Maximum Distance Separable Symbol-Pair Codes

ISIT 2012

Han Mao Kiah

Joint Work with: Yeow Meng Chee, Chengmin Wang

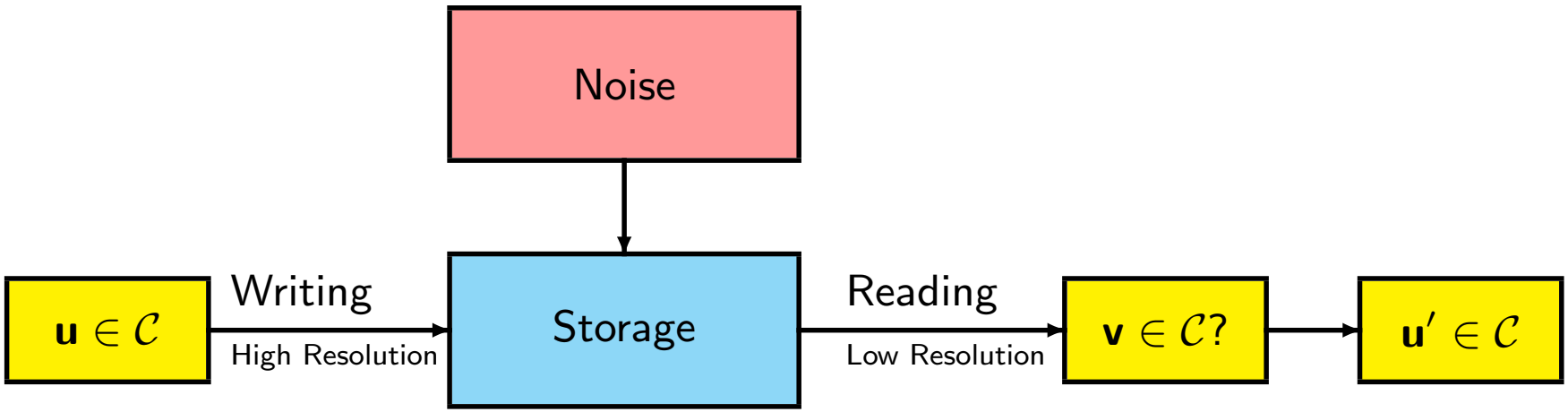
School of Physical and Mathematical Sciences,
Nanyang Technological University

6 Jul, 2012

Outline

Outline

Symbol-Pair Read Channel



A codeword

$$(u_0, u_1, \ldots, u_{n-1})$$

can only be read as

$$((u_0, u_1), (u_1, u_2), \ldots, (u_{n-1}, u_0)).$$

Pair-distance

Definition

Given $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$, $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$, the *pair-distance* between $\mathbf{u}$ and $\mathbf{v}$ is given by

$$D_{\mathrm{p}}(\mathbf{u}, \mathbf{v}) = |\{i : (u_i, u_{i+1}) \neq (v_i, v_{i+1})\}|.$$

Example

$$D_{\mathrm{p}}((0,0,0,0,0,0),(0,1,0,1,0,1)) = 6$$
$$D_{\mathrm{p}}((0,0,0,0,0,0),(0,0,0,1,1,1)) = 4$$

Theorem (Cassuto, Blaum '11)

If $0 < D_H(\mathbf{u}, \mathbf{v}) < n$,

$$D_H(\mathbf{u}, \mathbf{v}) + 1 \leq D_p(\mathbf{u}, \mathbf{v}) \leq 2D_H(\mathbf{u}, \mathbf{v}).$$

In the extreme cases in which $D_H(\mathbf{u}, \mathbf{v}) = 0$ *or* n, $D_p(\mathbf{u}, \mathbf{v}) = D_H(\mathbf{u}, \mathbf{v})$.

Outline

Singleton Bound

$\mathcal{C}$ is said to have *pair-distance* d if $D_{\mathrm{p}}(\mathbf{u}, \mathbf{v}) \geq d$ for all distinct $\mathbf{u}, \mathbf{v} \in \mathcal{C}$
Denote such a code by $(n, d)_q$-*symbol-pair code*.
The maximum size of an $(n, d)_q$-symbol-pair code is denoted $A_q^{\mathrm{p}}(n, d)$.

Theorem (Singleton Bound)

Let $q \geq 2$ and $2 \leq d \leq n$. Then

$$A_q^p(n, d) \leq q^{n-d+2}.$$

Hence, an $(n, d)_q$-symbol-pair code of size q^{n-d+2} is optimal and we call such a symbol-pair code *maximum distance separable* (MDS).

Outline

Trivial Fact

For distinct $\mathbf{u}, \mathbf{v}$, $D_{\mathrm{p}}(\mathbf{u}, \mathbf{v}) \geq 2$.

So, there exists an MDS $(n, 2)_q$-symbol-pair code for all $n \geq 2$ and $q \geq 2$.

Outline

From Classical MDS Codes

Proposition

An MDS $(n, d)_q$-code with $d < n$ is an MDS $(n, d+1)_q$-symbol-pair code.

Using Reed-Solomon codes, we have

Classical MDS	MDS Symbol-pair code
$(n, n-2)_q$ for $q = 2^m$, $n \leq q+2$	$(n, n-1)_q$ for $q = 2^m$, $n \leq q+2$
$(n, 4)_q$ for $q = 2^m$, $n \leq q+2$	$(n, 5)_q$ for $q = 2^m$, $n \leq q+2$
$(n, d)_q$ for q prime power, $3 \leq d \leq n-1$, $n \leq q+1$	$(n, d)_q$ for q prime power, $4 \leq d \leq n$, $n \leq q+1$
$(n, 2)_q$ for $n \geq 2$, $q \geq 2$	$(n, 3)_q$ for $n \geq 2$, $q \geq 2$

From Classical MDS Codes

Proposition

An MDS $(n, d)_q$-code with $d < n$ is an MDS $(n, d+1)_q$-symbol-pair code.

Theorem (Blanchard '93, '94, '95)

Let $2 \leq d \leq n$. Then there exists an MDS $(n, d)_q$-code for all q sufficiently large.

So, for $2 \leq d \leq n$, MDS $(n, d)_q$-symbol-pair codes exist for all q sufficiently large.

Outline

Interleaving Classical MDS Codes

Theorem (Cassuto and Blaum '11)

If there exist an $(n, d)_q$-code of size M_1 and an $(n, d)_q$-code of size M_2, then there exists a $(2n, 2d)_q$-symbol-pair code of size $M_1 M_2$.

Sketch of construction.

Take $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ from a $(n, d)_q$-code of size M_1 and $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ from a $(n, d)_q$-code of size M_2 to form the codeword,

$$(u_0, v_0, u_1, v_1, \ldots, u_{n-1}, v_{n-1}).$$

Repeat for all pairs $\mathbf{u}$, $\mathbf{v}$ to obtain the required code. □

Corollary

If there exists an MDS $(n, d)_q$-code, then there exists an MDS $(2n, 2d)_q$-symbol-pair code.

Outline

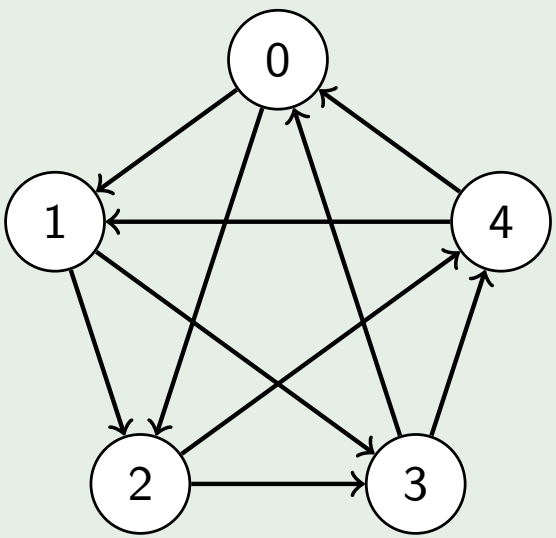
Extending Classical MDS Codes

Proposition

Suppose there exists an MDS $(n, d)_q$-code and there exists an eulerian graph of order n, size m and girth at least $n - d + 1$. Then there exists an MDS $(m, m - n + d + 1)_q$-symbol-pair code.

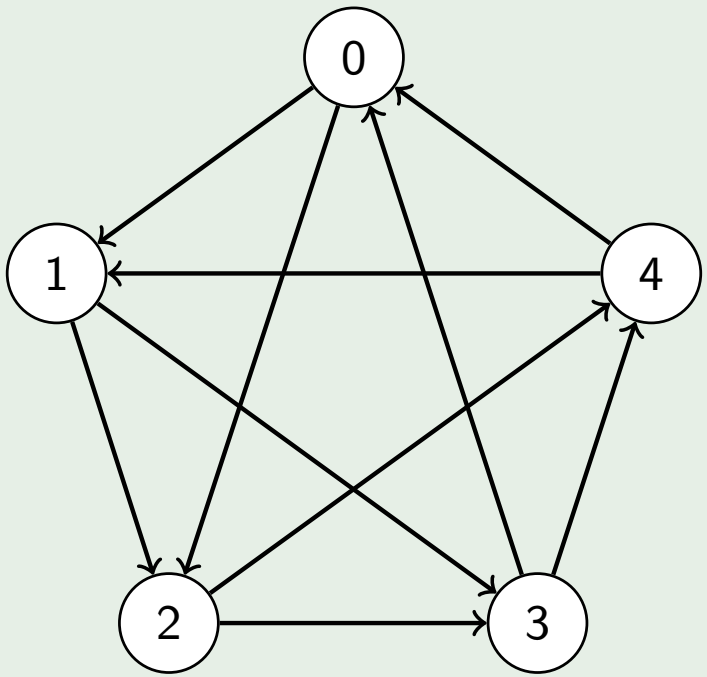
Example (Construction)

Extend MDS $(5, 3)_q$-code to obtain MDS $(10, 9)_q$-symbol-pair code using the following graph:



Example (Construction (ctd...))

Extend MDS $(5, 3)_q$-code to obtain MDS $(10, 9)_q$-symbol-pair code using the following graph:



$$(u_0, u_1, u_2, u_3, u_4) \mapsto (u_0, u_1, u_2, u_3, u_4, u_0, u_2, u_4, u_1, u_3)$$

Classical vs Symbol-Pair Codes

MDS Conjecture

If there exists a **linear** classical MDS $(n, d)_q$ code, then $n \leq q + 1$ or $q = 2^r$ and $d = 4$ or $d = q$, in which case $n \leq q + 2$.

Classical vs Symbol-Pair Codes

MDS Conjecture

If there exists a **linear** classical MDS $(n, d)_q$ code, then $n \leq q + 1$ or $q = 2^r$ and $d = 4$ or $d = q$, in which case $n \leq q + 2$.

- For any odd prime power q, there exists a classical MDS $(q, q - 2)_q$ code.

Classical vs Symbol-Pair Codes

MDS Conjecture

If there exists a **linear** classical MDS $(n, d)_q$ code, then $n \leq q + 1$ or $q = 2^r$ and $d = 4$ or $d = q$, in which case $n \leq q + 2$.

- For any odd prime power q, there exists a classical MDS $(q, q - 2)_q$ code.
- K_q is an eulerian graph of order q, size $q(q - 1)/2$ and girth 3.

Classical vs Symbol-Pair Codes

MDS Conjecture

If there exists a **linear** classical MDS $(n, d)_q$ code, then $n \leq q + 1$ or $q = 2^r$ and $d = 4$ or $d = q$, in which case $n \leq q + 2$.

- For any odd prime power q, there exists a classical MDS $(q, q-2)_q$ code.
- K_q is an eulerian graph of order q, size $q(q-1)/2$ and girth 3.
- So, there exists a MDS $(q(q-1)/2, q(q-1)/2 - 1)_q$-symbol-pair code.

Classical vs Symbol-Pair Codes

MDS Conjecture

If there exists a **linear** classical MDS $(n, d)_q$ code, then $n \leq q + 1$ or $q = 2^r$ and $d = 4$ or $d = q$, in which case $n \leq q + 2$.

- For any odd prime power q, there exists a classical MDS $(q, q-2)_q$ code.
- K_q is an eulerian graph of order q, size $q(q-1)/2$ and girth 3.
- So, there exists a MDS $(q(q-1)/2, q(q-1)/2 - 1)_q$-symbol-pair code.

Symbol-Pair Codes

There exists q-ary MDS symbol-pair codes of length $n = \Omega(q^2)$.

Outline

$\mathbb{Z}_q$-Linear Symbol-Pair Codes

Definition

A code $\mathcal{C}$ is said to be $\mathbb{Z}_q$-*linear* if $\mathbf{u}+\mathbf{v}, \lambda\mathbf{u} \in \mathcal{C}$ for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ and $\lambda \in \mathbb{Z}_q$.

The *pair-weight* of $\mathbf{u}$ is

$$\mathrm{wt}_{\mathrm{p}}(\mathbf{u}) = D_{\mathrm{p}}(\mathbf{u}, \mathbf{0}).$$

Lemma

Let $\mathcal{C}$ be a $\mathbb{Z}_q$-linear code. Then $\mathcal{C}$ has pair-distance $\min_{\mathbf{u} \in \mathcal{C} \setminus \{\mathbf{0}\}} \mathrm{wt}_{\mathrm{p}}(\mathbf{u})$.

MDS Symbol-Pair Codes with Distance Four

Proposition

Let $n \geq 4$ and define f and g as follows:

$$f : \mathbb{Z}_q^{n-2} \longrightarrow \mathbb{Z}_q$$
$$\mathbf{u} \longmapsto \sum_{i=0}^{n-3} (i+1)u_i,$$
$$g : \mathbb{Z}_q^{n-2} \longrightarrow \mathbb{Z}_q$$
$$\mathbf{u} \longmapsto \sum_{i=0}^{n-3} u_i.$$

Let $\mathcal{C} = \{(u_0, u_1, \ldots, u_{n-3}, f(\mathbf{u}), g(\mathbf{u})) : \mathbf{u} \in \mathbb{Z}_q^{n-2}\}$. Then $\mathcal{C}$ is a $\mathbb{Z}_q$-linear MDS $(n, 4)_q$-symbol-pair code.

MDS Symbol-Pair Codes with Distance Five

Proposition

Suppose that q is odd prime and $5 \leq n \leq 2q+3$. Define f, g and h as follows:

$$\begin{aligned} f : \mathbb{Z}_q^{n-3} &\longrightarrow \mathbb{Z}_q \\ \mathbf{u} &\longmapsto \sum_{i=0}^{n-4} (i+1)u_i, \\ g : \mathbb{Z}_q^{n-3} &\longrightarrow \mathbb{Z}_q \\ \mathbf{u} &\longmapsto \sum_{i=0}^{n-4} u_i. \\ h : \mathbb{Z}_q^{n-3} &\longrightarrow \mathbb{Z}_q \\ \mathbf{u} &\longmapsto \sum_{i=0}^{n-4} (-1)^i u_i. \end{aligned}$$

Let $\mathcal{C} = \{(u_0, u_1, \ldots, u_{n-4}, f(\mathbf{u}), g(\mathbf{u}), h(\mathbf{u})) : \mathbf{u} \in \mathbb{Z}_q^{n-3}\}$. Then $\mathcal{C}$ is a $\mathbb{Z}_q$-linear MDS $(n,5)_q$-symbol-pair code.

MDS Symbol-Pair Codes with Distance n

Proposition

Let $n \geq 2$ and let

$$\mathcal{C} = \begin{cases} \{(i,j,i,j,\ldots,i,j) : (i,j) \in \mathbb{Z}_q^2\}, & \text{if } n \text{ is even} \\ \{(i,j,i,j,\ldots,i,j,i+j) : (i,j) \in \mathbb{Z}_q^2\}, & \text{if } n \text{ is odd.} \end{cases}$$

Then $\mathcal{C}$ is a $\mathbb{Z}_q$-linear MDS $(n,n)_q$-symbol-pair code.

Outline

Cyclic Symbol-Pair Codes

Definition

$\mathcal{C}$ is *cyclic* if its automorphism group contains a cyclic group of order n. That is, $\mathcal{C}$ contains $(u_0, u_1, \ldots, u_{n-1})$ if and only if it also contains $(u_1, u_2, \ldots, u_{n-1}, u_0)$.

Example

The following code $\mathcal{C}$ is cyclic:

$$\begin{array}{lllll}
(0,0,0,0) & (1,1,1,1) & (2,2,2,2) & (3,3,3,3) & (4,4,4,4) \\
(0,1,2,3) & (0,2,1,4) & (0,3,4,2) & (0,4,3,1) & (1,3,2,4) \\
(3,0,1,2) & (4,0,2,1) & (2,0,3,4) & (1,0,4,3) & (4,1,3,2) \\
(2,3,0,1) & (1,4,0,2) & (4,2,0,3) & (3,1,0,4) & (2,4,1,3) \\
(1,2,3,0) & (2,1,4,0) & (3,4,2,0) & (4,3,1,0) & (3,2,4,1)
\end{array}$$

Furthermore, $\mathcal{C}$ is a MDS cyclic $(4,4)_5$-symbol-pair code.

Mendelsohn Designs

Let $\Sigma_*^n = \{\mathbf{u} \in \Sigma^n : u_0, u_1, \ldots, u_{n-1} \text{ are all distinct}\}$.
A vector $(u_0, u_1, u_2, \cdots, u_{n-1}) \in \Sigma_*^n$ is said to *cyclically contain* the ordered pairs $(u_0, u_1), (u_1, u_2), \cdots, (u_{n-1}, u_0)$.

Definition

A Mendelsohn design $\mathrm{M}(q, n)$ *is a pair* $(\Sigma, \mathcal{B})$, *where* $|\Sigma| = q$, $\mathcal{B} \subseteq \Sigma_*^n$, *such that each element of* Σ_*^2 *is cyclically contained in exactly one vector in* $\mathcal{B}$. *Elements of* $\mathcal{B}$ *are called* blocks.

Example

An $\mathrm{M}(5, 4)$:

$$\{(0, 1, 2, 3), (0, 2, 1, 4), (0, 3, 4, 2), (0, 4, 3, 1), (1, 3, 2, 4)\}$$

Construction of MDS Cyclic Symbol-Pair Codes from Mendelsohn Designs

Proposition

If there exists an $\mathrm{M}(q, n)$*, then there exists a cyclic MDS* $(n, n)_q$*-symbol-pair code.*

Sketch of Construction.

Let $\mathrm{M}(q, n) = (\Sigma, \mathcal{B})$. Check that $|\mathcal{B}| = q(q-1)/n$.

- For each $(u_0, u_1, \ldots, u_{n-1}) \in \mathcal{B}$, add all n cyclic shifts as codewords.
- For each $\sigma \in \Sigma$, add the codeword $(\sigma, \sigma, \ldots, \sigma)$.

This completes the construction. □

Example

	$(0,0,0,0)$	$(1,1,1,1)$	$(2,2,2,2)$	$(3,3,3,3)$	$(4,4,4,4)$
$\mathrm{M}(5,4):$	$(0,1,2,3)$	$(0,2,1,4)$	$(0,3,4,2)$	$(0,4,3,1)$	$(1,3,2,4)$
	$(3,0,1,2)$	$(4,0,2,1)$	$(2,0,3,4)$	$(1,0,4,3)$	$(4,1,3,2)$
	$(2,3,0,1)$	$(1,4,0,2)$	$(4,2,0,3)$	$(3,1,0,4)$	$(2,4,1,3)$
	$(1,2,3,0)$	$(2,1,4,0)$	$(3,4,2,0)$	$(4,3,1,0)$	$(3,2,4,1)$

Outline

Existence of MDS $(n, d)_q$-Symbol-Pair Codes

Determine the spectrum for MDS $(n, d)_q$-symbol-pair codes. That is, determine

$$Q(n, d) = \{q : \text{there exists a MDS } (n, d)_q\text{-symbol-pair code}\}.$$

Example

For $d \in \{2, 3, 4, n\}$,

$$Q(n, d) = \{q : q \geq 2\}.$$

Thank you for your attention!