From From t-wise balanced designs to orthogonal arrays

Don Kreher

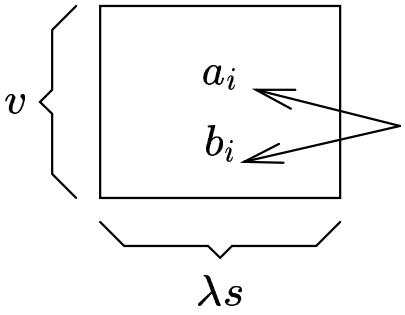
Michigan Technological University

kreher@mtu.edu

C.J. Colbourn and D.L. Kreher, Concerning difference matrices, *Designs, Codes and Cryptography*, **9**, 61-70 (1996).

D.L. Kreher, Orthogonal arrays of strength 3, *the Journal of Combinatorial Designs*, **4** (1995).

$(s, v; \lambda)$-Difference matrix based on the group G:

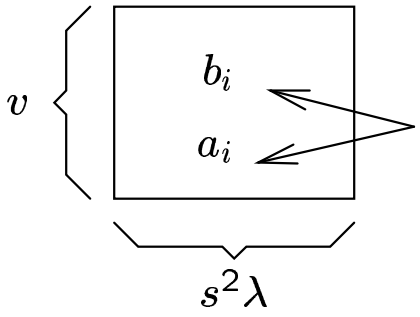


$\{a_i - b_i\} = \lambda G$, G Abelian.
$\{a_i b_i^{-1}\} = \lambda G$, G non-Abelian
$|G| = s$.

Example: $(3, 3; 1)$-difference matrix based on $\mathbb{Z}_3$

$$D = \begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{matrix}$$

OA$_\lambda(s, v)$ orthogonal Array:



$\{(a_i, b_i)\} = \lambda(X \times X)$
X a s-element set.

Example: $\mathrm{OA}_1(3,3)$

$$\underbrace{\begin{matrix}0&0&0\\0&1&2\\0&2&1\end{matrix}}_{D+0}\ \underbrace{\begin{matrix}1&1&1\\1&2&0\\1&0&2\end{matrix}}_{D+1}\ \underbrace{\begin{matrix}2&2&2\\2&0&1\\2&1&0\end{matrix}}_{D+2}$$

$(s, v; \lambda)$–Difference matrix $\Rightarrow$ $\mathrm{OA}_\lambda(s, v+1)$

Problem: Given s and λ what is the maximal v for which a $(s, v; \lambda)$-difference matrix exists?

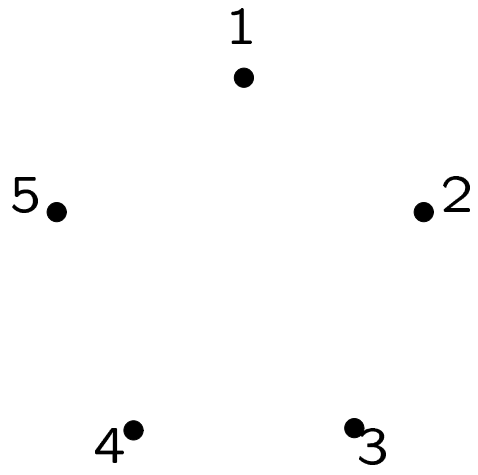
Upper and lower bounds on v

$\lambda \backslash s$	2	3	4	5	6
1	2	3	4	5	2
2	4	6	8	10	12 6
3	2	9	12	14 6	2
4	8	12	16	20	24 6
5	2	14 6	20 8	25	2
6	12	18	24 12	30 10	36 6
7	2	21 9	28 12	34 10	2
8	16	24	32	40 20	48 6
9	2	27	36	45 20	2
10	20	30	40 12	50	60 6

Data taken from forth coming book on orthogonal arrays by Hedayat, Sloane and Stufken.

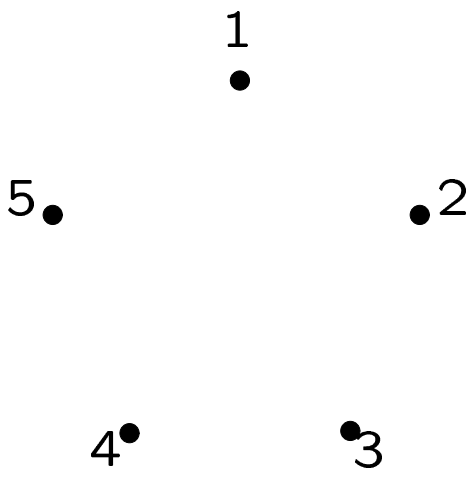
An ℓ by w PBD(v, λ) is a pair (X, A) where

- X is a v-element set of *points*;
- $\mathcal{A}$ is a w by ℓ array of subsets of X called *blocks*;
- every pair of points is in λ blocks; and
- the columns of A are partitions of X.

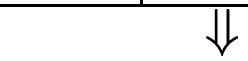


An

Example: A 4 by 3 PBD(5,1)

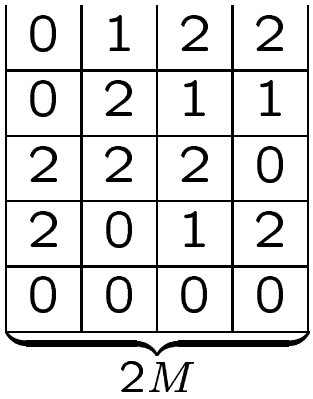


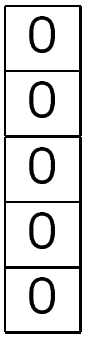
0	1 2 5	4 5	5	3 5
1	3 4	2 3	1 3	1 4
2	$\emptyset$	1	2 4	2

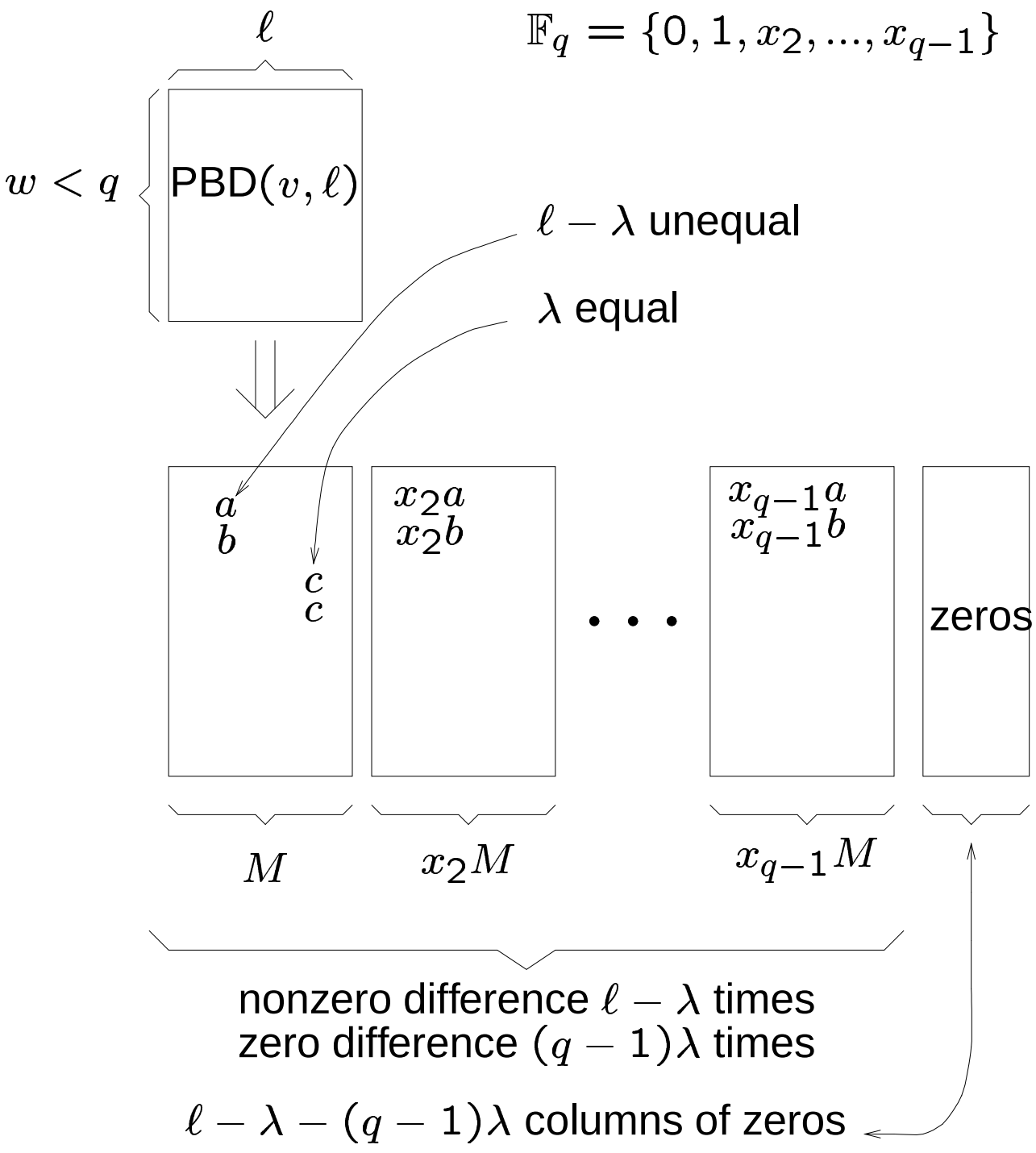


1	0	2	1	1
2	0	1	2	2
3	1	1	1	0
4	1	0	2	1
5	0	0	0	0

M


0 1 2 2
0 2 1 1
2 2 2 0
2 0 1 2
0 0 0 0
2M


0
0
0
0
0


ℓ
$\mathbb{F}_q = \{0, 1, x_2, ..., x_{q-1}\}$
$w < q$
PBD(v, ℓ)
$\ell - \lambda$ unequal
λ equal
a
b
c
c
$x_2 a$
$x_2 b$
$x_{q-1} a$
$x_{q-1} b$
zeros
M
$x_2 M$
$x_{q-1} M$
nonzero difference $\ell - \lambda$ times
zero difference $(q-1)\lambda$ times
$\ell - \lambda - (q-1)\lambda$ columns of zeros

Theorem 1 Let q be a prime power.

If there is an ℓ by w PBD(v, λ) with $w \leq q \leq \lfloor \frac{\ell}{\lambda} \rfloor$, then there exists a $(q, v; \ell - \lambda)$-difference matrix.

Theorem

Theorem 2. If an OA$(n, k; \lambda)$ exist with
λ constant rows, then over any group G of order $n+1$,
a $(n+1, k; \lambda(n-1))$-difference matrix exists.

Example. $G = \mathbb{Z}_4$

	1	1	1	2	2	2	3	3	3
	1	2	3	1	2	3	1	2	3
	1	2	3	3	1	2	2	3	1
	1	2	3	2	3	1	3	1	2

a	1	1	1	2	2	2	3	3	3
b	1	2	3	1	2	3	1	2	3
a-b	0	3	2	1	0	3	2	1	0

$\text{OA}_1(3,4) \Rightarrow (4,4;2)$-diff. matrix $\Rightarrow \text{OA}_2(4,5)$

Problem: Given s and λ what is the maximal v for which a (s, v, λ)–difference matrix exists?

Upper and lower bounds on v

$\lambda \backslash s$	2	3	4	5	6
1	2	3	4	5	2
2	4	6	8	10	12 6
3	2	9	12	14 6 7	2
4	8	12	16	20	24 6
5	2	14 6 7	20 8	25	2
6	12	18	24 12	30 10 17	36 6
7	2	21 9	28 12	34 10	2
8	16	24	32	40 20	48 6
9	2	27	36	45 20	2
10	20	30	40 12 13	50	60 6 11

Data taken from forth coming book on orthogonal arrays by Hedayat, Sloane and Stufken.

What's really going on?

1. We start with a matrix M with entries in $\mathbb{F}_q$
2. Multiply by the nonzeros

$$X \mapsto \alpha X$$

3. and then translate by all the elements of $\mathbb{F}_q$

$$X \mapsto \alpha X + \beta$$

But this is the affine group

$$\{X \mapsto \alpha X + \beta, \text{ where } \alpha, \beta \in \mathbb{F}_q, \alpha \neq 0\}$$

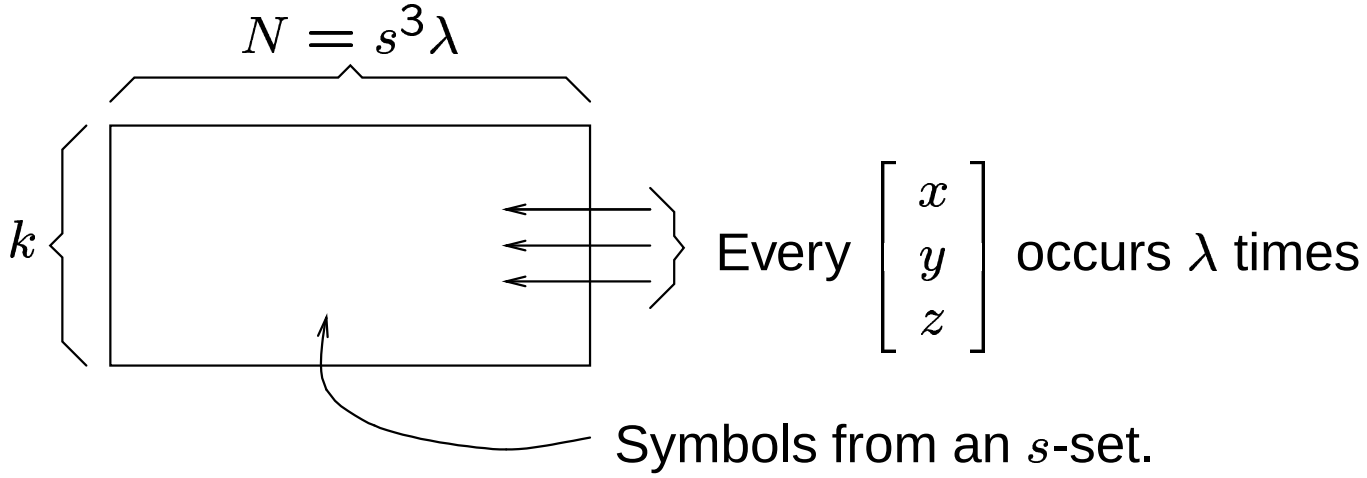
What’

This group has <u>two</u> orbits on order pairs namely:

(1) $\{(x,x) : x \in \mathbb{F}_q\}$

(2) $\{(x,y) : x,y \in \mathbb{F}_q, x \neq y\}$

Orthogonal array of size N, degree k, order s and strength 3: $OA_\lambda(3, k, s)$



Or

Example: An $OA_1(3, 4, 3)$

$$
\begin{array}{l}
000000000111111111222222222 \\
012012012012012012012012012 \\
012120201120201012201012120 \\
012201120120012201201120012
\end{array}
$$

Problem: Given s and λ what is the maximal k for which a $OA_\lambda(3, k, s)$ exists?

Existence results for orthogonal arrays of strength more than 2.

J. Bierbrauer and C.J. Colbourn, *Orthogonal arrays of strength more than two, The CRC Handbook of Combinatorial Designs.* C.J. Colbourn and J.H. Dinitz (Editors), CRC Press Boca Raton, 1996.

1. Bose-Bush (1952): $k \leq \left\lceil \frac{\lambda s^2 - 1}{s - 1} \right\rceil + 1$

2. An $OA_\lambda(t, k, s)$ is a $OA_{s\lambda}(t - 1, k, s)$.

3. A $OA_\lambda(t-1, k-1, s)$ can be obtained from a $OA_\lambda(t, k, s)$ by first selecting all columns that contain a fix symbol x in a given row i and then deleting row i.

4. Bush (1952): If $s > t$ is a prime power, then an $OA_1(t, s + 1, s)$ exists.

5. Bush (1952): If $s > 3$ is a power of 2, then an $OA_1(3, s + 2, s)$ exists.

6. Bush (1952): If $OA_{\lambda_1}(t, k, s_1)$ and $OA_{\lambda_2}(t, k, s_2)$ exists, then an $OA_{\lambda_1\lambda_2}(t, k, s_1 s_2)$ also exists.

7. Atsumi (1983): If t is even, then any $OA_{\lambda}(t, k, 2)$ implies the existence of an $OA_{\lambda}(t+1, k+1, 2)$. In particular an $OA_n(3, 4n, 2)$ exists whenever there is a Hadamard matrix of order 4n.

8. Bierbrauer-Mukhopadhyay (1995,1981):
If $m, n \geq 0$ are integers and p is a prime,
then a $OA_{p^{n(t-1)}}(t, p^{m+n}+1, p^m)$ exists for all $t \geq 3$
and an $OA_{p^{n(t-2)-m}}(t, pm+n, p^m)$ exists for all $t > p^n$.

9. Mukhopadhyay (1981):
If p is a prime and an $OA_{\lambda}(3, k, p^m)$ exists, then
a $OA_{\lambda p^{2(m+n)}}(3, kp^{m+n}, p^m)$ exists for all integers $n \geq 0$.

10. Mukhopadhyay (1981): If an $OA_{\lambda}(3, r, s)$ exists, so does an $OA_{s\lambda}(3, 2r, s)$.

A resolvable 3-(wk, k, λ) design is a pair (X, A) where

- X is a wk-element set of *points*;
- $\mathcal{A}$ is a ℓ by w array of k-subsets of X called *blocks*;
- every pair of points is in λ blocks; and
- the rows of A are partitions of X.

Example: A resolvable 3-$(8, 4, 1)$

1248	2358	3468	4578	5618	6728	7138
3567	4671	5712	6123	7234	1345	2456

A

Example: A resolvable 3-$(9, 3, 1)$

789	781	782	783	784	785	786	715	726	739	741	752	763	794	
124	235	346	459	561	692	913	826	839	841	852	863	894	815	$\cdots$
563	694	915	126	239	341	452	943	154	265	396	419	521	632	

	723	734	745	756	769	791	712	746	759	761	792	713	724	735
$\cdots$	845	856	869	891	812	823	834	925	136	249	351	462	593	614
	916	129	231	342	453	564	695	813	824	835	846	859	861	892

Let $\Omega = \{\omega_1, \omega_2, \ldots, \omega_{n+1}\}$, with $n + 1 \geq w$.

ω_1	789	781	782	783	784	785	786	715	726	739	
ω_2	124	235	346	459	561	692	913	826	839	841	$\cdots$
ω_3	563	694	915	126	239	341	452	943	154	265	

$\Downarrow$

1	ω_2	ω_1	ω_3	ω_3	ω_2	ω_3	ω_2	ω_1	ω_3	ω_2	
2	ω_2	ω_2	ω_1	ω_3	ω_3	ω_2	ω_3	ω_2	ω_1	ω_3	
3	ω_3	ω_2	ω_2	ω_1	ω_3	ω_3	ω_2	ω_3	ω_2	ω_1	
4	ω_2	ω_3	ω_2	ω_2	ω_1	ω_3	ω_3	ω_3	ω_3	ω_2	$\cdots$
5	ω_3	ω_2	ω_3	ω_2	ω_2	ω_1	ω_3	ω_1	ω_3	ω_3	
6	ω_3	ω_3	ω_2	ω_3	ω_2	ω_2	ω_1	ω_2	ω_1	ω_3	
7	ω_1	ω_1	ω_1	ω_1	ω_1	ω_1	ω_1	ω_1	ω_1	ω_1	
8	ω_1	ω_1	ω_1	ω_1	ω_1	ω_1	ω_1	ω_2	ω_2	ω_2	
9	ω_1	ω_3	ω_3	ω_2	ω_3	ω_2	ω_2	ω_3	ω_2	ω_1	

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{M}$

Let G be a group acting 3-transitively on Ω

$G = \{g_1, g_2, \ldots, g_{|G|}\}$

$|G| = m(n+1)n(n-1) = m(n^3 - n)$.

$M^G = [M^{g_1}, M^{g_2}, \ldots, M^{g_{|G|}}]$

$C =$ each constant column repeated x times.
(v by $x(n+1)$ matrix)

The number of blocks containing a pair of points disjoint from a third is $b_2^1 = \binom{v-3}{k-2}\lambda / \binom{v-t}{k-1}$.

Claim $[M^G, C]$ is an orthogonal array.

Consider any three rows

Type	in M	in M^G	in C	Total
x x x	λ	$\frac{\lvert G\rvert}{n+1}\lambda$	x	$x + mn(n-1)\lambda$
x x y	b_2^1	$\frac{\lvert G\rvert}{(n+1)n}b_2^1$	0	$mb_2^1(n-1)$
x y x	b_2^1	$\frac{\lvert G\rvert}{(n+1)n}b_2^1$	0	$mb_2^1(n-1)$
y x x	b_2^1	$\frac{\lvert G\rvert}{(n+1)n}b_2^1$	0	$mb_2^1(n-1)$
x y z	$r-\lambda-3b_2^1$	$\frac{\lvert G\rvert(r-\lambda-3b_2^1)}{(n+1)n(n-1)}$	0	$m(r-\lambda-3b_2^1)$

Choose n and x so that

1. $m(r - \lambda - 3b_2^1) = mb_2^1(n-1)$
2. $n + 1 \geq w$.
3. $x + mn(n-1)\lambda = mb_2^1(n-1)$

Choose

Theorem. Let G act 3-transitively on the $(n+1)$-set Ω and let $m(n^3-n)$ be the order of G. If a resolvable 3-(wk, k, λ) design $(X, \mathcal{B})$ exists such that

1. $n = (r-\lambda)/b_2^1 - 2$
2. $n+1 \geq w$
3. $n \leq b_2^1/\lambda$,

then an $OA_{mb_2^1(n-1)}(3, wk, n+1)$ also exists.

Use $G = PGL(2,q)$ on $\Omega = \mathbb{F}(q) \cup \{\infty\}$ and resolvable SQS(3q+5)'s.

Corollary A.
Let q be a prime power, $q \equiv 1, 5, 9 \pmod{12}$.
Then there exists an

$$OA_{(3q+1)(q-1)/2}(3, 3q+5, q+1),$$

except possibly for $q = 197$ or 773.

Use

Use $G = PGL(2, q)$ on $\Omega = \mathbb{F}(q) \cup \{\infty\}$ and resolvable 3-$(2q + 4, 3, 1)$.

Corollary B.
Let q be a prime power, $q \equiv 1 \pmod 3$.
Then there exists an

$$OA_{(2q+1)(q-1)}(3, 2q + 4, q + 1).$$

We don’t need 3-designs!

All that is required is a resolvable set-system $(X, \mathcal{B})$ such that

1. The number of blocks containing three points x, y, z is a constant λ that does not depend on the choice of x, y, z

2. The number of blocks containing two points x, y and disjoint from a third point $z \in X$, is a constant b_2^1 that does not depend on the choice of x, y, z

W

Do they exist? Can they be resolvable?

Example: The 1-factorization of the complete graph is a resolvable near 3-design with

$$\lambda = 0 \qquad \text{and} \qquad b_2^1 = 1$$

Example:

The revised theorem is:

Theorem: Let G act 3-transitively on the $(n+1)$-element set Ω and let $m(n^3-n)$ be the order of G. If a resolvable near 3-design $(X, \mathcal{B})$ exists such that $n = (r-\lambda)/b_2^1 - 2$ with $w - 1 \leq n \leq b_2^1/\lambda$, then a resolvable $OA_{mb_2^1(n-1)}(3, |X|, n+1)$ also exists.

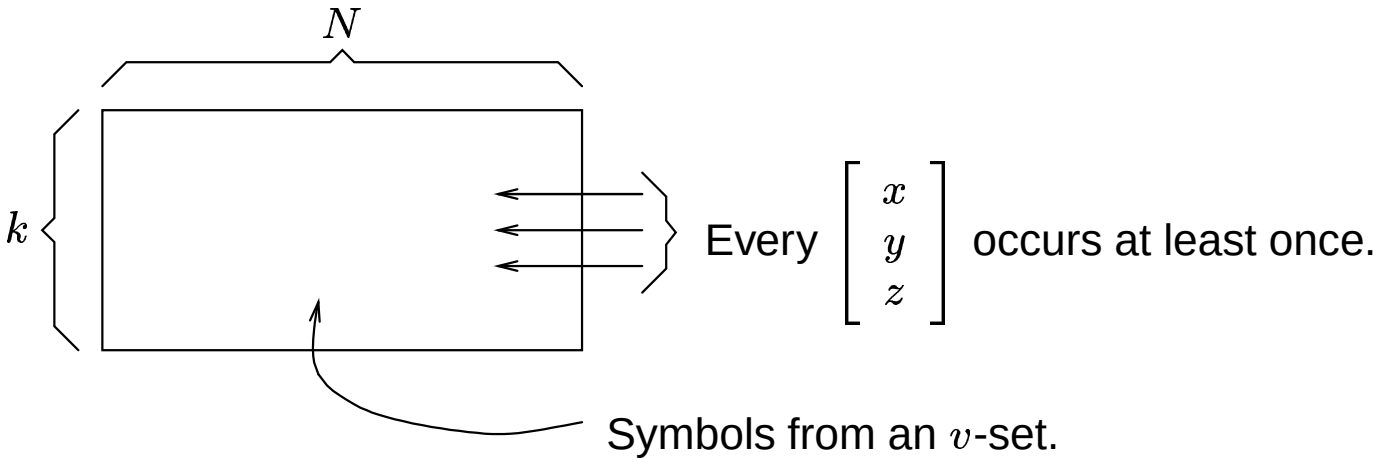
Example:

Corollary: Let q be an odd prime power. Then there exists an $OA_{q-1}(3, q+3, q+1)$.

Proof: Use 1-factorization of K_{q+3} and $GL_2(q)$.

The same methods can be used to construct covering arrays.

A Covering array of size N, degree k, order v and strength 3: $CA(N, 3, k, v)$



Example: Use a 1-factorization of K_6 and the group S_3 to obtain an optimal covering array: $CA(33, 3, 6, 3)$.

0 1 2 2 1	1 2 0 0 2	2 0 1 1 0	0 2 1 1 2	1 0 2 2 0	2 1 0 0 1	0 1 2
1 2 2 1 0	2 0 0 2 1	0 1 1 0 2	2 1 1 2 0	0 2 2 0 1	1 0 0 1 2	0 1 2
2 2 1 0 1	0 0 2 1 2	1 1 0 2 0	1 1 2 0 2	2 2 0 1 0	0 0 1 2 1	0 1 2
2 1 0 1 2	0 2 1 2 0	1 0 2 0 1	1 2 0 2 1	2 0 1 0 2	0 1 2 1 0	0 1 2
1 0 1 2 2	2 1 2 0 0	0 2 0 1 1	2 0 2 1 1	0 1 0 2 2	1 2 1 0 0	0 1 2
0 0 0 0 0	1 1 1 1 1	2 2 2 2 2	0 0 0 0 0	1 1 1 1 1	2 2 2 2 2	0 1 2

We also obtain a $CA(88, 3, 8, 4)$ from a 1-factorization of K_8 and the group A_4. This is best known, but may not be optimal.

This is work in progress with: M.A. Chateauneuf and C.J. Colbourn

CHAPTER **1**

FUNDAMENTALS OF COMBINATORIAL MATHEMATICS

1. What is combinatorial mathematics? Combinatorial mathematics also referred to as combinatorial analysis or combinatorics, is a mathematical discipline that began in ancient times. According to legend the Chinese Emperor Yu (C. 2200 B.C.) observed the magic square

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix}$$

on the shell of a divine turtle. ...

– H.J. Ryser,*Combinatorial Mathematics*, C.M. 14 (1963).

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} + 3 \begin{bmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix}$$