Expansions of abelian square-free groups

EXPANSIONS OF ABELIAN SQUAREFREE GROUPS

STEFANO FIORAVANTI

ABSTRACT. We investigate finitary functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ for a squarefree number n. We show that the lattice of all clones on the squarefree set $\mathbb{Z}_{p_1 \cdots p_m}$ which contain the addition of $\mathbb{Z}_{p_1 \cdots p_m}$ is finite. We provide an upper bound for the cardinality of this lattice through an injective function to the direct product of the lattices of all $(\mathbb{Z}_{p_i}, \mathbb{F}_i)$-linearly closed clonoids, $\mathcal{L}(\mathbb{Z}_{p_i}, \mathbb{F}_i)$, to the $p_i + 1$ power, where $\mathbb{F}_i = \prod_{j \in \{1,\ldots,m\} \setminus \{i\}} \mathbb{Z}_{p_j}$. These lattices are studied in [Fio20] and there we can find an upper bound for their cardinality. Furthermore, we prove that these clones can be generated by a set of functions of arity at most $\max(p_1, \ldots, p_m)$.

1. Introduction

The investigation of the lattice of all clones on a set A has been a fecund field of research in general algebra with results such as Emil Post's characterization of the lattice of all clones on a two-element set [Pos41]. This branch was developed further, e. g., in [Ros69, PK79, Sze86] and starting from [KBJ05], clones are used to study the complexity of certain constraint satisfaction problems (CSPs).

The aim of this paper is to describe the lattice of those clones on the set $\mathbb{Z}_n$ that contain the operation of addition of $\mathbb{Z}_n$, with n squarefree. Thus we want to study the part of the lattice of all clones on $\mathbb{Z}_n$ which is above the clone of all linear mappings.

In [Idz99] P. Idziak characterized the number of polynomial Mal'cev clones (clones containing the constants and a Mal'cev term) on a finite set A, which is finite if and only if $|A| \leq 3$. In [Bul02] A. Bulatov shows a full characterization of all infinitely many polynomial clones on the sets $\mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ that contain $+$, where p is a prime. Moreover, a description of polynomial clones on $\mathbb{Z}_{pq}$ containing the addition for distinct primes p and q is given in [AM07] and polynomial clones containing $+$ on $\mathbb{Z}_n$, for n squarefree, are described in [May08].

Date: October 4, 2023.
2020 *Mathematics Subject Classification.* 08A40.
Key words and phrases. Clonoids, Clones.
Supported by the Austrian Science Fund (FWF): P29931.

In [Kre19] S. Kreinecker proved that there are infinitely many non-finitely generated clones above the clone $\mathrm{Clo}(\mathbb{Z}_p \times \mathbb{Z}_p, +)$ of term operations of the group $(\mathbb{Z}_p \times \mathbb{Z}_p, +)$ for any prime $p > 2$.

Let C be a set of functions. We denote by $C^{[n]}$ the subset of n-ary functions in C. In this paper we will make often use of the concept of $(\mathbb{F}, \mathbb{K})$-linearly closed clonoid as defined in [Fio20, Definition 1.1] (generalization of [Fio19, Definition 1.1]). We recall this definition.

Definition 1.1. Let $m, s \in \mathbb{N}$, let $q_1, \dots, q_m, p_1, \dots p_s$ be powers of primes, and let $\mathbb{K} = \prod_{i=1}^m \mathbb{F}_{q_i}$, $\mathbb{F} = \prod_{i=1}^s \mathbb{F}_{p_i}$ be products of fields of orders $q_1, \dots, q_m, p_1, \dots p_s$. An $(\mathbb{F}, \mathbb{K})$-*linearly closed clonoid* is a non-empty subset C of $\bigcup_{k \in \mathbb{N}} \prod_{i=1}^s \mathbb{F}_{p_i}^{\prod_{j=1}^m \mathbb{F}_{q_j}^k}$ with the following properties:

(1) for all $n \in \mathbb{N}$, $\boldsymbol{a}, \boldsymbol{b} \in \prod_{i=1}^s \mathbb{F}_{p_i}$, and $f, g \in C^{[n]}$:
$$\boldsymbol{a}f + \boldsymbol{b}g \in C^{[n]};$$
(2) for all $l, n \in \mathbb{N}$, $f \in C^{[n]}$, $(\boldsymbol{x}_1, \dots, \boldsymbol{x}_m) \in \prod_{j=1}^m \mathbb{F}_{q_j}^l$, and $A_i \in \mathbb{F}_{q_i}^{n \times l}$:
$$g\colon (\boldsymbol{x}_1, \dots, \boldsymbol{x}_m) \mapsto f(A_1 \cdot \boldsymbol{x}_1^t, \cdots, A_m \cdot \boldsymbol{x}_m^t) \text{ is in } C^{[l]},$$

where with the juxtaposition $\boldsymbol{a}f$ we denote the Hadamard product of the two vectors (i.e. the component-wise product $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$).

In [Fio20, Theorems 1.2 and 1.3] we can find a complete description of the lattice of all $(\mathbb{F}, \mathbb{K})$-linearly closed clonoids with $\mathbb{F}$ and $\mathbb{K}$ products of finite fields of pair-wise coprime order.

The main result of this chapter regards the cardinality of the lattice of all clones on $\mathbb{Z}_s$ that contain $\mathrm{Clo}(\mathbb{Z}_s, +)$, where s is squarefree.

Theorem 1.2. *Let $s = p_1 \cdots p_m$ be a product of distinct primes and let $\mathbb{F}_i = \prod_{j \in [m] \setminus \{i\}} \mathbb{Z}_{p_j}$ for all $1 \leq i \leq n$. Then there is an injective function from the lattice $\mathcal{L}(\mathbb{Z}_s, +)$ of all clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$, to the direct product of the lattices of all $(\mathbb{Z}_{p_i}, \mathbb{F}_i)$-linearly closed clonoids, $\mathcal{L}(\mathbb{Z}_{p_i}, \mathbb{F}_i)$, to the $p_i + 1$ power, i. e:*
$$\mathcal{L}(\mathbb{Z}_s, +) \hookrightarrow \prod_{i=1}^n \mathcal{L}(\mathbb{Z}_{p_i}, \mathbb{F}_i)^{p_i+1}.$$

We will prove Theorem 1.2 in Section 5. Vice versa, we find also an embedding of the lattice of all $(\mathbb{Z}_{p_1}, \prod_{i=2}^m \mathbb{Z}_{p_i})$-linearly closed clonoids into the lattice of all clones above $\mathrm{Clo}(\mathbb{Z}_{p_1 \cdots p_m}, +)$, where $p_1, \dots, p_m$ are not necessarily distinct prime numbers.

Theorem 1.3. *Let $p_1, \ldots, p_m$ be prime numbers and let $\mathbb{F}_1 = \prod_{i=2}^{m} \mathbb{Z}_{p_i}$. Then the lattice of all $(\mathbb{Z}_{p_1}, \mathbb{F}_1)$-linearly closed clonoids is embedded in the lattice of all clones above $\mathrm{Clo}(\mathbb{Z}_{p_1 \cdots p_m}, +)$.*

From these results we can obtain bounds for the number of clones on $\mathbb{Z}_s$ that contain $\mathrm{Clo}(\mathbb{Z}_s, +)$.

Corollary 1.4. *Let $s = p_1 \cdots p_m$ be a product of distinct primes and let $\mathbb{F}_i = \prod_{j \in [n] \setminus \{i\}} \mathbb{Z}_{p_j}$. Then the number of clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ is bounded by:*

$$\sum_{i=1}^{m} |\mathcal{L}(\mathbb{Z}_{p_i}, \mathbb{F}_i)| - m + 1 \leq |\mathcal{L}(\mathbb{Z}_s, +)| \leq \prod_{i=1}^{m} |\mathcal{L}(\mathbb{Z}_{p_i}, \mathbb{F}_i)|^{p_i+1}.$$

We will prove Corollary 1.4 in Section 5. This corollary extends the finiteness results of [May08] for clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ which do not necessarily contain constants with s squarefree.

We can also use Theorem 1.2 to find a concrete bound on the arity of the generators of clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$, with s squarefree.

Corollary 1.5. *Let $s = p_1 \cdots p_m$ be a product of distinct prime numbers. Then every clone containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ can be generated by a set of functions of arity at most $\max(p_1, \ldots, p_m)$.*

The last theorem states that there is a dichotomy for the cardinalities of the clones of finite expanded abelian groups.

Theorem 1.6. *Let $\mathbf{G}$ be a finite abelian group. Then $\mathbf{G}$ has finitely many expansions up to term equivalence or, equivalently, the lattice of all clones containing $\mathrm{Clo}(G, +, -, 0)$ is finite if and only if $\mathbf{G}$ is of squarefree order.*

We will prove Theorem 1.6 in Section 5. Thus this theorem shows a surprising dichotomy about the cardinalities of the clones of finite expanded abelian groups up term equivalence. Indeed, the order of a group seems to have no connection in principle with the finiteness of the lattice of all distinct clones up term equivalence above the linear mappings on it.

2. Preliminaries and notation

We use boldface letters for vectors, e. g., $\boldsymbol{u} = (u_1, \ldots, u_n)$ for some $n \in \mathbb{N}$. Moreover, we will use $\langle \boldsymbol{v}, \boldsymbol{u} \rangle$ for the scalar product of the vectors $\boldsymbol{v}$ and $\boldsymbol{u}$. Let A be a set and let $0_A \in A$. We denote by $\mathbf{0}_n$ a constant 0_A vector of length n.

We denote by $[n]$ the set $\{i \in \mathbb{N} \mid 1 \leq i \leq n\}$ and by $[n]_0$ the set $[n] \cup \{0\}$. Moreover we denote by $\mathbb{N}_0$ the set $\mathbb{N} \cup \{0\}$. Let $\boldsymbol{x} \in \mathbb{Z}_p^n$ and let $\boldsymbol{a} \in [p-1]_0^n$. Then we denote by $\boldsymbol{x}^{\boldsymbol{a}}$ the product $\prod_{i=1}^n x_i^{a_i}$. We use also convention that an empty product is 1.

From now on we will consider the group $\prod_{i=1}^m \mathbb{Z}_{p_i}$ instead of $\mathbb{Z}_s$, where $s = \prod_{i=1}^m p_i$ is squarefree. We can observe that the two groups are isomorphic and thus equivalent for our purpose.

Moreover, we consider $\prod_{i=1}^m \mathbb{Z}_{p_i}^n$ instead of $(\prod_{i=1}^m \mathbb{Z}_{p_i})^n$ as the domain of the n-ary functions we want to study.

Let S be a set of finitary functions from a group G to itself . We denote by $\mathrm{Clg}(S)$ the *clone generated by* $S \cup \{+\}$ on G. Let $\mathbb{K}$ and $\mathbb{F}$ be product of finite fields with pair-wise coprime order. We write $\mathrm{Cig}(F)$ for the $(\mathbb{F}, \mathbb{K})$-linearly closed clonoid generated by a set of functions $F \subseteq \bigcup_{k \in \mathbb{N}} \mathbb{F}^{\mathbb{K}^k}$, as defined in [Fio20].

3. Facts about clones

In this paper we want to study sets of finitary functions from $\prod_{i=1}^m \mathbb{Z}_{p_i}$ to itself. The sets of functions that we want to study are the clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$, where s is a product of distinct primes.

Furthermore, let $n \in \mathbb{N}$. We denote by $\mathcal{L}(\mathbb{Z}_n, +)$ the lattice of all clones containing $\mathrm{Clo}(\mathbb{Z}_n, +)$.

In [May08] we can find a description for polynomial clones (clones containing all constants) which contain $\mathrm{Clo}(\mathbb{Z}_s, +)$, where s is a product of distinct primes. With a different strategy we will show a characterization that extends the finiteness result in [May08] to those clones of finite abelian groups that do not necessarily contain all constants.

Let us now show some basic facts about finitary functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$.

Remark 3.1. It is a well-known fact that every finite field is polynomially complete. Thus for all $f \colon \mathbb{F}_p^n \to \mathbb{F}_p$, there exists a sequence $\{a_{\boldsymbol{m}}\}_{\boldsymbol{m} \in [p-1]_0^n} \subseteq \mathbb{F}_p^n$ such that for all $\boldsymbol{x} \in \mathbb{F}_p^n$, f satisfies:

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{m} \in [p-1]_0^n} a_{\boldsymbol{m}} \boldsymbol{x}^{\boldsymbol{m}}.$$

We can observe that if $p_1, \dots, p_m$ are distinct prime numbers we can split a function $f \colon \prod_{i=1}^m \mathbb{Z}_{p_i}^n \to \prod_{i=1}^m \mathbb{Z}_{p_i}$ in $f = \sum_{i=1}^m f_i$, where $f_i = \prod_{j \in [m] \setminus \{i\}} p_j^{p_i - 1} f$. This implies, for example, that we can prove the following remark.

Remark 3.2. Let $p_1 \cdots p_m = s$ be a product of distinct prime numbers and let C be a clone containing $\mathrm{Clo}(\mathbb{Z}_s, +)$. Then for all $k \in \mathbb{N}$ and $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^k$, $h_{(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m)} \colon \prod_{i=1}^m \mathbb{Z}_{p_i}^k \to \prod_{i=1}^m \mathbb{Z}_{p_i}$ defined by:

$$h_{(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m)} \colon (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \mapsto (\langle \boldsymbol{a}_1, \boldsymbol{x}_1 \rangle, \ldots, \langle \boldsymbol{a}_m, \boldsymbol{x}_m \rangle)$$

is in C.

Let A be a set and let $\mathbb{F}_p$ be a field of order p. With the following lemma we show that every function from $\mathbb{F}_p^n \times A^s$ to $\mathbb{F}_p$ can be seen as the induced function of a polynomial of $\mathbf{R}[x_1, \ldots, x_n]$, where $\mathbf{R} = \mathbb{F}_p^{A^s}$. This easy fact will be often used later.

Lemma 3.3. *Let A be a set and let $\mathbb{F}_p$ be a field of order p. Then for every function f from $\mathbb{F}_p^n \times A^s$ to $\mathbb{F}_p$ there exists a sequence of functions $\{f_{\boldsymbol{m}}\}_{\boldsymbol{m} \in [p-1]_0^n}$ from A^s to $\mathbb{F}_p$ such that f satisfies for all $\boldsymbol{x} \in \mathbb{F}_p^n$, $\boldsymbol{y} \in A^s$:*

$$f(\boldsymbol{x}, \boldsymbol{y}) = \sum_{\boldsymbol{m} \in [p-1]_0^n} f_{\boldsymbol{m}}(\boldsymbol{y}) \boldsymbol{x}^{\boldsymbol{m}}.$$

The previous lemma in our setting implies the following.

Lemma 3.4. *Let $p_1, \ldots, p_m$ be distinct prime numbers. Then for every function f from $\prod_{i=1}^m \mathbb{Z}_{p_i}^n$ to $\prod_{i=1}^m \mathbb{Z}_{p_i}$ there exist m sequences of functions $\{f_{(i,\boldsymbol{h}_i)}\}_{\boldsymbol{h}_i \in [p_i-1]_0^n}$ from $\prod_{j \in [m]\setminus\{i\}} \mathbb{Z}_{p_j}^n$ to $\mathbb{Z}_{p_i}$, for all $i \in [m]$, such that f satisfies for all $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^n$:*

$$f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) = \Big(\sum_{\boldsymbol{h}_1 \in [p_1-1]_0^n} f_{(1,\boldsymbol{h}_1)}(\boldsymbol{x}_2, \ldots, \boldsymbol{x}_m) \boldsymbol{x}_1^{\boldsymbol{h}_1}, \ldots, \sum_{\boldsymbol{h}_m \in [p_m-1]_0^n} f_{(m,\boldsymbol{h}_m)}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1}) \boldsymbol{x}_m^{\boldsymbol{h}_m} \Big).$$

4. Embedding of the Clonoids

The aim of this section is to prove that for all $i \in [m]$ there exists an embedding of the lattice of all $(\mathbb{Z}_{p_i}, \mathbb{F}_i)$-linearly closed clonoids in the lattice of all clones containing $\mathrm{Clo}(\prod_{i \in [m]} \mathbb{Z}_{p_i}, +)$, where $p_1, \ldots, p_m$ are prime numbers and $\mathbb{F}_i = \prod_{j \in [m]\setminus\{i\}} \mathbb{Z}_{p_j}$. This clearly provides a lower bound for the cardinality of the lattice of all clones containing $\mathrm{Clo}(\mathbb{Z}_n, +)$ when n is squarefree.

For all $f \in \mathbb{Z}_{p_1}^{\mathbb{F}_1^n}$ we define $e(f) : \prod_{j=1}^m \mathbb{Z}_{p_j}^n \to \prod_{j=1}^m \mathbb{Z}_{p_j}$ by:

$$e(f) \colon (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \mapsto (f(\boldsymbol{x}_2, \ldots, \boldsymbol{x}_m), 0_{\mathbb{Z}_{p_2}}, \ldots, 0_{\mathbb{Z}_{p_m}})$$

for all $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in \prod_{j=1}^m \mathbb{Z}_{p_j}^n$.

Furthermore, we define γ from the lattice of all $(\mathbb{Z}_{p_1}, \mathbb{F}_1)$-linearly closed clonoids to the lattice of all clones containing $\mathrm{Clo}(\prod_{i\in[m]} \mathbb{Z}_{p_i}, +)$ such that for all $C \in \mathcal{L}(\mathbb{Z}_{p_1}, \mathbb{F}_1)$:

$$\gamma(C) := \bigcup_{n\in\mathbb{N}} \{e(g) + h_{(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m)} \mid g \in C^{[n]}, (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) \in \prod_{j=1}^m \mathbb{Z}_{p_j}^n\} \tag{4.1}$$

where $h_{(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_m)}$ is defined in Remark 3.2.

In order to prove Theorem 1.3 we first present an easy lemma omitting the proof.

Lemma 4.1. *Let $\mathbb{F} = \prod_{i=1}^s \mathbb{F}_{p_i}$ and $\mathbb{K} = \prod_{i=1}^m \mathbb{F}_{q_i}$ be products of finite fields. Let $X \subseteq \bigcup_{n\in\mathbb{N}} \mathbb{F}^{\mathbb{K}^n}$. Then $\mathrm{Cig}(X) = \bigcup_{n\in\mathbb{N}} X_n$ where:*
$X_0 := X$
$X_{n+1} := \{\boldsymbol{a}f + \boldsymbol{b}g \mid \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}, f, g \in X_n^{[r]}, r \in \mathbb{N}\} \cup \{g : (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m) \mapsto f(A_1 \cdot \boldsymbol{y}_1^t, \cdots, A_m \cdot \boldsymbol{y}_m^t) \mid f \in X_n^{[k]}, A_i \in \mathbb{F}_{q_i}^{k\times l}\}$.

We omit the straightforward proof of this Lemma which allows us to prove Theorem 1.3.

Proof of Theorem 1.3. Let γ be the function defined in (4.1). First we show that γ is well-defined and then we show that γ is injective and that γ is a homomorphism. Let C be a $(\mathbb{Z}_{p_1}, \mathbb{F}_1)$-linearly closed clonoid. Clearly $\gamma(C)$ contains the projections and the binary addition on $\prod_{i=1}^m \mathbb{Z}_{p_i}$. Moreover, let $f, f_1, \ldots, f_n \in \gamma(C)$ be an n-ary and n s-ary functions respectively. Then there exist $g_f, g_1, \ldots, g_n \in C$, $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^n$, and $(\boldsymbol{a}_{(1,j)}, \ldots, \boldsymbol{a}_{(m,j)}) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^s$, for all $j \in [n]$, such that:

$$f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) = (\langle \boldsymbol{a}_1, \boldsymbol{x}_1\rangle + g_f(\boldsymbol{x}_2, \ldots, \boldsymbol{x}_m), \langle \boldsymbol{a}_2, \boldsymbol{x}_2\rangle, \ldots, \langle \boldsymbol{a}_m, \boldsymbol{x}_m\rangle),$$

for all $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^n$ and for all $1 \le j \le n$:

$$f_j(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m) = (\langle \boldsymbol{a}_{(1,j)}, \boldsymbol{y}_1\rangle + g_j(\boldsymbol{y}_2, \ldots, \boldsymbol{y}_m), \langle \boldsymbol{a}_{(2,j)}, \boldsymbol{y}_2\rangle, \ldots, \langle \boldsymbol{a}_{(m,j)}, \boldsymbol{y}_m\rangle)$$

for all $(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^s$. Then $h = f \circ (f_1, \ldots, f_n)$ can be written as:

$$h(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m) = (\langle \boldsymbol{c}_1, \boldsymbol{y}_1\rangle + g_h(\boldsymbol{y}_2, \ldots, \boldsymbol{y}_m), \langle \boldsymbol{c}_2, \boldsymbol{y}_2\rangle, \ldots, \langle \boldsymbol{c}_m, \boldsymbol{y}_m\rangle),$$

where for all $u \in [m]$, $j \in [s]$, $(\boldsymbol{c}_u)_j = \sum_{i=1}^n (\boldsymbol{a}_u)_i (\boldsymbol{a}_{(u,i)})_j$ and $g_h\colon \prod_{i=2}^m \mathbb{Z}_{p_i}^s \to \mathbb{Z}_{p_1}$ is defined by:

$$g_h(\boldsymbol{y}_2,\dots,\boldsymbol{y}_m) = \langle \boldsymbol{a}_1, \mathbf{d}(\boldsymbol{y}_2,\dots,\boldsymbol{y}_m)\rangle + g_f(\langle \boldsymbol{a}_{(2,1)}, \boldsymbol{y}_2\rangle, \dots, \langle \boldsymbol{a}_{(2,n)}, \boldsymbol{y}_2\rangle \\ , \dots, \langle \boldsymbol{a}_{(m,1)}, \boldsymbol{y}_m\rangle, \dots, \langle \boldsymbol{a}_{(m,n)}, \boldsymbol{y}_m\rangle),$$

with $\mathbf{d}(\boldsymbol{y}_2,\dots,\boldsymbol{y}_m) = (g_1(\boldsymbol{y}_2,\dots,\boldsymbol{y}_m),\dots,g_n(\boldsymbol{y}_2,\dots,\boldsymbol{y}_m))$ for all $(\boldsymbol{y}_2, \dots, \boldsymbol{y}_m) \in \prod_{i=2}^m \mathbb{Z}_{p_i}^s$. We can see from Definition 1.1 that $g_h \in C$. Thus $\gamma(C)$ is closed under composition and γ is well-defined.

Next we prove that γ is injective. Let C and D be two $(\mathbb{Z}_{p_1}, \mathbb{F}_1)$-linearly closed clonoids such that $\gamma(C) = \gamma(D)$ and let $g \in C$ be an l-ary function. Then let $s\colon \prod_{i=1}^m \mathbb{Z}_{p_i}^l \to \prod_{i=1}^m \mathbb{Z}_{p_i}$ be such that $e(g) = s$. Then s is in $\gamma(C) = \gamma(D)$. By definition of γ, this implies that $e(g) = e(g') + h_{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_m)}$ for some $g' \in D$ and $(\boldsymbol{a}_1,\dots,\boldsymbol{a}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^l$. The only possibility is that $g = g' \in D$ and thus $C \subseteq D$. We can repeat this argument for the other inclusion and hence γ is injective. Furthermore, we have that for all $C, D \in \mathcal{L}(\mathbb{Z}_{p_1}, \mathbb{F}_1)$, $\gamma(C \cap D) = \gamma(C) \cap \gamma(D)$. We can observe that γ is monotone, thus $\gamma(C \vee D) \supseteq \gamma(C) \vee \gamma(D)$. For the other inclusion we prove by induction on n that $\gamma(C) \vee \gamma(D) \supseteq e(X_n)$, where $C \vee D = \bigcup_{n\in\mathbb{N}} X_n$ with:

$X_0 = C \cup D$
$X_{n+1} = \{af + bg \mid a, b \in \mathbb{Z}_{p_1}, f, g \in X_n^{[r]}, r \in \mathbb{N}\} \cup \{g\colon (\boldsymbol{y}_2,\dots,\boldsymbol{y}_m) \mapsto f(A_2 \cdot \boldsymbol{y}_2^t, \cdots, A_m \cdot \boldsymbol{y}_m^t) \mid f \in X_n^{[k]}, A_i \in \mathbb{Z}_{p_i}^{k\times l}, k, l \in \mathbb{N}\}$.

Base step $n = 0$: $e(C \cup D) = e(C) \cup e(D) \subseteq \gamma(C) \vee \gamma(D)$.

Induction step $n > 0$: suppose that the claim holds for $n-1$. Then let $g \in e(X_n)$. Thus there exists $u \in X_n$ such that $e(u) = g$ and either u is a linear combination of functions in X_{n-1} or there exist $f \in X_n^{[k]}$, $A_i \in \mathbb{Z}_{p_i}^{k\times l}$ for all $i \in [m]\backslash\{1\}$, and $k, l \in \mathbb{N}$ such that $u\colon (\boldsymbol{y}_2,\dots,\boldsymbol{y}_m) \mapsto f(A_2 \cdot \boldsymbol{y}_2^t, \cdots, A_m \cdot \boldsymbol{y}_m^t)$. In both cases we have $g \in \mathrm{Clg}(e(X_{n-1}) \cup \bigcup_{t\in\mathbb{N}}\{h_{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_m)} \mid (\boldsymbol{a}_1,\dots,\boldsymbol{a}_m) \in \prod_{i\in[m]} \mathbb{Z}_{p_i}^t\}) \subseteq \gamma(C) \vee \gamma(D)$ and this concludes the induction proof. By Lemma 4.1, $\gamma(C) \vee \gamma(D) \supseteq e(C \vee D)$.

We can observe that $\gamma(C \vee D)$ is the clone generated by $e(C \vee D)$, $+$ and all the mappings $h_{(\boldsymbol{a}_1,\dots,\boldsymbol{a}_m)}$ defined in Remark 3.2. Since $e(C \vee D) \subseteq \gamma(C) \vee \gamma(D)$, it follows that $\gamma(C \vee D) \subseteq \gamma(C) \vee \gamma(D)$. Hence γ is an embedding. □

5. A general bound

In the current section our goal is to determine a bound for the cardinality of the lattice of all clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$, where $s = p_1 \cdots p_m$ is a product of distinct primes. Theorem 5.9 gives a complete list of generators for a clone containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ that explains the connection between clonoids and clones in this case. The generators of Theorem 5.9 are substantially formed by a product of a unary member of a generating set of a $(\mathbb{Z}_{p_i}, \prod_{j\in[m]\setminus\{i\}} \mathbb{Z}_{p_j})$-linearly closed clonoid and a monomial generating a clone on $\mathbb{Z}_{p_i}$ for $i \in [m]$. This puts together the characterization in [Kre19]and [Fio20, Theorem 1.2] which are the main ingredients of this section.

We start showing some lemmata which we need to prove that clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ are strictly characterized by the $(\mathbb{Z}_{p_i}, \mathbb{F}_i)$-linearly closed clonoids, where we denote by $\mathbb{F}_i$ the product $\prod_{j\in[m]\setminus\{i\}} \mathbb{Z}_{p_j}$.

In this section we have to deal with polynomials whose coefficients are finitary functions from $\mathbb{F}_i$ to $\mathbb{Z}_{p_i}$. The next step will be to generalize some results in [Kre19] about p-linearly closed clonoids to polynomials in a polynomial ring over a set of countably many variables. Let us start with the notation. Let $\mathbf{R}$ be a ring. We fix an alphabet $X := \{x_i \mid i \in \mathbb{N}\}$ and we denote by $\mathbf{R}[X]$ the polynomial ring over $\mathbf{R}$ in the variables X.

Following [Kre19] we denote by $\mathrm{tD}(h)$ the *total degree of a monomial* h, which is defined as the sum of the exponents. We also denote by $\mathrm{tD}(f) := \max(\{d \mid d = \mathrm{tD}(h), h \text{ is a monomial in } f\})$ the maximum of the total degrees of monomials in f. Let $f \in \mathbf{R}[x_1, \dots, x_k]$ and let $\boldsymbol{x} = (x_1, \dots, x_k)$. Then f can be written as:

$$f = \sum_{\boldsymbol{m}\in\mathbb{N}_0^k} r_{\boldsymbol{m}} \boldsymbol{x}^{\boldsymbol{m}},$$

for some sequence $\{r_{\boldsymbol{m}}\}_{\boldsymbol{m}\in\mathbb{N}_0^k}$ in $\mathbf{R}$ with only finitely many non-zero members and where $\boldsymbol{x}^{\boldsymbol{m}} = \prod_{i=1}^n x_i^{m_i}$.

Next we introduce a notation for the composition of multivariate polynomials. Let $l, h \in \mathbb{N}$, $g, f_1, \dots, f_h \in \mathbf{R}[x_1, \dots, x_l]$, and let $\boldsymbol{b} = (b_1, \dots, b_h) \in \mathbb{N}^h$ with $1 \leq b_1 < b_2 < \cdots < b_h \leq l$. Then we define $g \circ_{\boldsymbol{b}} (f_1, \dots, f_h)$ by:

$$g \circ_{\boldsymbol{b}} (f_1, \dots, f_h) := g(x_1, \dots, x_{b_1-1}, f_1, x_{b_1+1}, \dots, x_{b_2-1}, f_2, x_{b_2+1}, \dots).$$

Let $\mathbf{R}[X]$ be a polynomial ring and let $f \in \mathbf{R}[X]$. Since later we want to introduce the induced function of a polynomial, in order to have a unique polynomial for every induced function, we consider the ideal I generated by the polynomials $x_i^p - x_i$ in $\mathbf{R}[X]$, for every $x_i \in X$. By [Eis95, Chapter 15.3] there is a unique remainder $\mathrm{rem}(f)$ of f with respect to I. This remainder has the property that the exponents of the variables are less or equal $p - 1$. Following [Kre19, Section 2], we define

$$\mathbf{R}[X]_p := \{ \sum_{\boldsymbol{m} \in [p-1]_0^k} r_{\boldsymbol{m}} \boldsymbol{x}^{\boldsymbol{m}} \mid k \in \mathbb{N}_0, r_{\boldsymbol{m}} \in R, \boldsymbol{x} = (x_1, \dots, x_k)\}$$

We can observe that these polynomials form a set of representatives of the set of all classes of the quotient $\mathbf{R}/I$.

With the next definition we want to introduce sets of polynomials in polynomial rings closed under composition from the right and from the left with linear mappings.

Definition 5.1. Let A be a set and let $\mathbf{R}$ be a ring. Let $\mathbf{R}^A[X]$ be a polynomial ring. An $\mathbf{R}^A$-*polynomial linearly closed clonoid* is a non-empty subset C of $\mathbf{R}^A[X]$ with the following properties:

(1) for all $f \in C$, $g \in C$, and $a, b \in \mathbf{R}$
$$af + bg \in C;$$
(2) for all $s \in \mathbb{N}$, $f \in C \cap \mathbf{R}^A[x_1, \dots, x_s]$, and $M \in \mathbf{R}^{s \times l}$:
$$g = f(M \cdot (x_1, \dots, x_l)^t) \text{ is in } C.$$

We can observe that item (2) of Definition 5.1 implies that for all $s, k \in \mathbb{N}$, $l \leq s$, $f \in C \cap \mathbf{R}^A[x_1, \dots, x_s]$, and $\boldsymbol{a} \in \mathbf{R}^k$:

$$g = f \circ_{(l)} (\prod_{i \in [k]} a_i x_i) \text{ is in } C.$$

Let $S \subseteq \mathbf{R}^A[X]$. Then we denote by $\langle S \rangle_{\mathbf{R}^A}$ the $\mathbf{R}^A$-*polynomial linearly closed clonoid* generated by S. We can see that $\mathbf{R}^A[X]_p$ forms an $\mathbf{R}^A$-linearly closed clonoid.

Let us now modify [Kre19, Lemmata 3.8 and 3.9] to deal with $\mathbf{R}^A$-polynomial linearly closed clonoids. Indeed [Kre19, Lemmata 3.8] is stated for $\mathbb{Z}_p$-polynomial linearly closed clonoids and works for $\mathbf{R}^A$-polynomial linearly closed clonoids in general with essentially the same proof as in [Kre19].

Lemma 5.2. *Let A be a set and let $\mathbf{R}$ be a ring. Let $d \in \mathbb{N}$, let $r \in \mathbf{R}^A$ and let $g \in \mathbf{R}^A[X]$ with $\mathrm{tD}(g) \leq d$, and the coefficient of $\boldsymbol{x}^{\mathbf{1}_d}$ in g is 0. Then $rx_1 \cdots x_d \in \langle \{rx_1 \cdots x_d + g\} \rangle_{\mathbf{R}^A}$.*

Proof. Let $g \in \mathbf{R}^A[X]$ and let $C := \langle \{rx_1 \cdots x_d + g\} \rangle_{\mathbf{R}^A}$. By setting all variables x_i with $i > d$ to 0, we may assume that $g \in \mathbf{R}^A[x_1, \dots, x_d]$.

Next we proceed by induction on the number of monomials of g in order to show that $rx_1 \cdots x_d \in \langle \{rx_1 \cdots x_d + g\} \rangle_{\mathbf{R}^A} \subseteq C$.

If $g = 0$ then the claim obviously holds. Let us suppose that $rx_1 \cdots x_d \in \langle \{rx_1 \cdots x_d + s\} \rangle_{\mathbf{R}^A}$ for every s with $t \geq 0$ monomials.

Let the number of monomials of g be $t+1$. We observe that there exist $x_l \in \{x_1, \dots, x_d\}$ and a monomial m of g such that x_l does not appear in m. Thus we obtain:

$$rx_1 \cdots x_d + g - (rx_1 \cdots x_d + g) \circ_{(l)} 0 = rx_1 \cdots x_d + g - g \circ_{(l)} 0 \in C.$$

Thus $g' := g - g \circ_{(l)} 0$ satisfies the properties that $\mathrm{tD}(g') \leq d$, the coefficient of $\boldsymbol{x}^{\mathbf{1}_d}$ in g' is 0, $g' \in \mathbf{R}^A[x_1, \dots, x_d]$ and g' has fewer monomials than g, since the monomial m is cancelled in $g - g \circ_{(l)} 0$. By the induction hypothesis $rx_1 \cdots x_d \in \langle \{rx_1 \cdots x_d + g'\} \rangle_{\mathbf{R}^A} \subseteq \langle \{rx_1 \cdots x_d + g\} \rangle_{\mathbf{R}^A}$ and the claim holds. □

With Lemma 5.2 we can now prove the following generalization of [Kre19, Lemma 3.9] with the same proof. The following Lemma generalizes [Kre19, Lemma 3.9], which is stated for $\mathbb{Z}_p$-polynomial linearly closed clonoids, to $\mathbb{Z}_p^n$-polynomial linearly closed clonoids.

Lemma 5.3. *Let $d, n \in \mathbb{N}$, let p be a prime and let f be a polynomial in $\mathbb{Z}_p^n[X]_p$ with $d := \mathrm{tD}(f)$. Let m be a monomial with coefficient $r \in \mathbb{Z}_p^n$ and $\mathrm{tD}(m) = d$. Then:*

$$rx_1 \dots x_d \in \langle \{f\} \rangle_{\mathbb{Z}_p^n}.$$

Proof. Let $f = \sum_{\boldsymbol{m} \in [p-1]_0^l} r_{\boldsymbol{m}} \boldsymbol{x}^{\boldsymbol{m}} \in \mathbb{Z}_p^n[x_1, \dots, x_l]_p$, $C := \langle \{f\} \rangle_{\mathbb{Z}_p^n}$, let $d := \mathrm{tD}(f)$, and let $m = r\boldsymbol{x}^{\boldsymbol{s}}$ be a monomial of f with $\mathrm{tD}(m) = d$. Without loss of generality we suppose $s_j > 0$ for all $j \in [u]$ for some $u \leq l$ and $s_j = 0$ otherwise. We prove by case distinction that $rx_1 \dots x_d \in \langle \{f\} \rangle_{\mathbb{Z}_p^n}$.

Case $s_j = 1$ for all $j \in [u]$: then clearly there exists g with $\mathrm{tD}(g) \leq d$ such that $r\boldsymbol{x}^{\boldsymbol{s}} + g = rx_1 \dots x_d + g \in C$ and the coefficient of $\boldsymbol{x}^{\boldsymbol{s}}$ in g is 0. By Lemma 5.2 we have that $rx_1 \dots x_d \in C$.

Case $\exists j \in [u]$ with $s_j > 1$: then we show that there exist h and g such that $h + g \in C$ with $h = r \prod_{i \in [u+1]} x_i^{t_i}$ and $\boldsymbol{t} = (s_1, \dots, s_{j-1}, s_j - 1, s_{j+1}, \dots, s_u, 1)$. Furthermore, g satisfies $\mathrm{tD}(g) \leq d$ and the coefficient of $\boldsymbol{y}^{(s_1, \dots, s_{j-1}, s_j - 1, s_{j+1}, \dots, s_u, 1)}$ in g is 0, where we denote by $\boldsymbol{y}$ the vector of variables $(x_1, \dots, x_{u+1})$. Let $g' = f - m \in \mathbb{Z}_p^n[x_1, \dots, x_l]_p$. Let $g'' := g' \circ_{(j)} (x_j + x_{u+1})$. Thus:

$$
\begin{aligned}
(m+g')\circ_{(j)}(x_j+x_{u+1}) =& r\boldsymbol{x}^{\boldsymbol{s}}\circ_{(j)}(x_j+x_{u+1})+g'\circ_{(j)}(x_j+x_{u+1})\\
=& r(\sum_{k\in[s_j]_0}\binom{s_j}{k}x_j^{s_j-k}x_{u+1}^k)\cdot\prod_{i\in[u]\setminus\{j\}}x_i^{s_i}+g''\\
=& r\cdot s_j\cdot\boldsymbol{y}^{(s_1,\dots,s_{j-1},s_j-1,s_{j+1},\dots,s_u,1)}+\\
&+r(\sum_{k\in[s_j]_0\setminus\{1\}}\binom{s_j}{k}x_j^{s_j-k}x_{u+1}^k)\cdot\prod_{i\in[u]\setminus\{j\}}x_i^{s_i}+g''.
\end{aligned}
$$

Note that s_j is invertible in $\mathbb{Z}_p$ and that $h+g=s_j^{-1}(m+g')\circ_{(j)}(x_j+x_{u+1})$ is in C with:

$$
\begin{aligned}
&h := r\cdot\boldsymbol{y}^{(s_1,\dots,s_{j-1},s_j-1,s_{j+1},\dots,s_u,1)}\\
&g = s_j^{-1}r(\sum_{k\in[s_j]_0\setminus\{1\}}\binom{s_j}{k}x_j^{s_j-k}x_{u+1}^k)\cdot\prod_{i\in[u]\setminus\{j\}}x_i^{s_i}+s_j^{-1}g''.
\end{aligned}
$$

Then h satisfies $\mathrm{tD}(h)=d$ with degree $\boldsymbol{t}$. Furthermore, g satisfies $\mathrm{tD}(g)\leq d$ and the coefficient of $\boldsymbol{y}^{(t_1,\dots,t_{j-1},t_j-1,t_{j+1},\dots,t_w,1)}$ in g is 0. Thus h and g are the searched polynomials. This implies that $rx_1\dots x_d+g'''\in C$ for some $g'''\in\mathbb{Z}_p^n[X]_p$ with $\mathrm{tD}(g''')\leq d$ and such that the coefficient of $\boldsymbol{x}^{\boldsymbol{1}_d}$ in g''' is 0. By Lemma 5.2 we have that $rx_1\dots x_d\in C$ and the claim holds. □

We are now ready to prove that an $\mathbb{Z}_p^n$-polynomial linearly closed clonoid generated by an element $f\in\mathbb{Z}_p^n[X]_p$ contains every monomial of f.

Lemma 5.4. *Let p be a prime and let $f\in\mathbb{Z}_p^n[X]_p$ be such that $h=r_{\boldsymbol{m}}\boldsymbol{x}^{\boldsymbol{m}}$ is a monomial of f. Then $h\in\langle f\rangle_{\mathbb{Z}_p^n}$.*

Proof. The proof is by induction on the number k of monomials in f.

Base step $k=1$: then clearly the claim holds.

Induction step $k>0$: suppose that the claim holds for every g with $k-1$ monomials. Let f be a polynomial with k monomials. Let $d=\mathrm{tD}(f)$ and let h be a monomial in f with degree d and coefficient r_h. By Lemma 5.3, we have that $r_hx_1\cdots x_d\in\langle f\rangle_{\mathbb{Z}_p^n}$. Clearly, this yields $h\in\langle f\rangle_{\mathbb{Z}_p^n}$. From the induction hypothesis we have that all $k-1$ monomials of $f-h$ are in $\langle f-h\rangle_{\mathbb{Z}_p^n}\subseteq\langle f\rangle_{\mathbb{Z}_p^n}$. Thus all monomials of f are in $\langle f\rangle_{\mathbb{Z}_p^n}$. □

In this section we have to deal with polynomials whose coefficients are finitary functions from $\mathbb{F}_i$ to $\mathbb{Z}_{p_i}$, where $\mathbb{F}_i=\prod_{j\in[m]\setminus\{i\}}\mathbb{Z}_{p_j}$ and

$p_1, \dots, p_m$ are distinct primes. In order to connect this strategy with the clones of an expanded group we define a non-standard concept of induced functions of a polynomial. Let A be a set with a fixed element 0. For every polynomial $f \in \mathbf{R}^{A^n}\ [x_1, \dots, x_k]_p$ of the form $f = \sum_{\boldsymbol{m} \in [p-1]_0^k} r_{\boldsymbol{m}} \boldsymbol{x}^{\boldsymbol{m}}$ we define its s-ary *induced function* $\overline{f}^{[s]} \colon R^s \times A^s \to R \times A$ by:

$$(\boldsymbol{x}, \boldsymbol{y}) \mapsto (\sum_{\boldsymbol{m} \in [p-1]_0^k} r_{\boldsymbol{m}}(\boldsymbol{y'}) \prod_{i=1}^{k} x_i^{m_i}, \mathbf{0}),$$

with $s \geq k, n$ and $\boldsymbol{y'} = (y_1, \dots, y_n)$. We can observe that we induce also the functions $\{r^{\boldsymbol{m}}\}_{\boldsymbol{m} \in [p-1]_0^k}$ coefficients of monomials in f and for this reason we require $s \geq n$. From now on, when not specified, $s = \max(k, n)$, indeed we want an arity of the induced function sufficiently large to induce both the monomials and the coefficients of the function induced. Next we show a lemma that connects the monomials of an $(\mathbb{Z}_p^{\prod_{i=1}^m \mathbb{Z}_{q_i}^n})$-polynomial linearly closed clonoid to functions of a clones on $\mathbb{Z}_{pq_1 \cdots q_m}$.

Lemma 5.5. *Let $p_1, \dots, p_m$ distinct primes, let $\mathbf{R}^A = \mathbb{Z}_{p_1}^{\prod_{i=2}^m \mathbb{Z}_{p_i}^n}$, and let $h, h_1 \in \mathbf{R}^A[X]_{p_1}$ with $h \in \langle h_1 \rangle_{\mathbf{R}^A}$. Then $\overline{h} \in \mathrm{Clg}(\{\overline{h_1}\})$.*

Proof. Let $\overline{f}, \overline{g} \in \mathrm{Clg}(\{\overline{h_1}\})^{[s]}$. Then we can observe that for all $a, b \in \mathbb{Z}_{p_1}$ we have that $\overline{af + bg} = h_{((a,b),\boldsymbol{0})} \circ (\overline{f}, \overline{g})$, where $\boldsymbol{0} = ((0_{\mathbb{Z}_{p_2}}, 0_{\mathbb{Z}_{p_2}}), \dots, (0_{\mathbb{Z}_{p_m}}, 0_{\mathbb{Z}_{p_m}}))$ and $h_{((a,b),\boldsymbol{0})}$ is defined in Remark 3.2.

Furthermore for all $M \in \mathbb{Z}_{p_1}^{s \times l}$ we have that $\overline{f(M \cdot (x_1, \dots, x_l))} = \overline{f} \circ (g_1, \dots, g_s)$ where $g_i : \prod_{i \in [m]} \mathbb{Z}_{p_i}^u \to \prod_{i \in [m]} \mathbb{Z}_{p_i}$ such that:

$$g_i : (\boldsymbol{x}, \boldsymbol{y}_2, \dots, \boldsymbol{y}_m) \mapsto (M_i(x_1, \dots, x_l)^t, (y_2)_i, \dots, (y_m)_i)$$

for all $(\boldsymbol{x}, \boldsymbol{y}_2, \dots, \boldsymbol{y}_m) \in \prod_{i \in [m]} \mathbb{Z}_{p_i}^u$,where M_i is the ith row of M and $u = \max(l, n)$.

We know that every clone C containing $\mathrm{Clo}(\mathbb{Z}_{p_1 \cdots p_m}, +)$ is closed under composition and, by Remark 3.2, contains every linear mapping $h_{(\boldsymbol{a}_1, \dots, \boldsymbol{a}_m)}$ with $\boldsymbol{a}_i \in \mathbb{Z}_{p_i}^n$. Then it is clear that if a function h can be generated from h_1 with item (1) or (2) of Definition 5.1, then the induced function $\overline{h}_1$ generates $\overline{h}$ in a clone containing $\mathrm{Clo}(\mathbb{Z}_{p_1 \cdots p_m}, +)$, simply composing $\overline{h}_1$ with the linear mappings of Remark 3.2 from the right and from the left. $\square$

With the next two lemmata we want to prove that in order to characterize clones containing $\mathrm{Clo}(\mathbb{Z}_s, +)$, with s squarefree, we have only to consider induced monomials with certain total degrees.

Lemma 5.6. *Let $d \in \mathbb{N}\backslash\{1\}$. Then for all $k, l \in \mathbb{N}$, for all $g \in \mathbb{Z}_p^{\prod_{i=1}^m \mathbb{Z}_{q_i}^l}$, and for all $\boldsymbol{m} \in [p-1]_0^k \backslash \{\boldsymbol{0}_k\}$ with $\mathrm{tD}(\boldsymbol{x}^{\boldsymbol{m}}) = u$ congruent to d modulo $p-1$ it follows that:*

$$\overline{r\boldsymbol{x}^{\boldsymbol{m}}} \in \mathrm{Clg}(\{\overline{rx_1 \cdots x_d}\}).$$

Proof. We can observe that composing $\overline{rx_1 \cdots x_d}$ with itself we obtain that

$$\overline{r^{l+1}x_1 \ldots x_{d+l(d-1)}} \in \mathrm{Clg}(\overline{rx_1 \cdots x_d})$$

for all $l \in \mathbb{N}$. Since $r^p = r$ yields $r^{s(p-1)+1} = r$ for all $s \in \mathbb{N}$, it follows for $l = s(p-1)$ that

$$\overline{rx_1 \cdots x_{d+s(p-1)(d-1)}} \in \mathrm{Clg}(\overline{rx_1 \cdots x_d})$$

Let $s \in \mathbb{N}$ be such that $d + s(p-1)(d-1) \geq \sum_{i=1}^k m_i$. Set the first m_1 variables in $\{x_1, \ldots, x_{d+s(p-1)(d-1)}\}$ to x_1, the next m_2 variables to x_2, and so forth with the last $d+s(p-1)(d-1) - \sum_{i\in[k-1]} m_i$ variables set to x_k. This yields

$$\overline{r\boldsymbol{x}^{\boldsymbol{m}}} \in \mathrm{Clg}(\overline{rx_1 \cdots x_d}).$$

□

Lemma 5.7. *Let $p_1, \ldots, p_m$ distinct primes, let $n \in \mathbb{N}$, let $f\colon \prod_{i=1}^m \mathbb{Z}_{p_i}^n \to \prod_{i=1}^m \mathbb{Z}_{p_i}$ be an n-ary function, and let $g = (p_2 \cdots p_m)^{p_1-1} f$. Let $\mathbf{R} = \mathbb{Z}_{p_1}$, $A = \prod_{i=2}^m \mathbb{Z}_{p_i}^n$, and $h \in \mathbf{R}^A[X]_{p_1}$ such that $\overline{h} = g$. Let h' be a monomial of h with coefficient r and $d = \mathrm{tD}(h')$. Then it follows that:*

$$\overline{rx_1 \cdots x_d} \in \mathrm{Clg}(\{f\}).$$

Proof. Let n, h, and let f be as in the hypothesis. By Lemma 5.3, we have that $rx_1 \cdots x_d \in \langle h' \rangle_{\mathbf{R}^A}$. By Lemma 5.4, $h' \in \langle h \rangle_{\mathbf{R}^A}$ and thus, by Lemma 5.5, $\overline{rx_1 \cdots x_d} \in \mathrm{Clg}(\{f\})$. □

We are now ready to prove the main result of this section which allows us to provide a bound for the lattice of all clones containing the addition of a squarefree abelian group.

Let $s = p_1 \cdots p_m$ be a product of distinct prime numbers. Then for all $i \in [m]$ and $j \in [p_i]_0$ we define $\rho_{(i,j)}\colon \mathcal{L}(\mathbb{Z}_s, +) \to \mathcal{L}(\mathbb{Z}_{p_i}, \mathbb{F}_i)$ by:

$$\rho_{(i,j)}(C) := \bigcup_{n\in\mathbb{N}} \{f\colon \mathbb{F}_i^n \to \mathbb{Z}_{p_i} \mid \overline{fx_1 \cdots x_j} \in C\} \tag{5.1}$$

for all $C \in \mathcal{L}(\mathbb{Z}_s, +)$. Let $\rho\colon \mathcal{L}(\mathbb{Z}_s, +) \to \prod_{i=1}^m \mathcal{L}(\mathbb{Z}_{p_i}, \mathbb{F}_i)^{p_i+1}$ be defined by $\rho(C) = (\rho_{(1,0)}(C), \ldots, \rho_{(1,p_1)}(C), \ldots, \rho_{(m,0)}(C), \ldots, \rho_{(m,p_m)}(C))$, for all $C \in \mathcal{L}(\mathbb{Z}_s, +)$.

Proof of Theorem 1.2. Let $s = p_1 \cdots p_m$ be a product of distinct prime numbers. We prove that for all $i \in [m]$ and for all $j \in [p_i]_0$, the map $\rho_{(i,j)}$ is well-defined and thus ρ is well-defined.

Let $C \in \mathcal{L}(\mathbb{Z}_s, +)$. Then we prove that $\rho_{(1,j)}(C)$, with $0 \leq j$, is a $(\mathbb{Z}_{p_1}, \mathbb{F}_1)$-linearly closed clonoid. To this end let $n \in \mathbb{N}$, $f, g \in \rho_{(1,j)}(C)^{[n]}$ and $a, b \in \mathbb{Z}_{p_1}$. Then $\overline{fx_1 \cdots x_j}, \overline{gx_1 \cdots x_j} \in C$. From the closure with $+$ we have that $\overline{(af + bg)x_1 \cdots x_j} \in C$ and thus $af + bg \in \rho_{(1,j)}(C)^{[n]}$ and item (1) of Definition 1.1 holds. Furthermore, let $u, n \in \mathbb{N}$, $f \in \rho_{(1,j)}(C)^{[u]}$, $A_r \in \mathbb{Z}_{p_r}^{u \times n}$, for all $r \in [m] \backslash \{1\}$, and let $g\colon \prod_{k=2}^m \mathbb{Z}_{p_k}^n \to \mathbb{Z}_{p_1}$ be defined by:

$$g\colon (\boldsymbol{x}_2, \ldots, \boldsymbol{x}_m) \mapsto f(A_2 \cdot \boldsymbol{x}_2^t, \cdots, A_m \cdot \boldsymbol{x}_m^t).$$

It is clear that $\overline{gx_1 \cdots x_j} \in \mathrm{Clg}(\{\overline{fx_1 \cdots x_j}\})$ as composition of $\overline{fx_1 \cdots x_j}$ and linear mappings of Remark 3.2. Thus $g \in \rho_{(1,j)}(C)$ which concludes the proof of item (2) of Definition 1.1. In the same way we can prove that $\rho_{(i,j)}$ is well-defined for all $i \in [m]$ and $j \in [p_i]_0$. Hence ρ is well-defined.

We prove that ρ is injective. Let $C, D \in \mathcal{L}(\mathbb{Z}_s, +)$ with $\rho(C) = \rho(D)$. Let $f \in C^{[n]}$. By Lemma 3.4 we have that there exist m sequences of functions $\{f_{(i,\boldsymbol{h}_i)}\}_{\boldsymbol{h}_i \in [p_i-1]_0^n}$ from $\prod_{j \in [m] \backslash \{i\}} \mathbb{Z}_{p_j}^n$ to $\mathbb{Z}_{p_i}$, for all $i \in [m]$, such that f satisfies for all $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^n$:

$$\begin{aligned} f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) = (&\sum_{\boldsymbol{h}_1 \in [p_1-1]_0^n} f_{(1,\boldsymbol{h}_1)}(\boldsymbol{x}_2, \ldots, \boldsymbol{x}_m)\boldsymbol{x}_1^{\boldsymbol{h}_1}, \ldots, \\ &\sum_{\boldsymbol{h}_m \in [p_m-1]_0^n} f_{(m,\boldsymbol{h}_m)}(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{m-1})\boldsymbol{x}_m^{\boldsymbol{h}_m}). \end{aligned}$$

Let $w \in \mathbf{R}^A[X]_{p_1}$ be such that $\overline{w}^{[n]} = \prod_{i=2}^m p_i^{p_1-1} f$, where $\mathbf{R}^A = \mathbb{Z}_{p_1}^{\mathbb{F}_1^n}$.

Let $h = f_{\boldsymbol{l}}\boldsymbol{x}^{\boldsymbol{l}}$ be a monomial of w and let $s = \mathrm{tD}(h)$. We prove that $\overline{h} \in D$ by case distinction.

Case $s = 0, 1$: from Lemma 5.7 it follows that $\overline{h} \in C$. By Definition 5.1, $f_{\boldsymbol{l}} \in \rho_{(1,s)}(C) = \rho_{(1,s)}(D)$ and thus $\overline{h} \in D$.

Case $s > 1$: let $d \in \mathbb{N}$ be such that $2 \leq d \leq p_1$ and $d = s$ modulo $p_1 - 1$. By Lemma 5.7, $C \supseteq \mathrm{Clg}(\{\overline{f_{\boldsymbol{l}}x_1 \cdots x_s}\})$. Thus, by Lemma 5.6, $C \supseteq \mathrm{Clg}(\{\overline{f_{\boldsymbol{l}}x_1 \cdots x_d}\})$ and thus $f_{\boldsymbol{l}} \in \rho_{(1,d)}(C) = \rho_{(1,d)}(D)$. Hence $\overline{f_{\boldsymbol{l}}x_1 \cdots x_d} \in D$ and, by Lemma 5.6, it follows that $\overline{f_{\boldsymbol{l}}\boldsymbol{x}^{\boldsymbol{l}}} \in D$. This holds for a generic induced monomial in $\prod_{i=2}^{m} p_i^{p_1-1} f$ and thus the function $\prod_{i=2}^{m} p_i^{p_1-1} f \in D$. With the same strategy we can prove that $\prod_{i\in[m]\setminus\{j\}} p_i^{p_j-1} f \in D$ for all $j \in [m]$ and thus $f = \sum_{j\in[m]} \prod_{i\in[m]\setminus\{j\}} p_i^{p_j-1} f \in D$. Hence $C \subseteq D$. With the same proof we have the other inclusion and thus ρ is injective. □

Note that ρ is only an injective function and not a lattice embedding. This happens because the $(\mathbb{Z}_{p_i}, \mathbb{F}_i)$-linearly closed clonoids that describe a clone in $\mathcal{L}(\mathbb{Z}_s, +)$ have several closure properties that are not preserved by the $(\mathbb{Z}_{p_i}, \mathbb{F}_i)$-linearly closed clonoid lattice join.

Proof of Corollary 1.4. The proof follows from Theorems 1.2, 1.3 and we observe the fact that the only clones in common in the embeddings of Theorem 1.3 is the clone of all linear mappings. For this reason we subtract $m-1$ from the left hand side of the inequalities. □

Corollary 5.8. *Let $s = p_1 \cdots p_m \in \mathbb{N}$ be a product of distinct primes and let $\mathbb{F}_i = \prod_{j\in[m]\setminus\{i\}} \mathbb{Z}_{p_j}$ for all $i \in [m]$. Then the number of clones containing* $\mathrm{Clo}(\mathbb{Z}_s, +)$ *is bounded by:*

$$|\mathcal{L}(\mathbb{Z}_s, +)| \leq \prod_{i=1}^{m} (\sum_{1\leq r\leq n_i} \binom{n_i}{r}_{p_i})^{p_i+1}$$

where $n_i = \prod_{j\in[m]\setminus\{i\}} p_j$ and

$$\binom{n}{k}_q = \prod_{i=1}^{k} \frac{q^{n-k+i}-1}{q^i-1}.$$

Proof. The proof follows from Corollary 1.4 and [Fio20, Theorem 1.4]. □

We can observe that the bound of Corollary 5.8 is not always reached. We are ready to prove the Dichotomy of Theorem 1.6 and the main result of this paper.

Proof of Theorem 1.6. The proof follows from Corollary 5.8 for an abelian group of squarefree order. By [Bul02] and [Kre19] a group **G** of non-squarefree order has infinitely many expansions up to term equivalence. □

This nice dichotomy in the behaviour of the expansions of a finite abelian group shows how different the expansions are in case of a squarefree abelian group and in case of a not squarefree one.

With the next two results we can also find a concrete bound for the arity of the generators that we need to characterize these clones.

Theorem 5.9. *Let $s = p_1 \cdots p_m$ be a product of distinct prime numbers and let $\mathbb{F}_i = \prod_{j\in[m]\setminus\{i\}} \mathbb{Z}_{p_j}$. Then a clone C containing* $\mathrm{Clo}(\mathbb{Z}_s, +)$ *is generated by $S = \bigcup_{i=1}^{m} S_i$ where:*

$$S_i := \bigcup_{j=0}^{p_i} \{\overline{rx_1\cdots x_j} \mid r\colon \mathbb{F}_i \to \mathbb{Z}_{p_i}, \overline{rx_1\cdots x_j} \in C\}.$$

Proof. Let C be a clone containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ and let $f \in C^{[n]}$. By Remark 3.4, for all $i \in [m]$ there exists a sequence $\{f_{(i,\boldsymbol{h}_i)}\}_{\boldsymbol{h}_i\in[p_i-1]_0^n}$ of functions from $\mathbb{F}_i^n$ to $\mathbb{Z}_{p_i}$, such that f satisfies for all $(\boldsymbol{x}_1,\dots,\boldsymbol{x}_m) \in \prod_{i=1}^m \mathbb{Z}_{p_i}^n$:

$$\begin{aligned} f(\boldsymbol{x}_1,\dots,\boldsymbol{x}_m) =&(\sum_{\boldsymbol{h}_1\in[p_1-1]_0^n} f_{(1,\boldsymbol{h}_1)}(\boldsymbol{x}_2,\dots,\boldsymbol{x}_m)\boldsymbol{x}_1^{\boldsymbol{h}_1},\dots, \\ &\sum_{\boldsymbol{h}_m\in[p_m-1]_0^n} f_{(m,\boldsymbol{h}_m)}(\boldsymbol{x}_1,\dots,\boldsymbol{x}_{m-1})\boldsymbol{x}_m^{\boldsymbol{h}_m}). \end{aligned}$$

Let $w \in \mathbf{R}^A[X]_{p_1}$ be such that $\overline{w}^{[n]} = \prod_{i=2}^m p_i^{p_1-1} f$, where $\mathbf{R}^A = \mathbb{Z}_{p_1}^{\mathbb{F}_1^n}$. Let $h = f_{\boldsymbol{l}} x^{\boldsymbol{l}}$ be a monomial of w and let $s = \mathrm{tD}(h)$. Then, by Lemmata 5.4 and 5.5, we have that $\overline{h} \in C$. Furthermore, let $d \in \mathbb{N}_0$ be such that if $s \neq 0, 1$, then $2 \leq d \leq p_1$ and $d = s$ modulo $p_1 - 1$. If $s = 0, 1$ then $s = d$. Thus, by Lemmata 5.6 and 5.7 it follows that $\mathrm{Clg}(\overline{h}) = \mathrm{Clg}(\{\overline{f_{\boldsymbol{l}} x_1 \cdots x_s}\}) = \mathrm{Clg}(\{\overline{f_{\boldsymbol{l}} x_1 \cdots x_d}\})$. Then let us consider the $(\mathbb{Z}_{p_1}, \mathbb{F}_1)$-linearly closed clonoid generated by $f_{\boldsymbol{l}}$. By [Fio20, Theorem 1.2], there exists a set unary functions F from $\mathbb{F}_1$ to $\mathbb{Z}_{p_1}$ such that $\mathrm{Cig}(\{F\}) = \mathrm{Cig}(\{f_{\boldsymbol{l}}\})$. Hence, by the embedding of Theorem 1.2 (5.1), we have that $\mathrm{Clg}(\{\overline{f_{\boldsymbol{l}} x_1 \cdots x_i}\}) = \mathrm{Clg}(\{\overline{g x_1 \cdots x_i} \mid g \in F\})$ for all $i \in [p_1]_0$. Hence $\overline{h} \in \mathrm{Clg}(S_1)$ and thus $\prod_{i=2}^m p_i^{p_1-1} f \in \mathrm{Clg}(S_1)$ since $\mathrm{Clg}(S_1)$ contains every induced monomial in $\prod_{i=2}^m p_i^{p_1-1} f$.

In the same way we can observe that $\prod_{j\in[m]\setminus\{i\}} p_j^{p_i-1} f \in \mathrm{Clg}(S_i)$ for all $i \in [m]$ and thus $f = \sum_{i\in[m]} \prod_{j\in[m]\setminus\{i\}} p_j^{p_i-1} f \in \mathrm{Clg}(\bigcup_{i\in[m]} S_i)$ and the claim holds. □

The proof of Corollary 1.5 follows directly from Theorem 5.9 and gives an important connection between a clone C containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ and its subsets of generators S_i, where s is a product of distinct primes. Theorem 5.9 gives a possibly redundant list of generators for a clone containing $\mathrm{Clo}(\mathbb{Z}_s, +)$ which shows how deep the link between clonoids and clones is. The generators of Theorem 5.9 are a product of a unary member of a set of generators for an $(\mathbb{Z}_{p_i}, \mathbb{F}_i)$-linearly closed clonoid and a monomial generating a clone on $\mathbb{Z}_{p_i}$. This unifies the characterization in [Kre19] and [Fio20, Theorem 1.2] and is the main reason why Theorem 1.2 works. This also justifies the use of polynomials of $\mathbb{Z}_p^n[X]$ done in this section to represent functions of a clone of a squarefree abelian group and gives a different perspective to these functions.

Using [Fio19, Theorem 1.3] we can refine Corollary 1.4 to the following version for clones containing the addition of $\mathbb{Z}_{pq}$, with p, q distinct primes.

Corollary 5.10. *Let p and q be distinct prime numbers. Let $\prod_{i=1}^{n} p_i^{k_i}$ and $\prod_{i=1}^{s} r_i^{d_i}$ be the factorizations of $g_p = x^{q-1} - 1$ in $\mathbb{Z}_p[x]$ and of $g_q = x^{p-1} - 1$ in $\mathbb{Z}_q[x]$ for irreducible p_i, q_i, respectively. Then:*

$$2\Big(\prod_{i=1}^{n}(k_i+1) + \prod_{i=1}^{s}(d_i+1)\Big) - 1 \leq |\mathcal{L}(\mathbb{Z}_{pq}, +)| \leq$$
$$\leq 2^{p+q+2} \prod_{i=1}^{n}(k_i+1)^{p+1} \prod_{i=1}^{s}(d_i+1)^{q+1} \leq 2^{qp+q+p}.$$

Acknowledgements

The author thanks Erhard Aichinger, who inspired this paper, and Sebastian Kreinecker for many hours of fruitful discussions. The author thanks the referee for his/her useful suggestions.

References

[AM07] E. Aichinger and P. Mayr. Polynomial clones on groups of order pq. *Acta Math. Hungar.*, 114(3):267–285, 2007.

[AM15] E. Aichinger and P. Mayr. Independence of algebras with edge term. *Internat. J. Algebra Comput.*, 25(7):1145–1157, 2015.

[Bul02] A. A. Bulatov. Polynomial clones containing the Mal'tsev operation of the groups $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. *Multiple-valued logic*, volume 8, pages 193–221, 2002.

[Eis95] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1995.

[Fio19] S. Fioravanti. Closed sets of finitary functions between finite fields of coprime order. arXiv:1910.11759, To appear in Algebra Universalis, 2019.

[Fio20] S. Fioravanti. Closed sets of finitary functions between products of finite fields of pair-wise coprime order. arXiv:2009.02237 2020.

[Idz99] P. M. Idziak. Clones containing Mal'tsev operations. *Internat. J. Algebra Comput.*, 9(2):213–226, 1999.

[Kre19] S. Kreinecker. Closed function sets on groups of prime order. *Journal of Multiple-Valued Logic and Soft Computing*, 33(1–2):51–74, 2019.

[KBJ05] A. Krokhin, A. A. Bulatov, and P. Jeavons. The complexity of constraint satisfaction: an algebraic approach. In *Structural theory of automata,* *semigroups, and universal algebra*, volume 207 of *NATO Sci. Ser. II Math. Phys. Chem.*, pages 181–213. Springer, Dordrecht, 2005. Notes taken by Alexander Semigrodskikh.

[May08] P. Mayr. Polynomial clones on squarefree groups. *Internat. J. Algebra Comput.*, 18(4):759–777, 2008.

[PK79] R. Pöschel and L. A. Kalužnin. *Funktionen- und Relationenalgebren*, volume 15 of *Mathematische Monographien [Mathematical Monographs]*. VEB Deutscher Verlag der Wissenschaften, Berlin, 1979. Ein Kapitel der diskreten Mathematik. [A chapter in discrete mathematics].

[Pos41] E. L. Post. The two-valued iterative systems of mathematical logic. *Annals of Mathematics Studies, no. 5*, pages viii+122, 1941.

[Ros69] I. Rosenberg. Maximal clones on algebras A and A^r. *Rend. Circ. Mat. Palermo (2)*, 18:329–333, 1969.

[Sze86] Á. Szendrei. *Clones in universal algebra*, volume 99 of *Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics]*. Presses de l'Université de Montréal, Montreal, QC, 1986.

Stefano Fioravanti, Institut für Algebra, Johannes Kepler Universität Linz, 4040 Linz, Austria

Email address: `stefano.fioravanti66@gmail.com`

URL: `http://www.jku.at/algebra`