Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Electronic Notes in Discrete Mathematics 23 (2005) 13–21

Electronic Notes in DISCRETE MATHEMATICS

www.elsevier.com/locate/endm

Links between Latin squares, nets, graphs and groups: Work inspired by a paper of A. Barlotti and K. Strambach

Aiso Heinze[1]

Lehrstuhl für Mathematikdidaktik
Universität Augsburg
86135 Augsburg, Germany

Mikhail Klin[2,3]

Department of Mathematics
Ben-Gurion University of the Negev
Beer Sheva, 84105, Israel

Abstract

Starting from a computer generated example of a transitive Latin square graph over a proper loop we describe a computer free interpretation of this specific strongly regular graph. Moreover, with this interpretation we were able to generalize the result to an infinite series of similar examples.

[1] Email: `aiso.heinze@math.uni-augsburg.de`

[2] Corresponding author, email: `klin@cs.bgu.ac.il`

[3] Partially supported by Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

1571-0653/$ – see front matter
doi:10.1016/j.endm.2005.06.103

1 Introduction

In his Ph.D. thesis [10], A. Heinze determined all partial difference sets (briefly, pds's) over groups of order up to 49. For this research he used computer catalogues of strongly regular graphs with a small number of vertices, which were created by E. Spence [17].

One of Heinze's results was a proof of the existence of two unusual pds's over groups of order 36, one such group being the direct product of two copies of the dihedral group of order 6. Both these pds's imply the same (up to isomorphism) strongly regular graph Γ with the parameters $(v, k, \lambda) = (36, 15, 6)$. $Aut(\Gamma)$ is of order 648 and acts transitively on the vertex set of Γ. Moreover, it turns out that Γ is a Latin square graph coming from a proper loop of order 6.

Later on, we realized that A. Barlotti and K. Strambach were looking for exactly such an example of a proper loop, see [2].

The main content of the current paper is a quite beautiful, computer-free interpretation of the graph Γ and its further generalization to an infinite series of similar examples.

2 Brief preliminaries

We start with a brief account of the main definitions, including Latin square as an $n \times n$ array together with its n^2-element set of ordered triples; quasigroups, loops and groups as algebraic structures associated to Latin squares; association schemes with 2, 3 and 4 classes; 3-nets, transversal designs and strongly regular graphs linked to Latin squares.

We next recall the most important methods of classification of Latin squares and various groups attributed to Latin squares and related combinatorial structures.

A loop L will be called a *proper loop* if its main class does not contain a group. For details and further references we mention the following important sources: [4], [14], [2], [12].

We also discuss the notion of a partial difference set (pds), e.g., see [9], and its specific case when it defines a Latin square graph.

Last but not least, we briefly consider an elegant interpretation of a Latin square as a certain induced subgraph of a Hamming graph with suitable parameters.

3 Classics and folklore

A number of results linking Latin squares to other structures play a significant role in our presentation.

Lemma 3.1 *Let L be a Latin square of order n, and let $\Gamma = LSG(L)$ be the Latin square graph defined by L. If $n \geq 5$, then cliques of order n in Γ necessarily correspond to lines of the associated 3-net $\mathfrak{N}(L)$.*

Lemma 3.2 *For $n \geq 5$, we can recover the 3-net $\mathfrak{N}(L)$ uniquely from the graph $\Gamma = LSG(L)$.*

Proposition 3.3 *For $n \geq 5$, $Aut(LSG(L)) = Aut(\mathfrak{N}(L))$.*

Proposition 3.4 *Let H be a group, and $L = L(H)$ a group Latin square. Then $Aut(\mathfrak{N}(L)) \cong (H^2 : Aut(H)).S_3$.*

Theorem 3.5 *Let H be a group, $L(H)$ its Cayley table, and $\Gamma = LSG(H)$ the Latin square graph defined by $L(H)$. Assume $|H| \geq 5$. Then $Aut(\Gamma) \cong (H^2 : Aut(H)).S_3$.*

Example 3.6

(a) $Aut(LSG(\mathbb{Z}_2 \times \mathbb{Z}_2)) \cong S_2 \wr S_4$, where $|S_2 \wr S_4| = 2^7 \cdot 3^2$,

(b) $|Aut(LSG(\mathbb{Z}_4))| = 192$.

Example 3.7

(a) $|Aut(LSG(\mathbb{Z}_6))| = 2^4 \cdot 3^3$,

(b) $|Aut(LSG(S_3))| = 2^4 \cdot 3^4$.

Theorem 3.8 *Let Q_1 be a group of order n, and let Q_2 be a loop of order n. Then Q_1 is isomorphic to Q_2 if and only if $\mathfrak{N}(Q_1) \cong \mathfrak{N}(Q_2)$.*

Corollary 3.9

(a) *If Q_1 and Q_2 are non-isomorphic groups of order n, then $\mathfrak{N}(Q_1) \ncong \mathfrak{N}(Q_2)$*

(b) *If a Latin square Q does not appear in the main class of any group, then*

$LSG(Q)$ is not isomorphic to any LSG over a group.

We will discuss briefly which of these results are classical and which are folklore. Important references here include [1], [8], [3], [13], as well as many others which, although deserving of credit, we cannot mention because of space limitations.

4 Proper loops with a regular group of collineations

A. Barlotti and K. Strambach wrote on p. 79 of [2]:

> "We were not able to decide whether there exists a proper finite loop having a sharply transitive group of collineations."

It turns out that such an example had already been provided in [10], although in slightly different terminology. This example gives a surprisingly simple resolution to their remark.

Proposition 4.1 [10] *Consider the Latin square Q_6 (# 3.1.1 in [4] indicated below:*

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

Then:

(a) *The main class of Q_6 does not contain a group;*

(b) *$G = Aut(LSG(Q_6))$ is a transitive permutation group of degree 36 and order 648;*

(c) *G has a regular subgroup.*

The original proof of Proposition 8 was accomplished by brute force, and relied heavily on computations performed with the aid of GAP, GRAPE, and nauty.

5 Computer-free interpretation

Using the computer packages GAP and COCO we were able to identify the group G of order 648 which appears in the formulation of Proposition 8. Its isomorphism type is $(S_3 \wr S_3)^{pos}$, that is the subgroup of all even permutations in the wreath product $S_3 \wr S_3$, where S_3 is the symmetric group of degree 3 (which is, of course, isomorphic to the dihedral group D_3 of degree 3).

After that, we obtained the following computer-free interpretation of a transversal design $TD(3,6)$ which may be associated with group G:

- Consider the auxiliary graph $\Delta = K_{3,3,3}$, that is, the complete 3-partite graph on 9 vertices which is regular of valency 6. Our group G is a subgroup of index 2 in $Aut(\Delta)$.
- Δ has exactly 72 spanning subgraphs, each isomorphic to the undirected cycle C_9. Group G has two orbits of length 36 in its action on these cycles. Select one such orbit; denote it as $\mathcal{L}$.
- Δ has 18 specific subgraphs which we shall call partial 1-factors, each on 6 vertices and regular of valency 1. Denote by $\mathcal{P}$ the collection of all such subgraphs.
- Consider the incidence structure $\mathfrak{S} = (\mathcal{P}, \mathcal{L})$, with incidence defined by natural inclusion. That is, a partial 1-factor is incident to a cycle provided the edge set of the former is contained in the edge set of the latter.

Proposition 5.1

(a) *The incidence structure $\mathfrak{S}$ is a transversal design $TD(3,6)$;*

(b) *$Aut(TD(3,6)) = G$;*

(c) *Up to isomorphism, G has two regular subgroups of order 36 in its action on set $\mathcal{L}$;*

(d) *A 3-net which is dual to the transversal design $\mathfrak{S}$ is isomorphic to $\mathfrak{N}(Q_6)$;*

(e) *Q_6 does not have a group in its main class.*

Note that our proof of the above nowhere depends on the use of a computer; instead it relies on only those theoretical elements briefly touched upon in Section 3.

Finally, analyzing the structure of $\mathfrak{S}$ and G together with Q_6, it becomes evident that we can interpret Q_6 as a "slightly corrupted" Cayley table for the dihedral group D_3 of order 6. This observation was in fact crucial for our further generalizations.

6 An infinite series

Our previous observation was very helpful in allowing us to develop a certain insight, and enabling us to construct one additional example of a Latin square graph on 196 vertices which comes from a quasigroup Q_{14} of order 14.

Originally, this example was also managed with the aid of the computer package COCO. However, subsequently we were able to give a computer-free interpretation, and to construct, in the same spirit as $TD(3, 6)$ above, a transversal design $TD(3, 14)$ corresponding to Q_{14}.

Finally, we realized that we were prepared to define an infinite series of examples.

Theorem 6.1 *Let $p \equiv 3 (\mod 4)$ be a prime number. Then there exists an incidence system $\mathfrak{S} = \mathfrak{S}_p$ such that:*

(a) *$\mathfrak{S}$ is a transversal design $TD(3, 2p)$;*

(b) *$G = Aut(\mathfrak{S}) \cong (S_3 \wr D_p)^{pos}$ is a permutation group of order $24p^3$ which acts transitively on the point and line sets of $\mathfrak{S}$ of cardinalities $6p$ and $4p^2$, respectively;*

(c) *As a transitive group of degree $4p^2$ in its action on the lines of $\mathfrak{S}$, G contains a regular subgroup $H \cong D_p \times D_p$ of order and degree $4p^2$;*

(d) *The dual structure to $\mathfrak{S}$ is a 3-net which is not coming from a suitable group of order $2p$.*

The main part of the proof relies on an auxiliary graph Δ with $3p$ vertices which is regular of valency $2p$; it is in fact a Cayley graph of the cyclic group $\mathbb{Z}_{3p}$ of order $3p$. Points and lines of the incidence structure $\mathfrak{S}_p$ are described in terms of certain subgraphs of Δ.

Finally, having a transversal design $\mathfrak{S}_p$, we may define a quasigroup Q_{2p} of order $2p$ (in fact, a loop) which is a certain modification of the dihedral group D_p.

7 Theoretical postscriptum

Having obtained all of these results and especially a nice description of the loop Q_{2p}, we became suspicious as to whether or not the loop itself was known to loop theorists. Moreover, we wanted to understand who was the first to use loop Q_6 in one or another context, possibly different from our goals.

A corresponding bibliographical search was arranged, a complete report on which would constitute one additional huge paper. Here we briefly mention the most important observations, as a rule without evident references.

A seminal paper was published by A. Sprague, see [18], a year before the paper [2]. In Sprague's paper, both partial sets corresponding to our $TD(3,6)$ are described in evident form. However, [18] does not contain an explicit description of the transversal design, in particular no question about its automorphism group is posed.

Conversely, various automorphism groups implicitly or explicitly related to Latin squares were considered in publications by many other mathematicians, including E. Schönhardt, A. Sade, R. Artzy, B. F. Bryant & H. Schneider, A. E. Malykh & A. N. Pekhletskaya, D. Betten, R. Bailey, Ch. Praeger.

Loops Q_{2p} and their generalizations were considered by many experts, especially E. Wilson, R. L. Wilson, Jr., E. G. Goodaire & D. A. Robinson, K. Kunen.

We believe that our approach sheds new light on various links between Latin squares, loops, groups, nets, graphs, partial difference sets and transversal designs.

Acknowledgement

Conceptually, this project goes back to the Moscow school, in particular to the collaboration of M. K. with I. A. Faradžev, A. V. Ivanov, and especially the late Ja. Ja. Gol'fand. More recent collaborations with E. van Dam, M. Muzychuk and A. Woldar have been very helpful.

We also acknowledge R. Bailey, D. Keedwell, R. Mathon, B. McKay, W. Myrvold, Ch. Praeger, S. Reichard, T. Spence and A. Sprague for valuable assistance, information and hints.

This project was initiated in August 2001, when M. K. was visiting Alex Rosa at McMaster University, Hamilton, Ontario. Long discussions with Alex of various issues related to Latin squares were very productive and stimulating.

References

[1] Babai, L., *Automorphism groups, isomorphism, reconstruction*, “Handbook of combinatorics”, Vol. 1, 2, Elsevier, Amsterdam, 1995, 1447–1540.

[2] Barlotti, A., and K. Strambach *The geometry of binary systems*, Advances in Mathematics **49** (1983), 1–105.

[3] van Dam,E., M. Klin, M. Muzychuk, and A. Woldar, *Some implications on amorphic association schemes*, in preparation.

[4] Denes, J., and A. D. Keedwell, “Latin squares and their applications,”Academic Press, New York–London, 1974.

[5] Faradžev,I. A., A. A. Ivanov, and M. H. Klin, *Galois correspondence between permutation groups and cellular rings (association schemes)*, Graphs and Combinatorics **6** (1990), 303-332.

[6] Faradžev, I. A., and M. H. Klin, *Computer package for computations with coherent configurations*, Proc. ISSAC-91, ACM Press, Bonn, 1991, 219-223.

[7] Faradžev, I. A., M. H. Klin, and M. E. Muzichuk, *Cellular rings and groups of automorphisms of graphs*, in: I. A. Faradžev, A. A. Ivanov, M. H. Klin and A. J. Woldar, eds., “Investigations in algebraic theory of combinatorial objects,” Kluwer Acad. Publ., Dordrecht, 1994, 1–152.

[8] Gol’fand, Ja. Ju., A. V. Ivanov, and M. H. Klin, *Amorphic cellular rings. I, II* (Russian), Investigations in Algebraic Theory of Combinatorial Objects, Institute for System Studies, Moscow, 1985, 32–38, 39–49. (English translation: I. A. Faradžev et al., eds., “Investigations in Algebraic Theory of Combinatorial Objects,” Kluwer Acad.Publ., Dordrecht, 1994, 167–187.

[9] Jorgensen, L. K., and M. Klin, *Switching of edges in strongly regular graphs I. A family of partial difference sets on 100 vertices,* Electron. J. Combin. **10** (2003), Research Paper 17, 31 pp. (electronic).

[10] Heinze, A., “Application of Schur rings in algebraic combinatorics: graphs, partial difference sets and cyclotomic schemes,” Ph.D. Thesis. Fachbereich Mathematik der Carl von Ossietzky Universität Oldenburg, 2001.

[11] McKay, B. D., “nauty User’s Guide (Version 1.5)” Computer Science Department, 1990, TR-CS-90-02, Australian National University.

[12] McKay, B. D., A. Meynert, and W. Myrvold, *Small Latin squares, quasigroups and loops,* Preprint, 2004.

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

[14] Pflugfelder, H. O. “Quasigroups and loops: Introduction,” Sigma Series in Pure Mathematics, 7, Heldermann Verlag, Berlin, 1990.

[15] Schönert, M. et al., “GAP – Groups, Algorithms, and Programming,” fifth edition, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1995.

[16] Soicher, L. H., *GRAPE: a system for computing with graphs and groups,* in: L. Finkelstein and W. M. Kantor, eds., “Groups and Computation” volume 11, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, (A.M.S., 1993, 287–291.

[17] Spence, E., Homepage, URL: http://www.maths.gla.ac.uk/ es/srgraphs.html.

[18] Sprague, A. P. *Translation nets,* Mitt. Math. Sem. Giessen **157** (1982), 46–68.