Algebraic Backgrounds for Data Structures Models

Volodymyr G. Skobelev

October 18, 2019

Skobelev Volodymyr Gennadievich, Dr. Phys.-Math. Sci., Dr. Tech. Sci, Full Professor,

V.M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine,

Taras Shevchenko National University of Kyiv,

e-mail: skobelevvg@gmail.com;

ALGEBRAIC BACKGROUNDS FOR DATA STRUCTURES MODELS

Skobelev V.G.

Abstract. The main aim of the Algebraic Aggregate Theory is to present uniformly data structures in mathematics and its applications in terms of Universal Algebra. In the given paper are characterized three sub-algebras of the Algebraic Aggregate Theory. These sub-algebras are the sub-algebra of ordered pairs, the successor sub-algebra and the algebra of Semi-Boolean Systems. Some applications of the obtained results for solving mathematical problems and software development are illustrated.

Key words: Semi-Boolean systems, data structures.

1. Introduction. Penetration of information technologies into all fields of mankind activity caused the need to deal with a wide class of super complex applied problems. For effective solution of the vast majority of these problems modern computers and/or clusters as well as the development of the relevant data structures are necessary. The essential characteristics for these data structures are that they should be accurately and uniformly characterized in terms of mathematical models and also they must be the necessary tool for the elaboration of the effective software. It is evident that Algebraic Systems are the most general mathematical models for data structures, and, besides, they give the possibility to solve effectively verification problems in the development process of IT-systems.

The development of data structures in Applied Algorithms Theory [1], as well as the development of Table Algebras [2] and their generalizations [3], have revealed deep internal links between data structures and classic Algebraic Systems (commutative and non-commutative, both). These internal links are based on studying the structure of Boolean algebra, Boolean rings and their generalizations (some short surveys of researches in this area are given in [4, 5]). Especially, the papers [6, 7] should be noted, since they have stimulated intensive researches of Semi-Boolean systems and their applications (see [9, 10, 11, 12, 13], for example).

During the last two decades, the theory of non-associative Algebraic Systems has been developing intensively, primarily due to their successful application in solving problems of information transmission and protection (see [14, 15, 16], for example). For this reason, the problem of construction of axioms systems for extensions of Semi-Boolean Systems intended for efficient representation and processing of both associative and non-associative Algebraic Systems is relevant. One of such constructions, formulated on the base of Universal Algebra, has been proposed in [17]. Due to high complexity of this Axioms System, it is natural to carry out its study in terms of sub-algebras defined by some of these axioms. This approach makes it possible not only to examine in detail the properties of the Semi-Boolean System defined by the proposed Axioms System but also, when it is necessary, to clarify and/or to detail the respective axioms. Presentation of the results obtained in this direction is the main aim of the given paper.

2. Previous results. The Algebraic Aggregate Theory [17] assumes that we deal with some non-empty set A, in which some element 0 is distinguished. There are defined on the set A the unary operation "$^\circ$", the binary operator "$(\; , \;)$", and two binary operations "$+$"and "$-$", satisfying the following Axioms System (it is supposed that $a, b, c, a', b' \in A$):

$$a - a = 0, \tag{1}$$

$$a + (b + c) = (a + b) + c, \tag{2}$$

$$a + b = b + a, \tag{3}$$

$$a + a = a, \tag{4}$$

$$(a + b) - c = (a - c) + (b - c), \tag{5}$$

$$a - (b + c) = (a - b) - c, \tag{6}$$

$$a + (b - a) = a + b, \tag{7}$$

$$a + (a - b) = a, \tag{8}$$

$$(a - b) - c = (a - c) - (b - c), \tag{9}$$

$$a - (b - c) = (a - b) + (a - (a - c)), \tag{10}$$

$$a^\circ = b^\circ \Rightarrow a = b, \tag{11}$$

$$(a, b) = (a', b') \Rightarrow a = a' \,\&\, b = b'. \tag{12}$$

Axioms (1)-(12) imply that the element 0 can be interpreted as the empty set, the unary operation "$^\circ$" can be interpreted as a successor operation, the binary operator "$(\; , \;)$" can be interpreted as an ordered pair, the binary operation "$+$" can be interpreted as the union of two sets, and the binary operation "$-$" can be interpreted as the difference of two sets.

Due to this Axioms System, the relation of partial ordering "$\leq$", and binary operations "$\vartriangle$" of the symmetric difference and "$\cdot$" of the intersection have been defined in [17], as follows (it is supposed that $a, b \in A$):

$$a \leq b \Leftrightarrow a - b = 0, \tag{13}$$

$$a \Delta b = (a - b) + (b - a), \tag{14}$$

$$a \cdot b = (a + b) - (a \Delta b). \tag{15}$$

It is pointed in [17] that on the base of (1)-(15) the following identities can be proved (it is supposed that $a, b, c \in A$):

$$a - a = b - b, \tag{16}$$

$$a+0=a, \tag{17}$$

$$a-0=a, \tag{18}$$

$$(a-b)+b=b, \tag{19}$$

$$a-(b-a)=a, \tag{20}$$

$$(a-b)-c=(a-c)-b, \tag{21}$$

$$a=(a-b)+(a-(a-b)), \tag{22}$$

$$a\cdot b=a-(a-b), \tag{23}$$

$$a\cdot b=b-(b-a), \tag{24}$$

$$a-(a-b)=b-(b-a), \tag{25}$$

$$a-(b\cdot c)=(a-b)+(a-c), \tag{26}$$

$$a-(b+c)=(a-b)\cdot(a-c). \tag{27}$$

Unfortunately, the evidence of identities (16)-(27) has not been provided in [17]. The difficulties encountered in finding evidence of these identities have been the main reason for analyzing the subsystems of the Algebraic System presented above.

The following inductive approach for converting the operator "(,)" into an algebraic operation on a suitable set has been proposed in [18].

Let $\mathsf{A}=\bigcup_{n=0}^{\infty}A^{(i)}$, where $A^{(0)}=A$ and

$$A^{(n)}=\bigcup_{i=0}^{n-1}\{(x,y)\,|\,x\in A^{(i)}\ \&\ y\in A^{(n-1-i)}\}\quad(n\in\mathbb{N}). \tag{28}$$

The axiom (12) can be extended from the set A onto the set A as follows:

$$(\forall x_1,x_2,y_1,y_2\in\mathsf{A})((x_1,y_1)=(x_2,y_2)\Leftrightarrow x_1=x_2\ \&\ y_1=y_2). \tag{29}$$

Due to (28) and (29), for any non-empty set A the sequence $A^{(0)},A^{(1)},\ldots,A^{(n)},\ldots$ consists of non-empty pair-wise non-intersecting sets, i.e. A is an infinite set for any non-empty set A. Thus, for any non-empty set A the A-associated infinite magma $\mathsf{M}_A=(\mathsf{A},\circ)$ can be defined, where $x\circ y=(x,y)\ \ (x,y\in\mathsf{A})$. The following properties of this magma have been established:

1. (Theorem 1 in [18]). For any non-empty set A the binary operation in the A-associated magma $\mathsf{M}_A=(\mathsf{A},\circ)$ is a surjection $\circ:\mathsf{A}\times\mathsf{A}\rightarrow\bigcup_{n=1}^{\infty}A^{(n)}$.

2. (Theorem 2 in [18]). For any non-empty set A the A-associated magma $\mathsf{M}_A=(\mathsf{A},\circ)$ is a cancellative magma.

3. (Proposition 4 in [18]). For any non-empty set A the A-associated magma $\mathsf{M}_A=(\mathsf{A},\circ)$ is not a quasigroup.

The interrelation between elements of the set A and rooted finite labeled as well as unlabeled binary trees has been studied in [18]. The main result is that the language presented by all these unlabeled binary trees is some proper non-empty sub-language of the Dyck language

$L_{D(2)}$ over the 2-letters alphabet. Besides, it has been illustrated that the magma $M_A=(A,\circ)$ can be used successively as some conceptual model in mathematics and its applications.

In [19] properties of the successor operation "$\circ$" have been studied. For this purpose, the axiom concerning this operation has been clarified as follows ($a^{n\circ}$ $(a\in A; n\in\mathbb{Z}_+)$ denotes the element $(\ldots(a^\circ)^\circ\ldots)^\circ$ of the set A, such that the operation "$\circ$" is applied n times):

Axiom 1. For any element $a\in A$ the infinite sequence $a,a^\circ,a^{2\circ},\ldots$ consists of pair-wise different elements of the set A.

Axiom 2. For any elements $a,b\in A$ the following formula is true: $a^\circ=b^\circ\Rightarrow a=b$.

Axiom 3. For any element $a\in A$ there exists some element $b\in A$ and an integer $n\in\mathbb{Z}_+$, such that $a=b^{n\circ}$, and besides $b\neq c^{m\circ}$ for each element $c\in A$ and each integer $m\in\mathbb{N}$.

Let

$$\mathrm{Core}(A)=\{a\in A\,|\,(\forall b\in A)(n\in\mathbb{N})(a\neq b^{n\circ})\},$$

and

$$\mathrm{Cl}_\circ(a)=\{a^{n\circ}\,|\,n\in\mathbb{Z}_+\}\quad(a\in A).$$

Then

$$A=\bigcup_{a\in\mathrm{Core}(A)}\mathrm{Cl}_\circ(a).$$

Besides, due to Axiom 1, for any element $a\in A$ the mapping $a^{n\circ}\to n$ $(n\in\mathbb{Z}_+)$ is an isomorphism between the sequence $a,a^\circ,a^{2\circ},\ldots$ and the sequence $0,1,2,\ldots$, i.e. the Mathematical Induction technique can be applied as a mathematical proof on the set A. We illustrate the value of this factor by the following example.

Example 1. Let $G=(N,T,P,S)$ be the CFG grammar, such that $N=\{S,U,V\}$, $T=\{\alpha,\beta\}$, and P consists of the following productions: $S\to\alpha V\,|\,\beta U$, $U\to\alpha\,|\,\alpha S\,|\,\beta UU$, $V\to\beta\,|\,\beta S\,|\,\alpha VV$ (see [20], for example). It is necessary to prove that the language $L(G)$ consists of all strings with equal number of symbols α and β.

We consider the following three hypotheses:

H_1: $S\overset{*}{\Rightarrow}w$ $\Leftrightarrow$ the string $w\in L(G)$ consists of the equal number of symbols α and β.

H_2: $U\overset{*}{\Rightarrow}w$ $\Leftrightarrow$ the string $w\in T^*$ consists of one more α than β.

H_3: $V\overset{*}{\Rightarrow}w$ $\Leftrightarrow$ the string $w\in T^*$ consists of one more β than α.

Let $\mathrm{Core}(A)=\{a,b,c\}$, and the elements of the sets $\mathrm{Cl}_\circ(x)=\{x^{n\circ}\,|\,n\in\mathbb{Z}_+\}$ $(x\in\mathrm{Core}(A))$ are interpreted as follows:

$a^{n\circ}$ $(n\in\mathbb{Z}_+)$ is the proposition: the hypothesis H_1 is true for all strings $w\in L(G)$, such that $d(w)=n+2$ (since the minimal length of a string $w\in L(G)$ derivable from S is 2);

$b^{n\circ}$ $(n\in\mathbb{Z}_+)$ is the proposition: the hypothesis H_2 is true for all strings $w\in T^*$, such that $d(w)=n+1$ (since the minimal length of a string $w\in T^*$ derivable from U is 1);

$c^{n\circ}$ $(n \in \mathbb{Z}_+)$ is the proposition: the hypothesis H_3 is true for all strings $w \in T^*$, such that $d(w) = n+1$ (since the minimal length of a string $w \in T^*$ derivable from V is 1).

The basis of induction. We must prove that propositions $x^{0\circ}$ $(x \in \mathrm{Core}(A))$ are true.

There exist only two accessible derivations of the length 2 from S: $S \Rightarrow \alpha V \Rightarrow \alpha\beta$ and $S \Rightarrow \beta U \Rightarrow \beta\alpha$. Thus, the proposition $a^{0\circ}$ is true. There exists only one accessible derivation of the length 1 from U: $U \Rightarrow \alpha$. Thus, the proposition $b^{0\circ}$ is true. There exists only one accessible derivation of the length 1 from V: $V \Rightarrow \beta$. Thus, the proposition $c^{0\circ}$ is true.

Inductive hypotheses. Assume that propositions $x^{n\circ}$ $(x \in \mathrm{Core}(A))$ are true for all $n = 0,1,\ldots,k$.

Induction. We must prove that propositions $x^{(k+1)\circ}$ $(x \in \mathrm{Core}(A))$ are true.

Let us prove that the proposition $a^{(k+1)\circ}$ is true.

Suppose, that $S \overset{*}{\Rightarrow} w$ $(d(w) = (k+1)+2)$. Then either $w = \alpha w_1$, or $w = \beta w_2$, where $d(w_1) = d(w_2) = k+2$. Thus, either $S \Rightarrow \alpha V \overset{*}{\Rightarrow} \alpha w_1$, or $S \Rightarrow \beta U \overset{*}{\Rightarrow} \beta w_2$.

Since $V \overset{*}{\Rightarrow} w_1$ $(d(w_1) = k+2)$, then by Inductive hypotheses $w_1 \in T^*$ consists of one more β than α, i.e. $w = \alpha w_1$ consists of the equal number of α and β. Similarly, since $U \overset{*}{\Rightarrow} w_2$ $(d(w_2) = k+2)$, then by Inductive hypotheses $w_2 \in T^*$ consists of one more α than β, i.e. $w = \beta w_2$ consists of the equal number of α and β.

Conversely, let the string $w \in T^*$ $(d(w) = (k+1)+2)$ consists of the equal number of α and β. Then either $w = \alpha w_1$ and $w_1 \in T^*$ consists of one more β than α, or $w = \beta w_2$, and $w_2 \in T^*$ consists of one more α than β.

Since $d(w_1) = d(w_2) = k+2$, then by Inductive hypotheses $V \overset{*}{\Rightarrow} w_1$ and $U \overset{*}{\Rightarrow} w_2$. Therefore, $S \Rightarrow \alpha V \overset{*}{\Rightarrow} \alpha w_1$ and $S \Rightarrow \beta U \overset{*}{\Rightarrow} \beta w_2$, i.e. $w \in L(G)$.

Let us prove that the proposition $b^{(k+1)\circ}$ is true.

Suppose, that $U \overset{*}{\Rightarrow} w$ $(d(w) = (k+1)+1)$. Since the first step of the derivation is either $U \Rightarrow \alpha S$, or $U \Rightarrow \beta UU$, we get that either $U \Rightarrow \alpha S \overset{*}{\Rightarrow} a w_1$, or $U \Rightarrow \beta UU \overset{*}{\Rightarrow} \beta w_2 w_3$.

Since $S \overset{*}{\Rightarrow} w_1$ $(d(w_1) = k+1)$, then by Inductive hypotheses w_1 consists of the equal number of α and β, i.e. $w = \alpha w_1$ consists of one more α than β.

Since $U \overset{*}{\Rightarrow} w_2$ $(d(w_2) \le k+1)$ and $U \overset{*}{\Rightarrow} w_3$ $(d(w_3) \le k+1)$, then by Inductive hypotheses each of the strings w_2 and w_3 consist of one more α than β, i.e. $w = \beta w_2 w_3$ consists of one more α than β.

Conversely, let the string $w \in T^*$ $(d(w)=(k+1)+2)$ consists of one more α than β. Then either $w=\alpha w_1$ $(d(w_1)=k+1)$ and $w_1 \in T^*$ consists of the equal number of α and β, or $w=\beta w_2 w_3$ $(d(w_2), d(w_3) \le k+1)$ and each of $w_2, w_3 \in T^*$ consists of one more α than β. Using Inductive hypotheses we get that $U \Rightarrow \alpha S \overset{*}{\Rightarrow} aw_1$ and $U \Rightarrow \beta UU \overset{*}{\Rightarrow} \beta w_2 w_3$.

The proposition $c^{(k+1)\circ}$ can be proved similarly.

This example and examples in [18] are compelling arguments that considered Algebraic System and its subsystems can be effectively used in different Solvers and Theorem Provers.

3. New results. It is assumed that for the sub-algebra $\mathfrak{A}=(A;\{0,+,-\})$ $(|A|>1)$ the following three axioms hold:

Axiom 4. For any elements $a,b \in A$ the following identities expressed only in terms of the operation “+” are true:

$$a+(b+c)=(a+b)+c, \tag{30}$$

$$a+b=b+a, \tag{31}$$

$$a+a=a, \tag{32}$$

$$a+0=a. \tag{33}$$

Axiom 5. For any elements $a,b \in A$ the following identities expressed only in terms of the operation “$-$” are true:

$$a-a=0, \tag{34}$$

$$(a-b)-c=(a-c)-(b-c), \tag{35}$$

$$0-a=0, \tag{36}$$

$$a-0=a, \tag{37}$$

$$a-(a-b)=b-(b-a). \tag{38}$$

Axiom 6. For any elements $a,b,c \in A$ the following identities are true:

$$(a+b)-c=(a-c)+(b-c), \tag{39}$$

$$a-(b+c)=(a-b)-c, \tag{40}$$

$$a+(b-a)=a+b, \tag{41}$$

$$a+(a-b)=a, \tag{42}$$

$$a-(b-c)=(a-b)+(a-(a-c)). \tag{43}$$

Let us consider some consequences from the Axiom 4.

Due to (30)-(33), the magma $(A,+)$ is some commutative idempotent monoid, and the element 0 is the identity element of this monoid. The partial ordering relation “$\le$” can be defined on the set A as follows:

$$a \le b \Leftrightarrow a+b=b. \tag{44}$$

Due to (33), the element 0 is the least element of the poset $(A,\le)$, i.e. $0 \le a$ for all $a \in A$. The partial ordering relations “$<$”, “$\ge$” and on the set A can be defined in the usual way.

Proposition 1. For any elements $a,b,c,d\in A$ the following formula is true:

$$a\le b\,\&\,c\le d\Rightarrow a+c\le b+d. \tag{45}$$

Proof. Since $a\le b$ then $a+b=b$. Since $c\le d$ then $c+d=d$. Due to (30) and (31),

$$(a+c)+(b+d)=a+(c+(b+d))=a+((c+b)+d)=a+((b+c)+d)=$$

$$=(a+(b+c))+d=((a+b)+c)+d=(b+c)+d=b+(c+d)=b+d.$$

Since $(a+c)+(b+d)=b+d$, we get $a+c\le b+d$.

Q.E.D.

Corollary 1. For any elements $a,b,c\in A$ the following formula is true:

$$a\le b\Rightarrow a+c\le b+c. \tag{46}$$

Proof. Due to (32), $c\le c$ for each element $c\in A$. Setting $d=c$ in (45), we get (46).

Q.E.D.

The partial ordering relation "$\le$" gives the possibility to define the following intervals on the poset $(A,\le)$:

$$[a,b]=\{x\in A\,|\,a\le x\,\&\,x\le b\}\quad (a,b\in A; a\le b), \tag{47}$$

$$(a,b]=\{x\in A\,|\,a< x\,\&\,x\le b\}\quad (a,b\in A; a< b), \tag{48}$$

$$[a,b)=\{x\in A\,|\,a\le x\,\&\,x< b\}\quad (a,b\in A; a< b), \tag{49}$$

$$(a,b)=\{x\in A\,|\,a< x\,\&\,x< b\}\quad (a,b\in A; a< b). \tag{50}$$

The operation "$+$" can be extended to the set of all intervals on the poset $(A,\le)$. For example, for any intervals $[a,b]$ and $[c,d]$ we set:

$$[a,b]+[c,d]=\{x+y\,|\,x\in[a,b]\,\&\,y\in[c,d]\}. \tag{51}$$

In the case when the summands are defined by (48)-(50), or the summands are intervals of different types their sum can be defined similarly.

Theorem 1. For any elements $a,b,c,d\in A$ the following inclusion is true:

$$[a,b]+[c,d]\subseteq[a+c,b+d]. \tag{52}$$

Proof. Let $z\in[a,b]+[c,d]$. Due to (51), $z=x+y$ for some $x\in[a,b]$ and $y\in[c,d]$. Due to (47), the inequalities $a\le x$, $x\le b$, $c\le y$ and $y\le d$ are true. Due to Proposition 1, we get:

$$a\le x\,\&\,c\le y\Rightarrow a+c\le x+y=z,$$

$$x\le b\,\&\,y\le d\Rightarrow z=x+y\le b+d.$$

Due to (47), the inequalities $a+c\le z$ and $z\le b+d$ imply that $z\in[a+c,b+d]$.

Since $z\in[a,b]+[c,d]$ implies that $z\in[a+c,b+d]$, the inclusion (52) is true.

Q.E.D.

The meaning of the Theorem 1 is as follows. The set $\mathfrak{S}$ of all monoids $(A,+)$ $(|A|>1)$ that satisfy to the Axiom 4 can be partitioned into two subsets $\mathfrak{S}_1^{(1)}$ and $\mathfrak{S}_2^{(1)}$, where the subset

$\mathfrak{S}_1^{(1)}$ consists of all monoids $(A,+)\in\mathfrak{S}$, such that for any elements $a,b,c,d\in A$ holds the identity $[a,b]+[c,d]=[a+c,b+d]$, and the subset $\mathfrak{S}_2^{(1)}$ consists of all monoids $(A,+)\in\mathfrak{S}$, such that for some elements $a,b,c,d\in A$ holds the strict inclusion $[a,b]+[c,d]=[a+c,b+d]$. It is evident that the structure of the elements of the subset $\mathfrak{S}_1^{(1)}$ differs significantly from the structure of the elements of the subset $\mathfrak{S}_2^{(1)}$.

For any element $a\in A$ the lower cone a^{∇} and the upper cone a^{Δ} can be defined in the usual way, i.e.

$$a^{\nabla}=\{x\in A\,|\,x\leq a\}, \tag{53}$$

$$a^{\Delta}=\{x\in A\,|\,a\leq x\}. \tag{54}$$

It is evident that for eny element $a\in A$ the lower cone a^{∇} has the least element 0 and the greatest element a, while for the upper cone a^{Δ} we can guarantee only the existence of the least element a.

The operation "$+$" can be extended to the set of all lower cones as well as to the set of all upper cones of the elements of the poset $(A,\leq)$ as follows:

$$a^{\nabla}+b^{\nabla}=\{x+y\,|\,x\in a^{\nabla}\ \&\ y\in b^{\nabla}\}, \tag{55}$$

$$a^{\Delta}+b^{\Delta}=\{x+y\,|\,x\in a^{\Delta}\ \&\ y\in b^{\Delta}\}. \tag{56}$$

Theorem 2. For any elements $a,b\in A$ the following inclusions are true:

$$a^{\nabla}+b^{\nabla}\subseteq(a+b)^{\nabla}, \tag{57}$$

$$a^{\Delta}+b^{\Delta}\subseteq(a+b)^{\Delta}. \tag{58}$$

Proof. Let $z\in a^{\nabla}+b^{\nabla}$. Due to (55), $z=x+y$ for some $x\in a^{\nabla}$ and $y\in b^{\nabla}$. Due to (53), the inequalities $x\leq a$ and $y\leq b$ hold for any elements $x\in a^{\nabla}$ and $y\in b^{\nabla}$. Due to Proposition 1, the inequalities $x\leq a$ and $y\leq b$ imply that $z=x+y\leq a+b$, i.e. $z\in(a+b)^{\nabla}$. Since $z\in a^{\nabla}+b^{\nabla}$ implies that $z\in(a+b)^{\nabla}$, then the inclusion (57) is true.

The inclusion (58) can be proved in a similar way.

Q.E.D.

The meaning of the theorem 2 is as follows. The set $\mathfrak{S}$ of all monoids $(A,+)$ $(|A|>1)$ that satisfy to the Axiom 4 can be partitioned into four subsets $\mathfrak{S}_1^{(2)}$, $\mathfrak{S}_2^{(2)}$, $\mathfrak{S}_3^{(2)}$ and $\mathfrak{S}_4^{(2)}$. The subset $\mathfrak{S}_1^{(2)}$ consists of all monoids $(A,+)$, such that for any elements $a,b\in A$ the following two identities hold: $a^{\nabla}+b^{\nabla}=(a+b)^{\nabla}$, and $a^{\Delta}+b^{\Delta}=(a+b)^{\Delta}$. The subset $\mathfrak{S}_2^{(2)}$ consists of all monoids $(A,+)$, such that for any elements $a,b\in A$ holds identity $a^{\nabla}+b^{\nabla}=(a+b)^{\nabla}$, and for some elements $c,d\in A$ holds the strict inclusion $c^{\Delta}+d^{\Delta}\subset(c+d)^{\Delta}$. The subset $\mathfrak{S}_3^{(2)}$ consists of all monoids $(A,+)$, such that for any elements $a,b\in A$ holds identity $a^{\Delta}+b^{\Delta}=(a+b)^{\Delta}$, and for some elements $c,d\in A$ holds the strict inclusion $c^{\nabla}+d^{\nabla}\subset(c+d)^{\nabla}$. The subset $\mathfrak{S}_4^{(2)}$ consists of all monoids $(A,+)$, such that for some elements $a,b \in A$ holds the strict inclusion $a^{\nabla}+b^{\nabla} \subset (a+b)^{\nabla}$, and for some elements $c,d \in A$ holds the strict inclusion $c^{\nabla}+d^{\nabla} \subset (c+d)^{\nabla}$. It is evident that the structure of the elements of the subsets $\mathfrak{S}_1^{(2)}$, $\mathfrak{S}_2^{(2)}$, $\mathfrak{S}_3^{(2)}$ and $\mathfrak{S}_4^{(2)}$ is significantly different.

Let $\mathfrak{F}_A = \{f_a\}_{a \in A}$ be the family of mappings defined as follows:

$$f_a(x) = x + a \quad (x \in A). \tag{59}$$

Due to (46), any f_a $(a \in A)$ is an isotone mapping. Due to Axiom 4, for any set A $(|A|>1)$ the set $\mathfrak{F}_A = \{f_a\}_{a \in A}$ is a commutative monoid of isotone mappings. Moreover, each mapping f_a $(a \in A)$ can be naturally extended on intervals and cones of the poset $(A,\le)$.

Let us consider some consequences from the Axiom 5.

Due to Axiom 5, $(A,-)$ is a non-commutative magma, and the element 0 is the left zero and the right identity element of this magma.

Proposition 2. The magma $(A,-)$ is a non-associative magma.

Proof. Let's assume the opposite, i.e. that $(A,-)$ is an associative magma. Then for all elements $a,b,c \in A$ the following identity is true:

$$a-(b-c) = (a-b)-c. \tag{60}$$

Substituting $b=0$ and $c=a$ in (60), and applying (36), (37) and (34), we get that for all $a \in A$

$$a-(0-a) = (a-0)-a \Leftrightarrow a-0 = a-a \Leftrightarrow a=0.$$

We get contradiction to the assumption that $|A|>1$.

Thus, the assumption that the magma $(A,-)$ is an associative magma is false.

Q.E.D.

Proposition 3. For all elements $a,b \in A$ the identity $(a-b)-a=0$ is true.

Proof. Substituting $c=a$ in (35) and applying (34) and (36), we get that for all $a,b \in A$

$$(a-b)-a = (a-a)-(b-a) \Leftrightarrow (a-b)-a = 0-(b-a) \Leftrightarrow (a-b)-a = 0.$$

Q.E.D.

Let us consider some consequences from the Axioms 4-6.

Proposition 4. For all elements $a,b \in A$ the following identity is true:

$$a-(a+b) = 0. \tag{61}$$

Proof. Substituting $b=a$ and $c=b$ in (40), we get that for all $a,b \in A$ the following identity is true:

$$a-(a+b) = (a-a)-b.$$

Applying (34) and (36) to this identity, we get that for all $a,b \in A$ the identity (61) is true.

Q.E.D.

Theorem 3. For any elements $a,b \in A$ the following formula is true:

$$a+b=b \Leftrightarrow a-b=0. \tag{62}$$

Proof. Let's assume that $a+b=b$. Due to (61), $a-b=0$, i.e. formula

$$a+b=b \Rightarrow a-b=0. \tag{63}$$

is true.

It is evident that (41) can be rewritten as follows:

$$b+(a-b)=a+b. \tag{64}$$

Let's assume that $a-b=0$. Due to (64), $a+b=b$, i.e. that formula

$$a-b=0 \Rightarrow a+b=b. \tag{65}$$

is true.

Formulae (63) and (65) imply that formula (62) is true.

Q.E.D.

Due to (44) and (62), the partial ordering "$\le$"on the set A can be defined as follows:

$$a \le b \Leftrightarrow a-b=0.$$

Therefore, in terms of Sets Theory, binary operations "$\vartriangle$"and "$\cdot$"defined by (14) and (15) can be naturally interpreted as the symmetric difference and the intersection of sets, respectively.

It seems actual to investigate in details the following special generalization of the sub-algebra $\mathfrak{A}=(A;\{0,+,-\})$ $(|A|>1)$.

Let Atoms $(|\mathrm{Atoms}|>1)$ be some fixed finite or countable set, π be some fixed partition of the set Atoms. The following sequence of sets can be defined:

$$X_0=\{\varnothing\},$$

$$X_1=\{\{x_i\}|x_i \in \mathrm{Atoms}\},$$

$$X_n=\{S \subseteq \mathrm{Atoms} \mid |S|=n \,\&\, (\forall x_i,x_j \in S)(x_i \ne x_j \Rightarrow x_i \not\equiv x_j (\mathrm{mod}\,\pi))\} \quad (n \ge 2).$$

Let

$$A=\bigcup_{i=0}^{\infty} X_i .$$

The operation "$+$" on the set A can be defined as follows. For any $x \in A$ we set $\varnothing+x=x+\varnothing=x$. For any $S_1,S_2 \in \bigcup_{i=1}^{\infty} X_i$ the sum S_1+S_2 is determined if and only if $x \not\equiv y (\mathrm{mod}\,\pi)$ for all $x \in S_1$ and $y \in S_2$. If the sum S_1+S_2 is determined, we set:

$$S_1+S_2=S_1 \cup S_2.$$

It is evident that "$+$" is associative-commutative operation, and it is a partial operation if and only if $\pi \ne \mathbf{0}$.

The operation "$-$" on the set A can be defined by identity:

$$S_1-S_2=S_1 \setminus S_2 \quad (S_1,S_2 \in A).$$

The operation "$\cdot$" on the set A can be defined by identity:

$$S_1 \cdot S_2 = S_1 \cap S_2 \quad (S_1, S_2 \in A).$$

The relation $\le$ of partial ordering on the set A can be defined by the following formula:

$$S_1 \le S_2 \Leftrightarrow S_1 \subseteq S_2 \quad (S_1, S_2 \in A).$$

In fact, in terms of this Algebra $\mathfrak{A} = (A; \{\varnothing, +, -\}) \quad (|A| > 1)$, under supposition that A is a finite set, sub-algebras of the Nominative Sets Algebra have been investigated in [21]. Moreover, it has been shown in [22] that if some linear ordering on the set Atoms is defined then quick algorithms for implementation operations of this Algebra can be designed.

4. Conclusions. In the given paper some researches related with the development of the Algebraic Aggregate Theory proposed in [17] are briefly presented. Examples considered in [18] and in this paper are a compelling argument for the possibility to apply this theory as a mathematical base for the construction and processing of data structures in mathematics and its applications, as well as in different Solvers and Theorem Provers. The use of this theory as some base in the study of nominative sets makes it possible to apply this theory effectively in the development and verification of software.

1. Aho A. Data structures and algorithms / A. Aho, J. Hopcroft, J. Ullman. – Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1983. – 427 pp.

2. Blau H.A. Table algebras / H.A. Blau // European Journal of Combinatorics. – 2009. – Vol. 30. – Issue 6. – P. 1426-1455.

3. Arad Z. Generalized table algebras / Z. Arad, E. Fisman, M. Muzychuk // Israel Journal of Mathematics. – 1999. – Vol. 114. – Issue 1. – P. 29–60.

4. McCune W. Short single axioms for Boolean algebra / W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, L. Wos // Journal of Automated Reasoning. – 2002. – Vol. 29, Issue 1. – P. 1-16.

5. Dadej A. On duality between order and algebraic structures in Boolean systems / A. Dadej, K. Halik // Journal of Mathematics and Applications. – 2013. – No. 36. – P. 35-62.

6. Abbott J.C. Semi-Boolean algebra / J.C. Abbott // Matematički Vesnik. – 1967. – Vol. 4, Issue 40. – P. 177–198.

7. Haglich P.P. Semi-Boolean algebras: empirical logic and rings / P.P. Haglich // Trident Scholar Project Report, No. 117. – Annapolis, Maryland, USA: U.S. Naval Academy, 1982. – 65 pp.

9. Manzonetto G. From λ-calculus to universal algebra and back / G. Manzonetto, A. Salibra // Lecture Notes in Computer Science. – 2008. – Vol. 5162. – P. 479-490.

10. Haglich P.P. Detecting emergent behaviors with semi-Boolean algebra / P.P. Haglich, C. Rouff, L. Pullum // The American Institute of Aeronautics and Astronautics: InfoTech

Conference, April 20-22, 2010, Atlanta, Georgia, USA: – 6 pp. – Published Online: 14 Jun 2012. – https://doi.org/10.2514/6.2010-3503

11. Salibra A. Boolean-like algebras / A. Salibra, A. Ledda, F. Paoli, T. Kowalski // Algebra Universalis. – 2013. – Vol. 69, No. 2. – P. 113-138.

12. Ledda A. On semi-Boolean-like algebras / A. Ledda, F. Paoli, A. Salibra // Acta Univ. Palacki. Olomuc., Fac. rer. nat., Mathematica. – 2013. – Vol. 52, No.1. – P. 101–120.

13. Kuznetsov E. General Boolean algebras, Boolean rings and extension algebras / E. Kuznetsov, E. Kuznetsova // Mathematical Foundations of Informatics: the 5th conference, July 3-6, 2019, Iasi, Romania: proceedings. – 2019. – P. 181-186.

14. S. Pumplun. The non-associative algebras used to build fast-decodable space-time block codes / S. Pumplun, A. Steele // Advances in Mathematics of Communications. – 2015. – Vol. 9, No. 4. – P. 449-469.

15. Shcherbacov V.A. Elements of quasigroup theory and applications / V.A. Shcherbacov. – Boca Raton, Florida, USA: CRC Press, 2017. – 576 pp.

16. Shah T. Literature survey on non-associative rings and developments / T. Shah, A. Razzaque, I. Rehman, M.A. Gondal, M. I. Faraz, K.P. Shum // European Journal of Pure and Applied Mathematics. – 2019. – Vol. 12, No. 2. – P. 370-408.

17. Drugus I. Towards an algebraic set theory for the formalization of data structures / I. Drugus // Mathematical Foundations of Informatics: the 4th conference, July 2-6, 2018, Chisinau, Republic of Moldova: proceedings. – 2018. – P. 73-89.

18. Drugus I. Imbrication algebras – algebraic structures of nesting order / I. Drugus, V.G. Skobelev // Computer Science Journal of Moldova. – 2018. – Vol. 26, no. 3. – P. 233-250.

19. Drugus I. Some developments of Aggregate Theory / I. Drugus, V.G. Skobelev // Mathematical Foundations of Informatics: the 5th conference, July 3-6, 2019, Iasi, Romania: proceedings. – 2019. – P. 171-180.

20. Krithivasan K. Introduction to formal languages, automata theory and computation / K. Krithivasan, R. Rama. – Uttar Pradesh, India: Pearson India Educational Services Pvt.Ltd, 2009. – 425 pp.

21. Skobelev V.G. Set-theoretic analysis of nominative data / V.G. Skobelev, M. Nikitchenko, I. Ivanov // Computer Science Journal of Moldova. – 2015. – Vol. 23, no. 3. – P. 270-288.

22. Skobelev V.G. Nominative data with ordered set of names / V.G. Skobelev, M. Nikitchenko, I. Ivanov // Computer Science Journal of Moldova. – 2017. – Vol. 25, no. 2. – P. 195-216.