Systematic encoding and permutation decoding for $\mathbb{Z}_{2^s}$-linear codes

Adrián Torres-Martín and Mercè Villanueva

Universitat Autònoma de Barcelona

Algebraic and Combinatorial Coding Theory

11-18 October 2020

Overview

Basic definitions

Basic definitions

Definition

A **code** C of length n over a finite field $\mathbb{F}_q$ is a nonempty subset of $\mathbb{F}_q^n$.

Definition

A code C with q^k codewords is **systematic** if there is a set I such that $|C_I| = q^k$. Such set I is called an **information set**.

Definition

A **systematic encoding** for I is an injective map $f : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, such that for any information vector $\mathbf{v} \in \mathbb{F}_q^k$, the codeword $f(\mathbf{v})$ satisfies $f(\mathbf{v})_I = \mathbf{v}$.

- Any linear code is systematic. In particular, it is permutation equivalent to a code with generator matrix in **standard form**:

$$G = \left(\begin{array}{c|c} Id_k & A \end{array} \right). \tag{1}$$

- The systematic encoding is just $f(\mathbf{v}) = \mathbf{v}G$.

$\mathbb{Z}_4$-linear codes

Linear codes over $\mathbb{Z}_4$

Definition

A $\mathbb{Z}_4$-additive code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$.

- A $\mathbb{Z}_4$-additive code may not be free as module (not always have basis).
- A $\mathbb{Z}_4$-additive code is isomorphic as a subgroup to $\mathbb{Z}_4^{t_1} \times \mathbb{Z}_2^{t_2}$. It is said to be of type $4^{t_1}2^{t_2}$ or (t_1, t_2).
- A $\mathbb{Z}_4$-additive code is permutation equivalent to a $\mathbb{Z}_4$-additive code with generator matrix in **standard form**:

$$\mathcal{G} = \begin{pmatrix} Id_{t_1} & A & B \\ \mathbf{0} & 2Id_{t_2} & 2C \end{pmatrix}. \quad (2)$$

- A $\mathbb{Z}_4$-additive code of type (t_1, t_2) can encode information vectors in the form $(\mathbf{b}_1, \mathbf{b}_2)$ where $\mathbf{b}_1 \in \mathbb{Z}_4^{t_1}$ and $\mathbf{b}_2 \in \mathbb{Z}_2^{t_2}$. The encoding consists then in the matrix multiplication $(\mathbf{b}_1, \mathbf{b}_2)\mathcal{G}$.

Gray map and $\mathbb{Z}_4$-linear codes

Definition

The **Gray map**, denoted by ϕ, maps $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ as follows:

$$\phi(0) = (0,0),\ \phi(1) = (0,1),\ \phi(2) = (1,1),\ \phi(3) = (1,0).$$

The coordinate-wise extension is denoted by Φ.

Definition

Let $\mathcal{C}$ be a $\mathbb{Z}_4$-additive code. Then the binary code $C = \Phi(\mathcal{C})$ is said to be a $\mathbb{Z}_4$-**linear code**.

- Note that a $\mathbb{Z}_4$-linear code may not be linear as a binary code.
- In 2014, a systematic encoding was presented for $\mathbb{Z}_4$-linear codes.

Systematic encoding for $\mathbb{Z}_4$-linear codes

1. Let $(\mathbf{a}_1, \mathbf{a}_2) \in \mathbb{Z}_2^{2t_1} \times \mathbb{Z}_2^{t_2}$ be the binary information vector.
2. Apply Φ^{-1} (which is bijective) to the $2t_1$ first coordinates $(\Phi^{-1}(\mathbf{a}_1), \mathbf{a}_2) = (\mathbf{b}_1, \mathbf{b}_2) \in \mathbb{Z}_4^{t_1} \times \mathbb{Z}_2^{t_2}$.
3. Apply $\sigma(\mathbf{b}_1, \mathbf{b}_2) = (\mathbf{b}_1, \mathbf{b}_2 - \psi(\mathbf{b}_1 A)) = (\mathbf{b}_1', \mathbf{b}_2')$, where $\psi : \mathbb{Z}_4$ to $\mathbb{Z}_2$.
4. Encode $(\mathbf{b}_1', \mathbf{b}_2')\mathcal{G} = (\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n) \in \mathcal{C} \subset \mathbb{Z}_4^n$.
5. Apply Φ and restrict to some coordinates J, to obtain again $(\mathbf{a}_1, \mathbf{a}_2) \in \mathbb{Z}_2^{2t_1} \times \mathbb{Z}_2^{t_2}$.

Systematic encoding for $\mathbb{Z}_4$-linear codes

Example

Consider the $\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $4^1 2^2$ with generator matrix in standard form:

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

1. Consider the binary information vector $(1,1,\ 0,1) \in \mathbb{Z}_2^2 \times \mathbb{Z}_2^2$.
2. Apply Φ^{-1}, and we have $(2,\ 0,1) \in \mathbb{Z}_4 \times \mathbb{Z}_2^2$.
3. Apply σ, and we obtain $\sigma(2,0,1) = (2,\ (0,1) - \psi(0,2)) = (2,\ 0,0)$.
4. The encoding $(2,0,1)\mathcal{G} = (2,0,0,2) \in \mathcal{C}$ is not systematic. However, after applying σ, the encoding $(2,0,0)\mathcal{G} = (2,0,2,2) \in \mathcal{C}$ is systematic.
5. Apply Φ and we have $(1,1,0,0,1,1,1,1)$. Then, we restrict to $\{1,2,3,5\}$ coordinates to obtain the information $(1,1,\ 0,1)$.

$\mathbb{Z}_{2^s}$-linear codes

Definition

A $\mathbb{Z}_{2^s}$-additive code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_{2^s}^n$.

- The $\mathbb{Z}_{2^s}$-additive codes may not be free as $\mathbb{Z}_{2^s}$-submodules.
- A $\mathbb{Z}_{2^s}$-additive code is isomorphic to $\mathbb{Z}_{2^s}^{t_1} \times \mathbb{Z}_{2^{s-1}}^{t_2} \times \cdots \times \mathbb{Z}_2^{t_s}$ and we say that the code is of **type** $(t_1, t_2, \ldots, t_s)$. Moreover, it is permutation equivalent to a $\mathbb{Z}_{2^s}$-additive code with generator matrix in **standard form**:

$$\mathcal{G} = \begin{pmatrix} Id_{t_1} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,s} \\ \mathbf{0} & 2Id_{t_2} & 2A_{1,2} & 2A_{1,3} & \cdots & \cdots & 2A_{1,s} \\ \mathbf{0} & \mathbf{0} & 4Id_{t_3} & 4A_{2,3} & \cdots & \cdots & 4A_{2,s} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & 2^{s-1}Id_{t_s} & 2^{s-1}A_{s-1,s} \end{pmatrix} \quad (3)$$

- A $\mathbb{Z}_{2^s}$-additive code of type $(t_1, t_2, \ldots, t_s)$ can encode information vectors in the form $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s)$ where $\mathbf{b}_i \in \mathbb{Z}_{2^{s+1-i}}^{t_i}$. The encoding consists then in the matrix multiplication $(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s)\mathcal{G}$.

Example

Consider the $\mathbb{Z}_8$-additive code of type $(2, 1, 1)$ with generator matrix in standard form:

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 3 & 1 & 4 & 6 \\ 0 & 1 & 5 & 4 & 2 & 7 \\ 0 & 0 & 2 & 6 & 2 & 2 \\ 0 & 0 & 0 & 4 & 0 & 4 \end{pmatrix}.$$

Consider an information vector $(7, 5, 3, 1) \in \mathbb{Z}_8^2 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. The corresponding codeword is $(7, 5, 3, 1)\mathcal{G} = (7, 5, 6, 4, 4, 7)$. Note that this encoding is not systematic.

Carlet's Gray map and $\mathbb{Z}_{2^s}$-linear codes

Definition

The **Gray map** generalization of Carlet is the map $\phi_s : \mathbb{Z}_{2^s} \longrightarrow \mathbb{Z}_2^{2^{s-1}}$, defined as

$$\phi_s(u) = (u_{s-1}, \ldots, u_{s-1}) + (u_0, \ldots, u_{s-2})Y_{s-1} \tag{4}$$

where $u \in \mathbb{Z}_{2^s}$ with $[u_0, \ldots, u_{s-1}]_2$ as its binary expansion and Y_{s-1} is a matrix whose columns are the elements of $\mathbb{Z}_2^{s-1}$. Let Φ_s be the coordinate-wise extension.

Definition

Let $\mathcal{C}$ be a $\mathbb{Z}_{2^s}$-additive code. Then the binary code $C = \Phi_s(\mathcal{C})$ is said to be a $\mathbb{Z}_{2^s}$-**linear code**.

- Note that a $\mathbb{Z}_{2^s}$-linear code may not be linear as a binary code.
- We generalize the systematic encoding presented for $\mathbb{Z}_4$-linear codes.

Systematic encoding for $\mathbb{Z}_{2^s}$-linear codes

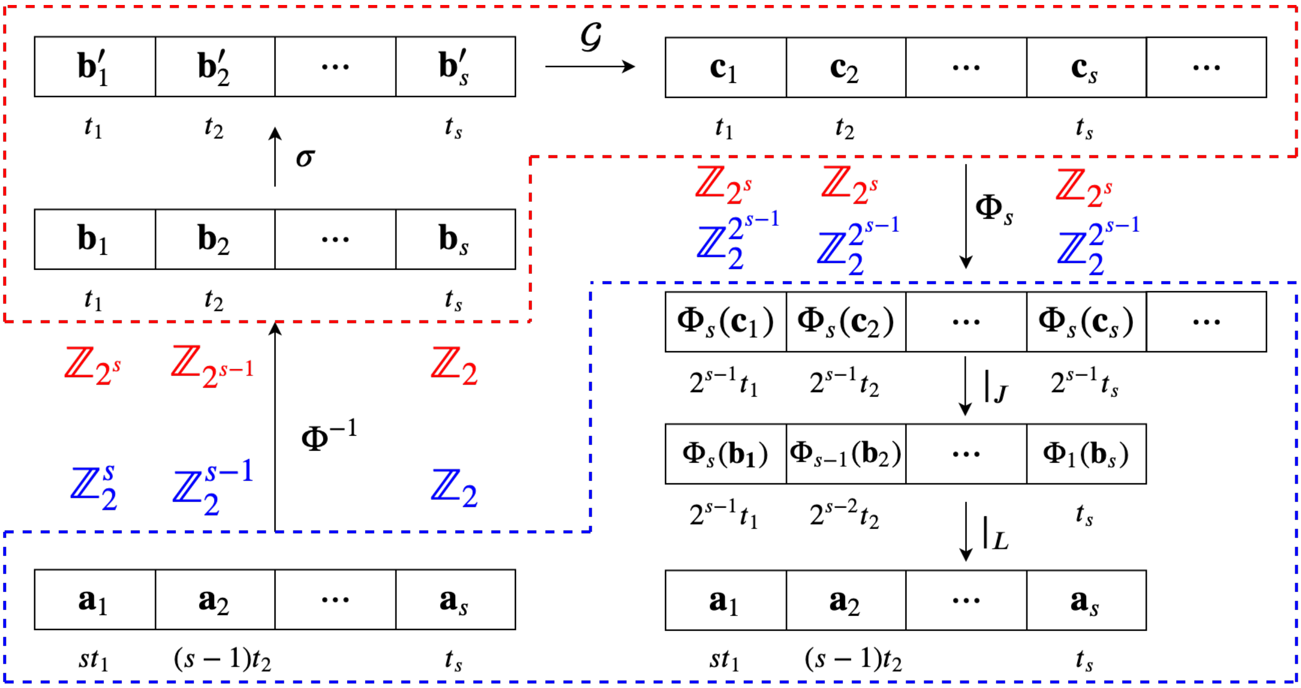

Figure: Schematic diagram of the systematic encoding

Systematic encoding for $\mathbb{Z}_{2^s}$-linear codes

Example

Consider the $\mathbb{Z}_8$-linear code $C = \Phi_3(\mathcal{C})$, where $\mathcal{C}$ is a $\mathbb{Z}_8$-additive code of type $(1,1,1)$ with generator matrix in standard form:

$$\mathcal{G} = \begin{pmatrix} 1 & 5 & 4 & 2 & 7 \\ 0 & 2 & 6 & 2 & 2 \\ 0 & 0 & 4 & 0 & 4 \end{pmatrix}.$$

Let $\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3) = (0,1,1,\ 1,0,\ 1)$ be an information vector.

$$\sigma(\Phi^{-1}(\mathbf{a}))\mathcal{G} = \sigma(3,3,1)\mathcal{G} = (3,0,0)\mathcal{G} = (3,7,5,6,5)$$

$$\phi_3(3)|_{\{1,2,3,4\}} = (0,1,1,0) \xrightarrow{|_{\{1,2,3\}}} (0,1,1)$$

$$\phi_3(7)|_{\{1,3\}} = (1,0,0,1)|_{\{1,3\}} = (1,0) \xrightarrow{|_{\{1,2\}}} (1,0)$$

$$\phi_3(5)|_{\{1\}} = (1,0,1,0)|_{\{1\}} = (1) \xrightarrow{|_{\{1\}}} (1).$$

Permutation decoding algorithm

Permutation decoding algorithm

- In 2014, an alternative Permutation Decoding method was introduced.
- It was designed to decode any binary code (linear or not), as long as it has a systematic encoding.

Definition

Let C be a t-error correcting code with information set I. Then a subset $S \subseteq \mathrm{PAut(C)}$ is a **PD-set** if for any vector $\mathbf{e}$ with $\mathrm{wt}(\mathbf{e}) \leq t$ there exists an element $\pi \in S$ such that $\mathrm{wt}(\pi(\mathbf{e})_I) = 0$.

Theorem

Let C be a binary systematic t-error-correcting code of length n. Let I be a set of systematic coordinates and let f be a systematic encoding for I. Suppose that $\mathbf{y} = \mathbf{x} + \mathbf{e}$ is a received vector, where $\mathbf{x} \in C$ and $\mathrm{wt}(\mathbf{e}) \leq t$. Then the systematic coordinates of $\mathbf{y}$ are correct iff $\mathrm{wt}(\mathbf{y} + f(\mathbf{y}_I)) \leq t$.

Permutation decoding algorithm

Example

Consider the $\mathbb{Z}_8$-additive code $\mathcal{C}$ with generator matrix

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 7 & 6 & 5 & 4 & 3 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

Let $C = \Phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_8$-linear code of type $(2, 0, 0)$ and error-correcting capability $t = 7$. The set $I = \{1, 2, 3, 5, 6, 7\}$ is an information set. Consider the information vector $\mathbf{a} = (1, 1, 0,\ 0, 1, 1)$.
Received vector:

$$\mathbf{y} = (1,0,1,0,0,0,1,0,0,0,0,0,1,0,1,0,0,0,1,1,1,0,0,1,1,1,1,1,0,1,0,1)$$

Restricting to I: $\mathbf{y}_I = (1, 0, 1, 0, 0, 1)$.

$$f(\mathbf{y}_I) = (0,1,0,1,0,0,1,1,0,1,1,0,1,1,1,1,1,0,1,0,1,1,0,0,1,0,0,1,0,0,0,0)$$

We have $\mathrm{wt}(\mathbf{y} + f(\mathbf{y}_I)) = 17 > 7 = t$.

Permutation decoding algorithm

Example

Consider the permutation of PAut(C):

$$\pi = (2,18)(3,19)(6,22)(7,23)(10,26)(11,27)(14,30)(15,31).$$

We have

$\pi(\mathbf{y}) = (1,0,1,0,0,0,0,0,0,1,1,0,1,1,0,0,0,0,1,1,1,0,1,1,1,0,0,1,0,0,1,1).$
$f(\pi(\mathbf{y})_I) = (1,0,1,0,0,0,0,0,0,1,1,0,1,1,0,0,0,1,0,1,1,1,1,1,1,0,0,1,0,0,1,1).$

We can see that $\mathrm{wt}(\pi(\mathbf{y}) + f(\pi(\mathbf{y})_I)) = 3 < 7 = t$. Therefore we decode

$$\pi^{-1}(f(\pi(\mathbf{y})_I)) \\ = (1,1,0,0,0,1,1,0,0,0,0,0,1,0,1,0,0,0,1,1,1,0,0,1,1,1,1,1,0,1,0,1)$$

and the information vector is $\mathbf{x}_I = (1,1,0,\ 0,1,1) = \mathbf{a}$.

Conclusions

Conclusions and further research

Conclusions

- We have found a systematic encoding for $\mathbb{Z}_{2^s}$-linear codes.
- We have shown how to use the alternative permutation decoding method for $\mathbb{Z}_{2^s}$-linear codes using this systematic encoding.

Further research

- To use the alternative permutation decoding method efficiently we need to find small enough PD-sets for families of $\mathbb{Z}_{2^s}$-linear codes.
- A MAGMA package for $\mathbb{Z}_{2^s}$-linear codes is already being developed. It will help to study $\mathbb{Z}_{2^s}$-linear codes and their PD-sets in more detail.
- A generalization of the systematic encoding may be applied to codes over $\mathbb{Z}_{p^s}$, where p is a prime, or over mixed alphabets $\mathbb{Z}_p\mathbb{Z}_{p^2}\dots\mathbb{Z}_{p^s}$.

Bibliography

- J. J. Bernal, J. Borges, C. Fernández-Córboda, and M. Villanueva, "Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes," Des. Codes and Cryptogr., vol. 76(2), pp. 269–277, 2015.
- C. Carlet, "$\mathbb{Z}_{2^k}$-linear codes," IEEE Trans. Inform. Theory, vol. 44(4), pp. 1543–1547, 1998.
- A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. S. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes," IEEE Trans. Inform. Theory, vol. 40(2), pp. 301–319, 1994.
- F. J. MacWilliams, "Permutation decoding of systematics codes," Bell System Tech. J., vol. 43, pp. 485–505, 1964.
- A. A. Nechaev, "The Kerdock code in a cyclic form," Discrete Math. Appl., vol. 1, pp. 365–384, 1991.

Thank you for your attention!