Commentationes Mathematicae Universitatis Carolinae

Aleš Drápal; Tomáš Kepka

Parity of orthogonal permutations

*Commentationes Mathematicae Universitatis Carolinae*, Vol. 28 (1987), No. 3, 427--432

Persistent URL: http://dml.cz/dmlcz/106555

COMMENTATIONES MATHEMATICAE UNIVERSITATIS CAROLINAE
28,3 (1987)

# PARITY OF ORTHOGONAL PERMUTATIONS

Aleš DRÁPAL, Tomáš KEPKA

Abstract: The parity of orthogonal permutations of some finite abelian groups is investigated.

Key words: Parity, orthogonal, permutation.

Classification: 20B25

---

This paper is a continuation of [2]. Here, we are investigating the parity of some orthogonal permutations which are not automorphisms. Again, the results yield constructions of idempotent quasigroups with prescribed order and parity of translations.

7. The case n=15. Let $G=Z_{15}(+)$. Consider the following two 14-cycles f and g:

f=(1 13 3 11 5 9 7 8 10 6 12 4 14 2),

g=(1 3 7 2 5 11 10 4 9 6 13 14 12 8).

It is easy to check that (f,g) is a pair of orthogonal permutations of C and that sgn(g)= -1=sgn(f).

7.1. Proposition. $\mathcal{O}(G,f)$ is an orthostrophic idempotent quasigroup of type (4) and order 15.

Proof. See [2, Lemma 3.6(iv)].

8. The case $n \leq 5$.

8.1. Proposition. (i) Every idempotent quasigroup of order 1 is of type (1).

(ii) There is no idempotent quasigroup of order 2.

(iii) Every idempotent quasigroup of order 3 is of type (4).

(iv) Every idempotent quasigroup of order 4 is of type (1).

Proof. (i) and (ii). Obvious.

(iii) Every translation is a 2-cycle.

(iv) Every translation is a 3-cycle.

8.2. <u>Proposition.</u> There is no idempotent quasigroup of order 5 and type (1).

Proof. Let, on the contrary, $Q(*)$ be such a quasigroup. Then its every (left or right) translation f is composed from two 2-cycles, and hence $f^2=1$. Therefore $a*b=c$ implies $c*b=a$ and $c*a=b$ for any $a,b,c\in Q$. Without loss of generality, we can assume $Q=\{1,2,3,4,5\}$ and $\mathcal{L}(1,Q(*))=(2\ 3)(4\ 5)$. Then $2*3=1$, and hence $2*1=3$. This implies $\mathcal{L}(2,Q(*))=(1\ 3)(4\ 5)$, a contradiction.

9. <u>The case</u> n=6

9.1. <u>Proposition.</u> There is no idempotent quasigroup of order 6 such that each right translation is an odd permutation.

Proof. Suppose that Q is such a quasigroup. Let $R=\{\mathcal{R}(a,Q);a\in Q\}$. For any $f\in R$, $f=(a\ b)(c\ d\ e)$, we denote the set $\{a,b\}$ by $D(f)$ and the set $\{c,d,e\}$ by $T(f)$. For $a,b\in Q$, let $f_{a,b}$ denote the (unique) permutation $f\in R$ with $f(a)=$ $=b$. Obviously, $\{a,b\}\subseteq T(f_{a,b})$ implies $\{a,b\}\subseteq T(f_{b,a})$.

(a) Suppose there are $f,g\in R$, $f\neq g$, such that $T(f)=T(g)=T$. Put $D=(D(f)\cup$ $\cup D(g))-(D(f)\cap D(g))$. As $D(f)\neq D(g)$, we have $Q=T\cup D(f)\cup D(g)$, and hence $\mathrm{card}(D)=2$. If $h\in R$, $f\neq h\neq g$, then $\max(\mathrm{card}(T(h)\cap D(f)), \mathrm{card}(T(h)\cap D(g)),$ $\mathrm{card}(T(h)\cap T))\leq 1$, and therefore $D\subseteq T(h)$. This allows for only two distinct translations h, a contradiction.

(b) The sets $D(f)$, $f\in R$ induce a graph on Q. Let G denote the graph complementary to such a graph. Then G has 9 edges and $\deg_G(x)\neq 1$ for any $x\in Q$. Moreover, by (a) $\deg_G(x)\neq 2$ for any $x\in Q$. Suppose that there exists $a\in Q$ with $\deg_G(a)=0$. The complete graph on five points has 10 edges, and therefore there is exactly one translation $f\in R$ such that $a\notin D(f)$. For any $g\in R$, $f\neq g$, we have $a\notin T(g)$, $T(f)\neq T(g)$ and $\mathrm{card}(D(f)\cap T(g))\leq 1$. Hence $\mathrm{card}(T(g)\cap T(f))=2$. However, this allows for at most three different translations g, a contradiction.

(c) By (a) and (b) we have $\deg_G(x)\geq 3$ for any $x\in G$. By counting the edges we find out that the equality has to take place. Choose any $a\in Q$ and let b,c,d be its adjacent points. Then either $f_{b,a}=f_{a,d}$ or $f_{b,a}=f_{a,c}$. Assume the latter one. Then $f_{b,a}=f_{a,c}=f_{c,b}$, $f_{d,a}=f_{a,b}=f_{b,d}$, $f_{c,a}=f_{a,d}=f_{d,c}$ and $f_{d,b}=$ $=f_{b,c}=f_{c,d}$. Therefore G has a complete subgraph on four points. However, such a graph cannot be extended to a 3-regular graph on six points.

9.2. <u>Corollary.</u> There is no idempotent quasigroup of order 6 and type (2) or (3) or (4).

9.3. Example. Consider the following quasigroup Q:

| Q | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 4 | 5 | 6 | 2 |
| 2 | 3 | 2 | 6 | 1 | 4 | 5 |
| 3 | 6 | 5 | 3 | 2 | 1 | 4 |
| 4 | 5 | 6 | 2 | 4 | 3 | 1 |
| 5 | 2 | 4 | 1 | 6 | 5 | 3 |
| 6 | 4 | 1 | 5 | 3 | 2 | 6 |

Then Q is an idempotent quasigroup of order 6 and type (1). (If P is a prolongation of Q, then $\mathcal{M}_l(P)=\mathcal{M}_r(P)=\mathcal{M}(P)=\mathcal{S}(P)$).

9.4. Example. Consider the following quasigroup Q:

| Q | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 4 | 5 | 6 | 2 |
| 2 | 4 | 2 | 1 | 6 | 3 | 5 |
| 3 | 5 | 6 | 3 | 1 | 2 | 4 |
| 4 | 6 | 5 | 2 | 4 | 1 | 3 |
| 5 | 2 | 4 | 6 | 3 | 5 | 1 |
| 6 | 3 | 1 | 5 | 2 | 4 | 6 |

The left translations of Q are even permutations as well as the right translation by 1. On the other hand, the remaining five right translations are odd permutations.

10. Numbers divisible by 8

10.1. Let $n\geq 2$ and let $m\geq 1$ be odd. Let $s=2^n m$, $t=2^{n-1}m$ and $G=G(+)=Z_2(+)\times Z_a(+)$. Put $A=\{(0,i);0\leq i<t\}$, $B=\{(0,i);t\leq i<s\}$, $C=\{(1,i);0\leq i<t-1\}$, $D=\{(1,i);t-1\leq i<s-1\}$ and $E=\{(1,s-1)\}$. Hence card(A)=card(B)=card(D)=t, card(C)=t-1, card(E)=1 and G is the disjoint union of these sets, $G=A\cup B\cup C\cup D\cup E$. Now, we shall define a transformation q of G as follows:

(i) $q((0,i))=(0,i)$ for every $(0,i)\in A$; hence $q|A=1_A$ and $q(A)=A$.

(ii) $q((0,i))=(1,i)$ for every $(0,i)\in B$; hence $q|B=\mathcal{L}((1,0),Q)|B$ and $q(B)=(D\cup E)-\{(1,t-1)\}$.

(iii) $q((1,i))=(1,i+1)$ for every $(1,i)\in C$; hence $q|C=\mathcal{L}((0,1),G)|C$ and $q(C)=(C\cup\{(1,t-1)\})-\{(1,0)\}$.

(iv) $q((1,i))=(0,i+1)$ for every $(1,i)\in D$; hence $q|D=\mathcal{L}((1,1),G)|D$ and $q(D)=B$.

(v) $q((1,s-1))=(1,0)$; hence $q|E=\mathcal{L}((0,1),G)|E$ and $q(E)=\{(1,0)\}$.

10.1.1. <u>Lemma.</u> q is a permutation of G and $sgn(q)=-1$.

Proof. Clearly, $q(G)=G$ and q is a permutation. On the other hand, it is easy to check that q is a cycle of length 3t, so that q is odd.

Now, put $f(x)=q(-x)$ and $g(x)=q(x)+x$ for every $x \in G$.

10.1.2. <u>Lemma.</u> Both f and g are permutations of G, (f,g) is a pair of orthogonal permutations and $sgn(f)=-1$.

Proof. First, f is a composition of q and the even permutation $x \longrightarrow -x$. Consequently, f is a permutation and $sgn(f)=-1$. Now, define four transformations of G by $h_1(x)=2x$, $h_2(x)=2x+(1,0)$, $h_3(x)=2x+(0,1)$ and $h_4(x)=2x+(1,1)$. Then $g|A=h_1|A$, $g|B=h_2|B$, $g|C=h_3|C$, $g|D=h_4|D$ and $g|E=h_3|E$. Further, $h_1(a) \neq h_1(b)$, if $a,b \in A$ (resp. B, $C \cup E$, D) and $a \neq b$, and $(1,0),(0,1),(1,1),(0,s-1),(1,s-1) \notin h_1(G)$. Using this, it is easy to see that g is injective, and therefore g is a permutation.

10.1.3. <u>Lemma.</u> $sgn(g)=-1$.

Proof. Let $<$ denote the sharp lexicographical ordering on G ($(i,j)<(k,l)$ iff either $i<k$ or $i=k$ and $j<l$). Put $M=\{(x,y);\ x,y \in G,\ x<y,\ g(x)>g(y)\}$ and $d=card(M)$. Then $sgn(g)=(-1)^d$ and $d=\sum d(U,V)$, $U,V \in \{A,B,C,D,E\}$, $d(U,V)=card((U \times V) \cap M)$. Clearly, $d(A,A)=d(A,B)=d(A,D)=d(A,E)=d(B,A)=d(B,B)=d(C,A)=d(C,B)=d(C,C)=d(C,D)=d(C,E)=d(D,A)=d(D,B)=d(D,C)=d(E,A)=d(E,B)=d(E,C)=d(E,D)=d(E,E)=0$. Further, $d(A,C)=\sum_{i=0}^{t-1} i=t(t-1)/2=2^{n-2}m(2^{n-1}m-1)$, $d(B,C)=card(B \times C)=t(t-1)=2^{n-1}m(2^{n-1}m-1)$, $d(B,D)=\sum_{i=0}^{t-1} i=t(t-1)/2=2^{n-2}m(2^{n-1}m-1)$, $d(B,E)=card(B)=t=2^{n-1}m$, $d(D,D)=t-1=2^{n-1}m-1$, $d(D,E)=card(D)=t=2^{n-1}m$. From this, $d=(s+1)t-1=(2^n m+1)2^{n-1}m-1$ is odd.

10.1.4. <u>Lemma.</u> $f^4$ is a 5-cycle.

Proof. f is composed from t-2 4-cycles of the form
((0,i) (1,s-i) (1,i+1) (0,s-i)), $1 \leq i \leq t-2$, from the 5-cycle
((0,t-1) (1,t+1) (0,t) (1,t) (0,t+1)) and from the 2-cycle
((1,0) (1,1)).

10.2. <u>Proposition.</u> Let $k \geq 3$ and let $m \geq 1$ be odd. Then there exists an orthostrophic idempotent quasigroup Q of order $2^k m$ and type (4). Moreover, $\mathcal{R}(a,Q)^4$ is a 5-cycle for any $a \in Q$.

10.3. Let $m=1$, $s=2^n$, $t=1^{n-1}$, $n \geq 2$.

10.3.1. <u>Lemma.</u> g contains the following n+2-cycle:
$((0,s-1)\dots(1,s-2^i-1)\dots(1,s-1))$, $0 \leq i \leq n-1$.

Proof. $g((1,s-1))=(1,s-2j+1)$ for any $2 \leq j \leq t+1$ and $g((0,s-1))=(1,s-2)$, $g((1,s-1))=(0,s-1)$.

Now, put $H=G-\{(1,s-1)\}$ and define a permutation h of H by $h(x)=g(x)$ for every $x \in H$, $x \neq (1,t-1)$ and $h((1,t-1))=(0,s-1)$.

10.3.2. Lemma. Let $a,a_1,\dots,a_n \in \{0,1\}$, $i=a_1 2^{n-1}+a_2 2^{n-2}+\dots+a_{n-1}2+a_n$, $0 \le i < s$. Then $h((a,i))=(a_1,2i+a)$ ($2i+a$ computed in $Z_s$).

Proof. Easy.

10.3.3. Lemma. Let $a_0,a_1,\dots,a_n \in \{0,1\}$, $i=a_1 2^{n-1}+\dots+a_{n-1}2+a_n$. For $0 \le j \le$ $\le n$, put $x_j=(a_j,2^j i+2^{j-1}a_0+2^{j-2}a_1+\dots+2a_{j-2}+a_{j-1})$. Then $x_0=(a_0,i)$ and $h(x_k)=$ $=x_{k+1}$ for any $0 \le k \le n-1$, $h(x_n)=x_0$.

Proof. Use 10.3.2.

10.3.4. Lemma. $h^{n+1}=1_H$.

Proof. This is clear from 10.3.3.

10.3.5. Lemma. $g^{n+1}$ is an $n+2$-cycle.

Proof. The result is an easy consequence of the preceding observations.

## 11. Numbers divisible by 4

11.1. Let $H=H(+)=Z_2(+)\times Z_2(+)$ and let $Q$ be a finite idempotent quasigroup of order $m \ge 3$. Put $G=H(+)\times Q$ and consider the following four 2-cycles from $\mathcal{S}(H)$: $f=((0,0)\ (0,1))$, $g=((0,1)\ (1,1))$, $h=((1,0)\ (1,1))$, $k=((0,1)(1,0))$. Define an operation $\circ$ on $H$ by $a \circ b=k(g(a)+h(b))$.

11.1.1. Lemma. $H(\circ)$ is an idempotent quasigroup and every of its translations is an even permutation.

Proof. Easy.

Put $G(\circ)=H(\circ)\times Q$ and let $t \in \mathcal{S}(Q)$ be a regular permutation (i.e. $t$ fixes no element). Now, we shall define an operation $*$ on $G$ as follows:

(i) $(a,x)*(b,y)=(a+b,xy)$ for all $a,b \in H$, $x,y \in Q$, $x \neq y \neq t(x)$.

(ii) $(a,x)*(b,x)=(a\circ b,x)$ for all $a,b \in H$ and $x \in Q$.

(iii) $(a,x)*(b,t(x))=(f(a+b),xt(x))$ for all $a,b \in H$, $x \in Q$.

11.1.2. Lemma. $G(*)$ is an idempotent quasigroup and every of its translations is an odd permutation.

Proof. From 6.1.1 and from the fact that $H$ together with the operation $(a,b) \longrightarrow f(a+b)$ is a quasigroup, it is easy to see that $G(*)$ is an idempotent quasigroup. Now, let $a \in H$ and $x \in Q$. Put $q=\mathcal{L}((a,x),G(*))$ and $p=\mathcal{L}((a,x),$ $G(\circ))$. Then $p$, $p^{-1}$ are even permutations and $\mathrm{sgn}(qp^{-1})=\mathrm{sgn}(q)$. But $qp^{-1}(\dots,y)=(\dots,y)$ for each $y \in Q$, and hence there are permutations $w_y$ of the set $H$ such that $qp^{-1}(b,y)=(w_y(b),y)$. Obviously, $\mathrm{sgn}(qp^{-1})=\prod \mathrm{sgn}(w_y)$. However, for $y \neq x,xt(x)$, $w_y=\mathcal{L}(a,H(+))\mathcal{L}(a,H(\circ))^{-1}$ and $\mathrm{sgn}(w_y)=1$. For $y=x$, $w_y=1_H$

and again $sgn(w_y)=1$. Finally, for $y=xt(x)$, $w_y=f\mathcal{L}(a,H(+))\mathcal{L}(a,H(\circ))^{-1}$ and $sgn(w_y)=sgn(f)=-1$. We have proved that the left translations of $G(*)$ are odd. In the right hand case, we can proceed similarly.

11.1.3. Lemma. Let m be odd, $Q=Z_m(\Delta)$, $x\Delta y=2x-y$. Then $\mathcal{L}((0,x),G(*))^4$ is a 3-cycle for every $x\in Q$.

Proof. Clearly, $\mathcal{L}((0,x),G(*))$ is composed from the following cycles:
$((a,y)\ (a,2x-y))$, $a\in H$, $y\in Q-\{x,t(x),2x-t(x)\}$;
$((0,x))$; $((b,x)\ (kh(b),x)\ ((kh)^2(b),x))$, $b=(0,1)$;
$((c,t(x))\ (c,2x-t(x)))$, $c=(1,0),(1,1)$;
$((0,t(x))\ (b,2x-t(x))\ (b,t(x))\ (0,2x-t(x)))$.

11.2. Corollary. Let $m\geq 3$ be odd. Then there exists an idempotent quasigroup of order 4m and type (4) such that $\mathcal{L}(a,Q)^4$ is a 3-cycle for some $a\in Q$.

## References


[1] J. DÉNES, A.D. KEEDWELL: Latin squares and their applications, Akadémiai Kiadó, Budapest, 1974.

[2] A. DRÁPAL, T. KEPKA: Parity of orthogonal automorphisms, Comment. Math. Univ. Carolinae 28(1987), 251-259.



Matematicko-fyzikální fakulta, Univerzita Karlova, Sokolovská 83,
18600 Praha 8, Czechoslovakia



(Oblatum 7.4. 1987)