# Pooling design and its construction

Chih-wen Weng
(with Yu-pei Huang and Wu, Hsin-Jung)

Department of Applied Mathematics, National Chiao Tung University

December 6, 2009

# 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 $1 \le i \le t$.
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 $j \in [n]$.

# 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 $j \in [n]$.
5. The weight of row $i$ in $M$ is $|T_i|$. The weight of column $j$ in $M$ is $|\{k | M_{kj} = 1\}|$.

# 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 $P \to \mathbf{P}$ 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.

# 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 $P \rightarrow \mathbf{P}$ 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.
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. $o_M : F_2^n \rightarrow F_2^t$ is called the output function of $M$.

## Example

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

$$\left(\begin{array}{c|cccccccc}
\text{Tests/Items} & 1 & 2 & \mathbf{3} & 4 & 5 & 6 & & \mathrm{o}_M(\{\mathbf{3}\}) \\
\hline
 & & & & & & & & \\
\text{one} & 1 & 1 & 1 & 0 & 0 & 0 & \longrightarrow & 1 \\
\text{Two} & 1 & 0 & 0 & 1 & 1 & 0 & \longrightarrow & 0 \\
\text{Three} & 0 & 1 & 0 & 1 & 0 & 1 & \longrightarrow & 0 \\
\text{Four} & 0 & 0 & 1 & 0 & 1 & 1 & \longrightarrow & 1
\end{array}\right)$$

## Example

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

$$
\left(\begin{array}{c|cccccccc}
\text{Tests/Items} & 1 & 2 & \mathbf{3} & 4 & 5 & 6 & & o_M(\{\mathbf{3}\}) \\
\hline
 & & & & & & & & \\
\text{one} & 1 & 1 & 1 & 0 & 0 & 0 & \rightarrow & 1 \\
\text{Two} & 1 & 0 & 0 & 1 & 1 & 0 & \rightarrow & 0 \\
\text{Three} & 0 & 1 & 0 & 1 & 0 & 1 & \rightarrow & 0 \\
\text{Four} & 0 & 0 & 1 & 0 & 1 & 1 & \rightarrow & 1
\end{array}\right)
$$

For the correctness of detecting we need to assume there is at most one infected item.

## Example

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

$$\left(\begin{array}{c|cccccccc} \text{Tests/Items} & 1 & 2 & \mathbf{3} & 4 & 5 & 6 & & o_M(\{\mathbf{3}\}) \\ \hline \\ \text{one} & 1 & 1 & 1 & 0 & 0 & 0 & \rightarrow & 1 \\ \text{Two} & 1 & 0 & 0 & 1 & 1 & 0 & \rightarrow & 0 \\ \text{Three} & 0 & 1 & 0 & 1 & 0 & 1 & \rightarrow & 0 \\ \text{Four} & 0 & 0 & 1 & 0 & 1 & 1 & \rightarrow & 1 \end{array}\right)$$

For the correctness of detecting we need to assume there is at most one infected item.

Both the infected sets $\{3, 4\}$ and $\{1, 6\}$ have the same output $(1, 1, 1, 1)$. So it is impossible to recover the infected set from the output.

## Definition

A $t \times n$ binary matrix $M$ is $d$-disjunct if for any column $M_{i_0}$ and any other $d$ columns $M_{i_1}, \ldots, M_{i_d}$ (allowing repeat if $n \leq d$), we have $M_{i_0} \not\subseteq \bigcup_{j=1}^{d} M_{i_j}$

**Definition**

A $t \times n$ binary matrix $M$ is $d$-disjunct if for any column $M_{i_0}$ and any other $d$ columns $M_{i_1}, \ldots, M_{i_d}$ (allowing repeat if $n \le d$), we have $M_{i_0} \not\subseteq \bigcup_{j=1}^{d} M_{i_j}$

**Definition**

$M$ is $\overline{d}$-separable if the outputs of any sets of at most $d$ columns are all distinct, i.e. the restriction function $o_M \restriction \binom{[n]}{\le d}$ is injective.

## Definition

A $t \times n$ binary matrix $M$ is $d$-disjunct if for any column $M_{i_0}$ and any other $d$ columns $M_{i_1}, \ldots, M_{i_d}$ (allowing repeat if $n \leq d$), we have $M_{i_0} \not\subseteq \bigcup_{j=1}^{d} M_{i_j}$

## Definition

$M$ is $\overline{d}$-separable if the outputs of any sets of at most $d$ columns are all distinct, i.e. the restriction function $o_M \restriction \binom{[n]}{\leq d}$ is injective.

An $t \times n$ $\overline{d}$-separable matrix can be used as a non-adaptive group testing design that contains $t$ group tests to test $n$ items, which can detect the defective items from the test output if the number of defective items is assumed not more than $d$.

### Definition

A $t \times n$ binary matrix $M$ is $d$-disjunct if for any column $M_{i_0}$ and any other $d$ columns $M_{i_1}, \ldots, M_{i_d}$ (allowing repeat if $n \leq d$), we have $M_{i_0} \not\subseteq \bigcup_{j=1}^{d} M_{i_j}$

### Definition

$M$ is $\overline{d}$-separable if the outputs of any sets of at most $d$ columns are all distinct, i.e. the restriction function $o_M \restriction \binom{[n]}{\leq d}$ is injective.

An $t \times n$ $\overline{d}$-separable matrix can be used as a non-adaptive group testing design that contains $t$ group tests to test $n$ items, which can detect the defective items from the test output if the number of defective items is assumed not more than $d$.

### Exercise

A $d$-disjunct matrix is $\overline{d}$-separable.

## Remark

1. $d$-disjunct matrices are also called $d$-cover-free families.
2. Group testing algorithms have applications in DNA library screening, information theory, cryptography, IC debugging, etc.
3. A non-adaptive group testing design is also called a Pooling design.

To construct a group testing design ( a $t \times n$ $d$-disjunct matrix), the following is considered:

1. test efficiency ($n$ is as large as possible);
2. usability ($d$ is as large as possible);
3. security (the rows weights are as large as possible).

To construct a group testing design ( a $t \times n$ $d$-disjunct matrix), the following is considered:

1. test efficiency ($n$ is as large as possible);
2. usability ($d$ is as large as possible);
3. security (the rows weights are as large as possible).

Since the sum of columns weights is the sum of rows weights, we also want the columns weights as large as possible.

To construct a group testing design ( a $t \times n$ $d$-disjunct matrix), the following is considered:

1. test efficiency ($n$ is as large as possible);
2. usability ($d$ is as large as possible);
3. security (the rows weights are as large as possible).

Since the sum of columns weights is the sum of rows weights, we also want the columns weights as large as possible.

We will see these requests do not always coincide with each other. Hence a compromise is necessary.

**Example**

The $n \times n$ identity matrix is $d$-disjunct for $d < n$.

## Example

The $n \times n$ identity matrix is $d$-disjunct for $d < n$.

Note that the matrix obtained from a $d$-disjunct matrix by deleting some columns is $d$-disjunct.

### Example

The $n \times n$ identity matrix is $d$-disjunct for $d < n$.

Note that the matrix obtained from a $d$-disjunct matrix by deleting some columns is $d$-disjunct.

### Definition

A $t \times n$ $d$-disjunct matrix is trivial if $n \leq t$.

## Exercise

Let $S$ be an antichain of $[N]$. Then the incidence matrix of $[N]$ and $S$ is 1-disjunct.

### Exercise

Let $S$ be an antichain of $[N]$. Then the incidence matrix of $[N]$ and $S$ is 1-disjunct.

### Theorem

*(Sperner 1928) Let $S$ be an antichain of $[N]$. Then* $|S| \le \binom{N}{\lfloor N/2 \rfloor}$.

### Exercise

Let $S$ be an antichain of $[N]$. Then the incidence matrix of $[N]$ and $S$ is 1-disjunct.

### Theorem

*(Sperner 1928) Let $S$ be an antichain of $[N]$. Then* $|S| \leq \binom{N}{\lfloor N/2 \rfloor}$.

### Exercise

(A. J. Macula, 1996) The incidence matrix of $\binom{[N]}{d}$ and $\binom{[N]}{k}$ is a $d$-disjunct matrix, where $d < k$.

# $d$-disjunct matrices with constant column weight $w$

Let $M$ be a $t \times n(d,t,w)$ $d$-disjunct matrix of constant column weight $w$.

**Theorem**

*(Erdös, Frankl and Füredi 1982)*

$$n(d,t,w) \leq \binom{t}{v} / \binom{w-1}{v-1},$$

*where* $v = \lceil w/d \rceil$.

# $d$-disjunct matrices with constant column weight $w$

Let $M$ be a $t \times n(d,t,w)$ $d$-disjunct matrix of constant column weight $w$.

**Theorem**

*(Erdös, Frankl and Füredi 1982)*

$$n(d,t,w) \le \binom{t}{v} \Big/ \binom{w-1}{v-1},$$

*where* $v = \lceil w/d \rceil$.

The equality is obtained in $w = 2d$ by using probabilistic method (Erdös, Frankl and Füredi 1985).

# $d$-disjunct matrices with constant column weight $w$

Let $M$ be a $t \times n(d,t,w)$ $d$-disjunct matrix of constant column weight $w$.

**Theorem**

*(Erdös, Frankl and Füredi 1982)*

$$n(d,t,w) \leq \binom{t}{v} \Big/ \binom{w-1}{v-1},$$

*where* $v = \lceil w/d \rceil$.

The equality is obtained in $w = 2d$ by using probabilistic method (Erdös, Frankl and Füredi 1985). We are interested in the case $w = d+1$.

# $d$-disjunct matrices with constant column weight $w$

Let $M$ be a $t \times n(d,t,w)$ $d$-disjunct matrix of constant column weight $w$.

**Theorem**

*(Erdös, Frankl and Füredi 1982)*

$$n(d,t,w) \leq \binom{t}{v} \Big/ \binom{w-1}{v-1},$$

*where* $v = \lceil w/d \rceil$.

The equality is obtained in $w = 2d$ by using probabilistic method (Erdös, Frankl and Füredi 1985). We are interested in the case $w = d+1$.

The EFF theorem implies

$$n(d,t,d+1) \leq \frac{t(t-1)}{2d}.$$

$M$ is nondegenerate if each row of $M$ has weight at least 2.

**Theorem**

*Suppose $M$ is nondegenerate. Then $n(d, t, d+1) \leq \frac{t(t-1)}{d(d+1)}$. Moreover equality holds iff $M$ is the points-blocks incidence matrix of a $2-(t, d+1, 1)$ design.*

$M$ is nondegenerate if each row of $M$ has weight at least 2.

## Theorem

*Suppose $M$ is nondegenerate. Then $n(d, t, d+1) \leq \frac{t(t-1)}{d(d+1)}$. Moreover equality holds iff $M$ is the points-blocks incidence matrix of a $2-(t, d+1, 1)$ design.*

## Proof.

1. Each row has at least two 1's;

$M$ is nondegenerate if each row of $M$ has weight at least 2.

## Theorem

*Suppose $M$ is nondegenerate. Then $n(d, t, d+1) \leq \frac{t(t-1)}{d(d+1)}$. Moreover equality holds iff $M$ is the points-blocks incidence matrix of a $2-(t, d+1, 1)$ design.*

## Proof.

1. Each row has at least two 1's;
2. Any two columns intersect at at most 1 row (Use $d$-disjunct and weight $d+1$ property);

$M$ is nondegenerate if each row of $M$ has weight at least 2.

### Theorem

*Suppose $M$ is nondegenerate. Then $n(d, t, d+1) \leq \frac{t(t-1)}{d(d+1)}$. Moreover equality holds iff $M$ is the points-blocks incidence matrix of a $2-(t, d+1, 1)$ design.*

### Proof.

1. Each row has at least two 1's;
2. Any two columns intersect at at most 1 row (Use $d$-disjunct and weight $d+1$ property);
3. Any two rows intersect at at most 1 column;

$M$ is nondegenerate if each row of $M$ has weight at least 2.

## Theorem

*Suppose $M$ is nondegenerate. Then $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$. Moreover equality holds iff $M$ is the points-blocks incidence matrix of a $2-(t,d+1,1)$ design.*

## Proof.

1. Each row has at least two 1's;
2. Any two columns intersect at at most 1 row (Use $d$-disjunct and weight $d+1$ property);
3. Any two rows intersect at at most 1 column;
4. $n(d,t,d+1)\binom{d+1}{2} \leq \binom{t}{2}$ (Counting elements in $\binom{[t]}{2}$ which are contained in some column).

$\square$

### Theorem

*If* $n(d,t,d+1) \geq t-1$ *then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

## Theorem

*If* $n(d,t,d+1) \geq t-1$ *then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

## Proof.

This is true if $M$ is nondegenerate. Assume $M$ is degenerate.

## Theorem

*If* $n(d,t,d+1) \geq t-1$ *then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

## Proof.

This is true if $M$ is nondegenerate. Assume $M$ is degenerate. Induction on $t$.

## Theorem

*If* $n(d,t,d+1) \geq t-1$ *then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

## Proof.

This is true if $M$ is nondegenerate. Assume $M$ is degenerate. Induction on $t$. Hence after rows permutation and columns permutation,

$M = \begin{pmatrix} * & 0 \\ * & M' \end{pmatrix}$, and by induction hypothesis we have

## Theorem

*If* $n(d,t,d+1) \geq t-1$ *then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

## Proof.

This is true if $M$ is nondegenerate. Assume $M$ is degenerate. Induction on $t$. Hence after rows permutation and columns permutation,
$M = \begin{pmatrix} * & 0 \\ * & M' \end{pmatrix}$, and by induction hypothesis we have

$$\begin{aligned} n-1 &\leq \frac{(t-1)(t-2)}{d(d+1)} \\ &\leq \frac{t(t-1)-2(t-1)}{d(d+1)} \\ &< \frac{t(t-1)-2d(d+1)+2}{d(d+1)} \\ &\leq \frac{t(t-1)}{d(d+1)} - 1. \end{aligned}$$

We have just shown

**Theorem**

*If* $n(d,t,d+1) \geq t-1$ *then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

We have just shown

### Theorem

*If* $n(d, t, d+1) \geq t-1$ *then* $n(d, t, d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

### Problem

Find a $t \times n(d, t, d+1)$ $d$-disjunct matrix of weight $d+1$ with

$$\frac{t(t-1)}{d(d+1)} < n(d, t, d+1) \leq t-2.$$

Note that this matrix is trivial $d$-disjunct in our definition, but it does not come by truncation of columns from a nontrivial constant weight $d$-disjunct matrix.

We have seen that

**Theorem**

*If* $n(d,t,d+1) \geq t-1$ *then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$, *in particular* $t \geq d(d+1)$.

We have seen that

**Theorem**

*If $n(d, t, d+1) \geq t-1$ then $n(d, t, d+1) \leq \frac{t(t-1)}{d(d+1)}$, in particular $t \geq d(d+1)$.*

Then for $t = d(d+1)$ we have

**Corollary**

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

We have seen that

**Theorem**

*Suppose $M$ is nondegenerate. Then* $n(d,t,d+1) \leq \frac{t(t-1)}{d(d+1)}$.

We have seen that

**Theorem**

*Suppose $M$ is nondegenerate. Then $n(d, t, d+1) \leq \frac{t(t-1)}{d(d+1)}$.*

Then for $t = (d+1)^2$ we have

**Corollary**

*Suppose $M$ is nondegenerate. Then $n(d, (d+1)^2, d+1) \leq (d+1)(d+2)$.*

We have just shown

**Corollary**

*Suppose $M$ is nondegenerate. Then* $n(d,(d+1)^2,d+1) \leq (d+1)(d+2)$.

The following example gives the equality.

We have just shown

**Corollary**

*Suppose $M$ is nondegenerate. Then $n(d, (d+1)^2, d+1) \leq (d+1)(d+2)$.*

The following example gives the equality.

**Example**

$(2-(q^2, q, 1)$ design$)$ Let $q$ be a prime power. The affine plane $F_q^2$ over $F_q$ has $q^2$ points and $q^2+q$ lines.

We have just shown

### Corollary

*Suppose M is nondegenerate. Then* $n(d, (d+1)^2, d+1) \leq (d+1)(d+2)$.

The following example gives the equality.

### Example

$(2-(q^2, q, 1)$ design$)$ Let $q$ be a prime power. The affine plane $F_q^2$ over $F_q$ has $q^2$ points and $q^2+q$ lines. Of course any line has $q$ points and any two lines intersect at at most 1 point.

We have just shown

### Corollary

*Suppose $M$ is nondegenerate. Then $n(d,(d+1)^2,d+1) \leq (d+1)(d+2)$.*

The following example gives the equality.

### Example

$(2-(q^2,q,1)$ design$)$ Let $q$ be a prime power. The affine plane $F_q^2$ over $F_q$ has $q^2$ points and $q^2+q$ lines. Of course any line has $q$ points and any two lines intersect at at most 1 point. Hence the points-lines incidence matrix is $t \times n$ $d$-disjunct with with constant weight $w$, where $t=q^2$, $n=q^2+q$ and $w=q=d+1$ satisfy

$$n = q^2+q = (d+1)(d+2).$$

We have just shown

### Corollary

*Suppose M is nondegenerate. Then* $n(d,(d+1)^2,d+1) \leq (d+1)(d+2)$.

The following example gives the equality.

### Example

$(2-(q^2,q,1)$ design$)$ Let $q$ be a prime power. The affine plane $F_q^2$ over $F_q$ has $q^2$ points and $q^2+q$ lines. Of course any line has $q$ points and any two lines intersect at at most 1 point. Hence the points-lines incidence matrix is $t \times n$ $d$-disjunct with with constant weight $w$, where $t=q^2$, $n=q^2+q$ and $w=q=d+1$ satisfy

$$n=q^2+q=(d+1)(d+2).$$

The first $q$ which is not a prime power is when $q=6=d+1$. In this case the equality does not hold.

# 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.

# Lines arrangement of a set $P$

Let $P$ be a set of $m \times u$ elements. We call an element of $P$ a point, and a $u$-subset of $P$ a *line*.

## Problem

Find a class $\mathcal{B}$ of lines in $P$ such that $|\mathcal{B}| > |P|$ and any two lines in $\mathcal{B}$ have at most one point of intersection.

# Lines arrangement of a set $P$

Let $P$ be a set of $m \times u$ elements. We call an element of $P$ a point, and a $u$-subset of $P$ a *line*.

**Problem**

Find a class $\mathcal{B}$ of lines in $P$ such that $|\mathcal{B}| > |P|$ and any two lines in $\mathcal{B}$ have at most one point of intersection.

Note that the incidence matrix of $P$ and $\mathcal{B}$ forms a nontrivial $(u-1)$-disjunct matrix of constant weight $u$.

# An example with $|P| = 6 \times 6$

吳欣融的答案 10/29/01

以11, 12, …, 16, 21, …, 26, …, 66代表36个元素。
以下是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 |

Designs, difference sets, finite geometries, probability methods, brute force are used in the construction $d$-disjunct matrices.

Designs, difference sets, finite geometries, probability methods, brute force are used in the construction $d$-disjunct matrices.

We will present a systematic way to realize the above example of *Wu* with 36 points and 37 lines, each line weight 6 and any two lines intersecting at at most 1 points.

We also construct $m(q+1)+1$ lines in a point set of $m(q+1)$ points, such that each line has weight $q+1$ and any two lines intersecting at at most 1 points, where $m \geq 2q-1$.

# 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 $F_q := \{0, a^0, a^1, \ldots, a^{q-2}\}$ 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 $F_q := \{0, a^0, a^1, \ldots, a^{q-2}\}$ 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 $F_q := \{0, a^0, a^1, \ldots, a^{q-2}\}$ 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 ${}_mT_q$

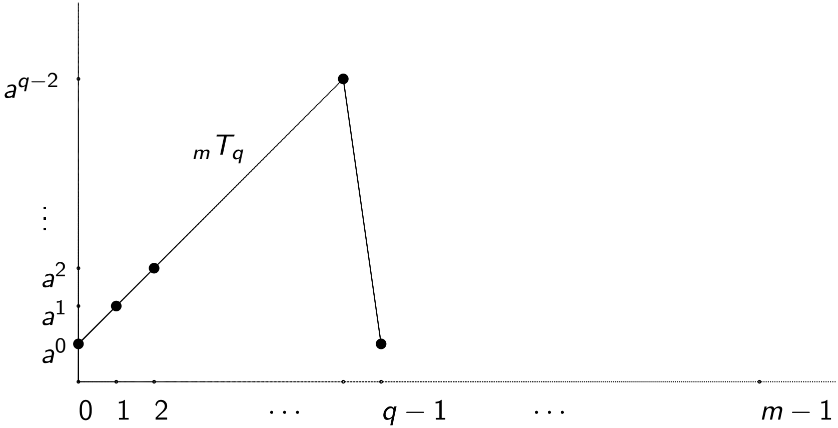
Let ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ be defined by

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

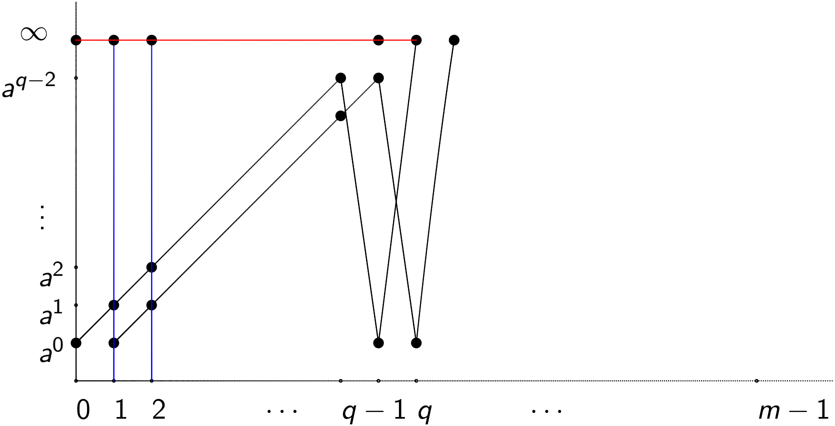
# The Set ${}_mT_q$

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

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

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

# ${}_mT_q$ 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.**

Given any pair $(c, d) \in \mathbb{Z}_m \times F_q$, solve the equations

$$(c, d) = (j, a^j) - (i, a^i)$$

for $0 \leq i < j \leq q - 1$.

# ${}_mT_q$ 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.**

Given any pair $(c, d) \in \mathbb{Z}_m \times F_q$, solve the equations

$$(c, d) = (j, a^j) - (i, a^i)$$

for $0 \leq i < j \leq q-1$. Note that $1 \leq c \leq q-1$ to have a solution.

# ${}_mT_q$ 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.**

Given any pair $(c, d) \in \mathbb{Z}_m \times F_q$, solve the equations

$$(c, d) = (j, a^j) - (i, a^i)$$

for $0 \leq i < j \leq q-1$. Note that $1 \leq c \leq q-1$ to have a solution. 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.**

Given any pair $(c, d) \in \mathbb{Z}_m \times F_q$, solve the equations

$$(c, d) = (j, a^j) - (i, a^i)$$

for $0 \leq i < j \leq q-1$. Note that $1 \leq c \leq q-1$ to have a solution. 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 $j = c+i$.

# ${}_mT_q$ 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.**

Given any pair $(c, d) \in \mathbb{Z}_m \times F_q$, solve the equations

$$(c, d) = (j, a^j) - (i, a^i)$$

for $0 \leq i < j \leq q - 1$. Note that $1 \leq c \leq q - 1$ to have a solution. 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 $(c, d) \in \mathbb{Z}_m \times F_q$. □

# 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

$$D_5 T_5 = \{ \begin{array}{l} (1,1),(1,2),(1,4),(1,3) \\ (2,3),(2,1),(2,2) \\ (3,2),(3,4) \\ (4,0) \quad \}. \end{array}$$

Hence

$$-D_5 T_5 = \{ \begin{array}{l} (4,4),(4,3),(4,1),(4,2) \\ (3,2),(3,4),(3,3) \\ (2,3),(2,1) \\ (1,0) \quad \}. \end{array}$$

# Non-example

We have seen

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

Hence

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

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

# Example

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

# Example

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

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

(The case $q = 3$) 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

(The case $q = 3$) 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

(The case $q = 3$) 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

(The case $q = 3$) Note that

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

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

# ${}_{2q-1}T_q$ 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 $-D_{{}_{2q-1}T_q} \cap D_{{}_{2q-1}T_q} = \emptyset$. $\square$

# 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. $\square$

# 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. □

Note that there are $mq$ lines and $mq$ points in $\mathbb{Z}_m \times F_q$, 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. $\square$

Note that there are $mq$ lines and $mq$ points in $\mathbb{Z}_m \times F_q$, 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 $(0, x) \notin -D_{{}_m T_q} \cup D_{{}_m T_q}$, we have $L \cap ((0, x) + L) = \emptyset$ for any nonzero $x \in F_q$ and $L \in \mathcal{B}$.

# 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).

# 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 $(i, \infty)$ to each line in a parallel class where $i \in \mathbb{Z}_m$ is first element (in the usual order) in $\mathbb{Z}_m$ not appearing in the first coordinate of any points of that 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 $(0, x) \notin -D_{{}_m T_q} \cup D_{{}_m T_q}$, 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 $(i, \infty)$ to each line in a parallel class where $i \in \mathbb{Z}_m$ is first element (in the usual order) in $\mathbb{Z}_m$ not appearing in the first coordinate of any points of that 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 $(i,\infty)$ to each line in a parallel class where $i \in \mathbb{Z}_m$ is first element (in the usual order) in $\mathbb{Z}_m$ not appearing in the first coordinate of any points of that 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 $0 \le i \le m-1$, and $V_i$ is called the $i$th vertical line. Set $H = \{(i, \infty) \mid 0 \le i \le q\}$ (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 $i$th 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

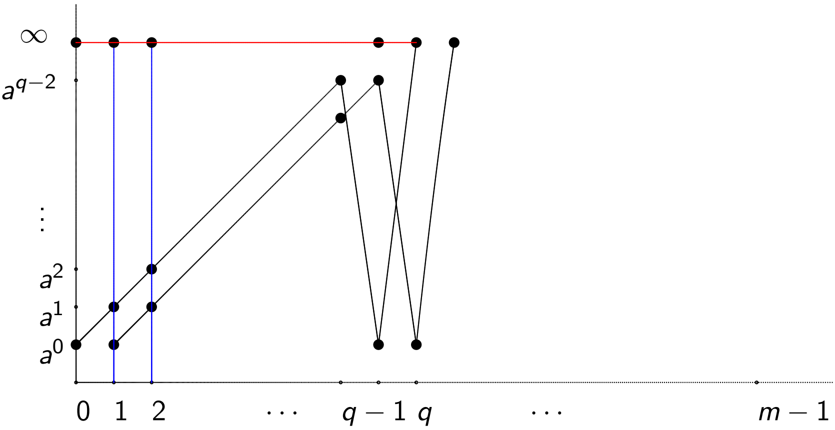
Suppose that ${}_mT_q \subseteq \mathbb{Z}_m \times F_q$ has the difference distinct property in $\mathbb{Z}_m \times F_q$, for example in the case $m \geq 2q-1$ or $m = q+1 = 6$.

# 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 and constant column weight $q+1$.

Note that in our construction each row has weight at least $q+1 = |{}_mT_q| + 1$.

# A Review of our result




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

# The end

Thank you for your attention.