A Construction of Permutation Codes and Improvement to the Gilbert-Varshamov Bound

Lingfei Jin

Fudan University

The 5th Sino-Korea International Conference on Coding Theory and Its Related Topics

2018.7.5

outline

- Introduction to permutation codes
- Our results
- Comparision

outline

- Introduction to permutation codes
- Our results
- Comparision

outline

- Introduction to permutation codes
- Our results
- Comparision

outline

- Introduction to permutation codes
- Our results
- Comparision

SECTION 1: Introduction to Permutation Codes

- Permutation codes (permutation arrays) were first studied as a combinatorial problem in 1977.
- This topic began to attract attentions for its application in power line communications, block ciphers, and multilevel flash memory from 2003.

(1) *P. Frankl and M. Deza, On the maximum number of permutations with given maximal or minimal distance, J. Combinatorial Theory Series A, Vol. 50, no 5, pp. 352-360,1977.*

(2) *N. Pavlidou, A. Vink, J. Yazdani and B. Honary, Power line communications: State of the art and future trends, IEEE Commun. Mag., vol. 41, no. 4, 2003.*

(3) *A. Jiang, R Mateescu and J. Bruck, Rank modulation for flash memories, in Proc. IEEE Int. Symp. Information Theory, 1736-1740, 2008*

Permutation group

A permutation σ is a bijection from the set $\{\alpha_1, \cdots, \alpha_n\}$ to itself.

$$\sigma = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \sigma(\alpha_1) & \sigma(\alpha_2) & \sigma(\alpha_3) & \cdots & \sigma(\alpha_n) \end{pmatrix}$$

- Let $\mathcal{S}_n$ be the set of all permutations of length n. Then $|\mathcal{S}_n| = n!$.
- Let A_n be the set of all even permutations of length n. Then $|A_n| = n!/2$.

Permutation group

A permutation σ is a bijection from the set $\{\alpha_1, \cdots, \alpha_n\}$ to itself.

$$\sigma = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \sigma(\alpha_1) & \sigma(\alpha_2) & \sigma(\alpha_3) & \cdots & \sigma(\alpha_n) \end{pmatrix}$$

- Let $\mathcal{S}_n$ be the set of all permutations of length n. Then $|\mathcal{S}_n| = n!$.
- Let A_n be the set of all even permutations of length n. Then $|A_n| = n!/2$.

- cycle notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

In cycle notation $\sigma = (125)(34)$.

- Any permutation can be uniquely represented as products of disjoint cycles.

- cycle notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

In cycle notation $\sigma = (125)(34)$.

- Any permutation can be uniquely represented as products of disjoint cycles.

Permutation Code

We can write permutations in "one line notation" as rearrangements of the alphabet $\{1, 2, \cdots, n\}$.

Definition

Let $\mathcal{S}_n$ be the set of all permutations of length n. A subset Γ of $\mathcal{S}_n$ is called a permutation code. The length of C is n and each permutation in C is called a codeword.

- Applications: power line communications, block ciphers, and multilevel flash memory.

Hamming distance

Definition

The Hamming distance between two permutations $\sigma, \tau \in \mathcal{S}_n$ is defined to be the number of coordinates that they differ,i.e.,

$$d_H(\sigma, \tau) = \sharp\{\alpha_i \in \{\alpha_1, \cdots, \alpha_n\} : \ \sigma(\alpha_i) \neq \tau(\alpha_i)\}$$

Alternatively, for $\sigma, \tau \in S_n$, their Hamming distance is the number of nonfixed points of $\sigma^{-1}\tau$.

$$d_H(\sigma, \tau) = d_H(id, \sigma^{-1}\tau)$$

where id is the identity of S_n.

- $d_H(\sigma, \tau)$ is the sum of length of disjoint cycles of $\sigma^{-1}\tau$

Example

Let $\sigma = 23451$ *and* $\tau = 12543$, *then*

$$d_H(\sigma, \tau) = 5.$$

One the other hand, $\sigma^{-1}\tau = 51432$,

$$d_H(id, \sigma^{-1}\tau) = 5.$$

The cycle notation is $\sigma^{-1}\tau = (152)(34)$

Note that distance 1 is never achieved for permutations, i.e., $d \geqslant 2$.

- An (n, d) permutation code is a subset Γ of $\mathcal{S}_n$ such that Hamming distance between distinct members of Γ is at least d.

- Example:

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

is an $(4, 4)$ permutation code. So as

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

Including any additional permutation will decrease the minimum distance.

- An (n, d) permutation code is a subset Γ of $\mathcal{S}_n$ such that Hamming distance between distinct members of Γ is at least d.

- Example:

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

is an $(4, 4)$ permutation code. So as

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

Including any additional permutation will decrease the minimum distance.

- $M(n, d)$: the maximum size of permutation codes of length n and minimum distance d.

Problem: Given n and d, how large can $M(n, d)$ be?

(1) Finding a nice code gives a lower bound;

(2) Algebraic arguments offer an upper bound.

- It is difficult to determine the exact value of $M(n, d)$.

- $M(n, d)$: the maximum size of permutation codes of length n and minimum distance d.

Problem: Given n and d, how large can $M(n, d)$ be?

(1) Finding a nice code gives a lower bound;

(2) Algebraic arguments offer an upper bound.

- It is difficult to determine the exact value of $M(n, d)$.

Basic results on $M(n, d)$

(i) $M(n, 2) = n!$;

(ii) $M(n, n) = n$;

(iii) $M(n, 3) = n!/2$;

Proof sketch:

In the group A_n, the quotient of any two permutations is even, so can not be a transposition. Thus

$$M(n, 3) \geqslant |A_n| = n!/2$$

Conversely, if $|\Gamma| > n!/2$, there must exist an odd permutation $\tau \in \Gamma$. Then there exists an even permutation $\sigma \in \Gamma$ s.t.$(12)\tau = \sigma$. This contradicts $d = 3$.

Basic results on $M(n, d)$

(i) $M(n, 2) = n!$;

(ii) $M(n, n) = n$;

(iii) $M(n, 3) = n!/2$;

Proof sketch:

In the group A_n, the quotient of any two permutations is even, so can not be a transposition. Thus

$$M(n, 3) \geqslant |A_n| = n!/2$$

Conversely, if $|\Gamma| > n!/2$, there must exist an odd permutation $\tau \in \Gamma$. Then there exists an even permutation $\sigma \in \Gamma$ s.t.$(12)\tau = \sigma$. This contradicts $d = 3$.

Basic results on $M(n, d)$

(i) $M(n, 2) = n!$;

(ii) $M(n, n) = n$;

(iii) $M(n, 3) = n!/2$;

Proof sketch:

In the group A_n, the quotient of any two permutations is even, so can not be a transposition. Thus

$$M(n, 3) \geqslant |A_n| = n!/2$$

Conversely, if $|\Gamma| > n!/2$, there must exist an odd permutation $\tau \in \Gamma$. Then there exists an even permutation $\sigma \in \Gamma$ s.t.$(12)\tau = \sigma$. This contradicts $d = 3$.

(v) $M(n,d) \leqslant nM(n-1,d)$.

Proof sketch:

Take all codewords which begin with a common symbol, delete that symbol. This a permutation code of length $n-1$ and distance d after relabelling.

Theorem (Johnson Bound)

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

(v) $M(n,d) \leqslant nM(n-1,d)$.

Proof sketch:

Take all codewords which begin with a common symbol, delete that symbol. This a permutation code of length $n-1$ and distance d after relabelling.

Theorem (Johnson Bound)

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

- Except for small lengths, not much results has been made for $4 \leqslant d \leqslant n-1$.
- Researchers focus on searching for good lower and upper bounds for $M(n, d)$.

Upper bound: Sphere-packing bound

- D(n,k): the set of all permutations in S_n which are exactly at distance k from the identity, $k = 1, 2, \cdots, n$, i.e.,

$$D(n,k) = \{\sigma \in S_n : \quad d_H(\sigma, id) = k\}.$$

$$|D(n,k)| = D_k \binom{n}{k},$$

where D_k is the number of derangements of order k, i.e.,$D_k = k! \sum_{j=0}^{k} (-1)^j / j!$, with convention that $D_0 = 0$.

$$M(n,d) \leqslant \frac{n!}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} |D(n,k)|}$$

Lower bound

The only general lower bound is the following GV bound.

Theorem (Gilbert-Varshamov bound)

One has

$$M(n,d) \geqslant \frac{n!}{V(n,d-1)} = \frac{n!}{\sum_{i=0}^{d-1} \binom{n}{i} D_i}, \tag{1}$$

where $V(n,r)$ stands for the volume of a ball of radius r in the Hamming space $\mathcal{S}_n$.

Case $d = 4$

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

Johnson bound: $n!/6$.

Sphere-Packing bound: $n!$

Theorem (Frankl and Deza, 1977)

$M(n, 4) \leqslant (n-1)!$

Case $d = 4$

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

Johnson bound: $n!/6$.

Sphere-Packing bound: $n!$

Theorem (Frankl and Deza, 1977)

$M(n, 4) \leqslant (n-1)!$

An improved upper bound for $d = 4$

Theorem (Duckes and Sawchuck,2010)

If $k^2 \leqslant n \leqslant k^2 + k - 2$ for some integer $k \geqslant 2$, then

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

- The idea is to use linear programming and characters of $\mathcal{S}_n$.
- If n is a square integer,

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

Lower bound for $M(n, 4)$

Consider the GV bound for $d = 4$.

$$M(n, 4) \geqslant \frac{6n!}{2n^3 - 3n^2 + n + 6}$$

- For example, $M(4, 4) = 4$.
- The Johnson bound $M(n, 4) = n!/6$ can be attained for $n = 4, 5, 6$.

- For small values of n and d, researchers have developed many computer searching strategies.
- The following paper computed the upper and lower bounds for $6 \leqslant n \leqslant 18, 4 \leqslant d \leqslant 18$.

D. Smith and R. Montemanni, A new table of permutation codes, Des. Codes Cryptogr., vol. 63, no. 2, pp. 241-253,2010.

The GV bound still remains to be the best asymptotical lower bound except for a recent improvement in the case of constant minimum distance.

Theorem (Gao, Yang and Ge,2013)

When d is fixed and n goes into infinity, we have

$$\frac{M_{GYG}(n,d)}{M_{GV}(n,d)} = \Omega(\log(n))$$

- F. Gao, Y. Yang and G. Ge, An improvement on the Gilbert-Varshamov bound for permutation codes, IEEE Trans. on IT, Vol 59, NO. 5, 2013.

SECTION 2: Our Construction

Our result

We employed the theory of function fields to give a new and simple lower bound on $M(n, d)$, namely,

Theorem (Main Theorem)

For two integers d, n with $4 \leqslant d \leqslant n$, one has

$$M(n, d) \geqslant \frac{n!}{p^{d-2}}, \tag{2}$$

where p is the smallest prime bigger than or equal to n.

Sketch of the proof:

- Step 1: Find a permutation code with size $M \geqslant \frac{n!}{p^{d-2}}$.
- Step 2: Prove that the permutation code has distance at least d.

- $n \leqslant p$ where p is a prime.
- $\alpha_1, \cdots, \alpha_n$ are n distinct elements in $\mathbb{F}_p$.
- $f(x)$ is an irr. polynomial with degree $d-2$ ($d \geqslant 4$)

Consider quotient ring $\mathbb{F}_p[x]/(f^2)$. Denote by G the multiplicative group of $\mathbb{F}_p[x]/(f^2)$, i.e.,

$$\begin{aligned} G := (F_p[x]/(f^2))^* &= (F_p[x]/(f^2)) \setminus \{gf : \deg g \leqslant d-3\} \\ &= \{\bar{h} \in \mathbb{F}_p[x]/(f^2) : \ \gcd(h, f) = 1\} \end{aligned}$$

- $n \leqslant p$ where p is a prime.
- $\alpha_1, \cdots, \alpha_n$ are n distinct elements in $\mathbb{F}_p$.
- $f(x)$ is an irr. polynomial with degree $d-2$ ($d \geqslant 4$)

Consider quotient ring $\mathbb{F}_p[x]/(f^2)$. Denote by G the multiplicative group of $\mathbb{F}_p[x]/(f^2)$, i.e.,

$$\begin{aligned} G := (F_p[x]/(f^2))^* &= (F_p[x]/(f^2)) \setminus \{gf : \deg g \leqslant d-3\} \\ &= \{\bar{h} \in \mathbb{F}_p[x]/(f^2) : \ \gcd(h, f) = 1\} \end{aligned}$$

$$G := (F_p[x]/(f^2))^* = (F_p[x]/(f^2)) \setminus \{gf : \deg g \leqslant d-3\}$$

We can see that

$$|G| = p^{2(\deg f)} - p^{\deg f}.$$

Now let us consider G^p. For any $h \in G$,

$$h = af + b \in G, \quad (b, f) = 1, b \neq 0, \deg b < \deg f.$$

$$h^p = a^p f^p + b^p = b^p \in G^p, \quad (b, f) = 1, b \neq 0, \deg b < \deg f.$$

$$G := (F_p[x]/(f^2))^* = (F_p[x]/(f^2)) \setminus \{gf : \deg g \leqslant d-3\}$$

We can see that

$$|G| = p^{2(\deg f)} - p^{\deg f}.$$

Now let us consider G^p. For any $h \in G$,

$$h = af + b \in G, \quad (b, f) = 1, b \neq 0, \deg b < \deg f.$$

$$h^p = a^p f^p + b^p = b^p \in G^p, \quad (b, f) = 1, b \neq 0, \deg b < \deg f.$$

$$|G^p| = p^{\deg f} - 1$$

Therefore,

$$|G/G^p| = \frac{|G|}{|G^p|} = p^{\deg f}$$

An element of G/G^p is denoted by $[h]$ for any $\bar{h} \in G$.

Our construction

Define the map

$$\pi : \quad \mathcal{S}_n \to G/G^p; \qquad \sigma \mapsto \left[\prod_{i=1}^{n}(x-\alpha_i)^{\sigma(i)}\right]. \tag{3}$$

By the Pigeonhole Principle, there exists an element $[w] \in G/G^p$ such that the size of $\pi^{-1}([w])$ is at least $\frac{n!}{p^{d-2}}$. Next we will prove that $\pi^{-1}([w])$ has minimum Hamming distance at least d.

Now we are going to prove the code has distance at least d.

Let σ and τ be two distinct elements in $\pi^{-1}([w])$. Then

$$\pi(\sigma) = \pi(\tau) = [w], i.e., \left[\prod_{i=1}^{n}(x-\alpha_i)^{\sigma(i)-\tau(i)}\right] = [1].$$

In other words, there exist nonzero polynomials $h(x)$ and $g(x)$ with $\gcd(h(x)g(x), f(x)) = 1$ and

$$\overline{\prod_{i=1}^{n}(x-\alpha_i)^{\sigma(i)-\tau(i)}} = \overline{(g(x)/h(x))^p}$$

as elements of G (note that an element of $G := (F_p[x]/(f^2))^*$ is a residue class).

This implies that

$$\frac{h(x)^p \prod_{i=1}^{n}(x-\alpha_i)^{\sigma(i)-\tau(i)}}{g(x)^p} \equiv 1 \bmod f(x)^2. \tag{4}$$

Denote by z the rational function on the left side of (4) and consider extension $\mathbb{F}_q(x)/\mathbb{F}_q(z)$.

- By applying Hurwitz genus formula, we can complete the proof.

This implies that

$$\frac{h(x)^p \prod_{i=1}^{n}(x-\alpha_i)^{\sigma(i)-\tau(i)}}{g(x)^p} \equiv 1 \bmod f(x)^2. \tag{4}$$

Denote by z the rational function on the left side of (4) and consider extension $\mathbb{F}_q(x)/\mathbb{F}_q(z)$.

- By applying Hurwitz genus formula, we can complete the proof.

Corollary

Denote by $M_{GV}(n,d)$ and $M_{New}(n,d)$ the GV bound and our bound, respectively, i.e.,

$$M_{GV}(n,d) = \frac{n!}{V(n,d-1)}, \qquad M_{New}(n,d) = \frac{n!}{p^{d-2}},$$

where p is the smallest prime such that $n \leqslant p$. Then

$$\frac{M_{New}(n,d)}{M_{GV}(n,d)} = \Omega(n)$$

for a constant d.

Proof:

As there exists a prime p between n and $2n-1$, we have $p < 2n$. Thus, we have

$$\begin{aligned}\frac{M_{New}(n,d)}{M_{GV}(n,d)} &= \frac{V(n,d-1)}{p^{d-2}} \geqslant \frac{\binom{n}{d-1} D_{d-1}}{(2n)^{d-2}} \\ &\geqslant \frac{D_{d-1}}{(d-1)!2^{d-2}} \times \frac{(n-d+2)^{d-2}}{n^{d-2}} \cdot n \\ &= \Omega(n).\end{aligned}$$

If n is a prime, then the following result shows that our bound still improves the GV bound by a factor n even for $d = O(\sqrt{n})$.

Corollary

If n is a prime, then we have

$$\frac{M_{New}(n,d)}{M_{GV}(n,d)} = \Omega(n)$$

for $d = O(\sqrt{n})$.

$$\frac{M_{New}(n,d)}{M_{GV}(n,d)} = \frac{V(n,d-1)}{n^{d-2}} \geqslant \frac{\binom{n}{d-1} D_{d-1}}{n^{d-2}}$$

$$\geqslant cn \times \prod_{i=1}^{d-2} \left(1 - \frac{i}{n}\right),$$

where c is a positive constant. Thus, it is sufficient to show that $\prod_{i=1}^{d-2} \left(1 - \frac{i}{n}\right) = \Omega(1)$ for $d = O(\sqrt{n})$.

Numerical comparisons

Table: Lower bound on $M(n,d)$ for $16 \leqslant n \leqslant 19$ and $4 \leqslant d \leqslant 5$

(n,d)	$M_{New}(n,d)$	$M_{GYG}(n,d)$	$M_{GV}(n,d)$
$(16,4)$	7.2397×10^{10}	5.744×10^{10}	1.6859×10^{10}
$(16,5)$	4.2586×10^{9}	3.3179×10^{9}	1.1873×10^{9}
$(17,4)$	1.2307×10^{12}	7.9309×10^{11}	2.736×10^{11}
$(17,5)$	7.2397×10^{10}	4.5006×10^{10}	1.552×10^{10}
$(18,4)$	1.7735×10^{13}	1.2331×10^{13}	3.5847×10^{12}
$(18,5)$	9.3342×10^{11}	6.5502×10^{11}	2.1831×10^{11}
$(19,4)$	3.3696×10^{14}	2.0392×10^{14}	5.7651×10^{13}
$(19,5)$	1.7735×10^{13}	1.0181×10^{13}	3.2882×10^{12}

Thanks for your attention!