Partial Difference Sets: Broadening the Scope of the Denniston Family

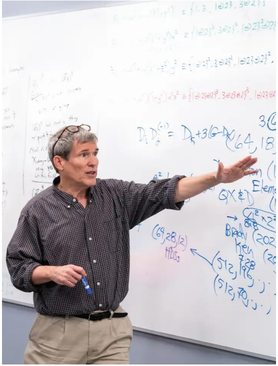
Shuxing Li

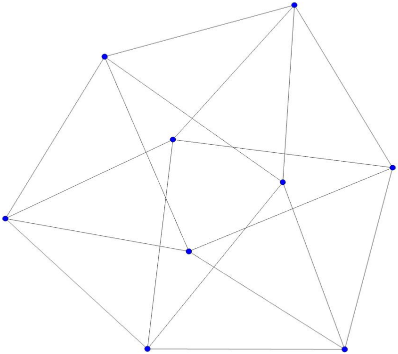
University of Delaware

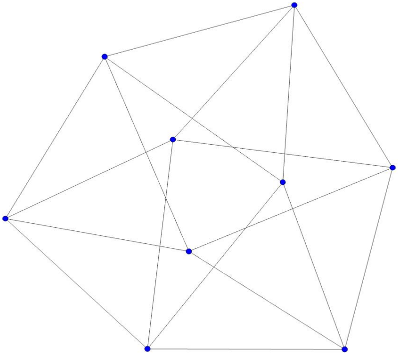
Joint work with James Davis, Sophie Huczynska, Laura Johnson, John Polhill

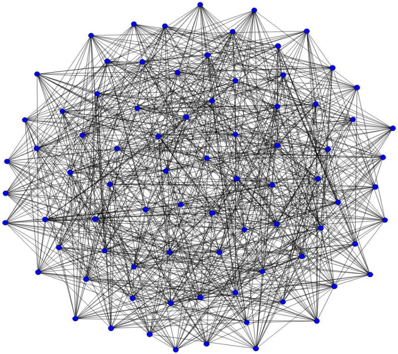
Hadamard 2025 at University of Seville

May-27-2025









Let $ax^2 + bxy + cy^2$ be an irreducible quadratic form over $\mathbb{F}_{2^m}$. Let H be an order 2^r subgroup of $(\mathbb{F}_{2^m}, +)$, with $1 \le r \le m-1$. Consider a subset

$$D = \{(x, y) \mid ax^2 + bxy + cy^2 \in H\} \subset \mathbb{F}_{2^m} \times \mathbb{F}_{2^m},$$

where $|D| = 1 + (2^m + 1)(2^r - 1)$.

Let $ax^2 + bxy + cy^2$ be an irreducible quadratic form over $\mathbb{F}_{2^m}$. Let H be an order 2^r subgroup of $(\mathbb{F}_{2^m}, +)$, with $1 \le r \le m-1$. Consider a subset

$$D = \{(x, y) \mid ax^2 + bxy + cy^2 \in H\} \subset \mathbb{F}_{2^m} \times \mathbb{F}_{2^m},$$

where $|D| = 1 + (2^m + 1)(2^r - 1)$.

Regarding D as a point set in the affine plane $\mathrm{AG}(2, 2^m)$, then D satisfies an intriguing property:

Let $ax^2 + bxy + cy^2$ be an irreducible quadratic form over $\mathbb{F}_{2^m}$. Let H be an order 2^r subgroup of $(\mathbb{F}_{2^m}, +)$, with $1 \le r \le m-1$. Consider a subset

$$D = \{(x,y) \mid ax^2 + bxy + cy^2 \in H\} \subset \mathbb{F}_{2^m} \times \mathbb{F}_{2^m},$$

where $|D| = 1 + (2^m + 1)(2^r - 1)$.

Regarding D as a point set in the affine plane $\mathrm{AG}(2, 2^m)$, then D satisfies an intriguing property:

every line in $AG(2, 2^m)$ intersects D in either 0 or 2^r points.

Let $ax^2 + bxy + cy^2$ be an irreducible quadratic form over $\mathbb{F}_{2^m}$. Let H be an order 2^r subgroup of $(\mathbb{F}_{2^m}, +)$, with $1 \leq r \leq m-1$. Consider a subset

$$D = \{(x, y) \mid ax^2 + bxy + cy^2 \in H\} \subset \mathbb{F}_{2^m} \times \mathbb{F}_{2^m},$$

where $|D| = 1 + (2^m + 1)(2^r - 1)$.

Regarding D as a point set in the affine plane $\mathrm{AG}(2, 2^m)$, then D satisfies an intriguing property:

every line in $AG(2, 2^m)$ intersects D in either 0 or 2^r points.

For instance, consider a line L in $\mathrm{AG}(2, 2^m)$ with equation $y = dx$, where $d \in \mathbb{F}_{2^m}$. Therefore, $D \cap L = \{x \in \mathbb{F}_{2^m} \mid (a + bd + cd^2)x^2 \in H\}$.

Let $ax^2+bxy+cy^2$ be an irreducible quadratic form over $\mathbb{F}_{2^m}$. Let H be an order 2^r subgroup of $(\mathbb{F}_{2^m},+)$, with $1 \le r \le m-1$. Consider a subset

$$D = \{(x,y) \mid ax^2+bxy+cy^2 \in H\} \subset \mathbb{F}_{2^m} \times \mathbb{F}_{2^m},$$

where $|D| = 1 + (2^m+1)(2^r-1)$.

Regarding D as a point set in the affine plane $\mathrm{AG}(2,2^m)$, then D satisfies an intriguing property:

every line in $AG(2,2^m)$ intersects D in either 0 or 2^r points.

For instance, consider a line L in $\mathrm{AG}(2,2^m)$ with equation $y = dx$, where $d \in \mathbb{F}_{2^m}$. Therefore, $D \cap L = \{x \in \mathbb{F}_{2^m} \mid (a+bd+cd^2)x^2 \in H\}$.

Note that $a+bd+cd^2 \neq 0$ and x^2 induces a permutation over $\mathbb{F}_{2^m}$ (due to $\mathbb{F}_{2^m}$ has characteristic 2), $|D \cap L| = 2^r$.

Embedding D into $\mathrm{PG}(2, 2^m)$

Embedding D into the projective plane $\mathrm{PG}(2, 2^m)$, we have a point set

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\},$$

with $|D'| = 1 + (2^m + 1)(2^r - 1)$, such that:

every line in $PG(2, 2^m)$ *intersect* D' *in either* 0 *or* 2^r *points.*

Embedding D into $\mathrm{PG}(2, 2^m)$

Embedding D into the projective plane $\mathrm{PG}(2, 2^m)$, we have a point set

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\},$$

with $|D'| = 1 + (2^m + 1)(2^r - 1)$, such that:

every line in $PG(2, 2^m)$ *intersect* D' *in either* 0 *or* 2^r *points.*

Therefore, D' is a *two-intersection set* in $\mathrm{PG}(2, 2^m)$.

Embedding D into $\mathrm{PG}(2, 2^m)$

Embedding D into the projective plane $\mathrm{PG}(2, 2^m)$, we have a point set

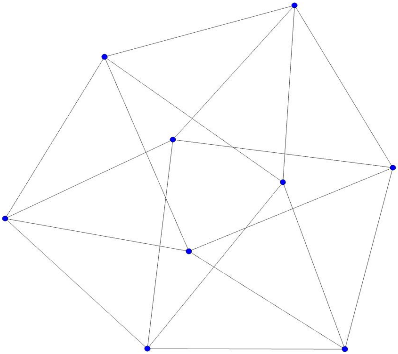
$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\},$$

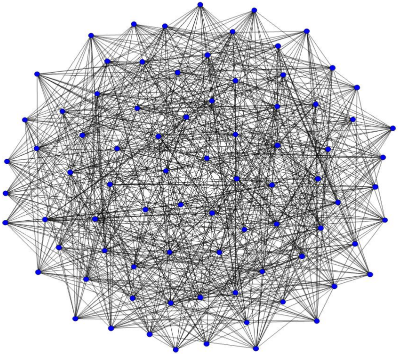
with $|D'| = 1 + (2^m + 1)(2^r - 1)$, such that:

every line in $PG(2, 2^m)$ *intersect* D' *in either* 0 *or* 2^r *points.*

Therefore, D' is a *two-intersection set* in $\mathrm{PG}(2, 2^m)$.

Two-intersection sets in $\mathrm{PG}(2, q)$ are well-appreciated structures, which lead to two-weight codes (coding theory), strongly regular graphs (graph theory), partial difference sets (design theory).





In addition to the two-intersection property, D' satisfies certain maximality.

In addition to the two-intersection property, D' satisfies certain maximality.

(n, d)-arc in $\mathrm{PG}(2, q)$

Let q be a prime power. An (n, d)-*arc* in $\mathrm{PG}(2, q)$ is a set of n points, of which no $d + 1$ points are collinear.

(n, d)-arc in PG$(2, q)$

Let q be a prime power. An *(n, d)-arc* in PG$(2, q)$ is a set of n points, of which no $d + 1$ points are collinear.

Example

Note that each line in PG$(2, q)$ consists of $q + 1$ points.

(1) For $d \geq q + 1$, all the points of PG$(2, q)$ form an (n, d)-arc in PG$(2, q)$.

(n, d)-arc in $PG(2, q)$

Let q be a prime power. An *(n, d)-arc* in $PG(2, q)$ is a set of n points, of which no $d + 1$ points are collinear.

Example

Note that each line in $PG(2, q)$ consists of $q + 1$ points.

(1) For $d \geq q + 1$, all the points of $PG(2, q)$ form an (n, d)-arc in $PG(2, q)$.

(2) For $d = q$, all the points in $PG(2, q)$ minus $q + 1$ points on an arbitrary line form an (n, q)-arc in $PG(2, q)$.

(n, d)-arc in $\mathrm{PG}(2, q)$

Let q be a prime power. An *(n, d)-arc* in $\mathrm{PG}(2, q)$ is a set of n points, of which no $d + 1$ points are collinear.

Example

Note that each line in $\mathrm{PG}(2, q)$ consists of $q + 1$ points.

(1) For $d \geq q + 1$, all the points of $\mathrm{PG}(2, q)$ form an (n, d)-arc in $\mathrm{PG}(2, q)$.

(2) For $d = q$, all the points in $\mathrm{PG}(2, q)$ minus $q + 1$ points on an arbitrary line form an (n, q)-arc in $\mathrm{PG}(2, q)$.

(3) For $d = 1$, an $(n, 1)$-arc in $\mathrm{PG}(2, q)$ must be a set consisting of one point.

(n, d)-arc in $PG(2, q)$

Let q be a prime power. An *(n, d)-arc* in $PG(2, q)$ is a set of n points, of which no $d + 1$ points are collinear.

Example

Note that each line in $PG(2, q)$ consists of $q + 1$ points.

(1) For $d \geq q + 1$, all the points of $PG(2, q)$ form an (n, d)-arc in $PG(2, q)$.

(2) For $d = q$, all the points in $PG(2, q)$ minus $q + 1$ points on an arbitrary line form an (n, q)-arc in $PG(2, q)$.

(3) For $d = 1$, an $(n, 1)$-arc in $PG(2, q)$ must be a set consisting of one point.

An (n, d)-arc in $PG(2, q)$ is *nontrivial* if $1 < d < q$.

$ax^2 + bxy + cy^2$ irreducible over $\mathbb{F}_{2^m}$; H subgroup of $(\mathbb{F}_{2^m}, +)$ with $|H| = 2^r$, $1 \leq r \leq m-1$, we have

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\}$$

satisfying $|D'| = 1 + (2^m + 1)(2^r - 1)$ and every line in $\mathrm{PG}(2, 2^m)$ intersecting D' in either 0 or 2^r points.

$ax^2 + bxy + cy^2$ irreducible over $\mathbb{F}_{2^m}$; H subgroup of $(\mathbb{F}_{2^m}, +)$ with $|H| = 2^r$, $1 \le r \le m-1$, we have

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\}$$

satisfying $|D'| = 1 + (2^m + 1)(2^r - 1)$ and every line in $\mathrm{PG}(2, 2^m)$ intersecting D' in either 0 or 2^r points.

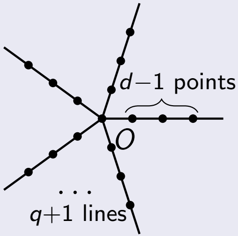
Therefore, D' is a $(1 + (2^m + 1)(2^r - 1), 2^r)$-arc in $\mathrm{PG}(2, 2^m)$.

Fix d and q, for an (n, d)-arc in $\mathrm{PG}(2, q)$, we have a simple upper bound on n:

$$n \leq 1 + (q + 1)(d - 1).$$

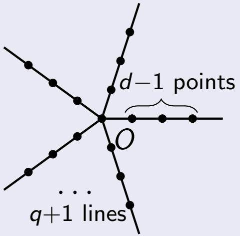
Fix d and q, for an (n, d)-arc in $\mathrm{PG}(2, q)$, we have a simple upper bound on n:

$$n \leq 1 + (q + 1)(d - 1).$$



Fix d and q, for an (n, d)-arc in $\mathrm{PG}(2, q)$, we have a simple upper bound on n:

$$n \leq 1 + (q+1)(d-1).$$



An (n, d)-arc in $\mathrm{PG}(2, q)$ with $n = 1 + (q+1)(d-1)$ is a *maximal arc*.

An (n, d)-arc in $\mathrm{PG}(2, q)$ with $n = 1 + (q + 1)(d - 1)$ is a *maximal arc*.

Denniston's maximal arc (Denniston, 1969)

$ax^2 + bxy + cy^2$ irreducible over $\mathbb{F}_{2^m}$, H subgroup of $(\mathbb{F}_{2^m}, +)$ with $|H| = 2^r$, $1 \le r < m$,

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\}$$

is a $(1 + (2^m + 1)(2^r - 1), 2^r)$ maximal arc in $\mathrm{PG}(2, q)$ with $1 \le r < m$.

Expand

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\}$$

into

$$\overline{D'} = \{z(1, x, y) : ax^2 + bxy + cy^2 \in H, z \in \mathbb{F}_{2^m}^*\} \subset (\mathbb{F}_{2^m}^3, +),$$

where $|\overline{D'}| = (2^{m+r} - 2^m + 2^r)(2^m - 1)$.

Expand

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\}$$

into

$$\overline{D'} = \{z(1, x, y) : ax^2 + bxy + cy^2 \in H, z \in \mathbb{F}_{2^m}^*\} \subset (\mathbb{F}_{2^m}^3, +),$$

where $|\overline{D'}| = (2^{m+r} - 2^m + 2^r)(2^m - 1)$.

For each nonzero element $g \in \mathbb{F}_{2^m}^3$,

$$|(\overline{D'} + g) \cap \overline{D'}| = \begin{cases} 2^m - 2^r + (2^{m+r} - 2^m + 2^r)(2^r - 2) & \text{if } g \in \overline{D'}, \\ (2^{m+r} - 2^m + 2^r)(2^r - 1) & \text{if } g \notin \overline{D'}. \end{cases}$$

Expand

$$D' = \{[1 : x : y] : ax^2 + bxy + cy^2 \in H\}$$

into

$$\overline{D'} = \{z(1, x, y) : ax^2 + bxy + cy^2 \in H, z \in \mathbb{F}_{2^m}^*\} \subset (\mathbb{F}_{2^m}^3, +),$$

where $|\overline{D'}| = (2^{m+r} - 2^m + 2^r)(2^m - 1)$.

For each nonzero element $g \in \mathbb{F}_{2^m}^3$,

$$|(\overline{D'} + g) \cap \overline{D'}| = \begin{cases} 2^m - 2^r + (2^{m+r} - 2^m + 2^r)(2^r - 2) & \text{if } g \in \overline{D'}, \\ (2^{m+r} - 2^m + 2^r)(2^r - 1) & \text{if } g \notin \overline{D'}. \end{cases}$$

$\overline{D'}$ is a $(2^{3m}, (2^{m+r} - 2^m + 2^r)(2^m - 1), 2^m - 2^r + (2^{m+r} - 2^m + 2^r)(2^r - 2), (2^{m+r} - 2^m + 2^r)(2^r - 1))$ *partial difference sets* in $\mathbb{F}_2^{3m}$, which are called Denniston partial difference set (in characteristic 2).

The Denniston maximal arc leads to a Denniston partial difference set of characteristic 2.

The Denniston maximal arc leads to a Denniston partial difference set of characteristic 2.

Remark

Denniston maximal arcs and Denniston partial difference sets are elegant structures in the sense that neat geometric property meets with neat combinatorial property.

The Denniston maximal arc leads to a Denniston partial difference set of characteristic 2.

Remark

Denniston maximal arcs and Denniston partial difference sets are elegant structures in the sense that neat geometric property meets with neat combinatorial property.

From the perspective of partial difference sets (PDSs), the majority of known constructions belong to one of the following two classical families:

- *the Latin square type family*
- *the negative Latin square type family*

The Denniston maximal arc leads to a Denniston partial difference set of characteristic 2.

Remark

Denniston maximal arcs and Denniston partial difference sets are elegant structures in the sense that neat geometric property meets with neat combinatorial property.

From the perspective of partial difference sets (PDSs), the majority of known constructions belong to one of the following two classical families:

- *the Latin square type family*
- *the negative Latin square type family*

The Denniston family stands out as a family of PDSs that is distinct from the two classical families with intrinsic connection to maximal arcs.

The Salient Question

Can we extend the Denniston maximal arcs to $\mathrm{PG}(2, q)$ with q being odd prime power?

The Salient Question

Can we extend the Denniston maximal arcs to $\mathrm{PG}(2, q)$ with q being odd prime power?

If so, then Denniston partial difference sets in odd characteristic follow.

The Salient Question

Can we extend the Denniston maximal arcs to $\mathrm{PG}(2,q)$ with q being odd prime power?

If so, then Denniston partial difference sets in odd characteristic follow.

However, the answer is a resounding No.

Theorem (Ball, Blokhuis, and Mazzocca, 1997)

There exists no maximal arcs in $PG(2,q)$ with odd prime power q.

The Salient Question

Can we extend the Denniston maximal arcs to $\mathrm{PG}(2,q)$ with q being odd prime power?

If so, then Denniston partial difference sets in odd characteristic follow.

However, the answer is a resounding No.

Theorem (Ball, Blokhuis, and Mazzocca, 1997)

There exists no maximal arcs in $PG(2,q)$ with odd prime power q.

The Unasked Question

Can we extend the Denniston PDSs from characteristic 2 to odd characteristic?

The Salient Question

Can we extend the Denniston maximal arcs to $\mathrm{PG}(2,q)$ with q being odd prime power?

If so, then Denniston partial difference sets in odd characteristic follow.

However, the answer is a resounding No.

Theorem (Ball, Blokhuis, and Mazzocca, 1997)

There exists no maximal arcs in $PG(2,q)$ with odd prime power q.

The Unasked Question

Can we extend the Denniston PDSs from characteristic 2 to odd characteristic?

Mimic the construction of Denniston PDSs in $\mathbb{F}_2^{3m}$ to generate Denniston PDSs in $\mathbb{F}_q^{3m}$ for odd prime power q.

The Salient Question

Can we extend the Denniston maximal arcs to $\mathrm{PG}(2, q)$ with q being odd prime power?

If so, then Denniston partial difference sets in odd characteristic follow.

However, the answer is a resounding No.

Theorem (Ball, Blokhuis, and Mazzocca, 1997)

There exists no maximal arcs in $PG(2, q)$ with odd prime power q.

The Unasked Question

Can we extend the Denniston PDSs from characteristic 2 to odd characteristic?

Mimic the construction of Denniston PDSs in $\mathbb{F}_2^{3m}$ to generate Denniston PDSs in $\mathbb{F}_q^{3m}$ for odd prime power q.

The nonexistence of maximal arcs in $\mathrm{PG}(2, q)$ with odd prime power q *seemingly* indicates a negative answer.

Then Came the Huge Surprise

Recently, there have been a series of constructions of Denniston PDSs in odd characteristic.

Then Came the Huge Surprise

Recently, there have been a series of constructions of Denniston PDSs in odd characteristic.

- Denniston $(p^{3m}, (p^{m+r} - p^m + p^r)(p^m - 1), p^m - p^r + (p^{m+r} - p^m + p^r)(p^r - 2), (p^{m+r} - p^m + p^r)(p^r - 1))$-PDS in $\mathbb{F}_p^{3m}$, p odd prime, $m \geq 2$, $r \in \{1, m-1\}$ (Davis, Huczynska, Johnson, and Polhill, 2024).

Then Came the Huge Surprise

Recently, there have been a series of constructions of Denniston PDSs in odd characteristic.

- Denniston $(p^{3m}, (p^{m+r} - p^m + p^r)(p^m - 1), p^m - p^r + (p^{m+r} - p^m + p^r)(p^r - 2), (p^{m+r} - p^m + p^r)(p^r - 1))$-PDS in $\mathbb{F}_p^{3m}$, p odd prime, $m \geq 2$, $r \in \{1, m-1\}$ (Davis, Huczynska, Johnson, and Polhill, 2024).
- Denniston $(q^{3m}, (q^{m+1} - q^m + q)(q^m - 1), q^m - q + (q^{m+1} - q^m + q)(q - 2), (q^{m+1} - q^m + q)(q - 1))$-PDS in $\mathbb{F}_q^{3m}$, q prime power, $m \geq 2$ (De Winter, 2025).

Then Came the Huge Surprise

Recently, there have been a series of constructions of Denniston PDSs in odd characteristic.

- Denniston $(p^{3m}, (p^{m+r} - p^m + p^r)(p^m - 1), p^m - p^r + (p^{m+r} - p^m + p^r)(p^r - 2), (p^{m+r} - p^m + p^r)(p^r - 1))$-PDS in $\mathbb{F}_p^{3m}$, p odd prime, $m \geq 2$, $r \in \{1, m-1\}$ (Davis, Huczynska, Johnson, and Polhill, 2024).
- Denniston $(q^{3m}, (q^{m+1} - q^m + q)(q^m - 1), q^m - q + (q^{m+1} - q^m + q)(q - 2), (q^{m+1} - q^m + q)(q - 1))$-PDS in $\mathbb{F}_q^{3m}$, q prime power, $m \geq 2$ (De Winter, 2025).
- Denniston $(q^{3m}, (q^{m+r} - q^m + q^r)(q^m - 1), q^m - q^r + (q^{m+r} - q^m + q^r)(q^r - 2), (q^{m+r} - q^m + q^r)(q^r - 1))$-PDS in $\mathbb{F}_q^{3m}$, q prime power, $m \geq 2$, $1 \leq r \leq m-1$ (Bao, Xiang, and Zhao, 2025).

The Unasked Question

Can we extend the Denniston PDSs from characteristic 2 to odd characteristic?

The answer is an unexpected Yes.

The Unasked Question

Can we extend the Denniston PDSs from characteristic 2 to odd characteristic?

The answer is an unexpected Yes.

How to reconcile these constructions with the nonexistence result of Ball, Blokhuis, and Mazzocca, that no maximal arcs in $PG(2, q)$ with odd prime power q exist?

Reconciliation (Bao, Xiang, Zhao, 2025)

For a prime power q and $1 \leq r \leq m-1$,

an (n, q^r) Denniston maximal arc in $\mathrm{PG}(2, q^m)$ $\Leftrightarrow$ a Denniston PDS S in $\mathbb{F}_q^{3m}$ which is $\mathbb{F}_{q^m}^*$ invariant: $\{\alpha x \mid x \in S\} = S$ for each $\alpha \in \mathbb{F}_{q^m}^*$

Reconciliation (Bao, Xiang, Zhao, 2025)

For a prime power q and $1 \leq r \leq m-1$,

an (n, q^r) Denniston maximal arc in $\mathrm{PG}(2, q^m)$ $\Leftrightarrow$ a Denniston PDS S in $\mathbb{F}_q^{3m}$ which is $\mathbb{F}_{q^m}^*$ invariant: $\{\alpha x \mid x \in S\} = S$ for each $\alpha \in \mathbb{F}_{q^m}^*$

Recently constructed Denniston PDSs in $\mathbb{F}_q^{3m}$ are $\mathbb{F}_q^*$ invariant but not $\mathbb{F}_{q^m}^*$ invariant

Reconciliation (Bao, Xiang, Zhao, 2025)

For a prime power q and $1 \le r \le m-1$,

an (n, q^r) Denniston maximal arc in $\mathrm{PG}(2, q^m) \Leftrightarrow$ a Denniston PDS S in $\mathbb{F}_q^{3m}$ which is $\mathbb{F}_{q^m}^*$ invariant: $\{\alpha x \mid x \in S\} = S$ for each $\alpha \in \mathbb{F}_{q^m}^*$

Recently constructed Denniston PDSs in $\mathbb{F}_q^{3m}$ are $\mathbb{F}_q^*$ invariant but not $\mathbb{F}_{q^m}^*$ invariant

The nonexistence of Denniston maximal arcs does not imply the nonexistence of Denniston PDSs, but only the nonexistence of Denniston PDSs with an additional $\mathbb{F}_{q^m}^*$ invariant property

Remark

Bao, Xiang, and Zhao (2025) established the existence of Denniston PDSs in elementary abelian groups for all possible parameters. It seems that the existence of Denniston PDSs in odd characteristic, after being open for more than five decades, has finally been resolved.

But, the true history is very complicated ...

But, the true history is very complicated ...

De Winter (2025) observed that, in a largely unnoticed paper, Bierbrauer and Edel (1997) constructed two-weight $[\frac{q^r(q^m-1)(q^m-q^{m-r}+1)}{q-1}, 3m]_q$ code with weights $q^{m+r-1}(q^m-q^{m-r}+1)$ and $q^{2m+r-1}-q^{2m-1}$. The construction gave Denniston PDSs in both even and odd characteristic, sharing the same parameter as Bao, Xiang, and Zhao (2025).

But, the true history is very complicated ...

De Winter (2025) observed that, in a largely unnoticed paper, Bierbrauer and Edel (1997) constructed two-weight $[\frac{q^r(q^m-1)(q^m-q^{m-r}+1)}{q-1}, 3m]_q$ code with weights $q^{m+r-1}(q^m - q^{m-r} + 1)$ and $q^{2m+r-1} - q^{2m-1}$. The construction gave Denniston PDSs in both even and odd characteristic, sharing the same parameter as Bao, Xiang, and Zhao (2025).

It remains unclear whether these two constructions are equivalent or not.

But, the true history is very complicated ...

De Winter (2025) observed that, in a largely unnoticed paper, Bierbrauer and Edel (1997) constructed two-weight $[\frac{q^r(q^m-1)(q^m-q^{m-r}+1)}{q-1}, 3m]_q$ code with weights $q^{m+r-1}(q^m - q^{m-r} + 1)$ and $q^{2m+r-1} - q^{2m-1}$. The construction gave Denniston PDSs in both even and odd characteristic, sharing the same parameter as Bao, Xiang, and Zhao (2025).

It remains unclear whether these two constructions are equivalent or not.

Hence, as a matter of fact, the nonexistence of Denniston maximal arcs in odd characteristic and the existence Denniston PDSs in odd characteristic have both been confirmed in the same year of 1997!

Our goal is to generalize Bao, Xiang, Zhao (2025), in order to broaden the scope of the family of Denniston PDSs.

Our goal is to generalize Bao, Xiang, Zhao (2025), in order to broaden the scope of the family of Denniston PDSs.

But but, the true history is very very complicated ...

Our goal is to generalize Bao, Xiang, Zhao (2025), in order to broaden the scope of the family of Denniston PDSs.

But but, the true history is very very complicated ...

After finishing our paper, we found another largely unnoticed paper by Ott (2016). Ott knew Bierbrauer and Edel (1997) have constructed Denniston PDSs in both even and odd characteristic and further generalized it (!).

Our goal is to generalize Bao, Xiang, Zhao (2025), in order to broaden the scope of the family of Denniston PDSs.

But but, the true history is very very complicated ...

After finishing our paper, we found another largely unnoticed paper by Ott (2016). Ott knew Bierbrauer and Edel (1997) have constructed Denniston PDSs in both even and odd characteristic and further generalized it (!).

Ott had the same idea as we do ($(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +) \to (\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, $\ell \geq 1$) (!!).

Our goal is to generalize Bao, Xiang, Zhao (2025), in order to broaden the scope of the family of Denniston PDSs.

But but, the true history is very very complicated ...

After finishing our paper, we found another largely unnoticed paper by Ott (2016). Ott knew Bierbrauer and Edel (1997) have constructed Denniston PDSs in both even and odd characteristic and further generalized it (!).

Ott had the same idea as we do ($(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +) \to (\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, $\ell \geq 1$) (!!).

Luckily, our construction includes Ott's as a special case.

Theorem (Li, Davis, Huczynska, Johnson, and Polhill, 2025+)

Let $s \geq 1$ and $q = p^s$ be a power of prime p. Let m and ℓ be positive integers. For each $0 \leq r \leq m$, there exists a $(v, k_r, \lambda_r, \mu_r)$ generalized Denniston PDS D_r in the elementary abelian p-group $G = \mathbb{Z}_p^{sm(2\ell+1)} \cong (\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where

$$\begin{aligned}
v =& q^{m(2\ell+1)}, \\
k_r =& \frac{(q^r-1)(q^{m\ell}-1)(q^{m(\ell+1)}-1)}{q^m-1} + q^{m\ell} - 1, \\
\lambda_r =& \frac{(q^r-1)(q^{m(\ell+1)}-1)}{q^m-1}\left(\frac{(q^r-1)(q^{m\ell}-1)}{q^m-1} - 1\right) + q^{m\ell} - 2, \\
\mu_r =& \frac{(q^r-1)(q^{m\ell}-1)}{q^m-1}\left(\frac{(q^r-1)(q^{m(\ell+1)}-1)}{q^m-1} + 1\right).
\end{aligned}$$

(1) Previously: $(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +)$. Our result: $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where $\ell \geq 1$. Our construction includes the previous construction and covers a much wider range of elementary abelian groups.

(1) Previously: $(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +)$. Our result: $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where $\ell \geq 1$. Our construction includes the previous construction and covers a much wider range of elementary abelian groups.

(2) Applying $p = 2$, $s = 1$, $\ell = 1$, and $1 \leq r \leq m - 1$, we recover the original work by Denniston (1969).

(1) Previously: $(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +)$. Our result: $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where $\ell \geq 1$. Our construction includes the previous construction and covers a much wider range of elementary abelian groups.

(2) Applying $p = 2$, $s = 1$, $\ell = 1$, and $1 \leq r \leq m - 1$, we recover the original work by Denniston (1969).

(3) Applying $m = 2$ and $r = 1$, we recover the construction by Momihara (2014).

(1) Previously: $(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +)$. Our result: $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where $\ell \geq 1$. Our construction includes the previous construction and covers a much wider range of elementary abelian groups.

(2) Applying $p = 2$, $s = 1$, $\ell = 1$, and $1 \leq r \leq m - 1$, we recover the original work by Denniston (1969).

(3) Applying $m = 2$ and $r = 1$, we recover the construction by Momihara (2014).

(4) Applying $r = 1$, we recover the construction by Ott (2016).

(1) Previously: $(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +)$. Our result: $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where $\ell \geq 1$. Our construction includes the previous construction and covers a much wider range of elementary abelian groups.

(2) Applying $p = 2$, $s = 1$, $\ell = 1$, and $1 \leq r \leq m - 1$, we recover the original work by Denniston (1969).

(3) Applying $m = 2$ and $r = 1$, we recover the construction by Momihara (2014).

(4) Applying $r = 1$, we recover the construction by Ott (2016).

(5) Applying p being an odd prime, $s = 1$, $\ell = 1$, and $r \in \{1, m - 1\}$, we recover the construction by Davis, Huczynska, Johnson, and Polhill (2024).

(1) Previously: $(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +)$. Our result: $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where $\ell \geq 1$. Our construction includes the previous construction and covers a much wider range of elementary abelian groups.

(2) Applying $p = 2$, $s = 1$, $\ell = 1$, and $1 \leq r \leq m - 1$, we recover the original work by Denniston (1969).

(3) Applying $m = 2$ and $r = 1$, we recover the construction by Momihara (2014).

(4) Applying $r = 1$, we recover the construction by Ott (2016).

(5) Applying p being an odd prime, $s = 1$, $\ell = 1$, and $r \in \{1, m - 1\}$, we recover the construction by Davis, Huczynska, Johnson, and Polhill (2024).

(6) Applying $\ell = 1$ and $r = 1$, we recover the construction by De Winter (2025).

(1) Previously: $(\mathbb{F}_q^m \times \mathbb{F}_q^{2m}, +)$. Our result: $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$, where $\ell \geq 1$. Our construction includes the previous construction and covers a much wider range of elementary abelian groups.

(2) Applying $p = 2$, $s = 1$, $\ell = 1$, and $1 \leq r \leq m - 1$, we recover the original work by Denniston (1969).

(3) Applying $m = 2$ and $r = 1$, we recover the construction by Momihara (2014).

(4) Applying $r = 1$, we recover the construction by Ott (2016).

(5) Applying p being an odd prime, $s = 1$, $\ell = 1$, and $r \in \{1, m - 1\}$, we recover the construction by Davis, Huczynska, Johnson, and Polhill (2024).

(6) Applying $\ell = 1$ and $r = 1$, we recover the construction by De Winter (2025).

(7) Applying $\ell = 1$ and $1 \leq r \leq m - 1$, we recover the construction by Bao, Xiang, and Zhao (2025).

Proof techniques

Our proof relies heavily on the elegant machinery established in Momihara and Xiang (2014), which presented a meticulous manipulation of Gauss sums.

Proof techniques

Our proof relies heavily on the elegant machinery established in Momihara and Xiang (2014), which presented a meticulous manipulation of Gauss sums.

Open Question

Our construction in group $(\mathbb{F}_q^{m\ell} \times \mathbb{F}_q^{m(\ell+1)}, +)$ relies crucially on the fact that $\ell + 1 - \ell = 1$. Would it be possible to ease or lift this restriction?

Main References

- S. Ball, A. Blokhuis, and F. Mazzocca, *Combinatorica*, 1997.
- J. Bao, Q. Xiang, and M. Zhao, *Finite Fields and Their Applications*, 2025.
- J. Bierbrauer and Y. Edel, *Journal of Combinatorial Designs*, 1997.
- J.A. Davis, S. Huczynska, L. Johnson, and J. Polhill, *Finite Fields and Their Applications*, 2024.
- R.H.F. Denniston, *Journal of Combinatorial Theory*, 1969.
- S. De Winter, *Combinatorial Theory*, 2025.
- S. Li, J.A. Davis, S. Huczynska, L. Johnson, and J. Polhill, *Preprint*.
- K. Momihara and Q. Xiang, *Finite Fields and Their Applications*, 2014.
- U. Ott. *Discrete Mathematics*, 2016.