Hyperidentities with permutations leading to the isotopy of invertible binary algebras to a group

Sergey S. Davidov and Davit A. Shahnazaryan

Abstract. Using the second-order formulas we obtained characterizations of binary invertible algebras principally isotopic to a group or to an abelian group.

1. Introduction

A binary algebra $(Q; \Sigma)$ is called an *invertible algebra* or *system of quasigroups* if each operation in Σ is a quasigroup operation. Invertible algebras with second order formulas first were considered by Shaufler [12, 13] in connection with coding theory. He pointed out that the resulting message would be more difficult to decode by unauthorized receiver than in the case when a single operation is used for calculation. Later such algebras were investigated by Aczel [1], Belousov [3, 4], Sade [11], Movsisyan [8, 9, 10] and others.

It is well known [5] that with each quasigroup A the next five quasigroups are connected:

$$A^{-1}$$
, ^{-1}A , $^{-1}(A^{-1})$, $(^{-1}A)^{-1}$, A^* ,

where $A^*(x,y) = A(y,x)$. These quasigroups are called *inverse quasigroups* or *parastrophes*. Like this, with each invertible algebra $(Q; \Sigma)$ the next five invertible algebras are connected:

 $(Q; \Sigma^{-1}), (Q; {}^{-1}\Sigma), (Q; {}^{-1}(\Sigma^{-1})), (Q; ({}^{-1}\Sigma)^{-1}), (Q; \Sigma^*),$

where

$$\Sigma^{-1} = \{A^{-1} | A \in \Sigma\},\$$

$$^{-1}\Sigma = \{^{-1}A | A \in \Sigma\},\$$

$$^{-1}(\Sigma^{-1}) = \{^{-1}(A^{-1}) | A \in \Sigma\},\$$

$$(^{-1}\Sigma)^{-1} = \{(^{-1}A)^{-1} | A \in \Sigma\},\$$

$$\Sigma^{*} = \{A^{*} | A \in \Sigma\}.$$

Each of these invertible algebras is called a *parastrophe of the algebra* $(Q; \Sigma)$.

Let us recall that the following absolutely closed second-order formula:

$$\forall X_1, \dots, X_m \forall x_1, \dots, x_n \quad (\omega_1 = \omega_2),$$

$$\forall X_1, \dots, X_k \exists X_{k+1} \dots, X_m \forall x_1, \dots, x_n \quad (\omega_1 = \omega_2)$$

where ω_1, ω_2 are words written in the functional variables, X_1, \ldots, X_m , and in the objective variables, x_1, \ldots, x_n , are called $\forall (\forall)$ -*identity* or hyperidentity and $\forall \exists (\forall)$ -*identity*. For see [8].

The groupoid Q(A) is *isotopic* to the groupoid Q(B) if exist three permutations α, β, γ of Q such that $\gamma B(x, y) = A(\alpha x, \beta y)$ for all $x, y \in Q$. The isotopy of the form $T = (\alpha, \beta, \varepsilon)$, where ε is the identity map, is called a *principal isotopy*.

2010 Mathematics Subject Classification: 20N05, 03C85, 20N99.

 ${\small {\sf Keywords: \ invertible \ algebra, \ second-order \ formula, \ hyperidentity, \ isotopy.}}$

The class of quasigroups isotopic to groups first were considered by Belousov [4]. Varieties of quasigroups isotopic to groups have been considered by Glukhov, Gvaramia, Sokhatsky and others. In [6] the concept of identities with permutations was introduced and isotopies of quasigroups to groups was characterized by these identities.

We introduce the notion of the hyperidentity with permutations and using these hyperidentities we obtain characterizations of binary invertible algebras principally isotopic to a group.

2. Auxiliary concepts and results

We start with some concepts and results, which are necessary for further considerations.

Definition 2.1. The triplet $T = (\alpha, \beta, \gamma)$ of permutations of the set Q is called an *autotopy* of the groupoid $Q(\cdot)$, if the identity $\gamma(x \cdot y) = \alpha x \cdot \beta y$ is true for for all $x, y \in Q$. If $T = (\alpha, \beta, \gamma)$ is an autotopy of the groupoid Q(A), then we write $A^T = A$.

In the case $\alpha = \beta = \gamma$ the triplet $T = (\alpha, \alpha, \alpha)$ is an automorphism. It is easy to see that the set of autotopies of $Q(\cdot)$ forms a group.

Definition 2.2. The third component γ of the autotopy $T = (\alpha, \beta, \gamma)$ of the groupoid $Q(\cdot)$ is called a *quasi-automorphism* of $Q(\cdot)$.

Lemma 2.3. (cf. [3]) Any quasi-automorphism γ of a group $Q(\cdot)$ has the form:

$$\gamma = \widetilde{R}_s \gamma_0, \quad (\gamma = \widetilde{L}_s \delta_0) \tag{1}$$

where $\gamma_0(\delta_0)$ is an automorphism of the group $Q(\cdot)$, $\tilde{R}_s x = x \cdot s$ ($\tilde{L}_s x = s \cdot x$), $s \in Q$ and, conversely, the map γ defined by the equality (1) is a quasi-automorphism of the group $Q(\cdot)$.

Lemma 2.4. (cf. [3]) Let γ be a quasi-automorphism of the group $Q(\cdot)$. Then γ is an automorphism if and only if $\gamma 1 = 1$, where 1 is the identity element of the group $Q(\cdot)$.

Lemma 2.5. (cf. [3]) Let $\alpha, \beta, \gamma, \delta, \sigma, \tau$ be permutations of the set Q, such that the equality $\beta(\alpha(x \cdot y) \cdot z) = \gamma x \cdot \delta(\sigma y \cdot \tau z)$

is valid in the group
$$Q(\cdot)$$
 for all $x, y, z \in Q$. Then the permutations $\alpha, \beta, \gamma, \delta, \sigma, \tau$ are quasi-
automorphisms of the group $Q(\cdot)$.

Lemma 2.6. (cf. [3]) A permutation α of Q is a quasi-automorphism of the group $Q(\cdot)$ if and only if for all $x, y \in Q$ the equality

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

where 1 is the identity of $Q(\cdot)$, is valid.

Theorem 2.7. (cf. [3]) If a non-empty set Q is a quasigroup under each of four operations A_1, A_2, A_3, A_4 satisfying the identity:

$$A_1(A_2(x,y),z) = A_3(x, A_4(y,z)),$$
(2)

then there exists the operation (\cdot) such $Q(\cdot)$ is a group isotopic to all these four quasigroups.

Theorem 2.8. (cf. [2]) if a non-empty set Q is a quasigroup under each of six operations $A_1, A_2, A_3, A_4, A_5, A_6$ satisfying the identity:

$$A_1(A_2(x,y), A_3(z,u)) = A_4(A_5(x,z), A_6(y,u)),$$
(3)

then there exists the operation (·) such that $Q(\cdot)$ is an abelian group isotopic to all these six quasigroups, i.e.,

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

where $\alpha, \beta, \gamma, \delta, \chi, \varphi, \psi, \theta$ are permutations of Q.

Definition 2.9. We say that a binary algebra $(Q; \Sigma)$ is *isotopic* to the groupoid $Q(\cdot)$, if each operation in Σ is isotopic to the groupoid $Q(\cdot)$, i.e., for every operation $A \in \Sigma$ there exists permutations $\alpha_A, \beta_A, \gamma_A$ of Q such that:

$$\gamma_A A(x, y) = \alpha_A x \cdot \beta_A y,$$

for every $x, y \in Q$.

Theorem 2.10. (cf. [7]) The invertible algebra $(Q; \Sigma)$ is principally isotopic to a group if and only if for all $A, B \in \Sigma$ the following second-order formula

$$A(^{-1}A(B(x, B^{-1}(y, z)), u), v) = B(x, B^{-1}(y, A(^{-1}A(z, u), v))),$$

is valid in the algebra $(Q; \Sigma \cup \Sigma^{-1} \cup {}^{-1} \Sigma)$.

3. Main results

We denote by $L_{A,a}$ and $R_{A,a}$ the left and right translations of the binary algebra $(Q; \Sigma)$:

 $L_{A,a}: x \mapsto A(a,x) \quad (R_{A,a}: x \mapsto A(x,a)).$

If $(Q; \Sigma)$ is an invertible algebra, then these translations are bijections for all $a \in Q$.

We will consider second order formulas (called hyperidentities with permutations or hyperidentities in $(Q; \Sigma)$) of the following form:

$$\beta_1^{A,B}A(\beta_2^{A,B}B(\beta_3^{A,B}x,\beta_4^{A,B}y),\beta_5^{A,B}z) = B(\beta_6^{A,B}x,\beta_7^{A,B}A(\beta_8^{A,B}y,\beta_9^{A,B}z)),$$

where x, y, z are objective variables, $\beta_i^{A,B} (i = 1, ..., 9)$ are permutations on Q dependent on $A, B \in \Sigma$. By doing paremeter replacement those formulas may be transformed into second order formulas with less number of parameters:

$$\alpha_1^{A,B} A(\alpha_2^{A,B} B(x,y),z) = B(\alpha_3^{A,B} x, \alpha_4^{A,B} A(\alpha_5^{A,B} y, \alpha_6^{A,B} z)).$$
(4)

Theorem 3.11. If the second order formula (4) is valid in the algebra $(Q; \Sigma)$ for all $A, B \in \Sigma$ and for some permutations $\alpha_i^{A,B}$ (i = 1, ..., 6), then the algebra $(Q; \Sigma)$ is principally isotopic to a group.

Conversely, if the invertible algebra $(Q; \Sigma)$ is principally isotopic to a group $Q(\cdot)$, then for all $A, B \in \Sigma$ there exist permutations $\alpha_i^{A,B}$ (i = 1, ..., 6) such that the second order formula (4) is valid in the algebra $(Q; \Sigma)$.

Proof. Let (4) hold in $(Q; \Sigma)$ for all $A, B \in \Sigma$ and for some permutations $\alpha_i^{A,B} (i = 1, ..., 6)$. The second order formula (4) is a particular case of (2), where

$$A_1(x,y) = \alpha_1^{A,B} A(x,y), \quad A_2(x,y) = \alpha_2^{A,B} B(x,y),$$

$$A_{3}(x,y) = B(\alpha_{3}^{A,B}x,y), \quad A_{4}(x,y) = \alpha_{4}^{A,B}A(\alpha_{5}^{A,B}x,\alpha_{6}^{A,B}y).$$

According to Theorem 2.7, the quasigroups A_1 , A_2 , A_3 , A_4 are isotopic to the same group $Q(\cdot)$:

$$A_1(x,y) = \alpha^{-1}(\beta x \cdot \gamma y), \quad A_2(x,y) = \alpha_1^{-1}(\beta_1 x \cdot \gamma_1 y),$$

$$A_3(x,y) = \lambda^{-1}(\mu x \cdot \nu y), \quad A_4(x,y) = \lambda_1^{-1}(\mu_1 x \cdot \nu_1 y).$$

Having in consideration the last equalities and (2) we get:

$$\alpha^{-1}(\beta\alpha_1^{-1}(\beta_1x\cdot\gamma_1y)\cdot\gamma z) = \lambda^{-1}(\mu x\cdot\nu\lambda_1^{-1}(\mu_1y\cdot\nu_1z))$$

or

$$\lambda \alpha^{-1} (\beta \alpha_1^{-1} (x \cdot y) \cdot z) = \mu \beta_1^{-1} x \cdot \nu \lambda_1^{-1} (\mu_1 \gamma_1^{-1} y \cdot \nu_1 \gamma^{-1} z).$$

According to Lemma 2.5, $\lambda \alpha^{-1} = \theta$ is a quasi-automorphism of the group $Q(\cdot)$. Fixing the operation A, we fix the permutation α , too. Then, every operation $B \in \Sigma$ has the form:

$$B(x,y) = A_3((\alpha_3^{A,B})^{-1}x,y) = A_3(\phi x,y) = \lambda^{-1}(\mu \phi x \cdot \nu y)$$

or

 $B(x,y) = \alpha^{-1} \theta^{-1} (\phi' x \cdot \nu y).$

Since the permutation θ^{-1} is a quasi-automorphism of the group $Q(\cdot),$ then

$$B(x,y) = \alpha^{-1} (\theta^{-1} \phi' x \cdot (\theta^{-1} 1)^{-1} \cdot \theta^{-1} \nu y) = \alpha^{-1} (\phi'' x \cdot \psi y)$$

where $\phi'' x = \theta^{-1} \phi' x (\theta^{-1} 1)^{-1}$, $\psi x = \theta^{-1} \nu x$ and 1 is the identity element of the group $Q(\cdot)$. Consider the operation:

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

 $Q(\circ)$ is isomorphic to the group $Q(\cdot).$ Thus, $(Q(\circ)$ is a group and

$$B(x,y) = \alpha^{-1} \phi'' x \circ \alpha^{-1} \psi y$$

or

$$B(x,y) = fx \circ gy.$$

Hence, Q(B) is principally isotopic to the group $Q(\circ)$ and since B is an arbitrary operation from Σ , this proves the statement.

Conversely, if an invertible algebra is principally isotopic to a group, then according to Theorem 2.10 the following formula is valid:

$$A(^{-1}A(B(x, B^{-1}(y, z)), u), v) = B(x, B^{-1}(y, A(^{-1}A(z, u), v))).$$

Taking into account that

$$A^{-1}(x, u) = R_{A^{-1}, u}x = L_{A^{-1}, x}u$$
 and $^{-1}A(v, x) = L_{-1A, v}x = R_{-1A, x}v$

the above formula may be re-written in the form:

$$A[R_{-1}{}_{A,u}B(x,z),v] = B[x, L_{B^{-1},y}A(R_{-1}{}_{A,u}L_{B^{-1},y}^{-1}z,v)]$$

This for u = a, y = b, where $a, b \in Q$ are fixed, gives (4), where

$$\alpha_1^{A,B} = \alpha_3^{A,B} = \alpha_6^{A,B} = \epsilon, \quad \alpha_2^{A,B} = R_{^{-1}A,a}, \quad \alpha_4^{A,B} = L_{B^{-1},b}, \quad \alpha_5^{A,B} = R_{^{-1}A,a}L_{B^{-1},b}^{-1},$$
 and completes the proof. \Box

Corollary 3.12. (cf. [6]) The class of quasigroups isotopic to a group is characterized by the identity:

$$x(b \setminus ((z/a)v)) = ((x(b \setminus z))/a)v,$$

where a and b are fixed.

Theorem 3.13. The invertible algebra $(Q; \Sigma)$ is principally isotopic to an abelian group if and only if for all $A, B \in \Sigma$ the second-order formula

$$A(^{-1}A(B(x,z),y), A^{-1}(y,B(w,u))) = A(^{-1}A(B(w,z),y), A^{-1}(y,B(x,u))).$$
(5)

Proof. Let $(Q; \Sigma)$ be an invertible algebra principally isotopic to an abelian group $Q(\cdot)$, i.e., every operation $A \in \Sigma$ has the form:

$$A(x,y) = \alpha_A x \cdot \beta_A y, \tag{6}$$

where α_A , β_A are permutations of the set Q. Then from (6) we obtain:

$$A^{-1}(x,y) = \beta_A^{-1}(\overline{\alpha_A x} \cdot y) \quad \text{and} \quad {}^{-1}A(x,y) = \alpha_A^{-1}(x \cdot \overline{\beta_A y}), \tag{7}$$

where \overline{x} is the inverse element of x in the group $Q(\cdot)$.

Using the identities (6) and (7) we can prove that left and right sides of (5) are the same.

Conversely, let (5) be satisfied in $(Q; \Sigma \cup \Sigma^{-1} \cup {}^{-1} \Sigma)$ for all $A, B \in \Sigma$. For y = a it has the form:

$$A(C(x, z), D(w, u)) = A(C(w, z), D(x, u)),$$
(8)

where $C(x, y) = {}^{-1}A(B(x, y), a)$ and $D(x, y) = A^{-1}(a, B(x, y))$.

Let's write (8) in the form:

$$A(C^*(z,x), D(w,u)) = A(C^*(z,w), D(x,u)).$$
(9)

Obviously, the operations C, C^* and D are inverse operations. According to Theorem 2.8, the quasigroups Q(A), $Q(C^*)$ and Q(D) are isotopic to the same abelian group $Q(\cdot)$. Hence,

$$A(x,y) = \alpha x \cdot \beta y, \quad C^*(x,y) = \alpha^{-1}(\gamma x \cdot \delta y), \quad D(x,y) = \beta^{-1}(\theta x \cdot \psi y),$$

for some permutations $\alpha, \beta, \gamma, \delta, \theta, \psi$ of Q.

Fixing the operation A, we also fix the permutation α . Then:

$$C^*(y,x) = C(x,y) = {}^{-1}A(B(x,y),a) = R_{-1}{}_{A,a}B(x,y) = \alpha^{-1}(\gamma y \cdot \delta x),$$

or

$$B(x,y)=R_{-1A,a}^{-1}\alpha^{-1}(\gamma y\cdot\delta x), \quad B(x,y)=R_{-1A,a}^{-1}\alpha^{-1}I(I\delta x\cdot I\gamma y),$$

where $I(x) = \overline{x}$ assigns to x its inverse \overline{x} calculated in the group $Q(\cdot)$. Then the permutation $\phi = I\alpha R_{-1}{}_{A,a}$ depends only on A. Thus, $Q(\circ)$, where $x \circ y = \varphi^{-1}(\varphi x \cdot \varphi y)$, is an abelian group is isomorphic to the group $Q(\cdot)$. In the group $Q(\circ)$ the operation B has the form:

$$B(x,y) = fx \circ gy,$$

where $f = \varphi^{-1}I\delta$, $g = \varphi^{-1}I\gamma$ are permutations of Q. Thus, Q(B) is principally isotopic to the group $Q(\circ)$ and since B is an arbitrary operation from Σ , this proves the theorem.

Theorem 3.14. If the second order formula

$$\alpha_1^{A,B} A[\alpha_2^{A,B} B(\alpha_3^{A,B} x, \alpha_4^{A,B} z), \alpha_5^{A,B} B(\alpha_6^{A,B} w, \alpha_7^{A,B} v)] = A[\alpha_8^{A,B} B(w, z), \alpha_9^{A,B} B(x, v)]$$
(10)

is valid in the invertible algebra $(Q; \Sigma)$ for all $A, B \in \Sigma$ and for some permutations $\alpha_i^{A,B}$ where $i = 1, 2, \ldots, 9$, then the algebra $(Q; \Sigma)$ is principally isotopic to an abelian group.

Conversely, if the invertible algebra $(Q; \Sigma)$ is principally isotopic to an abelian group $Q(\cdot)$, then for all $A, B \in \Sigma$ there are permutations $\alpha_i^{A,B}$, $i = 1, 2, \ldots, 9$, such that the second order formula (10) is valid in the algebra $(Q; \Sigma)$.

Proof. Let (10) holds in $(Q; \Sigma)$ for all $A, B \in \Sigma$ and for some permutations $\alpha_i^{A,B}$, i = 1, 2, ..., 9. Then (10) is a particular case of (3), where

$$A_1(x,y) = \alpha_1^{A,B} A(x,y), \quad A_2(x,y) = \alpha_2^{A,B} B(\alpha_3^{A,B} x, \alpha_4^{A,B} y), \quad A_3(x,y) = \alpha_5^{A,B} B(\alpha_6^{A,B} x, \alpha_7^{A,B} y),$$

$$A_4(x,y) = A(x,y), \quad A_5(x,y) = \alpha_8^{A,B} B(x,y), \quad A_6(x,y) = \alpha_9^{A,B} B(x,y).$$

According to Theorem 2.8, the quasigroups A_1 , A_2 , A_3 , A_4 , A_5 , A_6 are isotopic to the same abelian group $Q(\cdot)$:

$$A_1(x,y) = \alpha x \cdot \phi y, \quad A_2(x,y) = \alpha^{-1}(\gamma x \cdot \delta y), \quad A_3(x,y) = \phi^{-1}(\lambda x \cdot \beta y),$$

$$A_4(x,y) = \psi x \cdot \sigma y, \quad A_5(x,y) = \psi^{-1}(\gamma x \cdot \lambda y), \quad A_6(x,y) = \sigma^{-1}(\delta x \cdot \beta y).$$

Fixing B, we obtain $A_5(x,y) = \alpha_8^{A,B} B(x,y) = \psi^{-1}(\gamma x \cdot \lambda y)$. Thus ψ is fixed too. Then $Q(\circ)$, where

$$x \cdot y = \psi^{-1} x \circ \psi^{-1} y.$$

is an abelian group and $A(x,y) = A_4(x,y) = \psi x \cdot \sigma y = x \circ \psi^{-1} \sigma y$. Thus, Q(A) is principally isotopic to the group $Q(\circ)$ and as $A \in \Sigma$ is an arbitrary operation, this proves the statement.

Conversely, if the invertible algebra $(Q; \Sigma)$ is principally isotopic to an abelian group, then according to Theorem 3.13 the formula is valid:

 $A(^{-1}A(B(x,z),y), A^{-1}(y, B(w,u))) = A(^{-1}A(B(w,z),y), A^{-1}(y, B(x,u))).$

Then,

 $A[R_{^{-1}A,y}B(x,z),L_{A^{-1},y}B(w,u)] = A[R_{^{-1}A,y}B(w,z),L_{A^{-1},y}B(x,u)].$ This for fixed $y = a \in Q$ gives (10) with

$$\alpha_1 = \alpha_3 = \alpha_4 = \alpha_6 = \alpha_7 = \epsilon, \quad \alpha_8 = \alpha_2 = R_{-1}{}_{A,a}, \quad \alpha_5 = \alpha_9 = L_{A^{-1}{}_{,a}}.$$

Corollary 3.15. The class of quasigroups isotopic to an abelian group is characterized by the identitu:

where y is fixed.

$$(xz/y)(y\backslash wu) = (wz/y)(y\backslash xu),$$

References

- [1] J. Aczel, Yorlensungen uiber Funktionalgleichungen und ihre Anwendungem, Berlin, VEB Deutsch. Verl. Wiss., 1961.
- [2] J. Aczel, V.D. Belousov, f M. Hosszú, Generalized associativity and bisymmetry on quasigroups, Acta Math. Acad. Sci. Hung., 11 (1960), 127-136.
- [3] V.D. Belousov, Globaly associative systems of quasigroups, (Russian), Mat. Sb., **55(97)** (1961), 221 - 236.
- [4] V.D. Belousov, Balanced identities on quasigroups, (Russian), Mat. Sb., 70(112) (1966), 55 - 97.
- [5] V.D. Belousov, Foundations of the Theory of Quasigroups and Loops, (Russian), Nauka, Moscow, 1967.
- [6] G.B. Belyavskaya, A.Kh. Tabarov, Identities with permutations leading to linearity of a quasigroup, Discrete Math. Appl., 19 (2009), 172-190.
- [7] S. Davidov, S. Alvrtsyan, D. Shahnazaryan, Invertible binary algebras principally isotopic to a group, Asian-European J. Math., 13 (2020), 2050118.
- [8] Yu.M. Movsisyan, Introduction to the Theory of Algebras with Hyperidentities, (Russian), Yerevan State Univ., 1986.
- [9] Yu.M. Movsisyan, Hyperidentities and related concepts 1, Armenian J. Math., 9 (2017), no.2, 146 - 222.
- [10] Yu.M. Movsisyan, S.S. Davidov, Algebras that are nearly quasigroups, (Russian), Moscow, 2018.
- [11] A. Sade, Theorie des systemes demosiens de groupoids, Pacif. J. Math., 10 (1960), 625 - 660.
- [12] R. Schauffler, Uber die Bildung von Codewörten, Arch. Elektr. Uebertragung. 10 (1956), 303 - 314.
- [13] R. Schauffler, Die Assoziativität im Ganzen Besonders bei Quasigruppen, Math. Zeitschr., 67 (1957), 428 – 435.

Received January, 29, 2020 Faculty of Mechanics and Mathematics, Yerevan State University,1 Alex Manoogian, Yerevan, 0025, Republic of Armenia

E-mails: davidov@ysu.am, shahnazaryan94@gmail.com