Directly indecomposable finite monogenic entropic quasigroups with quasi-identity

Grzegorz Bińczak⋆
e-mail: binczak@mini.pw.edu.pl
Warsaw University of Technology, Poland
Joanna Kaleta
e-mail: joanna_kaleta@sggw.pl
Warsaw University of Agriculture, Poland

Definition 1. An algebra $(G,+,-,0,^*)$ is *an abelian group with involution* if:
(1) the reduct $(G,+,-,0)$ is an abelian group,
(2) it satisfies the following identities:

$$0^* = 0,\ a^{**} = a,\ (a+b)^* = a^* + b^*.$$

We denote the variety of all abelian groups with involution by AGI.

Definition 2. An algebra $(Q,\cdot,/,\backslash,1)$ is an *entropic quasigroup with quasi-identity* if it satisfies the following
identities:
(1) $a\cdot(a\backslash b) = b$, $(b/a)\cdot a = b$,
(2) $a\backslash(a\cdot b) = b$, $(b\cdot a)/a = b$,
(3) $(a\cdot b)\cdot(c\cdot d) = (a\cdot c)\cdot(b\cdot d)$,
(4) $a\cdot 1 = a$, $1\cdot(1\cdot a) = a$.

One-generated entropic quasigroups with quasi-identity are called *monogenic*.

Note that the identities 1, 2 and 3 define entropic quasigroups, whereas the identities 4 define the quasi-identity. We denote the variety of all entropic quasigroups with quasi-identity by EQ1.

More information concerning entropic quasigroups may be found in [3] and [5]. In the paper [1], it is proved that abelian groups with involution are equivalent to entropic quasigroups with quasi-identity:

Theorem 3. *If* $\mathcal{G} = (G,+,-,0,^*)$ *is an abelian group with involution then* $\Psi(\mathcal{G}) = (G,\cdot,/,\backslash,1)$ *is an entropic quasigroup with quasi-identity, where* $a\cdot b := a+(b^*)$, $a\backslash b := b^* + (-a^*)$, $a/b := a + (-b^*)$, $1 := 0$.

Theorem 4. *If* $\mathcal{Q} = (Q,\cdot,/,\backslash,1)$ *is an entropic quasigroup with quasi-identity then* $\Phi(\mathcal{Q}) = (Q,+,-,0,^*)$ *is an abelian group with involution, where* $a+b := a\cdot(1\cdot b)$, $(-a) := 1/(1\cdot a)$, $0 := 1$, $a^* := 1\cdot a$.

Abelian groups with involution form a special case of Ω-groups (see [4]).

Theorem 5 ([4], Theorem 6.39 (Krull-Schmidt))**.** *Let G be an Ω-group having both chain conditions on admissible subgroups. If*

$$G = H_1\times\ldots\times H_s = K_1\times\ldots\times K_t$$

are two decompositions of G into Ω-indecomposable factors, then $s = t$ and there is a reindexing so that $H_i \cong K_i$ for all i. Moreover, given any r between 1 and s, the reindexing may be chosen so that $G = H_1 \times \ldots \times H_r \times K_{r+1} \times \ldots \times K_s$.

The above Theorem implies that every finite entropic quasigroup with quasi-identity has the unique decomposition into indecomposable factors up to reindexing and isomorphism of these factors.

This talk consists of two parts. In the first part we recall some definitions and propositions from [1] and describe the class of finite monogenic entropic quasigroups with quasi-identity up to isomorphism. In the second part we give some conditions under which one finite monogenic entropic quasigroups with quasi-identity is a homomorphic image of another one. Moreover we give the sketch of the proof that directly indecomposable finite monogenic entropic quasigroup with quasi-identity has additive rank p^n, where p is prime. We give some examples of directly indecomposable finite monogenic entropic quasigroup with quasi-identity.

Let $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ be a monogenic entropic quasigroup with quasi-identity. Let $Q = \langle x \rangle$ and let $\Phi(\mathcal{Q}) = (Q, +, -, 0, ^*)$ be the abelian group with involution equivalent to $(Q, \cdot, /, \backslash, 1)$.

We define three types of *rank* of the generator x:

$$r_+(x) = \min\{n \in \mathbb{N} \mid nx = 0,\, n \geq 1\},$$
$$r_*(x) = \min\{n \in \mathbb{N} \mid n \geq 1,\ \exists_{k\in\mathbb{Z}}\ nx^* = kx\},$$
$$r_{*+}(x) = \min\{n \in \mathbb{N} \mid r_*(x)x^* = (r_*(x) + n)x\}.$$

Note that $r_+(x)$ is the usual rank of x in an abelian group.

Then we define

$$r_+(\mathcal{Q}) = r_+(x),\ r_*(\mathcal{Q}) = r_*(x),\ r_{*+}(\mathcal{Q}) = r_{*+}(x).$$

This definition does not depend on the choice of the generator x.

We denote the integer part of a by $E(a)$, whereas $(a)_b$ denotes the remainder obtained after dividing a by b.

Definition 6. Let $a, b, k \in \mathbb{N}$ and $a, b \geq 1$. Let $\gamma^k_{a,b} : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ be a mapping such that

$$\gamma^k_{a,b}(x, y) = ((x + E\left(\frac{y}{b}\right)(b + k))_a, (y)_b)$$

and let

$$(x, y) \oplus^k_{a,b} (z, t) = \gamma^k_{a,b}(x + z, y + t).$$

Definition 7. Let $a, b, k \in \mathbb{Z}$ and $a \geq 1, b \geq 1, k \geq 0$. Define

$$G^k_{a,b} = \left(\mathbb{Z}_a \times \mathbb{Z}_b, \oplus^k_{a,b}, \ominus^k_{a,b}, (0, 0), ^*\right),$$

where $\ominus^k_{a,b}(x, y) = \gamma^k_{a,b}(-x, -y)$ and $(x, y)^* = \gamma^k_{a,b}(y, x)$.

Let $Q^k_{a,b} = \Psi(G^k_{a,b})$ and $D = \{(a, b, k) \in \mathbb{Z}^3 \colon a \geq 1, b \geq 1, 0 \leq k < a, b|a, b|k, a|(2k + \frac{k^2}{b})\}$.

Theorem 8 ([1], Theorem 10)**.** *Let $(a, b, k) \in D$. Then $G^k_{a,b}$ is an abelian group with involution.*

Theorem 9 ([1], Theorem 11). *Let* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *be a finite cyclic entropic quasigroup with quasi-identity and* $a = r_+(Q)$, $b = r_*(Q)$, $k = r_{*+}(Q)$. *Then* $\mathcal{Q} \cong Q^k_{a,b}$.

The following Proposition gives some conditions under which one finite monogenic entropic quasigroups with quasi-identity is a homomorphic image of another one.

Proposition 10. *Let* $(a, b, k), (a', b', k') \in D$. *If*

$$a|a', \quad b|b', \quad a|(k' - \frac{b'}{b}k),$$

then

$$\gamma^k_{a,b}|_{\mathbb{Z}_{a'} \times \mathbb{Z}_{b'}} : \mathbb{Z}_{a'} \times \mathbb{Z}_{b'} \longrightarrow \mathbb{Z}_a \times \mathbb{Z}_b$$

is a homomorphism of $Q^{k'}_{a',b'}$ *onto* $Q^k_{a,b}$.

Theorem 11. *Let* $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, $a_1, a_2, b_1, b_2 \geq 1$, $\gcd(a_1, a_2) = 1$, $b_1|a_1$, $b_2|a_2$, $(a_1a_2, b_1b_2, k) \in D$. *If* $k_1 = \left(\frac{k}{b_2}\right)_{a_1}$ *and* $k_2 = \left(\frac{k}{b_1}\right)_{a_2}$ *then* $(a_1, b_1, k_1), (a_2, b_2, k_2) \in D$ *and*

$$Q^k_{a_1a_2, b_1b_2} \cong Q^{k_1}_{a_1,b_1} \times Q^{k_2}_{a_2,b_2}.$$

Theorem 12. *Let* $\mathcal{Q}$ *be a finite monogenic quasigroup in EQ1 with at least two different elements. If* $\mathcal{Q}$ *is directly indecomposable then* $r_+(\mathcal{Q}) = p^n$, *where* p *is prime.*

In the following Proposition we describe finite monogenic algebras in EQ1 for which additive rank is equal to p^n.

Proposition 13. *Let* $\mathcal{Q}$ *be a finite monogenic algebra in EQ1. If* $r_+(\mathcal{Q}) = p^n$, *where* p *is prime then* $\mathcal{Q}$ *is isomorphic to one of the following algebras in EQ1:*

(1) $Q^0_{p^n,p^m}$, $m \leq n$

(2) $Q^{p^n-2p^m}_{p^n,p^m}$, $m + 1 \leq n$

(3) $Q^{2^{n-1}}_{2^n,2^m}$, $m + 2 \leq n$

(4) $Q^{2^{n-1}-2^{m+1}}_{2^n,2^m}$, $m + 2 \leq n$.

Proposition 14. *If* $0 \leq m \leq n$ *then* $Q^0_{2^n,2^m}$ *is directly indecomposable.*

Proposition 15. *If* $0 < m \leq n$ *and* $p \neq 2$ *is prime then* $Q^0_{p^n,p^m}$ *is directly decomposable.*

References

[1] G. Bińczak, J. Kaleta, *Cyclic entropic quasigroups*, Demonstratio Mathematicae 42 (2009), 269–281.

[2] G. Bińczak, J. Kaleta, *Finite simple monogenic entropic quasigroups with quasi-identity*, to appear in Demonstratio Mathematicae

[3] O. Chein, H.O. Pflugfelder, J.D.H. Smith, *Quasigroups and Loops: Theory and Applications*, Heldermann Verlag, Berlin, 1990.

[4] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, New York, 1994
[5] J.D.H. Smith, *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, 1986