Department of Mathematics
Ludwig-Maximilians Universität
München (Germany)

Department of Mathematics
Ben-Gurion University of the Negev
Beer-Sheva (Israel)

An infinite series of proper loops, admitting a regular group of collineations: An approach via Algebraic Combinatorics

Aiso Heinze Mikhail Klin

heinze@math.lmu.de klin@cs.bgu.ac.il

Introduction and Preliminaries

The poster gives an outline about the discovering of an infinite series of proper loops Q_{2p} of order $2p$, p a prime, $p \equiv 3 \pmod 4$, for which the group $G = \mathrm{Aut}(\Gamma)$ contains a regular subgroup of order $4p^2$. Here $\Gamma = LSG(Q)$ is the Latin square graph naturally attributed to the loop Q. The problem of the existence of such loops goes back to A. Barlotti and K. Strambach [BarS83].

We first found Q_6 by a computer-based examination of a catalogue of strongly regular graphs from [Spe]. Creating a computer free description of all necessary features of Q_6, we discovered that Q_6 is the first member of an infinite series.

The methodology is based on a careful inspection of a suitable transversal design via an auxiliary structure whose automorphism group is isomorphic to the desired group G. Using specific features of this structure and various links between Latin squares, loops, groups, nets and transversal designs, we are able to prove all requested properties of the graph Γ and its corresponding loop Q_{2p}.

A Latin square of order n can be interpreted as an $n \times n$ array with n different entries, $n \geq 2$, such that each entry (= symbol) occurs exactly once in any row and in any column of the array.
A Latin square graph $LSG(L)$ is defined by the n^2 items of a Latin square L where two items regarded as vertices are adjacent if and only if they are in the same row, in the same column or if they have the same symbol in the Latin square. Each Latin square graph is a strongly regular graph with parameters $(n^2, 3(n-1), n, 6)$.

A quasigroup is a set Q with a binary operation "$\cdot$" such that for all $a, b \in Q$ the equations $a \cdot x = b$ and $y \cdot a = b$ have a unique solution in Q. Every Latin square may be interpreted as a multiplication table of a quasigroup, and for each quasigroup its Cayley table provides a Latin square.

A loop L is a quasigroup with an identity element $e \in L$ with the property $ex = xe = x$ for every $x \in L$. An associative loop is a group.

A 3-net of order n is an incidence structure $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ 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 (directions) $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ 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 in 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.

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 lines occupied in L by the same element.

The structure $\mathcal{S} = (\mathcal{L}, \mathcal{P})$ dual to a 3-net has $\mathcal{L}$ as points and $\mathcal{P}$ as lines, and the incidence relation transposed. It is called a transversal design $TD(3, n)$ and has three families of points each of cardinality n, which are called groups and n^2 blocks (lines). Two distinct points from the same groups are not collinear, while there is exactly one line through two distinct points from distinct groups.

The following statements are important for our results:
Lemma 1 [Bab95] For $n \geq 5$ we can reconstruct the 3-net $\mathcal{N}(L)$ uniquely from the graph $\Gamma = LSG(L)$.
This lemma implies the following graph theoretical reformulation.
Proposition 2 For $n \geq 5$ we have $\mathrm{Aut}(LSG(L)) = \mathrm{Aut}(\mathcal{N}(L))$.
We refer to [Moo91] and [God93] for the next proposition:
Proposition 3 Let H be a group of order n and let Q be a loop of order n. Then $H \simeq Q$ if and only if the corresponding 3-nets $\mathcal{N}(H)$ and $\mathcal{N}(Q)$ are isomorphic.
Corollary 4
(a) If H_1 and H_2 are nonisomorphic groups of order n, then $LSG(H_1) \not\cong LSG(H_2)$.
(b) If a Latin square L does not appear in a main class of any group, then $LSG(L)$ is not isomorphic to any Latin square graph over a group.

The loop Q_6 - the first member of an infinite series

The Remark of Barlotti and Strambach

In our project we investigate "group-like" quasigroups. By this we mean that we consider the strongly regular graph $\Gamma(Q)$ defined by a Latin square Q, find its automorphism group $G = \mathrm{Aut}(\Gamma(Q))$ and ask about such properties of G which are shared with cases when Q defines a group.

The first evident property of G is its transitivity. Such examples were provided in the literature. A more sophisticated property is to require that G is not only transitive but also contains a regular subgroup. A question about the existence of proper quasigroups which satisfy this property was implicitly posed by A. Barlotti and K. Strambach, see [BarS83], p. 79: "We were not able to decide whether there exists a proper finite loop having a sharply point transitive group of collineations."

The answer is surprisingly simple:
Proposition 5 Consider the following Latin square Q_6 (No 3.1.1 in [DenK74]):

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

Then:
(a) The main class of Q_6 does not contain a group;
(b) $G = \mathrm{Aut}(\Gamma(Q_6))$ is a transitive permutation group of degree 36 and order 648;
(c) G has a regular subgroup.

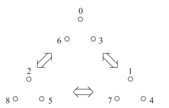
Note that the quasigroup Q_6 is a well-known object. In particular, the parts (a) and (b) of our claim can be extracted from many sources in the literature.
Part (c) may be extracted from [Spr82]. Nevertheless, it seems that, as an entity, the whole proposition appeared the first time in [Hei01], where it was proved with the aid of a computer.

A Model for Q_6: The auxiliary structure

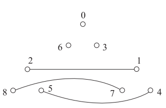
Consider the auxiliary graph $\Delta = \overline{3 \circ K_3}$ as depicted in the figure below (the sign $\Leftrightarrow$ means a set of nine edges of a complete bipartite graph $K_{3,3}$). One can check that $\mathrm{Aut}(\Delta) \cong S_3 \wr S_3$. Moreover, as a computer-based analysis showed our target group $G = \mathrm{Aut}(LSG(Q_6))$ is isomorphic to a subgroup $(S_3 \wr S_3)^{\mathrm{pos}}$ of $\mathrm{Aut}(\Delta)$.

We are starting with copies of the cycle C_9 as spanning subgraphs of Δ. There are exactly 72 of such spanning subgraphs which are Hamiltonian cycles in Δ. The action of G yields two orbits of length 36. Choose the orbit which includes the canonical cycle C_9.

To define an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ we consider partial 1-factors of Δ, i.e. a set of three edges of Δ which form a 1-factor of a graph $K_{3,3}$. An example of such a partial 1-factor is provided in the figure.

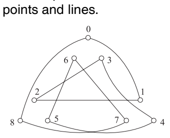


The auxiliary graph Δ.



Partial 1-factor of Δ.

The set of points $\mathcal{P}$ consists of all 18 partial 1-factors in Δ. The lines in $\mathcal{L}$ are exactly the 36 selected copies of C_9 from our orbit. It is clear from our construction that each Hamiltonian cycle in Δ can be splitted into three partial 1-factors. This provides a natural incidence relation between points and lines.



Hamiltonian cycle in Δ.

A Model for Q_6: The desired properties

One can prove that $\mathcal{S}$ is a model of a transversal design $TD(3, 6)$ and $\mathrm{Aut}(\mathcal{S}) \cong G$. We have an auxiliary structure which has the same automorphism group as our Latin square graph $LSG(Q_6)$.

Now, it turns out that $|G| = 648$. For the two existing groups of order 6 we get $|\mathrm{Aut}(LSG(\mathbb{Z}_6))| = 432$ and $|\mathrm{Aut}(LSG(S_3))| = 1296$. Thus, for each loop Q associated to $\mathcal{S}$ we get that $LSG(Q)$ is not isomorphic to $LSG(\mathbb{Z}_6)$ or $LSG(S_3)$ and therefore any loop associated to our transversal design $\mathcal{S}$ is not coming from a group. In other words, any loop corresponding to this design is indeed a proper loop.

Now we have to find a regular subgroup in the action $(G, \mathcal{P})$. For this purpose we may use the action of G on the graph Δ. It is sufficient to find a subgroup H of G such that all $h \in H, h \neq e$ does not preserve any of the 36 copies of the cycle C_9, which form the set $\mathcal{L}$.

Define $H_1 := K_1 \times K_2$ with $K_1 := <(0,3,6),(0,3)(2,5)>$ and $K_2 := <(1,4,7),(1,4)(2,5)>$.
Then:
(a) $K_1 \cong K_2 \cong S_3$, therefore $H_1 \cong S_3 \times S_3$;
(b) $H_1 \leq G$ and $|H_1| = 36$;
(c) no copy of C_9 in $\mathcal{L}$ is preserved by H_1.

Hence, we proved that we get an example which provides a positive answer on the question of Barlotti-Strambach.

In fact, our group G contains one more (up to isomorphism) regular subgroup $H_2 \cong (\mathbb{Z}_3)^2 \rtimes \mathbb{Z}_4$. Thus, G indeed has at least two regular subgroups. In fact, H_1, H_2 are all regular subgroups in G (up to isomorphism). This fact was established, using GAP [GAP99] (see details in [Hei01]).

A Model for Q_6: The construction of Q_6

An attractive way to construct our quasigroup Q_6 is to use the structures for points (partial 1-factors of Δ) and lines of $\mathcal{S}$ (Hamiltonian cycles in Δ). Then provided that the selection of groups for rows and colums is done, we get a purely combinatorial interpretation of the binary operation in the resulting quasigroup. Consider the first and second partial 1-factors, find a unique copy of C_9 through them and get one more partial 1-factor as a result of the mutiplication.

Each vertex of Δ is labeled by an element of $\mathbb{Z}_9$. Addition modulo 9 establishes a canonical bijection between each of the 3-element subsets: $X = \{0,3,6\}, Y = \{1,4,7\}$ and $Z = \{2,5,8\}$.

Thus let us consider an "abstract" 3-element set $\{a,b,c\}$. Then, using the canonical bijection, we attribute elements of $\{a,b,c\}$ to each of the above sets. Suppose, for example, that our rows are 1-factors between X and Y while the columns are 1-factors between Y and Z. Then we attribute to the rows permutations of $\{a,b,c\}$ (functions from X to Y), and similary to the columns (functions from Y to Z). Our element in the square will be again a permutation of $\{a,b,c\}$ (as function from X to Z). Thus, we may call the elements of our quasigroup by permutations from $S(\{a,b,c\})$ and we will get the following table (abc denotes the permuation (a,b,c)):

	e	abc	acb	ab	bc	ac
e	e	abc	acb	ab	bc	ac
abc	abc	acb	e	bc	ac	ab
acb	acb	e	abc	ac	ab	bc
ab	ab	ac	bc	abc	e	acb
bc	bc	ab	ac	acb	abc	e
ac	ac	bc	ab	e	acb	abc

Created Cayley table of the exceptional quasigroup Q_6.

An infinite series of loops Q_{2p}

The general case is, in principle, similar to the described procedure. Let p be a prime. $p \equiv 3 \bmod 4$. For the incident structure $\mathcal{S} = (\mathcal{P}, \mathcal{L})$ we take partial 1-factors of the graph $\Delta = \overline{3 \circ K_p}$ as points in $\mathcal{P}$ and copies of cycles C_{3p} as lines in $\mathcal{L}$.
We are able to prove that $\mathcal{S}$ is a transversal design $TD(3, 2p)$. Moreover, it turns out that $\mathrm{Aut}(\mathcal{S}) \cong (S_3 \wr D_p)^{\mathrm{pos}} = G$.
There are only two groups of order $2p$: $\mathbb{Z}_{2p}$ and D_p. For the associated Latin square graphs we get

$$|\mathrm{Aut}(LSG(\mathbb{Z}_{2p}))| = 24p^2(p-1) \text{ and } |\mathrm{Aut}(LSG(D_p))| = 24p^3(p-1).$$

Hence, we can conclude that our transversal design $\mathcal{S}$ with automorphism group G of order $24p^2$ does not come from a group.

Moreover, since G has a subgroup $(D_p \times D_p \times D_p)^{\mathrm{pos}}$ one can show that there is a regular subgroup $H = (D_p \times D_p \times <i>)^{\mathrm{pos}}$ in G (i is an involution) which has order $\frac{1}{2} \cdot 2p \cdot 2p \cdot 2 = 4p^2$. It is easy to see that each non-identity element of H does not fix any element of $\mathcal{L}$, i.e. any Hamiltonian cycle. Clearly, as an abstract group we have that $H \simeq D_p \times D_p$.

The Cayley table of a quasigroup Q_{2p}, which is implied by the existence of the transversal design $\mathcal{S}$, can be described as follows:
Identify the element set of Q_{2p} by that of D_p and consider D_p in its canonical action on the set $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Let $a = (0, 1, \ldots, p-1)$ be a generator of $\mathbb{Z}_p$. Then we will define the binary operation $\circ$ in Q_{2p} as follows (here xy means the usual multiplication in D_p):

$$x \circ y = \begin{cases} xya, & \text{if } x \text{ and } y \text{ are odd,} \\ xy, & \text{otherwise.} \end{cases}$$

We refer to [Kun2000] for an alternative discussion of some exceptional properties of this quasigroup.

References

[Bab95] L. Babai, Automorphism groups, isomorphism, reconstruction, in: Graham, R. L. et al., eds., *Handbook of combinatorics* (Elsevier, Amsterdam, 1995) 1447–1540.

[BarS83] A. Barlotti and K. Strambach, The geometry of binary systems, *Adv. Math.* **49** (1983) 1–105.

[DénK74] J. Dénes and A. D. Keedwell, *Latin Squares and their Application* (Academic Press, New York, London, 1974).

[GAP99] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.2; Aachen, St. Andrews, 1999. (http://www-gap.dcs.st-and.ac.uk/˜gap).

[God93] C. D. Godsil, *Algebraic combinatorics* (Chapman & Hall, New York, 1993).

[Hei2001] A. Heinze, *Applications of Schur rings in algebraic combinatorics: graphs, partial difference sets and cyclotomic schemes.* Ph.D. thesis, Department of Mathematics, Carl von Ossietzky University of Oldenburg (Germany) (2001).

[Kun2000] K. Kunen, The structure of conjugacy closed loops. *Trans. Amer. Math. Soc.* **352**(6) (2000) 2889–2911.

[Moo91] G. E. Moorhouse, Bruck nets, codes, and characters of loops, *Des. Codes Cryptogr.* **1**(1) (1991) 7–29.

[Spe] E. Spence, *Strongly regular graphs on at most 64 vertices.* http://www.maths.gla.ac.uk/˜es/srgraphs.html.

[Spr82] A. P. Sprague, Translation nets, *Mitt. Math. Semin. Gießen* **157** (1982) 46–68.