Polynomial clones containing the Mal'tsev operation of the groups $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$

Andrei A. Bulatov

Abstract. We give a complete description of clones that contain all the constant operations and the Mal'tsev operation of either the group $\mathbb{Z}_{p^2}$, or the group $\mathbb{Z}_p^2$. This description relies heavily on the structure of possible congruence lattices of corresponding algebras from the point of view of commutator theory and tame congruence theory.

AMS Mathematics Subject Classification: 08A40, 03B50.

1 Introduction

A set of operations on a finite set A is called a *clone* if it closed under superposition and contains all projection operations. In the case when A is a two-element set, a complete description of all clones on A was given by E.L.Post in [22]. When A has more than two elements there are uncountably many clones on A (see Ju.J.Yanov and A.A.Muchnik [31] or A.Hulanicki and S.Świerczkowski [11]). This fact leaves no hope for a good classification of clones in this case. Nevertheless, it is possible to study clones of restricted types, which are interesting from a practical or theoretical perspective.

In this paper we study those clones which, firstly, contain all the constant operations (we call such clones *polynomial*), and, secondly, contain the Mal'tsev operation of the group $\mathbb{Z}_{p^2}$ of integers modulo p^2, or of the group $\mathbb{Z}_p \times \mathbb{Z}_p$, p prime. A ternary operation $d(x, y, z)$ satisfying $d(x, x, y) = y = d(y, x, x)$ is called a *Mal'tsev operation.* The only Mal'tsev operations of those groups are $d(x, y, z) = x - y + z$ and $d'(x, y, z) = x \ominus y \oplus z$ respectively where $+, -$ and $\oplus, \ominus$ denote addition and subtraction of the groups. More precisely, we will assume that a set A of cardinality p^2 is endowed with the structure of $\mathbb{Z}_{p^2}$ (or $\mathbb{Z}_p^2$) in some way.

Clones connected with groups of integers are one of oldest and most classical objects of study in clone theory. Clones of polynomials of $\mathbb{Z}_n$ were studied in a number of papers of A. Salomaa, Á. Szendrei, D. Lau, A. Bulatov [25, 26, 27, 28, 17, 16, 2, 3]. Another series of papers investigates polynomials of the ring $\mathbb{Z}_n^\times$ of integers modulo n. Let Pol_n denote the clone of polynomials of $\mathbb{Z}_n^\times$, and $\mathbf{M}_n$ the clone of all operations preserving all congruences of $\mathbb{Z}_n^\times$. For the case when k is free of cubes, the interval $[\mathrm{Pol}_n, \mathbf{M}_n]$ was described in [23, 19]. It was shown in [23] that this interval is infinite if $k = p^3$. If k is free of squares the lattice of clones containing Pol_n was completely described in [29, 30]. Note that this description can be easily derived from results on arithmetical algebras [21]. G. Gavrilov [7, 8] exhibited some finite family of clones from $[\mathrm{Pol}_n, \mathbf{M}_n]$ for an arbitrary n. Furthermore, a complete description of the subclones of Pol_4 that contain d and all the constant operations was given in [15]. Finally, [18, 5, 24] give a description of clones containing the Mal'tsev operation $x - y + z$ of the group $\mathbb{Z}_p$ for $p = 3$, $p = 5$, p odd prime, respectively. This description can also be derived from the results of [20]. These papers provide a description of not only polynomial but all such clones.

Studying clones containing Mal'tsev operations d, d' is also motivated by progress in investigating Mal'tsev algebras [12, 4]. Algebras with the same universe are said to be *term* [*polynomially*] *equivalent* if they have the same clone of term [polynomial] operations. Thus, investigation of Mal'tsev clones [polynomial clones] on a set A is the same as investigation of term [polynomial] inequivalent Mal'tsev algebras with the universe A.

In [4] it was revealed that nilpotent non-Abelian algebras give rise to the most complicated case in studying Mal'tsev algebras. As was shown, the structure of small such algebras is very similar to the structure of algebras having d or d' as polynomial operations. So, this case looks appropriate for tackling the whole problem.

In this paper we give a complete description of polynomial clones containing the Mal'tsev operation of the group $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p^2$, p prime. We will assume $p > 2$ since the case $p = 2$ was completely studied in [4].

2 Preliminary remarks

Besides common calculations with polynomials over a ring, we will constantly use in the present paper the methods developed in the framework of modular commutator theory of R.Freese and R.McKenzie [6], the tame congruence theory of D.Hobby and R.McKenzie [10], and also the technique which is based on the notion of polynomially rich algebra that has been introduced and studied by P.Idziak and K.Słomczyńska in [13].

Since the approach from [13] is not widely known, we give basic definitions and results. Recall that tame congruence theory allows us to label prime quotients of the congruence lattice of a finite algebra by one of the five types $\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}$. The type of a prime quotient reflects the local structure of the algebra. The five types correspond therefore to the five possible forms of the local structure of a finite algebra: **1.** a finite set with a group action on it, **2.** a finite vector space over a finite field, **3.** a two element Boolean algebra, **4.** a two element lattice, **5.** a two element semilattice. The type of a prime quotient $\alpha \prec \beta$ in the congruence lattice $\mathsf{Con}\ \mathbb{A}$ is denoted by $\mathsf{typ}_{\mathbb{A}}(\alpha, \beta)$, or simply $\mathsf{typ}(\alpha, \beta)$ if $\mathbb{A}$ is clear from the context.

Now, let $\mathbb{A} = (A; F)$ be a finite algebra. By an $\mathbb{A}$-admissible operation we mean an operation f such that $\mathsf{Con}\ \mathbb{A}' = \mathsf{Con}\ \mathbb{A}$ where $\mathbb{A}' = (A; F \cup \{f\})$, and for any $\alpha, \beta \in \mathsf{Con}\ \mathbb{A}$ with $\alpha \prec \beta$ we have $\mathsf{typ}_{\mathbb{A}'}(\alpha, \beta) = \mathsf{typ}_{\mathbb{A}}(\alpha, \beta)$.

A finite algebra $\mathbb{A}$ is said to be *polynomially rich* if every $\mathbb{A}$–admissible operation is a polynomial of $\mathbb{A}$. It is *hereditarily polynomially rich* if all its homomorphic images are polynomially rich.

We recall also that the *commutator* of congruences α, β of an algebra $\mathbb{A}$ is the smallest congruence $\gamma = [\alpha, \beta]$ such that for any polynomial operation $f(x_1, \ldots, x_m, y_1, \ldots, y_n)$ of $\mathbb{A}$ and any $a_1 \overset{\beta}{\equiv} b_1, \ldots, a_m \overset{\beta}{\equiv} b_m$, $c_1 \overset{\alpha}{\equiv} d_1, \ldots,$ $c_n \overset{\alpha}{\equiv} d_n$,

$$f(a_1, \ldots, a_m, c_1, \ldots, c_n) \overset{\gamma}{\equiv} f(b_1, \ldots, b_m, c_1, \ldots, c_n)$$

implies

$$f(a_1, \ldots, a_m, d_1, \ldots, d_n) \overset{\gamma}{\equiv} f(b_1, \ldots, b_m, d_1, \ldots, d_n).$$

In fact, in a congruence-modular variety the commutator is uniquely determined by the binary operations of an algebra, i.e. the condition above can be relaxed by assuming $m = n = 1$. Moreover, in this case the commutator is a commutative monotone operation on congruence lattices of algebras from the variety. Throughout this paper we treat congruence lattices as labelled lattices with an additional binary operation of the commutator where labels show types of prime quotients.

We will often use the characterisation of polynomially rich Mal'tsev algebras given in [13]. The identity relation and the total equivalence will be denoted by $\underline{0}$, $\underline{1}$ respectively. The *centralizer* of a congruence α is the greatest congruence β such that $[\beta, \alpha] = \underline{0}$.

Theorem 1 ([13]) *Let $\mathbb{A}$ be a finite algebra that has a Mal'tsev polynomial. Then $\mathbb{A}$ is hereditarily polynomially rich iff for every subdirectly irreducible homomorphic image $\mathbb{D}$ of $\mathbb{A}$ the following conditions hold*

(SC1) *the centralizer of the monolith of $\mathbb{D}$ is not bigger than the monolith itself,*

(GFp) *if the monolith μ of $\mathbb{D}$ is Abelian (i.e. $[\mu, \mu] = \underline{0}$), then $(\underline{0}, \mu)$–minimal sets are polynomially equivalent to a one-dimensional vector space over a field* $\mathrm{GF}(p)$ *for some prime number p.*

Presence of a Mal'tsev polynomial restricts possible labels of the prime quotient $\alpha \prec \beta$ of the congruence lattice of a finite algebra to types **2** and **3**. The type $\mathsf{typ}(\alpha, \beta)$ of this prime quotient is obviously determined by the commutator square $[\beta, \beta]$:

$$\mathsf{typ}(\alpha, \beta) = \begin{cases} \mathbf{2}, & \text{if } [\beta, \beta] \leq \alpha, \\ \mathbf{3}, & \text{if } [\beta, \beta] \not\leq \alpha. \end{cases}$$

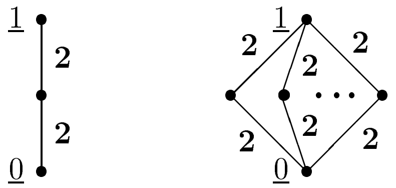
We will usually say that a clone $\mathbf{C}$ on A has a particular property if the algebra $(A; \mathbf{C})$ enjoys this property. For example, we will call clones [hereditarily] polynomially rich, nilpotent and so on. Moreover, by the congruence lattice of a clone $\mathbf{C}$ we mean the congruence lattice of the algebra $(A; \mathbf{C})$. For example, we will say that a clone is simple or subdirectly irreducible, meaning that $(A; \mathbf{C})$ is simple or subdirectly irreducible.

Let $\mathbb{A}$ be a finite algebra from a congruence modular variety. By the *labelled congruence lattice* of $\mathbb{A}$ we mean the lattice $\mathsf{Concom}\ \mathbb{A} = (\mathsf{Con}\ \mathbb{A}; \wedge, \vee, [\cdot, \cdot])$, that is, its congruence lattice endowed with the commutator operation, and in which prime quotients of the lattice are labelled by their types. The usefulness of the technique using polynomially rich algebras is based on the following result. The clone of all polynomial operations of an algebra $\mathbb{A}$ is denoted by $\mathsf{Pol}\ \mathbb{A}$.

Theorem 2 ([4]) *Let $\mathbb{A}$ be a finite algebra from a congruence modular variety. Then there exists a largest clone* $\mathbf{C}$ *on A containing* $\mathsf{Pol}\ \mathbb{A}$ *and such that* $\mathsf{Concom}\ (A; \mathbf{C}) = \mathsf{Concom}\ \mathbb{A}$. □

Let $\mathbb{L}$ be a lattice of equivalence relations on a finite set A such that $\mathbb{L} = \mathsf{Concom}\ \mathbb{A}$ for some algebra $\mathbb{A}$ and a Mal'tsev operation m that preserves $\mathbb{L}$. The theorem means in particular that there is a largest clone $\mathbf{C}$ with $m \in \mathbf{C}$ such that $\mathsf{Concom}\ (A; \mathbf{C}) = \mathbb{L}$. Analogously, if $\mathbb{L}$ is a lattice of equivalence relations whose prime quotients are labelled with types $\mathbf{2}, \mathbf{3}$ then there is at most one polynomially rich clone $\mathbf{C}$ that contains m and $\mathsf{Concom}\ (A; \mathbf{C}) = \mathbb{L}$.

To conclude this section we apply notions given above for Mal'tsev operations d, d' of groups $\mathbb{Z}_{p^2}$, $\mathbb{Z}_p^2$, $p > 2$ prime. To distinguish the group and the ring of integers modulo p^2 we will denote the ring by $\mathbb{Z}_{p^2}^{\times}$. The main purpose of the following statements is to describe all clones that contain d or d' but are not contained in $\mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$. The congruence lattices of $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p^2$ are respectively



Con $\mathbb{Z}_{p^2}$ Con $\mathbb{Z}_p \times \mathbb{Z}_p$

Figure. 1

Proposition 3 *If a clone* $\mathbf{C}$ *contains d' and its congruence lattice is not a chain then* $\mathbf{C}$ *is polynomially rich.*

Proof. Set $\mathbb{A} = (A, \mathbf{C})$. The only subdirectly irreducible homomorphic image of $\mathbb{A}$ is an algebra polynomially equivalent to the group $\mathbb{Z}_p$ or to the field $\mathrm{GF}(p)$. (In the following we will not distinguish polynomially equivalent algebras, e.g. in this case we would say that the homomorphic image *is* the group $\mathbb{Z}_p$.) Since both $\mathbb{Z}_p$ and $\mathrm{GF}(p)$ are simple, condition (SC1) holds trivially. Moreover, $\mathbb{Z}_p$ is a minimal algebra and is polynomially equivalent to a one-dimensional $\mathrm{GF}(p)$-vector space. Hence, it satisfies (GFp). □

In particular, the group $\mathbb{Z}_p^2$ is polynomially rich.

An algebra is called *E-minimal* if every idempotent of the semigroup of its unary polynomial operations is either a constant operation, or the identity mapping. Let $\mathbb{A}$ be a finite algebra, A its universe, and $U \subseteq A$. The *induced algebra* $\mathbb{A}|_U$ is defined to be the algebra $(U, \mathsf{Pol}\ \mathbb{A}|_U)$ where $\mathsf{Pol}\ \mathbb{A}|_U$ consists of restrictions of those operations from $\mathsf{Pol}\ \mathbb{A}$ which preserve U. For an element a and a congruence α we denote by $a/_\alpha$ the α-block containing a.

Lemma 4 *Let a subdirectly irreducible clone* $\mathbf{C}$ *contain* d *or* d'*, its monolith be Abelian, and let* $\mathbf{C}$ *not satisfy (GFp). Then* $\mathbf{C}$ *is* E*-minimal.*

Proof. Set $\mathbb{A} = (A, \mathbf{C})$. Let μ be the monolith of $\mathbb{A}$, U a $(\underline{0}, \mu)$-minimal set, and e an idempotent such that $e(A) = U$. Suppose that $e(a) = e(b)$ for some $a, b \in B = a/_\mu$. The operation $x + y = d(x, a, y)$ $[x + y = d'(x, a, y)]$ turns the μ-block B into an Abelian group where a is the zero-element. By putting $g(x, y) = e(x + y)$ we obtain

$$g(a, a) = e(a) = e(b) = g(a, b - a).$$

Since $[\mu, \mu] = \underline{0}$, this implies

$$e(c) = g(c, a) = g(c, b - a) = e(c - a + b)$$

for any $c \in B$. Therefore, $e(a) = e(a + k(b - a))$ for any k, and as p prime this means that B gets collapsed by e to a single point.

Applying Theorems 4.31 and 13.9 of [10] we obtain, first, that U is equal to its body, second, that the induced algebra $\mathbb{A}|_U$ is E-minimal, and finally that $|U| = q^k$ for certain prime q and integer k. Moreover, q is the size of each trace of U. Since e is bijective on each μ-block B such that $B \cap U \neq \varnothing$, each trace of U is a μ-block, and therefore $q = p$, $k \leq 2$. If $k = 1$ then U has only one trace and (GFp) holds. If $k = 2$ then $U = A$ and $\mathbb{A}$ is E-minimal. $\square$

We will denote by $\mathbb{L}_{\mathbf{i},\mathbf{j}}$ the labelled three-element chain $\underline{0} < \mu < \underline{1}$ where $\mathsf{typ}(\mu, \underline{1}) = \mathbf{i}$, $\mathsf{typ}(\underline{0}, \mu) = \mathbf{j}$ and $[\underline{1}, \mu] = \mu$. Analogously the two-element chain labelled by $\mathbf{i}$ will be denoted by $\mathbb{L}_{\mathbf{i}}$.

For an algebra $\mathbb{A}$ denote inductively $\theta_0 = \underline{1}$, $\theta_i = [\underline{1}, \theta_{i-1}]$. If $\theta_i = \underline{0}$ for some i then $\mathbb{A}$ is said to be *nilpotent*. By Lemma 4.36 of [10], every finite E-minimal Mal'tsev algebra having at least 3 elements is nilpotent.

Proposition 5 *If* $\mathbf{C}$ *contains* d *or* d' *and* $\mathsf{Concom}\ \mathbf{C}$ *is of the form* $\mathbb{L}_{\mathbf{3}}$, $\mathbb{L}_{\mathbf{i},\mathbf{j}}$, $\mathbf{i},\mathbf{j} \in \{\mathbf{2},\mathbf{3}\}$, *then* $\mathbf{C}$ *is polynomially rich.*

Proof. Since $[\underline{1},\mu] = \mu$ holds for the lattices of the form $\mathbb{L}_{\mathbf{i},\mathbf{j}}$ and $\underline{1}$ is the monolith in $\mathbb{L}_{\mathbf{3}}$, the clone $\mathbf{C}$ satisfies (SC1). Moreover, $\mathbf{C}$ is not nilpotent, therefore it is not E-minimal. If the monolith is non-Abelian, then we are done. Otherwise, by Lemma 4, $\mathbf{C}$ satisfies (GFp) and hence it is polynomially rich. $\square$

In particular, $\mathbb{Z}_{p^2}^{\times}$ is a polynomially rich algebra, because $\mathsf{Concom}\ \mathbb{Z}_{p^2}^{\times} = \mathbb{L}_{\mathbf{3},\mathbf{2}}$.

We also note one auxiliary assertion that will be used in Sections 3 and 4. It can be proved in the same way as the first four lines of the proof of Lemma 4.

Lemma 6 *If* $\mathbf{C}$ *is a subdirectly irreducible clone,* d *or* d' *belongs to* $\mathbf{C}$, μ *is a monolith of* $\mathbf{C}$, $\mu < \underline{1}$, *and* $\mathsf{typ}(\underline{0},\mu) = \mathbf{2}$, *then for any block* B *of* μ, *the algebra* $(A;\mathbf{C})|_B$ *is polynomially equivalent to* $\mathbb{Z}_p$.

We next study simple clones of type $\mathbf{2}$. The operation d' allows a clone $\mathbf{C}$ ($d' \in \mathbf{C}$) to have its congruence lattice labelled in an arbitrary way while d does not.

Proposition 7 *(1) There exists no clone that contains* d *and has* $\mathbb{L}_{\mathbf{2}}$ *as its labelled congruence lattice.*

(2) There exist exactly two clones which contain d' *and have* $\mathbb{L}_{\mathbf{2}}$ *as the labelled congruence lattice. One of them is polynomially rich, the other is the clone of all polynomials of a one-dimensional vector space over* $\mathrm{GF}(p^2)$.

Proof. As follows from [9], an algebra $\mathbb{A}$ such that $\mathsf{Concom}\ (\mathbb{A}) = \mathbb{L}_{\mathbf{2}}$ is polynomially equivalent to an R-module for a certain ring R.

(1) Suppose that a clone $\mathbf{C}$ contains d and $\mathsf{Concom}\ \mathbf{C} = \mathbb{L}_{\mathbf{2}}$. Set $\mathbb{A} = (A;\mathbf{C})$. Since $\mathbf{C}$ contains d, the additive group of the corresponding R-module is $\mathbb{Z}_{p^2}$ and R is a subring of the endomorphism ring of $\mathbb{Z}_{p^2}$. However, the endomorphism ring of $\mathbb{Z}_{p^2}$ is $\mathbb{Z}_{p^2}^{\times}$, therefore $\mathbb{A}$ must be polynomially equivalent to $\mathbb{Z}_{p^2}$. This means that there is no clone $\mathbf{C}$ such that $d \in \mathbf{C}$ and $\mathsf{Concom}\ \mathbf{C} = \mathbb{L}_{\mathbf{2}}$.

(2) Let $\mathbf{C}$ contain d', $\mathsf{Concom}\ \mathbf{C} = \mathbb{L}_{\mathbf{2}}$, and $\mathbb{A} = (A; \mathbf{C})$. Since $\mathbb{A}$ is simple, the condition (SC1) holds trivially and, by Lemma 4.28 [10], $\mathbb{A}$ is minimal if and only if it is E-minimal. The proof splits into two cases depending on whether the algebra $\mathbb{A}$ is minimal or not. Since $\mathbb{A}$ is simple, the $(\underline{0}, \underline{1})$–minimal sets consist of a single trace. Thus, if $\mathbb{A}$ is minimal then it must be polynomially equivalent to a one-dimensional vector space over $\mathrm{GF}(p^2)$. On the other hand, if $\mathbb{A}$ is not minimal then, by Lemma 4, it satisfies (GFp) and is therefore polynomially rich. □

As will be shown later, Propositions 3, 5, and 7 allow us to determine all clones which contain d or d' and are not contained in $\mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$. In particular, we have the following.

Proposition 8 *If a clone* $\mathbf{C}$ *contains* d *and* $\mathbf{C} \not\subseteq \mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$*, then* $\mathbf{C}$ *is polynomially rich and its congruence lattice is one of* $\mathbb{L}_{\mathbf{2},\mathbf{3}}, \mathbb{L}_{\mathbf{3},\mathbf{3}}$*, and* $\mathbb{L}_{\mathbf{3}}$*.*

Proof. The congruence lattice of $\mathbf{C}$ is a chain, because $d \in \mathbf{C}$. If $\mathbf{C}$ is simple, then by Proposition 7(1) $\mathsf{Concom}\ \mathbf{C} = \mathbb{L}_{\mathbf{3}}$. Otherwise $\mu < \underline{1}$ where μ is the monolith of $\mathbf{C}$. Since $\mathsf{Concom}\ \mathbb{Z}_{p^2}^{\times} = \mathbb{L}_{\mathbf{3},\mathbf{2}}$, and $\mathbb{Z}_{p^2}^{\times}$ is polynomially rich, $\mathbb{Z}_{p^2}^{\times}$ contains all operations which (together with d) preserve the condition $\mathsf{typ}(\underline{0}, \mu) = \mathbf{2}$. As $\mathbf{C} \not\subseteq \mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$, we have $\mathsf{typ}(\underline{0}, \mu) = \mathbf{3}$. Therefore, $[\underline{1}, \mu] = \mu$ and $\mathsf{Concom}\ \mathbf{C}$ is either $\mathbb{L}_{\mathbf{2},\mathbf{3}}$, or $\mathbb{L}_{\mathbf{3},\mathbf{3}}$. By Proposition 5, in all these three cases $\mathbf{C}$ is polynomially rich. □

3 Clones containing the Mal'tsev operation of the group $\mathbb{Z}_{p^2}$

In this section we examine clones containing the operation $d(x, y, z) = x - y + z$ where $+, -$ denote addition and subtraction of the group $\mathbb{Z}_{p^2}$, $p > 2$ prime. By Proposition 8, any clone $\mathbf{C}$ containing d and such that $\mathbf{C} \not\subseteq \mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$ is polynomially rich. Therefore we have to examine only subclones of $\mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$.

We denote the degree of a polynomial f by $\mathsf{deg} f$ and say that $f(x_1, \ldots, x_n)$ has degree k in x_1 ($\mathsf{deg}_1 f = k$ in symbols) if f can be represented in the form

$$x_1^k f_k(x_2, \ldots, x_n) + \ldots + x_1^1 f_1(x_2, \ldots, x_n) + f_0(x_2, \ldots, x_n)$$

where f_k is not the constant 0 operation. First of all we prove that any clone of polynomials is generated by polynomials of a special kind. A polynomial f in variables $x_1, \ldots, x_n$ is called *fully divisible* if, for any $i \leq n$, $f(x_1, \ldots, x_n) = 0$ whenever $x_i = 0$. Notice that f is fully divisible if and only if it is divisible by $x_1 \ldots x_n$. For a given set D of operations we will denote the clone generated by D and all the constant operations by $\langle\langle D \rangle\rangle$.

Lemma 9 *Suppose $f = f_1 + \ldots + f_r$, where $f_1, \ldots, f_r$ are fully divisible and $f_i + f_j$ is not fully divisible whenever $i \neq j$. Then $f_1, \ldots, f_r \in \langle\langle d, f \rangle\rangle$.*

Proof. Let f depend on variables $x_1, \ldots, x_n$ and denote by $X_i \subseteq \{x_1, \ldots, x_n\}$ the set of variables of f_i. Without loss of generality, let X_1 be a minimal set among $X_1, \ldots, X_r$. Then $f_1 = f(y_1, \ldots, y_n)$ where

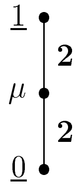
$$y_i = \begin{cases} x_i, & \text{if } x_i \in X_1; \\ 0 & \text{otherwise.} \end{cases}$$

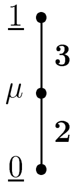
Thus f_1 and $f_2 + \ldots + f_r$ belong to $\langle\langle d, f \rangle\rangle$. Continuing by induction we get the required result. $\square$

Obviously, $f \in \langle\langle d, f_1, \ldots, f_r \rangle\rangle$.

Corollary 10 *Every Mal'tsev clone of polynomials is generated by a set of fully divisible polynomials.*

As above we consider a congruence lattice as a labelled lattice with the binary operation of commutator. Denote by $\mathbb{L}_{\mathbf{2},\mathbf{2}}$ and $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$ the lattices



, $[\underline{1}, \mu] = \mu$ and


, $[\underline{1}, \mu] = \underline{0}$

respectively. (The labelled lattice $\mathbb{L}_{\mathbf{2},\mathbf{2}}$ was defined in the previous section.) As the following lemmas say, an operation preserving one of these lattices satisfies some special conditions.

Lemma 11 *Suppose $f(x_1,\dots,x_n)$ is a fully divisible polynomial and the range of f is contained in $0/\mu$. Then*

$$f=\sum_{i=1}^{n}(x_i^p-x_i)f_i(x_1,\dots,x_n)+pf'(x_1,\dots,x_n) \tag{1}$$

where the degrees of f', f_i $(1\le i\le n)$ in each variable are less than p.

Proof. We prove Formula (1) by induction on n. We denote the polynomial obtained from f by replacing all the coefficients of f with their residues modulo μ by $f/_{\mu}$. The polynomial $f/_{\mu}$ will also be treated as an operation mapping $(\mathbb{Z}_{p^2}/_{\mu})^n$ to $\mathbb{Z}_{p^2}/_{\mu}$. Suppose $n=1$ and the range of f is contained in $0/\mu$. Then $f/_{\mu}$ is a polynomial of GF(p) and $f/_{\mu}\equiv 0$. The basis of identities of GF(p) is $\{px=0,\ x^p-x=0\}$, therefore the polynomial $f/_{\mu}$ belongs to the ideal generated by px and x^p-x in the ring of polynomials over GF(p), that is $f(x)=(x^p-x)f_1(x)+pf'(x)$. The degree of f' can be assumed to be less than p because of the identity $px^p=px$. If $\mathsf{deg} f_1\ge p$ then, since $(x^p-x)^2=0$ in $\mathbb{Z}_{p^2}$,

$$f(x)=(x^p-x)((x^p-x)f_1'(x)+f_1''(x))+pf'(x)=(x^p-x)f_1''(x)+pf'(x)$$

where $\mathsf{deg} f_1''<p$. The base case of the induction is proved.

Suppose (1) is proved for all $k<n$. Let us represent f in the form

$$f(x_1,\overline{x})=(x_1^p-x_1)f_1(\overline{x})+x_1^{p-1}f_2(\overline{x})+\ldots+x_1f_p(\overline{x})+f_{p+1}(\overline{x})+pf'(x_1,\overline{x})$$

where $\overline{x}$ denotes the vector $x_2,\dots,x_n$ and $pf'(x_1,\overline{x})$ is the sum of all monomials which are divisible by p. Since $f/_{\mu}\equiv 0$ and $(x_1^p-x_1)f_1(\overline{x})/_{\mu}\equiv pf'(x_1,\overline{x})/_{\mu}\equiv 0$ we have

$$(x_1^{p-1}f_2(\overline{x})+\ldots+f_{p+1}(\overline{x}))/_{\mu}\equiv 0.$$

This means that $f_2(\overline{x})/_{\mu}\equiv\ldots\equiv f_{p+1}(\overline{x})/_{\mu}\equiv 0$ and (1) follows from the induction hypothesis. □

A polynomial $f(x_1,\dots,x_n)$ is said to satisfy the *block-constant property* if for any blocks $B_1,\dots,B_n$ of μ the restriction $f|_{B_1\times\ldots\times B_n}$ is a constant operation.

Lemma 12 *Suppose $f(x_1, \ldots, x_n)$ is a fully divisible polynomial and $n > 1$.*

(i) If f belongs to a clone preserving $\mathbb{L}_{\mathbf{2},\mathbf{2}}$, then the range of f is contained in $0/\mu$ and f satisfies (1).

(ii) If f belongs to a clone preserving $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$, then f satisfies the block-constant property.

Proof. (i) Full divisibility of f means that $f(x_1, \ldots, x_n) = 0$ whenever one of $x_1, \ldots, x_n$ equals 0. Consequently, using the condition $[\underline{1}, \underline{1}] \leq \mu$ we have that, for any $a_1, \ldots, a_n \in \mathbb{Z}_{p^2}$,

$$\begin{array}{rcl} f(0, a_2, a_3, \ldots, a_n) & \overset{\mu}{\equiv} & f(0, 0, a_3, \ldots, a_n) = 0 \\ & \Downarrow & \\ f(a_1, a_2, a_3, \ldots, a_n) & \overset{\mu}{\equiv} & f(a_1, 0, a_3, \ldots, a_n) = 0. \end{array}$$

So, $f(a_1, \ldots, a_n) \in 0/_{\mu}$ as required.

(ii) For given blocks $B_1, \ldots, B_n$ of μ and $a_1 \in B_1$, $a_2, b_2 \in B_2, \ldots, a_n, b_n \in B_n$, we have

$$\begin{array}{rcl} 0 = f(0, a_2, \ldots, a_n) & = & f(0, b_2, \ldots, b_n) = 0 \\ & \Downarrow & \\ f(a_1, a_2, \ldots, a_n) & = & f(a_1, b_2, \ldots, b_n), \end{array}$$

because $[\underline{1}, \mu] = \underline{0}$. Therefore $f|_{B_1 \times \ldots \times B_n}$ does not depend on $x_2, \ldots, x_n$. It can be shown in a similar way that $f|_{B_1 \times \ldots \times B_n}$ does not depend on x_1. $\Box$

For unary operations a weaker form of Lemma 12(ii) holds.

Lemma 13 *If a unary polynomial f belongs to a clone which contains d and preserves $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$, then $f = ax + g(x)$ where $g(x)$ satisfies the block-constant property.*

Proof. Let $\mathbf{C}$ be the clone preserving $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$ and such that $d, f \in \mathbf{C}$. Also let $\mathbb{A} = (A; \mathbf{C})$, $B = 0/_{\mu}$. For the operation $f'(x) = f(x) - f(0)$ we have $f'(0) = 0$, and therefore $f'(B) \subseteq B$. By Lemma 6, $\mathbb{A}|_B$ is polynomially equivalent to $\mathbb{Z}_p$. Hence $f'|_B(x) = ax$, for a certain $a \in \mathbb{Z}_p$. For the operation $h(x, y) = f'(x + y) - a(x + y)$ and any $b \in B$, we have

$$h(0, 0) = f'(0) - a \cdot 0 = 0 = f'(b) - a \cdot b = h(b, 0).$$

Since h preserves the condition $[\underline{1}, \mu] = \underline{0}$, we obtain

$$h(0, c) = h(b, c),$$

for any $c \in \mathbb{Z}_{p^2}$, which means that $g(x) = f'(x) - a \cdot x + f(0)$ satisfies the block-constant property. As $f(x) = ax + g(x)$, this completes the proof. $\Box$

In the following our proof splits into two cases.

CASE 1. Non-nilpotent clones.

By Lemma 4 and Lemma 4.36 [10], all clones in this case satisfy the condition (GFp). So, only clones whose labelled congruence lattice is $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$ have to be considered separately. Note also that any minimal set of a Mal'tsev algebra equals its body, as follows from Theorem 8.5 of [10] or from results of [14]. In particular, if $\mathsf{typ}(\alpha, \beta) = \mathbf{3}$, then any $\langle \alpha, \beta \rangle$-minimal set is 2-element.

Lemma 14 *There is a unique clone* $\mathbf{C}$ *such that* Concom $\mathbf{C}$ *is* $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$ *and* $d \in \mathbf{C}$.

Proof. We prove that every fully divisible polynomial $f(x_1, \ldots, x_n)$ satisfying the block-constant property belongs to $\mathbf{C}$. Note that, for any a, b such that $a \overset{\mu}{\not\equiv} b$, there is a polynomial $t(x)$ of the Abelian group $\mathbb{Z}_{p^2}$ taking a to 0 and b to 1. Consequently, since any $\langle \mu, \underline{1} \rangle$-minimal set is two-element, $\{0, 1\}$ is a $\langle \mu, \underline{1} \rangle$-minimal set. Let e be a unary polynomial operation with the range $\{0, 1\}$ and such that $e^2 = e$. By Theorem 1, the algebra $(\{0, \ldots, p^2-1\}, \mathbf{C})/_{\mu}$ is a polynomially rich simple algebra of type **3**; therefore it is primal. Hence, for any n and blocks $B_1, \ldots, B_n$ of μ, there is an operation $g(x_1, \ldots, x_n) \in \mathbf{C}$ such that $g(x_1, \ldots, x_n) \overset{\mu}{\equiv} 1$ if $x_i \in B_i$ $(1 \leq i \leq n)$ and $g(x_1, \ldots, x_n) \overset{\mu}{\equiv} 0$ otherwise. Denote $eg(x_1, \ldots, x_n)$ by $g_{B_1,\ldots,B_n}$. We obtain

$$g_{B_1,\ldots,B_n}(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } x_i \in B_i,\ 1 \leq i \leq n \\ 0 & \text{otherwise.} \end{cases}$$

Further, for any $f(x_1, \ldots, x_n)$ satisfying the block-constant property, we have

$$f(x_1, \ldots, x_n) = \sum_{\substack{B_1, \ldots, B_n \\ \text{are blocks} \\ \text{of } \mu}} f(a_1, \ldots, a_n) \cdot g_{B_1,\ldots,B_n}(x_1, \ldots, x_n)$$

where $a_i \in B_i$ $(1 \leq i \leq n)$. Since $d(x, y, z) = x - y + z$ belongs to $\mathbf{C}$, the operation f also belongs to $\mathbf{C}$.

Moreover, by Lemma 13, each unary operation preserving $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$ is in $\mathbf{C}$. Thus by Lemma 12(ii), $\mathbf{C}$ is the clone of all operations preserving $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$. $\square$

CASE 2. Nilpotent clones.

Lemma 15 *If a fully divisible polynomial $f(x_1, \ldots, x_n)$, $n > 1$, preserving $\mathbb{L}_{\mathbf{2},\mathbf{2}}$ satisfies the block-constant property, then f is divisible by p.*

Proof. By Lemma 12(i), f is of the form (1). Suppose $(x_i^p - x_i) f_i(x_1, \ldots, x_n) \neq 0$ for some $i \leq n$ and $x_1, \ldots, x_n$. Without loss of generality, we may assume $i = 1$. This means that there are $a_1, \ldots, a_n \in A$ such that $f_1(a_1, \ldots, a_n) \notin 0/_{\mu}$. Substituting $a_2, \ldots, a_n$ for $x_2, \ldots, x_n$ we obtain

$$g(x_1) = (x_1^p - x_1) f_1(x_1, a_2, \ldots, a_n) + pg'(x_1, a_2, \ldots, a_n)$$

for a certain g', because $a_i^p - a_i$ is divisible by p, $2 \leq i \leq n$. Furthermore, since f_1, g' preserve μ, we have $f_1(a_1 + p, a_2, \ldots, a_n) = f_1(a_1, a_2, \ldots, a_n) + kp$, $g'(a_1 + p, a_2, \ldots, a_n) = g'(a_1, a_2, \ldots, a_n) + lp$ for certain integers k, l. Therefore

$$\begin{aligned} g(a_1 + p) &= (a_1^p - a_1 - p)(f_1(a_1, a_2, \ldots, a_n) + kp) + pg'(a_1, a_2, \ldots, a_n) = \\ &= (a_1^p - a_1) f_1(a_1, a_2, \ldots, a_n) + pg'(a_1, a_2, \ldots, a_n) - \\ &\quad -pf_1(a_1, a_2, \ldots, a_n) = \\ &= g(a_1) - pf_1(a_1, a_2, \ldots, a_n) \neq g(a_1), \end{aligned}$$

since $(a_1 + p)^p = a_1^p$ and $a_1^p - a_1 \in 0/_{\mu}$. This contradicts the assumption that f satisfies the block-constant property. Thus, $f = pf'(x_1, \ldots, x_n)$ as required. $\square$

If a non-unary fully divisible polynomial belongs to a nilpotent clone, then it preserves both conditions $[\underline{1}, \underline{1}] \leq \mu$ and $[\underline{1}, \mu] = \underline{0}$. Consequently, it preserves both labelled lattices $\mathbb{L}_{\mathbf{2},\mathbf{2}}, \mathbb{L}'_{\mathbf{3},\mathbf{2}}$. So, by Lemma 12, it satisfies the conditions of Lemma 15 and is divisible by p.

Corollary 16 *Every non-unary polynomial from a nilpotent clone containing d is divisible by p.*

By a *multi-linear* polynomial we mean a polynomial which is linear in each variable.

Lemma 17 *Suppose $pf(x_1, \dots, x_n)$ is a fully divisible polynomial of degree k and the degree of f in each variable is less than p. Then*

$$px_1 \dots x_k \in \langle\langle d, pf \rangle\rangle.$$

Proof. If f is a multi-linear polynomial, then pf is of the required form since $x_1 \dots x_n$ is a unique fully divisible multi-linear polynomial. Suppose $\mathsf{deg}_n f = l > 1$, that is

$$f = x_n^l f_l(x_1, \dots, x_{n-1}) + \dots + x_n f_1(x_1, \dots, x_{n-1}).$$

(As f is fully divisible, every summand of f is divisible by x_n.) Substituting $x_n + \dots + x_{n+l-1}$ instead of x_n we obtain

$$ax_n \dots x_{n+l-1} f_l(x_1, \dots, x_{n-1}) + f'(x_1, \dots, x_{n+l-1})$$

where $a = l! \in \mathbb{N}$ is not divisible by p and no monomial of f' contains all the variables $x_1, \dots, x_{n+l-1}$. Then, by Lemma 9, $x_n \dots x_{n+l-1} f_l(x_1, \dots, x_{n-1})$ can be derived.

Continuing this process, we obtain a multi-linear polynomial of degree k. $\square$

Lemma 18 *Let $f(x)$ be of the form $ax^p + pg(x)$ where a is not divisible by p and $\mathsf{deg} g < p$. Then $x^p \in \langle\langle d, f \rangle\rangle$.*

Proof. By substituting $x_1 + \dots + x_p$ for x we get a polynomial which contains only one monomial divisible by $x_1 \dots x_p$, namely, $ap! x_1 \dots x_p$. Therefore, $px_1 \dots x_p \in \langle\langle d, f \rangle\rangle$, and any polynomial which is divisible by p and is of degree p or less also belongs to $\langle\langle d, f \rangle\rangle$. Hence, $pg(x), x^p \in \langle\langle d, f \rangle\rangle$. $\square$

Denote by $\mathbf{E}$ the set of all polynomials f such that each non-linear monomial of f is divisible by p. Denote by $\mathbf{N}$ the set of all polynomials f such that each non-linear monomial is either of the form ax^p or is divisible by p.

Lemma 19 **E** *and* **N** *are the greatest E-minimal and the greatest nilpotent clone containing d respectively.*

Proof. One may easily check that **E**, **N** are clones, **E** is an E-minimal one and, as x^p witnesses, **N** is a nilpotent but not an E-minimal one. Take a polynomial $f \notin \mathbf{N}$. If f contains a non-unary monomial g which is not divisible by p, then a certain fully divisible polynomial containing g belongs to $\langle\langle d, f\rangle\rangle$ by Lemma 9. So, by Corollary 16, f cannot belong to any nilpotent clone. Suppose f has a unary monomial ax^k such that a and k are not divisible by p. Substituting $x + y$ for x we get the previous case.

If $k = sp$, $1 < s < p$, then substitute $x_1 + \ldots + x_s$ where none of $x_1, \ldots, x_n$ occurs in f for x. Every monomial of the polynomial we obtain is of the form

$$\frac{(sp)!}{k_1! \ldots k_s!} x_1^{k_1} \ldots x_s^{k_s}, \qquad k_1 + \ldots + k_s = sp$$

and p does not divide its coefficient if and only if each k_i $(1 \leq i \leq s)$ is divisible by p. So,

$$\frac{(sp)!}{p! \ldots p!} x_1^p \ldots x_s^p$$

is the only monomial divisible by $x_1 \ldots x_s$ whose coefficient is not divisible by p. Again, we get a non-unary monomial which is not divisible by p.

Let us take $f \notin \mathbf{E}$. If f belongs to some E-minimal clone, then $f \in \mathbf{N}$ by Lemma 4.36 of [10]. Consequently,

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) + a_1 x_1^p + \ldots + a_n x_n^p + h(x_1, \ldots, x_n)$$

where $g(x_1, \ldots, x_n) \in \mathbf{E}$ and has no unary monomial, and $h(x_1, \ldots, x_n)$ is a linear polynomial. Suppose without loss of generality that $a_1 \overset{\mu}{\not\equiv} 0$. Then $g(x_1, \ldots, x_n) + a_1 x_1^p + \ldots + a_n x_n^p \in \langle\langle d, f\rangle\rangle$. By Lemma 9, $pg_1(x_1) + a_1 x_1^p \in \langle\langle d, f\rangle\rangle$ for certain g_1 and, by Lemma 18, $x^p \in \langle\langle d, f\rangle\rangle$. The operation x^p is a non-identical and nontrivial idempotent unary operation. This contradicts the E-minimality of $\langle\langle d, f\rangle\rangle$. $\square$

Lemma 20 *Subclones of* **N** *containing d are precisely the following*

$$\mathbf{E}_k = \langle\langle d, px_1 \ldots x_k\rangle\rangle, \quad \mathbf{E} = \bigcup_{k \in \mathbb{N}} \mathbf{E}_k, \text{ and}$$

$$\mathbf{N}_n = \langle\langle d, x^p, px_1 \ldots x_n\rangle\rangle \quad (n \geq p), \quad \mathbf{N} = \bigcup_{n \in \mathbb{N} \setminus \{1, \ldots, p-1\}} \mathbf{N}_n.$$

Proof. The identity $px^p = px$ along with Corollaries 10, 16, and Lemmas 17, 18 imply that every subclone of $\mathbf{E}$ is generated by polynomials of the form $px_1 \dots x_n$ and every subclone of $\mathbf{N}$ is generated by polynomials of the form $px_1 \dots x_n$ and x^p. One can straightforwardly check that for any n, m ($2 \le m < n$), $px_1 \dots x_m \in \mathbf{E}_n$ while $px_1 \dots x_n \notin \mathbf{E}_m$. Therefore, $\mathbf{E}_m \ne \mathbf{E}_n$, $\mathbf{E}_m \subseteq \mathbf{E}_n$ whenever $m < n$ and for any subclone $\mathbf{C}$ of $\mathbf{E}$ such that n is the maximal degree of polynomials from $\mathbf{C}$ we have $\mathbf{C} = \mathbf{E}_n$. It is not hard to see that $px_1 \dots x_p \in \langle\langle d, x^p \rangle\rangle$, therefore $\mathbf{N}_1 = \ldots = \mathbf{N}_p$. The fact that the clones $\mathbf{N}_p, \mathbf{N}_{p+1}, \dots$ are distinct will be proved in Lemma 32. $\square$

The following theorem summarizes Proposition 5 and 7(1) and the results of Section 3.

Theorem 21 *The lattice of polynomial clones containing d is presented in the following diagram.*

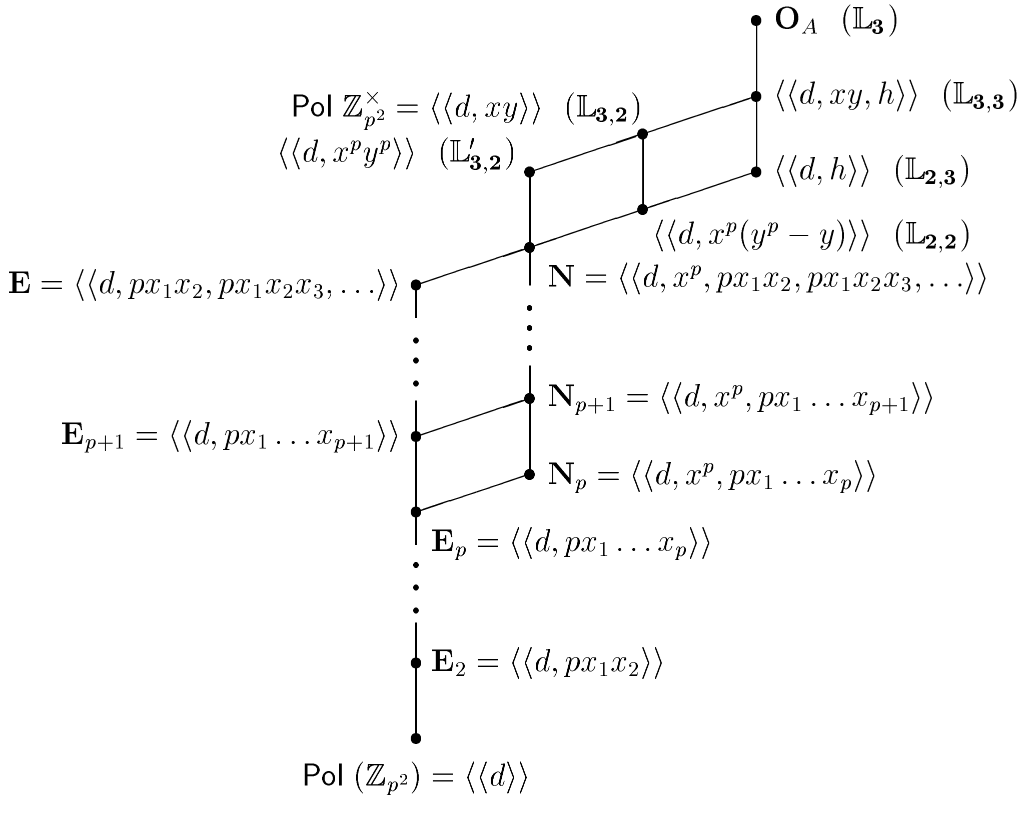


Figure 2

The operation h is defined as follows

$$h(x,y) = \begin{cases} (kl)p, & \text{if } x, y \in 0/\mu \text{ and } x = kp, y = lp; \\ 0, & \text{otherwise.} \end{cases}$$

4 Clones containing the Mal'tsev operation of the group $\mathbb{Z}_p^2$

In this section we explore clones containing the Mal'tsev operation $d'(x,y,z) = x \ominus y \oplus z$ where $\oplus, \ominus$ denote addition and subtraction of the group $\mathbb{Z}_p^2$. If **C** is a clone containing d' its congruence lattice must be a sublattice of the second lattice given in Figure 1, that is one of the following

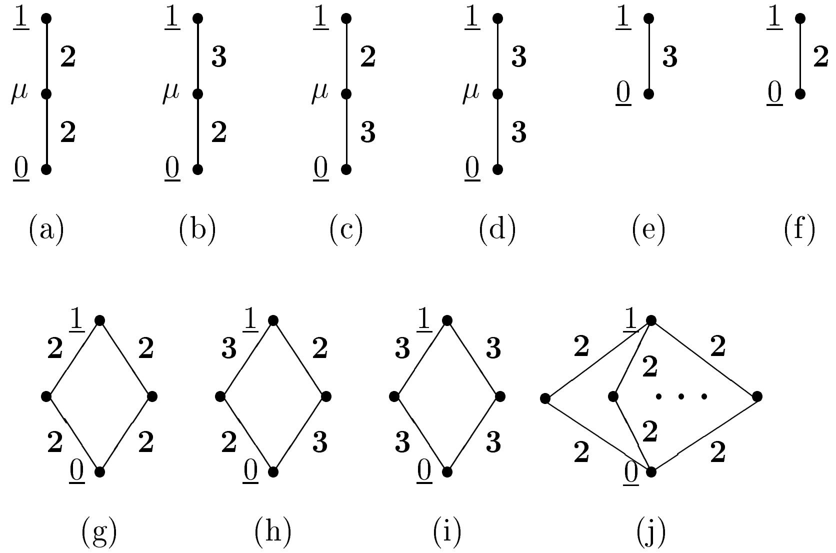


Figure 3

where the last lattice has n $(2 < n \leq p+1)$ atoms and its labels are determined by Corollary 5.20 of [10]. By Propositions 3, 5 and Theorem 2, in cases (c)–(e), and (g)–(j) **C** is polynomially rich and therefore, for each lattice $\mathbb{L}$ in those cases, there exists at most one clone that contains d' and has $\mathbb{L}$ as its labelled congruence lattice. Later, we shall exhibit clones for all these cases and prove that the only clone in case (j) is $\mathsf{Pol}\ \mathbb{Z}_p^2$. By easy calculation of the number of lattices in each of the cases (c)–(e), and (g)–(i) one may check that there are $p+1$ clones in cases (c),(d); 1 clone in (e); and $\frac{p(p+1)}{2}$ in cases (g),(h), and (i). By Proposition 7(2), there exist 2 clones in case (f). The biggest part of this section is devoted to exploring cases (a),(b).

We next show that in cases (a) and (b) $\mathbb{Z}_p^2$ can be endowed with the structure of $\mathbb{Z}_{p^2}^{\times}$ such that $\mathbf{C}$ is a subclone of $\mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$. Let us pick an atom of $\mathsf{Con}\ \mathbb{Z}_p^2$ and denote it by μ. The group $\mathbb{Z}_p^2$ can be represented as the set of all pairs (a,b) where $a,b \in \mathbb{Z}_p$ and $(a,b) \overset{\mu}{\equiv} (c,d)$ if and only if $b=d$. The required structure of $\mathbb{Z}_{p^2}^{\times}$ is provided by the identification $(a,b) \mapsto ap+b \in \mathbb{Z}_{p^2}$. Then the following identities hold

$$x^{p^2} = x^p, \quad px^p = px, \quad px + py = px \oplus py$$

where $\cdot$ is the usual multiplication of $\mathbb{Z}_{p^2}^{\times}$, px denotes the sum $x + \ldots + x$ of p summands if x is treated as an element of $\mathbb{Z}_{p^2}^{\times}$, and it denotes the endomorphism of the Abelian group $\mathbb{Z}_p \times \mathbb{Z}_p$ taking (a,b) to $(b,0)$ if x is treated as an element of this group. Moreover, $x \oplus y = x + y$ whenever $x, y \in 0/_{\mu}$. We will freely use both representations of elements from $\mathbb{Z}_p^2$.

Lemma 22 *There are polynomials $s(x,y)$, $s'(x,y)$ of $\mathbb{Z}_{p^2}^{\times}$ of degree p such that*
$x \oplus y = x + y + ps(x,y)$, *and*
$x + y = x \oplus y \oplus ps'(x,y)$.

Proof. Obviously, operations s, s' must satisfy

$$ps'(x,y) = -ps(x,y) = \begin{cases} p, & \text{if } x_2 + y_2 \geq p \text{ where } x = (x_1,x_2), y = (y_1,y_2), \\ 0 & \text{otherwise.} \end{cases}$$

The value of the operation $r(x) = x(x-1)\ldots(x-(p-1))$ is 0 whenever $x \in \{0,1,\ldots,p-1\}$. If $x = ap+b$, then $r(x) = ap \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) = -ap$ by Wilson's Theorem. Thus the operation

$$\overline{s}(x,y) = r(x) + r(y) - r(x+y).$$

acts as the required operation $ps(x,y)$.

By Lemma 11, $r(x) = (x^p - x) + pr'(x)$ where $\mathsf{deg} r' < p$. Consequently,

$$\begin{aligned}\overline{s}(x,y) &= (x^p - x) + pr'(x) + (y^p - y) + pr'(y) - ((x+y)^p - (x+y)) - \\ &\quad pr'(x+y) = x^p + y^p - (x+y)^p + p(r'(x) + r'(y) - r'(x+y)).\end{aligned}$$

The last polynomial is divisible by p and is of degree p. This means that it can be represented as $ps(x,y)$ where $s(x,y)$ is as required.

To complete the proof we note that $s'(x,y) = -s(x,y)$. □

So, the greatest nilpotent subclone $\mathbf{N}$ of $\mathsf{Pol}\ \mathbb{Z}_{p^2}^{\times}$ contains d'. Therefore, by Theorem 2, it is also the greatest nilpotent clone containing d' and such that μ is the only proper congruence.

Our aim is to prove that the structure of clones containing d' is very similar to the structure of clones containing d. To achieve this aim we establish results which are analogous to the results of the previous section and heavily use the description of clones $\mathbf{E}$ and $\mathbf{N}$.

As in the previous section, an operation $f(x_1, \ldots, x_n)$ is said to be fully divisible if for any $i \le n$ it holds that $f(x_1, \ldots, x_n) = (0,0)$ whenever $x_i = (0,0)$.

Lemma 23 *Any operation $f(x_1, \ldots, x_n)$ can be represented in the form $f = f_1 \oplus \ldots \oplus f_l$ where $f_1, \ldots, f_l \in \langle\langle d', f \rangle\rangle$ are fully divisible.*

Proof. Let $\mathcal{B}$ be a proper downset of the ordered set $\mathcal{P}_n$ of all subsets of $\{1, \ldots, n\}$. We prove by induction that there are $\{f_A \mid A \in \mathcal{B}\} \subseteq \langle\langle d', f \rangle\rangle$ and $f_{\mathcal{B}} \in \langle\langle d', f \rangle\rangle$ such that

- $f = \sum_{A \in \mathcal{B}} f_A \oplus f_{\mathcal{B}}$;
- f_A, $A \in \mathcal{B}$, is fully divisible and depends on variables x_i where $i \in A$; and
- $f_{\mathcal{B}}(x_1^A, \ldots, x_n^A) = (0,0)$ where

  $$x_i^A = \begin{cases} x_i, & \text{if } i \in A, \\ (0,0) & \text{otherwise,} \end{cases}$$

  for any $A \in \mathcal{B}$ and any $x_1, \ldots, x_n \in \mathbb{Z}_p^2$.

To establish the base case of the induction, put $f_{\varnothing} = f((0,0),\ldots,(0,0))$ and $f_{\{\varnothing\}} = f \ominus f_{\varnothing}$. Further, suppose that the required decomposition is found for a downset $\mathcal{B}$ and let $B \subseteq \{1,\ldots,n\}$ be a minimal set such that $B \notin \mathcal{B}$. Set $f_B = f_{\mathcal{B}}(x_1^B,\ldots,x_n^B)$ and $f_{\mathcal{B}\cup\{B\}} = f_{\mathcal{B}} \ominus f_B$. We have

$$f = \sum_{A\in\mathcal{B}} f_A \oplus f_{\mathcal{B}} = \sum_{A\in\mathcal{B}} f_A \oplus f_B \oplus f_{\mathcal{B}\cup\{B\}}.$$

To prove that f_B is fully divisible, we must prove that for any $j \in B$, the operation $f_B(x_1^{B'},\ldots,x_n^{B'})$ where $B' = B - \{j\}$ is the constant $(0,0)$. Actually, since for any $j \in B$, B' belongs to $\mathcal{B}$, $f_B(x_1^{B'},\ldots,x_n^{B'}) = f_{\mathcal{B}}(x_1^{B'},\ldots,x_n^{B'}) = (0,0)$ holds. Finally, we have $f_{\mathcal{B}\cup\{B\}}(x_1^B,\ldots,x_n^B) = f_{\mathcal{B}}(x_1^B,\ldots,x_n^B) \ominus f_{\mathcal{B}}(x_1^B,\ldots,x_n^B) = (0,0)$ and, for any $A \in \mathcal{B}$,

$$\begin{aligned} f_{\mathcal{B}\cup\{B\}}(x_1^A,\ldots,x_n^A) &= f_{\mathcal{B}}(x_1^A,\ldots,x_n^A) \ominus f_B(x_1^A,\ldots,x_n^A) = \\ &\quad (0,0) \ominus f_B(x_1^{A\cap B},\ldots,x_n^{A\cap B}) = (0,0) \ominus (0,0). \end{aligned}$$

Thus for $\mathcal{B} = \mathcal{P}_n$ we obtain

$$f = \sum_{A\in\mathcal{P}_n} f_A \oplus (0,0)$$

where all f_A are fully divisible and belong to $\langle\langle d', f\rangle\rangle$. □

By Lemma 22, a fully divisible operation $f(x_1,\ldots,x_n)$ from a nilpotent clone containing d' can be treated as a usual polynomial of $\mathbb{Z}_{p^2}^{\times}$. Moreover, this polynomial is divisible by $x_1 \ldots x_n$.

As in the previous section we consider two cases.

Case 1. Non-nilpotent clones.

By Proposition 5, every non-nilpotent clone whose labelled congruence lattice differs from $\mathbb{L}'_{\mathbf{3,2}}$ is polynomially rich. Furthermore, we may easily adapt the proofs of Lemmas 13 and 14 for clones containing d'.

Lemma 24 *If a unary operation f belongs to a clone, which contains d' and preserves $\mathbb{L}'_{\mathbf{3,2}}$, then $f = ax \oplus g(x)$ where $a \in \mathbb{Z}_p$ and g satisfies the block-constant property.*

This lemma can be proved in a quite analogous manner to Lemma 13. The only change required is to replace all occurences of $+, -$ with $\oplus, \ominus$ respectively.

Lemma 25 *There is a unique clone* $\mathbf{C}$ *such that* $\mathsf{Concom}\ \mathbf{C}$ *is* $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$ *and* $d' \in \mathbf{C}$*. Moreover,* $d \in \mathbf{C}$*.*

Proof. Notice first that $\mathsf{Pol}\ \mathbb{Z}^{\times}_{p^2}$ is a polynomially rich clone which contains both d and d'. Since $\mathsf{Concom}\ \mathbf{C} = \mathbb{L}'_{\mathbf{3},\mathbf{2}}$, we have $\mathbf{C} \subseteq \mathsf{Pol}\ \mathbb{Z}^{\times}_{p^2}$. This means that operations from $\mathbf{C}$ can be treated as polynomials of $\mathbb{Z}^{\times}_{p^2}$. We prove that every fully divisible polynomial $f(x_1, \ldots, x_n)$ satisfying the block-constant property belongs to $\mathbf{C}$. Note that for any $(a_1, b_1), (a_2, b_2)$ such that $(a_1, b_1) \stackrel{\mu}{\not\equiv} (a_2, b_2)$, there is a polynomial from $\mathbf{C}$ taking (a_1, b_1) to $(0, 0)$ and (a_2, b_2) to $(0, 1)$. Consequently, since any $\langle \mu, \underline{1} \rangle$-minimal set is two-element, $\{(0, 0), (0, 1)\}$ is a $\langle \mu, \underline{1} \rangle$-minimal set. Let e be a unary polynomial operation with the range $\{(0, 0), (0, 1)\}$ and such that $e^2 = e$. The algebra $(\mathbb{Z}_p^2, \mathbf{C})/_{\mu}$ is a polynomially rich simple algebra of type $\mathbf{3}$, therefore it is primal. Hence, for any n and blocks $B_1, \ldots, B_n$ of μ, there is an operation $g(x_1, \ldots, x_n) \in \mathbf{C}$ such that $g(x_1, \ldots, x_n) \stackrel{\mu}{\equiv} (0, 1)$ if $x_i \in B_i$ $(1 \le i \le n)$ and $g(x_1, \ldots, x_n) \stackrel{\mu}{\equiv} (0, 0)$ otherwise. Denote $eg(x_1, \ldots, x_n)$ by $g_{B_1, \ldots, B_n}$. We obtain

$$g_{B_1, \ldots, B_n}(x_1, \ldots, x_n) = \begin{cases} (0, 1) & \text{if } x_i \in B_i,\ 1 \le i \le n \\ (0, 0) & \text{otherwise.} \end{cases}$$

Since $(0, 0) \stackrel{\mu}{\not\equiv} (0, 1)$, for any $(a, b) \in \mathbb{Z}_p^2$, there exists $e_{(a,b)} \in \mathbf{C}$ such that $e_{(a,b)}(0, 0) = (0, 0)$ and $e_{(a,b)}(0, 1) = (a, b)$. Therefore, the operation

$$f(x_1, \ldots, x_n) = \sum_{\substack{B_1, \ldots, B_n \\ \text{are blocks} \\ \text{of } \mu}} e_{f(a_1, \ldots, a_n)}(g_{B_1, \ldots, B_n}(x_1, \ldots, x_n))$$

where $a_i \in B_i$ $(1 \le i \le n)$ belongs to $\mathbf{C}$, as $d'(x, y, z) = x \ominus y \oplus z$ belongs to $\mathbf{C}$.

Moreover, by Lemma 24, each unary operation preserving $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$ is in $\mathbf{C}$. Thus by, Lemma 12(ii), $\mathbf{C}$ is the clone of all operations preserving $\mathbb{L}'_{\mathbf{3},\mathbf{2}}$. $\square$

Lemma 26 *Every non-nilpotent clone containing* d' *is uniquely determined by its labelled congruence lattice. Moreover, every such clone contains* d*.*

CASE 2. Nilpotent clones.
The identity $p(x+y)=p(x\oplus y)$ implies that the analogue of Lemma 17 holds for clones containing d'.

Lemma 27 *Suppose $pf(x_1,\dots,x_n)$ is a fully divisible polynomial of degree k and the degree of f in each variable is less than p. Then*

$$px_1\dots x_k\in\langle\langle d',pf\rangle\rangle.$$

Proof. If f is a multi-linear polynomial, then pf is of the required form. Suppose $\mathsf{deg}_n f=l>1$, that is

$$f=x_n^l f_l(x_1,\dots,x_{n-1})+\dots+x_n f_1(x_1,\dots,x_{n-1}).$$

Substituting $x_n\oplus\dots\oplus x_{n+l-1}$ for x_n we obtain

$$\begin{aligned}
pf &= p\Big((x_n\oplus\dots\oplus x_{n+l-1})^l f_l(x_1,\dots,x_{n-1})\oplus\dots\\
&\qquad\oplus(x_n\oplus\dots\oplus x_{n+l-1})f_1(x_1,\dots,x_{n-1})\Big)\\
&= p(x_n\oplus\dots\oplus x_{n+l-1})^l f_l(x_1,\dots,x_{n-1})\oplus\dots\\
&\qquad\oplus p(x_n\oplus\dots\oplus x_{n+l-1})f_1(x_1,\dots,x_{n-1})\\
&= p(x_n+\dots+x_{n+l-1})^l f_l(x_1,\dots,x_{n-1})\oplus\dots\\
&\qquad\oplus p(x_n+\dots+x_{n+l-1})f_1(x_1,\dots,x_{n-1})\\
&= p\Big((x_n+\dots x_{n+l-1})^l f_l(x_1,\dots,x_{n-1})+\dots\\
&\qquad+(x_n+\dots+x_{n+l-1})f_1(x_1,\dots,x_{n-1})\Big)\\
&= p\Big(ax_n\dots x_{n+l-1}f_l(x_1,\dots,x_{n-1})+f'(x_1,\dots,x_{n+l-1})\Big)\\
&= pax_n\dots x_{n+l-1}f_l(x_1,\dots,x_{n-1})\oplus pf'(x_1,\dots,x_{n+l-1})
\end{aligned}$$

where $a=l!\in\mathbb{N}$ is not divisible by p and no monomial of f' contains all variables $x_1,\dots,x_{n+l-1}$. Then, by Lemma 23, $px_n\dots x_{n+l-1}f_l(x_1,\dots,x_{n-1})$ can be derived.

Continuing this process we obtain a multi-linear polynomial of degree k. $\square$

Corollary 28 *Every proper subclone of* $\mathbf{N}$ *containing* d' *is generated by* d', *constant operations, a set of unary operations and an operation of the form* $px_1 \dots x_n$.

So, to complete the description of clones containing d' we have to describe their possible unary parts.

The range of an operation f is denoted by $\mathsf{Im}\ f$.

Lemma 29 *Let* μ *be the only proper congruence of a clone* $\mathbf{C} \subseteq \mathbf{N}$ *and* $d' \in \mathbf{C}$. *Then* $px \in \mathbf{C}$.

Proof. As $\mathbf{C}$ destroys all the congruences except for μ, it contains a unary polynomial $e(x)$ such that e takes $(0,0)$ to itself and $(0,1)$ to $(1,0)$. We derive px from $e(x)$. Denote by g the operation $e(x \oplus y)$. We have

$$g((0,0),(0,0)) = e((0,0)) \overset{\mu}{\equiv} e((0,1)) = g((0,0),(0,1)). \tag{2}$$

Since $[\underline{1}, \underline{1}] \leq \mu$, it implies that the equality

$$e((a,b)) = g((a,b),(0,0)) \overset{\mu}{\equiv} g((a,b),(0,1)) = e((a,b+1))$$

holds for all $(a,b) \in \mathbb{Z}_p^2$. Moreover, e preserves μ, and so $e(x) \overset{\mu}{\equiv} e((0,0))$. Therefore, $\mathsf{Im}\ e \subseteq (0,0)/_{\mu}$.

Consider e on the block $B = (0,0)/_{\mu}$ of μ. By Lemma 6, the restriction of e to B is either a constant operation or a permutation. Suppose that it is a permutation, that is $e((1,0)) = (a,0) \neq (0,0)$.

By putting $e'(x) = e(x) \ominus ax$ we get an operation such that $e'((0,0)) = e'((1,0)) = (0,0)$ and $e'((0,1)) = (1,-a)$. The first two equalities mean that $e'(x) = (0,0)$ whenever $x \in B$. The pair $((0,0),(1,-a))$ generates the total congruence, so there is an operation $e'' \in \mathbf{C}$ such that $e''((0,0)) = (0,0), e''((1,-a)) = (1,0)$. It is easy to see that the operation $e''e'(x)$ takes $(0,1)$ to $(1,0)$ and $(b,0)$ to $(0,0)$ for every $b \in \mathbb{Z}_p$. As above, the range of $e''e'$ is contained in B and one may replace e with $e''e'$.

Thus, we may assume that for any $a \in \mathbb{Z}_p$,

$$g((0,0),(0,0)) = e((0,0)) = e((a,0)) = g((0,0),(a,0)).$$

Since $[\underline{1}, \mu] = 0$, this implies that

$$e((0,b)) = g((0,b),(0,0)) = g((0,b),(a,0)) = e((a,b))$$

for any $b \in \mathbb{Z}_p$, that is, e satisfies the block-constant property. Since $e \in \mathbf{C} \subseteq \mathbf{N}$, we have $e(x) = pf(x) + ax^p + bx + c$. As $e((0,0)) = (0,0)$, we get $c = (0,0)$. Then, since $e(x), pf(x) + ax^p$ satisfy the block-constant property but x does not, $b = 0$. Finally, $\mathsf{Im}\, e, \mathsf{Im}\, pf \subseteq B$ while $\mathsf{Im}\, x^p \not\subseteq B$. Therefore, a is divisible by p, and $e = pf(x)$ where f is a fully divisible polynomial. If $f(x) = ax$ then we are done. Otherwise, let the degree of f equal k. Then by Lemma 27, $f'(x_1, \ldots, x_k) = px_1 \ldots x_k \in \langle\langle d', f \rangle\rangle$ and therefore $px = f'(x, (0,1), \ldots, (0,1))$ also belongs to $\langle\langle d', f \rangle\rangle$. The lemma is proved. $\Box$

Denote by e_1, e_2 the coordinate endomorphisms of $\mathbb{Z}_p^2$; that is, the unary operations defined as follows

$$e_1((a,b)) = (a,0), \quad e_2((a,b)) = (0,b).$$

Since both these operations are endomorphisms of $\mathbb{Z}_p^2$, they preserve the commutator equality $[\underline{1}, \underline{1}] = \underline{0}$ and therefore belong to $\mathbf{N}$.

Lemma 30 *If a nilpotent clone* $\mathbf{C}$ *with* $d' \in \mathbf{C}$ *contains a unary fully divisible operation* $f(x)$ *which does not satisfy the block-constant property and* $\mathsf{Im}\, f \subseteq (0,0)/_{\mu}$, *then* $e_1 \in \mathbf{C}$.

Proof. Let us assume that $f(x)$ is not a constant on $(0,a)/_{\mu}$ for some $a \in \mathbb{Z}_p$ and $f((0,0)) = (0,0)$. Arguing as in the proof of the previous lemma one may show that f is non-constant on $B = (0,0)/_{\mu}$.

Claim 1. f can be chosen such that $f|_B(x) = x$.

By Lemma 6, $f|_B$ is a permutation, hence, $f' = f^k$ is the identity mapping for a certain k. So, $f'((a,0)) = (a,0)$ for all $a \in \mathbb{Z}_p$ and we may replace f with f'.

Claim 2. $f((a,b)) = (a + g(b), 0)$ for a certain operation $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$.

Fix $b \in \mathbb{Z}_p$ and let B' be the μ-block $(0,b)/_{\mu}$. By Lemma 6, every polynomial from $\mathbf{C}$ that maps B' to B' is a linear operation. In particular, $(f(x) \oplus (0,b))|_{B'} = (\alpha x_1 + \beta, b)$ where $x = (x_1, x_2)$. Therefore, we have

$$f((a,b)) = f'((a,b)) \ominus (0,b) = (\alpha a + \beta, 0)$$

where β depends on b only. Denote β by $g(b)$.

If $\alpha \neq 1$ then the equation $\alpha a + g(b) = a$ has a solution. Let a_0 be the solution. Set $h(x, y) = f(x \oplus y)$. Since $[\underline{1}, \mu] = 0$ the equality

$$h((0,0),(a_0,0)) = f((a_0,0)) = f((a_0,b)) = h((0,b),(a_0,0))$$

implies

$$f((a,0)) = h((0,0),(a,0)) = h((0,b),(a,0)) = f((a,b))$$

for any $a \in \mathbb{Z}_p$. This means $f((a,b)) = (a,0)$, a contradiction to our assumption that $\alpha \neq 1$. So, $\alpha = 1$ and $f((a,b)) = (a + g(b), 0)$.

CLAIM 3. $e_1 \in \mathbf{C}$.

The operation g acts on $\mathrm{GF}(p)$; therefore it can be represented by a polynomial of $\mathrm{GF}(p)$ of degree less than p. Suppose k is the minimal degree of polynomials g' such that $g'(0) = 0$ and $f'((a,b)) = (g'(b) + a, 0)$ for some operation $f' \in \mathbf{C}$. If $k = 0$ then we are done. Otherwise, let us represent g' in the form $g'(x) = \alpha x^k + g''(x)$ where $\mathsf{deg} g'' \leq k - 1$. If $k = 1$ then $e_1(x) = f'(x) \ominus \alpha p x$. So suppose $k > 1$.

For the operation $h(x) = f'(2x) \ominus 2f'(x)$ we have $h((a,b)) = (2\alpha(2^{k-1} - 1)b^k + g''(2b) - 2g''(b), 0)$. Taking $\beta = (2(2^{k-1} - 1))^{-1}$, we obtain that the operation $f''(x) = f'(x) \ominus \beta h(x)$ satisfies the properties:

(a) $f''\big|_B(x) = x$ because $h\big|_B(x) = f'\big|_B(2x) \ominus 2f'\big|_B(x) = 2x \ominus 2x = 0$;

(b) the range of f'' is contained in B; and

(c) $f''((a,b)) = (g'''(b)+a, 0)$ where $g'''(x) = \alpha x^k + g''(x) - (\alpha x^k + \beta(g''(2x) - 2g''(x)))$ has the degree less than k.

This contradicts minimality of k.

Thus the minimal value of k is 0 and $e_1 \in \mathbf{C}$. This completes the proof. $\square$

Corollary 31 *Let $\mathbf{C}$ be a nilpotent clone such that $d' \in \mathbf{C}$, and let $f \in \mathbf{C}$ be a unary operation. Then $f(x) = pg'(x) \oplus \alpha e_1(x) \oplus \beta x \oplus a$. Moreover, $pg' \in \mathbf{C}$ and if $\alpha \neq 0$ then $e_1 \in \mathbf{C}$.*

Proof. Set $a = f((0,0))$ and $\beta = c$ where $f((0,1)) \ominus a = (b,c)$. Then the operation $f'(x) = f(x) \ominus \beta x \ominus a$ takes $(0,0)$ to $(0,0)$ and $(0,1)$ to $(b,0)$.

This means that the range of f' does not exceed $B = (0,0)/\mu$. If $f'|_B$ does not satisfy the block-constant property then by Lemma 30, e_1 belongs to $\mathbf{C}$. By Lemma 6, $f'|_B$ is a linear operation. Since $f'((0,0)) = (0,0)$, it can be represented in the form $f'|_B(x) = (\alpha x_1, 0)$ where $x = (x_1, x_2)$. Therefore, the operation $f''(x) = f'(x) \ominus \alpha e_1(x)$ is a constant operation on B, and hence on each block of μ.

If f satisfies the block-constant property, then set $f'' = f'$. Since $f'' \in \mathbf{C} \subseteq \mathbf{N}$, we have $f''(x) = pg(x) + ax^p$. However, $\mathsf{Im}\ f'', \mathsf{Im}\ pg \subseteq B$ while $\mathsf{Im}\ x^p \nsubseteq B$. This means a is divisible by p, and therefore, f'' is divisible by p, as required. $\square$

We need some more notation. Set

$$\mathbf{E}'_n = \langle\langle d', px_1 \dots x_n \rangle\rangle \quad \text{and}$$
$$\mathbf{N}'_n = \langle\langle d', px_1 \dots x_n, e_1 \rangle\rangle.$$

Lemma 32 *Clones* $\mathbf{E}'_n, \mathbf{N}'_n, \mathbf{E}, \mathbf{N}$, $n \in \mathbb{N}$, *are distinct and are the subclones of* $\mathbf{N}$ *containing* d'.

Proof. By Lemma 27 and Corollaries 28 and 31, any subclone of $\mathbf{N}$ containing d' coincides with one of $\mathbf{E}'_n, \mathbf{N}'_n, \mathbf{E}, \mathbf{N}$, $n \in \mathbb{N}$. To prove that all those clones are distinct we use a construction which is quite similar to that used in [12, 4].

Let $V = \{(0,0), (0,1), \dots, (0, p-1)\}$ be treated as one-dimensional GF(p)-vector space (note that V is closed under $\oplus$) and let $B = (0,0)/_\mu$ as above. We define the operation $s\colon \mathbb{Z}_p^2 \to \{(0,0), (0,1)\}$ in the following way: $s((a,b)) = (0,0)$ if and only if $b = 0$. We denote elements of V^{n+1} by boldface symbols, for example, $\mathbf{w} = (w_1, \dots, w_{n+1})$. Furthermore, let H_n be the set of the linear mappings $\eta_1, \dots, \eta_{n+1}$ from V^{n+1} to V which are determined through the formula

$$\eta_i(\mathbf{v}_j) = \begin{cases} (0,1) & \text{if } i = j; \\ (0,0) & \text{otherwise} \end{cases}$$

where $\mathbf{v}_j = ((0,0), \dots, (0,0), (0,1), (0,0), \dots, (0,0))$ and the only nonzero element occurs on jth position. The symbol $\sum$ below denotes summation in the group $\mathbb{Z}_p^2$. Let

$$D_n = \left\{ \xi \in B^{V^{n+1}} : \sum_{\mathbf{v} \in V^{n+1}} \xi(\mathbf{v}) = (0,0) \right\} \cup \{ s(\eta_i) \mid \eta_i \in H_n \} \subseteq (\mathbb{Z}_p^2)^{V^{n+1}}$$

and let E_n be the subalgebra of $((\mathbb{Z}_p^2)^{V^{n+1}}; \oplus, \widehat{(0,0)}, \widehat{(0,1)}, \ldots, \widehat{(p-1,p-1)})$ generated by D_n where $\widehat{a}$ denotes the constant mapping $V^{n+1} \to \mathbb{Z}_p^2$ taking every vector to a. We will prove that E_n is preserved by operations $\oplus, e_1, px_1 \ldots x_n$ but is not preserved by $px_1 \ldots x_{n+1}$.

First, we observe that $D_n \cap B^{V^{n+1}} = E_n \cap B^{V^{n+1}}$. To see this, we prove that every $\xi \in E_n$ satisfies the condition

$$\sum_{\mathbf{v} \in V^{n+1}} \xi(\mathbf{v}) = (0,0). \tag{3}$$

For this, we check that (3) holds for $s(\eta_1), \ldots, s(\eta_{n+1})$ and all the constant mappings. Since $|V^{n+1}| = p^{n+1}$, we have

$$\sum_{\mathbf{v} \in V^{n+1}} \widehat{(c,d)}(\mathbf{v}) = p^{n+1}(c,d) = (0,0).$$

Further, representing $\mathbf{w} \in V^{n+1}$ in the form $\mathbf{w} = (w_1, \ldots, w_{n+1})$, for any $i \leq n+1$, we have $s(\eta_i)(\mathbf{w}) = (0,1)$ if $w_i \neq 0$, and $s(\eta_i)(\mathbf{w}) = (0,0)$ otherwise. Therefore

$$\sum_{\mathbf{v} \in V^{n+1}} s(\eta_i)(\mathbf{w}) = \sum_{\substack{(w_1,\ldots,w_{n+1}) \in V^{n+1} \\ w_i \neq 0}} (0,1) = p^n(p-1)(0,1) = (0,0).$$

Thus, since $\oplus$ preserves (3), we get the required result.

The equality $e_1(x \oplus y) = e_1(x) \oplus e_1(y)$ implies that (3) holds for $e_1(\xi)$ whenever it holds for $\xi \in (\mathbb{Z}_p^2)^{V^{n+1}}$. Since $e_1(\xi) \in B^{V^{n+1}}$, the set E_n is closed under e_1. Then check that $px_1 \ldots x_k$, $k \leq n$, preserves E_n. As $px(y \oplus z) = p(xy \oplus xz) = pxy \oplus pxz$, it suffices to check that $\xi = px_1 \ldots x_k \in E_n$ when $x_1, \ldots, x_k$ are elements of the generating set. If one of the x_i belongs to $B^{V^{n+1}}$ then ξ is the zero mapping. In the case when $x_i = \widehat{(c,d)}$ we have $\xi = dpx_1 \ldots x_{i-1}x_{i+1} \ldots x_k$. So we may assume that $x_1, \ldots, x_k \in \{s(\eta_1), \ldots, s(\eta_{n+1})\}$. Let $x_i = s(\eta_{j_i})$ for $i = 1, \ldots, k$. Since $k \leq n$, there is some j such that $j \notin \{j_1, \dots, j_k\}$. Without loss of generality, we may assume $j = 1$. Then

$$\begin{aligned}
\sum_{\mathbf{w}\in V^{n+1}} \xi(\mathbf{w}) &= \sum_{(w_1,\dots,w_{n+1})\in V^{n+1}} ps(w_{j_1})\dots s(w_{j_k}) \\
&= \sum_{(w_2,\dots,w_{n+1})\in V^{n}} p(ps(w_{j_1})\dots s(w_{j_k})) \\
&= (0,0).
\end{aligned}$$

Next we prove that $px_1 \dots x_{n+1}$ does not preserve E_n. Putting $\xi = ps(\eta_1)\dots s(\eta_{n+1})$ we get

$$\begin{aligned}
\sum_{\mathbf{w}\in V^{n+1}} \xi(\mathbf{w}) &= \sum_{(w_1,\dots,w_{n+1})\in V^{n+1}} ps(w_1)\dots s(w_{n+1}) \\
&= p \sum_{w_1\in V} s(w_1) \left(\sum_{(w_2,\dots,w_{n+1})\in V^{n+1}} s(w_2)\dots s(w_{n+1}) \right) \\
&= p\Big(\sum_{w_1\in V} s(w_1) \Big) \Big(\sum_{(w_2,\dots,w_{n+1})\in V^{n+1}} s(w_2)\dots s(w_{n+1}) \Big) \\
&= p(p-1)\Big(\sum_{(w_2,\dots,w_{n+1})\in V^{n+1}} s(w_2)\dots s(w_{n+1}) \Big) \\
&= \dots \\
&= p(p-1)^{n+1} \neq (0,0).
\end{aligned}$$

To prove that $\mathbf{E}_m \neq \mathbf{N}_n$ we observe that $e_1 \notin \mathbf{E}$. Actually, e_1 is an idempotent non-constant and non-surjective unary operation, while $\mathbf{E}$ is an E-minimal clone. $\square$

Since by Lemma 22, $d \in \mathbf{E}'_p$ and $d' \in \mathbf{E}_p$, $\mathbf{E}_n = \mathbf{E}'_n$ and $\mathbf{N}_n = \mathbf{N}'_n$ for all $n \geq p$.

Before completing this section we consider case (j) and give the required examples of clones in cases (c)–(e), and (g)–(i).

Lemma 33 *If a polynomial clone contains d' and has the congruence lattice of type (j), then it is equal to* $\mathsf{Pol}\ \mathbb{Z}_p^2$.

Proof. Let $\mathbf{C}$ be a clone from case (j) and $\mathbb{A} = (A; \mathbf{C})$. As is easily seen, $[\underline{1}, \underline{1}] = \underline{0}$, i.e., $\mathbb{A}$ is Abelian. Therefore it is polynomially equivalent to a module over a ring R where R can be treated as a subring of the endomorphism ring of the group $\mathbb{Z}_p^2$.

If $\mathbb{A}$ is minimal, then it is polynomially equivalent to a vector space and, since $d' \in \mathbf{C}$, the vector space is $\mathbb{Z}_p^2$. So suppose there is a non-constant unary operation $f \in \mathbf{C}$ such that $\mathsf{Im}\ f \neq \mathbb{Z}_p^2$. Taking $f(x) \ominus f((0,0))$, if necessary, we may assume $f((0,0)) = (0,0)$. The operation f is an endomorphism of $\mathbb{Z}_p^2$, therefore the sets $B = \{a \in \mathbb{Z}_p^2 \mid f(a) = (0,0)\}$ and $\mathsf{Im}\ f$ are subgroups of $\mathbb{Z}_p^2$. Denote by θ and η the congruences of $\mathbb{Z}_p^2$ such that B, $\mathsf{Im}\ f$ are θ- and η-blocks respectively. By the choice of f, both $\theta, \eta \neq \underline{0}, \underline{1}$. It is easy to see that θ, η are the only congruences of $\mathbb{Z}_p^2$ which are preserved by f. $\square$

We also exhibit the clones for cases (g),(h),(i) when the proper congruences are kernels of coordinate endomorphisms e_1, e_2. For other pairs of congruences the construction is quite similar. Let f_1, f_2 denote the operations

$$\begin{aligned} f_1((x_1,y_1),(x_2,y_2)) &= (0, y_1 \cdot y_2), \\ f_2((x_1,y_1),(x_2,y_2)) &= (x_1 \cdot x_2, 0). \end{aligned}$$

Then the required clones are $\langle\langle d', e_1\rangle\rangle$, $\langle\langle d', e_1, f_1\rangle\rangle$, $\langle\langle d', e_1, f_1, f_2\rangle\rangle$. Since $d' \in \mathbf{E}$, the clones presenting cases (c),(d),(e) can be found in Figure 2.

The results of this section are summarized in the following theorem.

Theorem 34 *A clone containing d' is either polynomially rich, or contains d, or is $\mathsf{Pol}\ \mathrm{GF}(p^2)$, or is one of the clones presented in the following diagram.*

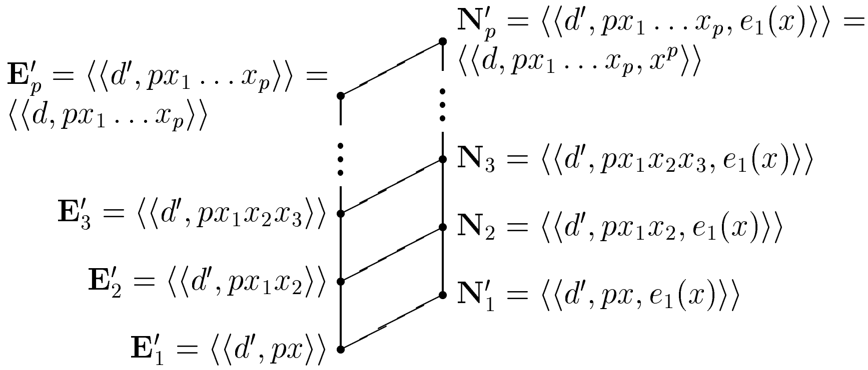


Figure 4

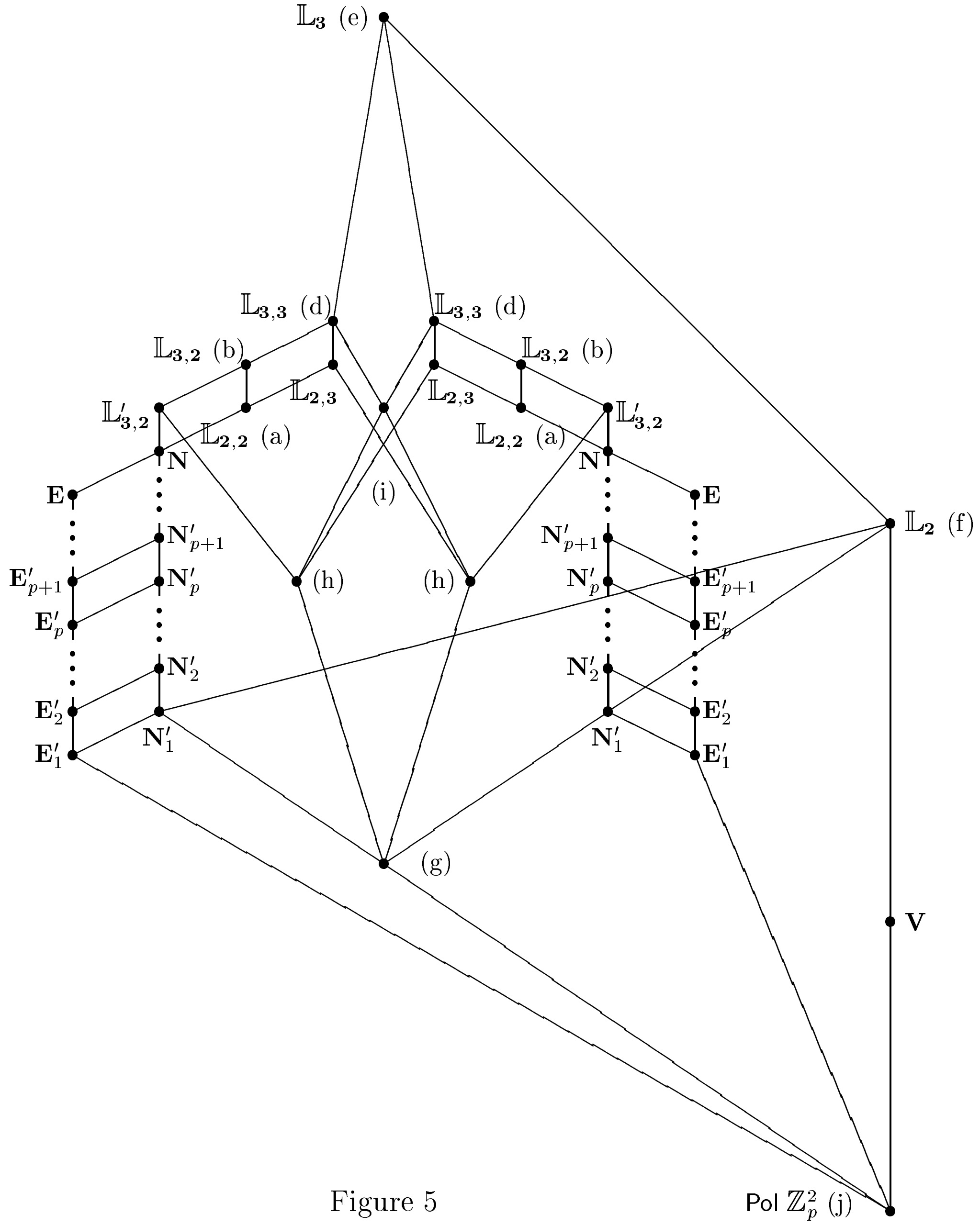


Figure 5

The lattice of all clones containing d' is too sophisticated to be drawn. However, in Figure 5 we endeavour to represent its main component, which, being repeated, forms the whole lattice. The polynomially rich clones are denoted either by the corresponding labelled lattices, or by one of the cases (a)–(j). Two simple Abelian clones on the right form the "axis" of the lattice (the clone of one-dimensional vector space is denoted by $\mathbf{V}$). Then the "ladders" consist of clones that have only one proper congruence, that is of types (a)–(d). Therefore, for each congruence of $\mathbb{Z}_p^2$, there exists a corresponding "ladder". The bottom of a "ladder" is presented in some detail in Figure 4 while the top is shown in Figure 2. The rhombus between the "ladders" consists of polynomially rich clones of types (g)–(i). Such a rhombus is assigned to each pair of congruences. So, every two of $p+1$ "ladders" are linked by a rhombus of that form.

5 Acknowledgment

The author gratefully thanks Pawel Idziak, who has inspired this work, for hours of fruitful discussions.

References

[1] I. Ágoston, L. Demetrovic, L. Hannák, *On the number of clones containing all constants,* in: Lectures in Universal Algebra, Coll. Math. Soc. János Bolyai, **43**(1983), 21–25.

[2] A. A. Bulatov, *Polynomial reducts of modules I. Rough classification,* Multiple-valued Logic, **3**(1998), 135–154.

[3] A. A. Bulatov, *Polynomial reducts of modules II. Algebras of primitive and nilpotent functions,* Multiple-valued Logic, **3**(1998), 173–193.

[4] A. A. Bulatov, P. M. Idziak, *Counting Mal'tsev clones on small sets,* Discrete Mathematics (submitted).

[5] M. Csikós, *Finitely generated clones with linear functions in P_3 and P_5*, Közl. MTA Számitástech. Automat. Kutató Int. Budapest **31**(1984), 7–21.

[6] R. Freese, R. McKenzie, *Commutator Theory for Congruence Modular Varieties*, London Math. Soc. Lecture Notes, 125, 1987.

[7] G. P. Gavrilov, *On the overstructure of the class of polynomials of multivalued logics,* [in Russian] Diskretnaja Matematika, **8**(1996), no. 3, 90–97.

[8] G. P. Gavrilov, *On closed classes of multi-valued logic that contain the class of polynomials,* [in Russian] Diskretnaja Matematika, **9**(1997), no. 2, 12–23.

[9] C. Herrmann, *Affine algebras in congruence modular varieties,* Acta Sci. Math. (Szeged), **41**(1979), 119–125.

[10] D. Hobby, R. McKenzie, *The structure of finite algebras,* Amer. Math. Soc. Contemporary Mathematics, vol. 76, Providence Rhode Island 1988.

[11] A. Hulanicki, S. Świerczkowski, *Number of algebras with a given set of elements,* Bull. Acad. Sci. Polon., Ser. Sci., math. Phys. et Astron., **8**(1960), 283–284.

[12] P. M. Idziak, *Clones with Mal'tsev operations,* International Journal of Algebra and Computation, **9**(1999), 213–226.

[13] P. M. Idziak, K. Słomczyńska, *Polynomially rich algebras,* Journal of Pure and Applied Algebra, **156**(2001), no.1, 33–68.

[14] K. A. Kearns, E. W. Kiss, *Modularity prevents tails,* Proc. of the AMS, **127**(1999), no.1, 11–19.

[15] A. A. Krokhin, K. L. Safin, E. V. Sukhanov, *On the structure of the lattice of closed classes of polynomials* [in Russian] Diskretnaja Matematika, **9**(1997), no.2, 24–40.

[16] D. Lau, *Über die Anzahl von abgeschlossenen Mengen linearer Funktionen der n-vertigen Logik,* EIK, **14**(1978), no.11, 561–563.

[17] D. Lau, *Über abgeschlossenen Mengen linearer Funktionen in mehrwertigen Logiken.* EIK, **24**(1988), no.7/8, 367–381.

[18] S. S. Marchenkov, *On clones in P_k containing homogeneous functions,* [in Russian] preprint Inst. Appl. Math. Acad. Sci. USSR, **35**(1984), 1–28.

[19] D. G. Meschaninov, *On some properties of the overstructure of classes of polynomials in P_k,* [in Russian], Mat. Zametki, **44**(1988), no.5, 673–681.

[20] R. McKenzie, *Para primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties,* Algebra Universalis **8**(1978), no.3, 336–348.

[21] A. Pixley, *Functional and affine completeness and arithmetical varieties,* Rosenberg Ivo et al., Algebras and orders. Proceedings of the NATO Advanced Study Institute and Seminaire de mathematiques superieures, Montreal, Canada, July 29–August 9, 1991. Dordrecht Kluwer Academic Publishers. NATO ASI Ser., Ser. C, Math. Phys. Sci. 389 (1993), 317–357.

[22] E. L. Post, *The two-valued iterative systems of mathematical logic* Annals of Math. Studies, no.5, Princeton University Press, N.J., 1941.

[23] A. B. Remizov, *On the overstructure of closed classes of Polynomials modulo k*, [in Russian], Diskretnaja Matematika, **1**(1989), no.1, 3–15.

[24] I. G. Rosenberg, *Clones on a prime cardinality universe containing an affine essential operation*, Tatra Mountains Math. Publ., **5**(1995), 201–215.

[25] A. A. Salomaa, *On infinitely generated sets of operations in finite algebras.* Ann. Univ. Turku, Ser.AI 74, 1964, 1–12.

[26] Á. Szendrei, *Idempotent reducts of Abelian groups,* Acta Sci. Math. (Szeged), **38**(1976), 171–182.

[27] Á. Szendrei *Idempotent reducts of modules I–II*, In: Universal Algebra (Proc. Conf. Esztergom, 1977), Colloq. Math. Soc. J.Bolyai, vol.29, 753–780.

[28] Á. Szendrei, *Clones of linear operations on finite sets,* In: Finite algebra and multiple-valued logic. (Proc. Conf. Szeged (Hungary), 1979), Colloq. Math. Soc. J.Bolyai, vol.28, 693–738.

[29] A. N. Tcherepov, *A description of the lattice of closed classes of P_k that contain the class of polynomials*, [in Russian] Probl. Kibernet., **40** (1983), 5–18.

[30] A. N. Tcherepov, *On the overstructure of the class of polynomials of P_k*, [in Russian] Proc. of seminar on Discrete Math. and Applications, MGU, Moscow, 1989, 93–96.

[31] Yu. Yanov, A. A. Muchnik, *On existence of k-valued closed classes without finite basis.* [in Russian] Dokl. AN SSSR **127** (1959), 44–46.

Andrei A. Bulatov
Dept. of Algebra and Discr. Math.
Ural State University
Lenin av. 51
620083 Ekaterinburg, Russia
andrei.bulatov@usu.ru