Spherically punctured biorthogonal codes

Ilya Dumer Olga Kapralova

University of California

ACCT 2012

Presented by: Grigory Kabatyansky

Outline

1. Motivation and summary of results
2. Reed-Muller (RM) codes – review
3. Spherically punctured Hadamard codes
4. Precoding
5. Construction of good codes
6. Punctured biorthogonal codes on the sphere of radius b
7. Open problems

Motivation

- Polar codes can achieve channel capacity on very long blocks

- Consider a new class of codes
  - that is shorter
  - that keeps the polarization property – by using cancellation (recursive) decoding

Motivation

- Polar codes can achieve channel capacity on very long blocks

- Consider a new class of codes
  - that is shorter
  - that keeps the polarization property – by using cancellation (recursive) decoding

Summary

1. Consider a new class of punctured RM(r,m) codes with positions restricted to the points of the hypercube $\mathbb{F}_2^m$ that have some fixed Hamming weight
2. Codeword weight is determined by the weight of its information block. This dependence is based on the values of Krawtchouk polynomials and is rather nontrivial. Typically, the larger the input weight, the larger the output weight
3. Find parameters of punctured codes and show that the minimum weight codewords are obtained on the input weights 1 or 2
4. Precode information blocks in some simple code. This increases the weight of the input block and the obtained codeword at the expense of the code rate. Some codes attain the Griesmer bound
5. Prove some new facts about Krawtchouk polynomials

Summary

1. Consider a new class of punctured $\mathrm{RM}(r,m)$ codes with positions restricted to the points of the hypercube $\mathbb{F}_2^m$ that have some fixed Hamming weight
2. Codeword weight is determined by the weight of its information block. This dependence is based on the values of Krawtchouk polynomials and is rather nontrivial. Typically, the larger the input weight, the larger the output weight
3. Find parameters of punctured codes and show that the minimum weight codewords are obtained on the input weights 1 or 2
4. Precode information blocks in some simple code. This increases the weight of the input block and the obtained codeword at the expense of the code rate. Some codes attain the Griesmer bound
5. Prove some new facts about Krawtchouk polynomials

Summary

1. Consider a new class of punctured $\mathrm{RM}(r, m)$ codes with positions restricted to the points of the hypercube $\mathbb{F}_2^m$ that have some fixed Hamming weight
2. Codeword weight is determined by the weight of its information block. This dependence is based on the values of Krawtchouk polynomials and is rather nontrivial. Typically, the larger the input weight, the larger the output weight
3. Find parameters of punctured codes and show that the minimum weight codewords are obtained on the input weights 1 or 2
4. Precode information blocks in some simple code. This increases the weight of the input block and the obtained codeword at the expense of the code rate. Some codes attain the Griesmer bound
5. Prove some new facts about Krawtchouk polynomials

Summary

1. Consider a new class of punctured RM(r, m) codes with positions restricted to the points of the hypercube $\mathbb{F}_2^m$ that have some fixed Hamming weight
2. Codeword weight is determined by the weight of its information block. This dependence is based on the values of Krawtchouk polynomials and is rather nontrivial. Typically, the larger the input weight, the larger the output weight
3. Find parameters of punctured codes and show that the minimum weight codewords are obtained on the input weights 1 or 2
4. Precode information blocks in some simple code. This increases the weight of the input block and the obtained codeword at the expense of the code rate. Some codes attain the Griesmer bound
5. Prove some new facts about Krawtchouk polynomials

Summary

1. Consider a new class of punctured RM(r, m) codes with positions restricted to the points of the hypercube $\mathbb{F}_2^m$ that have some fixed Hamming weight
2. Codeword weight is determined by the weight of its information block. This dependence is based on the values of Krawtchouk polynomials and is rather nontrivial. Typically, the larger the input weight, the larger the output weight
3. Find parameters of punctured codes and show that the minimum weight codewords are obtained on the input weights 1 or 2
4. Precode information blocks in some simple code. This increases the weight of the input block and the obtained codeword at the expense of the code rate. Some codes attain the Griesmer bound
5. Prove some new facts about Krawtchouk polynomials

Reed-Muller [Reed'54, Muller'54] and Spherically Punctured Codes

Reed-Muller (RM) Codes $\mathcal{R}(r, m)$

- Polynomial structure:

  Messages: polynomials of degree at most r in m boolean variables
  Encoding: truth table

- Parameters:

  Length $n = 2^m$. Dimension $k = \sum_{i=0}^{r} \binom{m}{i}$. Minimum distance $d = 2^{m-r}$.

Spherically punctured RM Codes $P(r, m, b)$ on a sphere of radius b

- Polynomial structure:

  Messages: polynomials of degree at most r in m boolean variables
  Encoding: truth table punctured to positions $x = (x_1, \ldots, x_m)$ such that $\text{wt}(x) = b$

- Parameters:
  - Length $n = \binom{m}{b}$
  - Dimension and distance?

Reed-Muller [Reed'54, Muller'54] and Spherically Punctured Codes

Reed-Muller (RM) Codes $\mathcal{R}(r, m)$

- Polynomial structure:

  Messages: polynomials of degree at most r in m boolean variables
  Encoding: truth table

- Parameters:

  Length $n = 2^m$. Dimension $k = \sum_{i=0}^{r} \binom{m}{i}$. Minimum distance $d = 2^{m-r}$.

Spherically punctured RM Codes $P(r, m, b)$ on a sphere of radius b

- Polynomial structure:

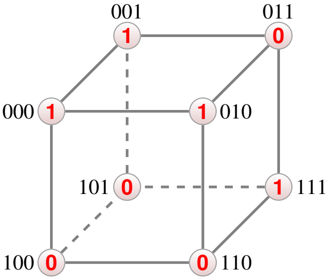
  Messages: polynomials of degree at most r in m boolean variables
  Encoding: truth table punctured to positions $x = (x_1, \ldots, x_m)$ such that $\text{wt}(x) = b$

- Parameters:
  - Length $n = \binom{m}{b}$
  - Dimension and distance?

Example: $m = 3$, $r = 2$

Message $f(x_1, x_2, x_3) = x_2x_3 + x_1 + 1$

Reed-Muller code $\mathcal{R}(2,3)$

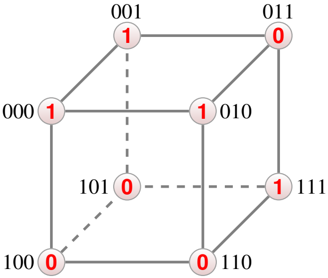


Codeword: (11100001)

Example: $m = 3,\, r = 2$

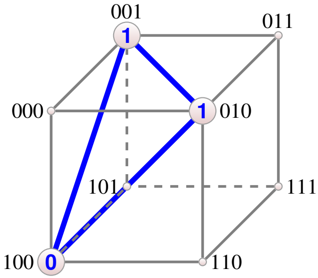
Message $f(x_1, x_2, x_3) = x_2x_3 + x_1 + 1$

Reed-Muller code $\mathcal{R}(2,3)$



Codeword: (11100001)

Spherically punctured code



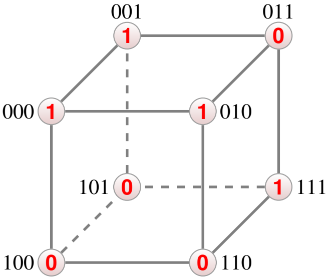
$P(2, 3, b = 1)$ codeword: (110)

$P(2, 3, b = 2)$ codeword: (000)

Example: $m = 3, r = 2$

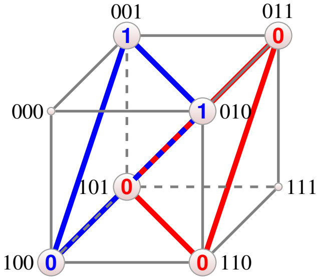
Message $f(x_1, x_2, x_3) = x_2x_3 + x_1 + 1$

Reed-Muller code $\mathcal{R}(2,3)$



Codeword: (11100001)

Spherically punctured code



$P(2,3,b=1)$ codeword: (110)

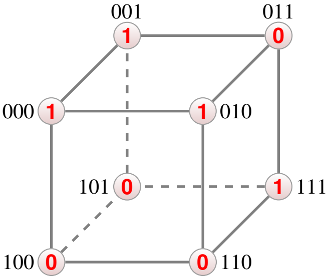
$P(2,3,b=2)$ codeword: (000)

Note: Non-zero $f(x)$ gives zero codeword

Example: $m = 3, r = 2$

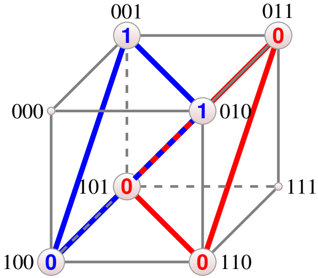
Message $f(x_1, x_2, x_3) = x_2x_3 + x_1 + 1$

Reed-Muller code $\mathcal{R}(2,3)$



Codeword: (11100001)

Spherically punctured code



$P(2,3,b=1)$ codeword: (110)

$P(2,3,b=2)$ codeword: (000)

Note: Non-zero $f(x)$ gives zero codeword

We now consider first order punctured codes $P(1,m,b)$

Spherically punctured Hadamard codes $H(m,b)$

The Hadamard codes $H(m)$:

- Formed by all linear functions of m variables

$$f(x_1,\ldots,x_m)=\sum_{i=1}^{m} f_i x_i \qquad f_i,x_i\in\{0,1\}$$

- Parameters: $n=2^m \quad k=m \quad d=2^{m-1}$

Definition

Spherically punctured Hadamard code $H(m,b)$ is the code $H(m)$ punctured to positions $x:\mathrm{wt}(x)=b$

The Hadamard code $H(4)$:

$$G_{H(4)}=\begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}$$

$n=16$

Spherically punctured Hadamard codes $H(m, b)$

The Hadamard codes $H(m)$:

- Formed by all linear functions of m variables

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} f_i x_i \qquad f_i, x_i \in \{0, 1\}$$

- Parameters: $n = 2^m \quad k = m \quad d = 2^{m-1}$

Definition

Spherically punctured Hadamard code $H(m, b)$ is the code $H(m)$ punctured to positions $x : \text{wt}(x) = b$

The Hadamard code $H(4)$:

$$G_{H(4)} = \begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}$$

$n = 16$

Spherically punctured Hadamard codes $H(m, b)$

The Hadamard codes $H(m)$:

- Formed by all linear functions of m variables

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} f_i x_i \qquad f_i, x_i \in \{0, 1\}$$

- Parameters: $n = 2^m \quad k = m \quad d = 2^{m-1}$

Definition

Spherically punctured Hadamard code $H(m, b)$ is the code $H(m)$ punctured to positions $x : \mathrm{wt}(x) = b$

The Hadamard code $H(4)$:

$$G_{H(4)} = \begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}$$

$n = 16$

Spherically punctured Hadamard codes $H(m, b)$

The Hadamard codes $H(m)$:

- Formed by all linear functions of m variables

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} f_i x_i \qquad f_i, x_i \in \{0, 1\}$$

- Parameters: $n = 2^m \quad k = m \quad d = 2^{m-1}$

Definition

Spherically punctured Hadamard code $H(m, b)$ is the code $H(m)$ punctured to positions x : wt$(x) = b$

The Hadamard code $H(4)$:

$$G_{H(4)} = \begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}$$

$n = 16$

Spherically punctured Hadamard codes $H(m,b)$

The Hadamard codes $H(m)$:

- Formed by all linear functions of m variables

$$f(x_1,\ldots,x_m)=\sum_{i=1}^{m} f_i x_i \qquad f_i, x_i \in \{0,1\}$$

- Parameters: $n=2^m \quad k=m \quad d=2^{m-1}$

Definition

Spherically punctured Hadamard code $H(m,b)$ is the code $H(m)$ punctured to positions $x : \mathrm{wt}(x)=b$

The Hadamard code $H(4)$:

$$G_{H(4)}=\begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}$$

$n=16$

The Punctured Hadamard code $H(4,2)$:

$$G_{H(4,2)}=\begin{bmatrix} 0&0&0&1&1&1\\ 0&1&1&0&0&1\\ 1&0&1&0&1&0\\ 1&1&0&1&0&0 \end{bmatrix}$$

$n=\binom{4}{2}=6$

The Punctured Hadamard code $H(m,2)$

Consider code $H(m,2)$. Ease to see that

- $H(m,2)$ has length $\binom{m}{2}$
- Codeword weight is determined by message weight

Lemma

Let $f(x) = \sum_{i=1}^{m} f_i x_i$ be a message such that wt$(f_1, f_2, \ldots, f_m) = w$.
Then codeword weight is $w(m-w)$

Pick x : wt$(x) = 2$

$$\begin{matrix} x_i \rightarrow \\ \\ x_j \rightarrow \end{matrix} \begin{bmatrix} 1 \\ \\ 1 \end{bmatrix}$$

The Punctured Hadamard code $H(m, 2)$

Consider code $H(m, 2)$. Ease to see that

- $H(m, 2)$ has length $\binom{m}{2}$
- Codeword weight is determined by message weight

Lemma

Let $f(x) = \sum_{i=1}^{m} f_i x_i$ *be a message such that* $wt(f_1, f_2, \ldots, f_m) = w$.
Then codeword weight is $w(m - w)$

Pick $x : \mathrm{wt}(x) = 2$

$$\begin{matrix} x_i \rightarrow \\ \\ x_j \rightarrow \end{matrix} \begin{bmatrix} 1 \\ \\ 1 \end{bmatrix}$$

The Punctured Hadamard code $H(m,2)$

Consider code $H(m,2)$. Ease to see that

- $H(m,2)$ has length $\binom{m}{2}$
- Codeword weight is determined by message weight

Lemma

Let $f(x) = \sum_{i=1}^{m} f_i x_i$ *be a message such that* wt$(f_1, f_2, \ldots, f_m) = w$.
Then codeword weight is $w(m-w)$

Pick x : wt$(x) = 2$

$$\begin{matrix} x_i \rightarrow \\ \\ x_j \rightarrow \end{matrix} \begin{bmatrix} 1 \\ \\ 1 \end{bmatrix}$$

The Punctured Hadamard code $H(m,2)$

Consider code $H(m,2)$. Ease to see that

- $H(m,2)$ has length $\binom{m}{2}$
- Codeword weight is determined by message weight

Lemma

Let $f(x) = \sum_{i=1}^{m} f_i x_i$ *be a message such that wt*$(f_1, f_2, \ldots, f_m) = w$.
Then codeword weight is $w(m-w)$

Pick $x : \text{wt}(x) = 2$

$$\begin{matrix} x_i \rightarrow \\ \\ x_j \rightarrow \end{matrix} \begin{bmatrix} 1 \\ \\ 1 \end{bmatrix}$$

The Punctured Hadamard code $H(m,2)$

Consider code $H(m,2)$. Ease to see that

- $H(m,2)$ has length $\binom{m}{2}$
- Codeword weight is determined by message weight

Lemma

Let $f(x) = \sum_{i=1}^{m} f_i x_i$ be a message such that wt$(f_1, f_2, \ldots, f_m) = w$.
Then codeword weight is $w(m-w)$

Pick $x : \text{wt}(x) = 2 \quad f : \text{wt}(f) = w$

The Punctured Hadamard code $H(m,2)$

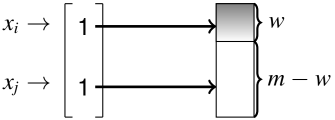
Consider code $H(m,2)$. Ease to see that

- $H(m,2)$ has length $\binom{m}{2}$
- Codeword weight is determined by message weight

Lemma

Let $f(x) = \sum_{i=1}^{m} f_i x_i$ *be a message such that wt*$(f_1, f_2, \ldots, f_m) = w$*.*
Then codeword weight is $w(m-w)$

Pick $x : \text{wt}(x) = 2 \quad f : \text{wt}(f) = w$



- Thus, $f(x) = 1$ if $f_i \neq f_j$
- The # of such x is $w(m-w)$

The Punctured Hadamard code $H(m,2)$

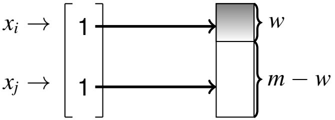
Consider code $H(m,2)$. Ease to see that

- $H(m,2)$ has length $\binom{m}{2}$
- Codeword weight is determined by message weight

Lemma

Let $f(x) = \sum_{i=1}^{m} f_i x_i$ *be a message such that wt*$(f_1, f_2, \ldots, f_m) = w$.
Then codeword weight is $w(m-w)$

Pick $x : \mathrm{wt}(x) = 2$ $\quad f : \mathrm{wt}(f) = w$



- Thus, $f(x) = 1$ if $f_i \neq f_j$
- The $\#$ of such x is $w(m-w)$

Corollary

- *Minimum distance of* $H(m,2)$ *is* $m-1$ *and is achieved at* $w = 1$
- *Dimension of* $H(m,2)$ *is* $m-1$ *(vector with* $w = m$ *gives zero codeword)*

Precoding

Motivating example:

- Consider code $H(m,\{1,2\})$ on spheres of radii $b=1,2$
- Message weight w
- Codeword weight $w + w(m-w)$

$$G_{H(4,\{1,2\})} = \left[\begin{array}{cccc|cccccc} 1&0&0&0&0&0&0&1&1&1\\ 0&1&0&0&0&1&1&0&0&1\\ 0&0&1&0&1&0&1&0&1&0\\ 0&0&0&1&1&1&0&1&0&0 \end{array}\right]$$

$\underbrace{\quad}_{b=1}$ $\underbrace{\quad}_{b=2}$

For example:

- if input alphabet is $\mathbb{F}_2^m$, then $d(m,\{1,2\}) = m$
- if input alphabet is parity check code $G[m,m-1,2]$, then $d(m,\{1,2\}) = 2m-2$

General scheme:

$$u \in \mathbb{F}_2^k \xrightarrow{\text{Precoding}} g \in \mathbf{G} \xrightarrow{H(m,B)} y \in H_{\mathbf{G}}(m,B)$$

Precoding

Motivating example:

- Consider code $H(m,\{1,2\})$ on spheres of radii $b=1,2$
- Message weight w
- Codeword weight $w+w(m-w)$

$$G_{H(4,\{1,2\})}=\left[\begin{array}{cccc|cccccc}1&0&0&0&0&0&0&1&1&1\\0&1&0&0&0&1&1&0&0&1\\0&0&1&0&1&0&1&0&1&0\\0&0&0&1&1&1&0&1&0&0\end{array}\right]$$

$$\underbrace{\qquad\qquad}_{b=1}\underbrace{\qquad\qquad\qquad}_{b=2}$$

For example:

- if input alphabet is $\mathbb{F}_2^m$, then $d(m,\{1,2\})=m$
- if input alphabet is parity check code $G[m,m-1,2]$, then $d(m,\{1,2\})=2m-2$

General scheme:

$$u\in\mathbb{F}_2^k \xrightarrow{\text{Precoding}} g\in\mathbf{G} \xrightarrow{H(m,B)} y\in H_{\mathbf{G}}(m,B)$$

Precoding

Motivating example:

- Consider code $H(m, \{1,2\})$ on spheres of radii $b = 1, 2$
- Message weight w
- Codeword weight $w + w(m - w)$

$$G_{H(4,\{1,2\})} = \underbrace{\left[\begin{array}{cccc|cccccc} 1&0&0&0&0&0&0&1&1&1 \\ 0&1&0&0&0&1&1&0&0&1 \\ 0&0&1&0&1&0&1&0&1&0 \\ 0&0&0&1&1&1&0&1&0&0 \end{array}\right]}_{b=1 \quad\quad b=2}$$

For example:

- if input alphabet is $\mathbb{F}_2^m$, then $d(m, \{1,2\}) = m$
- if input alphabet is parity check code $G[m, m-1, 2]$, then $d(m, \{1,2\}) = 2m - 2$

General scheme:

$$u \in \mathbb{F}_2^k \xrightarrow{\text{Precoding}} g \in \mathbf{G} \xrightarrow{H(m,B)} y \in H_{\mathbf{G}}(m, B)$$

Precoding

Motivating example:

- Consider code $H(m, \{1,2\})$ on spheres of radii $b = 1, 2$
- Message weight w
- Codeword weight $w + w(m - w)$

$$G_{H(4,\{1,2\})} = \left[\begin{array}{cccc|cccccc} 1&0&0&0&0&0&0&1&1&1 \\ 0&1&0&0&0&1&1&0&0&1 \\ 0&0&1&0&1&0&1&0&1&0 \\ 0&0&0&1&1&1&0&1&0&0 \end{array}\right]$$

$\underbrace{}_{b=1}\ \underbrace{}_{b=2}$

The more concentrated the input spectrum, the higher the minimum distance $d(m, \{1,2\})$

For example:

- if input alphabet is $\mathbb{F}_2^m$, then $d(m, \{1,2\}) = m$
- if input alphabet is parity check code $G[m, m-1, 2]$, then $d(m, \{1,2\}) = 2m - 2$

General scheme:

$$u \in \mathbb{F}_2^k \xrightarrow{\text{Precoding}} g \in \mathbf{G} \xrightarrow{H(m,B)} y \in H_{\mathbf{G}}(m, B)$$

Precoding

Motivating example:

- Consider code $H(m,\{1,2\})$ on spheres of radii $b=1,2$
- Message weight w
- Codeword weight $w+w(m-w)$

$$G_{H(4,\{1,2\})} = \underbrace{\left[\begin{array}{cccc|cccccc} 1&0&0&0&0&0&0&1&1&1\\ 0&1&0&0&0&1&1&0&0&1\\ 0&0&1&0&1&0&1&0&1&0\\ 0&0&0&1&1&1&0&1&0&0 \end{array}\right.}_{b=1}\underbrace{\left.\begin{array}{c}\end{array}\right]}_{b=2}$$

The more concentrated the input spectrum, the higher the minimum distance $d(m,\{1,2\})$

For example:

- if input alphabet is $\mathbb{F}_2^m$, then $d(m,\{1,2\})=m$
- if input alphabet is parity check code $G[m,m-1,2]$, then $d(m,\{1,2\})=2m-2$

General scheme:

$$u\in\mathbb{F}_2^k \xrightarrow{\text{Precoding}} g\in\mathbf{G} \xrightarrow{H(m,B)} y\in H_{\mathbf{G}}(m,B)$$

Precoding

Motivating example:

- Consider code $H(m, \{1,2\})$ on spheres of radii $b = 1, 2$
- Message weight w
- Codeword weight $w + w(m - w)$

$$G_{H(4,\{1,2\})} = \underbrace{\left[\begin{array}{cccc|cccccc} 1&0&0&0&0&0&0&1&1&1 \\ 0&1&0&0&0&1&1&0&0&1 \\ 0&0&1&0&1&0&1&0&1&0 \\ 0&0&0&1&1&1&0&1&0&0 \end{array}\right]}_{b=1 \qquad b=2}$$

The more concentrated the input spectrum, the higher the minimum distance $d(m, \{1,2\})$

For example:

- if input alphabet is $\mathbb{F}_2^m$, then $d(m, \{1,2\}) = m$
- if input alphabet is parity check code $G[m, m-1, 2]$, then $d(m, \{1,2\}) = 2m - 2$

General scheme:

$$u \in \mathbb{F}_2^k \xrightarrow{\text{Precoding}} g \in \mathbf{G} \xrightarrow{H(m,B)} y \in H_{\mathbf{G}}(m, B)$$

Precoding

Motivating example:

- Consider code $H(m, \{1,2\})$ on spheres of radii $b = 1, 2$
- Message weight w
- Codeword weight $w + w(m-w)$

$$G_{H(4,\{1,2\})} = \underbrace{\left[\begin{array}{cccc|cccccc} 1&0&0&0&0&0&0&1&1&1 \\ 0&1&0&0&0&1&1&0&0&1 \\ 0&0&1&0&1&0&1&0&1&0 \\ 0&0&0&1&1&1&0&1&0&0 \end{array}\right]}_{b=1 \quad\quad b=2}$$

The more concentrated the input spectrum, the higher the minimum distance $d(m, \{1,2\})$

For example:

- if input alphabet is $\mathbb{F}_2^m$, then $d(m, \{1,2\}) = m$
- if input alphabet is parity check code $G[m, m-1, 2]$, then $d(m, \{1,2\}) = 2m - 2$

General scheme:

$$u \in \mathbb{F}_2^k \xrightarrow{\text{Precoding}} g \in \mathbf{G} \xrightarrow{H(m,B)} y \in H_{\mathbf{G}}(m, B)$$

Precoding allows to build codes that attain Griesmer bound

Griesmer bound: for linear $[n,k,d]$ binary code $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$

Lemma

Let $G(s) = [2^s - 1, s, 2^{s-1}]$ be the shortened RM$(1,s)$ code. Then $H_{G(s)}(2^s - 1, \{1,2\})$ meets the Griesmer bound

- $H_{G(s)}(2^s - 1, \{1,2\})$ has dimension s
- $H_{G(s)}(2^s - 1, \{1,2\})$ has length $2^{2s-1} - 2^{s-1}$
- Each precoded message has weight 2^{s-1}
- Each codeword has weight 2^{2s-2}

Also, $H_{G(s)}(2^s - 1, B)$ for $B = \{1, 2, 2^s - 2, 2^s - 3\}$ (or any its subset) attains the Griesmer bound

Precoding allows to build codes that attain Griesmer bound

Griesmer bound: for linear $[n,k,d]$ binary code $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$

Lemma

Let $G(s) = [2^s - 1, s, 2^{s-1}]$ be the shortened RM$(1,s)$ code. Then $H_{G(s)}(2^s - 1, \{1,2\})$ meets the Griesmer bound

- $H_{G(s)}(2^s - 1, \{1,2\})$ has dimension s
- $H_{G(s)}(2^s - 1, \{1,2\})$ has length $2^{2s-1} - 2^{s-1}$
- Each precoded message has weight 2^{s-1}
- Each codeword has weight 2^{2s-2}

Also, $H_{G(s)}(2^s - 1, B)$ for $B = \{1, 2, 2^s - 2, 2^s - 3\}$ (or any its subset) attains the Griesmer bound

Precoding allows to build codes that attain Griesmer bound

Griesmer bound: for linear $[n, k, d]$ binary code $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$

Lemma

Let $G(s) = [2^s - 1, s, 2^{s-1}]$ be the shortened RM$(1, s)$ code. Then $H_{G(s)}(2^s - 1, \{1, 2\})$ meets the Griesmer bound

- $H_{G(s)}(2^s - 1, \{1, 2\})$ has dimension s
- $H_{G(s)}(2^s - 1, \{1, 2\})$ has length $2^{2s-1} - 2^{s-1}$
- Each precoded message has weight 2^{s-1}
- Each codeword has weight 2^{2s-2}

Also, $H_{G(s)}(2^s - 1, B)$ for $B = \{1, 2, 2^s - 2, 2^s - 3\}$ (or any its subset) attains the Griesmer bound

Precoding allows to build codes that attain Griesmer bound

Griesmer bound: for linear $[n,k,d]$ binary code $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil$

Lemma

Let $G(s) = [2^s - 1, s, 2^{s-1}]$ be the shortened RM$(1,s)$ code. Then $H_{G(s)}(2^s - 1, \{1,2\})$ meets the Griesmer bound

- $H_{G(s)}(2^s - 1, \{1,2\})$ has dimension s
- $H_{G(s)}(2^s - 1, \{1,2\})$ has length $2^{2s-1} - 2^{s-1}$
- Each precoded message has weight 2^{s-1}
- Each codeword has weight 2^{2s-2}

Also, $H_{G(s)}(2^s - 1, B)$ for $B = \{1, 2, 2^s - 2, 2^s - 3\}$ (or any its subset) attains the Griesmer bound

Precoding allows to build codes that attain Griesmer bound

Griesmer bound: for linear $[n,k,d]$ binary code $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$

Lemma

Let $G(s) = [2^s - 1, s, 2^{s-1}]$ be the shortened RM$(1,s)$ code. Then $H_{G(s)}(2^s - 1, \{1,2\})$ meets the Griesmer bound

- $H_{G(s)}(2^s - 1, \{1,2\})$ has dimension s
- $H_{G(s)}(2^s - 1, \{1,2\})$ has length $2^{2s-1} - 2^{s-1}$
- Each precoded message has weight 2^{s-1}
- Each codeword has weight 2^{2s-2}

Also, $H_{G(s)}(2^s - 1, B)$ for $B = \{1, 2, 2^s - 2, 2^s - 3\}$ (or any its subset) attains the Griesmer bound

Precoding allows to build codes that attain Griesmer bound

Griesmer bound: for linear $[n,k,d]$ binary code $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$

Lemma

Let $G(s) = [2^s - 1, s, 2^{s-1}]$ be the shortened RM$(1,s)$ code. Then $H_{G(s)}(2^s - 1, \{1,2\})$ meets the Griesmer bound

- $H_{G(s)}(2^s - 1, \{1,2\})$ has dimension s
- $H_{G(s)}(2^s - 1, \{1,2\})$ has length $2^{2s-1} - 2^{s-1}$
- Each precoded message has weight 2^{s-1}
- Each codeword has weight 2^{2s-2}

Also, $H_{G(s)}(2^s - 1, B)$ for $B = \{1, 2, 2^s - 2, 2^s - 3\}$ (or any its subset) attains the Griesmer bound

Precoding allows to build codes that attain Griesmer bound

Griesmer bound: for linear $[n,k,d]$ binary code $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$

Lemma

Let $G(s) = [2^s - 1, s, 2^{s-1}]$ be the shortened RM$(1,s)$ code. Then $H_{G(s)}(2^s - 1, \{1,2\})$ meets the Griesmer bound

- $H_{G(s)}(2^s - 1, \{1,2\})$ has dimension s
- $H_{G(s)}(2^s - 1, \{1,2\})$ has length $2^{2s-1} - 2^{s-1}$
- Each precoded message has weight 2^{s-1}
- Each codeword has weight 2^{2s-2}

Also, $H_{G(s)}(2^s - 1, B)$ for $B = \{1, 2, 2^s - 2, 2^s - 3\}$ (or any its subset) attains the Griesmer bound

Spherically punctured biorthogonal codes for general b

- Recall that first order RM$(1, m)$ code is formed by all affine functions of m variables

$$f(x_1, \ldots, x_m) = f_0 + \sum_{i=1}^{m} f_i x_i \qquad f_i, x_i \in \{0, 1\}$$

and has parameters : $n = 2^m \quad k = m + 1 \quad d = 2^{m-1}$

- Thus

$$\mathcal{R}(1, m) = H(m) \cup \{H(m) + \mathbf{1}\}$$

Definition

Spherically punctured biorthogonal code $P(m, b)$ is the code $\mathcal{R}(1, m)$ punctured to positions x so that wt$(x) = b$

Spherically punctured biorthogonal codes for general b

- Recall that first order RM$(1,m)$ code is formed by all affine functions of m variables

$$f(x_1,\ldots,x_m) = f_0 + \sum_{i=1}^{m} f_i x_i \qquad f_i, x_i \in \{0,1\}$$

and has parameters : $n = 2^m \quad k = m+1 \quad d = 2^{m-1}$

- Thus

$$\mathcal{R}(1,m) = H(m) \cup \{H(m) + \mathbf{1}\}$$

Definition

Spherically punctured biorthogonal code $P(m,b)$ is the code $\mathcal{R}(1,m)$ punctured to positions x so that wt$(x) = b$

Spherically punctured biorthogonal codes for general b

- Recall that first order RM$(1, m)$ code is formed by all affine functions of m variables

$$f(x_1, \ldots, x_m) = f_0 + \sum_{i=1}^{m} f_i x_i \qquad f_i, x_i \in \{0, 1\}$$

and has parameters : $n = 2^m \quad k = m + 1 \quad d = 2^{m-1}$

- Thus

$$\mathcal{R}(1, m) = H(m) \cup \{H(m) + \mathbf{1}\}$$

Definition

Spherically punctured biorthogonal code $P(m, b)$ is the code $\mathcal{R}(1, m)$ punctured to positions x so that $\mathrm{wt}(x) = b$

Spherically punctured biorthogonal code $P(m, b)$

Easy to see that:

- $P(m, b)$ has length $\binom{m}{b}$
- codeword weight is determined by message weight

Consider a message $f(x)$ whose linear part has weight w:

$$f(x) = f_0 + \sum_{i=1}^{m} f_i x_i \quad \text{so that} \quad \text{wt}(f_1, \ldots, f_m) = w$$

Lemma

Codeword weight is

$$\frac{1}{2}\left(\binom{m}{b} - (-1)^{f_0} K_b^m(w)\right),$$

where $K_b^m(w)$ is the binary Krawtchouk polynomial defined as

$$K_b^m(w) = \sum_{j=0}^{m} (-1)^j \binom{w}{j} \binom{m-w}{b-j}$$

We now study the minimum distance $d(m, b)$ of $P(m, b)$

Spherically punctured biorthogonal code $P(m, b)$

Easy to see that:

- $P(m, b)$ has length $\binom{m}{b}$
- codeword weight is determined by message weight

Consider a message $f(x)$ whose linear part has weight w:

$$f(x) = f_0 + \sum_{i=1}^{m} f_i x_i \quad \text{so that} \quad \text{wt}(f_1, \ldots, f_m) = w$$

Lemma

Codeword weight is

$$\frac{1}{2}\left(\binom{m}{b} - (-1)^{f_0} K_b^m(w)\right),$$

where $K_b^m(w)$ is the binary Krawtchouk polynomial defined as

$$K_b^m(w) = \sum_{j=0}^{m} (-1)^j \binom{w}{j}\binom{m-w}{b-j}$$

We now study the minimum distance $d(m, b)$ of $P(m, b)$

Spherically punctured biorthogonal code $P(m, b)$

Easy to see that:

- $P(m, b)$ has length $\binom{m}{b}$
- codeword weight is determined by message weight

Consider a message $f(x)$ whose linear part has weight w:

$$f(x) = f_0 + \sum_{i=1}^{m} f_i x_i \quad \text{so that} \quad \text{wt}(f_1, \ldots, f_m) = w$$

Lemma

Codeword weight is

$$\frac{1}{2}\left(\binom{m}{b} - (-1)^{f_0} K_b^m(w)\right),$$

where $K_b^m(w)$ is the binary Krawtchouk polynomial defined as

$$K_b^m(w) = \sum_{j=0}^{m} (-1)^j \binom{w}{j}\binom{m-w}{b-j}$$

We now study the minimum distance $d(m, b)$ of $P(m, b)$

Spherically punctured biorthogonal code $P(m,b)$

Easy to see that:

- $P(m,b)$ has length $\binom{m}{b}$
- codeword weight is determined by message weight

Consider a message $f(x)$ whose linear part has weight w:

$$f(x) = f_0 + \sum_{i=1}^{m} f_i x_i \quad \text{so that} \quad \text{wt}(f_1, \ldots, f_m) = w$$

Lemma

Codeword weight is

$$\frac{1}{2}\left(\binom{m}{b} - (-1)^{f_0} K_b^m(w)\right),$$

where $K_b^m(w)$ is the binary Krawtchouk polynomial defined as

$$K_b^m(w) = \sum_{j=0}^{m} (-1)^j \binom{w}{j}\binom{m-w}{b-j}$$

We now study the minimum distance $d(m,b)$ of $P(m,b)$

Minimum distance of $P(m, b)$

Theorem

Spherically punctured biorthogonal code $P(m, b)$ has

- *length* $\binom{m}{b}$
- *dimension* m
- *minimum distance*

$$d(m,b) = \begin{cases} \binom{m-1}{b-1}, & \text{if } m > 2b \\ \binom{m-1}{b}, & \text{if } m < 2b \\ 2\binom{m-2}{b}, & \text{if } m = 2b \end{cases}$$

- Finding the minimum distance of $P(m, b)$ is much more involved that for standard RM codes
- In RM(r, m) analysis, a hypercube is split into two identical subcubes, that behave similarly and yield a recursive estimate $(u \| u + v)$
- In our case, a sphere decomposes into two different subspheres. Furthermore, the subspheres may behave differently in terms of minimum distance

Minimum distance of $P(m, b)$

Theorem

Spherically punctured biorthogonal code $P(m, b)$ has

- *length* $\binom{m}{b}$
- *dimension* m
- *minimum distance*

$$d(m,b) = \begin{cases} \binom{m-1}{b-1}, & \text{if } m > 2b \\ \binom{m-1}{b}, & \text{if } m < 2b \\ 2\binom{m-2}{b}, & \text{if } m = 2b \end{cases}$$

- Finding the minimum distance of $P(m, b)$ is much more involved that for standard RM codes
- In RM(r, m) analysis, a hypercube is split into two identical subcubes, that behave similarly and yield a recursive estimate $(u|\ u + v)$
- In our case, a sphere decomposes into two different subspheres. Furthermore, the subspheres may behave differently in terms of minimum distance

Minimum distance of $P(m, b)$

Theorem

Spherically punctured biorthogonal code $P(m, b)$ has

- *length* $\binom{m}{b}$
- *dimension* m
- *minimum distance*

$$d(m,b) = \begin{cases} \binom{m-1}{b-1}, & \text{if } m > 2b \\ \binom{m-1}{b}, & \text{if } m < 2b \\ 2\binom{m-2}{b}, & \text{if } m = 2b \end{cases}$$

- Finding the minimum distance of $P(m, b)$ is much more involved that for standard RM codes
- In RM(r, m) analysis, a hypercube is split into two identical subcubes, that behave similarly and yield a recursive estimate $(u \| \; u + v)$
- In our case, a sphere decomposes into two different subspheres. Furthermore, the subspheres may behave differently in terms of minimum distance

Minimum distance of $P(m,b)$

Theorem

Spherically punctured biorthogonal code $P(m,b)$ has

- *length* $\binom{m}{b}$
- *dimension* m
- *minimum distance*

$$d(m,b)=\begin{cases}\binom{m-1}{b-1}, & \text{if } m>2b\\ \binom{m-1}{b}, & \text{if } m<2b\\ 2\binom{m-2}{b}, & \text{if } m=2b\end{cases}$$

- Finding the minimum distance of $P(m,b)$ is much more involved that for standard RM codes
- In RM(r,m) analysis, a hypercube is split into two identical subcubes, that behave similarly and yield a recursive estimate $(u\|\ u+v)$
- In our case, a sphere decomposes into two different subspheres. Furthermore, the subspheres may behave differently in terms of minimum distance

Minimum distance of $P(m, b)$

Split the sphere $S(m, b) = \{(x_1, \ldots, x_m) : \text{wt}(x) = b\}$ into two sub-spheres

- $S(m-1, b)$ that consists of $(x_1, \ldots, x_m) \in S(m, b)$ that have $x_m = 0$
- $S(m-1, b-1) = S(m, b) - S(m-1, b)$

Thus, $P(m, b)$ decomposes as:

$$(m-1, b-1) \nwarrow (m, b) \nearrow (m-1, b)$$

Node (m, b) might decompose into

- nodes of same types – easy case
- nodes of different types – hard case
- additional problems arise from zero codewords generated by nonzero input blocks

Minimum distance of $P(m, b)$

Split the sphere $S(m, b) = \{(x_1, \ldots, x_m) : \text{wt}(x) = b\}$ into two sub-spheres

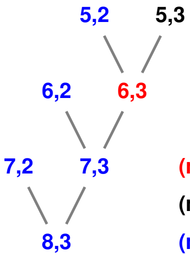
- $S(m-1, b)$ that consists of $(x_1, \ldots, x_m) \in S(m, b)$ that have $x_m = 0$
- $S(m-1, b-1) = S(m, b) - S(m-1, b)$

Thus, $P(m, b)$ decomposes as:

$$\begin{array}{ccc} (m-1, b-1) & & (m-1, b) \\ & \nwarrow \quad \nearrow & \\ & (m, b) & \end{array}$$

Node (m, b) might decompose into

- nodes of same types – easy case
- nodes of different types – hard case
- additional problems arise from zero codewords generated by nonzero input blocks



(m,b): $m = 2b$

(m,b): $m < 2b$

(m,b): $m > 2b$

Minimum of Krawtchouk polynomials

Corollary

For $b \in [1, m-1]$, and $w \in [1, m-1]$

$$\max\{|K_b^m(1)|, |K_b^m(2)|\} \geq |K_b^m(w)|$$

Similar result was previously known only in asymptotic setting for large m and linearly growing b

We now study ways to improve $d(m, b)$

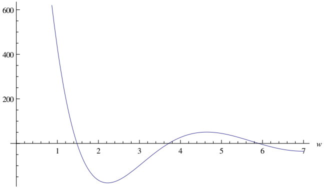
Precoding in the general case

Krawtchouk polynomial $K_b^m(w)$

- has b simple roots $r_1 < r_2 < \ldots < r_b$ so that

$$r_1 \geq \frac{m}{2} - \sqrt{b(m-b)}$$

- decays in $[0, r_1]$ and oscillates in $[r_1, r_b]$
- is 'small' in the oscillating region, i.e. $|K_b^m(w)| \leq 2^{-m\theta/2}\binom{m}{b}, \ \theta > 0$



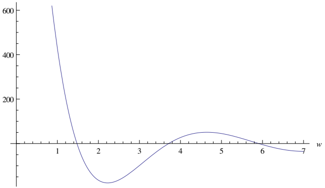
Good precoding would concentrate the weight spectrum close to the oscillating region

Thus, if the input spectrum of G is contained within $[\delta_{\min}, \delta_{\max}]$, then

$$d(m,b) \geq \frac{1}{2}\left(\binom{m}{b} - \max\left\{K_b^m(\delta), 2^{-m\theta/2}\binom{m}{b}\right\}\right), \delta = \begin{cases} \delta_{\min}, & \text{odd } b \\ \min\{\delta_{\min}, m - \delta_{\max}\}, & \text{even } b \end{cases}$$

This bound is exponentially tight

Precoding in the general case



Krawtchouk polynomial $K_b^m(w)$

- has b simple roots $r_1 < r_2 < \ldots < r_b$ so that

$$r_1 \geq \frac{m}{2} - \sqrt{b(m-b)}$$

- decays in $[0, r_1]$ and oscillates in $[r_1, r_b]$
- is 'small' in the oscillating region, i.e. $|K_b^m(w)| \leq 2^{-m\theta/2}\binom{m}{b}, \ \theta > 0$

Good precoding would concentrate the weight spectrum close to the oscillating region

Thus, if the input spectrum of G is contained within $[\delta_{\min}, \delta_{\max}]$, then

$$d(m,b) \geq \frac{1}{2}\left(\binom{m}{b} - \max\left\{K_b^m(\delta), 2^{-m\theta/2}\binom{m}{b}\right\}\right), \delta = \begin{cases} \delta_{\min}, & \text{odd } b \\ \min\{\delta_{\min}, m - \delta_{\max}\}, & \text{even } b \end{cases}$$

This bound is exponentially tight

Open problems

- Extend precoding to multi-layer construction
- Consider higher order RM codes

Thank you!

Open problems

- Extend precoding to multi-layer construction
- Consider higher order RM codes

Thank you!