Bent Partitiions

Nurdagül Anbar
(joint work with Tekgül Kalaycı and Wilfried Meidl)

Sabancı University, İstanbul

September 2021, BFA

p: a prime number

$\mathbb{V}_n$: An n-dimensional vector space over $\mathbb{F}_p$ (like $\mathbb{F}_p^n$, $\mathbb{F}_{p^n}$ or $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$)

$\mathbb{Z}_{p^k}$: the cyclic group of order p^k

Main Interest: Bent functions $f : \mathbb{V}_n \to \mathbb{V}_k$ or $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$

Definition: $f : \mathbb{V}_n \to \mathbb{V}_k$ (resp., $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$) is called *bent* if for any character χ of $\mathbb{V}_n \times \mathbb{V}_k$ (resp., $\mathbb{V}_n \times \mathbb{Z}_{p^k}$) that is non-trivial on $\mathbb{V}_k$ (resp., $\mathbb{Z}_{p^k}$) we have

$$|\sum_{x \in \mathbb{V}_n} \chi(x, f(x))| = p^{n/2}.$$

p: a prime number

$\mathbb{V}_n$: An n-dimensional vector space over $\mathbb{F}_p$ (like $\mathbb{F}_p^n$, $\mathbb{F}_{p^n}$ or $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$)

$\mathbb{Z}_{p^k}$: the cyclic group of order p^k

Main Interest: Bent functions $f : \mathbb{V}_n \to \mathbb{V}_k$ or $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$

Definition: $f : \mathbb{V}_n \to \mathbb{V}_k$ (resp., $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$) is called *bent* if for any character χ of $\mathbb{V}_n \times \mathbb{V}_k$ (resp., $\mathbb{V}_n \times \mathbb{Z}_{p^k}$) that is non-trivial on $\mathbb{V}_k$ (resp., $\mathbb{Z}_{p^k}$) we have

$$|\sum_{x \in \mathbb{V}_n} \chi(x, f(x))| = p^{n/2}.$$

p: a prime number

$\mathbb{V}_n$: An n-dimensional vector space over $\mathbb{F}_p$ (like $\mathbb{F}_p^n$, $\mathbb{F}_{p^n}$ or $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$)

$\mathbb{Z}_{p^k}$: the cyclic group of order p^k

Main Interest: Bent functions $f : \mathbb{V}_n \to \mathbb{V}_k$ or $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$

Definition: $f : \mathbb{V}_n \to \mathbb{V}_k$ (resp., $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$) is called *bent* if for any character χ of $\mathbb{V}_n \times \mathbb{V}_k$ (resp., $\mathbb{V}_n \times \mathbb{Z}_{p^k}$) that is non-trivial on $\mathbb{V}_k$ (resp., $\mathbb{Z}_{p^k}$) we have

$$|\sum_{x \in \mathbb{V}_n} \chi(x, f(x))| = p^{n/2}.$$

ϵ_{p^j}: primitive p^j-th root of unity in $\mathbb{C}$, i.e., $\epsilon_{p^j} = e^{2\pi i/p^j}$
For $f : \mathbb{V}_n \to \mathbb{V}_k$ and $(a, b) \in \mathbb{V}_n \times \mathbb{V}_k$, define

$$\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{V}_n} \epsilon_p^{\langle a,x\rangle_n + \langle b,f(x)\rangle_k},$$

where $\langle , \rangle_n$ and $\langle , \rangle_k$ are non-degenerate inner products of $\mathbb{V}_k$ and $\mathbb{V}_n$, respectively.
For $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$ and $(a, b) \in \mathbb{V}_n \times \mathbb{Z}_{p^k}$, define

$$\mathcal{H}_f(a, b) = \sum_{x \in \mathbb{V}_n} \epsilon_p^{\langle a,x\rangle_n} \epsilon_{p^k}^{bf(x)},$$

$f : \mathbb{V}_n \to \mathbb{V}_k$ (resp., $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$) is *bent* if $|\mathcal{W}_f(a, b)| = p^{n/2}$ (resp., $|\mathcal{H}_f(a, b)| = p^{n/2}$) for $a \in \mathbb{V}_n$ and any non-zero $b \in \mathbb{V}_k$ (resp., $b \in \mathbb{Z}_{p^k}$).

Remark: In general, $\mathbb{V}_n = \mathbb{F}_p^n$, $\mathbb{F}_{p^n}$ or $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $n = 2m$, and $\langle x, y\rangle = x \cdot y$, $\langle x, y\rangle = \mathrm{Tr}_n(xy)$ or $\langle (x, y), (z, w)\rangle = \mathrm{Tr}_m(xz + yw)$, respectively.

ϵ_{p^j}: primitive p^j-th root of unity in $\mathbb{C}$, i.e., $\epsilon_{p^j} = e^{2\pi i/p^j}$
For $f : \mathbb{V}_n \to \mathbb{V}_k$ and $(a, b) \in \mathbb{V}_n \times \mathbb{V}_k$, define

$$\mathcal{W}_f(a, b) = \sum_{x\in\mathbb{V}_n} \epsilon_p^{\langle a,x\rangle_n + \langle b,f(x)\rangle_k},$$

where $\langle , \rangle_n$ and $\langle , \rangle_k$ are non-degenerate inner products of $\mathbb{V}_k$ and $\mathbb{V}_n$, respectively.
For $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$ and $(a, b) \in \mathbb{V}_n \times \mathbb{Z}_{p^k}$, define

$$\mathcal{H}_f(a, b) = \sum_{x\in\mathbb{V}_n} \epsilon_p^{\langle a,x\rangle_n} \epsilon_{p^k}^{bf(x)},$$

$f : \mathbb{V}_n \to \mathbb{V}_k$ (resp., $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$) is *bent* if $|\mathcal{W}_f(a, b)| = p^{n/2}$ (resp., $|\mathcal{H}_f(a, b)| = p^{n/2}$) for $a \in \mathbb{V}_n$ and any non-zero $b \in \mathbb{V}_k$ (resp., $b \in \mathbb{Z}_{p^k}$).

Remark: In general, $\mathbb{V}_n = \mathbb{F}_p^n$, $\mathbb{F}_{p^n}$ or $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $n = 2m$, and $\langle x, y\rangle = x \cdot y$, $\langle x, y\rangle = \mathrm{Tr}_n(xy)$ or $\langle (x, y), (z, w)\rangle = \mathrm{Tr}_m(xz + yw)$, respectively.

Spread construction

Definition: A *partial spread* $\mathcal{S}$ of $\mathbb{V}_n$, $n = 2m$, is a set of m-dimensional subspaces of $\mathbb{V}_n$ that intersects trivially. If $|\mathcal{S}| = p^m + 1$, then $\mathcal{S}$ is called a *spread*.

Example: Desarguesian Spread
Let $\mathbb{V}_n = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. For $s \in \mathbb{F}_{p^m}$, set

$$U_s = \{(x, sx) \mid x \in \mathbb{F}_{p^m}\} \quad \text{and} \quad U = \{(0, y) \mid y \in \mathbb{F}_{p^m}\}.$$

Then $\mathcal{S} = \{U, U_s \mid s \in \mathbb{F}_{p^m}\}$ is a spread.

Construction of bent functions with a spread:
Let $\mathcal{S} = \{U_0, U_1, \ldots, U_{p^m}\}$ be a spread of $\mathbb{V}_n$, $n = 2m$, and let B be an abelian group of order p^k for some $1 \le k \le m$. We obtain a bent function from $\mathbb{V}_n$ to B as follows.

1. For every $c \in B$, the non-zero elements of exactly p^{m-k} of U_j, $1 \le j \le p^m$ are mapped to c.
2. The elements of U_0 are mapped to a fixed $c_0 \in B$.

Spread construction

Definition: A *partial spread* $\mathcal{S}$ of $\mathbb{V}_n$, $n = 2m$, is a set of m-dimensional subspaces of $\mathbb{V}_n$ that intersects trivially. If $|\mathcal{S}| = p^m + 1$, then $\mathcal{S}$ is called a *spread*.

Example: Desarguesian Spread
Let $\mathbb{V}_n = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. For $s \in \mathbb{F}_{p^m}$, set

$$U_s = \{(x, sx) \mid x \in \mathbb{F}_{p^m}\} \quad \text{and} \quad U = \{(0, y) \mid y \in \mathbb{F}_{p^m}\}.$$

Then $\mathcal{S} = \{U, U_s \mid s \in \mathbb{F}_{p^m}\}$ is a spread.

Construction of bent functions with a spread:
Let $\mathcal{S} = \{U_0, U_1, \ldots, U_{p^m}\}$ be a spread of $\mathbb{V}_n$, $n = 2m$, and let B be an abelian group of order p^k for some $1 \le k \le m$. We obtain a bent function from $\mathbb{V}_n$ to B as follows.

1. For every $c \in B$, the non-zero elements of exactly p^{m-k} of U_j, $1 \le j \le p^m$ are mapped to c.
2. The elements of U_0 are mapped to a fixed $c_0 \in B$.

Spread construction

Definition: A *partial spread* $\mathcal{S}$ of $\mathbb{V}_n$, $n = 2m$, is a set of m-dimensional subspaces of $\mathbb{V}_n$ that intersects trivially. If $|\mathcal{S}| = p^m + 1$, then $\mathcal{S}$ is called a *spread*.

Example: Desarguesian Spread
Let $\mathbb{V}_n = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. For $s \in \mathbb{F}_{p^m}$, set

$$U_s = \{(x, sx) \mid x \in \mathbb{F}_{p^m}\} \quad \text{and} \quad U = \{(0, y) \mid y \in \mathbb{F}_{p^m}\}.$$

Then $\mathcal{S} = \{U, U_s \mid s \in \mathbb{F}_{p^m}\}$ is a spread.

Construction of bent functions with a spread:
Let $\mathcal{S} = \{U_0, U_1, \ldots, U_{p^m}\}$ be a spread of $\mathbb{V}_n$, $n = 2m$, and let B be an abelian group of order p^k for some $1 \leq k \leq m$. We obtain a bent function from $\mathbb{V}_n$ to B as follows.

1. For every $c \in B$, the non-zero elements of exactly p^{m-k} of U_j, $1 \leq j \leq p^m$ are mapped to c.
2. The elements of U_0 are mapped to a fixed $c_0 \in B$.

Spread-like partition of $\mathbb{V}_n = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$

Let $m, k \in \mathbb{Z}^+$ such that $k|m$ and $\gcd(p^m - 1, p^k + p - 1) = 1$. Set $e = p^m - p^k - p$ and d such that $de \equiv 1 \bmod p^m - 1$.
For $s \in \mathbb{F}_{p^m}$, set

$$U_s = \{(x, sx^e) \mid x \in \mathbb{F}_{p^m}\} \quad \text{and} \quad U = \{(0, x) \mid x \in \mathbb{F}_{p^m}\}.$$

Similarly,

$$V_s = \{(x^d s, x) \mid x \in \mathbb{F}_{p^m}\} \quad \text{and} \quad V = \{(x, 0) \mid x \in \mathbb{F}_{p^m}\}.$$

For γ of $\mathbb{F}_{p^k}$, define

$$\mathcal{A}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} U_s^* \quad \text{and} \quad \mathcal{B}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} V_s^*,$$

where $U_s^* = U_s \setminus \{(0,0)\}$ and $V_s^* = V_s \setminus \{(0,0)\}$. Then

$$\Gamma_1 = \{U, \mathcal{A}(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\} \quad \text{and} \quad \Gamma_2 = \{V, \mathcal{B}(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\},$$

are two partitions of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ into $p^k + 1$ subsets.

Spread-like construction

Theorem (Pirsic-Meidl ($p=2$), A.-Meidl (p odd))

I. *Let f be a function from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_p$, for which every $c \in \mathbb{F}_p$ has the union of exactly p^{k-1} of the sets $\mathcal{A}(\gamma)$ (resp., $\mathcal{B}(\gamma)$) in its preimage set. Further suppose that f is constant c_0 on U (resp., V) for some $c_0 \in \mathbb{F}_p$. Then f is a bent function.*

II. *Let $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{Z}_{p^k}$ such that every $c \in \mathbb{Z}_{p^k}$ has exactly one of the sets $\mathcal{A}(\gamma)$ (resp., $\mathcal{B}(\gamma)$) in its preimage set, and $f(x) = c_0$ for all $x \in U$ (resp., $x \in V$), for some $c_0 \in \mathbb{Z}_{p^k}$. Then f is a bent function.*

Remark: The duals of the bent functions in I. of Γ_1 are in Γ_2 and vice versa.

Spread-like construction

Theorem (Pirsic-Meidl ($p = 2$), A.-Meidl (p odd))

I. *Let f be a function from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_p$, for which every $c \in \mathbb{F}_p$ has the union of exactly p^{k-1} of the sets $\mathcal{A}(\gamma)$ (resp., $\mathcal{B}(\gamma)$) in its preimage set. Further suppose that f is constant c_0 on U (resp., V) for some $c_0 \in \mathbb{F}_p$. Then f is a bent function.*

II. *Let $f : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{Z}_{p^k}$ such that every $c \in \mathbb{Z}_{p^k}$ has exactly one of the sets $\mathcal{A}(\gamma)$ (resp., $\mathcal{B}(\gamma)$) in its preimage set, and $f(x) = c_0$ for all $x \in U$ (resp., $x \in V$), for some $c_0 \in \mathbb{Z}_{p^k}$. Then f is a bent function.*

Remark: The duals of the bent functions in I. of Γ_1 are in Γ_2 and vice versa.

Remark: Spread-like partitions are different from spreads.

Proposition: (Dillon ($p = 2$), A.-Meidl (p odd))
Let $n = 2m$ an even integer, and let $f : \mathbb{V}_n \to \mathbb{F}_p$ be a spread bent function. Then f has (algebraic) degree $\deg(f) = (p-1)m$.

Example: Let $k|m$, $\gcd(p^m - 1, p^k + p - 1) = 1$ and $e = p^k + p - 1$. Let $f(x, y) : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ defined by $f(x, y) = \mathrm{Tr}_m(\alpha x^{-e} y)$, for a non-zero $\alpha \in \mathbb{F}_p^k$. Then f is a bent function obtained from $\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\}$. Moreover, the degree of f is $(p-1)(m-1)$.

Remark: Spread-like partitions are different from spreads.

Proposition: (Dillon ($p = 2$), A.-Meidl (p odd))
Let $n = 2m$ an even integer, and let $f : \mathbb{V}_n \to \mathbb{F}_p$ be a spread bent function. Then f has (algebraic) degree $\deg(f) = (p-1)m$.

Example: Let $k|m$, $\gcd(p^m - 1, p^k + p - 1) = 1$ and $e = p^k + p - 1$. Let $f(x, y) : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ defined by $f(x, y) = \mathrm{Tr}_m(\alpha x^{-e} y)$, for a non-zero $\alpha \in \mathbb{F}_p^k$. Then f is a bent function obtained from $\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\}$. Moreover, the degree of f is $(p-1)(m-1)$.

Remark: Spread-like partitions are different from spreads.

Proposition: (Dillon ($p = 2$), A.-Meidl (p odd))
Let $n = 2m$ an even integer, and let $f : \mathbb{V}_n \to \mathbb{F}_p$ be a spread bent function. Then f has (algebraic) degree $\deg(f) = (p-1)m$.

Example: Let $k|m$, $\gcd(p^m - 1, p^k + p - 1) = 1$ and $e = p^k + p - 1$. Let $f(x, y) : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ defined by $f(x, y) = \mathrm{Tr}_m(\alpha x^{-e} y)$, for a non-zero $\alpha \in \mathbb{F}_p^k$. Then f is a bent function obtained from $\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\}$. Moreover, the degree of f is $(p-1)(m-1)$.

Definition: Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a partition of $\mathbb{V}_n$. Suppose that every function with the following properties is bent:

I Every $c \in \mathbb{F}_p$ has exactly K/p of the sets $A_1, \ldots, A_K$ in its preimage set, and

II $f(x) = c_0$ for all $x \in U$ and some fixed $c_0 \in \mathbb{F}_p$.

Then we call Ω a *bent partition* of $\mathbb{V}_n$.

Example:

1. Spread and spread-like partitions are bent partitions.
2. Similarly constructed $\Gamma_1 = \{U, \mathcal{A}(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\}$ with the following values. (By MAGMA)
   - $m = 4$, $k = 2$ ($\gcd(2^m - 1, 2^k + 1) = 5$) and $e = 1$ or $e = 7$
   - $m = 8$, $k = 2$ ($\gcd(2^m - 1, 2^k + 1) = 5$) and $e = 23$

Question: Are there other classes of bent partitions?

Definition: Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a partition of $\mathbb{V}_n$. Suppose that every function with the following properties is bent:

I Every $c \in \mathbb{F}_p$ has exactly K/p of the sets $A_1, \ldots, A_K$ in its preimage set, and

II $f(x) = c_0$ for all $x \in U$ and some fixed $c_0 \in \mathbb{F}_p$.

Then we call Ω a *bent partition* of $\mathbb{V}_n$.

Example:

1. Spread and spread-like partitions are bent partitions.
2. Similarly constructed $\Gamma_1 = \{U, \mathcal{A}(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\}$ with the following values. (By MAGMA)
   - $m = 4$, $k = 2$ $(\gcd(2^m - 1, 2^k + 1) = 5)$ and $e = 1$ or $e = 7$
   - $m = 8$, $k = 2$ $(\gcd(2^m - 1, 2^k + 1) = 5)$ and $e = 23$

Question: Are there other classes of bent partitions?

Definition: Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a partition of $\mathbb{V}_n$. Suppose that every function with the following properties is bent:

I Every $c \in \mathbb{F}_p$ has exactly K/p of the sets $A_1, \ldots, A_K$ in its preimage set, and

II $f(x) = c_0$ for all $x \in U$ and some fixed $c_0 \in \mathbb{F}_p$.

Then we call Ω a *bent partition* of $\mathbb{V}_n$.

Example:

1. Spread and spread-like partitions are bent partitions.
2. Similarly constructed $\Gamma_1 = \{U, \mathcal{A}(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\}$ with the following values. (By MAGMA)
   - $m = 4$, $k = 2$ ($\gcd(2^m - 1, 2^k + 1) = 5$) and $e = 1$ or $e = 7$
   - $m = 8$, $k = 2$ ($\gcd(2^m - 1, 2^k + 1) = 5$) and $e = 23$

Question: Are there other classes of bent partitions?

Properties of bent partitions: (A.-Meidl, 2021)

Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a bent partition of $\mathbb{V}_n$. Then we have the following.

1. p divides K.
2. n is an even integer.
3. U is an affine subgroup of $\mathbb{V}_n$ of order $p^{n/2}$.
4. $|A_j| = p^{n/2}(p^{n/2} - 1)/K$ for all $j = 1, \ldots, K$. Moreover, $|A_j| \geq 2^{n/2-1}$ if $p = 2$ and $|A_j| \geq (p^{n/2} + 1)/2$ if p is odd.

Bent functions from bent partitions

Let $\Omega = \{U, A_1, \dots, A_K\}$ be a bent partition of $\mathbb{V}_n$. We consider $K = p^k$.

Theorem (A.-Meild, 2021)

I. *Every function* $f : \mathbb{V}_n \to \mathbb{V}_k$ *such that every element* $c \in \mathbb{V}_k$ *has the elements of exactly one of the sets* A_j, $1 \leq j \leq K$, *in its preimage, and* U *is mapped to* $c_0 \in \mathbb{V}_k$, *is bent.*

II. *Every function* $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$ *such that* $f(x) = j$ *if* $x \in A_j$ *and* $f(x) = 0$ *(w.l.o.g.) if* $x \in U$, *is bent.*

Recall:
$\mathbb{V}_n = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $k|m$, $\gcd(p^m-1, p^k+p-1) = 1$ and $e = p^m - p^k - p$.

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\}, \text{ where } \mathcal{A}(\gamma) = \bigcup_{\substack{s\in\mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s)=\gamma}} U_s^*$$

with $U_s = \{(x, sx^e) \mid x \in \mathbb{F}_{p^m}\}$ and $U = \{(0,x) \mid x \in \mathbb{F}_{p^m}\}$.

Let $k_1 < k_2$ be two divisors of m with $\gcd(p^m-1, p^{k_i}+p-1) = 1$ and $e_i = p^{k_i} + p - 1$ for $i = 1, 2$. Denote by $\Gamma_1^{(i)} = \{U, \mathcal{A}_i(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\}$ the bent partition corresponding to k_i and define

$$\mathcal{F}_i := \{f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p \ : \ f \text{ is a bent function obtained from } \Gamma_1^{(i)}\}.$$

Proposition: (A.-Kalaycı-Meidl, 2021)
Let $d = \gcd(m, k_2 - k_1)$. If $p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1)$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Recall:

$\mathbb{V}_n = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $k|m$, $\gcd(p^m-1, p^k+p-1) = 1$ and $e = p^m - p^k - p$.

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\}, \text{ where } \mathcal{A}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} U_s^*$$

with $U_s = \{(x, sx^e) \mid x \in \mathbb{F}_{p^m}\}$ and $U = \{(0,x) \mid x \in \mathbb{F}_{p^m}\}$.

Let $k_1 < k_2$ be two divisors of m with $\gcd(p^m-1, p^{k_i}+p-1) = 1$ and $e_i = p^{k_i} + p - 1$ for $i = 1, 2$. Denote by $\Gamma_1^{(i)} = \{U, \mathcal{A}_i(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\}$ the bent partition corresponding to k_i and define

$$\mathcal{F}_i := \{f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p \ : \ f \text{ is a bent function obtained from } \Gamma_1^{(i)}\}.$$

Proposition: (A.-Kalaycı-Meidl, 2021)

Let $d = \gcd(m, k_2 - k_1)$. If $p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1)$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Recall:
$\mathbb{V}_n = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $k|m$, $\gcd(p^m - 1, p^k + p - 1) = 1$ and $e = p^m - p^k - p$.

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\}, \text{ where } \mathcal{A}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} U_s^*$$

with $U_s = \{(x, sx^e) \mid x \in \mathbb{F}_{p^m}\}$ and $U = \{(0, x) \mid x \in \mathbb{F}_{p^m}\}$.

Let $k_1 < k_2$ be two divisors of m with $\gcd(p^m - 1, p^{k_i} + p - 1) = 1$ and $e_i = p^{k_i} + p - 1$ for $i = 1, 2$. Denote by $\Gamma_1^{(i)} = \{U, \mathcal{A}_i(\gamma) \mid \gamma \in \mathbb{F}_{p^k}\}$ the bent partition corresponding to k_i and define

$$\mathcal{F}_i := \{f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p \ : \ f \text{ is a bent function obtained from } \Gamma_1^{(i)}\}.$$

Proposition: (A.-Kalaycı-Meidl, 2021)
Let $d = \gcd(m, k_2 - k_1)$. If $p^m(p-1) > p^{m/2}(p^d - 2)(p^{k_1} - 1)$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Idea of the proof:

Let $\mathcal{A}_2(\gamma) \in \Gamma_1^{(2)}$ and

$$|S| > p^{k_1-1}, \text{ where } S = \{\mathcal{A}_1(\beta) \in \Gamma_1^{(1)} \ : \ \mathcal{A}_1(\beta) \cap \mathcal{A}_2(\gamma) \neq \emptyset\}.$$

Suppose that $f \in \mathcal{F}_1 \cap \mathcal{F}_2 \neq \emptyset$. If $f\,|_{\mathcal{A}_2(\gamma)} = c$ then $f\,|_{\mathcal{A}_1(\beta)} = c$ for all $\mathcal{A}_1(\beta) \in S$, a contradiction to f being bent function.

For $s \in \mathbb{F}_{p^m}^*$, $U_s^{(i)} = \{(x, sx^{e_i}) \ : \ x \in \mathbb{F}_{p^m}\}$ for $i = 1, 2$. We consider $\mathcal{A}_2(\gamma) \supseteq U_1^{(2)}$.

${U_s^{(1)}}^* \cap {U_1^{(2)}}^* \neq \emptyset \iff (x, sx^{e_1}) = (x, x^{e_2})$ for some $x \in \mathbb{F}_{p^m}^*$, i.e.,

$$s = x^{p^{k_1}(p^{k_2-k_1}-1)}$$

Hence, ${U_s^{(1)}}^* \cap {U_1^{(2)}}^* \neq \emptyset \iff s = y^{p^d-1}$ for some $y \in \mathbb{F}_{p^m}^*$, where $d = \gcd(m, k_2 - k_1)$.

Idea of the proof:

Let $\mathcal{A}_2(\gamma) \in \Gamma_1^{(2)}$ and

$$|S| > p^{k_1 - 1}, \text{ where } S = \{\mathcal{A}_1(\beta) \in \Gamma_1^{(1)} \ : \ \mathcal{A}_1(\beta) \cap \mathcal{A}_2(\gamma) \neq \emptyset\}.$$

Suppose that $f \in \mathcal{F}_1 \cap \mathcal{F}_2 \neq \emptyset$. If $f\mid_{\mathcal{A}_2(\gamma)} = c$ then $f\mid_{\mathcal{A}_1(\beta)} = c$ for all $\mathcal{A}_1(\beta) \in S$, a contradiction to f being bent function.

For $s \in \mathbb{F}_{p^m}^*$, $U_s^{(i)} = \{(x, sx^{e_i}) \ : \ x \in \mathbb{F}_{p^m}\}$ for $i = 1, 2$. We consider $\mathcal{A}_2(\gamma) \supseteq U_1^{(2)}$.

${U_s^{(1)}}^* \cap {U_1^{(2)}}^* \neq \emptyset \iff (x, sx^{e_1}) = (x, x^{e_2})$ for some $x \in \mathbb{F}_{p^m}^*$, i.e.,

$$s = x^{p^{k_1}(p^{k_2 - k_1} - 1)}$$

Hence, ${U_s^{(1)}}^* \cap {U_1^{(2)}}^* \neq \emptyset \iff s = y^{p^d - 1}$ for some $y \in \mathbb{F}_{p^m}^*$, where $d = \gcd(m, k_2 - k_1)$.

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\Longrightarrow |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \ : \ x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e, \ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\Longrightarrow N(\mathcal{X}) \leq p^m + p^{m/2}(p^d-2)(p^{k_1}-1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x, y) \in \mathcal{X} \Longleftrightarrow (x + c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\Longrightarrow$ There are at most $D := (p^m + p^{m/2}(p^d-2)(p^{k_1}-1))/p^{k_1}(p^d-1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\Longrightarrow |S| \geq \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1) \Longrightarrow |S| > p^{k_1-1}$.

$\square$

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\Longrightarrow |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \ : \ x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e,\ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\Longrightarrow N(\mathcal{X}) \le p^m + p^{m/2}(p^d-2)(p^{k_1}-1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x, y) \in \mathcal{X} \Longleftrightarrow (x + c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\Longrightarrow$ There are at most $D := (p^m + p^{m/2}(p^d-2)(p^{k_1}-1))/p^{k_1}(p^d-1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\Longrightarrow |S| \ge \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1) \Longrightarrow |S| > p^{k_1-1}$.

$\square$

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\implies |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \,:\, x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e,\ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\implies N(\mathcal{X}) \le p^m + p^{m/2}(p^d-2)(p^{k_1}-1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x,y) \in \mathcal{X} \iff (x+c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\implies$ There are at most $D := (p^m + p^{m/2}(p^d-2)(p^{k_1}-1))/p^{k_1}(p^d-1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\implies |S| \ge \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1) \implies |S| > p^{k_1-1}$.

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\Longrightarrow |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \ : \ x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e, \ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\Longrightarrow N(\mathcal{X}) \leq p^m + p^{m/2}(p^d - 2)(p^{k_1} - 1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x, y) \in \mathcal{X} \Longleftrightarrow (x + c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\Longrightarrow$ There are at most $D := (p^m + p^{m/2}(p^d - 2)(p^{k_1} - 1))/p^{k_1}(p^d - 1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\Longrightarrow |S| \geq \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d - 2)(p^{k_1} - 1) \Longrightarrow |S| > p^{k_1-1}$.

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\Longrightarrow |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \ : \ x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e, \ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\Longrightarrow N(\mathcal{X}) \leq p^m + p^{m/2}(p^d-2)(p^{k_1}-1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x, y) \in \mathcal{X} \Longleftrightarrow (x + c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\Longrightarrow$ There are at most $D := (p^m + p^{m/2}(p^d-2)(p^{k_1}-1))/p^{k_1}(p^d-1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\Longrightarrow |S| \geq \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1) \Longrightarrow |S| > p^{k_1-1}$.

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\Longrightarrow |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \ : \ x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e, \ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\Longrightarrow N(\mathcal{X}) \leq p^m + p^{m/2}(p^d - 2)(p^{k_1} - 1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x, y) \in \mathcal{X} \Longleftrightarrow (x + c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\Longrightarrow$ There are at most $D := (p^m + p^{m/2}(p^d - 2)(p^{k_1} - 1))/p^{k_1}(p^d - 1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\Longrightarrow |S| \geq \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d - 2)(p^{k_1} - 1) \Longrightarrow |S| > p^{k_1-1}$.

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\Longrightarrow |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \ : \ x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e, \ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\Longrightarrow N(\mathcal{X}) \leq p^m + p^{m/2}(p^d-2)(p^{k_1}-1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x, y) \in \mathcal{X} \Longleftrightarrow (x + c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\Longrightarrow$ There are at most $D := (p^m + p^{m/2}(p^d-2)(p^{k_1}-1))/p^{k_1}(p^d-1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\Longrightarrow |S| \geq \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1) \Longrightarrow |S| > p^{k_1-1}$.

For $s_i = y_i^{p^d-1}$, $\mathrm{Tr}_{k_1}^m(s_1) = \mathrm{Tr}_{k_1}^m(s_2)$ if and only if $y_2^{p^d-1} = x^{p^{k_1}} - x + y_1^{p^d-1}$ for some $x \in \mathbb{F}_{p^m}$.

$\Longrightarrow |S|$ is the number of cosets $y^{p^d-1} + \mathcal{Z}$, where $\mathcal{Z} = \{x^{p^{k_1}} - x \,:\, x \in \mathbb{F}_{p^m}\}$.

Consider the Kummer curve $\mathcal{X} : Y^{p^d-1} = X^{p^{k_1}} - X + e,\ e \in \mathbb{F}_{p^m}$.

Hasse-Weil bound $\Longrightarrow N(\mathcal{X}) \le p^m + p^{m/2}(p^d-2)(p^{k_1}-1)$, where $N(\mathcal{X})$ is the number of affine rational points.

$(x, y) \in \mathcal{X} \Longleftrightarrow (x + c, \zeta y) \in \mathcal{X}$ for $c \in \mathbb{F}_{p^{k_1}}$ and $\zeta^{p^d-1} = 1$.

$\Longrightarrow$ There are at most $D := (p^m + p^{m/2}(p^d-2)(p^{k_1}-1))/p^{k_1}(p^d-1)$ elements y^{p^d-1} lying in $e + \mathcal{Z}$.

$\Longrightarrow |S| \ge \frac{p^m-1}{(p^d-1)D}$.

$p^m(p-1) > p^{m/2}(p^d-2)(p^{k_1}-1) \Longrightarrow |S| > p^{k_1-1}$.

$\square$

Corollary: If $k_2 < m$ or $k_2 = m$ and $k_1 \leq m/4$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Open Cases: $(k_1, k_2) = (m/2, m)$ and $(k_1, k_2) = (m/3, m)$

Lemma: If $(k_1, k_2) = (m/2, m)$ then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Proof. Recall: $U_s^{(1)^*} \cap U_1^{(2)^*} \neq \emptyset \iff s = y^{p^{m/2}-1}$ for some $y \in \mathbb{F}_{p^m}^*$.

$\implies |S| = |\{\beta = \mathrm{Tr}_{m/2}^m(s) \,:\, s = y^{p^{m/2}-1} \text{ for some } y \in \mathbb{F}_{p^m}^*\}|$

Note that $\mathrm{Tr}_{m/2}^m(s) = s + s^{-1}$, i.e.,

$$\mathrm{Tr}_{m/2}^m(s_i) = \mathrm{Tr}_{m/2}^m(s) \iff s_i + \frac{1}{s_i} = s + \frac{1}{s}.$$

$\implies s_i$ is a root of $T^2 - (1/s + s)T + 1$.

$\implies$ There are at most two elements having the same relative trace.

$\implies |S| \geq 1/2|\{y^{p^{m/2}-1} \,:\, y \in \mathbb{F}_{p^m}^*\}| = (p^{m/2}+1)/2 > p^{m/2-1}$.

$\square$

Theorem (A.-Kalayci-Meidl, 2021)

If $k_1 \neq k_2$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Corollary: If $k_2 < m$ or $k_2 = m$ and $k_1 \leq m/4$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Open Cases: $(k_1, k_2) = (m/2, m)$ and $(k_1, k_2) = (m/3, m)$

Lemma: If $(k_1, k_2) = (m/2, m)$ then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Proof. Recall: $U_s^{(1)^*} \cap U_1^{(2)^*} \neq \emptyset \iff s = y^{p^{m/2}-1}$ for some $y \in \mathbb{F}_{p^m}^*$.

$\implies |S| = |\{\beta = \mathrm{Tr}_{m/2}^m(s) \,:\, s = y^{p^{m/2}-1}$ for some $y \in \mathbb{F}_{p^m}^*\}|$

Note that $\mathrm{Tr}_{m/2}^m(s) = s + s^{-1}$, i.e.,

$$\mathrm{Tr}_{m/2}^m(s_i) = \mathrm{Tr}_{m/2}^m(s) \iff s_i + \frac{1}{s_i} = s + \frac{1}{s}.$$

$\implies s_i$ is a root of $T^2 - (1/s + s)T + 1$.

$\implies$ There are at most two elements having the same relative trace.

$\implies |S| \geq 1/2|\{y^{p^{m/2}-1} \,:\, y \in \mathbb{F}_{p^m}^*\}| = (p^{m/2}+1)/2 > p^{m/2-1}$. $\square$

Theorem (A.-Kalayci-Meidl, 2021)

If $k_1 \neq k_2$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Corollary: If $k_2 < m$ or $k_2 = m$ and $k_1 \le m/4$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Open Cases: $(k_1, k_2) = (m/2, m)$ and $(k_1, k_2) = (m/3, m)$

Lemma: If $(k_1, k_2) = (m/2, m)$ then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Proof. Recall: $U_s^{(1)^*} \cap U_1^{(2)^*} \neq \emptyset \iff s = y^{p^{m/2}-1}$ for some $y \in \mathbb{F}_{p^m}^*$.

$\Longrightarrow |S| = |\{\beta = \mathrm{Tr}_{m/2}^m(s) \,:\, s = y^{p^{m/2}-1}$ for some $y \in \mathbb{F}_{p^m}^*\}|$

Note that $\mathrm{Tr}_{m/2}^m(s) = s + s^{-1}$, i.e.,

$$\mathrm{Tr}_{m/2}^m(s_i) = \mathrm{Tr}_{m/2}^m(s) \iff s_i + \frac{1}{s_i} = s + \frac{1}{s}.$$

$\Longrightarrow s_i$ is a root of $T^2 - (1/s + s)T + 1$.

$\Longrightarrow$ There are at most two elements having the same relative trace.

$\Longrightarrow |S| \ge 1/2|\{y^{p^{m/2}-1} \,:\, y \in \mathbb{F}_{p^m}^*\}| = (p^{m/2} + 1)/2 > p^{m/2-1}$.

$\square$

Theorem (A.-Kalayci-Meidl, 2021)

If $k_1 \neq k_2$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Corollary: If $k_2 < m$ or $k_2 = m$ and $k_1 \leq m/4$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Open Cases: $(k_1, k_2) = (m/2, m)$ and $(k_1, k_2) = (m/3, m)$

Lemma: If $(k_1, k_2) = (m/2, m)$ then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

Proof. Recall: $U_s^{(1)^*} \cap U_1^{(2)^*} \neq \emptyset \iff s = y^{p^{m/2}-1}$ for some $y \in \mathbb{F}_{p^m}^*$.

$\implies |S| = |\{\beta = \mathrm{Tr}^m_{m/2}(s) \ : \ s = y^{p^{m/2}-1}$ for some $y \in \mathbb{F}_{p^m}^*\}|$

Note that $\mathrm{Tr}^m_{m/2}(s) = s + s^{-1}$, i.e.,

$$\mathrm{Tr}^m_{m/2}(s_i) = \mathrm{Tr}^m_{m/2}(s) \iff s_i + \frac{1}{s_i} = s + \frac{1}{s}.$$

$\implies s_i$ is a root of $T^2 - (1/s + s)T + 1$.

$\implies$ There are at most two elements having the same relative trace.

$\implies |S| \geq 1/2|\{y^{p^{m/2}-1} \ : \ y \in \mathbb{F}_{p^m}^*\}| = (p^{m/2} + 1)/2 > p^{m/2-1}$.

$\square$

Theorem (A.-Kalayci-Meidl, 2021)

If $k_1 \neq k_2$, then $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$.

We wish you healthy days!