The identities of additive binary arithmetics

Anton A. Klyachko   Ekaterina V. Menshova

Faculty of Mechanics and Mathematics, Moscow State University
Moscow 119991, Leninskie gory, MSU
klyachko@mech.math.msu.su   ekaterina.menshova@gmail.com

Submitted: May 15, 2011. Accepted: Jan 26, 2011. Published: Feb 7, 2012.
Mathematics Subject Classifications: 08A70, 08A40, 08B20, 17A30

Operations of arbitrary arity expressible via addition modulo 2^n and bitwise addition modulo 2 admit a simple description. The identities connecting these two additions have a finite basis. Moreover, the universal algebra $\mathbb{Z}/2^n\mathbb{Z}$ with these two operations is rationally equivalent to a nilpotent ring and, therefore, generates a Specht variety.

0. Introduction

On the set of integers $\{0,1,\ldots,q-1\}=\mathbb{Z}_q$, where q is a power of two, we consider two natural operation: addition modulo q and bitwise addition modulo 2. In computer literature, these operations are usually denoted by `ADD` and `XOR`; they are hardware implemented in all modern computers, as far as we know.$^{*)}$

We consider two natural questions.

1. *What function $\mathbb{Z}_q^k \to \mathbb{Z}_q$ can be expressed via these two operations?*
2. *What identities connect these two operations?*

Theorem 1 gives a complete answer to the first question; we obtain a simple fast algorithm deciding whether or not an arbitrary given function can be expressed via `ADD` and `XOR`. We also calculate the total number of k-argument functions expressible via these two operation (Corollary 1).

We do not give an explicit answer to the second question, but we prove that, for each q, all identities connecting `ADD` and `XOR` follow from a finite number of such identities (Theorem 2) and there exists an algorithm writing down such a finite basis of identities for any given q (Corollary 2).

The problem of existence of finite basis of identities was extensively studied for groups, semigroups, rings, linear algebras (see, for example, [BaOl88], [Neum69], [Belo99], [VaZe89], [Grish99], [Zaits78], [Keme87], [Kras90], [Laty73], [Lvov73], [Olsh89], [Shch99], [GuKr03], [Kras09], [Speht52] and literature cited therein), but the "applied" algebra with operations `ADD` and `XOR` has never been studied from this point of view, as far as we known.

In algebraic term, Theorem 1 is an explicit description of the free algebras of the variety, generated by the algebra $\mathbb{Z}_q$ with two binary operations `ADD` and `XOR`; Theorem 2 says that this variety is finitely based (i.e. it has a finite basis of identities). See, for example, [BaOl88] or [GA91] for necessary information about varieties of universal algebras.

Most of Notation we use is standard. Note only that the addition modulo q (i.e. `ADD`) is denoted by $+$; the bitwise addition modulo 2 (i.e. `XOR`) is denote by $\oplus$. The symbol a_i denotes the ith bit of a number $a \in \mathbb{Z}_q$; the bits with negative numbers are assumed to be zero. The set $\{0,1,\ldots,q-1\}=\mathbb{Z}_q$ when considered as a universal algebra with operations $+$ and $\oplus$ is denoted by the symbol A_q. The

This work was supported by the Russian Foundation for Basic Research, project no. 11-01-00945.

*) Usually, the command `ADD` is simply called addition, because it is used mostly for obtaining the usual sum of positive integers; however, actually the processor performs the addition modulo a large number q (for example, $q=2^{32}$ for 32-bit processors etc.).

multiplication by integer numbers in A_q is always considered as multiplication modulo q. These multiplications are obviously expressed in terms of addition $+$, for example, $3x = x+x+x$ and $-3x = (-3)x = -(3x) = \underbrace{x+x+\ldots+x}_{3(q-1)\ terms}$.

The authors thank an anonymous referee for a lot of useful remarks and pointing out a flaw in the original proof of the main theorem (the easier direction). We also thank A. E. Pankratiev for useful comments.

1. Definitions and results

A function $f\colon A_q^k \to A_q$ is called *algebraic* if it can be expressed via operations $+$ and $\oplus$. More precisely, the set $F_{k,q}$ of algebraic k-argument functions is the inclusion-minimal set of functions, satisfying the following conditions:

1) the functions $f(x,y,\ldots) = x,\ f(x,y,\ldots) = y, \ldots$ belong to $F_{k,q}$;
2) if functions f and g belong to $F_{k,q}$, then the functions $f+g$ and $f\oplus g$ belong to $F_{k,q}$.

The set $F_{k,q}$ of all algebraic k argument functions forms a universal algebra with respect to operations $+$ and $\oplus$; this is the *free algebra of rank k of the variety generated by the algebra A_q*.

Theorem 1. *A function $f\colon A_q^k \to A_q$ is algebraic if and only if, for any i, the ith bit of its value is expressed via bits of the arguments by a formula of the form*

$$(f(x,y,\ldots))_i = g(x_i, y_i, \ldots; x_{i-1}, y_{i-1}, \ldots; x_{i-2}, y_{i-2}, \ldots; \ldots) \qquad (*)$$

(*the bits with negative numbers are assumed to be zero*), *where g is an independent of i Zhegalkin polynomial* (*over $\mathbb{Z}_2$*) *without free term, whose weight does not exceed 1.*

The *weight* or the *reduced degree* of a polynomial in variables

$$x_i, y_i, \ldots, x_{i-1}, y_{i-1}, \ldots, x_{i-2}, y_{i-2}, \ldots$$

is the maximal weight of its monomials; the weight of a monomial is the sum of weights of its variables; the weight of variables $x_{i-l}, y_{i-l}, \ldots$ is the number 2^{-l}. (Here, i is a formal parameter.)

Example 1. If $q = 8$ and $k = 1$, then there are exactly four Zhegalkin monomials whose weights does not exceed one: x_i (weight 1), x_{i-1} (weight $\frac{1}{2}$), x_{i-2} (weight $\frac{1}{4}$), and $x_{i-1}x_{i-2}$ (weight $\frac{3}{4}$). (Here, we use that no variable occurs in a Zhegalkin monomial more than once.) Therefore, there are 2^4 polynomials of weight not exceeding one. Thus, the algebra $F_{1,8}$ consists of 16 elements. For example, the algebraic function corresponding to the Zhegalkin polynomial $x_i \oplus x_{i-1}x_{i-2}$ has the form

$$f(x) = f(x_0,\ x_1,\ x_2) = (x_0 \oplus x_{-1}x_{-2},\ x_1 \oplus x_0x_{-1},\ x_2 \oplus x_1x_0) = (x_0,\ x_1,\ x_2 \oplus x_1x_0)$$

(because the bits with negative numbers are zero). In other words,

$$f(0) = 0,\ f(1) = 1,\ f(2) = 2,\ f(3) = 7,\ f(4) = 4,\ f(5) = 5,\ f(6) = 6,\ f(7) = 3.$$

Theorem 1 makes it possible to construct the following simple

ALGORITHM determining whether or not a given function $f\colon \mathbb{Z}_{2^\varkappa}^k \to \mathbb{Z}_{2^\varkappa}$ is algebraic (i.e. can be expressed via `ADD` and `XOR`).

1. Write the most significant bit $(f(x,y,\ldots))_{\varkappa-1}$ of the value of the function f as a Zhegalkin polynomial $g_{\varkappa-1}(x_0, y_0, \ldots, x_1, y_1, \ldots)$ in bits of arguments and verify that the weight of this

polynomial (for $i = \varkappa - 1$) does not exceed one and the free term is zero. If the weight is higher or the free term is nonzero, then exit the program with the answer `NO`.

2. Make the following substitutions in the polynomial $g_{\varkappa-1}$:

$$\begin{aligned} &x_0 \to 0,\ x_1 \to x_0,\ x_2 \to x_1, \dots,\ x_{\varkappa-1} \to x_{\varkappa-2}, \\ &y_0 \to 0,\ y_1 \to y_0,\ y_2 \to y_1, \dots,\ y_{\varkappa-1} \to y_{\varkappa-2}, \dots \end{aligned} \tag{$**$}$$

and verify that the obtained polynomial $g_{\varkappa-2}$ coincides with the polynomial giving $(\varkappa - 2)$-th bit of the function f. If not, then exit the program with the answer `NO`; if yes, then continue.

$$\dots \quad \dots \quad \dots$$

$\varkappa - 1$. Make substitutions $(**)$ in the polynomial g_2 and verify that the obtained polynomial g_1 coincides with the polynomial giving the 1st bit of the function f. If no, then exit the program with the answer `NO`; if yes, then continue.

$\varkappa$. Make substitution $(**)$ in the polynomial g_1 and verify that the obtained polynomial g_0 coincides with the polynomial giving the least significant bit of the function f. If no, then exit the program with the answer `NO`; if yes, then exit the program with the answer `YES`.

It is clear that this algorithm can be easily made uniform with respect to $\varkappa$.

For example, the function of multiplication of two numbers modulo q cannot be expressed via `ADD` and `XOR` (the algorithm stops at the first step because of the condition on the weight); this is not surprising, of course. However, the one-argument function $x \mapsto xy$ is algebraic for each given $y \in \mathbb{Z}_q$, as was already mentioned.

The proof of Theorem 1 is constructive and gives some algorithm making it possible to express a given function f via `ADD` and `XOR` (if it is expressible), but this algorithm is much more complicated.

Example 1 can be easily generalised. Calculating monomials for any q and k, we obtain the following assertion.

Corollary 1. *The free algebra $F_{k,q}$ comprises*

$$2^{\frac{1}{k!}\left(\frac{q}{2}+1\right)\left(\frac{q}{2}+2\right)\dots\left(\frac{q}{2}+k\right)-1} \tag{1}$$

elements.

Proof. In the case where $k = 1$, there are precisely $\frac{q}{2}$ monomials of weight at most one. Indeed, by virtue of the uniqueness of binary decomposition of an integer, there exists precisely one monomial of each weight $s \cdot \frac{2}{q}$, where $s \in \{1, 2, \dots, \frac{q}{2}\}$. Namely, this is the monomial

$$x_{i-l_1} x_{i-l_2} \dots x_{i-l_p}, \quad \text{where} \quad s = 2^{\varkappa-1-l_1} + 2^{\varkappa-1-l_2} + \dots + 2^{\varkappa-1-l_p}, \quad \text{and } 2^{\varkappa} = q.$$

This implies that, for any integer k, the number of monomials of weight at most one coincides with the number of nonzero tuples of nonnegative integers $(n_1, \dots, n_k)$ with sum at most $\frac{q}{2}$ (here, $n_i \cdot \frac{2}{q}$ is the weight with respect to the ith variable). It is well known that the number of such tuples is

$$\frac{(\frac{q}{2}+1)(\frac{q}{2}+2)\dots(\frac{q}{2}+k)}{k!} - 1.$$

Therefore, the total number of polynomials of weight at most one can be found by formula (1).

The following assertion is a reformulation of Theorem 1.

Theorem 1′. *A function $f\colon A_q^k \to A_q$ is algebraic if and only if it can be written in the form*

$$f(x, y, \ldots) = \bigoplus_i \left((2^{k_{i,1}}x) \odot (2^{k_{i,2}}x) \odot \ldots \odot (2^{l_{i,1}}y) \odot (2^{l_{i,2}}y) \odot \ldots \right),$$

where the inequality $2^{-k_{i,1}} + 2^{-k_{i,2}} + \ldots + 2^{-l_{i,1}} + 2^{-l_{i,2}} + \ldots \leqslant 1$ holds for each i.

Henceforth, the symbol $\odot$ denotes the bitwise multiplication modulo 2 (conjunction).

As for identities, we note first that, with respect to each of the operations $+$ and $\oplus$, the algebra A_q is an abelian group of exponent q and 2, respectively. Therefore, all identities involving only one of these two operations follow from the identities

$$(x + y) + z = x + (y + z),\ x + qy = x,\ x + y = y + x,$$
$$(x \oplus y) \oplus z = x \oplus (y \oplus z),\ x \oplus (y \oplus y) = x,\ x \oplus y = y \oplus x.$$

Identities involving the both operations are more complicated. The simplest example of such identity is $qx = x \oplus x$ which expresses the coincidence of the zero elements of these two group structures. A less trivial example is $\frac{q}{2}(x+y) = \frac{q}{2}(x \oplus y)$ (this identity expresses the coincidence of the additions $+$ and $\oplus$ at the least significant bit).

Theorem 2. *For any integer power of two q, the algebra A_q has a finite basis of identities. Moreover, the algebra A_q generates a Specht variety.*[*)]

The finiteness of an algebra per se does not implies the finiteness of a basis of its identities. A finite basis of identities exists for each finite group [OaPo64] (see also [Neum69]), each finite associative or Lie ring ([Lvov73], [Kruse73], [BaOl75]), but not for each finite semigroup and not for each finite ring (see [BaOl88]).

To prove Theorem 2, we use well-known nilpotency arguments rather than the finiteness. It is known that a finite basis of identities exists for any nilpotent ring (i.e. a ring in which all sufficiently long products vanish) and any nilpotent group (i.e. a group in which all sufficiently long multiple commutators equal to one) (see [Neum69]). The algebra A_q is neither a group nor a ring. However, it turns out that this algebra is *rationally equivalent* (in the sense of Mal'tsev) to a nilpotent ring, i.e. the algebra A_q can be endowed with a structure of nilpotent ring in such a way that the addition and multiplication of the ring can be expressed via operations $+$ and $\oplus$ and vice versa: the operation $+$ and $\oplus$ can be expressed via the addition and multiplication of the ring.

Theorem 3. *The algebra A_q is rationally equivalent to a nilpotent commutative nonassociative ring $(\mathbb{Z}_q, \oplus, \circ)$. The addition $\oplus$ is the usual bitwise addition modulo two, the multiplication $\circ$ is defined by the formula $x \circ y = 2(x \odot y)$, where $\odot$ is the bitwise multiplication modulo two (conjunction), and the multiplication by two is the multiplication by two modulo q, i.e. the shift of digits.*

In the following section, we prove Theorem 1. In section 3, we prove Theorem 3, which immediately implies Theorem 2, because any nilpotent ring has a finite basis of identities (and generates a Specht variety).

[*)] This means that any algebra of signature $(+, \oplus)$ satisfying all identities of the algebra A_q has a finite basis of identities.

2. Proof of Theorem 1

The element $[x,y] \overset{\text{def}}{=} x \oplus y \oplus (x+y)$ is called the *commutator* of the elements $x, y \in A_q$. The commutator is the difference between the sum $\oplus$ and the sum $+$ of two elements; the ith bit of the commutator $[x,y]$ is the carry to the ith digit during execution of the standard addition algorithm for $x+y$.

The following lemma is well known and widely used in electronic adders.

Proposition 1. *The bits of the commutator satisfies the equality*

$$[x,y]_i = x_{i-1}y_{i-1} \oplus [x,y]_{i-1}(x_{i-1} \oplus y_{i-1}). \tag{2}$$

Proof. The carry $c_i = [x,y]_i$ to the ith bit is formed as follows:

$$c_i = \begin{cases} 1, & \text{if among three bits } x_{i-1}, y_{i-1}, c_{i-1} \text{ the majority (i.e. two or three) is ones;} \\ 0, & \text{if among three bits } x_{i-1}, y_{i-1}, c_{i-1} \text{ the majority is zeros.} \end{cases}$$

The Zhegalkin polynomial for this Boolean function is

$$c_i = x_{i-1}y_{i-1} \oplus y_{i-1}c_{i-1} \oplus c_{i-1}x_{i-1} = x_{i-1}y_{i-1} \oplus c_{i-1}(x_{i-1} \oplus y_{i-1}),$$

as required.

Formula (2) can be rewritten in the form $[x,y] = 2(x \odot y \oplus [x,y] \odot (x \oplus y))$ or (applying distributivity of the multiplication by two with respect to $\odot$ and $\oplus$ and distributivity of $\odot$ with respect to $\oplus$) in the form

$$(2x) \odot (2y) = [x,y] \oplus (2[x,y]) \odot (2x) \oplus (2[x,y]) \odot (2y). \tag{2$'$}$$

Using formula (2), it is easy to show that the ith bit of the sum $x+y = x \oplus y \oplus [x,y]$ can be evaluated as

$$\begin{aligned}(x+y)_i &= x_i \oplus y_i \oplus x_{i-1}y_{i-1} \oplus x_{i-1}x_{i-2}y_{i-2} \oplus y_{i-1}x_{i-2}y_{i-2} \oplus \dots \\ &= \textit{the sum of all monomials of weight } 1.\end{aligned} \tag{2$''$}$$

Now, we proceed to prove Theorem 1. Let M be the set of all functions $A_q^k \to A_q$ of the form $(*)$. We have to prove two assertions.

1. Any function from $F_{k,q}$ belongs to M;
2. Any function from M belongs to $F_{k,q}$.

The first assertion is easy to verify. The functions $f(x,y,\dots) = x,\ f(x,y,\dots) = y, \dots$ belong to M, since the corresponding Zhegalkin polynomials $x_i,\ y_i, \dots$ have weight one. Suppose that some functions $f(x,y,\dots)$ and $g(x,y,\dots)$ belong to M, i.e.

$$\begin{aligned}(f(x,y,\dots))_i &= F(x_i, y_i, \dots; x_{i-1}, y_{i-1}, \dots; \dots), \\ (g(x,y,\dots))_i &= G(x_i, y_i, \dots; x_{i-1}, y_{i-1}, \dots; \dots),\end{aligned}$$

where F and G are Zhegalkin polynomials of weight at most one and without free term. Then

$$\begin{aligned}&(f(x,y,\dots) \oplus g(x,y,\dots))_i \\ &= F(x_i, y_i, \dots; x_{i-1}, y_{i-1}, \dots; \dots) \oplus G(x_i, y_i, \dots; x_{i-1}, y_{i-1}, \dots; \dots)\end{aligned}$$

and the weight of this Zhegalkin polynomial is at most one, i.e. $f \oplus g \in M$. According to $(2'')$, The ith bit of the function $f+g$ is

$$(f+g)_i = F \oplus G \oplus F'G' \oplus F'F''G'' \oplus F''G'G'' \oplus \ldots,$$

where the polynomial H' is obtained from $H = H(x_i, y_i, \ldots; x_{i-1}, y_{i-1}, \ldots; \ldots)$ by the shift of all bits:

$$H'(x_i, y_i, \ldots; x_{i-1}, y_{i-1}, \ldots; \ldots) = H(x_{i-1}, y_{i-1}, \ldots; x_{i-2}, y_{i-2}, \ldots; \ldots).$$

The weight of H' is at most half of the weight of H. Thus, the weight of

$$F \oplus G \oplus F'G' \oplus F'F''G'' \oplus F''G'G'' \oplus \ldots$$

is at most one and $f+g \in M$.

The remaining part of this section is the proof of the second assertion.

A *multiple commutators of complexity* n is a formal expression in variables $x, y, \ldots$ defined by induction as the follows:

each variable is a multiple commutator of complexity 1;

an expression $[u, v]$ is a multiple commutator of complexity n if the expressions u and v are multiple commutators and the sum of their complexities is n.

An obvious induction shows that a multiple commutator vanishes if at least one of the involving variables vanishes.

The *depth* $d(w)$ of a multiple commutator w is also defined by induction:

$d(x) = 0$ if x is a variable;

$d([u, v]) = \max(d(u), d(v)) + 1$.

For instance, the multiple commutator $[[x, y], [[z, t], x]]$ has complexity 5 and depth 3.

Lemma 1. *The ith bit of a multiple commutator w vanishes if $i < d(w)$.*

Proof. We use induction on depth. For depth 0, the assertion is true. Suppose that $d(u)$ lower bits of a multiple commutator u and $d(v)$ lower bits of a multiple commutator v vanish. Then formula (2) implies that $\max(d(u), d(v)) + 1$ lower bits of $[u, v]$ vanish, as required.

Lemma 2. *The depth of a multiple commutator of complexity at least 2^n is at least n.*

Proof. We use the induction on n. A multiple commutator of complexity 1 (i.e. a variable) has depth 0. A multiple commutator w of complexity $\geqslant 2^n$, where $n \geqslant 1$, has the form $w = [u, v]$. At least one from the multiple commutators u or v has complexity at least 2^{n-1} (otherwise, the complexity of w would be less than 2^n). By the induction hypothesis, the depth of this multiple commutator is at least $n-1$. This implies that the depth of w is at least n by the definition of depth.

Lemma 3. *In A_q, all multiple commutators of complexity $\geqslant q$ vanish.*

Proof. By Lemma 2, the depth of such a multiple commutator is at least $\log_2 q$ and, therefore, all bits of this multiple commutator vanish by Lemma 1.

Proof of theorem 1′. It is sufficient prove that any expression

$$(2^{k_1}x) \odot (2^{k_2}x) \odot \ldots \odot (2^{l_1}y) \odot (2^{l_2}y) \odot \ldots, \text{ where } 2^{-k_{i,1}} + 2^{-k_{i,2}} + \ldots + 2^{-l_{i,1}} + 2^{-l_{i,2}} + \ldots \leqslant 1,$$

is expressible via $\oplus$ and $+$. Let us prove a more strong assertion: *any expression of the form*

$$f = (2^k u) \odot (2^l v) \odot (2^m w) \odot \ldots, \quad \text{where } 2^{-k} + 2^{-l} + 2^{-m} + \ldots \leqslant 1 \text{ and } u, v, w, \ldots \text{ are multiple commutators} \tag{3}$$

is expressible via $\oplus$ *and* $+$ *(and variables).*

Suppose the contrary. Then there exists an expression of the form (3) inexpressible via $\oplus$ and $+$ and such that the inequality becomes the equality:

$$2^{-k} + 2^{-l} + 2^{-m} + \ldots = 1, \tag{4}$$

Indeed, $1 - (2^{-k} + 2^{-l} + 2^{-m} + \ldots)$ is a fraction of the form $\frac{s}{2^k}$, where k is the maximum of numbers $k, l, m, \ldots$, and, hence, the expression

$$f \odot \underbrace{(2^k u) \odot (2^k u) \odot \ldots \odot (2^k u)}_{s\ factors}$$

gives the same function as f, but the inequality transforms into the equality. Note that $2x = [x, x]$ and, hence, $2^k u$ is a multiple commutator provided u is a multiple commutator.

Let us choose among all nonalgebraic (not expressible via $\oplus$ and $+$) expressions (3) satisfying the equality (4), all expressions with minimal number of factors. Among all such minimal-length expressions, we choose an expression with the maximal sum of complexities of commutators $u, v, w, \ldots$. Such an expression f exists by Lemma 3.

The number of factors in this expression is at least two, because a multiple commutator can be expressed via $\oplus$ and $+$ by definition. Equality (4) implies that the two largest among exponents $k, l, m, \ldots$ are equal. Let us assume that $k = l$.

Using identity ($2'$), we obtain

$$\begin{aligned}
&(2^k u) \odot (2^k v) = (2 \cdot 2^{k-1} u) \odot (2 \cdot 2^{k-1} v) \\
&= [2^{k-1} u, 2^{k-1} v] \oplus (2[2^{k-1} u, 2^{k-1} v]) \odot (2 \odot 2^{k-1} u) \oplus (2[2^{k-1} u, 2^{k-1} v]) \odot (2 \cdot 2^{k-1} v) \\
&= 2^{k-1}[u, v] \oplus (2^k [u, v]) \cdot (2^k u) \oplus (2^k [u, v]) \odot (2^k v)
\end{aligned}$$

Therefore, expression (3) is the sum of three terms:

$$\begin{aligned}
f = &\Big((2^{k-1} t) \odot (2^m w) \odot \ldots \Big) \\
&\oplus \Big((2^k t) \odot (2^k u) \odot (2^m w) \odot \ldots \Big) \oplus \Big((2^k t) \odot (2^k v) \odot (2^m w) \odot \ldots \Big),
\end{aligned}$$

where $t = [u, v]$. All three terms satisfy equality (4).

The first term is algebraic, because its length (the number of factors) is less than the length of the initial expression f, whose length is minimal among all nonalgebraic expressions (3) satisfying equality (4).

The second and third terms have the same length as f, but their total complexity is higher (because the complexity of $t = [u, v]$ is one higher than the sum of complexities of u and v). Therefore, they are also algebraic by the choice of f. Thus, the expression f is algebraic as the sum of three algebraic terms. This contradiction completes the proof of Theorem $1'$ (and of Theorem 1).

3. Proof of Theorems 3 and 2

To prove Theorem 3, note that the algebra $\mathbb{Z}_q$ with the operations $\oplus$ and $\circ$ is, indeed, a nilpotent commutative nonassociative ring. The commutativity of the multiplication $\circ$ is obvious; the distributivity of the multiplication with respect to the addition $\oplus$ is obvious too. The nilpotency also holds: $((\ldots(x \circ y) \circ z) \circ \ldots = 0$ if the number of factors is at least $\log_2 q$. Note that the nilpotency index is generally large than $\log_2 q$, but it is at most q, i.e. any product of q elements (with any arrangements of brackets) vanishes. This can be shown similarly to Lemma 2 (the depth is at least logarithm of the length for any arrangements of brackets).

The multiplication $x \circ y = 2(x \odot y) = (2x) \odot (2y)$ is expressible via $+$ and $\oplus$ by Theorem $1'$. It remains to prove that the addition $+$ is expressible via the ring operations $\oplus$ and $\circ$.

Note that $+$ can be expressed via commutator and $\oplus$ (by the definition of the commutator): $x + y = x \oplus y \oplus [x, y]$. Therefore, it is sufficient to express commutator via $\oplus$ and $\circ$.

Lemma 4. *For any positive integer k, the commutator $[x, y]$ can be written in the form*

$$[x, y] = f_k(x, y) \oplus \underbrace{[x, y] \circ (x \oplus y) \circ (x \oplus y) \circ \ldots \circ (x \oplus y)}_{k+1\ factors}, \tag{5}$$

where f_k is a polynomial (in the sense of multiplication $\circ$ and addition $\oplus$). Henceforth, we assume that, in multiple products, all brackets are shifted to the left, for example, $a \circ b \circ c \circ d \overset{\text{def}}{=} ((a \circ b) \circ c) \circ d$.

Proof. If $k = 1$, then the required decomposition follows from the identity $(2')$:

$$[x, y] = x \circ y \oplus [x, y] \circ (x \oplus y). \tag{6}$$

For larger k, we use induction: having identity (5) for some k, we substitute identity (6) in it the right-hand side of (5) and obtain

$$\begin{aligned}[x, y] &= f_k(x, y) \oplus (x \circ y \oplus [x, y] \circ (x \oplus y)) \circ (x \oplus y) \circ (x \oplus y) \circ \ldots \circ (x \oplus y)\\ &= \underbrace{f_k(x, y) \oplus x \circ y \circ (x \oplus y) \circ (x \oplus y) \circ \ldots \circ (x \oplus y)}_{f_{k+1}(x,y)} \qquad\qquad ,\\ &\quad \oplus \underbrace{[x, y] \circ (x \oplus y) \circ (x \oplus y) \circ (x \oplus y) \circ \ldots \circ (x \oplus y)}_{k+2\ factors}\end{aligned}$$

as required.

Applying Lemma 4 for $k = \log_2 q$ and using the nilpotency of the ring, we obtain an expression of the commutator via $\oplus$ and $\circ$, namely, $[x, y] = f_{\log_2 q}(x, y)$ that completes the proof of Theorem 3.

Theorem 2 follows immediately from Theorem 3 and the following well-known fact.

Theorem (see [BaOl88]). *Each nilpotent ring has a finite basis of identities.*

Remark. The proof of the existence of a finite basis for the identities of nilpotent rings shows that all identities of such a ring follows from the identities involving at most n variables, where n is the nilpotency index, i.e. a number such that all products of n elements (with any arrangements of brackets) vanish. This implies the following fact.

Corollary 2. *All identities of the algebra A_q follows from the identities involving at most q elements. There exists an algorithm that, for any given $q = 2^{\varkappa}$, write out a finite basis of identities of A_q.*

This basis consists of the addition tables (for $+$ and $\oplus$) of the free algebra $F_{q,q}$.

REFERENCES

[GA91] Artamonov V. A., Salii V. N., Skornyakov L. A., Shevrin L. N., Shulgeifer E. G. General algebra, V.2, Moscow, Nauka. 1991.

[BaOl75] Bakhturin Yu. A., Olshanskii A. Yu. Identical relations in finite Lie rings, Mat. Sb., 96(138):4 (1975), 543-559. English translation in Mathematics of the USSR-Sbornik, 1975, 25:4, 507-523

[BaOl88] Bakhturin Yu. A., Olshanskii A. Yu. Identities. Algebra-2, Itogi Nauki i Tekhn. Ser. Sovr. probl. Mat. Fund. Napr, 18, VINITI, Moscow, 1988, 117-240. English translation: Identities, Algebra, II. Encyclopaedia of Mathematical Sciences, Current Problems in Mathematics, Fundamental Directions, vol. 18, Springer-Verlag, Berlin, 1991, pp. 117-240.

[Belo99] Belov A. Ya. On non-Specht varieties, Fund. i Prikl. Mat., 5:1 (1999), 47-66.

[VaZe89] Vais A. Ya., Zelmanov E. I. Kemer's theorem for finitely generated Jordan algebras, Izv. Vuzov. Ser. Mat., 1989, 6, 63-72. English translation in Soviet Math (Izv. VUZ) 33:6 38–47.

[Grish99] Grishin A. V. Examples of T-spaces and T-ideals over a field of characteristic two without the finite basis property, Fund. i Prikl. Mat., 5:1 (1999), 101-118.

[Zaits78] Zaitsev M. V. On finitely based varieties of Lie algebras, Mat. Sb., 106(148) (1978), 499-506. English translation in Mathematics of the USSR-Sbornik, 1979, 35:2, 165-171

[Keme87] Kemer A. R. Finite basis property of identities of associative algebras, Algebra i Logika, 26:5 (1987), 597-641. English translation in Algebra and Logic, 26:5 (1987), 362-397,

[Kras90] Krasilnikov A. N. The identities of a group with nilpotent commutator subgroup are finitely based, Izv. Acad. Nauk SSSR. Ser. Mat., 54:6 (1990), 1181-1195. English translation in Mathematics of the USSR-Izvestiya, 1991, 37:3, 539-553

[Laty73] Latyshev V. N. On some varieties of associative algebras, Izv. Acad, Nauk SSSR. Ser. Mat., 37:5 (1973), 1010-1037. English translation in Mathematics of the USSR-Izvestiya, 1973, 7:5, 1011-1038

[Lvov73] Lvov I. V. On varieties of associative rings, I, Algebra i Logika, 12 (1973), 269-297. English translation in Algebra and Logic 12, no. 3 (1973), 150-167

[Neum69] Neumann H. Varieties of groups. Springer-Verlag, 1967.

[Olsh89] Olshanskii A. Yu. Geometry of defining relations in groups. Moscow, Nauka, 1989. English translation: Geometry of defining relations in groups. Mathematics and its Applications (Soviet Series), vol. 70, Kluwer Academic Publishers Group, Dordrecht, 1991

[Shch99] Shchigolev V. V. Examples of infinitely based T-ideals, Fund. i Prikl. Mat., 5:1 (1999), 307-312.

[GuKr03] Gupta C.K., Krasilnikov A. N. The finite basis question for varieties of groups – Some recent results, Illinois Journal of Mathematics, 47:1-2 (2003), 273.

[Kras09] Krasilnikov A. N. A non-finitely based variety of groups which is finitely based as a torsion-free variety. Journal of Group Theory 2009 12:5, 735-743.

[Kruse73] Kruse R. L. Identities satisfied by a finite ring, J. Algebra, 26 (1973), 298-318.

[OaPo64] Oates S, Powell M. B. Identical relations in finite groups, J. Algebra 1 (1964),. 11-39.

[Speht52] Specht W. Gesetze in Ringen. I, Math. Z., 52 (1950), 557-589.