Weight distributions of $\mathbb{Z}_{p^s}$-additive simplex and MacDonald codes

C.Fernández-Córdoba, **S.Sánchez-Aragón** and M.Villanueva

8th Workshop on Design Theory, Hadamard Matrices and Applications
Sevilla, June 26th-30th, 2025

Work partially supported by the Spanish MICIN under Grant PID2022-137924NB-I00
and by the Catalan AGAUR grant 2021 SGR 00643.

CCSG
Combinatorics, Coding and Security Group

DEIC

UAB
Universitat Autònoma de Barcelona

Outline

Motivation

Since the publication in 1994 of the famous paper

A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, **40** *(1994), 301–319.*

the study of linear codes over rings has received a lot of attention.

Simplex and MacDonald codes over $\mathbb{Z}_{2^s}$ have been studied in

M.K. Gupta, M.C. Bhandari, and A.K. Lal: On some linear codes over $\mathbb{Z}_{2^s}$. *Designs, Codes and Cryptography, 36, no. 3, pp. 227–244 (2005).*

C. Fernández-Córdoba, C. Vela and M. Villanueva: Nonlinearity and Kernel of $\mathbb{Z}_{2^s}$-Linear simplex and MacDonald Codes. *IEEE Transactions on Information Theory, 68, no. 11, pp. 7174-7183 (2021).*

Our goal is to generalize and study these families of codes over $\mathbb{Z}_{p^s}$ for an arbitrary prime p and $s \geq 1$.

Outline

1. Motivation
2. $\mathbb{Z}_{p^s}$-additive codes
3. $\mathbb{Z}_{p^s}$-additive simplex and MacDonald codes
   - Construction of $\mathbb{Z}_{p^s}$-additive simplex codes
   - Results for $\mathbb{Z}_{p^s}$-additive simplex codes
   - Construction of $\mathbb{Z}_{p^s}$-additive MacDonald codes
4. Future research

$\mathbb{Z}_{p^s}$-additive codes

A **code** over $\mathbb{Z}_{p^s}$ of length n is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_{p^s}^n$.

If $\mathcal{C}$ has group structure, then it is called a $\mathbb{Z}_{p^s}$-**additive code**. In this case, $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{p^s}^n$, so it is isomorphic to an abelian structure $\mathbb{Z}_{p^s}^{t_1} \times \mathbb{Z}_{p^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_{p^2}^{t_{s-1}} \times \mathbb{Z}_{p}^{t_s}$, and we say that $\mathcal{C}$ is of **type** $(n; t_1, \dots, t_s)$.

A matrix with rows that are generators of a code is called a **generator matrix**.

There is a generator matrix of $\mathcal{C}$ (with minimum number of rows) having t_i rows of order $p^{s-(i-1)}$ for all $i \in \{1, \dots, s\}$.

Example

In $\mathbb{Z}_{27}$,

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 3 & 9 & 12 & 15 \\ 0 & 0 & 9 & 18 & 9 \end{pmatrix}$$

generates a linear code of type $(5; 1, 1, 1)$.

Weights for $\mathbb{Z}_{p^s}^n$

Consider $c = (c_1, \dots, c_n) \in \mathbb{Z}_{p^s}^n$. The **Hamming weight** of c is defined as

$$w_H(c) = |\{1 \leq i \leq n \mid c_i \neq 0\}|.$$

The **homogeneous weight** of c_i is defined as

$$w_{Hom}(c_i) = \begin{cases} 0 & \text{if } c_i = 0, \\ p^{s-1} & \text{if } c_i \neq 0 \text{ and } c_i \in \langle p^{s-1} \rangle, \\ (p-1)p^{s-2} & \text{otherwise,} \end{cases}$$

and $w_{Hom}(c) = \sum_{i=1}^n w_{Hom}(c_i)$.

Example

Consider $\mathbb{Z}_9 = \mathbb{Z}_{3^2}$ and $c = (0, 1, 2, 3, 4)$.
Then, $w_H(c) = 4$ and $w_{Hom}(c) = 3 \cdot 2 + 1 \cdot 3 = 9$.

These weights w define **distance functions** by taking $d(x, y) = w(x - y)$.

Order and valuation

We define the **order** of $x \in \mathbb{Z}_{p^s}^n$, denoted by $\mathrm{o}(x)$, as the smallest natural number m such that $mx = \mathbf{0}$.

We define the **valuation** of $x \in \mathbb{Z}_{p^s}^n \setminus \{\mathbf{0}\}$, denoted by $\nu(x)$, as the largest natural number k such that $x = p^k y$, where y is another nonzero element of $\mathbb{Z}_{p^s}^n$. For $x = \mathbf{0}$, we define its valuation as $\nu(\mathbf{0}) = \infty$.

For $x \neq \mathbf{0}$, $\mathrm{o}(x) = p^{s-\nu(x)}$.

Example

For $x = (0,1) \in \mathbb{Z}_4^2$, we have that $\mathrm{o}(x) = 4$ and $\nu(x) = 0$.
For $y = (2,2) \in \mathbb{Z}_4^2$, we have that $\mathrm{o}(y) = 2$ and $\nu(y) = 1$.

A Griesmer-type bound for $\mathbb{Z}_{p^s}$-additive codes

The minimum Hamming distance of a $\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ is

$$d_H(\mathcal{C}) = \min\{w_H(c) \mid c \in \mathcal{C}\backslash\{\mathbf{0}\}\}.$$

Theorem

Let $\mathcal{C}$ be a $\mathbb{Z}_{p^s}$-additive code of type $(n; t_1, \dots, t_s)$ and minimum Hamming distance $d_H(\mathcal{C})$, and let $k = \sum_{j=1}^{s} t_j$. Then, we have that

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_H(\mathcal{C})}{p^i} \right\rceil.$$

When this bound is met, the code $\mathcal{C}$ is optimal for the Griesmer-type bound.

K. Shiromoto and L. Storme, A Griesmer bound for linear codes over finite quasi-Frobenius rings. *Discrete Applied Mathematics*, 128, no. 1 pp. 263-274.

The generalized Gray map

The **generalized Gray map** $\Phi_s : \mathbb{Z}_{p^s} \longmapsto \mathbb{Z}_p^{p^{s-1}}$ is defined as follows:

$$\Phi_s(u) = (u_0, \ldots, u_{s-2}, u_{s-1})M_{s-1},$$

where $[u_0, u_1, \ldots, u_{s-1}]_p$ is the p-ary expansion of $u \in \mathbb{Z}_{p^s}$, $u = \sum_{i=0}^{s-1} u_i p^i$ with $u_i \in \{0, \ldots, p-1\}$, and

$$M_{s-1} = \begin{pmatrix} Y_{s-1} \\ \mathbf{1} \end{pmatrix}, \tag{1}$$

where Y_{s-1} is the matrix of size $s-1 \times p^{s-1}$ over $\mathbb{Z}_p$ such that its columns are all the elements of $\mathbb{Z}_p^{s-1}$. We define Φ_s over $\mathbb{Z}_{p^s}^n$ component-wise.

Example

The generalized Gray map for $\mathbb{Z}_8$ is $\Phi_3 : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_2^4$:

$$M_2 = \begin{pmatrix} 0011 \\ 0101 \\ 1111 \end{pmatrix}$$

$$\begin{array}{lcl@{\qquad}lcl} 0 = [000]_2 & \longmapsto & 0000 & 4 = [001]_2 & \longmapsto & 1111 \\ 1 = [100]_2 & \longmapsto & 0011 & 5 = [101]_2 & \longmapsto & 1100 \\ 2 = [010]_2 & \longmapsto & 0101 & 6 = [011]_2 & \longmapsto & 1010 \\ 3 = [110]_2 & \longmapsto & 0110 & 7 = [111]_2 & \longmapsto & 1001 \end{array}$$

Outline

Construction of $\mathbb{Z}_{p^s}$-additive simplex codes: type α

Let G_k^α be the matrix consisting of all possible distinct columns.

$$G_1^\alpha = \begin{pmatrix} 0 & 1 & 2 & \cdots & p^s-1 \end{pmatrix} \quad \text{and}$$

$$G_k^\alpha = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{2} & \cdots & \mathbf{p^s-1} \\ G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & \cdots & G_{k-1}^\alpha \end{pmatrix}.$$

The code generated by G_k^α, denoted by S_k^α, is called a $\mathbb{Z}_{p^s}$**-additive simplex code of type** $\boldsymbol{\alpha}$ with $k \geq 1$ generators.

Example

Consider $\mathbb{Z}_3$. Then, we have that

$$G_1^\alpha = (012), \quad G_2^\alpha = \begin{pmatrix} 000 & 111 & 222 \\ 012 & 012 & 012 \end{pmatrix}.$$

Construction of $\mathbb{Z}_{p^s}$-additive simplex codes: type β

Let G_k^β be the matrix constructed recursively as follows:

$$G_1^\beta = (1)\,, \quad G_2^\beta = \left(\begin{array}{ccccc} \mathbf{1} & 0 & p & \cdots & p^s - p \\ 0\,1\,2\,\ldots\,p^s-1 & 1 & 1 & \cdots & 1 \end{array} \right),$$

$$G_k^\beta = \left(\begin{array}{cccc} \mathbf{1} & \mathbf{0} & \cdots & \mathbf{p^s - p} \\ G_{k-1}^\alpha & G_{k-1}^\beta & \cdots & G_{k-1}^\beta \end{array} \right).$$

The code generated by G_k^β, denoted by S_k^β, is called a $\mathbb{Z}_{p^s}$-**additive simplex code of type $\boldsymbol{\beta}$** with $k \geq 1$ generators.

Example

Consider $\mathbb{Z}_9$. Then, we have that

$$G_1^\beta = (1)\,,$$

$$G_2^\beta = \left(\begin{array}{cccc} 111111111 & 0 & 3 & 6 \\ 012345678 & 1 & 1 & 1 \end{array} \right).$$

Results for $\mathcal{S}_k^\alpha$

Theorem

- S_k^α *has type* $(p^{sk}; k, 0, \ldots, 0)$.
- *For all* $c \in S_k^\alpha \backslash \{\mathbf{0}\}$, $w_H(c) = p^{sk} - p^{\nu(c)} p^{s(k-1)}$, *so*

  $$d_H(S_k^\alpha) = (p-1)p^{sk-1}.$$

  For every valuation $j \in \{0, 1, \ldots, s-1\}$, *there are* $p^{k(s-j)} - p^{k((s-j)-1)}$ *codewords of weight* $p^{sk} - p^j p^{s(k-1)}$.
- *For all* $c \in S_k^\alpha \backslash \{\mathbf{0}\}$, $w_{Hom}(c) = p^{s(k+1)-2}(p-1)$, *so*

  $$d_{Hom}(S_k^\alpha) = p^{s(k+1)-2}(p-1).$$

- $\mathcal{S}_k^\alpha$ *is not optimal for the Griesmer-type bound, for any prime* p *and* $s \geq 1$.

Results for $\mathcal{S}_k^\beta$

Theorem

- $\mathcal{S}_k^\beta$ *has type* $(p^{(s-1)(k-1)}\frac{p^k-1}{p-1}; k, 0, \dots, 0)$.
- *For all* $c \in S_k^\beta \backslash \{\mathbf{0}\}$, $w_H(c) = p^{(s-1)(k-1)}\frac{p^k-1}{p-1} - p^{\nu(c)}(p^{(s-1)(k-2)}\frac{p^{k-1}-1}{p-1})$, *so*
$$d_H(\mathcal{S}_k^\beta) = p^{s(k-1)}.$$
For every valuation $j \in \{0, 1, \dots, s-1\}$, *there are* $p^{k(s-j)} - p^{k((s-j)-1)}$ *codewords of weight* $p^{(s-1)(k-1)}\frac{p^k-1}{p-1} - p^j(p^{(s-1)(k-2)}\frac{p^{k-1}-1}{p-1})$.
- *For* $c \in \mathcal{S}_k^\beta$, $w_{Hom}(c) = \begin{cases} p^{sk-1} & \text{if } \nu(c) = s-1, \\ p^{sk-k-1}(p^k-1) & \text{if } \nu(c) < s-1, \\ 0 & \text{otherwise}, \end{cases}$
so
$$d_{Hom}(\mathcal{S}_k^\beta) = p^{sk-k-1}(p^k-1).$$
- $\mathcal{S}_k^\beta$ *is optimal for the Griesmer-type bound, for every prime* p *and* $s \geq 1$.

Results for $\Phi_s(\mathcal{S}_k^\alpha)$ and $\Phi_s(\mathcal{S}_k^\beta)$

The generalized Gray map is an isometry $\Phi_s : (\mathbb{Z}_{p^s}^n, d_{Hom}) \longmapsto (\mathbb{Z}_p^{p^{s-1}n}, d_H)$. Moreover, generalized Gray map images of any linear code are distance invariant, as $d(\Phi_s(x), \Phi_s(y)) = w_H(\Phi_s(x-y))$ for any $x, y \in \mathbb{Z}_{p^s}^n$.

Theorem

- *The code $\Phi_s(\mathcal{S}_k^\alpha)$ is a $(p^{s(k+1)-1}, p^{sk}, p^{s(k+1)-2}(p-1))$ code over $\mathbb{Z}_p$ having all codewords of the same Hamming weight equal to $p^{s(k+1)-2}(p-1)$, except the all-zero codeword.*
- *The code $\Phi_s(\mathcal{S}_k^\beta)$ with $k \geq 2$ is a $(p^{(s-1)k}\frac{p^k-1}{p-1}, p^{sk}, p^{sk-k-1}(p^k-1))$ code over $\mathbb{Z}_p$, having p^k-1 codewords of Hamming weight $p^{sk}-1$, $p^{sk}-p^k$ codewords of Hamming weight $p^{sk-k-1}(p^k-1)$ and one of Hamming weight zero.*

Construction of $\mathbb{Z}_{p^s}$-additive MacDonald codes: type α

Let $k \geq 1$ and $1 \leq u \leq k-1$. We define $G^\alpha_{k,u}$ as follows:

$$G^\alpha_{k,u} = \left(\begin{array}{ccc} G^\alpha_k & \backslash & \frac{\mathbf{0}}{G^\alpha_u} \end{array} \right) = \left(\begin{array}{cccccc} \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \cdots & \mathbf{p^s-1} \\ G^\alpha_{k-1,u} & G^\alpha_{k-1} & G^\alpha_{k-1} & G^\alpha_{k-1} & \cdots & G^\alpha_{k-1} \end{array} \right),$$

where $(A \backslash B)$ is the matrix A by deleting the columns of B.

The code generated by $G^\alpha_{k,u}$ is denoted by $M^\alpha_{k,u}$ and is called a **$\mathbb{Z}_{p^s}$-additive MacDonald code of type α** with $k \geq 1$ generators.

Example

Take $\mathbb{Z}_4$. Then, we have that

$$G^\alpha_{2,1} = \left(\begin{array}{cccc} \cancel{0000} & 1111 & 2222 & 3333 \\ \cancel{0123} & 0123 & 0123 & 0123 \end{array} \right).$$

Construction of $\mathbb{Z}_{p^s}$-additive MacDonald codes: type β

Let $k \geq 2$ and $1 \leq u \leq k-1$. We define $G^{\beta}_{k,u}$ as follows:

$$G^{\beta}_{k,u} = \left(\begin{array}{ccc} G^{\beta}_{k} & \backslash & \frac{\mathbf{0}}{G^{\beta}_{u}} \end{array} \right) = \left(\begin{array}{cccccc} \mathbf{1} & \mathbf{0} & \mathbf{p} & \mathbf{2p} & \cdots & \mathbf{p^s - p} \\ G^{\alpha}_{k-1} & G^{\beta}_{k-1,u} & G^{\beta}_{k-1} & G^{\beta}_{k-1} & \cdots & G^{\beta}_{k-1} \end{array} \right),$$

The code generated by $G^{\beta}_{k,u}$ is denoted by $M^{\beta}_{k,u}$ and is called a **$\mathbb{Z}_{p^s}$-additive MacDonald code of type β** with $k \geq 2$ generators.

Example

Consider $\mathbb{Z}_4$. Then, we have that

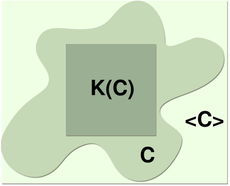
$$G^{\beta}_{3,1} = \left(\begin{array}{cccccc} 1111 & 1111 & 1111 & 1111 & 0000\cancel{0}0 & 222222 \\ 0000 & 1111 & 2222 & 3333 & 1111\cancel{0}2 & 111102 \\ 0123 & 0123 & 0123 & 0123 & 0123\cancel{1}1 & 012311 \end{array} \right).$$

Outline

1. Motivation
2. $\mathbb{Z}_{p^s}$-additive codes
3. $\mathbb{Z}_{p^s}$-additive simplex and MacDonald codes
   - Construction of $\mathbb{Z}_{p^s}$-additive simplex codes
   - Results for $\mathbb{Z}_{p^s}$-additive simplex codes
   - Construction of $\mathbb{Z}_{p^s}$-additive MacDonald codes
4. Future research

Future research

- Generalize the results for simplex codes defined over any finite chain ring.
- Study the weight distributions of $M^{\alpha}_{k,u}$ and $M^{\beta}_{k,u}$.
- Study the linearity of $\Phi_s(S^{\alpha}_k)$, $\Phi_s(S^{\beta}_k)$, as well as their kernel and rank.



Thank you for your attention!