EXPANSIONS OF $(\mathbb{Z}_p \times \mathbb{Z}_q, +)$

Stefano Fioravanti
June 2019, SANDGAL19
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER
UNIVERSITY LINZ

Clones

Definition

A **clone (closed set of operations)** on a set A is a subset of $\bigcup_{n\in\mathbb{N}} A^{A^n}$ which contains all the projections and is closed under composition.

Definition

Let $\mathbf{A} = (A, +, (f_i)_{i\in I})$ be an algebra. A $+$**-clone** of $\mathbf{A}$ is a clone which contains $+$.

Clones

Definition

A **clone (closed set of operations)** on a set A is a subset of $\bigcup_{n\in\mathbb{N}} A^{A^n}$ which contains all the projections and is closed under composition.

Definition

Let $\mathbf{A} = (A, +, (f_i)_{i\in I})$ be an algebra. A $+$**-clone** of $\mathbf{A}$ is a clone which contains $+$.

Our goal:

Theorem (SF)

Let p and q be different prime numbers. Then there are only finitely many expansions of $(\mathbb{Z}_p \times \mathbb{Z}_q, +)$.

Known results

[1] E. Aichinger, P. Mayr, Polynomial clones on groups of order pq, in: Acta Mathematica Hungarica, Volume 114, Number 3, Page(s) 267-285, 2007. (All 17 clones containing $(\mathbb{Z}_p \times \mathbb{Z}_q, +, (1,1))$);

[2] A. A. Bulatov, Polynomial clones containing the Mal'cev operation of the groups $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$, in: Mult.-Valued Log. 8(2) (2002) 193-221 (Multiple-valued logic in Eastern Europe). (All infinitely many clones containing $(\mathbb{Z}_p \times \mathbb{Z}_p, +, (1,0), (0,1))$);

[3] S. Kreinecker, Closed function sets on groups of prime order, Manuscript, arXiv:1810.09175, 2018. (All finitely many clones containing $(\mathbb{Z}_p, +)$).

Notations

We investigate clones containing $\mathrm{Clo}(\mathbb{Z}_p \times \mathbb{Z}_q, +)$. Hence $+$-clones.

Notations

We investigate clones containing $\mathrm{Clo}(\mathbb{Z}_p \times \mathbb{Z}_q, +)$. Hence $+$-clones.

We will always consider the functions of a clone of an expansions of $\mathbb{Z}_p \times \mathbb{Z}_q$ as functions from $\mathbb{Z}_p^n \times \mathbb{Z}_q^n$ split in the two components.

$$f(x_1, ..., x_n, y_1, ..., y_n) = (f_1(x_1, ..., x_n, y_1, ..., y_n),\ f_2(x_1, ..., x_n, y_1, ..., y_n)).$$

Notations

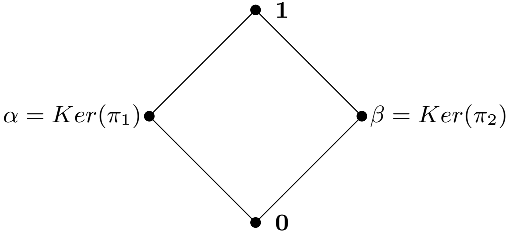
We investigate clones containing $\mathrm{Clo}(\mathbb{Z}_p \times \mathbb{Z}_q, +)$. Hence $+$-clones.

We will always consider the functions of a clone of an expansions of $\mathbb{Z}_p \times \mathbb{Z}_q$ as functions from $\mathbb{Z}_p^n \times \mathbb{Z}_q^n$ split in the two components.

$$f(x_1, ..., x_n, y_1, ..., y_n) = (f_1(x_1, ..., x_n, y_1, ..., y_n),\ f_2(x_1, ..., x_n, y_1, ..., y_n)).$$

We will always consider congruence lattices that are sublattices of:

$\mathrm{Con}((\mathbb{Z}_p \times \mathbb{Z}_q, +))$



Possible cases of labelled congruence lattices

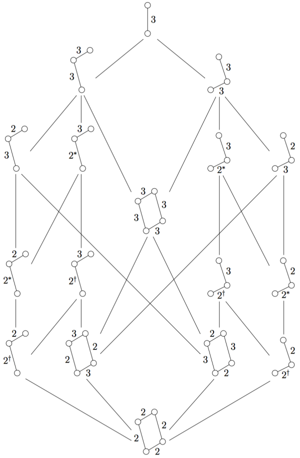


Figure: (P. Mayr's picture) Simple factors are labelled 2 if they are abelian and 3 otherwise. $2^{\dagger}$ means the factor is central; 2*means it is not central.

(p, q)-linear closed clonoids

Definition

Let p and q be powers of different primes, and let $\mathbb{F}_p$ and $\mathbb{F}_q$ be two fields of orders p and q. A (p, q)-linear closed clonoid is a non-empty subset C of $\bigcup_{n \in \mathbb{N}} \mathbb{F}_p^{\mathbb{F}_q^n}$ with the following properties:

(1) for all $f, g \in C^{[n]}$ and $a, b \in \mathbb{F}_p$:

$$af + bg \in C^{[n]};$$

(2) for all $f \in C^{[m]}$ and $A \in \mathbb{F}_q^{m \times n}$:

$$g : (x_1, \dots, x_n) \mapsto f(A \cdot (x_1, \dots, x_n)^t) \text{ is in } C^{[n]}.$$

A characterization

Theorem (SF 2018)

Let p and q be powers of different primes. Let $\prod_{i=1}^{n} p_i^{k_i}$ be the prime factorization of the polynomial $g = x^{q-1} - 1$ in $\mathbb{F}_p[x]$. Then the number of distinct (p, q)-linear closed clonoids is $2\prod_{i=1}^{n}(k_i + 1)$ and the lattice of all the (p, q)-linear closed clonoids, $\mathbf{L}(p, q)$, is isomorphic to:

$$\mathbf{2} \times \prod_{i=1}^{n} \mathbf{C}_{k_i+1}$$

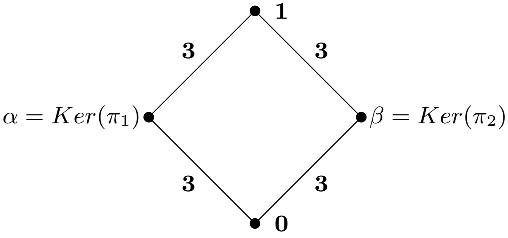
General expression of functions of $\mathbb{Z}_p \times \mathbb{Z}_q$

Lemma

Let p and q be distinct prime numbers. Then for every function f from $\mathbb{Z}_p^n \times \mathbb{Z}_q^n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ there exist two sequences of functions $\{f_{\mathbf{m}}\}_{\mathbf{m}\in\mathbb{Z}_p^n}$ from $\mathbb{Z}_q^n$ to $\mathbb{Z}_p$ and $\{s_{\mathbf{h}}\}_{\mathbf{h}\in\mathbb{Z}_q^n}$ from $\mathbb{Z}_p^n$ to $\mathbb{Z}_q$ such that for all $\mathbf{x} \in \mathbb{Z}_p^n$, $\mathbf{y} \in \mathbb{Z}_p^n$:

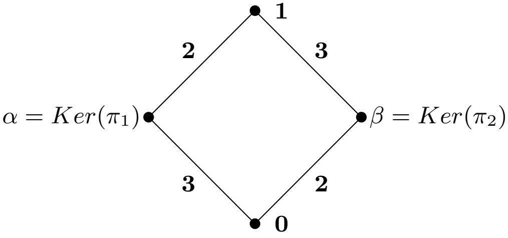
$$f(\mathbf{x}, \mathbf{y}) = \Big(\sum_{\mathbf{m}\in\mathbb{Z}_p^n} f_{\mathbf{m}}(\mathbf{y})\mathbf{x}^{\mathbf{m}} \; , \; \sum_{\mathbf{h}\in\mathbb{Z}_q^n} s_{\mathbf{h}}(\mathbf{x})\mathbf{y}^{\mathbf{h}} \Big).$$

$\mathrm{Con}(\mathbf{V})$



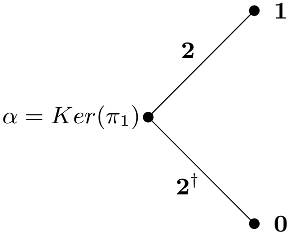
$$f(\mathbf{x}, \mathbf{y}) = \Big(\sum_{\mathbf{m} \in \mathbb{Z}_p^n} a_{\mathbf{m}} \mathbf{x}^{\mathbf{m}} \ , \ \sum_{\mathbf{h} \in \mathbb{Z}_q^n} b_{\mathbf{h}} \mathbf{y}^{\mathbf{h}} \Big).$$

Con($\mathbf{V}$)



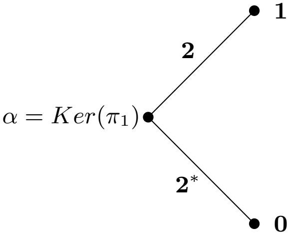
$$f(\mathbf{x},\mathbf{y}) = \Big(\sum_{\mathbf{m}\in\mathbb{Z}_p^n} a_{\mathbf{m}}\mathbf{x}^{\mathbf{m}}\ ,\ \mathbf{b}\mathbf{y} + d \Big).$$

$\mathrm{Con}(\mathbf{V})$



$$f(\mathbf{x}, \mathbf{y}) = \Big(\mathbf{ax} + c\ ,\ \mathbf{by} + f_0(\mathbf{x})\Big).$$

$\mathrm{Con}(\mathbf{V})$



$$f(\mathbf{x}, \mathbf{y}) = \Big(\mathbf{a}\mathbf{x} + c\ ,\ \mathbf{f}_1(\mathbf{x})\mathbf{y} + f_0(\mathbf{x})\Big).$$

Case of independent algebras

Definition

Two algebras $\mathbf{A}$ and $\mathbf{B}$ of the same variety $\mathbf{V}$ are **independent** if there exists a binary term in $\mathrm{Clo}(\mathbf{V})$ such that $\mathbf{A} \models t(x,y) \approx x$ and $\mathbf{B} \models t(x,y) \approx y$.

Case of independent algebras

Definition

Two algebras $\mathbf{A}$ and $\mathbf{B}$ of the same variety $\mathbf{V}$ are **independent** if there exists a binary term in $\mathrm{Clo}(\mathbf{V})$ such that $\mathbf{A} \models t(x, y) \approx x$ and $\mathbf{B} \models t(x, y) \approx y$.

Theorem (E. Aichinger, P. Mayr 2015; SF)

Let p and q be distinct prime numbers. Then for every group expansion $\mathbf{V}$ of $\mathbb{Z}_p \times \mathbb{Z}_q$ which respects the congruences $\{0, \alpha, \beta, 1\}$ it follows that:

(1) $\mathrm{Clo}(\mathbf{V}) = \mathrm{Clo}(\mathbf{V}_1) \times \mathrm{Clo}(\mathbf{V}_2)$ *for some $\mathbf{V}_1$ and $\mathbf{V}_2$ group expansions of $\mathbb{Z}_p$, and $\mathbb{Z}_q$;*

(2) $\mathrm{Clo}(\mathbf{V}_2)$ *is composed by affine functions $\Leftrightarrow [\alpha, \alpha] = 0$;*

(3) $\mathrm{Clo}(\mathbf{V}_1)$ *is composed by affine functions $\Leftrightarrow [\beta, \beta] = 0$.*

Number of expansions in the cases: $Con(\mathbb{Z}_p \times \mathbb{Z}_q, +, \mathcal{C}) = \{0, \alpha, \beta, 1\}$

$t(x, y) = mx + ny$ where

$$m \equiv_p 1 \qquad n \equiv_p 0$$

$$m \equiv_q 0 \qquad n \equiv_q 1$$

Number of expansions in the cases: $Con(\mathbb{Z}_p \times \mathbb{Z}_q, +, \mathcal{C}) = \{0, \alpha, \beta, 1\}$

$t(x, y) = mx + ny$ where

$$m \equiv_p 1 \qquad n \equiv_p 0$$
$$m \equiv_q 0 \qquad n \equiv_q 1$$

Theorem (SF, S. Kreinecker 2018)

Let p and q be distinct prime numbers. Let $n(x) := \sharp$ of divisors of $x - 1$. Then there are $(n(q) + 3) * (n(p) + 3)$ many group expansions of $\mathbb{Z}_p \times \mathbb{Z}_q$ which respect $\{0, \alpha, \beta, 1\}$. Moreover $(n(q) + 3) * 2$ of these expansions respect $[\alpha, \alpha] = 0$, $(n(p) + 3) * 2$ of these expansions respect $[\beta, \beta] = 0$, and 4 respect both.

Cases: $Con(\mathbb{Z}_p \times \mathbb{Z}_q, +, \mathcal{C}) \supseteq \{0, \alpha, 1\}$ **and** $[\alpha, \alpha] = 0$

Lemma

Let p and q distinct prime numbers. Then $\mathcal{C}$ is a clone of $\mathbb{Z}_p \times \mathbb{Z}_q$ which respects $\{\alpha, 1, 0\}$ and $[\alpha, \alpha] = 0$ if and only if for every n-ary function $f \in \mathcal{C}$ there exist: a sequence $\{a_{\mathbf{m}}\}_{\mathbf{m} \in \mathbb{Z}_p^n}$ from $\mathbb{Z}_p$, $\mathbf{f}_1 : \mathbb{Z}_p^n \mapsto \mathbb{Z}_q^n$, and $\mathbf{f}_0 : \mathbb{Z}_p^n \mapsto \mathbb{Z}_q$ such that:

$$\forall \mathbf{x} \in \mathbb{Z}_p^n, \mathbf{y} \in \mathbb{Z}_q^n \quad f(\mathbf{x}, \mathbf{y}) = \Big(\sum_{\mathbf{m} \in \mathbb{Z}_p^n} a_{\mathbf{m}} \mathbf{x}^{\mathbf{m}} \ , \ \mathbf{f}_1(\mathbf{x})\mathbf{y} + f_0(\mathbf{x}) \Big).$$

Theorem (SF)

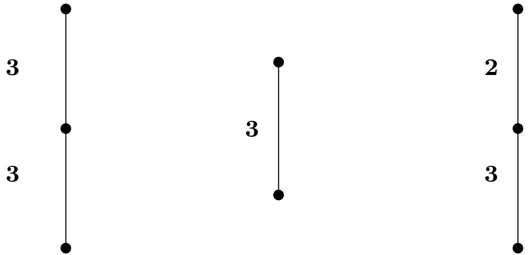
Let p and q be distinct prime numbers. Then the number n of expansions of $\mathbb{Z}_p \times \mathbb{Z}_q$ which respect $\{\alpha, 1, 0\}$ and $[\alpha, \alpha] = 0$ satisfies:

$$n \leq |L(q,p)|^2 |L(p)|,$$

where $\mathbf{L}(q,p)$ is the lattice of all (q,p)-linear closed clonoids and $\mathbf{L}(p)$ is the lattice of all $+$-clones on $\mathbb{Z}_p$.

Other cases

$Case\ 1$ $Case\ 2$ $Case\ 3$



Theorem (K. Kearnes, A. Szendrei)

If $\mathbf{A}$ is a finite algebra with a k-parallelogram term $(k > 1)$ such that $\mathbf{A}$ generates a residually small variety, then the relational clone of compatible relations of $\mathbf{A}$ is generated by relations of arity $\leqslant c$, where

$$c = max(k, c_0) \text{ and } c_0 = |A|^{|A|+1}(B(|A|+1)-1).$$

where $B(n)$ denotes the nth Bell's number.

Theorem (K. Kearnes, A. Szendrei)

If $\mathbf{A}$ is a finite algebra with a k-parallelogram term $(k > 1)$ such that $\mathbf{A}$ generates a residually small variety, then the relational clone of compatible relations of $\mathbf{A}$ is generated by relations of arity $\leqslant c$, where

$$c = max(k, c_0) \text{ and } c_0 = |A|^{|A|+1}(B(|A|+1) - 1).$$

where $B(n)$ denotes the nth Bell's number.

Theorem (SF)

Let p and q be different prime numbers. Then there are only finitely many expansions of $(\mathbb{Z}_p \times \mathbb{Z}_q, +)$.

Theorem (K. Kearnes, A. Szendrei)

If $\mathbf{A}$ is a finite algebra with a k-parallelogram term $(k > 1)$ such that $\mathbf{A}$ generates a residually small variety, then the relational clone of compatible relations of $\mathbf{A}$ is generated by relations of arity $\leqslant c$, where

$$c = max(k, c_0) \text{ and } c_0 = |A|^{|A|+1}(B(|A|+1)-1).$$

where $B(n)$ denotes the nth Bell's number.

Theorem (SF)

Let p and q be different prime numbers. Then there are only finitely many expansions of $(\mathbb{Z}_p \times \mathbb{Z}_q, +)$.

THANK YOU!!!!