Mutually Orthogonal Latin Squares: Covering and Packing Analogues

Charles J. Colbourn[1]

[1]School of Computing, Informatics, and Decision Systems Engineering
Arizona State University

Mile High Conference, 15 August 2013

Latin Squares

Definition

A *latin square* of *side* n (or *order* n) is an $n \times n$ array in which each cell contains a single symbol from an n-set S, such that each symbol occurs exactly once in each row and exactly once in each column.

1	0	3	4	5	6	7	2
2	3	5	0	6	7	4	1
0	1	2	3	4	5	6	7
3	4	0	7	1	2	5	6
4	5	6	1	7	0	2	3
5	6	7	2	0	3	1	4
6	7	4	5	2	1	3	0
7	2	1	6	3	4	0	5

Latin Squares

Definition

A *latin square* of *side* n (or *order* n) is an $n \times n$ array in which each cell contains a single symbol from an n-set S, such that each symbol occurs exactly once in each row and exactly once in each column.

1	0	3	4	5	6	7	2
2	3	5	0	6	7	4	1
0	1	2	3	4	5	6	7
3	4	0	7	1	2	5	6
4	5	6	1	7	0	2	3
5	6	7	2	0	3	1	4
6	7	4	5	2	1	3	0
7	2	1	6	3	4	0	5

Latin Squares

- Applying any permutation to the rows yields a latin square.
- The same for columns, and for symbols.

Mutually Orthogonal Latin Squares

Definition

Two latin squares L and L' of the same order are *orthogonal* if $L(a, b) = L(c, d)$ and $L'(a, b) = L'(c, d)$, implies $a = c$ and $b = d$.

An equivalent definition for orthogonality: Two latin squares of side n, $L = (a_{i,j})$ (on symbol set S) and $L' = (b_{i,j})$ (on symbol set S'), are *orthogonal* if every element in $S \times S'$ occurs exactly once among the n^2 pairs $(a_{i,j}, b_{i,j})$, $1 \leq i, j \leq n$.

Definition

A set of latin squares $L_1, \ldots, L_m$ is *mutually orthogonal*, or a set of *MOLS*, if for every $1 \leq i < j \leq m$, L_i and L_j are orthogonal. These are also referred to as *POLS*, *pairwise orthogonal* latin squares.

Mutually Orthogonal Latin Squares

Definition

Two latin squares L and L' of the same order are *orthogonal* if $L(a, b) = L(c, d)$ and $L'(a, b) = L'(c, d)$, implies $a = c$ and $b = d$.

An equivalent definition for orthogonality: Two latin squares of side n, $L = (a_{i,j})$ (on symbol set S) and $L' = (b_{i,j})$ (on symbol set S'), are *orthogonal* if every element in $S \times S'$ occurs exactly once among the n^2 pairs $(a_{i,j}, b_{i,j})$, $1 \leq i, j \leq n$.

Definition

A set of latin squares $L_1, \ldots, L_m$ is *mutually orthogonal*, or a set of *MOLS*, if for every $1 \leq i < j \leq m$, L_i and L_j are orthogonal. These are also referred to as *POLS*, *pairwise orthogonal* latin squares.

Mutually Orthogonal Latin Squares

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Orthogonal Arrays

Definition

An *orthogonal array* $\mathrm{OA}(k, s)$ is a $k \times s^2$ array with entries from an s-set S having the property that in any two rows, each (ordered) pair of symbols from S occurs exactly once.

Construction

Let $\{L_i : 1 \leq i \leq k\}$ be a set of k MOLS on symbols $\{1, \ldots, n\}$. Form a $(k+2) \times n^2$ array $A = (a_{ij})$ whose columns are $(i, j, L_1(i,j), L_2(i,j), \ldots, L_k(i,j))^T$ for $1 \leq i, j \leq k$. Then A is an orthogonal array, $OA(k+2, n)$. This process can be reversed to recover k MOLS of side n from an $OA(k+2, n)$, by choosing any two rows of the OA to index the rows and columns of the k squares.

Orthogonal Arrays

Definition

An *orthogonal array* OA(k, s) is a $k \times s^2$ array with entries from an s-set S having the property that in any two rows, each (ordered) pair of symbols from S occurs exactly once.

Construction

Let $\{L_i : 1 \leq i \leq k\}$ *be a set of* k *MOLS on symbols* $\{1, \ldots, n\}$*. Form a* $(k+2) \times n^2$ *array* $A = (a_{ij})$ *whose columns are* $(i, j, L_1(i,j), L_2(i,j), \ldots, L_k(i,j))^T$ *for* $1 \leq i, j \leq k$*. Then* A *is an orthogonal array,* $OA(k+2, n)$*. This process can be reversed to recover* k *MOLS of side* n *from an* $OA(k+2, n)$*, by choosing any two rows of the OA to index the rows and columns of the* k *squares.*

Orthogonal Arrays

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

$$\begin{pmatrix} 1111222233334444 \\ 1234123412341234 \\ 1234432121433412 \\ 1234341243212143 \\ 1234214334124321 \end{pmatrix}$$

Transversal Designs

Definition

A *transversal design* of *order* or *groupsize* n, *blocksize* k, and *index* λ, denoted $\text{TD}_\lambda(k, n)$, is a triple $(V, \mathcal{G}, \mathcal{B})$, where

1. V is a set of kn elements;
2. $\mathcal{G}$ is a partition of V into k classes (the *groups*), each of size n;
3. $\mathcal{B}$ is a collection of k-subsets of V (the *blocks*);
4. every unordered pair of elements from V is contained either in exactly one group or in exactly λ blocks, but not both.

When $\lambda = 1$, one writes simply $\text{TD}(k, n)$.

Transversal Designs

- Given a TD($n+1, n$), delete a group and treat both blocks and groups as lines to get an *affine plane of order n*. This can be reversed to get a TD($n+1, n$) from an affine plane.
- Given a TD($n+1, n$), add a point ∞, treat blocks as lines, and add ∞ to each group to form $n+1$ further lines, to get a *projective plane of order n*. This can be reversed to get a TD($n+1, n$) from a projective plane.

Transversal Designs

Construction

Let A be an $OA(k,n)$ on the n symbols in X. On $V = X \times \{1,\ldots,k\}$ (a set of size kn), form a set $\mathcal{B}$ of k-sets as follows. For $1 \leq j \leq n^2$, include $\{(a_{i,j}, i) : 1 \leq i \leq k\}$ in $\mathcal{B}$. Then let $\mathcal{G}$ be the partition of V whose classes are $\{X \times \{i\} : 1 \leq i \leq k\}$. Then $(V, \mathcal{G}, \mathcal{B})$ is a $TD(k,n)$. This process can be reversed to recover an $OA(k,n)$ from a $TD(k,n)$.

Transversal Designs

$$\begin{pmatrix} 1111222233334444 \\ 1234123412341234 \\ 1234432121433412 \\ 1234341243212143 \\ 1234214334124321 \end{pmatrix}$$

A TD$(5,4)$ derived from the OA$(5,4)$. On the element set $\{1,2,3,4\} \times \{1,2,3,4,5\}$, the blocks are

{ 11,12,13,14,15 }	{ 11,22,23,24,25 }	{ 11,32,33,34,35 }	{ 11,42,43,44,45 }
{ 21,12,43,34,25 }	{ 21,22,33,44,15 }	{ 21,32,23,14,45 }	{ 21,42,13,24,35 }
{ 31,12,23,44,35 }	{ 31,22,13,34,45 }	{ 31,32,43,24,15 }	{ 31,42,33,14,25 }
{ 41,12,33,24,45 }	{ 41,22,43,14,35 }	{ 41,32,13,44,25 }	{ 41,42,23,34,15 }

Mutually Orthogonal Latin Squares

- MOLS are central objects in combinatorics.
- Starting with Euler in 1782, who considered for which sides there exist two MOLS of that side.
- But after hundreds of papers (and hundreds of years), determining $N(n)$, the largest number of MOLS of side n is very far from complete.
- (The smallest unknown value is still $N(10)$.)

Mutually Orthogonal Latin Squares

- $N(n) \leq n-1$; a simple counting argument.
- $N(n) = n-1$ whenever n is a power of a prime; for example, over the finite field $\mathbb{F}_q$, consider the q^2 linear polynomials evaluated at the $q+1$ points from $\mathbb{F}_q \cup \{\infty\}$.
- $N(nm) \geq \min(N(n), N(m))$; a simple direct product.
- Recursive constructions: PBD closure, Wilson's constructions.
- Direct constructions: assume symmetries to limit computational search.

Mutually Orthogonal Latin Squares

Current Bounds on $N(n)$ for $n < 100$:

	0	1	2	3	4	5	6	7	8	9
0			1	2	3	4	1	6	7	8
10	2	10	5	12	*3*	*4*	15	16	*3*	18
20	*4*	5	*3*	22	7	24	4	26	5	28
30	*4*	30	31	5	*4*	5	8	36	*4*	5
40	7	40	5	42	5	6	*4*	46	8	48
50	6	5	5	52	5	6	7	7	*5*	58
60	*4*	60	*5*	*6*	63	7	*5*	66	*5*	6
70	6	70	*7*	72	*5*	7	6	*6*	*6*	78
80	9	80	8	82	6	*6*	*6*	*6*	*7*	88
90	*6*	*7*	*6*	*6*	*6*	*6*	7	96	6	*8*

Difference Matrices

Definition

Let $(G, \odot)$ be a group of order g. A $(g, k; \lambda)$-*difference matrix* is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G, so that for each $1 \leq i < j \leq k$, the multiset

$$\{d_{i\ell} \odot d_{j\ell}^{-1} : 1 \leq \ell \leq g\lambda\}$$

(the *difference list*) contains every element of G λ times.

When G is abelian, typically additive notation is used, so that differences $d_{i\ell} - d_{j\ell}$ are employed.

Difference Matrices

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 9 & 12 & 4 & 1 \\ 6 & 3 & 14 & 10 & 7 & 13 & 4 \\ 10 & 6 & 1 & 11 & 2 & 7 & 12 \end{pmatrix}.$$

Append a column of zeroes to $(B \mid -B)$ to get a $(15, 5; 1)$-difference matrix.

Difference Matrices and MOLS

- Develop the columns of the difference matrix under the action of G.
- This gives g translates of the difference matrix.
- Add a new row placing the index of the translate in this row, to get a set of $k-1$ MOLS of side g (actually, an OA$(k+1, g)$).
- So our example gives four MOLS(15).

Incomplete Latin Squares

Definition

An *incomplete latin square* ILS($n; b_1, b_2, \ldots, b_k$) is an $n \times n$ array A with entries from an n-set B, together with $B_i \subseteq B$ for $1 \leq i \leq k$ where $|B_i| = b_i$ and $B_i \cap B_j = \emptyset$ for $1 \leq i, j \leq k$. Moreover, each cell of A is empty or contains an element of B; the subarrays indexed by $B_i \times B_i$ are empty (these subarrays are *holes*); and the elements in row or column b are exactly those of $B \setminus B_i$ if $b \in B_i$, and of B otherwise.

Incomplete MOLS

Definition

Two incomplete latin squares (ILS($n; b_1, b_2, \ldots, b_s$)) are *orthogonal* if upon superimposition all ordered pairs in $(B \times B) \setminus \cup_{i=1}^{k}(B_i \times B_i)$ result. Two such squares are IMOLS($n; b_1, b_2, \ldots, b_s$). Then r-IMOLS($n; b_1, b_2, \ldots, b_s$) denotes a set of r ILS($n; b_1, b_2, \ldots, b_s$) that are pairwise orthogonal.

r-IMOLS($n; b_1, \ldots, b_s$) is equivalent to

1. an incomplete transversal design ITD($r + 2, n; b_1, \ldots, b_s$);
2. an incomplete orthogonal array IOA($r + 2, n; b_1, \ldots, b_s$).

Quasi-Difference Matrices

Definition

Let G be an abelian group of order n. A $(n, k; \lambda, \mu; u)$-*quasi-difference matrix* (QDM) is a matrix $Q = (q_{ij})$ with k rows and $\lambda(n-1+2u)+\mu$ columns, with each entry either empty (usually denoted by $-$) or containing a single element of G. Each row contains exactly λu empty entries, and each column contains at most one empty entry. Furthermore, for each $1 \leq i < j \leq k$, the multiset $\{q_{i\ell} - q_{j\ell} : 1 \leq \ell \leq \lambda(n-1+2u)+\mu,$ with $q_{i\ell}$ and $q_{j\ell}$ not empty$\}$ contains every nonzero element of G λ times and contains 0 μ times.

QDMs and Incomplete OAs

Construction

If a $(n, k; \lambda, \mu; u)$-QDM exists and $\mu \leq \lambda$, then an $ITD_\lambda(k, n+u; u)$ exists. Start with a $(n, k; \lambda, \mu; u)$-QDM A over the group G. Append $\lambda - \mu$ columns of zeroes. Then select u elements $\infty_1, \ldots, \infty_u$ not in G, and replace the empty entries ($-$), each by one of these infinite symbols, so that ∞_i appears exactly once in each row, for $1 \leq i \leq u$. Develop the resulting matrix over the group G (leaving infinite symbols fixed), to obtain a $k \times \lambda(n^2 + 2nu)$ matrix T. Then T is an incomplete orthogonal array with k rows and index λ, having $n + u$ symbols and one hole of size u.

A QDM Example

Consider the matrix:

$$\begin{pmatrix} - & 10 & 1 & 2 & 6 & 3 & 22 & 5 & 7 & 9 & 14 & 18 & 28 \\ 0 & 1 & 10 & 20 & 23 & 30 & 35 & 13 & 33 & 16 & 29 & 32 & 21 \\ 0 & 26 & 26 & 15 & 8 & 4 & 17 & 19 & 34 & 12 & 31 & 24 & 25 \\ 10 & - & 10 & 6 & 2 & 22 & 3 & 7 & 5 & 14 & 9 & 28 & 18 \\ 1 & 0 & 26 & 23 & 20 & 35 & 30 & 33 & 13 & 29 & 16 & 21 & 32 \\ 26 & 0 & 1 & 8 & 15 & 17 & 4 & 34 & 19 & 31 & 12 & 25 & 24 \end{pmatrix}.$$

Each column $(a, b, c, d, e, f)^T$ is replaced by columns $(a, b, c, d, e, f)^T$, $(b, c, a, f, d, e)^T$, and $(c, a, b, e, f, d)^T$ to obtain a $(37, 6; 1, 1; 1)$ quasi-difference matrix (QDM). Fill the hole of size 1 in the incomplete OA to establish that $N(38) \geq 4$.

V(m, t) Vectors

Definition

Let q be a prime power and let $q = mt + 1$ for m, t integer. Let ω be a primitive element of $\mathbb{F}_q$. A *V(m, t) vector* is a vector $(a_1, \ldots, a_{m+1})$ for which, for each $1 \leq k < m$, the differences $\{a_{i+k} - a_i : 1 \leq i \leq m+1, i+k \neq m+2\}$ represent the m cyclotomic classes of $\mathbb{F}_{mt+1}$ (compute subscripts modulo $m+2$).

$V(2,3)$ example: (0 1 4)

V(m, t) Vectors

Construction

A quasi-difference matrix from a $V(m,t)$ vector. Starting with a $V(m,t)$ vector $(a_1,\ldots,a_{m+1})$, form a single column of length $m+2$ whose first entry is empty, and whose remaining entries are $(a_1,\ldots,a_{m+1})$. Form t columns by multiplying this column by the powers of ω^m. From each of these t columns, form $m+2$ columns by taking the $m+2$ cyclic shifts of the column. The result is a $(q,m+2;1,0;t)$-QDM.

–	–	–	0	0	0	1	2	4	4	1	2
0	0	0	1	2	4	4	1	2	–	–	–
1	2	4	4	1	2	–	–	–	0	0	0
4	1	2	–	–	–	0	0	0	4	1	2

(7,4;1,0;3)-QDM $\Rightarrow$ 2-IMOLS(10,3) (and 2 MOLS(10)).

Relaxing(?) the Requirements

- Beyond 'incomplete' objects, there are numerous relaxations of MOLS. For example,
  - Two latin squares of side n are r-orthogonal ($n \leq r \leq n^2$) if their superposition has exactly r distinct ordered pairs.
  - Two $n \times m$ latin rectangles are *orthogonal* if no pair occurs twice in their superposition. (And so to MOLR.)
  - etc. etc.
- But we will look here at packing and covering analogues, which can be treated most naturally in the orthogonal array vernacular.

Orthogonal, Packing, and Covering Arrays

Definition

A $k \times N$ array on a set of v symbols is a packing or orthogonal or covering array when in every two rows, each (ordered) pair of symbols occurs at most once or exactly once or at least once.

Then $N \leq v^2$ or $N = v^2$ or $N \geq v^2$.

In the interests of time, we focus on covering arrays, first giving the more standard (and more general) definition.

Covering Array. Definition

- Let N, k, t, and v be positive integers.
- Let C be an $N \times k$ array with entries from an alphabet Σ of size v; we typically take $\Sigma = \{0, \ldots, v-1\}$.
- When $(\nu_1, \ldots, \nu_t)$ is a t-tuple with $\nu_i \in \Sigma$ for $1 \leq i \leq t$, $(c_1, \ldots, c_t)$ is a tuple of t column indices $(c_i \in \{1, \ldots, k\})$, and $c_i \neq c_j$ whenever $\nu_i \neq \nu_j$, the t-tuple $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ is a *t-way interaction*.
- The array *covers* the t-way interaction $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ if, in at least one row ρ of C, the entry in row ρ and column c_i is ν_i for $1 \leq i \leq t$.
- Array C is a *covering array* CA$(N; t, k, v)$ of *strength* t when every t-way interaction is covered.

Covering Array. Definition

- Let N, k, t, and v be positive integers.
- Let C be an $N \times k$ array with entries from an alphabet Σ of size v; we typically take $\Sigma = \{0, \ldots, v-1\}$.
- When $(\nu_1, \ldots, \nu_t)$ is a t-tuple with $\nu_i \in \Sigma$ for $1 \leq i \leq t$, $(c_1, \ldots, c_t)$ is a tuple of t column indices ($c_i \in \{1, \ldots, k\}$), and $c_i \neq c_j$ whenever $\nu_i \neq \nu_j$, the t-tuple $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ is a *t-way interaction*.
- The array *covers* the t-way interaction $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ if, in at least one row ρ of C, the entry in row ρ and column c_i is ν_i for $1 \leq i \leq t$.
- Array C is a *covering array* CA$(N; t, k, v)$ of *strength t* when every t-way interaction is covered.

Covering Array. Definition

- Let N, k, t, and v be positive integers.
- Let C be an $N \times k$ array with entries from an alphabet Σ of size v; we typically take $\Sigma = \{0, \ldots, v-1\}$.
- When $(\nu_1, \ldots, \nu_t)$ is a t-tuple with $\nu_i \in \Sigma$ for $1 \leq i \leq t$, $(c_1, \ldots, c_t)$ is a tuple of t column indices ($c_i \in \{1, \ldots, k\}$), and $c_i \neq c_j$ whenever $\nu_i \neq \nu_j$, the t-tuple $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ is a *t-way interaction*.
- The array *covers* the t-way interaction $\{(c_i, \nu_i) : 1 \leq i \leq t\}$ if, in at least one row ρ of C, the entry in row ρ and column c_i is ν_i for $1 \leq i \leq t$.
- Array C is a *covering array* CA$(N; t, k, v)$ of *strength t* when every t-way interaction is covered.

Covering Array. Example

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

CA(11;2,5,3)

Differences, Similarities

- Of course, orthogonal arrays are covering arrays, so they provide useful examples.
- Nevertheless the connections seem relatively weak:
  - Orthogonal arrays concerned with "large" v but $k \leq v + 1$; indeed typically for very small k
  - Covering arrays concerned with "small" v and all k
- Our CA(11;2,5,3) has too many columns to be an orthogonal array!

Differences, Similarities

- Recursive constructions for orthogonal arrays essentially all use arrays with small v to make ones with large v, but
- Recursive constructions for covering arrays essentially all use arrays with small k to make ones with large k.

Differences, Similarities

- IMOLS can lead to the best known covering arrays
  - 4-IMOLS(10,2) and CA(6;2,6,2) $\Rightarrow$ CA(102;2,6,10).
  - 4-IMOLS(22,3) and CA(13;2,6,3) $\Rightarrow$ CA(488;2,6,22).
  - 5-IMOLS($14,2^7$) and CA(6;2,7,2) $\Rightarrow$ CA(210;2,7,14).
  - 5-IMOLS($18,2^9$) and CA(6;2,7,2) $\Rightarrow$ CA(342;2,7,18).
  - 5-IMOLS($22,2^{11}$) and CA(6;2,7,2) $\Rightarrow$ CA(506;2,7,22).

Differences, Similarities

- "Fusion": We can sacrifice symbols: $CA(q^2; 2, k, q) \Rightarrow CA(q^2 - 1 - 2x; 2, k, q - x)$ for $1 \leq x < q$.
- "Augmentation": We can adjoin symbols: $CA(q^2; 2, k, q)$ and $CA(M; 2, k, 2) \Rightarrow CA(q^2 + (q - 1)(M - 1); 2, k, q + 1)$.
- "Projection": We can turn symbols into columns: $CA(q^2; 2, k, q) \Rightarrow CA(q^2 - x; 2, k + x, q - x)$ for $1 \leq x < q$ when $k \geq q$.
- These lead to many of the best known constructions for covering arrays with "small" k when v is not a powr of a prime.

Differences, Similarities

- "Fusion": We can sacrifice symbols: $\mathrm{CA}(q^2; 2, k, q) \Rightarrow \mathrm{CA}(q^2 - 1 - 2x; 2, k, q - x)$ for $1 \leq x < q$.
- "Augmentation": We can adjoin symbols: $\mathrm{CA}(q^2; 2, k, q)$ and $\mathrm{CA}(M; 2, k, 2) \Rightarrow \mathrm{CA}(q^2 + (q-1)(M-1); 2, k, q+1)$.
- "Projection": We can turn symbols into columns: $\mathrm{CA}(q^2; 2, k, q) \Rightarrow \mathrm{CA}(q^2 - x; 2, k + x, q - x)$ for $1 \leq x < q$ when $k \geq q$.
- These lead to many of the best known constructions for covering arrays with "small" k when v is not a powr of a prime.

Differences, Similarities

- "Fusion": We can sacrifice symbols: $\mathrm{CA}(q^2; 2, k, q) \Rightarrow \mathrm{CA}(q^2 - 1 - 2x; 2, k, q - x)$ for $1 \leq x < q$.
- "Augmentation": We can adjoin symbols: $\mathrm{CA}(q^2; 2, k, q)$ and $\mathrm{CA}(M; 2, k, 2) \Rightarrow \mathrm{CA}(q^2 + (q - 1)(M - 1); 2, k, q + 1)$.
- "Projection": We can turn symbols into columns: $\mathrm{CA}(q^2; 2, k, q) \Rightarrow \mathrm{CA}(q^2 - x; 2, k + x, q - x)$ for $1 \leq x < q$ when $k \geq q$.
- These lead to many of the best known constructions for covering arrays with "small" k when v is not a powr of a prime.

Differences, Similarities

- "Fusion": We can sacrifice symbols: $\mathrm{CA}(q^2; 2, k, q) \Rightarrow \mathrm{CA}(q^2 - 1 - 2x; 2, k, q - x)$ for $1 \leq x < q$.
- "Augmentation": We can adjoin symbols: $\mathrm{CA}(q^2; 2, k, q)$ and $\mathrm{CA}(M; 2, k, 2) \Rightarrow \mathrm{CA}(q^2 + (q-1)(M-1); 2, k, q+1)$.
- "Projection": We can turn symbols into columns: $\mathrm{CA}(q^2; 2, k, q) \Rightarrow \mathrm{CA}(q^2 - x; 2, k + x, q - x)$ for $1 \leq x < q$ when $k \geq q$.
- These lead to many of the best known constructions for covering arrays with "small" k when v is not a powr of a prime.

Differences, Similarities

–	0	1	1	0	cyclically permute columns
0	–	0	1	1	
1	0	–	0	1	
1	1	0	–	0	
0	1	1	0	–	
–	1	0	0	1	apply permutation (0 1) (–)
1	–	1	0	0	
0	1	–	1	0	
0	0	1	–	1	
1	0	0	1	–	
–	–	–	–	–	add constant row on symbol –

CA(11;2,5,3) – (– 0 1 1 0)

Cover Starters

- CA(11;2,5,3) – (– 0 1 1 0): 1-apart differences are 1, 0, 1; 2-apart differences are 1, 1, 0.
- In general, for a group Γ, a vector $(a_0, \ldots, a_{k-1})$ with $a_i \in \Gamma \cup \{\infty_1, \ldots, \infty_c\}$ so that
  - the i-apart differences (for $1 \leq i \leq k/2$) cover all elements of Γ, and
  - for each ∞_j and each $1 \leq i < k$ there is an ℓ with $a_\ell = \infty_j$ and $a_{\ell+i \bmod k} \in \Gamma$,

  is a cover starter that produces a covering array on k columns with $|\Gamma| + c$ symbols.
- This leads to many of the best examples of covering arrays for small values of k, but sadly the examples are all found by computer.

CA(N;2,20,10)

- At most 180 is claimed in 1996 by the authors of the commercial software AETG. But the online AETG does 198. So starts a long story ...
- Calvagna and Gargantini (2009) report results from 10 publicly available programs: 193, 197, 201, 210, 210, 212, 220, 231, 267.
- Simulated annealing does better: 183.
- A cover starter over $\mathbb{Z}_9$ found by Meagher and Stevens does 181.

CA(N;2,20,10)

- A variant of projection from a projective plane of order 13 does 178.
- From the CA(178;2,20,10), a computational postoptimization method produces 162.
- A cover starter over $\mathbb{Z}_7$ found by Lobb, Colbourn, Danziger, Stevens, and Torres does 155.
- But the “truth” might be much lower yet. We just don’t know.

What is needed?

- For MOLS, work has slowed: We know that $N(99) \geq 8$. This has been known since 1922. It is plausible that $N(99)$ is 10, or 50, or 90. Indeed what we know arises almost entirely from the finite field case and recursive methods.
- Perhaps we can make more progress on relaxations to covering arrays. MOLS (orthogonal arrays) yield a number of useful directions, but again we are handicapped by having to resort to computation – no reasonable theory for cases with few columns exists.
- What I am hoping is that people will look at other algebraic settings, not necessarily to find more MOLS, but to find reasonable approximations such as covering arrays.