Lower bounds on the minimum pseudoweight of codes with large automorphism group

Jens Zumbrägel
Claude Shannon Institute
University College Dublin

joint work with
Nigel Boston, Mark F. Flanagan, and Vitaly Skachek

Outline

Introduction

Further definitions

Codes with 2-transitive automorphism group

Codes with t-transitive automorphism group, $t > 2$

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Outline

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Introduction

- Low density parity-check (LDPC) codes achieve Shannon capacity of various channels and allow for efficient iterative decoding algorithms. [Gallager ’62, Luby et al. ’98, Richardson et al. ’01]

Introduction

- Low density parity-check (LDPC) codes achieve Shannon capacity of various channels and allow for efficient iterative decoding algorithms. [Gallager '62, Luby et al. '98, Richardson et al. '01]
- Decoding of binary LDPC codes using linear programming. [Feldman '03]

Introduction

- Low density parity-check (LDPC) codes achieve Shannon capacity of various channels and allow for efficient iterative decoding algorithms. [Gallager ’62, Luby et al. ’98, Richardson et al. ’01]
- Decoding of binary LDPC codes using linear programming. [Feldman ’03]
- Loss of decoding capability for concrete finite-length codes explained by (graph-cover/linear-programming) pseudo-codewords of low pseudoweight. [Koetter, Vontobel ’03-’05]

Introduction

- Low density parity-check (LDPC) codes achieve Shannon capacity of various channels and allow for efficient iterative decoding algorithms. [Gallager '62, Luby et al. '98, Richardson et al. '01]
- Decoding of binary LDPC codes using linear programming. [Feldman '03]
- Loss of decoding capability for concrete finite-length codes explained by (graph-cover/linear-programming) pseudo-codewords of low pseudoweight. [Koetter, Vontobel '03-'05]

$\Rightarrow$ Interest in codes with large minimum pseudoweight.
Minimum pseudoweight depends on the parity-check matrix of the code; it may be increased by adding redundant rows.

Parity-check codes

Let $\mathbb{F} = \mathbb{F}_2$ be the binary field.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Parity-check codes

Let $\mathbb{F} = \mathbb{F}_2$ be the binary field.

A *(linear) code* $\mathcal{C}$ is a subspace $\mathcal{C} \leq \mathbb{F}^n$. Let $k = \dim \mathcal{C}$ be its *dimension* and $d = \min\{\mathrm{w_H}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C} \setminus \{0\}\}$ its *minimum (Hamming) weight*.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Parity-check codes

Let $\mathbb{F} = \mathbb{F}_2$ be the binary field.

A *(linear) code* $\mathcal{C}$ is a subspace $\mathcal{C} \leq \mathbb{F}^n$. Let $k = \dim \mathcal{C}$ be its *dimension* and $d = \min\{\mathrm{w_H}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C} \setminus \{0\}\}$ its *minimum (Hamming) weight*.

Definition

A parity-check code is a pair $(\mathcal{C}, \boldsymbol{H})$, where $\mathcal{C}$ is a code and $\boldsymbol{H}$ is an $m \times n$ matrix such that

$$\mathcal{C} = \ker \boldsymbol{H} = \{\boldsymbol{c} \in \mathbb{F}_2^n \mid \boldsymbol{H}\,\boldsymbol{c}^T = \boldsymbol{0}^T\}\,.$$

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Minimum pseudoweight

For a parity-check code $(\mathcal{C}, \boldsymbol{H})$ we consider the *(AWGNC) minimum pseudoweight*

$$\mathrm{w}_{\mathrm{p}}^{\min} = \mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) ,$$

which indicates the error-correcting capability of linear programming or message passing decoding methods.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Minimum pseudoweight

For a parity-check code $(\mathcal{C}, \boldsymbol{H})$ we consider the *(AWGNC) minimum pseudoweight*

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}} = \mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \; ,$$

which indicates the error-correcting capability of linear programming or message passing decoding methods.

- $\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \leq d(\mathcal{C})$

Pseudocodeword redundancy

Definition

The pseudocodeword redundancy of a code $\mathcal{C}$ is defined as

$$\rho(\mathcal{C}) \;:=\; \inf\{m \mid \exists\, \boldsymbol{H} \in \mathrm{Mat}_{m\times n}(\mathbb{F}) : \mathcal{C} = \ker \boldsymbol{H},\; \mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) = d(\mathcal{C})\},$$

where $\inf \varnothing := \infty$.

Pseudocodeword redundancy

Definition

The pseudocodeword redundancy of a code $\mathcal{C}$ is defined as

$$\rho(\mathcal{C}) \; := \; \inf\{m \mid \exists\, \boldsymbol{H} \in \mathrm{Mat}_{m\times n}(\mathbb{F}) : \mathcal{C} = \ker \boldsymbol{H},\; \mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) = d(\mathcal{C})\},$$

where $\inf \varnothing := \infty$.

Proposition [Flanagan, Skachek, Z. '10]

For a random code $\mathcal{C}$ of fixed rate $R = \frac{k}{n}$, with high probability

$$\rho(\mathcal{C}) = \infty \, .$$

Pseudocodeword redundancy

Definition

The pseudocodeword redundancy of a code $\mathcal{C}$ is defined as

$$\rho(\mathcal{C}) := \inf\{m \mid \exists\, \boldsymbol{H} \in \mathrm{Mat}_{m\times n}(\mathbb{F}) : \mathcal{C} = \ker \boldsymbol{H},\ \mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) = d(\mathcal{C})\},$$

where $\inf \varnothing := \infty$.

Proposition [Flanagan, Skachek, Z. '10]

For a random code $\mathcal{C}$ of fixed rate $R = \frac{k}{n}$, with high probability

$$\rho(\mathcal{C}) = \infty\ .$$

Goal

Prove $\rho(\mathcal{C}) < \infty$ for certain codes $\mathcal{C}$ that have a large automorphism group.

Outline

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Fundamental cone

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code, where $\boldsymbol{H} \in \mathrm{Mat}_{m \times n}(\mathbb{F})$. Let $\mathcal{I} := \{1, \ldots, n\}$ and $\mathcal{J} := \{1, \ldots, m\}$ be the set of column resp. row indices. For $j \in \mathcal{J}$ let $\mathcal{I}_j := \{i \in \mathcal{I} : H_{j,i} \neq 0\}$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Fundamental cone

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code, where $\boldsymbol{H} \in \mathrm{Mat}_{m\times n}(\mathbb{F})$. Let $\mathcal{I} := \{1, \ldots, n\}$ and $\mathcal{J} := \{1, \ldots, m\}$ be the set of column resp. row indices. For $j \in \mathcal{J}$ let $\mathcal{I}_j := \{i \in \mathcal{I} : H_{j,i} \neq 0\}$.

Definition

The fundamental cone $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined as the set of all vectors $\boldsymbol{x} \in \mathbb{R}^n$ that satisfy the inequalities:

$$\forall j \in \mathcal{J}\ \forall \ell \in \mathcal{I}_j : \ x_\ell \leq \sum_{i \in \mathcal{I}_j \setminus \{\ell\}} x_i ,$$

$$\forall i \in \mathcal{I} : \ 0 \leq x_i .$$

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Fundamental cone (cont.)

Example

Let $\mathcal{C}$ be the $[7, 4, 3]$ Hamming code with parity-check matrix

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Fundamental cone (cont.)

Example

Let $\mathcal{C}$ be the $[7, 4, 3]$ Hamming code with parity-check matrix

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} .$$

The inequalities of the fundamental cone $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ are:

$$\begin{array}{lll} x_1 \leq x_2 + x_3 + x_5 & x_2 \leq x_3 + x_4 + x_6 & x_3 \leq x_4 + x_5 + x_7 \\ x_2 \leq x_1 + x_3 + x_5 & x_3 \leq x_2 + x_4 + x_6 & x_4 \leq x_3 + x_5 + x_7 \\ x_3 \leq x_1 + x_2 + x_5 & x_4 \leq x_2 + x_3 + x_6 & x_5 \leq x_3 + x_4 + x_7 \\ x_5 \leq x_1 + x_2 + x_3 & x_6 \leq x_2 + x_3 + x_4 & x_7 \leq x_3 + x_4 + x_5 \end{array}$$

$$0 \leq x_1 \quad 0 \leq x_2 \quad 0 \leq x_3 \quad 0 \leq x_4 \quad 0 \leq x_5 \quad 0 \leq x_6 \quad 0 \leq x_7$$

Minimum pseudoweight

Definition

The minimum pseudoweight of the parity-check code $(\mathcal{C}, \boldsymbol{H})$ is

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) := \min_{\boldsymbol{x} \in \mathcal{K}(\mathcal{C}, \boldsymbol{H}) \setminus \{0\}} \mathrm{w}_{\mathrm{p}}(\boldsymbol{x}) ,$$

where $\mathrm{w}_{\mathrm{p}}(\boldsymbol{x}) := \frac{\left(\sum_{i \in \mathcal{I}} x_i\right)^2}{\sum_{i \in \mathcal{I}} x_i^2}$ is the *(AWGNC) pseudoweight*.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Minimum pseudoweight

Definition

The minimum pseudoweight of the parity-check code $(\mathcal{C}, \boldsymbol{H})$ is

$$\mathrm{w}_\mathrm{p}^{\min}(\mathcal{C}, \boldsymbol{H}) := \min_{\boldsymbol{x} \in \mathcal{K}(\mathcal{C}, \boldsymbol{H}) \setminus \{0\}} \mathrm{w}_\mathrm{p}(\boldsymbol{x}) ,$$

where $\mathrm{w}_\mathrm{p}(\boldsymbol{x}) := \dfrac{\left(\sum_{i \in \mathcal{I}} x_i\right)^2}{\sum_{i \in \mathcal{I}} x_i^2}$ is the *(AWGNC) pseudoweight*.

- $\mathrm{w}_\mathrm{p}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq d \quad \Leftrightarrow \quad \forall x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H}) : d \sum_i x_i^2 \leq \left(\sum_i x_i\right)^2$

sfi Fondúireacht Eolaíochta Éireann Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Minimum pseudoweight

Definition

The minimum pseudoweight of the parity-check code $(\mathcal{C}, \boldsymbol{H})$ is

$$\mathrm{w}_\mathrm{p}^{\min}(\mathcal{C}, \boldsymbol{H}) := \min_{\boldsymbol{x} \in \mathcal{K}(\mathcal{C}, \boldsymbol{H}) \setminus \{0\}} \mathrm{w}_\mathrm{p}(\boldsymbol{x}) \,,$$

where $\mathrm{w}_\mathrm{p}(\boldsymbol{x}) := \frac{\left(\sum_{i \in \mathcal{I}} x_i\right)^2}{\sum_{i \in \mathcal{I}} x_i^2}$ is the *(AWGNC) pseudoweight*.

- $\mathrm{w}_\mathrm{p}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq d \quad \Leftrightarrow \quad \forall x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H}) : d \sum_i x_i^2 \leq \left(\sum_i x_i\right)^2$

Remark

Consider $\mathcal{C}$ as a subset of $\mathbb{R}^n$, where $0_\mathbb{F} \mapsto 0$ and $1_\mathbb{F} \mapsto 1$.
Then $\mathcal{C} \subseteq \mathcal{K}(\mathcal{C}, \boldsymbol{H})$ and $\mathrm{w}_\mathrm{p}|_\mathcal{C} = \mathrm{w}_\mathrm{H}$.
It follows $\mathrm{w}_\mathrm{p}^{\min}(\mathcal{C}, \boldsymbol{H}) \leq d(\mathcal{C})$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Automorphism group

Definition

The automorphism group $\mathrm{Aut}(\mathcal{C}) \leq S_n$ of a code $\mathcal{C}$ consists of all permutation of coordinate places which send $\mathcal{C}$ into itself (codewords go into codewords).

Automorphism group

Definition

The automorphism group $\mathrm{Aut}(\mathcal{C}) \leq S_n$ of a code $\mathcal{C}$ consists of all permutation of coordinate places which send $\mathcal{C}$ into itself (codewords go into codewords).

- $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^{\perp})$

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Automorphism group (cont.)

Definition

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code. The automorphism group $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H}) = \mathrm{Aut}(\boldsymbol{H})$ consists of all permutation of columns of $\boldsymbol{H}$ which send the set of rows of $\boldsymbol{H}$ into itself.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Automorphism group (cont.)

Definition

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code. The automorphism group $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H}) = \mathrm{Aut}(\boldsymbol{H})$ consists of all permutation of columns of $\boldsymbol{H}$ which send the set of rows of $\boldsymbol{H}$ into itself.

- $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H}) \leq \mathrm{Aut}(\mathcal{C})$

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Automorphism group (cont.)

Definition

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code. The automorphism group $\text{Aut}(\mathcal{C}, \boldsymbol{H}) = \text{Aut}(\boldsymbol{H})$ consists of all permutation of columns of $\boldsymbol{H}$ which send the set of rows of $\boldsymbol{H}$ into itself.

- $\text{Aut}(\mathcal{C}, \boldsymbol{H}) \leq \text{Aut}(\mathcal{C})$
- Any permutation in $\text{Aut}(\mathcal{C}, \boldsymbol{H})$ sends $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ into itself.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Automorphism group (cont.)

Definition

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code. The automorphism group $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H}) = \mathrm{Aut}(\boldsymbol{H})$ consists of all permutation of columns of $\boldsymbol{H}$ which send the set of rows of $\boldsymbol{H}$ into itself.

- $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H}) \leq \mathrm{Aut}(\mathcal{C})$
- Any permutation in $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H})$ sends $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ into itself.
- Let $\mathcal{C}$ be a code and let $\boldsymbol{H}$ consist of all rows in $\mathcal{C}^{\perp}$ of some weight w. Then $\mathcal{C}' := \ker \boldsymbol{H} \supseteq \mathcal{C}$ and $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{Aut}(\mathcal{C}', \boldsymbol{H})$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Automorphism group (cont.)

Definition

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code. The automorphism group $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H}) = \mathrm{Aut}(\boldsymbol{H})$ consists of all permutation of columns of $\boldsymbol{H}$ which send the set of rows of $\boldsymbol{H}$ into itself.

- $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H}) \leq \mathrm{Aut}(\mathcal{C})$
- Any permutation in $\mathrm{Aut}(\mathcal{C}, \boldsymbol{H})$ sends $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ into itself.
- Let $\mathcal{C}$ be a code and let $\boldsymbol{H}$ consist of all rows in $\mathcal{C}^{\perp}$ of some weight w. Then $\mathcal{C}' := \ker \boldsymbol{H} \supseteq \mathcal{C}$ and $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{Aut}(\mathcal{C}', \boldsymbol{H})$.

Goal

Obtain lower bounds on $\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H})$ for certain parity-check codes $(\mathcal{C}, \boldsymbol{H})$ that have a large automorphism group.

Fondúireacht Eolaíochta Éireann
sfi Science Foundation Ireland

Outline

Introduction

Further definitions

Codes with 2-transitive automorphism group

Codes with t-transitive automorphism group, $t > 2$

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes based on designs

Let $\boldsymbol{H}$ be an $m \times n$ matrix which is the point-block incidence matrix of a 2-(n, w_r, λ) design, i.e.

- every row has constant weight w_r,
- each 2 columns have λ common ones.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes based on designs

Let $\boldsymbol{H}$ be an $m \times n$ matrix which is the point-block incidence matrix of a 2-(n, w_r, λ) design, i.e.

- every row has constant weight w_r,
- each 2 columns have λ common ones.

Then

- every column has constant weight w_c,
- $nw_c = mw_r$ and $w_c(w_r - 1) = \lambda(n - 1)$.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes based on designs

Let $\boldsymbol{H}$ be an $m \times n$ matrix which is the point-block incidence matrix of a 2-(n, w_r, λ) design, i.e.

- every row has constant weight w_r,
- each 2 columns have λ common ones.

Then

- every column has constant weight w_c,
- $nw_c = mw_r$ and $w_c(w_r - 1) = \lambda(n - 1)$.

Proposition [Flanagan, Skachek, Z. '10]

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1} = 1 + \frac{w_c}{\lambda} .$$

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes based on designs

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{w_c}{\lambda}$$

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes based on designs

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{w_c}{\lambda}$$

Proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

sfi Fondúireacht Eolaíochta Éireann Science Foundation Ireland

Codes based on designs

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{w_c}{\lambda}$$

Proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $i \in \mathcal{I}$. Let $j \in \mathcal{J}$ such that $i \in \mathcal{I}_j$.
  Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.

Codes based on designs

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{w_c}{\lambda}$$

Proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $i \in \mathcal{I}$. Let $j \in \mathcal{J}$ such that $i \in \mathcal{I}_j$.
  Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Sum over j: $w_c x_i^2 \leq \lambda \sum_{\ell \neq i} x_\ell x_i$.

Codes based on designs

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{w_c}{\lambda}$$

Proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $i \in \mathcal{I}$. Let $j \in \mathcal{J}$ such that $i \in \mathcal{I}_j$.
  Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Sum over j: $w_c x_i^2 \leq \lambda \sum_{\ell \neq i} x_\ell x_i$.
- Sum over i: $w_c \sum_i x_i^2 \leq \lambda \sum_{\ell \neq i} x_\ell x_i$.

Codes based on designs

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{w_c}{\lambda}$$

Proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $i \in \mathcal{I}$. Let $j \in \mathcal{J}$ such that $i \in \mathcal{I}_j$.
  Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Sum over j: $w_c x_i^2 \leq \lambda \sum_{\ell \neq i} x_\ell x_i$.
- Sum over i: $w_c \sum_i x_i^2 \leq \lambda \sum_{\ell \neq i} x_\ell x_i$.
- Rewrite this as: $(1 + \frac{w_c}{\lambda}) \sum_i x_i^2 \leq (\sum_i x_i)^2$.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes based on designs

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{w_c}{\lambda}$$

Proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $i \in \mathcal{I}$. Let $j \in \mathcal{J}$ such that $i \in \mathcal{I}_j$.
  Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Sum over j: $w_c x_i^2 \leq \lambda \sum_{\ell \neq i} x_\ell x_i$.
- Sum over i: $w_c \sum_i x_i^2 \leq \lambda \sum_{\ell \neq i} x_\ell x_i$.
- Rewrite this as: $(1 + \frac{w_c}{\lambda}) \sum_i x_i^2 \leq (\sum_i x_i)^2$.

Hence, $\mathrm{w}_{\mathrm{p}}(x) \geq 1 + \frac{w_c}{\lambda}$. □

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes with 2-transitive automorphism group

Proposition

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code such that $\mathrm{Aut}(\boldsymbol{H})$ is 2-transitive. Let w_r be the weight of an arbitrary row of $\boldsymbol{H}$. Then

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1} \,.$$

sfi Fondúireacht Eolaíochta Éireann Science Foundation Ireland

Codes with 2-transitive automorphism group

Proposition

Let $(\mathcal{C}, \boldsymbol{H})$ be a parity-check code such that $\mathrm{Aut}(\boldsymbol{H})$ is 2-transitive. Let w_r be the weight of an arbitrary row of $\boldsymbol{H}$. Then

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1} .$$

First proof.

Observe that the rows of $\boldsymbol{H}$ with weight w_r form the point-block incidence matrix of a 2-design. Apply the last proposition. $\square$

Codes with 2-transitive automorphism group

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1}$$

Second proof.

Codes with 2-transitive automorphism group

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1}$$

Second proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes with 2-transitive automorphism group

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1}$$

Second proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $j \in \mathcal{J}$ be the index of a row with weight w_r, let $i \in \mathcal{I}_j$. Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.

sfi Fondúireacht Eolaíochta Éireann Science Foundation Ireland

Codes with 2-transitive automorphism group

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1}$$

Second proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $j \in \mathcal{J}$ be the index of a row with weight w_r, let $i \in \mathcal{I}_j$. Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Apply the automorphisms and sum up: $\sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} x_{i^\sigma}^2 \leq \sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_{\ell^\sigma} x_{i^\sigma}$.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes with 2-transitive automorphism group

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1}$$

Second proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $j \in \mathcal{J}$ be the index of a row with weight w_r, let $i \in \mathcal{I}_j$. Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Apply the automorphisms and sum up: $\sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} x_{i^\sigma}^2 \leq \sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_{\ell^\sigma} x_{i^\sigma}$.
- With $N := |\mathrm{Aut}(\boldsymbol{H})|$, $|\mathcal{I}_j| = w_r$, and by 2-transitivity this is: $\frac{N}{n} \sum_i x_i^2 \leq \frac{N(w_r - 1)}{n(n-1)} \sum_{i \neq \ell} x_\ell x_i$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Codes with 2-transitive automorphism group

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1}$$

Second proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $j \in \mathcal{J}$ be the index of a row with weight w_r, let $i \in \mathcal{I}_j$. Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Apply the automorphisms and sum up: $\sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} x_{i^\sigma}^2 \leq \sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_{\ell^\sigma} x_{i^\sigma}$.
- With $N := |\mathrm{Aut}(\boldsymbol{H})|$, $|\mathcal{I}_j| = w_r$, and by 2-transitivity this is: $\frac{N}{n} \sum_i x_i^2 \leq \frac{N(w_r - 1)}{n(n-1)} \sum_{i \neq \ell} x_\ell x_i$.
- Rewrite this as: $(1 + \frac{n-1}{w_r - 1}) \sum_i x_i^2 \leq (\sum_i x_i)^2$.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Codes with 2-transitive automorphism group

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 1 + \frac{n-1}{w_r - 1}$$

Second proof.

Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- Let $j \in \mathcal{J}$ be the index of a row with weight w_r, let $i \in \mathcal{I}_j$. Then $x_i \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell$ and $x_i^2 \leq \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_\ell x_i$.
- Apply the automorphisms and sum up: $\sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} x_{i^\sigma}^2 \leq \sum_{\sigma \in \mathrm{Aut}(\boldsymbol{H})} \sum_{\ell \in \mathcal{I}_j, \ell \neq i} x_{\ell^\sigma} x_{i^\sigma}$.
- With $N := |\,\mathrm{Aut}(\boldsymbol{H})|$, $|\mathcal{I}_j| = w_r$, and by 2-transitivity this is: $\frac{N}{n} \sum_i x_i^2 \leq \frac{N(w_r - 1)}{n(n-1)} \sum_{i \neq \ell} x_\ell x_i$.
- Rewrite this as: $(1 + \frac{n-1}{w_r - 1}) \sum_i x_i^2 \leq (\sum_i x_i)^2$.

Hence, $\mathrm{w}_{\mathrm{p}}(x) \geq 1 + \frac{n-1}{w_r - 1}$. □

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Examples

Let $\mathcal{C}$ be the $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code.
Let $\mathcal{C}^\perp$ be the $[2^m - 1, m, 2^{m-1}]$ simplex code.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Examples

Let $\mathcal{C}$ be the $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code.
Let $\mathcal{C}^\perp$ be the $[2^m - 1, m, 2^{m-1}]$ simplex code.

- $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^\perp) = \mathrm{GL}_m(2)$

Examples

Let $\mathcal{C}$ be the $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code.
Let $\mathcal{C}^\perp$ be the $[2^m - 1, m, 2^{m-1}]$ simplex code.

- $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^\perp) = \mathrm{GL}_m(2)$

1. Consider $(\mathcal{C}, \boldsymbol{H})$, where $\boldsymbol{H}$ consists of all nonzero codewords of $\mathcal{C}^\perp$.

Examples

Let $\mathcal{C}$ be the $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code.
Let $\mathcal{C}^\perp$ be the $[2^m - 1, m, 2^{m-1}]$ simplex code.

- $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^\perp) = \mathrm{GL}_m(2)$

1. Consider $(\mathcal{C}, \boldsymbol{H})$, where $\boldsymbol{H}$ consists of all nonzero codewords of $\mathcal{C}^\perp$.

$$2\text{-}(2^m - 1, 2^{m-1}, 2^{m-2}) \text{ design} \Rightarrow \mathrm{w}_\mathrm{p}^{\mathrm{min}} \geq 1 + \frac{2^m - 2}{2^{m-1} - 1} = 3\,.$$

Examples

Let $\mathcal{C}$ be the $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code.
Let $\mathcal{C}^\perp$ be the $[2^m - 1, m, 2^{m-1}]$ simplex code.

- $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^\perp) = \mathrm{GL}_m(2)$

1. Consider $(\mathcal{C}, \boldsymbol{H})$, where $\boldsymbol{H}$ consists of all nonzero codewords of $\mathcal{C}^\perp$.

$$2\text{-}(2^m - 1, 2^{m-1}, 2^{m-2}) \text{ design } \Rightarrow \mathrm{w}_\mathrm{p}^{\min} \geq 1 + \frac{2^m-2}{2^{m-1}-1} = 3\,.$$

2. Consider $(\mathcal{C}^\perp, \boldsymbol{H}^\perp)$, where $\boldsymbol{H}^\perp$ consists of all codewords of $\mathcal{C}$ of weight 3.

Examples

Let $\mathcal{C}$ be the $[2^m-1, 2^m-1-m, 3]$ Hamming code.
Let $\mathcal{C}^\perp$ be the $[2^m-1, m, 2^{m-1}]$ simplex code.

- $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}^\perp) = \mathrm{GL}_m(2)$

1. Consider $(\mathcal{C}, \boldsymbol{H})$, where $\boldsymbol{H}$ consists of all nonzero codewords of $\mathcal{C}^\perp$.

$$2\text{-}(2^m-1, 2^{m-1}, 2^{m-2}) \text{ design } \Rightarrow \ \mathrm{w}_\mathrm{p}^{\min} \geq 1 + \tfrac{2^m-2}{2^{m-1}-1} = 3\,.$$

2. Consider $(\mathcal{C}^\perp, \boldsymbol{H}^\perp)$, where $\boldsymbol{H}^\perp$ consists of all codewords of $\mathcal{C}$ of weight 3.

$$2\text{-}(2^m-1, 3, 1) \text{ design } \Rightarrow \ \mathrm{w}_\mathrm{p}^{\min} \geq 1 + \tfrac{2^m-2}{2} = 2^{m-1}\,.$$

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Examples (cont.)

Let $\boldsymbol{H}$ be the incidence matrix of a projective plane of order $q = 2^m$. Let $C = \ker \boldsymbol{H}$ be the projective geometry code.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Examples (cont.)

Let $\boldsymbol{H}$ be the incidence matrix of a projective plane of order $q = 2^m$. Let $C = \ker \boldsymbol{H}$ be the projective geometry code.

$$2\text{-}(q^2 + q + 1, q + 1, 1) \text{ design } \Rightarrow \mathrm{w}_\mathrm{p}^{\mathrm{min}} \geq 1 + \frac{q^2+q}{q} = q + 2\,.$$

Examples (cont.)

Let $\boldsymbol{H}$ be the incidence matrix of a projective plane of order $q = 2^m$. Let $C = \ker \boldsymbol{H}$ be the projective geometry code.

$$2\text{-}(q^2+q+1, q+1, 1) \text{ design } \Rightarrow \mathrm{w}_{\mathrm{p}}^{\min} \geq 1 + \tfrac{q^2+q}{q} = q+2\,.$$

Remark

The best bound for $\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H})$ achievable by taking convex combinations of *products of two inequalities* is

$$1 + \frac{n-1}{d^{\perp}-1}\,,$$

where $d^{\perp}$ is the minimum distance of $\mathcal{C}^{\perp}$.

Outline

Cubic inequalities

Instead of the quadratic inequality $d\sum_i x_i^2 \leq (\sum_i x_i)^2$ one can prove the *cubic* inequality $d(\sum_i x_i^2)(\sum_i x_i) \leq (\sum_i x_i)^3$,

Cubic inequalities

Instead of the quadratic inequality $d\sum_i x_i^2 \leq (\sum_i x_i)^2$ one can prove the *cubic* inequality $d(\sum_i x_i^2)(\sum_i x_i) \leq (\sum_i x_i)^3$,which may be rewritten as

$$(d-1)\sum_i x_i^3 + (d-3)\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k \ .$$

Cubic inequalities

Instead of the quadratic inequality $d\sum_i x_i^2 \leq (\sum_i x_i)^2$ one can prove the *cubic* inequality $d(\sum_i x_i^2)(\sum_i x_i) \leq (\sum_i x_i)^3$,which may be rewritten as

$$(d-1)\sum_i x_i^3 + (d-3)\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k \ .$$

Proposition

Let $\mathcal{C}$ be the $[8,4,4]$ extended Hamming code and let $\boldsymbol{H}$ consist of all codewords of $\mathcal{C}^\perp = \mathcal{C}$ of weight 4. Then $\mathrm{w}_\mathrm{p}^{\mathrm{min}}(\mathcal{C},\boldsymbol{H}) = 4$, and hence $\rho(\mathcal{C}) < \infty$.

Cubic inequalities

Instead of the quadratic inequality $d\sum_i x_i^2 \leq (\sum_i x_i)^2$ one can prove the *cubic* inequality $d(\sum_i x_i^2)(\sum_i x_i) \leq (\sum_i x_i)^3$,which may be rewritten as

$$(d-1)\sum_i x_i^3 + (d-3)\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k .$$

Proposition

Let $\mathcal{C}$ be the $[8,4,4]$ extended Hamming code and let $\boldsymbol{H}$ consist of all codewords of $\mathcal{C}^\perp = \mathcal{C}$ of weight 4. Then $\mathrm{w}_\mathrm{p}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) = 4$, and hence $\rho(\mathcal{C}) < \infty$.

- $\mathrm{Aut}(\mathcal{C}) = \mathrm{GA}_2(3)$, which is 3-transitive.

Proof

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 4$$

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Proof

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 4$$

Proof.

We may assume that $\boldsymbol{c}_1 = [1, 1, 1, 1, 0, 0, 0, 0]$ and $\boldsymbol{c}_2 = [1, 1, 0, 0, 1, 1, 0, 0]$ are in $\mathcal{C}$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Proof

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 4$$

Proof.
We may assume that $\boldsymbol{c}_1 = [1, 1, 1, 1, 0, 0, 0, 0]$ and $\boldsymbol{c}_2 = [1, 1, 0, 0, 1, 1, 0, 0]$ are in $\mathcal{C}$. Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Proof

$$\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) \geq 4$$

Proof.
We may assume that $\boldsymbol{c}_1 = [1, 1, 1, 1, 0, 0, 0, 0]$ and $\boldsymbol{c}_2 = [1, 1, 0, 0, 1, 1, 0, 0]$ are in $\mathcal{C}$. Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- $x_1 \leq x_2 + x_3 + x_4$,
  hence $x_1^2 x_5 \leq (x_2 + x_3 + x_4) x_1 x_5$.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Proof

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 4$$

Proof.

We may assume that $\boldsymbol{c}_1 = [1,1,1,1,0,0,0,0]$ and $\boldsymbol{c}_2 = [1,1,0,0,1,1,0,0]$ are in $\mathcal{C}$. Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- $x_1 \leq x_2 + x_3 + x_4$,
  hence $x_1^2 x_5 \leq (x_2 + x_3 + x_4) x_1 x_5$.
- Apply the automorphisms and sum up:
  $\frac{N}{n(n-1)} \sum_{i \neq j} x_i^2 x_j \leq \frac{3N}{n(n-1)(n-2)} \sum_{i \neq j \neq k \neq i} x_i x_j x_k$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Proof

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 4$$

Proof.

We may assume that $\boldsymbol{c}_1 = [1,1,1,1,0,0,0,0]$ and $\boldsymbol{c}_2 = [1,1,0,0,1,1,0,0]$ are in $\mathcal{C}$. Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- $x_1 \leq x_2 + x_3 + x_4$,
  hence $x_1^2 x_5 \leq (x_2 + x_3 + x_4) x_1 x_5$.
- Apply the automorphisms and sum up:
  $\frac{N}{n(n-1)} \sum_{i \neq j} x_i^2 x_j \leq \frac{3N}{n(n-1)(n-2)} \sum_{i \neq j \neq k \neq i} x_i x_j x_k$.
  Hence, $2 \sum_{i \neq j} x_i^2 x_j \leq \sum_{i \neq j \neq k \neq i} x_i x_j x_k$.

Proof

$$\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) \geq 4$$

Proof.

We may assume that $\boldsymbol{c}_1 = [1,1,1,1,0,0,0,0]$ and $\boldsymbol{c}_2 = [1,1,0,0,1,1,0,0]$ are in $\mathcal{C}$. Let $x \in \mathcal{K}(\mathcal{C}, \boldsymbol{H})$.

- $x_1 \leq x_2 + x_3 + x_4$,
  hence $x_1^2 x_5 \leq (x_2 + x_3 + x_4) x_1 x_5$.
- Apply the automorphisms and sum up:
  $\frac{N}{n(n-1)} \sum_{i \neq j} x_i^2 x_j \leq \frac{3N}{n(n-1)(n-2)} \sum_{i \neq j \neq k \neq i} x_i x_j x_k$.
  Hence, $2 \sum_{i \neq j} x_i^2 x_j \leq \sum_{i \neq j \neq k \neq i} x_i x_j x_k$.
- $x_1 \leq x_2 + x_3 + x_4$ and $x_2 \leq x_1 + x_5 + x_6$,
  hence $0 \leq (-x_1 + x_2 + x_3 + x_4)(x_1 - x_2 + x_5 + x_6) x_1$.

Proof (cont.)

- $2\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k$
- $0 \leq (-x_1 + x_2 + x_3 + x_4)(x_1 - x_2 + x_5 + x_6)x_1$

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Proof (cont.)

- $2\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k$
- $0 \leq (-x_1 + x_2 + x_3 + x_4)(x_1 - x_2 + x_5 + x_6)x_1$

.

- Apply the automorphisms and sum up: $\frac{N}{n}\sum_i x_i^3 - \frac{N}{n(n-1)}\sum_{i\neq j} x_i^2 x_j \leq \frac{4N}{n(n-1)(n-2)}\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Proof (cont.)

- $2\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k$
- $0 \leq (-x_1 + x_2 + x_3 + x_4)(x_1 - x_2 + x_5 + x_6)x_1$

- Apply the automorphisms and sum up:
  $\frac{N}{n}\sum_i x_i^3 - \frac{N}{n(n-1)}\sum_{i\neq j} x_i^2 x_j \leq \frac{4N}{n(n-1)(n-2)}\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.
  Hence, $21\sum_i x_i^3 - 3\sum_{i\neq j} x_i^2 x_j \leq 2\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Proof (cont.)

- $2\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k$
- $0 \leq (-x_1 + x_2 + x_3 + x_4)(x_1 - x_2 + x_5 + x_6)x_1$

.

- Apply the automorphisms and sum up: $\frac{N}{n}\sum_i x_i^3 - \frac{N}{n(n-1)}\sum_{i\neq j} x_i^2 x_j \leq \frac{4N}{n(n-1)(n-2)}\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.
  Hence, $21\sum_i x_i^3 - 3\sum_{i\neq j} x_i^2 x_j \leq 2\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.
- Adding 5 times the first inequality above yields $21\sum_i x_i^3 + 7\sum_{i\neq j} x_i^2 x_j \leq 7\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Proof (cont.)

- $2\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k$
- $0 \leq (-x_1 + x_2 + x_3 + x_4)(x_1 - x_2 + x_5 + x_6)x_1$

.

- Apply the automorphisms and sum up:
  $\frac{N}{n}\sum_i x_i^3 - \frac{N}{n(n-1)}\sum_{i\neq j} x_i^2 x_j \leq \frac{4N}{n(n-1)(n-2)}\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.
  Hence, $21\sum_i x_i^3 - 3\sum_{i\neq j} x_i^2 x_j \leq 2\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.
- Adding 5 times the first inequality above yields
  $21\sum_i x_i^3 + 7\sum_{i\neq j} x_i^2 x_j \leq 7\sum_{i\neq j\neq k\neq i} x_i x_j x_k$.
- That is, $(d-1)\sum_i x_i^3 + (d-3)\sum_{i\neq j} x_i^2 x_j \leq \sum_{i\neq j\neq k\neq i} x_i x_j x_k$ with $d = 4$.

Hence $\mathrm{w_p}(x) \geq 4$. □

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_\mathrm{p}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) = 8$.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) = 8$.

- $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined by $8 \cdot 759 + 24 = 6096$ inequalities.

Claude Shannon Institute
Discrete Mathematics, Coding, Cryptography and Information Security
www.shannoninstitute.ie

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) = 8$.

- $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined by $8 \cdot 759 + 24 = 6096$ inequalities.
- $\mathrm{Aut}(\boldsymbol{H}) = M_{24}$ is 5-transitive of order 244 823 040.

Fondúireacht Eolaíochta Éireann
Science Foundation Ireland

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_\mathrm{p}^{\min}(\mathcal{C}, \boldsymbol{H}) = 8$.

- $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined by $8 \cdot 759 + 24 = 6096$ inequalities.
- $\mathrm{Aut}(\boldsymbol{H}) = M_{24}$ is 5-transitive of order 244 823 040.

quadrics	$\frac{30}{7} = 4.285...$	10 products

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) = 8$.

- $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined by $8 \cdot 759 + 24 = 6096$ inequalities.
- $\mathrm{Aut}(\boldsymbol{H}) = M_{24}$ is 5-transitive of order 244 823 040.

quadrics	$\frac{30}{7} = 4.285\ldots$	10 products
cubics	$\frac{86}{17} = 5.058\ldots$	74 products

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) = 8$.

- $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined by $8 \cdot 759 + 24 = 6096$ inequalities.
- $\mathrm{Aut}(\boldsymbol{H}) = M_{24}$ is 5-transitive of order 244 823 040.

quadrics	$\frac{30}{7} = 4.285...$	10 products
cubics	$\frac{86}{17} = 5.058...$	74 products
quartics	$\frac{79545}{13259} = 5.999...$	2215 products

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_{\mathrm{p}}^{\mathrm{min}}(\mathcal{C}, \boldsymbol{H}) = 8$.

- $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined by $8 \cdot 759 + 24 = 6096$ inequalities.
- $\mathrm{Aut}(\boldsymbol{H}) = M_{24}$ is 5-transitive of order 244 823 040.

quadrics	$\frac{30}{7} = 4.285\ldots$	10 products
cubics	$\frac{86}{17} = 5.058\ldots$	74 products
quartics	$\frac{79545}{13259} = 5.999\ldots$	2215 products
qunitics	$\geq \frac{2795677}{419041} = 6.671\ldots$	$\geq$ 42 421 products

Extended Golay code

Conjecture

Let $\mathcal{C}$ be the $[24, 12, 8]$ extended Golay code and let $\boldsymbol{H}$ consist of all codewords of weight 8 (the octads). Then $\mathrm{w}_{\mathrm{p}}^{\min}(\mathcal{C}, \boldsymbol{H}) = 8$.

- $\mathcal{K}(\mathcal{C}, \boldsymbol{H})$ is defined by $8 \cdot 759 + 24 = 6096$ inequalities.
- $\mathrm{Aut}(\boldsymbol{H}) = M_{24}$ is 5-transitive of order 244 823 040.

quadrics	$\frac{30}{7} = 4.285\ldots$		10 products
cubics	$\frac{86}{17} = 5.058\ldots$		74 products
quartics	$\frac{79545}{13259} = 5.999\ldots$		2215 products
qunitics	$\geq \frac{2795677}{419041} = 6.671\ldots$	$\geq$	42 421 products

To be continued...

Thank you for your attention!