Math-Net.Ru

Общероссийский математический портал

Д. М. Мотин, О тождественных преобразованиях внутри коммутативных полу-
групп, *Дискрет. матем.*, 2007, том 19, выпуск 4, 139–149

DOI: <https://doi.org/10.4213/dm983>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.84.234.179

26 апреля 2023 г., 17:26:20

О тождественных преобразованиях внутри коммутативных полугрупп

© 2007 г. Д. М. Мотин

Доказано, что сложность перевода друг в друга равных термов длины не большей, чем n , над любой коммутативной полугруппой имеет порядок $n \log n$.

1. Введение

Тождественные преобразования формул, порожденных конечным набором булевых функций, играют важную роль в приложениях и, прежде всего, в разработке процессоров. В общем виде задача сложности тождественных преобразований не решена. В статье исследуется эта задача для термов, порожденных одной коммутативной ассоциативной бинарной операцией над некоторым множеством, которое с указанной операцией составляет некоторый объект, называемый коммутативной полугруппой.

Показывается, что для любой коммутативной полугруппы существует конечная полная система тождеств и любую пару равных термов длины (число знаков групповой операции в терме) не более, чем n , можно перевести друг в друга за число шагов, имеющее порядок $n \log n$, и за меньшее число шагов в общем случае указанный перевод невозможен. Кроме того, дополнительным результатом является новое доказательство существования конечной полной системы тождеств для коммутативных полугрупп.

2. Основные понятия и результаты

Пусть M — произвольное множество, $f(\cdot, \cdot)$ — бинарная операция над множеством M со значениями в M , обладающая свойствами ассоциативности и коммутативности. Пара (M, f) называется коммутативной полугруппой.

Для множества переменных $U = \{u_1, u_2, \dots, u_n, \dots\}$ над M и бинарной операции f над M систему $\Phi = \langle M, f, U \rangle$ назовем сигнатурой.

Определим термы над сигнатурой Φ :

- (1) любая переменная из U — терм,
- (2) если a_1, a_2 — термы, то $f(a_1, a_2)$ — терм над Φ ,

Класс всех термов над полугруппой $M = M(M, f)$ обозначим через $\langle f \rangle$. Термам индуктивно приписываем отображения над M , порожденные f , и называем их суперпозициями над M . Класс всех таких отображений обозначаем через $[f]$ и называем замыканием операции f .

Два термина называются равными, если они реализуют (им приписано) одно и то же отображение.

Далее под тождеством будем понимать запись вида $A = B$, где A и B — равные термины. Мерой $|A|$ термина A над (M, f) назовем число входящих в него символов f .

Пусть $M = M(M, f)$ — некоторая коммутативная полугруппа, а I — некоторая конечная система тождеств, $I = \{a_1 = b_1, a_2 = b_2, \dots, a_i = b_i\}$ над M , где $a_1, b_1, a_2, b_2, \dots, a_i, b_i \in \langle f \rangle$.

Система тождеств I над M называется полной, если для любых термов a и b над множеством M их равенство эквивалентно возможности получить из a терм b (и наоборот) с помощью конечного числа эквивалентных преобразований, осуществляемых тождествами из I .

Как показал П. Перкинс [1], для любой коммутативной полугруппы существует конечная полная система тождеств.

Далее будут рассматриваться только конечные полные системы тождеств. Для равных термов A и B из $\langle f \rangle$ обозначим через $L_f^I(A, B)$ наименьшее возможное число применений тождеств из I при переводе A и B друг в друга, и пусть

$$L_f^I = \max_{\substack{|A|, |B| \leq n \\ A=B}} L_f^I(A, B).$$

Таким образом, функция L_f^I характеризует сложность перевода произвольных равных термов A и B над $\langle f \rangle$ меры не более, чем n , друг в друга с помощью системы тождеств I .

Пусть $f(x, y) = (x \circ y)$ — операция, при которой M является коммутативной полугруппой. Далее установим справедливость следующих вспомогательных утверждений.

Лемма 1. Если $A, B \in \langle (x \circ y) \rangle$, $|A| \leq n$ и A отличается от B только расстановкой скобок, то с помощью ассоциативного тождества из A можно получить B со сложностью не более, чем $2n$.

Лемма 2. Если $A, B \in \langle (x \circ y) \rangle$, $|A| \leq n$, $A = B$, A состоит из тех же переменных и в том же количестве, что и B , то, используя тождества ассоциативности и коммутативности, из A можно получить B со сложностью не более, чем $6(n+1) \log(n+1)$.

Лемма 3. Существуют $A, B \in \langle (x \circ y) \rangle$, $|A| \leq n$, $A = B$, причем A состоит из тех же переменных и в том же количестве, что и B , такие что, используя тождества ассоциативности и коммутативности, мы можем получить из A терм B со сложностью не меньшей, чем $(n \log n)/20$.

Эти леммы понадобятся нам для обоснования следующего итогового результата.

Теорема 1. Пусть $M = (M, f)$ — конечная полугруппа, тогда для M существует конечная полная система тождеств (явно описывается некоторая система тождеств) и для любой полной системы тождеств I для M при $n \rightarrow \infty$ функция $L_f^I(n)$ имеет порядок, равный $n \log n$.

3. Подготовительные замечания

Легко видеть, что если терм $A \in \langle (x \circ y) \rangle$, то он в своей записи содержит $|A| + 1$ переменных (с учетом кратности их вхождения).

Пусть $A, B \in \langle (x \circ y) \rangle$, $|A| \leq n$, $|B| \leq n$, $A = B$ и A', B' — термы, полученные из термов A, B переименованием их переменных в переменные из множества $\{x_1, x_2, \dots, x_{2n+2}\}$ (одинаковые переменные переименовываются в одинаковые). Ясно, что переход, состоящий из последовательности тождеств из I (I — некоторая система тождеств), для получения из A терма B является также переходом от A' к B' и наоборот. Следовательно, функция $L_f^I(n)$ не изменится, если в ее определении мы будем брать максимум только по тем термам $A, B \in \langle f \rangle$, $A = B$, $|A| \leq n$, $|B| \leq n$, в записи которых встречаются только переменные из множества $\{x_1, x_2, \dots, x_{2n+2}\}$. Так что дальше будем считать, что рассматриваемые термы размера не более n зависят только от переменных из $\{x_1, x_2, \dots, x_{2n+2}\}$. Также введем обозначение $I^* = \{(x \circ y) = (y \circ x), ((x \circ y) \circ z) = (x \circ (y \circ z))\}$ и термы вида $(x_{i_1} \circ (x_{i_2} \circ (x_{i_3} \circ (\dots (x_{i_{k-2}} \circ (x_{i_{k-1}} \circ x_{i_k})) \dots))))$, где $i_1 \leq i_2 \leq i_3 \leq \dots \leq i_{k-1} \leq i_k$, $k \geq 1$, назовем каноническими.

4. Доказательство леммы 1

Рассмотрим в A подтерм вида $(C_1 \circ D_1)$, где C_1 — некоторый подтерм в A , а D_1 — крайняя справа переменная в A .

Возможны следующие ситуации.

- (а) C_1 — переменная, тогда полагаем $D_2 = (C_1 \circ D_1)$ и рассматриваем новый подтерм в A вида $(C_2 \circ D_2)$ (если такого подтерма C_2 нет, то получили канонический вид).
- (б) $C_1 = (K \circ L)$, где L — переменная, тогда за одну операцию из I^* переходим к подтерму вида $(K \circ (L \circ D_1))$ и полагаем $D_2 = (L \circ D_1)$, $C_2 = K$.
- (в) $C_1 = (K \circ L)$, где L — подтерм, не являющийся переменной, тогда за одну операцию переходим к $(K \circ (L \circ D_1))$ и полагаем $D_2 = D_1$, $C_2 = L$.

Далее рассматриваем подтерм $(C_2 \circ D_2)$. Для подтерма $(C_2 \circ D_2)$ применяем те же действия и т. д.

На k -м шаге имеем подтерм вида $(C_k \circ D_k)$, где C_k — некоторый подтерм в A , а D_k — подтерм, представляющий собой каноническую расстановку скобок для некоторого крайнего справа набора переменных в A .

Опять возможны следующие ситуации.

- (а) C_k — переменная, тогда полагаем $D_{k+1} = (C_k \circ D_k)$ и рассматриваем новый подтерм в A вида $(C_{k+1} \circ D_{k+1})$ (если такого подтерма C_{k+1} нет, то получили канонический вид).
- (б) $C_k = (K \circ L)$, где L — переменная, тогда за одну операцию из I^* переходим к подтерму вида $(K \circ (L \circ D_k))$ и полагаем $D_{k+1} = (L \circ D_k)$, $C_{k+1} = K$.
- (в) $C_k = (K \circ L)$, где L — подтерм, не являющийся переменной, тогда за одну операцию переходим к $(K \circ (L \circ D_k))$ и полагаем $D_{k+1} = D_k$, $C_{k+1} = L$.

Далее рассматриваем подтерм $(C_{k+1} \circ D_{k+1})$.

В итоге мы получим каноническую расстановку скобок. Ясно, что к этой же расстановке мы таким же образом можем привести и терм B . В обоих случаях, очевидно, что нам потребуется применить не более, чем n тождеств из I^*

Лемма доказана.

5. Доказательство леммы 2

Рассмотрим следующий алгоритм приведения произвольного терма $A \in \langle (x \circ y) \rangle$, $|A| \leq n$, к каноническому виду.

Не нарушая общности, будем считать, что A содержит ровно по одному разу переменные $x_1, x_2, \dots, x_k, x_{k+1}$, $k \leq n$ (одинаковые переменные можем нумеровать соседними индексами). Также для облегчения изложения будем считать, что $k = 2^h - 1$ для некоторого натурального h .

По лемме 1 можно за не более, чем $2n$ операций привести терм A к расстановке скобок (порядок переменных не меняется) $(\dots (((x_{i_1} \circ x_{i_2}) \circ (x_{i_3} \circ x_{i_4})) \circ ((x_{i_5} \circ x_{i_6}) \circ (x_{i_7} \circ x_{i_8}))) \circ \dots)$, т.е. сначала скобки наложены на пары последовательных переменных, затем такие пары последовательно сгруппированы по две и т.д.

Дальнейшие действия разобьем на следующие этапы.

- (1) Для каждой пары переменных $(x_{i_{2m-1}} \circ x_{i_{2m}})$ такой, что $i_{2m-1} > i_{2m}$, применим коммутативное тождество из I^* всего не более, чем $(k+1)/2$ раз.
- (2) Для каждой пары следующего уровня вложенности, т.е. пары вида $((x_{i_{2m-1}} \circ x_{i_{2m}}) \circ (x_{i_{2m+1}} \circ x_{i_{2m+2}}))$ применим следующий алгоритм.
 - (а) Если $i_{2m-1} \leq i_{2m+1}$, то переходим к $(x_{i_{2m-1}} \circ (x_{i_{2m}} \circ (x_{i_{2m+1}} \circ x_{i_{2m+2}})))$, если, далее, $i_{2m} > i_{2m+1}$, то переходим к $(x_{i_{2m-1}} \circ ((x_{i_{2m}} \circ x_{i_{2m+1}}) \circ x_{i_{2m+2}}))$, затем к $(x_{i_{2m-1}} \circ ((x_{i_{2m+1}} \circ x_{i_{2m}}) \circ x_{i_{2m+2}}))$, затем к $(x_{i_{2m-1}} \circ (x_{i_{2m+1}} \circ (x_{i_{2m}} \circ x_{i_{2m+2}})))$, кроме того, если $i_{2m} > i_{2m+2}$, то переходим к $(x_{i_{2m-1}} \circ (x_{i_{2m+1}} \circ (x_{i_{2m+2}} \circ x_{i_{2m}})))$ (здесь все индексы упорядочены по возрастанию).
 - (б) Если $i_{2m-1} > i_{2m+1}$, то переходим к $((x_{i_{2m+1}} \circ x_{i_{2m+2}}) \circ (x_{i_{2m-1}} \circ x_{i_{2m}}))$, а затем к пункту (а).

В обоих случаях потребовалось не более $3(2^2 - 1)$ операций.

Таких пар не более $(k+1)/4$, следовательно, чтобы упорядочить переменные во всех таких подтермах нужно не более $((k+1)/4)3(2^2 - 1)$ применений тождеств из I^* .

- (3) Переходим к следующему уровню вложенности $((x_{i_{2m-1}} \circ (x_{i_{2m}} \circ (x_{i_{2m+1}} \circ x_{i_{2m+2}}))) \circ (x_{i_{2m+3}} \circ (x_{i_{2m+4}} \circ (x_{i_{2m+5}} \circ x_{i_{2m+6}}))))$. Таких подтермов не более $(k+1)/2^3$, функций $\circ$ в каждом подтерме не более $(2^3 - 1)$ и на каждую $\circ$ нужно, как и раньше, не более 3 операций (переменные в каждом множителе упорядочены на предыдущем уровне), следовательно, на этом уровне для упорядочивания нужно не более $((k+1)/2^3)3(2^3 - 1)$ применений тождеств из I^* .

Аналогично проходим все оставшиеся слои вложенности (всего их $\log(k+1)$).

На первом шаге рассмотрим подтерм $((x_{i_{2m+1}} \circ (x_{i_{2m+2}} \circ (x_{i_{2m+3}} \circ \dots \circ (x_{i_{2m+2^l-1-1}} \circ x_{i_{2m+2^l-1}}) \dots))) \circ (x_{i_{2m+2^l-1+1}} \circ (x_{i_{2m+2^l-1+2}} \circ \dots \circ (x_{i_{2m+2^l-1}} \circ x_{i_{2m+2^l}}) \dots)))$. Таких подтермов не более $(k+1)/2^l$, функций $(x \circ y)$ в каждом подтерме не более $(2^l - 1)$, и на каждую $\circ$ нужно, как и раньше, не более 3 операций (переменные в каждом множителе упорядочены на предыдущем уровне), следовательно, на этом уровне для упорядочивания нужно не более $((k+1)/2^l)3(2^l - 1)$ применений тождеств из I^* .

В итоге мы приводим терм к каноническому виду. При этом мы использовали не более $3(k+1) \sum_{1 \leq m \leq \log(k+1)} ((2^m - 1)/2^m)$ операций, что равно

$$3(k+1) \log(k+1) + 2^{(-\log(k+1)-1)} - 1 = 3(k+1) \log(k+1) + 1/(2(k+1)) - 1 \leq 3(n+1) \log(n+1).$$

Следовательно, из того, что каждый терм можно привести к каноническому виду, и из единственности канонического терма (для данного набора переменных) вытекает, что достаточно не более $6(n+1) \log(n+1)$ применений тождеств для приведения некоторого терма к равному в условиях леммы.

Лемма доказана.

6. Доказательство леммы 3

Оценим число $N(m)$ термов из $\langle (x \circ y) \rangle$, содержащих m , $m \leq n$, символов функций $\circ$ и только переменные из множества $\{x_1, x_2, \dots, x_{m+1}\}$ по одному разу. Обозначим $N^{(m)}$ число возможных расстановок скобок в каждом терме, содержащем m символов функций $\circ$. Тогда справедлива зависимость

$$N^{(m)} = \sum_{i=0}^{m-1} N^{(i)} N^{(m-i-1)},$$

здесь каждое слагаемое соответствует выбору внешней функции $\circ$, и полагаем $N^{(0)} = 1$.

Рассмотрим производящую функцию (формальный ряд) вида

$$f(x) = \sum_{m=0}^{\infty} N^{(m)} x^m.$$

В силу вышеуказанной зависимости справедливо формальное равенство

$$f(x) = x f(x) f(x) + 1,$$

откуда получаем, что

$$f(x) = (1 - \sqrt{1 - 4x})/(2x) = - \sum_{m=1}^{\infty} ((-1)(-3) \dots (3 - 2m)(-4x)^m)/(2^m m! 2x),$$

откуда следует, что

$$N^{(m)} = \frac{(2m-1)!! 2^m}{(m+1)!} = \frac{(2m)! 2^m}{2^m m! (m+1)!} = \frac{(2m)!}{(m+1)! m!},$$

так как $(2m-1)!! = (2m)!/2^m m!$.

Все равенства были формальными. Теперь возьмем найденные коэффициенты $N^{(m)}$ и составим из них абсолютно сходящийся ряд $f(x)$. Такой ряд удовлетворяет уравнению $f(x) = x f(x) f(x) + 1$, откуда следует, что указанные коэффициенты удовлетворяют равенствам вида

$$N^{(m)} = \sum_{i=0}^{m-1} N^{(i)} N^{(m-i-1)}$$

(в силу единственности представления функции в виде степенного ряда).

Далее воспользуемся неравенствами, вытекающими из формулы Стирлинга,

$$\sqrt{2\pi nn^n} e^{-n} \leq n! \leq \sqrt{2\pi nn^n} e^{-n+1}.$$

Так как

$$\frac{m^m}{(m+1)^{m+1}} = (1 - 1/(m+1))^m / (m+1) \geq \frac{1}{2^m(m+1)}, \quad m \geq 1,$$

справедливо неравенство

$$N^{(m)} \geq 2^m / \sqrt{\pi(m+1)^3} e.$$

Кроме того, существует $m!$ возможных порядков переменных, следовательно,

$$N(m) \geq m! 2^m / \sqrt{\pi(m+1)^3} e \geq \frac{m^m 2^m \sqrt{2m}}{e^{m+1} \sqrt{(m+1)^3}}.$$

Обозначим $\leftrightarrow$ тождество из I^* , демонстрирующее коммутативность ($x \circ y = y \circ x$), а $()$ — тождество, показывающее ассоциативность $((x \circ y) \circ z = x \circ (y \circ z))$. Отметим, что применение $()$ к подчеркнутой $\circ$ означает переход

$$((A \circ B) \circ C) \longrightarrow (A \circ (B \circ C))$$

или, в другом случае,

$$(A \circ (B \circ C) \longrightarrow ((A \circ B) \circ C)).$$

Пусть $((K \circ L) \circ M)$ — подтерм некоторого терма над $(x \circ y)$, K, L, M из $\langle (x \circ y) \rangle$. При работе $()$ на конструкции $f = ((K \circ L) \circ M)$ происходит переход к $(K \circ (L \circ M))$, и очевидно, что этот переход никак не связан с изменениями внутренней структуры K, L, M и внешними (операции применяются к части терма вне f) изменениями, не меняющими f . Также $\leftrightarrow$ никак не влияет на внутреннюю структуру аргументов K и L функции, к которой применяется, и не влияет ни на какие части терма за пределами конструкции $(K \circ L)$.

Теперь рассмотрим подтерм вида

$$g = (((A \circ B) \circ (C \circ D)) \circ (E \circ F))$$

(допустим, что такой терм существует), где A, B, C, D, E, F — некоторые термы над $(x \circ y)$, и назовем подчеркнутую функцию выбранной. Из предыдущего абзаца следует, что воздействие $()$ или $\leftrightarrow$ на какой-либо символ $\circ$ за пределами g никак не повлияет на результат работы операций $()$, $\leftrightarrow$ над выбранной функцией, аналогично на выбранные преобразования не повлияет и действие наших операций внутри A, B, C, D, E, F , то есть действие операций $()$, $\leftrightarrow$ на символы функций из A, B, C, D, E, F и вне g (внешние функции) является коммутативным с воздействием на выбранную функцию (результат “вначале действуем на выбранную, потом на внешнюю функцию” равен результату “вначале действуем на внешнюю, потом на выбранную функцию”). Подтерм g обладает достаточной общностью, чтобы сказать, что для каждого символа функции в терме существует максимум 5 позиций функций (включая его самого), которые являются некоммутативными с ним.

Оценим число термов, которые можно получить из некоторого одного (например, канонического, содержащего n функций $\circ$ и только переменные из набора $\{x_1, x_2, \dots, x_{n+1}\}$ по одному разу) за k применений тождеств $()$ и $\leftrightarrow$.

Рис. 1.

Рис. 2.

Сначала рассмотрим случай $k \leq n$ и введем следующую конструкцию.

Приведенный ниже рис. 1 означает, что на первом шаге (применяя одно тождество) мы можем получить не более A новых различных термов, на втором шаге (ровно два тождества) не более $A(B + C)$ новых различных термов (B и C соответствуют некоторым различным ситуациям, которых может быть довольно большое число), на третьем — не более $A(B(D + E + F) + C(G + M))$ (то есть связи соответствуют умножению, а числа на одном горизонтальном уровне, связанные с некоторым одним вышестоящим числом, складываются; при этом мы движемся снизу вверх).

Далее, очевидно, что на первом шаге (применение одного тождества) мы не получим более $2n = m$ различных термов (n штук возможных $\leftrightarrow$ и n штук возможных $()$). На втором шаге возможен коммутативный случай, то есть вторая операция не применяется к указанным выше 5 случаям нарушения коммутативности, тогда число возможных вариантов не превосходит $(m - 10) \leq m$ (10 вариантов получаются из 2 видов операций $*$ на 5 позициях и $m = 2n$) для каждого терма из первого шага, и соответствующей вершине припишем $m/2$ (учитываем коммутативность). В некоммутативном случае, очевидно, имеется не более 10 ситуаций.

Таким образом, первые два уровня принимают вид, указанный на рис. 2.

Далее идем справа налево: для правой ветви можем попасть мимо полей некоммутативности уже ранее выбранных некоторых двух операций ($m/3$) или попасть в них (10 — в первую, построенную на первом уровне, и 10 — во вторую, появившуюся на втором). Для левой ветви $10/2$ попали в поле первой, но не второй операции и 10 попали в поле второй операции. Остальные возможности уже были рассмотрены в случае правой ветви.

Каждый новый уровень мы заполняем справа налево, для каждой вершины, вначале

рассматривая самый коммутативный случай (имеет дробный индекс) и продолжая по убыванию коммутативности, то есть сначала рассматриваем случай, когда проходим мимо полей некоммутативности, зачем случаи попадания в поля операций, построенных на ранних уровнях (начиная с первого) и, наконец, попадание в поле последней (вершинной) операции. Второй раз одну и ту же ситуацию не рассматриваем (если была справа, то ее отбрасываем).

Продолжая таким образом построение, строим k уровней.

Введем следующие обозначения, пусть N_i — число вершин на уровне t , N_t^2 — число двоек на уровне t , то есть число пар из вершин, которые соединены с некоторой одной вершиной на предыдущем уровне, причем с этой вершиной больше не соединена ни одна вершина на уровне t . Аналогично, N_t^3 — число троек на уровне t и так далее.

В дальнейшем любую вершину A нашей конструкции будем рассматривать двумя способами:

- (а) как некоторое множество преобразований (множество тождеств, применяемых к конкретным позициям функций), согласованное с другими преобразованиями, соответствующими вершинам вдоль пути от корня нашей конструкции к A , и будем обозначать это множество $[A]$;
- (б) как множество термов, которые можно получить из канонического терма, осуществляя преобразования, соответствующие вершинам вдоль пути от корня к A , и будем обозначаем его $\langle A \rangle$.

Докажем по индукции, что если A — вершина, соответствующая попаданию в поле некоммутативности своего родителя B , стоящего p уровней назад, то она породит на следующем уровне $p + 1$ вершину, которые отвечают преобразованиям полей некоммутативности вершин вдоль пути от A до B (по одной новой вершине на каждое поле).

Для уровней 1 и 2 это утверждение доказано при построении нашей конструкции.

Допустим, что оно доказано для уровня $t - 1$, тогда возьмем произвольную вершину G на уровне t и пусть $A_{t-1}, A_{t-2}, \dots, A_0 = \{\text{все возможные позиции функций}\}$ суть родители вершины G (индексы отображают уровень). Также предположим, что G соответствует воздействию на поле некоммутативности A_{t-p} , то есть является p -й дочерней вершиной для A_{t-1} .

Из вершины G выйдут вершины, соответствующие следующим случаям: попали в поле некоммутативности $P_1 = G$, в поля $P_2 = A_{t-1} \setminus G$, $P_3 = A_{t-2} \setminus \{G \cup A_{t-1}\}, \dots$, $P_{p+1} = A_{t-p} \setminus \{G \cup A_{t-1} \cup \dots \cup A_{t-p+1}\}$. Действительно, допустим из G выходит вершина K , соответствующая случаю непопадания в указанные поля, тогда из пути для K убираем применение операций из G (корректно в силу коммутативности операций из K и G). Получившаяся вершина M выходит правее из A (по построению) или из некоторой вершины на уровне t справа от A (если встретила раньше), значит ситуация K уже была (применяем операции $[G]$ к $\langle M \rangle$), а второй раз одинаковое (справа налево) построение мы не рассматриваем, получаем противоречие.

Далее, рассмотрим вершину, выходящую из G и попавшую в поле P_i . Если что-либо поменять в пути для G с сохранением результата $\langle G \rangle$, то, по построению, в месте первого изменения мы уйдем влево от исходного пути (так как второй раз одинаковую ситуацию справа налево не рассматриваем, а вершина G существует).

Допустим, что результат $\langle P_i \rangle$ встретился раньше справа от соответствующей ветки из G (правый путь с концом M). В силу того, что на поле вершины P_i ничего не воздействует на предыдущих уровнях, то какой бы путь, сохраняющий результат $\langle P_i \rangle$, мы ни рассматривали, всегда можно корректно переставить операции, соответствующие вершине P_i , в

Рис. 3.

конец или совсем их убрать (конечно результат новой цепочки будет совсем другим). В силу всего вышесказанного исходный путь для P_i и правый путь разветвляются только с помощью вершины P_i так, как показано на рис. 3.

Если $i = 1$, то $[P_i]$ действует на $\langle G \rangle$, то есть $X = G$, но G появляется только на уровне t (иначе уходим влево), поэтому $P_i = M$.

Если $i \neq 1$, то так как $[G]$ действует на $A_{t-p} \setminus \{A_{t-1} \cup \dots \cup A_{t-p+1}\}$, а $[P_i]$ — на $A_{t-i+1} \setminus \{G \cup A_{t-1} \cup \dots \cup A_{t-p+2}\}$, $i \leq p$, то, если в правом пути поменять P_i и G местами (возможно в силу коммутативности), то ветвление останется также в правую сторону. Теперь, если из правой ветки убрать вершину P_i , то результат $\langle G \rangle$ окажется справа от исходного, получаем противоречие.

Таким образом, мы доказали, что

$$N_t = N_{t+2}^2, \quad N_t^2 = N_{t-1}^2 + N_{t-1}^3 + \dots + N_{t-1}^{t-2} + N_{t-1}^{t-1},$$

а также

$$N_t^i = N_{t-1}^{i-1} + N_{t-1}^i + \dots + N_{t-1}^{t-2} + N_{t-1}^{t-1}$$

для всех $3 \leq i \leq t$.

Очевидно, что $N_2^2 = 1 \leq 2^2 2^{2-2}$. Допустим, что для всех $h < t$ доказано неравенство $N_h^i \leq 2^h 2^{h-i}$, $2 \leq i \leq h$. Тогда для $2 \leq i \leq t$

$$\begin{aligned} N_t^i &= N_{t-1}^{i-1} + N_{t-1}^i + \dots + N_{t-1}^{t-2} + N_{t-1}^{t-1} \\ &\leq 2^{t-1} 2^{t-i} + 2^{t-1} 2^{t-i-1} + \dots + 2^{t-1} 2^1 + 2^{t-1} 2^0 \\ &= 2^{t-1} (2^{t-i+1} - 1) \leq 2^t 2^{t-i}. \end{aligned}$$

Таким образом, мы доказали, что $N_t = N_{t+2}^2 \leq 4^{t+1}$. Если раскрыть скобки в сумме, соответствующей дереву, то число слагаемых равно $N_k - 1$ и каждое слагаемое не превосходит $10^k m^k / k!$, откуда следует, что общая схема за k шагов задает не более, чем

$$\begin{aligned} k 10^k 4^{k+1} m^k / k! &= k 4 \cdot 80^k n^k / k! \leq \frac{4k 80^k n^k}{\sqrt{2\pi k k^k} e^{-k}} \\ &\leq 320^n e^n \frac{4k}{\sqrt{2\pi k}} \leq 320^n e^n 4n \leq 320^n e^n 4^n \end{aligned}$$

термов. Для произвольного $k \geq n$, число термов, очевидно, не превышает

$$((320e)^n)^{k/n+1} = (320e)^{k+n}.$$

Допустим, что k таково, что, применяя не более k тождеств из I^* , можно получить все возможные термы (для данного начального терма), тогда справедливо неравенство

$$(320e)^{k+n} \geq \frac{n^n 2^n \sqrt{2n}}{e^{n+1} (n+1)^{3/2}} \geq \frac{n^n \sqrt{2n}}{2^n e (n+1)^{3/2}}$$

(так как $2^m/e^m \geq 1/2^m$), откуда

$$k \geq (n \log_{320e}(n/2) + \log_{320e}(\sqrt{2n}) - \log_{320e}(\sqrt{(n+1)^3}) - 1 - n),$$

и таким образом, так как

$$\log_{320e}(n) = (\log n) / \log(320e) \geq (\log n) / 10,$$

при достаточно больших n

$$k \geq n(\log n) / 20.$$

Лемма доказана.

7. Доказательство теоремы

Рассмотрим случай, когда система всех тождеств полугруппы M тривиальна, то есть, если $s = t$, $s, t \in \langle f \rangle$, то термы s и t содержат одни и те же переменные, каждая из которых входит в s и t одинаковое число раз. Очевидно, что система I^* , состоящая из тождеств ассоциативности и коммутативности, в этом случае является полной системой тождеств и в силу доказанных лемм при $n \rightarrow \infty$ функция $L_f^{I^*}(n)$ имеет порядок, равный $n \log n$.

Рассмотрим второй случай, когда существуют натуральные числа m и k такие, что выполняется тождество

$$(x \circ (x \circ \dots \circ x) \dots)) = (x \circ (x \circ (x \circ \dots \circ x) \dots)),$$

где слева m одинаковых переменных, а справа $m + k$. Пусть m_0 — наименьшее среди таких m , а k_0 — наименьшее среди указанных k при фиксированном $m = m_0$.

Терм t назовем приведенным, если любая переменная входит в него менее $m_0 + k_0$ раз. Согласно доказанным леммам, можно сгруппировать нужным образом одинаковые переменные в произвольном терме за время порядка $n \log n$, а затем с помощью указанного выше тождества за линейное время понизить число вхождений переменных, чтобы терм превратился в приведенный. Таким образом, далее мы будем рассматривать только приведенные термы.

Множество $B = \{x_1, x_2, \dots, x_n\}$ будем называть p -блоком приведенного терма s , если любая переменная $x_i \in B$ входит в s ровно p раз. Множество B назовем (p, q) -блоком приведенного тождества $s = t$, если B есть p -блок для s и q -блок для t , причем из чисел p и q хотя бы одно не равно 0. Длиной блока B будем называть число n . Если для конкретных p и q тождество $s = t$, $s, t \in \langle f \rangle$, имеет какой-нибудь (p, q) -блок, то оно

имеет и (единственный) максимальный блок, содержащий все остальные (p, q) -блоки для $s = t$.

Предположим, что все пары (p, q) занумерованы, так что можно говорить о 1-блоке, 2-блоке, ..., r -блоке, где $r = (m_0 + k_0)^2 - 1$. Таким образом, произвольному тождеству $s = t$ мы можем сопоставить вектор длины r , в котором на i -м месте стоит длина максимального i -блока, сформировав тем самым некоторое множество векторов (наборов). Позиция i в произвольном векторе называется значимой, если там стоит ненулевое значение. Наборы называются подобными, если у них один и тот же набор значимых позиций.

Для каждой группы подобных наборов K (таких групп конечное число) выберем конечное подмножество векторов $L = L(K)$ так, что для любого $y \in K$ существует $z \in L(K)$ такое, что $z \leq y$. Из таких подмножеств L сформируем (просто объединяя подмножества) некоторую систему тождеств I^* , предварительно добавив туда тождества ассоциативности и коммутативности.

Нетрудно видеть, что I^* — конечная полная система тождеств. Действительно, для любого приведенного тождества $s = t$ рассмотрим соответствующий ему вектор y , в I^* выбираем тождество $p = q$ с подобным вектором $z \leq y$. Далее, очевидно, что подставляя в тождество $p = q$ вместо некоторых переменных линейные термы, мы можем превратить его в тождество, которое после перестановки скобок и переменных за число шагов порядка $n \log n$ позволяет мгновенно переходить от s к t . Например, если разница i -х позиций векторов z и y равна m , то вместо некоторой переменной, соответствующей i -му блоку, надо в тождество $p = q$ подставить терм вида $(x_{i_1} \circ (x_{i_2} \circ (x_{i_3} \circ \dots \circ x_{i_m}) \dots))$.

Таким образом, с помощью конечной полной системы I^* мы можем осуществлять преобразования равных термов за число шагов порядка $n \log n$ при достаточно больших n .

В обоих случаях, с помощью любой другой конечной системы тождеств I мы можем получить из левых частей тождеств I^* их правые части (и наоборот) за конечное число шагов, поэтому $L_f^I(n)$ имеет тот же порядок роста, что и эта же функция для I^* .

Теорема доказана.

Список литературы

1. Перкинс П., Базисы для эквивалентных теорий полугрупп. *Киберн. сб.* (1974) **11**, 14–17.
2. Lyndon R. C., Identities in two-valued calculi. *Trans. Amer. Math. Soc.* (1951) **71**, №3, 457–465.
3. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б., *Функции алгебры логики и классы Поста*. Наука, Москва, 1966.

Статья поступила 22.11.2005.