 of Latin Squares

Ian Wanless

Monash University, Australia

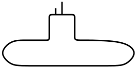
What do these mathematical words have in common?

- group,
- graph,
- set,
- manifold,
- field,
- design,
- matrix,
- category,
- module,
- ring,
- sequence,
- space?

What do these mathematical words have in common?

- group,
- graph,
- set,
- manifold,
- field,
- design,
- matrix,
- category,
- module,
- ring,
- sequence,
- space?

What do these mathematical words have in common?



- group,
- graph,
- set,
- manifold,
- field,
- design,
- matrix,
- category,
- module,
- ring,
- sequence,
- space?

Subsquares

A *latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{array}{|cccc} \hline 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{array}$ is a latin square of order 4.

Subsquares

A *latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{array}{|cccc} \hline 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{array}$ is a latin square of order 4.

In a latin square, a *subsquare* is a submatrix that is itself a latin square.

Subsquares

A *latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g.

$$\begin{array}{|cccc} \hline 1 & 2 & 3 & 4 \\ \boxed{2} & 4 & 1 & \boxed{3} \\ \boxed{3} & 1 & 4 & \boxed{2} \\ 4 & 3 & 2 & 1 \end{array}$$

is a subsquare of order 2.

In a latin square, a *subsquare* is a submatrix that is itself a latin square.

Subsquares

A *latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{array}{|cccc} \hline 1 & 2 & 3 & 4 \\ \boxed{2} & 4 & 1 & \boxed{3} \\ \boxed{3} & 1 & 4 & \boxed{2} \\ 4 & 3 & 2 & 1 \end{array}$ is a subsquare of order 2.

In a latin square, a *subsquare* is a submatrix that is itself a latin square.

A subsquare of order 2 is an *intercalate*.

Subsquares

A *latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{array}{|cccc} \hline 1 & 2 & 3 & 4 \\ \boxed{2} & 4 & 1 & \boxed{3} \\ \boxed{3} & 1 & 4 & \boxed{2} \\ 4 & 3 & 2 & 1 \end{array}$ is a subsquare of order 2.

In a latin square, a *subsquare* is a submatrix that is itself a latin square.

A subsquare of order 2 is an *intercalate*.

n will always be the order of my latin square.
k will always be the order of my subsquare.

Subsquares

A *latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g. $\begin{array}{|cccc} 1 & 2 & 3 & 4 \\ \boxed{2} & 4 & 1 & \boxed{3} \\ \boxed{3} & 1 & 4 & \boxed{2} \\ 4 & 3 & 2 & 1 \end{array}$ is a subsquare of order 2.

In a latin square, a *subsquare* is a submatrix that is itself a latin square.

A subsquare of order 2 is an *intercalate*.

n will always be the order of my latin square.
k will always be the order of my subsquare.

A subsquare is *proper* provided $1 < k < n$.

Subsquares

A *latin square* of order n is an $n \times n$ matrix in which each of n symbols occurs exactly once in each row and once in each column.

e.g.
$$\begin{array}{|cccc} \hline 1 & 2 & 3 & 4 \\ \boxed{2} & 4 & 1 & \boxed{3} \\ \boxed{3} & 1 & 4 & \boxed{2} \\ 4 & 3 & 2 & 1 \end{array}$$
is a subsquare of order 2.

In a latin square, a *subsquare* is a submatrix that is itself a latin square.

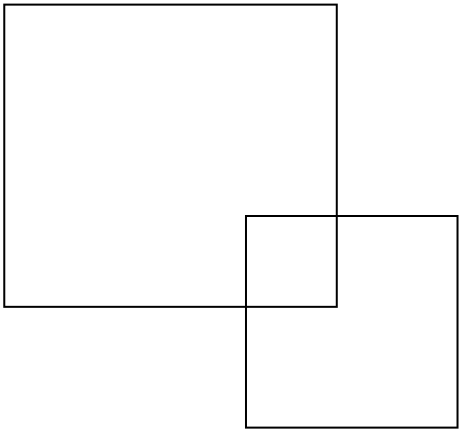
A subsquare of order 2 is an *intercalate*.

n will always be the order of my latin square.
k will always be the order of my subsquare.

A subsquare is *proper* provided $1 < k < n$. In fact $k \leqslant n/2$.

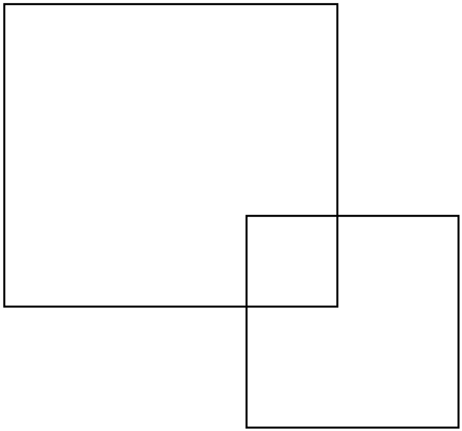
Intersectionality

The intersection of two subsquares...



Intersectionality

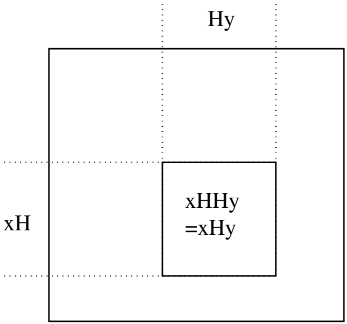
The intersection of two subsquares...



...is itself a subsquare.

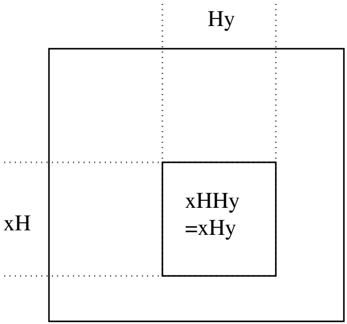
Group tables

Suppose H is a subgroup of order k in a group G of finite order n.



Group tables

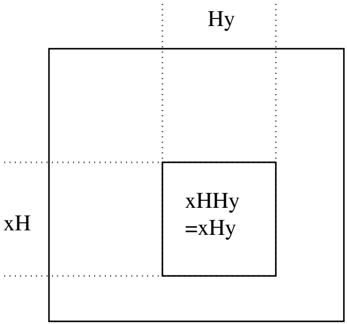
Suppose H is a subgroup of order k in a group G of finite order n.



...produces a subsquare of order k in the Cayley table of G.

Group tables

Suppose H is a subgroup of order k in a group G of finite order n.

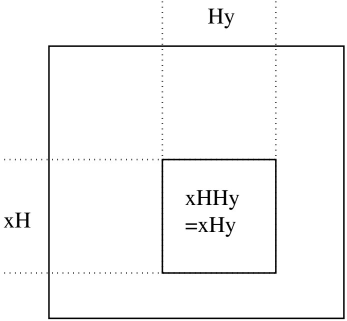


...produces a subsquare of order k in the Cayley table of G.

In fact, this is the only way that subsquares arise in group tables.

Group tables

Suppose H is a subgroup of order k in a group G of finite order n.



...produces a subsquare of order k in the Cayley table of G.

In fact, this is the only way that subsquares arise in group tables.

Corollary: The number of subsquares of order k in G is $(n/k)^2$ times the number of subgroups of order k.

Minimum number of subsquares

Consider the set of latin squares of order n.

Minimum number of subsquares

Consider the set of latin squares of order n.

The minimum number of $k \times k$ subsquares is 0 for almost all values of $1 < k < n$.

Minimum number of subsquares

Consider the set of latin squares of order n.

The minimum number of $k \times k$ subsquares is 0 for almost all values of $1 < k < n$.

If k does not divide n then we can use any group table.

Minimum number of subsquares

Consider the set of latin squares of order n.

The minimum number of $k \times k$ subsquares is 0 for almost all values of $1 < k < n$.

If k does not divide n then we can use any group table.
In other cases you have to be a bit cleverer, but it is (almost always) possible to avoid subsquares of order k.

Minimum number of subsquares

Consider the set of latin squares of order n.

The minimum number of $k \times k$ subsquares is 0 for almost all values of $1 < k < n$.

If k does not divide n then we can use any group table. In other cases you have to be a bit cleverer, but it is (almost always) possible to avoid subsquares of order k.

The two most studied problems are constructions for

- N_2 latin squares; i.e. ones without intercalates, and
- N_∞ latin squares; i.e. ones without proper subsquares

Intercalate-free latin squares

Theorem: For all orders $n \notin \{2, 4\}$ there exists a latin square with no intercalates.

Intercalate-free latin squares

Theorem: For all orders $n \notin \{2, 4\}$ there exists a latin square with no intercalates.

This was proved by a sequence of papers including:

- [Kotzig/Lindner/Rosa'75] Orders that aren't powers of 2.
- [McLeish'75] Powers of 2 that are > 32.
- [Kotzig/Turgeon'76] 16 and 32.
- [Denniston'78] catalogues all examples of order 8.
- [McLeish'80] (corrected in [W'01]) constructs examples for $n > 30$.

Subsquare-free latin squares

A tougher problem is to avoid all proper subsquares.

Subsquare-free latin squares

A tougher problem is to avoid all proper subsquares.

Conjecture: [Hilton'70] N_∞ latin squares exist for all $n \notin \{4, 6\}$.

Subsquare-free latin squares

A tougher problem is to avoid all proper subsquares.

Conjecture: [Hilton'70] N_∞ latin squares exist for all $n \notin \{4, 6\}$.

This conjecture has been confirmed as follows:

- [Denniston'78] Order 8.
- [Heinrich'80] Orders $pq \neq 6$ for primes p, q.
- [Andersen/Mendelsohn'82] Orders divisible by a prime $\geqslant 5$.
- [Gibbons/Mendelsohn'91] Order 12.
- [Elliot/Gibbons'92] Order 16,18.
- [W.'97] Orders < 256.
- [Maenhaut/W./Webb'07] Odd orders.
- [Allsop/W.'24+] All remaining orders.

Corrupted product

Let A, B be Latin squares of the same order that agree only in their principal entry.

Corrupted product

Let A, B be Latin squares of the same order that agree only in their principal entry.

Let M be an $m \times m$ Latin square.

Corrupted product

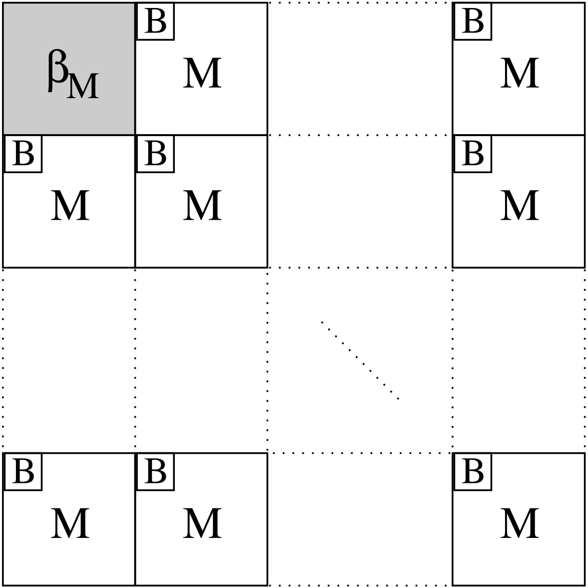
Let A, B be Latin squares of the same order that agree only in their principal entry.

Let M be an $m \times m$ Latin square.

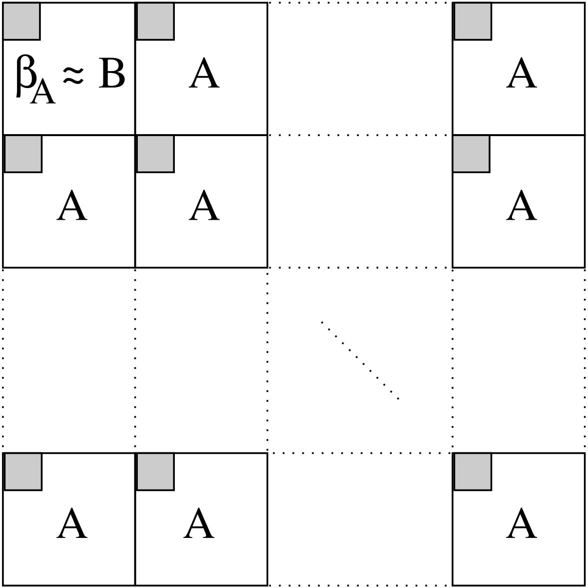
The *corrupted product* $P = (A, B) *_s M$ of shift $s \not\equiv 0 \bmod m$ is defined by

$$P\big[(i,j),(k,l)\big] = \begin{cases} \big(A[i,k], (M[j,l]+s)_m\big) & i = k = 1, \\ \big(B[i,k], M[j,l]\big) & (i,k) \neq (1,1) = (j,l), \\ \big(A[i,k], M[j,l]\big) & \text{otherwise;} \end{cases}$$

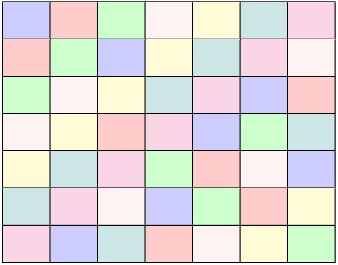
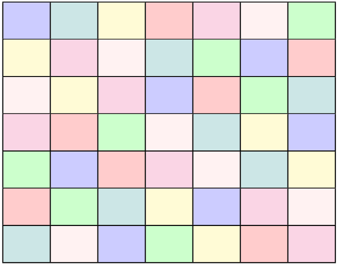
Corrupted products



Corrupted products



Corrupted products

$A =$  , $B =$  .

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

The corrupted product $(A, B) *_1 M$ is ...

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

.

Corrupted product

In [W'2001] I showed that, under certain conditions, the corrupted product has a unique subsquare.

Corrupted product

In [W'2001] I showed that, under certain conditions, the corrupted product has a unique subsquare.

To destroy this subsquare we switch a row cycle of length 3:

$$\left[\begin{array}{ccc} a & b & c \\ b & c & a \end{array}\right] \longrightarrow \left[\begin{array}{ccc} b & c & a \\ a & b & c \end{array}\right]$$

Corrupted product

In [W'2001] I showed that, under certain conditions, the corrupted product has a unique subsquare.

To destroy this subsquare we switch a row cycle of length 3:

$$\begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix} \longrightarrow \begin{bmatrix} b & c & a \\ a & b & c \end{bmatrix}$$

We use "corrupting pairs" (A,B) of order 8 and order 9 respectively to enlarge our N_∞ LSs by a factor of 8,9. The hard part is getting the inductive hypothesis right to allow us to repeatedly do this.

Corrupted product

In [W'2001] I showed that, under certain conditions, the corrupted product has a unique subsquare.

To destroy this subsquare we switch a row cycle of length 3:

$$\begin{bmatrix} a & b & c \\ b & c & a \end{bmatrix} \longrightarrow \begin{bmatrix} b & c & a \\ a & b & c \end{bmatrix}$$

We use "corrupting pairs" (A,B) of order 8 and order 9 respectively to enlarge our N_∞ LSs by a factor of 8,9. The hard part is getting the inductive hypothesis right to allow us to repeatedly do this.

Once we have that in place, we just need base cases of sizes $\{12, 16, 18, 24, 32, 36, 48, 54, 64, 72\}$.

Maximum number of intercalates

Let $S_k(n)$ be the maximum, over all order n latin squares, of the number of order k subsquares.

Maximum number of intercalates

Let $S_k(n)$ be the maximum, over all order n latin squares, of the number of order k subsquares.

Theorem: $S_2(n) \leqslant \frac{1}{4}n^2(n-1)$, with equality only achieved by elementary abelian 2-groups. [Heinrich/Wallis'81]

Maximum number of intercalates

Let $S_k(n)$ be the maximum, over all order n latin squares, of the number of order k subsquares.

Theorem: $S_2(n) \leqslant \frac{1}{4}n^2(n-1)$, with equality only achieved by elementary abelian 2-groups. [Heinrich/Wallis'81]

HW also showed that $S_2(n) > \frac{1}{45}n^3 + O(n^2)$.

Maximum number of intercalates

Let $S_k(n)$ be the maximum, over all order n latin squares, of the number of order k subsquares.

Theorem: $S_2(n) \leqslant \frac{1}{4}n^2(n-1)$, with equality only achieved by elementary abelian 2-groups. [Heinrich/Wallis'81]

HW also showed that $S_2(n) > \frac{1}{45}n^3 + O(n^2)$.

[Bartlett'13] & [Browning/Cameron/W.'14] show that $S_2(n) > \frac{1}{8}n^3 + O(n^2)$.

Maximum number of intercalates

Let $S_k(n)$ be the maximum, over all order n latin squares, of the number of order k subsquares.

Theorem: $S_2(n) \leqslant \frac{1}{4}n^2(n-1)$, with equality only achieved by elementary abelian 2-groups. [Heinrich/Wallis'81]

HW also showed that $S_2(n) > \frac{1}{45}n^3 + O(n^2)$.

[Bartlett'13] & [Browning/Cameron/W.'14] show that
$S_2(n) > \frac{1}{8}n^3 + O(n^2)$.
(The dihedral group has this many intercalates.)

Maximum number of intercalates

Let $S_k(n)$ be the maximum, over all order n latin squares, of the number of order k subsquares.

Theorem: $S_2(n) \leqslant \frac{1}{4}n^2(n-1)$, with equality only achieved by elementary abelian 2-groups. [Heinrich/Wallis'81]

HW also showed that $S_2(n) > \frac{1}{45}n^3 + O(n^2)$.

[Bartlett'13] & [Browning/Cameron/W.'14] show that
$S_2(n) > \frac{1}{8}n^3 + O(n^2)$.
(The dihedral group has this many intercalates.)

The latter paper also showed that elementary abelian 2-groups uniquely maximise the number of subsquares of order $k = 2^t$.

Subsquares of order 3

From [van Rees'90],

Theorem: $S_3(n) \leqslant \frac{1}{18} n^2(n-1)$, with equality when $n = 3^a$ for some a.

Subsquares of order 3

From [van Rees'90],

Theorem: $S_3(n) \leqslant \frac{1}{18}n^2(n-1)$, with equality when $n = 3^a$ for some a.

Conjecture: Equality is *only* achieved when $n = 3^a$.

Subsquares of order 3

From [van Rees'90],

Theorem: $S_3(n) \leqslant \frac{1}{18}n^2(n-1)$, with equality when $n = 3^a$ for some a.

Conjecture: Equality is *only* achieved when $n = 3^a$.

The conjecture is open, though from [Kinyon/W'11] we know

- It is true for $n < 33$.

Subsquares of order 3

From [van Rees'90],

Theorem: $S_3(n) \leqslant \frac{1}{18}n^2(n-1)$, with equality when $n = 3^a$ for some a.

Conjecture: Equality is *only* achieved when $n = 3^a$.

The conjecture is open, though from [Kinyon/W'11] we know

- It is true for $n < 33$.
- Equality can only be achieved for $n \equiv 3 \mod 6$.

Subsquares of order 3

From [van Rees'90],

Theorem: $S_3(n) \leqslant \frac{1}{18}n^2(n-1)$, with equality when $n = 3^a$ for some a.

Conjecture: Equality is *only* achieved when $n = 3^a$.

The conjecture is open, though from [Kinyon/W'11] we know

- It is true for $n < 33$.
- Equality can only be achieved for $n \equiv 3 \mod 6$.
- There are many interesting examples that achieve equality, not just the elementary abelian 3-groups. (There are at least 8 species of examples for $n = 27$.)

Subsquares of order 3

From [van Rees'90],

Theorem: $S_3(n) \leqslant \frac{1}{18}n^2(n-1)$, with equality when $n = 3^a$ for some a.

Conjecture: Equality is *only* achieved when $n = 3^a$.

The conjecture is open, though from [Kinyon/W'11] we know

- It is true for $n < 33$.
- Equality can only be achieved for $n \equiv 3 \mod 6$.
- There are many interesting examples that achieve equality, not just the elementary abelian 3-groups. (There are at least 8 species of examples for $n = 27$.)
- A quasigroup achieves equality iff every loop-isotope has exponent 3.

Subsquares of order 3

From [van Rees'90],

Theorem: $S_3(n) \leqslant \frac{1}{18}n^2(n-1)$, with equality when $n = 3^a$ for some a.

Conjecture: Equality is *only* achieved when $n = 3^a$.

The conjecture is open, though from [Kinyon/W'11] we know

- It is true for $n < 33$.
- Equality can only be achieved for $n \equiv 3 \mod 6$.
- There are many interesting examples that achieve equality, not just the elementary abelian 3-groups. (There are at least 8 species of examples for $n = 27$.)
- A quasigroup achieves equality iff every loop-isotope has exponent 3.
- There is a Steiner triple system associated with every row, column and symbol in any example that achieves equality.

Prime k

$S_2(n) \leqslant \frac{1}{4}n^2(n-1).$

$S_3(n) \leqslant \frac{1}{18}n^2(n-1).$

Prime k

$S_2(n) \leqslant \frac{1}{4}n^2(n-1).$

$S_3(n) \leqslant \frac{1}{18}n^2(n-1).$

Theorem: Fix a prime p. No latin square can have more than cubically many subsquares that are isotopic to $\mathbb{Z}_p$.

Prime k

$S_2(n) \leqslant \frac{1}{4}n^2(n-1)$.

$S_3(n) \leqslant \frac{1}{18}n^2(n-1)$.

Theorem: Fix a prime p. No latin square can have more than cubically many subsquares that are isotopic to $\mathbb{Z}_p$.

In fact you can't have more than cubically many copies of any subsquare that contains a cycle of length more than $k/2$.

Prime k

$S_2(n) \leqslant \frac{1}{4}n^2(n-1)$.

$S_3(n) \leqslant \frac{1}{18}n^2(n-1)$.

Theorem: Fix a prime p. No latin square can have more than cubically many subsquares that are isotopic to $\mathbb{Z}_p$.

In fact you can't have more than cubically many copies of any subsquare that contains a cycle of length more than $k/2$.

Open problem: Is there a family of latin squares with more than cubically many subsquares of order p?

Other small orders

Let $\psi(k)$ be the "correct exponent" for $S_k(n)$ as $n \to \infty$.

Formally, $\psi(k) = \limsup_{n\to\infty} \dfrac{\log S_k(n)}{\log n}$.

Other small orders

Let $\psi(k)$ be the "correct exponent" for $S_k(n)$ as $n \to \infty$.

Formally, $\psi(k) = \limsup_{n\to\infty} \dfrac{\log S_k(n)}{\log n}$.

k	$\psi(k)$
1	2
2	3
3	3
4	4
5	3
6	4
7	$3\ldots4$
8	5
9	4
10	4

Other small orders

Let $\psi(k)$ be the "correct exponent" for $S_k(n)$ as $n \to \infty$.

Formally, $\psi(k) = \limsup_{n\to\infty} \dfrac{\log S_k(n)}{\log n}$.

k	$\psi(k)$	
1	2	
2	3	
3	3	
4	4	
5	3	
6	4	$\longleftarrow \quad \mathbb{Z}_3^t \rtimes \mathbb{Z}_2$
7	$3 \ldots 4$	
8	5	
9	4	
10	4	$\longleftarrow \quad \mathbb{Z}_5^t \rtimes \mathbb{Z}_2$

General bounds

[Browning,Vojtěchovský,W'10] showed that $S_k(n) \leqslant n^{O(\sqrt{k})}$.

General bounds

[Browning,Vojtěchovský,W'10] showed that $S_k(n) \leqslant n^{O(\sqrt{k})}$.

[Browning,Stones,W'11] showed $S_k(n) \leqslant n^{\lceil \log_2 k \rceil + 2}$.

General bounds

[Browning,Vojtěchovský,W'10] showed that $S_k(n) \leqslant n^{O(\sqrt{k})}$.

[Browning,Stones,W'11] showed $S_k(n) \leqslant n^{\lceil \log_2 k \rceil + 2}$.

[Browning/Cameron/W.'14] show $S_k(n) \leqslant n^{3+\lfloor \log_2(k/3) \rfloor}$ when k is not a power of 2.

General bounds

[Browning,Vojtěchovský,W'10] showed that $S_k(n) \leqslant n^{O(\sqrt{k})}$.

[Browning,Stones,W'11] showed $S_k(n) \leqslant n^{\lceil \log_2 k \rceil + 2}$.

[Browning/Cameron/W.'14] show $S_k(n) \leqslant n^{3+\lfloor \log_2(k/3) \rfloor}$ when k is not a power of 2.

Proof idea: Recursively compile a list of subsquares by taking all subsquares which minimally contain some proper subsquare in your list.

General bounds

[Browning,Vojtěchovský,W'10] showed that $S_k(n) \leqslant n^{O(\sqrt{k})}$.

[Browning,Stones,W'11] showed $S_k(n) \leqslant n^{\lceil \log_2 k \rceil + 2}$.

[Browning/Cameron/W.'14] show $S_k(n) \leqslant n^{3+\lfloor \log_2(k/3) \rfloor}$ when k is not a power of 2.

Proof idea: Recursively compile a list of subsquares by taking all subsquares which minimally contain some proper subsquare in your list.

N.B. Elementary abelian 2 groups have $S_k(n) = \Theta(n^{2+\log_2 k})$ when k is a power of 2.

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have?

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

[McKay/W'99] conjectured that there will be $\mu_n(1+o(1))$ intercalates,

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

[McKay/W'99] conjectured that there will be $\mu_n(1+o(1))$ intercalates, and showed that almost all latin squares have at least $n^{3/2-\varepsilon}$ intercalates.

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

[McKay/W'99] conjectured that there will be $\mu_n(1+o(1))$ intercalates, and showed that almost all latin squares have at least $n^{3/2-\varepsilon}$ intercalates. Also, the probability of being N_2 is $O(\exp(-n^{2-\varepsilon}))$.

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

[McKay/W'99] conjectured that there will be $\mu_n(1+o(1))$ intercalates, and showed that almost all latin squares have at least $n^{3/2-\varepsilon}$ intercalates. Also, the probability of being N_2 is $O(\exp(-n^{2-\varepsilon}))$.

[Cavenagh/Greenhill/W'08] showed that almost surely there are at most $5n^{5/2}$ intercalates.

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

[McKay/W'99] conjectured that there will be $\mu_n(1+o(1))$ intercalates, and showed that almost all latin squares have at least $n^{3/2-\varepsilon}$ intercalates. Also, the probability of being N_2 is $O(\exp(-n^{2-\varepsilon}))$.

[Cavenagh/Greenhill/W'08] showed that almost surely there are at most $5n^{5/2}$ intercalates.

[Kwan/Sudakov'18] Showed there will be at least $\mu_n(1-o(1))$ intercalates.

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

[McKay/W'99] conjectured that there will be $\mu_n(1+o(1))$ intercalates, and showed that almost all latin squares have at least $n^{3/2-\varepsilon}$ intercalates. Also, the probability of being N_2 is $O(\exp(-n^{2-\varepsilon}))$.

[Cavenagh/Greenhill/W'08] showed that almost surely there are at most $5n^{5/2}$ intercalates.

[Kwan/Sudakov'18] Showed there will be at least $\mu_n(1-o(1))$ intercalates.
[Kwan/Sah/Sawhney'22] Proved a matching upper bound, proving the MW Conjecture.

The typical number of intercalates

If we choose a latin square at random how many intercalates will it have? Let $\mu_n = \frac{1}{4}n(n-1)$.

[McKay/W'99] conjectured that there will be $\mu_n(1+o(1))$ intercalates, and showed that almost all latin squares have at least $n^{3/2-\varepsilon}$ intercalates. Also, the probability of being N_2 is $O(\exp(-n^{2-\varepsilon}))$.

[Cavenagh/Greenhill/W'08] showed that almost surely there are at most $5n^{5/2}$ intercalates.

[Kwan/Sudakov'18] Showed there will be at least $\mu_n(1-o(1))$ intercalates.
[Kwan/Sah/Sawhney'22] Proved a matching upper bound, proving the MW Conjecture.
[Kwan/Sah/Sawhney/Simkin'23] showed that the probability of being N_2 is at least $\exp(-\mu_n + o(n^2))$.

The typical number of larger subsquares

[McKay/W'99] conjectured that the expected number of subsquares of order 3 will be $1/18$,

The typical number of larger subsquares

[McKay/W'99] conjectured that the expected number of subsquares of order 3 will be $1/18$, and that there will almost surely be no larger proper subsquare.

The typical number of larger subsquares

[McKay/W'99] conjectured that the expected number of subsquares of order 3 will be $1/18$, and that there will almost surely be no larger proper subsquare.

[Divoux/Kelly/Kennedy/Sidhu'23+] and [Gill/Mammoliti/W.'24+] show this conjecture for $k > \sqrt{n \log n}$.

The typical number of larger subsquares

[McKay/W'99] conjectured that the expected number of subsquares of order 3 will be $1/18$, and that there will almost surely be no larger proper subsquare.

[Divoux/Kelly/Kennedy/Sidhu'23+] and [Gill/Mammoliti/W.'24+] show this conjecture for $k > \sqrt{n \log n}$.

It follows that Latin square isomorphism can be tested in average-case polynomial time.

Summary of open problems

- van Rees conjecture (on maximising 3×3 subsquares).

Summary of open problems

- van Rees conjecture (on maximising 3×3 subsquares).
- How close can you get to the van Rees bound?

Summary of open problems

- van Rees conjecture (on maximising 3×3 subsquares).
- How close can you get to the van Rees bound?
- Can you embed more than cubically many STS(7)'s?

Summary of open problems

- van Rees conjecture (on maximising 3×3 subsquares).
- How close can you get to the van Rees bound?
- Can you embed more than cubically many STS(7)'s?
- Is it possible to have more than cubically many subsquares of (prime) order p?

Summary of open problems

- van Rees conjecture (on maximising 3×3 subsquares).
- How close can you get to the van Rees bound?
- Can you embed more than cubically many STS(7)'s?
- Is it possible to have more than cubically many subsquares of (prime) order p?
- Find the expected number of 3×3 subsquares.

Summary of open problems

- van Rees conjecture (on maximising 3×3 subsquares).
- How close can you get to the van Rees bound?
- Can you embed more than cubically many STS(7)'s?
- Is it possible to have more than cubically many subsquares of (prime) order p?
- Find the expected number of 3×3 subsquares.
- Show that subsquares of order > 3 are unlikely.

Summary of open problems

- van Rees conjecture (on maximising 3×3 subsquares).
- How close can you get to the van Rees bound?
- Can you embed more than cubically many STS(7)'s?
- Is it possible to have more than cubically many subsquares of (prime) order p?
- Find the expected number of 3×3 subsquares.
- Show that subsquares of order > 3 are unlikely.
- Can isomorphism be solved in average case polynomial time for STS and 1-factorisations?

The End!

The End!

That's all folks!!

Chein loops

$\otimes$	$(y,0)$	$(y,1)$
$(x,0)$	$(xy,0)$	$(yx,1)$
$(x,1)$	$(xy^{-1},1)$	$(y^{-1}x,0)$

Where the first coordinate is calculated in a subgroup G of index 2.

Chein loops

$\otimes$	$(y,0)$	$(y,1)$
$(x,0)$	$(xy,0)$	$(yx,1)$
$(x,1)$	$(xy^{-1},1)$	$(y^{-1}x,0)$

Where the first coordinate is calculated in a subgroup G of index 2.

Take G to be of exponent p and consider any subgroup H of order p.

Chein loops

$\otimes$	$(y, 0)$	$(y, 1)$
$(x, 0)$	$(xy, 0)$	$(yx, 1)$
$(x, 1)$	$(xy^{-1}, 1)$	$(y^{-1}x, 0)$

Where the first coordinate is calculated in a subgroup G of index 2.

Take G to be of exponent p and consider any subgroup H of order p. Then

$\otimes$	$(Hb, 0)$	$(cHa^{-1}, 1)$
$(aH, 0)$	$(aHb, 0)$	$(cH, 1)$
$(cHb, 1)$	$(cH, 1)$	$(aHb, 0)$

gives us a subsquare of order $2p$.

van Rees loops of order 27

- Elementary abelian group.
- Non-abelian group of exponent 3.
- A Bol loop with trivial center, discovered by [Keedwell'63].
- Two power-associative conjugacy closed loops, described in [Kinyon/Kunen'06].
- A universal left conjugacy closed loop (which is not conjugacy closed) with the left inverse property.
- A commutative, weak inverse property loop.
- A (noncommutative) weak inverse property loop such that each inner mapping of the form $L_x^{-1}R_x$ is an automorphism.

The Bol loop is the only one where each loop in the species has trivial center.

There are no other examples of order 27 with at least one nontrivial nucleus.