If structure = Latin square/design, a trade is the difference between any two structures.

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

Any trade in a Latin square must contain at least 2 rows, 2 columns, and 2 different elements. Each row, column and element in the trade must contain at least 2 entries, thus the size of a trade $\in \{4\} \cup \{6, 7, 8, \ldots\}$.

In this talk we will concentrate on trades on two, three, and four rows.

Latin trades on two rows

Consider a $2 \times n$ Latin rectangle.

1 2 3	4 5 6	7 8 9
2 3 1	5 6 4	8 9 7

It can be thought of as a permutation of the elements $\{1, \ldots, n\}$.

If we consider a random $2 \times n$ Latin rectangle, as we increase n, the expected number of cycles increases. (Wilf).

If we remove one entry from each row of a $2 \times n$ Latin rectangle which contains >2 cycles, there is a trade on the remaining ~~element~~ entries.

We call the remaining entries a chopped Latin rectangle.

A $2 \times n$ Latin rectangle containing only 1 cycle is isomorphic to 2 adjacent rows in $\mathbb{Z}_n$. If any entry is removed, no trade can be found in the remaining entries.

If structure = Latin square/design, a trade is the difference between any two structures.

A minimal defining set/critical set uniquely determines the rest of a design/Latin square in such a way that no subset does so.

Such a set must intersect each trade. Therefore the solution to an IP where each constraint corresponds to a trade is the size of the smallest defining set or critical set.

Latin trades on three rows

1	2	3	4	(5)	6	7	8	9	10
2	(3)	4	5	6	7	8	9	10	1
10	9	1	7	4	3	2	6	5	(8)

3	6	7	5	1	(4)	2
5	4	(1)	2	7	3	6
7	1	5	6	4	2	(3)

These can be considered as a set of $\binom{3}{2}=3$ permutations. Cavenagh (2002) wrote an algorithm to produce trades on 3 rows under certain conditions.

Permutations α, β, γ. Trades $T_1 \cap T_2 = S =$

0	e_1	$\alpha(e_1)$	...	$\alpha^{p-1}(e_1)$			
1	$\alpha(e_1)$	$\alpha^2(e_1)$	...	$\alpha^p(e_1)=e_2$	e_1	$\beta(e_1)$	...	$\beta^{q-1}(e_1)$
					$\beta(e_1)$	$\beta^2(e_1)$	...	$\beta^q(e_1)=e_2$
n-1								

If $\exists$ distinct elements e_1, e_2 such that

- $\alpha^p(e_1)=e_2$, $\beta^q(e_1)=e_2$ where $1 \le p, q \le n-1$
- $\alpha^g(e_1) \neq \beta^h(e_1)$, for all $0 \le g < p$, $0 \le h < q$, except $(g,h)=(0,0)$.

What is the dual concept of the trade?

How much of a structure is required in order to uniquely determine the remainder?

Defining sets in designs

Uniquely completable sets in Latin squares

A uniquely completable set for a Latin square L must intersect every trade in L. It is critical if no subset is uniquely completable.

Applications.

Cryptography, secret sharing schemes

(Cooper, Donovan, Seberry, A. Street)

Two kinds of IPs related to defining sets / trades — dual problems.

Minimize size of defining set. subject to: for each trade T, the defining set must intersect T at least once.	Minimize number of trades. subject to: for each set C smaller than the smallest defining set, must be at least one trade not intersecting C.

Approaches for solving 0-1 IP.

- branch-and-bound/branch-and-cut (CPLEX, many others)
- local search (WSAT)
- SAT solvers (PBS)

Branch-and-bound/cut is ineffective if constraints are symmetric e.g. symmetric Steiner systems or group-based Latin squares. Lots of useless subproblems to be examined. Therefore

- add symmetry-breaking clauses
- use a different approach.

Cavenagh's algorithm is complex, difficult to understand, and not presented in a symmetric way.

It is best to reinterpret his result as a statement about Latin trades on four rows.

Take a $4 \times n$ Latin rectangle and remove one entry from 3 of the rows. We can find a Latin trade on 3 rows from the remaining entries – one of these rows is the row with no entries removed.

Thus, when there is an empty row in a UC set, there are at most 2 other rows with exactly one entry. This means there are at least ~~most~~ $0+1+1+2(n-3) = 2n-4$ entries in any such set.

GOAL. Remove the "empty row" condition, then any UC set must have at least $2n-4$ entries, beating Horak et al's bound of $scs(n) \geq \lfloor (4n-8)/3 \rfloor$.

Lavenagh stated a conjecture:

"C. In any critical set P, there are at most three columns (or rows or entries) with at most one element. A corollary of the previous conjecture and the results of this paper would be that $|P| \geq 2n-4$ for any critical set P of order n."

In fact the conjecture itself would suffice to prove $scs(n) \geq 2n-4$. We reinterpret the conjecture as a statement about Latin trades on four rows.

Conjecture.
Take a $4 \times n$ Latin rectangle and remove one entry from each row. We can find a Latin trade on the remaining entries.

Philosophical Interlude

Are "existence" problems harder than "non-existence" problems in combinatorics, or vice versa?

For this problem, is it better to provide a construction for a trade if one exists, or merely to prove its existence?

The nature of the problem on 3 rows with 1 entry missing from 2 rows makes a construction easier - there is a "starting point" or "hook" in the form of the empty row.

Conjecture (continued).

First, the conjecture was verified for $n \leq 8$, as Cavenagh made the conjecture based on empirical results. For $n=8$, the 93561 8×4 non-isomorphic Latin rectangles were generated and I examined each of the 8" possibilities of removing 1 entry from each of the 4 rows. If there was a different "completion" of the ~~LR~~ with the same elements in each row and column, this implied the existence of a trade.

This established that $scs(8) \geq 12$.

(Previously only $scs(8) \geq 9$ was known by $scs(n) \geq n+1$ – Cooper et al.)

Choosing trades intelligently (see Surveys paper on defining sets) pp146-9

Much evidence to indicate trades on 3 rows/cols/elts very effective for determining smallest critical sets. Using these trades of size ≤ 10 for Latin squares of order 8, all squares with ≥ 16 or ≤ 4 2×2 subsquares are proven to have no CS of size < 16.

(98561 of 283657 main classes).

S.

1	6	3	4	5	2	8	7
5	7	1	2	3	8	6	4
4	5	2	8	6	7	3	1
?	2	8	7	1	6	4	5
⋮	8	4	6	7	1	5	3
○	4	⋮	3	8	5	1	2
	○		5	4	3	2	6
			5	1	2	4	7	8

S intersects every trade on ≤ 3 r's, c's, e's but S is NOT a critical set.

Second, integer programming techniques were used to determine how many different sizes of trades "covered" all the possibilities.

n	# different trade sizes needed.	
4	4	(4, 8, 10, 12)
5	7	(8, 9, 12, 14, 16 + two others)
6	6	(4, 6, 8, 9, 10, 12)
7	8	(4, 8, 9, 10, 12, 14, 18, 21)
8	7	

For $n < 8$, some chopped LRs required exactly one size of trade - e.g. some 4×7 chopped LRs require size 21.

2 3 1	6 4 5	
3 1 2	5 6 4	
5 6 4	1 2 3	
6 4 5	3 1 2	

·	·	1	·	4 ·
3	·	2	5	6 ·
·	·	4	·	2 ·
6	·	5	3	1 ·

only trades of size 12 here.

2	·	1	6	· ·
·	·	2	5	6 ·
5	·	·	1	2 ·
6	·	5	·	1 ·

2	·	1	6	4 ·
3	·	·	5	· ·
5	·	4	1	2 ·
6	·	·	3	· ·

Therefore we should look at

Cavenagh's conjecture.

In every $4 \times n$ Latin rectangle with one entry removed from each row, $\exists$ a Latin trade.

This implies that $scs(n) \geq 2n-4$.

Proven for $n=8$, thus $scs(8) \geq 12$,
and for rows of $\mathbb{Z}_4$, thus $scs(\mathbb{Z}_{11}) \geq 18$.

$$\left.\begin{array}{l} scs(n) \geq n-1 \\ scs(n) \geq 2n-4 \\ scs(n) \geq 3n-9 \\ \vdots \\ scs(n) \geq xn-x^2 \end{array}\right\} \rightarrow scs(n) = \left\lfloor n^2/4 \right\rfloor$$

Third, check the minimum number of trades which can be found in a $4 \times n$ chopped Latin rectangle

n	min. # trades missing
4	1
5	1
6	3
7	3
8	7
9	≤ 15 *

From order 8, there are 93561.4^4 distinct chopped LRs to look at; 300 of them have exactly 7 missing trades (264 unique sets.)

From the order 9 atomic Latin squares we can find examples where only 15 trades are missing.

Fourth, try to characterise 3-row chopped LRs and find which of them do not trades. Cavenagh found that when a trade could not be found in a $3 \times n$ LR with 1 entry removed from 2 rows, these 3 rows were isomorphic to 3 adjacent rows in $BC_n / \mathbb{Z}_n$.

0	1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	10	0
2	3	4	5	6	7	8	9	10	0	1

A similar idea exists in 3-row chopped LRs based on 3 rows which are adjacent taken from $\mathbb{Z}_n$.

0	1	2	3	4	5	6	7	8	9	10	no trade
1	2	3	4	5	6	7	8	9	10	0	– or 0
2	3	4	5	6	7	8	9	10	0	1	

Apart from the supersets of the first example and sets like the second, a trade can be found in any $3 \times n$ chopped LR on these rows.

Theorem

In $\mathbb{Z}_{2n+1}$, if we take any 3 adjacent rows, the following trades of size $\mathbb{Z}_{2n+4}$ are sufficient for finding trades on any chopped LR on these rows("0, 1, 2").

$A_{0\cdots 2n}$, $B_{0\cdots 2n}$

$$A_i = \{(0,x;x),(2,x;x+2) \mid x = i+2y,\ y = 0,\cdots,n\}$$
$$\cup \{(1,i;i+1),(1,i-1;i)\}$$

$$B_i = \{(0,x;x),(2,x;x+2) \mid x = i+2y,\ y = 0,\cdots,n-1\}$$
$$\cup \{(0,i-1;i-1),(1,i-1;i),(1,i-2;i-1),(2,i-2;i)\}$$

12'

```
.12.4.6.8.a.c.e
.23.........
.34.6.8.a.c.e.1

.1.34.6.8.a.c.e
...45.......
.3.56.8.a.c.e.1

.1.34.6.8.a.c.e
.234.........
.345.6.8.a.c.e.1

.1.3.56.8.a.c.e
.....67......
.3.5.78.a.c.e.1

.1.3.56.8.a.c.e
....56.......
.3.56.8.a.c.e.1

.1.3.5.78.a.c.e
.......89....
.3.5.7.9a.c.e.1

.1.3.5.78.a.c.e
......78.....
.3.5.78.a.c.e.1

.1.3.5.7.9a.c.e
........ab...
.3.5.7.9.bc.e.1

.1.3.5.7.9a.c.e
........9a...
.3.5.7.9a.c.e.1

.1.3.5.7.9.bc.e
..........cd..
.3.5.7.9.b.de.1

.1.3.5.7.9.bc.e
.........bc...
.3.5.7.9.bc.e.1

.1.3.5.7.9.b.de
............e0
.3.5.7.9.b.d.01

.1.3.5.7.9.b.de
..........de.
.3.5.7.9.b.de.1

.12.4.6.8.a.c.e
12..........
2.4.6.8.a.c.e.1

0.23.5.7.9.b.d.
..34.........
2.45.7.9.b.d.0.
```

```
0.2.45.7.9.b.d.
....56.......
2.4.67.9.b.d.0.

0.2.45.7.9.b.d.
...45........
2.45.7.9.b.d.0.

0.2.4.67.9.b.d.
......78.....
2.4.6.89.b.d.0.

0.2.4.67.9.b.d.
.....67.......
2.4.67.9.b.d.0.

0.2.4.6.89.b.d.
........9a....
2.4.6.8.ab.d.0.

0.2.4.6.89.b.d.
.......89.....
2.4.6.89.b.d.0.

0.2.4.6.8.ab.d.
.........bc...
2.4.6.8.a.cd.0.

0.2.4.6.8.ab.d.
.........ab....
2.4.6.8.ab.d.0.

0.2.4.6.8.a.cd.
...........de.
2.4.6.8.a.c.e0.

0.2.4.6.8.a.cd.
...........cd..
2.4.6.8.a.cd.0.

0.2.4.6.8.a.c.e
............e0
2.4.6.8.a.c.e0.

0.23.5.7.9.b.d.
.23.........
23.5.7.9.b.d.0.

0.2.4.6.8.a.c.e
1...........0
2.4.6.8.a.c.e.1

01.3.5.7.9.b.d.
1...........0
.3.5.7.9.b.d.01

01.3.5.7.9.b.d.
12..........
23.5.7.9.b.d.0.
```

In any four rows from $\mathbb{Z}_n$, $n > 5$, there exist 3 rows not isomorphic to 3 adjacent rows in $\mathbb{Z}_n$. Trades can always be found in these rows where 1 entry is removed from each row, for $n \leq 35$.

Thus, for odd $n \leq 35$, the smallest critical set in $\mathbb{Z}_n$ has size at least $2n-4$.

Combining the previous results:

- if ~~there exists~~ any pair of rows exists from the 4 rows with > 2 cycles, a trade exists
- if ~~there exists~~ any $4 \times m$ subrectangle exists, $4 \leq m \leq 8$, a trade exists
- if a $3 \times n$ subrectangle is isomorphic to 3 adjacent rows in $\mathbb{Z}_n$ can be found, a trade exists under certain conditions.

Limit as $n \to \infty$

As the expected number of cycles in a permutation of size n increases as $n \to \infty$, we have the following results, by generalizing the conjecture.

As $n \to \infty$, the proportion of Latin squares with smallest critical set of size $\geq 2n-4$ goes to 1.

This result is true if we change $2n-4$ to $3n-9$, $4n-16$, ... $xn-x^2$.

Since $\max_{x \in \mathbb{N}} \{xn - x^2\} = \lfloor n^2/4 \rfloor$,

as $x \to \infty$ and $n \to \infty$, the proportion of Latin squares with smallest critical set size $\geq xn - x^2$ goes to 1.

If we had $x \approx \frac{1}{2}n$ at each step, proportion of Latin squares with smallest critical set size $\lfloor n^2/4 \rfloor$ would go to 1.

Other attempted solution methods.

- Induction. "Prolonging" or "stripping" a transversal from an LR seems ineffective.
- Consider only $n \geq 8$ – it may simplify the proof – shades of Evans' theorem about LS embedding.
- Consider pairwise intersection of trades – for 4×8 chopped LRs, we can always find a pair with an intersection having only 2 or 3 entries per column. (2/93561.4[4] require 3 entries per column).
- Bidkhori – a generalized Latin square with entries from a set greater than the number of columns, similar to Mahmoodian/Mahdian's "silver matrix" idea.

Calculation of scs(8)

Using integer programming techniques and trades on three rows, cols, elts, found that ~(74000/283657 main classes of 8×8 LSs contain no CS of size ≤ 16. (~61% done). (≥15 intercalates, ≤4 intercalates).

Two main classes have the property that trades on three rows/cols/elts are insufficient to prove this. They have similar properties and seemingly the same spectrum of CS sizes (21–28).

Conjectures of Ms. Bidkhori.