A Survey of Permutation Codes

Peter J. Dukes

July 17, 2016

University of Victoria | Mathematics and Statistics

CUMC 2016 CCÉM

Classical binary codes

A *binary code* of *length* n and *distance* d is a subset $\mathcal{C}$ of $\{0,1\}^n$ such that any two distinct words in $\mathcal{C}$ differ in at least d positions.

Example. $\{000000, 000111, 111000, 111111\}$ is a binary code of length $n = 6$ and minimum distance $d = 3$.

Some nice algebraic constructions exist; for instance, the ideal

$$\langle x^3 + x + 1 \rangle \subset \mathbb{F}_2[x]/\langle x^7 - 1 \rangle$$

leads to a code with $n = 7$, $d = 3$, and $|\mathcal{C}| = 16$.

Classical binary codes

A *binary code* of *length* n and *distance* d is a subset $\mathcal{C}$ of $\{0,1\}^n$ such that any two distinct words in $\mathcal{C}$ differ in at least d positions.

Example. $\{000000, 000111, 111000, 111111\}$ is a binary code of length $n = 6$ and minimum distance $d = 3$.

Some nice algebraic constructions exist; for instance, the ideal

$$\langle x^3 + x + 1 \rangle \subset \mathbb{F}_2[x]/\langle x^7 - 1 \rangle$$

leads to a code with $n = 7$, $d = 3$, and $|\mathcal{C}| = 16$.

Classical binary codes

A *binary code* of *length* n and *distance* d is a subset $\mathcal{C}$ of $\{0,1\}^n$ such that any two distinct words in $\mathcal{C}$ differ in at least d positions.

Example. $\{000000, 000111, 111000, 111111\}$ is a binary code of length $n = 6$ and minimum distance $d = 3$.

Some nice algebraic constructions exist; for instance, the ideal

$$\langle x^3 + x + 1 \rangle \subset \mathbb{F}_2[x]/\langle x^7 - 1 \rangle$$

leads to a code with $n = 7$, $d = 3$, and $|\mathcal{C}| = 16$.

Hamming distance

The function $d_H : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_{\geq 0}$ defined by

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$$

is a metric on $\{0,1\}^n$ called *Hamming distance*.

Binary codes are sets in $\{0,1\}^n$ which are well-separated under d_H.

Applications: data compression, error-correction, and the "prisoner's hat problem".

Hamming distance

The function $d_H : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_{\geq 0}$ defined by

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$$

is a metric on $\{0,1\}^n$ called *Hamming distance*.

Binary codes are sets in $\{0,1\}^n$ which are well-separated under d_H.

Applications: data compression, error-correction, and the "prisoner's hat problem".

Hamming distance

The function $d_H : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_{\geq 0}$ defined by

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i\}|$$

is a metric on $\{0,1\}^n$ called *Hamming distance*.

Binary codes are sets in $\{0,1\}^n$ which are well-separated under d_H.

Applications: data compression, error-correction, and the "prisoner's hat problem".

Error-correction

Consider the code $\mathcal{C}_7$ containing 0000000, 1101000, and closed under cyclic shifts and complements. This is the code coming from the ideal $\langle x^3 + x + 1 \rangle$ mentioned earlier.

The minimum Hamming distance of $\mathcal{C}_7$ is 3. We have

$$|\mathcal{C}_7| = 16 = \frac{2^7}{\binom{7}{0} + \binom{7}{1}}.$$

So every binary word is either in $\mathcal{C}_7$, or within one bit of a unique word in $\mathcal{C}_7$. That is, if we send words chosen from $\mathcal{C}_7$, the transmission is robust against one error.

Error-correction

Consider the code $\mathcal{C}_7$ containing 0000000, 1101000, and closed under cyclic shifts and complements. This is the code coming from the ideal $\langle x^3 + x + 1 \rangle$ mentioned earlier.

The minimum Hamming distance of $\mathcal{C}_7$ is 3. We have

$$|\mathcal{C}_7| = 16 = \frac{2^7}{\binom{7}{0} + \binom{7}{1}}.$$

So every binary word is either in $\mathcal{C}_7$, or within one bit of a unique word in $\mathcal{C}_7$. That is, if we send words chosen from $\mathcal{C}_7$, the transmission is robust against one error.

Distance between permutations

Hamming distance d_H makes sense in $\mathcal{S}_n$ if we write permutations in "one line notation" as rearrangements of the alphabet $\{1, 2, \ldots, n\}$.

Example.

35412 and
32415 are at distance 2.

This distance is still a metric; however, observe that $d_H = 1$ is never achieved for permutations.

Distance between permutations

Hamming distance d_H makes sense in $\mathcal{S}_n$ if we write permutations in "one line notation" as rearrangements of the alphabet $\{1, 2, \ldots, n\}$.

Example.

35412 and
32415 are at distance 2.

This distance is still a metric; however, observe that $d_H = 1$ is never achieved for permutations.

Distance between permutations

Alternatively, for $\sigma, \tau \in \mathcal{S}_n$, their Hamming distance is the number of non-fixed points of $\sigma\tau^{-1}$.

Example.

$$\begin{array}{ccc} 35412 & \to & (134)(25) \\ 32415 & \to & (134) \end{array}$$

have quotient (25), with $d_H = 2$ non-fixed points.

With this, it is clear that d_H is translation-invariant: $d_H(\sigma,\tau) = d_H(\sigma\alpha,\tau\alpha) = d_H(\alpha\sigma,\alpha\tau)$.

Distance between permutations

Alternatively, for $\sigma, \tau \in \mathcal{S}_n$, their Hamming distance is the number of non-fixed points of $\sigma\tau^{-1}$.

Example.

$$\begin{array}{lcl} 35412 & \rightarrow & (134)(25) \\ 32415 & \rightarrow & (134) \end{array}$$

have quotient (25), with $d_H = 2$ non-fixed points.

With this, it is clear that d_H is translation-invariant: $d_H(\sigma, \tau) = d_H(\sigma\alpha, \tau\alpha) = d_H(\alpha\sigma, \alpha\tau)$.

Permutation codes

A *permutation code* of length n and distance d is a subset $\Gamma \subseteq \mathcal{S}_n$ such that the distance between distinct members of Γ is at least d.

Example.

$$\{1234, 2143, 3412\}$$

is a permutation code of length 4 and distance 4. So is

$$\{1234, 2143, 3412, 4321\}.$$

Including any additional permutation will decrease the minimum distance.

Permutation codes

A *permutation code* of length n and distance d is a subset $\Gamma \subseteq \mathcal{S}_n$ such that the distance between distinct members of Γ is at least d.

Example.

$$\{1234, 2143, 3412\}$$

is a permutation code of length 4 and distance 4. So is

$$\{1234, 2143, 3412, 4321\}.$$

Including any additional permutation will decrease the minimum distance.

Permutation codes

A *permutation code* of length n and distance d is a subset $\Gamma \subseteq \mathcal{S}_n$ such that the distance between distinct members of Γ is at least d.

Example.

$$\{1234, 2143, 3412\}$$

is a permutation code of length 4 and distance 4. So is

$$\{1234, 2143, 3412, 4321\}.$$

Including any additional permutation will decrease the minimum distance.

A toy application

Suppose we wish to transmit information using amplitude modulation on electrical power lines.

Using an ordinary binary code has the disadvantage of introducing possibly long stretches of low (or high) voltage.

A permutation code enjoys the property that the sum of amplitudes on each codeword is a constant. So over a relatively short block of time, the average deviation from ambient voltage is zero.

Yet we have sent data with error-correction!

A toy application

Suppose we wish to transmit information using amplitude modulation on electrical power lines.

Using an ordinary binary code has the disadvantage of introducing possibly long stretches of low (or high) voltage.

A permutation code enjoys the property that the sum of amplitudes on each codeword is a constant. So over a relatively short block of time, the average deviation from ambient voltage is zero.

Yet we have sent data with error-correction!

A toy application

Suppose we wish to transmit information using amplitude modulation on electrical power lines.

Using an ordinary binary code has the disadvantage of introducing possibly long stretches of low (or high) voltage.

A permutation code enjoys the property that the sum of amplitudes on each codeword is a constant. So over a relatively short block of time, the average deviation from ambient voltage is zero.

Yet we have sent data with error-correction!

A toy application

Suppose we wish to transmit information using amplitude modulation on electrical power lines.

Using an ordinary binary code has the disadvantage of introducing possibly long stretches of low (or high) voltage.

A permutation code enjoys the property that the sum of amplitudes on each codeword is a constant. So over a relatively short block of time, the average deviation from ambient voltage is zero.

Yet we have sent data with error-correction!

The question

$\boxed{\text{Given } n \text{ and } d\text{, how large can a permutation code be with these parameters?}}$

The maximum is denoted $M(n, d)$; this is increasing in n and decreasing in d.

- finding a nice code gives a lower bound
- (linear) algebraic arguments offer upper bounds

Example. $M(n, 2) = n!$.
Example. $M(n, n) = n$.

The question

> Given n and d, how large can a permutation code be with these parameters?

The maximum is denoted $M(n, d)$; this is increasing in n and decreasing in d.

- finding a nice code gives a lower bound
- (linear) algebraic arguments offer upper bounds

Example. $M(n, 2) = n!$.

Example. $M(n, n) = n$.

The question

$\boxed{\text{Given } n \text{ and } d\text{, how large can a permutation code be with these parameters?}}$

The maximum is denoted $M(n,d)$; this is increasing in n and decreasing in d.

- finding a nice code gives a lower bound
- (linear) algebraic arguments offer upper bounds

Example. $M(n,2) = n!$.
Example. $M(n,n) = n$.

The question

$\boxed{\text{Given } n \text{ and } d\text{, how large can a permutation code be with these parameters?}}$

The maximum is denoted $M(n, d)$; this is increasing in n and decreasing in d.

- finding a nice code gives a lower bound
- (linear) algebraic arguments offer upper bounds

Example. $M(n, 2) = n!$.
Example. $M(n, n) = n$.

The alternating group

The alternating group A_n (or its coset) gives a maximum permutation code with $d = 3$.

Theorem

For $n \geq 3$, $M(n,3) = n!/2$.

Proof sketch.

In the group A_n, the quotient of any two permutations is even, so can't be a transposition. Therefore, $M(n,3) \geq |A_n| = n!/2$.

Conversely, if $|\Gamma| > n!/2$, there must exist two elements in Γ belonging to the same pigeonhole $\{\sigma, (12)\sigma\}$. This contradicts $d = 3$. $\square$

The alternating group

The alternating group A_n (or its coset) gives a maximum permutation code with $d = 3$.

Theorem

For $n \geq 3$, $M(n, 3) = n!/2$.

Proof sketch.

In the group A_n, the quotient of any two permutations is even, so can't be a transposition. Therefore, $M(n, 3) \geq |A_n| = n!/2$.
Conversely, if $|\Gamma| > n!/2$, there must exist two elements in Γ belonging to the same pigeonhole $\{\sigma, (12)\sigma\}$. This contradicts $d = 3$. $\square$

Recursive upper bound

Theorem
$M(n, d) \leq n\, M(n-1, d)$.

Proof sketch.
Take all codewords which begin with a common symbol, and delete that symbol. After relabelling, this is a permutation code of length $n-1$ and minimum distance d. □

Corollary (Johnson bound)
$M(n, d) \leq n(n-1)\cdots(d+1)d = n!/(d-1)!$.

Recursive upper bound

Theorem

$M(n, d) \leq n\, M(n-1, d)$.

Proof sketch.

Take all codewords which begin with a common symbol, and delete that symbol. After relabelling, this is a permutation code of length $n-1$ and minimum distance d. □

Corollary (Johnson bound)

$M(n, d) \leq n(n-1)\cdots(d+1)d = n!/(d-1)!$.

Recursive upper bound

Theorem

$M(n, d) \leq n\, M(n-1, d)$.

Proof sketch.

Take all codewords which begin with a common symbol, and delete that symbol. After relabelling, this is a permutation code of length $n-1$ and minimum distance d. □

Corollary (Johnson bound)

$M(n, d) \leq n(n-1) \cdots (d+1)d = n!/(d-1)!$.

Sphere-packing upper bound

Theorem

$$M(n,d) \leq \frac{n!}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k} D_k}.$$

Proof sketch.

The denominator counts the ball B of radius $r = \frac{d-1}{2}$ in $\mathcal{S}_n$. If $\Gamma \subseteq \mathcal{S}_n$ is a permutation code realizing $M(n,d)$, then the balls of radius r centred at the codewords must be disjoint. That is,

$$|\Gamma| \cdot |B| \leq n!.$$

□

Sphere-packing upper bound

Theorem

$$M(n,d) \leq \frac{n!}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k} D_k}.$$

Proof sketch.

The denominator counts the ball B of radius $r = \frac{d-1}{2}$ in $\mathcal{S}_n$. If $\Gamma \subseteq \mathcal{S}_n$ is a permutation code realizing $M(n,d)$, then the balls of radius r centred at the codewords must be disjoint. That is,

$$|\Gamma| \cdot |B| \leq n!.$$

$\square$

Constructions and lower bounds

- MOLS(n) lead to permutation codes of distance $n-1$. (Colbourn, Kløve, Ling)
- Sharply k-transitive permutation groups lead to maximum permutation codes of distance $n-k+1$. (Deza, Vanstone)
- Permutation polynomials of degree t can be used for distance $n-t$. (Chu)
- Probabilistic techniques have seen success for distance $n-n^{1-\theta}$. (Keevash, Ku)

Constructions and lower bounds

- MOLS(n) lead to permutation codes of distance $n-1$. (Colbourn, Kløve, Ling)
- Sharply k-transitive permutation groups lead to maximum permutation codes of distance $n-k+1$. (Deza, Vanstone)
- Permutation polynomials of degree t can be used for distance $n-t$. (Chu)
- Probabilistic techniques have seen success for distance $n-n^{1-\theta}$. (Keevash, Ku)

Constructions and lower bounds

- MOLS(n) lead to permutation codes of distance $n-1$. (Colbourn, Kløve, Ling)
- Sharply k-transitive permutation groups lead to maximum permutation codes of distance $n-k+1$. (Deza, Vanstone)
- Permutation polynomials of degree t can be used for distance $n-t$. (Chu)
- Probabilistic techniques have seen success for distance $n-n^{1-\theta}$. (Keevash, Ku)

Constructions and lower bounds

- MOLS(n) lead to permutation codes of distance $n - 1$. (Colbourn, Kløve, Ling)
- Sharply k-transitive permutation groups lead to maximum permutation codes of distance $n - k + 1$. (Deza, Vanstone)
- Permutation polynomials of degree t can be used for distance $n - t$. (Chu)
- Probabilistic techniques have seen success for distance $n - n^{1-\theta}$. (Keevash, Ku)

Constructions and lower bounds

- MOLS(n) lead to permutation codes of distance $n-1$. (Colbourn, Kløve, Ling)
- Sharply k-transitive permutation groups lead to maximum permutation codes of distance $n-k+1$. (Deza, Vanstone)
- Permutation polynomials of degree t can be used for distance $n-t$. (Chu)
- Probabilistic techniques have seen success for distance $n-n^{1-\theta}$. (Keevash, Ku)

Other explicit constructions

- Computer search
  - Greedy selection of codewords, with modifications
  - Clique search, often assuming automorphisms
- Partitioning and gluing
- Isometric embeddings of some structure into $\mathcal{S}_n$

MOLS construction

A♠	J♡	Q♣	K♢
J♣	A♢	K♠	Q♡
Q♢	K♣	A♡	J♠
K♡	Q♠	J♢	A♣

Record the list of row indices for each symbol in each square:
A : 1234, J : 2143, Q : 3412, K : 4321,
$\spadesuit$: 1423, $\heartsuit$: 4132, $\diamondsuit$: 3241, $\clubsuit$: 2314.

MOLS construction

A♠	J♡	Q♣	K♢
J♣	A♢	K♠	Q♡
Q♢	K♣	A♡	J♠
K♡	Q♠	J♢	A♣

Record the list of row indices for each symbol in each square:
A : 1234, J : 2143, Q : 3412, K : 4321,
$\spadesuit$: 1423, $\heartsuit$: 4132, $\diamondsuit$: 3241, $\clubsuit$: 2314.

MOLS construction

A♠	J♡	Q♣	K♢
J♣	A♢	K♠	Q♡
Q♢	K♣	A♡	J♠
K♡	Q♠	J♢	A♣

Record the list of row indices for each symbol in each square:
A : 1234, J : 2143, Q : 3412, K : 4321,
$\spadesuit$: 1423, $\heartsuit$: 4132, $\diamondsuit$: 3241, $\clubsuit$: 2314.

A challenging case: $d = 4$

Consider upper bounds on $M(n, 4)$.

Johnson bound: $n!/6$.

Sphere-packing bound: $n!$. This is bad because n is even.

Theorem

$M(n, 4) = (n-1)!$

Proof idea.

Blob-packing: The blobs $A_\sigma = \{(1i)\sigma : 1 \leq i \leq n\}$, centred at codewords $\sigma \in \Gamma$, must be disjoint in any permutation code of distance 4. We have $|A_\sigma| = n$ for each σ, so $|\Gamma| \leq n!/n$. □

A challenging case: $d = 4$

Consider upper bounds on $M(n, 4)$.

Johnson bound: $n!/6$.

Sphere-packing bound: $n!$. This is bad because n is even.

Theorem

$M(n, 4) = (n-1)!$

Proof idea.

Blob-packing: The blobs $A_\sigma = \{(1i)\sigma : 1 \le i \le n\}$, centred at codewords $\sigma \in \Gamma$, must be disjoint in any permutation code of distance 4. We have $|A_\sigma| = n$ for each σ, so $|\Gamma| \le n!/n$. □

A challenging case: $d = 4$

Consider upper bounds on $M(n, 4)$.

Johnson bound: $n!/6$.

Sphere-packing bound: $n!$. This is bad because n is even.

Theorem

$M(n, 4) = (n-1)!$

Proof idea.

Blob-packing: The blobs $A_\sigma = \{(1i)\sigma : 1 \le i \le n\}$, centred at codewords $\sigma \in \Gamma$, must be disjoint in any permutation code of distance 4. We have $|A_\sigma| = n$ for each σ, so $|\Gamma| \le n!/n$. □

Association Schemes

A *k-class association scheme* on a set X is a list of binary relations $R_0, \dots, R_k$ on X satisfying

- R_0 is the identity
- the relations partition X^2, and
- a strong regularity condition

> given x and y with $(x, y) \in R_h$, the number of $z \in X$ for which both $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant depending only on $h, i, j \in \{0, \dots, k\}$.

These values p_{ij}^h are called the *structure constants*.

Association Schemes

A *k-class association scheme* on a set X is a list of binary relations $R_0, \ldots, R_k$ on X satisfying

- R_0 is the identity
- the relations partition X^2, and
- a strong regularity condition

given x and y with $(x, y) \in R_h$, the number of $z \in X$ for which both $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant depending only on $h, i, j \in \{0, \ldots, k\}$.

These values p_{ij}^h are called the *structure constants*.

Association Schemes

A *k-class association scheme* on a set X is a list of binary relations $R_0, \ldots, R_k$ on X satisfying

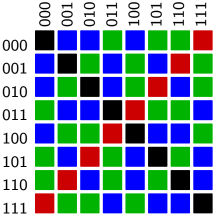
- R_0 is the identity
- the relations partition X^2, and
- a strong regularity condition

given x and y with $(x, y) \in R_h$, the number of $z \in X$ for which both $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant depending only on $h, i, j \in \{0, \ldots, k\}$.

These values p_{ij}^h are called the *structure constants*.

Hamming Scheme

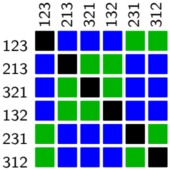
Example. Let $X = \{0,1\}^n$, R_i be disagreement in i places.



This is the *Hamming scheme*.

The Conjugacy Scheme

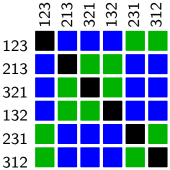
The symmetric group defines an association scheme, called the *conjugacy scheme*, where $X = \mathcal{S}_n$, relations are indexed by partitions of n, and $(\sigma, \tau) \in R_\mu$ if and only if $\sigma\tau^{-1}$ belongs to conjugacy class μ.



$$p_{ij}^h = \frac{|C_i||C_j|}{n!} \sum_{\chi} \frac{\chi(\phi_i)\chi(\phi_j)\chi(\phi_h)}{\chi(\mathrm{id})}$$

The Conjugacy Scheme

The symmetric group defines an association scheme, called the *conjugacy scheme*, where $X = \mathcal{S}_n$, relations are indexed by partitions of n, and $(\sigma, \tau) \in R_\mu$ if and only if $\sigma\tau^{-1}$ belongs to conjugacy class μ.



$$p_{ij}^h = \frac{|C_i||C_j|}{n!} \sum_\chi \frac{\chi(\phi_i)\chi(\phi_j)\chi(\phi_h)}{\chi(\mathrm{id})}$$

Cliques

Let $(X, \{R_i\})$ be a k-class association scheme.

For $J \subset \{1, \ldots, k\}$, a *J-clique* is a subset W of X such that for any $w_1, w_2 \in W$, $(w_1, w_2) \in R_j$ for some $j \in J$.

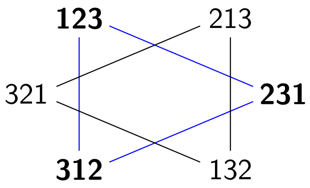
In the conjugacy scheme, cliques model permutation codes.

Cliques

Let $(X, \{R_i\})$ be a k-class association scheme.

For $J \subset \{1, \ldots, k\}$, a *J-clique* is a subset W of X such that for any $w_1, w_2 \in W$, $(w_1, w_2) \in R_j$ for some $j \in J$.

In the conjugacy scheme, cliques model permutation codes.



Delsarte LP bound

Delsarte's linear programming bound for J-cliques, specialized to permutation codes, is as follows.

$$\begin{array}{lll} \text{maximize:} & a_0 + a_1 + \cdots + a_{m-1} & \\ \text{subject to:} & \sum_{0 \le i < m} a_i \chi_k(\phi_i) \ge 0 & \text{for } 0 \le k < m, \\ & a_0 = 1, a_i \ge 0, & \text{and} \\ & a_i = 0 & \text{if } d_H(\mathrm{id}, \phi_i) \notin D. \end{array}$$

Using this, one can obtain decent upper bounds on $M(n, d)$ for various small parameters, say up to $n = 15$.

Sharpened bound for distance four

Theorem (joint with N. Sawchuck)

If n is a square integer,

$$M(n,4) \leq n!/(n+2).$$

The proof idea is to show

$$\chi(1) + 3\chi(2) + (n-2)\chi(3) \geq 0$$

using 'local optimization' on integer partitions of n.

Sharpened bound for distance four

Theorem (joint with N. Sawchuck)

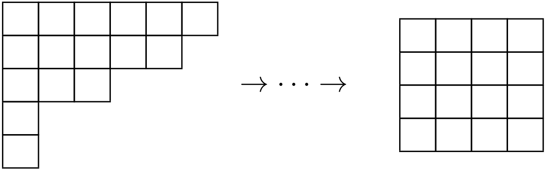
If n is a square integer,

$$M(n,4) \leq n!/(n+2).$$

The proof idea is to show

$$\chi(1) + 3\chi(2) + (n-2)\chi(3) \geq 0$$

using 'local optimization' on integer partitions of n.



Sharpened bound for distance four

Theorem (joint with N. Sawchuck)

If n is a square integer,

$$M(n,4) \leq n!/(n+2).$$

The full bound is

$$\frac{n!}{M(n,4)} \geq 1+\frac{(n+1)n(n-1)}{n(n-1)-(n-k^2)((k+1)^2-n)((k+2)(k-1)-n)}$$

for $k^2 \leq n \leq k^2+k-2$, which gives the best improvement for $n \approx k^2+k/2$.

What can we construct with distance four

On the construction side, it is difficult to do much better than greedy for $d = 4$:

$$M(n,4) \geq \frac{n!}{B_3} = \frac{n!}{1 + \binom{n}{2} + 2\binom{n}{3}}.$$

Can we shrink the gap between these bounds for $M(n,4)$?

What can we construct with distance four

On the construction side, it is difficult to do much better than greedy for $d = 4$:

$$M(n,4) \geq \frac{n!}{B_3} = \frac{n!}{1 + \binom{n}{2} + 2\binom{n}{3}}.$$

Can we shrink the gap between these bounds for $M(n,4)$?

Open problems

- Find or improve bounds on the smallest undecided cases $M(7,4)$ and $M(7,5)$. All we know is $343 \leq M(7,4) \leq 535$ and $77 \leq M(7,5) \leq 134$.
- Obtain better constructions for $M(n, n-1)$ when n is not a prime power. For general n, we only have $M(n, n-1) \geq n^{1+1/14.8}$, coming from the lower bound on mutually orthogonal latin squares. Some improvements are possible for special values of n.
- Study codes constrained by prescribed distance sets, or (more generally) conjugacy classes. As a special case, one has "equidistant permutation arrays" in which any two distinct codewords have the same distance.
- Add to the growing body of work on other metrics on S_n, such as the Kendall-τ metric or Ulam metric.
- Further study generalizations in two directions: "constant composition codes" and "injection codes".

Open problems

- Find or improve bounds on the smallest undecided cases $M(7,4)$ and $M(7,5)$. All we know is $343 \leq M(7,4) \leq 535$ and $77 \leq M(7,5) \leq 134$.
- Obtain better constructions for $M(n,n-1)$ when n is not a prime power. For general n, we only have $M(n,n-1) \geq n^{1+1/14.8}$, coming from the lower bound on mutually orthogonal latin squares. Some improvements are possible for special values of n.
- Study codes constrained by prescribed distance sets, or (more generally) conjugacy classes. As a special case, one has "equidistant permutation arrays" in which any two distinct codewords have the same distance.
- Add to the growing body of work on other metrics on $\mathcal{S}_n$, such as the Kendall-τ metric or Ulam metric.
- Further study generalizations in two directions: "constant composition codes" and "injection codes".

Open problems

- Find or improve bounds on the smallest undecided cases $M(7,4)$ and $M(7,5)$. All we know is $343 \leq M(7,4) \leq 535$ and $77 \leq M(7,5) \leq 134$.
- Obtain better constructions for $M(n, n-1)$ when n is not a prime power. For general n, we only have $M(n, n-1) \geq n^{1+1/14.8}$, coming from the lower bound on mutually orthogonal latin squares. Some improvements are possible for special values of n.
- Study codes constrained by prescribed distance sets, or (more generally) conjugacy classes. As a special case, one has "equidistant permutation arrays" in which any two distinct codewords have the same distance.
- Add to the growing body of work on other metrics on $\mathcal{S}_n$, such as the Kendall-τ metric or Ulam metric.
- Further study generalizations in two directions: "constant composition codes" and "injection codes".

Open problems

- Find or improve bounds on the smallest undecided cases $M(7,4)$ and $M(7,5)$. All we know is $343 \leq M(7,4) \leq 535$ and $77 \leq M(7,5) \leq 134$.
- Obtain better constructions for $M(n, n-1)$ when n is not a prime power. For general n, we only have $M(n, n-1) \geq n^{1+1/14.8}$, coming from the lower bound on mutually orthogonal latin squares. Some improvements are possible for special values of n.
- Study codes constrained by prescribed distance sets, or (more generally) conjugacy classes. As a special case, one has "equidistant permutation arrays" in which any two distinct codewords have the same distance.
- Add to the growing body of work on other metrics on $\mathcal{S}_n$, such as the Kendall-τ metric or Ulam metric.
- Further study generalizations in two directions: "constant composition codes" and "injection codes".

Open problems

- Find or improve bounds on the smallest undecided cases $M(7,4)$ and $M(7,5)$. All we know is $343 \leq M(7,4) \leq 535$ and $77 \leq M(7,5) \leq 134$.
- Obtain better constructions for $M(n, n-1)$ when n is not a prime power. For general n, we only have $M(n, n-1) \geq n^{1+1/14.8}$, coming from the lower bound on mutually orthogonal latin squares. Some improvements are possible for special values of n.
- Study codes constrained by prescribed distance sets, or (more generally) conjugacy classes. As a special case, one has "equidistant permutation arrays" in which any two distinct codewords have the same distance.
- Add to the growing body of work on other metrics on $\mathcal{S}_n$, such as the Kendall-τ metric or Ulam metric.
- Further study generalizations in two directions: "constant composition codes" and "injection codes".

References

W. Chu, C.J. Colbourn and P.J. Dukes, Constructions for permutation codes in powerline communications, Designs Codes Cryptography (2004).

P.J. Dukes, Coding with injections, Designs Codes Cryptography (2012).

P.J. Dukes and M. Bogaerts, Semidefinite programming for permutation codes, Discrete Math. (2014).

P.J. Dukes and N. Sawchuck, Bounds on permutation codes of distance four, J. Algebraic Combinatorics (2010).

- THE END -