CLOSED SETS OF FINITARY FUNCTIONS BETWEEN FINITE FIELDS OF COPRIME ORDER.

Stefano Fioravanti
September 2019, YRAC2019
Institute for Algebra
Austrian Science Fund FWF P29931

JOHANNES KEPLER UNIVERSITY LINZ

$(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids

Definition

Let p and q be powers of prime numbers. A $(\mathbb{F}_p, \mathbb{F}_q)$**-linear closed clonoid** is a non-empty subset C of $\bigcup_{n \in \mathbb{N}} \mathbb{F}_p^{\mathbb{F}_q^n}$ such that:

(1) if $f, g \in C^{[n]}$ then:

$$f +_p g \in C^{[n]};$$

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

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

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] J. Bulín, A. Krokhin, and J. Opršal, Algebraic approach to promise constraint satisfaction, arXiv:1811.00970, 2018.

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

$(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids

Proposition

The intersection of $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids is again a $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoid.

Definition

Let K be subset of n-ary function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $\mathcal{A}$ the set of all the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids. We define the **$(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoid generated by K** as:

$$C^{(p,q)}(K) = \bigcap_{\mathcal{C} \in \mathcal{B}} \mathcal{C}$$

where $\mathcal{B} = \{\mathcal{C} | \mathcal{C} \in \mathcal{A}, K \subseteq \mathcal{C}\}$.

Definition

Let f be an n-ary function from a group **G**$_1$ to a group **G**$_2$. We say that f is 0**-preserving** if:

$$f(0_{G_1}, ..., 0_{G_1}) = 0_{G_2}.$$

Definition

Let f be an n-ary function from a group **G**$_1$ to a group **G**$_2$. We say that f is 0**-preserving** if:

$$f(0_{G_1}, ..., 0_{G_1}) = 0_{G_2}.$$

Remark

Let p and q be prime numbers. The 0-preserving functions from $\mathbb{F}_q$ to $\mathbb{F}_p$ form a $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoid.

Other examples

(1) The constant functions.

Other examples

(1) The constant functions.

(2) All the functions.

Other examples

(1) The constant functions.

(2) All the functions.

Definition

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 **w** $\in \mathbb{F}_q^n$ there exists $k \in \mathbb{F}_p$ such that for every $\lambda \in \mathbb{F}_q - \{0\}$:

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

Other examples

(1) The constant functions.

(2) All the functions.

Definition

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 $\mathbf{w} \in \mathbb{F}_q^n$ there exists $k \in \mathbb{F}_p$ such that for every $\lambda \in \mathbb{F}_q - \{0\}$:

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

(3) The star functions (functions constant on rays from the origin, but not in the origin).

A characterization

Theorem (SF)

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

A characterization

Theorem (SF)

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

Corollary

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

Example

Matrix representation of a function $f : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$

$$f(i,j) = a_{ij} \text{ where } (a_{ij}) \in \mathbb{Z}_{11}^{5\times 5}$$

Example

Matrix representation of a function $f : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$

$$f(i,j) = a_{ij} \text{ where } (a_{ij}) \in \mathbb{Z}_{11}^{5\times 5}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & a_4 \\ 0 & 0 & 0 & a_3 & 0 \\ 0 & 0 & a_2 & 0 & 0 \\ 0 & a_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Example

Matrix representation of a function $f : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$

$$f(i,j) = a_{ij} \text{ where } (a_{ij}) \in \mathbb{Z}_{11}^{5\times 5}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & a_4 \\ 0 & 0 & 0 & a_3 & 0 \\ 0 & 0 & a_2 & 0 & 0 \\ 0 & a_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The function $f_1 : \mathbb{Z}_5 \mapsto \mathbb{Z}_{11}$ defined as $f_1(0) = 0$, $f_1(i) = a_i$ for $i = 1, \ldots, 4$ is in $C(\{f\})$.

Example

Matrix representation of a function $f : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$

$$f(i,j) = a_{ij} \text{ where } (a_{ij}) \in \mathbb{Z}_{11}^{5\times 5}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & a_4 \\ 0 & 0 & 0 & a_3 & 0 \\ 0 & 0 & a_2 & 0 & 0 \\ 0 & a_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The function $f_1 : \mathbb{Z}_5 \mapsto \mathbb{Z}_{11}$ defined as $f_1(0) = 0$, $f_1(i) = a_i$ for $i = 1, \ldots, 4$ is in $C(\{f\})$.

How to generate f from f_1 in a $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoid?

Example

Let us define the function $s : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$:

$$s(x, y) = f_1(y)$$

$$\begin{pmatrix} a_4 & a_4 & a_4 & a_4 & a_4 \\ a_3 & a_3 & a_3 & a_3 & a_3 \\ a_2 & a_2 & a_2 & a_2 & a_2 \\ a_1 & a_1 & a_1 & a_1 & a_1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Example

Let us define the function $s : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$:

$$s(x, y) = f_1(y) + f_1(y - x)$$

$$\begin{pmatrix} 2a_4 & a_3 + a_4 & a_2 + a_4 & a_1 + a_4 & a_4 \\ 2a_3 & a_2 + a_3 & a_1 + a_3 & a_3 & a_3 + a_4 \\ 2a_2 & a_1 + a_2 & a_2 & a_2 + a_4 & a_2 + a_3 \\ 2a_1 & a_1 & a_1 + a_4 & a_1 + a_3 & a_1 + a_2 \\ 0 & a_4 & a_3 & a_2 & a_1 \end{pmatrix}$$

Example

Let us define the function $s : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$:

$$s(x, y) = f_1(y) + f_1(y - x) + f_1(y - 2x)$$

$$\begin{pmatrix} 3a_4 & a_2 + a_3 + a_4 & a_2 + a_4 & a_1 + a_3 + a_4 & a_1 + a_4 \\ 3a_3 & a_1 + a_2 + a_3 & a_1 + a_3 + a_4 & a_2 + a_3 & a_3 + a_4 \\ 3a_2 & a_1 + a_2 & a_2 + a_3 & a_1 + a_2 + a_4 & a_2 + a_3 + a_4 \\ 3a_1 & a_1 + a_4 & a_1 + a_2 + a_4 & a_1 + a_3 & a_1 + a_2 + a_3 \\ 0 & a_3 + a_4 & a_1 + a_3 & a_2 + a_4 & a_1 + a_2 \end{pmatrix}$$

Example

Let us define the function $s : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$:

$$s(x, y) = f_1(y) + f_1(y - x) + f_1(y - 2x) + f_1(y - 3x) + f_1(y - 4x)$$

$$\begin{pmatrix} 5a_4 & \lambda & \lambda & \lambda & \lambda \\ 5a_3 & \lambda & \lambda & \lambda & \lambda \\ 5a_2 & \lambda & \lambda & \lambda & \lambda \\ 5a_1 & \lambda & \lambda & \lambda & \lambda \\ 0 & \lambda & \lambda & \lambda & \lambda \end{pmatrix}$$

where $\lambda = a_1 + a_2 + a_3 + a_4$

Example

Let us define the function $s : \mathbb{Z}_5^2 \mapsto \mathbb{Z}_{11}$:

$$s(x,y) = f_1(y) + f_1(y-x) + f_1(y-2x) + f_1(y-3x) + f_1(y-4x) - \sum_{k=1}^{q-1} f_1(kx)$$

$$\begin{pmatrix} 5a_4 & 0 & 0 & 0 & 0 \\ 5a_3 & 0 & 0 & 0 & 0 \\ 5a_2 & 0 & 0 & 0 & 0 \\ 5a_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Example

Let $n \in \mathbb{N}$ be s.t $n * 5 \equiv_{11} 1$. Hence $n * s$ is the function:

$$\begin{pmatrix} a_4 & 0 & 0 & 0 & 0 \\ a_3 & 0 & 0 & 0 & 0 \\ a_2 & 0 & 0 & 0 & 0 \\ a_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Example

for all $x, y \in \mathbb{Z}_5$:

$$f(x, y) = n * s(x - y, y)$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & a_4 \\ 0 & 0 & 0 & a_3 & 0 \\ 0 & 0 & a_2 & 0 & 0 \\ 0 & a_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Definition

Let $\mathbb{F}_q$ and $\mathbb{F}_p$ be finite fields and let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a unary function. Let α be a generator of the multiplicative subgroup $\mathbb{F}_q^\times$ of $\mathbb{F}_q$. We define the α-vector encoding of f as the vector $\mathbf{v} \in \mathbb{F}_p^q$ such that:

$$
\begin{aligned}
v_{i+1} &= f(\alpha^i) \quad \text{for} \quad 0 \leq i \leq q-2, \\
v_0 &= f(0).
\end{aligned}
$$

How to describe the unary functions

Proposition

Let C be a $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoid, and let α be a generator of the multiplicative subgroup $\mathbb{F}_q^{\times}$ of $\mathbb{F}_q$. Then the set S of all the α-vector encodings of unary functions in C is a subspace of $\mathbb{F}_p^q$ and it satisfies:

$$(x_0, x_k, x_{k+1}, \ldots, x_{q-1}, x_1, \ldots, x_{k-1}) \in S \quad (1)$$

and

$$(x_0, \ldots, x_0) \in S \quad (2)$$

for all $(x_0, \ldots, x_{q-1}) \in S$ and $k \in \{1, \ldots, q-1\}$.

A characterization

We denote by $A(p,q)$ and $C(p,q)$ respectively the linear transformations of $\mathbb{F}_p^q$ defined as:

$$A(p,q)((v_0,\ldots,v_{q-1})) = (v_0, v_k, v_{k+1},\ldots,x_{q-1},v_1,\ldots,v_{k-1})$$
$$C(p,q)((v_0,\ldots,v_{q-1})) = (v_0,\ldots,v_0)$$

A characterization

Definition

An **invariant subspace** of a linear operator T on some vector space V is a subspace W of V that is preserved by T; that is, $T(W) \subseteq W$.

A characterization

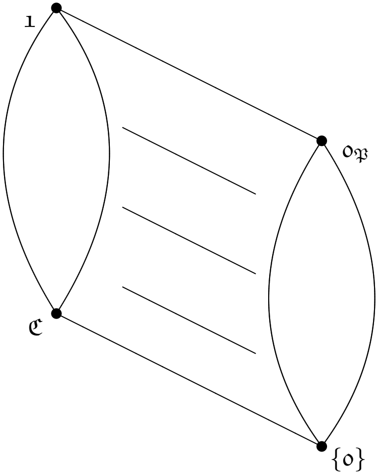
Definition

An **invariant subspace** of a linear operator T on some vector space V is a subspace W of V that is preserved by T; that is, $T(W) \subseteq W$.

Theorem (SF)

Let p and q be powers of distinct prime numbers. Then the lattice of all $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids $\mathbf{L}(p,q)$ is isomorphic to the lattice $\mathbf{L}(A(p,q), C(p,q))$ of all the $(A(p,q), C(p,q))$-invariant subspaces of $\mathbb{F}_p^q$.

Lattice of the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids



Lattice of the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids

Let us denote by $\mathbf{2}$ the two-elements chain and, in general, by $\mathbf{C}_k$ the chain with k elements.

Lattice of the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids

Let us denote by $\mathbf{2}$ the two-elements chain and, in general, by $\mathbf{C}_k$ the chain with k elements.

Theorem (SF)

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 $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids is $2\prod_{i=1}^n (k_i + 1)$ and the lattice of all the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids, $\mathbf{L}(p, q)$, is isomorphic to

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

Lattice of the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids

Corollary

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

Lattice of the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids

Corollary

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

Corollary

Every 0-preserving $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoid is principal (generated by a unary functions).

Lattice of the $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoids

Corollary

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

Corollary

Every 0-preserving $(\mathbb{F}_p, \mathbb{F}_q)$-linear closed clonoid is principal (generated by a unary functions).

THANK YOU!!!!