M a t h e m a t i c a
B a l k a n i c a

New Series Vol. 26, 2012, Fasc. 3–4

# On the Parastrophes of Polynomial Binary Quasigroups

*Simona Samardziska*

*Presented at MASSEE International Conference on Mathematics MICOM-2009*

A polynomial quasigroup is said to be a quasigroup $(Q, *)$ defined by a bivariate polynomial $P(x, y)$ over a ring $(Q, +, \cdot)$ by $x * y = P(x, y)$ for each $x, y \in Q$.

In this paper we investigate the parastrophic quasigroups of polynomial quasigroups, and give an explicit answer to the question whet-her a parastrophic operation of the quasigroup operation can be defined by a polynomial over the same ring. As an important corollary of this result, follows a theorem concerning the symmetric group of permutations on the ring $(Q, +, \cdot)$.

*MSC 2010*: 20N05,20N15.

*Key Words*: Permutation polynomial, polynomial quasigroup, parastrophic operation.

## 1. Quasigroups and their parastrophic operations

**Definition 1.** Let $\sigma$ be any permutation over the set $\{1, 2, 3\}$, i.e. $\sigma \in \mathcal{S}_3$, and let $(Q, f)$ be a binary quasigroup. The operation ${}^{\sigma}f$ defined by

$$ {}^{\sigma}f(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} \quad \Leftrightarrow \quad f(x_1, x_2) = x_3, $$

is called a $\sigma$- parastrophe of the quasigroup $(Q, f)$, or just a parastrophe.

From the definition, it is clear that for a given binary quasigroup $(Q, f)$, there are $3! - 1 = 5$ parastrophes.

**Proposition 1.** *Given a binary quasigroup $(Q, f)$, each of its parastrophes ${}^{\sigma}f$ also defines a binary quasigroup $(Q, {}^{\sigma}f)$.*

P r o o f. Let $a$ and $b$ be arbitrary elements of the quasigroup $Q$. We look at the solution of the equation

$$ {}^{\sigma}f(a,x) = b. \tag{1}$$

(The reasoning for the equation ${}^{\sigma}f(x,a) = b$ is analogous.)

Using the notations

$$\begin{aligned} a &= y_{\sigma(1)}\ , \\ x &= y_{\sigma(2)}\ , \\ b &= y_{\sigma(3)}\ , \end{aligned}$$

(1) becomes

$$ {}^{\sigma}f(y_{\sigma(1)}, y_{\sigma(2)}) = y_{\sigma(3)}, $$

which is equivalent to

$$ f(y_1, y_2) = y_3. $$

We have one of the two following cases:

*i/* $\sigma(2) = 3$ i.e. $y_3 = x$,

and since $f$ is a binary operation, $x$ is uniquely determined.

*ii/* $\sigma(2) \neq 3$ t.e. $x \in \{y_1, y_2\}$,

and since $f$ is a quasigroup operation, $x$ is uniquely determined.

Hence, ${}^{\sigma}f$ is a quasigroup operation. ∎

**Proposition 2.** *The relation "is parastrophic to" is an equivalence relation on the set of all binary quasigroups.*

P r o o f. Clearly, $(Q, {}^{\epsilon}f) = (Q, f)$ is parastrophic to $(Q, f)$, where $\epsilon$ is the identical permutation.

Let $g$ be parastrophic to $f$. That means that there is a permutation $\sigma \in S_3$ such that $g = {}^{\sigma}f$, i.e.

$$ g(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} \quad \Leftrightarrow \quad f(x_1, x_2) = x_3. \tag{2}$$

If we denote $y_i = x_{\sigma(i)}$, for $i \in \{1, 2, 3\}$, we get that

$$ g(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} \ \Leftrightarrow \ g(y_1, y_2) = y_3, \tag{3}$$

and therefore

$$\begin{aligned} f(x_1, x_2) = x_3 \quad &\Leftrightarrow \quad f(x_{\sigma(\sigma^{-1}(1))}, x_{\sigma(\sigma^{-1}(2))}) = x_{\sigma(\sigma^{-1}(3))} \ \Leftrightarrow \\ &\Leftrightarrow \quad f(y_{\sigma^{-1}(1)}, y_{\sigma^{-1}(2)}) = y_{\sigma^{-1}(3)}. \end{aligned} \tag{4}$$

From (2), (3) and (4)

$$ g(y_1, y_2) = y_3 \ \Leftrightarrow \ f(y_{\sigma^{-1}(1)}, y_{\sigma^{-1}(2)}) = y_{\sigma^{-1}(3)}, $$

i.e. $f$ is parastrofic to $g$.

Let $g$ be parastrophic to $f$, and $h$ parastrophic to $g$. Then, there are permutations $\sigma, \tau \in S_3$ such that, for every $x_i, y_j \in Q$

$$\begin{array}{rcl} g(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} & \Leftrightarrow & f(x_1, x_2) = x_3, \\ h(y_{\tau(1)}, y_{\tau(2)}) = y_{\tau(3)} & \Leftrightarrow & g(y_1, y_2) = y_3. \end{array}$$

Again, using the notation $y_i = x_{\sigma(i)}$, for $i \in \{1, 2, 3\}$, we have that

$$\begin{array}{rcccl} & h(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}) = x_{\sigma(\tau(3))} & \Leftrightarrow & h(y_{\tau(1)}, y_{\tau(2)}) = y_{\tau(3)} & \Leftrightarrow \\ \Leftrightarrow & g(y_1, y_2) = y_3 & \Leftrightarrow & g(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} & \Leftrightarrow \\ \Leftrightarrow & f(x_1, x_2) = x_3. & & & \end{array}$$

i.e., $h$ is parastrophic to $f$. ∎

As an easy corollary, follow the next two propositions.

**Proposition 3.** *Let $(Q, f)$ be a binary quasigroup. The parastrophic operations of $f$ satisfy the identities:*

$$\begin{array}{c} {}^{(13)}f(f(x_1, x_2), x_2) = x_1, \\ f({}^{(13)}f(x_1, x_2), x_2) = x_1, \\ {}^{(23)}f(x_1, f(x_1, x_2)) = x_2, \\ f(x_1, {}^{(23)}f(x_1, x_2)) = x_2, \\ {}^{(123)}f(x_2, f(x_1, x_2)) = x_1, \\ f(x_2, {}^{(123)}f(x_1, x_2)) = x_1, \\ {}^{(132)}f(f(x_1, x_2), x_1) = x_2, \\ f({}^{(132)}f(x_1, x_2), x_1) = x_2. \end{array}$$

**Proposition 4.** *Let $(Q, f)$ be a binary quasigroup. For the parastrophes of $f$ we have:*

$$\begin{array}{rcl} {}^{(12)}f(x_1, x_2) & = & f(x_2, x_1), \\ {}^{(123)}f(x_1, x_2) & = & {}^{(12)}({}^{(13)}f)(x_1, x_2), \\ {}^{(132)}f(x_1, x_2) & = & {}^{(12)}({}^{(23)}f)(x_1, x_2), \\ {}^{(13)}f(x_1, x_2) & = & {}^{(23)}({}^{(12)}({}^{(23)}f))(x_1, x_2). \end{array}$$

P r o o f. The first identity is clearly true. For the others, we have:

$$\begin{array}{rcl} {}^{(12)}({}^{(13)}f)(x_1, x_2) = x_3 & \Leftrightarrow & {}^{(13)}f(x_2, x_1) = x_3, \\ & \Leftrightarrow & f(x_3, x_1) = x_2, \\ & \Leftrightarrow & {}^{(123)}f(x_1, x_2) = x_3. \end{array}$$

$$\begin{aligned} {}^{(12)}({}^{(23)}f)(x_1,x_2)=x_3 &\Leftrightarrow {}^{(23)}f(x_2,x_1)=x_3,\\ &\Leftrightarrow f(x_2,x_3)=x_1,\\ &\Leftrightarrow {}^{(132)}f(x_1,x_2)=x_3. \end{aligned}$$

$$\begin{aligned} {}^{(23)}({}^{(12)}({}^{(23)}f))(x_1,x_2)=x_3 &\Leftrightarrow {}^{(12)}({}^{(23)}f)(x_1,x_3)=x_2,\\ &\Leftrightarrow {}^{(23)}f(x_3,x_1)=x_2,\\ &\Leftrightarrow f(x_3,x_2)=x_1,\\ &\Leftrightarrow {}^{(13)}f(x_1,x_2)=x_3. \end{aligned}$$

■

It is common to denote the quasigroup operation $f$ by "$*$", ${}^{(13)}f$ by "/", and ${}^{(23)}f$ by "\".

## 2. Polinomial quasigroups and their parastrophes

A polynomial $P(x)=a_0+a_1x+\cdots+a_dx^d$ in a finite ring $R$ is said to be a *permutation polynomial* if $P$ permutes the elements of $R$.

We say that a binary quasigroup $(Q,f)$ is a *polynomial quasigroup* if there is a ring $(Q,+,\cdot)$ and a bivariate polynomial $P(x,y)\in Q[x,y]$ such that

$$f(x,y)=P(x,y) \text{ for every } x,y\in Q.$$

Rivest [1] considers polynomials over $\mathbb{Z}_{2^w}$, where $w$ is a positive integer, that define binary quasigroups of order $2^w$. He proves the following statement.

**Theorem 1.** (a) *Let $P(x)=a_0+a_1x+\cdots+a_dx^d$ be a polynomial with integral coefficients. Then $P(x)$ is a permutation polynomial modulo $2^w$, $w\geq 2$, if and only if $a_1$ is odd, $(a_2+a_4+a_6+\dots)$ is even, and $(a_3+a_5+a_7+\dots)$ is even.*

(b) *A bivariate polynomial $P(x,y)=\sum_{i,j}a_{i,j}x^iy^j$, represents a quasigroup operation in $\mathbb{Z}_{2^w}$, $w\geq 2$, if and only if the four univariate polynomials $P(x,0)$, $P(x,1)$, $P(0,y)$ and $P(1,y)$, are all permutation polynomials in $\mathbb{Z}_{2^w}$.*

Let $(Q,f)$ be a binary polynomial quasigroup, and let $P(x,y)$ be its polynomial representation over the ring $(Q,+,\cdot)$. Let $(Q,{}^{\sigma}f)$ be the quasigroup defined by some parastrophic operation ${}^{\sigma}f$ of $f$.

We are interested if there is a polynomial $P_\sigma(x,y)$ over $(Q,+,\cdot)$ that defines $(Q,{}^{\sigma}f)$, i.e. a polynomial that satisfies

$$P_\sigma(x,y)=z \;\Leftrightarrow\; {}^{\sigma}f(x,y)=z.$$

We will look for such polynomials $P_{(12)}$, $P_{(13)}$, $P_{(23)}$, $P_{(123)}$, $P_{(132)}$, that represent the five parastrophic operations of $f$ respectively.

According to Proposition 3, these polynomials should satisfy the following identities.

$$P_{(12)}(x,y) = P(y,x) \tag{5}$$

$$\begin{aligned} P_{(13)}(P(x,y),y) &= x, \\ P(P_{(13)}(x,y),y) &= x, \end{aligned} \tag{6}$$

$$\begin{aligned} P_{(23)}(x,P(x,y)) &= y, \\ P(x,P_{(23)}(x,y)) &= y, \end{aligned} \tag{7}$$

$$\begin{aligned} P_{(123)}(y,P(x,y)) &= x, \\ P(y,P_{(123)}(x,y)) &= x, \end{aligned} \tag{8}$$

$$\begin{aligned} P_{(132)}(P(x,y),x) &= y, \\ P(P_{(132)}(x,y),x) &= y, \end{aligned} \tag{9}$$

It is clear that the next proposition is true.

**Proposition 5.** *Let $(Q,f)$ be a binary polynomial quasigroup, and let $P(x,y)$ be be its polynomial representation over the ring $(Q,+,\cdot)$.*

*If $P_{(12)}(x,y)$, (resp. $P_{(13)}(x,y)$; $P_{(23)}(x,y)$; $P_{(123)}(x,y)$; $P_{(132)}(x,y)$ ) is a polynomial satisfying (5), (resp. (6); (7); (8); (9)), then it defines the quasigroup $(Q,^{(12)}f(x,y))$ (resp. $(Q,^{(13)}f(x,y))$; $(Q,^{(23)}f(x,y))$; $(Q,^{(123)}f(x,y))$; $(Q,^{(132)}f(x,y))$ ).*

From Proposition 4, we conclude that if $P(x,y)$ defines the quasigroup $(Q,f)$, then there always exists a polynomial $P_{(12)}(x,y)$ that represents the quasigroup $(Q,^{(12)}f)$, defined by

$$P_{(12)}(x,y) = P(y,x).$$

The same proposition also tells us that it is enough to further investigate the existence of a polynomial representation only of the quasigroup $(Q,^{(23)}f)$. This means that if there is a polynomial representation of $(Q,^{(23)}f)$ for every quasigroup operation $f$ that is defined by a polynomial, then there is a polynomial representation of all of the parastrophic operations of $f$.

In the sequel, we will denote ${}^{(23)}f$ by the usual notation "\", and the polynomial representation, whose existence we investigate, by $P_{\backslash}(x, y)$.

### 3. Extending the notion of permutation

Let $Q$ be a final set with $n$ elements. Let $S$ denote the set of all mappings $f : Q^2 \to Q$ such that the projection $f_a(x) = f(a, x)$ is a permutation for every $a \in Q$.

Let $x \in Q$. We define an operation "$\bullet$" on $S$, by:

$$f \bullet g(x, y) = f(x, g(x, y)).$$

**Theorem 2.** *$(S, \bullet)$ is a group.*

Proof. Let $f, g \in S$ and let $(x, y) \in Q$. Then

$$(f \bullet g)_x(y) = f \bullet g(x, y) = f(x, g(x, y)) = f_x(g(x, y)) = f_x(g_x(y)) = f_x \circ g_x(y).$$

The later is a composition of permutations, thus a permutation, which means that $f \bullet g \in S$, i.e. the set $S$ is closed under the operation "$\bullet$".

The equality

$$\begin{aligned} f \bullet (g \bullet h)(x, y) &= f(x, g \bullet h(x, y)) = f(x, g(x, h(x, y))) = \\ &= f \bullet g(x, h(x, y)) = (f \bullet g) \bullet h(x, y), \end{aligned}$$

confirms the associative law, so $(S, \bullet)$ is a semigroup.

The mapping $e(x, y) = y$, clearly belongs to $S$, and it is the identity element in $S$ since

$$\begin{aligned} f \bullet e(x, y) &= f(x, e(x, y)) = f(x, y), \text{ and} \\ e \bullet f(x, y) &= e(x, f(x, y)) = f(x, y), \end{aligned}$$

for every mapping $f \in S$.

Let $f \in S$. We define a mapping $f' : Q^2 \to Q$ by:

$$f'(x, y) = z \;\Leftrightarrow\; f(x, z) = y.$$

We show that $f' = f^{-1}$. Since

$$f'_x(y) = f'(x, y) = z \;\Leftrightarrow\; f(x, z) = y \;\Leftrightarrow\; f_x(z) = y,$$

it follows that $f'_x = f_x^{-1}$, which means that $f'_x$ is a permutation, i.e. $f' \in S$.

Furthermore, if $z$ is such that $z = f' \bullet f(x,y)$, we have that

$$\begin{aligned} z &= f'(x, f(x,y)) \Leftrightarrow \\ \Leftrightarrow\ f(x,z) &= f(x,y) \Leftrightarrow \\ \Leftrightarrow\ f_x(z) &= f_x(y) \Leftrightarrow \\ \Leftrightarrow\ z &= y, \end{aligned}$$

and thus we conclude that

$$f' \bullet f(x,y) = y = e(x,y).$$

Similarly, since for $w = f \bullet f'(x,y)$,

$$\begin{aligned} w &= f(x, f'(x,y)) \Leftrightarrow \\ \Leftrightarrow\ f'(x,w) &= f'(x,y) \Leftrightarrow \\ \Leftrightarrow\ f'_x(w) &= f'_x(y) \Leftrightarrow \\ \Leftrightarrow\ w &= y, \end{aligned}$$

we get that

$$f \bullet f'(x,y) = y = e(x,y).$$

Hence, $f \bullet f' = f' \bullet f = e$, i.e. $f'$ is the inverse element of $f$ in $S$. ∎

The next corollary follows immediately from the definition of a quasigroup.

**Corollary 1.** *Let $(Q,f)$ be a finite binary quasigroup. Then $f$ belongs to $S$.*

This result leads us to the next one, which gives the answer to the main problem of this article.

**Corollary 2.** *Every finite polynomial quasigroup $(Q,*)$, defined by a polynomial over the ring $(Q,+,\cdot)$, has a polynomial parastrophe $(Q,\backslash)$.*

Proof. Let $(Q,*)$ be a binary poynomial quasigroup defined by the polynomial $P(x,y)$. Then, $P \in S$. Since $S$ is a finite group, every quasigroup has a finite order, thus there is $r \in \mathbb{N},\ r \leq |S|$, such that $P^r = e$, and

$$\begin{aligned} P^{r-1} \bullet P &= e, \\ P \bullet P^{r-1} &= e. \end{aligned}$$

This means that $P^{r-1}$ is the inverse element of $P$.
Also, obviously, $P^{r-1}(x,y) = P(x, P(x, \dots P(x,y)\dots))$ is a polynomial.

What's left is to show that $P^{r-1}$ defines the quasigroup $(Q, \backslash)$. But, this is a direct consequence of Proposition 5 and the fact that

$$P(x, P^{r-1}(x, y)) = e(x, y) = y = P^{r-1}(x, P(x, y)).$$

■

Even more, from Proposition 4, we have:

**Corollary 3.** *Let $(Q, *)$ be a finite polynomial quasigroup, defined by a polynomial over the ring $(Q, +, \cdot)$, Then every parastrophic operation of $(Q, *)$, has a polynomial representation over the same ring $(Q, +, \cdot)$.*

This result is of great importance to the application of the theory of quasigroups. It determines the extent to which such quasigroups can be used in the creation of one way functions, but also broadens their use in the creation of various types of cyphers. We hope, in the near future, this result will be implemented in a concrete way.

At the end, we give another important theorem, which emphasizes the nature of the set $S$, that it can be considered as a sort of an extension of the notion of permutation.

**Theorem 3.** *Let $n$ be the number of elements of $Q$, and let $\mathcal{S}_n$ be the group of permutations of $Q$. Then*

$$S \cong {\mathcal{S}_n}^n,$$

*where ${\mathcal{S}_n}^n$ is a direct product of $\mathcal{S}_n$.*

Proof. Let $\psi : \mathbb{Z}_n \to Q$ be a bijection. We define a mapping $\varphi : S \to {\mathcal{S}_n}^n$ by

$$\varphi(f) = (f_{\psi(0)}, f_{\psi(1)}, \ldots, f_{\psi(n-1)}).$$

This mapping is well defined. Indeed, let

$$(f_{\psi(0)}, f_{\psi(1)}, \ldots, f_{\psi(n-1)}) \neq (f'_{\psi(0)}, f'_{\psi(1)}, \ldots, f'_{\psi(n-1)})$$

be two distinct elements of the set ${\mathcal{S}_n}^n$. That means that there is an element $i \in \mathbb{Z}_n$, such that

$$f_{\psi(i)} \neq f'_{\psi(i)}.$$

So, there exists $x \in Q$ such that $f_{\psi(i)}(x) \neq f'_{\psi(i)}(x)$. In other words,

$$f(\psi(i), x) \neq f'(\psi(i), x),$$

i.e., $f \neq f'$.

We show that $\varphi$ is a bijection.

Let $f', f'' \in S$ and let $\varphi(f') = \varphi(f'')$. Then, $f'_{\psi(i)} = f''_{\psi(i)}$, for every $i \in \mathbb{Z}_n$, i.e.,

$$f'(\psi(i), x) = f''(\psi(i), x),$$

for every $i \in \mathbb{Z}_n$, and every $x \in Q$. Thus, $f' = f''$, and $\varphi$ is an injection.

For every $(f_{\psi(0)}, f_{\psi(1)}, \ldots, f_{\psi(n-1)}) \in \mathcal{S}_n$, there exists $f \in S$ such that

$$f(\psi(i), x) = f_{\psi(i)}(x),$$

so $\varphi$ is also a surjection.

Next, let $x \in Q$.

$$\begin{aligned}
&\varphi(f \bullet g)(x) = \\
=\ & ((f \bullet g)_{\psi(0)}, (f \bullet g)_{\psi(1)}, \ldots, (f \bullet g)_{\psi(n-1)})(x) = \\
=\ & ((f \bullet g)_{\psi(0)}(x), (f \bullet g)_{\psi(1)}(x), \ldots, (f \bullet g)_{\psi(n-1)}(x)) = \\
=\ & ((f \bullet g)(\psi(0), x), (f \bullet g)(\psi(1), x), \ldots, (f \bullet g)(\psi(n-1), x)) = \\
=\ & (f(\psi(0), g(\psi(0), x)), f(\psi(1), g(\psi(1), x)), \ldots, f(\psi(n-1), g(\psi(n-1), x))) = \\
=\ & (f(\psi(0), g_{\psi(0)}(x)), f(\psi(1), g_{\psi(1)}(x)), \ldots, f(\psi(n-1), g_{\psi(n-1)}(x))) = \\
=\ & (f_{\psi(0)}(g_{\psi(0)}(x)), f_{\psi(1)}(g_{\psi(1)}(x)), \ldots, f_{\psi(n-1)}(g_{\psi(n-1)}(x))) = \\
=\ & (f_{\psi(0)} \circ g_{\psi(0)}(x), f_{\psi(1)} \circ g_{\psi(1)}(x), \ldots, f_{\psi(n-1)} \circ g_{\psi(n-1)}(x)) = \\
=\ & (f_{\psi(0)}, f_{\psi(1)}, \ldots, f_{\psi(n-1)}) \circ (g_{\psi(0)}, g_{\psi(1)}, \ldots, g_{\psi(n-1)})(x) = \\
=\ & \varphi(f) \circ \varphi(f)(x)
\end{aligned}$$

Therefore, $\varphi$ is a homomorphism. ∎

Note that this isomorphism gives the cardinal number of the set $S$.

**Corollary 4.**

$$|S| = (n!)^n.$$

## References

[1] R. L. Rivest. Permutation polynomials modulo $2^w$. // *Finite Fields and Their Applications*, **7**, 2001, 287–292

*FON University,*
*Faculty of Communication and IT,*
*Skopje, Macedonia*
*E-MAIL:simona.samardziska@fon.edu.mk*

*Received 04.02.2012*