A comparative study of defining sets in designs

Nicholas Cavenagh University of Waikato A defining set for a design is a subset of the design which determines it uniquely.

A Latin square of order n is an $n \times n$ array with each symbol from a set of size n once per row and once per column.

Example 1. The following partially filled-in Latin square has precisely one completion to a Latin square of order 6.

0	1	2	3			
1	2					
2						,
						\rightarrow
					3	
				3	4	

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

A defining set for a design is a subset of the design which determines it uniquely.

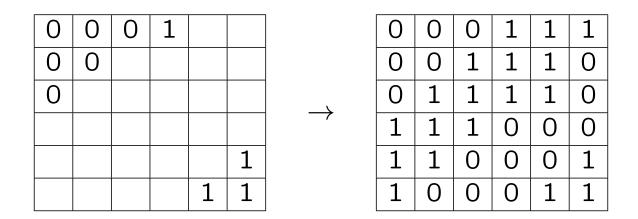
A Latin square of order n is an $n \times n$ array with each symbol from a set of size n once per row and once per column.

Example 1. The following partially filled-in Latin square has precisely one completion to a Latin square of order 6.

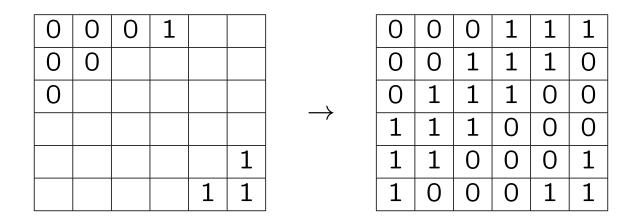
0	1	2	3			
1	2					
2						,
						\rightarrow
					3	
				3	4	

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

Example 2. The following is a defining set for a (0, 1)-matrix with constant row and column 3.

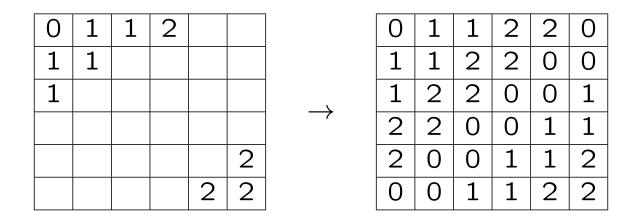


Example 2. The following is a defining set for a (0, 1)-matrix with constant row and column 3.



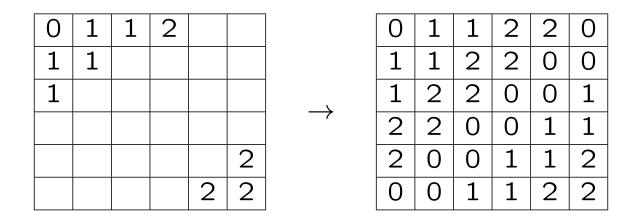
A frequency square $F(n; \lambda_1, \lambda_2, ..., \lambda_{\alpha})$ is an $n \times n$ array with symbol *i* occuring λ_i times in each row and column.

Example 3. The following is a defining set for F(6; 2, 2, 2). (Fitina, Seberry, Sarvate, 1999)



A frequency square $F(n; \lambda_1, \lambda_2, ..., \lambda_{\alpha})$ is an $n \times n$ array with symbol *i* occuring λ_i times in each row and column.

Example 3. The following is a defining set for F(6; 2, 2, 2). (Fitina, Seberry, Sarvate, 1999)



A critical set for a design is a minimal defining set. That is, a defining set is a critical set if the removal of any element results in more than one completion. Each of the above defining sets are also critical sets.

0	1	2	3		
1	2				
2					
					3
				3	4

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

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

 \nearrow

Y

0	0	0	1		
0	0				
0					
					1
				1	1

0	0	0	1	1	1
0	0	1	1	1	0
0	1	1	1	0	0
1	1	1	0	0	0
1	1	0	0	0	1
1	0	0	0	1	1

0	0	1	1	1	0
0	0	1	1	1	0
0	1	1	1	0	0
1	1	0	0	0	1
1	1	0	0	0	1
1	0	0	0	1	1

 \nearrow

K

0	1	1	2		
1	1				
1					
					2
				2	2

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

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

 \nearrow

Trades.

A trade in a design D is a subset $T \subseteq D$ for which there exists a disjoint mate T' such that $T' \cap T = \emptyset$ and $(D \setminus T) \cup T'$ is a design with the same paramaters (or type) as D. Together (T,T') is called a bitrade.

If the design is some kind of array, T and T' occupy the same set of cells and each row and column contains the same set of entries, but in a different order. **Observations:**

- 1. $D \subset L$ is a defining set for a design L if and only if for every trade $T \subseteq L$, $D \cap T \neq \emptyset$;
- 2. D is a critical set for a design L if and only if it is:
 (a) a defining set for L and
 (b) for each element e ∈ D there is a trade T ⊂ L such that T ∩ D = {e}.

Given a design D, we define sds(D) to be the size of the smallest defining set in D and

$$\mu(=\mu(D)) = \frac{sds(D)}{|D|}.$$

For each of the above designs, $\mu = 1/4$.

The following Latin squares have $\mu = 5/16$, $\mu = 6/25$ and $\mu = 7/25$ (Adams, Khodkar, 2001), respectively.

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

$\boxed{\theta}$	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

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

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

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

The following Latin squares have $\mu = 5/16$, $\mu = 6/25$ and $\mu = 7/25$ (Adams, Khodkar, 2001), respectively.

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

$\boxed{\theta}$	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

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

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

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

For a design D of some order n and "type" T(e.g. $T \in \{$ "Latin square"," frequency square" $\}$), $\mu(T,n) := \min\{\mu(D) \mid D \text{ is a design of type } T \text{ and order } n\}.$

We also define the surety of type T to be the following limit (if it exists):

 $\lim_{n\to\infty}\mu(T,n).$

Surety is a potentially interesting measure because:

- Surety is an indication of both the storability and the security of a design.
- Algebraic objects typically have surety 0.
- Purely combinatorial objects typically have surety 1.
- Designs are "interesting" as they often have non-trivial surety (strictly between 0 and 1).

Surety (or an equivalent concept) has been considered for various designs:

- member defining sets for Steiner designs (Gray and Ramsay, 1999),
- projective planes (Gray, Hamilton, O'Keefe (1997)),
- Hadamard designs (Seberry (1992), Sarvate and Seberry (1994)).

Let T(F) be the type $n \times n$ frequency square, with no symbol occuring more than n/2 times in each row/column.

The Conjecture.

$$\mu(T(F), n) = \begin{cases} 1/4 & \text{if } n \text{ is even;} \\ \lfloor n^2/4 \rfloor/n^2 & \text{if } n \text{ is odd.} \end{cases}$$

If The Conjecture is true, the surety of type T(F) is equal to 1/4.

Let scs(n) be the size of the smallest critical set in any Latin square of order n.

Sub-conjecture. For each integer $n \ge 1$, $scs(n) = \lfloor n^2/4 \rfloor$.

This conjecture is true for

- $n \leq 5$: Curran and van Rees (1978)
- n = 6,7: Adams and Kohdkar (2001)

• *n* = 8: Bean (2005)

Best known upper and lower bounds for general n:

For each $n \ge 1$, $scs(n) \le \lfloor n^2/4 \rfloor$. (Cooper, Donovan, Seberry (1991,1996)).

On the other hand, for all $n \ge 1$, $scs(n) \ge n \lfloor (\log n)^{1/3}/2 \rfloor$ (Cavenagh, 2007). Next consider a $2m \times 2m$ (0, 1)-matrix with constant row and column sum m. (Equivalently, a frequency square F(2m; m, m).)

Theorem. (Fitina, Seberry, Sarvate, 1999) $\mu(F(2m;m,m)) \leq 1/4.$

Theorem. (Cavenagh, 2011)

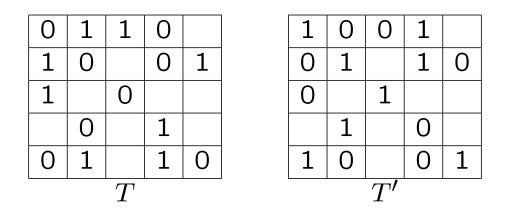
$$\mu(F(2m;m,m)) = 1/4.$$

Hence the surety of frequency squares of the form F(2m; m, m) is 1/4.

Why is The Conjecture tractible for (0, 1)-matrices, yet unverified for Latin squares?

Trades in (0, 1)-matrices.

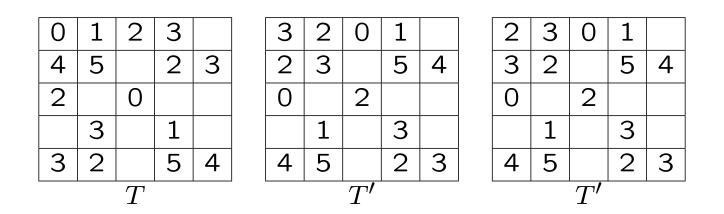
Here we consider a (0, 1)-matrix with fixed row and column sums. Since only two symbols are allowed, a trade T in a (0, 1)-matrix has a *unique* disjoint mate T'.



Moreover, each row and column must have the same number of 0's and 1's.

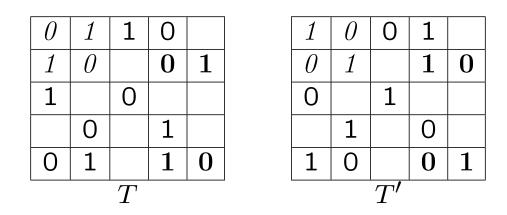
Trades in Latin squares.

A trade in a Latin square may have more than one disjoint mate:



Lemma.

Let M be a partially filled-in (0, 1)-matrix such that each row and column of M has at least one 0 and at least one 1. Then M contains a trade. Theorem. Any trade in a (0,1)-matrix can be partitioned into disjoint minimal trades (which are alternating 0 - 1-cycles):



Lemma. Suppose D is a defining set for a (0,1)-matrix M and $D \subset M$. Then $M \setminus D$ must have either a row or column containing only 0's or only 1's.

Consequence: Completing defining sets for (0,1)-matrices is easy (can be done in polynomial time), a rather boring Sudoku puzzle!!!

Theorem. (Colbourn, 1984) Deciding whether a partial Latin square is completable is NP-complete, even if there are no more than 3 unfilled cells in each row and column.

In the following critical set, no missing entry is directly "forced":

				4
	0	3		
2				
3		1		
			1	

Theorem. Let D be a critical set for a (0,1)-matrix M. Then D contains no trades. On the surface this theorem is non-intuitive!!!

Corollary. The complement of a critical set in a (0, 1)-matrix is always a defining set.

Th following is a critical set for a Latin square of order 4. It contains a trade; thus its complement is not a defining set.

0	1	2	3
1	0		
2		0	
3			

Theorem. Any defining set for a $2m \times 2m$ (0, 1)-matrix with constant row and columns sum m has size at least m^2 .

Proof by coin-flipping.

Corollary. Any critical set for a $2m \times 2m$ (0,1)-matrix with constant row and columns sum *m* has size *at most* $3m^2$.

Open problem: Do there exist critical sets which meet this bound? Not for small orders...

... but we can come close for large orders.

Lemma. For each $m \ge 2$, there exists a critical set in F(2m; m, m) of size $3m^2 - 8m + 8$.

For m = 5:

0	0	0	1	1	1		0	0	
0	0	0	1	1	1			0	
0	0	0	1	1	1			0	
1	1	1				1			
1	1	1				1			
1	1	1				1			
			1	1	1				
0	0	0						0	0
								0	0

We can exactly describe the structure of critical sets in F(2m; m, m) of minimal size.

Theorem. (Gale-Ryser, Walkup, Brualdi) A rectangular array on symbols 0 and 1 has no trades if and only if the rows and columns can be arranged so that a line with nonnegative gradient can be drawn with only 1's below the line and only 0's above the line.

$$\left[\begin{array}{rrrrr} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{array}\right]$$

Theorem. Let D be a defining set for a matrix $M \in F(2m; m, m)$ with size m^2 . Then M may be split into four quadrants:

$$M = \begin{bmatrix} E & F \\ \hline G & H \end{bmatrix}$$

such that each quadrant has no trades, E = H, F = G. Moreover D contains every 0 from quadrant E and every 1 from quadrant H and no other symbols. Example. A defining set in F(8; 4, 4):

0	0	0	0	1	1	1	1
θ	0	1	1	1	1	0	0
θ	1	1	1	1	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0
1	1	0	0	0	0	1	1
1	0	0	0	0	1	1	1
0	0	0	0	1	1	1	1

So we know all about the size of minimum defining sets for (0, 1)-matrices (in this special case)... but not yet for Latin squares.

Next steps:

- Look at frequency squares with at most 3 distinct symbols.
- Are there other designs with surety equal to 1/4???

Summary

- The surety for Latin squares and certain (0,1)-matrices with constant row and column sum appears to be the same (i.e. 1/4).
- This is perhaps because they can both belong to a broader class of frequency squares with constant surety.
- Current methods only handle special cases of "The Conjecture".

• Surety is a tool for comparing the structure of designs, and may unearth new connections between different types of designs. The idea of surety can be generalized. We can also consider:

- The size of the largest critical set in any design of a given type and order.
- The design of a given type and order which has the largest smallest critical set size (inf). For Latin squares,

$$n^2 - (e + o(1))n^{5/3} \le \inf \le n^2 - O(n^{3/2})$$

(Ghandehari, Hatami, Mahmoodian, 2005)

• The design of a given type and order which has the smallest largest critical set size (sup).