О тождественных преобразованиях внутри некоторых классов формул*

Д.Г. Мотин

В работе рассматривается порядок сложности перевода равных формул длины не более n над любым базисом, состоящим из одной коммутативной, ассоциативной и еще с одним ограничением на внутреннюю структуру функции k-значной логики от двух аргументов, друг в друга и показывается, что он имеет вид $n \log n$. Также рассмотрен вопрос о существовании конечных полных систем тождеств для аналогичных базисов без последнего ограничения на порождающую функцию.

Введение

Тождественные преобразования формул, порожденных конечным набором булевых функций, играют важную роль в приложениях и, прежде всего, в реальном синтезе процессоров.

В общем виде задача сложности тождественных преобразований не решена.

Здесь исследуется эта задача для класса Поста, построенного над базисом, состоящим из одной коммутативной, ассоциативной и обладающей «свойством 3» (то есть если $x \circ y$ — наша функция и $f(x)$, $g(y)$, $m(x)$, $n(y)$ — формулы над $\{x \circ y\}$, то из равенства формул $(f(x) \circ g(y)) = (m(x) \circ n(y))$ следует, что $f(x) = m(x)$ и $g(y) = n(y)$, а из равенства $(f(x) \circ g(y)) = m(x)$ — $f(x) = m(x)$ и $(x \circ g(y)) = x$; функции от двух аргументов. Показывается, что для любого базиса

*Работа выполнена при частичной поддержке РФФИ, грант № 02–01–00162.

такого типа существует конечная полная система тождеств, и что любую пару равных формул длины (число значков функции в формуле) не более 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 теорема, показывающая отсутствие необходимости в «свойстве 3» для существования конечной полной системы тождеств.

1. Основные понятия и результаты

Пусть $U = \{u_1, u_2, \dots, u_n, \dots\}$ — множество переменных со значениями в $E_k = \{0, 1, \dots, k-1\}$. Тогда для множества U, множества функциональных символов $F = \{f_1^{n_1}, f_2^{n_2}, \dots, f_k^{n_k}, \dots\}$, где индекс сверху соответствует арности, и множества функций k-значной логики $G = \{f_1^{n_1}, f_2^{n_2}, \dots, f_k^{n_k}, \dots\}$ систему $\Phi = \langle U, F, G\rangle$ назовем сигнатурой.

Определим формулы над сигнатурой Φ.

1) Если $f_i^{n_i} \in F$, то $f_i^{n_i}(x_1, x_2, \dots, x_{n_i})$ — формула, где $x_1, x_2, \dots, x_{n_i}$ — обозначения переменных из U.
2) Если $f_i^{n_i} \in F$ и $a_1, a_2, \dots, a_{n_i}$ — либо формулы, либо переменные, то $f_i^{n_i}(a_1, a_2, \dots, a_{n_i})$ — формула над Φ.
3) Слова в алфавите $U \cup F \cup \{(,)\}$, получаемые с помощью 1), 2) за конечное число шагов — формулы.

Класс всех формул над F обозначим через $\langle F\rangle$. Каждой формуле обычным образом индуктивно приписываем комбинацию функций из G, называемую суперпозицией. Класс всех таких функций обозначаем через $[F]$ и называем замыканием множества F. Множество F замкнуто, если $F = [F]$.

Две формулы называются равными, если они реализуют (им приписаны) одну и ту же функцию.

Функция k-значной логики $f(x_1, \dots, x_n)$ называется существенной, если она существенно зависит не менее чем от 2-х переменных.

Далее под тождеством будем понимать запись вида $A = B$, где A и B — равные формулы.

Мерой $|A|$ формулы A над Φ назовем число входящих в нее символов из F.

Пусть Б — некоторое множество функций k-значной логики, а I — некоторая **конечная** система тождеств $\{a_1 = b_1, a_2 = b_2, \ldots, a_i = b_i\}$ над Б, где $a_1, b_1, a_2, b_2, \ldots, a_i, b_i \in \langle \text{Б} \rangle$. Система тождеств I над Б называется полной, если для любых формул $\mathbf{a}$ и $\mathbf{b}$ над множеством Б их равенство эквивалентно возможности получить из $\mathbf{a}$ формулу $\mathbf{b}$ (и наоборот) с помощью конечного числа эквивалентных преобразований, осуществляемых тождествами из I.

Как показал Р.К. Линдон [1], для любого замкнутого класса функций **алгебры логики** существует полная конечная система тождеств.

Далее будут рассматриваться только полные конечные системы тождеств.

Для равных формул A и B из $\langle \text{Б} \rangle$ обозначим через $L^I_{\text{Б}}(A, B)$ наименьшее возможное число применений тождеств из I для перевода A в B, тогда пусть $L^I_{\text{Б}}(n) = \max\limits_{|A|,|B| \leqslant n,\ A=B} L^I_{\text{Б}}(A, B)$. Таким образом, функция $L^I_{\text{Б}}$ характеризует сложность перевода произвольных равных формул A и B над Б, меры не более n, друг в друга с помощью системы тождеств I.

Пусть $x \circ y$ — некоторая существенная функция k-значной логики от двух переменных, обладающая свойствами коммутативности, ассоциативности и «свойством 3», где под «свойством 3» будем понимать следование из равенства формул $(f(x) \circ g(y)) = (m(x) \circ n(y))$ равенств $f(x) = m(x)$ и $g(y) = n(y)$ ($f(x)$, $g(y)$, $m(x)$, $n(y)$ — формулы над $\{x \circ y\}$), а из $(f(x) \circ g(y)) = m(x)$ — равенств $f(x) = m(x)$ и $(x \circ g(y)) = x$.

Далее установим справедливость следующих вспомогательных утверждений.

Лемма 1. *Если $A, B \in \langle \{x \circ y\} \rangle$, $|A| \leqslant n$ и A отличается от B только расстановкой скобок, то из A можно получить B со сложностью не более, чем $2n$.*

Лемма 2. *Если $A, B \in \langle \{x \circ y\} \rangle$, $|A| \leqslant n$, $A = B$, 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 $A, B \in \langle\{x \circ y\}\rangle$ такие, что $|A| \leqslant n$, $A = B$, A состоит из тех же переменных и в том же количестве, что и B, и, используя тождества ассоциативности и коммутативности, мы можем получить из A формулу B со сложностью не менее, чем $\frac{n\log(n)}{20}$.*

Эти леммы понадобятся нам для обоснования следующих результатов.

Теорема 1. *Пусть $x * y$ — существенная функция k-значной логики, обладающая свойствами ассоциативности и коммутативности, тогда существует конечная полная система тождеств над базисом $Б = \{\,*\,\}$.*

Теорема 2. *Если $Б = \{x \circ y\}$ (функция $\circ$ описана выше), тогда для $Б$ существует конечная полная система тождеств, и для любой полной системы тождеств I для $\langle Б\rangle$ при $n \to \infty$ функция $L^I_Б(n)$ имеет порядок равный $n\log n$.*

2. Подготовительные замечания

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

Пусть $A, B \in Б = \langle\{x \circ y\}\rangle$, $|A| \leqslant n$, $|B| \leqslant n$, $A = B$ и обозначим A', B' формулы, полученные из формул A, B переименованием их переменных в переменные из множества $\{x_1, x_2, \ldots, x_{2n+2}\}$ (одинаковые переменные переименовываются в одинаковые). Ясно, что «переход», состоящий из последовательности тождеств из I (I — некоторая система тождеств), для получения из A формулы B является также «переходом» от A' к B' и наоборот. Следовательно, функция $L^I_Б(n)$ не изменится, если в ее определении мы будем брать максимум только по тем формулам $A, B \in \langle Б\rangle$, $A = B$, $|A| \leqslant n$, $|B| \leqslant n$, в записи которых встречаются только переменные из множества $\{x_1, x_2, \ldots, x_{2n+2}\}$.

Поэтому дальше мы будем считать, что рассматриваемые формулы меры не более n зависят только от переменных из $\{x_1, x_2, \ldots, x_{2n+2}\}$.

Также обозначим $I^* = \{(x \circ y) = (y \circ x), ((x \circ y) \circ z) = (x \circ (y \circ z))\}$ и формулы вида $(x_{i_1} \circ (x_{i_2} \circ (x_{i_3} \circ (\ldots (x_{i_{(k-2)}} \circ (x_{i_{(k-1)}} \circ x_{i_k})) \ldots))))$, где $i_1 \leqslant i_2 \leqslant i_3 \leqslant \ldots \leqslant i_{(k-1)} \leqslant i_k$, $k \geqslant 1$, назовем каноническими.

3. Доказательство леммы 1

Лемма 1. *Если $A, B \in \langle\{x \circ y\}\rangle$, $|A| \leqslant n$ и A отличается от B только расстановкой скобок, то из A можно получить B со сложностью не более, чем $2n$.*

Доказательство. Рассмотрим в A подформулу вида $(C_1 \circ D_1)$, где C_1 — некоторая подформула 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 новую подформулу в A вида $(C_2 \circ D_2)$ (если такой подформулы C_2 нет — получили канонический вид).

б) $C_1 = (K \circ L)$, где L — переменная, тогда за одну операцию из I^* переходим к формуле 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 — подформула не являющаяся переменной, тогда за одну операцию переходим к $(K \circ (L \circ D_1))$ и полагаем $D_2 = D_1$, $C_2 = L$.

Далее рассматриваем подформулу $(C_2 \circ D_2)$.

Для получившейся формулы $(C_2 \circ D_2)$ применяем те же действия и так далее.

На k-м шаге имеем подформулу вида $(C_k \circ D_k)$, где C_k — некоторая подформула в A, а D_k — подформула, представляющая 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 новую подформулу в A вида $(C_{k+1} \circ D_{k+1})$ (если такой подформулы C_{k+1} нет — получили канонический вид).

б) $C_k = (K \circ L)$, где L — переменная, тогда за одну операцию из I^* переходим к формуле 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 — подформула не являющаяся 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 подформулу $(C_{k+1} \circ D_{k+1})$ и т.д.

В итоге мы получим каноническую расстановку скобок. Ясно, что к этой же расстановке мы аналогичным образом можем привести и формулу B. В обоих случаях, очевидно, нам потребуется применить не более, чем n тождеств из I^* (для каждой функции $\circ$ мы применяем не более одной операции).

Лемма доказана.

4. Доказательство леммы 2

Лемма 2. *Если $A, B \in \langle\{x \circ y\}\rangle$, $|A| \leqslant n$, $A = B$, 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* $6(n+1)\log(n+1)$.

Доказательство. Рассмотрим следующий алгоритм приведения произвольной формулы $A \in \langle\{\,\circ\,\}\rangle$, $|A| \leqslant n$ к каноническому виду.

Не нарушая общности, будем считать, что A содержит ровно по одному разу переменные $x_1, x_2, \ldots, x_k, x_{k+1}$, $k \leqslant n$ (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 $2n$ операций привести нашу формулу A к следующей расстановке скобок (порядок переменных не меняется):

$$(...(((x_{i_1} \circ x_{i_2}) \circ (x_{i_3} \circ x_{i_4})) \circ ((x_{i_5} \circ x_{i_6}) \circ (x_{i_7} \circ x_{i_8}))) \circ \ldots).$$

То есть сначала скобки наложены на пары последовательных переменных, затем такие пары последовательно сгруппированы по две и так далее.

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 $\leqslant \frac{(k+1)}{2}$ раз.

2) Для каждой пары следующего уровня вложенности, то есть 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 $i_{(2m-1)} \leqslant i_{(2m+1)}$, 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 $(x_{i_{(2m-1)}} \circ (x_{i_{(2m+1)}} \circ (x_{i_{(2m+2)}} \circ x_{i_{(2m)}})))$ (в последней подформуле 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 $\frac{(k+1)}{4}$ следовательно, чтобы упорядочить переменные во всех таких подформулах нужно не более $\frac{(k+1)}{4} \cdot 3(2^2 - 1)$ применений тождеств из I^*.

3) Переходим к следующему уровню вложенности: $(((x_{i_{(2m-1)}} \circ (x_{i_{(2m)}} \circ (x_{i_{(2m+1)}} \circ x_{i_{(2m+2)}}))) \circ (x_{i_{(2m+3)}} \circ (x_{i_{(2m+4)}} \circ (x_{i_{(2m+5)}} \circ x_{i_{(2m+6)}}))))$. Аналогично таких подформул не более $\frac{(k+1)}{2^3}$, функций $\circ$ в каждой подформуле 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 $\frac{(k+1)}{2^3} \cdot 3(2^3 - 1)$ применений тождеств из I^*.
   И так далее аналогично проходим все оставшиеся слои вложенности (всего их $\log(k+1)$).

На l-м шаге имеем $((x_{i_{(2m+1)}} \circ (x_{i_{(2m+2)}} \circ (x_{i_{(2m+3)}} \circ \ldots \circ (x_{i_{(2m+2^{l-1}-1)}} \circ x_{i_{(2m+2^{l-1})}}) \ldots))) \circ (x_{i_{(2m+2^{l-1}+1)}} \circ (x_{i_{(2m+2^{l-1}+2)}} \circ \ldots \circ (x_{i_{(2m+2^{l}-1)}} \circ x_{i_{(2m+2^{l})}}) \ldots)))$. Таких подформул не более $\frac{(k+1)}{2^l}$, функций $\circ$ в каждой подформуле 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 $(\frac{(k+1)}{2^l}) \cdot 3(2^l - 1)$ применений тождеств из I^*.

В итоге мы приводим формулу A к каноническому виду. При этом мы использовали $\leqslant 3(k+1) \sum\limits_{m=1}^{\log(k+1)} \frac{(2^m-1)}{2^m}$ операций, что равно $3(k+1)(\log(k+1) + 2^{(-\log(k+1)-1)} - 1) = 3(k+1)(\log(k+1) + \frac{1}{(2(k+1))} - 1) \leqslant 3(n+1)\log(n+1)$.

Следовательно, из того, что каждую формулу можно привести к каноническому виду, и из единственности канонической формулы (для данного набора переменных) вытекает, что нам достаточно $\leqslant 6(n+1)\log(n+1)$ применений тождеств для приведения некоторой формулы к равной в условиях леммы.

Лемма доказана.

5. Доказательство леммы 3

Лемма 3. ***Существуют*** *$A, B \in \langle\{x \circ y\}\rangle$ такие, что $|A| \leqslant n$, $A = B$, A состоит из тех же переменных и в том же количестве, что и B, и, используя тождества ассоциативности и коммутативности, мы можем получить из A формулу B со сложностью не менее, чем $n\frac{\log(n)}{20}$.*

Доказательство. Оценим число $N(m)$ формул из $\langle\{x \circ y\}\rangle$, содержащих m значков функции $\circ$ и только переменные из множества $\{x_1, x_2, \ldots, x_{m+1}\}$ по одному разу. Обозначим N^m — число возможных расстановок скобок в каждой такой формуле. Тогда имеем следующую зависимость $N^m = \sum\limits_{i=0}^{m-1}(N^i N^{(m-i-1)})$ (каждое слагаемое соответствует выбору «внешней» функции $\circ$, которая разбивает формулу на две подформулы) и положим $N^0 := 1$.

Рассмотрим производящую функцию (формальный ряд) вида $f(x) = \sum\limits_{m=0}^{\infty} N^m x^m$. В силу вышеуказанной зависимости можем записать формальное равенство $f(x) = x \cdot f(x) \cdot f(x) + 1$, откуда получаем, что $f(x) = \frac{(1-\sqrt{1-4x})}{2x} = -\sum\limits_{m=1}^{\infty} \frac{((-1)(-3)\ldots(3-2m)(-4x)^m)}{(2^m \cdot m! \cdot 2x)}$, откуда

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

так как $(2m-1)!! = \frac{(2m)!}{(2^m \cdot m!)}$.

Все равенства были формальными. Теперь возьмем найденные коэффициенты N^m и составим из них абсолютно сходящийся ряд $f(x)$. Такой ряд удовлетворяет уравнению $f(x) = x \cdot f(x) \cdot f(x) + 1$, откуда следует, что указанные коэффициенты удовлетворяют равенствам вида $N^m = \sum\limits_{i=0}^{m-1} (N^i N^{(m-i-1)})$ (в силу единственности представления функции в виде степенного ряда).

Далее воспользуемся неравенствами, вытекающими из формулы Стирлинга:

$$\sqrt{2\pi n} \cdot n^n \cdot e^{-n} \leqslant n! \leqslant \sqrt{2\pi n} \cdot n^n \cdot e^{-n+1}.$$

Так как $\frac{m^m}{(m+1)^{m+1}} = (1 - \frac{1}{m+1})^m/(m+1) \geqslant \frac{1}{2^m \cdot (m+1)}$ $(m \geqslant 1)$, то $N^m \geqslant \frac{2^m}{(\sqrt{\pi(m+1)^3} \cdot e)}$.

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

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

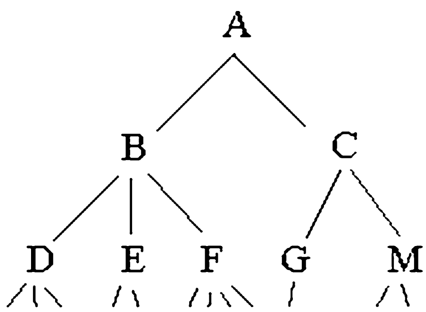
Обозначим через $\leftrightarrow$ тождество из I^*, демонстрирующее коммутативность $(x \circ y = y \circ x)$, а через $()$ — тождество, показывающее ассоциативность $((x \circ y) \circ z = x \circ (y \circ z))$. Отметим, что применение $()$ к подчеркнутой $\circ$ означает следующий переход: $((A \underline{\circ} B) \circ C) \xrightarrow{\text{применяем тождество}} (A \circ (B \circ C))$ или в другом случае $(A \circ (B \underline{\circ} C)) \xrightarrow{\text{применяем тождество}} ((A \circ B) \circ C)$.

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

Теперь рассмотрим подформулу вида $g = ((((A \circ B)\underline{\circ}(C \circ D)) \circ (E \circ F))$ (допустим существует), где A, B, C, D, E, F — некоторые формулы над $\{x \circ y\}$ и назовем подчеркнутую функцию «выбранной». Из предыдущего абзаца следует, что воздействие () или $\leftrightarrow$ на какой-либо значок $\circ$ 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. Таким образом действие операций (), $\leftrightarrow$ на значки функций из A, B, C, D, E, F и вне g («внешние» функции) является коммутативным с воздействием на «выбранную» функцию (результат «сперва действуем на „выбранную“, потом на „внешнюю“» равен результату «сперва на „внешнюю“, потом на „выбранную“»). Подформула g обладает достаточной общностью, чтобы сделать вывод, что для каждого значка функции в формуле существует максимум 5 позиций функций (включая его самого), которые являются некоммутативными с ним.

Оценим число формул, которые можно получить из некоторой одной (например, канонической, содержащей n функций $\circ$ и только переменные из набора $\{x_1, x_2, \dots, x_{n+1}\}$ по одному разу) за k применений тождеств () и $\leftrightarrow$.

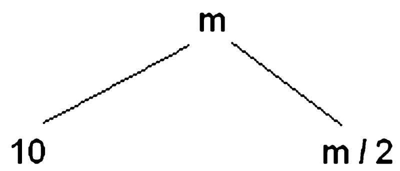
Сначала рассмотрим $k \leqslant n$ и введем конструкцию, показанную на следующем рисунке. Приведенная картинка означает, что на первом шаге (применяя одно тождество) из некоторой выбранной формулы мы можем получить не более A различных формул, на втором шаге (ровно два тождества) не более $A{\cdot}(B{+}C)$ «новых» различных формул (B и C соответствуют некоторым различным ситуациям, коих может быть довольно большое число), на третьем не более $A \cdot (B \cdot (D + E + F) + C \cdot (G + M))$ (то есть «связи» соответствуют умножению,



а числа на одном горизонтальном уровне, «связанные» с некоторым одним вышестоящим числом, складываются, при этом мы двигаемся снизу вверх).

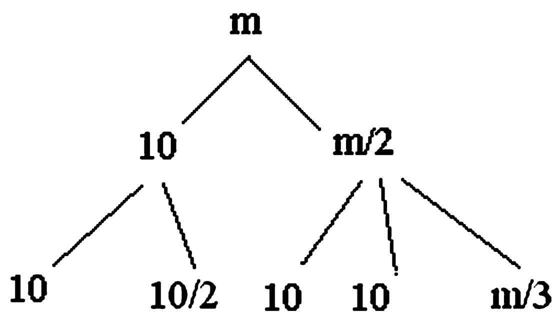
Построим такую конструкцию для нашей канонической формулы. Очевидно, что на первом шаге (применение одного тождества) мы не получим более $2n = m$ различных формул (n возможных вариантов для $\leftrightarrow$ и n для ()). На втором шаге возможен коммутативный случай, то есть вторая операция не применяется к указанным выше 5 случаям нарушения коммутативности. Тогда существует $\leqslant (m - 10) \leqslant m$ возможных вариантов ($10 = 2$ вида операций $\times$ 5 позиций и $m = 2n$) для каждой формулы из первого шага, поэтому соответствующей вершине сопоставим число $\frac{m}{2}$ (учитываем коммутативность). В некоммутативном случае, очевидно, существует не более 10 ситуаций для каждой формулы.

Таким образом первые два уровня принимают вид:



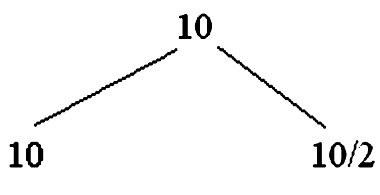
Далее идем справа налево:
для правой ветви можем попасть мимо «полей некоммутативности» уже ранее выбранных некоторых двух операций ($\frac{m}{3}$) или попасть в них (10 — в первую (построенную на первом уровне) и 10 — во вторую (появившуюся на втором)). Для левой ветви $\frac{10}{2}$ — попали в «поле»

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», затем 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). И при построении считаем конструкцию, соответствующую вершине на предыдущем уровне, «твердой», то есть некоммутативной **внутри себя**. И так далее, продолжая построение, строим наши k уровней.

Введем следующие обозначения: N_t — 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 мы 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. Будем обозначать $[A]$.

б) как множество формул, которые можно получить из канонической формулы, осуществляя преобразования, соответствующие вершинам вдоль пути от корня к A. Обозначаем $\langle A \rangle$.

Докажем по индукции, что если A — вершина, соответствующая попаданию в «поле некоммутативности» своего родителя B, стоящего p уровней назад, то она порождает на следующий уровень $p+1$ 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.

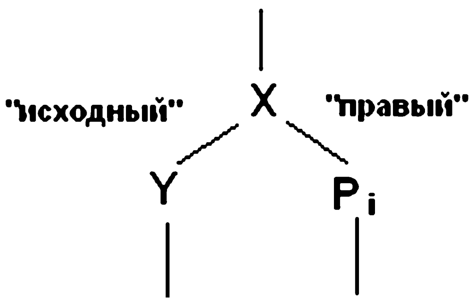
Допустим доказано для уровня $t-1$, тогда возьмем произвольную вершину G на уровне t и пусть $A_{t-1}, A_{t-2}, \ldots, A_0 = \{$все возможные позиции функций$\}$ — родители вершины G (индексы отображают уровень). Также предположим, что G соответствует воздействию на «поле некоммутативности» A_{t-p},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

Из вершины G выйдут вершины, соответствующие следующим случаям: попали в «поле некоммутативности» $P_1 = G$, в «поле» $P_2 = A_{t-1} \setminus G$, $P_3 = A_{t-2} \setminus \{G \cup A_{t-1}\}$, $\ldots$, $P_{p+1} = A_{t-p} \setminus \{G \cup A_{t-1} \cup \ldots \cup A_{t-p+1}\}$ — $p+1$ случай.

Действительно, допустим из G выходит вершина K определяемая непопаданием 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 встретили раньше), значит ситуация K уже была (применяем операции $[G]$ к $\langle M\rangle$), а второй раз одинаковое (справа налево) построение мы не рассматриваем — противоречие.

Далее, рассмотрим вершину P_i, выходящую из G. 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 результат $\langle P_i\rangle$ встретился раньше (правее) от соответствующей вершины из G (это «правый» путь с некоторым концом M на уровне $t+1$ и $\langle M\rangle = \langle P_i\rangle$). В силу вышесказанного, исходный путь для P_i и «правый» путь разветвляются только с помощью вершины P_i следующим образом:



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

Если $i \neq 1$, то так как $[G]$ действует на $A_{t-p} \setminus \{A_{t-1} \cup \ldots \cup A_{t-p+1}\}$, а $[P_i]$ на $A_{t-i+1} \setminus \{G \cup A_{t-1} \cup \ldots \cup A_{t-i+2}\}$, $i \leqslant p$, то можно «правый» путь перестроить после X так, чтобы на место P_i встали операции из G (это возможно, так как операции, соответствующие этим двум вершинам коммутативны и так как P_i должен стоять после появления в цепочке A_{t-p}, на «поле» которого действует G). В этом случае ветвление останется также в правую сторону (G действует на «поле некоммутативности» еще на более раннем уровне). Теперь если из перестроенной «правой» ветки «убрать» вершину P_i (возможно, так как нет операций воздействующих на ее «поле» на более поздних уровнях), то получится результат $\langle G \rangle$ справа от исходного — противоречие.

Таким образом мы доказали, что $N_t = N_{t+2}^2$ и $N_t^2 = N_{t-1}^2 + N_{t-1}^3 + \ldots + N_{t-1}^{t-2} + N_{t-1}^{t-1}$, а также $N_t^i = N_{t-1}^{i-1} + N_{t-1}^i + \ldots + N_{t-1}^{t-2} + N_{t-1}^{t-1}$ для всех $3 \leqslant i \leqslant t$.

Очевидно, что $N_2^2 = 1 \leqslant 2^2 \cdot 2^{2-2}$. Допустим, что для всех $h < t$ мы доказали неравенство $N_h^i \leqslant 2^h \cdot 2^{h-i}$, $2 \leqslant i \leqslant h$. Тогда для $2 \leqslant i \leqslant t$ имеем $N_t^i = N_{t-1}^{i-1} + N_{t-1}^i + \ldots + N_{t-1}^{t-2} + N_{t-1}^{t-1} \leqslant 2^{t-1} \cdot 2^{t-i} + 2^{t-1} \cdot 2^{t-i-1} + \ldots + 2^{t-1} \cdot 2^1 + 2^{t-1} \cdot 2^0 = 2^{t-1} \cdot (2^{t-i+1} - 1) \leqslant 2^t \cdot 2^{t-i}$.

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

$$k \cdot \frac{10^k \cdot 4^{k+1} \cdot m^k}{k!} = \frac{k \cdot 4 \cdot 80^k \cdot n^k}{k!} \leqslant \frac{k \cdot 4 \cdot 80^k \cdot n^k}{\sqrt{2 \cdot \pi \cdot k} \cdot k^k \cdot e^{-k}} \leqslant 320^n \cdot e^n$$

$$\left(\frac{k \cdot 4}{\sqrt{2 \cdot \pi \cdot k}} \leqslant 4 \cdot n \leqslant 4^n \right)$$

формул.

Для произвольного же $k \geqslant n$, число формул, очевидно, не превышает $((320 \cdot e)^n)^{k/n+1} = (320 \cdot e)^{k+n}$.

Допустим k такого, что применяя $\leqslant k$ тождеств из I^* мы можем получить все возможные формулы (для данной начальной формулы), тогда должно иметь место неравенство вида

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

(так как $\frac{2^m}{e^m} \geqslant \frac{1}{2^m}$), откуда $k \geqslant (n \cdot \log_{320 \cdot e}(\frac{n}{2}) + \log_{320 \cdot e}(\sqrt{2n}) - \log_{320 \cdot e}(\sqrt{(n+1)^3}) - 1 - n)$ и таким образом, $k \geqslant n \cdot \frac{\log(n)}{20}$ (так как $\log_{320 \cdot e}(n) = \frac{\log(n)}{\log(320 \cdot e)} \geqslant \frac{\log(n)}{10}$) при достаточно больших n. Следовательно, асимптотически $L_{\text{Б}}^{I^*}(n) \geqslant n \cdot \frac{\log(n)}{20}$.

Лемма доказана.

6. Доказательство теоремы 1

Теорема 1. *Пусть $x * y$ — существенная функция k-значной логики, обладающая свойствами ассоциативности и коммутативности, тогда существует конечная полная система тождеств над базисом $Б = \{ * \}$.*

Доказательство теоремы. В силу ассоциативности и коммутативности функции в дальнейшем доказательстве мы не будем обращать внимание на скобки или порядок переменных, а только на их количество.

Рассмотрим всевозможные равенства $A = B$, где $A, B \in \langle\{*\}\rangle$ и имеют вид $x{*}x{*}\ldots{*}x = x{*}x{*}\ldots{*}x$ (число значков в обоих частях различно), множество таких равенств не пусто, так как число функций от одной переменной конечно, а число формул вида $x * x * \ldots * x$ от одной фиксированной переменной x неограниченно. Далее, из этих равенств выберем такое, чтобы число $\max(|A|, |B|)$ было наименьшим. Такое равенство единственно. Действительно, допустим $A = B$, $C = D$, $A, B, C, D \in \langle\{*\}\rangle$ — формулы, в которых встречается только одна переменная x и $h = |A| = |C| = \max(|A|, |B|) = \max(|C|, |D|)$ — минимально, тогда, очевидно, $A = C$, $|B| < |A| = h$, $|D| < |C| = h$ и следовательно, имеем равенство $B = D$, откуда (h — минимально) $|B| = |D|$, то есть наши два тождества идентичны.

Для «минимального» тождества обозначим число $\max(|A|, |B|)$ как m. Ясно, что любую однопеременную формулу (в записи встречается только одна переменная) $A(x)$, $|A| \geqslant m$ с помощью этого тождества можно привести к формуле $A'(x) = A(x)$, $|A'| < m$, поэтому далее будем считать, что в любой формуле каждая переменная встречается не более m раз.

Рассмотрим множество всевозможных тождеств вида $A(y_1, y_2, \ldots, y_s) = B(y_1, y_2, \ldots, y_t)$ (запись $A(y_1, y_2, \ldots, y_s)$ означает, что в формуле хотя бы раз встречается каждая переменная от y_1 до y_s), $A, B \in \langle\{*\}\rangle$, $y_1, \ldots, y_{m^2 \cdot 2^{k^2}}$ — некоторый **фиксированный** набор переменных, $s, t \leqslant m^2 \cdot 2^{k^2}$ (то есть ограничено число переменных) и обозначим его I. Очевидно, что это множество конечно (считаем, что в любой формуле каждая переменная встречается не более m раз). Покажем, что I — полная система тождеств над $\{x * y\}$.

Рассмотрим произвольные формулы $A(x_1, \dots, x_s) = B(x_1, \dots, x_t)$, $A, B \in \langle\{*\}\rangle$, x_i — **произвольные** переменные.

Если $s, t \leqslant m^2 \cdot 2^{k^2}$ — все хорошо, $A = B \in I$ (с точностью до переименования переменных), то есть возможен переход $A \to B$ с помощью I.

Иначе ($s, t > m^2 \cdot 2^{k^2}$), считаем (вспоминая про ассоциативность и коммутативность функции) $A = a_1(x_1) * \dots * a_t(x_t)$, $B = b_1(x_1) * \dots * b_s(x_s)$, где a_i, b_j — однопеременные подформулы A и B, $|a_i|$, $|b_j| < m$, то есть среди $|a_i|$ и $|b_j|$ не более $m - 1$ различных чисел.

Введем еще «мнимую» однопеременную формулу — просто некоторый значок — $\varnothing(x) : \forall A, \;\; A \in \langle\{*\}\rangle$ выполнено $\varnothing(x) * A = A * \varnothing(x) = A$ (допускаем, что существует такая функция, на наших преобразованиях это никак не скажется), теперь можем считать $s = t$ (если в A есть, например, x_1, а в B нет, то вместо B рассматриваем $B * \varnothing(x_1)$).

Так как различных типов («тип» определяется значением меры) однопеременных подформул ровно m (учитывая мнимую) и $s = t > m^2 \cdot 2^{k^2}$, то среди $\{a_i(x_i) \;\; | \;\; 1 \leqslant i \leqslant t\}$ как минимум $m^2 \cdot 2^{k^2} + 1$ раз встречается один и тот же некоторый тип подформул (то есть существует число $< m$ такое, что не менее $m^2 \cdot 2^{k^2} + 1$ однопеременных подформул имеют меру равную этому числу).

Не нарушая общности, считаем, что $|a_1(x_1)| = \ldots = |a_r(x_r)|$, $r > m^2 \cdot 2^{k^2}$. Среди $b_1(x_1), \dots, b_r(x_r)$ аналогичным образом встречается $h > 2^{k^2}$ раз один и тот же **тип** подформул: считаем $|b_1(x_1)| = \ldots = |b_h(x_h)|$, остатки $b_{h+1}(x_{h+1}) * \dots * b_s(x_s)$ и $a_{h+1}(x_{h+1}) * \dots * a_t(x_t)$ обозначим соответственно $\tilde{B}, \tilde{A}$.

Рассмотрим значения $a_1(x_1) * \tilde{A}$ и $b_1(x_1) * \tilde{B}$ на одинаковых наборах, — получим множество упорядоченных пар (i, j), где $i, j \in \{0, \dots, k-1\}$, i — значение $a_1(x_1) * \tilde{A}$ на некотором наборе, j — значение $b_1(x_1) * \tilde{B}$ на этом же наборе. Выбирая по одному представителю от каждого подмножества одинаковых пар (например, из множества $\{(1,1), (2,3), (2,3), (2,3)\}$ берем $(1,1)$ и $(2,3)$), составляем множество **различных** пар I_1.

Далее рассматриваем $a_1(x_1) * a_2(x_2) * \tilde{A}$ и $b_1(x_1) * b_2(x_2) * \tilde{B}$ и аналогичным образом формируем множество I_2 и так далее пока не получим I_h.

Всего различных упорядоченных пар может быть k^2 следовательно, число возможных вариаций среди множеств I_i не более 2^{k^2}. Таким образом существуют индексы $1 \leqslant i, j \leqslant 2^{k^2} + 1 \leqslant h$, $i \neq j$ такие, что $I_i = I_j$, но тогда $I_{i+1} = I_{j+1}$, $I_{i+2} = I_{j+2}, \ldots$. Действительно, можно заметить, что I_{i+1} формируется следующим образом: берется произвольная пара (f, g) из I_i, значения a и b подформул a_i и b_i на одном и том же произвольном значении переменной x_i соответственно, и получается пара $(f * a, g * b) \in I_{i+1}$ — так для всех пар из I_i и значений x_i. Также формируется I_{j+1} (используются I_j и $a_j(x_j)$, $b_j(x_j)$), но $I_i = I_j$, $a_i(x) = a_j(x)$, $b_i(x) = b_j(x)$, x_i, x_j — разные переменные и встречаются только в $a_i(x_i)$, $b_i(x_i)$ и $a_j(x_j)$, $b_j(x_j)$ соответственно, значит имеет место совпадение I_{i+1} с I_{j+1}.

Поэтому существует индекс p, $1 \leqslant p < h$ и p — максимальный среди таких, что $I_p = I_h$. По построению I_h, все пары имеют совпадающие левые и правые части (I_h соответствует A и B, $A = B$). То есть мы нашли равные подформулы $A_{(1)} = a_1(x_1) * \ldots * a_p(x_p) * \tilde{A}$ и $B_{(1)} = b_1(x_1) * \ldots * b_p(x_p) * \tilde{B}$, в них число переменных $p + s - h < s$ — мы научились находить в равных формулах с числом переменных $> m^2 \cdot 2^{k^2}$ равные подформулы с меньшим числом переменных.

Теперь рассматриваем $A_{(1)} = B_{(1)}$, применяем тот же алгоритм, получаем подформулы $A_{(2)} = B_{(2)}$ и так далее. В итоге находим подформулы $A_{(d)} = B_{(d)}$, $A_{(d)}$ — подформула A, $B_{(d)}$ — подформула B, в которых не более $m^2 \cdot 2^{k^2}$ переменных, то есть $A_{(d)} = B_{(d)} \in I$ (с точностью до переименования переменных).

Допустим, что осуществляется переход с помощью I от $A_{(u)}$ к $B_{(u)}$. Как перейти от $A_{(u-1)}$ к $B_{(u-1)}$?

По построению $A_{(u-1)} = A_{(u)} * a(x_f) * \ldots * a(x_g)$, $B_{(u-1)} = B_{(u)} * b(x_f) * \ldots * b(x_g)$, где a, b — некоторые однопеременные формулы. Если $a = b$ — все хорошо. Допустим, $a \neq b$, тогда перейдем с помощью I от $A_{(u-1)}$ к $A'_{(u-1)} = B_{(u)} * a(x_f) * \ldots * a(x_g)$ и применим вышеприведенный алгоритм к $A'_{(u-1)}$ и $B_{(u-1)}$. Так как $g - f \leqslant 2^{k^2}$ (p выбирали максимальным) и $a \neq b$, то $a(x_f) * \ldots * a(x_g)$, очевидно, попадет в $\tilde{A}'_{(u-1)}$ («остаток» A, выделившийся после выбора «достаточно длинной» ($h > 2^{k^2}$) последовательности однопеременных подформул одного типа), а $b(x_f) * \ldots * b(x_g)$ в $\tilde{B}_{(u-1)}$, то есть внутрь новых равных подформул.

Продолжая для этих двух подформул процесс выделения равных подформул, заключаем, что в конце концов $a(x_f) * \ldots * a(x_g)$ и $b(x_f) * \ldots * b(x_g)$ попадут внутрь тождества из I, являющегося «подтождеством» $A'_{(u-1)} = B_{(u-1)}$ (с точностью до переименования переменных) следовательно, знаем как от $A_{(u-1)}$ перейти к $B_{(u-1)}$. Так поступенчато идем от $A_{(d)} = B_{(d)}$ к $A = B$ — теорема доказана.

7. Доказательство теоремы 2

Теорема 2. *Если $Б = \{x \circ y\}$ (функция $\circ$ определена в разделе 1), тогда для $Б$ существует конечная полная система тождеств и для любой полной системы тождеств I для $\langle Б \rangle$ при $n \to \infty$ функция $L^I_Б(n)$ имеет порядок равный $n \log n$.*

Доказательство теоремы. Пусть $A, B \in \langle \{x \circ y\} \rangle$, $A = B$, $|A| \leqslant n$, $|B| \leqslant n$ и, используя тождества ассоциативности и коммутативности, проделаем следующие действия:

1) Сначала приведем A к «промежуточному» представлению $(f_{i_1}(x_{i_1}) \circ (f_{i_2}(x_{i_2}) \circ (\ldots \circ (f_{i_{(k-1)}}(x_{i_{(k-1)}}) \circ f_{i_k}(x_{i_k})) \ldots)))$, где f_{i_1}, f_{i_2}, $\ldots$, $f_{i_{(k-1)}}$, f_{i_k} — некоторые формулы от одной переменной вида $(x \circ (x \circ (\ldots (x \circ x) \ldots)))$, $i_1 < i_2 < i_3 < \ldots < i_{(k-1)} < i_k$, в котором те же переменные и в том же количестве, что и в A.
2) Аналогично поступим с B: имеем $(g_{j_1}(x_{j_1}) \circ (g_{j_2}(x_{j_2}) \circ (\ldots \circ (g_{j_{(p-1)}}(x_{j_{(p-1)}}) \circ g_{j_p}(x_{j_p})) \ldots)))$, $j_1 < j_2 < j_3 < \ldots < j_{(k-1)} < j_k$.
3) Не нарушая общности (можем переименовывать переменные), будем считать, что в A и B встречаются следующие переменные x_1, x_2, $\ldots$, x_u, $u \leqslant 2n + 2$ (так как $|A| \leqslant n$, $|B| \leqslant n$). Согласуем однопеременные подформулы. Для этого рассмотрим два случая.

Случай А: если две формулы равны, то не существует переменной, встречающейся в одной формуле, но не встречающейся в другой.

Рассмотрим некоторое тождество вида $(x \circ (x \circ \ldots \circ (x \circ x) \ldots)) = (x \circ (x \circ \ldots \circ (x \circ x) \ldots))$, где количество значков $\circ$ различно в правой и левой частях и максимальное из этих чисел (**обозначим его**

m) является **наименьшим** среди подобных максимумов для формул такого вида (тождество существует и единственно — обоснование существования и единственности аналогично соответствующему доказательству в теореме 1). Наше тождество обозначим $\downarrow$.

Тождество $\downarrow$ позволяет любые формулы $A, B \in \langle\{\circ\}\rangle$, $A = B$ вида $A = (x\circ(x\circ\ldots\circ(x\circ x)\ldots))$, $B = (x\circ(x\circ\ldots\circ(x\circ x)\ldots))$ переводить друг в друга. Действительно, с помощью нашего тождества $\downarrow$ уменьшая меру формул, мы можем добиться (переходя от A к A', от B к B'), чтобы $|A'| < m$ и $|B'| < m$, но по определению числа m это возможно только, если $|A'| = |B'|$, то есть A', B' имеют одинаковый вид. Значит, чтобы перейти от A к B надо перейти от A к A', а затем, обращая переход $B \to B'$, перейти от A' к B.

Так как $A = B$, то для одинаковых переменных будем иметь (отождествляя все переменные кроме требуемой переменной x_i и используя «свойство 3») $f_i(x_i) = g_i(x_i)$.

Согласно сказанному выше, тождество $\downarrow$ позволяет осуществить переход $f_i(x_i) \to g_i(x_i)$. Проделывая эти действия для каждой переменной в A, очевидным образом получим B.

Случай B: существуют две равные формулы и некоторая переменная, встречающаяся в одной формуле, но не существующая в другой.

Рассмотрим некоторое тождество вида $(y\circ(x\circ(x\circ\ldots\circ(x\circ x)\ldots))) = y$, где количество значков $\circ$ в левой части (**обозначим его** m) является **наименьшим** для формул такого вида (тождество существует и единственно — обоснование как и раньше). Это тождество обозначим $\downarrow$.

Тождество $\downarrow$ позволяет любые формулы $A, B \in \langle\{\circ\}\rangle$, $A = B$ вида $A = (y\circ(x\circ(x\circ\ldots\circ(x\circ x)\ldots)))$, $B = (y\circ(x\circ(x\circ\ldots\circ(x\circ x)\ldots)))$ (иксов в какой-то формуле может и не быть), переводить друг в друга. Для этого с помощью нашего тождества $\downarrow$, уменьшая меру формул, мы можем добиться (переходя от A к A', от B к B'), чтобы $|A'| < m$ и $|B'| < m$, но по определению числа m это возможно только, если $|A'| = |B'|$. Действительно, допустим $0 < k = |A'| - |B'| < m$, тогда можем считать (дописываем одинаковое количество переменных x к формулам и нужным образом распределяем скобки), что $|A'| = m$, $0 < |B'| < m$, $A' = B'$, но $y = A'$ — тождество $\downarrow$, поэтому справедливо равенство $y = B'$ — противоречие определению m.

Итак, A', B' имеют одинаковый вид, следовательно, чтобы перейти от A к B надо перейти от A к A', а затем, обращая переход $B \to B'$, перейти от A' к B.

Отождествляя переменные в $\downarrow$, можно любые формулы $A, B \in \langle\{\circ\}\rangle$, $A = B$ вида $A = (x \circ (x \circ \ldots \circ (x \circ x) \ldots))$, $B = (x \circ (x \circ \ldots \circ (x \circ x) \ldots))$, переводить друг в друга. Для этого с помощью нашего тождества $\downarrow$, уменьшая меру формул, мы можем добиться (переходя от A к A', от B к B'), чтобы $|A'| < m$ и $|B'| < m$, но по определению числа m это возможно только, если $|A'| = |B'|$. Действительно, допустим $0 < k = |A'| - |B'| < m$, тогда допишем слева y к A' и B' — получим вышеизложенный случай. Итак, A', B' имеют одинаковый вид, следовательно, чтобы перейти от A к B надо перейти от A к A', а затем, обращая переход $B \to B'$, перейти от A' к B.

Так как $A = B$, то для одинаковых переменных будем иметь (отождествляя все переменные кроме требуемой переменной x_i и используя «свойство 3») $f_i(x_i) = g_i(x_i)$ или $(y \circ f(x_i)) = y$, где y — некоторая переменная.

Согласно сказанному выше, тождество $\downarrow$ позволяет осуществить переход $f_i(x_i) \to g_i(x_i)$ и $(y \circ f(x_i)) \to y$. Проделаем эти действия для каждой переменной в A и B (для случая $(y \circ f(x_i)) \to y$, возможно, придется применить тождество коммутативности, чтобы переместить $f(x_i)$ на место правого аргумента функции $\circ$ в A, также это надо учитывать и с B), очевидным образом получим формулы одинакового вида A', B'. Значит, чтобы перейти от A к B надо перейти от A к A', а затем, обращая переход $B \to B'$, перейти от A' к B.

Итак, в обоих случаях система тождеств $I^* = \{x \circ y = y \circ x,\ x \circ (y \circ z) = (x \circ y) \circ z$ и $\downarrow\}$ является полной конечной системой тождеств для Б. Кроме того, легко видеть, что все описываемые действия вида $f_i(x_i) \to g_i(x_i)$ и $(y \circ f(x_i)) \to y$ требуют не более, чем линейное по порядку количество применений третьего тождества из I^*. Следовательно, согласно лемме 2, данный алгоритм имеет сверху оценку порядка $n \log n$. Поскольку, 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, то оценка сверху имеет тот же порядок и для системы I.

Также, используя лемму 3, мы получаем порядок $n \log n$ для оценки снизу, и очевидным образом справедливо неравенство $S(I) \cdot L_{\text{Б}}^{I}(n) \geqslant L_{\text{Б}}^{I^*}(n) \geqslant \frac{n \cdot \log(n)}{20}$, где $S(I) = \min\{$число «применений» тождеств из I^* достаточное для получения из всех левых частей тождеств в I их правых частей$\}$. Откуда $L_{\text{Б}}^{I}(n) \geqslant C(I) \cdot n \log(n)$, где $C(I) = \frac{1}{S(I) \cdot 20}$.

Теорема доказана.

Замечание. Если рассмотреть аналоги конъюнкции и дизъюнкции в k-значной логике $\min(x, y)$, $\max()$, а также сложение по модулю k, то они обладают требуемыми в теореме свойствами и поэтому являются примерами функций, для которых тождественные преобразования в соответствующем множестве формул имеют порядок $n \log(n)$.

Список литературы

[1] Lyndon R.C. Identities in two-valued calculi // Trans. Amer. Math. Soc. 71. N 3 (1951). P. 457–465.

[2] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б. Функции алгебры логики и классы Поста. М.: Наука, 1966. С. 1–121.