Proper loops of order $2p$, p a prime

Nimrod Kriger
jointly with Mikhail Klin

Summer Seminar on Symmetry, Computer Algebra, Algebraic Graph Theory and beyond
BGU 2025

September 2025

Outline

Loops

We wish to consider loops which in a sense are very close to groups, however are not equivalent to groups. On this way we consider 3-nets and and Latin square strongly regular graphs.

We will reach full description of such loops of order $2p$, where p is a prime. (For loops of order p, p a prime, there is just one class of nice objects: cyclic group of order p.)

Latin squares

A **Latin square** L of order n is an $n \times n$ array with n different entries, such that each entry occurs exactly once in each row and each column of the array. As a rule, we use $1, \dots, n$ as symbols.

L is in **standard form** if in the first row and column its elements $1, \dots, n$ occur in natural order.

Quasigroups and loops

A **quasigroup** is a set Q with a binary operation $*$ such that, for all $a, b \in Q$, the equations $a * x = b$ and $y * a = b$ have a unique solution in Q.
We will not distinguish between Latin squares and quasigroups.
A **loop** N is a quasigroup with an identity element e such that $e * x = x * e = x$ for all $x \in N$.
Naturally, each loop defines a standard form Latin square.

A 3-net of order n

A **3-net of order n** is an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ which consists of an n^2-element set $\mathcal{P}$ of points and a $3n$-element set $\mathcal{L}$ of lines. The set $\mathcal{L}$ is partitioned into three disjoint families $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ of (parallel) lines, for which the following conditions hold:

(i) every point is incident with exactly one line of each family $\mathcal{L}_i$ $(i = 1, 2, 3)$;

(ii) two lines of different families have exactly one point in common;

(iii) two lines of the same family do not have a common point;

(iv) there exist three lines belonging to three different families which are not incident with the same point.

Directions (parallel classes)

The families $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ are called the **directions** or **parallel classes** of $\mathcal{S}$.
Each Latin square L of order n naturally produces a 3-net.
Points of this net are formed by the cells of L, while its directions correspond to horizontal lines, vertical lines and the cells occupied in L by the same element.
If L corresponds to a quasigroup Q, then the resulting 3-net is denoted by $\mathcal{N}(Q)$.

Groups $\Sigma(Q)$ and $\mathcal{T}(Q)$

The **collineation group** $\Sigma = \Sigma(Q)$ of a quasigroup Q is the (full) collineation group of the 3-net $\mathcal{N}(Q)$. By collineation we mean a permutation of points of $\mathcal{N}(Q)$, which maps a line to a line.

The group Σ has a normal subgroup $\mathcal{T} = \mathcal{T}(Q)$
of index ≤ 6, which maps every class of (parallel) lines onto itself.

This group $\mathcal{T}$ may be called the group of *direction preserving collineations* of $\mathcal{N}(Q)$.

Latin square graph

Let L be a Latin square of order n and let Ω denote the n^2-element set of its cells.
Let us say that two cells are adjacent if they are in the same row, or in the same column, or are occupied by the same symbol.

Latin square graph

The resulted graph $SRG(L) = \Gamma = (\Omega, E)$, is a (v, k, λ, μ)-strongly regular graph which is called a **Latin square graph.**

Its parameters are $v = n^2,\ k = 3(n-1),\ \lambda = n$ and $\mu = 6$.

Each strongly regular graph with such parameters is called a **pseudo-Latin square graph**,

while one coming from a Latin square is a **geometric graph.**

For a small number of vertices there is a complete list of strongly regular graphs (Spence) and hence we know all small pseudo-Latin square graphs.

Main class of a Latin square

Note that any Latin square can be regarded as a subset of $\{1, \ldots, n\}^3$.
That is, $L = \{(x, y, z) | 1 \leq x, y, z \leq n\}$ such that z is the symbol in row x and column y.
Consider exponentiation $S_n \uparrow S_3$ of symmetric groups of degree n and 3. This is a group of order $6 \cdot (n!)^3$ acting on n^3 elements.
The orbit of L under the action of $S_n \uparrow S_3$ on its triples is the **main class** of L.
A loop Q is a **proper loop** if its main class does not contain a group.

Main corollaries about the group case

Each Latin square L is the multiplication table of some quasigroup Q.
If Q is a group, then L is a **group Latin square**.
We wish to know some properties of strongly regular graphs (briefly SRGs), which are coming from a group Latin square.

Theorem

The following theorem is a folklore one, cf. Heinze-Klin (2009): Let H be a group, $\Gamma = SRG(H)$ be a Latin square graph with $|H| \geq 5$. Then

$$\mathrm{Aut}(SRG(\Gamma)) \cong (H^2 : \mathrm{Aut}(H)).S_3$$

that is, the extension of H^2 :Aut(H) by S_3.

Corollary

If H is a group, then Aut(SRG(H)) contains a regular subgroup (of order n^2, $n = |H|$.)

Theorem

Moorhouse (1991) proved:

1. If H_1 and H_2 are nonisomorphic groups of order n, then $SRG(H_1) \ncong SRG(H_2)$.
2. If a Latin square L does not appear in a main class of any group, then $SRG(L)$ is not isomorphic to any Latin square graph over a group.

Remark of Barlotti and Strambach

In 1983 Barlotti and Strambach posed the following remark:
"We where not able to decide whether there exists a proper finite loop having a sharply point transitive group of collineations".
In other words, does there exist a proper loop Q such that $\Sigma(Q)$ contains a regular subgroup.

Loop Q_6 and its prosperities

Consider the following Latin square Q_6 (J. Dènes, A. D. Keedwell 1974):

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \\ 3 & 1 & 2 & 6 & 4 & 5 \\ 4 & 6 & 5 & 2 & 1 & 3 \\ 5 & 4 & 6 & 3 & 2 & 1 \\ 6 & 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

Proposition

A. Heinze and M. Klin (2009) proved the following proposition:

- The main class of Q_6 does not contain a group;
- $G = Aut(SRG(Q_6))$ is a transitive permutation group of degree 36 and order 648;
- G has a regular subgroup

Brief story of Q_6

The loop Q_6 was known for a long while.
Sprague showed that the net corresponding to Q_6 contains a vertex transitive group of order 36, isomorphic to $S_3 \times S_3$.
He also described a corresponding SRG as a Cayley graph.
However, the complete group $Aut(SRG(Q_6))$ was not investigated.

An infinite series Q_{2p}

A. Heinze and M. Klin (2009) introduced an infinite series of proper loops Q_{2p}, p a prime, $p \cong 3 \pmod 4$, for which the group $G = Aut(SRG(Q_{2p}))$ contains a regular subgroup of order $4p^2$.

Characterizations of these loops

We wish to describe all those loops of order $2p$ which satisfy the desired properties.
We will give a suitable sufficient condition to find desired proper loops of order $2p$ for a prime $p \geq 3$.

Formulation of the criterion

Theorem

Sprague (1982) proved: Let K be a group of order n^2. Then the following conditions are equivalent:

1. *There exists a Latin square graph Γ over a suitable quasigroup Q of order n such that K is a regular subgroup of $\mathcal{T}(Q)$;*
2. *The group K contains three subgroups X_1, X_2, X_3 of order n, any two of which have an intersection of size 1.*

A relation to Cayley graphs

In this case we have $X = X_1 \cup X_2 \cup X_3 \setminus \{e\}$, where e is the identity element of K.
X is the connection set of a Cayley graph over K which is isomorphic to SRG Γ.
Such a connection set is called a **partial difference set** over K.

The criterion in the group case

If the quasigroup Q in Sprague criterion is indeed a group, then this criterion is automatically fulfilled. (A. Heinze and M. Klin 2009)

Strategy of search

Using Sprague criterion, we can find in principle all loops Q, such that $\mathcal{T}(Q)$ contains a regular subgroup.
First we classify all groups of order n^2, (up to isomorphism).
Then inspect each group to decide whether or not it contains 3 subgroups as mentioned in Sprague criterion.

$n = 2p$

It is impossible to describe all groups of order n^2 for arbitrary n. However, if $n = 2p$, p a prime, then this task became practical. So the first step of this work was the classification of the groups of order $(2p)^2$ in a suitable manner for the continuation of the work.

General picture

One can try to find in literature description of all groups of order $4p^2$.
However, we preferred to do this by our own, in style and form suitable for our goals.

Let K be a group of order $4p^2$ where p is a prime greater than 3. According to Sylow Theorems, K contains a normal Sylow p-subgroup, say N.
So, K is isomorphic to $N \rtimes_\sigma Q$ where $N \lhd H$ is a subgroup of order p^2 and $|Q| = 4$.
In other words, all groups of order $4p^2$ can be classified according to the action σ of Q on N.

Two cases

Now, there are two options for both N and Q:
$N \cong \mathbb{Z}_p^2$ or $N \cong \mathbb{Z}_{p^2}$, $Q \cong \mathbb{Z}_2^2$ or $Q \cong \mathbb{Z}_4$.
So we have to check all actions of each 4-order group on each p^2-order group.
We consider two cases: $p \equiv 3 \ (mod\ 4)$ and $p \equiv 1 \ (mod\ 4)$

$p \equiv 3 \pmod 4$ (a)

We start with $N \cong \mathbb{Z}_p^2$.
Recall that $Aut(N) \cong GL(2,p)$.
Up to conjugacy relation, $GL(2,p)$ contains two groups of order 2, say

$$k_1 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle, \; k_2 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

and hence one conjugacy class of subgroups which isomorphic to $\mathbb{Z}_2^2$, namely, $k_4 = \langle k_1, k_2 \rangle$.
There is also one class of cyclic groups of order 4, say
$k_3 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$.
Now let $N \cong \mathbb{Z}_{p^2}$.
Here $Aut(N) \cong \mathbb{Z}_{\varphi(p)} = \mathbb{Z}_{p(p-1)}$.
In this case $Aut(N)$ contains only one subgroup of order 2, say k_5 and no subgroup of order 4.

$p \equiv 3 \pmod 4$ (b)

We can conclude that up to isomorphism there are 12 groups of order $4p^2$ for $p \equiv 3$ (*mod* 4):

- $\mathbb{Z}_p^2 \times \mathbb{Z}_4$;
- $\mathbb{Z}_p^2 \rtimes_{\sigma_i} \mathbb{Z}_4$, $\sigma_i : \mathbb{Z}_4 \to k_i$ for $i = 1, 2, 3$;
- $\mathbb{Z}_p^2 \times \mathbb{Z}_2^2$;
- $\mathbb{Z}_p^2 \rtimes_{\sigma_i} \mathbb{Z}_2^2$, $\sigma_i : \mathbb{Z}_2^2 \to k_i$ for $i = 1, 2, 4$;
- $\mathbb{Z}_{p^2} \times \mathbb{Z}_4$;
- $\mathbb{Z}_{p^2} \rtimes_{\sigma} \mathbb{Z}_4$, $\sigma : \mathbb{Z}_4 \to k_5$;
- $\mathbb{Z}_{p^2} \times \mathbb{Z}_2^2$;
- $\mathbb{Z}_{p^2} \rtimes_{\sigma} \mathbb{Z}_2^2$, $\sigma : \mathbb{Z}_2^2 \to k_5$;

$p \equiv 1 \pmod 4$ (a)

This case is very similar to the former case with the exception of four conjugacy classes of cyclic subgroups of order 4 in $GL(2,p)$, and one subgroup of order 4 in $\mathbb{Z}_{p(p-1)}$.
Let i denote the fourth root of unity in $\mathbb{Z}_p$, and let

$$c_1 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle, \; c_2 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix} \right\rangle,$$

$$c_3 = \left\langle \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \right\rangle, \; c_4 = \left\langle \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \right\rangle;$$

represent the four conjugacy classes.
Also, let k_6 be a subgroup of order 4 in $\mathbb{Z}_{p(p-1)}$.

$p \equiv 1 \pmod 4$ (b)

Considering above results we can summarize that up to isomorphism there are 16 groups of order $4p^2$ for $p \equiv 1$ $(mod\ 4)$.

- $\mathbb{Z}_p^2 \times \mathbb{Z}_4$;
- $\mathbb{Z}_p^2 \rtimes_{\sigma_i} \mathbb{Z}_4$, $\sigma_i : \mathbb{Z}_4 \to k_i$ for $i = 1, 2$;
- $\mathbb{Z}_p^2 \rtimes_{\sigma_i} \mathbb{Z}_4$, $\sigma_i : \mathbb{Z}_4 \to c_i$ for $i = 1, 2, 3, 4$;
- $\mathbb{Z}_p^2 \times \mathbb{Z}_2^2$;
- $\mathbb{Z}_p^2 \rtimes_{\sigma_i} \mathbb{Z}_2^2$, $\sigma_i : \mathbb{Z}_2^2 \to k_i$ for $i = 1, 2, 4$;
- $\mathbb{Z}_{p^2} \times \mathbb{Z}_4$;
- $\mathbb{Z}_{p^2} \rtimes_{\sigma_i} \mathbb{Z}_4$, $\sigma_i : \mathbb{Z}_4 \to k_i$ for $i = 5, 6$;
- $\mathbb{Z}_{p^2} \times \mathbb{Z}_2^2$;
- $\mathbb{Z}_{p^2} \rtimes_{\sigma} \mathbb{Z}_2^2$, $\sigma : \mathbb{Z}_2^2 \to k_5$;

Basic definitions and notations

- A group which contains three subgroups X_1, X_2, X_3, such that $|X_i| = 2p$ and $|X_i \cap X_j| = 1$ for $i, j = 1, 2, 3,\ i \neq j$ is called a **good group**
- The three subgroups X_1, X_2, X_3 in the above definition will be called a **good triple**

Elimination of non-good groups

Analyzing structure of all groups of order $4p^2$, we eliminate all but four groups.
Finally, we show that only groups of the form $\mathbb{Z}_p^2 \rtimes_\sigma \mathbb{Z}_2^2$ may , in principle, be good.

List of good groups

To prove that indeed all the four groups of the form $\mathbb{Z}_p^2 \rtimes_\sigma \mathbb{Z}_2^2$ are good, we need to provide an example of a good triple for each group $H_i = \mathbb{Z}_p^2 \rtimes_{\sigma_i} \mathbb{Z}_2^2$ for $i = 1, 2, 3, 4$ as follows:

- $$\sigma_1(t_1) = \sigma_1(t_2) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};$$
- $$\sigma_2(t_1) = \sigma_2(t_2) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix};$$
- $$\sigma_3(t_1) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_3(t_2) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix};$$
- $$\sigma_4(t_1) = \sigma_4(t_2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Examples of good triples

Here we present an example of a good triple T_i for each good group H_i, $i = 1, 2, 3, 4$.

- $$T_1 = (\langle[(1,0), t_1]\rangle, \langle[(1,1), t_3]\rangle, \langle[(0,1), t_2], [(0,1), t_0]\rangle);$$

- $$T_2 = (\langle[(1,0), t_0], [(1,0), t_1]\rangle, \langle[(0,1), t_0], [(0,1), t_1]\rangle, \langle[(1,1), t_3]\rangle);$$

- $$T_3 = (\langle[(1,0), t_2]\rangle, \ \langle[(0,1), t_1]\rangle, \ \langle[(1,1), t_0], [(0,0), t_3]\rangle);$$

- $$T_4 = (\langle[(1,0), t_2]\rangle, \ \langle[(0,1), t_1]\rangle, \ \langle[(1,1), t_3]\rangle).$$

Classification of good triples in H_1 (a)

H_1 contains $3p+3$ subgroups of order $2p$ as follows:

1. There are $2p$ cyclic subgroups of the form $\langle [(1,b),t_i] \rangle\,,\ i=1,2,\ b\in\mathbb{Z}_p$.
2. There are $p+1$ cyclic subgroups of the form $\langle [(1,b),t_3] \rangle\,,\ b\in\mathbb{Z}_p$ or $\langle [(0,1),t_3] \rangle$.
3. This group contains only two dihedral subgroups of order $2p$: $\langle [(0,1),t_i],[(0,1),t_0] \rangle$ for $i=1,2$.

Classification of good triples in H_1 (b)

A good triple must contain exactly one subgroup of each type as above.
So at all there are $2p(p-1)$ good triples, all in one orbit under the induced action of $Aut(H_1)$.

Classification of good triples in H_2

We can conclude that there are $p^3(p+1)(p-1)$ good triples, all in one orbit under the induced action of $Aut(H_2)$.

Classification of good triples in H_3 (a)

$H_3 \cong D_p \times D_p$, where D_p is dihedral group of order $2p$.
This observation simplifies our analysis.

Classification of good triples in H_3 (b)

In this case, we have $p^4 - p^3 + p^2 - p$ good triples which partition into three orbits under the induced action of $Aut(D_p \times D_p)$. In the following list we present a representative from each orbit, (using a suitable notation):

1. $(< a, b >, < x, y >, < ax, abxy >)$. This orbit contains $p^2 - p$ triples, and each triple contains three copies of D_p.
2. $(< ay >, < xb >, < ax, ax, by >)$. This orbit contains $p^3 - p^2$ triples, and each triple contains two copies of C_{2p} and one copy of D_p.
3. $(< ay >, < xb >, < ax, ax, bxy >)$. This orbit contains $p^2(p-1)^2$ triples, and each triple contains two copies of C_{2p} and one copy of D_p.

Classification of good triples in H_4

In H_4 we have $6 \cdot \binom{p+1}{3}$ good triples.
All these triples are laying in one orbit under the induced action of $Aut(H_4)$.

What does mean geometric graph in this case

According to Sprague criterion any good triple (K_1, K_2, K_3) in a group H, is yielding a Cayley graph $Cay(H, X)$ which is isomorphic to a Latin square graph $SRG(Q)$ over a suitable quasigroup Q. As explained before, $X = (K_1 \cup K_2 \cup K_3) \setminus \{e\}$.

We have 6 graphs over 4 groups (a)

Let us take two good triples in an arbitrary group H say, $T_1 = (K_1, K_2, K_3)$, $T_2 = (L_1, L_2, L_3)$, and let X_1, X_2 denote the connection sets associated with T_1 and T_2 respectively.
Clearly, if T_1 and T_2 are laying in the same orbit of $Aut(H)$, then $Cay(H, X_2) \cong Cay(H, X_2)$.
Since our four good groups are yielding six orbits of good triples we have at most six different geometric graphs up to isomorphism.

We have 6 graphs over 4 groups (b)

Over H_1, H_2 and H_4 there is only one graph, say Γ_1, Γ_2 and Γ_4 respectively.
Put
$T_1 = \{\langle a, b\rangle, \langle x, y\rangle, \langle ax, by\rangle\},\ T_2 = \{\langle a, y\rangle, \langle x, b\rangle, \langle ax, by\rangle\}$
and
$T_3 = \{\langle a, y\rangle, \langle x, b\rangle, \langle ax, bxy\rangle\}$.
Let X_i denote the connection set associated with T_i, and let $\Gamma_{3,i}$ denote the corresponding Cayley graph.

Up to isomorphism there are just 3 graphs

We establish isomorphisms between the constructed Cayley graphs, proving that:

- $\Gamma_{3,1}$ to $\Gamma_{3,2}$;
- Γ_1 to $\Gamma_{3,1}$;
- Γ_2 to Γ_4.

CI-Groups

According to the isomorphism $\Gamma_{3,1} \cong \Gamma_{3,2}$ we showed:

Remark

$D_p \times D_p$ is not a CI-Group

Formulation of main theorem (a)

According to previous section, there are no more than three geometric graphs over a suitable loops of order $2p$, p a prime.

Formulation of main theorem (b)

The graphs $\Gamma_2, \Gamma_{3,2}, \Gamma_{3,3}$ contains a different number of copies of K_4, and hence they are non-isomorphic.

Theorem

There are exactly three geometric graphs over a suitable loops of order $2p$, p a prime.

Formulation of main theorem (c)

Theorem

1. $\Gamma_2 = SRG(\mathbb{Z}_{2p})$
2. $\Gamma_{3,2} = SRG(D_p)$
3. $\Gamma_{3,3} = SRG(Q_{2p})$

References

1. A. Barlotti and K. Strambach, The geometry of binary systems. Adv. in Math. 49 (1983), no. 1, 1–105.
2. J. Dènes, A. D. Keedwell, Latin squares and their application,Academic press, New York, 1974.
3. A. Heinze and M. Klin, Loops, Latin Squars and Strongly Regular Graphs: An algorithmic approach via Algebraic Combinatorics, in: M. Klin et al, *Algorithmic Algebraic Combinatorics and Grabner Bases* (Springer-Verlag Berlin Heidelberg, 2009) 3–65.
4. K. Kunen, The structure of conjugacy closed loops. Trans. Amer. Math. Soc. 352 (2000), no. 6, 2889–2911.
5. G. E. Moorhouse, Bruck nets, codes, and characters of loops. Des. Codes Cryptogr. 1 (1991), no. 1, 7–29.
6. E. Spence, Strongly regular graphs on at most 64 vertices. http://www.maths.gla.ac.uk/ es/srgraphs.html.
7. A. P. Sprague, Translation nets, Mitt. Math. Sem. Giessen No. 157 (1982), 46–68.

That's all folks!

THANKS