Clones between Group $(\mathbb{Z}_8, +)$ and Ring $(\mathbb{Z}_8, +, \cdot)$

Radka Schwartzová

Miroslav Ploščica

Pavol Jozef Šafárik University
SSAOS 2025,
Českovice, Czech Republic

8.9.2025

Funded by the European Union
NextGenerationEU

Funded by the EU NextGenerationEU through the Recovery and Resilience Plan for Slovakia under the project No. 09I03-03-V05-00008.

Contents

Lattice of Clones on a Set

Lemma

An intersection of any system of clones on a set A forms a clone on A.

Lemma

All clones on a set A form a complete lattice.

Lattice of Clones on a Set

Lemma

An intersection of any system of clones on a set A forms a clone on A.

Lemma

All clones on a set A form a complete lattice.

Lemma

An intersection of any system of clones on a set A forms a clone on A.

Lemma

All clones on a set A form a complete lattice.

If $|A| = 1$, then the clone lattice on A consists of one clone.

Lattice of Clones on a Set

Lemma

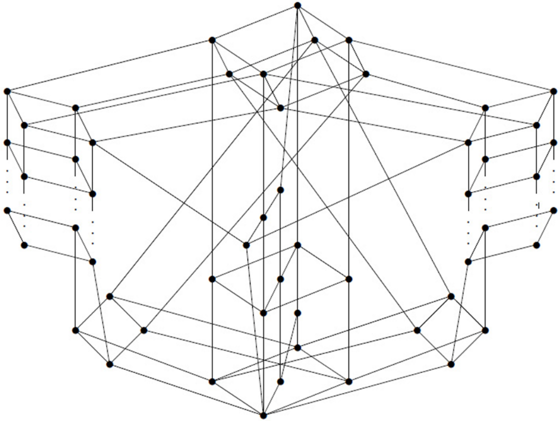
An intersection of any system of clones on a set A forms a clone on A.

Lemma

All clones on a set A form a complete lattice.

If $|A| = 1$, then the clone lattice on A consists of one clone.

If $|A| = 2$, then the clone lattice on A consists of countably many clones (Post's Lattice).



Lattice of Clones on a Set

Lemma

An intersection of any system of clones on the set A forms a clone on A.

Lemma

All clones on a set A form a complete lattice.

- *If $|A| = 1$, then the clone lattice on A consists of one clone.*
- *If $|A| = 2$, then the clone lattice on A consists of countably many clones (Post's Lattice).*
- *If $|A| > 2$, then the clone lattice on A consists of uncountable clones.*

Interval $\mathcal{J}_n$ in the Clone Lattice

$\mathcal{J}_n = \langle P(\mathbb{Z}_n, +), P(\mathbb{Z}_n, +, \cdot) \rangle$

Interval $\mathcal{J}_n$ in the Clone Lattice

$\mathcal{J}_n = \langle P(\mathbb{Z}_n, +), P(\mathbb{Z}_n, +, \cdot) \rangle$

The elements of $P(\mathbb{Z}_n, +)$ are all linear functions in the following form

$$p(x_1, \ldots, x_n) = a_0 + a_1 x_1 + a_2 x_2 + \cdots + a_n x_n,$$

where $a_0 \in \mathbb{Z}_n$, $a_1, \ldots, a_n \in \mathbb{Z}$.

Interval $\mathcal{J}_n$ in the Clone Lattice

$\mathcal{J}_n = \langle P(\mathbb{Z}_n, +), P(\mathbb{Z}_n, +, \cdot) \rangle$

The elements of $P(\mathbb{Z}_n, +)$ *are all linear functions in the following form*

$$p(x_1, \ldots, x_n) = a_0 + a_1 x_1 + a_2 x_2 + \cdots + a_n x_n,$$

where $a_0 \in \mathbb{Z}_n$, $a_1, \ldots, a_n \in \mathbb{Z}$.

The elements of $P(\mathbb{Z}_n, +, \cdot)$ *are all polynomial functions in the following form*

$$q(\mathbf{x}) = \sum_{\alpha} a_\alpha \mathbf{x}^\alpha,$$

where $\mathbf{x} = (x_1, \ldots, x_n)$*, the sum consists of finitely many tuples* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *of natural numbers, coefficients* a_α *belong to the set* $\mathbb{Z}_n$ *and* $\mathbf{x}^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$.

What Is Already Known about the Interval $\mathcal{J}_n = \langle P(\mathbb{Z}_n,+), P(\mathbb{Z}_n,+,\cdot)\rangle$?

Solved cases:

- $n =$ prime number p (Rosenberg, 1970)

$\mathfrak{J}_p$

What Is Already Known about the Interval $\mathcal{J}_n = \langle P(\mathbb{Z}_n, +), P(\mathbb{Z}_n, +, \cdot)\rangle$?

Solved cases:

- $n =$ prime number p (Rosenberg, 1970)

$\mathcal{J}_p$

Lemma

Let n, m be prime numbers. If $(m, n) = 1$, then

$$\mathcal{J}_{mn} \cong \mathcal{J}_m \times \mathcal{J}_n.$$

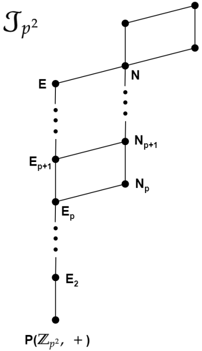
Corollary

It suffices to investigate the case $n = p^k$, where p is a prime number.

What Is Already Known about the Interval $\mathcal{J}_{p^k} = \langle P(\mathbb{Z}_{p^k}, +), P(\mathbb{Z}_{p^k}, +, \cdot)\rangle$?

Solved cases:

- $n = p^2$, where p is prime number (Krokhin et al. 1997; Idziak and Bulatov, 2003)



Open problem

What is the structure of the clone lattice of the interval $\mathcal{J}_{p^3}$?

Our result:
A complete characterization of the interval $\langle P(\mathbb{Z}_8, +), M_1 \rangle \subseteq \mathcal{J}_8$ in the clone lattice, where

$$\mathcal{J}_8 = \langle P(\mathbb{Z}_8, +), P(\mathbb{Z}_8, +, \cdot) \rangle, \quad (p = 2).$$

Used tools:

- 2^k-ary relations, where their elements are $\mathbf{x} = (x_A |\ A \in \mathcal{P}_k)$.
- (Möbius basis) We define $\mathbf{g}^A = (g_B^A\ | B \in \mathcal{P}_k) \in \mathbb{Z}_8^{P_k}$ for every $A \in \mathcal{P}_k$ as follows

$$g_B^A = \begin{cases} 1, & \text{if } A \subseteq B; \\ 0, & \text{otherwise.} \end{cases}$$

Lemma

Every $\mathbf{x} \in \mathbb{Z}_8^{\mathcal{P}_k}$ can be expressed in the form

$$\mathbf{x} = \sum_{A \in \mathcal{P}_k} a_A \mathbf{g}^A,$$

where

$$a_A = (-1)^{|A|} \sum_{B \subseteq A} (-1)^{|B|} x_B$$

for every $A \in \mathcal{P}_k$. The expression of the element $\mathbf{x}$ in this form is uniquely determined.

Definition of the Clone M_1 via an Invariant Relation

The clone M_1 consists of all ring polynomials $\mathbb{Z}_8$ that preserve the relation Z.

Definition

The relation Z is 2^4-ary relation on $\mathbb{Z}_8$, that consists of all elements $\mathbf{u} = (u_A \mid A \in \mathcal{P}_4)$ satisfying:

(1) $a_2 \equiv 2a_1 \pmod 4$, $a_4 \equiv 2a_3 \pmod 4$;

(2) $a_A \equiv 0 \pmod 2$, *if* $|A| \geq 2$;

(3) $a_A \equiv 0 \pmod 4$, *if* $|A| \geq 2$, $A \cap \{2, 4\} \neq \emptyset$;

(4) $a_A = 0$, *if* $\{2, 4\} \subseteq A$.

Definition of the Clone M_1 by Its Generators

Definition

Let $f(x_1, \ldots, x_n)$ be a polynomial with variables $x_1, \ldots, x_n$. A polynomial $f(x_1, \ldots, x_n)$ is fully divisible if it is divisible by $x_1 x_2 \ldots x_n$.

Lemma (Bulatov)

Every clone on the interval $\mathcal{J}_{p^k}$ is generated by its fully divisible members.

Definition of the Clone M_1 by Its Generators

Lemma

Let be $n \geq 2$, then n-ary fully divisible polynomial on $\mathbb{Z}_8$ preserve the relation Z iff it can be expressed in the form

$$f = 2x_1 \dots x_n(\sum_{i=1}^{n} a_i x_i^2 + \sum_{i=1}^{n} b_i x_i + c),$$

where $a_i, b_i \in \{0, 1\}$ for all i a $c \in \{0, 1, 2, 3\}$.

Definition of the Clone M_1 by Its Generators

Lemma

Let be $n \geq 2$, then n-ary fully divisible polynomial on $\mathbb{Z}_8$ preserve the relation Z iff it can be expressed in the form

$$f = 2x_1 \dots x_n(\sum_{i=1}^{n} a_i x_i^2 + \sum_{i=1}^{n} b_i x_i + c),$$

where $a_i, b_i \in \{0, 1\}$ for all i a $c \in \{0, 1, 2, 3\}$.

Lemma

Unary fully divisible polynomial on $\mathbb{Z}_8$ preserve Z iff it can be expressed in the form

$$f = ax^3 + bx^2 + cx,$$

where a, b are even.

What Are the Generators of Clones on the Interval $\langle P(\mathbb{Z}_8, +), M_1 \rangle \subseteq \mathcal{J}_8$?

Let us denote some n-ary $(n \geq 1)$ operations on $\mathbb{Z}_8$:

$$r_n = x_1 x_2 \ldots x_n;$$

$$t_n = \begin{cases} x_1 x_2 \ldots x_n (x_1 + \cdots + x_n), & \text{if } n \text{ is even;} \\ x_1 x_2 \ldots x_n (x_1 + \cdots + x_n + 1), & \text{if } n \text{ is odd;} \end{cases}$$

$$s_n = \begin{cases} x_1 x_2 \ldots x_n (x_1 + \cdots + x_n), & \text{if } n \text{ is even;} \\ x_1 x_2 \ldots x_n (x_1 + \cdots + x_n + 1), & \text{if } n \text{ is odd;} \end{cases}$$

$$u_n = x_1 x_2 \ldots x_n (x_1 + 1);$$

$$v_n = x_1 x_2 \ldots x_n (x_1 + x_2);$$

$$p_n = x_1^2 x_2 \ldots x_n;$$

$$q_n = x_1^3 x_2 \ldots x_n.$$

$C(f)$ = a clone generated by operation f, addition and constants.

What Are the Generators of Clones on the Interval $\langle P(\mathbb{Z}_8, +), M_1\rangle \subseteq \mathcal{J}_8$?

Let us denote some n-ary $(n \geq 1)$ operations on $\mathbb{Z}_8$:

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

$$t_n = \begin{cases} x_1 x_2 \dots x_n (x_1 + \dots + x_n), & \text{if } n \text{ is even;} \\ x_1 x_2 \dots x_n (x_1 + \dots + x_n + 1), & \text{if } n \text{ is odd;} \end{cases}$$

$$s_n = \begin{cases} x_1 x_2 \dots x_n (x_1 + \dots + x_n), & \text{if } n \text{ is even;} \\ x_1 x_2 \dots x_n (x_1 + \dots + x_n + 1), & \text{if } n \text{ is odd;} \end{cases}$$

$$u_n = x_1 x_2 \dots x_n (x_1 + 1);$$

$$v_n = x_1 x_2 \dots x_n (x_1 + x_2);$$

$$p_n = x_1^2 x_2 \dots x_n;$$

$$q_n = x_1^3 x_2 \dots x_n.$$

$C(f)$ = a clone generated by operation f, addition and constants.

Lemma

If $C(f) \subseteq M_1$, then $C(f)$ can be expressed in the form

$$C(2t_{n_1}) \vee C(2u_{n_2}) \vee C(2v_{n_3}) \vee C(2s_{n_4}) \vee C(2p_{n_5}) \vee C(2q_{n_6}) \vee C(2r_{n_7}) \vee C(4r_{n_8}).$$

Ordering of Clones on $\langle P(\mathbb{Z}_8, +), M_1\rangle$

Lemma

Let be $n \geq 1$*, then*

(i) $C(2p_n) \subseteq C(2q_n) \subseteq C(2p_{n+1})$;

(ii) $C(2p_n) \subseteq C(2r_{n+1}) \subseteq C(2q_{n+1}) \cap C(2r_{n+2})$;

(iii) $C(2s_n) \cup C(2u_n) \subseteq C(2r_{n+1})$;

(iv) $C(2v_{n+1}) \subseteq C(2q_n)$;

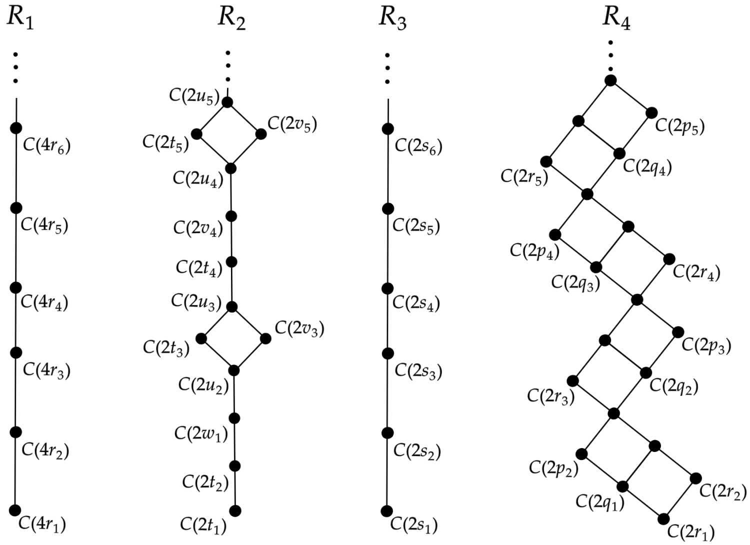
(v) $C(2q_1) \subseteq C(2u_2)$;

(vi) *if* n *is odd, then* $C(2s_n) \subseteq C(2p_n)$;

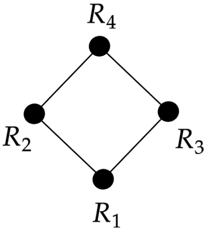
(vii) *if* n *is even, then* $C(2s_n) \subseteq C(2q_n)$;

(viii) $C(2r_n) \subseteq C(2p_{n+1}) \subseteq C(2r_{n+2})$.

$\vdots$


R_1
$C(4r_6)$
$C(4r_5)$
$C(4r_4)$
$C(4r_3)$
$C(4r_2)$
$C(4r_1)$
R_2
$C(2u_5)$
$C(2v_5)$
$C(2t_5)$
$C(2u_4)$
$C(2v_4)$
$C(2t_4)$
$C(2u_3)$
$C(2v_3)$
$C(2t_3)$
$C(2u_2)$
$C(2w_1)$
$C(2t_2)$
$C(2t_1)$
R_3
$C(2s_6)$
$C(2s_5)$
$C(2s_4)$
$C(2s_3)$
$C(2s_2)$
$C(2s_1)$
R_4
$C(2p_5)$
$C(2q_4)$
$C(2r_5)$
$C(2p_4)$
$C(2r_4)$
$C(2q_3)$
$C(2p_3)$
$C(2q_2)$
$C(2r_3)$
$C(2p_2)$
$C(2r_2)$
$C(2q_1)$
$C(2r_1)$

Ordering of Clones on $\langle P(\mathbb{Z}_8, +), M_1 \rangle$



Definition of the Clones via Invariant Relations

We define the following conditions depending on k:

(C1) $a_{2m} \equiv 2a_{2m-1} \pmod 4$ for $m = 1, \dots, k$;

(C2) $a_A = 0 \pmod 2$, if $|A| \geq 2$;

(C3) $a_A = 0 \pmod 4$, if $|A| \geq 2$, $A \nsubseteq N$;

(C4) $a_{N_m} + 2a_N = 0$, for $m = 1, \dots, k$;

(C5) $a_{N_m} = 0$ for $m = 1, \dots, k$;

(C6) $a_{N_1} + \cdots + a_{N_k} + 2a_N = 0$;

(C7) $a_{N_1} + \cdots + a_{N_k} = 0$;

(C8) $a_{N_1} = \cdots = a_{N_k}$;

(C9) $2a_N = 0$;

where $N = \{1, 3, 5, \dots, 2k-1\}$, $N_m = \{\{1, 3, 5, \dots, 2k-1\} - \{2m-1\}\} \cup \{2m\}$ for $m = 1, \dots, k$.

Definition

Let be $n = 4, 5, 6, 7, 8, 9$, then H_n is $2^{2^{k}}$-ary relation on $\mathbb{Z}_8$, that consists of all elements satisfying (C1), (C2), (C3) a (Cn).

	H_4	H_5	H_8	H_9
$2t_n$	$n < k$	$n < k$	$n < k+1$	$n < \infty$
$2u_n$	$n < k$	$n < k$	$n < k$	$n < \infty$
$2v_n$	$n < k$	$n < k$	$n < k$	$n < \infty$
$2s_n$	$n < k$	$n < \infty$	$n < \infty$	$n < k$
$2p_n$	$n < k$	$n < k$	$n < k$	$n < k$
$2q_n$	$n < k-1$	$n < k-1$	$n < k-1$(*)	$n < k$
$2r_n$	$n < k+1$	$n < k$	$n < k+1$	$n < k$
$4r_n$	$n < \infty$	$n < \infty$	$n < \infty$	$n < \infty$

	H_6 k even	H_6 k odd	H_7 k even	H_7 k odd
$2t_n$	$n < k+1$	$n < k$	$n < k+1$	$n < k$
$2u_n$	$n < k$	$n < k$	$n < k$	$n < k$
$2v_n$	$n < k+1$	$n < k+1$	$n < k+1$	$n < k+1$
$2s_n$	$n < k$	$n < k$	$n < \infty$	$n < \infty$
$2p_n$	$n < k+1$	$n < k$	$n < k$	$n < k+1$
$2q_n$	$n < k$	$n < k$	$n < k$	$n < k$
$2r_n$	$n < k$	$n < k+1$	$n < k+1$	$n < k$
$4r_n$	$n < \infty$	$n < \infty$	$n < \infty$	$n < \infty$

Definition

Let be $2 \leq l \leq k$. $R_{k,l}$ is 2^k-ary relation on $\mathbb{Z}_8$, where all elements satisfy the following conditions

(D1) $a_A = 0 \pmod 2$, *if* $|A| \geq 2$;

(D2) $a_A = 0 \pmod 4$, *if* $|A| \geq l$;

(D3) $a_{\{1,\ldots,k\}} = 0$.

$2t_n$	$n < k - l + 2$ a $n < k - 1$
$2u_n$	$n < k - l + 2$ a $n < k - 1$
$2v_n$	$n < k - l + 2$ a $n < k - 1$
$2s_n$	$n < l$ a $n < k - 1$
$2p_n$	$n < k - l + 2$ a $n < l$
$2q_n$	$n < k - l + 1$, $n < k - 2$ a $n < l$
$2r_n$	$n < k - l + 2$ a $n < l$
$4r_n$	$n < k$

Thank you for your attention :)