Codes, blocking sets and graphs

Anurag Bishnoi

TU Delft

DIAM Lunch Colloqium
10th May 2023
Delft, Netherlands

Overview

Extremal problems at the intersection of

- Coding theory
- Computer science
- Finite geometry

Overview

Extremal problems at the intersection of

- Coding theory
- Computer science
- Finite geometry

solved using probabilistic, graph theoretic and algebraic methods.

Overview

Extremal problems at the intersection of

- Coding theory
- Computer science
- Finite geometry

solved using probabilistic, graph theoretic and algebraic methods.

Joint work(s) with Noga Alon, Shagnik Das, Dion Gijswijt, Jozefien D'Haeseleer, Alessandro Neri, and Aditya Potukuchi.

Trifferent codes

A ternary code $C \subseteq \{0, 1, 2\}^n$ is called a *trifferent code* or a *perfect 3-hash code*, if for any three distinct codewords there is a coordinate where they all differ.

Trifferent codes

A ternary code $C \subseteq \{0,1,2\}^n$ is called a *trifferent code* or a *perfect 3-hash code*, if for any three distinct codewords there is a coordinate where they all differ.

$$
\begin{array}{ccccc}
0 & 0 & 0 & 0 & \leftarrow \\
1 & 0 & 1 & 2 & \\
2 & 0 & 2 & 1 & \\
0 & 2 & 2 & 2 & \leftarrow \\
1 & 1 & 2 & 0 & \\
2 & 1 & 0 & 2 & \leftarrow \\
1 & 2 & 0 & 1 & \\
0 & 1 & 1 & 1 & \\
2 & 2 & 1 & 0 &
\end{array}
$$

A trifferent code of size 9 and length 4.

The trifference problem

What is the largest size $T(n)$ of a trifferent code of length n?

The trifference problem

What is the largest size $T(n)$ of a trifferent code of length n?

n	1	2	3	4	5	6	7
$T(n)$	3	4	6	9	10	13	?

The trifference problem

What is the largest size $T(n)$ of a trifferent code of length n?

n	1	2	3	4	5	6	7
$T(n)$	3	4	6	9	10	13	?

Theorem (Körner 1973)

$$T(n) \leq 2\,(1.5)^n$$

The trifference problem

What is the largest size $T(n)$ of a trifferent code of length n?

n	1	2	3	4	5	6	7
$T(n)$	3	4	6	9	10	13	?

Theorem (Körner 1973)

$$T(n) \leq 2\,(1.5)^n$$

Theorem (Körner-Marton 1984)

$$T(n) \geq (9/5)^{n/4} \simeq (1.158)^n$$

Linear trifferent codes

Identify $\{0, 1, 2\}$ with the finite field $\mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$.

> *What is the largest size $T_L(n)$ of a trifferent code $C \subseteq \mathbb{F}_3^n$ which is also a* **linear subspace***?*

Linear trifferent codes

Identify $\{0, 1, 2\}$ with the finite field $\mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$.

> *What is the largest size $T_L(n)$ of a trifferent code $C \subseteq \mathbb{F}_3^n$ which is also a* **linear subspace***?*

For example, let C be

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 1 & 0 & 2 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 2 & 2 & 1 & 0 \end{matrix}$$

Linear trifferent codes

Identify $\{0, 1, 2\}$ with the finite field $\mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$.

> *What is the largest size $T_L(n)$ of a trifferent code $C \subseteq \mathbb{F}_3^n$ which is also a* **linear subspace***?*

For example, let C be

$$\begin{matrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \\ 0 & 2 & 2 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 1 & 0 & 2 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 2 & 2 & 1 & 0 \end{matrix}$$

then, $C = \langle \{(0, 1, 1, 1), (1, 0, 1, 2)\} \rangle$.

Motivation

- $T_L(n) \leq T(n)$.

Motivation

- $T_L(n) \leq T(n)$.

- Explicit constructions.

Motivation

- $T_L(n) \leq T(n)$.
- Explicit constructions.
- Probabilistic lower bounds.

Motivation

- $T_L(n) \leq T(n)$.
- Explicit constructions.
- Probabilistic lower bounds.
- Further motivations coming up soon ...

Previous bounds on linear trifferent codes

Previous bounds on linear trifferent codes

Theorem (Pohoata-Zakharov 2022)

Every linear trifferent code of length n has dimension at most $\frac{n}{4}$, and thus

$$T_L(n) \leq (1.3160)^n.$$

Previous bounds on linear trifferent codes

Theorem (Pohoata-Zakharov 2022)

Every linear trifferent code of length n has dimension at most $\frac{n}{4}$, and thus

$$T_L(n) \leq (1.3160)^n.$$

Theorem (Wang-Xing 2001)

There are (explicit) linear trifferent codes of length n and dimension $\frac{n}{112}$, and thus

$$T_L(n) \geq (1.0098)^n.$$

Our results

Bishnoi, D'Haeseleer, Gijswijt, Potukuchi, *Blocking sets, minimal codes and trifferent codes* arXiv:2301.09457

Theorem

Every linear trifferent code of length n has dimension at most $\frac{n}{4.55}$, and thus

$$T_L(n) \leq (1.273)^n.$$

Our results

Bishnoi, D'Haeseleer, Gijswijt, Potukuchi, *Blocking sets, minimal codes and trifferent codes* arXiv:2301.09457

Theorem

Every linear trifferent code of length n has dimension at most $\frac{n}{4.55}$, and thus

$$T_L(n) \leq (1.273)^n.$$

Theorem

There are linear trifferent codes of length n and size at least $\frac{1}{3}(9/5)^{n/4}$, and thus

$$T_L(n) \geq (1.158)^n.$$

Our results

Bishnoi, D'Haeseleer, Gijswijt, Potukuchi, *Blocking sets, minimal codes and trifferent codes* arXiv:2301.09457

Theorem

Every linear trifferent code of length n has dimension at most $\frac{n}{4.55}$, and thus

$$T_L(n) \leq (1.273)^n.$$

Theorem

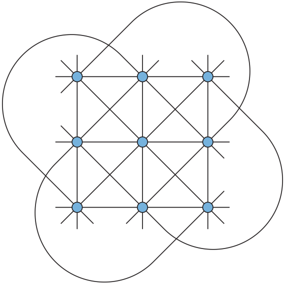
There are linear trifferent codes of length n and size at least $\frac{1}{3}(9/5)^{n/4}$, and thus

$$T_L(n) \geq (1.158)^n.$$

Theorem

An explicit construction of linear trifferent codes of length n and dimension $\frac{n}{13.5}$.

Finite affine spaces



The Affine plane $\mathbb{F}_3^2$

Points: $\mathbb{F}_q^2$
Lines: translates of 1-dimensional vector subspaces

Smallest affine blocking sets

$b_q(k, s) :=$ min number of points in the k-dimensional finite affine space that block every $(k - s)$-dimensional affine subspace.

Smallest affine blocking sets

$b_q(k,s) :=$ min number of points in the k-dimensional finite affine space that block every $(k-s)$-dimensional affine subspace.

Theorem (Jamison/Brouwer-Schrijver 1977)

$$b_q(k,1) = (q-1)k + 1.$$

Smallest affine blocking sets

$b_q(k, s) :=$ min number of points in the k-dimensional finite affine space that block every $(k - s)$-dimensional affine subspace.

Theorem (Jamison/Brouwer-Schrijver 1977)

$$b_q(k, 1) = (q - 1)k + 1.$$

Corollary

$$b_q(k, s) \geq (q^s - 1)(k - s + 1) + 1.$$

Smallest affine blocking sets

$b_q(k, s) :=$ min number of points in the k-dimensional finite affine space that block every $(k - s)$-dimensional affine subspace.

Theorem (Jamison/Brouwer-Schrijver 1977)

$$b_q(k, 1) = (q - 1)k + 1.$$

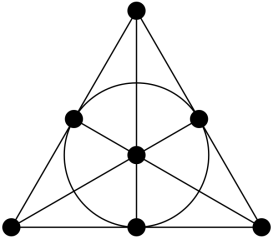
Corollary

$$b_q(k, s) \geq (q^s - 1)(k - s + 1) + 1.$$

Theorem (Lovász 1975)

$$b_q(k, s) \leq q^s \left(1 + \ln \begin{bmatrix} k \\ s \end{bmatrix}_q \right) \approx (q^s \ln q)(s(k - s)).$$

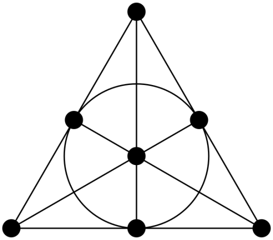
Projective blocking sets



The projective plane over $\mathbb{F}_2^3$.

How many 1-dimensional subspaces of $\mathbb{F}_q^k$ do we need to block every hyperplane?

Projective blocking sets



The projective plane over $\mathbb{F}_2^3$.

How many 1-dimensional subspaces of $\mathbb{F}_q^k$ do we need to block every hyperplane?

Answer: $q+1$ subspaces spanning a plane.

Strong blocking sets

How many 1-dimensional linear subspaces of $\mathbb{F}_q^k$ do we need to meet every $(k-1)$-dimensional linear subspace in a spanning set?

Strong blocking sets

How many 1-dimensional linear subspaces of $\mathbb{F}_q^k$ do we need to meet every $(k-1)$-dimensional linear subspace in a spanning set?

Let $\mathcal{S}_i$ be the set of i-dimensional linear subspaces of $\mathbb{F}_q^k$.

$$m_q(k) := \min\{|B| : B \subseteq \mathcal{S}_1, \langle B \cap H \rangle = H, \forall H \in \mathcal{S}_{k-1}\}.$$

Smallest strong blocking sets

Let $m_q(k)$ be the smallest size of a strong blocking set in $\mathbb{F}_q^k$.

Motivation: minimal error-correcting codes, digital fingerprinting, code-based cryptography, circuits in matroids, ...

Smallest strong blocking sets

Let $m_q(k)$ be the smallest size of a strong blocking set in $\mathbb{F}_q^k$.

Motivation: minimal error-correcting codes, digital fingerprinting, code-based cryptography, circuits in matroids, ...

Theorem (Alfarano, Borello, Neri, and Ravagnani 2022)

$$m_q(k) \geq (q+1)(k-1).$$

Smallest strong blocking sets

Let $m_q(k)$ be the smallest size of a strong blocking set in $\mathbb{F}_q^k$.

Motivation: minimal error-correcting codes, digital fingerprinting, code-based cryptography, circuits in matroids, ...

Theorem (Alfarano, Borello, Neri, and Ravagnani 2022)

$$m_q(k) \geq (q+1)(k-1).$$

Theorem (Héger and Nagy 2021)

$$m_q(k) \leq 2(q+1)(k-1).$$

Various new equivalences

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\boxed{\text{$\mathcal{L}$ is a strong blocking set in $\mathbb{F}_q^k$}} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \boxed{\text{$B = \bigcup_{\ell \in \mathcal{L}} \ell$ is an affine 2-blocking set in $\mathbb{F}_q^k$}} \arrow[d, leftrightarrow, "\text{for } q = 3"] \\
\boxed{\text{Minimal linear code of dimension k in $\mathbb{F}_q^{|\mathcal{L}|}$}} \arrow[r, leftrightarrow, "\text{for } q = 3"] & \boxed{\text{Linear trifferent code of dimension k in $\mathbb{F}_3^{(|B|-1)/2}$}}
\end{tikzcd}
$$

Equivalences between blocking sets and codes.

Various new equivalences

$$\begin{tikzcd}
\text{$\mathcal{L}$ is a strong blocking set in $\mathbb{F}_q^k$} \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \text{$B = \bigcup_{\ell \in \mathcal{L}} \ell$ is an affine 2-blocking set in $\mathbb{F}_q^k$} \arrow[d, leftrightarrow, "\text{for } q = 3"] \\
\text{Minimal linear code of dimension k in $\mathbb{F}_q^{|\mathcal{L}|}$} \arrow[r, leftrightarrow, "\text{for } q = 3"] & \text{Linear trifferent code of dimension k in $\mathbb{F}_3^{(|B|-1)/2}$}
\end{tikzcd}$$

Equivalences between blocking sets and codes.

New bounds and constructions for all of these objects!

Lower bounds on strong blocking sets

Theorem (B., D'Haeseleer, Gijswijt, Potukuchi 2023)

For any prime power q, there is a constant $c_q > 1$ such that

$$m_q(k) \geq (c_q - o(1))(q+1)(k-1).$$

The constant c_q is the unique solution $x \geq 1$ to the equation

$$M_q\left(\frac{q-1}{x(q+1)}\right) = \frac{1}{x(q+1)},$$

where M_q is the function appearing in the LP bound on asymptotic rate of a code.

Lower bounds on strong blocking sets

Theorem (B., D'Haeseleer, Gijswijt, Potukuchi 2023)

For any prime power q, there is a constant $c_q > 1$ such that

$$m_q(k) \geq (c_q - o(1))(q+1)(k-1).$$

The constant c_q is the unique solution $x \geq 1$ to the equation

$$M_q\left(\frac{q-1}{x(q+1)}\right) = \frac{1}{x(q+1)},$$

where M_q is the function appearing in the LP bound on asymptotic rate of a code.

Corollary

$$T_L(n) \leq \frac{n}{4c_3} + 1 \leq \frac{n}{4.55}$$

Upper bounds on blocking sets

Theorem (B., D'Haeseleer, Gijswijt, Potukuchi 2023)

$$b_q(k,s) \leq (q^s - 1) \cdot \frac{s(k-s)+s+2}{\log_q\left(\frac{q^4}{q^3-q+1}\right)} + 1.$$

Proof.

Pick random s-dimensional subspaces through the origin. □

Upper bounds on blocking sets

Theorem (B., D'Haeseleer, Gijswijt, Potukuchi 2023)

$$b_q(k,s) \leq (q^s - 1) \cdot \frac{s(k-s)+s+2}{\log_q\left(\frac{q^4}{q^3-q+1}\right)} + 1.$$

Proof.

Pick random s-dimensional subspaces through the origin. $\square$

Corollary

$$m_q(k) \leq (q+1)\frac{2k}{\log_q\left(\frac{q^4}{q^3-q+1}\right)}.$$

Corollary

$$T(n) \geq T_L(n) \geq \frac{1}{3}\left(\frac{9}{5}\right)^{n/4}$$

Explicit Constructions

Big open problem: construct small strong blocking sets explicitly.

Explicit Constructions

Big open problem: construct small strong blocking sets explicitly.

Theorem (Alon, B. , Das and Neri, 2023+)

An explicit construction of a strong blocking set in $\mathbb{F}_q^k$ of size $c(q+1)(k-1)$.

Explicit Constructions

Big open problem: construct small strong blocking sets explicitly.

Theorem (Alon, B. , Das and Neri, 2023+)

An explicit construction of a strong blocking set in $\mathbb{F}_q^k$ of size $c(q+1)(k-1)$.

Corollary

An explicit construction of affine-2 blocking sets in $\mathbb{F}_q^k$ of size $c(q^2-1)(k-1)+1$.

Explicit Constructions

Big open problem: construct small strong blocking sets explicitly.

Theorem (Alon, B. , Das and Neri, 2023+)

An explicit construction of a strong blocking set in $\mathbb{F}_q^k$ of size $c(q+1)(k-1)$.

Corollary

An explicit construction of affine-2 blocking sets in $\mathbb{F}_q^k$ of size $c(q^2-1)(k-1)+1$.

Corollary

An explicit construction of trifferent codes of size $3^{\frac{n}{4c}}$.

Integrity of a graph

Definition

For a graph G, let $\iota(G) = \min\{|S| + \kappa(G - S)\}$, where $\kappa(G - S)$ is the largest size of a connected component in $G - S$.

Examples: $\iota(K_n) = n, \iota(C_n) = 2\lceil\sqrt{n}\rceil - 1$ and $\iota(Q_n) =?$.

Integrity of a graph

Definition

For a graph G, let $\iota(G) = \min\{|S| + \kappa(G - S)\}$, where $\kappa(G - S)$ is the largest size of a connected component in $G - S$.

Examples: $\iota(K_n) = n, \iota(C_n) = 2\lceil\sqrt{n}\rceil - 1$ and $\iota(Q_n) =?$.

Theorem (Alon, B., Das, Neri, 2023+)

For any (n, d, λ)-graph G,

$$\iota(G) \geq \frac{d - \lambda}{d + \lambda} n.$$

The construction

Let V be a collection of n 1-dim vector subspaces of $\mathbb{F}_q^k$ that meets every hyperplane in at most $n-d$ points.

The construction

Let V be a collection of n 1-dim vector subspaces of $\mathbb{F}_q^k$ that meets every hyperplane in at most $n-d$ points.

Let $G=(V,E)$ be a graph with $\iota(G) \geq n-d+1$.

The construction

Let V be a collection of n 1-dim vector subspaces of $\mathbb{F}_q^k$ that meets every hyperplane in at most $n-d$ points.

Let $G=(V,E)$ be a graph with $\iota(G)\geq n-d+1$.

For each edge $e=uv$, let $\mathcal{P}_e$ be the collection of 1-dim subspaces contained in the span of u and v. Then the set

$$S=\cup_{e\in E}\mathcal{P}_e,$$

is a strong blocking set of size $n+(q-1)|E|$.

The construction

Let V be a collection of n 1-dim vector subspaces of $\mathbb{F}_q^k$ that meets every hyperplane in at most $n-d$ points.

Let $G=(V,E)$ be a graph with $\iota(G) \geq n-d+1$.

For each edge $e=uv$, let $\mathcal{P}_e$ be the collection of 1-dim subspaces contained in the span of u and v. Then the set

$$S = \cup_{e \in E} \mathcal{P}_e,$$

is a strong blocking set of size $n+(q-1)|E|$.

By using explicit $[n,k,d]_q$ codes with k,d linear in n (algebraic-geometric codes), and constant-degree expanders Ramanujan graphs, we get our explicit construction.

Future work

1. Improve the upper bound on $m_q(k)$, and in particular for $q = 3$.
2. Improve the lower bound $b_q(k, s) \geq (q^s - 1)(k - s + 1) + 1$ for $s > 1$.
3. Further explore the graph theoretic construction, and apply it to other problems in finite geometry/coding theory.

Future work

1. Improve the upper bound on $m_q(k)$, and in particular for $q = 3$.

2. Improve the lower bound $b_q(k, s) \geq (q^s - 1)(k - s + 1) + 1$ for $s > 1$.

3. Further explore the graph theoretic construction, and apply it to other problems in finite geometry/coding theory.

Thank you!