On chromatic number of Latin square graphs

Laura Gutierrez Funderburk[1] L. Goddyn[1]

[1]Department of Mathematics
Simon Fraser University

CUMC, July 2016

Overview

- Definitions and examples
- Motivation of the problem
- What is currently known
- Conjectures and open problems

Definition

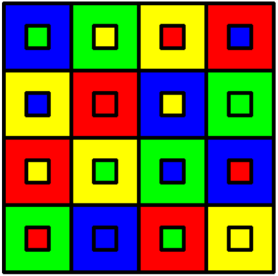
Latin Square: A *Latin square* ℓ of order n is an $n \times n$ array with cells $\{(r, c) | r, c \in \{0, 1, ..., n-1\}\}$; each cell contains a **symbol** from an alphabet of size n such that no symbol appears twice in any row or column.
Latin squares can be written as set of triples of the form (r, c, s).
For example,

a	b
b	a

can be written as $\{(1, 1, a), (1, 2, b), (2, 1, b), (2, 2, a)\}$

Definition

Orthogonal Mates: If there are two Latin Squares ℓ_1, ℓ_2, which when superimposed, give coordinates which are all different they are called **Mutually Orthogonal Latin Squares (MOLS)**. We say ℓ_1 is an orthogonal mate of ℓ_2 and vice versa.



Why is the study of Latin squares important?

In addition to being a mathematical object whose study I find absolutely fantastic, Latin squares have a wide range of applications that include but are not limited to cryptography, statistics and coding theory.
Here are two of my favourite examples.

Latin squares in Statistics

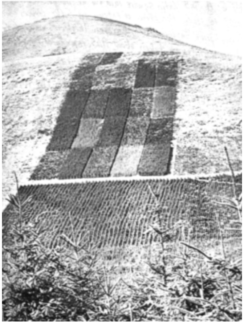
Latin squares are prominently applied to design experiments in statistics. Imagine we are asked to plant trees in a plantation. We have to choose all trees from one species (it is a plantation not a natural forest), but have say five species to choose from. How do we determine the species which is most suitable for our plantation?

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

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

A Latin square distribution of the test plants is a way to balance the bias of two factors.

Latin squares in Statistics



A 5 $\times$ 5 Latin square of 5 different tree species in Bettgelert Forest as part of an agricultural study. Photograph from around 1945. Plate 6 from J.F. Box, R.A. Fisher: The Life of a Scientist, Wiley New York, 1978.

Latin squares in Cryptography

The basic aim of cryptography is simple. A sender wants to send a message, but first encodes it so that no third party can read it. The receiver, upon receiving the same message, decodes it using the same code that was used to encrypt it. Latin squares can be used to achieve this. One way is by making use of MOLS of order n.

Latin squares in Cryptography

Consider the MOLS

$$\begin{matrix} |1\ 2\ 3|\ |3\ 1\ 2| \text{---} |(1,3)\ (2,1)\ (3,2)| \\ |2\ 3\ 1|\ |2\ 3\ 1| \text{---} |(2,2)\ (3,3)\ (1,1)| \\ |3\ 1\ 2|\ |1\ 2\ 3| \text{---} |(3,1)\ (1,2)\ (2,3)| \end{matrix}$$

and the letters

A I O
E C G
H L S

I can then send $(3,1),(2,2),(1,2),(1,2),(3,2)$ which says "HELLO".

Definition

Latin Square Graph: The *Latin square graph* of ℓ is the simple graph $\Gamma(\ell)$ whose vertices are the cells of ℓ and where distinct cells (r, c, s) and (r', c', s') are adjacent if (exactly) one of the equations $r = r', c = c', s = s'$ is satisfied.
Each edge of $\Gamma(\ell)$ is called, respectively, a **row edge**, a **column edge** or a **symbol edge**.

Definition

Cayley Table: Let $(G, \circ)$ be a finite group of order n. A *Cayley Table* for G is an $n \times n$ matrix, denoted L_G, where the (i, j) - cell contains the group element $g_i \circ g_j$, for some fixed enumeration $G = \{g_0, ..., g_{n-1}\}$.
If G is a cyclic group then L_G is called a **circulant** Latin square.

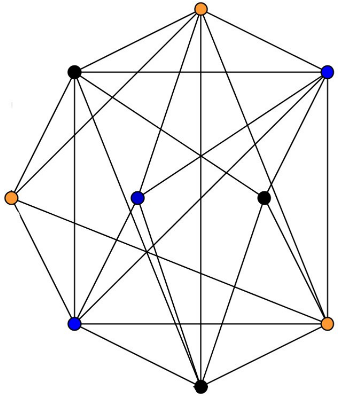
Example

Let $Z_3 = \{0, 1, 2\}$ and consider the group $(Z_3, +)$. Consider the Cayley table for Z_3, where each cell contains an element of the form $i + j$, for each $0 \leq i, j \leq 2$. This is a circulant Latin square denoted as L_{Z_3}

0	1	2
1	2	0
2	0	1

Example

We construct the graph of the circulant L_{Z_3}, denoted $\Gamma(L_{Z_3})$ with cells (i, j) for $i, j \in \{1, 2, 3\}$ each of which contains one symbol $g \in Z_3$. We denote this as (i, j, g).



Definition

Partial transversals of ℓ: A *partial transversal* of a Latin square ℓ of order n is a selection of $k < n$ cells where no two cells have the same row, column or symbol. If $k = n$ we simply call it a transversal of ℓ.

Chromatic number of ℓ: Let ℓ be a Latin square of order n. The *chromatic number* of ℓ, denoted by $\chi(\ell)$, is the minimum number of partial transversals of ℓ which together cover the cells of ℓ.

Why the chromatic number of Latin squares?

Although Latin square graphs have been widely studied as strongly regular graphs, their chromatic numbers appear to be unexplored. I next present some results on the paper "On the chromatic number of Latin squares", co-authored by L. Goddyn, N. Besharati, E.S. Mahmoodian and M. Morezaeefar.

Chromatic Number of Cayley Tables

Theorem 1[Goddyn, Besharati, Mahmoodian, Mortezaeefar, 2016]
For any finite group G of order n with identity element ϵ, the following are equivalent:
1. $\chi(L_G) = n$
2. $\chi(L_G) \leq n + 1$
3. L_G has a transversal
4. For some enumeration $g_1, g_2, ..., g_n$ of G we have $g_1 g_2 ... g_n = \epsilon$
5. Every Sylow 2-subgroup of G is either trivial or non-cyclic.

Chromatic Number of Cayley Tables

Corollary 2[Goddyn, Besharati, Mahmoodian, Mortezaeefar, 2016]
1. $\chi(L_G) = |G|$ for every group G of odd order.
2. For every group G of order n, either $\chi(L_G) = n$ or $\chi(L_G) \geq n + 2$.
3. Let G be an Abelian group of order n, $\chi(L_G) \geq n + 2$ if and only if G has a unique element of order 2.

Chromatic Number of Cayley Tables

Theorem 3[Goddyn, Besharati, Mahmoodian, Mortezaeefar, 2016]
For $n \geq 1$ the circulant Latin square of order n satisfies

$$\chi(L_{Z_n}) = n, \; n \text{ odd}$$
$$\chi(L_{Z_n}) = n+2, \; n \text{ even.}$$

Conjectures and Open problems

Conjecture 1.[Goddyn, Besharati, Mahmoodian, Mortezaeefar, 2016]
For all Latin square ℓ of order n,

$$n \leq \chi(\ell) \leq n+1, \text{ if } n \text{ is odd}$$
$$n \leq \chi(\ell) \leq n+2, \text{ if } n \text{ is even}$$

Conjecture 2.[Goddyn, Besharati, Mahmoodian, Mortezaeefar, 2016]
The same holds for the Cayley table for G, for any finite group G.
Open Problem.
Prove $\chi(L_{D_n}) \leq n+2$ for any Dihedral group D_n.

Further Reading and References I

[1] L. Goddyn, E.S. Mahmoodian, M. Mortezaeefar, N. Besharati.*On chromatic number of Latin square graphs*. Journal of Discrete Mathematics, 2016. [2] W. Baratta, J. Tang. *Latin Squares and their applications*. Oct 27 2009. [3] M. Schlund.*Graph Decompositions, Latin Squares, and Games*.

Thank you!