Clones of compatible operations on rings Z_n

Miroslav Ploščica, Ivana Varga

Šafárik's University, Košice, Slovakia

December 19, 2023

Motivation

Consider the following problems.

1. Let $f : R^n \to R$ be an n-ary operation on a ring R. Can we determine if f is expressible by a polynomial? What are the properties that distinguish the class of polynomial functions?

2. Let $(P, \leq)$ be a partially ordered set. Can we find a nice set of isotone (order preserving) operations, such that every isotone operation is a composition of functions from this set?

Clones

A *clone* on a set A is a set of finitary operations $A^n \to A$ $(n \geq 1)$ which contains all projections and is closed under composition.

Projections: $p_{n,i}(x_1, \ldots, x_n) = x_i$

Composition: For a n-ary operation f and k-ary operations $g_1, \ldots, g_n$ we define the k-ary operation $f(g_1, \ldots, g_n)$ by

$$f(g_1, \ldots, g_n)(\mathbf{x}) = f(g_1(\mathbf{x}), \ldots, g_n(\mathbf{x}))$$

for every $\mathbf{x} = (x_1, \ldots, x_k)$.

Examples

1. Polynomial operations on any ring (or any other algebraic structure) form a clone.
2. Operations preserving a given partial order (or any other relation) form a clone.

We say that an operation $f: \ A^n \to A$ preserves a relation $\alpha \subseteq A^k$ if
$(a_{11}, \ldots, a_{1k}) \in \alpha$,
$(a_{21}, \ldots, a_{2k}) \in \alpha$,
$\ldots$
$(a_{n1}, \ldots, a_{nk}) \in \alpha$
implies
$(f(a_{11}, \ldots, a_{n1}), f(a_{12}, \ldots, a_{n2}), \ldots, f(a_{1k}, \ldots, a_{nk})) \in \alpha$.

Pol-Inv correspondence

For a set C of operations on a set A let Inv(C) be the set of all relations on A preserved by every $f \in C$. (We call them *invariant relations of* C.)

For a set Σ of relations on a set A let Pol(Σ) be the set of all operations on A that preserve every $\alpha \in \Sigma$. (We call them *polymorphisms of* Σ.)

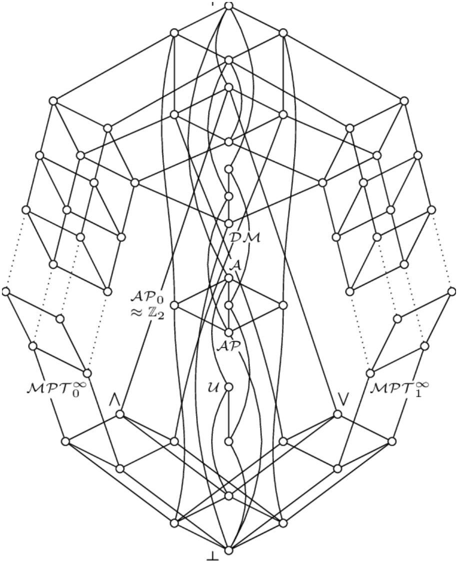
Theorem

For every clone C on a finite set A, Pol(Inv(C))$= C$.

So, on a finite set, there are two basic ways how to express a clone:

1. by giving a generating set of operations;
2. by giving a generating set of relations, i.e. expressing the clone as Pol(Σ).

Clones on 2-element set



A congruence θ of an algebra A is an equivalence relation, which is preserved by all basic operations $f: A^n \to A$ of the algebra A, that is

$$(a_1, b_1), \ldots, (a_n, b_n) \in \theta$$

implies

$$(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)) \in \theta.$$

A polynomial operation of an algebra A is a composition of basic operations of A and (unary) constant operations on A.
Clearly, every constant operation preserves every congruence.
Consequently, every polynomial operation preserves every congruence.

Compatible operations on algebras

A function $A^n \to A$ on an algebra A is called *compatible* (or *congruence-preserving*) if it preserves all congruences θ of A. Clearly,

- compatible operations form a clone $\mathrm{Comp}(A)$;
- $\mathrm{Comp}(A)$ contains $\mathrm{P}(A)$, the clone of all polynomials of A.

Notice that the clone $\mathrm{Comp}(A)$ is defined by means of invariant relations, while $\mathrm{P}(A)$ is given by a set of generators.

Algebra A is called *affine complete* if $\mathrm{Comp}(A) = \mathrm{P}(A)$.

Affine completeness

Affine completeness has been investigated for various kinds of algebras. In our talk we consider rings $\mathbb{Z}_n$ of integers modulo n. Well-known:

Theorem

The ring $\mathbb{Z}_n$ is affine complete if and only if n is square-free.

If n is not square-free, then we would like to investigate the interval between $\mathrm{P}(\mathbb{Z}_n)$ and $\mathrm{Comp}(\mathbb{Z}_n)$ in the lattice of clones. We denote this interval by $I(n)$.

Reduction to prime power

(Implicitly in Remizov 1989)

Theorem

If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ where $p_1, \dots, p_k$ are distinct primes, then the interval $I(n)$ is (as a lattice) isomorphic to

$$I(p_1^{\alpha_1}) \times \cdots \times I(p_k^{\alpha_k}).$$

So, in order to describe $I(n)$, we need to describe $I(p^k)$, that is to investigate the rings $\mathbb{Z}_n$, where $n = p^k$ is a prime power.

$n = p^2$

Theorem

The lattice $I(p^2)$ has two elements, that is, $\mathrm{Comp}(\mathbb{Z}_{p^2})$ covers $\mathrm{P}(\mathbb{Z}_{p^2})$.

(proved by Remizov 1989, Bulatov 2002, MP+IV 2021)
More information:
1. The clone $\mathrm{Comp}(\mathbb{Z}_{p^2})$ is generated by polynomials and any compatible nonpolynomial operation, for instance

$$\sigma(x,y) = \begin{cases} p, & \text{if } x, y = 0 \\ 0, & \text{otherwise.} \end{cases}$$

2. An operation on $\mathbb{Z}_{p^2}$ (any arity) is polynomial if and only if it preserves the congruence mod p and the 4-ary relation V defined as follows.

$(x_1, x_2, x_3, x_4) \in V$ if and only if

(V1) $x_1 - x_2 - x_3 + x_4 = 0$;

(V2) $x_i \equiv x_j (\mathrm{mod}\, p)$ for every $i, j \in \{1, 2, 3, 4\}$.

Where does this relation come from?

Commutators

If α and β are congruences of an algebra A, then $M(\alpha, \beta)_A$ is the subalgebra of A^4 generated by all 4-tuples of the form (a, a', a, a') with $(a, a') \in \alpha$ and (b, b, b', b') with $(b, b') \in \beta$. The elements of $M(\alpha, \beta)_A$ are usually considered as matrices 2×2. The commutator $[\alpha, \beta]_A$ is defined as the smallest congruence γ of A with the property that $(x_1, x_2, x_3, x_4) \in M(\alpha, \beta)$ and $(x_1, x_2) \in \gamma$ imply $(x_3, x_4) \in \gamma$.

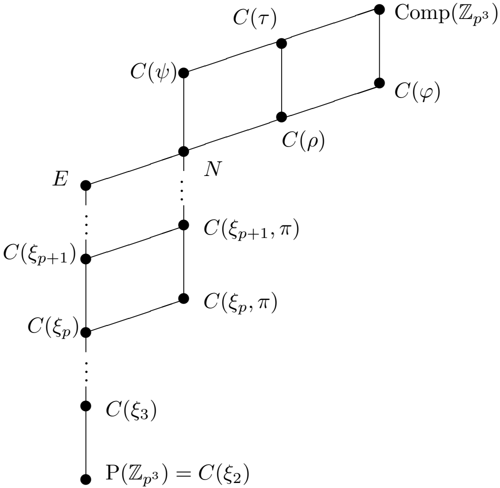
The relation V coincides with $M(\bmod p, \bmod p)$ calculated in the ring $\mathbb{Z}_{p^2}$. Its shape shows that $[\bmod p, \bmod p] = 0$. This will change when we expand the type of $\mathbb{Z}_{p^2}$ by the operation ρ. (The above commutator will be equal to $\bmod p$.)

$n = p^3$

The main aim of this talk is to describe all clones in the interval $I(p^3)$, both by means of generators and invariant relations.

The clone generated by the ring polynomials and nonpolynomial compatible operations f_1, ..., f_k will be denoted $C(f_1, \ldots, f_k)$.

Lattice $I(p^3)$



$\mathrm{Comp}(\mathbb{Z}_{p^3})$
$C(\tau)$
$C(\psi)$
$C(\varphi)$
$C(\rho)$
N
E
$C(\xi_{p+1}, \pi)$
$C(\xi_{p+1})$
$C(\xi_p, \pi)$
$C(\xi_p)$
$C(\xi_3)$
$\mathrm{P}(\mathbb{Z}_{p^3}) = C(\xi_2)$

Operations in our picture

The i-ary operation ξ_i on $\mathbb{Z}_{p^3}$ is defined by

$$\xi_i(\mathbf{x}) = \begin{cases} p^2 k_1 k_2 \dots k_i, & \text{if } \mathbf{x} = (k_1 p, \dots, k_i p) \text{ for some } k_1, \dots, k_i \\ 0, & \text{otherwise.} \end{cases}$$

The operation π is unary:

$$\pi(x) = \begin{cases} pk^p, & \text{if } x = kp \text{ for some } k \in \{0, \dots, p^2 - 1\} \\ 0, & \text{otherwise.} \end{cases}$$

Operations in our picture

The remaining operations ψ, ρ, τ and φ are binary, defined are as follows:

$$\psi(x,y)=\begin{cases} pk^p l^p, & \text{if } x=kp, y=lp \text{ for some } k,l\in\{0,\dots,p^2-1\} \\ 0, & \text{otherwise.}\end{cases}$$

$$\rho(x,y)=\begin{cases} pk^p (l^p-l), & \text{if } x=kp, y=lp \text{ for some } k,l\in\{0,\dots,p^2-1\} \\ 0, & \text{otherwise.}\end{cases}$$

$$\varphi(x,y)=\begin{cases} klp^2, & \text{if } x=kp^2, y=lp^2 \text{ for some } k,l\in\{0,\dots,p-1\} \\ 0, & \text{otherwise.}\end{cases}$$

$$\tau(x,y)=\begin{cases} klp, & \text{if } x=kp, y=lp \text{ for some } k,l\in\{0,\dots,p^2-1\} \\ 0, & \text{otherwise.}\end{cases}$$

Recall that the congruences of the ring $\mathbb{Z}_{p^3}$ form a 4-element chain $0 < \alpha < \beta < 1$, where $\alpha = \mathrm{mod}\, p^2$, $\beta = \mathrm{mod}\, p$.

The clones between N and $\mathrm{Comp}(\mathbb{Z}_{p^3})$ can be distinguished by relations $M(\alpha, \alpha)$, $M(\beta, \alpha)$ and $M(\beta, \beta)$ computed in the ring $\mathbb{Z}_{p^3}$. These are 4-ary relations and their explicit description is as follows.

Lemma

$(x_1, x_2, x_3, x_4) \in M(\alpha, \alpha)$ *iff*

(S1) $x_1 - x_2 - x_3 + x_4 = 0$;

(S2) $x_i \equiv x_j \pmod{p^2}$ *for every* $i, j \in \{1, 2, 3, 4\}$.

Upper part

Lemma

$(x_1, x_2, x_3, x_4) \in M(\beta, \alpha)$ *iff*

(T1) $x_1 - x_2 - x_3 + x_4 = 0$;

(T2) $x_1 \equiv x_3 (\bmod p^2)$;

(T3) $x_i \equiv x_j \pmod p$ *for every* $i, j \in \{1, 2, 3, 4\}$.

Lemma

$(x_1, x_2, x_3, x_4) \in M(\beta, \beta)$ *iff*

(U1) $x_1 - x_2 - x_3 + x_4 \equiv 0 (\bmod p^2)$;

(U2) $x_i \equiv x_j (\bmod p)$ *for every* $i, j \in \{1, 2, 3, 4\}$.

Preservation results

Theorem

- $M(\alpha, \alpha)$ *is preserved by* τ *and not preserved by* φ*;*
- $M(\beta, \alpha)$ *is preserved by* ψ *and not preserved by* ρ*;*
- $M(\beta, \beta)$ *is preserved by* φ *and not preserved by* ψ*;*

Relational descriptions

Theorem

- $f \in \mathrm{Comp}(\mathbb{Z}_{p^3})$ *iff it preserves congruences;*
- $f \in C(\tau)$ *iff it preserves congruences and* $M(\alpha, \alpha)$*;*
- $f \in C(\psi)$ *iff it preserves congruences and* $M(\beta, \alpha)$*;*
- $f \in C(\varphi)$ *iff it preserves congruences and* $M(\beta, \beta)$*;*
- $f \in C(\rho)$ *iff it preserves congruences,* $M(\alpha, \alpha)$ *and* $M(\beta, \beta)$*;*
- $f \in N$ *iff it preserves congruences,* $M(\beta, \alpha)$ *and* $M(\beta, \beta)$*.*

Consequences for commutators

Let $C \in I(p^3)$.

- $[\alpha, \alpha]_C = 0$ iff $C \subseteq C(\tau)$;
- $[\beta, \alpha]_C = 0$ iff $C \subseteq C(\psi)$;
- $[\beta, \beta]_C = \alpha$ iff $C \subseteq C(\varphi)$.

Lower part

The clones between $P(\mathbb{Z}_{p^3})$ and N have the same values of commutators. To distinguish them we can use the concept of n-ary commutator, introduced by Bulatov (2001).

For an integer $n \geq 3$ let P_n be the power set of $\{1, \ldots, n\}$. We use P_n for indexing 2^n-ary relations.

Let $\alpha_1, \ldots, \alpha_n$ be congruences of an algebra A. Let $M(\alpha_1, \ldots, \alpha_n)_A$ be the subalgebra of A^{2^n} generated by all 2^n-tuples $(\mathbf{u}(i, a, a')_J \mid J \in P_n)$, where $i \in \{1, \ldots, n\}$, $(a, a') \in \alpha_i$ and

$$\mathbf{u}(i, a, a')_J = \begin{cases} a, & \text{if } i \in J \\ a', & \text{if } i \notin J. \end{cases}$$

The n-ary commutator $[\alpha_1, \dots, \alpha_n]_A$ is defined as the smallest congruence on A satisfying for every $\mathbf{x} = (x_J \mid J \in P_n) \in M(\alpha_1, \dots, \alpha_n)_A$ the implication

$$(x_J, x_{J \cup \{n\}}) \in \gamma \text{ for every } J \subsetneq \{1, \dots, n-1\}$$

$$\implies \quad (x_{\{1,\dots,n-1\}}, x_{\{1,\dots,n\}}) \in \gamma.$$

(Bulatov has not defined the relation $M(\alpha_1, \dots, \alpha_n)$ explicitly. It was investigated later by Shaw(2014) and Opršal (2016).)

Relations R_n

We consider the 2^n-ary relation R_n on $\mathbb{Z}_{p^3}$, such that $\mathbf{x} = (x_J \mid J \in P_n) \in R_n$ if and only if the following conditions are satisfied:

(R1) $\sum_{K \in P_n} (-1)^{|K|} x_K = 0$.

(R2) $\sum_{K \subseteq J} (-1)^{|K|} x_K \equiv 0 \pmod{p^2}$ for every $J \in P_n$, $|J| \geq 2$;

(R3) $x_J \equiv x_\emptyset \pmod{p}$ for every $J \in P_n$;

Lemma

The relation R_n coincides with $M(\beta, \beta, \ldots, \beta)_{C(\xi_{n-1})}$ (n occurences of β). (Computed in the ring $\mathbb{Z}_{p^3}$ enhanced with the operation ξ_{n-1}.)

Preserving R_n

Theorem

The 2^n-ary relation R_n is preserved by ξ_{n-1} and π and not preserved by ξ_n.

Consequence:

Theorem

$f \in C(\xi_{n-1}, \pi)$ iff it preserves congruences and R_n.

Consequence:

Theorem

- *Let $n \leq p$. The n-ary commutator $[\beta, \ldots, \beta]_C$ is equal to 0 iff $C \subseteq C(\xi_{n-1})$.*
- *Let $n > p$. The n-ary commutator $[\beta, \ldots, \beta]_C$ is equal to 0 iff $C \subseteq C(\xi_{n-1}, \pi)$.*

Similarity of $\mathbb{Z}_{p^3}$ and $\mathbb{Z}_{p^2}$

It remains to distinguish $C(\xi_n)$ and $C(\xi_n, \pi)$. We define the 4-ary relation Q as follows:
$(x_1, x_2, x_3, x_4) \in Q$ if and only if the following conditions are satisfied:

(Q1) $x_1 - px_2 - x_3 + px_4 = 0$;

(Q2) $x_1 \equiv x_3 \pmod{p^2}$;

(Q3) $x_i \equiv x_j \pmod{p}$ for every $i, j \in \{1, \dots, 4\}$.

It is a relation connected with the similarity of the rings $\mathbb{Z}_{p^3}$ and $\mathbb{Z}_{p^2}$ in the sense of Commutator theory.

Preserving Q

Theorem

The relation Q is preserved by ξ_n for every n and not preserved by π.

Consequence:

Theorem

$f \in C(\xi_{n-1})$ iff it preserves congruences, R_n and Q. $(n > p)$

Especially:

Theorem

- *Let $p > 2$. Then $f \in P(\mathbb{Z}_{p^3})$ iff it preserves congruences and R_3.*
- *Let $p = 2$. Then $f \in P(\mathbb{Z}_{p^3})$ iff it preserves congruences, R_3, and Q.*

Reduction

Theorem

$I(p^{k+1})$ is isomorphic to the interval between $E_2(\mathbb{Z}_{p^k})$ and $\mathrm{Comp}(\mathbb{Z}_{p^k})$, where the clone $E_2(\mathbb{Z}_{p^k})$ is generated by the group polynomials (i.e. linear functions) and the operation $h(x,y) = pxy$.

For instance, the description of $I(p^4)$ requires a study of an interval in the lattice of clones on $\mathbb{Z}_{p^3}$ whose upper part is $I(p^3)$ descibed in this talk.

A slightly more general problem is

Problem

Describe all extensions of the clone of all linear functions on $\mathbb{Z}_{p^3}$.

Some clones on $\mathbb{Z}_8$

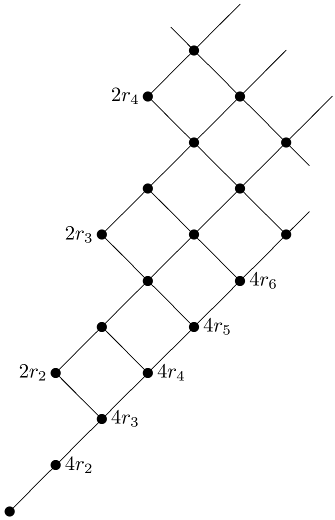
Denote

$$r_n = x_1 x_2 \dots x_n,$$

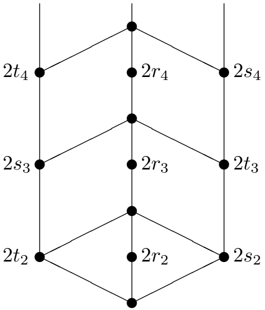
$$s_n = x_1 x_2 \dots x_n (x_1 + x_2 + \dots + x_n),$$

$$t_n = r_n + s_n.$$

Some clones on $\mathbb{Z}_8$



Some clones on $\mathbb{Z}_8$



Thanks

Thank you for attention.