*Discussiones Mathematicae*
*General Algebra and Applications 34 (2014) 5–26*
*doi:10.7151/dmgaa.1214*

# SOME FINITE DIRECTLY INDECOMPOSABLE NON-MONOGENIC ENTROPIC QUASIGROUPS WITH QUASI-IDENTITY

Grzegorz Bińczak

*Faculty of Mathematics and Information Sciences*
*Warsaw University of Technology*
*00–661 Warsaw, Poland*

**e-mail:** binczak@mini.pw.edu.pl

and

Joanna Kaleta

*Department of Applied Mathematics*
*Warsaw University of Agriculture*
*02–787 Warsaw, Poland*

**e-mail:** joanna_kaleta@sggw.pl

**Abstract**

In this paper we show that there exists an infinite family of pairwise non-isomorphic entropic quasigroups with quasi-identity which are directly indecomposable and they are two-generated.

**Keywords:** quasigroups, entropic quasigroups, abelian groups, involution.

**2010 Mathematics Subject Classification:** 20N05.

## 1. Introduction

This paper consists of two parts.

The first part of this work concerns of introducing definitions and theorems about entropic quasigroups with quasi-identity, abelian groups with involutions and some connections between them.

In the second part we define an Abelian group with involution of the form $W_{n,x_0}(\mathcal{G})$ and describe subalgebras of it. In the Theorem 17 we prove that if some conditions are satisfied and $W_{n,x_0}(\mathcal{G})$ is directly decomposable then $\mathcal{G}$ is also directly decomposable. Next we describe subalgebras of $Q^0_{2^m,2}$ and show that quasigroups $\Psi(W_{n,(2^{m-1},0)}(Q^0_{2^n,2}))$ are directly indecomposable for $m-1 \geq n \geq 1$. Contrary to Abelian groups there are two-generated (and not one-generated) entropic quasigroups beeing directly indecomposable. We show that there exists an infinite family of pairwise not-isomorphic entropic quasigroups with quasi-identity which are directly indecomposable and they are two-generated.

**Definition.** An *Abelian group with involution* is a set $G$, where are defined the binary operation $+$, the unary operations $-$ and $^*$, and the constant 0, which verify the following properties:

1. $(G, +, -, 0)$ is an Abelian group,
2. $0^* = 0,\ a^{**} = a,\ (a+b)^* = a^* + b^*$.

In such a case we will denote $(G, +, -, 0, ^*)$. The operation $-$ takes each element $a$ to its inverse $-a$ and $^*$ is the involution.

Moreover $(-a)^* = -(a^*)$ since $(-a)^* + a^* \overset{(2)}{=} (-a+a)^* = 0^* = 0$ so we use further the notation $-a^*$ instead of $(-a)^*$ and $-(a)^*$.

We denote the class of all Abelian groups with involution by $AGI$.

**Definition.** An *entropic* quasigroup is a set $Q$, where are defined the binary operations $\cdot$, $/$, $\backslash$, which verify the following properties:

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. $(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$.

In such a case we will denote $(Q, \cdot, /, \backslash)$. If there exists an element (which we will denote as 1) such that

(4) $a \cdot 1 = a$, $1 \cdot (1 \cdot a) = a$,

then we will say that $(Q, \cdot, /, \backslash)$ has a quasi-identity and denote $(Q, \cdot, /, \backslash, 1)$.

We denote the class of all entropic quasigroups with quasi-identity by EQ1.

**Definition.** If $\mathcal{G} = (G, +, -, 0, ^*)$ is an Abelian group with involution then we define $\Psi(\mathcal{G}) := (G, \cdot, /, \backslash, 1)$, where $a \cdot b := a + (b^*)$, $a \backslash b := b^* + (-a^*)$, $a/b := a + (-b^*)$, $1 := 0$.

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

The next result corresponds to Theorem 3 and 4 in [1]:

**Theorem 1.** *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* $a \cdot b := a + (b^*)$, $a \backslash b := b^* + (-a^*)$, $a/b := a + (-b^*)$, $1 := 0$.

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

By the Theorem given above we see that $\Psi: AGI \to EQ1$ and $\Phi: EQ1 \to AGI$.

The next result corresponds to Theorem 5 and 6 in [1]:

**Theorem 2.** *If* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *is an entropic quasigroup with quasi-identity then* $\Psi(\Phi(\mathcal{Q})) = \mathcal{Q}$.

*If* $\mathcal{G} = (G, +, -, 0, ^*)$ *is an Abelian group with involution then* $\Phi(\Psi(\mathcal{G})) = \mathcal{G}$.

**Theorem 3.** *The functions* $\Psi$ *and* $\Phi$ *defined above satisfy that* $\Psi = \Phi^{-1}$.

**Lemma 4.** *If* $\mathcal{G}_1 = (G_1, +_1, -_1, 0_1, ^{*_1})$ *and* $\mathcal{G}_2 = (G_2, +_2, -_2, 0_2, ^{*_2})$ *are Abelian groups with involution then* $\Psi(\mathcal{G}_1 \times \mathcal{G}_2) = \Psi(\mathcal{G}_1) \times \Psi(\mathcal{G}_2)$.

***Proof.*** We know that $\Psi(\mathcal{G}_1) = (G_1, \cdot_1, /_1, \backslash_1, 0_1)$, where $a \cdot_1 b = a +_1 (b^{*_1})$, $a \backslash_1 b = b^{*_1} + (-_1 a^{*_1})$, $a/_1 b = a +_1 (-_1 b^{*_1})$, for all $a, b \in G_1$ and $\Psi(\mathcal{G}_2) = (G_2, \cdot_2, /_2, \backslash_2, 0_2)$, where $a \cdot_2 b = a +_2 (b^{*_2})$, $a \backslash_2 b = b^{*_1} + (-_2 a^{*_2})$, $a/_2 b := a +_2 (-_2 b^{*_2})$, for every $a, b \in G_2$.

Then $\mathcal{G}_1 \times \mathcal{G}_2 = (G_1 \times G_2, +_3, -_3, (0_1, 0_2))^{*_3}$, where $(a_1, a_2) +_3 (b_1, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2)$, $-_3(a_1, a_2) = (-_1 a_1, -_2 a_2)$, $(a_1, a_2)^{*_3} = (a_1^{*_1}, a_2^{*_2})$ for all $a_1, b_1 \in G_1$ and $b_1, b_2 \in G_2$.

We have $\Psi(\mathcal{G}_1) \times \Psi(\mathcal{G}_2) = (G_1 \times G_2, \cdot_4, /_4, \backslash_4, (0_1, 0_2))$, where $(a_1, a_2) \cdot_4 (b_1, b_2) = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2) = (a_1 +_1 (b_1^{*_1}), a_2 +_1 (b_2^{*_2}))$ for all $a_1, b_1 \in G_1$, $a_2, b_2 \in G_2$, similarly for $/_4, \backslash_4$.

Moreover $\Psi(\mathcal{G}_1 \times \mathcal{G}_2) = (G_1 \times G_2, \cdot, /, \backslash, (0_1, 0_2))$, where $(a_1, a_2) \cdot (b_1, b_2) = (a_1, a_2) +_3 (b_1, b_2)^{*_3} = (a_1 +_1 (b_1^{*_1}), a_2 +_2 (b_2^{*_2}))$ for every $a_1, b_1 \in G_1$, $a_2, b_2 \in G_2$ similarly for $/, \backslash$.

Hence $\cdot_4 = \cdot$ and similarly $/_4 = /$, $\backslash_4 = \backslash$. Thus $\Psi(G_1 \times G_2) = \Psi(G_1) \times \Psi(G_2)$. ∎

If $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ is an entropic quasigroup with quasi-identity then $|\mathcal{Q}|$ indicates the cardinality of $Q$.

**Definition.** An entropic quasigroup with quasi-identity $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ is directly indecomposable if $|\mathcal{Q}| \neq 1$ and if $\mathcal{Q} \cong \mathcal{Q}_1 \times \mathcal{Q}_2$, where $Q_1, Q_2 \in EQ1$, then either $|\mathcal{Q}_1| = 1$ or $|\mathcal{Q}_2| = 1$.

Similarly directly indecomposability for Abelian groups with involution is defined.

**Definition.** Let $\mathcal{G} = (G, +, -, 0, ^*) \in AGI$. A subset $X \subseteq G$ is a subalgebra of $\mathcal{G}$ if and only if $0 \in X$, $x_1 + x_2 \in X$, $x^* \in X$, $-x \in X$ for every $x, x_1, x_2 \in X$.

Let $X \subseteq G$. The intersection of all subalgebras of $\mathcal{G}$ containing $X$ we denote by $\langle X \rangle$ (if $X = \{x\}$ then we use $\langle x \rangle$ instead of $\langle \{x\} \rangle$). We say that the set $X$ generates $\mathcal{G}$ if and only if $\langle X \rangle = G$.

A $\mathcal{G}$ has $k$ generators if and only if there exists $k$-element set $X$ which generates $\mathcal{G}$ and there does not exist $k-1$-element set $X$ which generates $\mathcal{G}$.

The following lemma concerning Abelian groups with involution can be proved similarly as for Abelian groups.

**Lemma 5.** *Let $\mathcal{G} \in AGI$ be a finite Abelian group and $|\mathcal{G}| > 1$. Then $\mathcal{G}$ is directly decomposable if and only if there are $B$ and $C$ being subalgebras of $\mathcal{G}$ such that $B \cap C = \{0\}$, $B + C = G$, $|B| > 1$ and $|C| > 1$.*

**Theorem 6.** *Let $\mathcal{G} = (G, +, -, 0, ^*)$ be an Abelian group with involution. If $\mathcal{G}$ is directly indecomposable then $\Psi(\mathcal{G})$ is directly indecomposable.*

***Proof.*** Let $\mathcal{G} = (G, +, -, 0, ^*)$ be an Abelian group with involution. Assume that $\mathcal{G}$ is directly indecomposable. We show that $\Psi(\mathcal{G})$ is directly indecomposable. If $\Psi(\mathcal{G}) \cong Q_1 \times Q_2$ then let $\mathcal{G}_1 = \Phi(Q_1)$ and $\mathcal{G}_2 = \Phi(Q_2)$. By Theorem 2 we have $\Psi(\mathcal{G}_1) = Q_1$ and $\Psi(\mathcal{G}_2) = Q_2$ so $\Psi(\mathcal{G}_1 \times \mathcal{G}_2) = \Psi(\mathcal{G}_1) \times \Psi(\mathcal{G}_2) = Q_1 \times Q_2 \cong \Psi(\mathcal{G})$ by Lemma 4. Hence $\mathcal{G}_1 \times \mathcal{G}_2 \cong \mathcal{G}$ and $|G_1| = 1$ or $|G_2| = 1$ since $\mathcal{G}$ is directly indecomposable. Thus $|Q_1| = |G_1| = 1$ or $|Q_2| = |G_2| = 1$ so $\Psi(\mathcal{G})$ is directly indecomposable. ■

Obviously every finite abelian group with involution G is isomorphic to a finite product of directly indecomposable finite abelian groups with involution. Moreover using Theorem [5, Theorem 6.39] this decomposition into directly indecomposable factors is unique (up to reindexing and isomorphism). After applying Theorem 6 and Lemma 4 we obtain similar result for finite entropic quasigroups with quasi-identity.

Hence to obtain structural theorem describing finite entropic quasigroups with quasi-identity it remains to find all finite directly indecomposable entropic quasigroups with quasi-identity.

We have already described (in [3]) directly indecomposable finite entropic quasigroups with quasi-identity having one generator.

In this paper we investigate finite two-generated directly indecomposable finite entropic quasigroups with quasi-identity.

More information concerning entropic quasigroups may be found in [4] and [6].

**Definition.** 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 $Q = \langle x \rangle$. We define three types of *rank* of the generator $x$:

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

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]).

We denote the integer part of $a \in \mathbb{R}$ by $E(a)$, whereas $(a)_b$ denotes the remainder obtained after dividing $a$ by $b$.

**Definition.** 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

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

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

**Theorem 7** ([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.*

## 2. Main theorem

We have already characterized all one-generated, directly indecomposable, entropic quasigroups with quasi-identity (see [3]).

In this section we find some two-generated, directly indecomposable, entropic quasigroups with quasi-identity.

For any abelian group with involution $\mathcal{G} = (G, +, -, 0, ^*)$ and some element $x_0 \in G$, and positive integer $n$ we define $W_{n,x_0}(\mathcal{G})$ which is also abelian group with involution (Theorem 9).

We can obtain from one-generated abelian group with involution $\mathcal{G}$ two-generated $W_{n,x_0}(\mathcal{G})$ just by means of $W_{n,x_0}$.

If $W_{n,x_0}(\mathcal{G})$ satisfies (H) then we can describe all subalgebras of $W_{n,x_0}(\mathcal{G})$ in order to decide when $W_{n,x_0}(\mathcal{G})$ is directly indecomposable.

In the Theorem 17 we prove that if some conditions are satisfied and $\mathcal{G}$ is directly indecomposable then $W_{n,x_0}(\mathcal{G})$ is also directly indecomposable. Next we describe subalgebras of $Q^0_{2^m,2}$ and show that quasigroups $\Psi(W_{n,(2^{m-1},0)}(Q^0_{2^n,2}))$ are directly indecomposable for $m-1 \geq n \geq 1$.

**Definition.** Let $\mathcal{G} = (G, +, -, ^*) \in AGI$ and $x_0 = x_0^*$, $2x_0 = 0$ for some $x_0 \in G$. Let $n \in \mathbb{N}$ and $n \geq 1$.

Let $W_{n,x_0}(\mathcal{G}) = (G \times \mathbb{Z}_{2^n}, +, -, (0,0), ^*)$, where

$$(g, y) + (g', y') := (g + g', (y + y')_{2^n}),$$

$$-(g, y) := (-g, (-y)_{2^n}),$$

$$(g, y)^* = \begin{cases} (g^*, y) & \text{for } \; 2 \mid y \\ (g^* + x_0, y) & \text{for } \; 2 \nmid y \end{cases}$$

**Example 8.** Let $m \in \mathbb{N}$ and $m > 1$. Let $\mathcal{G} = Q^0_{2^m,2} \in AGI$ and $x_0 = (2^{m-1}, 0) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2$. Then $2x_0 = \gamma^0_{2^m,2}(2^m, 0) = (0,0)$ and $x_0^* = \gamma^0_{2^m,2}(0, 2^{m-1}) = (2^{m-1}, 0)$ $= x_0$.

**Theorem 9.** *Let $\mathcal{G} = (G, +, -, ^*) \in AGI$ and $x_0 = x_0^*$, $2x_0 = 0$ for some $x_0 \in G$. Let $n \in \mathbb{N}$ and $n \geq 1$. Then $W_{n,x_0}(\mathcal{G}) \in AGI$.*

***Proof.*** It is obvoius that the reduct $(G \times \mathbb{Z}_{2^n}, +, -, (0,0))$ is an Abelian group.

Let $(g, y) \in G \times \mathbb{Z}_{2^n}$. If $2|y$ then $(g, y)^{**} = (g, y)$. If $2 \nmid y$ then $(g, y)^{**} = (g^* + x_0, y)^* = ((g^* + x_0)^* + x_0, y) = (g^{**} + x_0^* + x_0, y) = (g + x_0 + x_0, y) = (g, y)$. Let $(g, y), (g', y') \in G \times \mathbb{Z}_{2^n}$.

Consider the following cases:

1. If $2|y$ and $2|y'$ then $2|(y + y')_{2^n}$ and

$$\begin{aligned} ((g, y) + (g', y'))^* &= (g + g', (y + y')_{2^n})^* \\ &= ((g + g')^*, (y + y')_{2^n}) = (g^* + g'^*, (y + y')_{2^n}) \\ &= (g^*, y) + (g'^*, y') = (g, y)^* + (g', y')^*. \end{aligned}$$

2. If $2 \nmid y$ and $2|y'$ then $2 \nmid (y+y')_{2^n}$ and

$$\begin{aligned}((g,y)+(g',y'))^* &= (g+g',(y+y')_{2^n})^* \\ &= ((g+g')^*+x_0,(y+y')_{2^n}) \\ &= (g^*+x_0+g'^*,(y+y')_{2^n}) \\ &= (g^*+x_0,y)+(g'^*,y') = (g,y)^*+(g',y')^*.\end{aligned}$$

3. If $2 \nmid y$ and $2 \nmid y'$ then $2|(y+y')_{2^n}$ and

$$\begin{aligned}((g,y)+(g',y'))^* &= (g+g',(y+y')_{2^n})^* \\ &= ((g+g')^*,(y+y')_{2^n}) \\ &= (g^*+x_0+g'^*+x_0,(y+y')_{2^n}) \\ &= (g^*+x_0,y)+(g'^*+x_0,y') = (g,y)^*+(g',y')^*.\end{aligned}$$

■

**Definition.** Let $\mathcal{G} = (G,+,-,^*) \in AGI$, $k,n \in \mathbb{Z}$ and $0 \le k \le n$. Let $S$ be a subalgebra of $\mathcal{G}$ and $a_0 \in G$.

Then

$$[S,n,k,a_0] := \bigcup_{i=0}^{2^{n-k}-1} (S+ia_0) \times \{i2^k\}.$$

In order to decide when $W_{n,x_0}(\mathcal{G})$ is directly indecomposable we have to describe subalgebras of $W_{n,x_0}(\mathcal{G})$. For given $\mathcal{G} \in AGI$ we defined $[S,n,k,a_0] \subset G \times \mathbb{Z}_{2^n}$. The following theorem says when $[S,n,k,a_0]$ is a subalgebra of $W_{n,x_0}(\mathcal{G})$.

**Theorem 10.** *Let $\mathcal{G} = (G,+,-,^*) \in AGI$ and $x_0 = x_0^*$, $2x_0 = 0$ for some $x_0 \in G$. Let $n,k \in \mathbb{Z}$, $n \ge 1$ and $0 \le k \le n$. Let $S$ be a subalgebra of $\mathcal{G}$, $a_0 \in G$ and $a_0^* - a_0 \in S$, $2^{n-k}a_0 \in S$. Assume that $k > 0$ or $x_0 \in S$.*

*Then $[S,n,k,a_0]$ is a subalgebra of $W_{n,x_0}(\mathcal{G})$.*

***Proof.*** Let $a,b \in [S,n,k,a_0]$ then there exist $0 \le i,j \le 2^{n-k}-1$ such that $a \in (S+ia_0) \times \{i2^k\}$ and $b \in (S+ja_0) \times \{j2^k\}$.

Consider the following cases:

1. If $i+j \le 2^{n-k}-1$ then $a+b \in (S+ia_0) \times \{i2^k\} + (S+ja_0) \times \{j2^k\} = (S+(i+j)a_0) \times \{(i+j)2^k\}$ so $a+b \in [S,n,k,a_0]$.

2. If $i+j > 2^{n-k}-1$ then

$$\begin{aligned}a+b &\in (S+ia_0) \times \{i2^k\} + (S+ja_0) \times \{j2^k\} \\ &= (S+(i+j)a_0) \times \{((i+j)2^k)_{2^n}\}\end{aligned}$$

$$
\begin{aligned}
&= (S + 2^{n-k}a_0 + (i + j - 2^{n-k})a_0) \times \{(i + j - 2^{n-k})2^k\} \\
&= (S + (i + j - 2^{n-k})a_0) \times \{(i + j - 2^{n-k})2^k\}
\end{aligned}
$$

since $2^{n-k}a_0 \in S$. Hence $a + b \in [S, n, k, a_0]$.

Therefore $[S, n, k, a_0]$ is closed under $+$.

Let $a \in [S, n, k, a_0]$ then there exist $0 \le i \le 2^{n-k} - 1$ such that $a \in (S + ia_0) \times \{i2^k\}$. Then

$$
\begin{aligned}
-a &\in (S - ia_0) \times \{(-i2^k)_{2^n}\} \\
&= (S - 2^{n-k}a_0 + (2^{n-k} - i)a_0) \times \{(2^{n-k} - i)2^k\} \\
&= (S + (2^{n-k} - i)a_0) \times \{(2^{n-k} - i)2^k\}
\end{aligned}
$$

and $0 \le 2^{n-k} - i \le 2^{n-k} - 1$. Hence $-a \in [S, n, k, a_0]$ and $[S, n, k, a_0]$ is closed under $-$.

Let $a \in [S, n, k, a_0]$ then there exist $0 \le i \le 2^{n-k} - 1$ such that $a \in (S + ia_0) \times \{i2^k\}$.

Consider the following cases:

1. If $2 | i2^k$ then
$$
\begin{aligned}
a^* &\in (S + ia_0^*) \times \{i2^k\} \\
&= (S - i(a_0^* - a_0) + ia_0^*) \times \{i2^k\} \\
&= (S + ia_0) \times \{i2^k\}
\end{aligned}
$$

2. If $2 \nmid i2^k$ then $k = 0$ hence $x_0 \in S$ and
$$
\begin{aligned}
a^* &\in (S + ia_0^* + x_0) \times \{i2^k\} \\
&= (S - i(a_0^* - a_0) + ia_0^*) \times \{i2^k\} \\
&= (S + ia_0) \times \{i2^k\}
\end{aligned}
$$

Therefore $[S, n, k, a_0]$ is closed under $^*$. ■

Now, given $\mathcal{G} = (G, +, -, ^*) \in AGI$ such that $x_0 = x_0^*$ and $2x_0 = 0$ suppose that there exists $r \ge 1$ such that

$$
\left.
\begin{array}{ll}
\text{(i)} & 2^r g = 0 \text{ or } 2^r g = x_0 \text{ for all } g \in G \text{ and} \\
\text{(ii)} & 2^r g = 0 \Rightarrow g = g^* \text{ for all } g \in G
\end{array}
\right. \qquad (H)
$$

**Example 11.** Let $m \in \mathbb{N}$ and $m > 1$. Let $\mathcal{G} = Q^0_{2^m,2} \in AGI$ and $x_0 = (2^{m-1}, 0) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2$. Then the hypotheses (H) hold for $r = m - 1$:

Let $(a, b) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2$. Then

$$\begin{aligned} 2^{m-1}(a,b) &= \gamma^0_{2^m,2}(2^{m-1}a, 2^{m-1}b) = ((2^{m-1}a + E(\tfrac{2^{m-1}b}{2})2)_{2^m}, (2^{m-1}b)_2) \\ &= ((2^{m-1}(a+b))_{2^m}, 0) = \begin{cases} (0,0) & 2 \mid a+b \\ (2^{m-1},0) & 2 \nmid a+b \end{cases}. \end{aligned}$$

Hence if $2|a + b$ then $2^{m-1}(a, b) = (0, 0)$ and if $2 \nmid a + b$ then $2^{m-1}(a, b) = (2^{m-1}, 0) = x_0$. So the first hypothesis (H) is fullfilled.

Let $(a, b) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2$ and $2^{m-1}(a, b) = 0$. Then $2|a + b$.

If $b = 0$ then $2|a$ and $b + E(\frac{a}{2})2 = 0 + \frac{a}{2}2 = a$ so $(a, b)^* = \gamma^0_{2^n,2}(b, a) = ((b + E(\frac{a}{2})2)_{2^n}, (a)_2) = (a, 0) = (a, b)$.

If $b = 1$ then $2 \nmid a$ and $b + E(\frac{a}{2})2 = 1 + E(\frac{a}{2})2 = a$ so $(a, b)^* = \gamma^0_{2^n,2}(b, a) = ((b + E(\frac{a}{2})2)_{2^n}, (a)_2) = (a, 1) = (a, b)$.

Therefore the second hypothesis (H) is satisfied, too.

**Lemma 12.** *Let $\mathcal{G} = (G, +, -, ^*) \in AGI$ such that $x_0 = x_0^*$ and $2x_0 = 0$ for some $x_0 \in G$, and assume hypotheses (H) hold. Let $n \in \mathbb{N}$ and $r \geq n \geq 1$.*

*If $T$ is a subalgebra of $W_{n,x_0}(\mathcal{G})$ then $(x_0, 0) \in T$ or for all $(g, i) \in T$ we have $2|i$.*

***Proof.*** Assume that $(g, i) \in T$ and $2 \nmid i$ for some $g \in G$ and $i \in \mathbb{Z}_{2^n}$.

We will show that $(x_0, 0) \in T$. Observe that $2^r(g, i) = (2^r g, (2^r i)_{2^n}) = (2^r g, 0) \in T$ since $r \geq n$. If $2^r g = x_0$ then $(x_0, 0) \in T$. If $2^r g \neq x_0$ then $2^r g = 0$ and $g = g^*$. Moreover $(g, i)^* = (g^* + x_0, i) \in T$. Hence

$$\begin{aligned} T &\ni (g^* + x_0, i) + (2^r - 1)(g, i) \\ &= (g^* + x_0 + 2^r g - g, (2^r i)_{2^n}) \\ &= (g + x_0 - g, 0) = (x_0, 0) \end{aligned}$$

■

**Theorem 13.** *Let $\mathcal{G} = (G, +, -, ^*) \in AGI$ and $x_0 = x_0^*$, $2x_0 = 0$ for some $x_0 \in G$. Let $n \in \mathbb{N}$ and $n \geq 1$.*

*If $T$ is a subalgebra of $W_{n,x_0}(\mathcal{G})$ and $S = \{s \in G \colon (s, 0) \in T\}$ then $T = [S, n, k, a_0]$ for some $0 \leq k \leq n$ and $a_0 \in G$.*

***Proof.*** Let $T$ be a subalgebra of $W_{n,x_0}(\mathcal{G})$ and $S = \{s \in G \colon (s, 0) \in T\}$.

It is obvious that $S$ is a subalgebra of $\mathcal{G}$.

Let $P = \{i \in \mathbb{Z}_{2^n} \colon \exists_{g \in G} (g, i) \in T\}$. Then $P$ is a subgroup of $\mathbb{Z}_{2^n}$. Hence there exists $0 \leq k \leq n$ such that $P = \{i2^k \colon 0 \leq i < 2^{n-k}\}$.

If $k < n$ then $2^k \in P$ and there exists $a_0 := g \in G$ such that $(a_0, 2^k) \in T$.

If $k = n$ then $a_0 := 0$.

1. We show that $[S,n,k,a_0] \subseteq T$.

   Let $a \in [S,n,k,a_0]$ then there exists $0 \leq i \leq 2^{n-k}-1$ such that $a \in (S+ia_0) \times \{i2^k\}$. Hence $a = (s+ia_0, i2^k)$ for some $s \in S$. Moreover $(s,0) \in T$.

   Consider the following cases:

   (a) If $k < n$ then $(a_0, 2^k) \in T$ and $i(a_0, 2^k) = (ia_0, i2^k) \in T$ so $a = (s+ia_0, i2^k) = (s,0) + (ia_0, i2^k) \in T$.

   (b) If $k = n$ then $i = 0$ and $a = (s,0) \in T$.

2. We show that $T \subseteq [S,n,k,a_0]$.

   Let $y \in T$ then there exist $g \in G$ and $i \in \mathbb{Z}_{2^n}$ such that $y = (g,i)$. Hence $i \in P$ so there exists $0 \leq j < 2^{n-k}$ such that $i = j2^k$.

   Consider the following cases:

   (a) If $k < n$ then $(a_0, 2^k) \in T$ thus $(ja_0, j2^k) \in T$. Hence $(g, j2^k) - (ja_0, j2^k) = (g - ja_0, 0) \in T$ and $g - ja_0 \in S$ so $y = (g,i) = (g - ja_0 + ja_0, j2^k) \in (S + ja_0) \times \{j2^k\} \subseteq [S,n,k,a_0]$.

   (b) If $k = n$ then $i = 0$ and $g \in S$ so $y = (g,0) \in S \times \{0\} = [S,n,k,a_0]$.

Hence $T = [S,n,k,a_0]$. ■

The following theorem given the converse of Lemma 12 and uses Theorem 10 , Lemma 12 and Theorem 13. In particular it allows to characterize all subalgebras of $W_{n,x_0}(\mathcal{G})$ which satisty the hypotheses (H).

**Theorem 14.** *Let $\mathcal{G} = (G, +, -, ^*) \in AGI$ such that $x_0 = x_0^*$ and $2x_0 = 0$ for some $x_0 \in G$ and assume hypotheses (H) hold. $T$ is a subalgebra of $W_{n,x_0}(\mathcal{G})$ if and only if both conditions given below hold*

(i) *$(x_0, 0) \in T$ or for all $(g,i) \in T$ we have $2|i$,*

(ii) *$T = [S,n,k,a_0]$ for some $S$ beeing a subalgebra of $\mathcal{G}$, $0 \leq k \leq n$ and $a_0 \in G$ such that $a_0^* - a_0 \in S$ and $2^{n-k}a_0 \in S$.*

***Proof.*** $\Rightarrow$ From Lemma 12, if $T$ is a subalgebra then (i) holds. Furtheremore, from Theorem 13 we have that $T = [S,n,k,a_0]$ with $S = \{s \in G : (s,0) \in T\}$ and for some $0 \leq k \leq n$ and $a_0 \in G$. Therefore we only need to show that $a_0^* - a_0 \in S$ and $2^{n-k}a_0 \in S$.

Consider the following cases:

(a) if $k = n$ then $a_0 = 0$ and $a_0^* - a_0 = 0 \in S$ and $2^{n-k}a_0 = 0 \in S$.

(b) if $k < n$ then $(a_0, 2^k) \in T$ so $2^{n-k}(a_0, 2^k) = (2^{n-k}a_0, (2^n)_{2^n}) = (2^{n-k}a_0, 0) \in T$ so $2^{n-k}a_0 \in S$.

   (i) if $k > 0$ then $(a_0, 2^k)^* = (a_0^*, 2^k) \in T$ hence $(a_0^*, 2^k) - (a_0, 2^k) = (a_0^* - a_0, 0) \in T$ and $a_0^* - a_0 \in S$.

   (ii) if $k = 0$ then $(a_0, 2^k) = (a_0, 1) \in T$ and $2 \nmid 1$ so $(x_0, 0) \in T$ by Lemma 12. Moreover $T \ni (a_0, 1)^* - (a_0, 1) = (a_0^* + x_0, 1) - (a_0, 1) = (a_0^* - a_0 + x_0, 0)$ and $(x_0, 0) \in T$ hence $(a_0^* - a_0 + x_0, 0) - (x_0, 0) = (a_0^* - a_0, 0) \in T$ and $a_0^* - a_0 \in S$.

$\Leftarrow$ Suppose (i) and (ii) hold. We only need to show that $x_0 \in S$ or $k > 0$ and, then, we can conclude using Theorem 10.

(a) If $(x_0, 0) \in T$ then $(x_0, 0) \in T = [S, n, k, a_0] = \bigcup_{i=0}^{2^{n-k}-1}(S + ia_0) \times \{i2^k\}$ so $(x_0, 0) \in S \times \{0\}$ and $x_0 \in S$.

(b) If for all $(g, i) \in T$ we have $2|i$ then

   (i) if $k = n$ then $k > 0$ since $n \geq 1$.

   (ii) if $k < n$ then $(a_0, 2^k) \in (S + 1 \cdot a_0) \times \{1 \cdot 2^k\} \subseteq [S, n, k, a_0] = T$ so $2|2^k$ and $k > 0$.

By Theorem 10 $T = [S, n, k, a_0]$ is a subalgebra of $W_{n,x_0}(\mathcal{G})$. ■

**Lemma 15.** *Let $\mathcal{C}$ be an Abelian group, $A, B \leq \mathcal{C}$ and $a, b \in C$ then $(A + a) \cap (B + b) = \emptyset$ if and only if $a - b \notin A + B$*

***Proof.*** If $x \in (A + a) \cap (B + b) \neq \emptyset$ then there exist $a' \in A$ and $b' \in B$ such that $x = a' + a = b' + b$ so $a - b = (-a') + b' \in A + B$.

If $a - b \in A + B$ then there exist $a' \in A$ and $b' \in B$ such that $a - b = a' + b'$. Then $x := (-a') + a = b' + b \in (A + a) \cap (B + b)$ so $(A + a) \cap (B + b) \neq \emptyset$. ■

**Lemma 16.** *Let $\mathcal{G}$ be an Abelian group, $S \leq \mathcal{G}$, $a \in G$, $b \in G$ and $j \in \mathbb{Z}$. If there exists $w \in \mathbb{Z}$ such that $w > 0$, $wa \in S$, $wb \in S$, $S + a = S + jb$ and $\gcd(j, w) = 1$ then*

$$\{S + ia \colon i \in \mathbb{Z}_w\} = \{S + ib \colon i \in \mathbb{Z}_w\}.$$

***Proof.*** Let $L = \{S + ia \colon i \in \mathbb{Z}_w\}$ and $R = \{S + ib \colon i \in \mathbb{Z}_w\}$. First we show that $L \subseteq R$.

We know that $S + a = S + jb$ hence $a - jb \in S$ so if $i \in \mathbb{Z}_w$ then $i(a - jb) \in S$ and $S + ia = S + ijb \overset{wb \in S}{=} S + (ij)_w b \in R$. Therefore $L \subseteq R$.

Now we show that $R \subseteq L$.

We know that $S + a = S + jb$ and $\gcd(j, w) = 1$ hence $a - jb \in S$ and there exist $p, q \in \mathbb{Z}$ such that $pj + qw = 1$. Thus $S \ni pa - pjb = pa - (1 - qw)b = pa - b + qwb$ and $pa - b \in S$ since $wb \in S$. If $i \in \mathbb{Z}_w$ then $i(pa - b) \in S$ and $S + ib = S + ipa \overset{wa \in S}{=} S + (ip)_w a \in L$. Therefore $R \subseteq L$. ■

We show that if some conditions are fulfilled and $\mathcal{G}$ is directly indecomposable then $W_{n,x_0}(\mathcal{G})$ is directly indecomposable.

**Theorem 17.** *Let $\mathcal{G} = (G, +, -, ^*) \in AGI$ such that $x_0 = x_0^* \neq 0$ and $2x_0 = 0$ for some $x_0 \in G$, and assume hypotheses (H) hold.*

*Let $n \in \mathbb{N}$ and $r \geq n \geq 1$. Let $G_{n-1} := \{g \in G \colon \exists_{x \in G} 2^{n-1}x = g\}$. Moreover in case $n > 1$ assume that $\frac{|G|}{2^n} = |G_{n-1}|$ and for all subalgebras $S \leq \mathcal{G}$ such that $|G_{n-1}| < |S|$ we obtain that $G_{n-1} \subseteq S$.*

*If $\mathcal{G}$ is directly indecomposable then $W_{n,x_0}(\mathcal{G})$ is directly indecomposable.*

***Proof.*** Assume that $W_{n,x_0}(\mathcal{G})$ is directly decomposable. Then there exist subalgebras $T_1, T_2$ of the algebra $W_{n,x_0}(\mathcal{G})$ such that $T_1 \cap T_2 = \{(0,0)\}$, $|T_1| > 1$, $|T_2| > 1$ and $T_1 + T_2 = G \times \mathbb{Z}_{2^n}$.

We know that $(x_0, 0) \notin T_1 \cap T_2$ so $(x_0, 0) \notin T_1$ or $(x_0, 0) \notin T_2$. We can assume that $(x_0, 0) \notin T_2$. By Lemma 12 we have $T_2 \subseteq G \times \{i \in \mathbb{Z}_{2^n} \colon 2|i\}$.

By Theorem 14 we have

$$T_1 = [S_1, n, k_1, b_0] = \bigcup_{i=0}^{2^{n-k_1}-1} (S_1 + ib_0) \times \{i2^{k_1}\}$$

for some $S_1$ beeing a subalgebra of $\mathcal{G}$, $0 \leq k_1 \leq n$, $b_0 \in G$ such that $b_0^* - b_0 \in S_1$ and $2^{n-k_1} b_0 \in S_1$.

If $k_1 > 0$ then $T_1 \subseteq G \times \{i \in \mathbb{Z}_{2^n} \colon 2|i\}$ and $T_1 + T_2 \subseteq G \times \{i \in \mathbb{Z}_{2^n} \colon 2|i\}$ and we obtain a contradiction since $T_1 + T_2 = G \times \mathbb{Z}_{2^n}$. Hence $k_1 = 0$ and $T_1 \not\subseteq G \times \{i \in \mathbb{Z}_{2^n} \colon 2|i\}$ and by Lemma 12 we have $(x_0, 0) \in T_1$. Thus

$$\begin{aligned} T_1 &= (S_1 \times \{0\}) \\ &\cup ((S_1 + b_0) \times \{1\}) \cup \ldots \cup ((S_1 + (2^n - 1)b_0) \times \{2^n - 1\}), \end{aligned} \tag{1}$$

where

$$b_0^* - b_0 \in S_1, \quad 2^n b_0 \in S_1. \tag{2}$$

By Theorem 14 we have

$$T_2 = [S_2, n, k, a_0] = \bigcup_{i=0}^{2^{n-k}-1} (S_2 + ia_0) \times \{i2^k\}$$

for some $S_2$ beeing a subalgebra of $\mathcal{G}$, $0 \leq k \leq n$, $a_0 \in G$ such that $a_0^* - a_0 \in S_2$ and $2^{n-k} a_0 \in S_2$.

Consider the following cases:

1. If $k = n$ then $T_2 = S_2 \times \{0\}$ and $T_1 \cap T_2 = (S_1 \cap S_2) \times \{0\}$ so $S_1 \cap S_2 = \{0\}$ and by 1 we have

$$\begin{aligned} &G \times \mathbb{Z}_{2^n} = T_1 + T_2 = ((S_1 + S_2) \times \{0\}) \\ &\cup ((S_1 + S_2 + b_0) \times \{1\} \cup \ldots \cup (S_1 + S_2 + (2^n - 1)b_0) \times \{2^n - 1\} \end{aligned}$$

so $S_1 + S_2 = G$. Moreover $(x_0, 0) \in T_1$ and $x_0 \neq 0$ hence $x_0 \in S_1$ and $|S_1| > 1$. We know that $T_2 = S_2 \times \{0\}$ so $|S_2| = |T_2| > 1$. Therefore $\mathcal{G}$ is directly decomposable.

2. If $k < n$ then

$$\begin{aligned} T_2 = (S_2 \times \{0\}) \cup ((S_2 + a_0) \times \{2^k\}) \\ \cup \ldots \cup ((S_2 + (2^{n-k} - 1)a_0) \times \{(2^{n-k} - 1)2^k\}) \end{aligned} \tag{3}$$

where

$$a_0^* - a_0 \in S_2, \quad 2^{n-k} a_0 \in S_2 \tag{4}$$

and $0 < k < n$ because if $k = 0$ then $2^k = 1$ and $T_2 \not\subseteq G \times \{i \in \mathbb{Z}_{2^n} \colon 2|i\}$, so $k > 0$. Let $0 < i < 2^{n-k}$ by (3) we have

$$T_2 \cap (G \times \{i2^k\}) = (S_2 + ia_0) \times \{i2^k\}.$$

Moreover $T_1 \cap (G \times \{i2^k\}) = (S_1 + i2^k b_0) \times \{i2^k\}$ by (1). We know that $T_1 \cap T_2 = \{(0, 0)\}$ thus $T_1 \cap T_2 \cap (G \times \{i2^k\}) = \emptyset$ since $i2^k \neq 0$. Hence $(S_1 + i2^k b_0) \cap (S_2 + ia_0) = \emptyset$ so by Lemma 15 we have

$$i(a_0 - 2^k b_0) \notin S_1 + S_2 \tag{5}$$

for every $0 < i < 2^{n-k}$.

Let $0 < i < 2^{n-k}$. By (1) we have $T_1 \cap (G \times \{2^n - i2^k\}) = (S_1 + (2^n - i2^k)b_0) \times \{2^n - i2^k\}$. By (3) we have $T_2 \cap (G \times \{i2^k\}) = (S_2 + ia_0) \times \{i2^k\}$ hence

$$\begin{aligned} &(T_1 \cap (G \times \{2^n - i2^k\})) + (T_2 \cap (G \times \{i2^k\})) \\ &= (S_1 + (2^n - i2^k)b_0 + S_2 + ia_0) \times \{(2^n)_{2^n}\} \\ &= (S_1 + S_2 + i(a_0 - 2^k b_0)) \times \{0\} \end{aligned}$$

since $2^n b_0 \in S_1$ by (2).

Hence $(T_1+T_2)\cap(G\times\{0\}) = ((S_1+S_2)\cup\bigcup_{i=1}^{2^{n-k}-1}(S_1+S_2+i(a_0-2^kb_0)))\times\{0\}$ and

$$G=\bigcup_{i=0}^{2^{n-k}-1}(S_1+S_2+i(a_0-2^kb_0)) \tag{6}$$

since $T_1+T_2=G\times\mathbb{Z}_{2^n}$. Therefore there exists $0\le i_0<2^{n-k}$ such that

$$a_0\in S_1+S_2+i_0(a_0-2^kb_0). \tag{7}$$

Consider the following cases:

(a) If $2\nmid i_0$ then $\gcd(i_0,2^{n-k})=1$.

We show that $\mathcal{G}$ is isomorphic to direct product of $S_1$ and $B$, where $B$ is generated by $S_2\cup\{a_0\}$. By (4) we have $B=\bigcup_{i=0}^{2^{n-k}-1}(S_2+ia_0)$.

Let $L=\{S_1+S_2+i(a_0-2^kb_0)\colon i\in\mathbb{Z}_{2^{n-k}}\}$ and $R=\{S_1+S_2+ia_0\colon i\in\mathbb{Z}_{2^{n-k}}\}$. By lemma 16 (taking $a:=a_0$, $b:=a_0-2^kb_0$, $j:=i_0$, $S:=S_1+S_2$, $w:=2^{n-k}$) we obtain that $L=R$ since $S_1+S_2+a_0=S_1+S_2+i_0(a_0-2^kb_0)$ by (7).

Then

$$ia_0\notin S_1+S_2 \tag{8}$$

for every $0<i<2^{n-k}$ by (5) and since $R=L$.

Hence $S_1\cap(S_2+ia_0)=\emptyset$ for every $0<i<2^{n-k}$ by Lemma 15 and $S_1\cap S_2=\{0\}$ since $T_1\cap T_2=\{(0,0)\}$. Therefore $S_1\cap B=\{0\}$.

Moreover

$$\begin{aligned}S_1+B=S_1+\bigcup_{i=0}^{2^{n-k}-1}(S_2+ia_0)&=\bigcup_{i=0}^{2^{n-k}-1}(S_1+S_2+ia_0)\\ &\overset{L=R}{=}\bigcup_{i=0}^{2^{n-k}-1}(S_1+S_2+i(a_0-2^kb_0))\overset{(6)}{=}G\end{aligned}$$

and we have that $\mathcal{G}$ is isomorphic to direct product of $S_1$ and $B$.

Additionally $|S_1|>1$ since $0\neq x_0\in S_1$ and $|B|>1$ since $a_0\in B$ and $a_0\neq 0$ by (8).

Hence $\mathcal{G}$ is directly decomposable.

(b) If $2|i_0$ then $\gcd(1-i_0,2^{n-k})=1$.

We show that $\mathcal{G}$ is isomorphic to direct product of $S_2$ and $C$, where $C$ is generated by $S_1\cup\{2^kb_0\}$. By (2) we have

$$C=\bigcup_{i=0}^{2^{n-k}-1}S_1+i2^kb_0. \tag{9}$$

Let $L_1 = \{S_1 + S_2 + i(a_0 - 2^k b_0) \colon i \in \mathbb{Z}_{2^{n-k}}\}$ and $R_1 = \{S_1 + S_2 + i2^k b_0 \colon i \in \mathbb{Z}_{2^{n-k}}\}$. We know that $\gcd(1 - i_0, 2^{n-k}) = 1$ so there exist $t, s \in \mathbb{Z}$ such that $(1 - i_0)t + s2^{n-k} = 1$.

We show that $S_1 + S_2 + a_0 - 2^k b_0 = S_1 + S_2 + (-1 - ti_0)2^k b_0$. By (7) we have $(1 - i_0)a_0 + i_0 2^k b_0 \in S_1 + S_2$ so $S_1 + S_2 \ni t(1 - i_0)a_0 + ti_0 2^k b_0 = (1 - s2^{n-k})a_0 + ti_0 2^k b_0 = a_0 - s2^{n-k} a_0 + ti_0 2^k b_0$ and $a_0 + ti_0 2^k b_0 \in S_1 + S_2$ by (4). Hence $a_0 - 2^k b_0 + (1+ti_0)2^k b_0 \in S_1+S_2$ and $S_1+S_2+a_0-2^k b_0 = S_1+S_2+(-1-ti_0)2^k b_0$.

We know that $2|i_0$ so $\gcd(2^{n-k}, -1 - ti_0) = 1$ and by Lemma 16 (taking $j := -1 - ti_0$, $a := a_0 - 2^k b_0$, $b := 2^k b_0$, $S := S_1 + S_2$, $w := 2^{n-k}$) we have that $L_1 = R_1$.

Then

$$i2^k b_0 \notin S_1 + S_2 \tag{10}$$

for every $0 < i < 2^{n-k}$ by (5) and since $R_1 = L_1$.

Hence $S_2 \cap (S_1 + i2^k b_0) = \emptyset$ for every $0 < i < 2^{n-k}$ by Lemma 15 and $S_1 \cap S_2 = \{0\}$ since $T_1 \cap T_2 = \{(0, 0)\}$. Therefore $S_2 \cap C = \{0\}$.

Moreover

$$\begin{aligned} S_2 + C = S_2 + \bigcup_{i=0}^{2^{n-k}-1} (S_1 + i2^k b_0) &= \bigcup_{i=0}^{2^{n-k}-1} (S_1 + S_2 + i2^k b_0) \\ &\overset{L_1=R_1}{=} \bigcup_{i=0}^{2^{n-k}-1} (S_1 + S_2 + i(a_0 - 2^k b_0)) \overset{(6)}{=} G \end{aligned}$$

and we have that $\mathcal{G}$ is isomorphic to direct product of $S_2$ and $C$.

Additionally $|S_1| > 1$ since $0 \neq x_0 \in S_1$ so $|C| > 1$.

We prove that $|S_2| > 1$. Suppose that $|S_2| = 1$ then $S_1 + S_2 = S_1$ and by (7) there exists $s_1 \in S_1$ such that $a_0 = s_1 + i_0(a_0 - 2^k b_0)$ so

$$\begin{aligned} 2^{n-k-1} a_0 &= 2^{n-k-1} s_1 + 2^{n-k-1} i_0 (a_0 - 2^k b_0) \\ &= 2^{n-k-1} s_1 + 2^{n-k} a_0 \tfrac{i_0}{2} - 2^n b_0 \tfrac{i_0}{2} = 2^{n-k-1} s_1 - 2^n b_0 \tfrac{i_0}{2} \in S_1 \end{aligned} \tag{11}$$

since $2^{n-k} a_0 \in S_2 = \{0\}$ and $2^n b_0 \in S_1$ by (2).

Moreover $|G| = |C| \cdot |S_2| = |C| = |S_1| 2^{n-k}$ by (9) and (10). Hence $|G_{n-1}| = \frac{|G|}{2^n} < \frac{|G|}{2^{n-k}} = |S_1|$ thus $2^{n-1} b_0 \in G_{n-1} \subseteq S_1$ and $2^{n-1} b_0 \in S_1$ so by (11) we obtain $2^{n-k-1}(a_0 - 2^k b_0) = 2^{n-k-1} a_0 - 2^{n-1} b_0 \in S_1 = S_1 + S_2$ which contradicts (5). Hence $|S_2| > 1$ and $\mathcal{G}$ is directly decomposable. ∎

Now we shall study the case where $\mathcal{G} := Q^0_{2^n,2}$ (see Definition 1). In particular, in the following two lemmas we characterize the involution $*$ in $Q^0_{2^n,2}$.

**Lemma 18.** *Let $n \in \mathbb{Z}$ and $n \geq 1$. If $(a,b) \in \mathbb{Z}_{2^n} \times \mathbb{Z}_2$ and $2|a+b$ then $(a,b)^* = (a,b)$ in $Q^0_{2^n,2}$.*

***Proof.*** Consider the following cases:

1. If $b = 0$ then $2|a$ and $b + E(\frac{a}{2})2 = 0 + \frac{a}{2}2 = a$ so $(a,b)^* = \gamma^0_{2^n,2}(b,a) = ((b + E(\frac{a}{2})2)_{2^n}, (a)_2) = (a,0) = (a,b)$.
2. If $b = 1$ then $2 \nmid a$ and $b + E(\frac{a}{2})2 = 1 + E(\frac{a}{2})2 = a$ so $(a,b)^* = \gamma^0_{2^n,2}(b,a) = ((b + E(\frac{a}{2})2)_{2^n}, (a)_2) = (a,1) = (a,b)$.

■

**Lemma 19.** *Let $n \in \mathbb{Z}$, $n \geq 1$. If $(a,b) \in \mathbb{Z}_{2^n} \times \mathbb{Z}_2$ and $2 \nmid a+b$ then*

$$(a,b)^* = \begin{cases} (a-1,1) & for\ b = 0 \\ (a+1,0) & for\ b = 1 \end{cases}$$

*in $Q^0_{2^n,2}$*

***Proof.*** Consider the following cases:

1. If $b = 0$ then $2 \nmid a$ and $b + E(\frac{a}{2})2 = 0 + \frac{a-1}{2}2 = a - 1$ so $(a,b)^* = \gamma^0_{2^n,2}(b,a) = ((b + E(\frac{a}{2})2)_{2^n}, (a)_2) = (a-1,1)$.
2. If $b = 1$ then $2|a$ and $b + E(\frac{a}{2})2 = 1 + \frac{a}{2}2 = a + 1$ so $(a,b)^* = \gamma^0_{2^n,2}(b,a) = ((b + E(\frac{a}{2})2)_{2^n}, (a)_2) = (a+1,0)$.

■

In the definition below we introduce three possible forms of nontrivial subalgebras of $Q^0_{2^m,2}$.

**Definition.** Let $m.k \in \mathbb{Z}$, $m \geq 1$, $1 \leq k \leq m$. Let

$$S_{k,m,0} = \{(t2^k, 0) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2 \colon 0 \leq t < 2^{m-k}\},$$

$$S_{k,m,1} = S_{k,m,0} \cup \{(2^{k-1} - 1 + t2^k, 1) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2 \colon 0 \leq t < 2^{m-k}\},$$

$$S_{k,m,2} = S_{k,m,0} \cup \{(2^k - 1 + t2^k, 1) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2 \colon 0 \leq t < 2^{m-k}\}.$$

**Theorem 20.** *[3, 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.*

The followiong theorem describes all subalgebras of $Q^0_{2^m,2}$.

**Theorem 21.** *Let $m \in \mathbb{Z}$ and $m \geq 1$. Then $S$ is a subalgebra of $Q^0_{2^m,2}$ if and only if $S = \{(0,0)\}$ or $S = \mathbb{Z}_{2^m} \times \mathbb{Z}_2$, or $S = S_{k,m,0}$ for $k = 1, \ldots, m-1$, or $S = S_{k,m,1}$ for $k = 2, \ldots, m$, or $S = S_{k,m,2}$ for $k = 1, \ldots, m$.*

***Proof.*** It is easy to check that $S_{k,m,0} \le Q^0_{2^m,2}$ for $k = 1,\dots,m-1$, $S_{k,m,1} \le Q^0_{2^n,2}$ for $k = 2,\dots,m$, $S = S_{k,m,2} \le Q^0_{2^m,2}$ for $k = 1,\dots,m$.

Suppose that $S \le Q^0_{2^m,2}$ and $S \ne \{(0,0)\}$, and $S \ne \mathbb{Z}_{2^m} \times \mathbb{Z}_2$. Let $U = \{x \in \mathbb{Z}_{2^m} \colon (x,0) \in S\}$ then $U$ is a subgroup of $\mathbb{Z}_{2^m}$ hence there exists $0 \le k \le m$ such that $U = \{t2^k \in \mathbb{Z}_{2^m} \colon 0 \le t < 2^{m-k}\}$. Moreover

$$S \cap (\mathbb{Z}_{2^m} \times \{0\}) = \{(t2^k, 0) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2 \colon 0 \le t < 2^{m-k}\}. \tag{12}$$

If $k = 0$ then $1 \cdot 2^k = 1$ and $(1,0) \in S$ so $S = \mathbb{Z}_{2^m} \times \mathbb{Z}_2$. Hence $k > 0$.

Consider the following cases:

1. If $S \cap (\mathbb{Z}_{2^m} \times \{1\}) = \emptyset$ then $S \subseteq \mathbb{Z}_{2^m} \times \{0\}$. If $k = m$ then $U = \{0\}$ and $S = \{(0,0)\}$. Hence $1 \le k \le m-1$ and $S = U \times \{0\} = S_{k,m,0}$.

2. If $S \cap \mathbb{Z}_{2^m} \times \{1\} \ne \emptyset$ then there exists $x \in \mathbb{Z}_{2^m}$ such that $(x,1) \in S$. Let $r = (x)_{2^k}$ and $t = E(\frac{x}{2^k})$ then $x = t2^k + r$, where $0 \le r < 2^k$. Thus $(x,1) - t(2^k,0) = (r,1) \in S$. If $2|r$ then $2 \nmid r+1$ and as it was shown in the proof of Theorem 20 $(r,1)$ generates $Q^0_{2^m,2}$ so $S = \mathbb{Z}_{2^m} \times \mathbb{Z}_2$. Hence $2 \nmid r$ so $r = 2q+1$ for some $q \in \mathbb{Z}$. Thus

$$\begin{aligned} 2(r,1) &= 2(2q+1,1) = \gamma^0_{2^m,2}(4q+2,2) \\ &= ((4q+2+E(\tfrac{2}{2})2)_{2^m},0) = ((4q+4)_{2^m},0) \in S \end{aligned}$$

so by (12)

$$2^k | 4q+4. \tag{13}$$

Consider the following cases:

(a) If $k = 1$ then $(2,0) \in S$ by (12). Hence $(r,1) - q(2,0) = (r-2q,1) = (1,1) \in S$. It is easy to check that $S_{1,m,2}$ is generated by $(1,1)$ and $(2,0)$. Thus $S_{1,m,2} \subseteq S$. Moreover $S_{1,m,2} = \{(x,y) \in \mathbb{Z}_{2^m} \times \mathbb{Z}_2 \colon 2|x+y\}$ so as it was shown in the proof of Theorem 20 $S_{1,m,2}$ is the bigest nontrivial subalgebra of $Q^0_{2^m,2}$. Hence $S = S_{1,m,2}$.

(b) If $k \ge 2$ then by (13) $2^{k-2}|q+1$ so there exists $w \in \mathbb{Z}$ such that $q+1 = w2^{k-2}$. Hence $w2^{k-1} - 1 = 2(q+1) - 1 = 2q+1 = r$ and $0 < r < 2^k$ so

$$0 < w2^{k-1} - 1 < 2^k. \tag{14}$$

If $w \ge 3$ then $w2^{k-1} - 1 \ge 3 \cdot 2^{k-1} - 1 = 2^{k-1} + 2^k - 1 \ge 2 - 1 + 2^k = 1 + 2^k$ so by (14) $w = 1$ or $w = 2$.

(i) If $w=1$ then $r=w2^{k-1}-1=2^{k-1}-1$ so $(2^{k-1}-1,1)\in S$ and $S_{k,m,1}\subseteq S$ since $(2^{k-1}-1,1)$ generates $S_{k,m,1}$. If $(y,0)\in S$ then $2^k|y$ by (12) therefore $(y,0)\in S_{k,m,1}$. If $(y,1)\in S$ then

$$(y,1)-(2^{k-1}-1,1)=((y-2^{k-1}+1)_{2^m},0)\in S$$

so $2^k|y-2^{k-1}+1$ by (12) and there exists $t\in\mathbb{Z}$ such that $y-2^{k-1}+1=t2^k$ hence $y=2^{k-1}-1+t2^k$ and $0\le t<2^{m-k}$ since $y\in\mathbb{Z}_{2^m}$. Thus $(y,1)\in S_{k,m,1}$ and $S\subseteq S_{k,m,1}$. Therefore $S=S_{k,m,1}$.

(ii) If $w=2$ then $r=w2^{k-1}-1=2^k-1$ so $(2^k-1,1)\in S$ and $(2^k,0)\in S$ by (12). Thus $S_{k,m,2}\subseteq S$ since $S_{k,m,2}$ is generated by $(2^k-1,1)$ and $(2^k,0)$. If $(y,0)\in S$ then $2^k|y$ by (12) therefore $(y,0)\in S_{k,m,2}$. If $(y,1)\in S$ then

$$(y,1)-(2^k-1,1)=((y-2^k+1)_{2^m},0)\in S$$

so $2^k|y-2^k+1$ by (12) and there exists $t\in\mathbb{Z}$ such that $y-2^k+1=t2^k$ hence $y=2^k-1+t2^k$ and $0\le t<2^{m-k}$ since $y\in\mathbb{Z}_{2^m}$. Thus $(y,1)\in S_{k,m,2}$ and $S\subseteq S_{k,m,2}$. Hence $S=S_{k,m,2}$.

■

It turns out that:

**Lemma 22.** *Let $m,n\in\mathbb{Z}$, $m-1\ge n\ge 1$, $r=m-1$ and $x_0=(2^{m-1},0)$, $\mathcal{G}=Q^0_{2^m,2}$.*

*Then $x_0=x_0^*\neq(0,0)$, $2x_0=(0,0)$ and hypotheses (H) are satisfied for $r=m-1$.*

*Let $G_{n-1}:=\{g\in G\colon\exists_{x\in G}2^{n-1}x=g\}$. If $n>1$ then $\frac{|G|}{2^n}=|G_{n-1}|$ and for all subalgebras $S\le\mathcal{G}$ such that $|G_{n-1}|<|S|$ we obtain that $G_{n-1}\subseteq S$.*

*So all assumptions of Theorem 17 are satisfied.*

***Proof.*** By Lemma 18 $x_0^*=x_0$ since $2|2^{m-1}$. Moreover

$$2x_0=\gamma^0_{2^m,2}(2^m,0)=(0,0)$$

and $x_0=(2^{m-1},0)\neq(0,0)$.

The hypotheses (H) are satisfied for $r=m-1$ by Example 11.
Let $n>1$. We show that $G_{n-1}=S_{n-1,m,0}$, where $G_{n-1}:=\{g\in G\colon\exists_{x\in G}2^{n-1}x=g\}$.

If $(a,b)\in S_{n-1,m,0}$ then $b=0$ and $a=t2^{n-1}$ where $0\le t<2^{m-(n-1)}$ so $(a,b)=(t2^{n-1},0)=2^{n-1}(t,0)\in G_{n-1}$.

If $(a,b)\in G_{n-1}$ then there exists $(c,d)\in G$ such that $(a,b)=2^{n-1}(c,d)$. Moreover

$$2^{n-1}(c,d) = \gamma^0_{2^m,2}(2^{n-1}c, 2^{n-1}d) = ((2^{n-1}c + E(\tfrac{2^{n-1}d}{2})2)_{2^m}, (2^{n-1}d)_2)$$
$$\overset{n\geq 1}{=} ((2^{n-1}(c+d))_{2^m}, 0) \in S_{n-1,m,0}.$$

Hence

$$|G_{n-1}| = |S_{n-1,m,0}| = 2^{m-(n-1)} = \frac{|G|}{2^n}. \tag{15}$$

Let $S \leq \mathcal{G}$ and $|G_{n-1}| < |S|$. We show that $G_{n-1} \subseteq S$. Obviously $S \neq \{(0,0)\}$ and if $S = G$ then $G_{n-1} \subseteq S$. By Theorem 21 it remains to consider the following cases

1. $S = S_{k,m,0}$ for $1 \leq k \leq m-1$. Then $|S| = 2^{m-k} > |G_{n-1}| = 2^{m-n+1}$ by (15). Thus $m-k > m-n+1$ and $n-1 > k$ so $G_{n-1} = S_{n-1,m,0} \subseteq S_{k,m,0} = S$.
2. $S = S_{k,m,1}$ or $S = S_{k,m,2}$. Then $|S| = 22^{m-k} > |G_{n-1}| = 2^{m-n+1}$ by (15). Hence $m-k+1 > m-n+1$ and $n-1 > k-1$ so $n-1 \geq k$ and $2^k | 2^{n-1}$ thus $(2^{n-1}, 0) \in S_{k,m,0} \subseteq S$. Then $G_{n-1} = S_{n-1,m,0} \subseteq S$. ∎

**Theorem 23.** *Let $m, n \in \mathbb{Z}$ and $m-1 \geq n \geq 1$.*
*Then quasigroup $\Psi(W_{n,(2^{m-1},0)}(Q^0_{2^m,2}))$ is directly indecomposable.*

***Proof.*** By Theorem 6 it is sufficient to show that $W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$ is directly indecomposable. Using 22 and 17 we conclude that $W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$ is directly indecomposable since $Q^0_{2^m,2}$ is directly indecomposable by Theorem 20. ∎

Moreover we obtain that:

**Theorem 24.** *Let $m, n \in \mathbb{Z}$ and $m-1 \geq n \geq 1$.*
*Then quasigroup $\Psi(W_{n,(2^{m-1},0)}(Q^0_{2^m,2}))$ is two-generated.*

***Proof.*** It is sufficient to show that $W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$ is two-generated.

Let $x = ((1,0),0)$ and $y = ((0,0),1)$. If $((a,b),c) \in (\mathbb{Z}_{2^m} \times \mathbb{Z}_2) \times \mathbb{Z}_{2^n}$ then $((a,b),c) = ax + bx^* + cy$ so $x$ and $y$ generates $W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$.

Let

$$A = \{((a,b),c) \in (\mathbb{Z}_{2^m} \times \mathbb{Z}_2) \times \mathbb{Z}_{2^n} \colon 2|c\}$$
$$B = \{((a,b),c) \in (\mathbb{Z}_{2^m} \times \mathbb{Z}_2) \times \mathbb{Z}_{2^n} \colon 2|a+b\}$$
$$C = \{((a,b),c) \in (\mathbb{Z}_{2^m} \times \mathbb{Z}_2) \times \mathbb{Z}_{2^n} \colon 2|a+b+c\}.$$

We show that $A \leq W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$.

If $((a,b),c), ((a',b'),c') \in A$ then $2|c$ and $2|c'$. Hence $((a,b),c) + ((a',b'),c') = ((a,b) +_{Q^0_{2^m,2}} (a',b'), (c+c')_{2^n}) \in A$ since $2|c+c'$. Moreover $((a,b),c)^* = ((a,b)^*, c) \in A$.

We show that $B \leq W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$.

If $((a,b),c),((a',b'),c') \in B$ then $2|a+b$ and $2|a'+b'$. Hence $2|a+b+a'+b'$ and $2|(a+a'+E(\frac{b+b'}{2})2)_{2^m}+(b+b')_2$ thus

$$\begin{aligned}((a,b),c)\ &+((a',b'),c') = (\gamma^0_{2^m,2}(a+a',b+b'),(c+c')_{2^n})\\ &= (((a+a'+E(\tfrac{b+b'}{2})2)_{2^m},(b+b')_2),(c+c')_{2^n}) \in B\end{aligned}$$

and

1. if $2|c$ then $((a,b),c)^* = ((a,b)^*,c) \overset{18}{=} ((a,b),c) \in B$.
2. if $2 \nmid c$ then

$$\begin{aligned}((a,b),c)^* &= ((a,b)^* +_{Q^0_{2^m,2}} (2^{m-1},0),c) \overset{18}{=} ((a,b) +_{Q^0_{2^m,2}} (2^{m-1},0),c)\\ &= (\gamma^0_{2^m,2}(a+2^{m-1},b),c)\\ &= (((a+2^{m-1}+E(\tfrac{b}{2})2)_{2^m},(b)_2),c).\end{aligned}$$

Moreover $m-1 \geq 1$ so $2|2^{m-1}$ thus $2|(a+2^{m-1}+E(\frac{b}{2})2)_{2^m}+(b)_2$ since $2|a+b$. Hence $((a,b),c)^* \in B$.

We show that $C \leq W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$.

If $((a,b),c),((a',b'),c') \in C$ then $2|a+b+c$ and $2|a'+b'+c'$. Hence $2|a+b+c+a'+b'+c'$ and $2|(a+a'+E(\frac{b+b'}{2})2)_{2^m}+(b+b')_2+(c+c')_{2^n}$ thus

$$\begin{aligned}((a,b),c)\ &+((a',b'),c') = (\gamma^0_{2^m,2}(a+a',b+b'),(c+c')_{2^n})\\ &= (((a+a'+E(\tfrac{b+b'}{2})2)_{2^m},(b+b')_2),(c+c')_{2^n}) \in C\end{aligned}$$

and

1. if $2|c$ then $((a,b),c)^* = ((a,b)^*,c) \overset{18}{=} ((a,b),c) \in C$
2. if $2 \nmid c$ then $2 \nmid a+b$.
   (a) If $b=0$ then $2 \nmid a$ thus $2|a+c$ so $2|(a+1+2^{m-1})_{2^m}+1+c$ and

$$\begin{aligned}((a,b),c)^* &= ((a,b)^* +_{Q^0_{2^m,2}} (2^{m-1},0),c)\\ &\overset{19}{=} ((a-1,1) +_{Q^0_{2^m,2}} (2^{m-1},0),c)\\ &= (\gamma^0_{2^m,2}(a-1+2^{m-1},1),c)\\ &= (((a-1+2^{m-1}+E(\tfrac{1}{2})2)_{2^m},(1)_2),c)\\ &= (((a+1+2^{m-1})_{2^m},1),c) \in C.\end{aligned}$$

(b) If $b = 1$ then $2|a$ thus $2|a + 1 + c$ so $2|(a + 1 + 2^{m-1})_{2^m} + c$ and

$$\begin{aligned} ((a, b), c)^* &= ((a, b)^* +_{Q^0_{2^m,2}} (2^{m-1}, 0), c) \\ &\overset{19}{=} ((a + 1, 0) +_{Q^0_{2^m,2}} (2^{m-1}, 0), c) \\ &= (\gamma^0_{2^m,2}(a + 1 + 2^{m-1}, 0), c) \\ &= (((a + 1 + 2^{m-1} + E(\tfrac{0}{2})2)_{2^m}, (0)_2), c) \\ &= (((a + 1 + 2^{m-1})_{2^m}, 0), c) \in C. \end{aligned}$$

We show that $A \cup B \cup C = (\mathbb{Z}_{2^m} \times \mathbb{Z}_2) \times \mathbb{Z}_{2^n}$.

Let $((a, b), c) \in (\mathbb{Z}_{2^m} \times \mathbb{Z}_2) \times \mathbb{Z}_{2^n}$. If $2|c$ then $((a, b), c) \in C$. If $2 \nmid c$ and $2|a+b$ then $((a, b), c) \in B$. If $2 \nmid c$ and $2 \nmid a + b$ then $2|a + b + c$ and $((a, b), c) \in C$.

Hence every one-generated subalgebra $S$ of $W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$ is contained in $A$ or $B$, or $C$. Therefore $W_{n,(2^{m-1},0)}(Q^0_{2^m,2})$ is non-monogenic. ■

The following theorem summarizes all our considerations concerning quasigroups mentioned in the title of this paper.

**Theorem 25.** *In the variety EQ1 there exists an infinite family of pairwise non-isomorphic quasigroups which are directly indecomposable and they are two-generated and non-monogenic.*

***Proof.*** Let $R = \{\Psi(W_{n,(2^n,0)}(Q^0_{2^{n+1},2})) \colon n \in \mathbb{Z}, n \geq 1\}$. By Theorem 24 every element of $R$ is two-generated. From Theorem 23 it follows that every element of $R$ is directly indecomposable. Moreover if $n_1 < n_2$, $A_1 = \Psi(W_{n_1,(2^{n_1},0)}(Q^0_{2^{n_1+1},2}))$, $A_2 = \Psi(W_{n_2,(2^{n_2},0)}(Q^0_{2^{n_2+1},2}))$ then $|A_1| = 2^{2n_1+2} < 2^{2n_2+2} = |A_2|$ so $A_1$ is not isomorphic to $A_2$. ■

## REFERENCES

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

[2] G. Bińczak and J. Kaleta, *Finite simple monogenic entropic quasigroups with quasi-identity*, Demonstratio Math. **44** (2011) 17–27.

[3] G. Bińczak and J. Kaleta, *Finite directly indecomposable monogenic entropic quasi-groups with quasi-identity*, Demonstratio Math. **45** (2012) 519–532.

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

[5] J.J. Rotman, An Introduction to the Theory of Groups (Springer-Verlag, New York, 1994).

[6] J.D.H. Smith, Representation Theory of Infinite Groups and Finite Quasigroups (Université de Montréal, 1986).

Received 14 March 2013
First Revision 8 April 2013
Second Revision 25 July 2013