On a Particular Case of the Bisymmetric Equation for Quasigroups

Christophe Petit[1*], Mathieu Renauld, François-Xavier Standaert[1†]
[1]Université catholique de Louvain, Crypto Group,
Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium.

March 18, 2014

Abstract

We characterize the solutions of the equation

$$D(G(x,y),G(u,v)) = G(D(x,u),T(y,v)), \tag{1}$$

where D, G and T are quasigroups. We also discuss the particular case when $D = T$.

1 Introduction and Notations

A *quasigroup* on a set Q is an operation $(\cdot) : Q \times Q \to Q$ such that for any $a, b \in Q$, there are unique x, y such that $a \cdot x = b$ and $y \cdot a = b$. In this paper, we use small letters for elements of Q and capital letters for quasigroups. We use greek letters for permutations on Q. If $x \in Q$ and α is a permutation on Q, we write $\alpha(x)$ for the image of x by α. We write $\beta\alpha$ for the composition of α and β, where α is applied first.

Two quasigroups $\oplus$ and $\otimes$ on a same set Q are *isotopic* if there exist three permutations α, β, γ of Q such that for any $x, y \in Q$, we have $x \otimes y = (x\alpha \oplus y\beta)\gamma^{-1}$. When $(Q, +)$ is an Abelian group and α is a permutation on Q, we say that α is *additive* for $+$ if for any $x, y \in Q$, we have $\alpha(x + y) = \alpha(x) + \alpha(y)$. When α and β are two permutations on the same set Q, we say that α and β commute if for all $x \in Q$, we have $\alpha\beta(x) = \beta\alpha(x)$.

Functional equations on quasigroups have been previously considered in [1, 2, 3]. In [1], Aczél, Belousov and Hosszú studied various quasigroup equations, including the generalized bisymmetry equation:

$$A(B(x,y),C(u,v)) = D(E(x,u),F(y,v)).$$

They showed that for any solution of this equation, all the quasigroups A, B, C, D, E, F are isotopic to the same Abelian group. Here, we show that the additional constraints $B = C = D$, $A = E$ imply some additivity and commutativity properties.

*FRS-FNRS Research Collaborator at Université catholique de Louvain.
†FRS-FNRS Research Associate at Université catholique de Louvain.

2 Our Results

Let G, D, T satisfying (1). From Theorem 3 in Aczél, Belousov, Hosszú [1], there exist an Abelian group $+$ and 6 permutations $\psi, \epsilon, \delta, \varphi, \beta, \gamma$ such that:

$$G(x,y) = \psi(x) + \epsilon(y), \quad D(x,y) = \delta(x) + \varphi(y), \quad T(x,y) = \epsilon^{-1}(\beta(x) + \gamma(y)). \tag{2}$$

Let $-$ be such that $x + y = z \Leftrightarrow x = z - y$, and let e be the neutral element of $+$.

Proposition 1 *Let G, D, T be three quasigroups. These quasigroups satisfy*

$$D(G(x,y), G(u,v)) = G(D(x,u), T(y,v))$$

if and only if there exist an Abelian group $+$, two constants k_1, k_2 and four permutations $\hat{\psi}, \hat{\delta}, \hat{\varphi}, \epsilon$ such that the three permutations $\hat{\psi}$, $\hat{\delta}$ and $\hat{\varphi}$ are additive for $+$, the permutation $\hat{\psi}$ commutes with both $\hat{\delta}$ and $\hat{\varphi}$, and:

$$\begin{array}{rcl} G(x,y) & = & \hat{\psi}(x) + \epsilon(y) + k_1, \\ D(x,y) & = & \hat{\delta}(x) + \hat{\varphi}(y) + k_2, \\ T(x,y) & = & \epsilon^{-1}\left(\hat{\delta}\epsilon(x) + \hat{\varphi}\epsilon(y) + k_3\right), \end{array}$$

where $k_3 := \hat{\delta}(k_1) + \hat{\varphi}(k_1) - k_1 + k_2 - \hat{\psi}(k_2)$.

When we additionally impose $T = D$, we get:

Proposition 2 *Let G, D be two quasigroups. These quasigroups satisfy:*

$$D(G(x,y), G(u,v)) = G(D(x,u), D(y,v)) \tag{3}$$

if and only if there exist an Abelian group $+$, two constants k_1, k_2 and four permutations $\hat{\psi}, \hat{\delta}, \hat{\varphi}, \hat{\epsilon}$, all of them additive for $+$, such that both $\hat{\psi}$ and $\hat{\epsilon}$ commute with both $\hat{\delta}$ and $\hat{\varphi}$:

$$\hat{\delta}(k_1) + \hat{\varphi}(k_1) + k_2 = \hat{\psi}(k_2) + \hat{\epsilon}(k_2) + k_1,$$

and:

$$\begin{array}{rcl} G(x,y) & = & \hat{\psi}(x) + \hat{\epsilon}(y) + k_1, \\ D(x,y) & = & \hat{\delta}(x) + \hat{\varphi}(y) + k_2. \end{array}$$

3 Proof of Proposition 1

Proving that any G, D, T defined as in Proposition 1 satisfy Equation (1) is a straighforward check. We now prove that any solution of Equation (1) is as in Proposition 1.

From Equations (1) and (2), we get:

$$\delta(\psi(x) + \epsilon(y)) + \varphi(\psi(u) + \epsilon(v)) = \psi(\delta(x) + \varphi(u)) + \beta(y) + \gamma(v). \tag{4}$$

When $x = \psi^{-1}(e)$, Equation (4) gives:

$$\delta\epsilon(y) - \beta(y) = \psi(\delta\psi^{-1}(e) + \varphi(u)) + \gamma(v) - \varphi(\psi(u) + \epsilon(v)).$$

Since this equation must be satisfied for any y, u, v, the left and right terms must be equal to a constant value c_1. We deduce:

$$\delta\epsilon(y) - \beta(y) = c_1. \tag{5}$$

Taking $y = \beta^{-1}(e)$, we get:

$$c_1 = \delta\epsilon\beta^{-1}(e).$$

Similarly when $u = \psi^{-1}(e)$, Equation (4) gives:

$$\varphi\epsilon(v) - \gamma(v) = \psi(\delta(x) + \varphi\psi^{-1}(e)) + \beta(y) - \delta(\psi(x) + \epsilon(y)),$$

hence:

$$\varphi\epsilon(v) - \gamma(v) = c_2, \tag{6}$$

where:

$$c_2 = \varphi\epsilon\gamma^{-1}(e).$$

Susbtituting Equations (5) and (6) in Equation (4), we get:

$$\delta(\psi(x) + \epsilon(y)) + \varphi(\psi(u) + \epsilon(v)) = \psi(\delta(x) + \varphi(u)) + \delta\epsilon(y) - c_1 + \varphi\epsilon(v) - c_2.$$

We deduce the following functional equation in δ, ψ and φ only:

$$\delta(\psi(x) + y) + \varphi(\psi(u) + v) = \psi(\delta(x) + \varphi(u)) + \delta(y) + \varphi(v) - c_1 - c_2. \tag{7}$$

Taking $v = e$ and $x = \delta^{-1}(e)$, we get:

$$\psi\varphi(u) - \varphi\psi(u) = \delta\left(\psi\delta^{-1}(e) + y\right) - \delta(y) - \varphi(e) + c_1 + c_2,$$

which implies:

$$\psi\varphi(u) - \varphi\psi(u) = c_3, \tag{8}$$

where:

$$c_3 = \psi\varphi\psi^{-1}\varphi^{-1}(e).$$

Similarly substituting $y = e$ and $u = \varphi^{-1}(e)$ in Equation (7), we get:

$$\psi\delta(x) - \delta\psi(x) = \varphi\left(\psi\varphi^{-1}(e) + v\right) - \delta(e) - \varphi(v) + c_1 + c_2,$$

which implies:

$$\psi\delta(x) - \delta\psi(x) = c_4, \tag{9}$$

where:

$$c_4 = \psi\delta\psi^{-1}\delta^{-1}(e).$$

Equation (7) may be re-written as:

$$\delta\left(\delta^{-1}(x) + \delta^{-1}(y)\right) + \varphi\left(\varphi^{-1}(u) + \varphi^{-1}(v)\right) = \psi\left(\delta\psi^{-1}\delta^{-1}(x) + \varphi\psi^{-1}\varphi^{-1}(u)\right) + y + v - c_1 - c_2.$$

Using Equations (8) and (9), this leads to:

$$\delta\left(\delta^{-1}(x) + \delta^{-1}(y)\right) + \varphi\left(\varphi^{-1}(u) + \varphi^{-1}(v)\right) = \psi\left(\psi^{-1}(x + c_4) + \psi^{-1}(u + c_3)\right) + y + v - c_1 - c_2. \tag{10}$$

Since $+$ is Abelian, we can swap x and y or u and v without changing the left-hand term of Equation (10). We therefore obtain the following functional equation in ψ only:

$$\psi\left(\psi^{-1}(x \oplus c_4) + \psi^{-1}(u \oplus c_3)\right) + y + v = \psi\left(\psi^{-1}(y \oplus c_4) + \psi^{-1}(v \oplus c_3)\right) + x + u.$$

Replacing x by $\psi(x) - c_4$, u by $\psi(u) - c_3$, y by $\psi(y) - c_4$ and v by $\psi(v) - c_3$, we get:

$$\psi(x + u) - \psi(x) - \psi(u) = \psi(y + v) - \psi(y) - \psi(v),$$

hence:

$$\psi(x \oplus u) - \psi(x) - \psi(u) = c_5, \tag{11}$$

for a constant c_5 such that:

$$c_5 = \psi(e + e) - \psi(e) - \psi(e) = e - \psi(e).$$

Using Equation (11), Equation (10) becomes:

$$\delta(\delta^{-1}(x) + \delta^{-1}(y)) + \varphi(\varphi^{-1}(u) + \varphi^{-1}(v)) = x + y + u + v + c_4 + c_3 - \psi(e) - c_1 - c_2,$$

or:

$$\delta(x + y) - \delta(x) - \delta(y) = \varphi(u) + \varphi(v) - \varphi(u + v) + c_4 + c_3 - \psi(e) - c_1 - c_2. \tag{12}$$

This implies:

$$\delta(x + y) - \delta(x) - \delta(y) = c_6, \tag{13}$$

where $c_6 = e \ominus \delta(e)$. On the other hand, Equation (12) also implies:

$$\varphi(u) + \varphi(v) - \varphi(u + v) = c_7, \tag{14}$$

where $c_7 = \varphi(e)$. Let now:

$$\hat{\psi} := \psi - \psi(e).$$

Equation (11) implies

$$\hat{\psi}(x \oplus u) = \psi(x \oplus u) - \psi(e) = \psi(x) + \psi(u) - 2\psi(e) = \hat{\psi}(x) + \hat{\psi}(u), \tag{15}$$

in other words $\hat{\psi}$ is additive for $+$. Similarly, Equations (13) and (14) imply that $\hat{\delta} := \delta - \delta(e)$ and $\hat{\varphi} := \varphi - \varphi(e)$ are additive. Equation (8) and the additivity of $\hat{\varphi}$ and $\hat{\psi}$ now imply:

$$\hat{\psi}\hat{\varphi}(u) + \hat{\psi}\varphi(e) + \psi(e) = \hat{\varphi}\hat{\psi}(u) + \hat{\varphi}\psi(e) + \varphi(e) + c_3.$$

For $u = e$, it follows that:

$$\hat{\psi}\varphi(e) + \psi(e) = \hat{\varphi}\psi(e) + \varphi(e), + c_3$$

hence Equation (8) eventually implies that:

$$\hat{\psi}\hat{\varphi}(u) = \hat{\varphi}\hat{\psi}(u),$$

in other words $\hat{\psi}$ and $\hat{\varphi}$ commute. Similarly, Equation (9) implies that $\hat{\psi}$ and $\hat{\delta}$ commute. By Equations (5) and (6), we have:

$$\beta(x) + \gamma(y) = \delta\epsilon(x) - c_1 + \varphi\epsilon(y) - c_2 = \hat{\delta}\epsilon(x) + \hat{\varphi}\epsilon(y) + \delta(e) + \varphi(e) - c_1 - c_2.$$

Defining $k_1 := \psi(e)$, $k_2 := \delta(e) + \varphi(e)$ and $k_3 := \delta(e) + \varphi(e) - c_1 - c_2$, we deduce from Equation (2) that:

$$\begin{aligned} G(x, y) &= \hat{\psi}(x) + \epsilon(y) + k_1, \\ D(x, y) &= \hat{\delta}(x) + \hat{\varphi}(y) + k_2, \\ T(x, y) &= \epsilon^{-1}\left(\hat{\delta}\epsilon(x) + \hat{\varphi}\epsilon(y) + k_3\right), \end{aligned}$$

with $\hat{\psi}$, $\hat{\delta}$ and $\hat{\varphi}$ with the properties required. Using the additivity of $\hat{\delta}$, $\hat{\varphi}$ and $\hat{\psi}$, we compute:

$$\begin{aligned} D(G(x,y),G(u,v)) &= \hat{\delta}\left(\hat{\psi}(x)+\epsilon(y)+k_1\right)+\hat{\varphi}\left(\hat{\psi}(u)+\epsilon(v)+k_1\right)+k_2, \\ &= \hat{\delta}\hat{\psi}(x)+\hat{\delta}\epsilon(y)+\hat{\delta}(k_1)+\hat{\varphi}\hat{\psi}(u)+\hat{\varphi}\epsilon(v)+\hat{\varphi}(k_1)+k_2, \end{aligned}$$

and:

$$\begin{aligned} G(D(x,u),T(y,v)) &= \hat{\psi}\left(\hat{\delta}(x)+\hat{\varphi}(u)+k_2\right)+(\hat{\delta}\epsilon(y)+\hat{\varphi}\epsilon(v)+k_3)+k_1, \\ &= \hat{\psi}\hat{\delta}(x)+\hat{\psi}\hat{\varphi}(u)+\hat{\psi}(k_2)+\hat{\delta}\epsilon(y)+\hat{\varphi}\epsilon(v)+k_3+k_1. \end{aligned}$$

Since $\hat{\psi}$ commutes with both $\hat{\varphi}$ and $\hat{\delta}$, we deduce:

$$\begin{aligned} G(D(x,u),T(y,v)) &= \hat{\delta}\hat{\psi}(x)+\hat{\varphi}\hat{\psi}(u)+\hat{\psi}(k_2)+\hat{\delta}\epsilon(y)+\hat{\varphi}\epsilon(v)+k_3+k_1, \\ &= D(G(x,y),G(u,v))+\hat{\psi}(k_2)+k_3+k_1-\hat{\delta}(k_1)-\hat{\varphi}(k_1)-k_2. \end{aligned}$$

Equation (1) then implies:

$$k_3=\hat{\delta}(k_1)+\hat{\varphi}(k_1)-k_1+k_2-\hat{\psi}(k_2).$$

This concludes the proof of Proposition 1.

4 Proof of Proposition 2

Proving that any G,D,T defined as in Proposition 2 satisfy Equation (3) is a straighforward check. We now prove that any solution of Equation (3) is as in Proposition 2. By Proposition 1, we have:

$$G(x,y)=\hat{\psi}(x)+\hat{\epsilon}(y)+k_1, \qquad D(x,y)=\hat{\delta}(x)+\hat{\varphi}(y)+k_2$$

for permutations $\hat{\psi},\hat{\delta},\hat{\varphi},\hat{\epsilon}$ such that $\hat{\psi}$, $\hat{\delta}$ and $\hat{\varphi}$ are additive for $+$, and moreover $\hat{\psi}$ commutes with both $\hat{\delta}$ and $\hat{\varphi}$. By symmetry of D and G in Equation (3), $\hat{\epsilon}$ must also be distributive for $+$ and it must commute with both $\hat{\delta}$ and $\hat{\varphi}$. As in the proof of Proposition 1, we compute:

$$D(G(x,y),G(u,v))=\hat{\delta}\hat{\psi}(x)+\hat{\delta}\epsilon(y)+\hat{\delta}(k_1)+\hat{\varphi}\hat{\psi}(u)+\hat{\varphi}\epsilon(v)+\hat{\varphi}(k_1)+k_2.$$

Similarly, we have:

$$G(D(x,y),D(u,v)) = \hat{\psi}\hat{\delta}(x)+\hat{\psi}\hat{\varphi}(u)+\hat{\varphi}(k_2)+\hat{\epsilon}\hat{\delta}(y)+\hat{\epsilon}\hat{\varphi}(v)+\hat{\epsilon}(k_2)+k_1.$$

Equation (3) then leads to:

$$\hat{\delta}(k_1)+\hat{\varphi}(k_1)+k_2=\hat{\psi}(k_2)+\hat{\epsilon}(k_2)+k_1.$$

This concludes the proof of Proposition 2.

Acknowledgement. We thank the anonymous referee for his comments that helped us improve both the content of our main results and their presentation.

References

[1] J. Aczél, V. D. Belousov, and M. Hosszú. Generalized associativity and bisymmetry on quasigroups. *Acta Math. Hungar.*, **11** (1960), 127–136.

[2] V. D. Belousov. Some remarks on the functional equation of generalized distributions. *Aequationes Math.*, **1** (1968), 54–65.

[3] A. Krapez. Functional equations of generalized associativity, bisymmetry, transitivity and distributivity. *Publ. Inst. Math. N.S.*, **30 (44)** (1982), 81–87.