

Linear representation of algebras with non-associative operations which are satisfy in the balanced functional equations

Amir Ehsani

Department of Mathematics, Mahshshar Branch, Islamic Azad University, Mahshahr, Iran.

E-mail: a.ehsani@mhriau.ac.ir

Abstract. Algebras with a pair of non-associative binary operations (f, g) which are satisfy in the balanced quadratic functional equations with four object variables considered. First, we obtain a linear representation for the operations, of this kind of binary algebras (\mathbf{A}, f, g) , over an abelian group $(\mathbf{A}, +)$ and then we generalize the linear representation of operations, to an algebra (\mathbf{A}, F) with non-associative binary operations which are satisfy in the balanced quadratic functional equations with four object variables.

1. Introduction

A binary algebra \mathbf{A} is an ordered pair (A, F) , where A is a nonempty set and F is a family of binary operations $f : A^2 \rightarrow A$. The set A is called the universe (base, underlying set) of the algebra $\mathbf{A} = (A, F)$. If F is finite, say $F = \{f_1, \dots, f_k\}$, we often write (A, f_1, \dots, f_k) for (A, F) . The algebra \mathbf{A} is a groupoid if it has only one binary operation.

A quasigroup is a natural generalization of the concept of a group. Quasigroups differ from groups in that they need not be associative. A quasigroup is usually defined to be a groupoid (A, f) such that for any $a, b \in A$ there are unique solutions x, y of A , for the equations $f(a, x) = b$ and $f(y, a) = b$.

A loop is a quasigroup with unit (e) such that $f(e, x) = f(x, e) = x$. Groups are associative quasigroups, i.e. they satisfy: $f(f(x, y), z) = f(x, f(y, z))$ and they necessarily contain a unit.

If (A, f) is a quasigroup we say that f is a quasigroup operation.

Quasigroups are important algebraic (combinatorial, geometric) structures which arise in various areas of mathematics and other disciplines. We mention just a few of their applications: in combinatorics (as latin squares, see [1]), in geometry (as nets/webs, see [1] and [2]), in statistics (see [3]), in special theory of relativity (see [4]), in coding theory and cryptography ([5]).

A triple (α, β, γ) of bijections from a set G onto a set H is called an isotopism of a groupoid (G, \cdot) onto a groupoid (H, \circ) provided $\gamma(x \cdot y) = \alpha x \circ \beta y$ for all $x, y \in G$. (H, \circ) is then called an



isotope of (G, \cdot) , and groupoids (G, \cdot) and (H, \circ) are called isotopic to each other. An isotopism of (G, \cdot) onto (G, \cdot) is called an autotopism of (G, \cdot) .

Isotopism is a generalization of isomorphism. Isotopic image of a quasigroup is again a quasigroup. A loop isotopic to a group is isomorphic to it. Every quasigroup is isotopic to some loop i.e., it is a loop isotope.

Let α and β be permutations of G and let ι denote the identity map on G . Then (α, β, ι) is a principal isotopism of a groupoid (G, \cdot) onto a groupoid (G, \circ) means that (α, β, ι) is an isotopism of (G, \cdot) onto (G, \circ) .

A binary quasigroup (A, f) is linear over a group if $f(x, y) = \varphi x + a + \psi y$, where $(A, +)$ is a group, φ and ψ are automorphisms of the group $(A, +)$ and $a \in A$ is a fixed element.

A quasigroup linear over an Abelian group is also called a T-quasigroup.

Functional equation $s = t$ is quadratic if every variable appears exactly twice in $s = t$. Quadratic equation is balanced (or linear) if every variable appears exactly once in s and once in t .

The following are various functional equations.

$$f(f(x, y), z) = f(x, f(y, z)), \quad (1)$$

$$f(f(x, y), f(u, v)) = f(f(x, u), f(y, v)), \quad (2)$$

$$f(f(x, y), f(u, v)) = f(f(f(x, u), y), v), \quad (3)$$

$$f(x, f(y, z)) = f(f(x, y), f(x, z)), \quad (4)$$

$$f(f(x, y), f(y, z)) = f(x, z), \quad (5)$$

$$f(x, x) = x. \quad (6)$$

Associativity (1), mediality (2) and pseudomediality (3) are balanced, transitivity (5) is quadratic but not balanced while left distributivity (4) and idempotency (6) are not even quadratic.

A classification of quadratic level quasigroup functional equations with four variables is given in [6] and [7].

Let us consider the following balanced identities:

$$f(f(x, y), f(u, v)) = f(f(x, u), f(y, v)) \quad (7)$$

$$f(f(x, y), f(u, v)) = f(f(x, u), f(v, y)) \quad (8)$$

$$f(f(x, y), f(u, v)) = f(f(x, v), f(y, u)) \quad (9)$$

$$f(f(x, y), f(u, v)) = f(f(x, v), f(u, y)) \quad (10)$$

$$f(f(x, y), f(u, v)) = f(f(y, u), f(x, v)) \quad (11)$$

$$f(f(x, y), f(u, v)) = f(f(y, u), f(v, x)) \quad (12)$$

$$f(f(x, y), f(u, v)) = f(f(y, v), f(x, u)) \quad (13)$$

$$f(f(x, y), f(u, v)) = f(f(y, v), f(u, x)) \quad (14)$$

$$f(f(x, y), f(u, v)) = f(f(u, x), f(y, v)) \quad (15)$$

$$f(f(x, y), f(u, v)) = f(f(u, x), f(v, y)) \quad (16)$$

$$f(f(x, y), f(u, v)) = f(f(u, y), f(x, v)) \quad (17)$$

$$f(f(x, y), f(u, v)) = f(f(u, y), f(v, x)) \quad (18)$$

$$f(f(x, y), f(u, v)) = f(f(v, x), f(y, u)) \quad (19)$$

$$f(f(x, y), f(u, v)) = f(f(v, x), f(u, y)) \quad (20)$$

$$f(f(x, y), f(u, v)) = f(f(v, y), f(x, u)) \quad (21)$$

$$f(f(x, y), f(u, v)) = f(f(v, y), f(u, x)) \quad (22)$$

A quasigroup is called medial (or paramedial) if it satisfies (7) (or (22)). In the following theorems it is shown that every medial (paramedial) quasigroup is a T-quasigroup.

Theorem 1.1. [8] *If (Q, \cdot) is a medial quasigroup, then there exists an abelian group, $(Q, +)$, such that*

$$x \cdot y = \varphi(x) + c + \psi(y),$$

where $\varphi, \psi \in \text{Aut}(Q, +)$, $\varphi\psi = \psi\varphi$ and $c \in Q$.

Theorem 1.2. [9] *If (Q, \cdot) is a paramedial quasigroup, then there exists an abelian group, $(Q, +)$, such that*

$$x \cdot y = \varphi(x) + c + \psi(y),$$

where $\varphi, \psi \in \text{Aut}(Q, +)$, $\varphi\varphi = \psi\psi$ and $c \in Q$.

Equations (7)-(22) are also called non-Belousov level equations.

Theorem 1.3. [10] *Let a quasigroup satisfy a non-Belousov level equation. Then it is a T-quasigroup.*

Certain generalizations of medial and paramedial algebras with non-associative operations (quasigroup operations) and their linear representation were obtained in [11, 12].

2. MAIN RESULTS

As a generalization of equations (7)-(22), we consider the following functional equations:

$$f(g(x, y), g(u, v)) = g(f(x, u), f(y, v)) \quad (23)$$

$$f(g(x, y), g(u, v)) = g(f(x, u), f(v, y)) \quad (24)$$

$$f(g(x, y), g(u, v)) = g(f(x, v), f(y, u)) \quad (25)$$

$$f(g(x, y), g(u, v)) = g(f(x, v), f(u, y)) \quad (26)$$

$$f(g(x, y), g(u, v)) = g(f(y, u), f(x, v)) \quad (27)$$

$$f(g(x, y), g(u, v)) = g(f(y, u), f(v, x)) \quad (28)$$

$$f(g(x, y), g(u, v)) = g(f(y, v), f(x, u)) \quad (29)$$

$$f(g(x, y), g(u, v)) = g(f(y, v), f(u, x)) \quad (30)$$

$$f(g(x, y), g(u, v)) = g(f(u, x), f(y, v)) \quad (31)$$

$$f(g(x, y), g(u, v)) = g(f(u, x), f(v, y)) \quad (32)$$

$$f(g(x, y), g(u, v)) = g(f(u, y), f(x, v)) \quad (33)$$

$$f(g(x, y), g(u, v)) = g(f(u, y), f(v, x)) \quad (34)$$

$$f(g(x, y), g(u, v)) = g(f(v, x), f(y, u)) \quad (35)$$

$$f(g(x, y), g(u, v)) = g(f(v, x), f(u, y)) \quad (36)$$

$$f(g(x, y), g(u, v)) = g(f(v, y), f(x, u)) \quad (37)$$

$$f(g(x, y), g(u, v)) = g(f(v, y), f(u, x)) \quad (38)$$

Definition 2.1. A pair (f, g) of binary operations is called:

- medial (or entropic, in the sense of [13]), if the algebra (A, f, g) satisfies the equation (23),
- paramedial, if the algebra (A, f, g) satisfies the equation (38).

A binary algebra $\mathbf{A} = (A, F)$ is called:

- medial, if every pair of operations of the algebra \mathbf{A} is medial,
- paramedial, if every pair of operations of the algebra \mathbf{A} is paramedial.

A linear representation of a binary medial algebra with non-associative operations (quasigroup operations) and a linear representation of a binary paramedial algebra with non-associative operations (quasigroup operations) are obtained in [14] and [15], respectively.

The aim of this paper is to show that every binary algebra with quasigroup operations, which satisfies one of the (23)-(38), has linear representation over an abelian group.

Definition 2.2. If (Q, \cdot) is a group, then the bijection, $\alpha : Q \rightarrow Q$, is called a holomorphism of (Q, \cdot) if

$$\alpha(x \cdot y^{-1} \cdot z) = \alpha x \cdot (\alpha y)^{-1} \cdot \alpha z,$$

for every $x, y, z \in Q$.

Note that this concept is equivalent to the concept of quasiahomomorphism of groups [16]. The set of all holomorphisms of (Q, \cdot) is denoted by $Hol(Q, \cdot)$ and it is a group under the superposition of mappings: $(\alpha \cdot \beta)x = \beta(\alpha x)$, for every $x \in Q$.

The following properties of holomorphisms were proved for Muofang loops in [17].

Lemma 2.3. Let for bijections $\alpha_1, \alpha_2, \alpha_3$ on the group (Q, \cdot) , the following identity is satisfied:

$$\alpha_1(x \cdot y) = \alpha_2(x) \cdot \alpha_3(y).$$

Then $\alpha_1, \alpha_2, \alpha_3 \in Hol(Q, \cdot)$.

Lemma 2.4. Every holomorphism α of the group (Q, \cdot) has the following form:

$$\alpha x = \varphi x \cdot k$$

where, $\varphi \in Aut(Q, \cdot)$ and $k \in Q$.

Lemma 2.5. Let for bijections $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6$ on the group (Q, \cdot) the following identity be satisfied:

$$\alpha_1(\alpha_2(x \cdot y) \cdot z) = \alpha_3 x \cdot \alpha_4(\alpha_5 y \cdot \alpha_6 z).$$

Then $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6 \in Hol(Q, \cdot)$.

Lemma 2.6. *Let $\alpha_0 \in \text{Hol}(Q, \cdot)$ and $k \in Q$, then the mapping*

$$\alpha x = \alpha_0 x \cdot k$$

$x \in Q$, is also a holomorphism of the group (Q, \cdot) .

Theorem 2.7. *Let the set Q forms a quasigroup under the binary operations f and g . If the pair (f, g) of binary operations satisfies one of the (23)-(38), then there exists a binary operation '+' under which Q forms an abelian group and for arbitrary elements $x, y \in Q$ we have:*

$$\begin{aligned} f(x, y) &= \varphi_1(x) + \psi_1(y) + c_1, \\ g(x, y) &= \varphi_2(x) + \psi_2(y) + c_2, \end{aligned}$$

where c_1, c_2 are fixed elements of Q , and $\varphi_i, \psi_i \in \text{Aut}(Q, +)$ for $i = 1, 2$. The group $(Q, +)$ is unique up to isomorphisms.

Proof. We'll start with the proof of one case. Other cases can be proved with minor changes.

Let the set Q forms a quasigroup under the binary operations f and g and the pair of non-associative operations (quasigroup operations) (f, g) satisfies the equation (23). Then there exists an operation, '+', under which Q forms an abelian group on which all the following 6 quasigroups (A_1, \dots, A_6) are isotopic. And there exists 8 one-to-one mappings, $\alpha, \beta, \gamma, \delta, \epsilon, \psi, \varphi, \chi$ of Q onto itself such that:

$$\begin{aligned} A_1(x, y) &= \delta x + \varphi y, & A_2(x, y) &= \delta^{-1}(\alpha x + \beta y), \\ A_3(x, y) &= \varphi^{-1}(\chi x + \gamma y), & A_4(x, y) &= \psi x + \epsilon y, \\ A_5(x, y) &= \psi^{-1}(\alpha x + \chi y), & A_6(x, y) &= \epsilon^{-1}(\beta x + \gamma y), \end{aligned}$$

where, $f = A_1 = A_5 = A_6$ and $g = A_2 = A_3 = A_4$. Since $A_1 = A_5$ and $A_1 = A_5$, we have: $\psi, \epsilon \in \text{Hol}(Q, +)$.

Therefor, by using the previous lemma: $f(x, y) = \varphi_1(x) + \psi_1(y) + c_1$.

By the same manner the linearity of operation g will be obtain. □

Corollary 2.8. *Let (Q, F) be a binary algebra with quasigroup operations which satisfies one of the (23)-(38), then there exists an abelian group $(Q, +)$ such that every operation $f_i \in F$ is represented by the following rule:*

$$f_i(x, y) = \varphi_i(x) + c_i + \psi_i(y),$$

where $c_i \in Q$ and $\varphi_i, \psi_i \in \text{Aut}(Q, +)$. The group $(Q, +)$ is unique up to isomorphisms.

Proof. We'll proof one of th cases and the other cases can be proved with minor changes.

Let (Q, F) be a binary algebra with quasigroup operations which satisfies the equation (23). If $f_0 \in F$ is a fixed operation, then by the theorem 1.1, f is principally isotopic to the abelian group operation '+' on Q . Now, if $f_i \in F$ be any operation, then the pair of operations (f_0, f_i) is medial. Hence f_0 and f_i are pricipally isotopic to the another abelian group operation '*' on

Q . Thus, by transitivity of isotopy, any operation f_i is principally isotopic to the same abelian group operation '+'.
Hence, according to the proof of previous theorem, we have:

$$f_i(x, y) = \varphi_i(x) + \psi_i(y) + c_i,$$

where $c_i \in Q$ and $\varphi_i, \psi_i \in \text{Aut}(Q, +)$.

□

3. Conclusion

Algebras with non-associative operations (specially, algebras with quasigroup operations) which satisfy in balanced and non-balanced functional equations are important algebraic (combinatorial, geometric, logic) structures which arise in various areas of mathematics and other disciplines. For example, they have applications in combinatorics (as latin squares), in geometry (as nets/webs), in statistics, in special theory of relativity, in coding theory and cryptography, in logic (as second order formulas, hyperidentities and hypervarieties).

We consider 16 balanced quadratic identities (7)-(22) and we generalize them to 16 balanced quadratic functional equations (23)-(38) with two functional variables and four objective variables. If the set Q forms a quasigroup under the binary operations f and g and the pair (f, g) of binary operations satisfies one of the (23)-(38), then there exists a binary operation '+' under which Q forms an abelian group and for arbitrary elements $x, y \in Q$ we have:

$$\begin{aligned} f(x, y) &= \varphi_1(x) + \psi_1(y) + c_1, \\ g(x, y) &= \varphi_2(x) + \psi_2(y) + c_2, \end{aligned}$$

where c_1, c_2 are fixed elements of Q , and $\varphi_i, \psi_i \in \text{Aut}(Q, +)$ for $i = 1, 2$. The group $(Q, +)$ is unique up to isomorphisms.

As a consequence of this result, by putting $f = g$, a straightforward proof of theorems 1.1, 1.2 and 1.3 could be introduced.

Another corollary is the generalization of above result to an algebra (Q, F) with non-associative operations (quasigroup operations). Let (Q, F) be a binary algebra with quasigroup operations which satisfies one of the (23)-(38), then there exists an abelian group $(Q, +)$ such that every operation $f_i \in F$ is represented by the following rule:

$$f_i(x, y) = \varphi_i(x) + c_i + \psi_i(y),$$

where $c_i \in Q$ and $\varphi_i, \psi_i \in \text{Aut}(Q, +)$. The group $(Q, +)$ is unique up to isomorphisms.

There exist various balanced and non-balanced quadratic functional equations with two functional variables and four objective variables (approximately, 150 equations). The presence or absence of a linear representation for a pair of quasigroup operations (and as a generalization, for an algebra with quasigroup operations), which satisfy in these 150 quadratic functional equations, on an abelian group (or on a group) remains unproven.

References

- [1] Dénes J and Keedwell A D 1974 Latin squares and their applications, Acadmiai Kiadó, Budapest.
- [2] Belousov V D 1979 Configurations in algebraic nets (Russian), Shtiinca, Kishinev.
- [3] Fisher R A 1966 The design of experiments (8th edition), Oliver & Boyd, Edinburgh.
- [4] Ungar A 2001 Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession - The Theory of Gyrogroups and Gyrovector Spaces, Kluwer Academic Publishers, Dordrecht, Boston, London.
- [5] Shcherbacov V 2003 On some known possible applications of quasigroups in cryptology, manuscript. <http://www.karlin.mff.cuni.cz/drapal/krypto.pdf>.
- [6] Krapež A 2007 Quadratic level quasigroup equations with four variables I Publ. Inst. Math. (Beograd)(N.S.) **81(95)** 53-67.
- [7] Krapež A 2013 Quadratic level quasigroup equations with four variables II Publ. Inst. Math. (Beograd)(N.S.) **93(107)** 29-47.
- [8] Toyoda K 1941 On Axioms of linear functions Proc. 1941 Imp. Acad. Tokyo Conf. **17** 211-237.
- [9] Némec P and Kepka T 1971 T-quasigroups I Acta Univ. Carolin. Math. Phys. **12** 1 39-49.
- [10] Förg-Rob W and Krapež A 2005 Equations which preserve the height of variables Aequat. Math. **70** 63-76.
- [11] Ehsani A 2014 Characterization of regular medial algebras ScienceAsia **40** 175-181.
- [12] Ehsani A and Movsisyan Yu M 2014 A representation of paramedial n-ary groupoids Asian-European J. Math. **7** 1 (17 pages).
- [13] Ehsani A 2011 The generalized entropic property for a pair of operations Izv. Nats. Akad. Nauk Armenii Math. **46** 1 29-34 (Russian). Translation in 2011 J. Contemp. Math. Anal. **46** 1 56-60.
- [14] Nazari E and Movsisyan Yu M 2011 Transitive modes Demonstratio Math. **44** 3 511-522.
- [15] Ehsani A and Movsisyan Yu M 2013 Linear representation of medial-like algebras Communications in Algebra **41** 9 3429-3444.
- [16] Belousov V D 1967 Foundations of the theory of quasigroups and loops Nauka. Moscow.
- [17] Movsisyan Yu M 1986 Introduction to the theory of algebras with hyperidentities Yerevan State University Press Yerevan (Russian).