Reed-Muller codes: Information sets from defining sets*

José Joaquín Bernal and Juan Jacobo Simón

Universidad de Murcia
Spain

5ICMCTA 2017

*Supported by MINECO (MTM2016-77445) and Fundación Séneca of Murcia 19880/GERM/15

Outline

Introduction

Reed-Muller codes were introduced by D.E. Muller and I.S. Reed in 1954.

Introduction

Reed-Muller codes were introduced by D.E. Muller and I.S. Reed in 1954.

Structures
- Boolean functions (Polynomial codes)
- Geometric codes
- Group algebra codes (Affine-invariant codes)

Introduction

Looking for information sets:

- A. Blokhuis, G. E. Moorhouse: Some p-ranks related to orthogonal spaces. J. Algebraic Combin. vol. 4, 295-316 (1995)
- G. E. Moorhouse: Bruck nets, codes and characters of loops. Des. Codes Cryptogr. vol. 1, 7-29 (1991)
- J. D. Key, T. P. McDonough, V. C. Mavron: Partial permutation decoding for codes from finite planes. Eur. Journal of Combin. vol 26, 665-682 (2005)
- J. D. Key, T. P. McDonough, V. C. Mavron: Information sets and partial permutation decoding for codes from finite geometries. Finite fields and their applications, vol 12, 232-247 (2006)

Introduction

Looking for information sets:

- A. Blokhuis, G. E. Moorhouse: Some p-ranks related to orthogonal spaces. J. Algebraic Combin. vol. 4, 295-316 (1995)
- G. E. Moorhouse: Bruck nets, codes and characters of loops. Des. Codes Cryptogr. vol. 1, 7-29 (1991)
- J. D. Key, T. P. McDonough, V. C. Mavron: Partial permutation decoding for codes from finite planes. Eur. Journal of Combin. vol 26, 665-682 (2005)
- J. D. Key, T. P. McDonough, V. C. Mavron: Information sets and partial permutation decoding for codes from finite geometries. Finite fields and their applications, vol 12, 232-247 (2006)

Goal

To construct information sets for RM codes as Affine-Invariant codes

Affine-invariant codes

- $\mathbb{F}$ is the field with two elements

Affine-invariant codes

- $\mathbb{F}$ is the field with two elements
- G denotes the additive subgroup of the field with 2^m elements

Affine-invariant codes

- $\mathbb{F}$ is the field with two elements
- G denotes the additive subgroup of the field with 2^m elements
- α is a generator of the cyclic group $G^* = G \setminus \{0\}$

Affine-invariant codes

- $\mathbb{F}$ is the field with two elements
- G denotes the additive subgroup of the field with 2^m elements
- α is a generator of the cyclic group $G^* = G \setminus \{0\}$
- $n = 2^m - 1$

Affine-invariant codes

- $\mathbb{F}$ is the field with two elements
- G denotes the additive subgroup of the field with 2^m elements
- α is a generator of the cyclic group $G^* = G \setminus \{0\}$
- $n = 2^m - 1$

We consider the group algebra

$$\mathbb{F}G = \left\{ \sum_{g \in G} a_g X^g \mid a_g \in \mathbb{F} \right\}$$

Affine-invariant codes

- $\mathbb{F}$ is the field with two elements
- G denotes the additive subgroup of the field with 2^m elements
- α is a generator of the cyclic group $G^* = G \setminus \{0\}$
- $n = 2^m - 1$

We consider the group algebra

$$\mathbb{F}G = \left\{ \sum_{g \in G} a_g X^g \mid a_g \in \mathbb{F} \right\}$$

Remark. In terms of α we have $\mathbb{F}G = \{a_0 X^0 + \sum_{i=0}^{n-1} a_i X^{\alpha^i} \mid a_i \in \mathbb{F}\}$

Affine-invariant codes

Definition

A (linear) code $\mathcal{C} \subseteq \mathbb{F}G$ is an **extended cyclic code** if

$$\sum_{g \in G} a_g X^g \in \mathcal{C} \text{ implies } \left(\sum_{g \in G} a_g X^{\alpha g} \in \mathcal{C} \text{ and } \sum_{g \in G} a_g = 0 \right)$$

Affine-invariant codes

Definition

A (linear) code $\mathcal{C} \subseteq \mathbb{F}G$ is an **extended cyclic code** if

$$\sum_{g \in G} a_g X^g \in \mathcal{C} \text{ implies } \left(\sum_{g \in G} a_g X^{\alpha g} \in \mathcal{C} \text{ and } \sum_{g \in G} a_g = 0 \right)$$

Definition

An extended cyclic code $\mathcal{C} \subseteq \mathbb{F}G$ is **affine-invariant** if

$$\sum_{g \in G} a_g X^g \in \mathcal{C} \text{ implies } \sum_{g \in G} a_g X^{hg+k} \in \mathcal{C} \text{ for all } h, k \in G, h \neq 0$$

Affine-invariant codes

Definition

A (linear) code $\mathcal{C} \subseteq \mathbb{F}G$ is an **extended cyclic code** if

$$\sum_{g \in G} a_g X^g \in \mathcal{C} \text{ implies } \left(\sum_{g \in G} a_g X^{\alpha g} \in \mathcal{C} \text{ and } \sum_{g \in G} a_g = 0 \right)$$

Definition

An extended cyclic code $\mathcal{C} \subseteq \mathbb{F}G$ is **affine-invariant** if

$$\sum_{g \in G} a_g X^g \in \mathcal{C} \text{ implies } \sum_{g \in G} a_g X^{hg+k} \in \mathcal{C} \text{ for all } h, k \in G, h \neq 0$$

- $\mathcal{C}^* \subseteq \mathbb{F}G^*$ denotes the punctured code at X^0

Information sets in $\mathbb{F}G$

Definition

A set $\mathcal{I} \subseteq \{0, \alpha^0, \ldots, \alpha^{n-1}\}$ is an **information set** for a code $\mathcal{C} \subseteq \mathbb{F}G$, with dimension k, if $|\mathcal{I}| = k$ and $\mathcal{C}_{\mathcal{I}} = \mathbb{F}^k$.

The complementary set $\{0, \alpha^0, \ldots, \alpha^{n-1}\} \setminus \mathcal{I}$ is called a **set of check positions** for $\mathcal{C}$.

Information sets in $\mathbb{F}G$

Definition

A set $\mathcal{I} \subseteq \{0, \alpha^0, \ldots, \alpha^{n-1}\}$ is an **information set** for a code $\mathcal{C} \subseteq \mathbb{F}G$, with dimension k, if $|\mathcal{I}| = k$ and $\mathcal{C}_{\mathcal{I}} = \mathbb{F}^k$.

The complementary set $\{0, \alpha^0, \ldots, \alpha^{n-1}\} \setminus \mathcal{I}$ is called a **set of check positions** for $\mathcal{C}$.

Remarks.

- An information set for $\mathcal{C}$ is a set of check positions for $\mathcal{C}^\perp$ and vice versa

Information sets in $\mathbb{F}G$

Definition

A set $\mathcal{I} \subseteq \{0, \alpha^0, \ldots, \alpha^{n-1}\}$ is an **information set** for a code $\mathcal{C} \subseteq \mathbb{F}G$, with dimension k, if $|\mathcal{I}| = k$ and $\mathcal{C}_{\mathcal{I}} = \mathbb{F}^k$.

The complementary set $\{0, \alpha^0, \ldots, \alpha^{n-1}\} \setminus \mathcal{I}$ is called a **set of check positions** for $\mathcal{C}$.

Remarks.

- An information set for $\mathcal{C}$ is a set of check positions for $\mathcal{C}^\perp$ and vice versa
- Any information set for $\mathcal{C}^* \subseteq \mathbb{F}G^*$ will be a subset of $\{\alpha^0, \ldots, \alpha^{n-1}\}$

Information sets in $\mathbb{F}G$

Definition

A set $\mathcal{I} \subseteq \{0, \alpha^0, \ldots, \alpha^{n-1}\}$ is an **information set** for a code $\mathcal{C} \subseteq \mathbb{F}G$, with dimension k, if $|\mathcal{I}| = k$ and $\mathcal{C}_{\mathcal{I}} = \mathbb{F}^k$.

The complementary set $\{0, \alpha^0, \ldots, \alpha^{n-1}\} \setminus \mathcal{I}$ is called a **set of check positions** for $\mathcal{C}$.

Remarks.

- An information set for $\mathcal{C}$ is a set of check positions for $\mathcal{C}^\perp$ and vice versa
- Any information set for $\mathcal{C}^* \subseteq \mathbb{F}G^*$ will be a subset of $\{\alpha^0, \ldots, \alpha^{n-1}\}$
- An information set for $\mathcal{C}^*$ is also an information set for $\mathcal{C}$

Information sets in $\mathbb{F}G$

Definition

A set $\mathcal{I} \subseteq \{0, \alpha^0, \ldots, \alpha^{n-1}\}$ is an **information set** for a code $\mathcal{C} \subseteq \mathbb{F}G$, with dimension k, if $|\mathcal{I}| = k$ and $\mathcal{C}_{\mathcal{I}} = \mathbb{F}^k$.

The complementary set $\{0, \alpha^0, \ldots, \alpha^{n-1}\} \setminus \mathcal{I}$ is called a **set of check positions** for $\mathcal{C}$.

Remarks.

- An information set for $\mathcal{C}$ is a set of check positions for $\mathcal{C}^\perp$ and vice versa
- Any information set for $\mathcal{C}^* \subseteq \mathbb{F}G^*$ will be a subset of $\{\alpha^0, \ldots, \alpha^{n-1}\}$
- An information set for $\mathcal{C}^*$ is also an information set for $\mathcal{C}$
- If Γ is a set of check positions for $\mathcal{C}^*$ then $\Gamma \cup \{0\}$ is a set of check positions for $\mathcal{C}$.

Defining set

For any $s \in \{0, \ldots, n = 2^m - 1\}$ we consider the $\mathbb{F}$-linear map $\phi_s : \mathbb{F}G \to G$ given by

$$\phi_s \left(\sum_{g \in G} a_g X^g \right) = \sum_{g \in G} a_g g^s$$

where we assume that $0^0 = 1 \in \mathbb{F}$ by convention.

Defining set

For any $s \in \{0, \ldots, n = 2^m - 1\}$ we consider the $\mathbb{F}$-linear map $\phi_s : \mathbb{F}G \to G$ given by

$$\phi_s \left(\sum_{g \in G} a_g X^g \right) = \sum_{g \in G} a_g g^s$$

where we assume that $0^0 = 1 \in \mathbb{F}$ by convention.

Definition

Let $\mathcal{C} \subseteq \mathbb{F}G$ be an affine-invariant code. The set

$$D(\mathcal{C}) = \{i \mid \phi_i(x) = 0 \text{ for all } x \in \mathcal{C}\}$$

is called the **defining set** of $\mathcal{C}$.

Defining set

For any $s \in \{0, \ldots, n = 2^m - 1\}$ we consider the $\mathbb{F}$-linear map $\phi_s : \mathbb{F}G \to G$ given by

$$\phi_s\left(\sum_{g \in G} a_g X^g\right) = \sum_{g \in G} a_g g^s$$

where we assume that $0^0 = 1 \in \mathbb{F}$ by convention.

Definition

Let $\mathcal{C} \subseteq \mathbb{F}G$ be an affine-invariant code. The set

$$D(\mathcal{C}) = \{i \mid \phi_i(x) = 0 \text{ for all } x \in \mathcal{C}\}$$

is called the **defining set** of $\mathcal{C}$.

- $D(\mathcal{C}^*) := D(\mathcal{C}) \setminus \{0\}$

Reed-Muller codes

- For any natural number k its binary expansion is $\sum_{r\geq 0} k_r 2^r = k$ with $k_r = 0, 1$.

Reed-Muller codes

- For any natural number k its binary expansion is $\sum_{r\geq 0} k_r 2^r = k$ with $k_r = 0, 1$.
- The 2-weight or simply weight of k is $\mathrm{wt}(k) = \sum_{r\geq 0} k_r$

Reed-Muller codes

- For any natural number k its binary expansion is $\sum_{r\geq 0} k_r 2^r = k$ with $k_r = 0, 1$.
- The 2-weight or simply weight of k is $\mathrm{wt}(k) = \sum_{r\geq 0} k_r$

Definition

Given $0 \leq \rho \leq m$, the **Reed-Muller code of order ρ and length 2^m**, denoted by $R(\rho, m)$, is the affine-invariant code in $\mathbb{F}G$ with defining set

$$D(R(\rho, m)) = \{i \mid 0 \leq i < 2^m - 1 \text{ and } \mathrm{wt}(i) < m - \rho\}.$$

Reed-Muller codes

- For any natural number k its binary expansion is $\sum_{r\geq 0} k_r 2^r = k$ with $k_r = 0, 1$.
- The 2-weight or simply weight of k is $\mathrm{wt}(k) = \sum_{r\geq 0} k_r$

Definition

Given $0 \leq \rho \leq m$, the **Reed-Muller code of order ρ and length 2^m**, denoted by $R(\rho, m)$, is the affine-invariant code in $\mathbb{F}G$ with defining set

$$D(R(\rho, m)) = \{i \mid 0 \leq i < 2^m - 1 \text{ and } \mathrm{wt}(i) < m - \rho\}.$$

Remarks.

- The cases $\rho = 0, m$ are not considered

Reed-Muller codes

- For any natural number k its binary expansion is $\sum_{r\geq 0} k_r 2^r = k$ with $k_r = 0, 1$.
- The 2-weight or simply weight of k is $\mathrm{wt}(k) = \sum_{r\geq 0} k_r$

Definition

Given $0 \leq \rho \leq m$, the **Reed-Muller code of order ρ and length 2^m**, denoted by $R(\rho, m)$, is the affine-invariant code in $\mathbb{F}G$ with defining set

$$D(R(\rho, m)) = \{i \mid 0 \leq i < 2^m - 1 \text{ and } \mathrm{wt}(i) < m - \rho\}.$$

Remarks.

- The cases $\rho = 0, m$ are not considered
- $R(m-1, m)$ is the code of all even weight vectors in $\mathbb{F}G$ so we will assume that $\rho < m - 1$

Reed-Muller codes

- For any natural number k its binary expansion is $\sum_{r\geq 0} k_r 2^r = k$ with $k_r = 0, 1$.
- The 2-weight or simply weight of k is $\mathrm{wt}(k) = \sum_{r\geq 0} k_r$

Definition

Given $0 \leq \rho \leq m$, the **Reed-Muller code of order ρ and length 2^m**, denoted by $R(\rho, m)$, is the affine-invariant code in $\mathbb{F}G$ with defining set

$$D(R(\rho, m)) = \{i \mid 0 \leq i < 2^m - 1 \text{ and } \mathrm{wt}(i) < m - \rho\}.$$

Remarks.

- The cases $\rho = 0, m$ are not considered
- $R(m-1, m)$ is the code of all even weight vectors in $\mathbb{F}G$ so we will assume that $\rho < m - 1$
- $R(\rho, m)^\perp = R(m - \rho - 1, m)$

Reed-Muller codes

- For any natural number k its binary expansion is $\sum_{r\geq 0} k_r 2^r = k$ with $k_r = 0, 1$.
- The 2-weight or simply weight of k is $\mathrm{wt}(k) = \sum_{r\geq 0} k_r$

Definition

Given $0 \leq \rho \leq m$, the **Reed-Muller code of order ρ and length 2^m**, denoted by $R(\rho, m)$, is the affine-invariant code in $\mathbb{F}G$ with defining set

$$D(R(\rho, m)) = \{i \mid 0 \leq i < 2^m - 1 \text{ and } \mathrm{wt}(i) < m - \rho\}.$$

Remarks.

- The cases $\rho = 0, m$ are not considered
- $R(m-1, m)$ is the code of all even weight vectors in $\mathbb{F}G$ so we will assume that $\rho < m - 1$
- $R(\rho, m)^\perp = R(m - \rho - 1, m)$
- $R^*(\rho, m)$

Main problem

- How to obtain an information set for $R(\rho, m) \subseteq \mathbb{F}G$ from its defining set?

Main problem

- How to obtain an information set for $R(\rho, m) \subseteq \mathbb{F}G$ from its defining set?
- How to obtain an information set for $R(\rho.m) \subseteq \mathbb{F}G$ only in terms of its parameters?

Information sets for multidimensional cyclic codes

[BS]: J. J. Bernal, J. J. Simón: *Information sets from defining sets in abelian codes.* IEEE Trans. Inform. Theory, vol. 57, no. 12, 7990-7999 (2011)

Information sets for multidimensional cyclic codes

[BS]: J. J. Bernal, J. J. Simón: *Information sets from defining sets in abelian codes.* IEEE Trans. Inform. Theory, vol. 57, no. 12, 7990-7999 (2011)

Definition

A **multidimensional cyclic code** is an ideal of the polynomial algebra

$$\mathbb{A}(r_1, \ldots, r_l) = \mathbb{F}[X_1, \ldots, X_l] / \left\langle X_1^{r_1} - 1, \ldots, X_l^{r_l} - 1 \right\rangle$$

Information sets for multidimensional cyclic codes

[BS]: J. J. Bernal, J. J. Simón: *Information sets from defining sets in abelian codes.* IEEE Trans. Inform. Theory, vol. 57, no. 12, 7990-7999 (2011)

Definition

A **multidimensional cyclic code** is an ideal of the polynomial algebra

$$\mathbb{A}(r_1, \ldots, r_l) = \mathbb{F}[X_1, \ldots, X_l] / \left\langle X_1^{r_1} - 1, \ldots, X_l^{r_l} - 1 \right\rangle$$

An **information set** for a code $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_l)$ with dimension k is a set $\mathcal{I} \subseteq \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l}$ such that $|\mathcal{I}| = k$ and $\mathcal{C}_{\mathcal{I}} = \mathbb{F}^k$.

Defining sets for multidimensional cyclic codes

- R_i denotes the set of r_i-th roots of unity, $i = 1, \ldots, l$.
- The *root* set of $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_l)$ is

$$\mathcal{Z}(\mathcal{C}) = \left\{ (\beta_1, \ldots, \beta_l) \in \prod_{i=1}^{l} R_i \mid P(\beta_1, \ldots, \beta_l) = 0 \text{ for all } P \in \mathcal{C} \right\}.$$

Defining sets for multidimensional cyclic codes

- R_i denotes the set of r_i-th roots of unity, $i = 1, \ldots, l$.
- The *root* set of $\mathcal{C} \subseteq \mathbb{A}(r_1, \ldots, r_l)$ is

$$\mathcal{Z}(\mathcal{C}) = \left\{ (\beta_1, \ldots, \beta_l) \in \prod_{i=1}^{l} R_i \mid P(\beta_1, \ldots, \beta_l) = 0 \text{ for all } P \in \mathcal{C} \right\}.$$

Definition

Fixed $\{\alpha_1, \ldots, \alpha_l\}$, where α_i is a primitive r_i-th root of unity, $i = 1, \ldots, l$, the **defining set** of $\mathcal{C}$ with respect to $\{\alpha_1, \ldots, \alpha_l\}$ is

$$D_{\{\alpha_1, \ldots, \alpha_l\}}(\mathcal{C}) = \left\{ (a_1, \ldots, a_l) \in \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_l} \mid (\alpha_1^{a_1}, \ldots, \alpha_l^{a_l}) \in \mathcal{Z}(\mathcal{C}) \right\}.$$

General scheme

$$R(\rho, m) \subseteq \mathbb{F}G$$

General scheme

$$R(\rho, m) \subseteq \mathbb{F}G \quad \longrightarrow \quad R^*(\rho, m) \subseteq \mathbb{F}G^*$$

General scheme

$$R(\rho, m) \subseteq \mathbb{F}G \quad \longrightarrow \quad \begin{array}{c} R^*(\rho, m) \subseteq \mathbb{F}G^* \\ \downarrow \alpha \\ \mathcal{C}^* \subseteq \mathbb{A}(n) \end{array}$$

- α a primitive n-th root of unity. ($\mathbb{A}(n) = \mathbb{F}[X]/\langle X^n - 1\rangle$)

General scheme

$$\begin{array}{ccc} R(\rho, m) \subseteq \mathbb{F}G & \longrightarrow & R^*(\rho, m) \subseteq \mathbb{F}G^* \\ & & \downarrow \alpha \\ & & \mathcal{C}^* \subseteq \mathbb{A}(n) \end{array}$$

- α a primitive n-th root of unity. $(\mathbb{A}(n) = \mathbb{F}[X]/\langle X^n - 1\rangle)$
- $n = 2^m - 1 = r_1 \cdot r_2, \gcd(r_1, r_2) = 1,$

$$T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \text{ isomoprhism}$$

General scheme

$$\begin{array}{ccc} R(\rho, m) \subseteq \mathbb{F}G & \longrightarrow & R^*(\rho, m) \subseteq \mathbb{F}G^* \\ & & \downarrow \alpha \\ \mathcal{C} \subseteq \mathbb{A}(r_1, r_2) & \xleftarrow{T'} & \mathcal{C}^* \subseteq \mathbb{A}(n) \end{array}$$

- α a primitive n-th root of unity. $(\mathbb{A}(n) = \mathbb{F}[X]/\langle X^n - 1\rangle)$
- $n = 2^m - 1 = r_1 \cdot r_2, \gcd(r_1, r_2) = 1,$

$$T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \text{ isomoprhism}$$

- $D(\mathcal{C}) = T(D(\mathcal{C}^*))$
- $\mathcal{I}$ an information set for $\mathcal{C} \to T^{-1}(\mathcal{I})$ an information set for $\mathcal{C}^*$

General scheme

$$\begin{array}{ccc} R(\rho,m) \subseteq \mathbb{F}G & \longrightarrow & R^*(\rho,m) \subseteq \mathbb{F}G^* \\ \Uparrow & & \downarrow \alpha \\ \mathcal{C} \subseteq \mathbb{A}(r_1,r_2) & \xleftarrow{T'} & \mathcal{C}^* \subseteq \mathbb{A}(n) \end{array}$$

- α a primitive n-th root of unity. $(\mathbb{A}(n) = \mathbb{F}[X]/\langle X^n - 1\rangle)$
- $n = 2^m - 1 = r_1 \cdot r_2, \gcd(r_1, r_2) = 1,$

$$T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \text{ isomoprhism}$$

- $D(\mathcal{C}) = T(D(\mathcal{C}^*))$
- $\mathcal{I}$ an information set for $\mathcal{C} \to T^{-1}(\mathcal{I})$ an information set for $\mathcal{C}^*$

Information sets for first-order Reed-Muller codes

- $R(1, m)$

Information sets for first-order Reed-Muller codes

- $R(1, m)$
- $R(m-2, m)$

Information sets for first-order Reed-Muller codes

- $R(1, m)$
- $R(m-2, m) \longrightarrow \mathcal{D}(R^*(m-2, m)) = \{2^t \mid 0 \leq t < m\}$

Information sets for first-order Reed-Muller codes

- $R(1, m)$
- $R(m-2, m) \longrightarrow \mathcal{D}(R^*(m-2, m)) = \{2^t \mid 0 \leq t < m\}$
- $n = 2^m - 1 = r_1 \cdot r_2$ with $\gcd(r_1, r_2) = 1, r_1, r_2 > 1$

Information sets for first-order Reed-Muller codes

- $R(1, m)$
- $R(m-2, m) \longrightarrow \mathcal{D}(R^*(m-2, m)) = \{2^t \mid 0 \leq t < m\}$
- $n = 2^m - 1 = r_1 \cdot r_2$ with $\gcd(r_1, r_2) = 1, r_1, r_2 > 1$
- We fix α a n-th root of unity and $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ an isomoprhism

Information sets for first-order Reed-Muller codes

- $R(1, m)$
- $R(m-2, m) \longrightarrow \mathcal{D}(R^*(m-2, m)) = \{2^t \mid 0 \leq t < m\}$
- $n = 2^m - 1 = r_1 \cdot r_2$ with $\gcd(r_1, r_2) = 1, r_1, r_2 > 1$
- We fix α a n-th root of unity and $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ an isomoprhism

Theorem

Let $a = \mathrm{Ord}_{r_1}(2)$. Then the set $T^{-1}(\Gamma)$ where

$$\Gamma = \Gamma(\mathcal{C}) = \left\{(i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \mid 0 \leq i_1 < a, 0 \leq i_2 < \frac{m}{a}\right\}$$

is a set of check positions for $R^*(m-2, m)$. Furthermore,

A) $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ *is an information set for $R(1, m)$*

B) $\{\alpha^i \mid i \notin T^{-1}(\Gamma)\}$ *is an information set for $R(m-2, m)$*

Example $m = 6$

- In this case, $n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9, a = 3$.

Example $m = 6$

- In this case, $n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9, a = 3$.
- $\mathcal{D}(R^*(4,6)) = \{2^t \mid 0 \leq t < 6\} = \{1, 2, 4, 8, 16, 32\}$

Example $m = 6$

- In this case, $n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9, a = 3$.
- $\mathcal{D}(R^*(4,6)) = \{2^t \mid 0 \leq t < 6\} = \{1, 2, 4, 8, 16, 32\}$

$$\begin{array}{rcl} \Gamma & = & \{(i_1, i_2) \in \mathbb{Z}_7 \times \mathbb{Z}_9 \mid 0 \leq i_1 < 2, 0 \leq i_2 < 2\} \\ & = & \{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\} \end{array}$$

and then $T^{-1}(\Gamma) = \{0, 1, 9, 28, 36, 37\}$ (Chinese Remainder Theorem)

Example $m = 6$

- In this case, $n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9, a = 3$.
- $\mathcal{D}(R^*(4,6)) = \{2^t \mid 0 \leq t < 6\} = \{1, 2, 4, 8, 16, 32\}$

$$\begin{array}{rcl} \Gamma & = & \{(i_1, i_2) \in \mathbb{Z}_7 \times \mathbb{Z}_9 \mid 0 \leq i_1 < 2, 0 \leq i_2 < 2\} \\ & = & \{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\} \end{array}$$

and then $T^{-1}(\Gamma) = \{0, 1, 9, 28, 36, 37\}$ (Chinese Remainder Theorem)

Information sets

1. $\{0, 1, \alpha, \alpha^9, \alpha^{28}, \alpha^{36}, \alpha^{37}\}$ is an information set for $R(1,6)$

Example $m = 6$

- In this case, $n = 2^6 - 1 = 63, r_1 = 7, r_2 = 9, a = 3$.
- $\mathcal{D}(R^*(4,6)) = \{2^t \mid 0 \leq t < 6\} = \{1, 2, 4, 8, 16, 32\}$

$$\begin{array}{rcl} \Gamma & = & \{(i_1, i_2) \in \mathbb{Z}_7 \times \mathbb{Z}_9 \mid 0 \leq i_1 < 2, 0 \leq i_2 < 2\} \\ & = & \{(0,0), (1,0), (2,0), (0,1), (1,1), (2,1)\} \end{array}$$

and then $T^{-1}(\Gamma) = \{0, 1, 9, 28, 36, 37\}$ (Chinese Remainder Theorem)

Information sets

1. $\{0, 1, \alpha, \alpha^9, \alpha^{28}, \alpha^{36}, \alpha^{37}\}$ is an information set for $R(1,6)$
2. $\{\alpha^i \mid i \neq 0, 1, 9, 28, 36, 37\}$ is an information set for $R(4,6)$.

Example $m = 6$ (Continued)

Other information sets

T(1)	$T^{-1}(\Gamma)$
(1,1)	{0,1,9,28,36,37}
(2,1)	{0,1,18,36,46,72}
(1,2)	{0,9,14,23,36,50}
(2,2)	{0,14,18,32,36,50}
(3,1)	{0,10,19,28,45,54}

$\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ is an information set for $R(1, 6)$.

Information sets for second-order Reed-Muller codes

- $R(2, m)$

Information sets for second-order Reed-Muller codes

- $R(2, m)$
- $R(m-3, m)$

Information sets for second-order Reed-Muller codes

- $R(2, m)$
- $R(m-3, m)$

$$\longrightarrow \mathcal{D}(R^*(m-3, m)) = \{2^t \mid 0 \leq t < m\} \cup \{2^{t_1} + 2^{t_2} \mid 0 \leq t_1 < t_2 < m\}$$

Information sets for second-order Reed-Muller codes

- $R(2, m)$
- $R(m-3, m)$

  $\longrightarrow \mathcal{D}(R^*(m-3, m)) = \{2^t \mid 0 \leq t < m\} \cup \{2^{t_1} + 2^{t_2} \mid 0 \leq t_1 < t_2 < m\}$

- $n = 2^m - 1 = r_1 \cdot r_2$ with

  $$r_1 = 2^a - 1 \text{ and } \gcd(r_1, r_2) = 1, r_1, r_2 > 1$$

Information sets for second-order Reed-Muller codes

- $R(2, m)$
- $R(m-3, m)$

  $\longrightarrow \mathcal{D}(R^*(m-3, m)) = \{2^t \mid 0 \leq t < m\} \cup \{2^{t_1} + 2^{t_2} \mid 0 \leq t_1 < t_2 < m\}$

- $n = 2^m - 1 = r_1 \cdot r_2$ with

  $$r_1 = 2^a - 1 \text{ and } \gcd(r_1, r_2) = 1, r_1, r_2 > 1$$

- We fix α a n-th root of unity and $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ an isomorphism

Information sets for second-order Reed-Muller codes

Theorem

Let $m = ab$. Then the set $T^{-1}(\Gamma)$ where

$$\Gamma = \{(i_1, i_2) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \text{ such that } \left(0 \leq i_1 < \frac{a(a-1)}{2} \text{ and } 0 \leq i_2 < b^2\right) \text{ or } \left(\frac{a(a-1)}{2} \leq i_1 < \frac{a(a+1)}{2} \text{ and } 0 \leq i_2 < \frac{b(b+1)}{2}\right)\}$$

is a set of check positions for $R^*(m-3, m)$. Furthermore,

A) $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ *is an information set for* $R(2, m)$

B) $\{\alpha^i \mid i \notin T^{-1}(\Gamma)\}$ *is an information set for* $R(m-3, m)$.

Example $m = 8$

- In this case, $n = 2^8 - 1 = 255$.

Example $m = 8$

- In this case, $n = 2^8 - 1 = 255$.
- We choose the suitable decomposition $r_1 = 2^2 - 1 = 3, r_2 = 85$, so $a = 2$ and $b = 4$.

Example $m = 8$

- In this case, $n = 2^8 - 1 = 255$.
- We choose the suitable decomposition $r_1 = 2^2 - 1 = 3, r_2 = 85$, so $a = 2$ and $b = 4$.

$$\begin{aligned}\Gamma = & \{(i_1, i_2) \in \mathbb{Z}_3 \times \mathbb{Z}_{85} \text{ such that } (0 \leq i_1 < 1 \text{ and } 0 \leq i_2 < 16) \\ & \text{or } (1 \leq i_1 < 3 \text{ and } 0 \leq i_2 < 10)\} \\ = & \{(0,0), \ldots, (0,16), (1,0), \ldots, (1,9), (2,0), \ldots, (2,9)\}\end{aligned}$$

Example $m = 8$

- In this case, $n = 2^8 - 1 = 255$.
- We choose the suitable decomposition $r_1 = 2^2 - 1 = 3, r_2 = 85$, so $a = 2$ and $b = 4$.

$$\begin{aligned}\Gamma = & \{(i_1, i_2) \in \mathbb{Z}_3 \times \mathbb{Z}_{85} \text{ such that } (0 \leq i_1 < 1 \text{ and } 0 \leq i_2 < 16) \\ & \text{or } (1 \leq i_1 < 3 \text{ and } 0 \leq i_2 < 10)\} \\ = & \{(0,0), \ldots, (0,16), (1,0), \ldots, (1,9), (2,0), \ldots, (2,9)\}\end{aligned}$$

and then

$$\begin{aligned}T^{-1}(\Gamma) = & \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 85, 86, 87, 88, 89, 90, 91, 92, 93, \\ & 94, 96, 99, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 183\}.\end{aligned}$$

Example $m = 8$

- In this case, $n = 2^8 - 1 = 255$.
- We choose the suitable decomposition $r_1 = 2^2 - 1 = 3, r_2 = 85$, so $a = 2$ and $b = 4$.

$$\begin{aligned}\Gamma = & \{(i_1, i_2) \in \mathbb{Z}_3 \times \mathbb{Z}_{85} \text{ such that } (0 \leq i_1 < 1 \text{ and } 0 \leq i_2 < 16) \\ & \text{or } (1 \leq i_1 < 3 \text{ and } 0 \leq i_2 < 10)\} \\ = & \{(0,0), \ldots, (0,16), (1,0), \ldots, (1,9), (2,0), \ldots, (2,9)\}\end{aligned}$$

and then

$$\begin{aligned}T^{-1}(\Gamma) = & \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 85, 86, 87, 88, 89, 90, 91, 92, 93, \\ & 94, 96, 99, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 183\}.\end{aligned}$$

Information sets

1. $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ is an information set for $R(2, 8)$

Example $m = 8$

- In this case, $n = 2^8 - 1 = 255$.
- We choose the suitable decomposition $r_1 = 2^2 - 1 = 3, r_2 = 85$, so $a = 2$ and $b = 4$.

$$\begin{aligned}\Gamma = & \{(i_1, i_2) \in \mathbb{Z}_3 \times \mathbb{Z}_{85} \text{ such that } (0 \leq i_1 < 1 \text{ and } 0 \leq i_2 < 16) \\ & \text{or } (1 \leq i_1 < 3 \text{ and } 0 \leq i_2 < 10)\} \\ = & \{(0,0), \ldots, (0,16), (1,0), \ldots, (1,9), (2,0), \ldots, (2,9)\}\end{aligned}$$

and then

$$\begin{aligned}T^{-1}(\Gamma) = & \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 85, 86, 87, 88, 89, 90, 91, 92, 93, \\ & 94, 96, 99, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 183\}.\end{aligned}$$

Information sets

1. $\{0, \alpha^i \mid i \in T^{-1}(\Gamma)\}$ is an information set for $R(2, 8)$
2. $\{\alpha^i \mid i \notin T^{-1}(\Gamma)\}$ is an information set for $R(5, 8)$.

Example $m = 8$ (Continued)

r_1	r_2	a	$T^{-1}(\Gamma)$
3	85	2	{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 85, 86, 87, 88,89, 90, 91, 92, 93,94, 96, 99, 170, 171, 172, 173,174, 175, 176, 177, 178, 179, 180, 183 }
15	17	4	{ 0, 1, 2, 3, 17, 18, 19, 20, 34, 35, 36, 51, 52, 53, 68, 69,105, 120, 121, 122, 136,137, 138, 139, 153, 154, 155, 170,171, 172,187, 188, 189, 204,240, 241}

Information sets for $R(5, 8)$

Thank you very much for your attention!

Parameters for 2-nd order Reed-Muller codes

m	n	r_1	r_2	a	b
4	15	3	5	2	2
6	63	7	9	3	2
8	255	3	85	2	4
8	255	15	17	4	2
9	511	7	73	3	3
10	1023	3	341	2	5
12	4095	7	585	3	4
12	4095	63	65	6	2

Parameters for second order RM codes up to length 4096

Seeing $R^*(\rho, m)$ as a cyclic code

- $D(R^*(\rho, m)) = D(R(\rho, m)) \setminus \{0\}$
  $= \{i \mid 0 < i < 2^m - 1 \text{ and } \mathrm{wt}(i) < m - \rho\}.$

We fix α a n-th primitive root of unity. Then $R^*(\rho, m) \subseteq \mathbb{F}G^*$ is identified with a cyclic code $\mathcal{C}^* \subseteq \mathbb{A}(n) := \mathbb{F}[X]/\langle X^n - 1\rangle$ via the following map

$$\begin{array}{ccc} \mathbb{A}(n) & \longrightarrow & \mathbb{F}G \\ \displaystyle\sum_{i=0}^{n-1} a_i X^i & \mapsto & \displaystyle\left(-\sum_{i=0}^{n-1} a_i\right) X^0 + \sum_{i=0}^{n-1} a_i X^{\alpha^i}, \end{array}$$

Remarks.

- $\mathcal{D}(R^*(\rho, m)) \approx \mathcal{D}_\alpha(\mathcal{C}^*)$
- Inf. set for $\mathcal{C}^* \Leftrightarrow$ Inf. set for $R^*(\rho, m) \Rightarrow$ Inf. set for $R(\rho, m)$

Cyclic codes as 2-dimensional cyclic codes

1. $n = r_1 \cdot r_2, \gcd(r_1, r_2) = 1$. Then take $T : \mathbb{Z}_n \to \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$ isomorphism.
2. $\mathcal{C}^* \subseteq \mathbb{A}(n)$ cyclic with defining set $\mathcal{D}^*$ with respect to a primitive n-th root of unity α.
3. We consider $\mathcal{C} \subseteq \mathbb{A}(r_1, r_2) := \mathbb{F}[X_1, X_2]/\langle X_1^{r_1} - 1, X_2^{r_2} - 1\rangle$ the abelian code with defining set $T(\mathcal{D}^*)$ with respect to (β_1, β_2) where:

- Let η_1, η_2 be integers such that $\eta_1 r_1 + \eta_2 r_2 = 1$
- Define $\alpha_1 = \alpha^{\eta_2 r_2}, \alpha_2 = \alpha^{\eta_1 r_1}$
- Let $T(1) = (\delta_1, \delta_2)$.
- Define $(\beta_1, \beta_2) := (\alpha_1^{\delta_1^{-1}}, \alpha_1^{\delta_1^{-1}})$

Cyclic codes as 2-dimensional cyclic codes

$$\begin{array}{ccc} \mathbb{A}(n) & \xrightarrow{T'} & \mathbb{A}(r_1, r_2) \\ \sum a_i X^i & \mapsto & \sum b_{jl} X^j Y^l, \end{array}$$

where $b_{jl} = a_i$ if and only if $T(i) = (j, l)$.

- $T'(\mathcal{C}^*) = \mathcal{C}$
- If $\mathcal{I}$ is an information set for $\mathcal{C}$ then $T^{-1}(\mathcal{I})$ is an information set for $\mathcal{C}^*$.