Covering radius of permutations codes

Xiande Zhang

University of Science and Technology of China

(with Ian M. Wanless and Xin Wei)

Taichung, Aug 2019

Covering codes

- Metric space M: a set of points equipped with a metric d.
- Covering code: $P \subset M$.
- the covering radius of P in M: $\min r$ s.t. balls of radius r centered around all the points in P cover M.
- $\mathrm{cr}(P)$: the covering radius of $P \subset M$.
- two central problems:
  - the mathematical question: determine $\mathrm{cr}(P)$,
  - the practical problem: construct good covering codes.

Permutation codes

- metric space $M = S_n$.
- metric d: Hamming distance, l_1 distance, l_2 distance, l_∞ distance, Lee distance, Cayley distance, Kendalls τ distance, Ulam distance.
- P: a set of permutations.
- packing codes or error correcting codes:
  balls of radius e centered at all points of P are disjoint.

Hamming distance

- vector notation for permutations:
  $f = [f_1, f_2, \ldots, f_n]$ denotes a permutation mapping $i \to f_i$ for all $i \in [n]$.
- Hamming distance: $d_H(f, g) := |\{1 \leq i \leq n : f_i \neq g_i\}|$.
- E.g., $[1, 3, 2, 4, 5]$ has distance 3 with $[2, 3, 5, 4, 1]$.

Covering codes

- $f(n,s)$: min m
  s.t.$\exists\ P \subset S_n$ with $|P| = m$ and $\mathrm{cr}(P) \leq n - s$.
- $f(n,0) = 1$ and $f(n,n) = f(n,n-1) = n!$.
- $f(n,1) = \lfloor n/2 \rfloor + 1$ (Cameron & Wanless, 2005).
- Kézdy-Snevily (K-S) Conjecture, 2005:
  If n is even, then $f(n,2) = n$; if n is odd, then $f(n,2) > n$.

Known results

- Cameron & Wanless, 2005

$$\lfloor n/2 \rfloor + 2 \leq f(n,2) \leq \begin{cases} n & \text{if } n \text{ is even,} \\ \frac{5}{4}n + O(1) & \text{if } n \equiv 1 \mod 4, \\ \frac{4}{3}n + O(1) & \text{if } n \equiv 3 \mod 4. \end{cases}$$

- Wanless & Zhang, 2013

$$f(n,2) \leq \begin{cases} n + O(\log n) & \text{if } n \equiv 1,5 \pmod 6, \\ n+2 & \text{if } n \equiv 3 \pmod 6. \end{cases}$$

- Hendrey & Wanless, 2019+: $f(n,2) > 3n/4$.

Latin squares

- A Latin square of order n is an $n \times n$ array of n symbols, in which each symbol occurs exactly once in each row and column.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- A transversal of a Latin square is a set of entries which includes exactly one entry from each row and column and one of each symbol.

Conjectures

- If $\exists$ a Latin square of order n with no transversal, then $f(n, 2) \leq n$.
- No cyclic group of even order has a transversal (Maillet, 1894) $\Longrightarrow f(n, 2) \leq n$ for all even n.
- Ryser's Conjecture (1967): Each Latin square of odd order has at least one transversal.
- Brualdi's Conjecture (1974): Every Latin square of order n possesses a partial transversal of size $n - 1$.
- K-S Conj $\Longrightarrow$ Ryser's Con & Brualdi's Conj.

Summary

- K-S Conj: odd case $\Longrightarrow$ even case,
  Hendrey & Wanless, 2019+.
- Summary:

$$3n/4 < f(n,2) \leq \begin{cases} n & \text{if } n \text{ is even,} \\ n + O(\log n) & \text{if } n \equiv 1,5 \pmod 6, \\ n+2 & \text{if } n \equiv 3 \pmod 6. \end{cases}$$

covering radius

- 2005 & 2013: $\mathrm{cr}(AGL(1,q)) = \begin{cases} q-2 & \text{if } q \text{ is even,} \\ q-3 & \text{if } q \text{ is odd.} \end{cases}$
- Xia, 2017: $\mathrm{cr}(PGL(2,q)) = \begin{cases} q-2 & \text{if } q \text{ is even,} \\ q-3 & \text{if } q \text{ is odd.} \end{cases}$
- Cossidente, Marino & Pavese 2019: $\mathrm{cr}(PGL(3,q)) = q^2+q-3$.
- Bamberg, Praeger & Xia, 2019: 2-transitive unitary, Suzuki, and Ree groups.
- Keevash & Ku, 2006: the covering radius for sets of permutations in terms of a certain frequency parameter.

l_∞ metric

- $d_\infty(f,g) \triangleq \max_{i\in[n]} |f(i)-g(i)|$.
- E.g., $f=[1,2,3,4,5]$, $g=[2,3,4,5,1]$, $d_\infty(f,g)=4$.
- the relabeling of a code $C \subseteq S_n$ is

$$C^h \triangleq hCh^{-1} = \{hgh^{-1} : g \in C\}.$$

- E.g., $f=(1)(2)(3)(4)(5)$, $g=(1,2,3,4,5)$,
  $h=[4,1,3,2,5]$, $hfh^{-1}=(4)(1)(3)(2)(5)=f$,
  $hgh^{-1}=(4,1,3,2,5)=[3,5,2,1,4]$,
  $d_\infty(hfh^{-1},hgh^{-1})=3$
- $L_{max}(C) \triangleq \max_{h\in S_n} \mathrm{cr}(C^h)$ and $L_{min}(C) \triangleq \min_{h\in S_n} \mathrm{cr}(C^h)$.

Karni and Schwartz, 2018

- $G_n \triangleq \langle (1, 2, \ldots, n) \rangle$.
- $G_n^h = \langle (h_1, h_2, \ldots, h_n) \rangle \subseteq S_n$ some $h \in S_n$.
- $\mathrm{cr}(G_n) = n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor$.
- $L_{max}(G_n) = n - \left\lceil \frac{\sqrt{4n+1}-1}{2} \right\rceil$.
- $L_{min}(G_n) \geq n - \left\lceil \sqrt{2n \ln n + 2n} \right\rceil$.

upper bound $\mathrm{cr}(G_n)$

- Idea of proof: $\mathrm{cr}(G_n) \leq r$.
- Fix any permutation $f = [f_1, f_2, \ldots, f_n] \in S_n$, let $R_f = \emptyset$.
- For each i and each $g = [g_1, g_2, \ldots, g_n] \in G_n$, if $|f_i - g_i| > r$, then put g into R_f.
- if $|R_f| < n$, then $\mathrm{cr}(G_n) \leq r$.

Karni and Schwartz, 2018

- $D_n \triangleq \left\langle (1, 2, \ldots, n-1, n), \prod_{i=1}^{\lfloor \frac{n}{2} \rfloor} (i, n-i) \right\rangle$.
- $\mathrm{cr}(D_n) \leq \mathrm{cr}(G_n) = n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor$.
-

$$\mathrm{cr}(D_n) \geq \begin{cases} n - \left\lceil \dfrac{\sqrt{288n+297}-3}{16} \right\rceil, & n \in [4, 9], \\ n - \left\lceil \dfrac{\sqrt{288n+737}-1}{16} \right\rceil, & n \in [10, 911], \\ n - \left\lceil \dfrac{\sqrt{18n-18}}{4} \right\rceil, & n \geq 912. \end{cases}$$

- The gap goes to infinity when n grows.

Our results, 2019+

- $p, q \in \mathbb{N}^+$ and $p \geq q$,

$$G_{p,q} \triangleq \langle (1, 2, \cdots, p), (p+1, p+2, \cdots, p+q) \rangle .$$

- $\mathrm{cr}\left(G_{p,q}\right) = p + \left\lfloor \left(\sqrt{q + \frac{1}{8}} - \frac{\sqrt{2}}{2} \right)^2 - \frac{1}{8} \right\rfloor .$
- $L_{max}\left(G_{p,q}\right) = p + q - \left\lceil \frac{\sqrt{4q+1}-1}{2} \right\rceil .$
- $L_{min}(G_{p,q}) \geq L_{min}(G_p) \geq p - \left\lceil \sqrt{2p \ln(p) + 2p} \right\rceil .$

Our results, 2019+

- $\mathrm{cr}(D_n) \leq \mathrm{cr}(G_n) = n - \left\lfloor \frac{\sqrt{4n+1}+1}{2} \right\rfloor$.
- Idea of proof: $\mathrm{cr}(D_n) \geq r_0$.
- construct a permutation f_0 s.t. $d_\infty(f_0, g) > r_0 - 1$ for all $g \in D_n$.

Our results, 2019+

- $\mathrm{cr}(D_n) \geq r_0 = n - \left\lceil \frac{\sqrt{4n+13}+1}{2} \right\rceil$.
- let $k = n - r_0$, $d_t \triangleq \binom{t}{2}$ for $t \in [n]$.
- define a set of locations:

$$\lambda(i) = \begin{cases} d_k - d_{k-i+1} + 1, & i \in [k-1], \\ d_k + d_{i-n+k} - 2, & i \in [n-k+2, n]. \end{cases}$$

-

$$f_0(j) = \begin{cases} i, & \text{if } j = \lambda(i) \text{ for } i \in [k-1] \cup [n-k+2, l] \\ l+1, & \text{if } j = \lambda', \\ \text{arbitrary}, & \text{otherwise.} \end{cases}$$

Our results, 2019+

- upper bound$-r_0 = \begin{cases} 2, & n = m(m-1)-1, \text{ or} \\ & \quad m(m-1)-2, \\ 1, & \text{else.} \end{cases}$
- improved lower bound:
  When $n = m(m-1)-2$, $m(m-1)-1$ or $m(m-1)$,
  then $\mathrm{cr}(D_n) \geq r_0 + 1$.
- $\Longrightarrow$ upper$-$lower $= \begin{cases} 0, & n = m(m-1), \\ 1, & \text{else.} \end{cases}$

Our results, 2019+

n	3	4	5	6	7	8	9	10	11
$\mathrm{cr}(D_n)$	0_l	1_l	2_l	3_e	4_u	5_u	5_l	6_l	7_l
n	12	13	14	15	16	17	18	19	20
$\mathrm{cr}(D_n)$	8_e	9_u	10_u	11_u	12_u	12_l	13_l	14_l	15_e

Table: Exact values of $\mathrm{cr}(D_n)$ for small n

Question: $\mathrm{cr}(D_n) =?$, $\mathrm{cr}(AGL(1,q)) =?$

Thank you!