Perfect codes in Cayley graphs on $\mathbb{Z}_p^2$ and $\mathbb{Z}_{p^k}$

Yusuf Hafidh
University of Melbourne

Joint work with Sanming Zhou and Binzhou Xia

45th Australasian Combinatorics Conference
University of Western Australia
13 December 2023

Perfect code

Ball

Let u be a vertex of a connected graph Γ and r be a positive integer. The *ball* with radius r centered at u is denoted by $B_r(u)$. This is the set of vertices with distance at most r to u, i.e. $B_r(u) = \{v : d(v, u) \leq r\}$.

Perfect r-code

A set of vertices C of Γ, is called a *perfect r-code* in Γ if $\{B_r(u) : u \in C\}$ is a partition of $V(\Gamma)$.

Perfect 2-code in grid graph

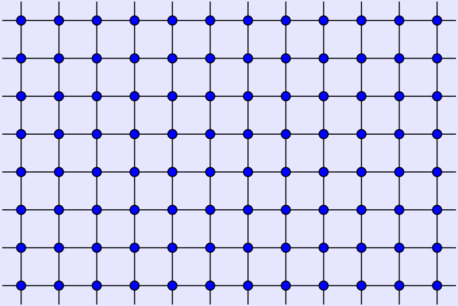

Figure 1. Grid graph

Perfect 2-code in grid graph

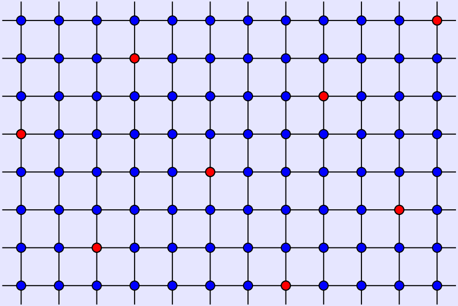

Figure 1. Grid graph

Perfect 2-code C

Perfect 2-code in grid graph

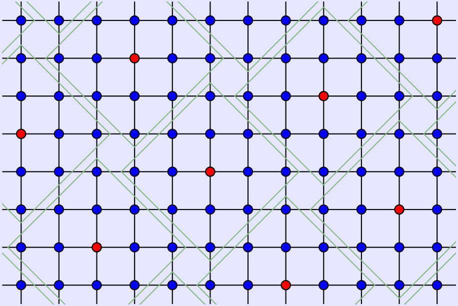

Figure 1. Grid graph

Perfect 2-code C

Balls with radius 2 centered at vertices in C

Relations

- A perfect r-code is an r-error correcting code in coding theory.

Relations

- A perfect r-code is an r-error correcting code in coding theory. (Also an error detecting code)

Relations

- A perfect r-code is an r-error correcting code in coding theory. (Also an error detecting code)
  - Coding theory : perfect r-code in q-ary alphabet of length n.
  - Graph theory : perfect r-code in the Hamming graph $H(n,q) = \underbrace{K_q \,\square \cdots \square\, K_q}_{n \text{ times}}$.

Relations

- A perfect r-code is an r-error correcting code in coding theory. (Also an error detecting code)
  - Coding theory : perfect r-code in q-ary alphabet of length n.
  - Graph theory : perfect r-code in the Hamming graph $H(n,q) = \underbrace{K_q \,\square \cdots \square\, K_q}_{n \text{ times}}$.
- A perfect 1-code is a dominating set in graph theory.

Cayley graph

Cayley graph

Let G be a group and $S \subseteq G \backslash \{0\}$. The *Cayley graph* $\Gamma = Cay(G, S)$ is the graph with vertex set G and edges from $x \in G$ to $x + s$, $s \in S$.

Cayley graph

Cayley graph

Let G be a group and $S \subseteq G \backslash \{0\}$. The *Cayley graph* $\Gamma = Cay(G, S)$ is the graph with vertex set G and edges from $x \in G$ to $x + s$, $s \in S$.

1. If S is closed under taking inverse elements (i.e. $S = -S$), then Γ is undirected.
2. If S generates G, then Γ is connected.

Cayley graph $Cay(\mathbb{Z}_{17}, \{1, \pm 5\})$

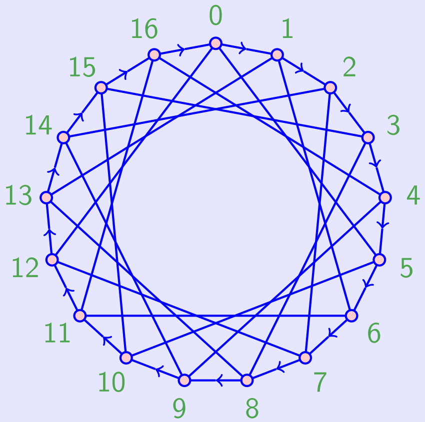

Figure 3. Cayley graph $Cay(\mathbb{Z}_{17}, \{1, \pm 5\})$

Motivation and Problem 1

- q-ary alphabet of length n using Hamming distance is represented as $H(q,n) = Cay(\mathbb{Z}_q, S)^n$ where $S = \mathbb{Z}_q \backslash \{0\}$.

Motivation and Problem 1

- q-ary alphabet of length n using Hamming distance is represented as $H(q,n) = Cay(\mathbb{Z}_q, S)^n$ where $S = \mathbb{Z}_q \setminus \{0\}$.
- q-ary alphabet of length n using Lee distance is represented as $Cay(\mathbb{Z}_q, S)^n$ where $S = \{\pm 1\}$.

Motivation and Problem 1

- q-ary alphabet of length n using Hamming distance is represented as $H(q, n) = Cay(\mathbb{Z}_q, S)^n$ where $S = \mathbb{Z}_q \backslash \{0\}$.
- q-ary alphabet of length n using Lee distance is represented as $Cay(\mathbb{Z}_q, S)^n$ where $S = \{\pm 1\}$.
- Problem 1: For which S does the Cayley graph $Cay(\mathbb{Z}_q, S)^n$ has a perfect code?

Perfect 1-codes in $Cay(\mathbb{Z}_p, S)^2$

Theorem 1

Let p be an odd prime and S a non-empty subset of $\mathbb{Z}_p$. Then $\Gamma = Cay(\mathbb{Z}_p, S)^2$ has a perfect 1-code if and only if $|S| = \frac{p-1}{2}$ and there is an $a \in \mathbb{Z}_p^*$ such that $aS \cap (-S) = \emptyset$.

Moreover, the perfect 1-codes are $\{(n, an + b) \mid n \in \mathbb{Z}_p\}$ for any $b \in \mathbb{Z}_p$.

Perfect 1-codes in $Cay(\mathbb{Z}_p, S)^2$

Theorem 1

Let p be an odd prime and S a non-empty subset of $\mathbb{Z}_p$. Then $\Gamma = Cay(\mathbb{Z}_p, S)^2$ has a perfect 1-code if and only if $|S| = \frac{p-1}{2}$ and there is an $a \in \mathbb{Z}_p^*$ such that $aS \cap (-S) = \emptyset$.

Moreover, the perfect 1-codes are $\{(n, an+b) \mid n \in \mathbb{Z}_p\}$ for any $b \in \mathbb{Z}_p$.

Note: Condition could be $\exists a \in \mathbb{Z}_p^* \ni aS \cap S = \emptyset$

Proof of Theorem 1

- If $Cay(\mathbb{Z}_p, S)^2$ has a perfect code C then $\mathbb{Z}_p^2 = C \oplus \{(0,0),(0,s),(s,0) \mid s \in S\}$.

Proof of Theorem 1

- If $Cay(\mathbb{Z}_p, S)^2$ has a perfect code C then $\mathbb{Z}_p^2 = C \oplus \{(0,0), (0,s), (s,0) \mid s \in S\}$.

- Rédei and Zwei (1947) : C is a coset of $\mathbb{Z}_p^2$ of order p.

Proof of Theorem 1

- If $Cay(\mathbb{Z}_p, S)^2$ has a perfect code C then $\mathbb{Z}_p^2 = C \oplus \{(0,0),(0,s),(s,0) \mid s \in S\}$.
- Rédei and Zwei (1947) : C is a coset of $\mathbb{Z}_p^2$ of order p.
- There is an $a \in \mathbb{Z}_p^*$ such that $C = \{(n, an+b) \mid n \in \mathbb{Z}_p\}$, $b \in \mathbb{Z}_p$.

Proof of Theorem 1

- If $Cay(\mathbb{Z}_p, S)^2$ has a perfect code C then $\mathbb{Z}_p^2 = C \oplus \{(0,0),(0,s),(s,0) \mid s \in S\}$.
- Rédei and Zwei (1947) : C is a coset of $\mathbb{Z}_p^2$ of order p.
- There is an $a \in \mathbb{Z}_p^*$ such that $C = \{(n, an+b) \mid n \in \mathbb{Z}_p\}$, $b \in \mathbb{Z}_p$.
- Establish that $as_1 \neq -s_2$ for $s_1, s_2 \in S$.

Proof of Theorem 1

$$\Gamma = Cay(\mathbb{Z}_7, \{1,4,5\})^2$$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

Proof of Theorem 1

$$\Gamma = Cay(\mathbb{Z}_7, \{1,4,5\})^2$$

Consider $(0,0) \in C$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

Proof of Theorem 1

$\Gamma = Cay(\mathbb{Z}_7, \{1,4,5\})^2$

Consider $(0,0) \in C$

Ball centered at $(0,0)$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

Proof of Theorem 1

$$\Gamma = Cay(\mathbb{Z}_7, \{1,4,5\})^2$$

Consider $(0,0) \in C$

Ball centered at $(0,0)$

$$C = \{(n, an) \mid n \in \mathbb{Z}_p\}$$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

Proof of Theorem 1

$\Gamma = Cay(\mathbb{Z}_7, \{1, 4, 5\})^2$

Consider $(0, 0) \in C$

Ball centered at $(0, 0)$

$C = \{(n, an) \mid n \in \mathbb{Z}_p\}$

For $(s_1, as_1) \in C, s_1 \in S,$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

Proof of Theorem 1

$\Gamma = Cay(\mathbb{Z}_7, \{1, 4, 5\})^2$

Consider $(0, 0) \in C$

Ball centered at $(0, 0)$

$C = \{(n, an) \mid n \in \mathbb{Z}_p\}$

For $(s_1, as_1) \in C, s_1 \in S$,
$as_1 + s_2 \neq 0$, for all $s_2 \in S$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

Proof of Theorem 1

$$\Gamma = Cay(\mathbb{Z}_7, \{1, 4, 5\})^2$$

Consider $(0, 0) \in C$

Ball centered at $(0, 0)$

$$C = \{(n, an) \mid n \in \mathbb{Z}_p\}$$

For $(s_1, as_1) \in C, s_1 \in S$,
$as_1 + s_2 \neq 0$, for all $s_2 \in S$

$$aS \cap (-S) \neq 0$$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

Proof of Theorem 1

$$\Gamma = Cay(\mathbb{Z}_7, \{1,4,5\})^2$$

Consider $(0,0) \in C$

Ball centered at $(0,0)$

$$C = \{(n, an) \mid n \in \mathbb{Z}_p\}$$

For $(s_1, as_1) \in C, s_1 \in S$,
$as_1 + s_2 \neq 0$, for all $s_2 \in S$

$$aS \cap (-S) \neq 0$$

$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$

If $aS \cap (-S) \neq \emptyset$, then $C = \{(n, an) \mid n \in \mathbb{Z}_p\}$ is a perfect code.

Examples

1. $S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}; \, a = 1.$

Examples

1. $S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$; $a = 1$.
2. $S = \left\{x_i \mid x_i \in \{\pm i\}, i = 1, \ldots, \frac{p-1}{2}\right\}$; $a = 1$.

Examples

1. $S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$; $a = 1$.
2. $S = \left\{x_i \mid x_i \in \{\pm i\}, i = 1, \ldots, \frac{p-1}{2}\right\}$; $a = 1$.
3. S is the set of quadratic residues of $\mathbb{Z}_p$; a is any quadratic residue for $p \equiv 3 \pmod 4$ and a is any non-quadratic residue for $p \equiv 1 \pmod 4$ (Paley graph).

Examples

1. $S = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$; $a = 1$.

2. $S = \left\{x_i \mid x_i \in \{\pm i\}, i = 1, \ldots, \frac{p-1}{2}\right\}$; $a = 1$.

3. S is the set of quadratic residues of $\mathbb{Z}_p$; a is any quadratic residue for $p \equiv 3 \pmod 4$ and a is any non-quadratic residue for $p \equiv 1 \pmod 4$ (Paley graph).

4. S is the set of non-quadratic residues of $\mathbb{Z}_p$; a is any quadratic residue for $p \equiv 3 \pmod 4$ and a is any non-quadratic residue for $p \equiv 1 \pmod 4$.

When $q \equiv 1 \pmod 4$, examples 3 and 4 is an undirected graph.

A generalization

As $Cay(\mathbb{Z}_p, S)^2 = Cay(\mathbb{Z}_p^2, S_2)$ where
$S_2 = \{(0, s), (s, 0) \mid s \in S\}$,

for which S does $Cay(\mathbb{Z}_q^2, S)$ has a perfect 1-code?

Perfect 1-codes in $Cay(\mathbb{Z}_p^2, S)$

Theorem 2

Let p be a prime. If Γ is not a complete graph, then $\Gamma = Cay(\mathbb{Z}_p^2, S)$ has a perfect 1-code if and only if $|S| = p - 1$ and S satisfy:

1. $\{s_1 \mid (s_1, s_2) \in S\} = \mathbb{Z}_p^*$, or
2. there is an $a \in \mathbb{Z}_p$ such that $\{as_1 + s_2 \mid (s_1, s_2) \in S\} = \mathbb{Z}_p^*$.

Perfect 1-codes in $Cay(\mathbb{Z}_p^2, S)$

Theorem 2

Let p be a prime. If Γ is not a complete graph, then $\Gamma = Cay(\mathbb{Z}_p^2, S)$ has a perfect 1-code if and only if $|S| = p - 1$ and S satisfy:

1. $\{s_1 \mid (s_1, s_2) \in S\} = \mathbb{Z}_p^*$, or
2. there is an $a \in \mathbb{Z}_p$ such that $\{as_1 + s_2 \mid (s_1, s_2) \in S\} = \mathbb{Z}_p^*$.

Theorem 3

Let p be a prime. If Γ is not a complete graph, then $\Gamma = Cay(\mathbb{Z}_p^2, S)$ has a perfect 1-code if and only if $|S| = p - 1$ and there are $a, b \in \mathbb{Z}_p$ such that $\{as_1 + bs_2 \mid (s_1, s_2) \in S\} = \mathbb{Z}_p^*$.

Motivation and problem 2

- Deng (2014) :
  - Characterization of $Cay(\mathbb{Z}_n, S)$ that has a perfect 1-code of prime size.
- Feng, Huang, Zhou (2017):
  - Characterization of $Cay(\mathbb{Z}_n, S)$ of degree prime minus one that has a perfect 1-code.
  - Characterization of $Cay(\mathbb{Z}_n, S)$ of $p^k - 1$ degree that has a perfect 1-code where p^k is relatively prime to $\frac{n}{p^k}$.
- Deng, Sun, Liu, Wang (2017): Perfect 1-codes on
  - $Cay(\mathbb{Z}_n, S)$ of degree $pq - 1$ and $p^k - 1$ for primes p, q, and $|S| + 1$ is relatively prime to $\frac{n}{|S|+1}$, and
  - $Cay(\mathbb{Z}_n, S)$ where $n = p^k q, p^2 q^2, pqr, p^2 qr, pqrs$, for different primes p, q, r, s, and $|S| + 1$ is relatively prime to $\frac{n}{|S|+1}$.

Motivation and problem 2

- Deng (2014) :
  - Characterization of $Cay(\mathbb{Z}_n, S)$ that has a perfect 1-code of prime size.
- Feng, Huang, Zhou (2017):
  - Characterization of $Cay(\mathbb{Z}_n, S)$ of degree prime minus one that has a perfect 1-code.
  - Characterization of $Cay(\mathbb{Z}_n, S)$ of $p^k - 1$ degree that has a perfect 1-code where p^k is relatively prime to $\frac{n}{p^k}$.
- Deng, Sun, Liu, Wang (2017): Perfect 1-codes on
  - $Cay(\mathbb{Z}_n, S)$ of degree $pq - 1$ and $p^k - 1$ for primes p, q, and $|S| + 1$ is relatively prime to $\frac{n}{|S|+1}$, and
  - $Cay(\mathbb{Z}_n, S)$ where $n = p^k q, p^2 q^2, pqr, p^2 qr, pqrs$, for different primes p, q, r, s, and $|S| + 1$ is relatively prime to $\frac{n}{|S|+1}$.
- Problem 2: What if $|S| + 1$ is not relatively prime to $\frac{n}{|S|+1}$?

Perfect 1-codes in $Cay(\mathbb{Z}_{p^k}, S)$

Theorem 4

Let p be an odd prime and $\Gamma = Cay(\mathbb{Z}_{p^k}, S)$ a connected non trivial graph, then Γ admits a perfect 1-code if and only if there are integers

$$0 = t_0 < t_1 < \cdots < t_n < t_{n+1} = k$$

and $1 \leq l_a \leq t_{a+1} - t_a$ for $a = 0, \ldots, n$ such that

$$S_0 = \left\{ \sum_{a=0}^{n} \left(i_a p^{s_a} + \alpha_{i_0,\ldots,i_a} p^{s_a + l_a} \right) \mid i_a = 0, \ldots, p^{l_a} - 1 \right\}$$

where $\alpha_{i_0,\ldots,i_a} \in \mathbb{Z}_{p^k}$.

Note : $S_0 = S \cup \{0\}$.

Proof idea

- C is a perfect code of $Cay(G,S) \iff G = C \oplus S_0$.

Proof idea

- C is a perfect code of $Cay(G,S) \iff G = C \oplus S_0$.
- Lemma 1 [9] :
  - For a finite abelian group G and $A \subseteq G$, L_A, the set of elements $g \in G$ such that $g + A = A$ is a subgroup of G (called the subgroups of periods of A), and $A = L_A \oplus B$ for some set B.

Proof idea

- C is a perfect code of $Cay(G, S) \iff G = C \oplus S_0$.
- Lemma 1 [9] :
  - For a finite abelian group G and $A \subseteq G$, L_A, the set of elements $g \in G$ such that $g + A = A$ is a subgroup of G (called the subgroups of periods of A), and $A = L_A \oplus B$ for some set B.
- De Bruijn (1953) : If $\mathbb{Z}_{p^k} = A \oplus B$, then one of A and B is periodic.

Proof idea

- C is a perfect code of $Cay(G, S) \iff G = C \oplus S_0$.
- Lemma 1 [9] :
  - For a finite abelian group G and $A \subseteq G$, L_A, the set of elements $g \in G$ such that $g + A = A$ is a subgroup of G (called the subgroups of periods of A), and $A = L_A \oplus B$ for some set B.
- De Bruijn (1953) : If $\mathbb{Z}_{p^k} = A \oplus B$, then one of A and B is periodic.
- Lemma 2 [9] :
  - Let $G = A \oplus B$ where A is periodic $(A = L_A \oplus D)$, then

$$G/L_A = (D + L_A)/L_A \oplus (B + L_A)/L_A,$$

where $(H + L_A)/L_A = \{h + L_A : h \in H\}$.

Proof idea

- C is a perfect code of $Cay(G, S) \iff G = C \oplus S_0$.
- Lemma 1 [9] :
  - For a finite abelian group G and $A \subseteq G$, L_A, the set of elements $g \in G$ such that $g + A = A$ is a subgroup of G (called the subgroups of periods of A), and $A = L_A \oplus B$ for some set B.
- De Bruijn (1953) : If $\mathbb{Z}_{p^k} = A \oplus B$, then one of A and B is periodic.
- Lemma 2 [9] :
  - Let $G = A \oplus B$ where A is periodic $(A = L_A \oplus D)$, then

$$G/L_A = (D + L_A)/L_A \oplus (B + L_A)/L_A,$$

where $(H + L_A)/L_A = \{h + L_A : h \in H\}$.
- Since $\mathbb{Z}_{p^k}/\mathbb{Z}_{p^l} \cong \mathbb{Z}_{p^{k-l}}$, we can use induction on k.

Good abelian group

- For an abelian group G, $G = A \oplus B$ is a factorization of G, and A and B are factors of G.
- A group G is said to be **good** if in every factorization of G, there is a periodic factor.
- All finite good abelian groups are precisely the following groups and their subgroups:

1. $\mathbb{Z}_p \times \mathbb{Z}_p$ [5]
2. $\mathbb{Z}_p \times \mathbb{Z}_3 \times \mathbb{Z}_3$ [7]
3. $\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_2 \times \mathbb{Z}_2$ [7]
4. $\mathbb{Z}_p \times \mathbb{Z}_4 \times \mathbb{Z}_2$ [7]
5. $\mathbb{Z}_{p^3} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ [7]
6. $\mathbb{Z}_{p^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ [7]
7. $\mathbb{Z}_p \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ [7]
8. $\mathbb{Z}_{2^\lambda} \times \mathbb{Z}_2$ [8]
9. $\mathbb{Z}_{p^\lambda} \times \mathbb{Z}_q$ [1]
10. $\mathbb{Z}_{p^2} \times \mathbb{Z}_{q^2}$ [6]
11. $\mathbb{Z}_{p^2} \times \mathbb{Z}_q \times \mathbb{Z}_r$ [6]
12. $\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r \times \mathbb{Z}_s$ [6]
13. $\mathbb{Z}_9 \times \mathbb{Z}_3$ [8]
14. $\mathbb{Z}_4 \times \mathbb{Z}_4$ [8]

where p, q, r, and s are different primes.

Perfect 1-codes in Cayley graphs with degree prime minus one

G	S_0	Requirement on S to be have a perfect 1-code	Perfect 1-code C
$\mathbb{Z}_p \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\|S_0\| = 3$	no requirement	$C = \langle(a,b,c)\rangle + (x,y,z)$ where $ord((a,b,c)) = 3p$, $s_1, s_2, s_1 - s_2 \notin \langle(a,b,c)\rangle$, and (x,y,z) any element of G
	$\|S_0\| = p$	$\{a \| (a,b,c) \in S_0\} = \mathbb{Z}_p$	$C = \{x\} \times \mathbb{Z}_3 \times \mathbb{Z}_3$ for some $x \in \mathbb{Z}_p$
$\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_2^2$	$\|S_0\| = p$	$\{a \| (a,b,c,d) \in S_0\} = \mathbb{Z}_p$	$C = \{x\} \times \mathbb{Z}_q \times \mathbb{Z}_2 \times \mathbb{Z}_2$ for some $x \in \mathbb{Z}_p$
$\mathbb{Z}_p \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$\|S_0\| = p$	$\{a \| (a,b,c) \in S_0\} = \mathbb{Z}_p$	$C = \{x\} \times \mathbb{Z}_4 \times \mathbb{Z}_2$ for some $x \in \mathbb{Z}_p$
$\mathbb{Z}_{p^3} \times \mathbb{Z}_2^2$	$\|S_0\| = p$	$\{a \pmod p \| (a,b,c) \in S_0\} = \mathbb{Z}_p$	$C = \langle(p,0,0),(0,1,0),(0,0,1)\rangle + (x,y,z)$ for some (x,y,z) in G
$\mathbb{Z}_{p^2} \times \mathbb{Z}_2^3$	$\|S_0\| = p$	$\{a \pmod p \| (a,b,c,d) \in S_0\} = \mathbb{Z}_p$	$C = \langle(p,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\rangle + (w,x,y,z)$ for some (w,x,y,z) in G
$\mathbb{Z}_p \times \mathbb{Z}_2^4$	$\|S_0\| = p$	$\{a \| (a,b,c,d,e) \in S_0\} = \mathbb{Z}_p$	$C = \{x\} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ for some $x \in \mathbb{Z}_p$

Perfect codes in $Cay(\mathbb{Z}_p \times \mathbb{Z}_3 \times \mathbb{Z}_3, S)$

G	S_0	Requirement on S to be have a perfect 1-code	Perfect 1-code C
$\mathbb{Z}_p \times \mathbb{Z}_3 \times \mathbb{Z}_3$	$\lvert S_0\rvert = 3$	Γ admits a perfect code for any $S = \{s_1, s_2\}$	$C = \langle(a,b,c)\rangle + (x,y,z)$ where $ord((a,b,c)) = 3p$, $s_1, s_2, s_1 - s_2 \notin \langle(a,b,c)\rangle$, and (x,y,z) any element of G
	$\lvert S_0\rvert = p$	$\{a \mid (a,b,c) \in S_0\} = \mathbb{Z}_p$	$C = \{x\} \times \mathbb{Z}_3 \times \mathbb{Z}_3$ for some $x \in \mathbb{Z}_p$
	$\lvert S_0\rvert = 9$, S_0 non-periodic	$\{(b,c) \mid (a,b,c) \in S_0\} = \mathbb{Z}_3 \times \mathbb{Z}_3$	$C = \{(x,y,z) \mid x \in \mathbb{Z}_p\}$ for some $y, z \in \mathbb{Z}_3$
	$\lvert S_0\rvert = 9$, S_0 periodic	$S_0 = L_{S_0} \oplus D$, $\{(0,b,c) + L_{S_0} \mid (a,b,c) + L_{S_0} \in (D + L_{S_0})/L_{S_0}\} \cong \mathbb{Z}_3$ in G/L_{S_0}	$C = \{(a,y,z) + l_a \mid a \in \mathbb{Z}_p\}$ for any $y, z \in \mathbb{Z}_3$ and $l_a \in L_{S_0}$
	$\lvert S_0\rvert = 3p$, S_0 non-periodic	There is $(\alpha, \beta) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ such that for every $a \in \mathbb{Z}_p$, (1) $\lvert\{(x,y,z) \in S_0 \mid x = a\}\rvert = 3$ and (2) $(\{(b,c) \mid (a,b,c) \in S_0\} + \langle(b,c)\rangle)/\langle(b,c)\rangle = (\mathbb{Z}_3 \times \mathbb{Z}_3)/\langle(0,b,c)\rangle$	$C = \{(x, y + r\alpha, z + r\beta) \mid r \in \mathbb{Z}_3\}$ for any $x \in \mathbb{Z}_p$ and $y, z \in \mathbb{Z}_3$
	$\lvert S_0\rvert = 3p$, S_0 periodic	$S_0 = L_{S_0} \oplus D$, There is a non-zero $(\alpha, \beta) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ such that $(D + \langle(0,\alpha,\beta)\rangle)/\langle(0,\alpha,\beta)\rangle$ is a complete set of residue in $G/\langle(0,\alpha,\beta)\rangle$ modulo $(L_{S_0} + \langle(0,\alpha,\beta)\rangle)/\langle(0,\alpha,\beta)\rangle$	$C = \{a(0,\alpha,\beta) + l_a \mid a \in \mathbb{Z}_3\}$ where $l_a \in L_{S_0}$

Perfect 1-codes in $Cay(\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_2 \times \mathbb{Z}_2, S)$

G	S_0	Requirement on S to be have a perfect 1-code	Perfect 1-code C
$\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\lvert S_0\rvert = p$	$\{a \mid (a,b,c,d) \in S_0\} = \mathbb{Z}_p$	$C = \{x\} \times \mathbb{Z}_q \times \mathbb{Z}_2 \times \mathbb{Z}_2$ for some $x \in \mathbb{Z}_p$
	$\lvert S_0\rvert = pq$, S_0 periodic	$S_0 = \{(a, b, c_a, d_a) \mid a \in \mathbb{Z}_p, b \in \mathbb{Z}_q\}$, $c_a, d_a \in \mathbb{Z}_2$	$C = \{(0, l_{y,z}, y, z) \mid (x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_2\}$, $l_{x,y} \in L_{S_0}$
	$\lvert S_0\rvert = pq$, S_0 non-periodic, $\left\lvert L_{(S_0+L_C)/L_C}\right\rvert = q$	$S_0 = \{(a, b, c_a, d_a) + l_{a,b} \mid a \in \mathbb{Z}_p, b \in \mathbb{Z}_q\}$, $c_a, d_a \in \mathbb{Z}_2$, $l_{a,b} \in L_C$	$C = L_C \cup (L_C + (w, x, y, z))$, where $L_C = \langle(0, 0, \alpha, \beta)\rangle$ and $(y, z) \notin \langle(\alpha, \beta)\rangle$
	$\lvert S_0\rvert = pq$, S_0 non-periodic, $\left\lvert L_{(S_0+L_C)/L_C}\right\rvert = p$	$S_0 = \{(a, b, c_b, d_b) + l_{a,b} \mid a \in \mathbb{Z}_p, b \in \mathbb{Z}_q\}$, $c_b, d_b \in \mathbb{Z}_2$, $l_{a,b} \in L_C$	$C = L_C \cup (L_C + (w, x, y, z))$, where $L_C = \langle(0, 0, \alpha, \beta)\rangle$ and $(y, z) \notin \langle(\alpha, \beta)\rangle$
	$\lvert S_0\rvert = 2p$, S_0 periodic	$S_0 = L_{S_0} \oplus D$ where $\lvert L_{S_0}\rvert = 2$, $\{a \mid (a, b, c, d) \in D\} = \mathbb{Z}_p$	$C = \{(0, b, aw, av) + l_{a,b} \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_q\}$, $l_{a,b} \in L_{S_0}$
	$\lvert S_0\rvert = 2p$, S_0 non-periodic	$S_0 = \{(\alpha, \beta b, \beta c, \beta d) + l_{\alpha,\beta} \mid \alpha \in \mathbb{Z}_p, \beta \in \mathbb{Z}_2\}$, $l_{\alpha,\beta} \in L_C$	$C = L_C \oplus D$, where $L_C = \langle(0, 0, \alpha, \beta)\rangle$ and $\{b \mid (a, b, c, d) \in D\} = \mathbb{Z}_q$

Perfect 1-codes in $Cay(\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_2 \times \mathbb{Z}_2, S)$

G	S_0	Requirement on S to be have a perfect 1-code	Perfect 1-code C
$\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\lvert S_0\rvert = 4$, S_0 periodic	$S_0 = \langle(0,0,y,z)\rangle \cup (\langle(0,0,y,z)\rangle + (a,b,c,d))$ where $a,b \neq 0$, $(c,d) \notin \langle(y,z)\rangle$, and $(y,z) \neq (0,0)$	$C = \{(\alpha,\beta,\gamma_{\alpha,\beta},\delta_{\alpha,\beta}) \mid (\alpha,\beta) \in \mathbb{Z}_p \times \mathbb{Z}_q\}$
	$\lvert S_0\rvert = 4$, S_0 non-periodic	$S_0 = \{\alpha(0,0,y,z) + \beta(a,b,c,d) + l_{\alpha,\beta} \mid \alpha,\beta \in \mathbb{Z}_2\}$ where $l_{\alpha,\beta} \in L_C$	$C = L_C \oplus D$ where $L_C = \langle(1,0,0,0)\rangle$ and $\{b \mid (a,b,c,d) \in D\} = \mathbb{Z}_q$, or $L_C = \langle(0,1,0,0)\rangle$ and $\{a \mid (a,b,c,d) \in D\} = \mathbb{Z}_p$
		$\{(c,d) \mid (a,b,c,d) \in S_0\} = \mathbb{Z}_2 \times \mathbb{Z}_2$	$C = \langle(1,1,0,0)\rangle$
	$\lvert S_0\rvert = 2pq$	$S_0 = \langle(1,1,0,0),(0,0,c,d)\rangle$ where $(c,d) \notin \langle(y,z)\rangle$, $(y,z) \neq (0,0)$	$C = \{(0,0,0,0),(w,x,y,z)\}$
	$\lvert S_0\rvert = 4p$, S_0 periodic	$S_0 = \{(a,b_{a,c,d},c,d) + l_{a,c,d} \mid a \in \mathbb{Z}_p, c,d \in \mathbb{Z}_2\}$, $b_{a,c,d} \in \mathbb{Z}_q$, $l_{a,c,d} \in L_{S_0}$	$C = \{(0,b,0,0) + l_b \mid b \in \mathbb{Z}_q\}$, $l_b \in L_{S_0}$
	$\lvert S_0\rvert = 4p$, S_0 non-periodic	$S_0 = \{a,b_{a,c,d},c,d \mid a \in \mathbb{Z}_p, c,d \in \mathbb{Z}_2\}$, $b_{a,c,d} \in \mathbb{Z}_q$	$C = \langle(0,1,0,0)\rangle$

References

[1] N. G. de Bruijn, On the factorisation of cyclic groups, Indag. Math. Kon. Ned, Akad. Wetensch. Amsterdam, 15 (1953), 370–377.

[2] Y.P. Deng, Efficient dominating sets in circulant graphs with domination number prime, Inform. Process. Lett., 114 (2014), 700–702.

[3] Y.P. Deng, Y.Q. Sun, Q. Liu and H.C. Wang, Efficient dominating sets in circulant graphs, Discrete Math., 340(7) (2017), 1503–1507.

[4] R. Feng, H. Huang, and S. Zhou, Perfect codes in circulant graphs, Discrete Math., 340 (2017), 1522–1527.

[5] L. Rédei and Zwei, Liickensatze iiber Polynome in endlichen Primkorpern mit Anwendungen auf die endlichen Abelschen Gruppen und die Gaussischen Summen. Acta Math., 79 (1947), 273–290.

[6] A. D. Sands, On the factorisation of finite abelian groups, Acta Math. Acad. Sci. Hung., g (1957), pp. 65–86.

[7] A. D. Sands, On the factorisation of finite abelian groups, II, Acta Math. Acad. Sci. Hung., 13 (1962), no.1-2, 153–169.

[8] A. D. Sands, The factorization of abelian groups, The Quarterly Journal of Mathematics, 10 (1959), 81–91.

[9] S. Szabó and A.D. Sands, Factoring Groups into Subsets, CRC Press, Taylor and Francis Group, (2009).