DEMONSTRATIO MATHEMATICA
Vol. XLV No 3 2012
10.1515/dema-2013-0397

G. Bińczak, J. Kaleta

FINITE DIRECTLY INDECOMPOSABLE MONOGENIC ENTROPIC QUASIGROUPS WITH QUASI-IDENTITY

Abstract. In this paper we characterize finite directly indecomposable monogenic entropic quasigroups with quasi-identity.

1. Introduction

This paper consists of three parts.

In the first part we recall some definitions and propositions from [1] and [2] and describe the set of ordered triples beeing the ranks of finite monogenic algebras in EQ1.

In the second part we characterize finite monogenic algebras in EQ1 having $r_+(\mathcal{Q}) = p^n$ for p prime.

In the third part we characterize finite monogenic algebras in EQ1 which are directly indecomposable. First, we prove that if $\mathcal{Q}$ is a nontrivial finite directly indecomposable monogenic entropic quasigroups with quasi-identity then $r_+(\mathcal{Q}) = p^n$, where p is prime. Then, we show that if a finite monogenic algebra in EQ1 has the additive rank of the form 2^n, where $n > 0$, then it is directly indecomposable. Next, we show that if a finite monogenic algebra in EQ1 has the additive rank of the form p^n, where $p \neq 2$ is prime and the rank r_* of the form p^m, where $m > 0$ then it is directly decomposable. Finally, we describe which finite monogenic algebras in EQ1 are directly indecomposable.

Definition 1.1. An algebra $(G, +, -, 0, ^*)$ is *an abelian group with involution* if:

(1) the reduct $(G, +, -, 0)$ is an abelian group,

2000 *Mathematics Subject Classification*: 20N05.
Key words and phrases: quasigroups, entropic quasigroups, abelian groups, involution.
Research supported by the Warsaw University of Technology under grant number 504G/1120/0054/000.

(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 1.2. 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) $a \cdot 1 = a$, $1 \cdot (1 \cdot a) = a$.

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 1.3. [1, 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 1.4. [1, 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 $a + b := a \cdot (1 \cdot b)$, $(-a) := 1/(1 \cdot a)$, $0 := 1$, $a^* := 1 \cdot a$.*

Theorem 1.5. [1, Theorem 5] *If $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ is an entropic quasigroup with quasi-identity then $\Psi(\Phi(\mathcal{Q})) = \mathcal{Q}$.*

Theorem 1.6. [1, Theorem 6] *If $\mathcal{G} = (G, +, -, 0, ^*)$ is an abelian group with involution then $\Phi(\Psi(\mathcal{G})) = \mathcal{G}$.*

Definition 1.7. One-generated entropic quasigroups with quasi-identity are called *monogenic*.

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:

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

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 (see [1]).

Theorem 1.8. [1, Theorem 8] *If $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ is a finite monogenic entropic quasigroup with quasi-identity, then the following hold:*

(1) $r_*(\mathcal{Q}) | r_+(\mathcal{Q})$,
(2) $r_*(\mathcal{Q}) | r_{*+}(\mathcal{Q})$,
(3) $0 \leq r_{*+}(\mathcal{Q}) < r_+(\mathcal{Q})$,
(4) $r_+(\mathcal{Q}) | 2r_{*+}(\mathcal{Q}) + \frac{r_{*+}(\mathcal{Q})^2}{r_*(\mathcal{Q})}$.

Note that in [1] monogenic quasigroups were called cyclic.

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

Definition 1.9. 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

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

and let

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

Let $T : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be a function such that $T(x, y) = (y, x)$.

Definition 1.10. Let $a, b, k \in \mathbb{Z}$ and $a \geq 1, b \geq 1, k \geq 0$. Define

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

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

Theorem 1.11. [1, Theorem 10] *Let $a, b, k \in \mathbb{Z}$ with $a \geq 1$, $b \geq 1$, $k \geq 0$ and $b|a$, $b|k$, $0 \leq k < a$, $a|(2k + \frac{k^2}{b})$. Then $Q^k_{a,b}$ is an abelian group with involution.*

Theorem 1.12. [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 $\Phi(\mathcal{Q}) \cong \mathcal{Q}^k_{a,b}$.*

Proposition 1.13. [2, Proposition 1.12] *Let $\mathcal{Q}$ be a finite monogenic algebra in EQ1 such that $\Phi(\mathcal{Q}) = Q^k_{a,b}$. Then $a = r_+(\mathcal{Q})$, $b = r_*(\mathcal{Q})$, $(k)_a = r_{*+}(\mathcal{Q})$.*

We define the set D. As we will see in a moment, it is the set of ordered triples beeing the ranks of finite monogenic algebras in EQ1.

Definition 1.14. Let $D = \{(a, b, k) \in \mathbb{Z}^3 \colon a \geq 1, b \geq 1, 0 \leq k < a, b|a, b|k, a|(2k + \frac{k^2}{b})\}$.

Theorem 1.15. *$D = \{(a,b,k) \in \mathbb{Z}^3$: there exists finite monogenic $\mathcal{Q}$ in* EQ1 *such that $a = r_+(\mathcal{Q})$, $b = r_*(\mathcal{Q})$ and $k = r_{*+}(\mathcal{Q})\}$.*

Proof. If there exists finite monogenic $\mathcal{Q}$ in EQ1 such that $a = r_+(\mathcal{Q})$, $b = r_*(\mathcal{Q})$ and $k = r_{*+}(\mathcal{Q})$ then $(a,b,k) \in D$ by Theorem 1.8.

If $(a,b,k) \in D$ then $Q^k_{a,b}$ is an abelian group with involution by Theorem 1.11. Then the algebra $\mathcal{Q} = \Psi(Q^k_{a,b})$ is a finite monogenic quasigroup in EQ1 by Theorem 1.3. By Theorem 1.6 we have $\Phi(\mathcal{Q}) = Q^k_{a,b}$ therefore according to Proposition 1.13 $r_+(\mathcal{Q}) = a$, $r_*(\mathcal{Q}) = b$, $r_{*+}(\mathcal{Q}) = (k)_a = k$ (since $0 \le k < a$). ∎

Proposition 1.16. *If $(a,b,k) \in D$ then $(\frac{a}{b}, 1, \frac{k}{b}) \in D$.*

Proof. Let $(a,b,k) \in D$. It is obvious that $0 \le \frac{k}{b} < \frac{a}{b}$. We show that

$$\frac{a}{b} \Big| \left(2\frac{k}{b} + \frac{(\frac{k}{b})^2}{1} \right). \tag{1.1}$$

We know that $a|(2k + \frac{k^2}{b})$, $b|a$ and $b|k$. Hence

$$\frac{a}{b} \Big| \left(2\frac{k}{b} + \frac{k^2}{b^2} \right)$$

and (1.1) is satisfied. ∎

2. Algebras in EQ1 having $r_+(\mathcal{Q}) = p^n$

Proposition 2.1. *Let $b = 1$ and $a = p^n$, where p is prime. Then $(a,b,k) \in D$ if and only if one of the following conditions is satisfied*

(1) $k = 0$,
(2) $k = p^n - 2$ *and* $n \ge 1$,
(3) $p = 2$, $k = 2^{n-1}$ *and* $n \ge 2$,
(4) $p = 2$, $k = 2^{n-1} - 2$ *and* $n \ge 2$.

Proof. It is easy to check that $(a,b,k) \in D$ if the conditions given above are fullfiled.

Let $b = 1$ and $a = p^n$, where p is prime. Let $(a,b,k) \in D$. Then

$$a = p^n | (2k + k^2) = k(k+2), \quad 0 \le k < p^n. \tag{2.1}$$

Suppose that $k \neq 0$ then

$$k = p^l \cdot x, \quad k + 2 = p^m \cdot y, \tag{2.2}$$

where $p \nmid x$ and $p \nmid y$. We know that $(a,b,k) \in D$, so $p^l \cdot x = k < a = p^n$ hence

$$l < n. \tag{2.3}$$

Moreover $2k + k^2 = k(k+2) = p^{l+m}xy$ and $p \nmid xy$ (since p is prime). Thus

$$n \leq l + m \tag{2.4}$$

by (2.1).

We have $l < n \leq l + m$ by (2.3) and (2.4). It follows that $0 < m$ and

$$p|k+2 \tag{2.5}$$

by (2.2).

We first show that

$$p \nmid k \Rightarrow k = p^n - 2. \tag{2.6}$$

If $p \nmid k$ then $p^n|k+2$ (by (2.1)) thus $p^n \leq k+2$ hence $p^n = k+2$ or $p^n = k+1$ using (2.1). If $p^n = k+1$ then $k+1|k+2$ and $k = 0$ - a contradiction. Therefore $p^n = k+2$ so $k = p^n - 2$ and $n \geq 1$ by (2.3). So we obtain the case 2.

Suppose that $p|k$. By (2.5) we have $p|k+2$ hence $p = 2$ and $l \geq 1$ by (2.2).

If $n = 1$ then $2|2k + k^2$ and $0 \leq k < 2$ thus $k = 0$ - a contradiction. Hence $n \geq 2$. Moreover

$$k + 2 = 2^l x + 2 = 2(2^{l-1}x + 1) \tag{2.7}$$

by(2.2).

Consider the following cases:

(1) $l > 1$. Then $l - 1 > 0$ and $2 \nmid 2^{l-1}x + 1$. By (2.1) and (2.7) we have $2^n|k(k+2) = 2^l x 2(2^{l-1}x + 1)$ hence $n \leq l + 1$. So $n = l + 1$ by (2.3). Therefore $l = n - 1$, $k = 2^{n-1}x < 2^n$ by (2.1). It means that $x = 1$ and $k = 2^{n-1}$. So we obtain the case 3.

(2) $l = 1$. Then $k = 2x$, $k+2 = 2x+2 = 2(x+1)$ and $2^n|k(k+2) = 4x(x+1)$ by (2.1). Hence $2^{n-2}|x(x+1)$ and $2^{n-2}|x+1$ since $2 \nmid x$. Let

$$x + 1 = 2^{n-2}z. \tag{2.8}$$

Moreover $2(x+1) = k + 2 < 2^n + 2 = 2(2^{n-1} + 1)$ by (2.1). Thus $x + 1 < 2^{n-1} + 1$ and $x + 1 \leq 2^{n-1}$ so $x + 1 = 2^{n-2}$ or $x + 1 = 2^{n-2}2$ by (2.8). If $x + 1 = 2^{n-2}$ then $x = 2^{n-2} - 1$ and $k = 2x = 2^{n-1} - 2$. So we obtain the case 4. If $x + 1 = 2^{n-2}2$ then $x = 2^{n-1} - 1$ and $k = 2x = 2^n - 2$. So we obtain the case 2. ∎

Proposition 2.2. *Let $a = p^n$, where p is prime. Then $(a, b, k) \in D$ if and only if $b = p^m$ and one of the following conditions is satisfied*

(1) $m \leq n$ *and* $k = 0$,
(2) $m + 1 \leq n$ *and* $k = p^n - 2p^m$,
(3) $m + 2 \leq n$, $p = 2$ *and* $k = 2^{n-1}$,
(4) $m + 2 \leq n$, $p = 2$ *and* $k = 2^{n-1} - 2^{m+1}$.

Proof. It is easy to check that $(a, b, k) \in D$ if the conditions given above are satisfied.

Let $a = p^n$, where p is prime. Let $(a, b, k) \in D$. Then $b|a$ so $b = p^m$ and $m \leq n$. By Proposition 1.16 we have $(\frac{a}{b}, 1, \frac{k}{b}) \in D$. Hence by Proposition 2.1 one of the above conditions is fullfiled. ∎

The following theorem characterizes finite monogenic algebras in EQ1 having $r_+(\mathcal{Q}) = p^n$ for p prime.

Theorem 2.3. *Let $\mathcal{Q}$ be a finite monogenic algebra in* EQ1. *Let $a = r_+(\mathcal{Q})$, $b = r_*(\mathbf{Q})$ and $k = r_{*+}(\mathcal{Q})$. If $a = p^n$, where p is prime then $\mathcal{Q}$ is isomorphic to one of the following algebras in* EQ1:

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

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

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

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

Proof. It is easy to check that the following algebras:

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

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

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

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

are in EQ1 by Theorems 1.11 and 1.3.

Let $\mathcal{Q}$ be a finite monogenic algebra in EQ1. Let $a = r_+(\mathcal{Q})$, $b = r_*(\mathbf{Q})$ and $k = r_{*+}(\mathcal{Q})$. Then $\mathcal{Q}$ is equivalent to the algebra $Q^k_{a,b}$ using Theorem 1.12. By Theorem 1.8 we have $(a, b, k) \in D$. Hence $\mathcal{Q}$ is isomorphic to one of the above algebras by Proposition 2.2. ∎

3. Directly indecomposable algebras in EQ1

Definition 3.1. An algebra $\mathcal{Q}$ is directly indecomposable if $|\mathcal{Q}| \neq 1$ and if $\mathcal{Q} = \mathcal{Q}_1 \times \mathcal{Q}_2$ implies $|\mathcal{Q}_1| = 1$ or $|\mathcal{Q}_2| = 1$.

The following proposition gives some conditions under which one finite monogenic entropic quasigroup with quasi-identity is a homomorphic image of another one. This proposition also serves as the technical help in proving Theorem 3.3.

Proposition 3.2. [2, Proposition 2.3] *Let* $(a,b,k),(a',b',k') \in D$. *If*

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

then

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

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

The following theorem gives the conditions under which some algebras in EQ1 are directly decomposable.

Theorem 3.3. *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* $k_1 = (\frac{k}{b_2})_{a_1}$ *and* $k_2 = (\frac{k}{b_1})_{a_2}$ *then* $(a_1,b_1,k_1),(a_2,b_2,k_2) \in D$ *and*

$$\mathcal{Q} \cong \mathcal{Q}_1 \times \mathcal{Q}_2,$$

where $\mathcal{Q}$ *is equivalent to* $Q^k_{a_1a_2,b_1b_2}$, $\mathcal{Q}_1$ *is equivalent to* $Q^{k_1}_{a_1,b_1}$ *and* $\mathcal{Q}_2$ *is equivalent to* $Q^{k_2}_{a_2,b_2}$.

Proof. First we show that $(a_1,b_1,k_1) \in D$. It remains to prove that $b_1|k_1$ and $a_1|2k_1 + \frac{k_1^2}{b_1}$. We know that $(a_1a_2,b_1b_2,k) \in D$ hence

$$a_1a_2|2k + \frac{k^2}{b_1b_2}, \tag{3.1}$$

$b_1b_2|k$ and $b_1|k$, $b_2|k$ thus $b_1|\frac{k}{b_2}$ and $b_1|k_1$ since $b_1|a_1$.

We have $a_1b_2|a_1a_2$ since $b_2|a_2$. Then $a_1b_2|2k + \frac{k^2}{b_1b_2}$ by (3.1). Hence

$$a_1|2\frac{k}{b_2} + \frac{k^2}{b_1b_2^2}. \tag{3.2}$$

Let $\frac{k}{b_2} = ta_1 + r$ where $0 \leq r < a_1$. Then $k_1 = r = \frac{k}{b_2} - ta_1$ and

$$\begin{aligned} 2k_1 + \tfrac{k_1^2}{b_1} &= 2\left(\tfrac{k}{b_2} - ta_1\right) + \tfrac{\left(\frac{k}{b_2} - ta_1\right)^2}{b_1} \\ &= 2\tfrac{k}{b_2} + \tfrac{k^2}{b_1b_2^2} - 2ta_1 - 2t\tfrac{k}{b_1b_2}a_1 + t\tfrac{a_1}{b_1}a_1 \end{aligned}$$

hence $a_1|2k_1 + \frac{k_1^2}{b_1}$ by (3.2). It ends the proof that $(a_1,b_1,k_1) \in D$.

Simillarly $(a_2,b_2,k_2) \in D$.

Let $h\colon \mathbb{Z}_{a_1a_2} \times \mathbb{Z}_{b_1b_2} \to (\mathbb{Z}_{a_1} \times \mathbb{Z}_{b_1}) \times \mathbb{Z}_{a_2} \times \mathbb{Z}_{b_2}$ be a function such that

$$h(x,y) = (\gamma^{k_1}_{a_1,b_1}(x,y), \gamma^{k_2}_{a_2,b_2}(x,y)).$$

By Proposition 3.2 $\gamma^{k_1}_{a_1,b_1}|\mathbb{Z}_{a_1a_2} \times \mathbb{Z}_{b_1b_2}$ is a homomorphism of $Q^k_{a_1a_2,b_1b_2}$ onto $Q^{k_1}_{a_1,b_1}$ and $\gamma^{k_2}_{a_2,b_2}|\mathbb{Z}_{a_1a_2} \times \mathbb{Z}_{b_1b_2}$ is a homomorphism of $Q^k_{a_1a_2,b_1b_2}$ onto $Q^{k_2}_{a_2,b_2}$. Hence h is a homomorphism of $Q^k_{a_1a_2,b_1b_2}$ into $Q^{k_1}_{a_1,b_1} \times Q^{k_2}_{a_2,b_2}$.

We show that $\ker h = \{(0,0)\}$. Let $(x,y) \in \mathbb{Z}_{a_1a_2} \times \mathbb{Z}_{b_1b_2}$ and $h(x,y) = ((0,0),(0,0))$ then $\gamma^{k_1}_{a_1,b_1}(x,y) = (0,0)$ and $\gamma^{k_2}_{a_2,b_2}(x,y) = (0,0)$.

Hence

$$a_1|x + E\left(\frac{y}{b_1}\right)(b_1+k_1), \quad b_1|y, \quad a_2|x + E\left(\frac{y}{b_2}\right)(b_2+k_2), \quad b_2|y \tag{3.3}$$

thus $b_1b_2|y$ (since $\gcd(b_1,b_2) = 1$) so $y = 0$. Therefore $a_1|x$, $a_2|x$ by (3.3). Hence $a_1a_2|x$ (since $\gcd(a_1,a_2) = 1$) so $x = 0$. Thus $\ker k = \{(0,0)\}$ so h is injective.

Moreover $|\mathcal{Q}| = |\mathcal{Q}_1 \times \mathcal{Q}_2| = a_1a_2b_1b_2$ so h is an isomorphism. ∎

The following theorem says what is the additive rank of every directly indecomposable algebra in EQ1.

Theorem 3.4. *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.*

Proof. Let $b = r_*(\mathcal{Q})$, $k = r_{*+}(\mathcal{Q})$ and $a = r_+(\mathcal{Q}) \neq p^n$, where p is prime. Let $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$, $b = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}$, where p_i are different prime numbers, $m_1 \geq 0, \ldots m_r \geq 0$ and $l_1 \geq 0, \ldots, l_r \geq 0$. We can assume that $m_1 > 0$ and $m_2 > 0$ since $a \neq p^n$, where p is prime.

Let $a_1 = p_1^{m_1}$, $a_2 = p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$, $b_1 = p_1^{l_1}$, $b_2 = p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}$, $k_1 = (\frac{k}{b_2})_{a_1}$ and $k_2 = (\frac{k}{b_1})_{a_2}$.

By Theorem 3.3

$$\mathcal{Q} \cong \mathcal{Q}_1 \times \mathcal{Q}_2,$$

where $\mathcal{Q}_1$ is equivalent to $Q^{k_1}_{a_1,b_1}$ and $\mathcal{Q}_2$ is equivalent to $Q^{k_2}_{a_2,b_2}$.

Moreover $a_1 > 1$ and $a_2 > 1$ since $m_1 > 0$ and $m_2 > 0$ so $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are nontrivial. Therefore $\mathcal{Q}$ is directly decomposable. ∎

The following two lemmas concerning entropic quasigroups with quasi-identity can be proved similarly like for abelian groups.

Lemma 3.5. *Let $\mathcal{Q} \in$ EQ1 be a finite quasigroup and $|\mathcal{Q}| > 1$. Then $\mathcal{Q}$ is directly decomposable if and only if there are B and C being subalgebras of $\mathcal{Q}$ such that $B \cap C = \{0\}$, $B \cup C$ generates $\mathcal{Q}$, $|B| > 1$ and $|C| > 1$.*

Lemma 3.6. *Let $\mathcal{Q} \in$ EQ1 be a finite quasigroup and $|Q| > 1$. Then $\mathcal{Q}$ is directly decomposable if and only if there are B and C being subalgebras of $\mathcal{Q}$ such that $B \cap C = \{0\}$, $|B| \cdot |C| = |Q|$, $|B| > 1$ and $|C| > 1$.*

Lemma 3.7. *Let $\mathcal{Q} \in$ EQ1 be a finite quasigroup. If there exists the bigest nontrivial ($\neq Q$) subalgebra of $\mathcal{Q}$, then $\mathcal{Q}$ is directly indecomposable.*

Proof. Let A be the bigest nontrivial subalgebra of $\mathcal{Q}$. Assume that $\mathcal{Q}$ is directly decomposable. By Lemma 3.5 there are B and C being subalgebras of $\mathcal{Q}$ such that $B \cap C = \{0\}$, $B \cup C$ generates $\mathcal{Q}$, $|B| > 1$ and $|C| > 1$. Since

A is the bigest nontrivial subalgebra of $\mathcal{Q}$, we have $B \subseteq A$ and $C \subseteq A$ hence $B \cup C \subseteq A$ and $Q \subseteq A$ a contradiction since A is nontrivial. Therefore $\mathcal{Q}$ is directly indecomposable. ∎

Lemma 3.8. *If* $(2^n, 2^m, k) \in D$ *then* $2|k$.

Proof. If $m > 0$ then $2^m|k$ so $2|k$. Suppose that $m = 0$. If $n = 0$, then $k = 0$ and $2|k$. If $n > 0$ then $2|2^n$ and $2^n|2k + k^2$ (since $(2^n, 2^m, k) \in D$) hence $2|k(k + 2)$ so $2|k$. ∎

Theorem 3.9. *Let* $\mathcal{Q} \in$ EQ1 *be a finite and monogenic quasiqroup,* $r_+(\mathcal{Q}) = 2^n$, $r_*(\mathcal{Q}) = 2^m$ *and* $n > 0$ *then* $\mathcal{Q}$ *is directly indecomposable.*

Proof. By Theorem 1.12 $\Phi(\mathcal{Q}) \cong Q^k_{2^n,2^m}$ where $k = r_{*+}(\mathcal{Q})$. Hence $\mathcal{Q} \cong \Psi(Q^k_{2^n,2^m})$.

Let $A = \{(x, y) \in \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^m} \colon 2|x + y\}$. First we prove that A is a subalgebra of $Q^k_{2^n,2^m}$.

(1) If $(x, y) \in A$ then $(x, y)^* = \gamma^k_{2^n,2^m}(y, x) = ((y+E(\frac{x}{2^m})(2^m+k))_{2^n}, (x)_{2^m})$.
If $m > 0$ then $(y + E(\frac{x}{2^m})(2^m + k))_{2^n} + (x)_{2^m} \equiv_2 y + x \equiv_2 0$ by Lemma 3.8.
If $m = 0$ then $(y + E(\frac{x}{2^m})(2^m + k))_{2^n} + (x)_{2^m} \equiv_2 y + x(1 + k) \equiv_2 0$ by Lemma 3.8, so $(x, y)^* \in A$.

(2) Let $(x, y) \in A$ and $(z, t) \in A$. Then $(x, y) \oplus^k_{2^n,2^m} (z, t) = \gamma^k_{2^n,2^m}(x + z, y + t) = ((x + z + E(\frac{y+t}{2^m})(2^m + k))_{2^n}, (y + t)_{2^m})$.
If $m > 0$ then $(x+z+E(\frac{y+t}{2^m})(2^m+k))_{2^n}+(y+t)_{2^m} \equiv_2 x+z+y+t \equiv_2 0$ by Lemma 3.8.
If $m = 0$ then $y = t = 0$ and $(x + z + E(\frac{y+t}{2^m})(2^m + k))_{2^n} + (y + t)_{2^m} \equiv_2 x + z \equiv_2 0$ so $(x, y) \oplus^k_{2^n,2^m} (z, t) \in A$.

We show that A is the bigest nontrivial subalgebra of $Q^k_{2^n,2^m}$. We prove that if $(x, y) \in Q^k_{2^n,2^m} \setminus A$ then (x, y) generates $Q^k_{2^n,2^m}$.

Let $(x, y) \in Q^k_{2^n,2^m} \setminus A$. It is enough to show that there exist $z_1, z_2 \in \mathbb{Z}$ such that $z_1(x, y) \oplus^k_{2^n,2^m} z_2(x, y)^* = (1, 0)$. Since $(x, y) \notin A$ we obtain $2 \nmid x + y$ so $\gcd(x + y, 2^n) = 1$, hence there are $t, s \in \mathbb{Z}$ such that $t(x + y) + s2^n = 1$. Similarly $\gcd((x - y)_{2^n}, 2^n) = 1$ and there are $u, v \in \mathbb{Z}$ such that $u(x - y)_{2^n} + v2^n = 1$. It is easy to check that

$$(-uyt + u)(x, y) \oplus^k_{2^n,2^m} (-uyt)(x, y)^* = (1, 0),$$

so (x, y) generates $Q^k_{2^n,2^m}$.

Hence A is the bigest nontrivial subalgebra of $Q^k_{2^n,2^m}$. Therefore $Q^k_{2^n,2^m}$ is directly indecomposable by Lemma 3.7. Thus $\mathcal{Q}$ is directly indecomposable. ∎

Contrary to abelian groups there are monogenic entropic quasigroups having an additve rank p^n (where p is prime) which are directly decomposable as we can see in the following theorem:

Theorem 3.10. *Let $\mathcal{Q} \in$ EQ1 be a finite and monogenic quasiqroup. If $r_+(\mathcal{Q}) = p^n$, $r_*(\mathcal{Q}) = p^m$ and $r_{*+}(\mathcal{Q}) = p^n - 2p^m$ where $p \neq 2$ is prime and $m > 0$, then $\mathcal{Q}$ is directly decomposable.*

Proof. It is sufficient to show that $\Psi(Q^0_{p^n,p^m}) \cong \mathcal{Q}$ is directly decomposable.

Let B be the subalgebra of $Q^k_{p^n,p^m}$ generated by $(p^n - 1, 1)$. Let C be the subalgebra of $Q^k_{p^n,p^m}$ generated by $(1, 1)$.

We show that $r_+(1,1) = p^m$, $r_*(1,1) = 1$, $r_{*+}(1,1) = 0$.

Let us observe that

$$\begin{aligned} p^m(1,1) &= \gamma^{p^n-2p^m}_{p^n,p^m}(p^m, p^m) \\ &= \left(\left(p^m + E(\frac{p^m}{p^m})(p^n - p^m)\right)_{p^n}, (p^m)_{p^m}\right) = (0,0) \end{aligned}$$

and

$$\begin{aligned} s(1,1) &= \gamma^{p^n-2p^m}_{p^n,p^m}(s, s) \\ &= \left(\left(s + E(\frac{k}{p^m})(p^n - p^m)\right)_{p^n}, (s)_{p^m}\right) \\ &= ((s)_{p^n}, (s)_{p^m}) = (s, s) \neq (0,0) \end{aligned}$$

for $0 < s < p^m$.

Moreover $(1,1)^* = (1,1)$. Hence $r_+(1,1) = p^m$, $r_*(1,1) = 1$, $r_{*+}(1,1) = 0$ and $|C| = p^m > 1$ since $m > 0$. Thus

$$C = \{(s,s) \in \mathbb{Z} \times \mathbb{Z} \colon 0 \leq s < p^m\}. \tag{3.4}$$

We prove that $r_+(p^n - 1, 1) = p^n$ and $r_*(p^n - 1, 1) = 1$.

We know that $s = E(\frac{s}{p^m})p^m + (s)_{p^m}$ for $s \in \mathbb{Z}$. Hence

$$p^m E\left(\frac{s}{p^m}\right) = s - (s)_{p^m}. \tag{3.5}$$

Let us notice that

$$\begin{aligned} p^n(p^n - 1, 1) &= \gamma^{p^n-2p^m}_{p^n,p^m}(p^n p^n - p^n, p^n) \\ &= \left(\left(p^{2n} - p^n + E\left(\frac{p^n}{p^m}\right)(p^n - p^m)\right)_{p^n}, (p^n)_{p^m}\right) = (0,0) \end{aligned}$$

and

$$
\begin{aligned}
(3.6)\qquad s(p^n-1,1) &= \gamma_{p^n,p^m}^{p^n-2p^m}(sp^n-s,s)\\
&= \left(\left(sp^n-s+E\left(\frac{s}{p^m}\right)(p^n-p^m)\right)_{p^n},(s)_{p^m}\right)\\
&= \left(-s-p^mE\left(\frac{s}{p^m}\right)_{p^n},(s)_{p^m}\right)\\
&\overset{(3.5)}{=} (((s)_{p^m}-2k)_{p^n},(s)_{p^m})\neq(0,0)
\end{aligned}
$$

for $0<s<p^n$ because if $((s)_{p^m}-2s)_{p^n}=(s)_{p^m}=0$ then $p^n|2s$ and then $p^n|s$ for $p\neq 2$ but $p^n\nmid s$ for $0<s<p^n$ - a contradiction.

Let us observe that

$$
\begin{aligned}
(p^n-1,1)^* &= \gamma_{p^n,p^m}^{p^n-2p^m}(1,p^n-1)\\
&= \left(\left(1+E\left(\frac{p^n-1}{p^m}\right)(p^n-p^m)\right)_{p^n},(p^n-1\Big)_{p^m}\right)\\
&= \left(\left(1-p^mE\left(\frac{p^n-1}{p^m}\right)\right)_{p^n},(p^n-1)_{p^m}\right)\\
&\overset{(3.5)}{=} ((1-(p^n-1-(p^n-1)_{p^m}))_{p^n},(p^n-1)_{p^m})\\
&= ((2+(p^n-1)_{p^m})_{p^n},(p^n-1)_{p^m})\\
&= (((p^n-1)_{p^m}-2(p^n-1))_{p^n},(p^n-1)_{p^m})\\
&\overset{(3.6)}{=} (p^n-1)(p^n-1,1).
\end{aligned}
$$

The last equation follows from (3.6) for $s=p^n-1$, hence $r_+(p^n-1,1)=p^n$, $r_*(p^n-1,1)=1$ and $|B|=p^n>1$ since $n\geq m>0$.

Now we show that $B\cap C=\{(0,0)\}$.

Let $x\in B\cap C$. Then there exists $0\leq s<p^n$ such that $x=s(p^n-1,1)\overset{(3.6)}{=}(((s)_{p^m}-2s)_{p^n},(s)_{p^m})\in C$ hence $((s)_{p^m}-2s)_{p^n}=(s)_{p^m}=((s)_{p^m})_{p^n}$ by(3.4) and $p^n|(s)_{p^m}-(((s)_{p^m}-2s)$ thus $p^n|2s$ therefore $p^n|s$ (since $p\neq 2$) there is why $s=0$ and $x=(0,0)$.

Hence $\mathcal{Q}\cong\Psi(Q^k_{p^n,p^m})$ is directly decomposable by Lemma 3.6. ∎

Theorem 3.11. *Let $\mathcal{Q}\in$ EQ1 be a finite and monogenic quasiqroup. If $r_+(\mathcal{Q})=p^n$, $r_*(\mathcal{Q})=p^m$ and $r_{*+}(\mathcal{Q})=0$ where $p\neq 2$ is prime and $m>0$ then $\mathcal{Q}$ is directly decomposable.*

Proof. It is sufficient to show that $\Psi(Q^{p^n-2p^m}_{p^n,p^m})\cong\mathcal{Q}$ is directly decomposable.

Let B be the subalgebra of $Q^k_{p^n,p^m}$ generated by $(p^n-1,1)$. Let C be the subalgebra of $Q^k_{p^n,p^m}$ generated by $(1,1)$.

We show that $r_+(1,1) = p^n$, $r_*(1,1) = 1$, $r_{*+}(1,1) = 0$.

We know that $s = E(\frac{s}{p^m})p^m + (s)_{p^m}$ for $s \in \mathbb{Z}$. Hence

$$p^m E\left(\frac{s}{p^m}\right) = s - (s)_{p^m}. \tag{3.7}$$

Let us observe that

$$\begin{aligned} p^n(1,1) &= \gamma^0_{p^n,p^m}(p^n,p^n) \\ &= \left(\left(p^n + E\left(\frac{p^n}{p^m}\right)p^m\right)_{p^n}, (p^n)_{p^m}\right) = (0,0) \end{aligned}$$

and

$$\begin{aligned} s(1,1) &= \gamma^0_{p^n,p^m}(s,s) \\ &= \left(\left(s + E\left(\frac{s}{p^m}\right)p^m\right)_{p^n}, (s)_{p^m}\right) \\ &\overset{(3.7)}{=} ((2s - (s)_{p^m})_{p^n}, (s)_{p^m}) \neq (0,0) \end{aligned}$$

for $0 < s < p^n$.

Since if $(2s - (s)_{p^m})_{p^n} = (s)_{p^m} = 0$ then $p^n | 2s$ thus $p^n | s$ (since $p \neq 2$) but $p^n \nmid s$ for $0 < s < p^n$ - a contradiction.

Moreover $(1,1)^* = (1,1)$. Hence $r_+(1,1) = p^n$, $r_*(1,1) = 1$, $r_{*+}(1,1) = 0$ and $|C| = p^n \geq p^m > 1$ since $m > 0$.

We prove that $r_+(p^n - 1, 1) = p^m$ and $r_*(p^n - 1, 1) = 1$.

Let us notice that

$$\begin{aligned} p^m(p^n - 1, 1) &= \gamma^0_{p^n,p^m}(p^m p^n - p^m, p^m) \\ &= \left(\left(p^m p^n - p^m + E\left(\frac{p^m}{p^m}p^m\right)_{p^n}, (p^m)_{p^m}\right) = (0,0)\right. \end{aligned}$$

and

$$\begin{aligned} s(p^n - 1, 1) &= \gamma^0_{p^n,p^m}(sp^n - s, s) \\ &= \left(\left(sp^n - s + E\left(\frac{s}{p^m}\right)p^m\right)_{p^n}, (s)_{p^m}\right) \\ &= ((-s)_{p^n}, s) = (p^n - s, s) \neq (0,0) \end{aligned} \tag{3.8}$$

for $0 < s < p^m$.

Let us observe that

$$\begin{aligned} (p^n - 1, 1)^* &= \gamma^0_{p^n,p^m}(1, p^n - 1) \\ &= \left(\left(1 + E\left(\frac{p^n - 1}{p^m}\right)p^m\right)_{p^n}, (p^n - 1)_{p^m}\right) \end{aligned} \tag{3.9}$$

$$\stackrel{(3.7)}{=} ((1+p^n-1-(p^n-1)_{p^m})_{p^n}, (p^n-1)_{p^m})$$
$$= (p^n-(p^n-1)_{p^m}, (p^n-1)_{p^m})$$
$$\stackrel{(3.8)}{=} (p^n-1)_{p_m}(p^n-1,1).$$

Hence $r_+(p^n-1,1)=p^m$, $r_*(p^n-1,1)=1$ and $|B|=p^m>1$ since $m>0$.

Thus

$$B=\{(p^n-s,s)\in\mathbb{Z}\times\mathbb{Z}\colon 1\le s<p^m\}\cup\{(0,0)\}. \tag{3.10}$$

Now we show that $B\cap C=\{(0,0)\}$.

Let $x\in B\cap C$. Then there exists $0\le s<p^n$ such that

$$x=\gamma^0_{p^n,p^m}(s,s)=((s+E(\frac{s}{p^m})p^m)_{p^n},(s)_{p^m})\in B$$

hence

$$p^n\Big|\left(s+E\left(\frac{s}{p^m}\right)p^m\right)_{p^n}+(s)_{p^m}$$

by 3.10 and

$$p^n|s+E\left(\frac{s}{p^m}\right)p^m+(s)_{p^m}=2s$$

therefore $p^n|s$ (since $p\neq 2$) there is why $s=0$ and $x=(0,0)$.

Therefore $\Psi(Q^k_{p^n,p^m})$ is directly decomposable by Lemma 3.6. Hence $\mathcal{Q}\cong\Psi(Q^k_{p^n,p^m})$ is directly decomposable. ∎

Theorem 3.12. *Let $\mathcal{Q}\in$ EQ1 be a finite and monogenic quasiqroup. Then $\mathcal{Q}$ is directly indecomposable if and only if one of the following contidions are satisfied:*

(1) $r_+(\mathcal{Q})=2^n$ *and* $n>0$,
(2) $r_+(\mathcal{Q})=p^n$, $r_*(\mathcal{Q})=1$ *and* $r_{*+}(\mathcal{Q})=0$, *where p is prime and* $n>0$,
(3) $r_+(\mathcal{Q})=p^n$, $r_*(\mathcal{Q})=1$ *and* $r_{*+}(\mathcal{Q})=p^n-2$, *where p is prime and* $n>0$.

Proof. Let $\mathcal{Q}\in$ EQ1 be a finite and monogenic quasiqroup and suppose that $\mathcal{Q}$ is directly indecomposable. By Theorem 3.4 $r_+(\mathcal{Q})=p^n$ where p is prime and $n>0$. If $p=2$ then we obtain the case1.

Suppose that $p\neq 2$.

Using Theorem 2.3 $\mathcal{Q}$ is isomorphic to one of the following algebras in EQ1:

(1) $\Psi(Q^0_{p^n,p^m})$, $m\le n$,
(2) $\Psi(Q^{p^n-2p^m}_{p^n,p^m})$, $m+1\le n$.

If $\mathcal{Q}$ is isomorphic to $\Psi(Q^0_{p^n,p^m})$ and $m>0$ then by Theorem 3.11 $\mathcal{Q}$ is directly decomposable - a contradiction. Hence $m=0$ and we obtain the case 2.

If $\mathcal{Q}$ is isomorphic to $\Psi(Q^{p^n-2p^m}_{p^n,p^m})$ and $m > 0$ then by Theorem 3.10 $\mathcal{Q}$ is directly decomposable - a contradiction. Thus $m = 0$ and we obtain the case 3.

Let $\mathcal{Q} \in$ EQ1 be a finite and monogenic quasiqroup and suppose that one of the following contidions are satisfied:

(1) $r_+(\mathcal{Q}) = 2^n$ and $n > 0$,
(2) $r_+(\mathcal{Q}) = p^n$, $r_*(\mathcal{Q}) = 1$ and $r_{*+}(\mathcal{Q}) = 0$, where p is prime and $n > 0$,
(3) $r_+(\mathcal{Q}) = p^n$, $r_*(\mathcal{Q}) = 1$ and $r_{*+}(\mathcal{Q}) = p^n - 2$, where p is prime and $n > 0$.

In the case 1 by Theorem 3.9 $\mathcal{Q}$ is directly indecomposable.

In the case 2 $\mathcal{Q} \cong \Psi(Q^0_{p^n,1})$ and $\Psi(Q^0_{p^n,1})$ has the bigest nontrivial subalgebra generated by $(p, 0)$, so by Lemma 3.7 $\mathcal{Q}$ is directly indecomposable.

In the case 3 $\mathcal{Q} \cong \Psi(Q^{p^n-2}_{p^n,1})$ and $\Psi(Q^{p^n-2}_{p^n,1})$ has the bigest nontrivial subalgebra generated by $(p, 0)$, so by Lemma 3.7 $\mathcal{Q}$ is directly indecomposable. ∎

References

[1] G. Bińczak, J. Kaleta, *Cyclic entropic quasigroups*, Demonstratio Math. 42 (2009), 269–281.
[2] G. Bińczak, J. Kaleta, *Finite simple monogenic entropic quasigroups with quasi-identity*, to appear in Demonstratio Math.
[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.

G. Bińczak
FACULTY OF MATHEMATICS AND INFORMATION SCIENCES
WARSAW UNIVERSITY OF TECHNOLOGY
00-661 WARSAW, POLAND
E-mail: binczak@mini.pw.edu.pl

J. Kaleta
DEPARTMENT OF APPLIED MATHEMATICS
WARSAW UNIVERSITY OF AGRICULTURE
02-787 WARSAW, POLAND
E-mail: joanna_kaleta@sggw.pl

Received November 18, 2010; revised version December 6, 2010.