Algebraic Constructions of Permutation Codes

FYP Presentation

Yeung Kar Wing

Supervisor: Prof Xing Chaoping

NANYANG TECHNOLOGICAL UNIVERSITY

24 April 2018

Outline

1. Introduction
   - Motivation
   - Groups and fields
   - Coding theory
   - Elementary results
2. Review of known constructions
   - Mutually orthogonal latin squares
   - $A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$
3. New constructions
   - Ring of integers modulo n
   - $AGL_n(\mathbb{F}_q)$ and $PGL_n(\mathbb{F}_q)$
4. Conclusion

Outline

1. Introduction
   - Motivation
   - Groups and fields
   - Coding theory
   - Elementary results
2. Review of known constructions
   - Mutually orthogonal latin squares
   - $A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$
3. New constructions
   - Ring of integers modulo n
   - $AGL_n(\mathbb{F}_q)$ and $PGL_n(\mathbb{F}_q)$
4. Conclusion

Motivation

In general, the main problems of coding theory are

- Determining the maximum size of the code given the distance and the length
- Constructing codes with maximum error-correction and small redundancy
- Constructing codes with efficient encoding and decoding algorithms

Motivation

In general, the main problems of coding theory are

- Determining the maximum size of the code given the distance and the length
- Constructing codes with maximum error-correction and small redundancy
- Constructing codes with efficient encoding and decoding algorithms

Why permutation codes?

- Powerline communications
- Flash memories

Outline

1. Introduction
   - Motivation
   - Groups and fields
   - Coding theory
   - Elementary results
2. Review of known constructions
   - Mutually orthogonal latin squares
   - $A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$
3. New constructions
   - Ring of integers modulo n
   - $AGL_n(\mathbb{F}_q)$ and $PGL_n(\mathbb{F}_q)$
4. Conclusion

Groups and fields

Definition 1.1.2.

Let $q = p^k$, where p is prime. The **affine general linear group** of degree n over $\mathbb{F}_q$ is the group of affine linear transformations, which are maps $\gamma_{A,b} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\gamma_{A,b}(u) = Au + b$, for $A \in GL_n(\mathbb{F}_q)$, $b \in \mathbb{F}_q^n$.

We denote it as $AGL_n(\mathbb{F}_q)$.

Groups and fields

Definition 1.1.2.

Let $q = p^k$, where p is prime. The **affine general linear group** of degree n over $\mathbb{F}_q$ is the group of affine linear transformations, which are maps $\gamma_{A,b} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\gamma_{A,b}(u) = Au + b$, for $A \in GL_n(\mathbb{F}_q)$, $b \in \mathbb{F}_q^n$.

We denote it as $AGL_n(\mathbb{F}_q)$.

The affine general linear group can also be defined as the semidirect product $\mathbb{F}_q^n \rtimes GL_n(\mathbb{F}_q)$, with composition as the group operation and $(C, d) \circ (A, b) = (CA, Cb + d)$.

Groups and fields

Definition 1.1.3.

Let $q = p^k$, where p is prime. The **projective general linear group** of degree n over $\mathbb{F}_q$ is defined to be the quotient of the general linear group by its center, the scalar matrices. In other words, $PGL_n(\mathbb{F}_q) = GL_n(\mathbb{F}_q)/Z(GL_n(\mathbb{F}_q))$, where $Z(GL_n(\mathbb{F}_q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\}$.

Groups and fields

Definition 1.1.3.

Let $q = p^k$, where p is prime. The **projective general linear group** of degree n over $\mathbb{F}_q$ is defined to be the quotient of the general linear group by its center, the scalar matrices. In other words, $PGL_n(\mathbb{F}_q) = GL_n(\mathbb{F}_q)/Z(GL_n(\mathbb{F}_q))$, where $Z(GL_n(\mathbb{F}_q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\}$.

While the affine general linear group acts on $\mathbb{F}_q^n$, the projective general linear group acts on the projective space $\mathbb{P}_q^{n-1}$.

Groups and fields

Definition 1.1.4.

Let $q = p^k$, where p is prime. The **projective space** of dimension $n-1$ over $\mathbb{F}_q$ is defined as $\mathbb{P}_q^{n-1} = (\mathbb{F}_q^n \setminus \{0\})/\sim$, where $\sim$ is defined by $(x_0, \cdots, x_{n-1}) \sim (y_0, \cdots, y_{n-1})$ if there exists $\lambda \in \mathbb{F}_q^*$ such that $(x_0, \cdots, x_{n-1}) = \lambda(y_0, \cdots, y_{n-1})$.

Groups and fields

Definition 1.1.4.

Let $q = p^k$, where p is prime. The **projective space** of dimension $n-1$ over $\mathbb{F}_q$ is defined as $\mathbb{P}_q^{n-1} = (\mathbb{F}_q^n \setminus \{0\})/\sim$, where $\sim$ is defined by $(x_0, \cdots, x_{n-1}) \sim (y_0, \cdots, y_{n-1})$ if there exists $\lambda \in \mathbb{F}_q^*$ such that $(x_0, \cdots, x_{n-1}) = \lambda(y_0, \cdots, y_{n-1})$.

Here, we can define the action of $PGL_n(\mathbb{F}_q)$ on $\mathbb{P}_q^{n-1}$ to be

$$A : \mathbb{P}_q^{n-1} \to \mathbb{P}_q^{n-1}$$
$$u \mapsto Au$$

where $A \in PGL_n(\mathbb{F}_q)$.

Groups and fields

Definition 1.1.5.

Let F be a field with characteristic p. The **Frobenius automorphism** on F is the map $\phi : F \to F$ such that x is mapped to x^p for all $x \in F$.

Definition 1.1.6.

Let $q = p^k$, where p is prime. The **Galois group of** $\mathbb{F}_q/\mathbb{F}_p$ is a cyclic group of order k generated by the Frobenius automorphism $\phi(x) = x^p$, and it is denoted by $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Groups and fields

Definition 1.1.7.

Let $q = p^k$, where p is prime. The **affine semilinear group** of degree n over $\mathbb{F}_q$ is the group of affine semilinear transformations, which are maps $\gamma_{A,\sigma,b} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\gamma_{A,\sigma,b}(u) = A\sigma(u) + b$, for $A \in GL_n(\mathbb{F}_q), \sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $b \in \mathbb{F}_q^n$.

We denote this group as $A\Gamma L_n(\mathbb{F}_q)$.

Groups and fields

Definition 1.1.7.

Let $q = p^k$, where p is prime. The **affine semilinear group** of degree n over $\mathbb{F}_q$ is the group of affine semilinear transformations, which are maps $\gamma_{A,\sigma,b} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\gamma_{A,\sigma,b}(u) = A\sigma(u) + b$, for $A \in GL_n(\mathbb{F}_q), \sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $b \in \mathbb{F}_q^n$.

We denote this group as $A\Gamma L_n(\mathbb{F}_q)$.

In particular, we have

$$A\Gamma L_1(\mathbb{F}_q) = \{ax^{p^i} + b \mid a, b \in \mathbb{F}_q, a \neq 0, 0 \leq i < n\}$$

Groups and fields

Definition 1.1.8.

Let $q = p^k$, where p is prime. The **projective semilinear group** of degree n over $\mathbb{F}_q$ is defined to be the semidirect product of the projective general linear group by the Galois group.

In other words, $P\Gamma L_n(\mathbb{F}_q) = PGL_n(\mathbb{F}_q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Groups and fields

Definition 1.1.8.

Let $q = p^k$, where p is prime. The **projective semilinear group** of degree n over $\mathbb{F}_q$ is defined to be the semidirect product of the projective general linear group by the Galois group.

In other words, $P\Gamma L_n(\mathbb{F}_q) = PGL_n(\mathbb{F}_q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Here, we have the natural action of $P\Gamma L_n(\mathbb{F}_q)$ on $\mathbb{P}_q^{n-1}$ to be

$$\begin{aligned}(A,\sigma) : \mathbb{P}_q^{n-1} &\to \mathbb{P}_q^{n-1} \\ u &\mapsto A\sigma(u)\end{aligned}$$

where $A \in P\Gamma L_n(\mathbb{F}_q), \sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Groups and fields

We will use a different (but equivalent) definition for the special case where the projective semilinear group has degree 2, and it is

$$P\Gamma L_2(\mathbb{F}_q) = \left\{ \frac{ax^{p^i}+b}{cx^{p^i}+d} \;\middle|\; a,b,c,d \in \mathbb{F}_q, ad \neq bc, 0 \leq i < n \right\}$$

.

This acts on the projective space of dimension 1, $\mathbb{P}^1_q$. However, instead of thinking it as "equivalent classes in $\mathbb{F}_q^2 - \{0\}$" as we have previously defined, we can think of it as "the affine space $\mathbb{F}_q$ with its points at infinity". This is the set $\mathbb{F}_q \cup \{\infty\}$.

Outline

Coding theory

Definition 1.2.5.

A **permutation code** C is a subset of S_n, and each element in C is called a **codeword**. The **length** of each codeword is n. If for every two codewords $u, v \in C$, the distance between u and v is at least d, we say that d is the **distance** of C. The **size** of the code C is usually denoted as M, and it is common to write the code C as a (n, M, d)-code.

Definition 1.2.6.

Given the parameters n and d, we denote the **maximum size** of such a code as $M(n, d)$.

Coding theory

Definition 1.2.7.

The **Hamming distance** between two codewords $\sigma, \tau \in S_n$ is defined as $d_H(\sigma, \tau) = |\{i \in \{1, \dots, n\} : \sigma(i) \neq \tau(i)\}|$.

Coding theory

Definition 1.2.7.

The **Hamming distance** between two codewords $\sigma, \tau \in S_n$ is defined as $d_H(\sigma, \tau) = |\{i \in \{1, \ldots, n\} : \sigma(i) \neq \tau(i)\}|$.

Note that we have

1. $d_H(\sigma, \tau) = d_H(e, \sigma\tau^{-1})$
2. $d_H(\sigma, \tau) = d_H(\gamma\sigma, \gamma\tau)$, for $\gamma \in S_n$

Coding theory

Definition 1.2.9.

Let C be an (n, M, d)-code. Then a **permutation array** of size $M \times n$ is an array whose rows are the image of σ on $(1, 2, \ldots, n)$, for all σ in C. We denote the permutation array as $PA(n, d)$, and we say that it has size M.

Coding theory

Definition 1.2.9.

Let C be an (n, M, d)-code. Then a **permutation array** of size $M \times n$ is an array whose rows are the image of σ on $(1, 2, \ldots, n)$, for all σ in C. We denote the permutation array as $PA(n, d)$, and we say that it has size M.

Example 1.2.10.

The Klein-4 subgroup $G = \{(), (12)(34), (13)(24), (14)(23)\}$ of S_4 is a $(4, 4, 4)$-code. The permutation array for this code is

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

and we call it a $PA(4, 4)$ of size 4.

Outline

1. Introduction
   - Motivation
   - Groups and fields
   - Coding theory
   - Elementary results
2. Review of known constructions
   - Mutually orthogonal latin squares
   - $A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$
3. New constructions
   - Ring of integers modulo n
   - $AGL_n(\mathbb{F}_q)$ and $PGL_n(\mathbb{F}_q)$
4. Conclusion

Elementary results

Proposition 1.3.1.

Let $M(n, d)$ be the maximum size of a permutation code with length n and Hamming distance d. Then the following statements are true:

(i) $M(n, 2) = n!$

(ii) $M(n, 3) = \frac{n!}{2}$

(iii) $M(n, n) = n$

(iv) $M(n, d) \geq M(n-1, d), M(n, d+1)$

(v) $M(n, d) \leq nM(n-1, d)$

(vi) $M(n, d) \leq \frac{n!}{(d-1)!}$

Elementary results

Here, $D(n,k)$ is the set of all permutations in S_n which are distance k from the identity.

Proposition 1.3.4 (GV bound).

$$M(n,d) \geq \frac{n!}{V(n,d-1)} = \frac{n!}{\sum_{k=0}^{d-1} |D(n,k)|}$$

Elementary results

Here, $D(n,k)$ is the set of all permutations in S_n which are distance k from the identity.

Proposition 1.3.4 (GV bound).

$$M(n,d) \geq \frac{n!}{V(n,d-1)} = \frac{n!}{\sum_{k=0}^{d-1} |D(n,k)|}$$

Proposition 1.3.5 (Sphere-packing upper bound).

$$M(n,d) \leq \frac{n!}{\sum_{k=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} |D(n,k)|}$$

Elementary results

Definition 1.3.6.

A permutation group $G \leq S_n$ is **transitive** if for every $x, y \in \{1, \ldots, n\}$, there exists a $\sigma \in G$ such that $\sigma(x) = y$.

In other words, if G is transitive, there will always be an element in G that will take us from x to y for any x, y in the set G acts on.

Elementary results

Definition 1.3.6.

A permutation group $G \leq S_n$ is **transitive** if for every $x, y \in \{1, \ldots, n\}$, there exists a $\sigma \in G$ such that $\sigma(x) = y$.

In other words, if G is transitive, there will always be an element in G that will take us from x to y for any x, y in the set G acts on.

Definition 1.3.7.

Let x, y be k-tuples consisting of non-repeating elements from $\{1, \ldots, n\}$, that is $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$, where $x_i, y_i \in \{1, \ldots, n\}$ for all $1 \leq i \leq k$ and $x_i \neq x_j, y_i \neq y_j$ for $i \neq j$. A permutation group $G \leq S_n$ is **sharply** k**-transitive** if for every such x, y of size k, there exists a unique $\sigma \in G$ such that $\sigma(x) = y$.

Elementary results

Proposition 1.3.9.

If G is a sharply k-transitive group acting on a set of size n, we then have $M(n, n-k+1) = \frac{n!}{(n-k)!}$.

Elementary results

Proposition 1.3.9.

If G is a sharply k-transitive group acting on a set of size n, we then have $M(n, n-k+1) = \frac{n!}{(n-k)!}$.

Sketch of proof.

1. From uniqueness, $g(1, \ldots, k) \neq h(1, \ldots, k)$
2. $g(1, \ldots, n)$ and $h(1, \ldots, n)$ has distance at least $n - k + 1$
3. $M(n, n-k+1) \geq |G| = \frac{n!}{(n-k)!}$
4. $M(n, n-k+1) \leq \frac{n!}{(n-k)!}$ from Proposition 1.3.1 (vi)

□

Elementary results

Proposition 1.3.9.

If G is a sharply k-transitive group acting on a set of size n, we then have $M(n, n-k+1) = \frac{n!}{(n-k)!}$.

Sketch of proof.

1. From uniqueness, $g(1, \ldots, k) \neq h(1, \ldots, k)$
2. $g(1, \ldots, n)$ and $h(1, \ldots, n)$ has distance at least $n - k + 1$
3. $M(n, n-k+1) \geq |G| = \frac{n!}{(n-k)!}$
4. $M(n, n-k+1) \leq \frac{n!}{(n-k)!}$ from Proposition 1.3.1 (vi)

$\square$

Example 1.3.10.

Consider the Mathieu groups M_{11} and M_{12}. It is well-known that they are sharply 4- and 5-transitive respectively. This gives us $M(11, 8) = 11 \cdot 10 \cdot 9 \cdot 8$ and $M(12, 8) = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

Elementary results

Definition 1.3.11.

Let q be a prime power. We say that $f \in \mathbb{F}_q[x]$ is a **permutation polynomial** if the function

$$\begin{aligned} f : \mathbb{F}_q &\to \mathbb{F}_q \\ c &\mapsto f(c) \end{aligned}$$

acts as a permutation on $\mathbb{F}_q$.

Elementary results

Definition 1.3.11.

Let q be a prime power. We say that $f \in \mathbb{F}_q[x]$ is a **permutation polynomial** if the function

$$\begin{aligned} f : \mathbb{F}_q &\to \mathbb{F}_q \\ c &\mapsto f(c) \end{aligned}$$

acts as a permutation on $\mathbb{F}_q$.

Let $N_d(q)$ denote the number of permutation polynomials over $\mathbb{F}_q$ of a given degree d, where $1 \le d \le q - 2$. We then have the following result.

Elementary results

Definition 1.3.11.

Let q be a prime power. We say that $f \in \mathbb{F}_q[x]$ is a **permutation polynomial** if the function

$$\begin{aligned} f : \mathbb{F}_q &\to \mathbb{F}_q \\ c &\mapsto f(c) \end{aligned}$$

acts as a permutation on $\mathbb{F}_q$.

Let $N_d(q)$ denote the number of permutation polynomials over $\mathbb{F}_q$ of a given degree d, where $1 \leq d \leq q-2$. We then have the following result.

Proposition 1.3.12.

Let q be a prime power. Then $M(q,d) \geq \sum_{i=1}^{q-d} N_i(q)$.

Outline

Mutually orthogonal latin squares

Colbourn et al. have shown that we can construct permutation codes using mutually orthogonal latin squares, which we will review in the following slides.

Mutually orthogonal latin squares

Colbourn et al. have shown that we can construct permutation codes using mutually orthogonal latin squares, which we will review in the following slides.

Definition 2.1.1.

Let S be a set of n symbols. A **latin square** of order n is an $n \times n$ matrix such that each symbol of S occurs exactly once in each row and each column.

Mutually orthogonal latin squares

Colbourn et al. have shown that we can construct permutation codes using mutually orthogonal latin squares, which we will review in the following slides.

Definition 2.1.1.

Let S be a set of n symbols. A **latin square** of order n is an $n \times n$ matrix such that each symbol of S occurs exactly once in each row and each column.

Definition 2.1.2.

Let L_1 and L_2 be latin squares of the same order on the sets S_1 and S_2 respectively. Then L_1 and L_2 are said to be **orthogonal** if each tuple (i, j) where $i \in S_1$, $j \in S_2$ occurs exactly once when we overlap L_1 and L_2.

Mutually orthogonal latin squares

Definition 2.1.3.

A collection of k $n \times n$ latin squares is said to be **mutually orthogonal** if every pair of latin squares in the collection is orthogonal, and we denote this collection as MOLS(n).

Mutually orthogonal latin squares

Definition 2.1.3.

A collection of k $n \times n$ latin squares is said to be **mutually orthogonal** if every pair of latin squares in the collection is orthogonal, and we denote this collection as MOLS(n).

Example 2.1.4.

This is a set of 2 mutually orthogonal latin squares of order 3. If we overlap these 2 latin squares, we get all possible tuples (i, j) where $i, j \in \{1, 2, 3\}$.

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

$\rightarrow$

(1,1)	(2,2)	(3,3)
(2,3)	(3,1)	(1,2)
(3,2)	(1,3)	(2,1)

Mutually orthogonal latin squares

Theorem 2.1.7.

If there exists s mutually orthogonal latin squares of order n, then there exists a $(n, n-1)$-code of size sn.

Mutually orthogonal latin squares

Theorem 2.1.7.

If there exists s mutually orthogonal latin squares of order n, then there exists a $(n, n-1)$-code of size sn.

Corollary 2.1.8.

For n prime power, $M(n, n-1) = n(n-1)$.

Mutually orthogonal latin squares

Theorem 2.1.7.

If there exists s mutually orthogonal latin squares of order n, then there exists a $(n, n-1)$-code of size sn.

Corollary 2.1.8.

For n prime power, $M(n, n-1) = n(n-1)$.

Proof.

Since n is a prime power, there exists a set of $n-1$ MOLS of order n. We can then apply Theorem 2.1.7 to get $M(n, n-1) \geq n(n-1)$.
Furthermore, from Proposition 1.3.1(vi), we also obtain $M(n, n-1) \leq n(n-1)$. The result then follows. $\square$

Outline

$A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$

Bereg et al. have shown that we are able to construct permutation codes via the affine and projective semilinear groups.

$A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$

Bereg et al. have shown that we are able to construct permutation codes via the affine and projective semilinear groups.

Theorem 2.2.1.

There exists a $(n, kn(n-1), n-p^{k^*})$-code arising from $A\Gamma L_1(\mathbb{F}_n)$, where k^* is the largest proper factor of k, and $n = p^k$.

$A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$

Bereg et al. have shown that we are able to construct permutation codes via the affine and projective semilinear groups.

Theorem 2.2.1.

There exists a $(n, kn(n-1), n - p^{k^*})$-code arising from $A\Gamma L_1(\mathbb{F}_n)$, where k^* is the largest proper factor of k, and $n = p^k$.

We know that

- $|A\Gamma L_1(\mathbb{F}_n)| = kn(n-1)$ and
- $A\Gamma L_1(\mathbb{F}_n)$ acts on $\mathbb{F}_n$ which is of size n.

To show that the distance is $n - p^{k^*}$, we make use of the fact that $AGL_1(\mathbb{F}_n)$ is normal in $A\Gamma L_1(\mathbb{F}_n)$, and find the distance of the cosets.

$A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$

Theorem 2.2.2.

There exists a $(n+1, kn(n+1)(n-1), n-p^{k^*})$-code arising from $P\Gamma L_2(\mathbb{F}_n)$, where k^* is the largest proper factor of k, and $n = p^k$.

$A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$

Theorem 2.2.2.

There exists a $(n+1, kn(n+1)(n-1), n-p^{k^*})$-code arising from $P\Gamma L_2(\mathbb{F}_n)$, where k^* is the largest proper factor of k, and $n = p^k$.

We know that

- $|\mathbb{F}_n \cup \{\infty\}| = n+1$ and
- $|P\Gamma L_2(\mathbb{F}_n)| = kn(n+1)(n-1)$.

We use a similar technique to show that the distance is $n - p^{k^*}$.

$A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$

Corollary 2.2.8.

For $n = 2^k$, k prime, we have $M(n, n-2) \geq kn(n-1)$.

Corollary 2.2.9.

For $n = 2^k$, k prime, we have $M(n+1, n-2) \geq kn(n+1)(n-1)$.

Outline

Ring of integers modulo n

Definition 3.1.1.

Let G be an abelian group, with the group operation denoted as addition. For A, $B \subseteq G$, we define the **sumset** of A and B to be $A + B := \{a + b \mid a \in A,\ b \in B\}$.

Ring of integers modulo n

Definition 3.1.1.

Let G be an abelian group, with the group operation denoted as addition. For $A,\ B \subseteq G$, we define the **sumset** of A and B to be $A + B := \{a + b \mid a \in A,\ b \in B\}$.

Remark

From this definition, we have $A - A = \{a - b \mid a,\ b \in A\} = A + (-A)$.

Remark

It is clear that $|A + B| \geq max\{|A|,\ |B|\}$.

n is a prime power

Suppose $n = p^r$, where p is prime and $r \geq 1$ is an integer.

Lemma 3.1.1.

If $I \subseteq \mathbb{Z}_n$ and $|I| \geq n - \phi(n) + 1$, then $\exists\, \alpha, \beta \in I, \alpha \neq \beta$ such that $\alpha - \beta \in \mathbb{Z}_n^*$, where $\phi(n)$ is the Euler totient function.

n is a prime power

Suppose $n = p^r$, where p is prime and $r \geq 1$ is an integer.

Lemma 3.1.1.

If $I \subseteq \mathbb{Z}_n$ and $|I| \geq n - \phi(n) + 1$, then $\exists\, \alpha, \beta \in I, \alpha \neq \beta$ such that $\alpha - \beta \in \mathbb{Z}_n^*$, where $\phi(n)$ is the Euler totient function.

Theorem 3.1.2.

For a prime power $n \geq 2$, there exists a permutation code $(n,\ \phi(n) \cdot n,\ \phi(n))$.

n is a prime power

Suppose $n = p^r$, where p is prime and $r \geq 1$ is an integer.

Lemma 3.1.1.

If $I \subseteq \mathbb{Z}_n$ and $|I| \geq n - \phi(n) + 1$, then $\exists\, \alpha, \beta \in I, \alpha \neq \beta$ such that $\alpha - \beta \in \mathbb{Z}_n^*$, where $\phi(n)$ is the Euler totient function.

Theorem 3.1.2.

For a prime power $n \geq 2$, there exists a permutation code $(n,\ \phi(n) \cdot n,\ \phi(n))$.

We have the group action of $\mathcal{A} = \{(a, b) \mid a \in \mathbb{Z}_n^*,\ b \in \mathbb{Z}_n\}$ on $\mathbb{Z}_n$ to be $\sigma\alpha = a\alpha + b$, where $\alpha \in \mathbb{Z}_n$, $\sigma \in \mathcal{A}$. We then make use of Lemma 3.1.1 to show that $d(\sigma_1, \sigma_2) \geq \phi(n)$ for all $\sigma_1, \sigma_2 \in \mathcal{A}$.

n is a prime power

Note that for n that is prime, $(n, \phi(n) \cdot n, \phi(n))$ is an optimal code, that is the maximal size has been achieved for the given length and distance.

n is a prime power

Note that for n that is prime, $(n, \phi(n) \cdot n, \phi(n))$ is an optimal code, that is the maximal size has been achieved for the given length and distance.

Recall that from the construction via MOLS(n) we obtained Corollary 2.2.9, which said that $M(n, n-1) = n(n-1)$ for n a prime power. Hence this construction gives the same result, for n that is prime.

n is not a prime power

Lemma 3.1.3.

If $(n - \phi(n)) \mid n$, then n is a prime power.

n is not a prime power

Lemma 3.1.3.
If $(n - \phi(n)) \mid n$, then n is a prime power.

Lemma 3.1.4.
If $n \geq 6$ is not a prime power, then for any $I \subseteq \mathbb{Z}_n$ with $|I| \geq n - \phi(n)$, we have $|I - I| \geq n - \phi(n) + 1$.

n is not a prime power

Lemma 3.1.3.

If $(n - \phi(n)) \mid n$, then n is a prime power.

Lemma 3.1.4.

If $n \geq 6$ is not a prime power, then for any $I \subseteq \mathbb{Z}_n$ with $|I| \geq n - \phi(n)$, we have $|I - I| \geq n - \phi(n) + 1$.

Theorem 3.1.5.

If $n \geq 6$ is not a prime power, there exists a $(n,\ \phi(n) \cdot n,\ \phi(n) + 1)$ permutation code.

Outline

1. Introduction
   - Motivation
   - Groups and fields
   - Coding theory
   - Elementary results
2. Review of known constructions
   - Mutually orthogonal latin squares
   - $A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$
3. New constructions
   - Ring of integers modulo n
   - $AGL_n(\mathbb{F}_q)$ and $PGL_n(\mathbb{F}_q)$
4. Conclusion

$AGL_n(\mathbb{F}_q)$ and $PGL_n(\mathbb{F}_q)$

We can also construct permutation codes using the affine and projective general linear group. That can be achieved with the help of the following lemma.

Lemma 3.2.1.

Suppose a group G acts on a finite set Ω, where $|\Omega| = n$. Let $\Omega^g := \{\omega \in \Omega \mid g\omega = \omega\}$. If $|\Omega^g| \leq t$ for all $g \in G, g \neq 1$, then there exists a $(n, |G|, n-t)$-code.

$AGL_n(\mathbb{F}_q)$

Recall that the affine general linear group, $AGL_n(\mathbb{F}_q) = \mathbb{F}_q^n \rtimes GL_n(\mathbb{F}_q)$, acts on $\mathbb{F}_q$ in the following manner:

$$\begin{aligned}(A, b) : \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ u &\mapsto Au + b\end{aligned}$$

where $(A, b) \in AGL_n(\mathbb{F}_q)$.

$AGL_n(\mathbb{F}_q)$

Recall that the affine general linear group, $AGL_n(\mathbb{F}_q) = \mathbb{F}_q^n \rtimes GL_n(\mathbb{F}_q)$, acts on $\mathbb{F}_q$ in the following manner:

$$\begin{aligned}(A, b) : \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ u &\mapsto Au + b\end{aligned}$$

where $(A, b) \in AGL_n(\mathbb{F}_q)$.

Theorem 3.2.1.

Let $n \geq 1$ be an integer and q be a prime power. Then there exists a $\left(q^n, q^n \prod_{i=0}^{n-1}(q^n - q^i), q^n - q^{n-1}\right)$-code.

$PGL_n(\mathbb{F}_q)$

Recall that we have defined the projective general linear group to be $PGL_n(\mathbb{F}_q) = GL_n(\mathbb{F}_q)/Z(GL_n(\mathbb{F}_q))$, where $Z(GL_n(\mathbb{F}_q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\}$. The projective general linear group acts on $\mathbb{P}_q^{n-1}$ in the following manner

$$\begin{aligned} A : \mathbb{P}_q^{n-1} &\to \mathbb{P}_q^{n-1} \\ u &\mapsto Au \end{aligned}$$

where $A \in PGL_n(\mathbb{F}_q)$.

$PGL_n(\mathbb{F}_q)$

Lemma 3.2.2.

Suppose $r = \min\{\text{rank}(\lambda A - I) \mid \lambda \in \mathbb{F}_q^*\} = \text{rank}(\lambda_0 A - I)$ for some λ_0, where $A, I \in GL_n(\mathbb{F}_q)$ and $A \neq kI$, for $k \in \mathbb{F}_q^*$. Then $\forall \lambda \neq \lambda_0$, we have that $\text{rank}(\lambda A - I) \geq n - r$.

$PGL_n(\mathbb{F}_q)$

Lemma 3.2.2.

Suppose $r = \min\{\text{rank}(\lambda A - I) \mid \lambda \in \mathbb{F}_q^*\} = \text{rank}(\lambda_0 A - I)$ for some λ_0, where $A, I \in GL_n(\mathbb{F}_q)$ and $A \neq kI$, for $k \in \mathbb{F}_q^*$. Then $\forall \lambda \neq \lambda_0$, we have that $\text{rank}(\lambda A - I) \geq n - r$.

Theorem 3.2.3.

Let $n \geq 1$ be an integer and q be a prime power. Then there exists a $\left(\frac{q^n-1}{q-1}, \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i), q^{n-1} - q + 2\right)$-code.

Conclusion

From the known constructions, for n prime power, we have these results:

- $M(n, n-1) = n(n-1)$ from MOLS(n),

Conclusion

From the known constructions, for n prime power, we have these results:

- $M(n, n-1) = n(n-1)$ from MOLS(n),
- $M(n, n-p^{k^*}) \geq kn(n-1)$ from $A\Gamma L_1(\mathbb{F}_n)$, and
- $M(n+1, n-p^{k^*}) \geq k(n+1)n(n-1)$ from $P\Gamma L_2(\mathbb{F}_n)$.

Conclusion

From the known constructions, for n prime power, we have these results:

- $M(n, n-1) = n(n-1)$ from $\mathrm{MOLS}(n)$,
- $M(n, n-p^{k^*}) \geq kn(n-1)$ from $A\Gamma L_1(\mathbb{F}_n)$, and
- $M(n+1, n-p^{k^*}) \geq k(n+1)n(n-1)$ from $P\Gamma L_2(\mathbb{F}_n)$.

From the new constructions, we have these results:

- $M(n, \phi(n)) \geq \phi(n) \cdot n$ for n prime power,
- $M(n, \phi(n)+1) \geq \phi(n) \cdot n$ for n not prime power,

Conclusion

From the known constructions, for n prime power, we have these results:

- $M(n, n-1) = n(n-1)$ from MOLS(n),
- $M(n, n-p^{k^*}) \geq kn(n-1)$ from $A\Gamma L_1(\mathbb{F}_n)$, and
- $M(n+1, n-p^{k^*}) \geq k(n+1)n(n-1)$ from $P\Gamma L_2(\mathbb{F}_n)$.

From the new constructions, we have these results:

- $M(n, \phi(n)) \geq \phi(n) \cdot n$ for n prime power,
- $M(n, \phi(n)+1) \geq \phi(n) \cdot n$ for n not prime power,
- $M(q^n, q^n - q^{n-1}) \geq q^n \prod_{i=0}^{n-1}(q^n - q^i)$, and
- $M(\frac{q^n-1}{q-1}, q^{n-1} - q + 2) \geq \frac{1}{q-1} \prod_{i=0}^{n-1}(q^n - q^i)$ where q is prime power.

Further study

For future research, one can explore the following areas:

- other metrics such as the Kendall tau and Ulam metric,

Further study

For future research, one can explore the following areas:

- other metrics such as the Kendall tau and Ulam metric,
- constant composition codes, and

Further study

For future research, one can explore the following areas:

- other metrics such as the Kendall tau and Ulam metric,
- constant composition codes, and
- algebraic constructions where n is not a prime power.

THE END