Aleš Drápal; Tomáš Kepka

On a distance of groups and Latin squares

Commentationes Mathematicae Universitatis Carolinae, Vol. 30 (1989), No. 4, 621--626

Persistent URL: http://dml.cz/dmlcz/106781

Comment.Math.Univ.Carolinae 30,4(1989)621–626

On a distance of groups and latin squares

ALEŠ DRÁPAL, TOMÁŠ KEPKA

Abstract. A lower bound for the distances of the tables of finite cyclic groups and latin squares is found.

Keywords: Group, latin square

Classification: 05B15

1. Introduction.

A groupoid is a non-empty set together with a binary operation and a quasigroup is a groupoid with unique division, so that the multiplication tables of finite quasigroups are latin squares. We denote by $\mathcal{Q}$ and $\mathcal{G}$ the classes of finite quasigroups and groups, resp.

Now, if $G = (A; \circ)$ and $H = (A, *)$ are two groupoids with the same finite underlying set A, $\mathrm{card}(A) = n$, we put $d = \mathrm{dist}(G, H) = \mathrm{card}(\{(a, b) \in A^{(2)}; a \circ b \neq a * b\})$. Clearly, $0 \leqslant d \leqslant n^2$ and $d = 0$ iff $G = H$. Further, it is easy to see that $d \geqslant 4$, provided $G \neq H$ and $G, H \in \mathcal{Q}$. On the other hand, by [1, Theorem 3.2.5], for every $n \geqq 2$, $n \neq 3$, there exist $G, H \in \mathcal{Q}$ with the same finite n-element underlying set such that $\mathrm{dist}(G, H) = 4$. Therefore, the minimal possible distance of two different finite quasigroups is 4 for $n \geqq 2$, $n \neq 3$, and (this may be checked easily) 6 for $n = 3$. In contrast to this simple result, the situation becomes more complicated if we consider the minimal possible distance of a quasigroup and a group.

For every $n \geqq 2$, let $\mathrm{gdist}(n) = \min \mathrm{dist}(G, H)$, where $G \in \mathcal{G}$, $H \in \mathcal{Q}$, $G \neq H$, and both G and H have the same finite n-element underlying set. One can show easily that $\mathrm{gdist}(n) \leqslant \mathrm{gdist}(p) \leqslant 2p$, p being the least prime dividing n. As $\mathrm{gdist}(2) = 4$, we have $\mathrm{gdist}(n) = 4$ for every even n. To get a lower bound of $\mathrm{gdist}(n)$ for n odd does not seem to be so easy and it is the purpose of this note to prove that $\mathrm{gdist}(n) \geqq e.\ln p + 3$ in this case. Finally, notice that the numbers $\mathrm{gdist}(n)$ were used in [2] for enumeration of associative triples in finite quasigroups.

Throughout this paper, let N denote the set of positive integers, Z the ring of integers and, for a prime p, Z_p the field of integers modulo p.

2. Matrices of special type.

In this section, let R be an integral domain and Q the quotient field of R. For $m, n \in N$, let $M(R, m, n)$ designate the set of $m \times n$ matrices over R. If $A(B, \dots)$ is a matrix, then $a_{i,j}(b_{i,j}, \dots)$ are the elements, $a_i(b_i, \dots)$ the rows and $_ja(_jb, \dots)$ the columns of $AB, \dots$.

Consider the following three conditions for a matrix $A \in M(R, m, n)$:

(1) $a_{ij} \in \{0, 1\}$ for all $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$;

(2) ${}_ja \neq 0$ for every $1 \leqslant j \leqslant n$;
(3) if $1 \leqslant i < k \leqslant m$, then $a_{ij} \neq 0 \neq a_{kj}$ for at most one $1 \leqslant j \leqslant n$.

Further, if $3 \leqslant n$ and $\alpha = (p, q, o) \in N^{(3)}$ is such that $\Sigma\alpha = p + q + o = n$, then we define the following condition:

(α) for every $1 \leqslant i \leqslant m$ there are exactly three indices t, k, l with $1 \leqslant t \leqslant p < k \leqslant p + q < l \leqslant n$ and $a_{ij} \neq 0$ iff $j \in \{t, k, l\}$.

If A satisfies (1) and (2), then (α) may be fulfilled for at most one $\alpha \in N^{(3)}$, $\sum\alpha = n$.

Let $\alpha = (p, q, o) \in N^{(3)}$, $n = \sum\alpha$. Denote by $R(\alpha)$ the set of $w \in R^{(n)}$ such that $w_1 = \cdots = w_p$, $w_{p+1} = \cdots = w_{p+q}$, $w_{p+q+1} = \cdots = w_n$ and $w_p + w_{p+q} + w_n = 0$. Then $R(\alpha)$ is a submodule of $R^{(n)}$ and it is a free R-module of dimension 2. Now, if $A \in M(R, m, n)$ is a matrix satisfying (1) and (α), then $Aw = 0$ for every $w \in R(\alpha)$ and we shall say that A is (R, α)-flat if $R(\alpha) = \{w \in R^{(n)}; Aw = 0\}$.

Lemma 2.1. *The following conditions are equivalent:*

(i) *A is (R, α)-flat.*
(ii) *A is (Q, α)-flat.*
(iii) *The rank of A over Q is $n - 2$ (and hence $n \leqslant m + 2$).*

PROOF : Clearly, A is (R, α)-flat iff it is (Q, α)-flat. Further, $n = \dim V + \dim W$, where V is the subspace of $Q^{(n)}$ generated by the rows of A and $W = \{w \in Q^{(n)}; Aw = 0\}$; we have $Q(\alpha) \subseteq W$, $\dim Q(\alpha) = 2$ and the rank of A is equal to $\dim V$. Consequently, $Q(\alpha) = W$ iff $\dim W = 2$ and iff the rank of A is $n - 2$. ∎

3. Determinants.

In the sequel, let R be an integral domain and Q the quotient field of R.

Lemma 3.1. *Let $n \in N$, $A \in M(R, n+1, n)$ and let $A_i \in M(R, n, n)$ be the matrix obtained from A by omission of the row a_i, $1 \leqslant i \leqslant n + 1$. Let $r_1, \ldots, r_{n+1} \in R$ be such that $\sum_{k=1}^{n+1} r_k a_k = 0$. Then $r_j \cdot \det A_i = (-1)^{i+j} \cdot \det A_j$ for all $1 \leqslant i \leqslant j \leqslant n+1$.*

PROOF : Put $B = A_j$. Then the i-th row b_i of B is equal to a_i. By substituting this row by the vector $-r_j a_j = \sum_{k \neq j} r_k a_k$ we get a matrix C such that $\det C = r_j \cdot (-1)^{j-i} \cdot \det A_i$ and $\det C = r_i \cdot \det A_j$. ∎

In the rest of this section, let $\alpha = (p, q, o) \in N^{(3)}$, $\sum\alpha = n$ and let $A \in M(R, m, n)$ be a matrix satisfying (1) and (α). For $s \in N$ and $1 \leqslant k_1 \leqslant \cdots \leqslant k_s \leqslant n$ we denote by $A[k_1, \ldots, k_s]$ the matrix $B \in M(R, m + s, n)$ such that $b_1 = a_1, \ldots, b_m = a_m$, $b_{ij} = 0$ and $b_{ik_{i-m}} = 1$ for all $m < i \leqslant m + s$ and $j \neq k_{i-m}$.

Lemma 3.2. *Let $n = m + 2$ and $1 \leqslant r \leqslant p < s \leqslant p + q < t \leqslant n$. Then $\det A[r, s] = \det A[s, t] = -\det A[r, t]$.*

PROOF : Consider the matrix $B = A[r, s, t] \in M(R, n+1, n)$. The rows $b_1, \ldots, b_{n+1}$ are not linearly independent in $Q^{(n)}$, and hence $\sum r_k b_k = 0$ for some $r_k \in R$ such that at least one of them is not zero. If $\operatorname{rank}_Q A < m$, then all the determinants

in question are zero. Hence, assume that $\operatorname{rank}_Q A = m$, so that either $r_{n-1} \neq 0$ or $r_{n+1} \neq 0$. Further, let $v, w \in R(\alpha)$ be such that $v_p = w_p = 1$, $v_{p+q} = w_n = -1$ and $v_n = w_{p+q} = 0$. Then $b_k v = b_k w = 0$ for $1 \leqslant k \leqslant m$ and $r_{n-1} - r_n = (\sum r_1 b_1)v = 0 = (\sum r_1 b_1)w = r_{n-1} - r_{n+1}$. Consequently, $r_{n-1} = r_n = r_{n+1} \neq 0$ and the rest follows from 3.1.

Let $1 \leqslant r < s \leqslant n$. Omitting the columns r^a and s^a of A we get a matrix from $M(R, m, n-2)$. This matrix will be denoted by $A(r,s)$. ∎

Let $J(\alpha)$ denote the set of $(r,s) \in N^{(2)}$ such that either $1 \leqslant r \leqslant p < s \leqslant n$ or $1 \leqslant r \leqslant p+q < s \leqslant n$.

Lemma 3.3. *Let* $n = m+2$ *and* (r,s), $(r',s') \in J(\alpha)$. *Then* $\det A[r,s] = \pm \det A[r',s'] = \pm \det A(r,s) = \pm \det A(r',s')$.

PROOF : Easy (use 3.2). ∎

Now, if $R = Z$ and $n = m+2$, then we put $\Delta(A) = |\det A[r,s]|$, $(r,s) \in J(\alpha)$.

Lemma 3.4. *Let* $n = m+2$. *Then* A *is* (R,α)*-flat iff* $\det A[r,s] \neq 0$ *for* $(r,s) \in J(\alpha)$.

PROOF : Suppose that $r \leqslant p < s \leqslant p+q$ and put $B = A[r,s]$. If $w \in Q^{(n)}$, then $Bw = 0$ iff $Aw = 0$ and $w_r = w_s = 0$. In such a case, $w \in Q(\alpha)$ implies $w = 0$ and so $\det A[r,s] \neq 0$, provided A is (R,α)-flat. Now, suppose that $\det A[r,s] \neq 0$ and let $v \in R^{(n)}$, $Av = 0$. Define $u \in R^{(n)}$ by $u_1 = \cdots = u_p = -v_r$, $u_{p+1} = \cdots = u_{p+q} = -v_s$ and $u_{p+q+1} = \cdots = u_n = v_r + v_s$. Then $u \in R(\alpha)$, $B(v-u) = 0$, $v - u = 0$ and $v = u$. ∎

4. Some enumerations.

Lemma 4.1. *Let* $n \in N$ *and let* $A \in M(Z,n,n)$ *be a matrix satisfying (1) such that there exists* $1 \leqslant r < n$ *with* $a_{ij}a_{ik} = 0$ *whenever* $1 \leqslant i,j,k \leqslant n$ *and either* $j,k \leqslant r$ *or* $r < j,k$. *Then* $\det A \in \{0,1,-1\}$.

PROOF : For any $1 \leqslant i \leqslant n$, let $t(i)$ denote the number of indices $1 \leqslant j \leqslant n$ with $a_{ij} = 1$; by the hypothesis, we have $t(i) \leqslant 2$. Further, let $v \in Z^{(n)}$ be such that $v_j = 1$ for $1 \leqslant j \leqslant r$ and $v_j = -1$ for $r < j \leqslant n$. Clearly, $a_i v = 0$ whenever $t(i) = 2$. Hence either $\det A = 0$ or $t(i) = 1$ for some $1 \leqslant i \leqslant n$. If $1 \leqslant j \leqslant n$ is such that $a_{ij} = 1$, then $\det A = (-1)^{i+j} \cdot \det B$, where B is obtained by deletion of the i-th row and the j-th column from A; we have $B \in M(Z, n-1, n-1)$ and the result follows by induction. ∎

In the following three lemmas, let $m \in N$, $n = m+2$, $\alpha = (p,q,o) \in N^{(3)}$, $\sum \alpha = n$ and let $A \in M(Z,m,n)$ be a matrix satisfying (1) and (α). For all $1 \leqslant j \leqslant n$, put $s(A,j) = \sum_{i=1}^{m} a_{ij}$. Obviously, $\sum_{j=1}^{p} s(A,j) = \sum_{j=p+1}^{p+q} s(A,j) = \sum_{j=p+q+1}^{n} s(A,j) = m$.

Lemma 4.2.

(i) *If* $p = 1$, *then* $\Delta(A) \leqslant 1$.

(ii) *If* $p \geqslant 2$ *and* $1 \leqslant k \leqslant p$, *then* $\Delta(A) \leqslant \sum_{j=1, j\neq k}^{p} s(A,j)$.

PROOF : (i) We have $(1,2) \in J(\alpha)$ and $\det A(1,2) \in \{0,1,-1\}$ by 4.1.

(ii) The rows of the matrix $A(k,p+1)$ can de permuted in such a way that we obtain a matrix B with the following property:

If $1 \leqslant i \leqslant i' \leqslant m$, $1 \leqslant j,j' \leqslant p-1$ and $b_{ij} = 1 = b_{i'j'}$, then $j \leqslant j'$ and if $b_i = 0$, then $b_{i'} = 0$. Therefore, $b_{ij} = 1$ iff $s(B,1)+\cdots+s(B,j-1) < i \leqslant s(B,1)+\cdots+s(B,j)$. Now, denote by K the set of ordered $p-1$-tuples $u = (u_1,\ldots,u_{p-1})$ such that $1 \leqslant u_1 < \cdots < u_{p-1} \leqslant m$ and by $B(u)$ the submatrix of B induced by the intersection of the first $p-1$ columns of B and of the rows $b_{u_1},\ldots,b_{u_{p-1}}$. Further, let $B[u]$ denote the complement of $B(u)$, i.e. the submatrix of B obtained be deletion of indicated rows and columns. Expanding $\det B$ along the first $p-1$ columns, we get the inequality $|\det B| \leqslant \sum_{u \in K} |\det B(u)| \cdot |\det B[u]|$. However, by 4.1, $|\det B[u]| \in \{0,1\}$ and it is easy to see that $\det B(u) \neq 0$ (and then $|\det B(u)| = 1$) iff $s(B,1)+\cdots+s(B,j-1) < u_j \leqslant s(B,1)+\cdots+s(B,j)$ for any $1 \leqslant j \leqslant p-1$. The rest is clear, since the latter case occurs just $\prod_{j=1}^{p-1} s(B,j)$ - times. ∎

Lemma 4.3. *Put* $r = \min(p,q,o)$.

(i) *If* $r = 1$, *then* $\Delta(A) \leqslant 1$.
(ii) *If* $m \leqslant 5$, *then* $\Delta(A) \leqslant 2$.
(iii) *If* $m = 6$, *then* $\Delta(A) \leqslant 3$.
(iv) *If* $r \geqslant 2$ *and* $m \geqslant 5$, *then* $\Delta(A) \leqslant ((m-3)/(r-1))^{r-1}$.

PROOF : We can assume without loss of generality that $r = p$. Now, (i) follows from 4.2(i). If $m \leqslant 3$, then $p = 1$. Hence, suppose for a moment that $4 \leqslant m \leqslant 6$ and $p \geqslant 2$. Then $p = 2$ and $\Delta(A) \leqslant m/2$ by 4.2(ii). Similarly, if $m = 6$, then $\Delta(A) \leqslant 3$. Finally, let $m \geqslant 5$ and $p \geqslant 2$. Then $2p < m$ and hence there is $1 \leqslant k \leqslant p$ with $s(A,k) \geqslant 3$. We have $\sum_{j=1, j\neq k}^{p} s(A,j) \leqslant m-3$ and $\Delta(A) \leqslant ((m-3)/(p-1))^{p-1}$ by 4.2(ii). ∎

Lemma 4.4. *If* $m \geqslant 6$, *then* $\Delta(A) < e^{(m-3)/e}$.

PROOF : The result follows easily from 4.3 (iv). ∎

For a prime π we define $\delta(\pi)$ to be the least $m \in N$ such that there exists a matrix $A \in M(Z,m,m+2)$ with the following properties: A satisfies (1), (3) and (α) for some $\alpha \in N^3$ with $\sum\alpha = m+2$, $\Delta(A) \neq 0$ and π divides $\Delta(A)$. Notice that A satisfies (2) since $\Delta(A) \neq 0$. Further, although (3) does not follow from the remaining assumptions, the definition of $\delta(\pi)$ is independent of it; dropping this condition we get the same numbers. The proof of this fact is easy and it is omited as the result will not be used in the sequel.

Lemma 4.5. $\delta(2) = 4$ *and* $\delta(\pi) > e.\ln\pi + 3$ *for any prime* $\pi \geqslant 3$.

PROOF : This is an easy consequence of 4.4. ∎

Let π be a prime, $m,n \in N$ and let $A \in M(Z,m,n)$ be a matrix satisfying (1), (3) and (α) for some $\alpha \in N^3$, $\sum\alpha = n$. Denote by$f$ the natural projection of Z onto Z_π.

Lemma 4.6. *Suppose that $n = m + 2$. The following conditions are equivalent:*

(i) $\Delta(A) \neq 0$ *and* π *divides* $\Delta(A)$.

(ii) A *is* (Z, α)*-flat and* $f(A)$ *is not* (Z_π, α)*-flat.*

PROOF : Apply 3.4. ∎

Lemma 4.7. *Suppose that A is (Z, α)-flat and $f(A)$ is not (Z_π, α)-flat. Then $\delta(\pi) \leqslant m$.*

PROOF : By 2.1, $n \leqslant m + 2$. Assume that $n < m + 2$. Then the rows of A are not linearly independent over Q and there are $r_1, \ldots, r_m \in Z$ and $1 \leqslant k \leqslant m$ such that $r_k \neq 0$, π does not divide r_k and $r_1 a_1 + \cdots + r_m a_m = 0$. Denote by B the matrix obtained from A by omission of the row a_k. Then $B \in M(Z, m-1, n)$ and it is easy to check that B satisfies (1), (3), (α), B is (Z, α)-flat and $f(B)$ is not (Z_π, α)-flat. Proceeding in this way we get a matrix $C \in M(Z, n-2, n)$ satisfying (1), (3) and (α) such that C is (Z, α)-flat and $f(C)$ is not (Z, α)-flat. The rest follows from 4.6. ∎

5. Partial groupoids and matrices.

A non-empty set K together with a partial binary operation is called a partial groupoid. We denote by $M(K)$ the set of ordered pairs $(a, b) \in K^{(2)}$ such that the product ab is defined and we put $B(K) = \{a; (a, b) \in M(K)\}$, $C(K) = \{b; (a, b) \in M(K)\}$ and $D(K) = \{ab; (a, b) \in M(K)\}$. The cardinalities of the sets $B(K)$, $C(K)$ and $D(K)$ are denoted by $p(K)$, $q(K)$ and $o(K)$, resp. The partial groupoid K is said to be balanced if the sets $B(K)$, $C(K)$ and $D(K)$ are pair-wise disjoint and it is said to be reduced if K is the union of these sets. The partial groupoid K is said to be cancellative if $ab \neq ac$ and $ed \neq fd$ whenever (a, b), (a, c), (e, d), $(f, d) \in M(K)$ and $b \neq c$, $e \neq f$. We denote by T the class of balanced reduced cancellative partial groupoids.

Let K and L be partial groupoids. A mapping f of K into L is called a homomorphism if $(f(a), f(b)) \in M(L)$ and $f(ab) = f(a)f(b)$ whenever $(a, b) \in M(K)$. The homomorphism f is called trivial if the sets $f(B(K))$, $f(C(K))$ and $f(D(K))$ contain each just one element. The partial groupoid K is said to be L-flat if every homomorphism of K into L is trivial.

For each $n \geqslant 2$, let $\xi(n)$ denote the minimum of all card $(M(K))$ where $K \in T$ is such that K is $(Z, +)$-flat but not G-flat for an n-element group G. By [4,Proposition 4.1], $\xi(n) \leqslant \mathrm{gdist}(n)$. In the rest of this section we shall prove that $\delta(\pi) = \xi(\pi)$ for every prime number $\pi \geqslant 2$.

Fix three pair-wise disjoint infinite countable sets $B = \{b_1, b_2, \ldots\}$, $C = \{c_1, c_2, \ldots\}$ and $D = \{d_1, d_2, \ldots\}$. A finite partial groupoid $K \in T$ is said to be in a normalized form if $B(K) = \{b_1, \ldots, b_{p(K)}\}$, $C(K) = \{c_1, \ldots, c_{q(K)}\}$, $D(K) = \{d_1, \ldots, d_{o(K)}\}$.

Let K be a finite partial groupoid in a normalized form and let ρ be a linear order defined on $M(K)$; $M(K) = \{x_1, \ldots, x_m\}$ and $(x_i, x_j) \in \rho$ iff $i \leqslant j$. We shall define a matrix $E = E(K, \rho) \in M(Z, m, n)$, $n = p + q + o$, $p = p(K)$, $q = q(K)$, $o = o(K)$ as follows : $e_{ij} = 1$ iff there are $r, s, t \in N$ such that $x_i = (b_r, c_s)$, $b_r c_s = d_t$ in K and either $j = r$ or $j = p + s$ or $j = p + q + t$; $e_{ij} = 0$ in all the remaining cases.

The matrix E satisfies (1) and (α) for $\alpha = (p, q, o)$. It satisfies (2) and (3) as well, since K is reduced and cancellative. If g is a mapping of K into Z and $w \in Z^{(n)}$ is such that $w_i = g(b_i)$, $w_j = g(c_{j-p})$ and $w_k = -g(d_{k-p-q})$ for all $1 \leqslant i \leqslant p < j \leqslant p+q < k \leqslant n$, then g is a homomorphism of K into $(Z,+)$ iff $Ew = 0$; in this case, g is trivial iff $w \in Z(\alpha)$. Similarly, if π is a prime, f is the natural projection of Z onto Z_π, g is a mapping of K into Z and $v \in Z^{(n)}$ is defined similarly as w above, then g is a homomorphism of K into $(Z_\pi,+)$ iff $f(E)v = 0$; again, g is trivial iff $v \in Z_\pi(\alpha)$.

Theorem 5.1. *e.ln*$\pi + 3 \leqslant \delta(\pi) = \xi(\pi)$ *for every prime* $\pi \geqslant 3$.

PROOF : First, let $K \in T$ be such that K is $(Z,+)$-flat, not $(Z_\pi,+)$-flat and $m = \mathrm{card}(M(K)) = \xi(\pi)$. We can assume that K is in a normalized form. Then the matrix $E = E(K,\rho)$ is (Z,α)-flat and $f(E)$ is not (Z_π,α)-flat. By 4.7, $\delta(\pi) \leqslant m$ and $\delta(\pi) \leqslant \xi(\pi)$. The inverse inequality is clear. ∎

Corollary 5.2. *Let* $n \geqslant 3$ *be an odd integer and let* π *be the least prime dividing* n. *Then* e.ln$\pi + 3 \leqslant \mathrm{gdist}(n)$.

PROOF : By [4,Proposition 4.2], $\xi(\lambda) \leqslant \mathrm{gdist}(n)$ for a prime λ dividing n. The result now follows from 5.1. ∎

REFERENCES

[1] J.Dénes, 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), 251–265.

[3] A.Drápal, T.Kepka, *Group modifications of some partial groupoids*, Annals of Discr. Math **18** (1983), 319–332.

[4] A.Drápal, T.Kepka, *Groups distances of latin squares*, Comment. Math. Univ. Carolinae **26** (1985), 275–289.

Fac. of Math. and Phys., Charles Univ., Sokolovská 83, 186 00 Prague, Czechoslovakia

(*Received* June 19,1989)