УДК 512.572+519.516.5+519.696+512.554 MSC: 08A70, 08A40, 08B20, 17A30

ТОЖДЕСТВА АДДИТИВНОЙ ДВОИЧНОЙ АРИФМЕТИКИ

Антон А. Клячко Екатерина В. Меньшова
Механико-математический факультет
Московского государственного университета
Москва 119991, Ленинские горы, МГУ
klyachko@mech.math.msu.su ekaterina.menshova@gmail.com

Операции произвольной арности, выражающиеся через сложение по модулю 2^n и побитовое сложение по модулю 2, допускают простое описание. Тождества, связывающие эти два сложения, имеют конечный базис. Более того, универсальная алгебра $\mathbb{Z}/2^n\mathbb{Z}$ с этими двумя операциями рационально эквивалентна нильпотентному кольцу и, следовательно, порождает шпехтово многообразие.

0. Введение

На множестве чисел $\{0, 1, \ldots, q-1\} = \mathbb{Z}_q$, где q является степенью двойки, рассматриваются две естественные операции: сложение по модулю q и побитовое сложение по модулю 2. В компьютерной литературе эти операции принято обозначать ADD и XOR; они аппаратно реализованы на всех современных ЭВМ, насколько мы знаем.*)

Мы рассматриваем два естественных вопроса.

1. *Какие функции $\mathbb{Z}_q^k \to \mathbb{Z}_q$ выражаются через эти две операции?*
2. *Какие тождества связывают эти две операции?*

На первый вопрос мы даём исчерпывающий ответ (теорема 1) — простой алгоритм, позволяющий по любой функции быстро ответить, выражается ли она через ADD и XOR, и вычисляем общее число функций от k аргументов, выражающихся через эти две операции (следствие 1).

На второй вопрос явного ответа мы не даём, но доказываем, что при каждом q все тождества, связывающие ADD и XOR, следуют из конечного числа таких тождеств (теорема 2) и существует алгоритм, выписывающий такой конечный базис тождеств для любого заданного q (следствие 2). Вопрос о наличии конечного базиса тождеств интенсивно исследовался для групп, полугрупп, колец, линейных алгебр (см., например, [БаОл88], [Нейм69], [Бело99], [ВаЗе89], [Гриш99], [Зайц78], [Keме87], [Крас90], [Латы73], [Льво73], [Ольш89], [Щиго99], [GuKr03], [Kras09], [Speht52] и литературу там цитируемую), но «прикладная» алгебра с операциями ADD и XOR никогда не изучалась с этой точки зрения, насколько нам известно.

На алгебраическом языке теорема 1 представляет собой явное описание свободных алгебр многообразия, порождённого алгеброй $\mathbb{Z}_q$ с двумя бинарными операциями ADD и XOR, а теорема 2 утверждает, что это многообразие конечно базируемо (то есть имеет конечный базис тождеств). Необходимые сведения о многообразиях универсальных алгебр можно прочитать, например, в [БаОл88] или в [ОА91].

Обозначения, которые мы используем в целом стандартны. Отметим только, что операцию сложения по модулю q (то есть ADD) мы будем обозначать символом $+$, а операцию побитового сложения по модулю 2 (то есть XOR) мы будем обозначать символом $\oplus$. Символ a_i обозначает i-й бит числа $a \in \mathbb{Z}_q$, причём биты с отрицательными номерами считаются нулевыми. Множество $\{0, 1, \ldots, q-1\} = \mathbb{Z}_q$, рассматриваемое как универсальная алгебра с операциями $+$ и $\oplus$, мы обозначаем символом A_q. Умножение на целые числа в алгебре A_q мы всегда трактуем как умножение по модулю q. Эти умножения очевидным образом выражаются через сложение $+$, например, $3x = x + x + x$, а $-3x = (-3)x = -(3x) = \underbrace{x + x + \ldots + x}_{3(q-1)\ \text{слагаемых}}$.

Авторы благодарят анонимного рецензента за множество полезных замечаний и обнаружение ошибки в первоначальном доказательстве основной теоремы (в лёгкую сторону). Мы благодарны также А. Е. Панкратьеву за полезные комментарии.

1. Определения и результаты

Функцию $f\colon A_q^k \to A_q$ мы называем *алгебраической*, если она выражается через операции $+$ и $\oplus$. Более точно, множеством $F_{k,q}$ алгебраических функций от k аргументов мы называем минимальное по включению множество функций, удовлетворяющее следующим условиям:

1) функции $f(x, y, \ldots) = x$, $f(x, y, \ldots) = y, \ldots$ принадлежат $F_{k,q}$;
2) если функции f и g принадлежат $F_{k,q}$, то функции $f + g$ и $f \oplus g$ принадлежат $F_{k,q}$.

Множество $F_{k,q}$ всех алгебраических функций от k аргументов образует универсальную алгебру относительно операций $+$ и $\oplus$, которая является *свободной алгеброй ранга k многообразия, порождённого алгеброй A_q*.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант №11-01-00945.

*) Команду ADD называют обычно просто сложением, поскольку она используется чаще всего для получения обычной суммы натуральных чисел, однако в действительности процессор выполняет сложение по некоторому большому модулю q (например, $q = 2^{32}$ для 32-разрядных процессоров и т.д.).

Теорема 1. *Функция $f\colon A_q^k \to A_q$ является алгебраической тогда и только тогда, когда i-й бит её значения для любого i выражается через биты аргументов при помощи формулы вида*

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

(биты с отрицательными номерами считаются нулевыми), где g — некоторый не зависящий от i многочлен (Жегалкина) без свободного члена над $\mathbb{Z}_2$, вес которого не превосходит единицы.

Весом или *приведённой степенью* многочлена от переменных $x_i, y_i, \ldots, x_{i-1}, y_{i-1}, \ldots, x_{i-2}, y_{i-2}, \ldots$ мы называем максимум весов его мономов, под весом монома мы понимаем сумму весов входящих в него переменных, а под весом переменных $x_{i-l}, y_{i-l}, \ldots$ мы понимаем число 2^{-l}. (Здесь i считается формальным параметром.)

Пример 1. Если $q = 8$ и $k = 1$, то имеется всего четыре монома Жегалкина вес которых не превосходит единицы: x_i (вес 1), x_{i-1} (вес $\frac{1}{2}$), x_{i-2} (вес $\frac{1}{4}$) и $x_{i-1}x_{i-2}$ (вес $\frac{3}{4}$). (Здесь мы пользуемся тем, что степень монома Жегалкина по каждой переменной не превосходит единицы.) Следовательно, имеется 2^4 многочленов веса не больше единицы. Таким образом, алгебра $F_{1,8}$ состоит из шестнадцати элементов. Например, алгебраическая функция, соответствующая многочлену Жегалкина $x_i \oplus x_{i-1}x_{i-2}$ имеет вид

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

(поскольку биты с отрицательными номерами считаются нулевыми). Другими словами,

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

Теорема 1 позволяет построить следующий простой

АЛГОРИТМ, выясняющий по данной функции $f\colon \mathbb{Z}_{2^\varkappa}^k \to \mathbb{Z}_{2^\varkappa}$, является ли она алгебраической (то есть выражается ли она через `ADD` и `XOR`).

1. Записать старший бит $(f(x,y,\ldots))_{\varkappa-1}$ значения функции f в виде многочлена Жегалкина $g_{\varkappa-1}(x_0, y_0, \ldots, x_1, y_1, \ldots)$ от битов аргументов и проверить, что вес этого многочлена (для $i = \varkappa - 1$) не превосходит единицы и свободный член нулевой. Если вес больше или свободный член ненулевой, то завершить программу с ответом `НЕТ`.
2. Сделать в многочлене $g_{\varkappa-1}$ следующие подстановки:

$$x_0 \to 0,\ x_1 \to x_0,\ x_2 \to x_1, \ldots,\ x_{\varkappa-1} \to x_{\varkappa-2},\ y_0 \to 0,\ y_1 \to y_0,\ y_2 \to y_1, \ldots,\ y_{\varkappa-1} \to y_{\varkappa-2}, \ldots \qquad (**)$$

   и проверить, совпадает ли полученный многочлен $g_{\varkappa-2}$ с многочленом, задающим $(\varkappa-2)$-й бит функции f. Если нет, то завершить программу с ответом `НЕТ`; если да, то продолжить.

$$\ldots \quad \ldots \quad \ldots$$

$\varkappa - 1$. Сделать в многочлене g_2 подстановки $(**)$ и проверить, совпадает ли полученный многочлен g_1 с многочленом, задающим первый бит функции f. Если нет, то завершить программу с ответом `НЕТ`; если да, то продолжить.

$\varkappa$. Сделать в многочлене g_1 подстановки $(**)$ и проверить, совпадает ли полученный многочлен g_0 с многочленом, задающим младший бит функции f. Если нет, то завершить программу с ответом `НЕТ`; если да, то завершить программу с ответом `ДА`.

Понятно, что этот алгоритм легко сделать однородным по $\varkappa$.

Например, функция умножения двух чисел по модулю q не выражается через `ADD` и `XOR` (наш алгоритм оборвётся на первом шаге из-за условия на вес), что, конечно, неудивительно. Однако функция одного аргумента $x \mapsto xy$ при каждом фиксированном $y \in \mathbb{Z}_q$ является алгебраической, как уже отмечалось.

Доказательство теоремы 1 конструктивное и оно даёт некоторый алгоритм, позволяющий выразить данную функцию f через `ADD` и `XOR` (при условии, что она выражается), но этот алгоритм далеко не такой простой и быстрый.

Пример 1 нетрудно обобщить, пересчитав мономы при произвольных q и k, и получить следующее утверждение.

Следствие 1. *Свободная алгебра $F_{k,q}$ состоит из*

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

элементов.

Доказательство. В случае $k = 1$ имеется ровно $\frac{q}{2}$ мономов веса не больше единицы. Действительно, в силу однозначности двоичного разложения числа существует ровно один моном каждого веса $s\cdot\frac{2}{q}$, где $s \in \{1, 2, \ldots, \frac{q}{2}\}$. А именно, моном

$$x_{i-l_1}x_{i-l_2}\ldots x_{i-l_p}, \quad \text{где} \quad s = 2^{\varkappa-1-l_1} + 2^{\varkappa-1-l_2} + \ldots + 2^{\varkappa-1-l_p}, \quad \text{а } 2^\varkappa = q.$$

Отсюда следует, что число мономов веса не больше единицы при произвольном целом k совпадает с числом ненулевых наборов неотрицательных целых чисел $(n_1, \dots, n_k)$, сумма которых не превосходит $\frac{q}{2}$ (здесь, $n_i \cdot \frac{2}{q}$ — это вес относительно i-й переменной). Количество таких наборов, как известно, равно

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

Значит, общее количество многочленов веса не больше единицы задаётся формулой (1).

Следующее утверждение представляет собой переформулировку теоремы 1.

Теорема 1′. *Функция $f\colon A_q^k \to A_q$ является алгебраической тогда и только тогда, когда она может быть записана в виде*

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

где для каждого i имеет место неравенство $2^{-k_{i,1}} + 2^{-k_{i,2}} + \dots + 2^{-l_{i,1}} + 2^{-l_{i,2}} + \dots \leqslant 1$.

Здесь и далее символ $\odot$ обозначает побитовое умножение по модулю два (конъюнкцию).

Что касается тождеств, в первую очередь можно заметить, что относительно каждой из операций $+$ и $\oplus$ алгебра A_q является абелевой группой экспоненты q и 2, соответственно. Поэтому все тождества, включающие только одну из двух операций являются следствиями следующей системы тождеств:

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

С тождествами, включающими обе операции, дело обстоит сложнее. Простейшим примером такого рода может служить тождество $qx = x \oplus x$, выражающее тот факт, что нулевые элементы двух групповых структур совпадают. Менее тривиальный пример тождества выглядит так: $\frac{q}{2}(x+y) = \frac{q}{2}(x \oplus y)$ (это тождество выражает то, что сложения $+$ и $\oplus$ совпадают в младшем бите).

Теорема 2. *Для любой целой степени двойки q алгебра A_q обладает конечным базисом тождеств. Более того, алгебра A_q порождает шпехтово многообразие.**)

Конечность алгебры сама по себе не влечёт конечности базиса её тождеств. Конечным базисом тождеств обладает каждая конечная группа [ОаРо64] (см. также [Нейм69]), каждое конечное ассоциативное или лиево кольцо ([Льво73], [Kruse73], [БаОл75]), но не каждая конечная полугруппа и не каждое конечное кольцо (см. [БаОл88]).

Для доказательства теоремы 2 мы используем не столько конечность, сколько хорошо известные соображения нильпотентности. Например, известно, что конечным базисом тождеств обладает всякое нильпотентное кольцо (то есть кольцо, в котором все достаточно длинные произведения равны нулю) и всякая нильпотентная группа (то есть группа, в которой все достаточно длинные кратные коммутаторы равны единице) (см. [Нейм69]). Алгебра A_q не является конечно же ни группой, ни кольцом. Однако оказывается, что эта алгебра *рационально эквивалентна* (в смысле Мальцева) некоторому нильпотентному кольцу, то есть на алгебре A_q можно ввести структуру нильпотентного кольца так, что сложение и умножение кольца будут выражаться через операции $+$ и $\oplus$ и наоборот: операции $+$ и $\oplus$ будут выражаться через сложение и умножение этого кольца.

Теорема 3. *Алгебра A_q рациональна эквивалентна нильпотентному коммутативному неассоциативному кольцу $(\mathbb{Z}_q, \oplus, \circ)$. Сложение $\oplus$ есть обычное побитовое сложение по модулю два, умножение $\circ$ определяется следующей формулой $x \circ y = 2(x \odot y)$, где $\odot$ — побитовое умножение по модулю два (конъюнкция), а умножение на два есть умножение на два по модулю q, то есть сдвиг разрядов.*

В следующем параграфе мы доказываем теорему 1. В параграфе 3 мы доказываем теорему 3, из которой теорема 2 немедленно вытекает в силу упомянутой выше конечной базируемости тождеств нильпотентных колец.

---

*) Это значит, что любая алгебра сигнатуры $(+, \oplus)$, в которой выполнены все тождества алгебры A_q, имеет конечный базис тождеств.

2. Доказательство теоремы 1

Коммутатором элементов $x, y \in A_q$ назовем элемент $[x, y] \overset{\text{опр}}{=} x \oplus y \oplus (x + y)$. Коммутатор представляет собой разницу между суммой $\oplus$ и суммой $+$ двух элементов; i-й бит коммутатора $[x, y]$ — это перенос в i-й разряд при суммировании $x + y$ «в столбик».

Следующая хорошо известная лемма широко используется в электронных сумматорах.

Утверждение 1. *Для битов коммутатора имеет место равенство*

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

Доказательство. Перенос $c_i = [x, y]_i$ в i-й разряд образуется следующим образом:

$$c_i = \begin{cases} 1, & \text{если среди трёх битов } x_{i-1}, y_{i-1}, c_{i-1} \text{ большинство (то есть два или три) составляют единицы;} \\ 0, & \text{если среди трёх битов } x_{i-1}, y_{i-1}, c_{i-1} \text{ большинство составляют нули.} \end{cases}$$

В виде многочлена Жегалкина эта булева функция записывается так:

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

что и требовалось.

Формулу (2) можно переписать в виде $[x, y] = 2(x \odot y \oplus [x, y] \odot (x \oplus y))$ или (воспользовавшись дистрибутивностью умножения на двойку относительно $\odot$ и $\oplus$ и дистрибутивностью $\odot$ относительно $\oplus$) в виде

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

С помощью формулы (2) нетрудно показать, что i-й бит суммы $x + y = x \oplus y \oplus [x, y]$ записывается в виде многочлена Жегалкина от битов слагаемых следующим образом:

$$(x + y)_i = x_i \oplus y_i \oplus x_{i-1}y_{i-1} \oplus x_{i-1}x_{i-2}y_{i-2} \oplus y_{i-1}x_{i-2}y_{i-2} \oplus \ldots = \textit{сумма всех мономов веса } 1. \tag{2$''$}$$

Приступим к доказательству теоремы 1. Пусть M — множество всех функций $A_q^k \to A_q$ вида $(*)$. Необходимо доказать два утверждения.

1. Любая функция из $F_{k,q}$ принадлежит M;
2. Любая функция из M принадлежит $F_{k,q}$.

Первое утверждение проверяется непосредственно. Функции $f(x, y, \ldots) = x$, $f(x, y, \ldots) = y, \ldots$ принадлежат M, так как соответствующие многочлены Жегалкина x_i, $y_i, \ldots$ имеют вес один. Допустим, что функции $f(x, y, \ldots)$ и $g(x, y, \ldots)$ лежат в M, то есть

$$(f(x, y, \ldots))_i = F(x_i, y_i, \ldots; x_{i-1}, y_{i-1}, \ldots; \ldots), \quad (g(x, y, \ldots))_i = G(x_i, y_i, \ldots; x_{i-1}, y_{i-1}, \ldots; \ldots),$$

где F и G — многочлены Жегалкина веса не больше единицы и без свободного члена. Тогда

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

и вес многочлена Жегалкина, стоящего в правой части этого равенства, не превосходит, стало быть, единицы, то есть $f \oplus g \in M$. Для функции $f + g$ i-й бит, согласно формуле $(2'')$, записывается следующим образом:

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

где многочлен H' получается из многочлена $H = H(x_i, y_i, \ldots; x_{i-1}, y_{i-1}, \ldots; \ldots)$, сдвигом всех битов:

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

Вес многочлена H' по крайней мере вдвое меньше, чем вес многочлена H. Поэтому вес многочлена

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

не превосходит единицы и $f + g \in M$.

Оставшаяся часть параграфа посвящена доказательству второго утверждения.

Кратные коммутаторы сложности n определим индуктивно как следующие формальные выражения от переменных $x, y, \ldots$:

каждую из этих переменных будем считать кратным коммутатором сложности 1;

выражение $[u, v]$ назовём кратным коммутатором сложности n, если выражения u и v являются кратными коммутаторами и сумма их сложностей есть n.

Очевидная индукция показывает, что кратный коммутатор равен нулю, если хотя бы одна из переменных, входящих в него, равна нулю.

Глубину $d(w)$ кратного коммутатора w также определим индуктивно:

$d(x) = 0$, если x — переменная;

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

Например, кратный коммутатор $[[x, y], [[z, t], x]]$ имеет сложность 5 и глубину 3.

Лемма 1. *В кратном коммутаторе биты с номерами, меньшими чем его глубина, равны нулю.*

Доказательство. Индукция по глубине. При глубине 1 утверждение верно. Если в кратных коммутаторах u и v равны нулю $d(u)$ и $d(v)$ младших битов, соответственно, то по формуле (2) мы получаем, в $[u, v]$ равны нулю $\max(d(u), d(v)) + 1$ младших битов, что и требовалось.

Лемма 2. *Кратный коммутатор сложности $\geqslant 2^n$ имеет глубину не меньше n.*

Доказательство. Докажем это индукцией по n. Действительно, кратный коммутатор сложности 1 (то есть переменная) имеет глубину 0. Кратный коммутатор w сложности $\geqslant 2^n$, где $n \geqslant 1$, имеет вид $w = [u, v]$. При этом хотя бы хотя бы один из кратных коммутаторов u или v имеет сложность $\geqslant 2^{n-1}$ (иначе у w сложность была бы меньше 2^n). По предположению индукции, глубина этого кратного коммутатора не меньше $n-1$, а это значит, что глубина w не меньше n по определению глубины.

Лемма 3. *В A_q любой кратный коммутатор сложности $\geqslant q$ равен нулю.*

Доказательство. По лемме 2 глубина такого кратного коммутатора не меньше $\log_2 q$ и, следовательно, по лемме 1 все биты этого кратного коммутатора нулевые.

Доказательство теоремы 1$'$. Достаточно доказать, что произвольное выражение

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

выражается через операции $\oplus$ и $+$. Мы будем доказывать более общий факт: *всякое выражение вида*

$$f = (2^k u) \odot (2^l v) \odot (2^m w) \odot \ldots, \quad \textit{где } 2^{-k} + 2^{-l} + 2^{-m} + \ldots \leqslant 1, \textit{ а } u, v, w, \ldots \textit{ — кратные коммутаторы} \tag{3}$$

(а не только переменные), выражается через операции $\oplus$ и $+$ (от переменных).

Допустим противное. Тогда найдётся выражение вида (3), не выражающихся через $\oplus$ и $+$, и в котором неравенство превращается в равенство:

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

Это следует из того, что $1 - (2^{-k} + 2^{-l} + 2^{-m} + \ldots)$ представляет собой дробь вида $\frac{s}{2^k}$, где k — максимальное из чисел $k, l, m, \ldots$, а значит выражение

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

задаёт ту же функцию, что f, но неравенство превращается в равенство. Заметим, что $2x = [x, x]$ и, следовательно, $2^k u$ есть кратный коммутатор, если u есть кратный коммутатор.

Выберем из всех неалгебраических (не выражающихся через $\oplus$ и $+$) выражений (3), удовлетворяющих равенству (4), минимальные по числу сомножителей, а из всех минимальных по числу сомножителей выражений, выберем выражение с максимальной суммарной сложностью коммутаторов $u, v, w, \ldots$. Такое выражение f существует по лемме 3.

Число сомножителей в этом выражении, разумеется, больше единицы, так как кратный коммутатор выражается через $\oplus$ и $+$ по определению. Далее, из равенства (4) следует, что два самых больших среди показателей $k, l, m, \ldots$ равны. Будем считать, что $k = l$.

Воспользовавшись тождеством (2$'$), мы получаем

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

Следовательно, выражение (3) переписывается в виде суммы трёх слагаемых:

$$f = \Big((2^{k-1}t) \odot (2^m w) \odot \ldots\Big) \oplus \Big((2^k t) \odot (2^k u) \odot (2^m w) \odot \ldots\Big) \oplus \Big((2^k t) \odot (2^k v) \odot (2^m w) \odot \ldots\Big), \quad \text{где } t = [u, v].$$

Каждое из этих слагаемых удовлетворяет равенству (4).

Первое слагаемое алгебраическое, так как его длина меньше, чем у исходного выражения f, которое по построению является минимальным по длине среди неалгебраических выражений (3), удовлетворяющих равенству (4).

Второе и третье слагаемые имеют ту же длину, что f, но их сложность больше (так как сложность коммутатора $t = [u, v]$ на единицу больше суммы сложностей u и v). Следовательно, они также являются алгебраическими по выбору f. Таким образом, выражение f алгебраично, как сумма трёх алгебраических слагаемых. Полученное противоречие завершает доказательство теоремы 1$'$ (а значит, и теоремы 1).

3. Доказательство теорем 3 и 2

Для доказательства теоремы 3 заметим, что алгебра $\mathbb{Z}_q$ с операциями $\oplus$ и $\circ$ действительно является нильпотентным коммутативным неассоциативным кольцом. Коммутативность умножения $\circ$ очевидны, дистрибутивность умножения относительно сложения $\oplus$ — тоже, нильпотентность также имеется: $((\ldots(x\circ y)\circ z)\circ\ldots=0$, если число сомножителей не меньше $\log_2 q$. Заметим, что ступень нильпотентности этого кольца обычно больше, чем $\log_2 q$, но она не превосходит q, то есть произведение любых q элементов (с любой расстановкой скобок) равно нулю. Это доказывается аналогично лемме два (глубина не меньше логарифма от длины для любой расстановки скобок).

Умножение $x\circ y=2(x\odot y)=(2x)\odot(2y)$ выражается через $+$ и $\oplus$ по теореме $1'$. Осталось доказать, что сложение $+$ выражается через кольцевые операции $\oplus$ и $\circ$.

Заметим, что сложение $+$ выражается через коммутатор и $\oplus$ (по определению коммутатора): $x+y=x\oplus y\oplus[x,y]$. Поэтому достаточно выразить коммутатор через $\oplus$ и $\circ$.

Лемма 4. *Для любого натурального k коммутатор $[x,y]$ может быть записан в виде*

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

где f_k — многочлен (в смысле умножения $\circ$ и сложения $\oplus$). Здесь и далее мы считаем, что в кратных произведениях все скобки сдвинуты влево, например, $a\circ b\circ c\circ d\overset{\text{опр}}{=}((a\circ b)\circ c)\circ d$.

Доказательство. При $k=1$ нужное разложение даёт тождество $(2')$:

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

Далее по индукции: имея при некотором k тождество (5), мы подставляем в его правую часть тождество (6) и получаем

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

что и требовалось.

Применяя лемму 4 при $k=\log_2 q$ и пользуясь нильпотентностью кольца, мы получаем выражение коммутатора через $\oplus$ и $\circ$, а именно, $[x,y]=f_{\log_2 q}(x,y)$. Теорема 3 доказана.

Теорема 2 немедленно вытекает из теоремы 3 и следующего хорошо известного утверждения.

Теорема (см. [БаОл88]). *Каждое нильпотентное кольцо обладает конечным базисом тождеств.*

Замечание. Доказательство теоремы о конечной базируемости тождеств нильпотентного кольца показывает, что все тождества такого кольца следуют из тождеств, включающих не более n переменных, где n — степень нильпотентности, то есть такое число, что все произведения n элементов (с любой расстановкой скобок) равны нулю. Это влечёт следующий факт:

Следствие 2. *Все тождества алгебры A_q следуют из тождеств, зависящих от не более чем q элементов. Существует алгоритм, который по любому числу $q=2^{\varkappa}$ выписывает конечный базис тождеств алгебры A_q.*

Этот базис представляет собой просто таблицы сложения (для $+$ и $\oplus$) свободной алгебры $F_{q,q}$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[OA91] Артамонов В. А., Салий В. Н., Скорняков Л. А., Шеврин Л. Н., Шульгейфер Е. Г. Общая алгебра, Т.2, М.: Наука, 1991.

[БаОл75] Бахтурин Ю. А., Ольшанский А. Ю. Тождественные соотношения в конечных кольцах Ли, Матем. сб., 96(138):4 (1975), 543-559.

[БаОл88] Бахтурин Ю. А., Ольшанский А. Ю. Тождества, Алгебра-2, Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления, 18, ВИНИТИ, М., 1988, 117-240.

[Бело99] Белов А. Я. О нешпехтовых многообразиях, Фундамент. и прикл. матем., 5:1 (1999), 47-66.

[ВаЗе89] Вайс А. Я., Зельманов Е. И. Теорема Кемера для конечно порожденных йордановых алгебр, Изв. вузов. Сер. матем., 1989, 6, 63-72.

[Гриш99] Гришин А. В. Примеры не конечной базируемости Т-пространств и Т-идеалов в характеристике 2, Фундамент. и прикл. матем., 5:1 (1999), 101-118.

[Зайц78] Зайцев М. В. О конечной базируемости многообразий алгебр Ли, Матем. сб., 106(148) (1978), 499-506.

[Keme87] Кемер А. Р. Конечная базируемость тождеств ассоциативных алгебр, Алгебра и логика, 26:5 (1987), 597-641.

[Крас90] Красильников А. Н. О конечности базиса тождеств групп с нильпотентным коммутантом, Изв. АН СССР. Сер. матем., 54:6 (1990), 1181-1195.

[Латы73] Латышев В. Н. О некоторых многообразиях ассоциативных алгебр, Изв. АН СССР. Сер. матем., 37:5 (1973), 1010-1037.

[Льво73] Львов И. В. О многообразиях ассоциативных колец, I, Алгебра и логика, 12 (1973), 269-297.

[Нейм69] Нейман Х. Многообразия групп. - М.: Мир, 1969.

[Ольш89] Ольшанский А. Ю. Геометрия определяющих соотношений в группах. М.: Наука, 1989.

[Щиго99] Щиголев В. В. Примеры бесконечно базируемых Т-идеалов, Фундамент. и прикл. матем., 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.