A lower bound on permutation codes of distance $n-1$

Sergey Bereg and Peter J. Dukes*

June 22, 2021

University of Victoria | Mathematics & Statistics

Permutation Codes

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

Permutation Codes

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

Example

A permutation code of length 4 and distance 4:

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

Permutation Codes

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

Example

A permutation code of length 4 and distance 4:

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

A larger one:

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

Including any additional permutation will decrease the minimum distance.

Elementary values/bounds

Let $M(n, d)$ denote the maximum size of a permutation code of length n and distance d.

Elementary values/bounds

Let $M(n,d)$ denote the maximum size of a permutation code of length n and distance d.

- $M(n,n) = n$ (latin square)
- $M(n,2) = n!$ (all $\mathcal{S}_n$)
- $M(n,3) = n!/2$ (alternating group)

Elementary values/bounds

Let $M(n,d)$ denote the maximum size of a permutation code of length n and distance d.

- $M(n,n) = n$ (latin square)
- $M(n,2) = n!$ (all $\mathcal{S}_n$)
- $M(n,3) = n!/2$ (alternating group)

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

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

Codes from MOLS

Let $N(n)$ denote the maximum number of MOLS of side length n.

Colbourn-Kløve-Ling (2004): $N(n) \geq r \;\Rightarrow\; M(n, n-1) \geq rn$.
(Take all rn transversals and convert to permutations.)

Beth (1984): $N(n) \geq n^{1/14.8}$ for sufficiently large n.

Therefore, $M(n, n-1) \geq n^{1+14.8} \geq n^{1.0675}$ for large n.

A partial converse

We have $M(6,5) = 18$ in spite of $N(6) = 1$.

Example

Here is a convenient code of size 12 given as 'orthogonal' partial latin squares.

1	4			3	2
	2	1		4	3
		3	2	1	4
3			4	2	1
4	1	2	3		
2	3	4	1		

1		5	6	2	
5	2	6	1		
2	6		5		1
	1	2		6	5
6		1		5	2
	5		2	1	6

	6	4	3		5
6			5	3	4
4	5	3		6	
5	3	6	4		
	4		6	5	3
3		5		4	6

Main Result

Theorem (B.-D.,2020)

$M(n, n-1) \geq n^{1.0797}$ for sufficiently large n.

Main Result

Theorem (B.-D.,2020)

$M(n, n-1) \geq n^{1.0797}$ for sufficiently large n.

Sketch of proof:

- $M(q, q-1) \geq q(q-1)$ for prime powers q.

Main Result

Theorem (B.-D.,2020)

$M(n, n-1) \geq n^{1.0797}$ *for sufficiently large n.*

Sketch of proof:

- $M(q^2, q^2 - 1) \sim q^4$ for prime powers q.

Main Result

Theorem (B.-D.,2020)

$M(n, n-1) \geq n^{1.0797}$ *for sufficiently large n.*

Sketch of proof:

- $M(q^2, q^2 - 1) \sim q^4$ for prime powers q.
- $M(q^2 + 1, q^2) \geq q^3$ for prime powers q.

Main Result

Theorem (B.-D.,2020)

$M(n, n-1) \geq n^{1.0797}$ *for sufficiently large n.*

Sketch of proof:

- $M(q^2, q^2 - 1) \sim q^4$ for prime powers q.
- $M(q^2 + 1, q^2) \geq q^3$ for prime powers q.
- Adapt Wilson's construction for MOLS.
- Apply a number sieve.

Q: Can we raise the exponent for MOLS and/or PC?

Thank you

References

S. Bereg and P.J. Dukes, A lower bound on permutation codes of distance $n-1$. *DCC* (2020) 88, 63–72.

T. Beth, Eine Bemerkung zur Abschtzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren. *Abh. Math. Sem. Univ. Hamburg* 53 (1983), 284–288.

R.M. Wilson, Concerning the number of mutually orthogonal Latin squares. *Discrete Math.* 9 (1974), 181–198.