Local arcs, locally repairable codes, large blocking sets

Ferdinand Ihringer (伊林格)

Joint work with Yue Zhou.

南方科技大学
Southern University of Science and Technology (SUSTech)

August 2026, AsiaComb (Daejeon, Korea)

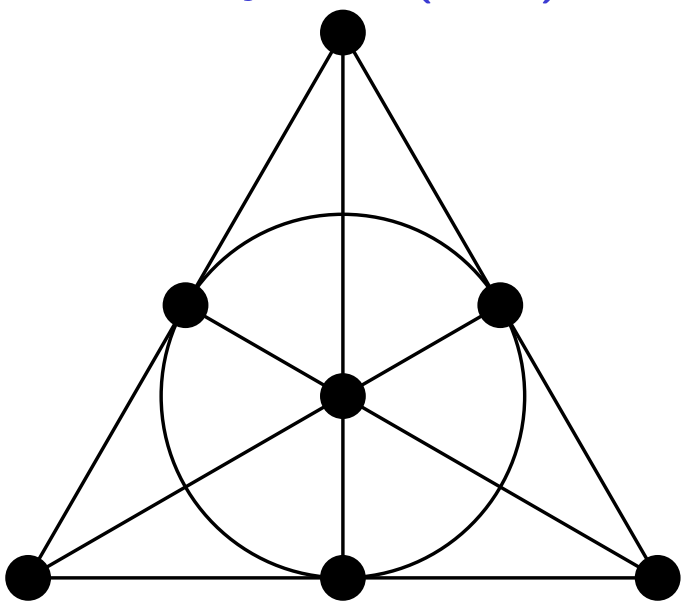
Point-Line Pairs

Problem

*Pick a set Y of **incident point-line pairs** (P, L) in a projective plane of order q such that $P \notin L'$ and $P' \notin L$ for all distinct $(P, L), (P', L') \in Y$.*

***How large** can Y be?*

This is a **strong representative system (SRS)**.[1]



[1] This is closely related to finding a large minimal blocking set.

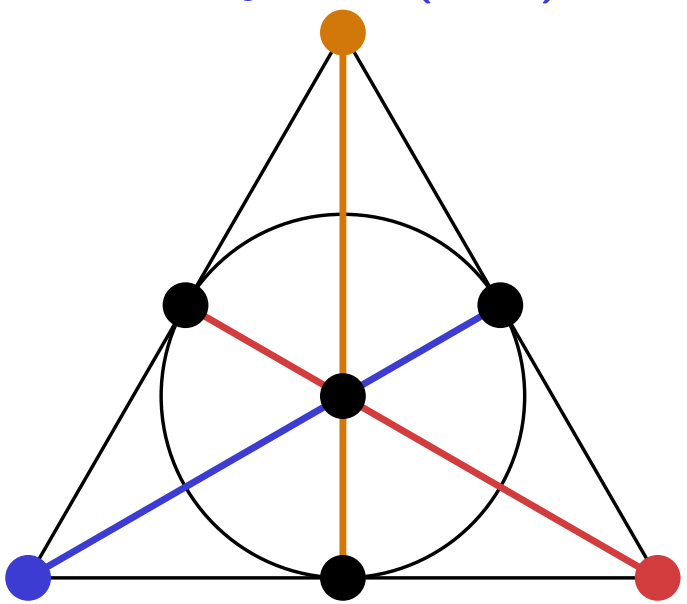
Point-Line Pairs

Problem

*Pick a set Y of **incident point-line pairs** (P, L) in a projective plane of order q such that $P \notin L'$ and $P' \notin L$ for all distinct $(P, L), (P', L') \in Y$.*

***How large** can Y be?*

This is a **strong representative system (SRS)**.[1]

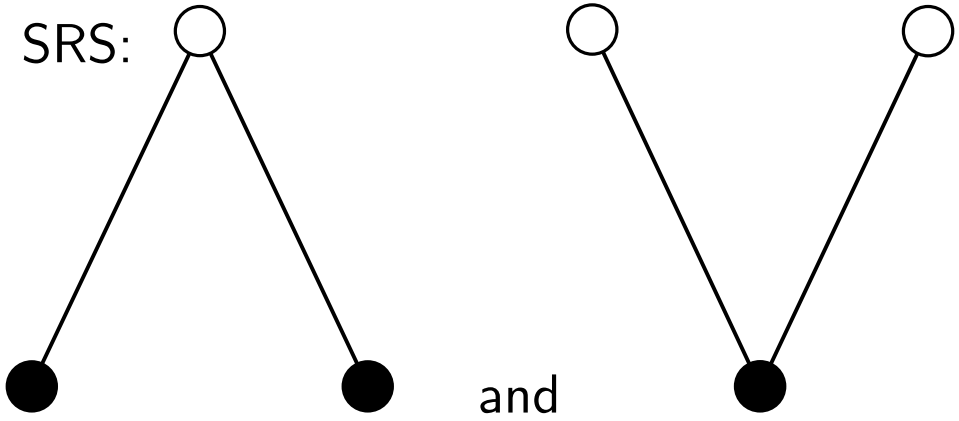


[1] This is closely related to finding a large minimal blocking set.

As a forbidden subgraph problem

What are the **forbidden configurations in the incidence graph**?

For pairs $(P, L), (P', L')$ in SRS:



and

Problem

What happens if we forbid other configurations?

We will discuss one today!

Unitals

In PG$(2, q)$ with q a square, this is easy.

Example

A **unital** $\mathcal{U}$ in PG$(2, q)$ gives rise to an SRS of size $q^{1.5} + 1$.

E.g., the Hermitian unital is, up to symmetry, the set of points $\langle x \rangle$ satisfying $x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} + x_3^{\sqrt{q}+1} = 0$.

Simply take (P, L) with $P \in \mathcal{U}$ and L the (unique) tangent at P.

This is **optimal**!

Theorem (Bruen, Thas (1977))

An SRS has size at most $q^{1.5} + 1$.

Szőnyi's Construction

Example

A trivial example of size $q+1$:

- Fix a line K.
- For each point $P \in K$, pick a line $L_P \neq K$.

Can we do better?

Szőnyi's Construction

Example

A trivial example of size $q+1$:

- Fix a line K.
- For each point $P \in K$, pick a line $L_P \neq K$.

Can we do better?

Theorem (Szönyi (1992))

There exists an SRS of size $\Omega(q \log q)$.

Proof.

Ramsey argument in Paley graphs. □

Verstraëte's Construction

Theorem (Hunter, Pohoata, Verstraëte, Zhang (2026*))

- *For every prime, there exists an SRS of size* $\gg q^{1.2334}$.
- *For every prime power, there exist SRS of size* $\gg q^{1.1167}$.

Recall: For square prime powers $q = p^{2t}$, unitals gave $q^{1.5} + 1$.

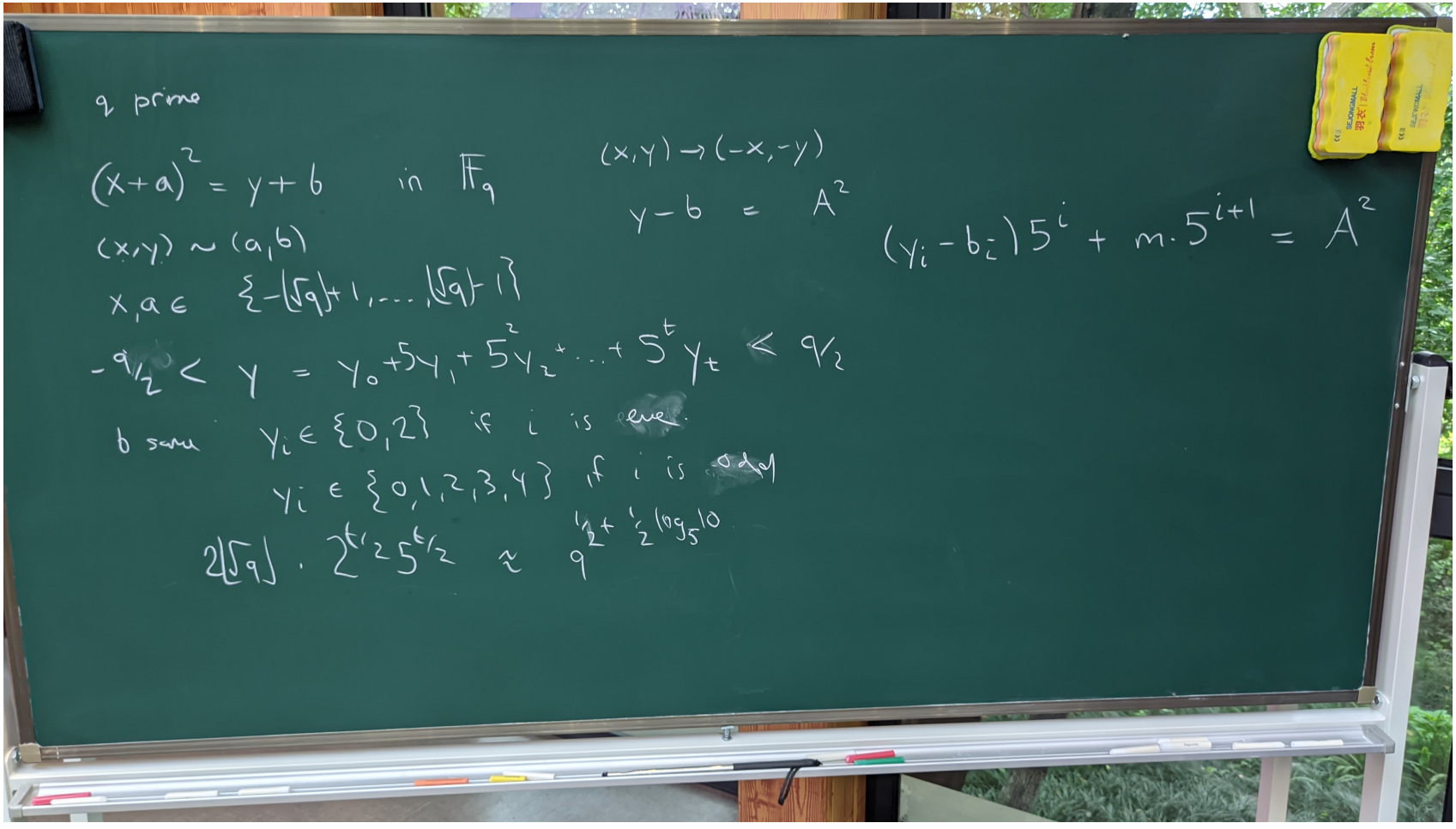
The **proof** uses:

Theorem (Ruzsa (1984); Beigel and Gasarch (2008))

There exists a square-difference-free subset of $[N]$ *of size at least* $N^{0.7334}$.

Note: $0.5 + 0.7334 = 1.2334$.

Why "Verstraëte's Construction"?



08 July 2025, BIRS Workshop, Hangzhou, China.

Pohoata's Construction

With the help of ChatGPT:

Theorem (Pohoata (late June 2026*))

For every fixed prime $r \geq 5$, for a $\frac{2}{r-1}$-fraction of all primes, there exists an SRS of size

$$\Omega(q^{1.5-2/(r-1)}).$$

Idea: Repeat Rusza's construction by something more complicated.

Locally Repairable Codes

Definition (LRCs)

A linear code C over $\mathbb{F}_q$ is a **locally repairable code (LRC)** with locality r if the i-th symbol c_i of $c \in C$ can be represented by a linear combination of r **other** coordinates (which are independent of c).

Example

Over $\mathbb{F}_2$, take

$$(a, b, c, d) \mapsto (a, b, a + b, c, d, c + d).$$

Repair groups are $\{1, 2, 3\}$ and $\{4, 5, 6\}$.

These satisfy a standard **Singleton-type bound**.

The **maximal length** of Singleton-optimal LRCs: popular open problem.

LRCs and Local Arcs

Theorem (Fang, Tao, Fu, Chen (2024))

*A Singleton-optimal $(n, m, 6; 3)$-LRC code with **disjoint repair groups** is equivalent to a **collection $\mathcal{S}$ of 4-subsets of points of PG$(2, q)$** such that*

1. $S \cap S' = \emptyset$,
2. $S \cup S'$ *is an arc, i.e., no three points collinear,*

for all distinct $S, S' \in \mathcal{S}$, where $n = 4|\mathcal{S}|$ and $m = 3|\mathcal{S}| - 3$.

LRCs and Local Arcs

Theorem (Fang, Tao, Fu, Chen (2024))

*A Singleton-optimal $(n, m, 6; 3)$-LRC code with **disjoint repair groups** is equivalent to a **collection $\mathcal{S}$ of 4-subsets of points of PG$(2, q)$** such that*

1. $S \cap S' = \emptyset$,
2. $S \cup S'$ *is an arc, i.e., no three points collinear,*

for all distinct $S, S' \in \mathcal{S}$, where $n = 4|\mathcal{S}|$ and $m = 3|\mathcal{S}| - 3$.

This motivated:

Definition (Ih., Zhou (2026*))

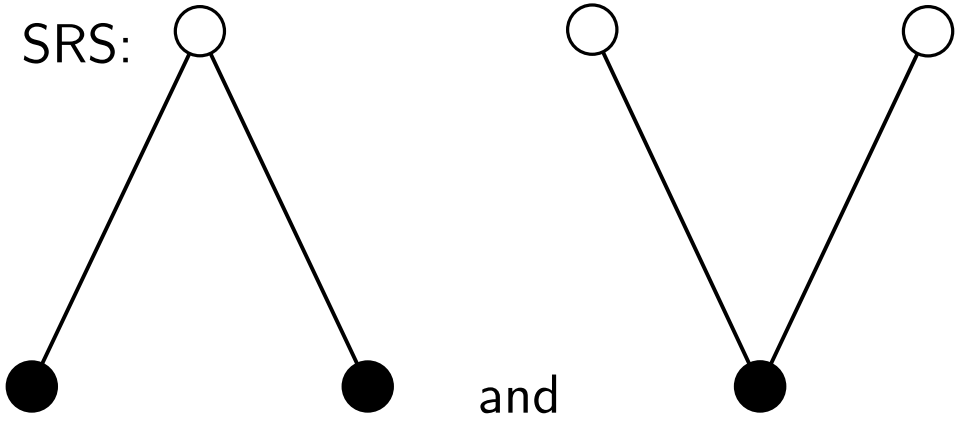
Let $\mathcal{S}$ be a collection of subsets of points of PG$(2, q)$ such that (1) and (2) above hold. Then we call $\mathcal{S}$ a **local arc**.

Call $\mathcal{S}$ **k-uniform** if $|S| = k$ for all $S \in \mathcal{S}$.

The Connection to SRS

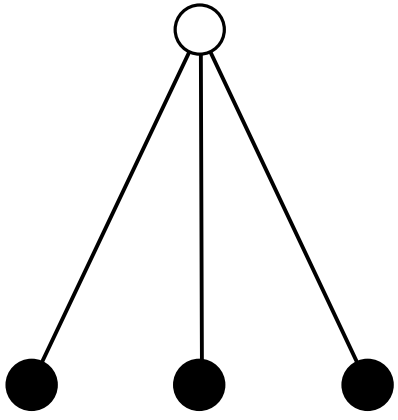
What are the **forbidden configurations in the incidence graph**?

For pairs $(P, L), (P', L')$ in SRS:



and

For pairs S, S' in a k-uniform local arcs:



A Trivial Construction

Example

Take an oval $\mathcal{O}$, i.e., a set of $q+1$ points $\langle x \rangle$ satisfying

$$x_1 x_3 = x_2^2.$$

Then we can find a k-uniform local arc $\mathcal{S}$ with $|\mathcal{S}| = \lfloor \frac{q+1}{k} \rfloor$.

One can improve this!

Example (Lu, Xiong (2026*))

A construction of size $\approx \frac{q}{2}$ for $k = 4$. Better by a factor of 2.

Upper Bounds

Consider a k-uniform local arc $\mathcal{S}$ in $\mathrm{PG}(2,q)$, where $m = |\mathcal{S}|$.

Fang, Tao, Fu, Chen (2024): For $k = 4$, $mk \leq \left(\frac{\sqrt{2}}{\sqrt{3}} + o(1)\right) q^{1.5}$.

Theorem (Ih., Zhou (2026*))

$$mk \leq \left(\frac{\sqrt{2}}{\sqrt{k-1}} + o(1)\right) q^{1.5}.$$

Proof: expander-mixing lemma.

A New Construction

Problem

Is there a construction larger than $O(q)$?

Theorem (Ih., Zhou (2026*))

Let $q = p^h$. Let s be the size of a maximum k-uniform local arc. Then

1. *If h odd, then $s = \Omega(q^{1.1167+0.1167/h})$.* *If $h = 1$, $s = \Omega(q^{1.2334})$.*
2. *If $h = 4$, then $s = \Omega(q^{1.1167})$.*
3. *If $h \equiv 2 \pmod 4$, then $s = \Omega(q^{1.25-0.2666/h})$.*
4. *If $h \equiv 0 \pmod 4$, $h > 4$, then $s = \Omega(q^{1.25-0.7666/h})$.*

- Inspired by an early version of Verstraëte's Construction.
- **Key idea:** combine additive combinatorics and finite geometry.

Framework

We use the following definition of $\mathrm{PG}(2,q)$ associated with the planar function $f(x) = x^2$:

Points: $\{(x,y) : x,y \in \mathbb{F}_q\}$

Lines: $\{[a,b] : a,b \in \mathbb{F}_q\}$

Incidence: (x,y) is incident with $[a,b]$ if $y - b = (x-a)^2$

Framework

We use the following definition of $\mathrm{PG}(2,q)$ associated with the planar function $f(x) = x^2$:

Points: $\{(x,y) : x,y \in \mathbb{F}_q\} \cup \{(z) : z \in \mathbb{F}_q \cup \{\infty\}\}$;

Lines: $\{[a,b] : a,b \in \mathbb{F}_q\} \cup \{[c] : c \in \mathbb{F}_q \cup \{\infty\}\}$;

Incidence: (x,y) is incident with $[a,b]$ if $y - b = (x-a)^2$;
(x,y) is incident with $[c]$ if $x = c$;
(z) is incident with $[a,b]$ if $z = b$;
(z) is incident with $[\infty]$;
(∞) is incident with $[c]$.

We **only** care about the **affine points**.

Structure of the Construction

First only for $q = p$ prime!

Step 1:

Construct a **generic arc** D in $\mathbb{Z}^2$ with k points.

Step 2:

Find a **suitable set of translations** T to obtain a k-uniform local arc $\{D + \tau : \tau \in T\}$ in $\mathbb{Z}^2$.

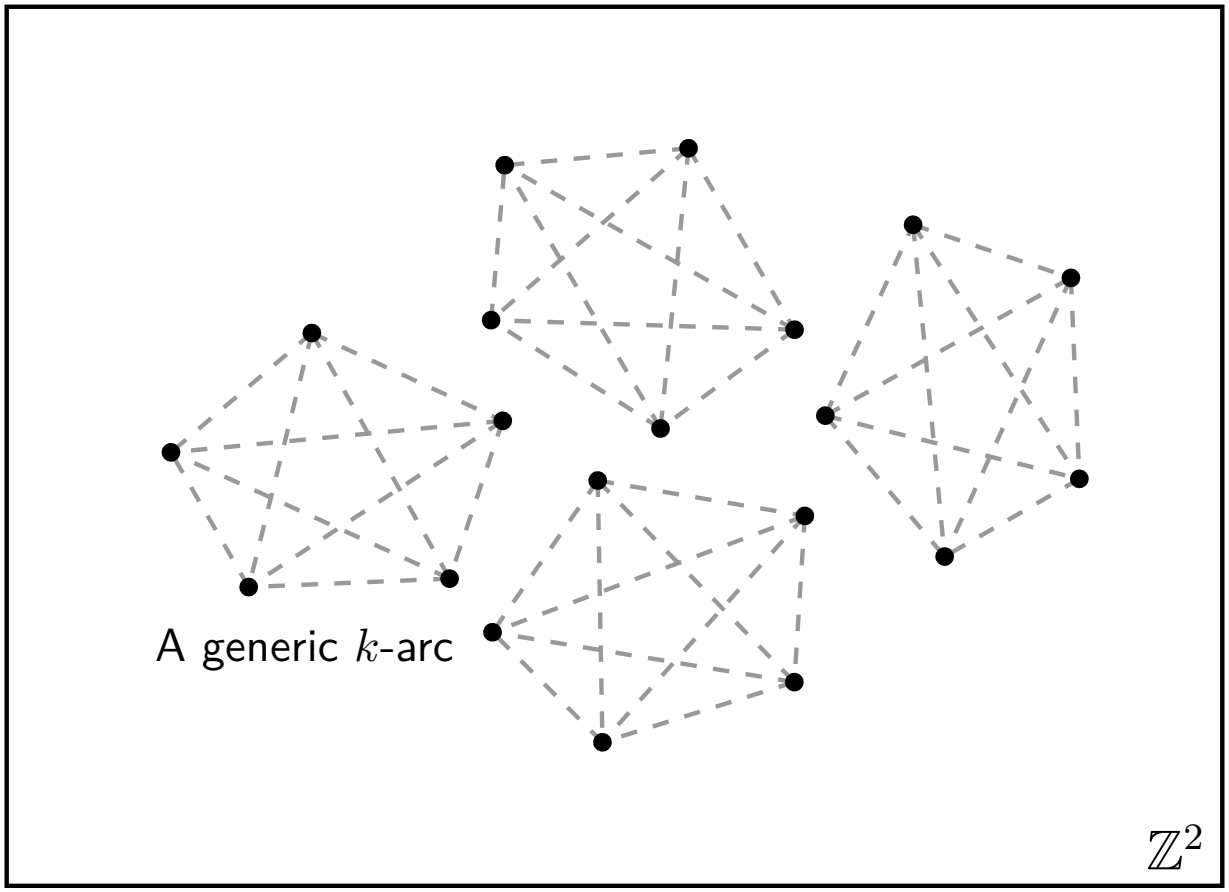
Step 3:

Project from $\mathbb{Z}^2$ to $\mathbb{F}_p^2$ for p large enough.

Step 1: Generic Local Arcs

The following is a **generic arc** of size k:

$$D := \left\{ (x, 2x) : x = \lfloor \tfrac{k^2}{2} \rfloor + 2i \text{ for } i = 0, 1, \ldots, k-1 \right\}.$$



Step 2: Square-difference free sets (1)

Needed: A large **square-difference-free set** modulo m.

Based on Ruzsa (1984):

Example (Beigel and Gasarch (2008))

For $m = 205$, the set $A = \{0, 2, 8, 14, 77, 79, 85, 96, 103, 109, 111, 181\}$ is square-difference-free modulo m.

For a point (x, y), write $y = \sum_{i=0}^{\infty} y_i m^i$ in the **m-ary representation**.

Use the translations

$$T = \left\{ \left(x, \sum_{i=0}^{\infty} y_i m^i \right) : x \in \mathbb{Z}, y_{\text{even}} \in A, y_{\text{odd}} \in \{0, \ldots, m-1\} \right\}.$$

Step 2: Square-difference free sets (2)

Recall

$$T = \left\{ \left(x, \sum_{i=0}^{\infty} y_i m^i \right) : x \in \mathbb{Z}, y_{\text{even}} \in A, y_{\text{odd}} \in \{0, \ldots, m-1\} \right\}.$$

The argument for integers is that

$$(x-a)^2 = y - b \neq 0$$

in the m-adic representation means that

1. the first digit where y and b differ is **even**,
2. it is also a **nonsquare** modulo m.

This contradicts $(x-a)^2$ being a square.

Step 3: Project onto $\mathbb{F}_p^2$

Recall

$$T = \left\{ \left(x, \sum_{i=0}^{\infty} y_i m^i \right) : x \in \mathbb{Z}, y_{\text{even}} \in A, y_{\text{odd}} \in \{0, \ldots, m-1\} \right\}.$$

Problem: This parity argument stops working modulo p.

Step 3: Project onto $\mathbb{F}_p^2$

Recall

$$T = \left\{ \left(x, \sum_{i=0}^{\infty} y_i m^i \right) : x \in \mathbb{Z}, y_{\text{even}} \in A, y_{\text{odd}} \in \{0, \ldots, m-1\} \right\}.$$

Problem: This parity argument stops working modulo p.

Trick: Keep x small enough so that calculating in $\mathbb{F}_p$ is like $\mathbb{Z}$.

Solution: We square, so keeping $|x|$ smaller than $\sqrt{p}$ is enough, i.e., for $B \approx \sqrt{p}$. We also need to end the sum at $t \approx \log_m p$. That is,

$$T = \left\{ \left(x, \sum_{i=0}^{\textbf{t-1}} y_i m^i \right) : \textbf{x} \in \textbf{[-B, B]}, y_{\text{even}} \in A, y_{\text{odd}} \in \{0, \ldots, m-1\} \right\}.$$

Step 3: Project onto $\mathbb{F}_p^2$

Recall

$$T = \left\{ \left(x, \sum_{i=0}^{\infty} y_i m^i \right) : x \in \mathbb{Z}, y_{\text{even}} \in A, y_{\text{odd}} \in \{0, \ldots, m-1\} \right\}.$$

Problem: This parity argument stops working modulo p.

Trick: Keep x small enough so that calculating in $\mathbb{F}_p$ is like $\mathbb{Z}$.

Solution: We square, so keeping $|x|$ smaller than $\sqrt{p}$ is enough, i.e., for $B \approx \sqrt{p}$. We also need to end the sum at $t \approx \log_m p$. That is,

$$T = \left\{ \left(x, \sum_{i=0}^{\textbf{t-1}} y_i m^i \right) : \textbf{x} \in \textbf{[-B, B]}, y_{\text{even}} \in A, y_{\text{odd}} \in \{0, \ldots, m-1\} \right\}.$$

Size:

$$|T| \approx 2|B| \cdot |A|^{t/2} m^{t/2} = C m^t |A|^{t/2} = C p^{1+\frac{1}{2}\log_m |A|} \approx C p^{1.2334}.$$

The lifting to prime powers $q = p^h$ works similarly.

What about Pohoata?

In our construction, the **set of translations** can be replaced by something **denser**.

If we replace Verstraëte by Pohoata, then:

Theorem ((unpublished))

Let $q = p$ and $r \geq 5$ prime. Let s be the size of a maximum k-uniform local arc. Then, for a $\frac{2}{r-1}$ fraction of primes p,

$$s = \Omega(q^{1.5-2/(r-1)}).$$

Then our paper was already accepted, so we did not adjust our proof.[2]

[2] An LLM can do it for you. It is just a complicated search and replace.

Some Problems

Our regime has k fixed.

Problem

Investigate the case where k grows with q.

Problem

*Investigate these **induced Turán problems** in PG$(2, q)$ more generally.*

Problem

Can the construction be generalized to other LRCs?

Thank you for your attention!