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](http://dml.cz/dmlcz/106555)

Terms of use:

© Charles University in Prague, Faculty of Mathematics and Physics, 1987

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project DML-CZ: The Czech Digital Mathematics Library [http://project.dml.cz](http://project.dml.cz)
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 \( G=\mathbb{Z}_{15}(+) \). Consider the following two 14-cycles \( f \) and \( g \):
\[
\begin{align*}
  f &= (1 \ 13 \ 3 \ 11 \ 5 \ 9 \ 7 \ 8 \ 10 \ 6 \ 12 \ 4 \ 14 \ 2), \\
  g &= (1 \ 3 \ 7 \ 2 \ 5 \ 11 \ 10 \ 4 \ 9 \ 6 \ 13 \ 14 \ 12 \ 8).
\end{align*}
\]

It is easy to check that \((f,g)\) is a pair of orthogonal permutations of \( G \) and that \( \text{sgn}(g) = -1 = \text{sgn}(f) \).

7.1. Proposition. \( O'(G,f) \) 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.
Every translation is a 3-cycle.

8.2. Proposition. 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 \( a \star b = c \) implies \( c \star b = a \) and \( c \star a = b \) for any \( a, b, c \in Q \). Without loss of generality, we can assume \( Q = \{1, 2, 3, 4, 5\} \) and \( \mathcal{D}(1, 2, 3, 4, 5) = (2 3)(4 5) \). Then \( 2 \star 3 = 1 \), and hence \( 2 \star 1 = 3 \). This implies \( \mathcal{D}(2, 3, 4, 5, 6) = (1 3)(4 5), \) a contradiction.

9. The case \( n = 6 \)

9.1. Proposition. 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 \( R = \{ x: (a, b); a \in Q \} \). For any \( f \in R, f = (a, b) \in \mathcal{D}(f) \) and the set \( \{c, d, e\} \) by \( \mathcal{D}(f) \). For \( a, b \in Q \), let \( f_{a, b} \) denote the (unique) permutation \( f \in R \) with \( f(a) = b \). Obviously, \( \{a, b\} \subseteq \mathcal{D}(f_{a, b}) \) implies \( f_{a, b} \in \mathcal{D}(f_{a, b}) \).

(a) Suppose there are \( f, g \in R, f * g \), such that \( T(f) = T(g) = T \). Put \( \mathcal{D}(f) = (D(f) \cup \mathcal{D}(g)) - (D(f) \cap \mathcal{D}(g)) \). As \( \mathcal{D}(f) \neq \mathcal{D}(g) \), we have \( \mathcal{D}(T(f) \cap \mathcal{D}(g)) \), and hence \( \mathcal{D}(D(f) \cap \mathcal{D}(g)) \). If \( h \in R, f \neq h \neq g \), then \( \mathcal{D}(T(h) \cap \mathcal{D}(f)) \), \( \mathcal{D}(T(h) \cap \mathcal{D}(g)) \), and \( \mathcal{D}(T(h) \cap \mathcal{D}(f)) \leq 1 \), and therefore \( \mathcal{D}(T(h)) \leq 1 \). This allows for only two different translations \( h \), a contradiction.

(b) The sets \( \mathcal{D}(f), f \in R \) 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) \( \deg_G(x) \geq 2 \) 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 \( a \mathcal{D}(f) \). For any \( g \in R, f * g \), we have \( a \mathcal{D}(g), T(f) \neq T(g) \) and \( \mathcal{D}(T(f) \cap \mathcal{D}(g)) \leq 1 \). Hence \( \mathcal{D}(T(g) \cap \mathcal{D}(f)) = 2 \).

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 \( b, c \neq a, d \) or \( b, d \neq a, c \). Assume the latter one. Then \( f_{b, a} \neq f_{c, b}, f_{d, a} \neq f_{b, d}, f_{c, a} \neq f_{a, d}, f_{d, c} \neq f_{a, d}, \) and \( f_{d, d} = f_{c, c} \). 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. Corollary. There is no idempotent quasigroup of order 6 and type (2) or (3) or (4).
9.3. Example. Consider the following quasigroup $Q$:

\[
\begin{array}{cccccc}
Q & 1 & 2 & 3 & 4 & 5 & 6 \\
1 & 1 & 3 & 4 & 5 & 6 & 2 \\
2 & 3 & 2 & 6 & 1 & 4 & 5 \\
3 & 6 & 5 & 3 & 2 & 1 & 4 \\
4 & 5 & 6 & 2 & 4 & 3 & 1 \\
5 & 2 & 4 & 1 & 6 & 5 & 3 \\
6 & 4 & 1 & 5 & 3 & 2 & 6 \\
\end{array}
\]

Then $Q$ is an idempotent quasigroup of order 6 and type (1). (If $P$ is a prolongation of $Q$, then $M_1(P)=M_r(P)=M(P)=\mathcal{U}(P)$).

9.4. Example. Consider the following quasigroup $Q$:

\[
\begin{array}{cccccc}
Q & 1 & 2 & 3 & 4 & 5 & 6 \\
1 & 1 & 3 & 4 & 5 & 6 & 2 \\
2 & 4 & 2 & 1 & 6 & 3 & 5 \\
3 & 5 & 6 & 3 & 1 & 2 & 4 \\
4 & 6 & 5 & 2 & 4 & 1 & 3 \\
5 & 2 & 4 & 6 & 3 & 5 & 1 \\
6 & 3 & 1 & 5 & 2 & 4 & 6 \\
\end{array}
\]

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 $G=G(+)=Z_2(+) \times Z_8(+)$. Put $A=\{(0,1); 0 < i < t\}$, $B=\{(0,1); t < i < s\}$, $C=\{(1,i); 0 < i < t-1\}$, $D=\{(1,i); t-1 < i < s-1\}$ and $E=\{(1,s-1)\}$. Hence $\text{card}(A)=\text{card}(B)=\text{card}(D)=t$, $\text{card}(C)=t-1$, $\text{card}(E)=1$ 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) $q((0,1))=(0,1)$ for every $(0,1) \in A$; hence $q|A=1_A$ and $q(A)=A$.

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

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

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

(v) $q((1,s-1))=(1,0)$; hence $q|E=\mathscr{E}((0,1), G)|E$ and $q(E)=\{(1,0)\}$. 
- 429 -
10.1.1. **Lemma.** 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 ∈ G.

10.1.2. **Lemma.** 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→ -x. Consequently, f is a permutation and sgn(f)= -1. Now, define four transformations of G by h₁(x)=2x, h₂(x)=2x+(1,0), h₃(x)=2x+(1,1) and h₄(x)=2x+(1,1). Then g|A=h₁|A, g|B=h₂|B, g|C=h₃|C, g|D=h₄|D and g|E=h₃|E. Further, h₄(a) ≠ h₁(b), if a,b ∈ A (resp. B, C∪E, D) and a ≠ b, and (1,0),(1,1), (0,s-1),(1,s-1)∈ h₁(G). Using this, it is easy to see that g is injective, and therefore g is a permutation.

10.1.3. **Lemma.** 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= i(x,y); x,y ∈ G, x < y, g(x) > g(y)} and d=card(M). Then sgn(g)=(-1)^d and d=Σ d(U,V), U,V∈ {A,B,C,D,E}, d(U,V)=card((U×V)∩ 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(D,D)=d(D,E)=d(E,A)=d(E,B)= d(E,C)=d(E,D)=d(E,E)=0. Further, d(A,C)=x=1 i=1 t(t-1)/2=2^n-2m(2^n-1-1), d(B,C)=card(B×C)=t(t-1)=2^n-1m(2^n-1-1), d(B,D)=t=2^n-1m, d(D,D)=t(t-1)=2^n-1m-1, d(D,E)=card(D)=t=2^n-1m. From this, d=(s+1)t-1=(2^n+1)2^n-1m-1 is odd.

10.1.4. **Lemma.** f^4 is a 5-cycle.

Proof. f is composed from t-2 4-cycles of the form

((0,1) (1,s-1) (1,i+1) (0,s-1)), 1 ≤ i ≤ t-2, from the 5-cycle

((0,1) (1,i+1) (0,t) (1,t) (0,t+1)) and from the 2-cycle

((1,0) (1,1)).

10.2. **Proposition.** Let k≥3 and let m≥1 be odd. Then there exists an orthostrophic idempotent quasigroup Q of order 2^km and type (4). Moreover, R(a,q)^4 is a 5-cycle for any a ∈ Q.

10.3. Let m=1, s=2^n, t=1^n-1, n ≥ 2.

10.3.1. **Lemma.** g contains the following n+2-cycle:

((0,s-1)...(1,s-2^n-1)...(1,s-1)), 0 ≤ i ≤ n-1.

Proof. g(1,s-1)=(1,s-2^n+1) for any 2 ≤ j ≤ 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 x ∈ H.
every $x \in H$, $x \neq (1, t-1)$ and $h((1, t-1)) = (0, s-1)$.

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

10.3.3. **Lemma.** Let $a_0, a_1, \ldots, a_n \in \{0, 1\}$, $i = a_1 2^{n-1} + \cdots + a_{n-1} 2 + a_n$. For $0 \leq j \leq n$, put $x_j = (a_0, 2^j 2^j - a_1 2^{j-1} - a_2 2^{j-2} - \cdots - a_{j-1} 2 + a_j)$. Then $x_0 = (a_0, 1)$ and $h(x_k) = x_{k+1}$ for any $0 \leq k < n - 1$, $h(x_n) = x_0$.
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 $m \geq 3$. Put $G = H(+) \times Q$ and consider the following four 2-cycles from $\mathcal{G}(H)$: $f = ((0, 0) (0, 1)), g = ((0, 1) (1, 1)), h = ((1, 0) (1, 1)), k = ((0, 1)(1, 0))$. 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 $t \in \mathcal{G}(Q)$ be a regular permutation (i.e. $t$ fixes no element). Now, we shall define an operation $\ast$ on $G$ as follows:
(i) $(a, x) \ast (b, y) = (a \circ b, xy)$ for all $a, b \in H$, $x, y \in Q$, $x \neq y \neq t(x)$.
(ii) $(a, x) \ast (b, x) = (a \circ b, x)$ for all $a, b \in H$ and $x \in Q$.
(iii) $(a, x) \ast (b, t(x)) = (f(a \circ b), xt(x))$ for all $a, b \in H$, $x \in Q$.

11.1.2. **Lemma.** $G(\ast)$ 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 $(a, b) \mapsto f(a \circ b)$ is a quasigroup, it is easy to see that $G(\ast)$ is an idempotent quasigroup. Now, let $a \in H$ and $x \in Q$. Put $q = \mathcal{L}((a, x), G(\ast))$ and $p = \mathcal{L}((a, x), G(\circ))$. Then $p, p^{-1}$ are even permutations and $\text{sgn}(q p^{-1}) = \text{sgn}(q)$. But $q^{-1}(\ldots, y) = (\ldots, y)$ for each $y \in Q$, and hence there are permutations $\omega_y$ of the set $H$ such that $q^{-1}(b, y) = (\omega_y(b), y)$. Obviously, $\text{sgn}(q p^{-1}) = \prod y \text{sgn}(\omega_y)$. However, for $y \neq x, xt(x)$, $\omega_y = \mathcal{L}(a, H(\circ)) \mathcal{L}(a, H(\circ))^{-1}$ and $\text{sgn}(\omega_y) = 1$. For $y = x$, $\omega_y = 1_H$. 

- 431 -
and again $\text{sgn}(w_y) = 1$. Finally, for $y = xt(x)$, $w_y = f^L(a,H(+))L(a,H(*)^{-1}$ and $\text{sgn}(w_y) = \text{sgn}(f) = -1$. We have proved that the left translations of $G(\ast)$ are odd. In the right hand case, we can proceed similarly.

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

**Proof.** Clearly, $L((0,x),G(\ast))$ is composed from the following cycles:

- $((e,y)(a,2x-y))$, $a \in H$, $y \in Q - \{ x, t(x), 2x-t(x) \}$;
- $((0,x))$;
- $((b,x)(kh(b),x)((kh)^2(b),x))$, $b = (0,1)$;
- $((c,t(x))(c,2x-t(x)))$, $c = (1,0),(1,1)$;
- $((0,t(x))(b,2x-t(x))(b,t(x))(0,2x-t(x)))$.

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

**References**


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

(Oblatum 7.4. 1987)