MEDIAL SYSTEM S AND FULL ALGEBRA WHIT IDENTITY

Dr.EBRAHIM NAZARI
University faculty member of Farhangian, iran

Dr. hamidreza rostami
Department of Education Gilangharb

سرشناسه	:	نظری، ابراهیم، ۱۳۵۳ - Nazari, ,Ebrahim
عنوان و نام پدیدآور	:	/ Ebrahim Nazari, Hamidreza Medial systems and full algebra whit identity Rostami.
مشخصات نشر	:	کرمانشاه: ابراهیم نظری، ۱۳۹۳= ۲۰۱۴م.
مشخصات ظاهری	:	۷۷ ص.
شابک	:	۱۵۰۰۰۰ریال : 978-964-04-9841-5
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	انگلیسی.
یادداشت	:	کتابنامه .
آوانویسی عنوان	:	مدیال ...
موضوع	:	جبر تعویض‌پذیر
موضوع	:	جبر
موضوع	:	نظریه اعداد جبری
شناسه افزوده	:	رستمی، حمیدرضا، ۱۳۵۳ -
شناسه افزوده	:	Rostam,Hamid Reza
رده بندی کنگره	:	QA۲۵۱/۱۳۹۳۳ ۴م۶ن/
رده بندی دیویی	:	۲۴/۵۱۲
شماره کتابشناسی ملی	:	۳۶۵۰۵۰۱

Contents

Preface

The Urgency of the Problem

The class of algebras which are defined by (hyper)identities is called a (hyper)variety. For example, semigroups, quasigroups, groups, rings, lattices, Boolean algebras are varieties. But the class of fields is not a variety (followed from the classical Birkhoff theorem [1] on varieties). Below we give an example of a hypervariety also.

First, let us define some formulae, which are investigated in this thesis. A hyperidentity is a second order formula:

$$\forall X_1, \ldots, X_m \forall x_1, \ldots, x_n \ (w_1 = w_2), \tag{1}$$

where $X_1, \ldots, X_m$ are the functional variables (symbols of operations) and $x_1, \ldots, x_n$ are the objective variables in the words (terms)of w_1, w_2. Generally hyperidentities are written without a quantifier prefix: $w_1 = w_2$. We say that the hyperidentity, $w_1 = w_2$, holds (is valid) in an algebra, $(Q; \Sigma)$, or an algebra, $(Q; \Sigma)$, satisfies the hyperidentity, $w_1 = w_2$, if this equality is valid when every objective variable, x_i, is replaced by an arbitrary element of Q and every functional variable, X_j, is replaced by any operation of the corresponding arity from Σ [2, 3].

The hyperidentity is also called a $\forall(\forall)$-identity. m is called the functional rank and n is called the objective rank of the given hyperidentity (1).

Let $\mathfrak{A} = (Q; \Sigma)$ and $T_{\mathfrak{A}} = \{|A| \,|A \in \Sigma\}$, where $|A|$ is the arity of the operation, $A \in \Sigma$. An algebra, $\mathfrak{A} = (Q; \Sigma)$, is called medial or abelian, if $\mathfrak{A}$ satisfies the following hyperidentity of mediality:

$$X(Y(x_{11}, \ldots, x_{1m}), \ldots, Y(x_{n1}, \ldots, x_{nm})) = Y(X(x_{11}, \ldots, x_{n1}), \ldots, X(x_{1m}, \ldots, x_{nm}))$$

for every $m, n \in T_{\mathfrak{A}}$. So, the class of medial algebras is a hypervariety.

Examples. Let $Q(\cdot)$ be a medial semigroup, i.e. a semigroup with the identity: $xy \cdot uv = xu \cdot yv$. The following function:

$$f(x, y) = z_1^{k_1} \cdot z_2^{k_2} \cdots z_n^{k_n}, \quad n \in \mathbb{N}, \ \ k_n \in \mathbb{N},$$

where $z_i \neq z_{i+1}$ and $z_i \in \{x, y\}$, is called a binary polynomial of the semigroup, $Q(\cdot)$. If Σ_Q is a set of the binary polynomials of the medial semigroup, $Q(\cdot)$, then in the binary algebra, $(Q; \Sigma_Q)$, the hyperidentity of mediality:

$$X(Y(x,y),Y(u,v)) = Y(X(x,u),X(y,v)) \tag{2}$$

is valid, i.e. the algebra, $(Q; \Sigma_Q)$, is medial. Analogical result is valid for ternary and, in general, for n-ary polynomials of semigroups.

If $Q(A)$ is a medial quasigroup, i.e. a quasigroup with the identity:

$$A(A(x,y),A(u,v)) = A(A(x,u),A(y,v)),$$

A^{-1} and ${}^{-1}A$ are right and left inverse operations of A, then in the algebra, $(Q; A, A^{-1}, {}^{-1}A)$, the hyperidentity (2) is valid, i.e. the algebra, $(Q; A, A^{-1}, {}^{-1}A)$, is medial.

If $Q(A)$ is a distributive quasigroup, i.e. a quasigroup with the identity:

$$A(x,A(u,v)) = A(A(x,u),A(x,v)),$$

$$A(A(x,y),u) = A(A(x,u),A(y,u)),$$

A^{-1} and ${}^{-1}A$ are right and left inverse operations of A, then in the algebra, $(Q; A, A^{-1}, {}^{-1}A)$, the following hyperidentities of distributivity is valid:

$$X(x,Y(y,z)) = Y(X(x,y),X(x,z)),$$

$$X(Y(x,y),z) = Y(X(x,z),X(y,z)).$$

The following second order formula is called a $\forall\exists(\forall)$-identity:

$$\forall X_1,\ldots,X_k \exists X_{k+1},\ldots,X_m \forall x_1,\ldots,x_n\ (w_1 = w_2), \tag{3}$$

where w_1 and w_2 are the words (terms) in the functional, $X_1,\ldots,X_m$, and in the objective variables, $x_1,\ldots,x_n$.

k is called functional rank of the given $\forall\exists(\forall)$-identity (3).

The satisfiability of these second-order formulae in the algebra, $(Q;\Sigma)$, is understood by the quantifiers, $(\forall X_i)$, and $(\exists X_j)$ means: "for every value, $X_i = A \in \Sigma$, of the corresponding arity" and "there exists a value $X_j = A \in \Sigma$ of the corresponding arity". This semantics is compatible with bihomomorphism of the algebras [2], that are defined as the pairs, $\left(\varphi, \tilde{\psi}\right)$, of maps with the condition:

$$\varphi\, A(x_1, \ldots, x_n) = \left[\tilde{\psi}(A)\right](\varphi x_1, \ldots, \varphi x_n)\ .$$

An algebra with an $\forall\exists(\forall)$-identity of mediality is called a medial system. So every medial algebra is a medial system.

In paper [4] the Hamiltonian varieties are characterized by $\forall\exists(\forall)$-identities. The variety, V, is called Hamiltonian, if from the condition, $\mathfrak{A} \leqslant \mathcal{L} \in V$, follows that the basic set of $\mathfrak{A}$ is a class of equivalence for some congruence of $\mathcal{L}$. In paper [5] the discriminator varieties are characterized by $\forall\exists(\forall)$-identities.

In paper [6] the $\forall\exists(\forall)$-identities of associativity of rank 2 and one $\forall\exists(\forall)$-identities of mediality of rank 3 are studied.

In the first part of this thesis the $\forall\exists(\forall)$-identities of mediality of rank $\leqslant 2$ are studied.

In the second part of this thesis the left (right) invertible algebras with hyperidentity of mediality (2) are studied.

During the second World War R. Schauffler worked for the German Cryptography service and developed a method of error detection based on using of identities with functional variables, in which the check digits are calculated through an associative system with quasigroup operations [7–9]. Particularly, he proved the following result [9].

Schauffler theorem. *Let Q be a non-empty set. For any pair of (binary) quasigroups, $Q(A)$ and $Q(B)$, there exists a pair of quasigroups, $Q(C)$ and $Q(D)$, with the identity*

$$A(B(x,y),z) = C(x,D(y,z)) \tag{4}$$

iff the cardinality $|Q| \leqslant 3$.

In other words, if Ω_Q is a set of all (binary) quasigroups on the set, Q, then in the

algebra, $(Q;\Omega_Q)$, the following $\forall\exists(\forall)$-identity of associativity is satisfied:

$$\forall X, Y \exists Z, U \forall x, y, z (X(Y(x,y),z) = Z(x,U(y,z))) \tag{5}$$

iff the cardinality $|Q| \leqslant 3$.

In paper [6] another proof of Schauffler's theorem is suggested, while in papers [10–13] this result is extended for ternary and n-ary quasigroups cases, as well as for topological n-ary quasigroups.

In paper [14] the following result is proved.

Let Q be a non-empty set. For every pair of (binary) groupoids, $Q(A)$ and $Q(B)$, there exists a pair of (binary) groupoids, $Q(C)$ and $Q(D)$, with the identity (4) iff the set, Q, is infinite or singleton.

In other words, if G_Q is a set of all (binary) operations on the set, Q, then in the algebra, $(Q;G_Q)$,the second order formula (5) is satisfied iff the set, Q, is infinite or singleton.

A more general result is proved in paper [15].

Let Q be a non-empty set. For every pair of (binary) quasigroups, $Q(A)$ and $Q(B)$, there exists a pair of (binary) groupoids, $Q(C)$ and $Q(D)$, with the identity (4) iff the cardinality $|Q| \leqslant 3$ or the set, Q, is infinite.

Besides, in paper [15] the satisfiability of $\forall\exists(\forall)$-identities of associativity of rank 1 is also considered.

The mentioned problems are still open for the medial identity:

$$A(B(x,y),C(u,v)) = D(E(x,u),F(y,v)),$$

i.e. for the medial systems. One of the main goal of this dissertation thesis is solution of the mentioned problems for medial systems.

The Aim and Objectives of the Dissertation

The main aims of the present investigation are the following:

1) To characterize the invertible algebras with $\forall\exists(\forall)$-identities and $\forall\exists_1(\forall)$-identities of mediality of rank 2;

2) To characterize the full invertible algebras with $\forall\exists(\forall)$-identities of mediality of rank 2;

3) To characterize the sets which satisfies the $\forall\exists(\forall)$-identities and $\forall\exists_2(\forall)$-identities of mediality (with special quantifiers) of rank 1 or 2;

4) To describe the connection between the right (left) invertible medial algebras and right (left) product of binary functions;

5) Application obtaining results for transitive modes (i.e. medial and idempotent algebras).

The Objects of the Investigation

The objects of this investigation are the $\forall\exists(\forall)$-identities and hyperidentities of mediality, the right (left) invertible algebras, the right (left) group of binary functions, the idempotent and medial algebras (modes), the transitive modes.

The Methods of the Investigation

In this thesis we used the results of quasigroup and loops theory, as well as: the concept of the group of holomorphisms; the concept of the group of isotopisms; the concept of the group of the left (right) invertible operations.

The Novelty of the Results

The main results of the thesis are new and concern the above mentioned directions. The following five types of results are proved in the thesis:

1. If invertible algebra $(Q;\Sigma)$ satisfy the $\forall\exists_1(\forall)$-identity of mediality of functional rank 2 then there exists an abelian group $Q(\circ)$ such that any operation $A_i \in \Sigma$ is determined by the rule:

$$A_i(x,y) = \varphi_i x \circ t_i \circ \psi_i y,$$

where $\varphi_i, \psi_i \in \operatorname{Aut} Q(\circ)$ and $t_i \in Q$.

2. In the full invertible algebra, $(Q;\Omega_Q)$, the $\forall\exists(\forall)$-identity of mediality of functional rank 2 is satisfied iff the cardinality $|Q| \leqslant 3$.

3. In the full algebra, $(Q;G_Q)$, the $\forall\exists(\forall)$-identity of mediality of functional rank 2 is

satisfied iff the set, Q, is infinite or singleton.

4. In the full invertible algebra, $(Q;\Omega_Q)$, the $\forall\exists_2(\forall)$-identity of mediality of functional rank 2 is satisfied iff the cardinality $|Q| \leqslant 3$, or Q is infinite.

5. If $(Q;\Sigma)$ is a transitive mode, then there exists a field $Q(+,\cdot)$ such that every operation $A \in \Sigma$ is determined by the rule:

$$A(x,y) = (e-a)x + ay,$$

where e is the identity element of the field and $a \in Q$ (and depends on A).

The Practical Significance of the Results

The results of dissertation can be used in theory of quasigroups and loops, in studies of groups of the left and right invertible binary operations, in characterization of the left (right) invertible medial algebras, in the characterization of the left (right) medial quasigroups, as well as in universal algebras.

The Approbation of the Outcome

The main results of the thesis were presented to the following international scientific conferences:

– Computer Science and Information technologies, 2009 (CSIT 2009);

– Workshop on Non-Classical Algebraic Structures, Bedlowo, Poland, June 2-3, 2010.

– Arbeitstagung Algemeine Algebra (80th Workshop on general Algebra), Bedlowo, Poland, June 4-6, 2010.

Publications

The following papers on the subject were published in: [52]– [55].

The Structure of the Work

The thesis is consisted of a Preface, two Chapters, Conclusion and References.