Algebra Univers. (2020) 81:52

1420-8911/20/040001-14
published online September 27,2020
https://doi.org/10.1007/s00012-020-00683-5

Algebra Universalis

Closed sets of finitary functions between finite fields of coprime order

Stefano Fioravanti

Abstract. We investigate the finitary functions from a finite field $\mathbb{F}_q$ to the finite field $\mathbb{F}_p$, where p and q are powers of different primes. An $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid is a subset of these functions which is closed under composition from the right and from the left with linear mappings. We give a characterization of these subsets of functions through the invariant subspaces of the vector space $\mathbb{F}_p^{\mathbb{F}_q \setminus \{0\}}$ with respect to a certain linear transformation with minimal polynomial $x^{q-1} - 1$. Furthermore we prove that each of these subsets of functions is generated by one unary function.

Mathematics Subject Classification. 08A40.

Keywords. Clonoids, Clones.

1. Introduction

The problem of characterizing sets of functions that satisfy some closure properties plays an increasingly important role in General Algebra. E. Post's characterization of all clones on a two-element set [13] is a foundational result in this field, which was developed further, e.g., in [14,12,15,10]. Starting from [9], clones are used to study the complexity of certain constraint satisfaction problems (CSPs).

The aim of this paper is to describe sets of functions from $\mathbb{F}_q$ to $\mathbb{F}_p$ that are closed under all linear mappings from the left and from the right, in the case p and q are powers of distinct primes. We are dealing with sets of functions with different domains and codomains; such sets are investigated, e.g., in [1] and are called clonoids. Let $\mathbf{B}$ be an algebra, and let A be a non-empty set. For a subset C of $\bigcup_{n\in\mathbb{N}} B^{A^n}$ and $k \in \mathbb{N}$, we let $C^{[k]} := C \cap B^{A^k}$. According to

Presented by R. Pöschel.
The research was supported by the Austrian Science Fund (FWF):P29931.

Definition 4.1 of [1] we call C a *clonoid* with source set A and target algebra $\mathbf{B}$ if

(1) for all $k \in \mathbb{N}$: $C^{[k]}$ is a subuniverse of $\mathbf{B}^{A^k}$, and
(2) for all $k, n \in \mathbb{N}$, for all $(i_1, \ldots, i_k) \in \{1, \ldots, n\}^k$, and for all $c \in C^{[k]}$, the function $c' \colon A^n \to B$ with $c'(a_1, \ldots, a_n) := c(a_{i_1}, \ldots, a_{i_k})$ lies in $C^{[n]}$.

By (1) every clonoid is closed under composition with operations of $\mathbf{B}$ on the left. In particular we are interested in those clonoids whose target algebra is the vector space $\mathbb{F}_p$ which are closed under composition with linear mappings also from the right side.

Definition 1.1. 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. An $(\mathbb{F}_p, \mathbb{F}_q)$-*linearly 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 $n \in \mathbb{N}$, $f, g \in C^{[n]}$ and $a, b \in \mathbb{F}_p$:
$$af + bg \in C^{[n]};$$
(2) for all $m, n \in \mathbb{N}$, $f \in C^{[m]}$ and $A \in \mathbb{F}_q^{m\times n}$:
$$g \colon (x_1, \ldots, x_n) \mapsto f(A \cdot (x_1, \ldots, x_n)^t)$$
is in $C^{[n]}$.

Clonoids are of interest since they naturally arise in the study of promise constraint satisfaction problems (PCSPs). These problems are investigated, e.g., in [4], and recently in [5] clonoid theory has been used to give an algebraic approach to PCSPs. Moreover, a description of the set of all $(\mathbb{Z}_p, \mathbb{Z}_q)$-linearly closed clonoids, where p and q are distinct primes, is a useful tool to investigate (polynomial) clones on $\mathbb{Z}_p \times \mathbb{Z}_q$ or to represent polynomial functions of semidirect products of groups. In [8] S. Kreinecker characterized linearly closed clonoids on $\mathbb{Z}_p$, where p is a prime, and found a description of all clones on $\mathbb{Z}_p$ that contain the addition, all iterative algebras on $\mathbb{Z}_p$ which are closed under composition with the clone generated by $+$ from both sides, and proved that there are infinitely many non-finitely generated clones above $\mathrm{Clo}(\mathbb{Z}_p \times \mathbb{Z}_p, +)$ for $p > 2$.

Our main result (Theorem 1.3) provides a complete description of the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids, where p and q are powers of different primes. First, an important observation is that each such clonoid is generated by its subset of unary members (Theorem 4.3). We can say even more about the generators of an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid.

Theorem 1.2. *Let p and q be powers of different primes. Then every $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid is generated by one unary function.*

The proof of this result is given in Section 5. With Theorem 4.3 and the characterization of the invariant subspaces lattice of a cyclic linear transformation over a finite-dimensional vector space in [3], we obtain a description of the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids as a direct product of chains (Section 5).

The structure of the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids depends on the prime factorization of the polynomial $g = x^{q-1} - 1$ in $\mathbb{F}_p[x]$. Once this factorization is known, it is easy to find this lattice. Let us denote by $\mathbf{2}$ the two-element chain and, in general, by $\mathbf{C}_k$ the chain with k elements. Moreover, we denote by $\mathcal{L}(p, q)$ the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids.

Theorem 1.3. *Let p and q be powers of different primes. Let $\prod_{i=1}^{n} p_i^{k_i}$ be the factorization of the polynomial $g = x^{q-1} - 1$ in $\mathbb{F}_p[x]$ into its irreducible divisors. Then the number of distinct $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids is $2\prod_{i=1}^{n}(k_i + 1)$ and the lattice $\mathcal{L}(p, q)$ of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids is isomorphic to*

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

2. Preliminaries and notations

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 $\boldsymbol{u}$.

We write $\mathrm{Clg}(S)$ for the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid generated by a set of functions S. The $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids form a lattice with the intersection as meet and the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid generated by the union as join. The top element of the lattice is the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid of all functions and the bottom element consists of only the constant zero functions. Let f be an n-ary function from a group $\mathbf{G}_1$ to a group $\mathbf{G}_2$. We say that f is 0-*preserving* if $f(0_{\mathbf{G}_1}, \ldots, 0_{\mathbf{G}_1}) = 0_{\mathbf{G}_2}$.

As examples of non-trivial $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids we can see that the set of all 0-preserving finitary functions from $\mathbb{F}_q$ to $\mathbb{F}_p$ forms an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid and that the following set of functions forms an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid.

Definition 2.1. Let p and q be powers of primes and let f be a function from $\mathbb{F}_q^n$ to $\mathbb{F}_p$. The function f is a *star function* if and only if for every vector $\boldsymbol{w} \in \mathbb{F}_q^n$ there exists $k \in \mathbb{F}_p$ such that for every $\lambda \in \mathbb{F}_q \backslash \{0\}$:

$$f(\lambda \boldsymbol{w}) = k.$$

It is easy to see that the star functions form an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid for every p and q and they represent an instance of the nice behaviour that the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids have in relation to the lines of the space $\mathbb{F}_q^n$. Indeed, the composition with scalar multiplications from the right hand side can be used to permute the values that functions of $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid have in lines that pass through the origin.

3. Preliminaries from linear algebra

In this section we review some concepts of linear algebra that we need in order to find a description of the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids, where

p and q are powers of distinct primes. We recall that a *T-invariant subspace* of a linear operator T of a vector space V is a subspace W of V that is preserved by T; that is, $T(W) \subseteq W$. Let S be a set of linear operators of a vector space V. We can consider the S-invariant subspaces lattice of V and we denote it by $\mathcal{L}(S)$.

In Section 5 we will see that the problem to find the structure of the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids can be reduced to the problem to find all T-invariant subspaces of the vector space $\mathbb{F}_p^{\mathbb{F}_q \setminus \{0\}}$, where T is a certain linear transformation that permutes the components of $\mathbb{F}_p^{\mathbb{F}_q \setminus \{0\}}$. In [3] the structure of the invariant subspaces lattice of a linear transformation on a finite-dimensional vector space over an arbitrary field has been studied, and in [6] the number of invariant subspaces of a finite vector space with respect to a linear operator is determined.

Let T be a linear transformation on a finite-dimensional vector space V over a field $\mathbb{K}$ and let g be the minimal polynomial of T. We call T *primary* if $g = f^c$ for some irreducible polynomial f and some positive integer c. We know from [3, Theorem 1] that, with the prime factorization of $g = \prod_{i=1}^{s} p_i^{k_i}$ over $\mathbb{K}[\boldsymbol{x}]$, we can split the vector space V into what is called its *primary decomposition*:

$$V = \bigoplus_{i=1}^{s} V_i,$$

and $V_i = \ker(p_i(T)^{k_i})$ are called the *primary components* of V. According to [3], the lattice $\mathcal{L}(T)$ of the T-invariant subspaces of V is a direct product of the lattices $\mathcal{L}(T_i)$, where $T_i = T|_{V_i}$. Thus:

$$\mathcal{L}(T) = \prod_{i=1}^{s} \mathcal{L}(T_i).$$

Definition 3.1. Let V be a vector space, let M be a subspace of V, and let T be a linear transformation. If M is generated by $\{x, Tx, T^2x, \dots\}$ for some $x \in V$, then T is called *cyclic*, M is called a *T-cyclic subspace*, and x is called a *T-cyclic vector* for M.

Remark 3.2. Let V be a finite dimensional vector space over a field $\mathbb{K}$ and let $T\colon V \to V$ be a linear operator such that V is T-cyclic. Then every T-invariant subspace of V is T-cyclic.

Proof. Let $W = \langle \boldsymbol{w}_1, \dots, \boldsymbol{w}_n \rangle$ be a T-invariant subspace of V and let $\boldsymbol{v}$ be a T-cyclic vector of V. Then there exist $p_1, \dots, p_n \in \mathbb{K}[x]$ such that $\boldsymbol{w}_i = p_i(T)\boldsymbol{v}$ for all $i \in \{1, \dots, n\}$. Let $d = \gcd(p_1, \dots, p_n)$. Then $W = \{q(T)(d(T)\boldsymbol{v}) \mid q \in \mathbb{K}[x]\}$. Thus W is T-cyclic with T-cyclic vector $d(T)\boldsymbol{v}$. □

In [3, Lemma 2] it is proved that $\mathcal{L}(T)$ is a chain if and only if T is cyclic and primary. In particular they show that if the minimal polynomial of T is $g = f^n$, with f irreducible, then:

$$\mathcal{L}(T) = \{\ker(f(T)^k) \mid k \in \{0, 1, \dots, n\}\}.$$

4. Generators of $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids

In this section our aim is to find a set of unary generators of an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid. In general we will see that it is the unary part of an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid that determines the clonoid. To this end we shall show the following Lemma.

Lemma 4.1. *Let $\mathbb{F}_p$ and $\mathbb{F}_q$ be finite fields and let $f, g\colon \mathbb{F}_q^n \to \mathbb{F}_p$ be functions such that there exists $\boldsymbol{b} \in \mathbb{F}_q^n \setminus \{(0,\dots,0)\}$ with $f(\lambda \boldsymbol{b}) = g(\lambda(1,0,\dots,0))$ for all $\lambda \in \mathbb{F}_q$ and $f(\boldsymbol{x}) = g(\boldsymbol{y}) = 0$ for all $\boldsymbol{x} \in \mathbb{F}_q^n \setminus \{\lambda \boldsymbol{b} \mid \lambda \in \mathbb{F}_q\}$ and $\boldsymbol{y} \in \mathbb{F}_q^n \setminus \{\lambda(1,0,\dots,0) \mid \lambda \in \mathbb{F}_q\}$. Then $f \in \mathrm{Clg}(\{g\})$.*

Proof. Let $n \in \mathbb{N}$ and $\boldsymbol{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n \setminus \{(0,\dots,0)\}$. Let $1 \le i \le n$ be such that $b_i \neq 0$ and let $f, g\colon \mathbb{F}_q^n \to \mathbb{F}_p$ be functions as in the hypothesis. Moreover, let $L = \{s\boldsymbol{b} \mid s \in \mathbb{F}_q\}$ be the line of the space $\mathbb{F}_q^n$ generated by the vector $\boldsymbol{b}$. Let us consider $\boldsymbol{l}_j \in \mathbb{F}_q^n$ for $1 \le j \le n-1$ such that the solutions of the system formed by the equations $(\langle \boldsymbol{l}_j, \boldsymbol{y} \rangle = 0)_{1 \le j \le n-1}$ describe the line L of $\mathbb{F}_q^n$. Then:

$$g(b_i^{-1} x_i, \langle \boldsymbol{l}_1, \boldsymbol{x} \rangle, \dots, \langle \boldsymbol{l}_{n-1}, \boldsymbol{x} \rangle) = f(\boldsymbol{x}), \qquad \text{for all } \boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n.$$

Hence $g \in \mathrm{Clg}(\{g\})$ and the claim holds. □

In order to show the main theorem of the section we introduce the definition of *Lagrange interpolation functions*, which are functions built to have a value different from zero only in one point, and they can be seen as characteristic functions of a point in the vector space $\mathbb{F}_q^n$ with codomain $\{0,1\} \subseteq \mathbb{F}_p$.

Definition 4.2. Let $\boldsymbol{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$. The *$n$-ary Lagrange interpolation function* $f_{\boldsymbol{a}}$ from $\mathbb{F}_q$ to $\mathbb{F}_p$ is the function defined by:

$$f_{\boldsymbol{a}}(\boldsymbol{a}) = 1,$$
$$f_{\boldsymbol{a}}(\boldsymbol{x}) = 0, \quad \text{for } \boldsymbol{x} \in \mathbb{F}_q^n \setminus \{\boldsymbol{a}\}.$$

We are now ready to prove that an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid C is generated by its unary part.

Theorem 4.3. *Let p and q be powers of different primes. Then every $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid C is generated by its unary functions. Thus $C = \mathrm{Clg}(C^{[1]})$.*

Proof. The inclusion $\supseteq$ is obvious. For the other inclusion let C be an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid and let f be an n-ary function in C. In order to prove that $f \in \mathrm{Clg}(C^{[1]})$ we show that $f' = f - f(\boldsymbol{0})$ is in $\mathrm{Clg}(C^{[1]})$, where $f(\boldsymbol{0})$ is the constant n-ary function with value $f(\boldsymbol{0})$. This implies the claim because the n-ary constant function with value $f(\boldsymbol{0})$ is in $\mathrm{Clg}(C^{[1]})$ by Definition 1.1. We can see that f' is a 0-preserving function of C. The strategy is to interpolate f' in every line passing through the origin. To this end, let

$$R = \{L_i \mid 1 \le i \le (q^n - 1)/(q-1) = s\}$$

be the set of all s distinct lines of the space $\mathbb{F}_q^n$ that pass through the origin, parametrized by the vectors $\boldsymbol{l}_i \in \mathbb{F}_q^n$ with $i \in \{1, \dots s\} = I$. For all $i \in I$, let $f_{L_i} \colon \mathbb{F}_q^n \to \mathbb{F}_p$ be defined by:

$$f_{L_i}(\lambda \boldsymbol{l}_i) = f'(\lambda \boldsymbol{l}_i), \quad \text{for } \lambda \in \mathbb{F}_q,$$
$$f_{L_i}(\boldsymbol{x}) = 0, \quad \text{for } \boldsymbol{x} \in \mathbb{F}_q^n \backslash \{\lambda \boldsymbol{l}_i \mid \lambda \in \mathbb{F}_q\}.$$

Since f' is 0-preserving we can write f' as:

$$f' = \sum_{i=1}^{s} f_{L_i}.$$

To prove that $f \in \mathrm{Clg}(C^{[1]})$ it is therefore sufficient to show that $f_{L_i} \in \mathrm{Clg}(C^{[1]})$ for all $L_i \in R$. Let $i \in I$ and let $g \colon \mathbb{F}_q \to \mathbb{F}_p$ be a function such that $f_{L_i}(x\boldsymbol{l}_i) = g(x) = f'(x\boldsymbol{l}_i)$. Then we prove by induction on the arity m that the function $t_m \colon \mathbb{F}_q^m \to \mathbb{F}_p$ defined by:

$$t_m(x, 0, \dots, 0) = g(x), \quad \text{for all } x \in \mathbb{F}_q,$$
$$t_m(x_1, \dots, x_n) = 0, \quad \text{for } \boldsymbol{x} \in \mathbb{F}_q^n \backslash \{\lambda(1, 0, \dots, 0) \mid \lambda \in \mathbb{F}_q\},$$

is in $\mathrm{Clg}(C^{[1]})$.

Case $m = 1$: if $m = 1$ then $t_1 = g$ is a unary function of $C^{[1]}$.

Case $m > 1$: by the induction hypothesis we know that $t_{m-1} \in \mathrm{Clg}(C^{[1]})$. We define $s_m \colon \mathbb{F}_q^2 \to \mathbb{F}_q^m$ by $s_m(i, j) = (i, j, 0, \dots, 0)$. We denote by $f_{s_m(h,k)}$ the Lagrange interpolation function of the point $s_m(h, k)$ (Definition 4.2). Let us define the function $r \colon \mathbb{F}_q^m \to \mathbb{F}_p$ by:

$$r(\boldsymbol{x}) = \sum_{a \in \mathbb{F}_q} t_{m-1}(x_1 - ax_2, x_3, \dots, x_m) - \sum_{a \in \mathbb{F}_q \backslash \{0\}} t_{m-1}(ax_2, x_3, \dots, x_m) \tag{4.1}$$

for all $\boldsymbol{x} = (x_1, \dots, x_m) \in \mathbb{F}_q^m$. We prove that:

$$r(x_1, \dots, x_m) = q t_m(x_1, \dots, x_m)$$

for all $(x_1, \dots, x_m) \in \mathbb{F}_q^m$.

Case $x_i \neq 0$ for some $i \in \{3, ..., n\}$: then $r(\boldsymbol{x}) = 0 = t_m(\boldsymbol{x})$.

Case $x_2 = 0$: in this case $r(\boldsymbol{x}) = \sum_{a \in \mathbb{F}_q} g(x_1 - ax_2) - \sum_{a \in \mathbb{F}_q \backslash \{0\}} g(ax_2) = qg(x_1)$ for all $x_1 \in \mathbb{F}_q$, as required.

Case $x_2 \neq 0$: we have $r(\boldsymbol{x}) = \sum_{a \in \mathbb{F}_q} g(x_1 - ax_2) - \sum_{a \in \mathbb{F}_q \backslash \{0\}} g(ax_2) = \sum_{a \in \mathbb{F}_q} g(a) - \sum_{a \in \mathbb{F}_q \backslash \{0\}} g(a) = g(0) = 0$.

Because of (4.1), we have $r \in \mathrm{Clg}(\{t_{m-1}\}) \subseteq \mathrm{Clg}(C^{[1]})$. Hence we have that $qt_m \in \mathrm{Clg}(C^{[1]})$ and thus $t_m \in \mathrm{Clg}(C^{[1]})$. This concludes the induction. Thus $t_n \in \mathrm{Clg}(C^{[1]})$ and we can see that $f_{L_i}(\lambda \boldsymbol{l}_i) = t_n(\lambda(1, 0, \dots, 0)) = g(\lambda)$, for all $\lambda \in \mathbb{F}_q$, and $f_{L_i}(\boldsymbol{x}) = t_n(\boldsymbol{y}) = 0$ for all $\boldsymbol{x} \in \mathbb{F}_q^n \backslash \{\lambda \boldsymbol{l}_i \mid \lambda \in \mathbb{F}_q\}$ and $\boldsymbol{y} \in \mathbb{F}_q^n \backslash \{\lambda(1, 0, \dots, 0) \mid \lambda \in \mathbb{F}_q\}$. By Lemma 4.1, $f_{L_i} \in \mathrm{Clg}(\{t_n\}) \subseteq \mathrm{Clg}(C^{[1]})$, which concludes the proof. □

Theorem 4.4. *Let p and q be two powers of distinct primes. Then the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid of all 0-preserving functions is generated by the unary Lagrange interpolation function f_1 (Definition 4.2).*

Proof. The proof follows directly from Theorem 4.3 since $\mathrm{Clg}(f_1)$ contains every 0-preserving unary function. □

The following two corollaries of Theorem 4.3 tell us that there are only finitely many distinct $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids.

Corollary 4.5. *Let p and q be powers of different primes. Let C and D be two $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids. Then $C = D$ if and only if $C^{[1]} = D^{[1]}$.*

Corollary 4.6. *Let p and q be powers of distinct prime numbers. Then every $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid has a set of finitely many unary functions as generators, and hence there are only finitely many distinct $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids.*

5. The lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids

In this section we investigate the structure of the lattice $\mathcal{L}(p, q)$ of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids through a characterization of their unary parts. We call the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids that are composed by only 0- preserving functions 0-*preserving* $(\mathbb{F}_p, \mathbb{F}_q)$-*linearly closed clonoids*. We will see that there is an isomorphism between the sublattice $\mathcal{L}_0(p, q)$ of the 0-preserving $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids and the lattice of subspaces that are invariant under a particular cyclic linear transformation $A(p, q)$ on the vector space $\mathbb{F}_p^{\mathbb{F}_q - 1}$.

In order to characterize the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids we need the definition of a *monoid ring*.

Definition 5.1. Let $\langle M, + \rangle$ be a monoid and let $\langle R, +, \odot \rangle$ be a commutative ring with identity. Let

$$S := \{f \in R^M \mid f(a) \neq 0 \text{ for only finitely many } a \in M\}.$$

We define the *monoid ring* of M over R as the ring $(S, +, \cdot)$. Here $+$ is the point-wise addition of functions and $(\sigma \cdot \rho)(a) := \sum_{b \in M} \sigma(b) \odot \rho(a - b)$. We denote the monoid ring of M over R by $R[M]$.

Using the notation of [2] for all $a \in M$ we define τ_a to be the element of R^M with $\tau_a(a) = 1$ and $\tau_a(M \backslash \{a\}) = \{0\}$. We observe that for all $f \in R[M]$ there is an $\boldsymbol{r} \in R^M$ such that $f = \sum_{a \in M} r_a \tau_a$ and that we can multiply such expressions using the rule $\tau_a \cdot \tau_b = \tau_{a+b}$.

Definition 5.2. Let $\mathbb{F}_p$ and $\mathbb{F}_q$ be finite fields and let $\mathbb{F}_q^\times = (\mathbb{F}_q, \cdot)$ be the multiplicative monoid reduct of $\mathbb{F}_q$. We define the action $*\colon \mathbb{F}_p[\mathbb{F}_q^\times] \times \mathbb{F}_p^{\mathbb{F}_q} \to \mathbb{F}_p^{\mathbb{F}_q}$ for all $a \in \mathbb{F}_q^\times$ and $f \in \mathbb{F}_p^{\mathbb{F}_q}$ by

$$(\tau_a * f)(x) = f(ax).$$

So for $\sigma \in \mathbb{F}_p[\mathbb{F}_q^\times]$ with $\sigma = \sum_{a \in \mathbb{F}_q^\times} z_a \tau_a$, then

$$(\sigma * f)(x) = \sum_{a \in \mathbb{F}_q^\times} z_a f(ax).$$

We can observe that V is an $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodule of $\mathbb{F}_p^{\mathbb{F}_q}$ if and only if it is a subspace of $\mathbb{F}_p^{\mathbb{F}_q}$ satisfying

$$x \mapsto f(ax) \in V, \tag{5.1}$$

for all $f \in V$ and $a \in \mathbb{F}_q$. Clearly the following lemma holds.

Lemma 5.3. *Let p and q be powers of primes. Then the unary part of an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid is an $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodule of $\mathbb{F}_p^{\mathbb{F}_q}$.*

In order to show the following results we use the Galois correspondence between clonoids and pairs of relations as developed in [11].

Definition 5.4. For a set I and $R \subseteq A^I$, $S \subseteq B^I$ let

$$\mathrm{Pol}(R, S) := \{f \colon A^k \to B \mid k \in \mathbb{N}, f(R, \ldots, R) \subseteq S\}$$

denote the set of finitary functions preserving (R, S). We call $\mathrm{Pol}(R, S)$ the set of *polymorphisms* of the relational pair (R, S).

Let $R := \{(S_i, T_i) \mid i \in I\}$ be a set of pairs of relations on A and B. Then the set of functions that are polymorphisms of all pairs of all the relations in R is denoted by $\mathrm{Pol}(R)$.

Lemma 5.5. *Let p and q be powers of distinct primes. Let U be the subspace of $\mathbb{F}_q^{\mathbb{F}_q}$ that is generated by the identity map on $\mathbb{F}_q$, and let V be an $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodule of $\mathbb{F}_p^{\mathbb{F}_q}$. Then $\mathrm{Pol}(U, V)$ is an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid with unary part V.*

Proof. By Definition 5.4 we have that $V \subseteq \mathrm{Pol}(U, V)$ and every unary function in $\mathrm{Pol}(U, V)^{[1]}$ is in V. Thus $\mathrm{Pol}(U, V)^{[1]} = V$.

Next we show that $\mathrm{Pol}(U, V)$ is an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid. Let $f, g \in \mathrm{Pol}(U, V)$ be m-ary. Thus the functions $x \mapsto f(c_1 x, \ldots, c_m x)$ and $x \mapsto g(c_1 x, \ldots, c_m x)$ are in V for all $c_1, \ldots, c_m \in \mathbb{F}_q$.

Let $a, b \in \mathbb{F}_p$ and let $b_1, \ldots, b_m \in \mathbb{F}_q$. Then

$$(af + bg)(b_1 x, \ldots, b_m x) = af(b_1 x, \ldots, b_m x) + bg(b_1 x, \ldots, b_m x),$$

for all $x \in \mathbb{F}_q$. Hence $af + bg \in \mathrm{Pol}(U, V)$.

Next let $n \in \mathbb{N}$, let $A \in \mathbb{F}_q^{m \times n}$, and let $b_1, \ldots, b_n \in \mathbb{F}_q$. Then

$$x \mapsto f(A \cdot (b_1 x, \ldots, b_n x)^t) = f\left(\sum_{i=1}^{n} A_{1i} b_i x, \ldots, \sum_{i=1}^{n} A_{mi} b_i x\right)$$

is in V. Hence the n-ary function $g \colon \mathbb{F}_q^n \to \mathbb{F}_p$ such that $g \colon (x_1, \ldots, x_n) \mapsto f(A \cdot (x_1, \ldots, x_n)^t)$ is in $\mathrm{Pol}(U, V)$ and thus $\mathrm{Pol}(U, V)$ is an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid. □

A clonoid C with source set A and target algebra $\mathbf{B}$ is *finitely related* if there exists a finite set of pairs of finitary relations R on A and B such that $C = \mathrm{Pol}(R)$. It can be easily observed that every finitely related clonoid is the clonoid of polymorphisms of a single pair of relations.

Together with Theorem 4.3, Lemma 5.5 implies immediately the following.

Lemma 5.6. *Let p and q be powers of distinct primes. Then every $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid is finitely related.*

Corollary 5.7. *Let p and q be powers of distinct primes. Then the function $\pi^{[1]}$ that sends an $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoid to its unary part is an isomorphism between the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids and the lattice of all $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodules of $\mathbb{F}_p^{\mathbb{F}_q}$.*

With the next lemma we begin to characterize the unary parts of the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids. In order to do so we consider the group ring $\mathbb{F}_p[\mathbb{F}_q \backslash \{0\}]$ and the $(\mathbb{F}_p[\mathbb{F}_q \backslash \{0\}], *)$-submodules of $\mathbb{F}_p^{\mathbb{F}_q \backslash \{0\}}$ where $*$ is the restriction of the action defined in Definition 5.2 and $\mathbb{F}_q \backslash \{0\}$ is the multiplicative group of $\mathbb{F}_q$.

Lemma 5.8. *Let p and q be powers of distinct primes. Then the lattice of all $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodules of $\mathbb{F}_p^{\mathbb{F}_q}$ is the direct product of the lattice of all $(\mathbb{F}_p[\mathbb{F}_q \backslash \{0\}], *)$-submodules of $\mathbb{F}_p^{\mathbb{F}_q \backslash \{0\}}$ (isomorphic to $\mathcal{L}_0(p,q)$) and the two-element chain $\mathbf{2}$.*

Proof. Let $V_0, V_1 \subseteq \mathbb{F}_p^{\mathbb{F}_q}$ be defined by:

$$V_0 := \{\boldsymbol{v} \in \mathbb{F}_p^{\mathbb{F}_q} \mid v_0 = 0\},$$
$$V_1 := \{\lambda(1, \dots, 1) \mid \lambda \in \mathbb{F}_p\}.$$

It is clear that V_0 and V_1 are $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodules of $\mathbb{F}_p^{\mathbb{F}_q}$ and we denote the lattices of all $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodules of V_0 and V_1 by $\mathcal{L}_0$ and $\mathcal{L}_1$. We can observe that $\mathcal{L}_1 \cong \mathbf{2}$. Moreover, $V_0 + V_1 = \mathbb{F}_p^{\mathbb{F}_q}$ and $V_0 \cap V_1 = 0$. Let W be an $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodule of $\mathbb{F}_p^{\mathbb{F}_q}$. Then we have that either $W \leq V_0$ or $W \geq V_1$, since $\boldsymbol{v} \notin V_0$ implies $v_0 \neq 0$ and thus that $(1, \dots, 1)$ is in the $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodule of $\mathbb{F}_p^{\mathbb{F}_q}$ generated by $\boldsymbol{v}$. Next, we show that $W = (W \cap V_0) + (W \cap V_1)$:

Case $W \leq V_0$: then $(W \cap V_0) + (W \cap V_1) = W + (W \cap V_1) = W$

Case $W \geq V_1$: then $(W \cap V_0) + (W \cap V_1) = (W \cap V_0) + V_1$ which is equal to $W \cap (V_0 + V_1) = W$, using the modular law. Thus the function γ from the lattice $\mathcal{L}_0 \times \mathcal{L}_1$ to the lattice of all $(\mathbb{F}_p[\mathbb{F}_q^\times], *)$-submodules of $\mathbb{F}_p^{\mathbb{F}_q}$ such that $\gamma \colon (R, W) \mapsto R + W$ is clearly surjective and order preserving. Furthermore, let $(R_1, W_1), (R_2, W_2) \in \mathcal{L}_0 \times \mathcal{L}_1$ with $R_1 + W_1 = R_2 + W_2$. Then, since $R_1, R_2 \leq V_0, W_1, W_2 \leq V_1$, and $V_0 \cap V_1 = 0$, $R_1 = (R_1 + W_1) \cap V_0 = (R_2 + W_2) \cap V_0 = R_2$, using the modular law. With the same strategy we can prove that $W_1 = W_2$ and it is clear that γ^{-1} is order preserving. Thus γ is a lattice isomorphism.

Hence, by Corollary 5.7, $\mathcal{L}(p,q)$ is isomorphic to $\mathbf{2} \times \mathcal{L}_0$. Furthermore, the lattice $\mathcal{L}_0$ is isomorphic to $\mathcal{L}_0(p,q)$ via the isomorphism $\pi_{\geq 2} \colon \mathcal{L}_0 \to \mathcal{L}_0(p,q)$ such that:

$$\pi_{\geq 2}(C) := \{(v_1, \dots, v_{q-1}) \mid (0, v_1, \dots, v_{q-1}) \in C\}, \tag{5.2}$$

for all $C \in \mathcal{L}_0$. □

The next step is to characterize the lattice $\mathcal{L}_0(p,q)$. To this end we observe that $V \in \mathcal{L}_0(p,q)$ if and only if is a subspace of $\mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}}$ satisfying

$$x \mapsto f(ax) \in V, \tag{5.3}$$

for all $f \in V$ and $a \in \mathbb{F}_q\setminus\{0\}$.

Let α be a generator of the multiplicative subgroup of $\mathbb{F}_q$. The closure under the linear transformation $A(p,q)\colon \mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}} \to \mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}}$ defined as $A(p,q)(f) = x \mapsto f(\alpha x)$ is enough to describe the property to be closed under all the $q-1$ linear transformations in (5.3). We can see that the minimal polynomial of $A(p,q)$ is $x^{q-1}-1$.

Thus the last step is to characterize the lattice of the $A(p,q)$-invariant subspaces of $\mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}}$. This is sufficient to conclude our characterization of the lattice of all $(\mathbb{F}_p,\mathbb{F}_q)$-linearly closed clonoids since we know from Corollary 5.7 and Lemma 5.8 that $\mathcal{L}(p,q) \cong \mathbf{2} \times \mathcal{L}_0(p,q)$ and the lattice of all the $A(p,q)$-invariant subspaces of $\mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}}$ is isomorphic to the lattice $\mathcal{L}_0(p,q)$ of all $(\mathbb{F}_p,\mathbb{F}_q)$-linearly closed clonoids composed by 0-preserving functions and to the lattice of all $(\mathbb{F}_p[\mathbb{F}_q\setminus\{0\}], *)$-submodules of $\mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}}$.

Corollary 5.7 and Lemma 5.8 describe the structure of the lattice of all $(\mathbb{F}_p,\mathbb{F}_q)$-linearly closed clonoids in case p and q are powers of distinct primes. In Figure 1 we draw a scheme of the lattice of all $(\mathbb{F}_p,\mathbb{F}_q)$-linearly closed clonoids. On the right hand side we have the 0-preserving part and on the left, the part with constants. Let $\mathbf{1}, \mathbf{0_P}, \mathbf{C}, \{\mathbf{0}\}$ denote the $(\mathbb{F}_p,\mathbb{F}_q)$-linearly closed clonoids of all functions, of all 0-preserving functions, of all constants, and of the zero constants respectively.

The lattice of invariant subspaces under a linear transformation on finite-dimensional vector spaces was characterized in [3]. We can see that $A(p,q)$ has minimal polynomial $g = x^{q-1}-1$. Let $g = \prod_{i=1}^{s} p_i^{k_i}$ be the prime factorization

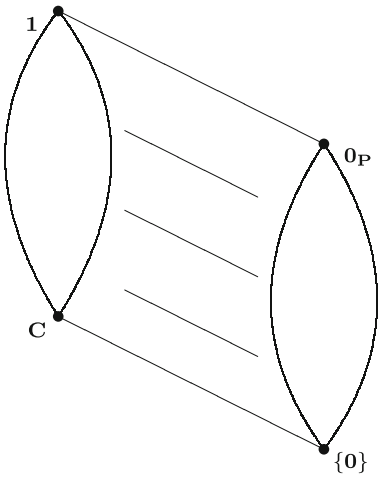

FIGURE 1. .

of g over $\mathbb{F}_p[x]$. We define $V_i = \ker(p_i(A(p,q))^{k_i})$, and $A(p,q)_i = A(p,q)|_{V_i}$. We know from [3] that with the prime factorization of g we can split our vector space $\mathbb{F}_q^{\mathbb{F}_q\setminus\{0\}}$ into its primary decomposition:

$$\mathbb{F}_q^{\mathbb{F}_q\setminus\{0\}} = \bigoplus_{i=1}^{s} V_i.$$

According to [3] the lattice $\mathcal{L}(A(p,q))$ of the $A(p,q)$-invariant subspaces of $\mathbb{F}_q^{\mathbb{F}_q\setminus\{0\}}$, is:

$$\mathcal{L}(A(p,q)) \cong \prod_{i=1}^{s} \mathcal{L}(A(p,q)_i). \tag{5.4}$$

We can observe that $\mathbb{F}_q^{\mathbb{F}_q\setminus\{0\}}$ is an $A(p,q)$-cyclic space generated by the vector $(1,0,\ldots,0)$. Thus, every $A(p,q)$-invariant subspace of $\mathbb{F}_q^{\mathbb{F}_q\setminus\{0\}}$ is $A(p,q)$-cyclic, by Remark 3.2.

With these tools we are now ready to prove Theorems 1.2 and 1.3.

Proof of Theorem 1.2.. Let C be an $(\mathbb{F}_p,\mathbb{F}_q)$-linearly closed clonoid and let C_0 be its 0-preserving part. Let V be the image of C_0 under the isomorphism of Corollary 5.7 and let (V_1,V_2) be the image of V under the isomorphism of Lemma 5.8. Furthermore let W be the image of V_1 under $\pi_{\geq 2}$. We have observed that W is an $A(p,q)$-cyclic space. Let $\boldsymbol{v}$ be the $A(p,q)$-cyclic vector for W (Definition 3.1). We can observe that $f = (0, v_1, \ldots, v_{q-1})$ is a generator for $C_0^{[1]}$ and thus, by Theorem 4.3, is a unary generator for C_0. Furthermore, either $C_0 = C$ or $C_0 \subset C$.

Case $C_0 = C$: then C is generated by f.

Case $C_0 \subset C$: then $\{1\} \in C$, where 1 is the constant unary function with value 1. Let f be the unary generator of C_0. We will prove that C is generated by $h = f + 1$. Indeed, let $g \in C$ be an n-ary function. Then, there exists a 0-preserving n-ary function g_0 such that $g = g_0 + g(\boldsymbol{0})$, where $g(\boldsymbol{0})$ is the constant n-ary function with value $g(\boldsymbol{0})$. Hence, $g \in \mathrm{Clg}(\{g_0\}) \vee \mathrm{Clg}(\{g(\boldsymbol{0})\}) \subseteq \mathrm{Clg}(\{f\}) \vee \mathrm{Clg}(\{1\}) \subseteq \mathrm{Clg}(\{h\})$. Thus $C = \mathrm{Clg}(\{h\})$ and the claim holds. □

Proof of Theorem 1.3. Let p and q be powers of distinct primes and let $\prod_{i=1}^{n} p_i^{k_i}$ be the prime factorization of the polynomial $g = x^{q-1} - 1$ in $\mathbb{F}_p[x]$. First we know from Corollary 5.7 and Lemma 5.8 that $\mathcal{L}(p,q) \cong \mathbf{2} \times \mathcal{L}_0(p,q)$. Furthermore, we know that $\mathcal{L}_0(p,q)$ is isomorphic to the lattice of all $A(p,q)$-invariant subspaces of $\mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}}$. We have observed that $A(p,q)$ has g as minimal polynomial. So let V_i be the ith primary component and let $(A(p,q))_i$ be the ith restriction of $A(p,q)$ with minimal polynomial $p_i^{k_i}$, for $i = 1,\ldots,n$. Then we know that $\mathbb{F}_p^{\mathbb{F}_q\setminus\{0\}}$ is $(A(p,q))$-cyclic with $(1,0,\ldots,0)$ as $(A(p,q))$-cyclic vector. Hence also V_i is $(A(p,q))$-cyclic, for $i = 1,\ldots,n$, as a subspace of an $(A(p,q))$-cyclic space (Remark 3.2). From [3, Lemma 2], the lattice of all

$A(p,q)_i$-invariant subspaces of V_i is isomorphic to the chain with $k_i + 1$ elements. Thus, from (5.4), we have that:

$$\mathcal{L}(p,q) \cong \mathbf{2} \times \prod_{i=1}^{n} \mathbf{C}_{k_i+1}$$

and the claim holds. □

With this theorem we have completely characterized the structure of the lattice $\mathcal{L}(p,q)$ using the prime factorization of the polynomial $x^{q-1}-1$, which can be easily computed. We conclude our investigation with a corollary that shows how the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids is structured.

Corollary 5.9. *Let p and q be powers of distinct primes. Then the lattice $\mathcal{L}(p,q)$ of the $(\mathbb{F}_p, \mathbb{F}_q)$-linearly closed clonoids is a distributive lattice.*

Proof. It follows from Theorem 1.3 that $\mathcal{L}(p,q)$ is a direct product of chains and hence is distributive. □

Acknowledgements

The author thanks Erhard Aichinger, who inspired this paper, and Sebastian Kreinecker for many hours of fruitful discussions. The author thanks the referees for their useful suggestions.

Funding Open access funding provided by Johannes Kepler University Linz.

References

[1] Aichinger, E., Mayr, P.: Finitely generated equational classes. J. Pure Appl. Algebra **220**(8), 2816–2827 (2016)

[2] Aichinger, E., Moosbauer, J.: Chevalley Warning type results on abelian groups (2019, preprint)

[3] Brickman, L., Fillmore, P.A.: The invariant subspace lattice of a linear transformation. Can. J. Math. **19**, 810–822 (1967)

[4] Brakensiek, J., Guruswami, V.: Promise constraint satisfaction structure theory and a symmetric Boolean dichotomy. In: Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'18). pp. 1782–1801. SIAM, Philadelphia (2018)

[5] Bulín, J., Krokhin, A., Opršal, J.: Algebraic approach to promise constraint satisfaction. In: Proceedings of the Annual ACM Symposium on Theory of Computing (STOC '19). pp. 602–613. ACM, New York (2019)

[6] Fripertinger, H.: The number of invariant subspaces under a linear operator on finite vector spaces. Adv. Math. Commun. **5**(2), 407–416 (2011)

[7] Harnau, W.: Ein verallgemeinerter Relationenbegriff für die Algebra der mehrwertigen Logik. I. Grundlagen Rostock. Math. Kolloq. **28**, 5–17 (1985). (German)

[8] Kreinecker, S.: Closed function sets on groups of prime order. J Multiple-Val Logic Soft Comput **33**(1–2), 51–74 (2019)

[9] Krokhin, A., Bulatov, A.A., Jeavons, P.: The complexity of constraint satisfaction: an algebraic approach. In: Structural theory of automata, semigroups, and universal algebra. NATO Sci. Ser. II Math. Phys. Chem., vol. 207, pp. 181–213. Springer, Dordrecht (2005)

[10] Lehtonen, E.: Closed classes of functions, generalized constraints, and clusters. Algebra Universalis **63**(2–3), 203–234 (2010)

[11] Pippenger, N.: Galois theory for minors of finite functions. Discrete Math. **254**, 405–419 (2002)

[12] Pöschel, R., Kalužnin, L.A.: Funktionen- und Relationenalgebren. Mathematische Monographien[Mathematical Monographs], vol. 15. VEB Deutscher Verlag der Wissenschaften, Berlin (1979)

[13] Post, E.L.: The two-valued iterative systems of mathematical logic. Ann. of Math. Stud., vol. 5. Princeton University Press, Princeton (1941)

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

[15] Szendrei, Á.: Clones in universal algebra. In: Séminaire de Mathématiques Supérieures. Seminar on Higher Mathematics, vol. 99. Presses de l'Université de Montréal, Montréal (1986)

Stefano Fioravanti
Institut für Algebra
Johannes Kepler Universität Linz
4040 Linz
Austria
e-mail: stefano.fioravanti66@gmail.com

Received: 25 October 2019.
Accepted: 2 September 2020.