Sudoku, Counting, and Orthogonality
INMAA Student Workshop

Crystal Lorch and John Lorch

Ball State University

April 10, 2010

Workshop Outline

- Introduction to sudoku

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

A linear sudoku solution of parallel type

Workshop Outline

- Introduction to sudoku
- Counting junior sudoku solutions: two methods

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

A linear sudoku solution of parallel type

Workshop Outline

- Introduction to sudoku
- Counting junior sudoku solutions: two methods
- Linearity in the context of sudoku solutions

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

A linear sudoku solution of parallel type

Workshop Outline

- Introduction to sudoku
- Counting junior sudoku solutions: two methods
- Linearity in the context of sudoku solutions
- Producing orthogonal sudoku mates

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

A linear sudoku solution of parallel type

Latin square and sudoku definitions

- A **latin square** of order n^2 is an $n^2 \times n^2$ array with n^2 distinct symbols. Each symbol appears once in each row and column.

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

Latin square of order 4

Latin square and sudoku definitions

- A **latin square** of order n^2 is an $n^2 \times n^2$ array with n^2 distinct symbols. Each symbol appears once in each row and column.
- Literature dates to Euler (1782); used in experimental design and error correcting codes.

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

Latin square of order 4

Latin square and sudoku definitions

- A **latin square** of order n^2 is an $n^2 \times n^2$ array with n^2 distinct symbols. Each symbol appears once in each row and column.
- Literature dates to Euler (1782); used in experimental design and error correcting codes.
- A **sudoku solution** is a latin square with an added condition: Each symbol appears in each $n \times n$ subsquare.

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

Latin square of order 4

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

Sudoku solution of order 4

Counting junior sudoku solutions

We refer to sudoku solutions of order 4 as *junior sudoku solutions*.

Counting junior sudoku solutions

We refer to sudoku solutions of order 4 as *junior sudoku solutions*.

Task

List all junior sudoku solutions with upper left subsquare $\begin{matrix} 0 & 1 \\ 2 & 3 \end{matrix}$.

Use your answer to determine the total number of junior sudoku solutions.

Counting junior sudoku solutions

We refer to sudoku solutions of order 4 as *junior sudoku solutions*.

Task

List all junior sudoku solutions with upper left subsquare $\begin{matrix} 0 & 1 \\ 2 & 3 \end{matrix}$.

Use your answer to determine the total number of junior sudoku solutions.

Example:

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

Counting junior sudoku solutions

We refer to sudoku solutions of order 4 as *junior sudoku solutions*.

Task

List all junior sudoku solutions with upper left subsquare $\begin{matrix} 0 & 1 \\ 2 & 3 \end{matrix}$.

Use your answer to determine the total number of junior sudoku solutions.

Example:

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

There are 12 junior sudoku solutions with a fixed upper-left subsquare, and 288 junior sudoku solutions total.

Counting latin squares and sudoku solutions

Some counting results:

There are 5524751496156892842531225600 latin squares of order 9. [S. Bammel and J. Rothenstein, 1975]

Counting latin squares and sudoku solutions

Some counting results:

There are 5524751496156892842531225600 latin squares of order 9. [S. Bammel and J. Rothenstein, 1975]

There are 6670903752021072936960 sudoku solutions of order 9. [B. Felgenhauer and F. Jarvis, 2005]

Counting latin squares and sudoku solutions

Some counting results:

There are 5524751496156892842531225600 latin squares of order 9. [S. Bammel and J. Rothenstein, 1975]

There are 6670903752021072936960 sudoku solutions of order 9. [B. Felgenhauer and F. Jarvis, 2005]

There are 776966836171770144107444346734230682311065600000 latin squares of order 11. [B.D. McKay and I.M. Wanless, 2005]

Interlude: sudoku anatomy

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

Location

Interlude: sudoku anatomy

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

Location

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

Row

Interlude: sudoku anatomy

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

Location

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

Column

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

Row

Interlude: sudoku anatomy

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

Location

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

Column

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

Row

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

Subsquare

Interlude: sudoku anatomy

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

Location

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

Column

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

Large row

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

Row

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

Subsquare

Interlude: sudoku anatomy

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

Location

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

Column

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

Large row

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

Row

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

Subsquare

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

Large column

Equivalence classes of sudoku solutions

Two sudoku solutions are **equivalent** if one can be obtained from the other by some combination of

- relabeling symbols, and
- rearranging the underlying grid in a way that preserves the set of sudoku solutions (e.g., rotation).

Equivalence classes of sudoku solutions

Two sudoku solutions are **equivalent** if one can be obtained from the other by some combination of

- relabeling symbols, and
- rearranging the underlying grid in a way that preserves the set of sudoku solutions (e.g., rotation).

How many "inequivalent" junior sudoku solutions are there? We present two approaches.

Equivalence classes of sudoku solutions

Two sudoku solutions are **equivalent** if one can be obtained from the other by some combination of

- relabeling symbols, and
- rearranging the underlying grid in a way that preserves the set of sudoku solutions (e.g., rotation).

How many "inequivalent" junior sudoku solutions are there? We present two approaches.

Task

Describe ways to rearrange the underlying grid so as to preserve the set of sudoku solutions. (When applied to any sudoku solution, such a rearrangement should yield another sudoku solution.)

Sudoku group generators

Basic ways to produce equivalent sudoku solutions from a given solution:

- Relabeling
- Swap large rows; swap large columns
- Swap rows within a large row; swap columns within a large column
- 90° clockwise rotation
- reflection across the main diagonal (i.e., transpose)

Sudoku group generators

Basic ways to produce equivalent sudoku solutions from a given solution:

- Relabeling
- Swap large rows; swap large columns
- Swap rows within a large row; swap columns within a large column
- 90° clockwise rotation
- reflection across the main diagonal (i.e., transpose)

These manipulations, viewed as functions on the set X of sudoku solutions, generate a **group** G under function composition, called the **sudoku group**. The group G **acts** on X by

$$g.x = g(x), \qquad g \in G, x \in X.$$

Orbits

Let H be a group acting on X and $x \in X$. The set

$$H.x = \{h.x \mid h \in H\} \subset X$$

is called the **orbit** of H containing x.

Orbits

Let H be a group acting on X and $x \in X$. The set

$$H.x = \{h.x \mid h \in H\} \subset X$$

is called the **orbit** of H containing x.
For example, let ρ represent a 90° clockwise rotation, $R = \{e, \rho, \rho^2, \rho^3\} \subset G$ the subgroup of rotations, and

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

Orbits

Let H be a group acting on X and $x \in X$. The set

$$H.x = \{h.x \mid h \in H\} \subset X$$

is called the **orbit** of H containing x.

For example, let ρ represent a 90° clockwise rotation, $R = \{e, \rho, \rho^2, \rho^3\} \subset G$ the subgroup of rotations, and

$$x = \left[\begin{array}{cc|cc} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ \hline 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \end{array}\right].$$

Then

$$R.x = \left\{ \left[\begin{array}{cc|cc} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ \hline 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \end{array}\right], \left[\begin{array}{cc|cc} 3 & 1 & 2 & 0 \\ 2 & 0 & 3 & 1 \\ \hline 1 & 3 & 0 & 2 \\ 0 & 2 & 1 & 3 \end{array}\right] \right\}.$$

A sudoku subgroup and associated orbits

- Let X_{fix} denote the 12 sudoku solutions with fixed upper-left subsquare $\begin{matrix} 0 & 1 \\ 2 & 3 \end{matrix}$, and
- Let K denote the **subgroup** of the sudoku group whose elements leave the upper-left subsquare of any sudoku solution unchanged. Note that $K = \{e, r, c, rc\}$, where r swaps the bottom two rows and c swaps the rightmost two columns.

A sudoku subgroup and associated orbits

- Let X_{fix} denote the 12 sudoku solutions with fixed upper-left subsquare $\begin{matrix} 0 & 1 \\ 2 & 3 \end{matrix}$, and
- Let K denote the **subgroup** of the sudoku group whose elements leave the upper-left subsquare of any sudoku solution unchanged. Note that $K = \{e, r, c, rc\}$, where r swaps the bottom two rows and c swaps the rightmost two columns.

Task

(a) K acts on X_{fix}. List the elements of $K.x_1$, $K.x_2$, and $K.x_5$.

(b) Aside from those listed in part (a), are there any other K-orbits in X_{fix}?

(c) What do your answers to parts (a) and (b) say about the number of G-orbits in X? (Hint: Due to relabelings, every G-orbit in X intersects X_{fix}.)

At most three orbits

"Number of inequivalent sudoku solutions" = "Number of G-orbits in X"

At most three orbits

"Number of inequivalent sudoku solutions" = "Number of G-orbits in X"

Proposition

There are at most three G-orbits in X, namely $G.x_1$, $G.x_2$, and $G.x_5$.

At most three orbits

"Number of inequivalent sudoku solutions" = "Number of G-orbits in X"

Proposition

There are at most three G-orbits in X, namely $G.x_1$, $G.x_2$, and $G.x_5$.

- There are three K-orbits in X_{fix}: $K.x_1 = \{x_1, x_4, x_9, x_{12}\}$, $K.x_2 = \{x_2, x_3, x_{10}, x_{11}\}$, and $K.x_5 = \{x_5, x_6, x_7, x_8\}$.

At most three orbits

"Number of inequivalent sudoku solutions" = "Number of G-orbits in X"

Proposition

There are at most three G-orbits in X, namely $G.x_1$, $G.x_2$, and $G.x_5$.

- There are three K-orbits in X_{fix}: $K.x_1 = \{x_1, x_4, x_9, x_{12}\}$, $K.x_2 = \{x_2, x_3, x_{10}, x_{11}\}$, and $K.x_5 = \{x_5, x_6, x_7, x_8\}$.
- Any G-orbit in X meets X_{fix} due to relabelings.

At most three orbits

"Number of inequivalent sudoku solutions" = "Number of G-orbits in X"

Proposition

There are at most three G-orbits in X, namely $G.x_1$, $G.x_2$, and $G.x_5$.

- There are three K-orbits in X_{fix}: $K.x_1 = \{x_1, x_4, x_9, x_{12}\}$, $K.x_2 = \{x_2, x_3, x_{10}, x_{11}\}$, and $K.x_5 = \{x_5, x_6, x_7, x_8\}$.
- Any G-orbit in X meets X_{fix} due to relabelings.
- Let $G.x_i$ and $G.x_j$ be two distinct (therefore non-intersecting) G-orbits in X. Can assume $x_i, x_j \in X_{\text{fix}}$. Then $K.x_i$ and $K.x_j$ must be distinct orbits in X_{fix}.

At most two orbits

Proposition

There are at most two G-orbits in X, namely $G.x_1$ and $G.x_2$

At most two orbits

Proposition

There are at most two G-orbits in X, namely $G.x_1$ and $G.x_2$

Task

Show by producing an example that $G.x_2$ and $G.x_5$ have nontrivial intersection.

At most two orbits

Proposition

There are at most two G-orbits in X, namely $G.x_1$ and $G.x_2$

Task

Show by producing an example that $G.x_2$ and $G.x_5$ have nontrivial intersection.

Are the two remaining orbits, $G.x_1$ and $G.x_2$, really distinct or is there just a single G-orbit in X? Aside from brute force computation, how can we tell?

An invariant property

A property P that can be attributed to some elements of X is called **invariant** (or G-invariant) if for any $g \in G$ and $x \in X$ we have $g.x$ possessing P whenever x possesses P.

We can show that there are exactly two G-orbits in X by finding a property P that is

- G-invariant,
- possessed by x_1, and
- not possessed by x_2.

Invariant property: transversals

Definition

A **transversal** is a collection of four locations in which every row, column, and symbol is represented exactly once.

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

Invariant property: transversals

Definition

A **transversal** is a collection of four locations in which every row, column, and symbol is represented exactly once.

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

Possession of a transversal is a G-invariant property; x_1 possesses a transversal and x_2 does not.

Overview of results for junior sudoku

Theorem

There are 288 junior sudoku solutions but only 2 inequivalent solutions.

Overview of results for junior sudoku

Theorem

There are 288 junior sudoku solutions but only 2 inequivalent solutions.

Methods of establishing latter result of the theorem:

1. Invariant property (our previous investigation), and
2. Burnside's Formula:
   - $N \cdot |G| = \sum_{g \in G} |X^g|$ ($N=$ number of orbits, $X^g = \{x \in X \mid g.x = x\}$)
   - Need to know more about the structure of G to apply Burnside: $G \cong S_4 \times H$, where $H \cong (D_4 \times D_4) \rtimes \mathbb{Z}_2$.

Overview of results for ordinary sudoku

Theorem

(Jarvis and Russell, 2006) There are 5,472,730,538 inequivalent sudoku solutions of order 9.

Overview of results for ordinary sudoku

Theorem

(Jarvis and Russell, 2006) There are 5,472,730,538 inequivalent sudoku solutions of order 9*.*

- Method of proof: Burnside's Formula, using GAP for group computations.
- Can invariants be useful in counting order 9 sudoku solutions?

Array locations via a 4-dimensional vector space

- $\mathbb{Z}_3 = \{0, 1, 2\}$ is the finite field of order 3.
- **Array** of order 9 has 9 symbols each appearing 9 times.
- Each location has an **address** $x_1x_2x_3x_4 \in \mathbb{Z}_3^4$ where
  - x_1 and x_3 denote the large row and column, resp,
  - x_2 and x_4 denote the small row and column, resp.

0	1	2	1	2	0	8	6	7
3	4	5	7	8	6	2	0	*
6	7	8	4	5	3	5	3	4
1	2	0	5	3	4	2	0	1
4	5	3	6	7	8	0	1	2
7	8	6	8	6	7	3	4	5
2	0	1	3	4	5	7	8	6
5	3	4	6	7	8	1	2	0
8	6	7	0	1	2	4	5	3

Asterisk in location with address 0122

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

0 0 0	0 0 0	0 0 0

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001 \rangle$.

Parallel linear arrays

An array is **linear** if the locations housing any given symbol form a coset of a 2-dimensional subspace of $\mathbb{Z}_3^4$. Linear arrays come in two flavors:

- If every such coset originates from a *single* two dimensional subspace, then the array is of **parallel type**;
- otherwise the array is of **non-parallel type** (not discussed here).

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

Linear array of parallel type corresponding to $\langle 0010, 0001\rangle$.

Constructing a parallel array

Task

(a) List all nine members of the subspace $g = \langle 1002, 0212 \rangle \subset \mathbb{Z}_3^4$. (That is, find all linear combinations $a \cdot 1002 + b \cdot 0212$ where $a, b \in \mathbb{Z}_3$.)

(b) Draw a 9×9 grid and place the symbol '0' in the locations with addresses lying in g.

(c) Place the symbol '1' in the locations lying in $0100 + g$; '2' in $0200 + g$; '3' in $1000 + g$; '4' in $1100 + g$; '5' in $1200 + g$; '6' in $2000 + g$; '7' in $2100 + g$; '8' in $2200 + g$.

(d) Note that the resulting array M_g is a sudoku solution. Make conjectures as to what must be true of g in order for the resulting parallel linear array to be a sudoku solution.

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

M_g from task

From parallel linear arrays to sudoku solutions

Lemma

A pair of 2-planes in $\mathrm{Gr}(2, \mathbb{F}^4)$ intersect trivially if and only if any two cosets of these planes intersect in a single vector in $\mathbb{F}^4$.

Proposition

Let M_g be a linear array of parallel type generated by a 2-plane $g \in \mathrm{Gr}(2, \mathbb{F}^4)$. The array M_g is a sudoku solution if and only if g has trivial intersection with

$$\begin{aligned} g_c &= \langle 1000, 0100 \rangle, \\ g_r &= \langle 0010, 0001 \rangle, \text{ and} \\ g_{ss} &= \langle 0100, 0001 \rangle. \end{aligned}$$

Matrix representations of parallel linear sudoku solutions

If $A, B \in M^{2\times 2}(\mathbb{F})$ we let $\begin{bmatrix} A \\ B \end{bmatrix}$ denote the subspace of $\mathbb{F}^4$ spanned by the columns of the matrix $\begin{pmatrix} A \\ B \end{pmatrix}$.

Proposition

A 2-plane $g \in \mathrm{Gr}(2, \mathbb{F}^4)$ generates a linear sudoku solution of parallel type if and only if there exists a non-lower triangular invertible 2×2 matrix $C \in M^{2\times 2}(\mathbb{F})$ such that $g = \begin{bmatrix} I \\ C \end{bmatrix}$.

Proof of proposition (forward direction)

Assume $g = \begin{bmatrix} A \\ B \end{bmatrix}$ generates a linear sudoku solution of parallel type. Then A and B must be invertible to guarantee that g has trivial intersection with both g_r and g_c, respectively. Therefore

$$g = \begin{bmatrix} A \\ B \end{bmatrix} = \left[\begin{pmatrix} A \\ B \end{pmatrix} A^{-1} \right] = \begin{bmatrix} I \\ BA^{-1} \end{bmatrix},$$

and we choose $C = BA^{-1}$. The matrix C is invertible, and must also be non-lower triangular or else the second column of $\begin{pmatrix} I \\ C \end{pmatrix}$ will lie in $g \cap g_{ss}$, contradicting the fact that g and g_{ss} must have trivial intersection.

Definition of orthogonality

- Two latin squares are **orthogonal** if superimposition yields all possible ordered pairs of symbols.

Orthogonal squares

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

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

Definition of orthogonality

- Two latin squares are **orthogonal** if superimposition yields all possible ordered pairs of symbols.

Orthogonal squares

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

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

31	20	13	02
23	32	01	10
12	03	30	21
00	11	22	33

Definition of orthogonality

- Two latin squares are **orthogonal** if superimposition yields all possible ordered pairs of symbols.
- Orthogonality is preserved by
  - Relabeling either square
  - Rearrangement applied to both squares

Orthogonal squares

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

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

31	20	13	02
23	32	01	10
12	03	30	21
00	11	22	33

Questions about orthogonality

Questions about orthogonality:

1. How does one produce orthogonal pairs of sudoku solutions?

Questions about orthogonality

Questions about orthogonality:

1. How does one produce orthogonal pairs of sudoku solutions?

2. What can be said about the size of a family of mutually orthogonal sudoku solutions?

Questions about orthogonality

Questions about orthogonality:

1. How does one produce orthogonal pairs of sudoku solutions?

2. What can be said about the size of a family of mutually orthogonal sudoku solutions?

These are restrictions of classical questions about latin squares. We address these questions for **linear** sudoku solutions.

Linearity and orthogonality

Proposition

Let $g, h \in \mathrm{Gr}(2, \mathbb{F}^4)$ *and* M_g, M_h *be linear sudoku solutions of parallel type generated by* $g = \begin{bmatrix} I \\ C_1 \end{bmatrix}$ *and* $h = \begin{bmatrix} I \\ C_2 \end{bmatrix}$*, respectively. The following are equivalent:*

(a) *The two solutions are orthogonal.*

(b) g *and* h *have trivial intersection.*

(c) $\det(C_1 - C_2) \neq 0$.

Orthogonal parallel linear arrays

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

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

Linearity and orthogonality

Proposition

Let $g, h \in \mathrm{Gr}(2, \mathbb{F}^4)$ and M_g, M_h be linear sudoku solutions of parallel type generated by $g = \begin{bmatrix} I \\ C_1 \end{bmatrix}$ *and* $h = \begin{bmatrix} I \\ C_2 \end{bmatrix}$*, respectively. The following are equivalent:*

(a) *The two solutions are orthogonal.*

(b) *g and h have trivial intersection.*

(c) $\det(C_1 - C_2) \neq 0$.

Orthogonal parallel linear arrays

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

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

31	20	13	02
23	**3**2	0**1**	10
12	03	**3**0	2**1**
00	1**1**	22	**3**3

Task

Let $C_1 = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$ and $g = \begin{bmatrix} I \\ C_1 \end{bmatrix}$.

(a) Check that $g = \langle 1002, 0212 \rangle$. Observe from the previous task that g generates a parallel linear sudoku solution M_g.

(b) Find a 2×2 matrix C_2 such that $h = \begin{bmatrix} I \\ C_2 \end{bmatrix}$ generates a sudoku solution M_h that is orthogonal to M_g.

(c) Construct M_h and check directly that it and M_g form an orthogonal pair.

For example, if $h = \langle 1012, 0120 \rangle$, we have

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

M_h from task

Orthogonality result

Theorem

([2] or [7]) For each prime power q there exists a complete orthogonal family of sudoku solutions of order q^2 consisting of parallel linear solutions. The size of this family is $q(q-1)$.

- C. Arcos, G. Brookfield, and R. Krebs, *Mini-sudokus and groups*, Math. Mag. **83** no. 2 (2010), 111-122.
- R.A. Bailey, P.J. Cameron, and R. Connelly, *Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes*, Amer. Math. Monthly **115** (2008), 383-403.
- S. Bammel and J. Rothstein, *The number of* 9×9 *Latin squares*, Discrete Mathematics **11** (1975), 93-95.
- B. Felgenhauer and F. Jarvis, *Mathematics of Sudoku I*, Math. Spectrum **39** (2006), 15-22. to appear. (Preprint available at www.afjarvis.staff.shef.ac.uk/maths/felgenhauer_jarvis_spec1.pdf)
- F. Jarvis and E. Russell, *Mathematics of Sudoku II*, Math. Spectrum **39** (2006), 54-58. (Preprint available at www.afjarvis.staff.shef.ac.uk/maths/russell_jarvis_spec2.pdf).

- C. Lorch and J. Lorch, 'Enumerating small sudoku puzzles in a first abstract algebra course', *PRIMUS* **18** (2008), 149-158.
- J. Lorch, *Orthogonal combings of linear sudoku solutions*, Australas. J. Comb., to appear.
- J. Lorch, *A quick construction of mutually orthogonal sudoku solutions*, under review.
- B.D. McKay and I.M. Wanless, *On the Number of Latin Squares*, Ann. Combin. **9** (2005), 335-344.