Some progress on permutation codes

Yiting Yang

College of Mathematical Science

Tongji University

The 10th Cross-strait conference on graph theory and combinatorics, Taichung

August 20, 2019

Outline

Permutation code

Definition

Let S_n be the set of all permutations of length n. The *permutation code* C is just a subset of S_n equipped with a distance metric.

The *length* of C is n and each permutation in C is called a *codeword*.

Application: Powerline communication and Flash memories

Hamming and Chebyshev metrics

Definition

For two distinct permutations $\sigma, \pi \in S_n$, their *Hamming distance* $d_H(\sigma, \pi)$ is the number of elements that they differ.

Definition

Let $\pi = \pi_1\pi_2\ldots,\pi_n, \sigma = \sigma_1\sigma_2\ldots,\sigma_n \in S_n$. The *Chebyshev distance* between π and σ is

$$d_C(\pi, \sigma) = \max\{|\pi_j - \sigma_j||1 \le j \le n\}.$$

Permutation code of minimum distance d

Example

Let $\sigma = 23451$ and $\pi = 12543$. Then

$$d_H(\sigma, \pi) = 5 \text{ and } d_C(\sigma, \pi) = 2.$$

We say a permutation code C is a Hamming (n, d)-permutation code if the Hamming distance of any pair of distinct permutations in C is at least d.

Similarly, C is called a Chebyshev (n, d)-permutation code if the Chebyshev distance of any pair of distinct permutations in C is at least d.

$A_H(n,d)$ and $A_C(n,d)$

The maximum number of codewords in a Hamming (n,d)-permutation code is denoted by $A_H(n,d)$.

The maximum number of codewords in a Chebyshev (n,d)-permutation code is denoted by $A_C(n,d)$.

Problems:

- Construct permutation codes with large size under Hamming or Chebyshev distance.

- Find $A_H(n,d)$ and $A_C(n,d)$, or give some good lower or upper bounds of them.

Basic results on $A_H(n,d)$

1. $A_H(n,2) = n!$;
2. $A_H(n,3) = n!/2$;
3. $A_H(n,n) = n$;
4. $A_H(n,d) \leq nA_H(n-1,d)$.

Sphere-packing bound

Definition

Let $D(n,k)$ $(k = 0, 1, \ldots, n)$ denote the set of all permutations in S_n which are exactly at distance k from the identity.

Clearly, $|D(n,k)| = D_k\binom{n}{k}$.
Let $B_H(n,d)$ be the size of the set of the permutations at distance at most d from the identity. Then $B_H(n,d) = \sum_{k=0}^{d} D_i\binom{n}{k}$.

Theorem

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

The upper bound for $A_H(n,4)$

Theorem (Frankl and Deza, 1977)

$$A_H(n,4) \leq (n-1)!.$$

Theorem (Dukes and Sawchuck, 2010)

If $k^2 \leq n \leq k^2+k-2$ for some integer $k \geq 2$, then

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

Gilbert-Varshamov bound

Theorem

$$A_H(n,d) \geq \frac{n!}{\sum_{k=0}^{d-1} D_k \binom{n}{k}}.$$

Graph theory model

We define a *Cayley graph*

$$\Gamma(n,d) := \Gamma(S_n, S(n,d-1)),$$

where $S(n,d-1)$ is the set of all the permutations with more than $n-d$ fixed points.
By the definition, $\Gamma(n,d)$ is a regular graph of degree which equals the size of the generating set, i.e.,

$$\Delta(n,d) = |S(n,d-1)| = \sum_{k=1}^{d-1} \binom{n}{k} D_k.$$

The codewords of an (n,d) permutation code are vertices of an independent set in $\Gamma(n,d)$. Conversely, any independent set in $\Gamma(n,d)$ is an (n,d)-permutation code.

A result on the independent number

For $m \geq 1$ and $x \geq 0$, we define the function $f_m(x)$ by

$$f_m(x) = \int_0^1 \frac{(1-t)^{1/m}}{m + (x-m)t} dt.$$

Theorem (Li and Rousseau, 1996)

Let $m \geq 1$ be an integer, and let G be a graph of order N with average degree Δ. If any subgraph induced by a neighborhood has maximum degree less than m, then

$$\alpha(G) \geq N \cdot f_m(\Delta) \geq N \cdot \frac{\log(\Delta/m) - 1}{\Delta}.$$

Our improvement for small d I

We use $G(n,d)$ to denote the subgraph induced by the neighborhood of identity in $\Gamma(n,d)$. Then $G(n,d)$ has vertex set

$$V(G(n,d)) = S(n,d-1) = \bigcup_{k=1}^{d-1} D(n,k).$$

We denote the maximum degree in $G(n,d)$ by $m(n,d)$.

Lemma

For any positive integer $n \geq 7$*, we have* $m(n,2)=0$, $m(n,3)=0$, $m(n,4)=4n-8$, $m(n,5)=7n^2-31n+34$.

Our improvement for small d II

Theorem (Gao, Yang and Ge, 2013)

Let $m'(n,d) = m(n,d) + 1$, *and*

$$A_H^{IS}(n,d) := n! \cdot \int_0^1 \frac{(1-t)^{1/m'(n,d)}}{m'(n,d) + [\Delta(n,d) - m'(n,d)]\, t} \cdot dt.$$

Then $A_H(n,d) \geq A_H^{IS}(n,d)$.

$A_H^{IS}(13,5) = 2147724$ greatly improves the best known result which is $A_H(13,5) \geq 878778$.

Asymptotic results

Lemma

When n goes to infinity,

$$m(n,d) = O(n^{d-3}).$$

Theorem (Gao, Yang and Ge, 2013)

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

$$\frac{A_H^{IS}(n,d)}{A_H^{GV}(n,d)} = \Omega(\log(n)).$$

The case d/n is fixed

Theorem (Tait, Vardy, and Verstraete, 2015)

Let d/n *be a fixed ratio with* $0 < d/n < 1/2$. *Then as* $n \to \infty$, *then*

$$A_H(n,d) = \Omega\left(\log n \frac{n!}{B_H(d-1)}\right).$$

Our further improvement

Theorem (Wang, Yang, Zhang and Ge, 2017)

Let n, d be integers and let p be a prime greater than or equal to n. Then, we have

$$A_H(n,d) \geq \frac{n!}{p^{d-2}}.$$

Corollary

Let d be fixed and $n \to \infty$. Then

$$A_H(n,d) = \Omega\left(n\frac{n!}{B_H(d-1)}\right).$$

Idea of the proof

Idea: For any graph G of order n, $\alpha(G) \geq \frac{n}{\chi(G)}$.

Consider the coloring $f : S_n \to \mathbb{Z}_p^{d-1}$ whose value at $\sigma \in S_n$ is defined by

$$f(\sigma) = A\sigma (\text{mod } p),$$

where A is a $(d-1) \times n$ Vandermonde matrix as follows ($a_1, a_2 \ldots, a_n$ are distinct numbers in $\{0, 1, \ldots, p-1\}$):

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \ldots & a_n^{d-2} \end{pmatrix}$$

Claim: This coloring is a proper coloring with p^{d-2} colors.

Sphere-packing and GV bounds on $A_C(n,d)$

Let $B_C(n,d)$ denote the number of permutations in S_n within Chebyshev distance d from the identity permutation.

Theorem

$$\frac{n!}{B_C(n,d-1)} \leq A_C(n,d) \leq \frac{n!}{B_C(n,\lfloor (d-1)/2 \rfloor)}.$$

Permanent and $B_C(n, d)$

Definition

Let A be a $n \times n$ matrix. Then the permanent of A is defined by

$$per A = \sum_{\pi \in S_n} a_{1,\pi_1} \dots a_{n,\pi_n}.$$

Let $A^{(n,d)}$ be the $n \times n$ matrix with $a_{i,j}^{(n,d)} = 1$ if $|i - j| \leq d$ and $a_{i,j}^{(n,d)} = 0$ otherwise.

Lemma

$$B_C(n, d) = per A^{(n,d)}.$$

Upper bound for $B_C(n, d)$

Lemma

$$per A \leq \prod_{i=1}^{n} (r_i!)^{1/r_i},$$

where r_i is the number of ones in row i.

Theorem (Kløve et al., 2010)

$$B_C(n, d) \leq [(2d+1)!]^{n/(2d+1)}.$$

Construction of $B^{(n,d)}$

Define the matrix $B^{(n,d)}$ as follows:

$$b_{i,j}^{(n,d)} = \begin{cases} 0 & \text{if } i > j + d \text{ or } j > i + d, \\ 2 & \text{if } i + j \le d + 1 \text{ or } i + j \ge 2n + 1 - d, \\ 1 & \text{otherwise.} \end{cases}$$

Theorem (Kløve, 2011)

$$per B^{(n,d)} \le 2^{2d} per A^{(n,d)}.$$

Example

$$A^{(6,2)} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$B^{(6,2)} = \begin{pmatrix} 2 & 2 & 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 2 & 2 \end{pmatrix}$$

Lower bound for $B_C(n,d)$

Theorem

If A is an $n \times n$ matrix where the sum of the elements in any row or column is k, then

$$per A \geq n! k^n / n^n.$$

Theorem (Kløve, 2011)

$$B_C(n,d) \geq \frac{n!(2d+1)^n}{2^{2d} n^n}.$$

Bounds for $A_C(n,d)$

Theorem (Kløve, 2010)

$$\frac{n!}{[(2d-1)!]^{n/(2d-1)}} \leq A_C(n,d) \leq \frac{2^{d-1}n^n}{d^n}.$$

A better lower bound for $B_C(n,d)$

Let $B_{d,2}$ be the upper left corner of $B^{(n,d)}$.

Theorem (Kløve, 2011)

$$\mathrm{per} B^{(n+2d,d)} \leq \mathrm{per} A^{(n,d)} per(B_{d,2})^2.$$

Conjecture (Kløve, 2011)

For any positive integer d,

$$per(B_{d,2}) = \sum_{m=0}^{d} \binom{d}{m} (m+1)^d.$$

Proof of Kløve's conjecture

Theorem (Guo and Yang, 2017)

$$\mathrm{per}(B_{d,x}) = \sum_{m=0}^{d} \binom{d}{m} (m+1)^d (x-1)^{d-m}.$$

It is equivalent to

$$\mathrm{per}(B_{d,x+1}) = \sum_{m=0}^{d} \binom{d}{m} (d-m+1)^d x^m. \tag{4.1}$$

Therefore, it suffices to show that the coefficient b_m of x^m in $\mathrm{per}(B_{d,x+1})$ is equal to $\binom{d}{m}(d-m+1)^d$.

What does the martix $B_{d,x+1}$ look like?

$$B_{2,x+1} = \begin{pmatrix} x+1 & x+1 & 1 & 0 \\ x+1 & 1 & 1 & 1 \end{pmatrix},$$

$$B_{3,x+1} = \begin{pmatrix} x+1 & x+1 & x+1 & 1 & 0 & 0 \\ x+1 & x+1 & 1 & 1 & 1 & 0 \\ x+1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Kendall's τ-metric

Definition

Given a permutation $\sigma \in S_n$, an adjacent transposition, $(i, i+1)$, for some $1 \leq i \leq n-1$, is an exchange of the two adjacent elements $\sigma(i)$ and $\sigma(i+1)$ in σ.

Definition

Given two permutations $\sigma, \pi \in S_n$, the Kendall's τ-distance between σ and π, $d_K(\sigma, \pi)$, is defined as the minimum number of adjacent transpositions needed to transform σ into π.

Basic properties

Theorem (Barg and Mazumdar, 2010)

For $\sigma, \pi \in S_n$,

$$d_K(\sigma, \pi) = |\{(i,j) : \sigma^{-1}(i) < \sigma^{-1}(j) \wedge \pi^{-1}(i) > \pi^{-1}(j)\}|.$$

Corollary

For $\sigma, \pi \in S_n$,

$$d_K(\sigma, \pi) + d_K(\sigma^r, \pi) = \binom{n}{2}.$$

Bounds on $A_K(n,d)$

Definition

A permutation code C under Kendall's τ-metric with minimum distance d is a subset of S_n such that any two distinct permutations σ and π, $d_K(\sigma,\pi) \geq d$.

Let $A_K(n,d)$ be the size of the code with the maximum size.

Theorem (Jiang, Schwartz and Bruck, 2010)

$$\frac{n!}{B_K(d-1)} \leq A_K(n,d) \leq \frac{n!}{B_K(\lfloor \frac{d-1}{2} \rfloor)}.$$

Our improvement for the lower bound

Theorem (Barg and Mazumdar, 2010)

Let $m = ((n-2)^{t+1} - 3)/(n-3)$, *where* $n-2$ *is a prime power. Then we have*

$$A_K(n, 2t+1) \geq \begin{cases} n!/(t(t+1)m), & t \text{ odd}; \\ n!/(t(t+2)m), & t \text{ even}. \end{cases}$$

Theorem (Wang, Yang, Zhang and Ge, 2017)

Let $m = ((n-2)^{t+1} - 3)/(n-3)$, *where* $n-2$ *is a prime power. Then we have*

$$A_K(n, 2t+1) \geq \frac{n!}{(2t+1)m}.$$

Upper bounds

Definition

An anticode $\mathcal{A}$ of diameter D in S_n is a subset $\mathcal{A}$ of S_n such that $d_K(x, y) \leq D$ for any $x, y \in \mathcal{A}$.

Theorem (Buzaglo and Etzion, 2015)

If a code $\mathcal{C} \subset S_n$ has minimum Kendall's τ-distance d, and an anticode $\mathcal{A} \subset S_n$ has maximum Kendall's τ-distance $d-1$, then

$$|\mathcal{C}| \leq \frac{n!}{|\mathcal{A}|}.$$

Two open problems on the anticodes

Definition

Let $x, y \in S_n$ such that $d_K(x, y) = 1$, the double ball of radius R centered at x and y is defined by

$$DB(x, y, R) = B(x, R) \cup B(y, R).$$

1. Is a ball with radius R in S_n always optimal as an anticode with diameter $2R$ in S_n, for $2 \leq R \leq \frac{\binom{n}{2}}{2}$?

2. Is the double ball with radius R in S_n always optimal as an anticode with diameter $2R + 1$ in S_n, for $2 \leq R \leq \frac{\binom{n}{2}-1}{2}$?

Some other metrics

- Ulam metric d_U: minimum number of translocations needed.
- Calay metric d_C: minimum number of transpositions needed.
- Generalized Cayley metric d_{gC}: minimum number of interval transpositions needed.
- Generalized Kendall τ-metric d_{gK}: minimum number of interval adjacent transpositions needed.
  Clearly, we have the following inequality:

$$d_{gC}(\pi_1, \pi_2) \leq d_{gK}(\pi_1, \pi_2) \leq d_U(\pi_1, \pi_2) \leq d_K(\pi_1, \pi_2).$$

Block permutation distance

Definition

The block permutation distance between π_1 and π_2 ($d_B(\pi_1, \pi_2)$)is d if and only if $(d+1)$ is the minimum number of blocks the permutation π_1 needs to be divided into in order to obtain π_2 through block level permutation.

Theorem (S.Yang et al.,2019)

$$d_{gC}(\pi_1, \pi_2) \leq d_B(\pi_1, \pi_2) \leq 4d_{gC}(\pi_1, \pi_2).$$

Reference

- A. Barg and A. Mazumdar, Codes in permutations and error correction for rank modulation. IEEE Trans. Inform. Theory, **56**(7):3158-3165, 2010.
- S. Buzaglo and T. Etzion, Bounds on the size of permutation codes with the Kendall τ-metric. IEEE Trans. Inform. Theory, **61**(6):3241-3250, 2015.
- P. J. Cameron and C. Y. Ku, Intersection families of the permutations, *European J. Combin.* **24** (2003) 881-890.
- W. Chu, C. J. Colbourn, and P. Dukes, Constructions for Permutation Codes in Powerline Commnications, *Des. Codes Cryptogr.* **32** (2004), 51-64.
- D. H. Smith and R. Montemanin, A new table of permutation codes, *Des. Codes Cryptogr.* **63** (2)(2012), 241-253.

P. Diaconis, *Group Representations in probability and Statistics*, Hayward, CA: Inst. Math. Statist., 1988.

P. Dukes and N. Sawchuck, bounds on permutation codes of distance four, *J. Algebraic Combin.* **31**(1) (2010), 143-158.

P. Frankl, M. Deza, On the maximum number of permuations with givern maximal or minimal distance, *J. Combin. Theory Ser. A* **22** (3) (1977), 352-360.

J. Guo and Y. Yang, Proof of a conjecture of Kløve on permutation codes under the Chebychev distance, to appear

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

- T. Kløve, T. Lin, S. Tsai, and W. Tzeng, Permutation Arrays Under the Chebyshev Distance, *IEEE Tran. Inform. Theory,* **56**(6), 2611-2617 (2010).
- T. Kløve, Lower bounds on the size of spheres of permutations under the Chebyshev distance, *Des. Codes Cryptogr.*, **59** 183-191 (2011).
- D. H. Lehmer, Permutations with strongly restricted displacements,in *Combinatorial Theory and its applications II,* P. Erdos, A. Renyi, and V. T. Sos, Eds. Amsterdam, The Netherlands: North Holland, 1970.
- N. Pavlidou, A. J. H. Vinck, J. Yazdani and B. Honary, Powerline communications: State of the art and future trends, *IEEE Communications Magazine,* (2003), 34-40.

Y. Li and C. C. Rousseau, On book-complete graph Ramsey numbers, *J. Combin. Theory Ser. B* **68**(1) (1996), 36-44.

M. Tait, A. Vardy, and J. Verstraete, Asymptotic improvement of the gilbert-varshamov bound on the size of permutation codes. arXiv preprint arXiv:1311.4925, 2013.

X. Wang, Y. Zhang, Y. Yang, and G. Ge, New bounds of permutation codes under Hamming metric and Kendall τ-metric, Des. Codes Cryptogr., 85(3) (2017), 533-545.

J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed. Cambridge, U. K.: Cambridge Univ. Press, 2011.

F. Gao, Y. Yang, and G. Ge, An Improvement on the Gilbert-Varshamov Bound for Permutation Codes, *IEEE Tran. Inform. Theory*, **59** (5), 3059-3063 (2013).

- Y. Chee and V. K. Vu, Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics, *in Proc. IEEE Int. Symp. Inf. Theory, Hawaii,* USA, Jun. 2014, 2959C2963.
- S. Yang, C. Shoeny and Lara Dolecek, Theoretical Bounds and Constructions of Codes in the Generalized Cayley Metric. *IEEE Trans. Information Theory,* **65**(8): 4746-4763 (2019).

Thank you!