Quasigroups and Related Systems **28** (2020), 53 – 76

Translatability determines the structure of certain types of idempotent quasigroups

Wieslaw A. Dudek and *Robert A. R. Monzo*

Abstract. We prove that in certain types of k-translatable idempotent quasigroups, the value of k determines all possible orders of k-translatable idempotent quasigroups of a particular type. From this, all k-translatable idempotent quesigroups of that type can be calculated, as well as their parastrophe types. Four operators on the collection of all idempotent, translatable quasigroups are defined and formulae determining relationships amongst them are given. Necessary and sufficient conditions are given for particular types of idempotent, translatable quasigroups to be perpendicular to their dual quasigroup.

1. Introduction

The notion of a k-translatable groupoid was an outcrop of the observation that certain quadratical quasigroups are translatable [6]. This led to the determination of the structure of idempotent, translatable quasigroups in general and of types of idempotent, translatable quasigroups in particular (Theorems 4.2 and 4.27 [5]). These results and Theorem 4.2 [7] inspired the work in this paper.

To say that an idempotent quasigroup $(Q, \cdot)$ of order n is k-translatable is a powerful statement. It implies that $x \cdot y = [ax + by]_n$ for some $a \in \{2, 3, \ldots, n\}$ and odd $n > 1$, where $[a + b]_n = 1$, $[a + kb]_n = 0$ and $[t]_n$ equals t calculated modulo n (cf. [5]). In addition, the greatest common divisor of a and n is 1, as is that of b and n and k and n. Also, there exist unique values a', b' and k' such that $[aa']_n = [bb']_n = [kk']_n = 1$, where k' is the value of the translatability of the dual quasigroup $(Q, *)$ and $x * y = [bx + ay]_n$. Therefore, $[b + k'a]_n = 0$. The products of the parastrophes of $(Q, \cdot)$ and their translatability can also be determined (cf. [5]). We note that idempotent k-translatable quasigroups are medial, that is they satisfy the identity $xy \cdot zw = xz \cdot yw$, and therefore they are what is called in the literature IM-quasigroups (cf. [9]). We denote the collection of all idempotent, medial quasigroups as **IMQ**. We define **IKQ** as the collection of all idempotent, k-translatable quasigroups. By Corollary 4.5 [5], **IKQ** $\subset$ **IMQ**.

To simplify the size of some of the tables we will sometimes let (a, b) denote the idempotent k-translatable quasigroup $x \cdot y = [ax + by]_n$, where $[a + b]_n = 1$. For

2020 Mathematics Subject Classification: 20N02; 20N05
Keywords: Quasigroup; pentagonal quasigroup; translatability; idempotent.

example, $(3,3)$ denotes the idempotent 4-translatable quasigroup $x \cdot y = [3x+3y]_5$, and $(2,10)$ denotes the idempotent 2-translatable quasigroup $x \cdot y = [2x+10y]_{11}$.

In this paper we examine certain types of idempotent k-translatable quasigroups. Each type $\mathbf{T}$ in Table 3.1 satisfies a single identity $u_T = v_T$, with $u_T = u_T(x,y)$ and $v_T = v_T(x,y)$. Each identity yields a function $F_T(a)$ such that $[F_T(a)]_n = 0$. This formula allows us to calculate the possible values of n; that is, for each value of a, the formula determines the possible orders of the members of $\mathbf{T}$. Also, the value of a' and k' are determined by the value of k.

The function H_T denotes the function $H_T = H_T(k)$, where $[H_T(k)]_n = 0$. The products of the parastrophes of a given $(Q,\cdot) \in \mathbf{T}$ and the value of their translatability can also be determined by k, the value of the translatability of $(Q,\cdot)$. Also, in any type $\mathbf{T}$ we can calculate all k-translatable quasigroup members of $\mathbf{T}$, for any value of k. We give tables of such quasigroup members for each type $\mathbf{T}$ and each value of k, for $k \in \{2,3,\ldots,10\}$. The main results are given in Tables 3.1, 3.2, 3.3 and 3.4, from which most other results and tables follow.

We examine, for each $\mathbf{T}$, the dual collection $\mathbf{T}^*$ and the inverse collection $-\mathbf{T}$ and prove that the above analysis also applies to these collections of quasigroups. Some interrelationships between different types of idempotent k-translatable quasigroups, their dual collections, their inverse collections and the collections $\mathbf{T}^{+1}$ and $\mathbf{T}^{-1}$ are also given.

We will show how these results link with the work of Belousov. He proved that any minimal non-trivial identity in a quasigroup is parastrophically equivalent to one of seven identity types [1]. We prove that five of those identities determine types of idempotent k-translatable quasigroups and that the remaining two identities do not. We prove in Corollary 6.4 that if $\mathbf{T}$ is the collection of quadratical quasigroups or the collection of affine regular octagonal quasigroups, then any quasigroup member of $\mathbf{T}$ is perpendicular to its dual quasigroup.

2. Preliminary definitions, examples and results

A *groupoid* (in other terminology: a *magma*) is a non-empty set Q with a binary operation (called a *multiplication*) defined on Q and denoted by dot or juxtaposition. For clarity of record we will limit the number of parentheses. Instead of $(x \cdot y) \cdot z$, we will write $xy \cdot z$.

Let us recall that a groupoid $(,\cdot)$ is a *quasigroup* if for every $a,b \in Q$ there exist unique elements $x,y \in Q$ such that $ax = b$ and $ya = b$. An element x of a groupoid $(Q,\cdot)$ is idempotent if $x \cdot x = x$. A finite groupoid $Q = \{1,2,\ldots,n\}$ is called *k-translatable*, where $1 \leqslant k < n$, if the second row of its multiplication table is obtained from the first row by inserting the last k entries of the first row into the first k entries of the second row and the first $n-k$ entries of the first row into the last $n-k$ entries of the second row. This operation is repeated from the second row, to obtain the entries of the third row, and so on until the table is filled (cf. [5]).

The following are the Cayley tables of a 2-translatable idempotent quasigroup of order 3, a 3-translatable idempotent quasigroup of order 5 and a 4-translatable idempotent quasigroup of order 7.

	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

	1	2	3	4	5
1	1	3	5	2	4
2	5	2	4	1	3
3	4	1	3	5	2
4	3	5	2	4	1
5	2	4	1	3	5

	1	2	3	4	5	6	7
1	1	3	5	7	2	4	6
2	7	2	4	6	1	3	5
3	6	1	3	5	7	2	4
4	5	7	2	4	6	1	3
5	4	6	1	3	5	7	2
6	3	5	7	2	4	6	1
7	2	4	6	1	3	5	7

It is known that an idempotent k-translatable quasigroup of order n is induced by the additive group of integers modulo n, where, for simplicity of our calculations, 0 is identified with n, i.e., instead of $Q = \{0, 1, \dots, n-1\}$ we consider the set $Q = \{1, 2, \dots, n\}$. In this convention, an idempotent k-translatable quasigroup of order n has the form

$$x \cdot y = [ax + (1-a)y]_n, \quad \text{where} \quad [a + k(1-a)]_n = 0$$

and the greatest common divisor of k and n is 1. Obviously, the greatest common divisor of a and n (also $a-1$ and n) must be 1. The value n must be odd and greater than or equal to 3, while $k \geqslant 2$ (cf. [5, Lemma 4.1]).

It follows that idempotent k-translatable quasigroups satisfy particular identity types if and only if $[F_T(a)]_n = 0$ for some function $F_T(a)$ that is determined by the identity that defines the type T.

The identity types here explored determine well-known types of quasigroups, such as *quadratical* ($\mathbf{Q}$: $xy \cdot x = zx \cdot yz$), *hexagonal* ($\mathbf{H}$: $xy \cdot x = y$), *golden square* ($\mathbf{GS}$: $(xy \cdot z) \cdot z = y$), *right modular* ($\mathbf{RM}$: $xy \cdot z = zy \cdot x$) and *left modular* ($\mathbf{LM}$: $x \cdot yz = z \cdot yx$), *affine regular octagonal* ($\mathbf{ARO}$: $xy \cdot y = yx \cdot x$) and *pentagonal* ($\mathbf{P}$: $(xy \cdot x)y \cdot x = y$). In addition we examine the identities $(yx \cdot x)x = y$ (denoted as $\mathbf{C3}$) and $x(y \cdot yx) = y$ (denoted as $\mathbf{U}$).

For a given collection $\mathbf{T}$ of idempotent k-translatable quasigroups we define the following collection of quasigroups

$$\begin{aligned}
\mathbf{T}^* &= \{(1-a, a) \in \mathbf{IMQ}\} \mid (a, 1-a) \in \mathbf{T}\},\\
-\mathbf{T} &= \{(-a, 1+a) \in \mathbf{IMQ} \mid (a, 1-a) \in \mathbf{T}\},\\
\mathbf{T}^{+\mathbf{t}} &= \{(a+t, 1-a-t) \in \mathbf{IMQ} \mid (a, 1-a) \in \mathbf{T}\},\\
\mathbf{T}^{-\mathbf{t}} &= \{(a-t, 1+t-a) \in \mathbf{IMQ} \mid (a, 1-a) \in \mathbf{T}\},
\end{aligned}$$

where $t \in \{1, 2, \dots\}$.

These two theorems, that are a modification of Theorems 4.26 and 4.27 from [5], will be used later.

Theorem 2.1. *A k-translatable, naturally ordered quasigroup $(Q,\cdot)$ of order n with the multiplication defined by $x \cdot y = [ax + (1-a)y]_n$, where $a \in \mathbb{Z}_n$ and $[a+(1-a)k]_n = 0$ is*

(1) *quadratical if and only if $[2a^2 - 2a + 1]_n = 0$,*

(2) *hexagonal if and only if $[a^2 - a + 1]_n = 0$,*

(3) *GS-quasigroup if and only if $[a^2 - a - 1]_n = 0$,*

(4) *right modular quasigroup if and only if $[a^2 + a - 1]_n = 0$,*

(5) *left modular quasigroup if and only if $[a^2 - 3a + 1]_n = 0$,*

(6) *ARO-quasigroup if and only if $[2a^2]_n = 1$,*

(7) *$C3$ quasigroup if and only if $[a^3]_n = 1$.*

Theorem 2.2. *A naturally ordered quasigroup $(Q,\cdot)$ of order n with the multiplication defined by $x \cdot y = [ax + (1-a)y]_n$, where $a \in \mathbb{Z}_n$ and $[a+(1-a)k]_n = 0$ is a k-translatable*

(1) *quadratical quasigroup if and only if $k = [1 - 2a]_n$,*

(2) *hexagonal quasigroup if and only if $k = [1 - a]_n$,*

(3) *GS-quasigroup if and only if $k = [a + 1]_n$,*

(4) *right modular quasigroup if and only if $k = [-1 - a]_n$,*

(5) *left modular quasigroup if and only if $k = [a - 1]_n$,*

(6) *ARO-quasigroup if and only if $k = [-1 - 2a]_n$,*

(7) *$C3$ quasigroup if and only if $[(1 - a^2)k]_n = 1$.*

We will also need the following characterization of a pentagonal quasigroup proved in [7].

Theorem 2.3. *A groupoid $(Q,\cdot)$ of order $n > 2$ is a pentagonal quasigroup induced by the group $\mathbb{Z}_n$ if and only if $x \cdot y = [ax + (1-a)y]_n$ and $[a^4 - a^3 + a^2 - a + 1]_n = 0$ for some $a \in \mathbb{Z}_n$ such that a and n, also $a - 1$ and n, are relatively prime. Such a quasigroup is k-translatable for $k = [1 - a - a^3]_n$.*

3. The main theorem

In this section we find identities amongst various types of idempotent, k-translatable quasigroup types $\mathbf{T}$ and their dual and inverse collections $\mathbf{T}^*$ and $-\mathbf{T}$. We then find the values of $H_T(k)$, a, a' and k' as functions of k.

Theorem 3.1. *The following identities between classes of idempotent quasigroups induced by the additive groups* $\mathbb{Z}_n$ *are valid:*

(1) $\mathbf{Q} = \mathbf{Q}^*$,

(2) $\mathbf{H} = \mathbf{H}^* = -\mathbf{C3}$,

(3) $\mathbf{GS} = \mathbf{GS}^* = -\mathbf{RM}$,

(4) $\mathbf{RM} = -(\mathbf{GS}^*)$,

(5) $\mathbf{LM} = \mathbf{RM}^*$,

(6) $\mathbf{ARO} = -\mathbf{ARO}$,

(7) $\mathbf{C3} = -\mathbf{H} = -(\mathbf{H}^*)$.

Proof. In the proof we use Theorem 2.1.

(1): $(a, 1-a) \in \mathbf{Q} \Leftrightarrow [2a^2 - 2a + 1]_n = 0 \Leftrightarrow [2(1-a)^2 - 2(1-a) + 1]_n = 0 \Leftrightarrow$
$(1-a, a) \in \mathbf{Q} \Leftrightarrow (a, 1-a) \in \mathbf{Q}^*$.

(2): $(a, 1-a) \in \mathbf{H} \Leftrightarrow [a^2 - a + 1]_n = 0 \Leftrightarrow [(1-a)^2 - (1-a) + 1]_n = 0 \Leftrightarrow$
$(1-a, a) \in \mathbf{H} \Leftrightarrow (a, 1-a) \in \mathbf{H}^*$
and
$(a, 1-a) \in \mathbf{C3} \Leftrightarrow [a^2 + a + 1]_n = 0 \Leftrightarrow [(-a)^2 - (-a) + 1]_n = 0 \Leftrightarrow$
$(-a, a+1) \in \mathbf{H} \Leftrightarrow (a, 1-a) \in -\mathbf{H}$. So, $\mathbf{H}^* = \mathbf{H} = -(-\mathbf{H}) = -\mathbf{C3}$.

(3): $\mathbf{GS} = \mathbf{GS}^* = -\mathbf{RM}$ and $\mathbf{RM} = -\mathbf{GS}$.
$(a, 1-a) \in \mathbf{GS} \Leftrightarrow [a^2 - a - 1]_n = 0 \Leftrightarrow [(1-a)^2 - (1-a) - 1]_n = 0 \Leftrightarrow$
$(1-a, a) \in \mathbf{GS} \Leftrightarrow (a, 1-a) \in \mathbf{GS}^*$

(4): $(a, 1-a) \in \mathbf{RM} \Leftrightarrow [a^2 + a - 1]_n = 0 \Leftrightarrow [(-a)^2 - (-a) - 1]_n = 0 \Leftrightarrow$
$(-a, a+1) \in \mathbf{GS} \Leftrightarrow (a, 1-a) \in -\mathbf{GS}$. So, $-\mathbf{RM} = -(-\mathbf{GS}) = \mathbf{GS}$.

(5): $\mathbf{RM} = \mathbf{LM}^*$ and $\mathbf{LM} = \mathbf{RM}^*$.
$(a, 1-a) \in \mathbf{RM} \Leftrightarrow [a^2 + a - 1]_n = 0 \Leftrightarrow [(1-a)^2 - 3(1-a) + 1]_n = 0 \Leftrightarrow$
$(1-a, a) \in \mathbf{LM} \Leftrightarrow (a, 1-a) \in \mathbf{LM}^*$.

(6): $(a, 1-a) \in \mathbf{ARO} \Leftrightarrow [2a^2 - 1]_n = 0 \Leftrightarrow [2(-a)^2 - 1]_n = 0 \Leftrightarrow$
$(-a, a+1) \in \mathbf{ARO} \Leftrightarrow (a, 1-a) \in -\mathbf{ARO}$.

(7) is a consequence of the above facts. □

Theorem 3.2. *If* **T** *is any one of the following types:* **Q**, **H**, **GS**, **RM**, **LM**, **ARO**, **ARO***, **C3**, **C3***, **P**, **P***, **U**, **U***, −**LM**, −(**C3***), −**U**, −(**U***), −(**ARO***), −**P** *or* −(**P***), *then the values of* $F_T(a)$, $H_T(k)$, k, a, a' *and* k' *are as indicated in the tables below, where all entries are calculated modulo* n.

Table 3.1.

T	$F_T(a)$	k	$H_T(k)$
Q	$2a^2-2a+1$	$1-2a$	k^2+1
H	a^2-a+1	$1-a$	k^2-k+1
GS	a^2-a-1	$a+1$	k^2-3k+1
RM	a^2+a-1	$-1-a$	k^2+k-1
LM	a^2-3a+1	$a-1$	k^2-k-1
ARO	$2a^2-1$	$-1-2a$	k^2+2k-1
ARO*	$2a^2-4a+1$	$2a-1$	k^2-2k-1
C3	a^2+a+1	$ta-t$	$3k^2-3k+1$
C3*	a^2-3a+3	$3-a$	k^2-3k+3
P	$a^4-a^3+a^2-a+1$	$1-a^3-a$	$k^4-2k^3+4k^2-3k+1$
P*	$a^4-3a^3+4a^2-2a+1$	$1-a^3+2a^2-2a$	$k^4-3k^3+4k^2-2k+1$
U	a^3-3a^2+2a-1	a^2-2a+1	k^3-2k^2+k-1
U*	a^3-a+1	$1-a^2-a$	k^3-k^2+2k-1

Table 3.2.

T	a	a'	k'
Q	$2a=1-k$	$k+1$	$-k$
H	$1-k$	k	$1-k$
GS	$k-1$	$k-2$	$3-k$
RM	$-1-k$	$-k$	$k+1$
LM	$k+1$	$2-k$	$k-1$
ARO	$2a=-1-k$	$-k-1$	$k+2$
ARO*	$2a=k+1$	$3-k$	$k-2$
C3	$1-3k$	$3k-2$	$3-3k$
C3*	$3-k$	$-tk$	$tk+1$
P	$-k^3+k^2-3k+1$	k^3-2k^2+4k-2	$-k^3+2k^2-4k+3$
P*	$-k^3+2k^2-2k+1$	k^3-3k^2+4k-1	$-k^3+3k^2-4k+2$
U	k^3-k^2	$2k-k^2$	k^2-2k+1
U*	$-1-k^2$	$-k^2+k-1$	k^2-k+2

Table 3.3.

T	$F_T(a)$	k	$H_T(k)$
$-$**LM**	a^2+3a+1	$5k=1-a$	$5k^2-5k+1$
$-$(**C3***)	a^2+3a+3	$7k=3-a$	$7k^2-9k+3$
$-$**U**	a^3+3a^2+2a+1	$7k=-a^2-4a+1$	$7k^3-10k^2+5k-1$
$-$(**U***)	a^3-a-1	a^2+a+1	k^3-5k^2+4k-1
$-$(**ARO***)	$2a^2+4a+1$	$7k=1-2a$	$7k^2-6k+1$
$-$**P**	$a^4+a^3+a^2+a+1$	$5k=a^4-a^2-2a+2$	$5k^4-10k^3+10k^2-5k+1$
$-$(**P***)	$a^4+3a^3+4a^2+2a+1$	$11k=-a^3-4a^2-8a+1$	$11k^4-21k^3+16k^2-6k+1$

Table 3.4.

T	a	a'	k'
$-$**LM**	$1-5k$	$5k-4$	$5-5k$
$-$(**C3***)	$3-7k$	$3a'=7k-6$	$3k'=9-7k$
$-$**U**	$-7k^2+3k-1$	$-7k^2+10k-4$	$7k^2-10k+5$
$-$(**U***)	k^2-4k+1	$-k^2+5k-3$	k^2-5k+4
$-$(**ARO***)	$2a=1-7k$	$7k-5$	$6-7k$
$-$**P**	$-5k^3+5k^2-5k+1$	$5k^3-10k^2+10k-4$	$-5k^3+10k^2-10k+5$
$-$(**P***)	$-11k^3+10k^2-6k+1$	$11k^3-21k^2+16k-5$	$-11k^3+21k^2-16k+6$

Proof. The values of k listed in Table 3.1, column 3, can be checked using the fact that $[a+k(1-a)]_n=0$. In the case of **P**, $[a+(1-a-a^3)(1-a)]_n = [a^4-a^3+a^2-a+1]_n=0$. Note that $C3$ quasigroups have order $n=3t+1$ (cf. [2]) and so $[2t]_n=[-1-t]_n$. Therefore, $[a+(ta-t)(1-a)]_n=[-ta^2+2ta-t+a]_n = [-t(a^2+a+1)]_n=0$, which proves that $k=[ta-t]_n$ in $C3$ quasigroups with order $n=3t+1$.

Once the values of k in Table 3.1 have been verified, these can be used to check the values of a, listed in Table 3.2, as a function of k, using also the value of $F_T(a)$. For example, in the case of **P*** since $k=[1-a^3+2a^2-2a]_n$, using the fact that $[a^4-3a^3+4a^2-2a+1]_n=0$ it follows that $k^2=[-a^3+a^2-a]_n$ and $k^3=[-2a^2+a-1]_n$. Then, we get $[-k^3+2k^2-2k+1]_n = [(2a^2-a+1)+(-2a^3+2a^2-2a)+(-2+2a^3-4a^2+4a)+1]_n = a$. Similarly, for **U** we can calculate that $k^2=[a^2-a]_n$ and $k^3=[a^2]_n$. Hence, $a=[k^3-k^2]_n$. Using these values of a as a function of k, substituting them into the formula $0=[F_T(a)]_n$ gives the value of $H_T(k)$ listed in column 3 of Table 3.1. Alternatively, we can substitute the value of a as a function of k into the formula $[a+k(1-a)]_n=0$. So, with **P** for example, $[a+k(1-a)]_n=0$ and $a=[-k^3+k^2-3k+1]$. Therefore, $0=[-k^3+k^2-3k+1+k(k^3-k^2+3k)]_n=[k^4-2k^3+4k^2-3k+1]_n$.

The listings of the values of a' in Table 3.2 can be checked using the fact that $[ka]_n = [k+a]_n$. For example, in $\mathbf{Q}$, $[2a^2-2a+1]_n = 0$ and $k = [1-2a]_n$. Then $[a(k+1)]_n = [(1-2a)+2a]_n = 1$ and so $a' = k+1$. In the case of $\mathbf{C3}^*$, $[(-tk)a]_n = [-t(k+a)]_n = [-t((3-a)+a)]_n = [-3t]_n = 1$ and so $a' = [-tk]_n$ in a $\mathbf{C3}^*$ quasigroup of order $n = 3t+1$.

The values of k' in Table 3.2 follow from the fact that $k' = [1-a']_n$, which in turn follows from the fact that $0 = [b+k'a]_n = [k'a+(1-a)]_n = [k'+(1-a)a']_n$.

$-\mathbf{LM}$: If $(a, 1-a) \in -\mathbf{LM}$, then $(-a, a+1) \in \mathbf{LM}$ and, by Theorem 2.1, $0 = [(-a)^2-3(-a)+1]_n = [a^2+3a+1]_n$. Now $1 = [a(-a-3)]_n$ and so, $a' = [-a-3]_n$. But $k' = [1-a']_n = [a+4]_n$. Then, $1 = [kk']_n = [k(a+4)]_n = [5k+a]_n$ and so, $[5k]_n = [1-a]_n$ and $a = [1-5k]_n$. Therefore, $a' = [-a-3]_n = [5k-4]_n$ and $k' = [a+4]_n = [5-5k]_n$. Finally, $1 = [kk']_n = [5k-5k^2]_n$ and so, $0 = [5k^2-5k+1]_n$.

$-(\mathbf{C3}^*)$: If $(a, 1-a) \in -(\mathbf{C3}^*)$, then $(-a, 1+a) \in \mathbf{C3}^*$ and, by Theorem 2.1, $0 = [(-a)^3-3(-a)+3]_n = [a^2+3a+3]_n$. But $k = [a(k-1)]_n$ and so, $0 = [(k-1)a^2+3(k-1)a+3(k-1)]_n$ which, using the fact that $[ka]_n = [k+a]_n$, implies $0 = [7k+a-3]_n$. Therefore, $[7k]_n = [3-a]_n$ and $a = [3-7k]_n$. Now, $1 = [kk']_n = [a(k-1)k']_n = [(3-7k)(k-1)k']_n = [10-7k-3k']_n$ and so $[3k']_n = [9-7k]_n$. The last gives $3 = [9k-7k^2]_n$ and so, $0 = [7k^2-9k+3]_n$. Moreover, $k' = [1-a']_n$ implies $[3k']_n = [3-3a']_n$ and $[3a']_n = [3-3k']_n = [7k-6]_n$.

$-\mathbf{U}$: If $(a, 1-a) \in -\mathbf{U}$, then $(-a, a+1) \in \mathbf{U}$ and, according to Table 3.1, $0 = [(-a)^3-3(-a)+2(-a)-1]_n = [a^3+3a^2+2a+1]_n$. Using this fact and the fact that $k = [a(k-1)]_n$, the identity $0 = [(k-1)^3(a^3+3a^2+2a+1)]_n$ implies $0 = [7k^3-10k^2+5k-1]_n$. Then, $1 = [7k^3-10k^2+5k]_n = [k(7k^2-10k+5)]_n$ implies $k' = [7k^2-10k+5]_n$. Consequently, $a' = [1-k']_n = [-7k^2+10k-4]_n$.

Using the fact that $[ka]_n = [k+a]_n$, the identity $0 = [k(a^3+3a^2+2a+1)]_n$ implies $[7k]_n = [-a^2-4a+1]_n$. Also, since $1 = [7k+a^2+4a]_n$, $a' = [7ka'+a+4]_n$ we obtain $a = [a'-4-7ka']_n = [(-7k^2+10k-4)-4-7k(-7k^2+10k-4)]_n = [49k^3-77k^2+38k-8]_n = [7(7k^3-10k^2+5k-1)+(-7k^2+3k-1)]_n$. Thus, $a = [-7k^2+3k-1]_n$.

$-(\mathbf{U}^*)$: If $(a, 1-a) \in -(\mathbf{U}^*)$, then $(-a, 1+a) \in \mathbf{U}^*$. Hence, by Table 3.1, $0 = [(-a)^3-(-a)+1]_n = [a^3-a-1]_n$. Then, $[a+(a^2+a+1)(1-a)]_n = [-a^3+a+1]_n = 0$ implies $k = [a^2+a+1]_n$. But $k = [a(k-1)]_n$, so $[(k-1)k]_n = [(k-1)(a^2+a+1)]_n = [3k+a-1]_n$. Hence, $a = [k^2-4k+1]_n$. Also, $k = [a(k-1)]_n = [(k^2-4k+1)(k-1)]_n = [k^3-5k^2+5k-1]_n$ and so, $[k^3-5k+4k-1]_n = 0$. Then, $[k(k^2-5k+4)]_n = 1$. Thus, $k' = [k^2-5k+4]_n$ and $a' = [1-k']_n = [-k^2+5k-3]_n$.

$-(\mathbf{ARO}^*)$: If $(a, 1-a) \in -(\mathbf{ARO}^*)$, then $(-a, 1+a) \in \mathbf{ARO}^*$ and, by Table 3.1, $0 = [2(-a)^2-4(-a)+1]_n = [2a^2+4a+1]_n$. Since $k = [a(k-1)]_n$ we also have $0 = [(k-1)^2(2a^2+4a+1)]_n = [7k^2-6k+1]_n$. So, $1 = [6k-7k^2]_n = [k(6-7k)]_n$ and therefore, $k' = [6-7k]_n$ and $a' = [7k-5]_n$. Now, $0 = [k(2a^2+4a+1)]_n$ together with $[ka]_n = [k+a]_n$ imply $0 = [2a+7k-1]_n$. So, $[2a]_n = [1-7k]_n$ and $[7k]_n = [1-2a]_n$.

$-\mathbf{P}$: If $(a, 1-a) \in -\mathbf{P}$, then $(-a, 1+a) \in \mathbf{P}$. Hence, by Table 3.1, we have $0 = [(-a)^4 - (-a)^3 + (-a)^2 - (-a) + 1]_n = [a^4 + a^3 + a^2 + a + 1]_n$. Using the fact that $[ka]_n = [k+a]_n$, the identity $0 = [k(a^4 + a^3 + a^2 + a + 1)]_n$ implies $0 = [5k + a^3 + 2a^2 + 3a - 1]_n$. Applying $k = [a(k-1)]_n$ to the identity $0 = [(k-1)^4(a^4+a^3+a^2+a+1)]_n$ we obtain $0 = [5k^4 - 10k^3 + 10k^2 - 5k + 1]_n$. Thus, $1 = [k(-5k^3 + 10k^2 - 10k + 5)]_n$. Consequently, $k' = [-5k^3 + 10k^2 - 10k + 5]_n$ and $a' = [5k^3 - 10k^2 + 10k - 4]_n$. Now, from $[(-5k^3 + 5k^2 - 5k + 1)a']_n = [-25k^6 + 75k^5 - 125k^4 + 125k^3 - 80k^2 + 30k - 4]_n = [-5k^2(5k^4 - 10k^3 + 10k^2 - 5k+1) + 5k(5k^4 - 10k^3 + 10k^2 - 5k + 1) - 5(5k^4 - 10k^3 + 10k^2 - 5k + 1) + 1]_n = 1$ we conclude that $a = [-5k^3 + 5k^2 - 5k + 1]_n$.

$-(\mathbf{P}^*)$: If $(a, 1-a) \in -(\mathbf{P}^*)$, then $(-a, 1+a) \in \mathbf{P}^*$. Hence, by Table 3.1, we have $0 = [(-a)^4 - 3(-a)^3 + 4(-a)^2 - 2(-a) + 1]_n = [a^4 + 3a^3 + 4a^2 + 2a + 1]_n$. Using the fact that $[ka]_n = [k+a]_n$, the identity $0 = [k(a^4+3a^3+4a^2+2a+1)]_n$ implies $0 = [11k+a^3+4a^2+8a-1]_n$. Then, using the fact that $k = [a(k-1)]_n$, the identisty $0 = [(k-1)^4(a^4+3a^3+4a^2+2a+1)]_n$ implies $0 = [11k^4 - 21k^3 + 16k^2 - 6k + 1]_n$. This means that $1 = [-11k^3+21k^2-16k+6]_n$. So, $k' = [-11k^4 - 21k^3 + 16k^2 + 6]_n$ and $a' = [11k^3 - 21k^2 + 16k - 5]_n$. Finally, using $0 = [11k^4 - 21k^3 + 16k^2 - 6k + 1]_n$, we can calculate that $[aa']_n = 1$ for $a = [-11k^3 + 10k^2 - 6k + 1]_n$.

This completes the proof of Theorem 3.2 □

Theorem 3.3. *Let $(Q, \cdot)$ be an idempotent k-translatable quasigroup of order n. If m divides n, then $(Q, \cdot)$ has an idempotent k'-translatable subquasigroup of order m, where $k' = [k]_m$.*

Proof. An idempotent k-translatable quasigroup $(Q, \cdot)$ of order n is induced by the group $\mathbb{Z}_n$ and its automorphism $\varphi(x) = [ax]_n$, where a and n are relatively prime. If m divides n, then $\mathbb{Z}_n$ has a subgroup $(H, +)$ of order m. It is isomorphic to the group $\mathbb{Z}_m$. Since a and m are relatively prime too, φ calculated modulo m, is an automorphism of the group $\mathbb{Z}_m$ and $[a + (1-a)k']_m = 0$ for $k' = [k]_m$. So, $(H, \cdot)$ is an idempotent k'-translatable quasigroup induced by $\mathbb{Z}_m$ and consequently by the subgroup $(H, +)$. □

4. Idempotent k-translatable quasigroups for $k \leqslant 10$

Using our Theorem 3.2 for each value of k we can calculate all idempotent k-translatable quasigroups for the types of quasigroups discussed in the previous section. To calculate the orders of these quasigroups we bear in mind that the order n is odd and that the values of $F_T(a)$ and $H_T(k)$ calculated in Tables 3.1 to 3.4 are equivalent to 0 modulo n. For example, for $k = 5$ in $\mathbf{H}$, we have $0 = [k^2 - k + 1]_n = [21]_n = [3 \cdot 7]_n$. This means that for $k = 5$ the possible orders $n > k$ are 7 or 21. Using Table 3.2 we see that for $n = 7$, $a = [1-k]_7 = [-4]_7 = 3$; for $n = 21$, $a = [-4]_{21} = 17$. Thus, $(3, 5)$ and $(17, 5)$ are members of $\mathbf{H}$. Similarly for $\mathbf{C3}^*$ and $k = 6$ we have $H_T(6) = 21$, so possible order n of a 6-translatable $C3^*$

quasigroup is 3, 7 or 21. But, in this case should be $n > 6$ and $n = 3t + 1$. Thus a 6-translatable $C3^*$ quasigroup has order 7. Then, by Table 3.2, $a = [-3]_7 = 4$ and $[F_T(4)]_7 = 0$. Hence a multiplication of a 6-translatable $C3^*$ quasigroup of order 7 is given by $x \cdot y = [4x + 4y]_7$. Therefore $(4, 4) \in \mathbf{C3}^*$.

Calculations for other cases are similar and we skip them. Obtained results are presented in Tables 4.1 and 4.2.

Table 4.1.

T	$k = 2$	$k = 3$	$k = 4$	$k = 5$	$k = 6$
Q	(2,4)	(4,2)	(7,11)	(11,3)	(16,22)
H	(2,2)	(5,3)	(10,4)	(3,5), (17,5)	(26,6)
GS	–	–	(3,3)	(4,8)	(5,15)
RM	(2,4)	(7,5)	(14,6)	(23,7)	(34,8)
LM	–	(4,2)	(5,7)	(6,14)	(7,23)
ARO	(2,6)	(5,3)	(9,15)	(14,4)	(20,28)
ARO*	–	–	(6,2)	(3,5)	(15,9)
C3	(2,6)	(11,9)	(26,12)	(47,15)	(4,4), (9,5) (74,18)
C3*	–	–	(6,2)	(11,3)	(4,4)
P	(2,10)	(4,2), (7,5) (29,27)	(122,60)	(347,115)	(794,198)
P*	(2,4)	(17,15)	(5,7), (82,40)	(4,8), (9,23) (257,85)	(10,2), (58,14) (626,156)
U	–	(7,5)	(3,3), (6,2) (13,23)	(21,59)	(31,119)
U*	(2,6)	(13,11)	(3,3), (5,7) (38,18)	(83,27)	(154,38)
−**LM**	(2,10)	(17,15)	(42,20)	(77,25)	(122,30)
−(**C3***)	(2,12)	(8,6), (21,19)	(54,26)	(3,5), (6,14) (101,33)	(28,40)
−(**ARO***)	(2,16)	(13,11)	(31,59)	(56,18)	(26,6), (88,130)
−**U**	(2,4) (2,24)	(58,56)	(206,102)	(4,8), (16,44) (488,162)	(946,236)
−(**U***)	–	–	–	(6,14)	(13,47)
−**P**	(2,30)	(107,105)	(5,7), (25,47) (522,260)	(4,8), (49,143) (1577,525)	(3722,930)
−(**P***)	(2,60)	(7,5),(22,20) (227,225)	(3,3), (5,7) (22,10), (38,18) (53,103),(115,327) (1138,568)	(3467,1155)	(26,6), (266,66) (8210,2052)

Table 4.2.

T	$k=7$	$k=8$	$k=9$	$k=10$
Q	$(22,4)$	$(3,11),(29,37)$	$(37,5)$	$(46,56)$
H	$(37,7)$	$(12,8),(50,8)$	$(65,9)$	$(4,10),(82,10)$
GS	$(6,24)$	$(7,35)$	$(8,4),(8,48)$	$(9,63)$
RM	$(3,9),(47,9)$	$(62,10)$	$(79,11)$	$(98,12)$
LM	$(8,34)$	$(9,3),(9,47)$	$(10,62)$	$(11,79)$
ARO	$(27,5)$	$(35,45)$	$(44,6)$	$(3,15)$
ARO*	$(4,14)$	$(28,20)$	$(5,27)$	$(45,35)$
C3	$(107,21)$	$(3,11),(146,24)$	$(5,27)$	$(242,30)$
C3*	$(27,5)$	$(38,6)$	$(13,7),(51,7)$	$(66,8)$
P	$(27,5),(52,10)$ $(1577,315)$	$(190,472)$ $(2834,472)$	$(8,4),(308,184)$ $(4727,675)$	$(6,6),(593,169)$ $(7442,930)$
P*	$(53,259)$ $(1297,259)$	$(2402,400)$	$(5,27),(20,132)$ $(4097,585)$	$(6,6),(35,27)$ $(28,94),(523,148)$ $(6562,820)$
U	$(43,209)$	$(6,12),(11,13)$ $(57,335)$	$(4,20),(23,3)$ $(73,43),(73,503)$	$(91,719)$
U*	$(257,51)$	$(398,66)$	$(13,7),(23,13))$ $(13,83),(51,83)$ $(583,83)$	$(818,102)$
$-$**LM**	$(177,35)$	$(242,40)$	$(13,7),(317,45)$	$(6,6),(33,9)$ $(402,50)$
$-$(**C3***)	$(237,47)$	$(326,54)$	$(103,61),(429,61)$	$(546,68)$
$-$(**ARO***)	$(127,25)$	$(173,229)$	$(226,32)$	$(286,356)$
$-$**U**	$(66,324)$ $(1622,324)$	$(12,8),(46,112)$ $(2558,426)$	$(3796,542)$	$(19,5),(118146)$ $(5378,672)$
$-$(**U***)	$(22,4)$	$(33,191)$	$(46,314)$	$(6,6),(12,38)$ $(61,17),(61,479)$
$-$**P**	$(3,9),(138,684)$ $(7527,1505)$	$(9,3),(623,829)$ $(13682,2280)$	$(37,5),(562,80)$ $(22997,3285)$	$(8,24),(735,587)$ $(36402,4550)$
$-$(**P***)	$(13,59),(48,234)$ $(16627,3325)$	$(30242,5040)$	$(4359,7263)$ $(50843,7263)$	$(6,6),(6403,1829)$ $(80482,10060)$

Note that similar results can be obtained for negative values of k. Obtained quasigroups will be $[k]_n$-translatable quasigroups of order $n > 2$, where n is a divisor of $H_T(k)$.

For example, for $\mathbf{U}^*$, where $0 = [k^3 - k^2 + 2k - 1]_n$, substituting $k = -5$ gives $0 = [-161]_n = [161]_n = [7 \cdot 23]_n$. If $n = 7$, then $a = [-1 - k^3]_n = [-26]_7 = 2$, which gives $x \cdot y = [2x + 6y]_7$. Since $[2^3 - 2 + 1]_7 = 0$, $(2,6) \in \mathbf{U}^*$. If $n = 23$, then $a = [-26]_{23} = [-3]_{23} = 20$ and $[(-3)^3 - (-3) + 1]_{23} = 0$. So, $(20,4) \in \mathbf{U}^*$.

In this case, $k = [-5]_{23} = 18$. Finally, if $n = 161$, then $a = [-26]_{161} = 135$, $(135, 27) \in \mathbf{U}^*$ and $k = [-5]_{161} = 156$.

In a similar way we can calculate analogous results for quasigroups other types $\mathbf{T}$ mentioned in the previous sections.

Below we present obtained results for $\mathbf{U}^*$, where $k \in \{-1, -2, \ldots, -10\}$, once again omitting the detailed calculations.

Table 4.3.

k	n	a	$\mathbf{U}^*$	$[k]_n$
-1	5	3	$(3,3)$	4
-2	17	12	$(16,6)$	15
-3	43	33	$(33,11)$	40
-4	89	72	$(72,18)$	85
-5	$161 = 7 \cdot 23$	$[-26]_n$	$(2,6),(20,4),(135,27)$	$2,18,156$
-6	$265 = 5 \cdot 53$	$[-37]_n$	$(3,3),(16,38),(228,38)$	$4,47,259$
-7	$407 = 11 \cdot 37$	$[-50]_n$	$(5,7),(24,14),(357,51)$	$4,30,400$
-8	593	528	$(528,66)$	585
-9	829	747	$(747,83)$	820
-10	$1121 = 19 \cdot 59$	$[-101]_n$	$(13,7),(17,43),(1020,102)$	$9,49,1111$

In [10] Vidak proved that if $(Q, \cdot)$ is a pentagonal quasigroup then $(Q, \circ)$, defined as $x \circ y = (yx \cdot x)x \cdot y$, is a golden square quasigroup. If the pentagonal quasigroup $(Q, \cdot)$ is also translatable and of order n then, as we have seen, $x \cdot y = [ax+(1-a)y]_n$, with $[a^4-a^3+a^2-a+1]_n = 0$ and $x \circ y = [(a-a^4)x+(1+a^4-a)y]_n$. We can easily check that $(Q, \circ) \in \mathbf{GS}$ using Table 3.1. Since $[a^5+1]_n = 0$, we have also $[(a-a^4)+(1-a^4+a)(1+a^4-a)]_n = 0$. Therefore, $(Q, \circ)$ is $[1-a^4+a]_n$-translatable. So, for every translatable pentagonal quasigroup of order n there is a translatable golden square quasigroup of order n. Note that by [7] a finite pentagonal quasigroup has order $5s$ or $5s+1$. By Table 4.1, a 6-translatable GS-quasigroup has order 19. Hence, it is not pentagonal.

Notice that $\{(3, 9), (9, 3)\} \subseteq -\mathbf{P}$. Accordingly, we have the following definition.

Definition 4.1. The set $dp(\mathbf{T}) = \{(a, 1-a) \,|\, (a, 1-a), (1-a, a) \in \mathbf{T}\}$ is called the *set of* $\mathbf{T}$ *dual pairs*.

If $\mathbf{T} \in \{\mathbf{Q}, \mathbf{H}, \mathbf{GS}\}$ then, by Theorem 3.1, $\mathbf{T} = \mathbf{T}^*$ and $dp(\mathbf{T}) = \mathbf{T} = dp(\mathbf{T}^*)$. From Table 3.1, it follows that if $(a, 1-a) \in \mathbf{RM} \cap \mathbf{RM}^* = \mathbf{RM} \cap \mathbf{LM}$, then $0 = [a^2+a-1]_n = [a^2-3a+1]_n$ and so $[4a]_n = 2$. Thus $0 = [4(a^2+a-1)]_n = [2a-2]_n$ gives $[2a]_n = 2$. Hence, $2 = [4a]_n = [2(2a)]_n = 4$ and so $[2]_n = 0$. This is impossible because $2 < a < n$. Similarly, $\mathbf{LM} \cap \mathbf{LM}^* = \emptyset$. In this way we have proved:

Proposition 4.2. $dp(\mathbf{LM}) = \emptyset = dp(\mathbf{RM})$.

Proposition 4.3. $dp(\mathbf{C3}) = \{(4,4)\} = dp(\mathbf{C3}^*)$.

Proof. $C3$ and $C3^*$-quasigroups have order $n = 3t+1$.

If $(a, 1-a) \in dp(\mathbf{C3})$, then, by Table 3.1, we have $0 = [(1-a)^2 + (1-a) + 1]_n = [a^2 - 3a + 3]_n$ which together with $0 = [a^2 + a + 1]_n$ gives $[4a]_n = 2$. Consequently, $0 = [4(a^2 + a + 1)]_n = [2a + 6]_n$, i.e., $[2a]_n = [-6]_n$. So, $2 = [4a]_n = [2(2a)]_n = [-12]_n$ which means that $0 = [14]_n$. But $n = 3t+1$, so $n = 7$. Therefore, $[2a]_7 = 1$ and $a = 4$.

If $(a, 1-a) \in dp(\mathbf{C3}^*)$, then, by Table 3.1, we have $0 = [a^2 - 3a + 3]_n$. Also, $0 = [(1-a)^2 - 3(1-a) + 3]_n = [a^2 + a + 1]_n$ and consequently, $0 = [a^2 - 3a + 3]_n = [(a^2 + a + 1) - 4a + 2]_n = [-4a + 2]_n$. So, $[4a]_n = 2$. Thus $0 = [4(a^2 - 3a + 3)]_n = [2a + 6]_n$, i.e., $[2a]_n = [-6]_n$. Hence $2 = [2(2a)]_n = [-12]_n$. So, $[14]_n = 0$ and, as in the previous case, $n = 7$, $a = 4$. □

Proposition 4.4. $dp(\mathbf{ARO}) = \emptyset = dp(\mathbf{ARO}^*)$.

Proof. $0 = [2a^2 - 1]_n$ and $0 = [2(1-a)^2 - 1]_n = [2a^2 - 4a + 1]_n$. So, $[4a - 2]_n = 0$ and $2 = [4a^2]_n = [2a]_n$. Hence, $1 = [2a^2]_n = [2a]_n = 2$, contradiction. □

Proposition 4.5. $dp(\mathbf{U}) = \{(3,3)\} = dp(\mathbf{U}^*)$.

Proof. If $(a, 1-a) \in dp(\mathbf{U})$, then $0 = [(1-a)^3 - 3(1-a)^2 + 2(1-a) - 1]_n = [-a^3 + a - 1]_n$, which gives $[a^3]_n = [a-1]_n$. Therefore, $0 = [a^3 - 3a^2 + 2a - 1]_n = [-3a^2 + 3a - 2]_n$, i.e., $[3a^2]_n = [3a - 2]_n$. Hence, $[3(a-1)]_n = [3a^3]_n = [3a^2 - 2a]_n = [a-2]_n$. So, $[2a]_n = 1$. Thus $[a^2]_n = [2a(a^2)]_n = [2(a-1)]_n = [2a-2]_n = [-1]_n$. Consequently, $a = [(2a)a]_n = [-2]_n$. This together with $[a^3]_n = [a-1]_n$ implies $n = 5$ and $a = 3$.

Now, if $(a, 1-a) \in dp(\mathbf{U}^*)$, then $0 = [a^3 - a + 1]_n$ and $0 = [(1-a)^3 - (1-a) + 1]_n = [-(a^3 - a + 1) + 3a^2 - 3a + 2]_n = [3a^2 - 3a + 2]_n$, by Table 3.1. Thus, $[3a^2]_n = [3a-2]_n$ and $0 = [3a^2 - 2a + 3]_n = [(3a-2)a - 3a + 3]_n = [-2a + 1]_n$. Hence, $[2a]_n = 1 = [4a^2]_n$. So, $[a+1]_n = [(2a)a + 4a^2]_n = [6a^2]_n = [6a - 4]_n = [3 - 4]_n = [-1]_n$. So, $a = [-2]_n$ and $1 = [2a]_n = [-4]_n$. Thus, $0 = [5]_n$ and $a = 3$. □

Proposition 4.6. $dp(-\mathbf{LM}) = \{(6,6)\}$.

Proof. If $(a, 1-a) \in dp(-\mathbf{LM})$, then $0 = [a^2 + 3a + 1]_n$ and $0 = [(1-a)^2 + 3(1-a) + 1]_n = [a^2 - 5a + 5]_n = [(a^2 + 3a + 1) - 8a + 4]_n = [-8a + 4]_n$. Hence, $[8a]_n = 4$ and $0 = [8(a^2 + 3a + 1)]_n = [4a + 20]_n$. Thus, $4 = [2(4a)]_n = [-40]_n$ and so $[44]_n = 0$. Since n must be odd (cf. [5, Lemma 4.1]), $n = 11$ and $[8a]_{11} = 4$. This equation has only one solution $a = 6$. □

The proofs of the next two propositions are very similar to the proof of Proposition 4.6.

Proposition 4.7. $dp(-(\mathbf{C3}^*) = \{(10,10)\}$.

Proposition 4.8. $dp(-(\mathbf{U}^*)) = \{(6,6)\}$.

Proposition 4.9. $dp(-(\mathbf{ARO}^*)) = \{(4,4)\}$.

Proof. For $(a, 1-a) \in dp(-(\mathbf{ARO}^*))$ we have $0 = [2a^2+4a+1]_n$. Also $0 = [2(1-a)^2 + 4(1-a)+1]_n = [2a^2-8a+7]_n = [(2a^2+4a+1)-12a+6]_n = [-12a+6]_n$. Hence, $[12a]_n = 6$ and $0 = [6(2a^2+4a+1)]_n = [6a+18]_n$. Thus, $6 = [2(6a)]_n = [-36]_n$ and so $[42]_n = 0$. Since, n must be odd, n is equal to 3, 7 or 21. For $n = 3$ the possible values of a are 1 or 2. These values do not satisfy the condition $[2a^2+4a+1]_3 = 0$, so the case $n = 3$ is impossible. For $n = 21$ the equation $[12a]_{21} = 6$ is solved only by $a = 4$, but then $[2a^2+4a+1]_{21} \neq 0$, This also is impossible. The equation $[12a]_7 = 6$ has only one solution $a = 4$. It satisfies the equation $[2a^2+4a+1]_7 = 0$. Hence $dp(-(\mathbf{ARO}^*)) = \{(4,4)\}$. □

Proposition 4.10. $dp(-\mathbf{U}) = \{(12,12)\})$.

Proof. For the pair $(a, 1-a) \in dp(-\mathbf{U})$ we have $0 = [a^3+3a^2+2a+1]_n$ and $0 = [(1-a)^3+3(1-a)^2+2(1-a)+1]_n = [-a^3+6a^2-11a+7]_n = [9a^2-9a+8]_n$. Hence, $[9a^2]_n = [9a-8]_n$ which together with $0 = [9(a^3+3a^2+2a+1)]_n$ gives $[46a]_n = [23]_n$. Consequently, $[a^2]_n = [-22a+40]_n$ and $[207a]_n = [368]_n$. So, $[23a]_n = [230a-207a]_n = [115-368]_n = [-253]_n$. Thus, $[23]_n = [46a]_n = [-506]_n$. Therefore $n = 529$ or $n = 23$.

For $n = 529$ we have $[23a]_{529} = [-253]_{529} = 276$ and $a = 12$. But such a does not satisfy $[a^3+3a^2+2a+1]_{529} = 0$. If $n = 23$, then from $[a^2]_{23} = [-22a+40]_{23}$ it follows that $a = 12$. Such a satisfies $[a^3+3a^2+2a+1]_{23} = 0$. □

Proposition 4.11. $dp(\mathbf{P}) = \{(6,6)\} = dp(\mathbf{P}^*)$.

Proof. If $(a, 1-a) \in dp(\mathbf{P})$, then $0 = [a^4-a^3+a^2-a+1]_n$, i.e., $[a^5]_n = [-1]_n$. In this case also $0 = [(1-a)^4-(1-a)^3+(1-a)^2-(1-a)+1]_n = [-2a^3+3a^2-a]_n$. So, $[2a^3]_n = [3a^2-a]_n$, whence, multiplying by a^3, a^2 and a we obtain, respectively, $[a^4]_n = [2a-3]_n$, $[a^3]_n = [3a^4+2]_n = [6a-7]_n$ and $[a^2]_n = [3a^3-2a^4]_n = [14a-15]_n$, which together with $[a^4-a^3+a^2-a+1]_n = 0$ gives $[9a]_n = 10$. Thus, $[10a]_n = [9a^2]_n = 5$. So, $a = [-5]_n$ and $[55]_n = 0$. Hence n is equal to 5, 11 or 55. The case $n = 5$ is impossible because in this case $a = 0$, Also the case $n = 55$ is impossible since a and n should be relatively prime. For $n = 11$, $a = 6$ satisfies these conditions.

If $(a, 1-a) \in dp(\mathbf{P}^*)$, then $0 = [a^4-3a^3+4a^2-2a+1]_n$. In this case also $0 = [(1-a)^4-3(1-a)^3+4(1-a)^2-2(1-a)+1]_n = [a^4-a^3+a^2-a+1]_n$. So, $(a, 1-a) \in \mathbf{P} \cap \mathbf{P}^*$. Also $(1-a, a) \in \mathbf{P} \cap \mathbf{P}^*$. Thus, $dp(\mathbf{P}^*) \subseteq dp(\mathbf{P}) = \{(6,6)\}$. Direct computation shows that $(6,6) \in dp(\mathbf{P}^*)$. Therefore $dp(\mathbf{P}) = dp(\mathbf{P}^*)$. □

Proposition 4.12. $dp(-\mathbf{P}) = \{(3,9),(9,3),(16,16),(47,295),(295,47)\}$.

Proof. If $(a, 1-a) \in dp(-\mathbf{P})$, then, by Table 3.3,

$$[a^4+a^3+a^2+a+1]_n = 0, \tag{1}$$

which implies $[a^5]_n = 1$. Then also, $0 = [(1-a)^4+(1-a)^3+(1-a)^2+(1-a)+1]_n = [a^4 - 5a^3 + 10a^2 - 10a + 5]_n$, i.e.,

$$[a^4]_n = [5a^3 - 10a^2 + 10a - 5]_n. \tag{2}$$

From this, multiplying by a and 4, we obtain $[5a^4]_n = [10a^3 - 10a^2 + 5a + 1]_n$ and $[4a^4]_n = [20a^3 - 40a^2 + 40a - 20]_n$. So,

$$[a^4]_n = [-10a^3 + 30a^2 - 35a + 21]_n.$$

Therefore, $[-50a^3 + 150a^2 - 175a + 105]_n = [5a^4]_n = [10a^3 - 10a^2 + 5a + 1]_n$, whence, as a consequence, we get

$$[60a^3]_n = [160a^2 - 180a + 104]_n.$$

On the other hand, (1) together with (2) imply $[6a^3]_n = [9a^2-11a+4]_n$. Thus, $[90a^2 - 110a + 40]_n = [60a^3]_n = [160a^2 - 180a + 104]_n$. So,

$$[70a^2]_n = [70a - 64]_n. \tag{3}$$

From this, multiply successively by a^4, a and a^2 we get $[70a]_n = [70 - 64a^4]_n$, $[70a^3]_n = [6a - 64]_n$ and $[70a^4]_n = [6a^2 - 64a]_n$, which, together with (1), gives $0 = [70(a^4 + a^3 + a^2 + a + 1)]_n = [6a^2 + 82a - 58]_n$, i.e.,

$$[6a^2]_n = [58 - 82a]_n. \tag{4}$$

Since $[64a^2]_n = [70a-6a^2-64]_n$, by (3), we also have $[4a^2]_n = [64a^2-60a^2]_n = [(70a - 6a^2 - 64) - (580 - 820a)]_n = [890 - 6a^2 - 644]_n$ and so, $[890a - 644]_n = [4a^2 + 6a^2]_n = [4a^2 + 58 - 82a]_n$. Hence, $[4a^2]_n = [972a - 702]_n$. Then $[2a^2]_n = [6a^2-4a^2]_n = [760-1054a]_n$. Thus, $[972a-702]_n = [2(2a^2]_n = [1520-2108a]_n$. So, $[3080a]_n = [2222]_n$ and $[3080a^2]_n = [2222a]_n$. Now, using this equation and (3), we obtain $0 = [44(70a^2-70a+64)]_n = [3080a^2-3080a+2816]_n = [-858a+2816]_n$. Thus, $[858a]_n = [2816]_n$, which implies, $[2574a]_n = [3(858a)]_n = [8448]_n$. Hence, $[506a]_n = [3080a - 2574a] = [-6226]_n$, $[352a]_n = [858a - 506a] = [9042]_n$ and $[308a]_n = [2(858a) - 4(352a)]_n = [-30536]_n$. Consequently,

$$[44a]_n = [352a - 308a]_n = [39578]_n. \tag{5}$$

But $[39578]_n = [44a]_n = [308a - 6(44a)]_n = [-30536 - 237468]_n = [-268004]_n$. So, $[307582]_n = 0$. Since $307582 = 2 \times 11^2 \times 31 \times 41$ and n must be an odd number, the possible values of n are 11, 31, 41, 121, 341, 451, 1 271, 3 751, 4 961, 13 981 and 153 791.

We will consider each case separately. Note first that $(a, b) \in dp(-\mathbf{P})$ if and only if both a and b satisfy (1) and $[a+b]_n = 1$. Then a and b satisfy the congruence (5) too.

$(n = 11)$. Since $k < n = 11$, from Tables 4.1 and 4.2 it follows that in this case only pairs $(3, 9)$ and $(9, 3)$ are dual.

$(n = 31)$. Then (5) reduces to the congruence $13a \equiv 22 (\mathrm{mod}\ 31)$. Since the greatest common divisor of 13 and 31 is 1, this congruence has only one solution $a = 16$. This solution satisfies (1). Obviously, $(16, 16) \in dp(-\mathbf{P})$.

$(n = 41)$. Then (5) has the form $3a \equiv 13 (\mathrm{mod}\ 41)$ and has only one solution $a = 18$. The pair $(18, 24) \in -\mathbf{P}$, but 24 does not satisfies the above congruence. Thus for $n = 41$ the set $dp(-\mathbf{P})$ is empty.

$(n = 121)$. Then $44a \equiv 11 (\mathrm{mod}\ 121)$. Since the greatest common divisor of 44 and 11 is 11, this congruence has 11 solutions. Any a satisfying the congruence $44a \equiv 11 (\mathrm{mod}\ 121)$ satisfies also the congruence $4a \equiv 1 (\mathrm{mod}\ 11)$, which has only one solution $a = 3$. Thus the set S of solutions of $44a \equiv 11 (\mathrm{mod}\ 121)$ consists of the numbers the form $3 + 11k$, $k = 0, 1, 2, \ldots, 10$. Since for any $a, b \in S$ we have $[a + b]_{11} = 6$, so $[a + b]_{121} \neq 1$. This means that for $n = 121$ the set $dp(-\mathbf{P})$ is empty.

$(n = 341)$. Then $44a \equiv 22 (\mathrm{mod}\ 341)$. This congruence has 11 solutions. Any a satisfying this congruence satisfies also the congruence $4a \equiv 2 (\mathrm{mod}\ 31)$, which has only one solution $a = 16$. Thus the solutions of $44a \equiv 22 (\mathrm{mod}\ 341)$ have the form $x = 16 + 31k$, $k = 0, 1, 2, \ldots, 10$. Direct calculations shows that only pairs $(47, 295)$ and $(295, 47)$ are dual.

$(n = 451)$. Then $44a \equiv 341 (\mathrm{mod}\ 451)$. This congruence has 11 solutions. Any a satisfying this congruence also satisfies the congruence $4a \equiv 31 (\mathrm{mod}\ 41)$, which has only one solution $a = 18$. Thus $S = \{18 + 41k \mid k = 0, 1, \ldots, 10\}$ is the set of solutions of $44a \equiv 341 (\mathrm{mod}\ 451)$. Since $[a + b]_{41} = 36$ for all $a, b \in S$, in the case $n = 451$ there no dual pairs.

$(n = 1271)$. Then $44a \equiv 177 (\mathrm{mod}\ 1271)$. This congruence is satisfied only by $a = 264$. The pair $(264, 1008) \in -\mathbf{P}$, but 1008 does not satisfy this congruence. So, for $n = 1271$ the set $dp(-\mathbf{P})$ is empty.

$(n = 3751)$. Then $44a \equiv 2068 (\mathrm{mod}\ 3751)$. This congruence has 11 solutions. Any a satisfying this congruence satisfies also the congruence $4a \equiv 188 (\mathrm{mod}\ 341)$, which has only one solution $x = 47$. Thus $S = \{47 + 341k \mid k = 0, 1, \ldots, 10\}$ contains all solutions of the congruence $44a \equiv 2068 (\mathrm{mod}\ 3751)$. Since $[a + b]_{341} = 94$ for all $a, b \in S$, in this case there no dual pairs.

$(n = 4961)$. Then $44a \equiv 4851 (\mathrm{mod}\ 4961)$. This congruence has 11 solutions. Any a satisfying this congruence satisfies also the congruence $4a \equiv 441 (\mathrm{mod}\ 451)$, which has only one solution $a = 223$. Thus $S = \{223 + 451k \mid k = 0, 1, \ldots, 10\}$ contains all solutions of the congruence $44a \equiv 441 (\mathrm{mod}\ 4851)$. Since $[a + b]_{451} = 446$ for all $a, b \in S$, also in this case there no dual pairs.

$(n = 13\,981)$. Then $44a \equiv 11616 (\mathrm{mod}\ 13981)$. This congruence has 11 solutions. Proceeding as in previous cases we can see that $S = \{264 + 1271k \mid k = 0, 1, \ldots, 10\}$ contains all solutions of this congruence. Since $[a + b]_{1271} = 528$ for all $a, b \in S$, in this case there no dual pairs too.

($n = 153\,791$). Then $44a \equiv 39578 (\mathrm{mod}\ 153791)$. Analogously as in previous cases we can see that the set $S = \{7890 + 13981k \mid k = 0, 1, \ldots, 10\}$ contains all solutions of this congruence and $[a+b]_{13981} \neq 1$ for $a, b \in S$. So, in this case there no dual pairs.

This completes the proof. □

Proposition 4.13. $dp(-(\mathbf{P}^*)) = \{(3,3), (5,7), (6,6), (7,5)\}$.

Proof. If $(a, 1-a) \in dp((-\mathbf{P})^*)$, then, by Table 3.3,

$$[a^4 + 3a^3 + 4a^2 + 2a + 1]_n = 0 \tag{6}$$

and $0 = [(1-a)^4 + 3(1-a)^3 + 4(1-a)^2 + 2(1-a) + 1]_n = [a^4 - 7a^3 + 19a^2 - 23a + 11]_n$, i.e.,

$$[a^4]_n = [7a^3 - 19a^2 + 23a - 11]_n. \tag{7}$$

Comparing (6) with (7) we obtain

$$[10a^3]_n = [15a^2 - 25a + 10]_n. \tag{8}$$

Multiplying this equation by 11 and a we obtain $[110a^3]_n = [165a^2 - 275a + 110]_n$ and $[10a^4]_n = [15a^3 - 25a^2 + 10a]_n$.

From (6) we have $[10a^4]_n = [-30a^3 - 40a^2 - 20a - 10]_n$, which together with the last equation implies $[45a^3]_n = [-15a^2 - 30a - 10]_n$. Comparing this equation with (8) multiplied by 4 we obtain

$$[5a^3]_n = [-75a^2 + 70a - 50]_n. \tag{9}$$

Consequently, $[-150a^2 + 140a - 100]_n = [10a^3]_n = [15a^2 - 25a + 10]_n$. So, $[165a^2]_n = [165a - 110]_n$. Thus,

$$[110a^3]_n = [165a^2 - 275a + 110]_n = [-110a]_n \tag{10}$$

and $[110a^4]_n = [-110a^2]_n$. Now, multiplying (6) by 110 and applying the last two expressions we obtain $[330a^2]_n = [110a - 110]_n$. This and (10) imply $[-330a]_n = [330a^3]_n = [110a^2 - 110a]_n$. So, $[110a^2]_n = [-220a]_n$ and $[110a^3]_n = [-220a^2]_n$. Hence $[-110a]_n = [110a^3]_n = [-220a^2]_n$. Thus $[110a]_n = [220a^2]_n$. Consequently, $[110a - 110]_n = [330a^2]_n = [220a^2 + 110a^2]_n = [110a + 110a^2]_n$. Hence $[110a^2]_n = [-110]_n$. Therefore, $[110a]_n = [220a^2]_n = [-220]_n$ and $[-110]_n = [110a^2] = [-220a]_n = [440]_n$, i.e., $[550]_n = 0$. Since n must be odd, the possible values of n are 5, 11, 25, 55 and 275.

($n = 5$). Direct calculation shows that in this case only $(3,3) \in dp(-(\mathbf{P})^*)$.

($n = 11$). In this case only $(5,7), (6,6), (7,5) \in dp(-(\mathbf{P}^*))$.

($n = 25$). Any a satisfying (6) and (7) satisfies also (9), which for $n = 25$ has the form $[5a^3]_{25} = [20a]_{25}$. Solutions of this equation also satisfy the equation $[a^3]_5 = [4a]_5$. This equation has two solutions that are relatively prime to 5, namely $a = 2$ and $a = 3$. Thus the solutions of $[5a^3]_{25} = [20a]_{25}$ should be in one of the following sets: $S' = \{2+5k \mid k = 0,1,2,3,4\}$ or $S'' = \{3+5k \mid k = 0,1,2,3,4\}$. For $(a,b) \in dp(-(\mathbf{P}^*))$, $[a+b]_{25} = 1$. This is possible only for $a, b \in S''$. But it is easy to check that none of $a \in S''$ satisfies (6). (Also none of $a \in S'$ satisfies (6).) Hence for $n = 25$ the set $dp(-(\mathbf{P}^*))$ is empty.

($n = 275$). The number of solutions of the congruence (9) calculated modulo $275 = 11 \times 25$ is equal to $t_1 \times t_2$, where t_1 is the number of the solutions of (9) calculated modulo 11 and t_2 is the number of the solutions of (9) calculated modulo 25 (cf. [11]). Since $t_2 = 0$, for $n = 275$ the set $dp(-(\mathbf{P}^*))$ is empty. □

5. Moving from one type to another

The mappings $\mathbf{T} \mapsto \mathbf{T}^*$, $\mathbf{T} \mapsto -\mathbf{T}$, $\mathbf{T} \mapsto \mathbf{T}^{+\mathbf{t}}$ and $\mathbf{T} \mapsto \mathbf{T}^{-\mathbf{t}}$ transform one type of idempotent k-translatable quasigroups to another. We already know that $\mathbf{H} = \mathbf{H}^* = -\mathbf{C3}$, $\mathbf{GS} = \mathbf{GS}^* = -\mathbf{RM}$, $\mathbf{RM} = \mathbf{LM}^* = -\mathbf{GS}$, $\mathbf{LM} = \mathbf{RM}^*$, $\mathbf{ARO} = -\mathbf{ARO}$ and $\mathbf{C3} = -\mathbf{H}$. These formulae allow us to move from certain types to others. For example, to move from $\mathbf{GS}$ to $\mathbf{RM}$ we convert any $(a, 1-a) \in \mathbf{GS}$ to $(-a, 1+a)$ and then $(-a, 1+a) \in \mathbf{RM}$. Similarly, to move from $\mathbf{C3}$ to $\mathbf{H}$ we convert any $(a, 1-a) \in \mathbf{C3}$ to $(-a, 1+a)$ and then $(-a, 1+a) \in \mathbf{H}$. To move from $\mathbf{RM}$ to $\mathbf{LM}$ we convert any $(a, 1-a) \in \mathbf{RM}$ to $(1-a.a)$ and then $(1-a, a) \in \mathbf{LM}$. Also, $(\mathbf{GS})^{+\mathbf{1}} = \mathbf{LM}$, $(\mathbf{LM})^{-\mathbf{1}} = \mathbf{GS}$ and $\mathbf{LM} = (\mathbf{GS})^{+\mathbf{1}} = (-\mathbf{RM})^{+\mathbf{1}} = (-(\mathbf{LM}^*))^{+\mathbf{1}}$. We prove below that $\mathbf{T} = (-(\mathbf{T}^*))^{+\mathbf{1}}$ for any type $\mathbf{T} \subseteq \mathbf{IKQ}$.

Notice that $\mathbf{T} = \mathbf{T}^*$ does not imply $-(\mathbf{T}^*) = (-\mathbf{T})^*$ because, $\mathbf{H} = \mathbf{H}^*$ and $-\mathbf{H} = \mathbf{C3}$ and so, $(-\mathbf{H})^* = \mathbf{C3}^* \neq \mathbf{C3} = -(\mathbf{H}^*)$. This proves the following proposition.

Proposition 5.1. *In general,* $(-\mathbf{T})^* \neq -(\mathbf{T}^*)$.

Theorem 5.2. *For any type* $\mathbf{T}$ *of idempotent k-translatable quasigroups*

$$-\mathbf{T} = (\mathbf{T}^*)^{-\mathbf{1}} \quad \textit{and} \quad \mathbf{T} = -((\mathbf{T}^*)^{-\mathbf{1}}) = (-(\mathbf{T}^*))^{+\mathbf{1}}.$$

Proof. We have $(a, 1-a) \in (\mathbf{T}^*)^{-\mathbf{1}} \Leftrightarrow (a+1, -a) \in \mathbf{T}^* \Leftrightarrow (-a, a+1) \in \mathbf{T} \Leftrightarrow (a, 1-a) \in -\mathbf{T}$. Since $-(-\mathbf{T}) = \mathbf{T}$, from $-\mathbf{T} = (\mathbf{T}^*)^{-\mathbf{1}}$ it follows $\mathbf{T} = -((\mathbf{T}^*)^{-\mathbf{1}})$. Also, $(a, 1-a) \in \mathbf{T} \Leftrightarrow (1-a, a) \in \mathbf{T}^* \Leftrightarrow (a-1, 2-a) \in -(\mathbf{T}^*) \Leftrightarrow (a, 1-a) \in (-(\mathbf{T}^*))^{+\mathbf{1}}$. □

Corollary 5.3. $\mathbf{T}^* = -(\mathbf{T}^{-\mathbf{1}}) = (-\mathbf{T})^{+\mathbf{1}} = ((\mathbf{T}^{-\mathbf{1}})^*)^{-\mathbf{1}} = ((-(\mathbf{T}^*))^*)^{-\mathbf{1}}$.

Proof. As a consequence of Theorem 5.2 we get, $\mathbf{T}^* = -(-(\mathbf{T}^*)) = ((-(\mathbf{T}^*))^*)^{-\mathbf{1}}$. Also, $-(\mathbf{T}^*) = ((\mathbf{T}^*)^*)^{-\mathbf{1}} = \mathbf{T}^{-\mathbf{1}}$ implies $\mathbf{T}^* = -(\mathbf{T}^{-\mathbf{1}}) = ((\mathbf{T}^{-\mathbf{1}})^*)^{-\mathbf{1}}$. Finally, $\mathbf{T}^* = (-\mathbf{T})^{+\mathbf{1}}$. □

Corollary 5.4. $\mathbf{T} = (-(\mathbf{T}^*))^{+1} = -((\mathbf{T}^*)^{-1})$.

Proof. Observe that $(a, 1-a) \in \mathbf{T} \Leftrightarrow (1-a, a) \in \mathbf{T}^* \Leftrightarrow (a-1, 2-a) \in -(\mathbf{T}^*) \Leftrightarrow (a, 1-a) \in (-(\mathbf{T}^*))^{+1}$. So, $\mathbf{T} = (-(\mathbf{T}^*))^{+1}$. Also, $(\mathbf{T}^*)^{-1} = ((-\mathbf{T})^{+1})^{-1} = -\mathbf{T}$, by Corollary 5.3. Hence, $\mathbf{T} = -((\mathbf{T}^*)^{-1})$. □

Corollary 5.5. $-(\mathbf{T}^*) = \mathbf{T}^{-1}$ *and* $(-\mathbf{T})^* = \mathbf{T}^{+1}$.

Proof. From Corollary 5.3 it follows that $-(\mathbf{T}^*) = \mathbf{T}^{-1}$. Then, $(a, 1-a) \in (-\mathbf{T})^* \Leftrightarrow (1-a, a) \in -\mathbf{T} \Leftrightarrow (a-1, 2-a) \in \mathbf{T} \Leftrightarrow (a, 1-a) \in \mathbf{T}^{+1}$. □

We can now answer the question, *when does* $-(\mathbf{T}^*) = (-\mathbf{T})^*$?

Theorem 5.6. $(-\mathbf{T})^* = -(\mathbf{T}^*) \Leftrightarrow \mathbf{T}^{+1} = \mathbf{T}^{-1} \Leftrightarrow \mathbf{T} = \mathbf{T}^{+2} \Leftrightarrow \mathbf{T} = \mathbf{T}^{-2}$.

Proof. Indeed, by Corollary 5.5, $(-\mathbf{T})^* = -(\mathbf{T}^*) \Leftrightarrow \mathbf{T}^{+1} = \mathbf{T}^{-1}$. We also have, $\mathbf{T}^{+1} = \mathbf{T}^{-1} \Leftrightarrow \mathbf{T} = \mathbf{T}^{+2} \Leftrightarrow \mathbf{T} = \mathbf{T}^{-2}$. □

Theorem 5.7. $-(\mathbf{T}^{+1}) = (-\mathbf{T})^{+1} \Leftrightarrow -(\mathbf{T}^{-1}) = (-\mathbf{T})^{-1} \Leftrightarrow (\mathbf{T}^*)^{+1} = (\mathbf{T}^{-1})^* \Leftrightarrow (\mathbf{T}^*)^{-1} = (\mathbf{T}^{-1})^* \Leftrightarrow (-\mathbf{T})^* = -(\mathbf{T}^*)$.

Proof. We have $(a, 1-a) \in -(\mathbf{T}^{+1}) \Leftrightarrow (-a, 1+a) \in \mathbf{T}^{+1} \Leftrightarrow (-1-a, 2+a) \in \mathbf{T} \Leftrightarrow (2+a, -1-a) \in \mathbf{T}^* \Leftrightarrow (a, 1-a) \in (\mathbf{T}^*)^{-2} = (-\mathbf{T})^{-1}$ and $(-\mathbf{T})^{+1} = \mathbf{T}^*$, by Corollary 5.3. Therefore, $-(\mathbf{T}^{+1}) = (-\mathbf{T})^{+1} \Leftrightarrow \mathbf{T}^* = (-\mathbf{T})^{-1} \Leftrightarrow -(\mathbf{T}^{-1}) = (-\mathbf{T})^{-1}$. But by Corollary 5.3 we also have $(-\mathbf{T})^* = -((-\mathbf{T})^{-1})$, so $\mathbf{T}^* = (-\mathbf{T})^{-1} \Leftrightarrow (-\mathbf{T})^* = -(\mathbf{T}^*)$. □

6. Orthogonality

Definition 6.1. Two quasigroups $(Q, \cdot)$ and $(Q, \circ)$ are called *orthogonal* if, for every $s, t \in Q$, the equations $x \cdot y = s$ and $x \circ y = t$ have unique solutions $x, y \in Q$.

Not every pair of idempotent translatable quasigroups of the same order are orthogonal. The criterion of orthogonality of such quasigroups is given by the following theorem that also can be deduced from results obtained in [8].

Theorem 6.2. *The quasigroups* $(Q, \cdot)$ *and* $(Q, \circ)$*, where* $x \cdot y = [ax + (1-a)y]_n$ *and* $x \circ y = [cx + (1-c)y]_n$ *are orthogonal if* $a - c$ *and* n *are relatively prime.*

Proof. Since $x \cdot y = [ax + (1-a)y]_n$ and $x \circ y = [cx + (1-c)y]_n$ are quasigroup operations, a and n (also c and n) are relatively prime. So, there are $a', c' \in Q$ such that $[aa']_n = [cc']_n = 1$.

Let $s, t \in Q$. Suppose that

$$\begin{cases} x \cdot y = [ax + (1-a)y]_n = s, \\ x \circ y = [cx + (1-c)y]_n = t. \end{cases}$$

Multiply the first equation by a' and the second by c', we obtain the following system of equations

$$\begin{cases} [x + (a' - 1)y]_n = sa', \\ [x + (c' - 1)y]_n = tc', \end{cases}$$

that will be written as

$$\begin{cases} [(a' - c')y]_n = sa' - tc', \\ [x + (c' - 1)y]_n = tc'. \end{cases}$$

This system has a unique solution if and only if the mapping $\varphi(y) = [(a' - c')y]_n$ transforms Q onto Q. This is possible only in the case when $a' - c'$ and n are relatively prime. Since p divides $a' - c'$ if and only if p divides $a - c$, $a' - c'$ and n are relatively prime if and only if $a - c$ and n are relatively prime. This observation completes the proof. $\square$

Corollary 6.3. *A quasigroup $(Q, \cdot)$, where $x \cdot y = [ax + (1 - a)y]_n$, and its dual quasigroup $(Q, *)$ are orthogonal if and only if $2a - 1$ and n are relatively prime.*

Applying this corollary to Table 3.1 we obtain

Corollary 6.4. *Quasigroups from* **Q** *and* **ARO** *are orthogonal to their dual quasigroups.*

7.Belousov's identities

Belousov in [1] proved the following Theorem.

Theorem 7.1. *Any minimal nontrivial identity in a quasigroup is parastrophically equivalent to one of the following identity types: $x(x \cdot xy) = y$, $x(y \cdot yx) = y$, $x \cdot xy = yx$, $xy \cdot x = y \cdot xy$, $xy \cdot yx = y$, $xy \cdot y = x \cdot xy$ and $yx \cdot xy = y$.*

We now explore these identities within **IKQ**. Observe first that the identity $x(x \cdot xy) = y$ defines the type **C3**, the identity $x(y \cdot yx) = y$ defines the type **U** and the identity $x \cdot xy = yx$ defines the type **LM**.

Proposition 7.2. *In* **IKQ** *each of the identities $xy \cdot x = y \cdot xy$ and $xy \cdot yx = y$ define a quadratical quasigroup.*

Proof. Since $x \cdot y = [ax + (1 - a)y]_n$, each of these identities implies the identity $2a^2 - 2a + 1_n = 0$. So, by Theorem 2.1, $(G, \cdot)$ is quadratical. $\square$

Proposition 7.3. *There are no quasigroups in* **IKQ** *that satisfy either of the identities $xy \cdot y = x \cdot xy$ or $yx \cdot xy = y$.*

Proof. In **IKQ** each of these identities imply the identity $[2a^2 - 2a]_n = 0$. This implies $0 = [k(2a^2 - 2a)]_n = [2(ka)a - 2ka]_n = [2(k + a)a - 2(k + a)]_n = [2a^2]_n = [2a]_n$. So, $0 = [2ak]_n = [2(k + a)]_n = [2k]_n$, and consequently $2 = [2kk']_n = 0$, a contradiction. $\square$

8. Parastrophes

Each quasigroup $Q = (Q, \cdot)$ determines five new quasigroups $Q_i = (Q, \circ_i)$ (called *parastrophes* or *conjugate quasigroups*), where the operation $\circ_i$ is defined as follows:

$$\begin{aligned}
x \circ_1 y = z &\Leftrightarrow x \cdot z = y,\\
x \circ_2 y = z &\Leftrightarrow z \cdot y = x,\\
x \circ_3 y = z &\Leftrightarrow z \cdot x = y,\\
x \circ_4 y = z &\Leftrightarrow y \cdot z = x,\\
x \circ_5 y = z &\Leftrightarrow y \cdot x = z.
\end{aligned}$$

It is not difficult to observe that these parastrophes are pairwise dual. Namely, $Q^* = Q_5$, $Q_1^* = Q_4$ and $Q_2^* = Q_3$.

In general, such defined parastrophes are not isotopic, but if $(Q, \cdot)$ is an idempotent k-translatable quasigroup of order n, then all its parastrophes are isotopic (cf. [5]) and have simple form.

Theorem 8.1. *Parastrophes of a k-translatable idempotent quasigroup $(Q, \cdot)$ with the multiplication defined by $x \cdot y = [ax + by]_n$ are t-translatable idempotent quasigroups of the form:*

$$\begin{aligned}
x \circ_1 y &= [(1 - b')x + b'y]_n,\\
x \circ_2 y &= [a'x + (1 - a')y]_n,\\
x \circ_3 y &= [(1 - a')x + a'y]_n,\\
x \circ_4 y &= [b'x + (1 - b')y]_n,\\
x \circ_5 y &= [(1 - a)x + ay]_n.
\end{aligned}$$

Q_1 is t-translatable for $t = a$, Q_2 for $t = b'$, Q_3 for $t = b$, Q_4 for $t = a'$, Q_5 for $t = k'$.

Proof. By simple computations we can see that the parastrophes of $(Q, \cdot)$ have the above form. So they are idempotent quasigroups. Their t-translatability follows from the fact that $[a + b]_n = 1$ and $[a' + b']_n = [a'b']_n$. □

Corollary 8.2. *Parastrophes of a k-translatable quadratical quasigroup $(Q, \cdot)$ with the multiplication $x \cdot y = [ax + by]_n$, have the form:*

$$\begin{aligned}
x \circ_1 y &= [kx + (1 - k)y]_n,\\
x \circ_2 y &= [(k + 1)x - ky]_n,\\
x \circ_3 y &= [-kx + (k + 1)y]_n,\\
x \circ_4 y &= [(1 - k)x + ky]_n,\\
x \circ_5 y &= [(1 - a)x + ay]_n.
\end{aligned}$$

Theorem 8.3. *If $(Q, \cdot)$ with $x \cdot y = [ax + by]_n$ is a k-translatable quadratical quasigroup, then its parastrophe types are as in the table below, where (u, v) in the column $x \circ_i y$ and the row **T** means that the parastrophe $x \circ_i y$ of $(Q, \cdot)$ is of type **T** only for $a = u$ and $b = v$.*

	$x \cdot y$	$x \circ_1 y$	$x \circ_2 y$	$x \circ_3 y$	$x \circ_4 y$	$x \circ_5 y$
Q	*always*	$(2,4)$	$(4,2)$	$(2,4)$	$(4,2)$	*always*
H	*never*	*never*	*never*	*never*	*never*	*never*
GS	*never*	$(4,2)$	$(2,4)$	$(4,2)$	$(2,4)$	*never*
RM	$(2,4)$	$(2,4)$	*never*	*never*	$(4,2)$	$(4,2)$
LM	$(4,2)$	*never*	$(4,2)$	$(2,4)$	*never*	$(2,4)$
ARO	*never*	*never*	$(11,7)$	$(7,11)$	*never*	*never*
ARO*	*never*	$(7,11)$	*never*	*never*	$(11,7)$	*never*
C3	$(3,11)$	*never*	$(3,11)$	$(11,3)$	*never*	$(11,3)$
C3*	$(11,3)$	$(11,3)$	*never*	*never*	$(3,11)$	$(3,11)$
P	$(4,2)$	*never*	$(4,2)$	$(2,4)$	*never*	$(2,4)$
P*	$(2,4)$	$(2,4)$	*never*	*never*	$(4,2)$	$(4,2)$
U	*never*	$(4,2)$	$(2,4)$	$(4,2)$	$(2,4)$	*never*
U*	*never*	$(4,2)$	$(2,4)$	$(4,2)$	$(2,4)$	*never*
−**LM**	$(5,37)$	*never*	$(5,37)$	$(37,5)$	*never*	$(37,5)$
−(**C3***)	$(60,38)$	$(3,11)$	$(56,6)$	$(6,56)$	$(11,3)$	$(38,60)$
−(**ARO***)	*never*	$(11,7)$	$(11,3),(62,28)$ $(596,562)$	$(3,11),(28,62)$ $(562,596)$	$(7,11)$	*never*
−**U**	*never*	$(2,4)$	$(46,56)$	$(56,46)$	$(4,2)$	*never*
−(**U***)	*never*	$(2,4)$	$(7,11)$	$(11,7)$	$(4,2)$	*never*
−**P**	$(37,5)$	*never*	$(37,5)$	$(5,37)$	*never*	$(5,37)$
−(**P***)	$(153,89)$	$(4,2)$	*never*	*never*	$(2,4)$	$(89,153)$

Proof. In the proof we will use conditions given in Table 3.1 and the fact that an idempotent k-translatable quasigroup $(Q,\cdot)$ is quadratical if and only if $x\cdot y=[ax+(1-a)y]_n$, where $n>1$ is odd, $[2a^2-2a+1]_n=0$, $k=[1-2a]_n$ and $[k^2]_n=-1$. Moreover, since $Q^*=Q_5$, $Q_1^*=Q_4$ and $Q_2^*=Q_3$, it is sufficient verity only when Q, Q_1 and Q_2 are fixed type **T**, i.e., for which values of (a,b) $Q,Q_1,Q_2\in\mathbf{T}$.

$\mathbf{T}=\mathbf{Q}$.

• Since, $\mathbf{Q}=\mathbf{Q}^*$ (Theorem 3.1), the quasigroup Q_5 always is quadratical.

• $x\circ_1 y=[kx+(1-k)y]_n$. Thus, $0=[2k^2-2k+1]_n=[4a-3]_n=[-2k-1]_n$. So, $0=[(-2k-1)k]_n=[2-k]_n$. Hence $k=2$, $n=k^2+1=5$ and $[2a]_5=4$, which gives $(2,4)$.

• $x\circ_2 y=[(k+1)x-ky]_n$. Then $0=[2(k_1)^2-2(k+1)=1]_n=[2k-1]_n$. So, $0=[(2k-1)k]_n=[-2-k]_n$. Hence, $n=k^2+1=5$, $[2a]_5=3$ and $a=4$, which gives $(4,2)$.

$\mathbf{T}=\mathbf{H}$.

If $Q \in \mathbf{H}$, then $0 = [2a^2 - 2a + 1]_n = [a^2 - a + 1]_n$, which is impossible. So, $Q \notin \mathbf{H}$.
• If $Q_1 \in \mathbf{H}$, then $0 = [k^2 - k + 1]_n = [-1 - k + 1]_n = [-k]_n$, a contradiction.
• If $Q_2 \in \mathbf{H}$, then $0 = [(k+1)^2 - (k+1) + 1]_n = [k^2 + k + 1]_n = [k]_n$, a contradiction.
$\mathbf{T} = -(\mathbf{ARO}^*)$. If $Q \in -(\mathbf{ARO}^*)$, then $0 = [2a^2 - 2a + 1]_n = [a^2 + 4a + 1]_n$. This gives $[6a]_n = 0$. But then $0 = [3(2a^2 - 2a + 1)]_n = 3$. So, must be $n = 3$ and $a = 2$, which is impossible
• If $Q_1 \in -(\mathbf{ARO}^*)$, then $0 = [2k^2 + 4k + 1]_n$ implies $[4k]_n = 1$. Thus $[-4]_n = k$, $n = k^2 + 1 = 17$ and $[2a]_{17} = [1 - k]_{17} = 5$. So, $a = 11$, which gives the pair $(11, 7)$.
• If $Q_2 \in -(\mathbf{ARO}^*)$, then $0 = [2(k+1)^2 + 4(k+1) + 1]_n = [8k+5]_n$. Hence, $[8k]_n = [-5]_n$, $[-5k]_n = [-8]_n$ and $k = [16k - 15k]_n = [-34]_n$. Thus $0 = [k^2 + 1]_n = 1157$ means that the possible values of n are 13, 89 and 1157. For $n = 13$ we obtain $k = [-13]_{13} = 5$ and $2a = [1 - k]_{13} = 9$. So, $a = 11$, which gives the pair $(11, 3)$. By similar calculations, for $n = 89$ we get $k = 55$ and $(62, 28)$, for $n = 1157$ we obtain $k = 1123$ and $(598, 562)$.

For other types the proof is analogous, so we omit it. □

References

[1] **V.D. Belousov**, *Parastrophic-orthogonal quasigroups*, Quasigroups and Related Systems, **13** (2005), 25 – 72.

[2] **F.E. Bennet, E. Mendelsohn and N.S. Mendelsohn**, *Resolvable perfect cyclic designs*, J. Combin. Theory (A), 29 (1980), 142 – 150.

[3] **W.A. Dudek**, *Parastrophes of quasigroups*, Quasigroups and Related Systems **23** (2015), 221 – 230.

[4] **W.A. Dudek and R.A.R. Monzo**, *On the fine structure of quadratical quasigroups*, Quasigroups and Related Systems, **24** (2016), 205 – 218.

[5] **W.A. Dudek and R.A.R. Monzo**, *The structure of idempotent translatable quasigroups*, Bull. Malays. Math. Sci. Soc. **43** (2020), 1603 – 1621.

[6] **W.A. Dudek and R.A.R. Monzo**, *Translatable quadratical quasigroups*, arXiv:1708.08830v1 [math.RA].

[7] **W.A. Dudek and R.A.R. Monzo**, *Translatable pentagonal quasigroups*, Ricerche di Mat.

[8] **G.L. Mullen and V.A. Shcherbacov**, *On orthogonality of binary operations and squares*, Bul. Acad. Stiinte Republ. Moldova, ser. Mat. **2** (2005), 3 – 42.

[9] **S. Vidak**, *Pentagonal quasigroups*, Quasigroups and Related Systems, **22** (2014), 147 – 158.

[10] **S. Vidak**, *The Napoleon-Barlotti Theorem in pentagonal quasigroups*, Glasnik Matematički, **51(71)** (2016), 359 – 377.

[11] **I.M. Vinogradov**, *Foundations of the theory of numbers*, (Russian), Nauka, Moscow (1965).

Received December 15, 2019

W.A. Dudek
Faculty of Pure and Applied Mathematics,
Wroclaw University of Science and Technology,
50-370 Wroclaw, Poland
Email: wieslaw.dudek@pwr.edu.pl

R.A.R. Monzo
Flat 10, Albert Mansions, Crouch Hill,
London N8 9RE, United Kingdom
E-mail: bobmonzo@talktalk.net