Line-parallelisms of $\mathrm{PG}(n, 2)$ from Preparata-like codes

Vladislav Taranchuk
(joint work with Philipp Heering)

September 2, 2025

7th Finite Geometry Conference

Irsee, Germany

GHENT UNIVERSITY

Line-spreads

Definition.
A **line-spread** of $\mathrm{PG}(n, q)$ is a partition of the points of $\mathrm{PG}(n, q)$ into lines of $\mathrm{PG}(n, q)$.

Line-spreads

Definition.
A **line-spread** of $\mathrm{PG}(n, q)$ is a partition of the points of $\mathrm{PG}(n, q)$ into lines of $\mathrm{PG}(n, q)$.

- Equivalently, a line-spread of $\mathrm{PG}(n, q)$ can be thought of as partition of the non-zero vectors of $\mathbb{F}_q^{n+1}$ into 2-dimensional subspaces.

Line-spreads

Definition.
A **line-spread** of $\mathrm{PG}(n, q)$ is a partition of the points of $\mathrm{PG}(n, q)$ into lines of $\mathrm{PG}(n, q)$.

- Equivalently, a line-spread of $\mathrm{PG}(n, q)$ can be thought of as partition of the non-zero vectors of $\mathbb{F}_q^{n+1}$ into 2-dimensional subspaces.
- Simple counting argument implies line-spreads only exist in $\mathrm{PG}(n, q)$ if n is odd.

Line-spreads

Definition.
A **line-spread** of $PG(n, q)$ is a partition of the points of $PG(n, q)$ into lines of $PG(n, q)$.

- Equivalently, a line-spread of $PG(n, q)$ can be thought of as partition of the non-zero vectors of $\mathbb{F}_q^{n+1}$ into 2-dimensional subspaces.
- Simple counting argument implies line-spreads only exist in $PG(n, q)$ if n is odd.
- On the other hand, when n is odd, many line-spreads are known to exist in $PG(n, q)$ for any prime power q.

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n, q)$ is a partition of the lines of $\mathrm{PG}(n, q)$ into line-spreads.

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n, q)$ is a partition of the lines of $\mathrm{PG}(n, q)$ into line-spreads.

- Equivalently, this is a partition of all 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ into line-spreads.

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n, q)$ is a partition of the lines of $\mathrm{PG}(n, q)$ into line-spreads.

- Equivalently, this is a partition of all 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ into line-spreads.
- Line-parallelisms of $\mathrm{PG}(n, q)$ consist of $\frac{q^n-1}{q-1}$ line-spreads.

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n, q)$ is a partition of the lines of $\mathrm{PG}(n, q)$ into line-spreads.

- Equivalently, this is a partition of all 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ into line-spreads.
- Line-parallelisms of $\mathrm{PG}(n, q)$ consist of $\frac{q^n-1}{q-1}$ line-spreads.
- Again, we have a necessary condition that n is odd.

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n, q)$ is a partition of the lines of $\mathrm{PG}(n, q)$ into line-spreads.

- Equivalently, this is a partition of all 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ into line-spreads.
- Line-parallelisms of $\mathrm{PG}(n, q)$ consist of $\frac{q^n-1}{q-1}$ line-spreads.
- Again, we have a necessary condition that n is odd. *But is it sufficient?*

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n, q)$ is a partition of the lines of $\mathrm{PG}(n, q)$ into line-spreads.

- Equivalently, this is a partition of all 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ into line-spreads.
- Line-parallelisms of $\mathrm{PG}(n, q)$ consist of $\frac{q^n-1}{q-1}$ line-spreads.
- Again, we have a necessary condition that n is odd. *But is it sufficient?*
- Sufficient for $q = 2$ (Zaitsev, Zinoviev, and Semakov 1973 and Baker 1976)

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n,q)$ is a partition of the lines of $\mathrm{PG}(n,q)$ into line-spreads.

- Equivalently, this is a partition of all 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ into line-spreads.
- Line-parallelisms of $\mathrm{PG}(n,q)$ consist of $\frac{q^n-1}{q-1}$ line-spreads.
- Again, we have a necessary condition that n is odd. *But is it sufficient?*
- Sufficient for $q=2$ (Zaitsev, Zinoviev, and Semakov 1973 and Baker 1976)
- Sufficient for any $q>2$ when $n=2^k-1$ (Beutelspacher 1974)

Line-parallelisms

Definition.
A **line-parallelism** (or **line-packing**) of $\mathrm{PG}(n, q)$ is a partition of the lines of $\mathrm{PG}(n, q)$ into line-spreads.

- Equivalently, this is a partition of all 2-dimensional subspaces of $\mathbb{F}_q^{n+1}$ into line-spreads.
- Line-parallelisms of $\mathrm{PG}(n, q)$ consist of $\frac{q^n-1}{q-1}$ line-spreads.
- Again, we have a necessary condition that n is odd. *But is it sufficient?*
- Sufficient for $q = 2$ (Zaitsev, Zinoviev, and Semakov 1973 and Baker 1976)
- Sufficient for any $q > 2$ when $n = 2^k - 1$ (Beutelspacher 1974)
- Sufficient for $q = 3, 4, 8, 16$ (Xu and Feng 2023)

Notions in Coding Theory

Definition.
A **linear code** with parameters $[n, k, d]_q$ is a k-dimensional subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ such that the Hamming distance between any two vectors in $\mathcal{C}$ is at least d.

Notions in Coding Theory

Definition.
A **linear code** with parameters $[n, k, d]_q$ is a k-dimensional subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ such that the Hamming distance between any two vectors in $\mathcal{C}$ is at least d.

Example: Let H be the $t \times (2^t - 1)$ matrix over $\mathbb{F}_2$ whose columns are formed precisely by all non-zero vectors of $\mathbb{F}_2^t$.

Notions in Coding Theory

Definition.
A **linear code** with parameters $[n, k, d]_q$ is a k-dimensional subspace $\mathcal{C}$ of $\mathbb{F}_q^n$ such that the Hamming distance between any two vectors in $\mathcal{C}$ is at least d.

Example: Let H be the $t \times (2^t - 1)$ matrix over $\mathbb{F}_2$ whose columns are formed precisely by all non-zero vectors of $\mathbb{F}_2^t$.

The null space of H is called the **binary linear Hamming code** $\mathrm{Ham}(t, 2)$ which has parameters

- Length $n = 2^t - 1$.
- Dimension $k = 2^t - t - 1$.
- Minimum distance $d = 3$.

More on the Hamming code

The minimum weight codewords of $\mathrm{Ham}(t,2)$ correspond to lines in $PG(t-1,2)$.

More on the Hamming code

The minimum weight codewords of $\mathrm{Ham}(t, 2)$ correspond to lines in $PG(t-1, 2)$.

- Minimum weight codewords have three non-zero entries, say in positions i, j, k.

More on the Hamming code

The minimum weight codewords of $\mathrm{Ham}(t, 2)$ correspond to lines in $PG(t-1, 2)$.

- Minimum weight codewords have three non-zero entries, say in positions i, j, k.
- Therefore, the columns H_i, H_j, H_k of H must sum to zero, thus $\{0, H_i, H_j, H_k\}$ is a 2-dimensional subspace of $\mathbb{F}_2^t$.

More on the Hamming code

The minimum weight codewords of $\mathrm{Ham}(t, 2)$ correspond to lines in $PG(t-1, 2)$.

- Minimum weight codewords have three non-zero entries, say in positions i, j, k.
- Therefore, the columns H_i, H_j, H_k of H must sum to zero, thus $\{0, H_i, H_j, H_k\}$ is a 2-dimensional subspace of $\mathbb{F}_2^t$.
- It follows that the codeword associated with any 2-dimensional subspace in this way belongs to $\mathrm{Ham}(t, 2)$.

Partitioning the linear Hamming code

Let P_t is a binary code with length $n = 2^t - 1$, minimum distance $d = 5$, and size such that $|\mathrm{Ham}(t, 2)|/|P_t| = 2^{t-1}$.

Partitioning the linear Hamming code

Let P_t is a binary code with length $n = 2^t - 1$, minimum distance $d = 5$, and size such that $|\mathrm{Ham}(t, 2)|/|P_t| = 2^{t-1}$. **If Ham$(t, 2)$ can be partitioned into 2^{t-1} copies of P_t, then:**

Partitioning the linear Hamming code

Let P_t is a binary code with length $n = 2^t - 1$, minimum distance $d = 5$, and size such that $|\mathrm{Ham}(t,2)|/|P_t| = 2^{t-1}$. **If Ham$(t,2)$ can be partitioned into 2^{t-1} copies of P_t, then:**

- The copy of P_t containing the zero codeword does not contain any weight three codewords of $\mathrm{Ham}(t,2)$.

Partitioning the linear Hamming code

Let P_t is a binary code with length $n = 2^t - 1$, minimum distance $d = 5$, and size such that $|\mathrm{Ham}(t,2)|/|P_t| = 2^{t-1}$.
If Ham$(t,2)$ can be partitioned into 2^{t-1} copies of P_t, then:

- The copy of P_t containing the zero codeword does not contain any weight three codewords of $\mathrm{Ham}(t,2)$.
- Thus the minimum weight codewords of $\mathrm{Ham}(t,2)$ are split amongst the remaining $2^{t-1} - 1$ copies of P_t.

Partitioning the linear Hamming code

Let P_t is a binary code with length $n = 2^t - 1$, minimum distance $d = 5$, and size such that $|\mathrm{Ham}(t,2)|/|P_t| = 2^{t-1}$.
If Ham$(t,2)$ can be partitioned into 2^{t-1} copies of P_t, then:

- The copy of P_t containing the zero codeword does not contain any weight three codewords of $\mathrm{Ham}(t,2)$.
- Thus the minimum weight codewords of $\mathrm{Ham}(t,2)$ are split amongst the remaining $2^{t-1} - 1$ copies of P_t.
- Any two codewords of weight 3 in the same copy of P_t must have disjoint supports since P_t has minimum distance 5.

Partitioning the linear Hamming code

Let P_t is a binary code with length $n = 2^t - 1$, minimum distance $d = 5$, and size such that $|\mathrm{Ham}(t, 2)|/|P_t| = 2^{t-1}$.
If Ham$(t, 2)$ can be partitioned into 2^{t-1} copies of P_t, then:

- The copy of P_t containing the zero codeword does not contain any weight three codewords of $\mathrm{Ham}(t, 2)$.
- Thus the minimum weight codewords of $\mathrm{Ham}(t, 2)$ are split amongst the remaining $2^{t-1} - 1$ copies of P_t.
- Any two codewords of weight 3 in the same copy of P_t must have disjoint supports since P_t has minimum distance 5.
- Consequently, each copy of P_t contains codewords corresponding to a line-spread of $PG(t-1, 2)$ and all the line-spreads together yield a parallelism.

Preparata-like codes

Definition.
We call a binary code P_t **Preparata-like** if it has length $2^t - 1$, contains 2^{2^t-2t} codewords and has minimum distance 5.

Preparata-like codes

Definition.
We call a binary code P_t **Preparata-like** if it has length $2^t - 1$, contains $2^{2^t - 2t}$ codewords and has minimum distance 5.

The following is a list of all known Preparata-like codes of length $2^t - 1$ which are known to be contained in $\mathrm{Ham}(t, 2)$.

Preparata-like codes

Definition.
We call a binary code P_t **Preparata-like** if it has length $2^t - 1$, contains $2^{2^t - 2t}$ codewords and has minimum distance 5.

The following is a list of all known Preparata-like codes of length $2^t - 1$ which are known to be contained in $\mathrm{Ham}(t, 2)$.

- 1968: Preparata constructs the first class of such codes.

Preparata-like codes

Definition.
We call a binary code P_t **Preparata-like** if it has length $2^t - 1$, contains $2^{2^t - 2t}$ codewords and has minimum distance 5.

The following is a list of all known Preparata-like codes of length $2^t - 1$ which are known to be contained in $\mathrm{Ham}(t, 2)$.

- 1968: Preparata constructs the first class of such codes.
- 1983: Baker, van Lint, and Wilson simplify and generalize Preparata's construction. This leads to the class of **generalized Preparata codes**.

Preparata-like codes

Definition.
We call a binary code P_t **Preparata-like** if it has length $2^t - 1$, contains $2^{2^t - 2t}$ codewords and has minimum distance 5.

The following is a list of all known Preparata-like codes of length $2^t - 1$ which are known to be contained in $\mathrm{Ham}(t, 2)$.

- 1968: Preparata constructs the first class of such codes.
- 1983: Baker, van Lint, and Wilson simplify and generalize Preparata's construction. This leads to the class of **generalized Preparata codes**.
- 2000: van Dam and Fon-Der-Flaass construct crooked Preparata-like codes from crooked functions.

2 Partitioning the Hamming code

It is known that any generalized Preparata code gives rise to a partition of the linear Hamming code of the same length.

Partitioning the Hamming code

It is known that any generalized Preparata code gives rise to a partition of the linear Hamming code of the same length.

- 1973: Zaitsev, Zinoviev, and Semakov prove this fact for the classical Preparata code. Also independently noted by Baker in 1976.

Partitioning the Hamming code

It is known that any generalized Preparata code gives rise to a partition of the linear Hamming code of the same length.

- 1973: Zaitsev, Zinoviev, and Semakov prove this fact for the classical Preparata code. Also independently noted by Baker in 1976.
- 1983: Baker, van Lint, and Wilson prove this fact for the generalized Preparata codes.

Partitioning the Hamming code

It is known that any generalized Preparata code gives rise to a partition of the linear Hamming code of the same length.

- 1973: Zaitsev, Zinoviev, and Semakov prove this fact for the classical Preparata code. Also independently noted by Baker in 1976.
- 1983: Baker, van Lint, and Wilson prove this fact for the generalized Preparata codes.
- 2016: V. A. Zinoviev and D. V. Zinoviev gave a new and inequivalent partitioning using generalized Preparata codes via a group theoretic approach.

Partitioning the Hamming code

It is known that any generalized Preparata code gives rise to a partition of the linear Hamming code of the same length.

- 1973: Zaitsev, Zinoviev, and Semakov prove this fact for the classical Preparata code. Also independently noted by Baker in 1976.
- 1983: Baker, van Lint, and Wilson prove this fact for the generalized Preparata codes.
- 2016: V. A. Zinoviev and D. V. Zinoviev gave a new and inequivalent partitioning using generalized Preparata codes via a group theoretic approach.

Theorem (Heering and T. 2025+).
Let P_t be any Preparata-like code contained inside the Hamming code $\mathrm{Ham}(t, 2)$ of the same length. Then $\mathrm{Ham}(t, 2)$ can be partitioned into additive translates of P_t.

3 Crooked functions

Definition (Bending and Fon-Der-Flaass (1998)).
A function $f(x)$ over $\mathbb{F}_{2^n}$ is called crooked if $f(0) = 0$ and for $a \neq 0$, the sets

$$H_a = \{f(x + a) + f(x) : x \in \mathbb{F}_{2^n}\}$$

are all distinct and are the complement of a hyperplane.

Crooked functions

Definition (Bending and Fon-Der-Flaass (1998)).
A function $f(x)$ over $\mathbb{F}_{2^n}$ is called crooked if $f(0) = 0$ and for $a \neq 0$, the sets

$$H_a = \{f(x+a) + f(x) : x \in \mathbb{F}_{2^n}\}$$

are all distinct and are the complement of a hyperplane.

Definition.
Let f and f' be two crooked functions over $\mathbb{F}_{2^n}$. We say

1. f' is **linearly equivalent** to f if there exists linear permutations L_1, L_2 of $\mathbb{F}_{2^n}$ such that $f' = L_1 f L_2$.
2. f' is **affine equivalent** to f if there exists affine permutations A_1, A_2 of $\mathbb{F}_{2^n}$ such that $f' = A_1 f A_2$.

Parallelisms from crooked functions

Definition.
Let f be a crooked function over $\mathbb{F}_{2^n}$ and $V = \mathbb{F}_{2^n} \times \mathbb{F}_2$. The coloring function $c_f : V \times V \to \mathbb{F}_{2^n}$ is defined by

$$c_f((x, x_1), (y, y_1)) = f(x) + f(y) + f(x + y) + f(x_1 y + y_1 x).$$

Parallelisms from crooked functions

Definition.
Let f be a crooked function over $\mathbb{F}_{2^n}$ and $V = \mathbb{F}_{2^n} \times \mathbb{F}_2$. The coloring function $c_f : V \times V \to \mathbb{F}_{2^n}$ is defined by

$$c_f((x, x_1), (y, y_1)) = f(x) + f(y) + f(x + y) + f(x_1 y + y_1 x).$$

- c_f is constant and non-zero on lines of $\mathrm{PG}(n, 2)$.

Parallelisms from crooked functions

Definition.
Let f be a crooked function over $\mathbb{F}_{2^n}$ and $V = \mathbb{F}_{2^n} \times \mathbb{F}_2$. The coloring function $c_f : V \times V \to \mathbb{F}_{2^n}$ is defined by

$$c_f((x, x_1), (y, y_1)) = f(x) + f(y) + f(x + y) + f(x_1 y + y_1 x).$$

- c_f is constant and non-zero on lines of $\mathrm{PG}(n, 2)$.
- Any two lines given the same color $\mathbb{F}_{2^n}^*$ do not intersect.

Parallelisms from crooked functions

Definition.
Let f be a crooked function over $\mathbb{F}_{2^n}$ and $V = \mathbb{F}_{2^n} \times \mathbb{F}_2$. The coloring function $c_f : V \times V \to \mathbb{F}_{2^n}$ is defined by

$$c_f((x, x_1), (y, y_1)) = f(x) + f(y) + f(x + y) + f(x_1 y + y_1 x).$$

- c_f is constant and non-zero on lines of $\mathrm{PG}(n, 2)$.
- Any two lines given the same color $\mathbb{F}^*_{2^n}$ do not intersect.
- It follows that each color class of lines is a line-spread, and all together form a line-parallelism.

The equivalence problem

Definition.
Two line parallelisms Π_1 and Π_2 of $\mathrm{PG}(n, 2)$ are **equivalent** if there exists a collineation of $\mathrm{PG}(n, 2)$ which maps the line-spreads of Π_1 to the line-spreads of Π_2.

3 The equivalence problem

Definition.
Two line parallelisms Π_1 and Π_2 of $\mathrm{PG}(n,2)$ are **equivalent** if there exists a collineation of $\mathrm{PG}(n,2)$ which maps the line-spreads of Π_1 to the line-spreads of Π_2.

Theorem (Heering and T. 2025+).
Let $f(x)$ and $f'(x)$ be crooked over $\mathbb{F}_{2^n}$ with $n > 1$ odd and let Π_f and $\Pi_{f'}$ be the parallelisms induced by c_f and $c_{f'}$.

1. If $f(x)$ and $f'(x)$ are linearly equivalent, then Π_f and $\Pi_{f'}$ are equivalent.
2. Suppose further that $f(x)$ and $f'(x)$ are quadratic and that $n > 3$. It holds that Π_f and Π_f' are equivalent if and only $f(x)$ and $f'(x)$ are affine equivalent.

3 Survey of known line-parallelisms of $PG(n, 2)$

The following list describes all known line-parallelisms of $\mathrm{PG}(n, 2)$ (which also includes our contribution).

Survey of known line-parallelisms of $PG(n, 2)$

The following list describes all known line-parallelisms of PG$(n, 2)$ (which also includes our contribution).

1. Crooked line-parallelisms arising from the partition of the linear Hamming code into additive translates of any crooked Preparata-like code.

3 Survey of known line-parallelisms of $PG(n, 2)$

The following list describes all known line-parallelisms of $\mathrm{PG}(n, 2)$ (which also includes our contribution).

1. Crooked line-parallelisms arising from the partition of the linear Hamming code into additive translates of any crooked Preparata-like code.
2. Line-parallelisms arising from the partitioning of the linear Hamming code into cosets of the generalized Preparata codes via a group theoretical approach.

3 Survey of known line-parallelisms of $PG(n, 2)$

The following list describes all known line-parallelisms of $\mathrm{PG}(n, 2)$ (which also includes our contribution).

1. Crooked line-parallelisms arising from the partition of the linear Hamming code into additive translates of any crooked Preparata-like code.
2. Line-parallelisms arising from the partitioning of the linear Hamming code into cosets of the generalized Preparata codes via a group theoretical approach.
3. A construction of line-parallelisms of $\mathrm{PG}(n, 2)$ by Wettl in 1994, inequivalent to those coming from the generalized Preparata codes.

3 Survey of known line-parallelisms of $PG(n,2)$

The following list describes all known line-parallelisms of PG(n, 2) (which also includes our contribution).

1. Crooked line-parallelisms arising from the partition of the linear Hamming code into additive translates of any crooked Preparata-like code.
2. Line-parallelisms arising from the partitioning of the linear Hamming code into cosets of the generalized Preparata codes via a group theoretical approach.
3. A construction of line-parallelisms of PG(n, 2) by Wettl in 1994, inequivalent to those coming from the generalized Preparata codes.
4. Specific examples in PG(3, 2), PG(5, 2), PG(7, 2), PG(9, 2) mostly obtained by computer.

Conclusion

Can the coloring function method be used to resolve more cases for the existence of parallelisms when $q > 2$?

3 Conclusion

Can the coloring function method be used to resolve more cases for the existence of parallelisms when $q > 2$?

We have some ideas, come talk to us if you're interested!

Thank you!