Зборник радова Математичког института, Нова серија, књ. 1 (9), 1976.
Recueil des travaux de l'Institut Mathématique, Nouvelle série, № 1 (9), 1976.

Симпозијум КВАЗИГРУПЕ И ФУНКЦИОНАЛНЕ ЈЕДНАЧИНЕ
Symposium en QUASIGROUPES ET EQUATIONS FONCTIONNELLES
Београд—Нови Сад, 18—21. 9. 1974.

LATIN SQUARES, *P*-QUASIGROUPS AND GRAPH DECOMPOSITIONS

A. D. Keedwell

In this mainly expository paper, we discuss two particular types of quasigroup (latin square) which have connections with other branches of mathematics, notably with statistics, graph theory and coding theory.

A square $n \times n$ matrix L on n distinct symbols is called *row complete* if every pair of symbols of L occurs just once as an adjacent pair of elements in some row of L. It is called *row latin* if each symbol occurs exactly once in each row of the matrix. The concepts *column complete* and *column latin* are similarly defined. A square matrix which is both row latin and column latin is called a *latin square.*

We shall also find it convenient to call a rectangular matrix R of size $m \times n$ or $n \times m$ *row complete*, where $m \leqslant \left[\frac{1}{2}n\right]$, if each *unordered* pair of its symbols occurs just once as an adjacent pair of elements in some row of R. Here, [ ] denotes "integer part".

Row complete latin squares are used in statistics in connection with the design of experiments. They are of particular value for the design of sequential experiments but may also be useful for eliminating interactions between adjacent plots in field experiments. A detailed explanation of these applications is given in [2]. Here, we shall be content to give a single illustration. In an experiment on farm animals, it is desired to apply a number of different dietary treatments to a given animal in succession. The effect of a given treatment on the animal may be affected both by the number of treatments which that animal has already received and also by the nature of the immediately preceding treatment which it has had applied to it. If several animals are available for treatment, the first possibility can be allowed for statistically if it can be arranged that the number n of animals to be treated is equal to the number of treatments to be applied and if the order in which the treatments are to be applied to these n animals is allowed to be determined by the order of the entries in the n rows of an $n \times n$ latin square (whose n distinct elements denote the n treatments). Then any particular experiment has a different number of predecessors for each of the n different animals, since a given element of the latin square is preceded by a different number of other elements in each of the n rows of the square. The possibility of interaction between one experiment and the

immediately preceding one can also be allowed for if the latin square chosen is row complete. The resulting experiment is then said to be statistically "balanced" both with respect to the effect of the immediately preceding experiment and also with respect to the number of preceding experiments.

Until very recently, the only row complete latin squares known were multiplication tables of groups (or quasigroups isotopic to groups). Also each of these known row complete latin squares had the property that it could be made column complete as well by a suitable reordering of its rows. In fact, it is not difficult to show:

Theorem 1. *Every row complete latin square which represents the multiplication table of a group can be made column complete as well as row complete by suitably reordering its rows.*

Proof: — Let the given square be the multiplication table of the group G where $h_1, h_2, \ldots, h_n$ and $g_1, g_2, \ldots, g_n$ are two orderings of the elements of G, as in Fig. 1.

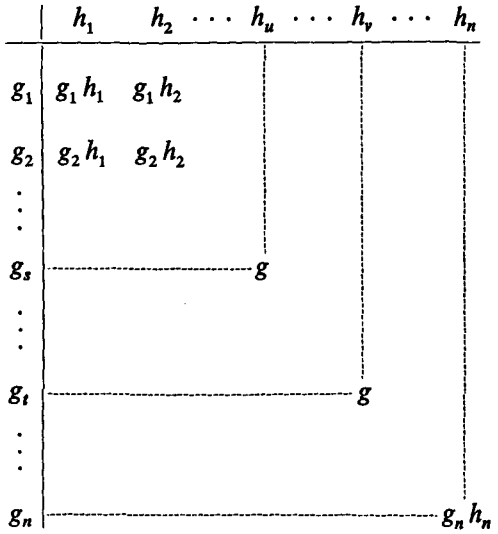

Fig. 1

Since the square is row complete the elements $h_1^{-1} h_2, h_2^{-1} h_3, \ldots, h_{n-1}^{-1} h_n$ are all distinct and are the non-identity elements of the group in a new order: for suppose that $h_u^{-1} h_{u+1} = h_v^{-1} h_{v+1} = k$ say. Let the arbitrary element g of G occur in the s^{th} row of column u and in the t^{th} row of column v. Then $g = g_s h_u = g_t h_v$. The entries in the $(u+1)^{\text{th}}$ column of row s and in the $(v+1)^{\text{th}}$ column of row t are $g_s h_{u+1} = (g_s h_u)(h_u^{-1} h_{u+1}) = gk$ and $g_t h_{v+1} = (g_t h_v)(h_v^{-1} h_{v+1}) = gk$ respectively. Hence, the ordered pair (g, gk) occur as adjacent elements in both the s^{th} and the t^{th} rows of the square, contrary to hypothesis.

Now let the rows be reordered according to the permutation

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ h_1^{-1} & h_2^{-1} & \cdots & h_n^{-1} \end{pmatrix}$$

so that the reordered square takes the form shown in Fig. 2. This reordering will not affect the row completeness.

Moreover, in the new square each ordered pair of elements will occur at most once as a pair of adjacent elements in the columns : for, suppose that the entries of the $(s, u)^{\text{th}}$ and $(t, v)^{\text{th}}$ cells are the same, equal to g say. Then, $h_s^{-1} h_u = g = h_t^{-1} h_v$. The entries of the $(s+1, u)^{\text{th}}$ and $(t+1, v)^{\text{th}}$ cells must then be distinct, for $h_{s+1}^{-1} h_u = h_{t+1}^{-1} h_v$ would imply $(h_{s+1}^{-1} h_s)(h_s^{-1} h_u) = (h_{t+1}^{-1} h_t)(h_t^{-1} h_v)$ and so $(h_{s+1}^{-1} h_s) g = (h_{t+1}^{-1} h_t) g$. But then, $h_{s+1}^{-1} h_s = h_{t+1}^{-1} h_t$ whence $(h_{s+1}^{-1} h_s)^{-1} = (h_{t+1}^{-1} h_t)^{-1}$. Thus we would have $h_s^{-1} h_{s+1} = h_t^{-1} h_{t+1}$ which is contrary to hypothesis. This shows that the new square is column complete as well as row complete and so proves the theorem.

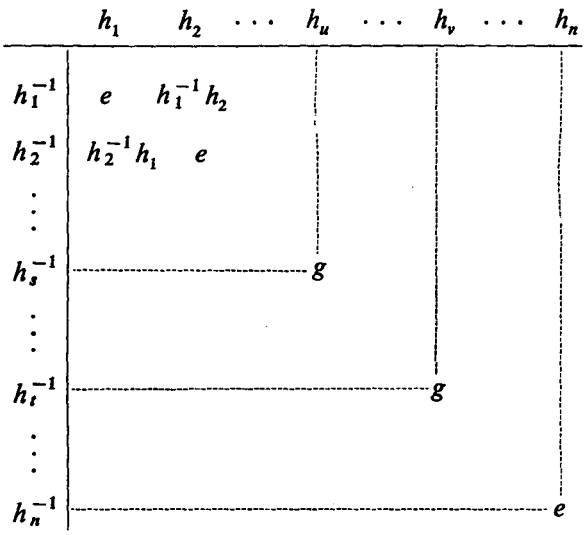

Fig. 2.

The above theorem was first given in [8]. An examination of the proof suggests the hypothesis that the theorem is also true for an inverse property loop G which satisfies the identity $(gh)(h^{-1}k) = gk$ for all g, h, k in G. However (as V.D. Belousov pointed out to the author during the Conference itself) such a loop is already a group. To see this, write $h^{-1}k = l$. Then $k = (eh)(h^{-1}k) = hl$ and so $(gh)l = g(hl)$ for all g, h, l in G.

The multiplication table of finite group G can be written in the form of a row complete latin square if and only if the group is *sequenceable* : that is, if and only if there exists an ordering of the elements $g_1, g_2, \ldots, g_n$ of G such that the partial products $p_s = \prod_{i=1}^{s} g_i$ for $s = 1, 2, \ldots n$ are all distinct. (For the orginal proof, see [4].). To see the necessity of this condition, let the row complete latin square $L = (g_{ij})$ be the multiplication table of G so that $g_{ij} = g_i g_j$. In that case $g_{ij}^{-1} g_{i,j+1} = g_j^{-1} g_i^{-1} g_i g_{j+1} = g_j^{-1} g_{j+1} = h_j$ say for all values of i. Suppose that $h_j = h_{j'}$ for $j' \neq j$. Then, because $g_{i'j'} = g_{ij}$ for some value of i'

(each element of G occurs exactly once in each column of L), we have $g_{i',j'+1} = g_{i'j'}\, h_{j'} = g_{ij}\, h_j = g_{i,j+1}$. However, this contradicts the row completeness of L. Thus $h_j \neq h_{j'}$ unless $j' = j$. Consider now the first row of L. Its j^{th} element is $g_{ij} = g_{11}\,(g_{11}^{-1} g_{12})\,(g_{12}^{-1} g_{13}) \cdots (g_{1,j-1}^{-1} g_{1j}) = g_{11}\, h_1 h_2 \cdots h_{j-1}$. Since the elements of the first row of L are all different, it follows that the partial products $\prod_{k=1}^{j-1} h_k$ for $j = 2, 3, \ldots, n-1$ are all distinct, where the elements $h_1\, h_2, \ldots, h_{n-1}$ are the non-identity elements of G. That is, the elements $e, h_1\, h_2, \ldots, h_{n-1}$ form a sequencing for G. To see the sufficiency of the condition, consider the latin square $L = (g_{ij})$ where $g_{ij} = p_i^{-1} p_j$, p_i being one of the partial products defined above. We require to show that the ordered pair of elements (u, v) of G occur consecutively in some row of L. That is, we require to find integers i, j such that $p_i^{-1} p_j = u$ and $p_i^{-1} p_{j+1} = v$. From these two equations, $u g_{j+1} = v$. This determines j. Then $p_i = p_j u^{-1}$ and this fixes i. Thus, every pair of elements of G occurs exactly once and L is row complete.

Evidently, $p_1 = g_1 = e$ (where e denotes the group identity) is necessary for a group G to be sequenceable. If the group G is abelian, it is known that $p_n = e$ unless G has a unique element h of order two and that, in the latter case, $p_n = h$. (see [12]). Thus, a finite abelian group can be sequenceable only if it has a unique element of order two. B. Gordon [4] has proved that this condition is sufficient as well as necessary. Namely, a finite abelian group is sequenceable if and only if it is the direct product of two groups A and B such that A is a cyclic group of order 2^k, $k > 0$, and B is of odd order.

As regards the sequenceability of groups of odd order, little is known. It is clear from the preceding remarks that an abelian group of odd order cannot be sequenceable. The non-abelian group of smallest odd order is the (unique) non-abelian group of order 21 generated by two elements a and b with the defining relations $a^7 = b^3 = e$, $ab = ba^2$. This group has been shown to be sequenceable by N. S. Mendelsohn [10]. The non-abelian group of order 27 generated by two elements a and b with the defining relations $a^p = b^q = e$, $ab = ba^r$, where $p = 9$, $q = 3$ and $r = 4$, has been shown to be sequenceable by the present author [6] and very recently the groups on two generators with similar structure having orders 39 ($p = 13$, $q = 3$, $r = 3$), 55 ($p = 11$, $q = 5$, $r = 3$) and 57 ($p = 19$, $q = 3$, $r = 7$) have been shown to be sequenceable by L. L. Wang [13]. The present author has conjectured in [6] that all non-abelian groups on two generators are sequenceable and the recent results of L. L. Wang lend strength to this conjecture.

As regards non-abelian sequenceable groups of even order, B. Gordon [4] has shown that the dihedral groups D_3 and D_4 of orders 6 and 8 are not sequenceable, and J. Dénes and E. Török [3] have shown that the dihedral groups D_5, D_6, D_7 and D_8 of orders 10, 12, 14 and 16 are sequenceable but that the remaining non-abelian groups of orders less than or equal to 14 are not sequenceable.

It is known that there are no row complete latin squares of orders 2, 3, 5 or 7. This has been shown by D. Warwick [14] and by P. J. Owens [11]. Very recently, P. J. Owens has constructed the first examples of row complete latin squares which are not the multiplication tables of groups (that is, they do not satisfy the quadrangle condition, see [2]). These are of orders 8 and

10. He has also constructed a row complete latin square of order 14 which cannot be made column complete as well by any reordering of its rows.

Finally, we mention that a row complete latin square of order n defines a decomposition of the complete directed graph on n vertices into disjoint Hamiltonian paths. To see this, let the vertices of the graph be labelled by means of the symbols of the square. Then each row of the square defines a Hamiltonian path whose directed edges are given by the ordered pairs of adjacent symbols in that row. This fact was first observed by N. S. Mendelsohn [10] and by J. Dénes and E. Török [3]. If n is even, a row complete $\frac{1}{2}n \times n$ latin rectangle similarly defines a decomposition of the complete undirected graph on n vertices into disjoint Hamiltonian paths. Also, suitable row complete latin rectangles exist for all even values of n, as is shown in [7] and [2]. (Since each Hamiltonian path has $n-1$ edges and the complete undirected graph has $\frac{1}{2}n(n-1)$ edges, no decomposition of this kind can exist if n is odd).

Another type of quasigroup (latin square) which defines decompositions of the complete undirected graph is the so-called *P-quasigroup (or partition quasigroup)*.

Let us first define a *P*-groupoid.

Definition. A groupoid $(Q, \cdot)$ is called a *P-groupoid* if it satisfies the following three properties: (i) $a \cdot a = a$ for all $a \in Q$; (ii) $a \neq b$ implies $a \neq a \cdot b$ and $b \neq a \cdot b$ for all $a, b \in Q$; (iii) $a \cdot b = c$ implies and is implied by $c \cdot b = a$ for all $a, b, c \in Q$.

A one-to-one correspondence between *P*-groupoids of n elements and decompositions of the complete undirected graph on n vertices into disjoint closed paths is easily established by labelling the vertices of the graph with the elements of the *P*-groupoid and prescribing that the edges (a, b) and (b, c) shall belong to the same closed path of the graph if and only if $a \cdot b = c$, $a \neq b$. We deduce at once that the number of elements of a *P*-groupoid is odd. *A P*-groupoid which is also a quasigroup is called a *P-quasigroup*. Thus, a *P*-quasigroup is an idempotent quasigroup with the additional property that whenever the relation $a \cdot b = c$ holds in $(Q, \cdot)$ so also does the relation $c \cdot b = a$.

The concepts of *P*-groupoid and *P*-quasigroup were introduced by A. Kotzig [9]. The following facts were first pointed out in [7], [5], [1] and [8] respectively.

Observation 1. *A decomposition of the complete undirected graph on n vertices $v_1, v_2, \ldots, v_n$ into disjoint closed paths corresponds to a P-quasigroup $(V, \cdot)$ if and only if, for fixed values of i and k, (v_i, v_j) and (v_j, v_k) are adjacent edges of a closed path for one and only one value of j.*

Proof. If $(V, \cdot)$ is a *P*-quasigroup, the entry k occurs once and once only in the i^{th} row of the multiplication table of $(V, \cdot)$. Let the column in which this entry occurs be the j^{th}. Then we have $i \cdot j = k$ and (v_i, v_j), (v_j, v_k) are adjacent edges of a closed path of G_n for this value of j and no other.

Observation 2. *Commutative P-quasigroups of order n exist exactly when $n \equiv 1$ or 3 mod 6 and then and only then the complete undirected graph on n vertices can be decomposed into disjoint triangular circuits.*

Proof. The vertices of the triangles define the triads of a Steiner triple system.

Observation 3. A P-quasigroup of order n exists which defines a decomposition of the complete undirected graph on n vertices into disjoint Hamiltonian circuits whenever n is a prime.

Proof. We define the required P-quasigroup by taking the set $V=\{1, 2, \ldots n\}$ and observing that, if an operation $(\cdot)$ is defined on V by the statement $r \cdot s = 2s - r \pmod{n}$, we obtain a P-quasigroup $(V, \cdot)$ having the desired property.

For further details and a discussion of the connection between $(V, \cdot)$ and a certain row complete latin square, see [1].

Observation 4. The existence of a P-quasigroup of order $n = 2r+1$ which defines a decomposition of the complete undirected graph on n vertices into a single Eulerian closed path is equivalent to the existence of a codeword on $2r+1$ symbols of length $r(2r+1)+1$ in which no pair of consecutive symbols and no pair of nearly consecutive symbols is repeated.

Proof. Two symbols of a codeword are said to be *nearly consecutive* if they are separated by a single symbol. We may establish a correspondence between Eulerian circuits of the complete undirected graph G_n on n vertices and codewords of length $\frac{1}{2}n(n-1)+1$ by regarding each pair of consecutive symbols of the codeword as representing an edge of the graph joining the vertices represented by those two symbols. The last symbol of the codeword is taken to be the same as the first in order that the path represented should be closed. Since each edge of the graph occurs exactly once in an Eulerian circuit, each pair of consecutive symbols must occur once and only once in the corresponding codeword. Also if the Eulerian circuit is to correspond to a P-quasigroup, each pair of nearly consecutive symbols must occur in the codeword at most once otherwise the property stated in observation 1 above would be violated.

In his original paper [9], A. Kotzig raised the question "For which values of n does a P-quasigroup exist which defines a decomposition of the complete undirected graph on n vertices into a single Eulerian closed path ?" He showed that such a P-quasigroup exists for the orders $n=3$ and 7 but not when $n=5$. Subsequent work on this topic has made use of the equivalence with the codeword existence problem which is stated in observation 4 above and has shown that suitable P-quasigroups exist whenever $n = 4r+3$ except possibly when $r \equiv 127 \bmod 595$ and whenever $n = 4r+1$ $(r \neq 1)$ except possibly when $r \equiv 5 \bmod 7$.

The main theorem required is as follows:

Theorem 2. *Let U denote a sequence of non-zero integers $u_1, u_2, \ldots, u_r$ such that $-r \leqslant u_i \leqslant r$ and $|u_j| \neq |u_i|$ unless $j=i$ (so that $|u_1|, |u_2|, \ldots, |u_r|$ is a reordering of the natural numbers $1, 2, \ldots r$). Let $\sigma_s = \sum_{i=1}^{s} u_i \bmod 2r+1$. Also, let $u_i + u_{i+1} \equiv h_i \bmod 2r+1$ for $i = 1, 2, \ldots, r-1$, where $-r \leqslant h_i \leqslant r$; and let h_r denote the smallest integer congruent to $u_r + u_1$ modulo $2r+1$. Then, if such a*

sequence U exists with the following additional properties: (a) the integers $|h_i|$ are all distinct for $i=1, 2, \ldots, r$; and (b) $(\sigma_r, 2r+1)=1$, there exists a codeword on $2r+1$ symbols of length $r(2r+1)+1$ in which no pair of consecutive symbols and no pair of nearly consecutive symbols is repeated. (Equivalently, there exists an Eulerian circuit of the complete undirected graph on $2r+1$ vertices which corresponds to a *P*-quasigroup).

If such a sequence U exists with the following alternative additional properties: (a) the integers $|h_i|$ are all distinct for $i=1, 2, \ldots, r-1$ and no one of them is equal to 1; (b)* $u_1=1$ or 2; and (c)* $i fu_1=1$, $(-3+\sigma_r, 2r+1)=1$; if $u_1=2$, $(-2+\sigma_r, 2r+1)=1$, then there exists a codeword on $4r+3$ symbols of length $(2r+1)(4r+3)+1$ in which no pair of consecutive symbols and no pair of nearly consecutive symbols is repeated.*

The second part of this theorem is due to the present author and a proof will be found in [8]. The first part is the joint work of the present author and A. J. W. Hilton. It is proved in [5].

Once the theorem has been established, it only remains to show the existence of suitable sequences U. By way of illustration we state the following theorem which is proved fully in [5].

Theorem 3. *The following sequences U satisfy the conditions (a) and (b) of theorem 1:* —

$$r=2t;\ u_1=-2t,\ u_2=2t-2,\ u_3=2t-4, \ldots, u_{t-1}=4,\ u_t=2,\ u_{t+1}=1,$$

$$u_{t+2}=3, \ldots, u_{2t-1}=2t-3,\ u_{2t}=2t-1,\ \textit{modulo}\ 4t+1;\ t\neq 1\ \textit{and}\ t\not\equiv 5\ \textit{mod}\ 7;$$

$$r=2t+1;\ u_1=-(2t+1),\ u_2=2t-1,\ u_3=2t-3, \ldots, u_t=3,\ u_{t+1}=1,$$

$$u_{t+2}=2,\ u_{t+3}=4, \ldots, u_{2t}=2t-2,\ u_{2t+1}=2t,\ \textit{modulo}\ 4t+3;\ t\not\equiv 1\ \textit{mod}\ 7.$$

Theorem 2 and the sequences obtained in [8] and [5] together solve Kotzig's problem for all values of n of the form $4r+1$ except $r=1$ and $r\equiv 5$ mod 7 and they also solve it for all values of n of the form $4r+3$ except when $r\equiv 127$ mod 595. It is likely that the construction of further sequences U which satisfy the conditions of theorem 2 (that is, sequences U additional to the several classes of such sequences obtained in [8] and [5]) would enable Kotzig's *P*-quasigroup problem and the equivalent codeword existence problem to be resolved completely.

REFERENCES

[1] J. Dénes and A. D. Keedwell, *On P-quasigroups and decompositions of complete undirected graphs*, J. Combinatorial Theory, Ser. B., 13 (1972), 270—275.

[2] J. Dénes and A. D. Keedwell, "*Latin Squares and their Applications*", Akadémiai Kiadó, Budapest/English Universities Press, London/Academic Press, New York, 1974.

[3] J. Dénes and E. Török, *Groups and Graphs.* "*Combinatorial Theory and its Applications*", pp. 257—289, North Holland, Amsterdam, 1970.

[4] B. Gordon, *Sequences in groups with distinct partial products.* Pacific J. Math., 11 (1961), 1309—1313.

[5] A. J. W. Hilton and A. D. Keedwell, *Further results concerning P-quasigroups and complete graph decompositions*, Discrete Math. 14 (1976), 311—318.

[6] A. D. Keedwell, *Some problems concerning complete latin squares*, "Combinatoric" (Proc. British Combinatorial Conf., 1973), pp. 89—96, London Math. Soc. Lecture Note Series 13, Cambridge Univ. Press, 1974.

[7] A. D. Keedwell, *Some connections between latin squares and graphs*, Atti del Colloquio Internazionale sulle Teorie Combinatorie, Roma, 1973.

[8] A. D. Keedwell, *Row complete squares and a problem of A. Kotzig concerning P-quasigroups and Eulerian circuits*, J. Combinatorial Theory, Ser. A., 18 (1975), 291—304.

[9] A. Kotzig, *Groupoids and partitions of complete graphs*, "*Combinatorial Structures and their Applications*" (Proc. Colloq. Calgary, 1969), pp. 215—221, Gordon and Breach, New York, 1970.

[10] N. S. Mendelsohn, *Hamiltonian decomposition of the complete directed n-graph*, "Theory of Graphs" (Proc. Colloq. Tihany, 1966) pp. 237—241, Academic Press, New York, 1968.

[11] P. J. Owens, *Solutions to two problems of Dénes and Keedwell on row complete latin squares*, To appear in J. Combinatorial Theory.

[12] L. J. Paige, *A Note on finite abelian groups*, Bull. Amer. Math. Soc. 53 (1947), 590—593.

[13] L. L. Wang, *A test for the sequencing of a class of finite groups with two generators*, Amer. Math. Soc. Notices 20 (1973), 73 T—A 275.

[14] D. Warwick, *Methods of construction and a computer search for row complete latin squares*, Undergraduate Special Study, University of Surrey, 1973.

University of Surrey
Guildford, Surrey GU2 5XH