Two minimal clones whose join is gigantic

Gábor Czédli

JATE Bolyai Institute, Szeged, Aradi vértanúk tere 1, HUNGARY–6720.
E-mail: czedli@math.u-szeged.hu

Key words: clone, minimal clone, majority operation, lattice.
Mathematics Subject Classification: 08A40

Abstract. Let A be a finite set such that the greatest prime divisor of $|A|$ is at least 5. Then two minimal clones are constructed on A such that their join contains all operations.

This research was partially supported by the NFSR of Hungary (OTKA), grant no. T023186, T022867 and T026243, and also by the Hungarian Ministry of Education, grant no. FKFP 1259/1997.

Given a finite set A with at least two elements, the clones on A form an atomic algebraic lattice $\mathbf{L}_A$. The atoms of $\mathbf{L}_A$ are called minimal clones. Szabó [5] raised the question that what is the minimal number $n = n(|A|)$ such that the greatest element $\mathbf{1}_A$ of $\mathbf{L}_A$ is the join of n atoms. In other words, how many minimal clones are necessary to generate the clone of all operations on A? He proved $2 \leq n(|A|) \leq 3$ and $n(p) = 2$ for p prime, cf. [5]. Later in [6] he also showed $n(2p) = 2$ for primes $p \geq 5$. Our goal is not only to extend these results but also to simplify the proof in [6] for the $2p$ case. Many of Szabó's ideas from [5] and [6] will be used in the present paper.

Theorem 1. *Let A be a finite set, and let p divide the number of elements of A for some prime $p \geq 5$. Then there exist two minimal clones on A whose join contains all operations on A.*

The proof relies on the following lemma.

Lemma 2. *Let $|A| = pk$ for a prime $p \geq 5$ and an integer $k \geq 2$. Then there are a lattice structure $(A, \vee, \wedge)$ and a fixed point free permutation $g : A \to A$ of order p such that, with the notation m for the ternary majority operation $m : A^3 \to A$, $(x, y, z) \mapsto (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$, the algebra $\mathcal{A} = (A, m, g)$ is simple, it has no proper subalgebra and it has no nontrivial automorphism.*

Proof of Lemma 2. Let $A = \{0 = a_{0,1},\ 1 = a_{k+1,p},\ a_{1,1}, \ldots, a_{1,p-1},\ a_{2,1}, \ldots, a_{2,p-1},\ a_{3,1}, \ldots, a_{3,p},\ \ldots,\ a_{k,1}, \ldots, a_{k,p}\}$. Consider the lattice structure $(A, \vee, \wedge)$ on A as depicted in Figure 1. (Notice that this lattice is a Hall–Dilworth gluing of k modular nondistributive lattices of length 2.)

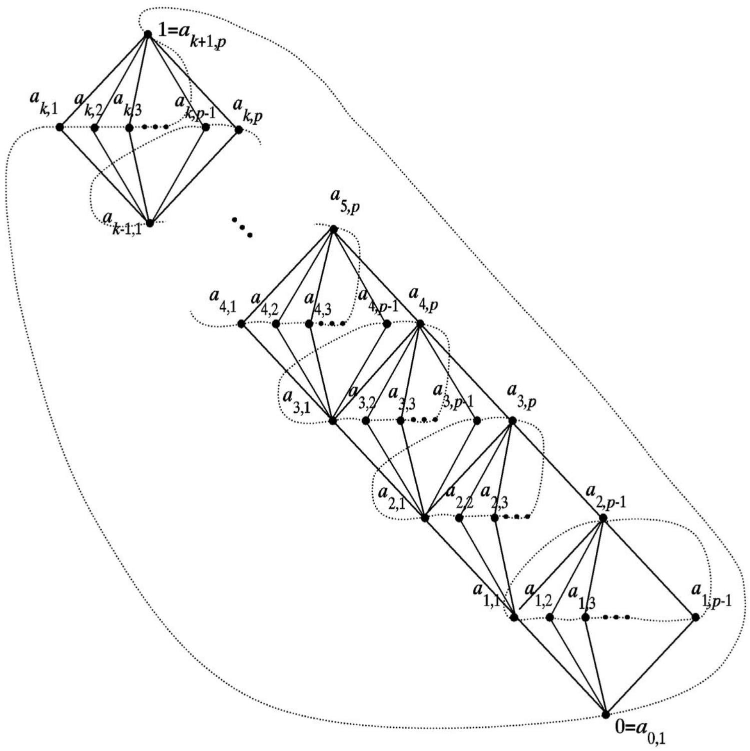

Figure 1

Let g be the following permutation:

$$(0a_{k,1}a_{k,2}\dots a_{k,p-2}1)(a_{1,1}\dots a_{1,p-1}a_{2,p-1})\times$$
$$(a_{2,1}\dots a_{2,p-2}a_{3,p}a_{3,p-1})(a_{3,1}\dots a_{3,p-2}a_{4,p}a_{4,p-1})\times$$
$$(a_{4,1}\dots a_{4,p-2}a_{5,p}a_{5,p-1})\dots(a_{k-1,1}\dots a_{k-1,p-2}a_{k,p}a_{k,p-1}).$$

In Figure 1 the g-orbits are indicated by dotted lines.

Now if Θ is a congruence of $\mathcal{A}$ then $x \wedge y = m(x,y,0)$ and $x \vee y = m(x,y,1)$ preserve Θ, so Θ is a lattice congruence as well. But our lattice is simple, whence so is $\mathcal{A}$.

Now let S be a subalgebra of $\mathcal{A}$, Clearly, S is the union of some g-orbits. From $m(a_{i,1}, a_{i,2}, a_{i,3}) = a_{i-1,1}$ $(1 \le i \le k)$ we infer that if S includes the g-orbit of $a_{i,1}$ then it includes the g-orbit of $a_{i-1,1}$. Since $a_{k,1}$ and $a_{0,1} = 0$ belong to the same orbit, S includes all orbits. This shows that $\mathcal{A}$ has no proper subalgebra.

An element $x \in A$ is called m-irreducible if $A \setminus \{x\}$ is closed with respect to m. Using the monotonicity of m we easily conclude that 1 is m-irreducible. The doubly (i.e., both meet and join) irreducible elements are m-irreducible as well. The computational rules

$$\begin{aligned} &m(a_{i1}, a_{i,2}, a_{i,3}) = a_{i-1,0} \qquad (1 \le i \le k),\\ &m(a_{1,1}, a_{1,2}, 1) = a_{2,p-1},\\ &m(a_{j-1,1}, a_{j-1,2}, 1) = a_{j,p} \qquad (3 \le j \le k) \end{aligned}$$

imply that the rest of elements are m-reducible. Now 0 is the only m-reducible element with the property that all other elements in its g-orbit are m-irreducible. Hence 0 is a fixed point of every automorphism τ of $\mathcal{A}$. Since the set of fixed points of τ is either empty or a subalgebra, all elements are fixed points and τ is the identity map of A. Hence $\mathcal{A}$ has no nontrivial automorphism. This proves Lemma 2. ⋄

The transition from Lemma 2 to Theorem 1 is essentially the same as that in Szabó [6].

Proof of Theorem 1. Since the case when $|A|$ is a prime is settled in [5], we can assume that $|A| = kp$ for $k \ge 2$ and $p \ge 5$. The clone $[m]$ generated by m (in case of any lattice) is known to be a minimal one, cf. e.g. Kalouznin and Pöschel [3, page 115, 4.4.5.(ii)]. Clearly, the permutation g also generates a minimal clone. To prove that $[m] \vee [g] = \mathbf{1}_A$ it suffices to show that no relation from the six types in the famous Rosenberg Theorem [4] is preserved both by m and g. (Note that Rosenberg Theorem is cited in [2] as Thm. A.) Since m is a majority operation, it does not preserve linear relations and h-regular relations by [2, Lemma 6]. It is easy to check that if a central relation is preserved by m and g then its centrum elements form a subalgebra of $\mathcal{A}$. So the lack of proper subalgebras excludes central relations. Since the simplicity of $\mathcal{A}$ and the lack of nontrivial automorphisms obviously exclude two further kinds of Rosenberg's relations, we are left with the case of a bounded partial order $\rho \subseteq A^2$ preserved by m and g. If u is the smallest element with respect to ρ then $(u, g(u)) \in \rho$ gives $(g^{p-1}(u), g^p(u)) = (g^{p-1}(u), u) \in \rho$, which contradicts $g^{p-1}(u) \neq u$. (Alternatively, $x \wedge y = m(x, y, 0)$ and $x \vee y = m(x, y, 1)$ also preserve ρ. Since $(A, \vee, \wedge)$ is a simple lattice, ρ is the original lattice order or its dual by [1, Cor. 1], so ρ is evidently not preserved by g.) This proves Theorem 1. ⋄

Concluding remarks. While we do not know if $n(|A|) = 2$ holds for all finite sets A with at least two elements, Lemma 2 surely fails when $|A| = 2^k$, $k > 1$. (Indeed, then $\{0, g(0)\}$ is a proper subalgebra.) The case when 3 is the greatest prime divisor of $|A| > 3$ is less clear. All we know at present is that Lemma 2 fails for $|A| = 6$ but holds for $|A| \in \{9, 12, 18\}$. For example, the lattice we used for $|A| = 18$ is given in Figure 2, the corresponding permutation g is

$$(0, 16, 15)(1, 4, 5)(2, 3, 9)(6, 7, 14)(8, 10, 17)(11, 12, 13),$$

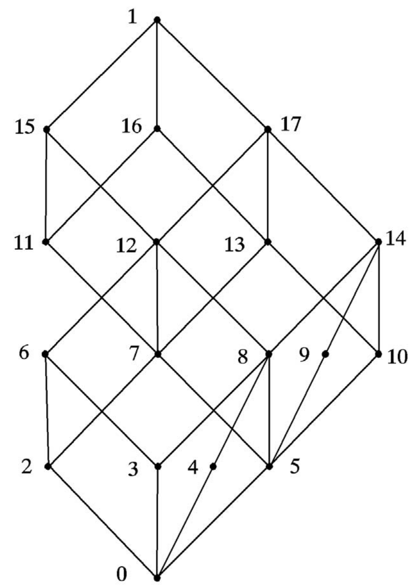

Figure 2

and the reasoning is considerably longer than in the proof of Lemma 2. Unfortunately, the particular arguments for 9, 12 and 18 have not given a clue to more generality.

References

[1] G. Czédli and L. Szabó , Quasiorders of lattices versus pairs of congruences , Acta Sci. Math. (Szeged) , 60 , 1995 , 207–211 .

[2] P. P. Pálfy, L. Szabó and Á. Szendrei , Automorphism groups and functional completeness , Algebra Universalis , 15 , 1982 , 385–400 .

[3] R. Pöschel and L. A. Kalouznin , Functionen- und Relationenalgebren , VEB Deutscher Verlag d. Wissenschaften , Berlin , 1979 .

[4] I. G. Rosenberg , La structure des fonctions de plusiers variables sur un ensemble fini , C. R. Acad. Sci. Paris, Ser. A. B. , 260 , 1965 , 3817–3819 .

[5] L. Szabó , On minimal and maximal clones , Acta Cybernetica , 10 , 1992 , 322–327 .

[6] L. Szabó , On minimal and maximal clones II , Acta Cybernetica , submitted .