# Multispreads and additive intriguing sets in Hamming graphs

Denis Krotov
(j.w. with Ivan Mogilnykh)

Sobolev Institute of Mathematics, Novosibirsk

Graphs and Groups, Complexity and Convexity (G2C2)
Shijiazhuang, China, August 11–25, 2024

# Introduction

spreads $\subset$ $\mu$-fold spreads $\subset$ **multispreads** $\subset$ $\mu$-fold space partitions

- ($\mu$-fold) spreads, or $t$-spreads — (multifold) partitions of the vector space into $t$-subspaces;
- **multispreads** — $\mu$-fold partitions of the vector space $\mathbb{F}_q^m$ into $t$-multisubspaces (subspaces of different dimensions $r \le t$, counted with multiplisity $q^{t-r}$);
- (multifold) space partitions — (multifold) partitions of the vector space into subspaces of (possibly) different dimensions;
- Motivation: correspondence between multispreads, additive *intriguing sets* (completely regular codes with covering radius 1) in Hamming graphs, and additive one-weight codes.

# Introduction

spreads ⊂ $\mu$-fold spreads ⊂ **multispreads** ⊂ $\mu$-fold space partitions

- ($\mu$-fold) spreads, or $t$-spreads — (multifold) partitions of the vector space into $t$-subspaces;
- **multispreads** — $\mu$-fold partitions of the vector space $\mathbb{F}_q^m$ into $t$-multisubspaces (subspaces of different dimensions $r \le t$, counted with multiplisity $q^{t-r}$);
- (multifold) space partitions — (multifold) partitions of the vector space into subspaces of (possibly) different dimensions;
- Motivation: correspondence between multispreads, additive *intriguing sets* (completely regular codes with covering radius 1) in Hamming graphs, and additive one-weight codes.

# Introduction

spreads $\subset$ $\mu$-fold spreads $\subset$ **multispreads** $\subset$ $\mu$-fold space partitions

- ($\mu$-fold) spreads, or $t$-spreads — (multifold) partitions of the vector space into $t$-subspaces;
- **multispreads** — $\mu$-fold partitions of the vector space $\mathbb{F}_q^m$ into $t$-multisubspaces (subspaces of different dimensions $r \leq t$, counted with multiplisity $q^{t-r}$);
- (multifold) space partitions — (multifold) partitions of the vector space into subspaces of (possibly) different dimensions;
- Motivation: correspondence between multispreads, additive *intriguing sets* (completely regular codes with covering radius 1) in Hamming graphs, and additive one-weight codes.

# Introduction

spreads $\subset$ $\mu$-fold spreads $\subset$ **multispreads** $\subset$ $\mu$-fold space partitions

- ($\mu$-fold) spreads, or $t$-spreads — (multifold) partitions of the vector space into $t$-subspaces;
- **multispreads** — $\mu$-fold partitions of the vector space $\mathbb{F}_q^m$ into $t$-multisubspaces (subspaces of different dimensions $r \le t$, counted with multiplisity $q^{t-r}$);
- (multifold) space partitions — (multifold) partitions of the vector space into subspaces of (possibly) different dimensions;
- Motivation: correspondence between multispreads, additive *intriguing sets* (completely regular codes with covering radius 1) in Hamming graphs, and additive one-weight codes.

# Introduction

spreads $\subset$ $\mu$-fold spreads $\subset$ **multispreads** $\subset$ $\mu$-fold space partitions

- ($\mu$-fold) spreads, or $t$-spreads — (multifold) partitions of the vector space into $t$-subspaces;
- **multispreads** — $\mu$-fold partitions of the vector space $\mathbb{F}_q^m$ into $t$-multisubspaces (subspaces of different dimensions $r \le t$, counted with multiplisity $q^{t-r}$);
- (multifold) space partitions — (multifold) partitions of the vector space into subspaces of (possibly) different dimensions;
- Motivation: correspondence between multispreads, additive *intriguing sets* (completely regular codes with covering radius 1) in Hamming graphs, and additive one-weight codes.

# OUTLINE

- definitions;
- connection: multispreads, intriguing sets (CR-1), one-weight codes;
- multispreads: necessary condition;
- multispreads: simple special cases;
- multispreads: constructions;
- multispreads: characterized cases:
  corresponding to additive intriguing sets in
  $H(n,p^2)$, $H(n,2^3)$, $H(n,2^4)$, $H(n,3^3)$;
- duality

# Definition: intriguing sets

- A set of vertices of a regular (Hamming) graph is called an intriguing set (completely regular code of covering radius $\mathbf{1}$, CR-$\mathbf{1}$) with quotient matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

  if every codeword is adjacent to $a$ codewords and $b$ non-codewords and every non-codeword is adjacent to $c$ codewords and $d$ non-codewords.
- equivalent notions: equitable 2-partitions, perfect 2-colorings, 2-partition designs, . . .

# Definition: intriguing sets

- A set of vertices of a regular (Hamming) graph is called an intriguing set (completely regular code of covering radius $1$, CR-$1$) with quotient matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

  if every codeword is adjacent to $a$ codewords and $b$ non-codewords and every non-codeword is adjacent to $c$ codewords and $d$ non-codewords.
- equivalent notions: equitable 2-partitions, perfect 2-colorings, 2-partition designs, ...

# Notations from coding theory

- $\mathbb{F}_q^n$ — the space of $n$-tuples (words) of elements of $\mathbb{F}_q = \mathrm{GF}(q)$.
- The weight of a word is the number of nonzero elements in it; the Hamming distance between two words is the number of positions in which they differ.
- A subspace (linear code) or an additive subgroup (additive code) of $\mathbb{F}_q^n$ is said to be a one-weight code if all non-zero codewords have the same weight.
- If $q = p^t$, $p$ prime, then additive codes are just $\mathbb{F}_p$-linear codes in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is considered as $t$-dimensional vector space over $\mathbb{F}_p$.
- Choosing any $\mathbb{F}_p$-basis in $\mathbb{F}_q$, we can represent $\mathbb{F}_q^n$ as $(\mathbb{F}_p^t)^n$, the set of words of length $n$ over $\mathbb{F}_p^t$,
  or the set of words of length $nt$ over $\mathbb{F}_p$, where each word is divided into $n$ blocks of length $t$.
- Important: the Hamming metric is still $q$-ary: when counting the weight or the distance, we consider an element of $\mathbb{F}_p^t$ as one symbol. Example ($p = 2$, $q = 2^3 = 8$): 000 <u>001</u> <u>110</u> 000 <u>111</u>

# Notations from coding theory

- $\mathbb{F}_q^n$ — the space of $n$-tuples (words) of elements of $\mathbb{F}_q = \mathrm{GF}(q)$.
- The weight of a word is the number of nonzero elements in it; the Hamming distance between two words is the number of positions in which they differ.
- A subspace (linear code) or an additive subgroup (additive code) of $\mathbb{F}_q^n$ is said to be a one-weight code if all non-zero codewords have the same weight.
- If $q = p^t$, $p$ prime, then additive codes are just $\mathbb{F}_p$-linear codes in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is considered as $t$-dimensional vector space over $\mathbb{F}_p$.
- Choosing any $\mathbb{F}_p$-basis in $\mathbb{F}_q$, we can represent $\mathbb{F}_q^n$ as $(\mathbb{F}_p^t)^n$, the set of words of length $n$ over $\mathbb{F}_p^t$,
  or the set of words of length $nt$ over $\mathbb{F}_p$, where each word is divided into $n$ blocks of length $t$.
- Important: the Hamming metric is still $q$-ary: when counting the weight or the distance, we consider an element of $\mathbb{F}_p^t$ as one symbol. Example ($p = 2$, $q = 2^3 = 8$): 000 <u>001</u> <u>110</u> 000 <u>111</u>

# Notations from coding theory

- $\mathbb{F}_q^n$ — the space of $n$-tuples (words) of elements of $\mathbb{F}_q = \mathrm{GF}(q)$.
- The weight of a word is the number of nonzero elements in it; the Hamming distance between two words is the number of positions in which they differ.
- A subspace (linear code) or an additive subgroup (additive code) of $\mathbb{F}_q^n$ is said to be a one-weight code if all non-zero codewords have the same weight.
- If $q = p^t$, $p$ prime, then additive codes are just $\mathbb{F}_p$-linear codes in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is considered as $t$-dimensional vector space over $\mathbb{F}_p$.
- Choosing any $\mathbb{F}_p$-basis in $\mathbb{F}_q$, we can represent $\mathbb{F}_q^n$ as $(\mathbb{F}_p^t)^n$, the set of words of length $n$ over $\mathbb{F}_p^t$, or the set of words of length $nt$ over $\mathbb{F}_p$, where each word is divided into $n$ blocks of length $t$.
- Important: the Hamming metric is still $q$-ary: when counting the weight or the distance, we consider an element of $\mathbb{F}_p^t$ as one symbol. Example ($p = 2$, $q = 2^3 = 8$): 000 <u>001</u> <u>110</u> 000 <u>111</u>

# Notations from coding theory

- $\mathbb{F}_q^n$ — the space of $n$-tuples (words) of elements of $\mathbb{F}_q = \mathrm{GF}(q)$.
- The weight of a word is the number of nonzero elements in it; the Hamming distance between two words is the number of positions in which they differ.
- A subspace (linear code) or an additive subgroup (additive code) of $\mathbb{F}_q^n$ is said to be a one-weight code if all non-zero codewords have the same weight.
- If $q = p^t$, $p$ prime, then additive codes are just $\mathbb{F}_p$-linear codes in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is considered as $t$-dimensional vector space over $\mathbb{F}_p$.
- Choosing any $\mathbb{F}_p$-basis in $\mathbb{F}_q$, we can represent $\mathbb{F}_q^n$ as $(\mathbb{F}_p^t)^n$, the set of words of length $n$ over $\mathbb{F}_p^t$, or the set of words of length $nt$ over $\mathbb{F}_p$, where each word is divided into $n$ blocks of length $t$.
- Important: the Hamming metric is still $q$-ary: when counting the weight or the distance, we consider an element of $\mathbb{F}_p^t$ as one symbol. Example ($p = 2$, $q = 2^3 = 8$): 000 001 110 000 111

# Notations from coding theory

- $\mathbb{F}_q^n$ — the space of $n$-tuples (words) of elements of $\mathbb{F}_q = \mathrm{GF}(q)$.
- The weight of a word is the number of nonzero elements in it; the Hamming distance between two words is the number of positions in which they differ.
- A subspace (linear code) or an additive subgroup (additive code) of $\mathbb{F}_q^n$ is said to be a one-weight code if all non-zero codewords have the same weight.
- If $q = p^t$, $p$ prime, then additive codes are just $\mathbb{F}_p$-linear codes in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is considered as $t$-dimensional vector space over $\mathbb{F}_p$.
- Choosing any $\mathbb{F}_p$-basis in $\mathbb{F}_q$, we can represent $\mathbb{F}_q^n$ as $(\mathbb{F}_p^t)^n$, the set of words of length $n$ over $\mathbb{F}_p^t$,
  or the set of words of length $nt$ over $\mathbb{F}_p$, where each word is divided into $n$ blocks of length $t$.
- Important: the Hamming metric is still $q$-ary: when counting the weight or the distance, we consider an element of $\mathbb{F}_p^t$ as one symbol. Example ($p = 2$, $q = 2^3 = 8$): 000 <u>001</u> <u>110</u> 000 <u>111</u>

# Notations from coding theory

- $\mathbb{F}_q^n$ — the space of $n$-tuples (words) of elements of $\mathbb{F}_q = \mathrm{GF}(q)$.
- The weight of a word is the number of nonzero elements in it; the Hamming distance between two words is the number of positions in which they differ.
- A subspace (linear code) or an additive subgroup (additive code) of $\mathbb{F}_q^n$ is said to be a one-weight code if all non-zero codewords have the same weight.
- If $q = p^t$, $p$ prime, then additive codes are just $\mathbb{F}_p$-linear codes in $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is considered as $t$-dimensional vector space over $\mathbb{F}_p$.
- Choosing any $\mathbb{F}_p$-basis in $\mathbb{F}_q$, we can represent $\mathbb{F}_q^n$ as $(\mathbb{F}_p^t)^n$, the set of words of length $n$ over $\mathbb{F}_p^t$, or the set of words of length $nt$ over $\mathbb{F}_p$, where each word is divided into $n$ blocks of length $t$.
- Important: the Hamming metric is still $q$-ary: when counting the weight or the distance, we consider an element of $\mathbb{F}_p^t$ as one symbol. Example ($p = 2$, $q = 2^3 = 8$): 000 <u>001</u> <u>110</u> 000 <u>111</u>

# check matrix

- Every subspace of $\mathbb{F}_p^{nt}$ can be represented by a generator matrix, whose rows form basis.
- Every subspace $C$ of the space $nt$-words over $\mathbb{F}_p$ can be represented as the null-space, $\mathrm{null}(M)$, of an $(nt - \dim C) \times nt$ matrix $M$, called a check matrix of the $\mathbb{F}_p$-linear code $C$.
- Since we consider the positions of $nt$-words as arranged into blocks, the columns of a check matrix are also naturally grouped into $n$ groups.

$$H = \begin{pmatrix} 00 & 00 & 01 & 01 & 10 & 10 & 01 & 01 & 10 & 01 & 01 & 10 & 00 \\ 01 & 01 & 10 & 10 & 00 & 00 & 01 & 10 & 01 & 11 & 11 & 10 & 00 \\ 10 & 10 & 00 & 00 & 01 & 01 & 10 & 01 & 01 & 10 & 10 & 10 & 00 \end{pmatrix}$$

# check matrix

- Every subspace of $\mathbb{F}_p^{nt}$ can be represented by a generator matrix, whose rows form basis.
- Every subspace $C$ of the space $nt$-words over $\mathbb{F}_p$ can be represented as the null-space, $\mathrm{null}(M)$, of an $(nt - \dim C) \times nt$ matrix $M$, called a check matrix of the $\mathbb{F}_p$-linear code $C$.
- Since we consider the positions of $nt$-words as arranged into blocks, the columns of a check matrix are also naturally grouped into $n$ groups.

$$H = \begin{pmatrix} 00 & 00 & 01 & 01 & 10 & 10 & 01 & 01 & 10 & 01 & 01 & 10 & 00 \\ 01 & 01 & 10 & 10 & 00 & 00 & 01 & 10 & 01 & 11 & 11 & 10 & 00 \\ 10 & 10 & 00 & 00 & 01 & 01 & 10 & 01 & 01 & 10 & 10 & 10 & 00 \end{pmatrix}$$

# check matrix

- Every subspace of $\mathbb{F}_p^{nt}$ can be represented by a generator matrix, whose rows form basis.
- Every subspace $C$ of the space $nt$-words over $\mathbb{F}_p$ can be represented as the null-space, $\mathrm{null}(M)$, of an $(nt - \dim C) \times nt$ matrix $M$, called a check matrix of the $\mathbb{F}_p$-linear code $C$.
- Since we consider the positions of $nt$-words as arranged into blocks, the columns of a check matrix are also naturally grouped into $n$ groups.

$$H = \begin{pmatrix} 0\,0 & 0\,0 & 0\,1 & 0\,1 & 1\,0 & 1\,0 & 0\,1 & 0\,1 & 1\,0 & 0\,1 & 0\,1 & 1\,0 & 0\,0 \\ 0\,1 & 0\,1 & 1\,0 & 1\,0 & 0\,0 & 0\,0 & 0\,1 & 1\,0 & 0\,1 & 1\,1 & 1\,1 & 1\,0 & 0\,0 \\ 1\,0 & 1\,0 & 0\,0 & 0\,0 & 0\,1 & 0\,1 & 1\,0 & 0\,1 & 0\,1 & 1\,0 & 1\,0 & 1\,0 & 0\,0 \end{pmatrix}$$

# Connection of one-weight codes and intriguing sets

**Lemma**

*Assume that an* $m \times nt$ *matrix* $M$ *over* $\mathbb{F}_p$ *is a generator matrix if the code* $C$ *and a check matrix of the code* $C^{\perp}$. $C$ *is a one-weight code with weight* $w$ *if and only if* $C^{\perp}$ *is an intriguing set with quotient matrix* $\begin{pmatrix} \cdot & \cdot \\ \mu & \cdot \end{pmatrix}$, *where* $w \cdot p^{t-1} = \mu \cdot p^{m-1}$.

# Treating a group $T$ of columns in a check matrix

- For a given finite multiset $T$ of vectors, by $\langle\langle T \rangle\rangle$ we denote the multiset
$$\langle\langle T \rangle\rangle := \left\{ \sum_{v \in T} a_v v : \ a_v \in \mathbb{F}_p \right\}$$
of all $q^{|T|}$ linear combinations of elements from $T$.
- Every such $\langle\langle T \rangle\rangle$ will be called a multisubspace, or $t$-multisubspace, (of the vector space) with a "basis" $T$.
- For a multisubspace $S$, we denote $S^* := S - \{0\}$.

# Treating a group $T$ of columns in a check matrix

- For a given finite multiset $T$ of vectors, by $\langle\langle T\rangle\rangle$ we denote the multiset
$$\langle\langle T\rangle\rangle := \left\{ \sum_{v\in T} a_v v : \; a_v \in \mathbb{F}_p \right\}$$
of all $q^{|T|}$ linear combinations of elements from $T$.
- Every such $\langle\langle T\rangle\rangle$ will be called a multisubspace, or $t$-multisubspace, (of the vector space) with a “basis” $T$.
- For a multisubspace $S$, we denote $S^* := S - \{0\}$.

# Treating a group $T$ of columns in a check matrix

- For a given finite multiset $T$ of vectors, by $\langle\!\langle T \rangle\!\rangle$ we denote the multiset
$$\langle\!\langle T \rangle\!\rangle := \Big\{ \sum_{v \in T} a_v v : \ a_v \in \mathbb{F}_p \Big\}$$
of all $q^{|T|}$ linear combinations of elements from $T$.
- Every such $\langle\!\langle T \rangle\!\rangle$ will be called a multisubspace, or $t$-multisubspace, (of the vector space) with a "basis" $T$.
- For a multisubspace $S$, we denote $S^* := S - \{0\}$.

# Multispreads

- We will call a collection $(S_1, \ldots, S_n)$ of $t$-multisubspaces of $\mathbb{F}_p^m$ a $(\lambda, \mu)$-multispread, or multispread, if there hold

$$S_1 \uplus \ldots \uplus S_n = (n+\lambda)\times\{\bar{0}\} \uplus \mu\times\mathbb{F}_p^{m*}.$$

- or, equivalently,

$$S_1^* \uplus \ldots \uplus S_n^* = \lambda\times\{\bar{0}\} \uplus \mu\times\mathbb{F}_p^{m*},$$

where ${S_i}^* = S_i - \{\bar{0}\}$.

- $(0,\mu)$-multispreads are known as $\mu$-fold spreads (in this case, $S_i$ are ordinary $t$-dimensional subspaces, without multiplicity larger than 1);
in particular, $(0,1)$-multispreads are spreads;

# Multispreads

- We will call a collection $(S_1, \ldots, S_n)$ of $t$-multisubspaces of $\mathbb{F}_p^m$ a $(\lambda, \mu)$-multispread, or multispread, if there hold

$$S_1 \uplus \ldots \uplus S_n = (n + \lambda)\times\{\bar{0}\} \uplus \mu\times\mathbb{F}_p^{m*}.$$

- or, equivalently,

$$S_1^* \uplus \ldots \uplus S_n^* = \lambda\times\{\bar{0}\} \uplus \mu\times\mathbb{F}_p^{m*},$$

where ${S_i}^* = S_i - \{\bar{0}\}$.

- $(0, \mu)$-multispreads are known as $\mu$-fold spreads (in this case, $S_i$ are ordinary $t$-dimensional subspaces, without multiplicity larger than 1);
in particular, $(0, 1)$-multispreads are spreads;

# Multispreads

- We will call a collection $(S_1, \ldots, S_n)$ of $t$-multisubspaces of $\mathbb{F}_p^m$ a $(\lambda, \mu)$-multispread, or multispread, if there hold

$$S_1 \uplus \ldots \uplus S_n = (n+\lambda) \times \{\bar{0}\} \uplus \mu \times \mathbb{F}_p^{m*}.$$

- or, equivalently,

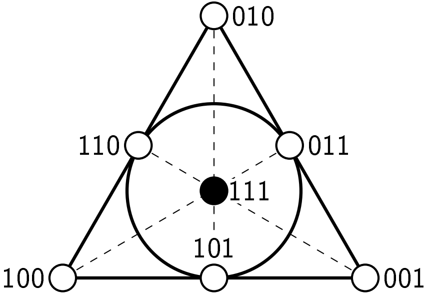
$$S_1^* \uplus \ldots \uplus S_n^* = \lambda \times \{\bar{0}\} \uplus \mu \times \mathbb{F}_p^{m*},$$

  where ${S_i}^* = S_i - \{\bar{0}\}$.

- $(0, \mu)$-multispreads are known as $\mu$-fold spreads
  (in this case, $S_i$ are ordinary $t$-dimensional subspaces, without multiplicity larger than 1);
  in particular, $(0, 1)$-multispreads are spreads;

# Example: $(1,2)$-multispread, $\mathbb{F}_2^3$, $t=2$.

An example of a $(1,2)$-multispread in $\mathbb{F}_2^3$ from four 2-subspaces $\langle\langle 100, 010\rangle\rangle$, $\langle\langle 100, 001\rangle\rangle$, $\langle\langle 010, 001\rangle\rangle$, $\langle\langle 110, 011\rangle\rangle$, and one 1-subspace $\langle\langle 111, 000\rangle\rangle$ (having multiplicity 2, as a multisubspace).



# Multispreads $\leftrightarrow$ additive intriguing sets (CR-1)

**Theorem**

*Assume $M$ is an $m \times nt$ matrix over $\mathbb{F}_p$ with groups of columns $T_1, \ldots, T_n$ (each group has $t$ columns). The code $\mathrm{null}(M)$ is an $\mathbb{F}_p$-linear intriguing set in the Hamming space $H(n,q)$, $q = p^t$, with quotient matrix*

$$\begin{pmatrix} \lambda & n(q-1)-\lambda \\ \mu & n(q-1)-\mu \end{pmatrix}$$

*if and only if $\{\langle\langle T_1 \rangle\rangle, \ldots, \langle\langle T_n \rangle\rangle\}$ is a $(\lambda,\mu)$-multispread, i.e.,*

$$\langle\langle T_1 \rangle\rangle^* \uplus \ldots \uplus \langle\langle T_n \rangle\rangle^* = \lambda \times \{\bar{0}\} \uplus \mu \times \mathbb{F}_p^{m*}.$$

- The famous Bonisoli theorem [1] that characterizes linear one-weight codes corresponds to $t = 1$, i.e., $q = p$.

[1] Bonisoli, A. Every Equidistant Linear Code Is a Sequence of Dual Hamming Codes, Ars Comb. 1984

# Multispreads $\leftrightarrow$ additive intriguing sets (CR-1)

**Theorem**

*Assume $M$ is an $m \times nt$ matrix over $\mathbb{F}_p$ with groups of columns $T_1, \ldots, T_n$ (each group has $t$ columns). The code $\mathrm{null}(M)$ is an $\mathbb{F}_p$-linear intriguing set in the Hamming space $H(n,q)$, $q = p^t$, with quotient matrix*

$$\begin{pmatrix} \lambda & n(q-1)-\lambda \\ \mu & n(q-1)-\mu \end{pmatrix}$$

*if and only if $\{\langle\!\langle T_1 \rangle\!\rangle, \ldots, \langle\!\langle T_n \rangle\!\rangle\}$ is a $(\lambda,\mu)$-multispread, i.e.,*

$$\langle\!\langle T_1 \rangle\!\rangle^* \uplus \ldots \uplus \langle\!\langle T_n \rangle\!\rangle^* = \lambda \times \{\bar{0}\} \uplus \mu \times \mathbb{F}_p^{m*}.$$

- The famous Bonisoli theorem [1] that characterizes linear one-weight codes corresponds to $t = 1$, i.e., $q = p$.

[1] Bonisoli, A. Every Equidistant Linear Code Is a Sequence of Dual Hamming Codes, Ars Comb. 1984

# A necessary condition and Wrong conjecture

$$S_1^* \uplus \ldots \uplus S_n^* = \lambda \times \{\bar{0}\} \uplus \mu \times \mathbb{F}_p^{m*},$$

- CONJECTURE. Assume that $t \le m$ and $p \le \mu$. A $(\lambda, \mu)$-multispread exists if and only if

$$\lambda + \mu(p^m - 1) \text{ is divisible by } p^t - 1;$$

  that is, if and only if

$$\lambda \equiv -\mu(p^m - 1) \bmod p^t - 1.$$

- This divisibility condition is necessary but (oops!) not sufficient.
- Denote by $\lambda_{\min} = \lambda_{\min}(p, t, m, \mu)$ the smallest nonnegative integer $\lambda$ satisfying the divisibility condition.

# A necessary condition and Wrong conjecture

$$S_1^* \uplus \ldots \uplus S_n^* = \lambda \times \{\bar{0}\} \uplus \mu \times \mathbb{F}_p^{m*},$$

- CONJECTURE. Assume that $t \leq m$ and $p \leq \mu$. A $(\lambda, \mu)$-multispread exists if and only if

$$\lambda + \mu(p^m - 1) \text{ is divisible by } p^t - 1;$$

that is, if and only if

$$\lambda \equiv -\mu(p^m - 1) \bmod p^t - 1.$$

- This divisibility condition is necessary but (oops!) not sufficient.
- Denote by $\lambda_{\min} = \lambda_{\min}(p, t, m, \mu)$ the smallest nonnegative integer $\lambda$ satisfying the divisibility condition.

# A necessary condition and Wrong conjecture

$$S_1^* \uplus \ldots \uplus S_n^* = \lambda \times \{\bar{0}\} \uplus \mu \times \mathbb{F}_p^{m*},$$

- CONJECTURE. Assume that $t \leq m$ and $p \leq \mu$. A $(\lambda, \mu)$-multispread exists if and only if

$$\lambda + \mu(p^m - 1) \text{ is divisible by } p^t - 1;$$

  that is, if and only if

$$\lambda \equiv -\mu(p^m - 1) \bmod p^t - 1.$$

- This divisibility condition is <u>necessary</u> but (oops!) <u>not sufficient</u>.
- Denote by $\lambda_{\min} = \lambda_{\min}(p, t, m, \mu)$ the smallest nonnegative integer $\lambda$ satisfying the divisibility condition.

# The divisibility condition is NOT sufficient

## Lemma (additional necessary condition for small $\mu$)

*If a $(\lambda, \mu)$-multispread exists, then there is an integer $n_0$ such that*

$$\mu \frac{q^m - 1}{q^t - 1} \leq n_0 \leq \mu \frac{q^m - 1}{q^t - q^{i_{\mathrm{mx}}}}$$

*where* $i_{\mathrm{mx}} = \min\{\lfloor \log_q(\mu) \rfloor, t - 1\}$.

## Corollary

*For any $\lambda$, there are no $(\lambda, 2)$- and $(\lambda, 3)$-multispreads from 4-multisubspaces of $\mathbb{F}_2^5$.*

# The divisibility condition is NOT sufficient: EXAMPLE

**Corollary**

*For any $\lambda$, there are no $(\lambda, 2)$- and $(\lambda, 3)$-multispreads from 4-multisubspaces of $\mathbb{F}_2^5$.*

- Proof for $\mu = 3$.

$$\lambda \overset{\mathrm{mod}\ p^t-1}{\equiv} -\mu(p^m - 1) = -3 \cdot (2^5 - 1) = -93 \overset{\mathrm{mod}\ 15}{\equiv} 12.$$

Since $\mu = 3 < 2^2$, every 4-multisubspace from the multispread has

- rank 4 (contributes 0 to $\lambda$), or
- rank 3 (contributes 1 to $\lambda$), or
- rank 0 (contributes 15 to $\lambda$).

We see that the multispread has at least 12 multisubspaces of rank 3. They cover at least $12 \cdot 14 = 168$ nonzero points, which is larger than $\mu \times |\mathbb{F}_2^{5*}| = 3 \times 31 = 93$, a contradiction.

# Special case: $t \geq m$

**Theorem**

*A $(\lambda, \mu)$-multispread, $t \geq m$ exists if and only if $\mu$ is divisible by $p^{t-m}$ and*

$$\lambda = \lambda_{\min} + \ell(p^t - 1) = (p^{t-m} - 1)\frac{\mu}{p^{t-m}} + \ell(p^t - 1)$$

*for some nonnegative integer $\ell$.*

- *Sufficiency.* Take $\mu/p^{t-m}$ times the $t$-multisubspace that spans the whole $m$-dimensional space and $\ell$ times the trivial $t$-multisubspace of rank-0.
- *Nessecity.* Since the maximum rank of a multisubspace is $m$, all multiplicities are divisible by $p^{t-m}$. The remaining is the divisibility condition

# Special case: $\mu < p$

**Theorem**

*A $(\lambda, \mu)$-multispread such that $\mu < p$ exists if and only if $\mu$ is divisible by $\frac{p^t-1}{p^s-1}$, where $s = \gcd(t, m)$, and $\lambda$ is divisible by $p^t - 1$.*

- If $\mu < p$, then a $(\lambda, \mu)$-multispread can only consist of multisubspaces of rank 0 and $t$. Hence, the collection of $t$-subspaces forms a $\mu$-fold spread, while the multisubspaces of rank 0 forms a $(\lambda = \ell(p^t - 1), 0)$-multispread (where $\ell$ is the number of 0-subspaces).

# Special case: $\mu < p$

**Theorem**

*A $(\lambda, \mu)$-multispread such that $\mu < p$ exists if and only if $\mu$ is divisible by $\frac{p^t-1}{p^s-1}$, where $s = \gcd(t, m)$, and $\lambda$ is divisible by $p^t - 1$.*

- If $\mu < p$, then a $(\lambda, \mu)$-multispread can only consist of multisubspaces of rank 0 and $t$. Hence, the collection of $t$-subspaces forms a $\mu$-fold spread, while the multisubspaces of rank 0 forms a $(\lambda{=}\ell(p^t{-}1), 0)$-multispread (where $\ell$ is the number of 0-subspaces).

# Basic constructions of multispreads

**Lemma**

*If $A$ and $B$ are $(\lambda, \mu)$- and $(\lambda', \mu')$-multispreads from $t$-multisubspaces of $\mathbb{F}_p^m$, then $A \uplus B$ is a $(\lambda + \lambda', \mu + \mu')$-multispread.*

# Basic constructions of multispreads

**Lemma**

*If there is a $(\lambda, \mu)$-multispread from $M$ $t$-multisubspaces of $\mathbb{F}_p^m$, $M = \frac{\mu(p^m-1)+\lambda}{p^t-1}$, then there is a $(\lambda', \mu')$-multispread from $t'$-multisubspaces of $\mathbb{F}_p^{m'}$, where*

(a) $m' = m, \quad t' = t, \quad \lambda' = \lambda + p^t - 1, \quad \mu' = \mu$;

(b) $m' = m, \quad t' = t, \quad \lambda' = \lambda, \quad \mu' = \mu + \frac{p^t-1}{p^s-1}$, where $s = \gcd(t, m)$;

(c) $m' = m + t, \quad t' = t, \quad \lambda' = \lambda, \quad \mu' = \mu$;

(d) $m' = m - 1, \quad t' = t, \quad \lambda' = \lambda + (p-1)\mu, \quad \mu' = p\mu$;

(e) $m' = m, \quad t' = t + 1, \quad \lambda' = p\lambda + (p-1)M, \quad \mu' = p\mu$;

(f) $p' = p^{\frac{1}{s}}, \quad m' = ms, \quad t' = ts, \quad \lambda' = \lambda, \quad \mu' = \mu$, where $p = p'^s$.

# Basic constructions: increasing $\lambda$

**Lemma**

*If there is a $(\lambda, \mu)$-multispread from $t$-multisubspaces of $\mathbb{F}_p^m$, then there is a $(\lambda', \mu')$-multispread from $t'$-multisubspaces of $\mathbb{F}_p^{m'}$, where*

(a) $m' = m, \quad t' = t, \quad \underline{\lambda' = \lambda + (p^t - 1)}, \quad \mu' = \mu;$

Proof: It follows from the existence of a $(p^t - 1, 0)$-multispread, which consists of one $t$-multisubset of rank 0.

# Basic constructions: increasing $\mu$

**Lemma**

*If there is a $(\lambda, \mu)$-multispread from $t$-multisubspaces of $\mathbb{F}_p^m$, $t \leq m$, then there is a $(\lambda', \mu')$-multispread from $t'$-multisubspaces of $\mathbb{F}_p^{m'}$, where*

(b) $m' = m$, $t' = t$, $\lambda' = \lambda$, $\underline{\mu' = \mu + \frac{p^t-1}{p^s-1}}$, *where* $s = \gcd(t, m)$;

Proof: It follows from the existence of a $(0, \frac{p^t-1}{p^s-1})$-multispread (known as $\frac{p^t-1}{p^s-1}$-fold spread in the literature).

# Basic constructions: increasing $m$

**Lemma**

*If there is a $(\lambda, \mu)$-multispread from $t$-multisubspaces of $\mathbb{F}_p^m$, $t \leq m$, then there is a $(\lambda', \mu')$-multispread from $t'$-multisubspaces of $\mathbb{F}_p^{m'}$, where*

(c) $\underline{m' = m + t}$, $\quad t' = t, \quad \lambda' = \lambda, \quad \mu' = \mu;$

*Proof*: Use a known partition of $\mathbb{F}_p^{m'} = \mathbb{F}_p^{m+t}$ into an $m$-subspace and $t$-subspaces [2]:

- Let $U$ be a $t$-subspace (over $\mathbb{F}_p$) of $\mathbb{F}_{p^m}$.
  Partition of $\mathbb{F}_{p^m} \times U \sim \mathbb{F}_p^{m+t}$:
  - $\{(\alpha u|u) : u \in U\}$ — $t$-subspace for each $\alpha \in \mathbb{F}_{p^m}$;
  - $\{(v|\mathbf{0}) : v \in \mathbb{F}_{p^m}\}$ — $m$-subspace.

[2] T. Bu. Partitions of a vector space. Discrete Math., 31:79–83, 1980.

# Basic constructions: projection

**Lemma**

*If there is a $(\lambda, \mu)$-multispread from $t$-multisubspaces of $\mathbb{F}_p^m$, then there is a $(\lambda', \mu')$-multispread from $t'$-multisubspaces of $\mathbb{F}_p^{m'}$, where*

(d) $\underline{m' = m - 1}$, $t' = t$, $\underline{\lambda' = \lambda + (p-1)\mu}$, $\underline{\mu' = p\mu}$.

*Proof*: Projection: $\mathbb{F}_p^m \to \mathbb{F}_p^{m-1}$ by removing the last component.

- $t$-multisubspace of $\mathbb{F}_q^m \longrightarrow t$-multisubspace of $\mathbb{F}_p^{m-1}$.
- Since the preimage of every non-zero vector in $\mathbb{F}_p^{m-1}$ is $p$ non-zero vectors in $\mathbb{F}_p^m$, we get $\underline{\mu' = p\mu}$.
- Since the preimage of the zero vector in $\mathbb{F}_p^{m-1}$ is the zero vector and $p-1$ non-zero vectors in $\mathbb{F}_p^m$, we get $\underline{\lambda' = \lambda + (p-1)\mu}$.

# Basic constructions: increasing $t$

**Lemma**

*If there is a $(\lambda, \mu)$-multispread from $M$ $t$-multisubspaces of $\mathbb{F}_p^m$, $M = \frac{\mu(p^m-1)+\lambda}{p^t-1}$, then there is a $(\lambda', \mu')$-multispread from $t'$-multisubspaces of $\mathbb{F}_p^{m'}$, where*

(e) $m' = m, \quad t' = t + 1, \quad \lambda' = p\lambda + (p-1)M, \quad \mu' = p\mu;$

*Proof*: (e) is obtained if we treat $t$-multisubspaces as $(t+1)$-multisubspaces, with the corresponding multiplicities of vectors.

# Basic constructions: treatment for subfield

**Lemma**

*If there is a $(\lambda,\mu)$-multispread from t-multisubspaces of $\mathbb{F}_p^m$ and $p = p'^s$, then there is a $(\lambda',\mu')$-multispread from $t'$-multisubspaces of $\mathbb{F}_{p'}^{m'}$, where*

(f) $p' = p^{1/s}, \quad m' = ms, \quad t' = ts, \quad \lambda' = \lambda, \quad \mu' = \mu.$

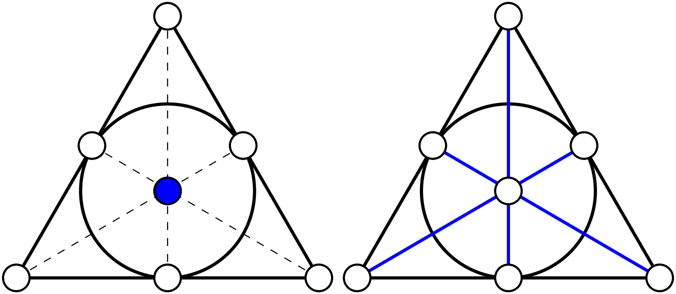
Proof: treat $\mathbb{F}_p^k$ as $\mathbb{F}_{p'}^{sk}$.

# Switching construction

By removing an $(m-2)$-dimensional subspace $S$ and adding all $p+1$ $(m-1)$-dimensional subspaces including $S$, we keep the property of being a multispread, but change the parameters:

$$(\lambda, \mu) \quad \to \quad (\lambda-(p-1),\, \mu+1).$$

The inverse operation is also useful.



# Special construction: from the Desarguesian spread in $\mathbb{F}_{p^6}$

- $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$; $\bar{D} = \{\mathbb{F}_{p^3}, a_1\mathbb{F}_{p^3}, \ldots, a_{p^3}\mathbb{F}_{p^3}\}$ — a partition of $\mathbb{F}_{p^6}$.
- Let $T$ be a 4-dimensional $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^6}$ that intersects with $p+1$ subspaces from $\bar{D}$ (call them $\bar{D}^2_T$) in a 2-dimensional subspace and the other $p^3-p$ subspaces from $\bar{D}$ (call them $\bar{D}^1_T$) in a 1-dimensional subspace.
- $\bar{D}$ itself is a $(\lambda_0, \mu = p)$-multispread, $\lambda_0 = (p-1)(p^3+1)$;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T) \cup (\bar{D} - \bar{D}^2_T)$ is a $(\lambda_1, \mu = p+1)$-multispread;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_1) \cup \mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_2) \cup (\bar{D} - \bar{D}^2_{T_1} - \bar{D}^2_{T_2})$ is a $(\lambda_2, \mu = p+2)$-multispread if $\bar{D}^2_{T_1}$ and $\bar{D}^2_{T_2}$ are disjoint;
- Collecting $(p^3+1)/(p+1)$ such 4-subspaces $T_i$ with mutually disjoint $\bar{D}^2_{T_i}$, we get $(\lambda_j, \mu = p+j)$-multispread for any $j$, with minimum possible $\lambda$.
- Good $T$: the null-space of the Trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ and its multiplicative cosets.

# Special construction: from the Desarguesian spread in $\mathbb{F}_{p^6}$

- $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$; $\bar{D} = \{\mathbb{F}_{p^3}, a_1\mathbb{F}_{p^3}, \ldots, a_{p^3}\mathbb{F}_{p^3}\}$ — a partition of $\mathbb{F}_{p^6}$.
- Let $T$ be a 4-dimensional $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^6}$ that intersects with $p+1$ subspaces from $\bar{D}$ (call them $\bar{D}^2_T$) in a 2-dimensional subspace and the other $p^3 - p$ subspaces from $\bar{D}$ (call them $\bar{D}^1_T$) in a 1-dimensional subspace.
- $\bar{D}$ itself is a $(\lambda_0, \mu = p)$-multispread, $\lambda_0 = (p-1)(p^3+1)$;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T) \cup (\bar{D} - \bar{D}^2_T)$ is a $(\lambda_1, \mu = p+1)$-multispread;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_1) \cup \mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_2) \cup (\bar{D} - \bar{D}^2_{T_1} - \bar{D}^2_{T_2})$ is a $(\lambda_2, \mu = p+2)$-multispread if $\bar{D}^2_{T_1}$ and $\bar{D}^2_{T_2}$ are disjoint;
- Collecting $(p^3+1)/(p+1)$ such 4-subspaces $T_i$ with mutually disjoint $\bar{D}^2_{T_i}$, we get $(\lambda_j, \mu = p+j)$-multispread for any $j$, with minimum possible $\lambda$.
- Good $T$: the null-space of the Trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ and its multiplicative cosets.

# Special construction: from the Desarguesian spread in $\mathbb{F}_{p^6}$

- $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$; $\bar{D} = \{\mathbb{F}_{p^3}, a_1\mathbb{F}_{p^3}, \ldots, a_{p^3}\mathbb{F}_{p^3}\}$ — a partition of $\mathbb{F}_{p^6}$.
- Let $T$ be a 4-dimensional $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^6}$ that intersects with $p+1$ subspaces from $\bar{D}$ (call them $\bar{D}^2_T$) in a 2-dimensional subspace and the other $p^3-p$ subspaces from $\bar{D}$ (call them $\bar{D}^1_T$) in a 1-dimensional subspace.
- $\bar{D}$ itself is a $(\lambda_0, \mu = p)$-multispread, $\lambda_0 = (p-1)(p^3+1)$;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T) \cup (\bar{D} - \bar{D}^2_T)$ is a $(\lambda_1, \mu = p+1)$-multispread;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_1) \cup \mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_2) \cup (\bar{D} - \bar{D}^2_{T_1} - \bar{D}^2_{T_2})$ is a $(\lambda_2, \mu = p+2)$-multispread if $\bar{D}^2_{T_1}$ and $\bar{D}^2_{T_2}$ are disjoint;
- Collecting $(p^3+1)/(p+1)$ such 4-subspaces $T_i$ with mutually disjoint $\bar{D}^2_{T_i}$, we get $(\lambda_j, \mu = p+j)$-multispread for any $j$, with minimum possible $\lambda$.
- Good $T$: the null-space of the Trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ and its multiplicative cosets.

## Special construction: from the Desarguesian spread in $\mathbb{F}_{p^6}$

- $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$; $\bar{D} = \{\mathbb{F}_{p^3}, a_1\mathbb{F}_{p^3}, \ldots, a_{p^3}\mathbb{F}_{p^3}\}$ — a partition of $\mathbb{F}_{p^6}$.
- Let $T$ be a 4-dimensional $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^6}$ that intersects with $p+1$ subspaces from $\bar{D}$ (call them $\bar{D}^2_T$) in a 2-dimensional subspace and the other $p^3-p$ subspaces from $\bar{D}$ (call them $\bar{D}^1_T$) in a 1-dimensional subspace.
- $\bar{D}$ itself is a $(\lambda_0, \mu = p)$-multispread, $\lambda_0 = (p-1)(p^3+1)$;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T) \cup (\bar{D} - \bar{D}^2_T)$ is a $(\lambda_1, \mu = p+1)$-multispread;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_1) \cup \mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_2) \cup (\bar{D} - \bar{D}^2_{T_1} - \bar{D}^2_{T_2})$ is a $(\lambda_2, \mu = p+2)$-multispread if $\bar{D}^2_{T_1}$ and $\bar{D}^2_{T_2}$ are disjoint;
- Collecting $(p^3+1)/(p+1)$ such 4-subspaces $T_i$ with mutually disjoint $\bar{D}^2_{T_i}$, we get $(\lambda_j, \mu = p+j)$-multispread for any $j$, with minimum possible $\lambda$.
- Good $T$: the null-space of the Trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ and its multiplicative cosets.

# Special construction: from the Desarguesian spread in $\mathbb{F}_{p^6}$

- $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$; $\bar{D} = \{\mathbb{F}_{p^3}, a_1\mathbb{F}_{p^3}, \ldots, a_{p^3}\mathbb{F}_{p^3}\}$ — a partition of $\mathbb{F}_{p^6}$.
- Let $T$ be a 4-dimensional $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^6}$ that intersects with $p+1$ subspaces from $\bar{D}$ (call them $\bar{D}^2_T$) in a 2-dimensional subspace and the other $p^3 - p$ subspaces from $\bar{D}$ (call them $\bar{D}^1_T$) in a 1-dimensional subspace.
- $\bar{D}$ itself is a $(\lambda_0, \mu = p)$-multispread, $\lambda_0 = (p-1)(p^3+1)$;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T) \cup (\bar{D} - \bar{D}^2_T)$ is a $(\lambda_1, \mu = p+1)$-multispread;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_1) \cup \mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_2) \cup (\bar{D} - \bar{D}^2_{T_1} - \bar{D}^2_{T_2})$ is a $(\lambda_2, \mu = p+2)$-multispread if $\bar{D}^2_{T_1}$ and $\bar{D}^2_{T_2}$ are disjoint;
- Collecting $(p^3+1)/(p+1)$ such 4-subspaces $T_i$ with mutually disjoint $\bar{D}^2_{T_i}$, we get $(\lambda_j, \mu = p+j)$-multispread for any $j$, with minimum possible $\lambda$.
- Good $T$: the null-space of the Trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ and its multiplicative cosets.

# Special construction: from the Desarguesian spread in $\mathbb{F}_{p^6}$

- $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$; $\bar{D} = \{\mathbb{F}_{p^3}, a_1\mathbb{F}_{p^3}, \ldots, a_{p^3}\mathbb{F}_{p^3}\}$ — a partition of $\mathbb{F}_{p^6}$.
- Let $T$ be a 4-dimensional $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^6}$ that intersects with $p+1$ subspaces from $\bar{D}$ (call them $\bar{D}^2_T$) in a 2-dimensional subspace and the other $p^3-p$ subspaces from $\bar{D}$ (call them $\bar{D}^1_T$) in a 1-dimensional subspace.
- $\bar{D}$ itself is a $(\lambda_0, \mu = p)$-multispread, $\lambda_0 = (p-1)(p^3+1)$;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T) \cup (\bar{D} - \bar{D}^2_T)$ is a $(\lambda_1, \mu = p+1)$-multispread;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_1) \cup \mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_2) \cup (\bar{D} - \bar{D}^2_{T_1} - \bar{D}^2_{T_2})$ is a $(\lambda_2, \mu = p+2)$-multispread if $\bar{D}^2_{T_1}$ and $\bar{D}^2_{T_2}$ are disjoint;
- Collecting $(p^3+1)/(p+1)$ such 4-subspaces $T_i$ with mutually disjoint $\bar{D}^2_{T_i}$, we get $(\lambda_j, \mu = p+j)$-multispread for any $j$, with minimum possible $\lambda$.
- Good $T$: the null-space of the Trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ and its multiplicative cosets.

# Special construction: from the Desarguesian spread in $\mathbb{F}_{p^6}$

- $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^6}$; $\bar{D} = \{\mathbb{F}_{p^3}, a_1\mathbb{F}_{p^3}, \ldots, a_{p^3}\mathbb{F}_{p^3}\}$ — a partition of $\mathbb{F}_{p^6}$.
- Let $T$ be a 4-dimensional $\mathbb{F}_p$-subspace of $\mathbb{F}_{p^6}$ that intersects with $p+1$ subspaces from $\bar{D}$ (call them $\bar{D}^2_T$) in a 2-dimensional subspace and the other $p^3-p$ subspaces from $\bar{D}$ (call them $\bar{D}^1_T$) in a 1-dimensional subspace.
- $\bar{D}$ itself is a $(\lambda_0, \mu = p)$-multispread, $\lambda_0 = (p-1)(p^3+1)$;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T) \cup (\bar{D} - \bar{D}^2_T)$ is a $(\lambda_1, \mu = p+1)$-multispread;
- $\mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_1) \cup \mathrm{Orbit}_{\mathbb{F}^\times_{p^3}}(T_2) \cup (\bar{D} - \bar{D}^2_{T_1} - \bar{D}^2_{T_2})$ is a $(\lambda_2, \mu = p+2)$-multispread if $\bar{D}^2_{T_1}$ and $\bar{D}^2_{T_2}$ are disjoint;
- Collecting $(p^3+1)/(p+1)$ such 4-subspaces $T_i$ with mutually disjoint $\bar{D}^2_{T_i}$, we get $(\lambda_j, \mu = p+j)$-multispread for any $j$, with minimum possible $\lambda$.
- Good $T$: the null-space of the Trace map $\mathbb{F}_{p^6} \to \mathbb{F}_{p^2}$ and its multiplicative cosets.

# $t = 2$: $p^2$-ary additive one-weight codes

**Theorem**

*Conjecture holds for $t = 2$ and any $m \geq 2$ (any $p$).*

- *Sketch:* It is sufficient to construct $(\lambda_{\min}, \mu)$-multispread for $m = 3$ and $\mu \in \{p, p+1, \ldots, 2p\}$.
  - $(\lambda = p-1, \mu = p)$: the projection of a spread of $\mathbb{F}_p^4$.
  - $(\lambda = 0, \mu = p+1)$: multifold spread consisting of all 2-subspaces.
  - $(\lambda = 0, \mu = 2p+2)$: multifold spread consisting of all 2-subspaces with multiplicity 2.
  - $(\lambda_{\min}, \mu = 2p+2-i)$, $i = 1, 2, ..., p$: switching by replacing a pencil of projective lines through a projective point $x$ by $x$ (we need $i$ such points, no 3 of them lying on one line).

# $t = 3$: 8-, 27-ary additive one-weight codes

**Theorem**

*Conjecture holds for $t = 3$ and any $m \equiv 1 \bmod t$ (any $p$).*

- *Sketch:* Consider a spread of $\mathbb{F}_p^4$ into $p^2+1$ subspaces of dimension 2. If we treat 2-subspaces as 3-multisubspaces (basic construction (e)), we get a $(\lambda_{\min} = (p^2+1)(p-1), \mu = p)$-multispread. Then, by switching (replacing a multisubspace of rank 2 by $p+1$ multisubspace of rank 3) we increase $\mu$ one-by-step.

**Theorem (involves computations for $p=2$, $\mu=3$ and $p=3$, $\mu=4,5$)**

*Conjecture holds for $t = 3$ and any $m \equiv 2 \bmod t$, $p = 2, 3$.*

- Note that for $m \equiv 0 \bmod t$, all parameters are solved by (ordinary) $t$-spreads.

# $t = 3$: 8-, 27-ary additive one-weight codes

**Theorem**

*Conjecture holds for $t = 3$ and any $m \equiv 1 \bmod t$ (any $p$).*

- *Sketch:* Consider a spread of $\mathbb{F}_p^4$ into $p^2+1$ subspaces of dimension 2. If we treat 2-subspaces as 3-multisubspaces (basic construction (e)), we get a $(\lambda_{\min} = (p^2+1)(p-1),\ \mu = p)$-multispread. Then, by switching (replacing a multisubspace of rank 2 by $p+1$ multisubspace of rank 3) we increase $\mu$ one-by-step.

**Theorem (involves computations for $p=2$, $\mu=3$ and $p=3$, $\mu=4,5$)**

*Conjecture holds for $t = 3$ and any $m \equiv 2 \bmod t$, $p = 2, 3$.*

- Note that for $m \equiv 0 \bmod t$, all parameters are solved by (ordinary) $t$-spreads.

# $t = 3$: 8-, 27-ary additive one-weight codes

**Theorem**

*Conjecture holds for $t = 3$ and any $m \equiv 1 \bmod t$ (any $p$).*

- *Sketch:* Consider a spread of $\mathbb{F}_p^4$ into $p^2+1$ subspaces of dimension 2. If we treat 2-subspaces as 3-multisubspaces (basic construction (e)), we get a ($\lambda_{\min} = (p^2+1)(p-1)$, $\mu = p$)-multispread. Then, by switching (replacing a multisubspace of rank 2 by $p+1$ multisubspace of rank 3) we increase $\mu$ one-by-step.

**Theorem (involves computations for $p{=}2$, $\mu{=}3$ and $p{=}3$, $\mu{=}4, 5$)**

*Conjecture holds for $t = 3$ and any $m \equiv 2 \bmod t$, $p = 2, 3$.*

- Note that for $m \equiv 0 \bmod t$, all parameters are solved by (ordinary) $t$-spreads.

# $t = 4$: 16-ary additive one-weight codes

**Theorem (special construction)**

*Conjecture holds for $t = 4$ and any $m \equiv 2 \bmod 4$ (any $p$).*

**Theorem (involves computations for $(\lambda, \mu) = (9, 3)$)**

*Conjecture holds for $t = 4$ and any $m \equiv 3 \bmod 4$, $p = 2$.*

**Theorem (involves computations for $\mu \in \{2, 3\}$, $m = 9$)**

*Conjecture holds for $t = 4$ and any $m \equiv 1 \bmod 4$, $p = 2$, except for $m = 5$, $\mu \in \{2, 3\}$.*

- In the last case, for $\mu \in \{2, 3\}$, $m = 5$ conjecture fails, and we needed to solve $m = 5 + t = 9$ (solved with computer and prescribed Aut).

# First problem for $t=3$, $m=5$ and in general for $m=2t-1$

1st open question: $\mu = p+1$, $\lambda = (p^2+1)(p-1)$

| $p$ | $\lambda$ | $\mu$ | 2-dim | 3-dim | comment |
|---|---|---|---|---|---|
| $p$ | $(p^2+1)(p-1)$ | $p+1$ | $p^2+1$ | $p^3+1$ | |
| 2 | 5 | 3 | 5 | 9 | ∃, ILP [3] |
| 3 | 20 | 4 | 10 | 28 | ∃, ILP [4] |
| 4 | 51 | 5 | 17 | 65 | ? |
| 5 | 104 | 6 | 26 | 126 | ? |

- *Problem*: find $p^{t-1}+1$ $(t-1)$-subspaces and $p^t+1$ $t$-subspaces of $\mathbb{F}_p^{2t-1}$ ($p$ prime power) such that each nonzero point belongs to $p+1$ chosen $t$-subspaces or to 1 chosen $t$-subspace and 1 chosen $(t-1)$-subspace.
- *Equivalent dual* (see the next slide) *problem* : find $p^{t-1}+1$ $t$-subspaces and $p^t+1$ $(t-1)$-subspaces of $\mathbb{F}_p^{2t-1}$ such that each nonzero point belongs to exactly 2 chosen subspaces.

[3] $\max|\mathrm{Aut}| = 6$

[4] $\max|\mathrm{Aut}| = 6$ (Sascha Kurz, private communication)

# Duality

**Theorem (special case of [a])**

[a] [S. El-Zanati, G. Seelinger, P. Sissokho, L. Spence, C. Vanden Eynden. On $\lambda$-fold partitions of finite vector spaces and duality. Discrete Math., 2011]

*A multiset $S = \{C_1, \ldots, C_n\}$ from t-multisubspaces of $\mathbb{F}_p^m$ is a $(\lambda, \mu)$-multispread if and only if $\{C_1^\perp, \ldots, C_n^\perp\}$ is a $\nu$-fold partition of $\mathbb{F}_p^m$, where*

$$\nu = n - p^{m-t}\mu$$

*or, equivalently,*

$$(p^t - 1)\nu = (p^{m-t} - 1)\mu + \lambda.$$

# Problems

- Construct multispreads with new parameters (not necessarily the first unsolved)
- Characterize infinite sequences of parameters.
- (difficult) Construct multispreads with given ranks of subspaces, characterize admissible parameters (including the collection of ranks).

# NEW: Connection with mixed orthogonal arrays

(joint work with Ferruh Özbudak and Vladimir Potapov)

- OA$(M, q_1 \cdot q_2 \cdot \ldots \cdot q_n, t)$ is code $C$ in $[q_1] \times [q_2] \times \ldots \times [q_m]$ such that fixing the values in any $t$ different positions $i_1$, $i_2$, ..., $i_t$ we always get $\frac{|C|}{q_{i_1} q_{i_2} \cdots q_{i_t}}$ codewords.
- Equivalently, it is an algebraic $t$-design (avoiding $t$ largest nonmain eigenvalues) in the multigraph

$$H = \frac{Q}{q_1} K_{q_1} \square \frac{Q}{q_2} K_{q_2} \square \cdots \square \frac{Q}{q_n} K_{q_n}, \quad \text{where } Q = \mathrm{l.c.m.}(q_1, ..., q_n).$$

# NEW: Connection with mixed orthogonal arrays

(joint work with Ferruh Özbudak and Vladimir Potapov)

- OA$(M, q_1 \cdot q_2 \cdot \ldots \cdot q_n, t)$ is code $C$ in $[q_1] \times [q_2] \times \ldots \times [q_m]$ such that fixing the values in any $t$ different positions $i_1$, $i_2$, ..., $i_t$ we always get $\frac{|C|}{q_{i_1} q_{i_2} \cdots q_{i_t}}$ codewords.
- Equivalently, it is an algebraic $t$-design (avoiding $t$ largest nonmain eigenvalues) in the multigraph

$$H = \frac{Q}{q_1} K_{q_1} \Box \frac{Q}{q_2} K_{q_2} \Box \cdots \Box \frac{Q}{q_n} K_{q_n}, \quad \text{where } Q = \mathrm{l.c.m.}(q_1, ..., q_n).$$

# Mixed OA attaining the generalized B.-F. bound

- The generalized Bierbrouer–Friedman bound for algebraic $t$-designs in arbitrary regular multigraph and for multigraph $H$ above:

$$\frac{|C|}{|G|} \geq \frac{-\theta_{t+1}}{\theta_0 - \theta_{t+1}}$$

$$\frac{|C|}{q_1 q_2 \dots q_n} \geq 1 - (1 - \frac{1}{q})\frac{n}{t+1}$$

where $q$ is the harmonic mean of all $q_i$, $i = 1, ..., n$.

- The algebraic designs satisfying the g. B.-F. bound above are $\equiv$ independent intriguing sets.
- Additive independent intriguing sets in $H$, where $q_i = p^{r_i}$ correspond to $t$-multispreads in $\mathbb{F}_p^m$, where $t = \max_i r_i$ ($r_i$ are the ranks of the corresponding subspaces).

# Mixed OA attaining the generalized B.-F. bound

- The generalized Bierbrouer–Friedman bound for algebraic $t$-designs in arbitrary regular multigraph and for multigraph $H$ above:

$$\frac{|C|}{|G|} \geq \frac{-\theta_{t+1}}{\theta_0 - \theta_{t+1}}$$

$$\frac{|C|}{q_1 q_2 \ldots q_n} \geq 1 - (1 - \frac{1}{q})\frac{n}{t+1}$$

where $q$ is the harmonic mean of all $q_i$, $i = 1, \ldots, n$.

- The algebraic designs satisfying the g. B.-F. bound above are $\equiv$ independent intriguing sets.
- Additive independent intriguing sets in $H$, where $q_i = p^{r_i}$ correspond to $t$-multispreads in $\mathbb{F}_p^m$, where $t = \max_i r_i$ ($r_i$ are the ranks of the corresponding subspaces).

# Mixed OA attaining the generalized B.-F. bound

- The generalized Bierbrouer–Friedman bound for algebraic $t$-designs in arbitrary regular multigraph and for multigraph $H$ above:
$$\frac{|C|}{|G|} \geq \frac{-\theta_{t+1}}{\theta_0 - \theta_{t+1}}$$
$$\frac{|C|}{q_1 q_2 \ldots q_n} \geq 1 - (1 - \frac{1}{q})\frac{n}{t+1}$$
where $q$ is the harmonic mean of all $q_i$, $i = 1, \ldots, n$.
- The algebraic designs satisfying the g. B.-F. bound above are $\equiv$ independent intriguing sets.
- Additive independent intriguing sets in $H$, where $q_i = p^{r_i}$ correspond to $t$-multispreads in $\mathbb{F}_p^m$, where $t = \max_i r_i$
($r_i$ are the ranks of the corresponding subspaces).