, $(u, v), (v, v) \in \rho$ imply that $w \neq v$ and $(w, v) = (f(u, v), f(v, v)) \in \rho$ which is not valid.

Claim 5 *If f is binary then the restrictions of f to $\{0, 1, \ldots, p-1\}$ and to $\{p, p+1 \ldots, 2p-1\}$ are projections.*

By Claim 4, $f(0, 1) \in \{0, 1\}$, and without loss of generality we can suppose that $f(0, 1) = 0$. Then

$$f(p-1, 0) = f(0\pi^{-1}, 1\pi^{-1}) = f(0, 1)\pi^{-1} = 0\pi^{-1} = p-1$$

and

$$f(p-2, p-1) = f(0\pi^{-2}, 1\pi^{-2}) = f(0, 1)\pi^{-2} = 0\pi^{-2} = p-2.$$

Let $i \in \{2, \ldots, p-2\}$. From

$$(p-1, 0), (0, i) \in \rho, \ (p-1, i) \notin \rho \ \text{ and } \ f(0, i) \in \{0, i\}$$

it follows that

$$(p-1, f(0,i)) = (f(p-1,0), f(0,i)) \in \rho \quad \text{and} \quad f(0,i) = 0.$$

Similarly, from

$$(p-2,0), (p-1,p-1) \in \rho, \ (p-2,p-1) \notin \rho \quad \text{and} \quad f(0,p-1) \in \{0,p-1\}$$

it follows that

$$(p-2, f(0,p-1)) = (f(p-2,p-1), f(0,p-1)) \in \rho \quad \text{and} \quad f(0,p-1) = 0.$$

Hence for any $x \in \{0,1,\ldots,p-1\}$ we have that $f(0,x) = 0$, which together with the fact that $f \in \operatorname{Pol}\pi$ imply that the restriction of f to $\{0,1,\ldots,p-1\}$ is the first projection. One can show by a very similar argument that the restriction of f to $\{p,p+1,\ldots,2p-1\}$ is also projection.

Claim 6 *If f is binary then f is a projection.*

Taking into consideration Claim 5, we can suppose without loss of generality that the restriction of f to $\{0,1,\ldots,p-1\}$ is the first projection. First we show that the restriction of f to $\{p,p+1,\ldots,2p-1\}$ is also the first projection. In deed, if the restriction of f to $\{p,p+1,\ldots,2p-1\}$ is the second projection then from $(2,p),(0,p+1) \in \rho$ we obtain that $(2,p+1) = (f(2,0), f(p,p+1)) \in \rho$ which is not valid.

If f is not the first projection then for some $a \in \{0,1,\ldots,p-1\}$ and $b \in \{p,p+1,\ldots,2p-1\}$ we have that $f(a,b) = b$ or $f(b,a) = a$. If $f(a,b) = b$ then choose a positive integer k such that $a\pi^k \in C$ and $v = b\pi^k \notin C$. Put $u = a\pi^k$ and $v = b\pi^k$. Now

$$f(u,v) = f(a\pi^k, b\pi^k) = f(a,b)\pi^k = b\pi^k = v \notin C.$$

Since $(2,u),(0,v) \in \rho$ and $2 \neq v$ (because of $v = b\pi^k \in \{p,p+1,\ldots,2p-1\}$) it follows that $(2,v) = (f(2,0), f(u,v)) \in \rho$ which is not valid.

If $f(b,a) = a$ then choose a positive integer k such that $a\pi^k \notin C$ and $v = b\pi^k \in C$. Put $u = a\pi^k$ and $v = b\pi^k$. Now

$$f(v,u) = f(b\pi^k, a\pi^k) = f(b,a)\pi^k = a\pi^k = u \notin C.$$

Since $(p+1,v),(p,u) \in \rho$ and $p+1 \neq u$ (because of $u = a\pi^k \in \{0,1,\ldots,p-1\}$) it follows that $(p+1,u) = (f(p+1,p), f(v,u)) \in \rho$ which is not valid. Hence f is the first projection.

Claim 7 *f cannot be a Mal'cev operation.*

Indeed, if f is a Mal'cev operation, then $(2,0),(0,0),(0,3) \in \rho$ implies that $(2,3) = (f(2,0,0), f(0,0,3)) \in \rho$ which is not valid.

Claim 8 *f cannot be a nontrivial semi-projection.*

Let f be a nontrivial n-ary semi-projection ($n \geq 3$). We can suppose that f is a first semi-projection. Observe that $f(c, a_2 \ldots, a_n) \in C$ for any $c \in C$ and $a_2, \ldots, a_n \in A$. Indeed, if $c \in C$ and $a_2, \ldots, a_n \in A$ then for any $a \in A$ we have $(c, a), (a_2, c), \ldots, (a_n, c) \in \rho$ which implies that

$$(f(c, a_2 \ldots, a_n), a) = (f(c, a_2, \ldots, a_n), f(a, c, \ldots, c)) \in \rho$$

and $f(c, a_2 \ldots, a_n) \in C$. Since f is not the first projection $f(a_1, \ldots, a_n) = a \neq a_1$ for some $a_1, \ldots, a_n \in A$. Then, by (*), $a_1\pi^k \in C$ and $a\pi^k \notin C$ for some k. It follows that

$$f(a_1\pi^k, \ldots, a_n\pi^k) = f(a_1, \ldots, a_n)\pi^k = a\pi^k,$$

a contradiction.

Claim 9 *f cannot be a majority operation.*

Let f be a majority operation. First observe that $f(a, b, c) \in C$ if at least two elements among a, b, c belong to C. Indeed, if e.g. $a, b \in C$ then for any $x \in A$ from $(a, x), (b, x), (x, 0) \in \rho$ it follows that

$$(f(a, b, c), x) = (f(a, b, c), f(x, x, 0)) in \rho$$

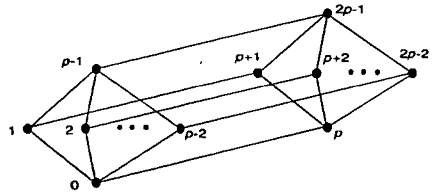
which implies that $f(a, b, c) \in C$.

Now let $a, b, c \in A$ be pairwise distinct elements. Clearly, $f(a, b, c)$ is different from at least two of the elements a, b, c, say from a and b. Then, by (*), for some k we have $u = a\pi^k \in C$ and $t = f(a, b, c)\pi^k \notin C$. Put $v = b\pi^k$ and $w = c\pi^k$. Thus

$$f(u, v, w) = f(a\pi^k, b\pi^k, c\pi^k) = f(a, b, c)\pi^k = t$$

and, taking into consideration the above observation, we have that $v \notin C$. Since $f(a, b, c) \neq b$, therefore $v \neq t$ and $(v, t) \notin \rho$. On the other hand $(v, u), (v, v), (0, w) \in \rho$ implies that $(v, t) = (f(v, v, 0), f(u, v, w)) \in \rho$. This contradiction implies that f cannot be a majority operation. Now we are in a position to complete the proof of the theorem. If $\mathrm{Pol}\{\rho, \pi\} \neq \mathbf{J}_A$ then there is a nontrivial operation in $\mathrm{Pol}\{\rho, \pi\}$ which is either a unary operation or an idempotent binary operation or a majority operation or a Mal'cev operation or a semi-projection (see e.g. [4]). Since , by Claims 3, 6, 7, 8 and 9, these cases cannot occur we have that $\mathrm{Pol}\{\rho, \pi\} = \mathbf{J}_A$. □

Theorem 2 *Let $A = \{0, 1, \ldots, 2p-1\}$ where p is a prime number with $p \geq 5$ and let $(A; \vee, \wedge)$ be the lattice given by the following diagram:*



Let us define a ternary operation d and a permutation π on A as follows:

$$d(x,y,z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$$

and

$$\pi = (0\ 1\ p+2\ \ldots\ 2p-2\ 2p-1)(p+1\ p\ 2\ \ldots\ p-2\ p-1).$$

Then d and π generate minimal clones such that the clone generated by d and π is $\mathbf{O}_A$.

Proof: Suppose that A, p, d and π satisfy the hypotheses of the theorem. Then it is known that π and d generate minimal clones, respectively (see e.g. [2]). We have to show that $\mathbf{A} = (A; d, \pi)$ is a primal algebra, i.e., every operation on A is a term operation of $\mathbf{A}$.

First observe that $\mathbf{A}$ has no proper subalgebra. Indeed, the proper subalgebras of $(A;\pi)$ are $\{0, 1, p+2, \ldots, 2p-2, 2p-1\}$ and $\{p, p+1, 2, \ldots, p-2, p-1\}$ only. Furthermore,

$$d(p+2, p+3, p+4) = p \notin \{0, 1, p+2, \ldots, 2p-2, 2p-1\}$$

and

$$d(2,3,4) = 0 \notin \{p, p+1, 2, \ldots, p-2, p-1\}.$$

Since $d(x,y,0) = x \wedge y$ and $d(x,y,2p-1) = x \vee y$ for any $x, y \in A$, therefore the congruence relations of $\mathbf{A}$ and $(A; \vee, \wedge, \pi)$ are the same. One can check easily that $(A; \vee, \wedge)$ has two nontrivial congruence relations only. One of them has two blocks

$$B = \{0, 1, \ldots, p-1\} \quad \text{and} \quad C = \{p, p+1, \ldots, 2p-1\},$$

and the blocks of the other are

$$\{k, p+k\},\ k = 0, \ldots, p-1.$$

It is easy to check that π does not preserve these two equivalence relations. Hence we have that $\mathbf{A}$ is a simple algebra.

Next we show that the identity map is the only automorphism of $\mathbf{A}$. To show this let τ be an automorphism of $\mathbf{A}$. Since τ is also an automorphism of the algebra $(A;d)$, for any $\Theta \in \mathrm{Con}\,(A;d) = \mathrm{Con}\,(A;\vee,\wedge)$ we have that $\Theta\tau \in \mathrm{Con}\,(A;d)$. It follows that either $B\tau = B$ or $B\tau = C$. Hence $\tau|_B$ is either an automorphism of $(B;d)$ or an i somorphism between $(B;d)$ and $(C;d)$. For any $x \in B\tau$ we have that

$$d(x, 0\tau, (p-1)\tau) = d(x\tau^{-1}, 0, p-1)\tau = (x\tau^{-1})\tau = x.$$

Using this fact it is easy to show that either $\{0\tau, (p-1)\tau\} = \{0, p-1\}$ or $\{0\tau, (p-1)\tau\} = \{p, 2p-1\}$. If $0\tau = p-1$ then

$$1\tau = (0\pi)\tau = 0(\pi\tau) = 0(\tau\pi) = (0\tau)\pi = (p-1)\pi = p+1 \quad \text{and} \quad B\tau \neq B, C.$$

If $0\tau = p$ then

$$1\tau = (0\pi)\tau = 0(\pi\tau) = 0(\tau\pi) = (0\tau)\pi = p\pi = 2 \quad \text{and} \quad B\tau \neq B, C.$$

If $0\tau = 2p-1$ then

$$1\tau = (0\pi)\tau = 0(\pi\tau) = 0(\tau\pi) = (0\tau)\pi = (2p-1)\pi = 0 \quad \text{and} \quad B\tau \neq B, C.$$

Taking into consideration that $B\tau = B$ or $B\tau = C$, it follows that $0\tau = 0$. Since the set of fixed points of τ is a subalgebra of $\mathbf{A}$ therefore τ is the identity map.

No we are in a position to complete the proof. By [5], every finite, simple, surjective algebra without proper subalgebra is either quasiprimal or affine or term equivalent to a matrix power of a unary algebra. Since affine algebras and matrix powers of unary algebras cannot have majority term operations and d is a majority operation, we obtain that $\mathbf{A}$ is quasiprimal (i.e. every operation on A admitting all isomorphisms beetwen subalgebras of $\mathbf{A}$ is a term operation of $\mathbf{A}$). Taking into consideration that $\mathbf{A}$ has no proper subalgebras and nontrivial automorphisms, it follows that $\mathbf{A}$ is a primal algebra. □

References

[1] P. P. Pálfy, L. Szabó and Á. Szendrei, Automorphism groups and functional completeness, *Algebra Universalis* **15** (1982), 385-400.

[2] R. Pöschel and L. A. Kalužnin, *Funktionen- und Relationenalgebren*, VEB Deutscher Verlag d. Wissenschaften, Berlin, 1979.

[3] I. G. Rosenberg, Completeness properties of multiple-valued logic algebras, in: *Computer Science and Multiple-Valued Logic, Theory and Applications* (ed. D. C. Rine), North-Holland (1977); pp. 144-186.

[4] L. Szabó, On minimal and maximal clones, *Acta Cybernetica* **10** (1992), 323–327.

[5] Á. Szendrei, Simple surjective algebras having no proper subalgebras, *J. Austral. Math. Soc.* **48** (1990), 434–454.

Received March, 1998