Covering arrays of strength 3

Don Kreher

Michigan Technological University

kreher@mtu.edu

- C.J. Colbourn and D.L. Kreher, Concerning difference matrices, *Designs, Codes and Cryptography*, **9**, 67-70 (1996).

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

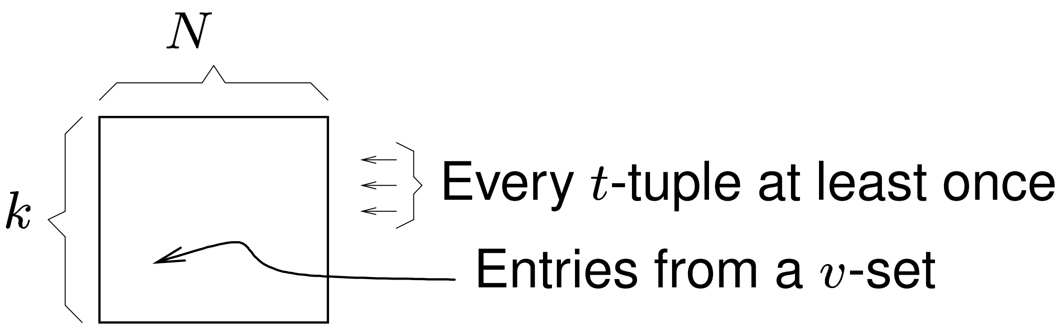
⇒ M.A. Chateauneuf, C.J. Colbourn and D.L.Kreher, Covering arrays of strength 3, *Designs Codes and Cryptography*, **16**, 235-242 (1999).

- C.J. Colbourn and D. L.Kreher, J. P. McSorley, and D.R. Stinson, Orthogonal Arrays of Strength 3 from 3–designs *submited*.

Y2K
Compliant

A Covering array $CA(N; t, k, v)$ of

size N, strength t, degree k and order v is



Example: A $CA(11, 2, 5, 3)$

$$\boxed{\begin{array}{ccccccccccc}
1&0&2&1&2&2&2&1&0&1&0\\
2&2&1&1&0&1&2&0&1&2&0\\
2&1&2&0&1&1&0&2&2&1&0\\
1&2&0&2&1&2&1&2&1&0&0\\
0&1&1&2&2&0&1&1&2&2&0
\end{array}}$$

$CAN(t, k, v) = \min\{N :$ there is a $CA(N, t, k, v)\}$.

So, $CAN(2, 5, 3) \leq 11$.

What's known for $t = 2$, $v = 2$

Katona 1973, Kleitman & Spencer 1973:

$$
k = \binom{N-1}{\lceil \frac{N}{2} \rceil} \left\{ \begin{array}{c c}
 & \overbrace{}^{N-1} \\
\boxed{\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{array}} & \boxed{\begin{array}{c} 00111 \\ 01011 \\ 10011 \\ 01101 \\ 10101 \\ 11001 \\ 01110 \\ 10110 \\ 11010 \\ 11100 \end{array}}
\end{array} \right. \leftarrow \left\{ \begin{array}{l} \lceil \frac{N}{2} \rceil\text{-subsets} \\ \text{of an } N-1\text{-set} \end{array} \right.
$$

This is optimal and for k large it implies

$$
N = \log k + \frac{1}{2} \log \log k \cdots
$$

What's known for $t = 2$, $v > 2$

Gargano, Körner, Vaccaro 1990:

$$N = \frac{v}{2} \log k(1 + o(1))$$

Probabilistic — No explicit construction !

Only a few exact values are known.

For $t = 2$, $v = 3$:

k :	2	3	4	5	6	$7-12$	$13-16$	$\cdots$
N :	9	9	9	11	≤ 12	≤ 15	≤ 18	$\cdots$

Östegård

What's known for $t = 3$, $v = 2$

$$\underbrace{3.2\ldots \log k(1+o(1))}_{\text{Klietman \& Spencer 1973}} < CAN(3,k,2) < \underbrace{7.5\ldots \log k(1+o(1))}_{\text{Roux 1987}}$$

Probabilistic — No explicit construction !

Only a few exact values are known.

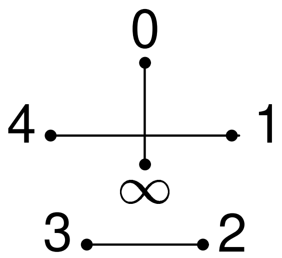
$$\begin{array}{l|ccccccc} k & 3 & 4 & 5 & 6-11 & 12-14 & 16 & \cdots \\ \hline N & 8 & 8 & 10 & 12 & \le 16 & \le 17 & \cdots \end{array}$$

$$\overbrace{\qquad\uparrow\qquad}^{}$$
Kreher & Tonchev

A table of bounds for $k < 1,771,561$ is given in the survey:

N. Sloane, Covering Arrays and Intersecting Codes, *JCD* **1, 51-63 (1993).**

Two Small Constructions



Constructing a $CA(33;3,6,3)$.

<u>Step 1</u>

$0 \to$	$0 - \infty$	$1 - \infty$	$2 - \infty$	$3 - \infty$	$4 - \infty$
$1 \to$	$1 - 4$	$2 - 0$	$3 - 1$	$4 - 2$	$0 - 3$
$2 \to$	$2 - 3$	$3 - 4$	$4 - 0$	$0 - 1$	$1 - 2$

0	0	1	2	2	1
1	1	0	1	2	2
2	2	1	0	1	2
3	2	2	1	0	1
4	1	2	2	1	0
∞	0	0	0	0	0

We get a starter array M

Step 2

Let $G = \text{Sym}\{0, 1, 2\}$ and apply G to M

$$[M^G, C] = [M^{g_1}, M^{g_2}, M^{g_3}, M^{g_4}, M^{g_5}, M^{g_6}, C]$$

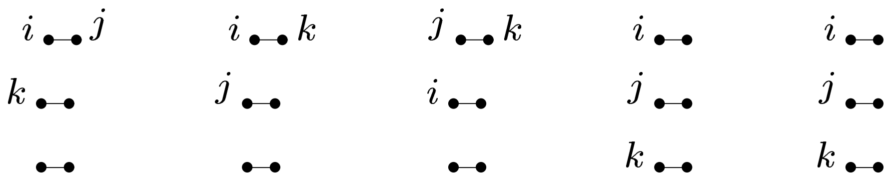
.

$(0)(1)(2)$	$(0,1,2)$	$(0,2,1)$	$(1,2)$	$(0,1)$	$(0,2)$	
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
						C

On 3-tuples G has 5 orbits:

1. $\{(x,x,y) : x \neq y\}$
2. $\{(x,y,x) : x \neq y\}$
3. $\{(y,x,x) : x \neq y\}$
4. $\{(x,y,z) : x \neq y \neq z \neq x\}$
5. $\{(x,x,x) : x \neq y \neq z \neq x\}$

Consider any 3 rows $i,j,k \in \{0,1,2,3,4,\infty\}$.



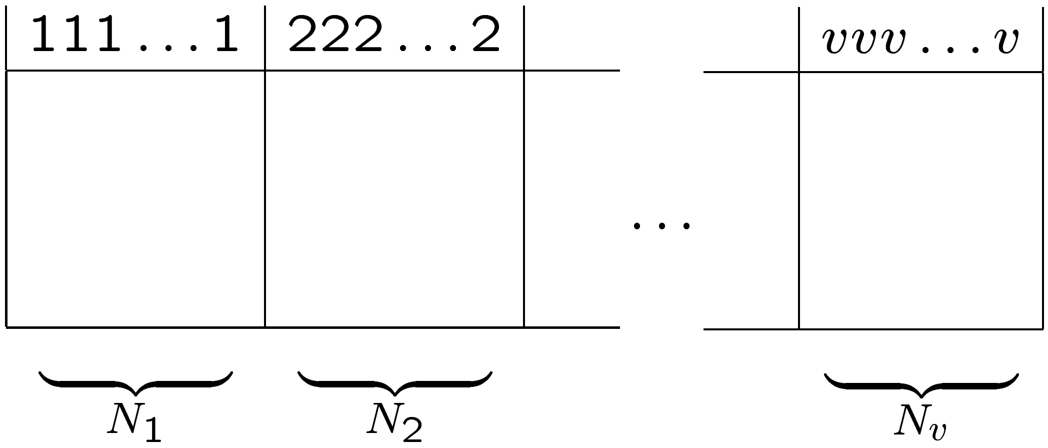
$$\begin{array}{cccccc}
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
i \rightarrow & \mathrm{x} & \mathrm{x} & \mathrm{y} & \mathrm{x} & \mathrm{x} \\
j \rightarrow & \mathrm{x} & \mathrm{y} & \mathrm{x} & \mathrm{y} & \mathrm{y} \\
k \rightarrow & \mathrm{y} & \mathrm{x} & \mathrm{x} & \mathrm{z} & \mathrm{z}
\end{array}$$

Therefore $[M^G, C]$ is a $CA(33;3,6,3)$.

Theorem.

$$CAN(t,k,v) \geq v \cdot CAN(t-1,k-1,v)$$

proof.



Each are $CA(N_i; t-1, k-1, v)$. []

So,

$$\underbrace{33 \geq CAN(3,6,3)}_{\text{construction}} \underbrace{\geq 3 \cdot CAN(2,5,3)}_{\text{Theorem}} = 3 \cdot \underbrace{11}_{\text{Östegård}} = 33$$

Theorem. $CAN(3,6,3) = 33$

Constructing a $CA(84; 3, 8, 4)$.

<u>Step 1</u>

Get one-factorization of K_8 with vertex set

$$\begin{aligned} \mathrm{GF}(8) &= \mathbb{Z}_2[X]/(x^3 + x + 1) \\ &= \{0, 1, x, x^2, x^3, \ldots, x^7\}. \end{aligned}$$

$0 \rightarrow$	$0 \bullet\!\!-\!\!\bullet x^0$	$0 \bullet\!\!-\!\!\bullet x^1$	$0 \bullet\!\!-\!\!\bullet x^2$	$0 \bullet\!\!-\!\!\bullet x^3$	$0 \bullet\!\!-\!\!\bullet x^4$	$0 \bullet\!\!-\!\!\bullet x^5$	$0 \bullet\!\!-\!\!\bullet x^6$
$1 \rightarrow$	$x^1 \bullet\!\!-\!\!\bullet x^3$	$x^2 \bullet\!\!-\!\!\bullet x^4$	$x^3 \bullet\!\!-\!\!\bullet x^5$	$x^4 \bullet\!\!-\!\!\bullet x^6$	$x^5 \bullet\!\!-\!\!\bullet x^0$	$x^6 \bullet\!\!-\!\!\bullet x^1$	$x^0 \bullet\!\!-\!\!\bullet x^2$
$2 \rightarrow$	$x^2 \bullet\!\!-\!\!\bullet x^6$	$x^3 \bullet\!\!-\!\!\bullet x^0$	$x^4 \bullet\!\!-\!\!\bullet x^1$	$x^5 \bullet\!\!-\!\!\bullet x^2$	$x^6 \bullet\!\!-\!\!\bullet x^3$	$x^0 \bullet\!\!-\!\!\bullet x^4$	$x^1 \bullet\!\!-\!\!\bullet x^5$
$3 \rightarrow$	$x^4 \bullet\!\!-\!\!\bullet x^5$	$x^5 \bullet\!\!-\!\!\bullet x^6$	$x^6 \bullet\!\!-\!\!\bullet x^0$	$x^0 \bullet\!\!-\!\!\bullet x^1$	$x^1 \bullet\!\!-\!\!\bullet x^2$	$x^2 \bullet\!\!-\!\!\bullet x^3$	$x^3 \bullet\!\!-\!\!\bullet x^4$

0	0	0	0	0	0	0	0
x^0	0	2	3	3	1	2	1
x^1	1	0	2	3	3	1	2
x^2	2	1	0	2	3	3	1
x^3	1	2	1	0	2	3	3
x^4	3	1	2	1	0	2	3
x^5	3	3	1	2	1	0	2
x^6	2	3	3	1	2	1	0

We get a starter array M

Step 2

Let $G = \text{Alt}\{0,1,2,3\}$ and apply G to M

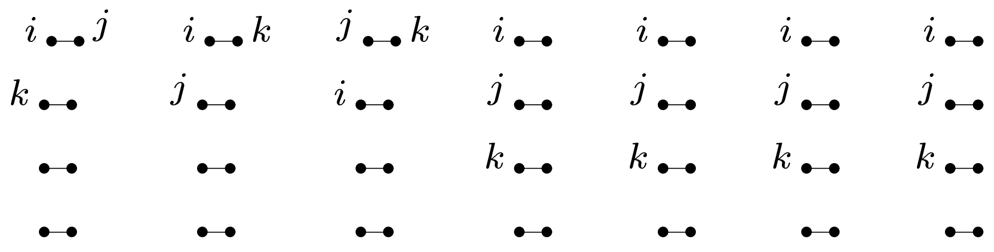
$$[M^G, C] = [M^{g_1}, M^{g_2}, M^{g_3}, \ldots, M^{g_{12}}, C]$$

Here $C = \left.\boxed{\begin{array}{c} 0\,1\,2\,3 \\ 0\,1\,2\,3 \\ \vdots \\ 0\,1\,2\,3 \end{array}}\right\}$ 8 rows

On 3-tuples G has 6 orbits:

1. $\{(x,x,y) : x \neq y\}$
2. $\{(x,y,x) : x \neq y\}$
3. $\{(y,x,x) : x \neq y\}$
4. $\{(x,y,z) : x \neq y \neq z \neq x\}$ Two orbits
5. $\{(x,x,x) : x \neq y \neq z \neq x\}$

Consider any 3 rows $i, j, k \in \{0, 1, x^1, x^2, \ldots, x^6\}$.



$$
\begin{array}{cccccccc}
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
i \rightarrow & \text{x} & \text{x} & \text{y} & \text{x} & \text{x} & \text{x} & \text{x} \\
j \rightarrow & \text{x} & \text{y} & \text{x} & \text{y} & \text{y} & \text{y} & \text{y} \\
k \rightarrow & \text{y} & \text{x} & \text{x} & \text{z} & \text{z} & \text{z} & \text{z}
\end{array}
$$

$$\underbrace{\hspace{4cm}}_{\text{4 chances}}$$

So this works.

Theorem.

$$CAN(3, 8, 4) \leq 7 * 12 + 4 = 88$$

Corollary.

$$CAN(2, 7, 4) \leq 22$$

Sample

On rows x^2, x^4, x^5 we get:

even=(0,3,2)

Bummer!

2	1	0	2	3	3	1
3	1	2	1	0	2	3
3	3	1	2	1	0	2

odd=(0,3,1,2)

Yea!

Using the affine group

$$AF(q) = \{x \mapsto \alpha x + \beta, \alpha, \beta \in GF(q), \alpha \neq \beta\}$$

could lead to $CAN(3, 2q, q) \leq (2q-1)q^2$,
but ..... it still eludes us.

The next case $q = 5$: The are 396 one-factorizations of K_{10}.

One-factorization of K_{10} has 9 one-factors.

One-factor's labeled by $GF(5) = \mathbb{Z}_5$ in $5! = 120$ ways.

Search space has size $120^9 \approx 2^{62}$. Too big!

Staszek observes, we use $G = AF(5)$ as automorphism group.

Only $6 = 120/(5 \cdot 4)$ cosets of $AF(5)$ in $Sym(5)$.

Search space is only of size $6^9 \approx 2^{23}$. . . . . Feasible!

The unique solutions is:

$$M = \begin{array}{|ccccccccc|}
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 3 & 4 & 2 & 4 & 3 & 2 \\
1 & 1 & 0 & 4 & 3 & 4 & 2 & 2 & 3 \\
3 & 4 & 2 & 0 & 1 & 2 & 3 & 4 & 3 \\
3 & 2 & 4 & 1 & 0 & 3 & 2 & 3 & 4 \\
2 & 4 & 3 & 3 & 2 & 0 & 1 & 2 & 4 \\
2 & 3 & 4 & 2 & 3 & 1 & 0 & 4 & 2 \\
4 & 2 & 3 & 2 & 4 & 4 & 3 & 0 & 1 \\
4 & 3 & 2 & 4 & 2 & 3 & 4 & 1 & 0 \\
\hline
\end{array}$$

$[M^G, C]$ is a $CA(185; 3, 10, 5)$. Way cool!

Permuting rows and columns we get

$$
M = \begin{array}{|c|cc|cc|cc|cc|}
\hline
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
1 & 1 & 0 & 4 & 2 & 2 & 3 & 4 & 3 \\
1 & 0 & 1 & 2 & 4 & 3 & 2 & 3 & 4 \\
\hline
2 & 3 & 4 & 1 & 0 & 4 & 2 & 2 & 3 \\
2 & 4 & 3 & 0 & 1 & 2 & 4 & 3 & 2 \\
\hline
4 & 3 & 2 & 3 & 4 & 1 & 0 & 4 & 2 \\
4 & 2 & 3 & 4 & 3 & 0 & 1 & 2 & 4 \\
\hline
3 & 2 & 4 & 3 & 2 & 3 & 4 & 1 & 0 \\
3 & 4 & 2 & 2 & 3 & 4 & 3 & 0 & 1 \\
\hline
\end{array}
$$

This has the form

$$
\begin{array}{|c|c|c|c|c|}
\hline
\begin{array}{c} 0 \\ 0 \end{array} & B & B & B & B \\
\hline
\begin{array}{c} \alpha \\ \alpha \end{array} & I & A_1 & A_2 & A_3 \\
\hline
\begin{array}{c} \alpha^2 \\ \alpha^2 \end{array} & \bar{A}_3 & I & A_1 & A_2 \\
\hline
\begin{array}{c} \alpha^3 \\ \alpha^3 \end{array} & \bar{A}_2 & \bar{A}_3 & I & A_1 \\
\hline
\begin{array}{c} \alpha^4 \\ \alpha^4 \end{array} & \bar{A}_1 & \bar{A}_2 & \bar{A}_3 & I \\
\hline
\end{array}
$$

Choosing different representatives and adding column of 0s

$$M = \begin{array}{|cc|cc|cc|cc|cc|}
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 2 & 2 & 4 & 4 & 3 & 3 \\
\hline
0 & 1 & 1 & 0 & 3 & 4 & 3 & 2 & 2 & 4 \\
0 & 1 & 0 & 1 & 4 & 3 & 2 & 3 & 4 & 2 \\
\hline
0 & 2 & 3 & 4 & 2 & 0 & 1 & 3 & 1 & 4 \\
0 & 2 & 4 & 3 & 0 & 2 & 3 & 1 & 4 & 1 \\
\hline
0 & 4 & 3 & 2 & 1 & 3 & 4 & 0 & 2 & 1 \\
0 & 4 & 2 & 3 & 3 & 1 & 0 & 4 & 1 & 2 \\
\hline
0 & 3 & 2 & 4 & 1 & 4 & 2 & 1 & 3 & 0 \\
0 & 3 & 4 & 2 & 4 & 1 & 1 & 2 & 0 & 3 \\
\hline
\end{array}$$

Which is symmetric

Using Gargano, Körner, Vaccaro result for k we have

$$CAN(2,k,v) = \frac{v}{2}\log(k(1+o(1))$$

so the recursive upper bound suggest that

$$CAN(3,k+1,v) \leq \frac{v^2}{2}\log(k(1+o(1))$$

Using perfect hash families and orthogonal arrays instead of starter arrays and groups we can get using a result of Atici,Magliveras, Stinson and Wei:

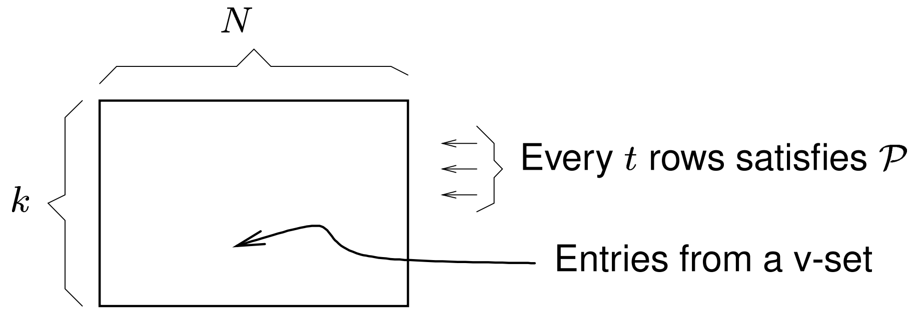
$$CAN(3,5^{2^j},v) \leq 3\cdot 4^j v^3, \text{ for all } j$$

So

$$CAN(3,k,v) \leq \frac{3v^3}{(\log 5)^2}(\log k)^2, \text{when } k = 5^{2^j}$$

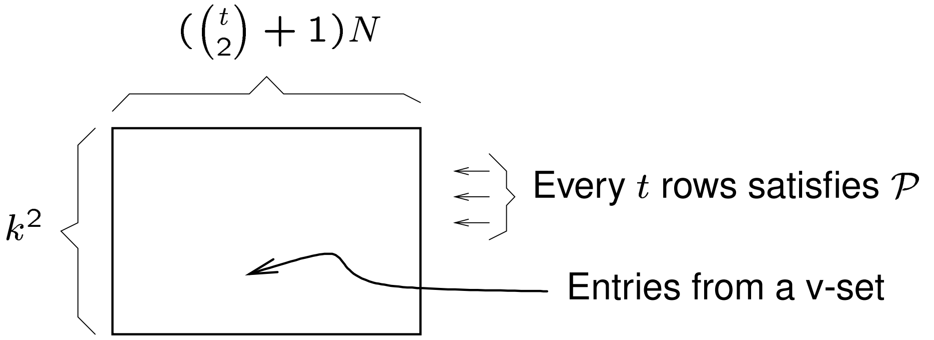
What Atici, Magilveras, Stinson and Wei really prove is:

Let $A =$



where $\mathcal{P}$ is a property that does not depend on the ordering of the t rows and $\gcd(k, \binom{t}{2}!) = 1$, then there is an array B such that

$B =$



There is a $CA(33; 3, 5, 3)$.

$$\begin{aligned}\Rightarrow CA(33 \cdot 4; 3, 5^2, 3) \quad &\Rightarrow \quad CA(33 \cdot 4^2; 3, 5^{2^2}, 3) \\ &\Rightarrow \quad CA(33 \cdot 4^3; 3, 5^{2^3}, 3) \\ &\Rightarrow \quad \cdots \Rightarrow CA(33 \cdot 4^j; 3, 5^{2^j}, 3)\end{aligned}$$

So

$$CAN(3, k, 3) \leq \frac{33}{(\log 5)^2}(\log k)^2 \approx 6.12(\log k)^2$$

when $k = 5^{2^j}$.