Quasigroups and Related Systems **13** (2005), 25 – 72

Parastrophic-orthogonal quasigroups

Valentin D. Belousov

Abstract

Annotated translation of *Parastrophic-orthogonal quasigroups*, Acad. Nauk Moldav. SSR, Inst. Mat.s Vychisl. Tsentrom, Kishinev, 1983, prepared by A.D.Keedwell and P.Syrbu based on the original Russian and on an earlier English translation supplied to the first author by Belousov himself.

The notion of orthogonality plays an important role in the theory of Latin squares, and consequently also in the theory of quasigroups, because every finite quasigroup has a Latin square as its Cayley table and, conversely, every Latin square is the multiplication table of a certain quasigroup.

The concept of orthogonality can be described very easily in algebraic language. Two quasigroups $Q(A)$, $Q(B)$ (i.e. quasigroups with operations A and B defined on the same set Q) are orthogonal if the system of equations $A(x,y) = a$, $B(x,y) = b$ has a unique solution for every pair of elements $a, b \in Q$.

There is significant interest in the investigation of quasigroups orthogonal to their parastrophes (for the definitions see below). However, in the past, the questions mainly considered have been some combinatorial ones which have arisen in connection with these investigations. We mention, for example, the Phelps papers (for example [6]) which are devoted to the study of the spectrum of α-orthogonal quasigroups, i.e. quasigroups A which are orthogonal to their parastrophe ${}^{\alpha}\!A$.

Special cases of such quasigroups were considered earlier in connection with other problems having purely algebraic character. For example, Stein

2000 Mathematics Subject Classification: 20N15, 20N05
Keywords: Quasigroup, parastrophe, orthogonality

[8] studied quasigroups with the identity $x \cdot xy = yx$. It is easy to see that such a quasigroup $Q(\cdot)$ is orthogonal to its parastrophe $Q(*)$, where $x * y = yx$.

Indeed, let us consider the system of equations $xy = a$, $yx = b$. If there exists a solution then, by the identity $x \cdot xy = yx$, it must be $xa = b$, whence we obtain x uniquely: $x = b/a$. The element y also is uniquely determined: $y = x\backslash a = (b/a)\backslash a$. In this way, if a solution exists, it is uniquely determined. It remains to show that the obtained values of x, y satisfy the given system of equations. We have $xy = (b/a)((b/a)\backslash a) = a$, because in the quasigroup $Q(\cdot)$ the basic identity $x(x\backslash y) = y$ is satisfied. Further we have $yx = [(b/a)\backslash a](b/a)$. Let $b/a = c$, $c\backslash a = d$, then $b = ca$, $a = cd$ and $yx = dc$. But $b = ca = c \cdot cd = dc$, by the Stein identity. Therefore $yx = dc = b$.

Thus, from the fact that the above identity holds in a quasigroup $Q(\cdot)$, it follows that a pair of orthogonal parastrophes is related to this quasigroup.

As will be shown below, other identities also have this property: that is, they imply the existence of orthogonal parastrophes. Such identities, in particular ones which are minimal in some sense, will be completely described. It will be shown that, up to a certain kind of equivalence, there are exactly seven types of such identities (including the Stein identity mentioned above).

Of course, it would be important to give a description of the seven types of quasigroup obtained , i.e. a description of loops isotopic to them. But a search for such a description of isotopic loops was unsuccessful because these quasigroups are defined by identities containing only two variables. Nevertheless, if we make the assumption that quasigroups satisfying the minimal identities are isotopic to groups, then we can obtain some additional information about such groups.

§0. Necessary preliminaries from the theory of quasigroups

1⁰. The set Q with one binary operation $(\cdot)$ is called a *quasigroup* if the equations $ax = b$, $ya = b$ have unique solutions for all $a, b \in Q$. A quasigroup with an *identity*, i.e. with an element e such that $ae = ea = a$ for all $a \in Q$, is called a *loop*. We shall denote quasigroups and loops by $Q(\cdot)$ or, if the operation is denoted as a function, say $A(a, b) = c$, by $Q(A)$. Also the operations $(\cdot)$ and A will be called quasigroups (or loops).

2⁰. A quasigroup $(\circ)$ is *isotopic* to a quasigroup $(\cdot)$, where $(\circ)$ and $(\cdot)$

are defined on the same set Q, if there exists a triplet $T = (\alpha, \beta, \gamma)$ of permutations of the set Q such that $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$. The relation of isotopy determines an equivalence on the set of all quasigroups defined on the set Q.

3⁰. Let $Q(\cdot)$ be a quasigroup, $L_a : x \to ax$, $R_a : x \to xa$. The mappings L_a, R_a are permutations of the set Q. The isotope $Q(\circ)$, where $x \circ y = R_a^{-1}x \cdot L_b^{-1}y$, of the quasigroup $Q(\cdot)$ is a loop with the identity ba.

4⁰. Let $Q(\cdot)$ be a quasigroup. The solution of the equation $ax = b$ is denoted by $x = a \backslash b$ and the solution of the equation $ya = b$ by $y = b/a$. The operations so defined are called *inverses* of $(\cdot)$, or, more precisely, the *right* (respectively, *left*) *division* for $(\cdot)$. The operations $(\ \backslash\ )$ and $(\ /\ )$ also define quasigroups. If a quasigroup is denoted by A, then the operations of right and left division will be denoted by A^{-1} and ${}^{-1}A$, respectively. The latter operations also have inverses: $(A^{-1})^{-1} = A$, ${}^{-1}(A^{-1})$ and ${}^{-1}({}^{-1}A) = A$, $({}^{-1}A)^{-1}$. Moreover, one can consider the operations $\left[{}^{-1}(A^{-1})\right]^{-1}$, ${}^{-1}\left[({}^{-1}A)^{-1}\right]$, but these operations are identical with A^*, where $A^*(x, y) = A(y, x)$.

The following equalities are equivalent:

$$A(x,y) = z \longleftrightarrow A^{-1}(x,z) = y \longleftrightarrow {}^{-1}A(z,y) = x \longleftrightarrow$$

$${}^{-1}(A^{-1})(y,z) = x \longleftrightarrow ({}^{-1}A)^{-1}(z,x) = y \longleftrightarrow A^*(y,x) = A(x,y).$$

In what follows, we shall use the following notations for cycles: $(1\,2) = s$, $(1\,3) = l$, $(2\,3) = r$. The cycles l, r generate the group S_3. Moreover, we have $rlr = lrl = s$. Thus $A^{-1} = {}^rA$, ${}^{-1}A = {}^lA$, $A^* = {}^sA$.

5⁰. The operations A, A^{-1}, ${}^{-1}A$, ${}^{-1}(A^{-1})$, $({}^{-1}A)^{-1}$, A^* are called the *parastrophes*[1] of the operation A. Parastrophes of a quasigroup A are frequently denoted by ${}^\sigma A$, where $\sigma \in S_3$ – the symmetric group of degree 3. More exactly, we have the equivalences:

$${}^\sigma A(x', y') = z' \longleftrightarrow A(x,y) = z,$$

[1]Editors' Note: These operations have also been called *conjugates* of the operation A by other authors, especially in the U.S.A. The word *parastrophe* dates back to 1915 and was used by Sade(1959)[14] and Artzy(1963)[9] before its adoption by Belousov. The name "conjugate" seems to have originated with Stein in the 1950s and was used in [8]. It has the disadvantage that its use in the present context conflicts with its more usual meaning in the context of group and loop theory for describing equivalence relative to inner automorphisms. [The reader should note that footnotes labelled $a, b, \ldots$ were in the original Russian text and in the English version sent to Keedwell by Belousov himself but footnotes numbered 1, 2, ... have been inserted by the Editors.]

where $(x', y', z') = \sigma(x, y, z)$. For example, ${}^{-1}(A^{-1}) = {}^{\alpha}A$, where $\alpha(x, y, z) = (y, z, x)$, i.e. $\alpha = (1\,2\,3)$.

The relations:

$${}^{\tau}({}^{\sigma}A) = {}^{\tau\sigma}A, \qquad B = {}^{\sigma}A \longleftrightarrow A = {}^{\sigma^{-1}}B$$

hold for the parastrophes.

6^0. The quasigroup operation $(\cdot)$ and its inverses ($\backslash$) and ($/$) are interconnected by the following identities:

$$x(x\backslash y) = y, \qquad x\backslash(xy) = y,$$

$$(y/x)x = y, \qquad (yx)/x = y.$$

The quasigroup $Q(\cdot)$ can be considered as a universal algebra $Q(\cdot, \backslash, /)$.

7^0. Two operations A and B (not necessarily quasigroup operations), defined on the set Q, are *orthogonal* if the system of equations

$$A(x, y) = a, \quad B(x, y) = b$$

is uniquely soluble for all $a, b \in Q$. We use the notation $A \perp B$ to express this. It is clear that $A \perp B$ implies $B \perp A$.

8^0. If $\bar{\varphi}$ is a mapping of the set Q^2 into itself, then there are two operations C, D such that $\bar{\varphi}(x, y) = (C(x, y), D(x, y))$. The mapping $\bar{\varphi}$ is a permutation if and only if $C \perp D$. The mapping $\bar{\varphi}$ is denoted by (C, D): $\bar{\varphi} = (C, D)$. The pair of operations C, D is uniquely determined by the mapping $\bar{\varphi}$. The following theorem is valid (see [2]): *if $A \perp B$, where A, B are quasigroup operations, and $\bar{\theta} = (A, B)$, then the inverse permutation $\bar{\theta}^{-1}$ has the form $\bar{\theta}^{-1} = (A', B')$, where A' and B' are also quasigroup operations.*

The identity permutation $\bar{\varepsilon}$ on Q^2 defines a pair F, E of operations on Q such that $F(a, b) = a$, $E(a, b) = b$ for all $a, b \in Q$: that is, $\bar{\varepsilon} = (F, E)$.

If $\bar{\varphi}$, $\bar{\psi}$ are two permutations on the set Q^2, then, by definition, $(A\bar{\varphi})\bar{\psi} = A(\bar{\varphi}\bar{\psi})$, and $(A, B)\bar{\varphi} = (A\bar{\varphi}, B\bar{\varphi})$ for all A, B, $\bar{\varphi}$, $\bar{\psi}$. Also, by definition, we have $(A\bar{\varphi})(x, y) = A(\bar{\varphi}(x, y))$.

9^0. A system $\Sigma = \{A_1, A_2, \ldots, A_k\}$ is called an *orthogonal system of quasigroups* (or, for brevity, an OSQ), if

1) $A_i \perp A_j$ for all $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$, and

2) $A_1 = F$, $A_2 = E$.

We remark that the operations $\{A_3, A_4, \ldots, A_k\}$ must be quasigroups because $A \perp E$ and $A \perp F$ imply that A is a quasigroup.

§1. Minimal identities and connections with orthogonalities

Let us consider the algebra $Q(\Sigma)$, where Σ is some system of quasigroup operations (quasigroups) defined on the set Q, and let $w_1 = w_2$ be an identity in $Q(\Sigma)$. We denote the number of free elements in the word w by $|w|$. Let $l = |w_1| + |w_2|$.

Now, we shall determine all nontrivial identities in $Q(\Sigma)$ having the minimal length l.

The identity $w_1 = w_2$ will be called *nontrivial*, if

$a)$ there is no subword of the form $A(u,u)$ (no "square"),

$b)$ there are no isolated free elements.

The first condition can be justified by remarking that $A(u,u)$ can be replaced by αu, i.e. by a unary operation, but we are considering only binary operations. The second condition is also reasonable: the identity $w_1 = w_2$ with an isolated element z (that is, in $w_1 = w_2$, the element z occurs only once) can be transformed to the form $w' = z$. Then, by fixing all elements in w', we get $w' = z_1$, $w' = z_2$, where z_1, z_2 are arbitrary elements of Q, i.e. $z_1 = z_2$, whence we obtain that Q has only one element.

Let us determine the minimal l. It is clear that $l \geqslant 3$. If $l = 3$, then the identity $w_1 = w_2$ is trivial, since the condition $a)$ or $b)$ is violated. If $l = 4$, then the identity $w_1 = w_2$ contains two free elements x, y exactly twice, otherwise condition $a)$ or $b)$ does not hold. In this case, the identity has the form $A(x,(B(x,y)) = y$ or $A(x,y) = B(x,y)$. [It appears that the identity might also have the form $A(B(x,y),x) = y$ for example but, by replacing A by its parastrophe A^* in this instance, we obtain $A^*(x,B(x,y)) = y$, which is an identity of the first type. Similar arguments can be used for other cases.] But these two identities are also trivial, because the first determines the right inverse operation $B = A^{-1}$ and the second implies that $A = B$.

Thus, the minimal length l of a nontrivial identity $w_1 = w_2$ must be equal to 5 (at least). If $l = 5$, the identity $w_1 = w_2$ contains only two free elements x, y. More than three free elements is not possible because the condition $b)$ would be violated. If the identity contains exactly three free elements x, y, z then, as is easy to see, the condition $b)$ is violated in that case too.

Therefore the identity $w_1 = w_2$ (if of length 5) contains only two free elements x, y and one of them, say x, is contained in it three times and the other twice, otherwise the condition $b)$ would be violated.

With the help of transformations to inverse operations where necessary, the identity $w_1 = w_2$ can be transformed to the form $w' = y$, where w'

contains the element x three times and y just once. The identity $w' = y$ might have, a priori, any one of the following forms:

1^0. $A(z_1, B(z_2, C(z_3, z_4))) = y$,

2^0. $A(z_1, B(C(z_2, z_3), z_4)) = y$,

3^0. $A(B(z_1, z_2), C(z_3, z_4)) = y$,

4^0. $A(B(C(z_1, z_2), z_3), z_4) = y$,

5^0. $A(B(z_1, C(z_2, z_3)), z_4) = y$.

We see immediately that the identity $w' = y$ cannot have the form 3^0 because, by condition a), one of z_1 or z_2 must be y and, likewise, one of z_3 or z_4 must be y but then y would occur in $w' = y$ three times, which contradicts the assumption that y occurs only twice.

Further we can remark that, with the aid of the transformation $K \to K^*$, we can transform the identities 2^0, 4^0 and 5^0 to the form 1^0. For example, in the case of 5^0 we get $A^*(z_4, B(z_1, C(z_2, z_3))) = y$. Next, let us consider the identity 1^0. It is evident that either z_3 or z_4 must be y. Let $z_4 = y$ (if $z_3 = y$, we replace C by C^*). The remaining elements are equal to x: $z_1 = z_2 = z_3 = x$. Thus, any nontrivial minimal identity of the algebra $Q(\Sigma)$ can be transformed into the form:

$$A(x, B(x, C(x, y))) = y. \tag{1.1}$$

For example, suppose that a nontrivial minimal identity of the form

$$A(B(x, y), C(x, y)) = x. \tag{1.2}$$

is given. We transform it to

$$^{-1}A(x, C(x, y)) = B(x, y).$$

Let $B(x, y) = z$, whence $y = B^{-1}(x, z)$. Consequently, we can write

$$^{-1}A(x, C(x, B^{-1}(x, z))) = z,$$

i.e. (1.2) is transformed to the form of (1.1).

Using multiplication of operations, the identity (1.1) can be rewritten in abbreviated form as

$$ABC = E, \tag{1.3}$$

where $E(x, y) = y$ for all $x, y \in Q$.

Remark 1. It is easy[2] to deduce that the following equalities are equivalent to (1.3):

$$BCA = E, \tag{1.4}$$
$$CAB = E, \tag{1.5}$$
$$C^{-1}B^{-1}A^{-1} = E, \tag{1.6}$$
$$B^{-1}A^{-1}C^{-1} = E, \tag{1.7}$$
$$A^{-1}C^{-1}B^{-1} = E. \tag{1.8}$$

Remark 2. If A, B, C are quasigroups satisfying (1.3) then the following conditions must be satisfied[3]:

$$B \neq A^{-1}, \qquad C \neq B^{-1}, \qquad A \neq C^{-1}. \tag{1.9}$$

Orthogonality. Π-quasigroups.

The orthogonality of operations is closely connected with minimal nontrivial identities. This assertion follows from the following lemma.

Lemma 1. *Let A, B be quasigroups. Then $A \perp B$ if and only if there exists a quasigroup K such that $KBA^{-1} = E$.*

Proof. Necessity. Let $A \perp B$, then $\bar{\theta} = (A, B)$ is a permutation. Consequently, $\bar{\theta}^{-1}$ also is a permutation. If $\bar{\theta}^{-1} = (C, D)$, then C and D are quasigroups (see 8^0 of §0) and

$$\bar{\theta}^{-1}\bar{\theta} = (C, D)(A, B) = (C(A, B), D(A, B)) = (F, E) = \bar{\varepsilon}$$

($\bar{\varepsilon}$ is the identity permutation of Q^2). Consequently, $C(A, B) = F$, i.e. $C(A(x, y), B(x, y)) = x$. Hence we get ${}^{-1}C(x, B(x, y)) = A(x, y) = z$. From this we can obtain y: namely, $y = A^{-1}(x, z)$ and in consequence ${}^{-1}C(x, B(x, A^{-1}(x, z))) = z$ or, briefly, ${}^{-1}CBA^{-1} = E$, i.e. $K = {}^{-1}C$.

Sufficiency. Let $KBA^{-1} = E$, where K is a quasigroup. We show that

$$x_0 = {}^{-1}K(a, b), \qquad y_0 = A^{-1}({}^{-1}K(a, b), a) \tag{1.10}$$

[2] Editors' Note: For example, $A(x, B(x, C(x, y))) = y \longrightarrow C(x, A(x, B(x, C(x, y))))$ $= C(x, y) \longrightarrow B(x, C(x, A(x, B(x, C(x, y))))) = B(x, C(x, y))$ or $B(x, C(x, A(x, z)) = z$, which is (1.4). Also $A(x, B(x, C(x, y))) = y \longrightarrow {}^{r}A(x, y) = B(x, C(x, y)) \longrightarrow C(x, y) =$ ${}^{r}B(x, {}^{r}A(x, y)) \longrightarrow {}^{r}C(x, {}^{r}B(x, {}^{r}A(x, y))) = y$, which is (1.6).

[3] Suppose that $B = A^{-1}$ in (1.4). Then $A(x, A^{-1}(x, C(x, y)) = y$. Let $A^{-1}(x, C(x, y) = z$. Then $A(x, z) = C(x, y)$ by definition of A^{-1}. But this contradicts $A(x, z) = y$ which is the given equality.

is a solution of the system of equations $A(x,y)=a,\ B(x,y)=b$.

Indeed, we have

$$\begin{aligned} A(x_0,y_0) &= A({}^{-1}K(a,b), A^{-1}({}^{-1}K(a,b),a)) \\ &= AA^{-1}({}^{-1}K(a,b),a) = E({}^{-1}K(a,b),a) = a, \\ B(x_0,y_0) &= B(x_0, A^{-1}(x_0,a)) = BA^{-1}(x_0,a) = d. \end{aligned}$$

Then

$$K(x_0,d) = K(x_0, BA^{-1}(x_0,a)) = KBA^{-1}(x_0,a) = E(x_0,a) = a. \quad (1.11)$$

But from the first equality of (1.10) it follows that $K(x_0,b)=a$. Comparing this with (1.11), we obtain $d=b$ so $B(x_0,y_0)=b$.

Thus, the solution exists. Finally, we show the uniqueness of this solution. Let x_1, y_1 be a second pair of solutions so that $A(x_1,y_1)=a$, $B(x_1,y_1)=b$. Then $B(x_1,y_1)=B(x_1,A^{-1}(x_1,a))=BA^{-1}(x_1,a)=b$. Hence it follows that $K(x_1, BA^{-1}(x_1,a)) = K(x_1,b)$, or

$$KBA^{-1}(x_1,a) = K(x_1,b),$$

so $a=K(x_1,b)$ since $KBA^{-1}=E$, whence $x_1={}^{-1}K(a,b)$.

This together with (1.10) implies that $x_1=x_0$. Now it follows easily that $y_1=y_0$. Indeed,$y_1=A^{-1}(x_1,a)=A^{-1}(x_0,a)=y_0$, because $A(x_0,y_0)=a$. Consequently $y_1=y_0$. □

Next, by writing the equality (1.3) in the form $AB(C^{-1})^{-1}=E$, we conclude that $B\perp C^{-1}$. From (1.4) and (1.5), we deduce that $C\perp A^{-1}$, $A\perp B^{-1}$ so we have the following lemma.

Lemma 2. *If, in the system $Q(\Sigma)$, the minimal nontrivial identity $ABC=E$ holds, then $A\perp B^{-1},\ B\perp C^{-1},\ C\perp A^{-1}$.* □

Minimal nontrivial identities in quasigroups.

Suppose that a quasigroup $Q(\cdot)$ is given. It can be considered as an algebra $Q(\cdot,\backslash,/),\ (\cdot)=A$. Of course, a minimal nontrivial identity can be satisfied in a single quasigroup too. It will take the form

$${}^{\alpha}A{}^{\beta}A{}^{\gamma}A = E,$$

where $\alpha,\beta,\gamma\in S_3$.

We make the following definition:

Definition 1. A quasigroup A is called a Π-*quasigroup of type* $[\alpha, \beta, \gamma]$ if it satisfies the identity ${}^{\alpha}\!A{}^{\beta}\!A{}^{\gamma}\!A = E$.

Remark 3. By virtue of the identities (1.4) – (1.8), the quasigroup A also has the following types: $[\beta, \gamma, \alpha]$, $[\gamma, \alpha, \beta]$, $[r\gamma, r\beta, r\alpha]$, $[r\beta, r\alpha, r\gamma]$, $[r\alpha, r\gamma, r\beta]$.

Remark 4. In view of (1.9), a Π-quasigroup A satisfies the following inequalities: ${}^{\beta}\!A \neq ({}^{\alpha}\!A)^{-1}$, ${}^{\gamma}\!A \neq ({}^{\beta}\!A)^{-1}$, ${}^{\alpha}\!A \neq ({}^{\gamma}\!A)^{-1}$ or ${}^{\beta}\!A \neq {}^{r\alpha}\!A$, ${}^{\gamma}\!A \neq {}^{r\beta}\!A$, ${}^{\alpha}\!A \neq {}^{r\gamma}\!A$: that is, we must have

$$\beta \neq r\alpha, \qquad \gamma \neq r\beta, \qquad \alpha \neq r\gamma. \tag{1.12}$$

By applying Lemma 2 to a Π-quasigroup A of type $[\alpha, \beta, \gamma]$, we obtain

$${}^{\alpha}\!A \perp {}^{r\beta}\!A, \qquad {}^{\beta}\!A \perp {}^{r\gamma}\!A, \qquad {}^{\gamma}\!A \perp {}^{r\alpha}\!A.$$

We shall use the notation

$$\alpha \perp \beta(A) \tag{1.13}$$

if ${}^{\alpha}\!A \perp {}^{\beta}\!A$. In what follows, we shall write $\alpha \perp \beta$ instead of (1.13) if the relevant quasigroup operation A is clear from the context. Thus a Π-quasigroup A of type $[\alpha, \beta, \gamma]$ will satisfy the following orthogonality relations:

$$\alpha \perp r\beta, \qquad \beta \perp r\gamma, \qquad \gamma \perp r\alpha.$$

In the sequel, we shall write $\alpha \perp \beta(\sigma)$ instead of $\alpha \perp \beta({}^{\sigma}\!A)$. It is evident that

$$\alpha \perp \beta(\sigma) \longleftrightarrow \alpha\sigma \perp \beta\sigma.$$

Indeed, $\alpha \perp \beta(\sigma)$ means that ${}^{\alpha}({}^{\sigma}\!A) \perp {}^{\beta}({}^{\sigma}\!A)$ or ${}^{\alpha\sigma}\!A \perp {}^{\beta\sigma}\!A$, that is, $\alpha\sigma \perp \beta\sigma$.

Parastrophic equivalence[4].

Let us consider the following two transformations[5] of the type of a Π-quasigroup:

$$f[\alpha, \beta, \gamma] = [\beta, \gamma, \alpha], \qquad h[\alpha, \beta, \gamma] = [r\gamma, r\beta, r\alpha]. \tag{1.14}$$

[4]Both the original Russian text and (in some places) Belousov's English translation of it have been modified in this section particularly so as to make the meaning clear.

[5]These are admissible because of Remark 3.

It is easy to see that $f^3 = 1,\ h^2 = 1$. Moreover, we have $fh = hf^2$. Indeed,

$$fh[\alpha,\beta,\gamma] = f[r\gamma, r\beta, r\alpha] = [r\beta, r\alpha, r\gamma] = h[\gamma,\alpha,\beta] = hf^2[\alpha,\beta,\gamma].$$

Thus, the transformations f and h generate the group

$$S^0 = \{1, f, f^2, h, fh, f^2h\},$$

which is isomorphic to S_3.

We remark now that, if A has the type $[\alpha,\beta,\gamma]$, then ${}^{\sigma}\!A$ has the type $[\alpha\sigma^{-1}, \beta\sigma^{-1}, \gamma\sigma^{-1}]$. This fact suggests making the next definition which has the effect of defining a transformation of the type $[\alpha,\beta,\gamma]$:

$$[\alpha,\beta,\gamma]\theta = [\alpha\theta, \beta\theta, \gamma\theta]. \tag{1.15}$$

Thus, the preceding remark implies that ${}^{\theta}\!A$ has the type $[\alpha,\beta,\gamma]$, when A has the type $[\alpha\theta,\beta\theta,\gamma\theta]$. The equality (1.15) implies also that if some minimal nontrivial identity is satisfied in $Q(A)$, then some minimal nontrivial identity holds for each parastrophe also which is related to the preceding one by (1.15). If $T = [\alpha,\beta,\gamma]$ is the type of a quasigroup A, then we can apply the transformations (1.14) and (1.15) to T to obtain a relation of the form $T' = (gT)\theta$, where $g \in S^0$, $\theta \in S_3$. It is clear that $(gT)\theta = g(T\theta)$, therefore we shall write $T' = gT\theta$.

Definition 2. Π-quasigroups B and A are called *parastrophically equivalent* if their types T' and T are connected by a relation of the form $T' = gT\theta$ for some $g \in S^0$ and $\theta \in S_3$. Notation: $T' \sim T$ and $B \sim A$. We shall also say that the types T' and T are *parastrophically equivalent.*

It is easy to see that parastrophic equivalence is in fact an equivalence relation.

Remark to Definition 2. Parastrophic equivalence means that if some minimal identity of type T is satisfied in a Π-quasigroup A, then a well-defined minimal nontrivial identity of type $T' = gT\theta$ is satisfied in its parastrophe.[6]

To determine the equivalence classes under parastrophic equivalence, we look for representatives of these classes. Because $T = [\alpha,\beta,\gamma] =$

[6]An earlier investigation of this idea was made by A. Sade. See [14] or page 66 of [4]. The concept was also defined (using the name *conjugate-equivalent*) by T. Evans, see page 46 of [13].

$[1, \beta\alpha^{-1}, \gamma\alpha^{-1}]\alpha$, it follows that $T \sim [1, \sigma, \tau]$, where $\sigma = \beta\alpha^{-1}$, $\tau = \gamma\alpha^{-1}$. Thus the class representatives should have the form $[1, \sigma, \tau]$. Moreover, the conditions (1.12) must be satisfied, namely:

$$\sigma \neq r1, \quad \tau \neq r\sigma, \quad 1 \neq r\tau,$$

That is,

$$\sigma \neq r, \quad \tau \neq r, \quad \tau \neq r\sigma. \tag{1.16}$$

First, we consider the case $\sigma = 1$, i.e. we consider the type of the form $[1, 1, \tau]$. The conditions (1.16) become

$$1 \neq r, \quad \tau \neq r, \quad \tau \neq r1,$$

so they reduce to $\tau \neq r$. Thus, we can choose the types

$$T_1 = [1, 1, 1], \quad T_2 = [1, 1, l], \quad T_3 = [1, 1, rl], \quad T_4 = [1, 1, lr], \quad T_5 = [1, 1, s]$$

as class representatives under parastrophic equivalence.

Now let us consider the case when $\sigma \neq 1$, i.e. the type $[1, \sigma, \tau]$. As a consequence of condition (1.16), we also have:

$$\sigma \neq 1, \quad \tau \neq 1, \quad \sigma \neq \tau. \tag{1.17}$$

Indeed, suppose that $\tau = 1$, $T = [1, \sigma, 1]$. But then $f^2T = [1, 1, \sigma]$, so $T \sim T_i$, where i is one of the numbers $2, 3, 4, 5$. If $\sigma = \tau$, then $T = [1, \sigma, \sigma]$, whence $fT = [\sigma, \sigma, 1] = [1, 1, \sigma^{-1}]\sigma$ and therefore $T = f^2[1, 1, \sigma^{-1}]\sigma$ so $T \sim [1, 1, \sigma^{-1}]$. That is, $T \sim T_i$. Taking into account conditions (1.16) and $(1, 17)$, the following representatives for the equivalence classes are possible:

$$\begin{aligned} &T_6 = [1, l, lr], && T_7 = [1, l, s], && T_8 = [1, rl, lr], \\ &T_9 = [1, rl, s], && T_{10} = [1, lr, l], && T_{11} = [1, lr, rl], \\ &T_{12} = [1, s, l], && T_{13} = [1, s, rl]. \end{aligned}$$

We shall show that

$$T_{13} \sim T_{10} \sim T_7,$$
$$T_{12} \sim T_9 \sim T_6.$$

Indeed, we have

$$hT_{10} = h[1, lr, l] = [rf, rlr, r] = [1, lrllr, s]rl = [1, l, s]rl = T_7rl,$$
$$fT_{13} = f[1, s, rl] = [s, rl, 1] = [1, rls, s]s = [1, rllrl, s]s = [1, l, s]s = T_7s.$$

Consequently, $T_{10} \sim T_7$ and $T_{13} \sim T_7$.

Furthermore, we have

$$fT_9 = f[1, rl, s] = [rl, s, 1] = [1, slr, lr]rl = [1, l, lr]rl = T_6 rl,$$
$$fT_{12} = f[1, s, l] = [s, l, 1] = [1, ls, s]s = [1, rl, s] = T_9 s.$$

Therefore, $T_9 \sim T_6$ and $T_{12} \sim T_9$.

We have also the equivalences:

$$T_5 \sim T_2, \quad T_4 \sim T_3. \tag{1.18}$$

Indeed,

$$fhT_5 = fh[1, 1, s] = f[rs, r, r] = [r, r, rs] = [1, 1, rsr]r = [1, 1, l]r = T_2 r,$$

$$fhT_4 = fh[1, 1, lr] = f[rlr, r, r] = [r, r, s] = [1, 1, sr]r = [1, 1, rl]r = T_3 r,$$

We shall use the second equality again later, so we write

$$fhT_4 = T_3 r. \tag{1.19}$$

This proves the equivalences (1.18), so finally only the following class representatives for parastrophic equivalence remain:

$$T_1,\ T_2,\ T_4,\ T_6,\ T_8,\ T_{10},\ T_{11}\ . \tag{1.20}$$

We shall show that the seven types listed in (1.20) are pairwise parastrophically non-equivalent.

a) T_8 and T_{11} are parastrophically non-equivalent to any other type. This follows from the following relations:

$$fT_8 = T_8 rl, \quad f^2T_8 = T_8 lr, \quad hT_8 = T_8 s, \quad fhT_8 = T_8 l, \quad f^2hT_8 = T_8 r,$$

$$fT_{11} = T_{11} lr,\ \ f^2T_{11} = T_{11} rl,\ \ hT_{11} = T_{11} l,\ \ fhT_{11} = T_{11} s,\ \ f^2hT_{11} = T_{11} r\,. \tag{1.21}$$

Thus, any type $T' \neq T_8$ which is parastrophically equivalent to T_8 has the form $gT_8\alpha = (T_8\beta)\alpha = T_8\gamma = [\gamma, \varphi, \psi]$, where $\gamma \neq 1$, i.e. none of the types (1.20) is equivalent to T_8 other than T_8 itself. An analogous assertion is valid for T_{11}.

b) We shall use the following trivial observations. *If all the components of T are identical and $T' \sim T$, then all the components of T' also are identical.*

If two components of T are identical and $T' \sim T$, then two components of T' also are identical.

From this it follows at once that none of the types (1.20) is parastrophically equivalent to T_1 (except T_1 itself).

c) From *a*) and *b*) it follows that T_6 and T_7 and, likewise, T_2 and T_4, are parastrophically non-equivalent pairs.

The types T_6 and T_7 cannot be parastrophically equivalent to T_2 and T_4 because T_2 and T_4 have two identical components, while T_6 and T_7 have their components all different.

We shall show that $T_2 \nsim T_4$. For this purpose, we determine gT_2, where g runs through the whole group S^0:

$$gT_2 = [1,1,l],\ [1,l,1],\ [l,1,1],\ [rl,r,r],\ [r,r,rl],\ [r,rl,r]. \tag{1.22}$$

Now we determine $T_4\alpha$, where α runs through the whole group S_3:

$$T_4\alpha = [1,1,lr],\ [r,r,l],\ [l,l,s],\ [rl,rl,1],\ [lr,lr,rl],\ [s,s,r]. \tag{1.23}$$

From (1.22) and (1.23), we conclude that $T_2 \nsim T_4$. Similarly, we can prove that $T_6 \nsim T_{10}$.

Therefore, we have seven classes for parastrophic equivalence, the representatives of which are listed in (1.20). We determine the identity defined by each of these types and, in each case, we obtain the equivalent identity when this identity is written in terms of the basic quasigroup operation A alone.

1) Type $T_1 = [1,1,1]$. The corresponding identity is determined by the equality $AAA = E$. If $A = (\cdot)$, then it is the following identity

$$x(x \cdot xy) = y.$$

2) Type $T_2 = [1,1,l]$. The corresponding identity is determined by the equality $AA\,{}^lA = E$. If $A = (\cdot)$, then ${}^lA = (\,/\,)$ and the identity takes the form

$$x(x(x/y)) = y. \tag{1.24}$$

Let $x/y = z$, whence $x = zy$. Consequently (1.24) can be transformed into the following identity:

$$(zy)(zy \cdot z) = y.$$

Multiplying on the left by z and replacing zy by x, we obtain

$$z[(zy)(zy \cdot z)] = zy, \tag{1.25}$$

$$\text{or} \qquad z(x \cdot xz) = x.$$

Thus, an identity of type T_2 is equivalent to (1.25).

3) Type $T_4 = [1, 1, lr]$. The corresponding identity is determined by the equality $AA\,{}^{lr}\!A = E$. Let $A = (\cdot)$, then ${}^{lr}\!A(x, y) = y/x$. Consequently, the identity has the form

$$x(x(y/x)) = y. \tag{1.26}$$

Let $y/x = z$, then $y = zx$. So the identity (1.26) can be transformed into the equality $x \cdot xz = zx$. This is Stein's identity (or, in the terminology of [4], Stein's first law).

4) Type $T_6 = [1, l, lr]$. To this type corresponds the equality $A\,{}^{l}\!A\,{}^{lr}\!A = E$. If $A = (\cdot)$, then ${}^{l}\!A = (\,/\,)$, ${}^{lr}\!A(x, y) = y/x$, and consequently T_6 determines the identity

$$x(x/(y/x)) = y. \tag{1.27}$$

Let $y/x = u$, $x/u = v$. Then $y = ux$, $x = vu$, whence $y = u \cdot vu$. The identity (1.27) becomes transformed into the form

$$vu \cdot v = u \cdot vu.$$

5) Type $T_{10} = [1, lr, l]$. We consider a type parastrophically equivalent to T_{10}: namely, $fT_{10} = [lr, l, 1]$. To this type corresponds the equality ${}^{lr}\!A\,{}^{l}\!AA = E$. If $A = (\cdot)$, then ${}^{l}\!A = (\,/\,)$, ${}^{lr}\!A(x, y) = y/x$ and the corresponding identity has the form:

$$(x/xy)/x = y,$$

whence it follows that $yx = x/xy$ and so

$$yx \cdot xy = x.$$

This is precisely Stein's third law (see [4]).

6) Type $T_8 = [1, rl, lr]$. The corresponding identity is determined by the equality $A\,{}^{rl}\!A\,{}^{lr}\!A = E$. If $A = (\cdot)$, then ${}^{lr}\!A(x, y) = y/x$, ${}^{rl}\!A(x, y) = y\backslash x$. Consequently, to the type T_8 corresponds the identity:

$$x((y/x)\backslash x) = y. \tag{1.28}$$

Let $y/x = u$, $u\backslash x = v$. Then $y = ux$, $x = uv$, whence $y = u \cdot uv$, and the identity (1.28) has the form

$$uv \cdot v = u \cdot uv.$$

In the terminology of [4], this is Schröder's first law.

Finally, we consider

7) Type $T_{11} = [1, lr, rl]$. The corresponding equality is $A^{lr}A^{rl}A = E$, and the corresponding identity has the form

$$x((y\backslash x)/x) = y. \tag{1.29}$$

Let $y\backslash x = u,\ u/x = v$. Then $x = yu,\ u = vx$. Consequently, the identity (1.29) takes the form $xv = y$. Combining the last equality with the others, we get

$$x = yu = xv \cdot vx,$$

i.e. (1.29) is equivalent to the identity

$$xv \cdot vx = x,$$

which is Schröder's second law (see [4]).

We summarize the results obtained in the following table

No.	Type	Identity	Derived form	Note
1.	$T_1 = [1, 1, 1]$	$x(x \cdot xy) = y$	$x(x \cdot xy) = y$	
2.	$T_2 = [1, 1, l]$	$x(x(x/y)) = y$	$x(y \cdot yx) = y$	
3.	$T_4 = [1, 1, lr]$	$x(x(y/x)) = y$	$x \cdot xy = yx$	Stein's 1st law
4.	$T_6 = [1, l, lr]$	$x(x/(y/x)) = y$	$xy \cdot x = y \cdot xy$	Stein's 2nd law[7]
5.	$T_{10} = [1, lr, l]$	$(x/xy)/x = y$	$xy \cdot yx = y$	Stein's 3nd law
6.	$T_8 = [1, rl, lr]$	$x((y/x)\backslash x) = y$	$xy \cdot y = x \cdot xy$	Schröder's 1st law
7.	$T_{11} = [1, lr, rl]$	$x((y\backslash x)/x) = y$	$yx \cdot xy = y$	Schröder's 2nd law

Table 1.

Thus, we have proved

Theorem 1. *Any minimal nontrivial identity in a quasigroup is parastrophically equivalent to one of the identity types listed in* (1.20). □

[7]Editors' Remark: Stein's 2nd law is misquoted in [4] because of a compositing error.

Editors Comments: The same result[8] was obtained later (1989) by F. E. Bennett [10] working independently and using an earlier closely-related theorem due to T. Evans [13]. Bennett also investigated the spectrum of orders for which a quasigroup satisfying each particular one of the seven identity types exists. The results obtained by Bennett, Evans and other authors are summarized in Chapter 4, Section 36 of [12]. However, Belousov's work on this topic and on Quasigroups in general is not mentioned in that summary. It is also the case that Belousov seemed unaware of the work of Evans which is closely related to his own and predates it. In fact, in the 1970s and 1980s, Congressus Numerantium was not available in USSR and Belousov's published booklet was not available in Canada.

Example. Consider the minimal nontrivial identity

$$(x/y)\backslash(y\backslash x) = x, \tag{1.30}$$

or in alternative notation

$$A^{-1}({}^{-1}A(x,y), A^{-1}(y,x)) = x. \tag{1.31}$$

We transform the identity (1.31) to the form $ABC = E$. We have

$$A^{-1}({}^{-1}A(x,y), (A^{-1})^*(x,y)) = x,$$

whence

$${}^{-1}(A^{-1})(x, (A^{-1})^*(x,y)) = {}^{-1}A(x,y). \tag{1.32}$$

Let ${}^{-1}A(x,y) = z$. Then $y = ({}^{-1}A)^{-1}(x,z)$. Consequently, from (1.32) we obtain

$${}^{-1}(A^{-1})(x, (A^{-1})^*(x, ({}^{-1}A)^{-1}(x,z)) = z,$$

or

$${}^{lr}A(x, {}^{sr}A(x, {}^{rl}A(x,z))) = z,$$

$${}^{lr}A\,{}^{sr}A\,{}^{rl}A = E,$$

i.e. Our identity has type $T = [lr, sr, rl] = [lr, rl, rl]$. We transform T:

$$\begin{aligned} T &= [lr, rl, rl] = [lrlr, 1, 1]rl = [rl, 1, 1]rl \\ &= f^2[1, 1, rl]rl = f^2 T_3 rl. \end{aligned}$$

[8]Bennett's list consists of T_4, T_8, T_{10} T_{11} and the duals of T_1, T_6 and T_5 (equivalent to T_2).

But, $T_3 = fhT_4r$ (as was proved in (1.19)), whence

$$T = f^2(fhT_4r)rl = hT_4l.$$

Consequently, T is parastrophically equivalent to T_4, and the identity (1.30) is equivalent to an identity of type T_4, i.e. to Stein's identity for ${}^lA = (\,/\,)$. Indeed, let $(\circ) = (\,/\,)$, so that $x/y = x \circ y$. From (1.30), it follows that $(x \circ y)\backslash(y\backslash x) = x$,

$$\begin{aligned} (x \circ y)x &= y\backslash x, \\ y((x \circ y)x) &= x. \end{aligned} \tag{1.33}$$

Let $(x \circ y)x = z$. Then $x \circ y = z/x = z \circ x$ and from (1.33) we obtain

$$x/((x \circ y)x) = y, \qquad x \circ ((x \circ y)x) = y.$$

Finally, $x \circ y = z \circ x$ and $x \circ z = y$ imply the Stein law $x \circ (x \circ z) = z \circ x$.

Remarks. 1) The names of the identities (in Table 1) originate from Sade's paper [7]. In this paper a list of 63 identities, basic identities and generalized identities, is given. The identities of types T_4, T_6, T_8, T_{10}, T_{11} are given the numbers $12, 13, 14, 16, 15$ respectively in [7] and these names are cited in the monograph of Dénes and Keedwell [4].

2) In Norton and Stein's paper [5], idempotent quasigroups satisfying the identity T_{11} $(xy \cdot yx = x)$ are considered. These authors obtained a condition on the order which holds for a quasigroup of this type and also one for the finite idempotent quasigroups which satisfy the identity T_{10} $(xy \cdot yx = y)$. Furthermore, they gave examples of such quasigroups: namely, the ones which are defined by the following tables:

	a	b	c	d
a	a	c	d	b
b	d	b	a	c
c	b	d	c	a
d	c	a	b	d

Table 2.

	a	b	c	d	e
a	a	c	d	e	b
b	d	b	e	c	a
c	e	a	c	b	d
d	b	e	a	d	c
e	c	d	b	a	e

Table 3.

3) Quasigroups satisfying the identity T_4 $(x \cdot xy = yx)$ are considered in the paper [8] by Stein. The following example is given of a Stein quasigroup (i.e. of a quasigroup satisfying Stein's first law T_4). The epithet "Stein quasigroup" was given in [3] for brevity.

	a	b	c	d
a	a	c	d	b
b	d	b	a	c
c	b	d	c	a
d	c	a	b	d

Table 4.

As can be seen, the quasigroups given in Table 2 and Table 4 are identical, i.e. they satisfy both of the identities T_4 and T_{11}: $x \cdot xy = yx$, $xy \cdot yx = x$. They also satisfy the identity $xy \cdot x = y$, called the identity of semisymmetry in Sade's terminology [7], who devoted a series of papers to them.

4) In Stein's paper [8] the identities T_6 $(xy \cdot x = y \cdot xy)$ and T_8 $(xy \cdot y = x \cdot xy)$ are mentioned and examples of such quasigroups are constructed.

5) Minimal identities occur in the study of paratopy of OSQ (see 9^0 of § 0). Let $\Sigma = \{A_i\}$, $i = 1, 2, \ldots, k$, be an OSQ. A permutation $\bar{\theta}$ of the set Q^2 is called a *paratopy* of the OSQ Σ if the system $\{A_1\bar{\theta}, A_2\bar{\theta}, \ldots, A_k\bar{\theta}\}$ is identical to Σ. For $k = 4$ (for $k \leqslant 3$ we have trivial cases) an OSQ admitting at least one paratopy can be one of nine types [2]. These systems take the form $\{F, E, A, A'\}$, where A' can be expressed in terms of A. For example, $A' = A^*$, $A' = {}^{-1}(A^{-1})$, $A' = ({}^{-1}A)^{-1}A$, and so on. In seven of these cases it has been shown that the quasigroup must satisfy some minimal identity. Two of these identities are T_1 and T_{10}, while the other five are parastrophically equivalent to identities of type T_1, T_{10} and T_6.

Orthogonality and parastrophy.

In the preceding Section, we showed that, if $Q(\cdot)$ is a Π-quasigroup, $(\cdot) = A$, of type $[\alpha, \beta, \gamma]$, then the following parastrophes are pairwise orthogonal

$$\alpha \perp r\beta, \qquad \beta \perp r\gamma, \qquad \gamma \perp r\alpha. \tag{1.34}$$

In order to describe all mutually orthogonal parastrophes of a quasigroup of one of the seven types mentioned above, we first look at some properties of orthogonality of parastrophes. We recall that $\alpha \perp \beta(\sigma)$ means that $\alpha \perp \beta({}^{\sigma}\!A)$.

1) If $\alpha \perp \beta$, then $s\alpha \perp s\beta$. Indeed, this follows from the more common assertion: *If $A \perp B$, then $A^* \perp B^*$ and conversely.* The latter statement follows from the fact that the system of equations $A(x, y) = a$, $B(x, y) = b$ is equivalent to the system of equations $A^*(y, x) = a$, $B^*(y, x) = b$.

2) If $\alpha\perp\beta$, then $1\perp\beta\alpha^{-1}(\alpha)$, $1\perp\alpha\beta^{-1}(\beta)$. This follows from the fact proved above: $\alpha\perp\beta(\sigma)$ *is equivalent to* $\alpha\sigma\perp\beta\sigma$.

We return to the discussion of orthogonality of parastrophes of Π-quasigroups. By property 1), the following orthogonalities follow from (1.34):

$$s\alpha\perp sr\beta, \quad s\beta\perp sr\gamma, \quad s\gamma\perp sr\alpha,$$

or

$$s\alpha\perp rl\beta, \quad s\beta\perp rl\gamma, \quad s\gamma\perp rl\alpha. \tag{1.35}$$

Applying property 2) for $T=[\alpha,\beta,\gamma]$ to the orthogonalities (1.34) and (1.35), we obtain

$$\begin{array}{lll} 1\perp r\beta\alpha^{-1}(\alpha), & 1\perp r\gamma\beta^{-1}(\beta), & 1\perp r\alpha\gamma^{-1}(\gamma),\\ 1\perp\alpha\beta^{-1}r(r\beta), & 1\perp\beta\gamma^{-1}r(r\gamma), & 1\perp\gamma\alpha^{-1}r(r\alpha),\\ 1\perp rl\beta\alpha^{-1}s(s\alpha), & 1\perp rl\gamma\beta^{-1}s(s\beta), & 1\perp rl\alpha\gamma^{-1}s(s\gamma),\\ 1\perp s\alpha\beta^{-1}lr(rl\beta), & 1\perp s\beta\gamma^{-1}lr(rl\gamma), & 1\perp s\gamma\alpha^{-1}lr(rl\alpha). \end{array} \tag{1.36}$$

In particular, for the case $\alpha=1$, we get

$$\begin{array}{lll} 1\perp r\beta(1), & 1\perp r\gamma\beta^{-1}(\beta), & 1\perp r\gamma^{-1}(\gamma),\\ 1\perp\beta^{-1}r(r\beta), & 1\perp\beta\gamma^{-1}r(r\gamma), & 1\perp\gamma r(r),\\ 1\perp rl\beta s(s), & 1\perp rl\gamma\beta^{-1}s(s\beta), & 1\perp rl\gamma^{-1}s(s\gamma),\\ 1\perp s\beta^{-1}lr(rl\beta), & 1\perp s\beta\gamma^{-1}lr(rl\gamma), & 1\perp s\gamma lr(rl). \end{array} \tag{1.37}$$

Applying the relations (1.37) to Π-quasigroups of the types given in Table 1 we obtain the results presented below.

No.	Type	Orthogonality
1.	$T_1=[1,1,1]$	$1\perp r(1,r)$, $1\perp l(rl,s)$
2.	$T_2=[1,1,l]$	$1\perp r(1,r)$, $1\perp l(rl,s)$, $1\perp rl(1,r,rl,l)$, $1\perp lr(r,lr,rl,s)$
3.	$T_4=[1,1,lr]$	$1\perp r(1,r,l,rl)$, $1\perp l(r,rl,lr,s)$, $1\perp s(1,s)$
4.	$T_6=[1,l,lr]$	$1\perp r(l,rl)$, $1\perp l(r,lr)$, $1\perp rl(1,r,lr,s)$, $1\perp lr(1,l,rl,s)$
5.	$T_{10}=[1,rl,l]$	$1\perp rl(l,rl)$, $1\perp lr(lr,r)$, $1\perp s(1,s)$
6.	$T_8=[1,rl,lr]$	$1\perp r(1,r,l,rl,lr,s)$, $1\perp l(1,l,r,rl,lr,s)$
7.	$T_{11}=[1,lr,rl]$	$1\perp s(1,r,l,rl,lr,s)$

Table 5.

Here, for the sake of brevity, we have written $\alpha\perp\theta(\beta_1, \beta_2, \dots, \beta_k)$ instead of $\alpha\perp\theta(\beta_1)$, $\alpha\perp\theta(\beta_2), \dots, \alpha\perp\theta(\beta_k)$.[9]

If we restrict ourselves to parastrophes of the basic operation, i.e. to orthogonalities of the form $\alpha\perp\beta$, then (taking into account the equivalence $\alpha\perp\beta(\theta) \longleftrightarrow \alpha\theta\perp\beta\theta$), we obtain the following table:[10]

No.	Type	Orthogonality
1.	$T_1 = [1, 1, 1]$	$1\perp r,\ rl\perp s$
2.	$T_2 = [1, 1, l]$	$1\perp r,\ 1\perp rl,\ r\perp s,\ rl\perp s,\ rl\perp lr,\ l\perp r$
3.	$T_4 = [1, 1, lr]$	$1\perp r,\ 1\perp s,\ l\perp rl,\ rl\perp s,\ r\perp lr$
4.	$T_6 = [1, l, lr]$	$1\perp lr,\ 1\perp rl,\ r\perp lr,\ l\perp rl,\ r\perp s,\ l\perp s$
5.	$T_{10} = [1, rl, l]$	$1\perp s,\ l\perp r,\ rl\perp lr$
6.	$T_8 = [1, rl, lr]$	$1\perp r,\ 1\perp l,\ r\perp lr,\ l\perp rl,\ s\perp rl,\ s\perp lr$
7.	$T_{11} = [1, lr, rl]$	$1\perp s,\ r\perp rl,\ l\perp lr$

Table 6.

We end this Section with some remarks.

Remark 1. Identities of type T_8 and T_{11} are invariant under parastrophy, i.e. these identities hold in any parastrophe. Indeed, from (1.21) it follows that, for an arbitrary parastrophe σ, there exists a transformation $g \in S^0$, such that $gT_8 = T_8\sigma$. From the remark after Definition 2 it follows that, if the identity T_8 holds in $Q(A)$, then the identity $gT_8\sigma^{-1}$ holds in $Q({}^\sigma A)$: that is, by virtue of (1.21), T_8 holds in $Q({}^\sigma A)$ for every $\sigma \in S_3$. The same assertion holds for an identity of type T_{11}.

These facts can be proved directly. Consider an identity of type T_{11}. That is, one which is equivalent to

$$xy \cdot yx = x. \tag{1.38}$$

Let $xy = u$, $yx = v$, then $uv = x$. From these equalities it follows that $x\backslash u = y$, $y\backslash v = x$, $u\backslash x = v$. Hence $x = y\backslash v = (x\backslash u)(u\backslash x)$, that is, $(x\backslash u)\backslash(u\backslash x) = x$. From the same relations $xy = u$, $yx = v$, $uv = x$ it follows

[9] In a paper of M. E. Stickel and H. Zhang[15], these authors claimed incorrectly that the following results from Belousov's Table 5 were new: For a quasigroup of type T_{10}, $1\perp rl(l, rl)$ (re-proved by Stickel, 1994) and, for a quasigroup of type T_6, $1\perp l(r, lr)$ (stated in the paper just mentioned). (In the notation of Stickel and Zhang, "a parastrophe of $QG4$ satisfies $QG2$ and a parastrophe of $QG7$ satisfies $QG1$.")

[10] Table 3 of Stickel and Zhang's 1994 paper[15] (which was obtained with the aid of a computer) contains the same information as Belousov's Table 6 below.

at once that $u/y = x$, $v/x = y$, $x/v = u$, whence $x = u/y = (x/v)/(v/x)$, i.e.

$$(x/v)/(v/x) = x. \tag{1.39}$$

So the identity T_{11} holds both in $Q(\,/\,)$ and in $Q(\,\backslash\,)$, and hence it holds in the other parastrophes too.

Furthermore, it follows from the above that the identities (1.38) and (1.39) are not only parastrophically equivalent but they are equivalent in the usual sense as well.

Remark 2. **1**) Quasigroups satisfying any one of the identities T_4, T_{10}, T_{11} are anti-commutative (that is, the equality $ab = ba$ holds if and only if $a = b$).

We begin with the identity T_{10}. Let $ab = ba = c$. Then $c^2 = ab \cdot ba = b$ and $c^2 = ba \cdot ab = a$. Consequently, $a = b$. Similarly, we can show this fact for T_{11}.

In the case of T_4 we have $ac = a \cdot ab = ba = c$, $bc = b \cdot ba = ab = c$, i.e. $ac = bc$, whence $a = b$.

2) Quasigroups satisfying any one of the identities T_4, T_6, T_8 are idempotent. Indeed, for Stein's law (T_4) idempotency follows directly by putting $x = y$. This gives $x \cdot x^2 = x^2 = xx$, whence $x^2 = x$. In the identity T_6 $(xy \cdot x = y \cdot xy)$, let $y = e_x$, where $xe_x = x$.[11] Then $xe_x \cdot x = e_x \cdot xe_x$ or $xx = e_x x$: that is, $x = e_x$. Then $x^2 = xx = xe_x = x$. Finally, putting $y = e_x$ in T_8 $(xy \cdot y = x \cdot xy)$, we obtain $x = x^2$.

§2. Π-quasigroups.

Π-quasigroups are defined by identities containing only two free variables so we should not expect to obtain their complete description: that is, the description of all loops which are isotopic to these quasigroups.

First, the following question arises: "For which values of n (where n is a natural number) do there exist Π-quasigroups of type $[\alpha, \beta, \gamma]$?" This question is combinatorial in character and several investigations concerning it have been made: for example, the papers of Phelps who considered orthogonality of the form $A \perp {}^{\sigma}\!A$, where ${}^{\sigma}\!A$ is a parastrophe of A. Such an orthogonality is connected with the equality $A' A\, {}^{\tau\sigma}\!A = E$ or $A' A\, {}^{\tau}\!A = E$ (i.e. A and τ determine A'). Therefore, it leads to a class of quasigroups

[11] Editors' Note: The element e_x, so defined, is called the *right local identity* for the element x.

more general than the class of Π-quasigroups. In [6] the spectrum[12] of A is considered, i.e. the collection of all positive integers n for which there exists $A \perp^{\sigma} A$.

Here we consider a different question. It is known [3] that if a Stein quasigroup (in our classification a Π-quasigroup of type T_4) is isotopic to a group, then that group is metabelian. We are interested in analogous questions for other Π-quasigroups: that is, we shall investigate Π-quasigroups isotopic to groups. We shall consider each type separately.

1) Π-quasigroups $A = (\cdot)$ of type $T_1 = [1, 1, 1]$.

In such a quasigroup, the following identity is satisfied:

$$x(x \cdot xy) = y. \tag{2.1}$$

Let $x + y = R_a^{-1}x \cdot L_b^{-1}y$, so that $Q(+)$ is a loop with $0 = ba$ as identity element. For the sake of brevity, let $R_a = R,\ L_b = L$. Then $xy = Rx + Ly$, and replacing the operation $(\cdot)$ by $(+)$ in (2.1), we get

$$Rx + L(Rx + L(Rx + Ly)) = y,$$

$$\text{or} \qquad x + L(x + L(x + Ly)) = y. \tag{2.2}$$

By putting $x = 0$, we deduce that $L^3 = 1$.[13]

From (2.2) we deduce that

$$x + L(x + Ly) = L^{-1}(-x + y),$$

whence

$$x + L(x + y) = L^{-1}(-x + L^{-1}y). \tag{2.3}$$

For a suitable choice of a, b we can make $L^{-1}0 = 0$. Indeed, $L^{-1}0 = 0$ is equivalent to $L0 = 0$ or $L_b(ba) = ba,\ b \cdot ba = ba$, whence $ba = a$, i.e. it is necessary that $b = f_a$, where f_a is the left local identity for the element a (cf. the right local identity e_a used earlier). Putting $y = 0$ in (2.3) we have

$$x + Lx = L^{-1}(-x). \tag{2.4}$$

[12] Editors' Note: A lot of work has been done on this question in recent years. The interested reader will find a summary of the results obtained prior to 1996 in [12] which we mentioned earlier. A more recent paper on this topic is [11] by F.E.Bennett and H. Zhang

[13] The original text says "If $x = 0$, then $L^3 = 1$".

With the help of (2.4) we can transform (2.3):[14]

$$
\begin{aligned}
L^{-1}(-x+L^{-1}y) &= L^{-1}(-x+L^{-1}(-(-y))) = L^{-1}(-x-y+L(-y)) \\
&= -(-x-y+L(-y)+L(-(-x-y+L(-y))) \\
&= -L(-y)+y+x+L(-L(-y)+y+x).
\end{aligned}
$$

Thence, after replacing $-y$ by y and using (2.3), we get

$$-Ly-y+x+L(-Ly-y+x) = x+L(x-y). \tag{2.5}$$

Let $-Ly-y+x=u$ so that $x=y+Ly+u$. Then the equality (2.5) takes the form

$$u+Lu = y+Ly+u+L(y+Ly+u-y),$$

whence

$$L(y+Ly+u-y) = -u-Ly-y+u+Lu. \tag{2.6}$$

Now (2.4) and (2.6) together imply that

$$L(L^{-1}(-y)+u-y) = -u-L^{-1}(-y)+L^{-1}(-u).$$

Writing $-v$ for y and $-u$ for u, we have

$$L(L^{-1}v-u+v) = u-L^{-1}v+L^{-1}u,$$

whence

$$L^{-1}(u-L^{-1}v+L^{-1}u) = L^{-1}v-u+v.$$

Let $L^{-1}=\lambda$. Then

$$\lambda(u-\lambda v+\lambda u) = \lambda v-u+v. \tag{2.7}$$

We introduce a new operation:

$$v\circ\lambda u = \lambda v-u+v.$$

[14]Editors' Note: provided that $b=f_a$ and that $(+)$ is an associative operation. Belousov states at the beginning of this Section that he is interested in quasigroups of each type T_i which are isotopic to groups. It follows that the loop principal isotope $(Q,+)$ of a quasigroup of type T_1 is itself isotopic to a group and so, by Albert's Theorem (Theorem 1.4 of [1] or Theorem 1.3.4 of [4]), this principal isotope is a group. The main results of this long subsection are that $(Q,+)$ satisfies the relation $2x+2y+2z=2(x+y+z)$ and that, if there is an element 0 in Q satisfying the relation (2.11), then there is a loop $(Q,\oplus)$, defined as in (2.16), for which Theorems 2 and 3 hold. However, the loop $(Q,\oplus)$ itself does not appear to be isotopic either to $(Q,+)$ or to the original quasigroup $(Q,\cdot)$ of type T_1.

It is easy to see that $Q(\circ)$ is a quasigroup: using the equality (2.7), we find that the equations $a \circ x = b$, $y \circ a = b$ are equivalent to the equations:

$$\lambda a - x + a = b, \qquad \lambda(a - \lambda y + \lambda a) = b$$

which are uniquely soluble for any given $a, b \in Q$. In what follows, we shall suppose that

$$\lambda I = I\lambda,$$

where $Ix = -x$. The relation $\lambda I = I\lambda$ is equivalent to $LI = IL$.

We should like to know under what conditions this last equality holds. First we remark that, because $0 = ba = f_a a = a$, we have

$$R^{-1}x = R_a^{-1}x = R_0^{-1}x = x/0$$

$$\text{and} \qquad L^{-1}x = L_b^{-1}x = L_{f_a}^{-1}x = L_{f_0}^{-1}x = f_0 \backslash x.$$

Therefore, $x + y = R_a x \cdot L_b^{-1} y = (x/0) \cdot (f_0 \backslash y)$. In particular, $x + Ix = 0$ implies that $(x/0) \cdot (f_0 \backslash Ix) = 0$, whence we obtain

$$f_0 \backslash Ix = (x/0) \backslash 0.$$

We have $f_0 \backslash Ix = L^{-1}Ix$ from above. Let $\varphi x = L^{-1}Ix$, then

$$(x/0) \backslash 0 = \varphi x.$$

But $\varphi L = L\varphi$, because $\varphi = L^{-1}I$ and $LI = IL$. Thus,[15] since

$$\varphi L x = (Lx/0) \backslash 0$$

(by putting Lx for x in the preceding equation) and since

$$L\varphi x = L[(x/0) \backslash 0].$$

follows directly from the same preceding equation, we get

$$(Lx/0) \backslash 0 = L[(x/0) \backslash 0].$$

Since $L = L_b = L_{f_a} = L_{f_0}$, it follows that

$$(f_0 x/0) \backslash 0 = f_0[(x/0) \backslash 0]. \tag{2.8}$$

[15] The following three lines of textual explanation were not in the original text or its translation.

Let

$$(x/0)\backslash 0 = u, \qquad (f_0x/0)\backslash 0 = v. \tag{2.9}$$

Then (2.8) implies that

$$v = f_0u \tag{2.10}$$

and, from (2.9), we get

$$(x/0) \cdot u = 0, \qquad (f_0x/0) \cdot v = 0,$$

whence it follows that

$$0/u = x/0, \qquad 0/v = f_0x/0.$$

These equalities, together with (2.10), imply that

$$x = (0/u) \cdot 0, \qquad f_0x = (0/v) \cdot 0 = (0/f_0u) \cdot 0.$$

So, finally we get

$$f_0[(0/u)0] = (0/f_0u)0. \tag{2.11}$$

We prove the converse statement: if there is an element 0 in Q satisfying the condition (2.11) then, in the isotope $x + y = R_a^{-1}x \cdot L_b^{-1}y$, where $a = 0$ and $b = f_0$, the equality $LI = IL$ is satisfied with $L = L_{f_0}$ and $R = R_0$.

First we note that $0/u = I_0^{-1}u$, where the mapping I_0 is determined by the equality $x \cdot I_0x = 0$. Thus, (2.11) is equivalent to the equality $L_{f_0}R_0I_0^{-1} = R_0I_0^{-1}L_{f_0}$ or

$$LRI_0^{-1} = RI_0^{-1}L. \tag{2.12}$$

In order to express I_0 in terms of I, we replace the operation $(+)$ by $(\cdot)$ in the equation $(x + Ix) = 0$ so as to get $R_a^{-1}x \cdot L_b^{-1}Ix = 0$ or, for brevity, $R^{-1}x \cdot L^{-1}Ix = 0$ and so $x \cdot L^{-1}IRx = 0$, whence, by the definition of I_0, we obtain $I_0 = L^{-1}IR$. Substituting this expression into (2.12), we get $LR(R^{-1}IL) = R(R^{-1}IL)L$, whence it follows that $LI = IL$.

Assume now that an element 0 satisfying (2.11) exists (so that $LI = IL$ and $\lambda L = L\lambda$). Under this assumption it follows from (2.7) that

$$\lambda I(-\lambda u + \lambda v - u) = v \circ u,$$

$$\lambda I(I\lambda u + \lambda v + Iu) = v \circ u,$$

$$\lambda I(\lambda Iu - I\lambda v + Iu) = v \circ u,$$

$$\lambda I(Iu \circ I\lambda v) = v \circ u, \tag{2.13}$$

or

$$(\lambda I)^{-1}(v \circ u) = Iu \circ I\lambda v,$$

whence (using the preceding equality twice) it follows that

$$(\lambda I)^{-2}(v \circ u) = (\lambda I)^{-1}(Iu \circ I\lambda v) = I^2\lambda v \circ I\lambda Iu$$

and so $\quad (\lambda I)^{-2}(v \circ u) = \lambda v \circ \lambda u,$

because $I^2 = 1$ and $\lambda I = I\lambda$. But $(\lambda I)^{-2} = \lambda^{-2}I^{-2} = \lambda^{-2} = L^2 = L^{-1}$ because $L^3 = 1$. Thus,

$$\lambda(v \circ u) = \lambda v \circ \lambda u,$$

i.e λ is an automorphism of the quasigroup $Q(\circ)$.

We determine a loop which is an LP-isotope of the quasigroup $(\circ)$ and for which the LP-isotopism is given by

$$x \oplus y = \bar{R}_0^{-1}x \circ \bar{L}_0^{-1}y, \tag{2.14}$$

where $\bar{R}_0 x = x \circ 0$ and $\bar{L}_0 x = 0 \circ x$.

We remark that $0 \circ 0 = 0$, i.e. 0 is the identity of the loop $Q(\oplus)$. Indeed, $0 \circ 0 = \lambda 0 - 0 + 0 = \lambda 0 = L_{f_0}^{-1} 0 = 0$. Moreover, we have

$$\bar{L}_0 x = 0 \circ x = \lambda 0 - x + 0 = -x = Ix,$$

$$\bar{R}_0 x = x \circ 0 = \lambda x - 0 + x = \lambda x + x = L^{-1}x + x = L^{-1}x + L(L^{-1}x).$$

Taking into account the equality (2.4), we obtain

$$\bar{R}_0 x = L^{-1}(-L^{-1}x) = L^{-1}IL^{-1}x = L^{-2}Ix = LIx.$$

So, $\bar{L}_0^{-1} = I$, $\bar{R}_0^{-1} = IL^{-1} = I\lambda$ and consequently

$$x \oplus y = I\lambda x \circ Iy. \tag{2.15}$$

From this and the definition of the operation $(\circ)$, we conclude that

$$x \oplus y = \lambda I\lambda x - Iy + I\lambda x, \qquad \text{or} \qquad x \oplus y = I\lambda^2 x + y + I\lambda x.$$

But $\lambda^2 = L^{-2} = L = \lambda^{-1}$, hence

$$x \oplus y = I\lambda^{-1}x + y + I\lambda x. \tag{2.16}$$

We prove the following assertion.

Theorem 2. *The loop $Q(\oplus)$ defined by the equality* (2.14) *is a Moufang loop.*

Proof. We show first that λ is an automorphism of the loop $Q(\oplus)$. For this purpose, we use the equality (2.15) and the fact that λ is an automorphism of $Q(\circ)$. We have

$\lambda(x \oplus y) = \lambda(I\lambda x \circ Iy) = \lambda I\lambda x \circ \lambda Iy = I\lambda(\lambda x) \circ I\lambda y = \lambda x \oplus \lambda y$, so

$$\lambda(x \oplus y) = \lambda x \oplus \lambda y. \tag{2.17}$$

Next we show that I is an anti-automorphism of the loop $Q(\oplus)$. For this purpose, we replace the operation $(\circ)$ in (2.13) by $(\oplus)$ with the aid of (2.15):

$$\lambda I(\lambda^{-1}I^{-1}Iu \oplus I^{-1}I\lambda v) = \lambda^{-1}I^{-1}v \oplus I^{-1}u,$$

$$I\lambda(\lambda^{-1}u \oplus \lambda v) = I\lambda^{-1}v \oplus Iu,$$

$$I(u \oplus \lambda^2 v) = I\lambda^{-1}v \oplus Iu. \tag{2.18}$$

Since $\lambda^2 = \lambda^{-1}$, by replacing $\lambda^{-1}v$ by v in (2.18), we get

$$I(u \oplus v) = Iv \oplus Iu \tag{2.19}$$

as required. We need also the following equality:

$$\lambda x + x = x + \lambda x = \lambda^{-1}Ix \tag{2.20}$$

which we now prove. Putting $u = 0$ and $v = 0$ in turn in the equality (2.7), we get

1) putting $u = 0$: $\lambda(-\lambda v) = \lambda v + v$ or

$$\lambda I\lambda v = \lambda v + v, \quad \lambda^2 Iv = \lambda v + v, \quad \lambda^{-1}Iv = \lambda v + v;$$

2) putting $v = 0$: $\lambda(u + \lambda u) = -u$ or

$$u + \lambda u = \lambda^{-1}(-u), \quad u + \lambda u = \lambda^{-1}Iu.$$

Finally, we prove the relation:

$$(x \oplus y) \oplus x = x + y + x. \tag{2.21}$$

Using (2.19) and then (2.16) twice, we have

$$\begin{aligned}(x \oplus y) \oplus x &= I(Ix \oplus I(x \oplus y)) = I(I\lambda^{-1}Ix + I(x \oplus y) + I\lambda Ix)\\ &= I^2\lambda Ix + I^2(x \oplus y) + I^2\lambda^{-1}Ix = \lambda Ix + (x \oplus y) + \lambda^{-1}Ix\\ &= \lambda Ix + \lambda^{-1}Ix + y + \lambda Ix + \lambda^{-1}Ix.\end{aligned}$$

But, from (2.20), $\lambda Ix + \lambda^{-1}Ix = \lambda Ix + \lambda^2 Ix = \lambda Ix + \lambda(\lambda Ix) = \lambda^{-1}I(\lambda Ix) = \lambda^{-1}II\lambda x = x$. Consequently, $(x \oplus y) \oplus x = x + y + x$.

Now it is easy to show that $Q(\oplus)$ is a (left) Bol loop. We calculate separately the left and right hand sides of the Bol identity:

$$\begin{aligned} w_1 &= x \oplus (y \oplus (x \oplus z)) \\ &= I\lambda^{-1}x + (I\lambda^{-1}y + (I\lambda^{-1}x + z + I\lambda x) + I\lambda y) + I\lambda x, \\ w_2 &= (x \oplus (y \oplus x)) \oplus z = I\lambda^{-1}(x \oplus (y \oplus x)) + z + I\lambda(x \oplus (y \oplus x)) \end{aligned}$$

from (2.16). But, by (2.17), (2.19) and (2.21), we have

$$\begin{aligned} I\lambda(x \oplus (y \oplus x)) &= I(\lambda x \oplus \lambda(y \oplus x)) = I\lambda(y \oplus x) \oplus I\lambda x \\ &= (I\lambda x \oplus I\lambda y) \oplus I\lambda x = I\lambda x + I\lambda y + I\lambda x. \end{aligned}$$

Similarly, we obtain

$$I\lambda^{-1}(x \oplus (y \oplus x)) = I\lambda^{-1}x + I\lambda^{-1}y + I\lambda^{-1}x.$$

Therefore we get the following expression for w_2:

$$w_2 = (I\lambda^{-1}x + I\lambda^{-1}y + I\lambda^{-1}x) + z + (I\lambda x + I\lambda y + I\lambda x).$$

Comparing the forms of w_1 and w_2 thus obtained and using the fact that $(+)$ is an associative operation, we conclude that $w_1 = w_2$: that is, we obtain the Bol identity. In order to show that $Q(\oplus)$ is in fact a Moufang loop it is sufficient to apply the anti-automorphism I to both sides of the left Bol identity $w_1 = w_2$, where w_1 and w_2 are determined as above, and then after replacing Ix, Iy and Iz by x, y and z respectively, we obtain the right Bol identity. But if $Q(\oplus)$ is both a left and right Bol loop, then it is a Moufang loop [1]. Our theorem is proved. □

The following result also is true.

Theorem 3. *The loop $Q(\oplus)$ is a group if and only if $Q(+)$ is a metabelian group.*

Proof. Indeed, from (2.16), we have

$$\begin{aligned} &x \oplus (y \oplus z) = I\lambda^{-1}x + (I\lambda^{-1}y + z + I\lambda y) + I\lambda x, \\ &(x \oplus y) \oplus z = I\lambda^{-1}(x \oplus y) + z + I\lambda(x \oplus y). \end{aligned}$$

Equating the right hand sides of these equations, assuming that $(Q,\oplus)$ is a group, and then transferring terms,[16] we obtain

$$[\lambda^{-1}(x\oplus y)+I\lambda^{-1}x+I^{-1}\lambda y]+z=z+[I\lambda(x\oplus y)+\lambda x+\lambda y]. \tag{2.22}$$

Putting $z=0$, we see that $t_1=t_2$, where

$$t_1=\lambda^{-1}(x\oplus y)+I\lambda^{-1}x+I\lambda^{-1}y, \qquad t_2=I\lambda(x\oplus y)+\lambda x+\lambda y$$

and it follows from (2.22) that $t_1(=t_2)$ is in the centre Z of the group $Q(+)$. But

$$t_1=(\lambda^{-1}x\oplus\lambda^{-1}y)+I\lambda^{-1}x+I\lambda^{-1}y$$

so the latter expression is an element of Z. Replacing x and y by λx and λy respectively, we obtain

$$\begin{gathered}(x\oplus y)+Ix+Iy\in Z,\\ I\lambda^{-1}x+y+I\lambda x+Ix+Iy\in Z,\\ I\lambda^{-1}x+y+I(x+\lambda x)+Iy\in Z.\end{gathered}$$

But (2.20) implies $x+\lambda x=\lambda^{-1}Ix=I\lambda^{-1}x$ and so

$$\begin{gathered}I\lambda^{-1}x+y+\lambda^{-1}x+Iy\in Z,\\ -\lambda^{-1}x+y+\lambda^{-1}x-y\in Z.\end{gathered}$$

Replacing x by λx and y by $-y$, we get

$$-x-y+x+y\in Z, \tag{2.23}$$

i.e. $[x,y]\in Z$, where $[x,y]$ is the commutator of x,y in $Q(+)$. The last relation shows that $Q(+)$ is a metabelian group.

Conversely, starting from (2.23) and reversing the steps, we show that $t_1\in Z$. If we then show that $t_1=t_2$, it will follow that (2.22) holds. But this equality is equivalent to the associativive law in $Q(\oplus)$. We proceed to prove that $t_1=t_2$:

$$\begin{aligned}t_1&=\lambda^{-1}(x\oplus y)+I\lambda^{-1}x+I\lambda^{-1}y\\ &=-((x\oplus y)+\lambda(x\oplus y))+I\lambda^{-1}x+I\lambda^{-1}y \qquad \text{by } (2.20)^{17}\\ &=-\lambda(x\oplus y)-(x\oplus y)+I\lambda^{-1}x+I\lambda^{-1}y\\ &=I\lambda(x\oplus y)-(I\lambda^{-1}x+y+I\lambda x)+I\lambda^{-1}x+I\lambda^{-1}y \qquad \text{by } (2.16)^{17}\\ &=I\lambda(x\oplus y)-I\lambda x-y-I\lambda^{-1}x+I\lambda^{-1}x+I\lambda^{-1}y\\ &=I\lambda(x\oplus y)+\lambda x-y+I\lambda^{-1}y=I\lambda(x\oplus y)+\lambda x-y+y+\lambda y \text{ by } (2.20)^{17}\end{aligned}$$

[16] Editors' Note: We add $\lambda^{-1}(x\oplus y)$ on the left to both sides, then λx on the right and finally λy on the right.

$$= I\lambda(x \oplus y) + \lambda x + \lambda y = t_2.$$

Thus, $t_1 = t_2$ and the theorem is proved. $\square$

Finally, we show that a group $Q(+)$ which is isotopic to a Π-quasigroup satisfying the identity T_1 must satisfy the identity

$$2(x + y + x) = 2x + 2y + 2x. \tag{2.24}$$

Indeed, consider the loop $Q(\oplus)$. In this loop we have the equality

$$I(x \oplus y) = Iy \oplus Ix.$$

Replacing $(\oplus)$ by $(+)$ in this identity and using (2.16), we obtain

$$I(I\lambda^{-1}x + y + I\lambda x) = I\lambda^{-1}(Iy) + Ix + I\lambda(Iy).$$

$L.H.S. = -(-\lambda^{-1}x + y - \lambda x) = \lambda x - y + \lambda^{-1}x$ so we get

$$\lambda x + Iy + \lambda^{-1}x = \lambda^{-1}y + Ix + \lambda y. \tag{2.25}$$

Since $\lambda^{-1}x = -I\lambda^{-1}x = -(x + \lambda x) = -(\lambda x + x)$ by (2.20), we have $\lambda^{-1}x = -\lambda x - x$ and $\lambda^{-1}y = -y - \lambda y$ and so (2.25) implies

$$\lambda x - y - \lambda x - x = -y - \lambda y - x + \lambda y,$$

whence

$$y + \lambda x - y - \lambda x = -\lambda y - x + \lambda y + x,$$

$$[-y, -\lambda x] = [\lambda y, x],$$

or, after replacing $-y$ and $-\lambda x$ by y and x respectively:

$$[y, x] = [I\lambda y, I\lambda^{-1}x]. \tag{2.26}$$

Applying (2.26) to the right-hand side of the same identity, we obtain

$$[y, x] = [(I\lambda)^2 y, (I\lambda^{-1})^2 x],$$

$$[y, x] = [\lambda^2 y, \lambda^{-2} x].$$

But $\lambda^3 = (L^{-1})^3 = L^{-3} = 1$, so,

$$[y, x] = [\lambda^{-1}y, \lambda x]. \tag{2.27}$$

[17] The explanatory remarks have been added by the Editors.

From the equality (2.26) we also get

$$[Iy, Ix] = [\lambda y, \lambda^{-1}x]. \tag{2.28}$$

Finally, applying (2.27) to the right-hand side of the same identity, we get

$$\begin{aligned} [y, x] &= [\lambda^{-2}y, \lambda^2 x], \\ [y, x] &= [\lambda y, \lambda^{-1}x]. \end{aligned} \tag{2.29}$$

Comparing (2.28) and (2.29), we have

$$[Iy, Ix] = [y, x],$$

or, in expanded form,

$$\begin{aligned} -Iy - Ix + Iy + Ix &= -y - x + y + x, \\ y + x - y - x &= -y - x + y + x, \end{aligned}$$

whence it follows that

$$\begin{aligned} x + y + y + x - y - x &= y + x, \\ x + x + y + y + x &= x + y + x + x + y, \\ 2x + 2y + 2x &= x + y + x + x + y + x = 2(x + y + x) \end{aligned}$$

which proves (2.24).

Remark 5. If $Q(+)$ is metabelian then the identity (2.24) is satisfied automatically.

Example of a Π-quasigroup which satisfies an identity of type T_1.

Let $x \cdot y = x + y$, where $Q(\cdot)$ is a group of exponent 3, in additive notation $3x = 0$. Here, evidently, $R = L = 1$.[18] The condition $LI = IL$ holds trivially. The quasigroup $(\circ)$ has the form: $x \circ y = x - y + x = y - x + y$. The loop $(\oplus)$ is defined by the equality: $x \oplus y = I\lambda^{-1}x + y + I\lambda y = Ix + y + Ix = -x + y - x = -x + y + 2x$. It is known [1] that $(\oplus)$ is a commutative Moufang loop.

[18]Editors' Remark: The original text says "Let $(Q, \cdot)$ be a group of exponent 3, in additive notion $3x = 0$. Here, evidently, $R = L = 1$." but this text does not make good sense.

2) Π-quasigroups $A = (\cdot)$ of type $T_2 = [1, 1, l]$.

Such quasigroups satisfy the identity

$$x(y \cdot yx) = y. \tag{2.30}$$

We suppose that the quasigroup $Q(\cdot)$ has an idempotent element 0 and we consider the LP-isotope $x + y = R^{-1}x \cdot L^{-1}y$, where $R = R_0$, $L = L_0$ and so 0 is the identity of the loop $Q(+)$.

Replacing $(\cdot)$ by $(+)$ in (2.30), we get

$$Rx + L(Ry + L(Ry + Lx)) = y. \tag{2.31}$$

Assume that $Q(+)$ is a group and that $RL = LR$. Then (2.31) implies that

$$L(y + L(y + x)) = -RL^{-1}x + R^{-1}y.$$

If $y = 0$, then $L^2x = -RL^{-1}x$, whence $L^2 = IRL^{-1}$ and so $R = IL^3$ (where $Ix = -x$). We note that $IL = LI$, because $IL = RL^{-3}L = L^{-2}R = LI$. Consequently, the following equality must hold in $Q(+)$:

$$L(y + L(y + x)) = L^2x + IL^{-3}y. \tag{2.32}$$

and (since $x \cdot y = Rx + Ly$) the quasigroup operation $(\cdot)$ can be expressed in terms of $(+)$ as follows:

$$x \cdot y = -L^3x + Ly. \tag{2.33}$$

It is easy to check the converse statement. The quasigroup $Q(\cdot)$ defined by (2.33), where $(+)$ is a group and L is a permutation satisfying the identity (2.32), will be a Π-quasigroup of type $[1, 1, l]$, i.e. in this quasigroup the identity (2.30) will be satisfied. We have

$$\begin{aligned} x(y \cdot yx) &= -L^3x + L(-L^3y + L(-L^3y + Lx)) \\ &= -L^3x + L^2(Lx) + IL^{-3}(-L^3y) \\ &= -L^3x + L^3x + IL^{-3}IL^3y = y. \end{aligned}$$

Putting $x = 0$ in (2.32) we get $L(y + Ly) = IL^{-3}y$, whence

$$1 + L^4 + L^5 = 0.$$

If L is an automorphism of the group $Q(+)$, then (2.32) implies that $Ly + L^2y + L^2x = L^2x + IL^{-3}y$ and, from above, we also have $Ly + L^2y = IL^{-3}y$ whence $IL^{-3}y + L^2x = L^2x + IL^{-3}y$, and so $y + x = x + y$: that is, in this case the group $Q(+)$ is abelian.

3) Π-quasigroups $A = (\cdot)$ of type $T_4 = [1, 1, lr]$.

Such a quasigroup $(Q, \cdot)$ is a Stein quasigroup in which the identity $x \cdot xy = yx$ holds. In [3] it was proved that, if $Q(\cdot)$ is isotopic to a group, then this group is metabelian.

4) Π-quasigroups $A = (\circ)$ of type $T_6 = [1, l, lr]$.

In such quasigroups the identity

$$x \circ (y \circ x) = (y \circ x) \circ y \tag{2.34}$$

holds. From (2.34) it follows at once that $Q(\circ)$ is idempotent. Indeed, let $y = f_x$. Then, $x \circ (f_x \circ x) = (f_x \circ x) \circ f_x$ or $x \circ x = x \circ f_x$ and so $x = f_x$. Thus, $y = f_x \Rightarrow x = f_x$ and so $x \circ x = f_x \circ x$ for every choice of x: that is, $x \circ x = x$ for every choice of x.

Let $x \cdot y = R_1^{-1} x \circ L_1^{-1} y$, where 1 is a fixed element of Q. It is clear that 1 is the identity of the loop $Q(\cdot)$. After transformation of $(\circ)$ into $(\cdot)$, the equality (2.34) takes the form

$$Rx \cdot L(Ry \cdot Lx) = R(Ry \cdot Lx) \cdot Ly, \tag{2.35}$$

where $R = R_1,\ L = L_1$. By replacing y and x by $L^{-1}y$ and $L^{-1}x$ respectively in (2.35), we obtain

$$RL^{-1}x \cdot L(RL^{-1}y \cdot x) = R(RL^{-1}y \cdot x) \cdot y$$

or

$$\varphi x \cdot L(\varphi y \cdot x) = R(\varphi y \cdot x)y, \tag{2.36}$$

where φ denotes the mapping RL^{-1}.

Further we assume that $Q(\cdot)$ is a group. Let $\varphi y \cdot x = z$. Then $x = I\varphi y \cdot z$ (where $Iu = u^{-1}$) and (2.36) implies that

$$\varphi(I\varphi y \cdot z)Lz = Rz \cdot y, \qquad \varphi(I\varphi y \cdot z) = RzyILz,$$

$$\varphi(yz) = Rz \cdot \varphi^{-1}Iy \cdot ILz. \tag{2.37}$$

If $z = 1$, then $\varphi = \varphi^{-1}I$ and so $\varphi^2 = I$ and the equality (2.37) takes the form

$$\varphi(yz) = Rz \cdot \varphi y \cdot ILz. \tag{2.38}$$

It is easy to observe that (2.38) and $\varphi^2 = I$ together imply (2.37).

We determine $\varphi(xyz)$ in two ways:

$$\varphi(xyz) = \varphi(xy \cdot z) = Rz\varphi(xy)ILz = RzRy\varphi xILyILz,$$
$$\varphi(xyz) = \varphi(x \cdot yz) = R(yz)\varphi xIL(yz).$$

Consequently,

$$RzRy\varphi xILyILz = R(yz)\varphi xIL(yz),$$

whence, replacing φx by x, we obtain

$$(IR(yz)RzRy)x = x(IL(yz)LzLy). \tag{2.39}$$

Putting $x = 1$, we deduce that the equality (2.39) implies

$$IR(yz)RzRy = IL(yz)LzLy = C^{-1}(y,z), \quad \text{say.}$$

Then (2.39) implies that $C^{-1}(y,z)$ belongs to the centre Z of $Q(\cdot)$. So,

$$R(yz) = RzRyC(y,z), \qquad L(yz) = LzLyC(y,z). \tag{2.40}$$

Now we show that R and L commute. Putting $x = 1$ and $y = 1$ in turn into (2.36), we deduce that

$$L\varphi y = R\varphi y \cdot y, \qquad \varphi x \cdot Lx = Rx,$$

whence $Ly = Ry \cdot \varphi^{-1}y$ or $\varphi^{-1}y = IRy \cdot Ly$ and $\varphi x = RxILx$. But $I\varphi = \varphi^{-1}$, so $I(Rx \cdot ILx) = IRx \cdot Lx$. That is, $Lx \cdot IRx = IRx \cdot Lx$ or

$$Rx \cdot Lx = Lx \cdot Rx = x \tag{2.41}$$

because $x = x \circ x = Rx \cdot Lx$ from the definition of the operation $(\cdot)$. Replacing x by $L^{-1}x$ in (2.41), we obtain $RL^{-1}x \cdot x = L^{-1}x$, or $\varphi x \cdot x = L^{-1}x$. Also, from above, $\varphi x = Rx \cdot ILx = ILx \cdot Rx$ because Lx and Rx commute. On the other hand, the equality $RL^{-1}x \cdot x = L^{-1}x$ implies that

$$L^{-1}Rx = RL^{-1}Rx \cdot Rx = (RL^{-1})^2Lx \cdot Rx = \varphi^2Lx \cdot Rx = ILx \cdot Rx.$$

Consequently, $\varphi x = L^{-1}Rx$ or $RL^{-1} = L^{-1}R$, whence $RL = LR$.

Theorem 4. *Suppose that the mappings R and L of a group $Q(\cdot)$ satisfy the conditions* (2.40) *and* (2.41)*, where $C(x,y)$ is in the centre Z of $Q(\cdot)$. Then the isotope $Q(\circ)$, where $x \circ y = Rx \cdot Ly$, is a Π-quasigroup of type* $[1, l, lr]$.

Proof. To prove this theorem, we compute the left and right sides of the equality (2.34) using (2.40).

$$x \circ (y \circ x) = Rx \cdot L(Ry \cdot Lx) = RxL^2xLRyC(Ry, Lx),$$
$$(y \circ x) \circ y = R(Ry \cdot Lx) \cdot Ly = RLxR^2yC(Ry, Lx)Ly.$$

But $RxL^2x = LRx$ and $R^2yLy = RLy$ as we now show.

$$RxL^2x = RxIR^2x = RxIR(Rx) = L(Rx) = LRx,$$
$$R^2yLy = IL^2yLy = IL(Ly)Ly = RLy.$$

Here we used the equalities $R^2 = IL^2$ (which follows from $\varphi^2 = I$ and $RL^{-1} = L^{-1}R$) and $x \cdot IRx = Lx$, $ILx \cdot x = Rx$ (the latter identities being a consequence of $Lx \cdot Rx = x$). Thus,

$$x \circ (y \circ x) = LRxLRyC(Ry, Lx),$$
$$(y \circ x) \circ y = RLxRLyC(Ry, Lx),$$

whence, because $RL = LR$, we obtain $x \circ (y \circ x) = (y \circ x) \circ y$. □

Now we prove the following result.

Theorem 5. *If a group is isotopic to a* Π*-quasigroup of type* $[1, l, lr]$*, then it is metabelian.*

Proof. For the proof we use the equality (2.38): namely,

$$\varphi(yz) = Rz\varphi yILz.$$

But $\varphi = RL^{-1}$. We showed above that $RL = LR$ and $IL = R^2L^{-1}$, where the last equality follows from $R^2 = IL^2$. So, (2.38) can be written as follows:

$$L^{-1}R(yz) = Rz \cdot L^{-1}Ry \cdot L^{-1}R^2z,$$
$$R(yz) = L(Rz \cdot L^{-1}Ry \cdot L^{-1}R^2z). \tag{2.42}$$

Next we determine $L(uvw)$ using the second equality of (2.40):

$$L(uvw) = L(uv \cdot w) = LwL(uv)C(uv, w)$$
$$= LwLvLuC(u, v)C(uv, w) = LwLvLuD(u, v, w),$$

where $C(u, v)C(uv, w) = D(u, v, w) \in Z$, the centre of the group $Q(\cdot)$.

Consequently, from (2.42) and the first equality of (2.40), we obtain

$$RzRyC(y,z) = L(L^{-1}R^2z)L(L^{-1}Ry)L(Rz)D(Rz, L^{-1}Ry, L^{-1}R^2z),$$
$$RzRyC(y,z) = R^2zRyLRzD(Rz, L^{-1}Ry, L^{-1}R^2z),$$
$$RzRy = R^2zRyLRzK(y,z), \tag{2.43}$$

where $K(y,z) = D(Rz, L^{-1}Ry, L^{-1}R^2z)C^{-1}(y,z) \in Z$.

Replacing Rz, Ry by z, y respectively in (2.43), we get

$$zy = Rz \cdot y \cdot Lz \cdot K(R^{-1}y, R^{-1}z),$$

where $K(R^{-1}y, R^{-1}z) \in Z$. But $z = Rz \cdot Lz$ from (2.41), so

$$Rz \cdot Lz \cdot y = Rz \cdot y \cdot Lz \cdot K(R^{-1}y, R^{-1}z), \quad Lz \cdot y = y \cdot Lz \cdot K(R^{-1}y, R^{-1}z),$$
$$z \cdot y = y \cdot z \cdot K(R^{-1}y, R^{-1}L^{-1}z), \tag{2.44}$$

where $K(R^{-1}y, R^{-1}L^{-1}z) \in Z$. So, (2.44) implies that $[z,y] = K(R^{-1}y, R^{-1}L^{-1}z)$, i.e. $[z,y] \in Z$, which means that $Q(\cdot)$ is metabelian.[19] □

5) Π-quasigroups $A = (\cdot)$ of type $T_{10} = [1, lr, l]$.

In such quasigroups

$$xy \cdot yx = y. \tag{2.45}$$

We remark at once that these quasigroups and also quasigroups satisfying the identity $xy \cdot yx = x$ are difficult to characterize completely even if we suppose that they are isotopic to groups.

We assume that there is an idempotent element 0 in the quasigroup $Q(\cdot)$ and we consider the isotope $x + y = R_0^{-1}x \cdot L_0^{-1}y$, whence $x \cdot y = Rx + Ly$ (where $R = R_0$, $L = L_0$ and $0 \cdot 0 = 0$ is the identity of the loop $Q(+)$). Replacing the operation $(\cdot)$ by $(+)$ in (2.45), we get

$$R(Rx + Ly) + L(Ry + Lx) = y. \tag{2.46}$$

Putting $x = 0$ and $y = 0$ in turn into (2.46), we obtain $RLy + LRy = y$ and $R^2x + L^2x = 0$, or

$$RL + LR = 1, \tag{2.47}$$
$$R^2 + L^2 = 0. \tag{2.48}$$

[19]The Editors have simplified and made unambiguous the latter part of this proof by a change of notation for the centre elements and by inserting missing symbols denoting the operation $(\cdot)$.

Let us suppose now that $Q(+)$ is a group and that R and L are automorphisms of this group. Then it follows from (2.46) that

$$R^2x + RLy + LRy + L^2x = y,$$

whence, by (2.47), we obtain

$$R^2x + y + L^2x = y,$$

or

$$y + L^2x = -R^2x + y.$$

But (2.48) implies that $-R^2x = L^2x$, and consequently we have

$$y + L^2x = L^2x + y;$$

that is, in this case the group $Q(+)$ is abelian.

Now, we strengthen our suppositions. Suppose that $RL = LR$, then (2.47) implies that $2RL = 1$, $2RLx = x$, $2x = L^{-1}R^{-1}x$, i.e. the mapping $\tau : x \to 2x$ is a permutation of the set Q, $\tau = L^{-1}R^{-1}$.

We determine another connection between R and L. It is evident that $R(2x) = 2Rx$, hence $R(2LR) = R$ is equivalent to $2R^2L = R$. But $R^2 = -L^2$, whence $2(-L^2)L = R$, $R = -2L^3$. By symmetry, $L = -2R^3$. Moreover, we have $R^2 + L^2 = R^2 + (-2R^3)^2 = R^2 + 4R^6 = 0$, whence it follows that $4R^4 = -1$. Analogously, $4L^4 = -1$. We obtain the same connection using the three relations $2RL = 1$, $L = -2R^3$, $R = -2L^3$ alone.

The following proposition is true: *if $Q(+)$ is an abelian group having L as an automorphism and if $4L^3 = -1$ and $x \cdot y = -2L^3x + Ly$, then $Q(\cdot)$ is a Π-quasigroup of type $[1, lr, l]$*:

$$\begin{aligned} xy \cdot yx &= -2L^3(-2L^3x + Ly) + L(-2L^3y + Lx) \\ &= 4L^6x - 2L^4y - 2L^4y + L^2x = L^2(1 + 4L^4)x - 4L^4y = y. \end{aligned}$$

Example of a π-quasigroup of type $[1, lr, l]$. Let $Q(+, \cdot)$ be the field of complex numbers. We define $x \circ y = a(x + iy)$, where $a^2 = -\frac{1}{2}i$. Then $Q(\circ)$ is a Π-quasigroup of type $[1, lr, l]$. Indeed, we have

$$\begin{aligned} (x \circ y) \circ (y \circ x) &= a(a(x + iy) + ia(y + ix)) \\ &= a^2(x + iy + iy - x) = 2a^2iy = y. \end{aligned}$$

Here $Rx = ax,\ Lx = aix.$[20]

6) Π-quasigroups $A = (\cdot)$ of type $T_8 = [1, rl, lr]$.

In such quasigroups the identity

$$xy \cdot y = x \cdot xy. \tag{2.49}$$

is satisfied. Let $x + y = R_a^{-1}x \cdot L_b^{-1}y$. Then $x \cdot y = Rx + Ly$, where $R = R_a$, $L = L_b$. Replacing the operation $(\cdot)$ by $(+)$ in (2.49), we get

$$R(Rx + Ly) + Ly = Rx + L(Rx + Ly),$$

whence

$$R(x + y) + y = x + L(x + y). \tag{2.50}$$

Putting $y = 0$ (where $0 = ba$ is the identity of the loop $Q(+)$), we obtain $Rx = x + Lx$. This together with (2.50) imply that

$$[x + y + L(x + y)] + y = x + L(x + y),$$

and so $$y + L(x + y) + y = L(x + y).$$

provided that $(Q, +)$ is a group.

Replacing $L(x + y)$ by x we have

$$y + x + y = x.$$

From this it follows that $2y = 0$ and $x + y = y + x$. Therefore, we have proved the following proposition.

Theorem 6. *If a group is isotopic to a Π-quasigroup of type $[1, rl, lr]$, then it is an abelian group of exponent two.* □

The equality $Rx = x + Lx$ shows that L is a complete mapping.[a] We show that, if $Q(+)$ is an abelian group of exponent two and L is a complete

[20] Here, 0 is an idempotent element of the quasigroup $(Q, \circ)$ and $R_0x = x \circ 0 = ax + 0$, $L_0x = 0 \circ x = 0 + aix$.

[a] A permutation φ is called *a complete mapping* for a quasigroup $Q(\cdot)$ if there exists another permutation φ' of the set Q such that $x \cdot \varphi(x) = \varphi'(x)$ for all $x \in Q$.
Editors' Remark: The mapping φ' is called the *orthomorphism* corresponding to φ.

mapping, then $Q(\cdot)$, where $x \cdot y = x + Lx + Ly$, is a Π-quasigroup of type $[1, rl, lr]$. Indeed,

$$
\begin{aligned}
x \cdot xy &= x + Lx + L(xy) = x + Lx + L(x + Lx + Ly), \\
xy \cdot y &= xy + L(xy) + Ly = x + Lx + Ly + L(x + Lx + Ly) + Ly \\
&= x + Lx + L(x + Lx + Ly).
\end{aligned}
$$

Consequently, $x \cdot xy = xy \cdot y$.

We end this Section by showing that an arbitrary group of exponent two has a complete mapping. For this purpose, we remark that any finite group Q of exponent two can be presented as a set of n-tuples $\{\bar{a} = (a_1, a_2, \ldots, a_n)\}$, where $a_i \in \{0, 1\}$ – the cyclic group of order two. It is clear that $2\bar{a} = \bar{0}$ and that $\bar{0} = (0, 0, ..., 0)$. We define the mapping L on Q by putting

$$L\bar{a} = (a_1 + a_2, a_2 + a_3, \ldots, a_{n-1} + a_n, a_1).$$

It is evident that L produces a permutation of the set Q. We determine R, where $R\bar{a} = \bar{a} + L\bar{a}$:

$$
\begin{aligned}
R\bar{a} &= (a_1, a_2, \ldots, a_{n-1}, a_n) + (a_1 + a_2, a_2 + a_3, \ldots, a_{n-1} + a_n, a_1) \\
&= (a_1 + a_1 + a_2, a_2 + a_2 + a_3, \ldots, a_{n-1} + a_{n-1} + a_n, a_n + a_1) \\
&= (a_2, a_3, \ldots, a_n, a_n + a_1).
\end{aligned}
$$

Clearly, R is a permutation of the set Q and so L is a complete mapping. Therefore, we have proved that *any finite group of exponent two is isotopic to a* Π-*quasigroup of type* $[1, rl, lr]$.

It remains to consider the last case.

7) Π-quasigroups $A = (\cdot)$ of type $T_{11} = [1, lr, rl]$.

In such quasigroups the identity

$$xy \cdot yx = x. \tag{2.51}$$

holds. Very little can be said about these quasigroups apart from the fact that they are similar to the Π-quasigroups of type $[1, lr, l]$. Assuming that $Q(\cdot)$ has an idempotent element 0 then, by putting $R_0 = R$, $L_0 = L$ and replacing the operation $(\cdot)$ by $(+)$ in (2.51), where $x + y = R^{-1}x \cdot L^{-1}y$, we obtain the equality

$$R(Rx + Ly) + L(Ry + Lx) = x,$$

whence it follows that

$$RL + LR = 0,$$
$$R^2 + L^2 = 1. \tag{2.52}$$

If we suppose also that $Q(+)$ is a group and that R and L are automorphisms of this group then, contrary to the situation for quasigroups of type $T_{10} = [1.lr, l]$, the mapping R cannot be expressed in terms of L. However, we can construct examples of groups $Q(+)$ with automorphisms R and L satisfying (2.52). One such example is the quasigroup defined by Table 2.

§3. Some remarks

1. From Table 6 it follows that, when a quasigroup $Q(\cdot)$ satisfies some minimal identity from that Table, then $(\cdot)$ is orthogonal to one or more parastrophes of $(\cdot)$. So, we have a natural question: *Under which systems of identities from Table* 1 *will a quasigroup* $(\cdot)$ *be orthogonal to all of its parastrophes?*

First we give such a table (Table 7).

No.	Orthogonality	No of identity in Table 1
1.	$1 \perp r$	1, 2, 3, 6
2.	$1 \perp l$	6
3.	$1 \perp rl$	2, 4
4.	$1 \perp lr$	4
5.	$1 \perp s$	3, 5, 7

Table 7

From the table, we see that the identities 4 and 6 must both be satisfied in order to ensure the orthogonalities $1 \perp l$, $1 \perp lr$, i.e. the identities $xy \cdot x = y \cdot xy$ and $xy \cdot y = x \cdot xy$ must both be satisfied. To guarantee the remaining orthogonalities we have to take the following combinations: $(3, 4, 6)$, $(5, 4, 6)$ or $(7, 4, 6)$, i.e. we need to add one of the identities $x \cdot xy = yx$, $yx \cdot xy = x$ or $xy \cdot yx = x$ to the previous two identities.

We shall consider each case separately.

1st case: $(3, 4, 6)$.

We have the identities

$$x \cdot xy = yx, \qquad xy \cdot x = y \cdot xy, \qquad xy \cdot y = x \cdot xy. \tag{3.1}$$

If we put $u = xy$ and $v = yx$, the identities (3.1) take the form

$$xu = v, \qquad ux = yu, \qquad uy = xu.$$

We calculate $v \cdot xv$ in two ways:

$$v \cdot xv = (yx)(x \cdot yx) = (yx)(yx \cdot y) = y \cdot yx = xy = u.$$

Here we used the identities 3 and 4.

$$\begin{aligned} v \cdot xv &= (yx)(x \cdot yx) = (x \cdot xy)[x(x \cdot xy)] = (xu)(x \cdot xu) \\ &= (x \cdot xu)x = ux \cdot x = u \cdot ux = xu. \end{aligned}$$

Here we used all the identities from (3.1). Comparing the results obtained, we get $xu = u$. But Stein's identity $x \cdot xy = yx$ implies idempotency. (Putting $x = y$ in this identity, we obtain $x \cdot xx = xx$, whence $x^2 = x$.) So the equality $xu = u$ can be re-written in the form $xu = uu$. Therefore $u = x$: that is, $xy = x = xx$ and so $y = x$. Thus, the identities (3.1) are all satisfied only in a one-element set.

2ND CASE: $(5, 4, 6)$.

We have

$$yx \cdot xy = x, \qquad xy \cdot x = y \cdot xy, \qquad xy \cdot y = x \cdot xy. \tag{3.2}$$

The equality $x = y$ follows directly since

$$x = (xy \cdot x)(x \cdot xy) = (y \cdot xy)(xy \cdot y) = xy,$$

and, because x and y independently may be any elements from Q, the equality $x = xy$ implies that all elements of Q are equal. So, in this case also, the identities from (3.2) hold simultaneously only in a one-element quasigroup.

3RD case: $(7, 4, 6)$.

We have the identities

$$xy \cdot yx = x, \qquad xy \cdot x = y \cdot xy, \qquad xy \cdot y = x \cdot xy.$$

Here the proof is almost an exact copy of that above. We have

$$x = (x \cdot xy)(xy \cdot x) = (xy \cdot y)(y \cdot xy) = xy,$$

and so on.

So, we have proved

Theorem 7. *A Π-quasigroup $Q(A)$ in which minimal identities (of specified types) hold cannot be orthogonal to all of its parastrophes.* $\square$

On the other hand, it is easy to construct a quasigroup A such that ${}^{\sigma}\!A \perp {}^{\tau}\!A$ for any specified $\sigma, \tau \in S_3$. Here is an example: $A(x, y) = 2x + 3y$, where $Q(+, \cdot)$ is the field of rational numbers. The parastrophes of A are as follows:

$$A^{-1}(x,y) = \tfrac{1}{3}(-2x+y), \qquad {}^{-1}A(x,y) = \tfrac{1}{2}(x-3y),$$
$${}^{-1}(A^{-1}) = -\tfrac{1}{2}(3x-y), \qquad ({}^{-1}A)^{-1}(x,y) = -\tfrac{1}{3}(-x+2y),$$
$$A^{*}(x,y) = 3x+2y.$$

Since the determinant of the system of equations ${}^{\sigma}\!A(x, y) = a$, ${}^{\tau}\!A(x, y) = b$ for each pair $\sigma, \tau \in S_3$ is not equal to zero, we have ${}^{\sigma}\!A \perp {}^{\tau}\!A$.

2. The connection between minimal identities and orthogonality suggests the following question: *Are there other identities which give rise to orthogonal parastrophes?*

To obtain a reply to this question, we return to the notion of a minimal nontrivial identity. As was shown earlier, every such identity can be written in the form $ABC = E$ or, more precisely,

$$A(x, B(x, C(x, y))) = y. \tag{3.3}$$

As we remarked earlier, all other minimal nontrivial identities can be transformed to this form. Thus, in particular, the identity:

$$G[K(x, y), L(x, y)] = x. \tag{3.4}$$

can be so transformed.

The converse statement is valid too: *an identity of the form* (3.3) *is equivalent to an identity of the form* (3.4). Indeed, (3.3) implies that

$${}^{-1}A(y, B(x, C(x, y))) = x. \tag{3.5}$$

Let $C(x, y) = z$, then $y = C^{-1}(x, z)$, whence (3.5) becomes

$${}^{-1}A[C^{-1}(x, z), B(x, z)] = x, \tag{3.6}$$

and so we obtain an identity of the form (3.4).

We deduce that

Lemma 3. *If the quasigroups G, K, L are connected by the identity* (3.4), *then $K \perp L$.*[21]

Proof. Indeed, comparing (3.6) and (3.4) we can write $G = {}^{-1}A$, $K = C^{-1}$ and $L = B$. Hence $A = {}^{-1}G$, $B = L$, $C = K^{-1}$ and the equality $ABC = E$ takes the form ${}^{-1}GLK^{-1} = E$. Then $L \perp K$ follows from Lemma 1. □

Using the notation of § 0, the identity (3.4) can be written in the form $G\bar{\theta} = F$ or $G(K, L) = F$, where $\bar{\theta} = (K, L)$, because $G\bar{\theta}(x, y) = G(K, L)(x, y) = G[K(x, y), L(x, y)] = x$.

We also have the following result:

Lemma 4. *If K, L are orthogonal quasigroups, then there exists a unique quasigroup G such that $G(K, L) = F$.*

Proof. Indeed, let $K \perp L$, then $\bar{\theta} = (K, L)$ is a permutation of the set Q^2. For $\bar{\theta}$ there exists an inverse permutation $\bar{\theta}^{-1} = (G, H)$, where the operations G and H must be quasigroups by the theorem of §0. Furthermore, we have $\bar{\theta}^{-1}\bar{\theta} = (G, H)\bar{\theta} = (G\bar{\theta}, h\bar{\theta}) = \bar{\varepsilon}$, where $\bar{\varepsilon}$ is the identity permutation of Q^2. But $\bar{\varepsilon} = (F, E)$, thus $(G\bar{\theta}, H\bar{\theta}) = (F, E)$, whence it follows that $G\bar{\theta} = F$ or $G(K, L) = F$. □

Next we show that there exist identities of length greater than five with the required property. Suppose that a quasigroup $Q(\cdot, \backslash, /)$ is given and let $f(u, v)$ be an arbitrary word of length at least two in this quasigroup. Further, let ${}^{\sigma}\!A$, ${}^{\tau}\!A$ be two parastrophes of the quasigroup $(\cdot) = A$. Consider the identity

$$f({}^{\sigma}\!A(x, y), {}^{\tau}\!A(x, y)) = x. \tag{3.7}$$

The word $f(u, v)$ defines some binary operation. Let ${}^{\sigma}\!A = B$. Then $x = {}^{-1}B(B(x, y), y)$. Consequently, the identity (3.7) can be written in the form

$$f(B(x, y), {}^{\tau}\!A(x, y)) = {}^{-1}B(B(x, y), y),$$

$$({}^{-1}B)^{-1}(B(x, y), f(B(x, y), {}^{\tau}\!A(x, y)) = y. \tag{3.8}$$

[21] Editors' Note: T. Evans stated this result as an if and only if theorem in his 1975 paper[13] and F. E. Bennett [10] then used that theorem to obtain his seven identities equivalent to those in Table 1.

We define a subword f' in the following way:

$$f'(u,v) = ({}^{-1}B)^{-1}(u, f(u,v)),$$

i.e. $f'(u.v)$ also defines a certain binary operation on the quasigroup $Q(\cdot)$. Therefore (3.8) has the form

$$f'({}^{\sigma}\!A(x,y), {}^{\tau}\!A(x,y)) = y. \tag{3.9}$$

Let $({}^{\sigma}\!A, {}^{\tau}\!A) = \bar{\theta}$ be a mapping on the set Q^2. Equalities (3.7) and (3.9) can be written briefly as:

$$f\bar{\theta} = F, \qquad f'\bar{\theta} = E.$$

Consequently, $\bar{\varepsilon} = (F,E) = (f\bar{\theta}, f'\bar{\theta}) = (f,f')\bar{\theta}$ (cf. 8^0 of § 0). The pair (f,f') also defines some mapping $\bar{\varphi}$, so we can write $\bar{\varphi} = (f,f')$. Thus, $\bar{\varphi}\bar{\theta} = \bar{\varepsilon}$. In the case when Q is finite, Q^2 is finite too, and then $\bar{\varphi}$, $\bar{\theta}$ are permutations of the set Q^2. Because $\bar{\theta} = ({}^{\sigma}\!A, {}^{\tau}\!A)$ is a permutation, we obtain ${}^{\sigma}\!A \perp {}^{\tau}\!A$.

Moreover, because $\bar{\varphi} = (f,f') = \bar{\theta}^{-1}$, $\bar{\varphi}$ also is a permutation, we can apply the theorem in 8^0 of § 0 and deduce that f is a quasigroup.

For instance, let $f(u,v) = (uv)(v\backslash u)$ and let

$${}^{\sigma}\!A(x,y) = x\backslash y, \quad {}^{\tau}\!A(x,y) = yx.$$

We obtain the identity

$$[(x\backslash y)(yx)][(yx)\backslash(x\backslash y)] = x.$$

Then $(\backslash)\perp(*)$, where $x*y = yx$, and the mapping $A : (u,v) \to (uv)(v\backslash u)$ will be a quasigroup.

3. When we investigated identities of the above kind taken from the types in Table 1, we attempted to transform them into a particular form: namely, to identities equivalent to the originals but containing only one basic operation $(\cdot)$. In this connection, we make two remarks. In general, besides the identities listed in that table, there are six other minimal nontrivial identities involving only one operation. We list them below (they can be obtained in a simple way):

1) $(xy\cdot x)x = y$ (T_2), 2) $(yx\cdot y)x = y$ (T_6), 3) $(xy\cdot y)x = y$ (T_2),

4) $(yx\cdot x)x = y$ (T_1), 5) $x(y\cdot xy) = y$ (T_6), 6) $x(x\cdot yx) = y$ (T_2).

The identity type from Table 1 which is equivalent to each of the six listed identities is given in parentheses. It is interesting to add that the identities 2) and 5) are parastrophically equivalent to an identity of type T_6 having length six. This can be checked directly: the identity T_6, i.e. $xy \cdot x = y \cdot xy$ is parastrophically equivalent to an identity of type $T_6 = [1, l, lr]$, i.e. $x(x/(y/x)) = y$ which is equivalent to the identity $y/(x/(y/x)) = x$. Replacing (/) by $(*)$ and then putting $x*y = yx$, i.e. applying parastrophic equivalence, we obtain $y * (x * (y * x)) = x$, that is, $(xy \cdot x)y = x$, which is exactly the identity 2).[b]

In connection with the above, we should make the following (second) remark. The identity T_6, i.e. $xy \cdot x = y \cdot xy$, is not minimal in our sense because it has length six. But it is equivalent to the identity $x(x/(y/x)) = y$, which is minimal. It is easy to see that, if we have an identity of the form

$$f_1(x, y, z) = f_2(x, y, z),$$

where $z = xy$, and if the number of occurrences of x (or y) is smaller than the number of occurrences of $z = xy$ then, after replacing x by z/y in the first case or y by $x\backslash z$ in the second case, we obtain an identity of shorter length. For example, in the identity T_6 (i.e. $xy \cdot x = y \cdot xy$) which has length six, the elements x and y occur only once while the subword $z = xy$ is repeated twice. But, putting z/y instead of x, we obtain the identity $z(z/y) = yz$ which has length five.

4. The identities implying orthogonality of parastrophes which are considered above involve only two variables. This raises the question: *Are there identities containing more than two variables which imply the orthogonality of parastrophes of a given quasigroup?* We show that such identities exist. A general method of constructing such identities is the following. Let $D(x, y) = y$ be a minimal nontrivial identity which holds in the quasigroup $Q(\cdot)$, i.e. $D = ABC$, where A, B, C are parastrophes of the quasigroup $(\cdot)$. Consider the following identity $w_1 = w_2$, where w_1 (or w_2) has the form

$$w_1 = \ldots D(u, v) \ldots,$$

where u, v are some subwords. The dots denote variables, parentheses and operation symbols which have been omitted, while D denotes the product

[b]In obtaining such identities, we considered also identities of the form $(xy \cdot x)y = y$ for example, but such ones can be omitted because, for instance, the example given here is equivalent to the identity $xy \cdot x = y/y$, which is trivial according to our definition since it has a subword of the form $A(y, y)$.

ABC, where A, B, C are parastrophes of the operation $(\cdot)$. We assume further that the subword u contains the free element x exactly once and that the subword v contains the free element y exactly once. Moreover, we suppose that x and y do not appear elsewhere in w_1 and that the free element y appears exactly once in w_2.

We make a retraction of all elements except x and y in the identity $w_1 = w_2$, i.e. we replace all elements except x and y by constant elements of Q. Then u and v become replaced by αx and βy respectively, while w_1 and w_2 are replaced by $\gamma D(\alpha x, \beta y)$ and δy respectively, i.e. we obtain the identity

$$\gamma D(\alpha x, \beta y) = \delta y,$$

which is valid for any x and y in Q. Since all these transformations are made in the quasigroup $Q(\cdot)$, α, β, γ, δ are permutations of the set Q. Replacing αx and βy by x and y, we get

$$\gamma D(x, y) = \delta\beta^{-1} y,$$

whence we obtain $\beta\delta^{-1}\gamma D(x, y) = y$ or

$$\varphi D(x, y) = y, \tag{3.10}$$

where $\varphi = \beta\delta^{-1}\gamma$. More precisely, because $D = ABC$, the equality (3.10) can be written as

$$\varphi A(x, B(x, C(x, y))) = y. \tag{3.11}$$

Let us define the operation A' by $A'(x, y) = \varphi A(x, y)$. Then (3.11) can be written briefly in the form $A'BC = E$, which means that $B \perp C^{-1}$.

Example. Consider the identity

$$(zx)[(zx)(zx \cdot ty)] = z^2(zy \cdot t). \tag{3.12}$$

We may choose zx and ty as the subwords u and v. The left side takes the form $w_1 = u(u \cdot uv)$. Replacing z and t by fixed elements α and β, we obtain the identity $\alpha x(\alpha x(\alpha x \cdot \beta y)) = \gamma y$, whence, replacing αx by x and βy by y, we get $x(x \cdot xy) = \gamma\beta^{-1} y$ or $\beta\gamma^{-1}[x(x \cdot xy)] = y$. If $A = (\cdot)$ and $A' = \varphi A$, where $\varphi = \beta\gamma^{-1}$, and φA is defined by $(\varphi A)(x, y) = \varphi A(x, y)$, then $A'AA = E$, i.e. $A \perp A^{-1}$.

We remark that quasigroups satisfying the identity (3.12) do exist. For example, an abelian group $Q(\cdot)$ of exponent three (i.e. $x^3 = 1$ for all $x \in Q$) satisfies (3.12).

Nontrivial quasigroups (ones with more than one element) satisfying specified identities obtained in the above way do not always exist. An example of such an identity is

$$[(x \cdot xy)z]t = (xy \cdot y)(zt). \tag{3.13}$$

Here, the identity $D(x, y) = y$ is some identity of type T_8, i.e. $x((y/x)\backslash x) = y$ (cf. Table 1), the derived form of which is $x \cdot xy = xy \cdot y$. In other words, by changing some of the operations in (3.13) to parastrophes, it can be transformed[22] to $\{\{x[(y/x)\backslash x]\}z\}t = y \cdot zt$, which is the form wanted.

However, if we put $x = f_y$ in (3.13), we get $yz \cdot t = y^2 \cdot zt$.

Replacing z by y and then cancelling y^2 gives the equality $t = yt$, which is valid for all y and t in Q. But in a nontrivial quasigroup such an identity is impossible.

5. In this last subsection, we formulate some questions:

1. In §2, we studied Π-quasigroups which are isotopic to groups. For Π-quasigroups satisfying identities of types T_2, T_{10} and T_{11}, we were unable to obtain a complete answer. Therefore, we pose the following problem: *Find a complete characterization of groups isotopic to quasigroups which satisfy one of the identities* $x(y \cdot yx) = y$, $xy \cdot yx = y$ and $xy \cdot yx = x$.

2. The following question generalizes that raised in the first subsection of this Section: *Under which systems of identities will a quasigroup* $(Q, \cdot)$ *be orthogonal to all of its parastrophes?*

3. In the second subsection of this Section, we constructed identities of arbitrary length containing two free elements which guarantee the orthogonality of two parastrophes. *Prove that any identity involving two free elements which guarantees the orthogonality of at least two parastrophes of the quasigroup* $Q(\cdot)$ *has the form described in that subsection.*

4. Finally, we pose the general problem: *Describe all identities which, when satisfied in a quasigroup* $Q(\cdot)$*, guarantee the orthogonality of some parastrophes of the given quasigroup.*

In place of this, probably, we should seek to solve a more restricted problem: namely, *Do there exist identities with two free elements which imply the orthogonality of some parastrophes but which do not have retracts?* (cf. subsection 4 of this Section)

[22]We have $x((y/x)\backslash x) = y$. Put $y/x = u$ and $u\backslash x = v$. Then $y = ux$ and $x = uv$ so $uv \cdot v = y = u \cdot uv$. Since (3.13) can be written as $[(u \cdot uv)z]t = (uv \cdot v)(zt)$ by changing the variables, it is equivalent to $yz \cdot t = y \cdot zt$ or $((x[(y/x)\backslash x])z)t = y \cdot zt$ which is the form claimed.

References

[1] **V. D. Belousov**: *Foundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow, 1967.

[2] **V. D. Belousov**: *Systems of orthogonal operations*, (Russian), Mat. Sb. (N.S.) **77(119)** (1968), 38 – 58.

[3] **V. D. Belousov and A. A. Gvaramiya**: *On Stein quasigroups*, (Russian), **44** (1966), 537 – 544.

[4] **J. Dénes and A. D. Keedwell**: *Latin squares and their applications*, Acadêmiai Kiadó, Budapest and Academic Press, New York, 1974.

[5] **D. A. Norton and S. K. Stein**: *Cycles in algebraic systems*, Proc. Amer. Math. Soc. **7** (1956), 999 – 1004.

[6] **K. T. Phelps**: *Conjugate orthogonal quasigroups*, J. Combinatorial Theory, **A25** (1978), 117 – 127.

[7] **A. Sade**: *Quasigroupes obéissant á certaines lois*, Rev. Fac. Sci. Univ. Istambul. Sér. **22** (1957), 151 – 184.

[8] **S. K. Stein**: *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228 – 256.

[9] **R. Artzy**: *Isotopy and parastrophy of quasigroups.* Proc. Amer. Math. Soc. **14** (1963), 429 – 431.

[10] **F. E. Bennett**: *The spectra of a variety of quasigroups and related combinatorial designs*, Discrete Math. **77** (1989), 29 – 50.

[11] **F. E. Bennett H. Zhang**: *Latin squares with self-orthogonal conjugates*, Discrete Math. **284** (2004), 45 – 55.

[12] **F. E. Bennett**: *Quasigroups*, in "Handbook of Combinatorial Designs", Eds. C. J. Colbourn and J. H. Dinitz, CRC Press, 1996.

[13] **T. Evans**: *Algebraic structures associated with latin squares and orthogonal arrays*, Congressus Numerantium **13** (1975), 31 – 52.

[14] **A. Sade**: *Quasigroupes parastrophiques. Expressions et identités*, Math. Nachr. **20** (1959), 73 – 106.

[15] **M. E. Stickel and H. Zhang**: *First results of studying quasigroup identities by re-writing techniques*, Proc. Workshop on Automated Theorem Proving, Tokyo, 1994.

Note. Bibliographic items [9] to [15] have been added by the Editors and relate to the numbered footnotes and the Comments on page 40.