Nontrivial Pooling Designs

Chih-wen Weng
(with Huang, Tayuan & Wu, Hsin-Jung)

Department of Applied Mathematics, National Chiao Tung University

Binary matrix for group testing

1. Let $[n] := \{1, 2, \ldots, n\}$ be a set of items containing a subset $P \subseteq [n]$, the set of defected item.

Binary matrix for group testing

1. Let $[n] := \{1, 2, \ldots, n\}$ be a set of items containing a subset $P \subseteq [n]$, the set of defected item.
2. We want to collect a group $\{T_1, T_2, \ldots, T_t\}$ of t tests, each test T_i is a subset of $[n]$ for $1 \leq i \leq t$.

Binary matrix for group testing

1. Let $[n] := \{1, 2, \ldots, n\}$ be a set of items containing a subset $P \subseteq [n]$, the set of defected item.
2. We want to collect a group $\{T_1, T_2, \ldots, T_t\}$ of t tests, each test T_i is a subset of $[n]$ for $1 \leq i \leq t$.
3. We arrange such a group testing design by the following binary matrix M.

Binary matrix for group testing

1. Let $[n] := \{1, 2, \ldots, n\}$ be a set of items containing a subset $P \subseteq [n]$, the set of defected item.
2. We want to collect a group $\{T_1, T_2, \ldots, T_t\}$ of t tests, each test T_i is a subset of $[n]$ for $1 \leq i \leq t$.
3. We arrange such a group testing design by the following binary matrix M.
4. Let M be the $t \times n$ binary matrix defined by

$$M_{ij} = \begin{cases} 1, & j \in T_i; \\ 0, & j \notin T_i \end{cases}$$

for $1 \leq i \leq t$ and $j \in [n]$.

The output of a group testing

1. Let $\mathbf{P} \in F_2^n$ denote the characteristic vector of $P \subseteq [n]$.

The output of a group testing

1. Let $\mathbf{P} \in F_2^n$ denote the characteristic vector of $P \subseteq [n]$.
2. The map $P \to \mathbf{P}$ is a bijection from the power set of $[n]$ to F_2^n.

The output of a group testing

1. Let $\mathbf{P} \in F_2^n$ denote the characteristic vector of $P \subseteq [n]$.
2. The map $P \rightarrow \mathbf{P}$ is a bijection from the power set of $[n]$ to F_2^n.
3. We use $\mathbf{P} \subseteq \mathbf{P}'$ if $P \subseteq P'$, and similar for using other set notations in vectors.

The output of a group testing

1. Let $\mathbf{P} \in F_2^n$ denote the characteristic vector of $P \subseteq [n]$.
2. The map $P \to \mathbf{P}$ is a bijection from the power set of $[n]$ to F_2^n.
3. We use $\mathbf{P} \subseteq \mathbf{P}'$ if $P \subseteq P'$, and similar for using other set notations in vectors.
4. $o_M(\mathbf{P}) := \bigcup_{i \in P} M_i = M \star \mathbf{P}$, where $\star$ is the matrix product by using Boolean sum to replace addition.

The output of a group testing

1. Let $\mathbf{P} \in F_2^n$ denote the characteristic vector of $P \subseteq [n]$.
2. The map $P \to \mathbf{P}$ is a bijection from the power set of $[n]$ to F_2^n.
3. We use $\mathbf{P} \subseteq \mathbf{P}'$ if $P \subseteq P'$, and similar for using other set notations in vectors.
4. $o_M(\mathbf{P}) := \bigcup_{i \in P} M_i = M \star \mathbf{P}$, where $\star$ is the matrix product by using Boolean sum to replace addition.
5. $o_M : F_2^n \to F_2^t$ is called the output function of M.

The output of a group testing

1. Let $\mathbf{P} \in F_2^n$ denote the characteristic vector of $P \subseteq [n]$.
2. The map $P \to \mathbf{P}$ is a bijection from the power set of $[n]$ to F_2^n.
3. We use $\mathbf{P} \subseteq \mathbf{P}'$ if $P \subseteq P'$, and similar for using other set notations in vectors.
4. $o_M(\mathbf{P}) := \bigcup_{i \in P} M_i = M \star \mathbf{P}$, where $\star$ is the matrix product by using Boolean sum to replace addition.
5. $o_M : F_2^n \to F_2^t$ is called the output function of M.

Disjunct matrix

1. Note that $o_M(\mathbf{P} \cup \mathbf{P}') = o_M(\mathbf{P}) \cup o_M(\mathbf{P}')$ for $P, P' \subseteq [n]$.

Disjunct matrix

1. Note that $o_M(\mathbf{P} \cup \mathbf{P}') = o_M(\mathbf{P}) \cup o_M(\mathbf{P}')$ for $P, P' \subseteq [n]$.
2. In particular if $P \subseteq P''$ then $o_M(\mathbf{P}) \subseteq o_M(\mathbf{P}'')$.

Disjunct matrix

1. Note that $o_M(\mathbf{P} \cup \mathbf{P}') = o_M(\mathbf{P}) \cup o_M(\mathbf{P}')$ for $P, P' \subseteq [n]$.
2. In particular if $P \subseteq P''$ then $o_M(\mathbf{P}) \subseteq o_M(\mathbf{P}'')$.
3. For $W \subseteq F_2^n$, M is W-disjunct if $o_M(\mathbf{P}) \not\subseteq o_M(\mathbf{P}'')$ for any $\mathbf{P}, \mathbf{P}'' \in W$ with $P \not\subseteq P''$.

Disjunct matrix

1. Note that $o_M(\mathbf{P} \cup \mathbf{P}') = o_M(\mathbf{P}) \cup o_M(\mathbf{P}')$ for $P, P' \subseteq [n]$.
2. In particular if $P \subseteq P''$ then $o_M(\mathbf{P}) \subseteq o_M(\mathbf{P}'')$.
3. For $W \subseteq F_2^n$, M is W-disjunct if $o_M(\mathbf{P}) \not\subseteq o_M(\mathbf{P}'')$ for any $\mathbf{P}, \mathbf{P}'' \in W$ with $P \not\subseteq P''$.
4. In the above definition, it suffices to assume $|P| = 1$.

Disjunct matrix

1. Note that $o_M(\mathbf{P} \cup \mathbf{P}') = o_M(\mathbf{P}) \cup o_M(\mathbf{P}')$ for $P, P' \subseteq [n]$.
2. In particular if $P \subseteq P''$ then $o_M(\mathbf{P}) \subseteq o_M(\mathbf{P}'')$.
3. For $W \subseteq F_2^n$, M is W-disjunct if $o_M(\mathbf{P}) \not\subseteq o_M(\mathbf{P}'')$ for any $\mathbf{P}, \mathbf{P}'' \in W$ with $P \not\subseteq P''$.
4. In the above definition, it suffices to assume $|P| = 1$.
5. M is d-disjunct if for any $d+1$ distinct columns M_{i_0}, M_{i_1}, $\ldots$, M_{i_d}, we have $M_{i_0} \not\subseteq \bigcup_{j=1}^{d} M_{i_j}$

Exercise

Show that a d-disjunct matrix is $\binom{[n]}{\leq d}$-disjunct.

Decidable matrix

1. Note that $o_M(\mathbf{P})_i = 0$ iff $P \cap T_i = \emptyset$ iff $P \subseteq \overline{T_i}$.

Decidable matrix

1. Note that $o_M(\mathbf{P})_i = 0$ iff $P \cap T_i = \emptyset$ iff $P \subseteq \overline{T_i}$.
2. Hence $P \subseteq \bigcap_{o_M(\mathbf{P})_i=0} \overline{T_i}$.

Decidable matrix

1. Note that $o_M(\mathbf{P})_i = 0$ iff $P \cap T_i = \emptyset$ iff $P \subseteq \overline{T_i}$.
2. Hence $P \subseteq \bigcap_{o_M(\mathbf{P})_i = 0} \overline{T_i}$.
3. For $W \subseteq F_2^n$, M is W-decidable if $P = \bigcap_{o_M(\mathbf{P})_i = 0} \overline{T_i}$ for any $\mathbf{P} \in W$.

Decidable matrix

1. Note that $o_M(\mathbf{P})_i = 0$ iff $P \cap T_i = \emptyset$ iff $P \subseteq \overline{T_i}$.
2. Hence $P \subseteq \bigcap_{o_M(\mathbf{P})_i=0} \overline{T_i}$.
3. For $W \subseteq F_2^n$, M is *W-decidable* if $P = \bigcap_{o_M(\mathbf{P})_i=0} \overline{T_i}$ for any $\mathbf{P} \in W$.
4. A $\binom{[n]}{d}$-decidable matrix is called *d-decidable*.

Decidable matrix

1. Note that $o_M(\mathbf{P})_i = 0$ iff $P \cap T_i = \emptyset$ iff $P \subseteq \overline{T_i}$.
2. Hence $P \subseteq \bigcap_{o_M(\mathbf{P})_i = 0} \overline{T_i}$.
3. For $W \subseteq F_2^n$, M is *W-decidable* if $P = \bigcap_{o_M(\mathbf{P})_i = 0} \overline{T_i}$ for any $\mathbf{P} \in W$.
4. A $\binom{[n]}{d}$-decidable matrix is called *d-decidable*.
5. A $\binom{[n]}{\leq d}$-decidable matrix is called *$\overline{d}$-decidable*.

Exercise

Show that a W-disjunct matrix is W-decidable.

Decidable matrix

1. Note that $o_M(\mathbf{P})_i = 0$ iff $P \cap T_i = \emptyset$ iff $P \subseteq \overline{T_i}$.
2. Hence $P \subseteq \bigcap_{o_M(\mathbf{P})_i=0} \overline{T_i}$.
3. For $W \subseteq F_2^n$, M is W-decidable if $P = \bigcap_{o_M(\mathbf{P})_i=0} \overline{T_i}$ for any $\mathbf{P} \in W$.
4. A $\binom{[n]}{d}$-decidable matrix is called d-decidable.
5. A $\binom{[n]}{\leq d}$-decidable matrix is called $\overline{d}$-decidable.

Exercise

Show that a W-disjunct matrix is W-decidable.

Problem

Find a W-decidable matrix which is not W-disjunct?

Separable matrix

1. For $W \subseteq F_2^n$, M is W-separable if the restricted function $o_M \restriction W$ of o_M to W is injective.

Separable matrix

1. For $W \subseteq F_2^n$, M is W-separable if the restricted function $o_M \restriction W$ of o_M to W is injective.
2. If M is W-separable then for each vector u in the output set $o_M(W)$ there exists a unique vector $\mathbf{P} \in W$ such that $o_M(\mathbf{P}) = u$, i.e. the set P of positive items can be decoded from the output vector u.

Separable matrix

1. For $W \subseteq F_2^n$, M is W-separable if the restricted function $o_M \restriction W$ of o_M to W is injective.
2. If M is W-separable then for each vector u in the output set $o_M(W)$ there exists a unique vector $\mathbf{P} \in W$ such that $o_M(\mathbf{P}) = u$, i.e. the set P of positive items can be decoded from the output vector u.
3. A $\binom{[n]}{\leq d}$-separable matrix is also called $\overline{d}$-separable.

Separable matrix

1. For $W \subseteq F_2^n$, M is W-separable if the restricted function $o_M \restriction W$ of o_M to W is injective.
2. If M is W-separable then for each vector u in the output set $o_M(W)$ there exists a unique vector $\mathbf{P} \in W$ such that $o_M(\mathbf{P}) = u$, i.e. the set P of positive items can be decoded from the output vector u.
3. A $\binom{[n]}{\leq d}$-separable matrix is also called $\overline{d}$-separable.
4. A $\binom{[n]}{d}$-separable matrix is also called d-separable.

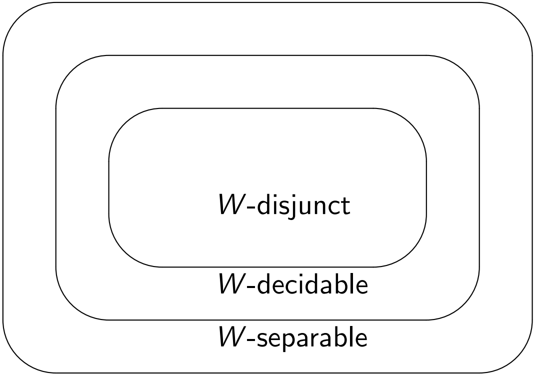
Separable matrix

1. For $W \subseteq F_2^n$, M is W-separable if the restricted function $o_M \restriction W$ of o_M to W is injective.
2. If M is W-separable then for each vector u in the output set $o_M(W)$ there exists a unique vector $\mathbf{P} \in W$ such that $o_M(\mathbf{P}) = u$, i.e. the set P of positive items can be decoded from the output vector u.
3. A $\binom{[n]}{\leq d}$-separable matrix is also called $\overline{d}$-separable.
4. A $\binom{[n]}{d}$-separable matrix is also called d-separable.

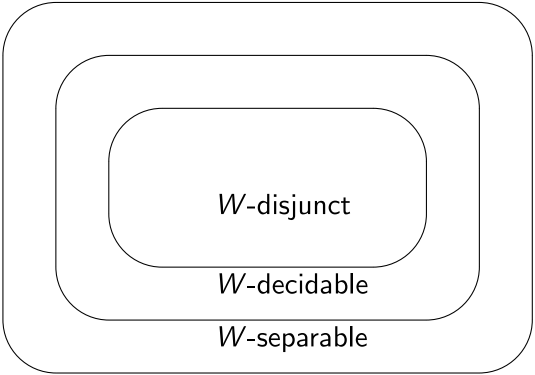
Exercise

A W-decidable matrix is W-separable for any $W \subseteq F_2^n$.

Relations



Relations



Find the relation between the above three classes of binary matrices with slightly changing W and possibly adding or deleting a few rows.

Note that for each $t \times n$ binary matrix M there exists a unique maximal $W_M \subseteq F_2^n$ such that M is W_M-decidable, in fact, $W_M = \{\mathbf{P} \in F_2^n \mid P = \bigcap_{o_M(\mathbf{P})_i = 0} \overline{T_i}\}$.

A property distinguishes decidable matrix from others

Note that for each $t \times n$ binary matrix M there exists a unique maximal $W_M \subseteq F_2^n$ such that M is W_M-decidable, in fact, $W_M = \{\mathbf{P} \in F_2^n \mid P = \bigcap_{o_M(\mathbf{P})_i = 0} \overline{T_i}\}$.

Problem

Study the map $M \to W_M$.

1-disjunct matrix

Example

A 1-disjunct matrix to detect the infected item **3** from $\{1, 2, \mathbf{3}, 4, 5, 6\}$:

Tests/Items	1	2	**3**	4	5	6		$o_M(\{\mathbf{3}\})$
one	1	1	1	0	0	0	$\rightarrow$	1
Two	1	0	0	1	1	0	$\rightarrow$	0
Three	0	1	0	1	0	1	$\rightarrow$	0
Four	0	0	1	0	1	1	$\rightarrow$	1

1-disjunct matrix

Example

A 1-disjunct matrix to detect the infected item **3** from $\{1, 2, \mathbf{3}, 4, 5, 6\}$:

Tests/Items	1	2	**3**	4	5	6		$o_M(\{\mathbf{3}\})$
one	1	1	1	0	0	0	$\to$	1
Two	1	0	0	1	1	0	$\to$	0
Three	0	1	0	1	0	1	$\to$	0
Four	0	0	1	0	1	1	$\to$	1

In fact the above 4×6 matrix M has $W_M =$
$\binom{[6]}{\leq 1} \cup \{\{3, 5, 6\}, \{2, 4, 6\}, \{1, 4, 5\}, \{4, 5, 6\}, \{1, 2, 3, 4, 5, 6\}\}$.

n-disjunct matrix

Example

For $t = n$ the $t \times n$ identity matrix I is F_2^n-disjunct.

n-disjunct matrix

Example

For $t = n$ the $t \times n$ identity matrix I is F_2^n-disjunct.

In applying to a group testing, we need the number t of tests is smaller than the number n of items, otherwise we would rather test the items one by one.

Nontrivial M

An $t \times n$ binary matrix is nontrivial if $t < n$.

Nontrivial M

An $t \times n$ binary matrix is nontrivial if $t < n$.

Example

Let q be a prime power. The affine plane F_q^2 over F_q has q^2 points and $q^2 + q$ lines.

Nontrivial M

An $t \times n$ binary matrix is nontrivial if $t < n$.

Example

Let q be a prime power. The affine plane F_q^2 over F_q has q^2 points and $q^2 + q$ lines. Since any line has q points and any two lines intersect at most 1 point, the points of a line can not be covered by the union of other $q - 1$ lines.

Nontrivial M

An $t \times n$ binary matrix is nontrivial if $t < n$.

Example

Let q be a prime power. The affine plane F_q^2 over F_q has q^2 points and $q^2 + q$ lines. Since any line has q points and any two lines intersect at most 1 point, the points of a line can not be covered by the union of other $q - 1$ lines. Hence the points-lines incidence matrix M is $(q - 1)$-disjunct matrix,

Nontrivial M

An $t \times n$ binary matrix is nontrivial if $t < n$.

Example

Let q be a prime power. The affine plane F_q^2 over F_q has q^2 points and $q^2 + q$ lines. Since any line has q points and any two lines intersect at most 1 point, the points of a line can not be covered by the union of other $q - 1$ lines. Hence the points-lines incidence matrix M is $(q-1)$-disjunct matrix, and it is nontrivial since $n = q^2 + q > q^2 = t$.

Nontrivial M

An $t \times n$ binary matrix is nontrivial if $t < n$.

Example

Let q be a prime power. The affine plane F_q^2 over F_q has q^2 points and $q^2 + q$ lines. Since any line has q points and any two lines intersect at most 1 point, the points of a line can not be covered by the union of other $q - 1$ lines. Hence the points-lines incidence matrix M is $(q - 1)$-disjunct matrix, and it is nontrivial since $n = q^2 + q > q^2 = t$.

Problem

For each positive integer q find a nontrivial $(q - 1)$-disjunct matrix with $t = q^2$.

Nontrivial M

An $t \times n$ binary matrix is nontrivial if $t < n$.

Example

Let q be a prime power. The affine plane F_q^2 over F_q has q^2 points and $q^2 + q$ lines. Since any line has q points and any two lines intersect at most 1 point, the points of a line can not be covered by the union of other $q - 1$ lines. Hence the points-lines incidence matrix M is $(q-1)$-disjunct matrix, and it is nontrivial since $n = q^2 + q > q^2 = t$.

Problem

For each positive integer q find a nontrivial $(q-1)$-disjunct matrix with $t = q^2$.

The first q which is not a prime power is when $q = 6$.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2 + r + 1, r + 1, 1)$ design.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2 + r + 1, r + 1, 1)$ design.
3. An affine plane of order r is a 2-$(r^2, r, 1)$ design.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2+r+1, r+1, 1)$ design.
3. An affine plane of order r is a 2-$(r^2, r, 1)$ design.
4. It is known that there is a projective plane of order r if and only if there is an affine plane of order r.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2 + r + 1, r + 1, 1)$ design.
3. An affine plane of order r is a 2-$(r^2, r, 1)$ design.
4. It is known that there is a projective plane of order r if and only if there is an affine plane of order r.
5. The points and lines structure in F_q^2 gives an affine plane of order q when q is a prime power.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2+r+1, r+1, 1)$ design.
3. An affine plane of order r is a 2-$(r^2, r, 1)$ design.
4. It is known that there is a projective plane of order r if and only if there is an affine plane of order r.
5. The points and lines structure in F_q^2 gives an affine plane of order q when q is a prime power.
6. The existence of finite projective planes of other orders is an open question.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2 + r + 1, r + 1, 1)$ design.
3. An affine plane of order r is a 2-$(r^2, r, 1)$ design.
4. It is known that there is a projective plane of order r if and only if there is an affine plane of order r.
5. The points and lines structure in F_q^2 gives an affine plane of order q when q is a prime power.
6. The existence of finite projective planes of other orders is an open question.
7. The case $r = 6$ has been ruled out by Bruck-Ryser-Chowla theorem.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2+r+1, r+1, 1)$ design.
3. An affine plane of order r is a 2-$(r^2, r, 1)$ design.
4. It is known that there is a projective plane of order r if and only if there is an affine plane of order r.
5. The points and lines structure in F_q^2 gives an affine plane of order q when q is a prime power.
6. The existence of finite projective planes of other orders is an open question.
7. The case $r = 6$ has been ruled out by Bruck-Ryser-Chowla theorem.
8. The next case $r = 10$ has been ruled out by massive computer calculations.

Affine plane and projective plane

1. In general for any positive integer r, prime power or not, we can define affine plane using the language of designs.
2. A projective plane of order r is a 2-$(r^2+r+1, r+1, 1)$ design.
3. An affine plane of order r is a 2-$(r^2, r, 1)$ design.
4. It is known that there is a projective plane of order r if and only if there is an affine plane of order r.
5. The points and lines structure in F_q^2 gives an affine plane of order q when q is a prime power.
6. The existence of finite projective planes of other orders is an open question.
7. The case $r = 6$ has been ruled out by Bruck-Ryser-Chowla theorem.
8. The next case $r = 10$ has been ruled out by massive computer calculations.
9. There is nothing more known, in particular $r = 12$ is still open.

Nontrivial 5-disjunct matrix with 36 rows

Since there is no affine plane of order 6, we must find some other way to construct a nontrivial 5-disjunct matrix with 36 rows.

Nontrivial 5-disjunct matrix with 36 rows

Since there is no affine plane of order 6, we must find some other way to construct a nontrivial 5-disjunct matrix with 36 rows.

In the following we will give a system to construct nontrivial d-disjunct matrices including the above case.

Nontrivial 5-disjunct matrix with 36 rows

Since there is no affine plane of order 6, we must find some other way to construct a nontrivial 5-disjunct matrix with 36 rows.

In the following we will give a system to construct nontrivial d-disjunct matrices including the above case.

Note that if there exists a nontrivial d-disjunct matrix with $(d+1)^2 - 1$ rows then EFF's conjecture is false. See page 29 of the book "Pooling Designs and nonadaptive group testing" by Ding-Zhu Du and Frank K. Hwang for a description of EFF's conjecture.

A 36 × 37 5-disjunct matrix

吴欣融的答案 10/29/01

以11,12,…,16,21,…,26,…,66代表36个元素。
以下之37个子集任二子集最多有一共同元素，
故每一子集会被任意其它五个子集的联集覆盖。

①	11	22	33	54	65	26	⑲	11	52	23	64	45	56
②	12	23	34	55	66	21	⑳	12	53	24	65	46	51
③	13	24	35	56	61	22	㉑	13	54	25	66	41	52
④	14	25	36	51	62	23	㉒	14	55	26	61	42	53
⑤	15	26	31	52	63	24	㉓	15	56	21	62	43	54
⑥	16	21	32	53	64	25	㉔	16	51	22	63	44	55
⑦	11	32	43	24	55	36	㉕	11	62	53	44	35	66
⑧	12	33	44	25	56	31	㉖	12	63	54	45	36	61
⑨	13	34	45	26	51	32	㉗	13	64	55	46	31	62
⑩	14	35	46	21	52	33	㉘	14	65	56	41	32	63
⑪	15	36	41	22	53	34	㉙	15	66	51	42	33	64
⑫	16	31	42	23	54	35	㉚	16	61	52	43	34	65
⑬	11	42	63	34	25	46	㉛	11	21	31	41	51	61
⑭	12	43	64	35	26	41	㉜	12	22	32	42	52	62
⑮	13	44	65	36	21	42	㉝	13	23	33	43	53	63
⑯	14	45	66	31	22	43	㉞	14	24	34	44	54	64
⑰	15	46	61	32	23	44	㉟	15	25	35	45	55	65
⑱	16	41	62	33	24	45	㊱	16	26	36	46	56	66
㊲	11	12	13	14	15	16							

Forward difference property

1. Let q be a prime power and $m \geq q$ be an integer.

Forward difference property

1. Let q be a prime power and $m \geq q$ be an integer.
2. Let $F_q := \{0, a^0, a^1, \ldots, a^{p-2}\}$ denote the finite field of q elements, where a is a generator of the cyclic multiplication group $F_q^* := F_q - \{0\}$.

Forward difference property

1. Let q be a prime power and $m \geq q$ be an integer.
2. Let $F_q := \{0, a^0, a^1, \ldots, a^{p-2}\}$ denote the finite field of q elements, where a is a generator of the cyclic multiplication group $F_q^* := F_q - \{0\}$.
3. Let $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ be the addition group of integers modulo m. We use the order of integers to order the elements in $\mathbb{Z}_m$, e.g. $0 < 1$.

Forward difference property

1. Let q be a prime power and $m \geq q$ be an integer.
2. Let $F_q := \{0, a^0, a^1, \ldots, a^{p-2}\}$ denote the finite field of q elements, where a is a generator of the cyclic multiplication group $F_q^* := F_q - \{0\}$.
3. Let $\mathbb{Z}_m := \{0, 1, \ldots, m-1\}$ be the addition group of integers modulo m. We use the order of integers to order the elements in $\mathbb{Z}_m$, e.g. $0 < 1$.
4. A subset $T \subseteq \mathbb{Z}_m \times F_q$ is said to have the forward difference distinct property in $\mathbb{Z}_m \times F_q$ if the set

$$D_T := \{(j, y) - (i, x) \mid (i, x), (j, y) \in T \text{ with } i < j\}$$

consists of $\frac{|T|(|T|-1)}{2}$ elements.

The Set ${}_mT_q$

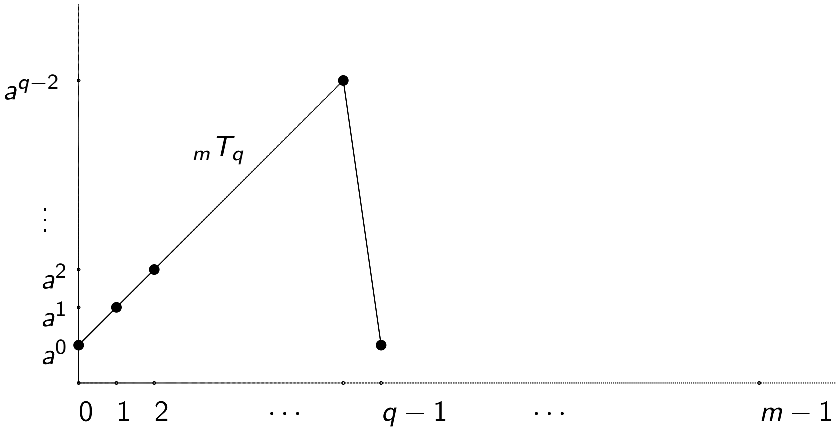
Let ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ be defined by

$$ {}_mT_q = \{(i, a^i) \mid i \in \mathbb{Z}_m, 0 \leq i \leq q-1\}. $$

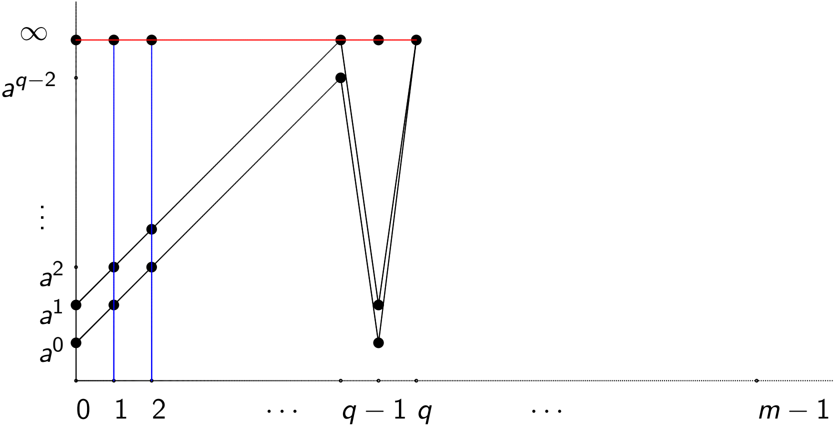
The Set ${}_mT_q$

Let ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ be defined by

$$ {}_mT_q = \{(i, a^i) \mid i \in \mathbb{Z}_m, 0 \leq i \leq q-1\}. $$



A preview of the finial result



Lines in $Z_m \times (F_q \cup \{\infty\})$

The Set ${}_5T_5$

For $q = 5$, $a = 2$,

$$ {}_5T_5 = \{(0,1),(1,2),(2,4),(3,3),(4,1)\} $$

and

$$ \begin{aligned} D_{{}_5T_5} = \{ \quad & (1,1),(1,2),(1,4),(1,3) \\ & (2,3),(2,1),(2,2) \\ & (3,2),(3,4) \\ & (4,0) \quad \}. \end{aligned} $$

The Set ${}_5T_5$

For $q = 5$, $a = 2$,

$${}_5T_5 = \{(0,1),(1,2),(2,4),(3,3),(4,1)\}$$

and

$$\begin{aligned} D_{{}_5T_5} \quad = \{ \quad & (1,1),(1,2),(1,4),(1,3) \\ & (2,3),(2,1),(2,2) \\ & (3,2),(3,4) \\ & (4,0) \quad \}. \end{aligned}$$

Since $|D_{{}_5T_5}| = 10$, the set ${}_5T_5$ has the forward difference distinct property in $\mathbb{Z}_5 \times F_5$.

Difference Property

A subset $T \subseteq \mathbb{Z}_m \times F_q$ is said to have the difference distinct property in $\mathbb{Z}_m \times F_q$ if the set $-D_T \cup D_T$ consists of $|T|(|T|-1)$ elements.

Difference Property

A subset $T \subseteq \mathbb{Z}_m \times F_q$ is said to have the difference distinct property in $\mathbb{Z}_m \times F_q$ if the set $-D_T \cup D_T$ consists of $|T|(|T|-1)$ elements.

From the structure of $D_{{}_mT_q}$ we find $(0,x) \notin -D_{{}_mT_q} \cup D_{{}_mT_q}$ for any $x \in F_q$. This property will be used later.

Non-example

We have seen

$$\begin{aligned} D_{5\,T_5} = \{ \quad & (1,1),(1,2),(1,4),(1,3) \\ & (2,3),(2,1),(2,2) \\ & (3,2),(3,4) \\ & (4,0) \quad \}. \end{aligned}$$

Non-example

We have seen

$$\begin{aligned} D_{5}\,T_5 \quad = \{ \quad & (1,1),(1,2),(1,4),(1,3) \\ & (2,3),(2,1),(2,2) \\ & (3,2),(3,4) \\ & (4,0) \quad \}. \end{aligned}$$

Hence

$$\begin{aligned} -D_{5}\,T_5 \quad = \{ \quad & (4,4),(4,3),(4,1),(4,2) \\ & {\color{red}(3,2),(3,4)},(3,3) \\ & {\color{red}(2,3),(2,1)} \\ & (1,0) \quad \}. \end{aligned}$$

Non-example

We have seen

$$D_{_5T_5} = \{ \begin{array}{l} (1,1),(1,2),(1,4),(1,3) \\ (2,3),(2,1),(2,2) \\ (3,2),(3,4) \\ (4,0) \end{array} \}.$$

Hence

$$-D_{_5T_5} = \{ \begin{array}{l} (4,4),(4,3),(4,1),(4,2) \\ \color{red}{(3,2),(3,4)},(3,3) \\ \color{red}{(2,3),(2,1)} \\ (1,0) \end{array} \}.$$

Since $|-D_{_5T_5} \cup D_{_5T_5}| = 16 \neq 20$, the set $_5T_5$ does not have the difference distinct property in $\mathbb{Z}_5 \times F_5$.

Embedding

For positive integers $n < m$, the set $\mathbb{Z}_n$ can be viewed as a subset of $\mathbb{Z}_m$ in the usual way. Hence we have $\mathbb{Z}_n \times F_q \subseteq \mathbb{Z}_m \times F_q$.

Embedding

For positive integers $n < m$, the set $\mathbb{Z}_n$ can be viewed as a subset of $\mathbb{Z}_m$ in the usual way. Hence we have $\mathbb{Z}_n \times F_q \subseteq \mathbb{Z}_m \times F_q$. In this setting, again

$$\begin{aligned} D_{6}{}_{T_5} = D_{5}{}_{T_5} \quad = \{ \quad & (1,1),(1,2),(1,4),(1,3) \\ & (2,3),(2,1),(2,2) \\ & (3,2),(3,4) \\ & (4,0) \quad \}. \end{aligned}$$

Embedding

For positive integers $n < m$, the set $\mathbb{Z}_n$ can be viewed as a subset of $\mathbb{Z}_m$ in the usual way. Hence we have $\mathbb{Z}_n \times F_q \subseteq \mathbb{Z}_m \times F_q$. In this setting, again

$$
\begin{aligned}
D_{{}_6T_5} = D_{{}_5T_5} = \{ \quad & (1,1),(1,2),(1,4),(1,3) \\
& (2,3),(2,1),(2,2) \\
& (3,2),(3,4) \\
& (4,0) \quad \}.
\end{aligned}
$$

Hence considering as the negative in $\mathbb{Z}_6 \times F_5$, we have

$$
\begin{aligned}
-D_{{}_6T_5} = \{ \quad & (5,4),(5,3),(5,1),(5,2) \\
& (4,2),(4,4),(4,3) \\
& (3,3),(3,1) \\
& (2,0) \quad \}.
\end{aligned}
$$

Since $|-D_{{}_6T_5} \cup D_{{}_6T_5}| = 20$ now, the set ${}_6T_5$ has the difference distinct property in $\mathbb{Z}_6 \times F_5$.

Problem

Determine the prime power integer q such that with a suitable choice of a generator $a \in F_q$, the set ${}_{q+1}T_q$ has the difference distinct property in $\mathbb{Z}_{q+1} \times F_q$.

Problem

Determine the prime power integer q such that with a suitable choice of a generator $a \in F_q$, the set ${}_{q+1}T_q$ has the difference distinct property in $\mathbb{Z}_{q+1} \times F_q$.

By direct computing by hands, we find the above statement is true for $q = 2, 4, 5$ and is false for $q = 3, 7$ (First two primes in $4k + 3$ form).

Problem

Determine the prime power integer q such that with a suitable choice of a generator $a \in F_q$, the set ${}_{q+1}T_q$ has the difference distinct property in $\mathbb{Z}_{q+1} \times F_q$.

By direct computing by hands, we find the above statement is true for $q = 2, 4, 5$ and is false for $q = 3, 7$ (First two primes in $4k + 3$ form).

Example

Note that

$$ {}_4T_3 \quad = \quad \{(0,1),(1,2),(2,1)\}, $$

Problem

Determine the prime power integer q such that with a suitable choice of a generator $a \in F_q$, the set ${}_{q+1}T_q$ has the difference distinct property in $\mathbb{Z}_{q+1} \times F_q$.

By direct computing by hands, we find the above statement is true for $q = 2, 4, 5$ and is false for $q = 3, 7$ (First two primes in $4k + 3$ form).

Example

Note that

$$\begin{aligned} {}_4T_3 &= \{(0,1),(1,2),(2,1)\}, \\ D_{{}_4T_3} &= \{(1,1),(1,2),(2,0)\}, \end{aligned}$$

Problem

Determine the prime power integer q such that with a suitable choice of a generator $a \in F_q$, the set ${}_{q+1}T_q$ has the difference distinct property in $\mathbb{Z}_{q+1} \times F_q$.

By direct computing by hands, we find the above statement is true for $q = 2, 4, 5$ and is false for $q = 3, 7$ (First two primes in $4k + 3$ form).

Example

Note that

$$\begin{aligned} {}_4T_3 &= \{(0,1),(1,2),(2,1)\}, \\ D_{{}_4T_3} &= \{(1,1),(1,2),(2,0)\}, \\ -D_{{}_4T_3} &= \{(3,2),(3,1),(2,0)\}. \end{aligned}$$

Problem

Determine the prime power integer q such that with a suitable choice of a generator $a \in F_q$, the set ${}_{q+1}T_q$ has the difference distinct property in $\mathbb{Z}_{q+1} \times F_q$.

By direct computing by hands, we find the above statement is true for $q = 2, 4, 5$ and is false for $q = 3, 7$ (First two primes in $4k + 3$ form).

Example

Note that

$$\begin{aligned} {}_4T_3 &= \{(0,1),(1,2),(2,1)\}, \\ D_{{}_4T_3} &= \{(1,1),(1,2),(2,0)\}, \\ -D_{{}_4T_3} &= \{(3,2),(3,1),(2,0)\}. \end{aligned}$$

Hence the set ${}_4T_3$ does not have the difference distinct property in $\mathbb{Z}_4 \times F_3$.

${}_mT_q$ has the forward difference distinct property

Theorem

The set ${}_mT_q$ has the forward difference distinct property in $\mathbb{Z}_m \times T_q$.

${}_mT_q$ has the forward difference distinct property

Theorem

The set ${}_mT_q$ has the forward difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

Suppose for $0 \leq i < j \leq q - 1$ we have $j - i = c$ and $a^j - a^i = d$.

${}_mT_q$ has the forward difference distinct property

Theorem

The set ${}_mT_q$ has the forward difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

Suppose for $0 \leq i < j \leq q-1$ we have $j - i = c$ and $a^j - a^i = d$. Note that $1 \leq c \leq q-1$.

${}_mT_q$ has the forward difference distinct property

Theorem

The set ${}_mT_q$ has the forward difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

Suppose for $0 \leq i < j \leq q-1$ we have $j - i = c$ and $a^j - a^i = d$. Note that $1 \leq c \leq q-1$. If $c = q-1$ then $j = q-1$ and $i = 0$.

${}_mT_q$ has the forward difference distinct property

Theorem

The set ${}_mT_q$ has the forward difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

Suppose for $0 \le i < j \le q-1$ we have $j - i = c$ and $a^j - a^i = d$. Note that $1 \le c \le q-1$. If $c = q-1$ then $j = q-1$ and $i = 0$. If $c \ne q-1$ then $a^i = d/(a^{j-i} - 1) = d/(a^c - 1)$ and $j = c + i$.

${}_mT_q$ has the forward difference distinct property

Theorem

The set ${}_mT_q$ has the forward difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

Suppose for $0 \leq i < j \leq q-1$ we have $j - i = c$ and $a^j - a^i = d$. Note that $1 \leq c \leq q-1$. If $c = q-1$ then $j = q-1$ and $i = 0$. If $c \neq q-1$ then $a^i = d/(a^{j-i} - 1) = d/(a^c - 1)$ and $j = c + i$. In each case the pair $(i, a^i), (j, a^j)$ is unique determined by the element $(c, d) \in \mathbb{Z}_m \times F_q$. □

${}_{2q-1}T_q$ has the difference distinct property

Theorem

For $m \geq 2q-1$*, the set* ${}_mT_q$ *has the difference distinct property in* $\mathbb{Z}_m \times T_q$.

${}_{2q-1}T_q$ has the difference distinct property

Theorem

For $m \geq 2q-1$, the set ${}_mT_q$ has the difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

By the theorem in the last page we have
$|D_{{}_mT_q}| = |-D_{{}_mT_q}| = q(q-1)/2$.

${}_{2q-1}T_q$ has the difference distinct property

Theorem

For $m \geq 2q-1$, the set ${}_mT_q$ has the difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

By the theorem in the last page we have $|D_{{}_mT_q}| = |-D_{{}_mT_q}| = q(q-1)/2$. The first coordinate of an element in $D_{{}_{2q-1}T_q}$ runs from 1 to $q-1$, and the first coordinate of an element in $-D_{{}_{2q-1}T_q}$ from $m+1-q$ to $m-1$.

${}_{2q-1}T_q$ has the difference distinct property

Theorem

For $m \geq 2q-1$, the set ${}_mT_q$ has the difference distinct property in $\mathbb{Z}_m \times T_q$.

Proof.

By the theorem in the last page we have $|D_{{}_mT_q}| = |-D_{{}_mT_q}| = q(q-1)/2$. The first coordinate of an element in $D_{{}_{2q-1}T_q}$ runs from 1 to $q-1$, and the first coordinate of an element in $-D_{{}_{2q-1}T_q}$ from $m+1-q$ to $m-1$. The assumption $m \geq 2q-1$ implies $-D_{{}_{2q-1}T_q} \cap D_{{}_{2q-1}T_q} = \emptyset$. □

Lines with any two intersecting in at most a point

Theorem

Suppose that ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ *has the difference distinct property in* $\mathbb{Z}_m \times F_q$*. Set* $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$*. Then* $|L \cap L'| \leq 1$ *for any distinct* $L, L' \in \mathcal{B}$*.*

Lines with any two intersecting in at most a point

Theorem

Suppose that ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ *has the difference distinct property in* $\mathbb{Z}_m \times F_q$. *Set* $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$. *Then* $|L \cap L'| \leq 1$ *for any distinct* $L, L' \in \mathcal{B}$.

Proof.

Routine. □

Lines with any two intersecting in at most a point

Theorem

Suppose that ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ has the difference distinct property in $\mathbb{Z}_m \times F_q$. Set $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$. Then $|L \cap L'| \leq 1$ for any distinct $L, L' \in \mathcal{B}$.

Proof.

Routine. □

An element in $\mathcal{B}$ is called a line and an element in $Z_m \times F_q$ is called a point.

Lines with any two intersecting in at most a point

Theorem

Suppose that ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ has the difference distinct property in $\mathbb{Z}_m \times F_q$. Set $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$. Then $|L \cap L'| \leq 1$ for any distinct $L, L' \in \mathcal{B}$.

Proof.

Routine. □

An element in $\mathcal{B}$ is called a line and an element in $Z_m \times F_q$ is called a point. Note that there are mq lines and mq points, and a line has $q = |T|$ points with q different first coordinates.

Lines with any two intersecting in at most a point

Theorem

Suppose that $_mT_q \subseteq \mathbb{Z}_m \times F_q$ has the difference distinct property in $\mathbb{Z}_m \times F_q$. Set $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$. Then $|L \cap L'| \leq 1$ for any distinct $L, L' \in \mathcal{B}$.

Proof.

Routine. □

An element in $\mathcal{B}$ is called a line and an element in $Z_m \times F_q$ is called a point. Note that there are mq lines and mq points, and a line has $q = |T|$ points with q different first coordinates. Apparently more lines can be added to $\mathcal{B}$ still having the conclusion of the above theorem, for example, adding vertical lines to $\mathcal{B}$.

Adding an infinity point to each line

As previous page, assume that any two lines in $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$ intersect at at most one point.

Adding an infinity point to each line

As previous page, assume that any two lines in $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$ intersect at at most one point.

Since $(0, x) \notin -D_{{}_mT_q} \cup D_{{}_mT_q}$, we have $L \cap ((0, x) + L) = \emptyset$ for any nonzero $x \in F_q$ and $L \in \mathcal{B}$.

Adding an infinity point to each line

As previous page, assume that any two lines in $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$ intersect at at most one point.

Since $(0, x) \notin -D_{{}_m T_q} \cup D_{{}_m T_q}$, we have $L \cap ((0, x) + L) = \emptyset$ for any nonzero $x \in F_q$ and $L \in \mathcal{B}$. Then $\mathcal{B}$ is partitioned into m classes with each class consisting of parallel lines (non-intersecting lines).

Adding an infinity point to each line

As previous page, assume that any two lines in $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$ intersect at at most one point.

Since $(0, x) \notin -D_{{}_m T_q} \cup D_{{}_m T_q}$, we have $L \cap ((0, x) + L) = \emptyset$ for any nonzero $x \in F_q$ and $L \in \mathcal{B}$. Then $\mathcal{B}$ is partitioned into m classes with each class consisting of parallel lines (non-intersecting lines). We add a common point (i, ∞) to each line in a parallel class where $i \in \mathbb{Z}_m$ is not appearing in the first coordinate of any points of the line and $i - 1$ appearing in some point of the line.

Adding an infinity point to each line

As previous page, assume that any two lines in $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$ intersect at at most one point.

Since $(0, x) \notin -D_{{}_mT_q} \cup D_{{}_mT_q}$, we have $L \cap ((0, x) + L) = \emptyset$ for any nonzero $x \in F_q$ and $L \in \mathcal{B}$. Then $\mathcal{B}$ is partitioned into m classes with each class consisting of parallel lines (non-intersecting lines). We add a common point (i, ∞) to each line in a parallel class where $i \in \mathbb{Z}_m$ is not appearing in the first coordinate of any points of the line and $i - 1$ appearing in some point of the line. This forms a new set $\mathcal{B}'$ of Lines with underground point set $Z_m \times (F_q \cup \{\infty\})$.

Adding an infinity point to each line

As previous page, assume that any two lines in $\mathcal{B} = \{u +_m T_q \mid u \in \mathbb{Z}_m \times F_q\}$ intersect at at most one point.

Since $(0, x) \notin -D_{{}_m T_q} \cup D_{{}_m T_q}$, we have $L \cap ((0, x) + L) = \emptyset$ for any nonzero $x \in F_q$ and $L \in \mathcal{B}$. Then $\mathcal{B}$ is partitioned into m classes with each class consisting of parallel lines (non-intersecting lines). We add a common point (i, ∞) to each line in a parallel class where $i \in \mathbb{Z}_m$ is not appearing in the first coordinate of any points of the line and $i - 1$ appearing in some point of the line. This forms a new set $\mathcal{B}'$ of Lines with underground point set $Z_m \times (F_q \cup \{\infty\})$. Note that any two distinct lines in $\mathcal{B}'$ intersect in at most one point too.

Vertical Lines and infinite line

Set $V_i = \{(i, j) \mid j \in F_q \cup \{\infty\}\ \}$ for $0 \leq i \leq m - 1$, and V_i is called the ith vertical line. Set $H = \{(i, \infty) \mid 0 \leq i \leq q\}$ (here assuming $m > q$), and H is called an infinite line.

Vertical Lines and infinite line

Set $V_i = \{(i,j) \mid j \in F_q \cup \{\infty\}\ \}$ for $0 \le i \le m-1$, and V_i is called the ith vertical line. Set $H = \{(i,\infty) \mid 0 \le i \le q\}$ (here assuming $m > q$), and H is called an infinite line.

Set $\mathcal{B}'' := \mathcal{B}' \cup \{H, V_0, V_1, \ldots, V_{m-1}\}$. Then $|Z_m \times (F_q \cup \{\infty\})| = m(q+1)$ and $|\mathcal{B}''| = m(q+1)+1$.

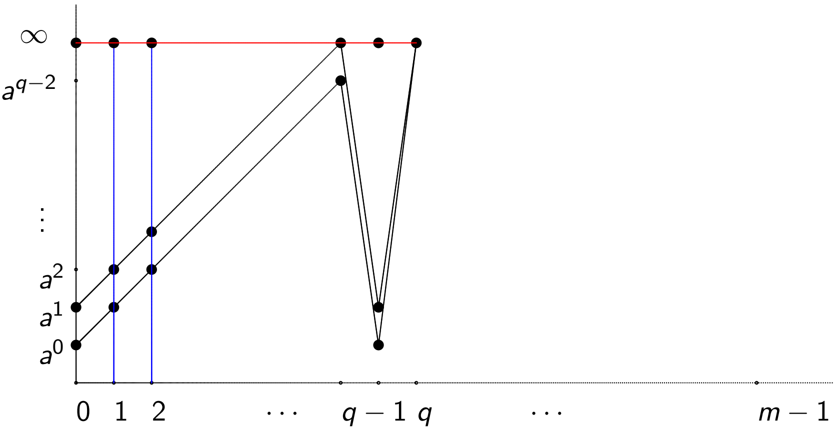
Conclusion

Suppose that ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ has the difference distinct property in $\mathbb{Z}_m \times F_q$, for example in the case $m \geq 2q - 1$ or $m = q + 1 = 6$.

Conclusion

Suppose that ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ has the difference distinct property in $\mathbb{Z}_m \times F_q$, for example in the case $m \geq 2q - 1$ or $m = q + 1 = 6$. Let M be the incidence matrix of $\mathbb{Z}_m \times (F_q \cup \{\infty\})$ and $\mathcal{B}''$. Then M is a nontrivial q-disjunct matrix with $m(q + 1)$ rows.

A Review of our result



Lines in $Z_m \times (F_q \cup \{\infty\})$

The end

Thank you for your attention.