COMMENTATIONES MATHEMATICAE UNVERSITATIS CAROLINAE

26,2 (1985)

GROUP DISTANCES OF LATIN SQUARES

Aleš DRÁPAL and Tomáš KEPKA

Abstract: Some results concerning the distances between the tables of finite groups and latin squares are proved.

Key words: Group, latin square.

Classification: 05B15

For an integer $n \geq 2$, let gdist(n) denote the least non-zero number of changes in the Cayley table of an n-element group to obtain another latin square. These numbers play an important rôle in the problem concerning the largest possible number of associative triples of elements in finite non-associative quasigroups (see [2]). The purpose of this short note is to develop a technique which might be useful in finding some lower bounds for the numbers gdist(n).

1. Preliminaries. Throughout this note, the terminology, notation, etc., of [3] is used.

Recall that $\mathcal{R}$ denotes the category of reduced partial groupoids and $\mathcal{T}$ the full subcategory of $\mathcal{R}$ consisting of reduced balanced cancellative partial groupoids.

A homomorphism f of a partial groupoid K into a partial groupoid L is called complete if for all $(x,y) \in M(L)$ such that $x,y,xy \in f(K)$ there exists a pair $(a,b) \in M(K)$ with $f(a) = x$ and

$f(b) = y$ (then $f(ab) = xy$). Obviously, every strong homomorphism is complete.

A partial groupoid L is called a (complete, strong) partial subgroupoid of a partial groupoid K if $L \subseteq K$ and this inclusion is a (complete, strong) homomorphism.

Let $K \in \mathcal{R}$. We shall say that K is trivial if card $B(K) =$ $=$ card $C(K) =$ card $D(K) = 1$. In this case, $1 \leq$ card $K \leq 3$ and card $K = 3$, provided K is balanced. A homomorphism f of K into $L \in \mathcal{R}$ is called trivial if $f[K]$ is a trivial partial groupoid. In this case, $f[K]$ is a strong partial subgroupoid of L, provided L is balanced.

Let $K \in \mathcal{R}$ and $d \in K$. Put $r(d) = r(K,d) =$ card $\{(a,b,c);$ $a,b,c \in K,\ ab = c,\ d \in \{a,b,c\}\}$. Since K is reduced, $r(d) \geq 1$.

Let $K,L \in \mathcal{R}$. We shall say that K is an immediate (strongly) open extension of L if L is a (strong) complete partial subgroupoid of K and $r(K,d) = 1$ for every $d \in K - L$. Further, we shall say that K is an (strongly) open extension of L if there exists a finite sequence $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ such that $n \geq 1$, $K_0 = L$, $K_n = K$ and K_{i+1} is an immediate (strongly) open extension of K_i for each $0 \leq i < n$.

A partial groupoid $K \in \mathcal{T}$ is called (strongly) open if it is non-trivial and it is a (strongly) open extension of a trivial partial subgroupoid $L \in \mathcal{T}$.

1.1. __Lemma.__ Let $K \in \mathcal{T}$ and let $a,b,c \in K$ be such that $ab = c$. Then $L = \{a,b,c\}$ is a three-element strong partial subgroupoid of K and L is a trivial partial groupoid.

__Proof.__ Obvious.

1.2. __Lemma.__ Let $K \in \mathcal{T}$ be such that $m(K) \leq 3$. Then:

(i) $r(a) = 1$ for at least one $a \in A(K)$.

(ii) K is strongly open, provided it is non-trivial.

Proof. Easy.

1.3. Lemma. Let $K \in \mathcal{T}$ be such that $m(K) = 4$. Then exactly one of the following three cases takes place:

(i) $r(a) = 1$ for at least one $a \in A(K)$ and K is strongly open.

(ii) $r(a) \geq 2$ for every $a \in A(K)$, $r(d) = 1$ for at lest one $d \in D(K)$, K is open and K is not strongly open.

(iii) $r(a) \geq 2$ for every $a \in A(K)$, $r(d) \geq 2$ for every $d \in D(K)$, K is not open and $H(K)$ is a cyclic group of order 2.

Proof. Easy.

1.4. Lemma. Let $K, L \in \mathcal{T}$ be such that K is an open extension of L and let f be a homomorphism of L into a division groupoid G. Then f can be extended to a homomorphism of K into G.

Proof. We can assume that K is an immediate open extension of L. However, then the result is clear.

1.5. Lemma. Let $K \in \mathcal{T}$ be open and let G be a non-trivial division groupoid. Then there exists at least one non-trivial homomorphism of K into G.

Proof. If $m(K) = 2$ then the result is obvious. Suppose that $m(K) \geq 3$. Then there is a strong partial subgroupoid L of K such that $m(L) = 2$ and K is an open extension of L. Now, the result follows from 1.4.

1.6. Lemma. Let F be a homomorphism of a partial groupoid K into a group G and let $(a,b) \in M(K)$. Then there exists a homomorphism g of K into G such that $g(a) = g(b) = g(ab) = 1$. Moreover, g is non-trivial, provided f is so.

Proof. Put $g(c) = f(a)^{-1}f(c)$, $g(d) = f(d)f(b)^{-1}$ and $g(e) = f(a)^{-1}f(e)f(b)^{-1}$ for all $c \in B(K)$, $d \in C(K)$ and $e \in D(K)$.

1.7. **Lemma.** Let f be a non-trivial homomorphism of a partial groupoid $K \in \mathcal{T}$ into a group G and let H be a normal subgroup of G. Then there exists either a non-trivial homomorphism of K into H or a non-trivial homomorphism of K into G/H.

Proof. With respect to 1.6 , we can assume that 1 is contained in all the sets $f(B(K))$, $f(C(K))$, $f(D(K))$. Denote by g the natural homomorphism of G onto G/H. If gf is a trivial homomorphism then $f(K) \subseteq H$.

1.8. **Lemma.** Let $K \in \mathcal{T}$ and G be a group. Then there exists a non-trivial homomorphism of K into G iff there exists a non-trivial homomorphism of $H(K)$ into G.

Proof. Choose $x = (a,b) \in M(K)$ and consider the congruence $s = s_x$ by [3, Lemma 2.2], the natural homomorphism q of K onto $L = K/s$, the isomorphism h of $G(L)$ onto $H(K)$ by [3, Lemma 5.2] and the modificative homomorphism g of L into $G(L)$ by [3, Proposition 3.1]. Now, let f be a non-trivial homomorphism of K into G. With regard to 1.6, we can assume that $f(a) = f(b) = 1$. Then $s \subseteq \ker f$, and hence $f = kq$, k being a non-trivial homomorphism of L into G. We have $k = pg$ for a homomorphism p of $G(L)$ into G and ph^{-1} is a non-trivial homomorphism of $H(K)$ into G. Conversely, let k be a non-trivial homomorphism of $H(K)$ into G. Put $f = khgq$. Then f is a homomorphism of K into G and $f(a) = f(b) = f(ab) = 1$. On the other hand, the group $k(H(K))$ is generated by $f(K)$ and it is non-trivial. Consequently, f is non-trivial.

1.9. **Lemma.** Let $K \in \mathcal{T}$ be non-trivial, $ab = c$ for some $a,b,c \in K$ and let G be a non-trivial division groupoid. Suppose that either $r(a) = r(b) = 1$ or $r(a) = r(c) = 1$ or $r(b) = r(c) = 1$. Then there exists at least one non-trivial homomorphism of K into G.

Proof. It is divided into several parts.

(i) $r(a) = r(b) = r(c) = 1$. Let $x,y \in G$ be such that $x \neq y$. Define a mapping f of K into G by $f(u) = f(v) = x$, $f(w) = xx$, $f(a) = f(b) = y$ and $f(c) = yy$ for all $u \in B(K)$, $v \in C(K)$, $w \in D(K)$, $u \neq a$, $v \neq b$ and $w \neq d$. Then f is a non-trivial homomorphism of K into G.

(ii) $r(a) = r(b) = 1$ and $r(c) \geq 2$. Let $x,y \in G$ be such that $x \neq y$. There exists $z \in G$ such that $yz = xx$. Now, define f by $f(u) = f(v) = x$, $f(w) = xx$, $f(a) = y$, $f(b) = z$ for all $u \in B(K)$, $v \in C(K)$ and $w \in D(K)$, $u \neq a$, $v \neq b$.

(iii) $r(a) = r(c) = 1$ and $r(b) \geq 2$. Let $x,y \in G$, $x \neq y$. Define f by $f(u) = f(v) = x$, $f(w) = xx$, $f(a) = y$ and $f(c) = yx$ for all $u \in B(K)$, $v \in C(K)$ and $w \in D(K)$, $u \neq a$, $w \neq c$.

(iv) $r(b) = r(c) = 1$ and $r(a) \geq 2$. In this case, we can proceed similarly as in (iii).

2. Homomorphisms into groups. Let G be a non-trivial group. A partial groupoid K is said to be G-flat (or only flat) if every homomorphism of K into G is trivial.

Let $n \geq 2$ be an integer. We denote by $z(n) = z(G,n)$ the minimum of all $m(K)$ where $K \in \mathcal{T}$ is flat and there exists a non-trivial homomorphism of K into an n-element group.

2.1. Lemma. Let $K \in \mathcal{T}$ be flat.

(i) If f is a homomorphism of K into $L \in \mathcal{T}$ then $f[K]$ is flat.

(ii) K is not open.

(iii) If K is an open extension of $L \in \mathcal{T}$ then L is flat.

Proof. Use 1.4 and 1.5.

2.2. Lemma. Suppose that G is a torsionfree group and let $K \in \mathcal{T}$ be such that H(K) is a torsion group. Then K is flat.

Proof. This follows immediately from 1.8.

2.3. Lemma. Let $K \in \mathcal{T}$ be non-trivial and flat and let $a,b,c \in K$ be such that $ab = c$. Then either $r(a) \geq 2$, $r(b) \geq 2$ or $r(a) \geq 2$, $r(c) \geq 2$ or $r(b) \geq 2$, $r(c) \geq 2$.

Proof. This follows immediately from 1.9.

2.4. Proposition. Let $n \geq 2$ be an integer and let $K \in \mathcal{T}$ be a partial groupoid such that $m(K) = z(n)$. Suppose that there exists a non-trivial homomorphism f of K into an n-element group H. Then $r(a) \geq 2$ for every $a \in K$.

Proof. Assume, on the contrary, that $r(a) = 1$ for some $a \in K$. There are three different elements $x,y,z \in K$ such that $xy = z$ and $a \in \{x,y,z\}$. Now, with respect to 2.3, the following cases can arise:

(i) $r(x) = 1$, $r(y) \geq 2$ and $r(z) \geq 2$. Put $L = K - \{x\}$. Then $L \in \mathcal{T}$, L is a strong partial subgroupoid of K, $m(L) = m(K) - 1$, K is an open extension of L and L is flat. According to 1.7, we can assume that $1 \in f(B(L)) \cap f(C(L)) \cap f(D(L))$. Since $f|L$ is trivial, $f(L) = 1$. Then $f(x) = f(x)1 = f(x)f(y) = f(xy) = f(z) = 1$ and f is trivial, a contradiction.

(ii) $r(x) \geq 2$, $r(y) = 1$ and $r(z) \geq 2$. We can proceed similarly as in (i).

(iii) $r(x) \geq 2$, $r(y) \geq 2$ and $r(z) = 1$. Again, we can proceed similarly as in (i) (in this case, $L = K - \{z\}$ is a complete partial subgroupoid of K).

2.5. Lemma. Suppose that G is a torsionfree group. Then $4 \leq z(n) \leq 2n$ for every $n \geq 2$.

__Proof.__ By 2.1(ii) and 1.2(ii), $m(K) \geq 4$ for every non-trivial flat partial groupoid $K \in \mathcal{T}$. Hence $4 \leq z(n)$. Further, consider the partial groupoid $Z = Z(n, \circ)$ defined in [4, § 7]. Then $m(Z) = 2n$ and $H(Z)$ is a cyclic group of order n. Consequently, Z is flat by 2.2 and $z(n) \leq 2n$.

2.6. __Proposition.__ Suppose that G is a torsionfree group. Then for every $n \geq 2$, $z(n) = 4$ iff n is even.

__Proof.__ First, let $z(n) = 4$. Then there are $K \in \mathcal{T}$ and a group H such that K is flat, $m(K) = 4$, H contains just n elements and there exists a non-trivial homomorphism of K into H. The partial groupoid K is not open, and so $H(K)$ is a two-element group by 1.3(iii). By 1.8, there is a non-trivial homomorphism of $H(K)$ into H. In particular, n is even. Now, let n be even. Then we can proceed conversely.

2.7. __Proposition.__ Let $n \geq 3$ be odd. Then $z(n)$ is equal to the minimum of all $z(p)$, p being a prime dividing n.

__Proof.__ The result follows from 1.7 and the fact that n is prime, provided there is a simple group of order n.

3. __Homomorphisms into ordered partial groupoids.__ In this section, let G be a cancellative reduced partial groupoid linearly ordered by an ordering $\leq$, i.e. $\leq$ is a linear ordering defined on G and $ab \leq cd$ whenever $(a,b), (c,d) \in M(G)$, $a \leq c$ and $b \leq d$.

3.1. __Lemma.__ Let $I = (K(\circ), K(*))$ be a couple of finite simple companions. Then every homomorphism of $K(\circ)$ into G is trivial.

__Proof.__ Let f be a homomorphism of $K = K(\circ)$ into G. There is an element $x \in f(D(K))$ such that $y \not\leq x$ for any $y \in f(D(K))$. Put

$N = \{(a,b) \in M(K);\ f(a \circ b) = x\}$ and define a relation r on N by $((a,b),(c,d)) \in r$ iff $f(a) = f(c)$ and $f(b) = f(d)$. Since G is cancellative, each of the two equalities implies the other. Obviously, r is an equivalence and we denote by $N_1,\dots,N_k$ the blocks of r. Without loss of generality, we can assume that $f(a_1) < f(a_2) < \dots < f(a_k)$, $(a_i,b_i) \in N_i$. Now, we are going to prove that N_1 is an admissible subset of $M(K)$ in the sense of [4, § 5]. Let $(a,b) \in N_1$. Put $P = \{(u,v) \in M(K);\ f(u * v) = x,\ f(u) = f(a)\}$, $Q = \{(u,v) \in M(K);\ f(u * v) = x,\ f(v) = f(b)\}$. The rest of the proof is divided into several parts.

(i) If $(u,v) \in P$ and $u * v = u \circ w$ then $f(u \circ w) = x$, $(u,w) \in N_1$. Conversely, if $(u,w) \in N_1$ and $u \circ w = u * v$ then $(u,v) \in P$. Hence we have injective mappings of P into N_1 and of N_1 into P, so that card P = card N_1.

(ii) Similarly as in (i) we can show that card Q = card N_1.

(iii) Let $(u,v) \in Q$. We have $u * v = w \circ v = u \circ z$, $f(a)f(b) = x = f(u * v) = f(u \circ z) = f(u)f(z)$, so that $(u,z) \in N$ and $f(a) \le f(u)$. On the other hand, $x = f(a)f(b) \le f(u)f(v)$, since $f(b) = f(v)$, hence $x = f(u)f(v) = f(u \circ v)$, $f(u) = f(a)$ and $(u,v) \in N_1$. We have proved that $Q \subseteq N_1$. Now, it is easy to see that $Q \subseteq P$.

(iv) By (i),(ii) and (iii), we have $P = Q = N_1$. Consequently, N_1 is an admissible subset of $M(K)$. Since the couple I is simple, $N_1 = M(K)$ and f is trivial.

3.2. <u>Corollary</u>. Let $K \in \mathcal{T}$ be a primary groupoid and let G be a linearly ordered non-trivial group. Then K is G-flat.

4. <u>The main result</u>

4.1. <u>Proposition</u>. Let G be a linearly ordered non-trivial group. Then, for every $n \ge 2$, $z(G,n) \le \mathrm{gdist}(n)$.

Proof. The result is an immediate consequence of 3.2 and [3, Proposition 7.5].

4.2. Proposition. Let G be a linearly ordered non-trivial group and $n \geq 2$ and integer. Then there is a prime p dividing n such that $z(G,p) \leq \mathrm{gdist}(n)$.

Proof. The result follows from 4.1 and 2.7.

References

[1] J. DÉNES and A.D. KEEDWELL: Latin Squares and Their Applications, Akadémiai Kiadó, Budapest, 1974.

[2] A. DRÁPAL: On quasigroups rich in associative triples, Discrete Math. 44(1983), 251-165.

[3] A. DRÁPAL and T. KEPKA: Group modifications of some partial groupoids, Annals of Discr. Math. 18(1983), 319-332.

[4] A. DRÁPAL and T. KEPKA: Exchangeable partial groupoids I, Acta Univ. Carolinae 24(1983), 57-72.

Matematicko-fyzikální fakulta, Univerzita Karlova, Sokolovská 83, 186 00 Praha 8, Czechoslovakia

(Oblatum 8.10. 1984)