A. Krapež; Mark Aadrian Taylor

Irreducible Belousov equations on quasigroups

Czechoslovak Mathematical Journal, Vol. 43 (1993), No. 1, 157–175

Persistent URL: http://dml.cz/dmlcz/128378

Czechoslovak Mathematical Journal, 43 (118) 1993, Praha

IRREDUCIBLE BELOUSOV EQUATIONS ON QUASIGROUPS

A. KRAPEŽ, Beograd, M. A. TAYLOR, Wolfville

(Received September 2, 1991)

INTRODUCTION

Among the many quasigroup equations that have been investigated (see for example the work by Denes and Keedwell [3]), of particular interest are those that are balanced. A balanced equation is one in which each variable appears precisely once on both sides. The general study of balanced equations on quasigroups was initiated by Belousov [1] and he was who defined those balanced equations [2] which were named after him in [4] by the present authors.

In [2], it was proved that every Belousov equation is equivalent to a system of equations of a certain type (Theorem 2 below). This result was extended in [4] (Theorem 3 below) where it was shown that any finite set of Belousov equations is equivalent to a single equation again of restricted type.

The thrust of both papers is to replace a single Belousov equation or a set of Belousov equations by equations which are of lesser length. In [4] an example is given of a single equation of the restricted type which is itself equivalent to a shorter equation. The question then arises "which Belousov equations are not equivalent to a shorter Belousov equation?" In this paper we show that such irreducible Belousov equations correspond to polynomials from $1 + x\mathbb{Z}_2[x]$. These polynomials also play a major role in determining the irreducible Belousov equations equivalent to a set of Belousov equations.

In the final section of the paper, it is shown that the lattice of Belousov varieties of equational quasigroups is isomorphic to the lattice of polynomials from $1+x\mathbb{Z}_2[x]$, together with the zero polynomial, under divisibility.

Although the present work is motivated by our previous paper [4], it is essentially independent of it.

We start by reviewing some key definitions and result from [2] and [4].

The set of variables which appear in a term u is called the *content* of u, and is denoted by $\langle u \rangle$.

An equation $w_1 = w_2$ is *balanced* if $\langle w_1 \rangle = \langle w_2 \rangle$ and every variable from $\langle w_1 \rangle$ appears exactly once in w_1 and w_2.

A balanced equation $w_1 = w_2$ is *Belousov* if for every subterm u of w_1 there exists a subterm v of w_2 such that $\langle u \rangle = \langle v \rangle$.

For completeness we include:

Theorem 1. (Krapež [5], Belousov [2]). *A quasigroup satisfying a balanced but not Belousov equation is isotopic to a group.*

A Belousov equation $u_1 \cdot u_2 = v_1 \cdot v_2$ is said to be *separable* if $\langle u_1 \rangle = \langle v_1 \rangle$ (and consequently $\langle u_2 \rangle = \langle v_2 \rangle$).

Lemma 1. (Belousov [2]). *The separable Belousov equation $u_1 \cdot u_2 = v_1 \cdot v_2$ is equivalent to the pair of equations $u_1 = v_1$ and $u_2 = v_2$.*

Let uv be a binary product. Then u is said to be a *left companion* in uv and v a *right companion*. Also u and v are said to be *companions* of each other.

A variable x appearing in an equation is said to be an *isolated variable* if none of its companions is a variable.

The following two theorems are mentioned in the introduction.

Theorem 2. (Belousov [2]). *Every Belousov equation is equivalent to a system of inseparable Belousov equations with no isolated variables.*

In [4] we strengthened Theorem 2 to:

Theorem 3. *Any (finite) set of Belousov equations is equivalent to a single inseparable Belousov equation with no isolated variables.*

However, in the same paper we showed that there are inseparable Belousov equations with no isolated variables which are equivalent to shorter Belousov equations, for example

$$(xy \cdot uv)(st \cdot zw) = (ts \cdot wz)(vu \cdot yx)$$

is equivalent to $xy = yx$.

We define an *irreducible* Belousov equation to be one which is not equivalent to a shorter Belousov equation, with the understanding that one equation is shorter than another if it contains fewer variables.

The aim of this paper is to characterize irreducible Belousov equations.

CORRESPONDENCES

The use of trees to represent equations is a valuable heuristic device. In [4] a system was introduced in an attempt to formalize the manipulation of equations via trees. We have subsequently modified this system in such a way as to reduce the technical results associated with it while maintaining its applicability to Belousov equations.

The basis for the formal system is best illustrated by considering a particular example.

The equation $xy \cdot (uv \cdot w) = (vu \cdot w) \cdot yx$ has the following tree representation:

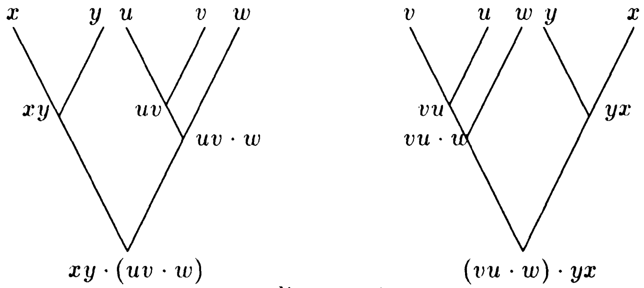

diagram 1

In addition to the variables x, y, u, v, w the term $t = xy \cdot (uv \cdot w)$ has subterms xy, $(uv \cdot w)$ and uv. The subterm $t_1 = uv \cdot w$ is a right companion in t, the subterm $t_2 = uv$ is a left companion in t, and the subterm u is a left companion in t_2. Using R to denote a right companion and L a left companion, the position of any subterm in a term can be described by means of a word in these two letters. Thus the position of u is given by $RLL(u)$. The position of the other subterms is easily obtained when the tree is appropriately labelled (diagram 2).

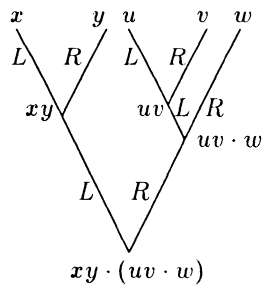

diagram 2

Thus we have $L(xy)$, $LL(x)$, $LR(y)$, $R(uv \cdot w)$, $RL(uv)$, $RLL(u)$, $RLR(v)$ and $RR(w)$.

The position of the term $xy \cdot (uv \cdot w)$ is described by the empty word Λ: $\Lambda(xy \cdot (uv \cdot w))$.

The word which describes the position of a subterm in a given term is a *path* to that subterm. A *branch* is path to a variable.

In general, for any term $w = t_1 t_2$ define L to be the path to t_1 and R the path to t_2, and recursively if p is the path to the subterm $u = u_1 u_2$ of w then pL is the path to u_1 and pR is the path to u_2.

For a subterm u of w with path p the word $p(u)$ is called a *vector* in w.

The letters S and T, possibly subscripted, will be used to denote either L or R.

We define the *length* $|S_1 \ldots S_m|$ of the path $S_1 \ldots S_m$ to be $m(|\Lambda| = 0)$ and the *length* $|t|$ of the term t as $|x| = 0$ if $t \equiv x$ and $|u \cdot v| = \max(|u|, |v|) + 1$ if $t \equiv u \cdot v$. The *length* of the vector $S_1 \ldots S_m(t)$ is defined by $|S_1 \ldots S_m t| = m + |t|$.

Notice that the length of a vector is the length of the longest branch in it.

For an equation $u = v$ we define $|u = v| = \max(|u|, |v|)$. If $u = v$ is Belousov then $|u| = |v|$ and $|u = v| = |u|$.

If $E = \{E_1, \ldots, E_n\}$ is a set of equations then $|E| = \max(|E_1|, \ldots, |E_n|)$.

If $w_1 = w_2$ is a Belousov equation and u_1 is a subterm of w_1 then w_2 has a unique subterm u_2 such that $\langle u_1 \rangle = \langle u_2 \rangle$. This establishes a *correspondence* between the path to u_1, p_1 say, and the path p_2 to u_2. We denote this correspondence by $p_1(u_1) \to p_2(u_2)$.

The equation $xy \cdot (uv \cdot w) = (vu \cdot w) \cdot yx$ has the following correspondences:

$$
\begin{aligned}
LL(x) &\to RR(x) \\
LR(y) &\to RL(y) \\
L(xy) &\to R(yx) \\
RLL(u) &\to LLR(u) \\
RLR(v) &\to LLL(v) \\
RL(uv) &\to LL(vu) \\
RR(w) &\to LR(w) \\
R(uv \cdot w) &\to L(vu \cdot w) \\
\Lambda(xy \cdot (uv \cdot w)) &\to \Lambda((vu \cdot w) \cdot yx)
\end{aligned}
$$

This list is easily obtained by labelling the trees given in diagram 1 in the manner of diagram 2.

Notice that the subwords in L and R on both sides of the symbol $\to$ are of the same length. This is a characteristic property of Belousov equations.

Consider the correspondence $RRL(u) \to LLR(u)$, from the list given above. We can obtain the path on the right of $\to$ from the path on the left by changing the first letter R to L, leaving the second letter L as it is and finally changing the third letter L to R. If we indicate the change from L to R (or vice versa) by 1, and 0 indicates no change, then the pattern 101 describes the transformation of one path to the other. Similarly, for the correspondence $LL(x) \to RR(x)$ the resulting pattern would be 11.

The concept of the pattern of a correspondence is central to the determination of the irreducible Belousov equations.

Assume that a quasigroup equation $w_1 = w_2$ is given, with a correspondence $S_1 \dots S_n(t_1) \to T_1 \dots T_n(t_2)$. Then the *pattern* (for this correspondence) is a word $\alpha_1 \dots \alpha_n$ in 0 and 1 such that $\alpha_i = 0$ iff $S_i = T_i$ and $\alpha_i = 1$ iff $S_i \neq T_i$. We also say that the correspondence $S_1 \dots S_n(t_1) \to T_1 \dots T_n(t_2)$ has the pattern $\alpha_1 \dots \alpha_n$, or even that paths $S_1 \dots S_n$ and $T_1 \dots T_n$ have the pattern $\alpha_1 \dots \alpha_n$. The pattern $\alpha_1 \dots \alpha_n$ is a *normal pattern* iff $\alpha_1 = \alpha_n = 1$.

The action of a pattern $\alpha_1, \alpha_2 \dots \alpha_n$ on a term $t = t_1 \cdot t_2$ is given by

1. $0\alpha_2 \dots \alpha_n * (t_1 \cdot t_2) = \big(\alpha_2 \dots \alpha_n * (t_1)\big) \cdot \big(\alpha_2 \dots \alpha_n * (t_2)\big)$
2. $1\alpha_2 \dots \alpha_n * (t_1 \cdot t_2) = \big(\alpha_2 \dots \alpha_n * (t_2)\big) \cdot \big(\alpha_2 \dots \alpha_n * (t_1)\big)$ when $t = t_1 \cdot t_2$.

When $t \equiv x$, a variable, then

3. $\alpha_1\alpha_2 \dots \alpha_n * (x) = \alpha_1\alpha_2 \dots \alpha_n(y \cdot z)$ where y and z are new variables and every other occurrence of x is also replaced by $y \cdot z$.

The action of a pattern $\alpha_1\alpha_2 \dots \alpha_n$ on a vector with path $S_1S_2 \dots S_m$ to the term t is given by

4. $\alpha_1 \dots \alpha_n * \big(S_1S_2 \dots S_m(t)\big) = S_1^{\alpha_1}S_2^{\alpha_2} \dots S_n^{\alpha_n}S_{n+1} \dots S_m(t)$ where $S_i^0 = S_i$, $L^1 = R$ and $R^1 = L$, in the case that $m \geqslant n$, or,
5. $\alpha_1 \dots \alpha_n * \big(S_1S_2 \dots S_m(t)\big) = S_1^{\alpha_1}S_2^{\alpha_2} \dots S_m^{\alpha_m} * (\alpha_{m+1} \dots \alpha_n * t)$ when $m < n$.

Parts 1, 2 and 3 also define the action of patterns on terms and equations. For example the equation $z = 101 * z$, where z is a variable may be written successively as

$$
\begin{aligned}
z_1z_2 &= (01 * z_2) \cdot (01 * z_1) \\
z_3z_4 \cdot z_5z_6 &= \big((1 * z_5) \cdot (1 * z_6)\big)\big((1 * z_3) \cdot (1 * z_4)\big), \\
(x_3y_3 \cdot x_4y_4)(x_5y_5 \cdot x_6y_6) &= (y_5x_5 \cdot y_6x_6)(y_3x_3 \cdot y_4x_4)
\end{aligned}
$$

where $z_1 = z_3z_4$, $z_2 = z_5z_6$, and $z_i = x_iy_i$, $i = 3, 4, 5, 6$.

Note also that

$$z_1 \cdot z_2 = 0 * z$$
$$z_3z_4 \cdot z_5z_6 = 00 * z = 0^2 * z$$
$$(x_3y_3 \cdot x_4y_4)(x_5y_5 \cdot x_6y_6) = 0^3 * z.$$

Consider the equation $x \cdot yz = zy \cdot x$. Replace y on both sides by uv. We get a new equation $x(uv \cdot z) = (z \cdot uv)x$, also Belousov and evidently equivalent to the previous one. We call it an inflation of the equation $x \cdot yz = zy \cdot x$.

In general, we get an *inflation* of an equation E by replacing all occurrences of a variable x by $y \cdot z$ where y and z are new variables, and defining an inflation of an inflation of E to be also an inflation of E. An equation $u = v$ is a *deflation* of the equation $s = t$ if $s = t$ is an inflation of $u = v$.

Notice that every inflation of an equation E is equivalent to E.

If $w_1 = w_2$ is an equation of length $k \leqslant n$ then there is an inflation which extends all branches in $w_1 = w_2$ to be of length n. This is achieved by the action of the pattern 0^n (0 repeated n times) on both w_1 and w_2. As an illustration, the effect of applying the pattern 0^3 to the equation $xy \cdot z = z \cdot yx$ is shown at the beginning of the next section.

In general the action of 0^n to one (or both) sides of $w_1 = w_2$ is to increase the length of any branches with length less than n by inflating variables. If no branch in $w_1 = w_2$ has length less that n, the equations $w_1 = w_2$ and $0^n * w_1 = 0^n * w_2$ are identical. Whatever the value of n, the equations $w_1 = w_2$ and $0^n * w_1 = 0^n * w_2$ are equivalent. This is noted by Lemma 2.

Lemma 2. $0^n * w_1 = 0^n * w_2$ *iff* $w_1 = w_2$.

Consider now the equation

$$w_1 \equiv x_1x_2 \cdot x_3x_4 = x_4x_3 \cdot x_2x_1 \equiv w_2$$

and the term t given by

$$(y_1y_2 \cdot y_3y_4) \cdot z.$$

The tree representations are given by diagrams 3 and 4. In w_1 and w_2 the branches are all of length 2. The term t has four branches of length 3 and one branch of length 1. The term $0^2 * t$ has the tree representation given by diagram 5, where $z = z_1 \cdot z_2$.

Notice that $0^2 * t$ is of the form w_1 where $x_1 = y_1y_2$, $x_2 = y_3y_4$, $x_3 = z_1$ and $x_4 = z_2$. Consequently $(y_1y_2 \cdot y_3y_4) \cdot z_1z_2 = z_2z_1 \cdot (y_3y_4 \cdot y_1y_2)$.

We have *applied* the equation $w_1 = w_2$ to the term t. For the tree representation see diagram 6.

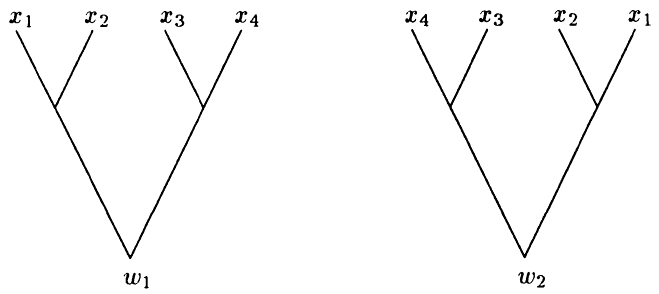

diagram 3

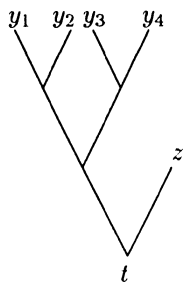

diagram 4

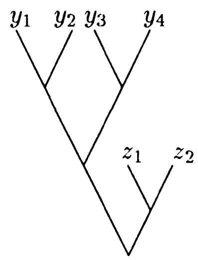

diagram 5

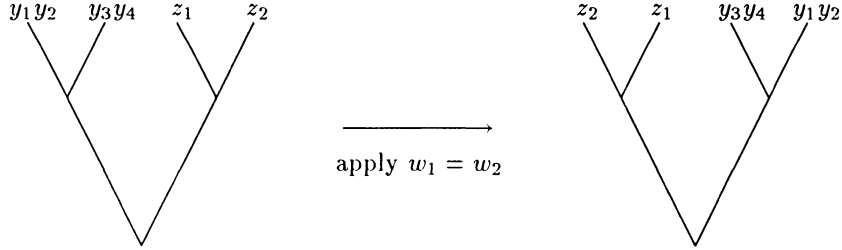

diagram 6

The process of applying an equation to a term may be extended to applying an equation $w_1 = w_2$ to an equation $u_1 = u_2$. In the latter case $w_1 = w_2$ may be applied to any subterm of u_1 or u_2.

This is illustrated by the following simple example:

We will apply $xy = yx$ first to the subterm uv

$$uv \cdot w = w \cdot vu$$

to get

$$vu \cdot w = w \cdot vu.$$

We now apply $xy = yx$ to $vu \cdot w$ which results in,

$$w \cdot vu = w \cdot vu.$$

THE STRUCTURE OF IRREDUCIBLE BELOUSOV EQUATIONS

In this section we show that all branch correspondences of an irreducible Belousov equation have the same pattern.

Consider the pair of equations

$$xy \cdot z = z \cdot yx$$
$$(rs \cdot uv) \cdot tw = wt \cdot (vu \cdot sr).$$

Then $0^3 * (xy \cdot z) = 0^3 * (z \cdot yx)$ becomes successively

$$(0^2 * xy) \cdot (0^2 * z) = (0^2 * z) \cdot (0^2 * xy)$$
$$\big((0 * x) \cdot (0 * y)\big)\big((0 * z_1) \cdot 0 * z_2)\big) = \big((0 * z_1) \cdot (0 * z_2)\big)\big((0 * y) \cdot (0 * x)\big)$$
$$w_1 \equiv (x_1x_2 \cdot y_1y_2)(z_3z_4 \cdot z_5z_6) = (z_3z_4 \cdot z_5z_6)(y_1y_2 \cdot x_1x_2) \equiv w_2.$$

Similarly $(rs \cdot uv) \cdot tw = wt \cdot (vu \cdot sr)$ under the action of 0^3 becomes

$$w_3 \equiv (rs \cdot uv)(t_1t_2 \cdot w_5w_6) = (w_5w_6 \cdot t_1t_2)(vu \cdot sr) \equiv w_4.$$

We now *apply* the equation $w_3 = w_4$ to the term w_1, that is rename the variables $r = x_1$, $s = x_2$, $u = y_1$, $v = y_2$, $t_1 = z_3$, $t_2 = z_4$, $w_5 = z_5$, $w_6 = z_6$ to get an equation

$$(x_1x_2 \cdot y_1y_2)(z_3z_4 \cdot z_5z_6) = (z_5z_6 \cdot z_3z_4)(y_2y_1 \cdot x_2x_1).$$

We conclude

$$(z_3z_4 \cdot z_5z_6)(y_1y_2 \cdot x_2x_1) = (z_5z_6 \cdot z_3z_4)(y_1y_2 \cdot x_2x_1).$$

Lemma 1 yields

$$z_3z_4 \cdot z_5z_6 = z_5z_6 \cdot z_3z_4$$

and

$$y_1y_2 \cdot x_1x_2 = y_2y_1 \cdot x_2x_1$$

The first of these equations deflates to $xy = yx$; the second separates and also gives the commutativity equation. This example serves to illustrate the following.

Lemma 3. *Let $u = v$ and $s = t$ be Belousov equations with $|u| = n > 1$ and $|s| < n$. Then provided s is not identically equal to t there exists a set E of Belousov equations with $|E| < n$ such that $E \cup \{s = t\}$ is equivalent to $\{u = v,\ s = t\}$.*

Proof. By Lemma 2 $u = v$ iff $0^n * u = 0^n * v$ and $s = t$ iff $0^n * s = 0^n * t$. We can assume without loss of generality that $u = v$ and $s = t$ are both nonseparable, i.e. $u \equiv u_1u_2$ and $v \equiv v_1v_2$ with $\langle u_1\rangle = \langle v_2\rangle$ as well as $s \equiv s_1s_2$ and $t \equiv t_1t_2$ with $\langle s_1\rangle = \langle t_2\rangle$. Then

$$(0^{n-1} * u_1) \cdot (0^{n-1} * u_2) = 0^n * u = 0^n * v = (0^{n-1} * v_1) \cdot (0^{n-1} * v_2)$$

and similarly

$$(0^{n-1} * s_1) \cdot (0^{n-1} * s_2) = (0^{n-1} * t_1) \cdot (0^{n-1} * t_2).$$

Renaming the variables we can set $0^n * u \equiv 0^n s$ which also means that $0^{n-1} * u_1 \equiv 0^{n-1} * s_1$ and $0^{n-1} * u_2 \equiv 0^{n-1} * s_2$.

The right hand sides of $0^n * u = 0^n * v$ and $0^n * s = 0^n * t$ become equal as well, i.e.

$$(1) \qquad (0^{n-1} * v_1) \cdot (0^{n-1} * v_2) = (0^{n-1} * t_1) \cdot (0^{n-1} * t_2).$$

Since

$$\langle 0^{n-1} * v_2\rangle = \langle 0^{n-1} * u_1\rangle = \langle 0^{n-1} * s_1\rangle = \langle 0^{n-1} * t_2\rangle$$

(1) separates into

$$(2) \qquad 0^{n-1} * v_1 = 0^{n-1} * t_1 \quad \text{and}$$

$$(3) \qquad 0^{n-1} * v_2 = 0^{n-1} * t_2.$$

The equations $s = t$, (2) and (3) are consequences of $s = t$ and $u = v$. Moreover, $|\{s = t,\ (2),\ (3)\}| < n$.

On the other hand $s = t$, (2) and (3) imply $0^n * u = 0^n * s = 0^n * t = 0^{n-1} * t_1 \cdot 0^{n-1} * t_2 = 0^{n-1} * v_1 \cdot 0^{n-1} * v_2 = 0^n v$. In particular $s = t$, (2) and (3) imply $u = v$. □

A Belousov equation which is not equivalent to any set of Belousov equations of lesser length is said to be *length irreducible*.

A length irreducible equation which is not an inflation is said to be a *minimal* equation.

Corollary 1. *Let $u = v$ be a minimal Belousov equation and let $s = t$ be a consequence which is not an inflation and such that $|u| = |s = t|$. Then either $s = t$ or $t = s$ is identical to $u = v$.*

Proof. We can assume that $u = v$ is nontrivial, i.e. $|u| > 1$. Lemma 3 ensures that $s = t$ is not separable because otherwise $u = v$ could be length reduced.

Let $u \equiv u_1 u_2$, $v \equiv v_1 v_2$, $s \equiv s_1 s_2$ and $t \equiv t_1 t_2$ with $\langle u_1 \rangle = \langle v_2 \rangle$ and $\langle s_1 \rangle = \langle t_2 \rangle$. Set $0^n * u \equiv 0^n * s$. Then $(0^{n-1} * v_1) \cdot (0^{n-1} * v_2) = (0^{n-1} * t_1) \cdot (0^{n-1} * t_2)$ separates into

$$\begin{aligned} 0^{n-1} * v_1 &= 0^{n-1} * t_1 \\ \text{and} \quad 0^{n-1} * v_2 &= 0^{n-1} * t_2. \end{aligned}$$

If either of these equations is not equivalent to $x = x$ then it follows by Lemma 3 that $u = v$ is not irreducible. Hence $0^{n-1} * v_1 \equiv 0^{n-1} * t_1$ and $0^{n-1} * v_2 \equiv 0^{n-1} * t_2$ i.e. $0^n * t \equiv 0^n * v$ and the required result is obtained by deflating the equation $0^n * s = 0^n * t$. □

Lemma 4. *Let $u = v$ be a minimal Belousov equation with a correspondence $p * t_1 \longrightarrow q * t_2$. Then there are subterms t_3 and t_4 such that $q * t_3 \longrightarrow p * t_4$ is also a correspondence.*

Proof. In $0^n * u = 0^n * v$ there are paths p', q', r and r' such that

$$pp' * x \longrightarrow qq' * x$$

and

$$qq' * y \to rr' * y \quad (|r| = |q|)$$

for some variables x and y.

If we apply the equation $0^n * u = 0^n * v$ to $0^n * v$ we will get an equation $0^n * v = w$. Thus we have

$$0^n * u = 0^n * v = w$$

and correspondence $pp' * x \to qq' * x \to rr' * x$. In particular $0^n * u = w$ has a correspondence $pp' * x \to rr' * x$. However, as a consequence of Corollary 1, $0^n * u \equiv w$ and it then follows that $r \equiv p$. So there is a term t_3 with a path q in u and a term t_4 with a path p in v such that $q * t_3 \to p * t_4$. □

Theorem 4. *All the branch correspondences of a minimal Belousov equation have the same pattern*

P r o o f. We can assume that the given minimal equation $u = v$ is nontrivial, i.e. $n = |u = v| > 1$. Then by Lemma 2, $0^n * u = 0^n * v$ is equivalent to $u = v$.

Consider the correspondence $L_1 L_2 \ldots L_n(x) \to L^{\alpha_1} \ldots L^{\alpha_n}(x)$ (L_i is L indexed for position) with the pattern $p = \alpha_1 \ldots \alpha_n$. We will prove that all correspondences of $u = v$ with paths of length $k (0 < k \leqslant n)$ have the pattern $\alpha_1 \ldots \alpha_k$.

Since $u = v$ is irreducible and nontrivial, we have $u \equiv u_1 u_2$ and $v \equiv v_1 v_2$ with $\langle u_1 \rangle = \langle v_2 \rangle$. Then $L(u_1) \to R(v_2)$ and $R(u_2) \to L(v_1)$, so correspondences with paths L and R both have the pattern 1.

Assume now that $S_1 \ldots S_m(t_1) \to S_1^{\alpha_1} \ldots S_m^{\alpha_m}(t_2)$ for all $m \leqslant k$ and all $S_1, \ldots, S_m$ and appropriate t_1, t_2, and that there is a correspondence with the pattern $\alpha_1 \ldots \alpha_k$ $(1 - \alpha_{k+1})$. Let $L_1 L_2 \ldots L_j R T_{j+2} \ldots T_{k+1}(t)$ be a left-most such vector, i.e.

$$\begin{aligned}(4) \qquad & L_1 L_2 \ldots L_j R T_{j+2} \ldots T_k T_{k+1}(t) \to \\ & L^{\alpha_1} \ldots L^{\alpha_j} R^{\alpha_{j+1}} T_k^{\alpha_k} T_{j+2}^{\alpha_{j+2}} \ldots T_k^{\alpha_k} T_{k+1}^{1-\alpha_{k+1}}(t')\end{aligned}$$

for some T's while

$$(5) \qquad L_1 L_2 \ldots L_{j+1} S_{j+2} \ldots S_{k+1}(s) \to L^{\alpha_1} \ldots L^{\alpha_{j+1}} S_{j+2}^{\alpha_{j+2}} \ldots S_{k+1}^{\alpha_{k+1}}(s')$$

for all possible S's.

Let t_1 be the subterm in $0^n * u$ which has the path $L_1 L_2 \ldots L_j$. The term t_1 is then inflated to the term $0^n * t_1$ which results in an inflation $u_1 = v_1$ of the equation $0^n * u = 0^n * v$. In essence the equation $u_1 = v_1$ is obtained from $0^n * u = 0^n * v$ by

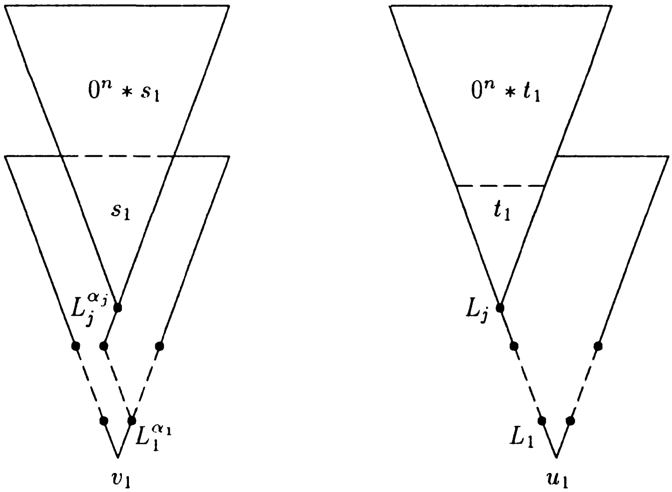

diagram 7

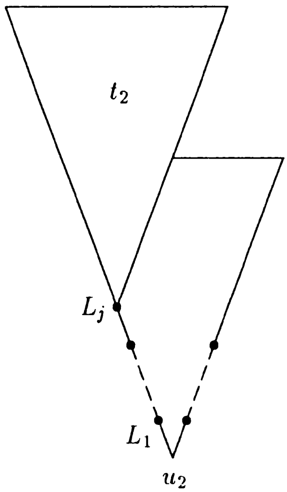

diagram 8

replacing t_1 in $0^n * u$ by $0^n * t_1$ and inflating the subterm s_1 of $0^n * v$ with the same content as t_1 accordingly (see diagram 7).

The equation $u_1 = v_1$ has the property that all branches of $0^n * u$ with a subpath $L_1 L_2 \dots L_j$ at the beginning have length $n + j$.

The equation $0^n * u = 0^n * v$ is then applied to the subterm $0^n * t_1$ of u_1 to give $0^n * t_1 = t_2$. The replacement of $0^n * t_1$ in u_1 by t_2 constructs a term u_2 (see diagram 8) and of course $u_1 = u_2$. This leads to

(6) $$u_2 = v_1.$$

In equation (6) there is a correspondence

$$L_1 L_2 \dots L_j R^{\alpha_1} T_{j+2}^{\alpha_2} \dots T_k^{\alpha_{k-j}} T_{k+1}^{\alpha_{k-j+1}}(t_3) \to$$
$$L^{\alpha_1} \dots L^{\alpha_j} R^{\alpha_{j+1}} T_{j+2}^{\alpha_{j+2}} \dots T_k^{\alpha_k} T_{k+1}^{1-\alpha_{k+1}}(t_4).$$

Form equation (6) we derive two more equations. First by applying the equation $0^n * u = 0^n * v$ to u_2 we obtain

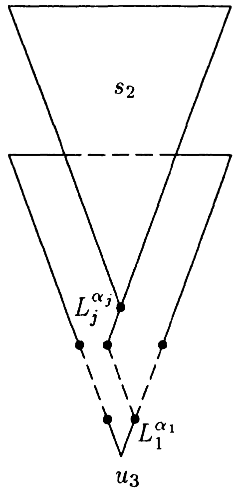

diagram 9

(7) $$u_2 = u_3.$$

Notice that (7) is an inflation of a non trivial equation $v_2 = v_3$ of length n. The second equation derived from (6) is

(8) $$u_3 = v_1.$$

Equation (8) has a correspondence

(9) $$L^{\alpha_1} \dots L^{\alpha_j} (R^{\alpha_1})^{\alpha_{j+1}} (T_{j+2}^{\alpha_2})^{\alpha_{j+2}} \dots (T_k^{\alpha_{k-1}})^{\alpha_k} (T_{k+1}^{\alpha_{k-j+1}})^{\beta}(t_5) \to$$
$$L^{\alpha_1} \dots L^{\alpha_j} R^{\alpha_{j+1}} T_{j+2}^{\alpha_{j+2}} \dots T_k^{\alpha_k} T_{k+1}^{1-\alpha_{k+1}}(t_4)$$

where $\beta \in \{0, 1\}$.

As suggested by (9), equation (8) is exactly j times separable so we get an equation ($s_2 = 0^n * s_1$) with a correspondence

$$(R^{\alpha_1})^{\alpha_{j+1}}(T_{j+2}^{\alpha_2})^{\alpha_{j+2}}\dots(T_k^{\alpha_{k-j}})^{\alpha_k}(T_{k+1}^{\alpha_{k-j+1}})^{\beta}(t_5) \to$$
$$R^{\alpha_{j+1}}T_{j+2}^{\alpha_{j+2}}\dots T_k^{\alpha_k}T_{k+1}^{1-\alpha_{k+1}}(t_4).$$

The equation $s_2 = 0^n * s_1$ is a consequence of $0^n * u = 0^n * v$ and of the length n. Therefore it is identical to either $0^n * u = 0^n * v$ or $0^n * v = 0^n * u$. By our induction hypothesis a correspondence with a path of length $k - j + 1 (< k)$ has to be $\alpha_1 \dots \alpha_{k-j+1}$. So $(T_{k+1}^{\beta})^{\alpha_{k-j+1}}$ transforms into $T_{k+1}^{1-\alpha_{k+1}}$ which is possible only if $\beta \neq \alpha_{k+1}$. But then (7) yields the correspondence

$$L_1 \dots L_j R^{\alpha_1}T_{j+2}^{\alpha_2}\dots T_k^{\alpha_{k-j}}T_{k+1}^{\alpha_{k-j+1}}(t_3) \to$$
$$L^{\alpha_1}\dots L^{\alpha_j}(R^{\alpha_1})^{\alpha_{j+1}}(T_{j+2}^{\alpha_2})^{\alpha_{j+2}}\dots(T_k^{\alpha_{k-j}})^{\alpha_k}(T_{k+1}^{\alpha_{k-j+1}})^{\beta}(t_5).$$

As noted before, (8) can be deflated to $v_2 = v_3$ of length n and we have the correspondence ($\alpha_1 = 1$ so $R^{\alpha_1} = L$)

$$\begin{gathered}L_1 \dots L_j L T_{j+2}^{\alpha_2}\dots T_k^{\alpha_{k-j}}T_{k+1}^{\alpha_{k-j+1}}(t_6) \to \\ L^{\alpha_1}\dots L^{\alpha_j}L^{\alpha_{j+1}}(T_{j+2}^{\alpha_2})^{\alpha_{j+2}}\dots(T_k^{\alpha_{k-j}})^{\alpha_k}(T_{k+1}^{\alpha_{k-j+1}})^{\beta}(t_7).\end{gathered} \tag{10}$$

with the pattern $\alpha_1 \dots \alpha_k \beta$ ($\beta \neq \alpha_{k+1}$). Since $v_2 = v_3$ is a consequence of $u = v$ of the same length, by Corollary 1, either $v_2 = v_3$ or $v_3 = v_2$ is identical to $0^n * u = 0^n * v$. By Lemma 4 we have that in any case the correspondence (10) belongs to $0^n * u = 0^n * v$, contradicting (5). This means that our assumption about the existence of a correspondence (4) with the pattern $\alpha_1 \dots \alpha_k(1 - \alpha_{k+1})$ is not sound and hence all correspondences with a path of length $k + 1$ have the pattern $\alpha_1 \dots \alpha_k \alpha_{k+1}$.

The statement of the theorem follows by induction. □

A length reducible Belousov equation is equivalent to a finite set of length irreducible Belousov equations, which by Lemma 3 and Corollary 1 are either the same or can be further reduced one by another until a single length irreducible equation remains. Thus we have

Theorem 5. *Every finite set of non trivial Belousov equations is equivalent to a single Belousov equation of the form $v = p * v$, for some normal pattern p and variable v.*

An equation of the form $w = p * w$ is called a *pattern equation.* If p is a normal pattern and w a term with all variables occurring precisely once and with all branches of length $|p|$ then the equation is a *normal equation*. Using actions of patterns on vectors, we see that $w = p * w$ iff $0^{|p|} * z = p * z$. Also $0^{|p|} * z = p * z$ is a normal equation iff p is a normal pattern.

Normal equations and $\mathbb{Z}_2[x]$

A finite set of Belousov equations is equivalent to a finite set of minimal equations which in turn is equivalent to a single minimal Belousov equation. This single minimal equation may be obtained by applying the techniques and results of the previous section either on an *ad hoc* basis or by devising an appropriate algorithm. In either case the process can prove to be very complex when equations with a large number of variables are involved. However, we now show that the canonical bijection between the set of pattern equations and polynomials over $\mathbb{Z}_2$ leads to the determination of the irreducible equation equivalent to a set of Belousov equations through the division properties of $\mathbb{Z}_2[x]$.

The bijection mentioned in the preceding paragraph maps the pattern equation $z = p * z$ with the pattern $p = \alpha_0 \ldots \alpha_n$ to the polynomial $p(x) = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{Z}_2[x]$.

It is clear that if $p = \alpha_0 \ldots \alpha_n$ is a pattern of length n then $0p = 0\alpha_0 \ldots \alpha_n$ and $p0 = \alpha_0 \ldots \alpha_n 0$ are patterns of length $n + 1$ and further $z = 0p * z$ iff $z = p * z$ iff $z = p0 * z$.

The equations $z = 0^n * z$ are trivial equations for all $n \in \mathbb{N}$, thus we refer to 0^n as a trivial pattern. The pattern $p = 010101100$ is non trivial and it is easily checked that $z = p * z$ iff $z = q * z$ where $q = 101011$.

This illustrates

Lemma 5. *For every non-trivial pattern p there is a normal pattern q such that $z = p * z$ iff $z = q * z$.*

Lemmas 6–10 follow from the properties of patterns acting on terms and the correspondence between patterned equations and polynomials over $\mathbb{Z}_2$.

Lemma 6. *The pattern equation $z = p * z$ is normal iff $p(x) \in 1 + x\mathbb{Z}_2[x]$ (i.e. $p(x) \equiv 1 \pmod{x}$ in $\mathbb{Z}_2[x]$).*

Lemma 7. *If $p(x) = x^m q(x)$ for $m \in \mathbb{N}$ then $z = p * z$ iff $z = q * z$.*

Lemma 8. *If p, q, r are patterns and $p * z = q * (r * z)$ then $p(x) = q(x) + r(x)$.*

The above lemmas lead to

Lemma 9. *Let $z = p * z$ and $z = q * z$ be two normal equations. Then $z = r * z$, where $r(x) = a(x)p(x) + b(x)q(x)$, is a consequence of $z = p * z$ and $z = q * z$ for every $a(x)$, $b(x) \in \mathbb{Z}_2[x]$.*

Lemma 10. *If $p(x)$ is a divisor of $q(x)$ in $\mathbb{Z}_2[x]$ then $z = p * z$ implies $z = q * z$.*

As corollary to this lemma we have

Theorem 6. *Let $z = p * z$ and $z = q * z$ be two normal equations. Then this pair of equations is equivalent to the single equation $z = r * z$, where $r(x)$ is the gratest common divisor of $p(x)$ and $q(x)$.*

Proof. It is well known that the g.c.d. of $p(x)$ and $q(x)$ is of the form $a(x)p(x)+b(x)q(x)$ for some $a(x)$, $b(x) \in \mathbb{Z}_2[x]$ so $z = r * z$ is a consequence of the two given equations.

On the other hand, $p(x) = c(x)r(x)$ for some $c(x) \in \mathbb{Z}_2[x]$ since $r(x)$ is a divisor of $p(x)$. So, by Lemma 11, $z = p * z$ follows from $z = r * z$.

Similarly $z = q * z$ is implied as well. □

Using the division algorithm for $\mathbb{Z}_2[x]$ we obtain

Corollary 2. *Let $z = p * z$ and $z = q * z$ be two normal equations. Then $z = p * z$ implies $z = q * z$ iff $p(x)$ divides $q(x)$ in $\mathbb{Z}_2[x]$.*

Lemma 12. *Let $S_0 \dots S_n(x) \to T_0 \dots T_n(x)$ with $p = \alpha_0 \dots \alpha_n$ be a branch correspondence of a Belousov equation $u = v$. Then the equation $z = p * z$ is implied by $u = v$.*

Proof. Without loss of generality we may assume that $S_0 \dots S_n(x) \to T_0 \dots T_n(x)$ is a correspondence of $w \equiv 0^{|u|} * u = v$ and that this equation is non-separable.

Theorem 5 ensures the existence of a normal pattern q such that $u = v$ iff $z = q * z$. Let $q = \beta_0 \dots \beta_m$ then $m \leqslant n + 1$.

Applying $z = q * z$ to $w = v$ gives as a consequence an equation $w = v'$ with a correspondence

$$S_0 \dots S_m S_{m+1} \dots S_n(x) \to T_0^{\beta_0} T_1^{\beta_1} \dots T_m^{\beta_m} T_{m+1} \dots T_n(x),$$

$w = v'$ is separable because $\beta_0 = 1$ and $S_0 = T_0^1$. Assuming the equation to be k_1 times separable, one of the consequences will be an equation $u_1 = v_1$ with the correspondence

$$S_{k_1} \dots S_n(x) \to T_{k_1}^{b_{k_1}} \dots T_m^{b_m} T_{m+1} \dots T_n(x).$$

Denoting the pattern for this correspondence by q_1, the polynomial relationship describing the action of the patterns is given by

$$p(x) - q(x) = x^{k_1} q_1(x).$$

the process is repeated to obtain a sequence of equations $u_i = v_i$ each of which is a consequence of $u = v$, and a sequence of polynomial equations

$$q_1(x) - q(x) = x^{k_2} q_2(x)$$

$$\dots\dots\dots\dots\dots$$

$$\dots\dots\dots\dots\dots$$

$$q_{i-1}(x) - q(x) = x^{k_i} q_i(x)$$

where $q_i = \gamma_1\gamma_2 \dots \gamma_e$ is the pattern of the correspondence

$$S_k \dots S_n(x) \to S_k^{\gamma_1} \dots S_{k+e}^{\gamma_e} T_{k+e+1} \dots T_n(x)$$

in the equation $u_i = v_i$.

The process terminates with $|q_j| < m + 1$. However, if $|u_j = v_j| < m + 1$ then because $u_j = v_j$ is a consequence of $z = q * z$, it must be a trivial equation $u_j \equiv v_j$. Consequently $q_j(x) = 0$. It then follows that $q(x)$ is a factor of all the $q_i(x)$ and therefore a factor of $p(x)$.

The required result that $z = p * z$ is implied by $u = v$ follows by applying $z = q * z$ appropriately to $x = 0^{|p|} * x$. □

Theorem 6 and Lemma 12 then give us

Theorem 7. *Let $u = v$ be a Belousov equation and let $\{p_i\}$ be the set of patterns of all branch correspondences of $u = v$. Then $u = v$ iff $z = p * z$, where $p(x)$ is the g.c.d. of $\{p_i(x)\}$.*

We illustrate Theorem 7 by means of an example.

The equation

$$(xy \cdot uv)(st \cdot zw) = (ts \cdot wz)(vu \cdot yx)$$

was mentioned earlier. The patterns of correspondences to branches of variables which are companions of each other are the same, e.g.

$$LLL(x) \to RRR(x)$$

$$\text{and} \quad LLR(y) \to RRL(y)$$

have the same pattern 111.

The other patterns are given by the branch correspondences

$$\begin{aligned} LRL(u) &\to RLR(u) && \text{pattern } 111 \\ RLL(s) &\to LLR(s) && \text{pattern } 101 \\ RRL(z) &\to LRR(z) && \text{pattern } 101. \end{aligned}$$

There are only two distinct patterns, 111 and 101. These have polynomial representations $1+x+x^2$ and $1+x^2$ and their g.c.d. is 1. Hence the original equation is equivalent to $z = 1 * z$, i.e. $xy = yx$.

As mentioned in the introduction, the aim of this paper is to characterize irreducible Belousov equations, that is characterize those Belousov equations which are not equivalent to a Belousov equation with fewer variables. It is now a simple exercise to show

Theorem 8. *The irreducible Belousov equations are precisely the normal Belousov equations.*

The lattice of Belousov varieties

Theorem 7 shows us that any (set of) Belousov equation(s) is equivalent to a single normal Belousov equation. We define bp to be the normal Belousov equation $z = p*z$ and denote by Bp the class of quasigroups defined by it. For example $B1$, $B11$, $B101$ are those classes of quasigroups defined respectively be the laws

(b1) $\forall xy(xy = yx)$

(b11) $\forall xyuv(xy \cdot uv = vu \cdot yz)$

(b101) $\forall xyzsuvwt\big((xy \cdot zs)(uv \cdot wt) = (vu \cdot tw)(yx \cdot sz)\big).$

Further, we define

(b0) $$\forall x(x = x)$$

so that $B0$ is the class of all quasigroups. However, despite being equationally defined (within the class of all quasigroups) neither $B0$ nor any of the Bp (p-normal pattern) are varieties.

This is because a quasigroup $(Q, \cdot)$ defined by a single binary operation may have a subalgebra which is not necessarily a quasigroup. However, every quasigroup $(Q, \cdot)$

with a single operation may be represented as an algebra $(Q, \cdot, /, \backslash)$ with three binary operations for which

$$(Q1) \qquad (x/y)y = x$$

$$(Q2) \qquad (xy)/y = x$$

$$(Q3) \qquad x(x\backslash y) = y$$

$$(Q4) \qquad x\backslash(xy) = y.$$

Conversely, if $(Q, \cdot, /, \backslash)$ is an algebra with three binary operations in which $(Q1)$, ..., $(Q4)$ hold (i.e. an *equational quasigroup*) then $(Q, \cdot)$ is a quasigroup in the usual sense. Equational quasigroups do form a variety and clearly there is a one-to-one correspondence between quasigroups and equational quasigroups [6]. Moreover, there is a one-to-one correspondence between the classes Bp (p-normal pattern) and *Belousov varieties* EBp i.e. classes of all equational quasigroups satisfying the law bp.

If we define BL to be the lattice of all classes Bp (p-normal equation) including $B0$, EBL to be the lattice of all Belousov varieties and L the lattice of polynomials from $1 + x\mathbb{Z}_2[x]$, together with the zero polynomial, under divisibility, then from Corollary 2 we easily derive

Theorem 9. $BL \simeq EBL \simeq L$.

This work was supported in part by R.F.N. Srbije through the Matematički Institut and by N.S.E.R.C. grant A8144.

References

[1] *Belousov, V. D.*: Balanced identities in quasigroups, (Russian) Mat. Sb. (N.S.) *70 (112)* (1966), 55–97.

[2] *Belousov, V. D.*: Quasigroups with completely reducible balanced equations, (Russian), Issledovaniya po teorii binarnykh i n-arnykh kvazigrupp, Matematicheskie Issledovaniya, Shtiinca, Kishinev tome *83* (1985), 11–25.

[3] *Dénes, J. and Keedwell, A. D.*: Latin squares and their applications, Academic Press, New York-London, 1974.

[4] *Krapež, A. and Taylor, M. A.*: Belousov equations on quasigroups, Aequationes Math. *34* (1987), 174–185.

[5] *Krapež, A.*: On solving a system of balanced functional equations on quasigroups III, Publ. Inst. Math. (Beograd) *26 (40)* (1979), 145–156.

[6] *Mal'cev, A. I.*: Algebraic Systems, Springer-Verlag, New York, Heidelberg, Berlin, 1973.

Authors' addresses: A. Krapež, Matematički institut, Knez Mihailova 35, 110 00 Beograd, Yugoslavia, M. A. Taylor, Department of Mathematics, Acadia University, Wolfville, N.S. B0P 1X0, Canada.