

ОБ ИНВАРИАНТНЫХ КЛАССАХ ФУНКЦИЙ, БЕСПОВТОРНО ВЫРАЗИМЫХ ФОРМУЛАМИ*)

Д. Ю. Черухин

Показано, что мощность множества инвариантных классов функций 2-значной логики, неповторно выражимых формулами в фиксированном полном конечном базисе, счётна; доказана возможность описания этих классов с помощью запрещённых подфункций и контекстно-свободных грамматик. Для каждого $k > 2$ приведён пример конечного базиса в k -значной логике, для которого мощность множества таких классов равна континууму.

Понятие инвариантного класса булевых функций было введено С. В. Яблонским в работе [3]. Он показал, что мощность множества таких классов равна континууму. Мы ограничимся только теми классами, в которых все функции неповторно выражимы формулами в фиксированном конечном базисе (неповторная выражимость рассматривалась А. В. Кузнецовым [1]). Другими словами, это те классы, которые содержат конечное число неразложимых функций. Целью настоящей статьи является доказательство следующих утверждений.

Теорема 1. *Для любого полного конечного булева базиса B мощность множества инвариантных классов, состоящих из функций, неповторно выражимых формулами над B , счётна.*

Теорема 2. *Для любого $k > 2$ существует конечный базис B_k функций k -значной логики такой, что мощность множества инвариантных классов, состоящих из функций, неповторно выражимых формулами над B_k , равна континууму.*

Кроме того, покажем, что каждый инвариантный класс, состоящий из функций, неповторно выражимых в конечном булевом базисе B ,

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-01175), Федеральной целевой программы «Интеграция» (объединенный проект АО-110), программы «Университеты России» (проект 992206) и Программы поддержки ведущих научных школ РФФИ (проект 00-15-96103).

может быть порождён (в определённом смысле) конечным числом запрещённых подфункций и задан множеством формул, выводимых в контекстно-свободной грамматике специального вида.

1. Функции k -значной логики

Функцией k -значной логики называется функция $f: \{0, \dots, k-1\}^n \rightarrow \{0, \dots, k-1\}$. Множество всех функций k -значной логики обозначим через P_k . Подмножество $K \subseteq P_k$ называется *инвариантным классом*, если K замкнуто относительно операций добавления и изъятия несущественных переменных, перестановки переменных и подстановки констант вместо переменных.

Пусть $B \subseteq P_k$ — конечное множество функций (*базис*). *Формулой* над B (в базисе B) называется выражение вида c , где c — константа из B , или $f(F_1, \dots, F_n)$, где f — n -местная функция из B , $n \geq 1$, а каждое выражение F_1, \dots, F_n является или формулой над B , или *переменной* из множества $\{x_1, x_2, \dots\}$ (определение формулы индуктивно). Для удобства переменные также будем считать формулами. Формула F , реализующая функцию f , называется *бесповторной*, если каждая существенная переменная функции f входит в F ровно один раз. Функция f *бесповторно выражима* над B (в базисе B), если f выражима некоторой бесповторной формулой над B .

Обозначим через $\mathcal{E}(B)$ множество всех функций, бесповторно выражимых в базисе B . Так как множество $\mathcal{E}(B)$ является подмножеством множества $\mathcal{E}(B^*)$ для некоторого полного базиса B^* , то из теоремы 1 следует, что для любой конечной системы $B \subseteq P_2$ мощность множества инвариантных классов в $\mathcal{E}(B)$ не более чем счётна. Из теоремы 2, напротив, следует, что при $k > 2$ существует полный базис $B^* \subseteq P_k$, в котором мощность множества инвариантных классов равна континууму (очевидно, эта мощность не больше континуума).

Рассмотрим *булеву* функцию f , т. е. функцию 2-значной логики. Будем говорить, что функция $f(x_1, \dots, x_n)$ *возрастает (убывает) по i -й переменной*, $1 \leq i \leq n$, если для любых двоичных констант $c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n$ число $f(c_1, \dots, c_{i-1}, 0, c_{i+1}, \dots, c_n)$ не больше (не меньше) числа $f(c_1, \dots, c_{i-1}, 1, c_{i+1}, \dots, c_n)$. Каждую функцию $f(x_1, \dots, x_n)$, существенно зависящую от всех своих переменных, можно представить в виде $f'(\varphi_1(x_1), \dots, \varphi_n(x_n))$, где $\varphi_1, \dots, \varphi_n$ — перестановки и f' — функция, не убывающая ни по одной переменной (нужно взять $\varphi_i(x) = \bar{x}$ для тех и только тех i , для которых функция f убывает по x_i). Функцию f' назовём *неубывающим представителем* функции f . Функция f' обладает следующим свойством: для каждого i найдутся такие

константы $c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_n$, что

$$f'(c_1, \dots, c_{i-1}, x_i, c_{i+1}, \dots, c_n) \equiv x_i. \quad (1)$$

Тождество (1) является исключительным свойством 2-значной логики, приводящим, как увидим, к различию результатов теорем 1 и 2.

Функция h называется *подфункцией* функции f , если h может быть получена из f подстановкой констант вместо некоторых переменных. При этом переменная, вместо которой подставлена константа, удаляется из списка переменных с сохранением порядка следования оставшихся переменных.

Рассмотрим произвольный булев базис B . Обозначим через $[B]$ базис, состоящий из всех функций h таких, что h существенно зависит от всех своих переменных и является подфункцией некоторой функции из базиса B . Пусть g — произвольная функция, неповторно выразимая в базисе B и не равная тождественно константе. Представим g в виде неповторной формулы F над B . Формулу F преобразуем в формулу F_1 над $[B]$ такую, что F_1 тождественно равна формуле F , в F_1 отсутствуют константы и все переменные формулы F_1 существенны. Для этого несущественные переменные формулы F заменим константами, а затем исключим из полученной формулы константы и несущественные переменные базисных функций, заменив базисные функции их подфункциями из $[B]$.

Далее обозначим через B' множество всех таких функций f' от двух или большего числа переменных, что f' является неубывающим представителем некоторой функции из $[B]$ или отрицания некоторой функции из $[B]$. Формулу F_1 преобразуем в формулу F' над множеством $B' \cup \{\neg\}$ такую, что F' тождественно равна формуле F и отрицания в F' могут быть только перед переменными. Такое преобразование можно осуществить последовательно, начиная от внешней функции формулы и двигаясь от формулы к её подформулам.

Таким образом, полученная формула F' над множеством функций $B' \cup \{\neg\}$ неповторно реализует функцию g , не содержит констант и фиктивных переменных и каждое отрицание в F' находится непосредственно перед переменной. Всякую формулу, удовлетворяющую этим свойствам, обозначим через $F_B(g)$. Введём вспомогательное множество переменных $\{y^0, y^1\}$. Обозначим через $F'_B(g)$ формулу, полученную из $F_B(g)$ заменой каждой переменной без отрицания на переменную y^1 и каждой переменной с отрицанием на переменную y^0 . Формула $F'_B(g)$ характеризует функцию g с точностью до перестановки переменных, добавления и изъятия несущественных переменных.

2. Частично упорядоченные множества

Рассмотрим частично упорядоченные множества (ЧУМ) с нестрогим отношением частичного порядка \leq и соответствующим строгим отношением $<$, которые будем иногда называть *предшествованием* и *строгим предшествованием* соответственно. *Бесконечно возрастающей (убывающей) цепью* в ЧУМ M называется такая бесконечная последовательность t_1, t_2, \dots элементов из M , что выполнены неравенства $t_1 < t_2 < \dots$ ($t_1 > t_2 > \dots$). ЧУМ M назовём *коротким*, если в нём отсутствуют бесконечно убывающие цепи, и *узким*, если в нём отсутствуют бесконечные множества попарно несравнимых элементов. Элемент $t \in M$ называется *минимальным*, если в M нет элемента t' такого, что $t' < t$. Два различных минимальных элемента несравнимы. Множество всех минимальных элементов в M обозначим через $\min M$.

Утверждение 1. *Если ЧУМ M является коротким, то для любого $t_1 \in M$ существует элемент $t \in \min M$, предшествующий элементу t_1 .*

Доказательство. Пусть, напротив, ни один элемент из $\min M$ не предшествует элементу t_1 . Так как $t_1 \leq t_1$, то $t_1 \notin \min M$. Поэтому существует элемент $t_2 \in M$ такой, что $t_2 < t_1$. Для t_2 также не найдётся предшествующего ему минимального элемента (в противном случае этот минимальный элемент предшествовал бы и элементу t_1). Поэтому найдётся элемент $t_3 \in M$ такой, что $t_3 < t_2$. Действуя так, получим бесконечно убывающую цепь элементов $t_1 > t_2 > \dots$. Противоречие. Утверждение 1 доказано.

Утверждение 2. *В любом коротком узком бесконечном ЧУМ существует бесконечно возрастающая цепь.*

Доказательство. Пусть M — короткое узкое бесконечное ЧУМ. Так как M короткое, то в силу утверждения 1 любой элемент $t \in M$ предшествует некоторому минимальному элементу. Поэтому множество $\min M$ непусто. Последнее состоит из попарно несравнимых элементов. Поэтому в силу узости множества M множество $\min M$ конечно. Обозначим через t_1 тот минимальный элемент, который предшествует бесконечному числу элементов из M . Пусть M_1 — множество всех элементов, которым предшествует t_1 . Применяя то же рассуждение к множеству M_1 , выберем в нём элемент t_2 и бесконечное подмножество M_2 , состоящее из элементов, которым предшествует t_2 . Действуя так далее, получим бесконечно возрастающую цепь $t_1 < t_2 < \dots$. Утверждение 2 доказано.

Подмножество $K \subseteq M$ назовём *инвариантным* классом, если вместе с каждым своим элементом K содержит все предшествующие ему

элементы. Класс K можно рассматривать как ЧУМ с отношением порядка, унаследованным из M . Множество всех инвариантных классов в M обозначим через $I(M)$. Множество $I(M)$ также можно рассматривать как ЧУМ с отношением теоретико-множественного вложения классов. Пусть $P \subseteq M$ и $Q \subseteq M$. Обозначим через $Z(P; Q)$ множество всех элементов из P , не предшествующих ни одному элементу из Q . Если P — инвариантный класс (в частности, $P = M$), то множество $Z(P; Q)$ является инвариантным классом и называется классом, порождённым (в P) множеством запретов Q .

Лемма 1. Пусть M — не более чем счётное короткое ЧУМ. Тогда следующие условия равносильны:

- а) множество M узко;
- б) число инвариантных классов в M не более чем счётно;
- с) каждый инвариантный класс может быть порождён конечным множеством запретов.

Доказательство. Импликация с) \Rightarrow б) следует из того, что число всевозможных конечных подмножеств множества M не более чем счётно. Докажем, что из отрицания а) следует отрицание б), т. е. докажем импликацию б) \Rightarrow а).

Пусть множество M не узко. Тогда в M существует бесконечное подмножество P попарно несравнимых элементов. Рассмотрим произвольное подмножество $Q \subseteq P$ и инвариантный класс $\langle Q \rangle = \{m \in M \mid \exists q \in Q \ m \leq q\}$. Если $Q_1 \subseteq P$, $Q_2 \subseteq P$ и $Q_1 \neq Q_2$, то $\langle Q_1 \rangle \neq \langle Q_2 \rangle$. Действительно, существует либо $q \in Q_1 \setminus Q_2$, либо $q \in Q_2 \setminus Q_1$. В первом случае элемент q несравним со всеми элементами из Q_2 , поэтому q не предшествует ни одному из них, а значит, $q \notin \langle Q_2 \rangle$, в то же время $q \in \langle Q_1 \rangle$; второй случай аналогичен. Таким образом, имеем континуум инвариантных классов $\langle Q \rangle$, $Q \subseteq P$, т. е. б) не выполнено.

Наконец докажем, что из отрицания с) следует отрицание а), т. е. импликацию а) \Rightarrow с). Пусть существует инвариантный класс K , который нельзя породить конечным множеством запретов. Пусть $P = M \setminus K$. В силу инвариантности K имеем $K = Z(M; P)$. Покажем, что $K = Z(M; \min P)$. Действительно, $K = Z(M; P) \subseteq Z(M; \min P)$. С другой стороны, если $t \in Z(M; \min P)$, то ни для одного $p \in \min P$ не выполнено $p \leq t$. Поэтому в P нет элемента q такого, что $q \leq t$ (в противном случае, если существует $q \in P$, $q \leq t$, то по утверждению 1 существует $p \in \min P$, $p \leq q$, а тогда $p \leq t$; противоречие). Следовательно, $t \in Z(M; P) = K$. Элементы множества $\min P$ попарно несравнимы, в то же время класс K не может быть порождён конечным множеством запретов. Поэтому $\min P$ — бесконечное множество, а значит, M не узко. Лемма 1 доказана.

Объединением непересекающихся ЧУМ M_1 и M_2 называется их теоретико-множественное объединение $M_1 \cup M_2$ с отношением частичного порядка, унаследованным от множеств M_1 и M_2 ; при этом элементы $m_1 \in M_1$ и $m_2 \in M_2$ считаются несравнимыми. *Произведением* ЧУМ M_1 и M_2 называется их декартово произведение $M_1 \times M_2$ с покоординатным отношением частичного порядка $((m_1, m_2) \leq (m'_1, m'_2) \iff m_1 \leq m'_1 \text{ и } m_2 \leq m'_2)$.

Лемма 2. Пусть M_1 и M_2 — узкие короткие ЧУМ. Тогда множества $M_1 \cup M_2$ и $M_1 \times M_2$ узки и коротки.

Доказательство. Сначала рассмотрим объединение множеств $M = M_1 \cup M_2$. Из любой бесконечно убывающей цепи $m_1 > m_2 > \dots$ в M можно выбрать бесконечно убывающую подцепь, состоящую только из элементов множества M_1 или только из элементов M_2 . Аналогично из бесконечного множества $\{m_1, m_2, \dots\}$ попарно несравнимых элементов в M можно выбрать бесконечное подмножество, состоящее только из элементов M_1 или только из элементов M_2 . Поэтому если множества M_1 и M_2 являются узкими (короткими), то множество M является узким (коротким).

Теперь рассмотрим множество $M' = M_1 \times M_2$. Пусть M' не является коротким. Тогда в M' существует бесконечно убывающая последовательность пар $(m_1^1, m_2^1) > (m_1^2, m_2^2) > \dots$. Рассмотрим множества $Q_i = \{m_j^i \mid j = 1, 2, \dots\}$, $i = 1, 2$. Хотя бы одно из них бесконечно в силу того, что пары (m_j^1, m_j^2) , $j = 1, 2, \dots$ попарно различны. Пусть, например, Q_1 бесконечно. Тогда из множества Q_1 можно выбрать бесконечно убывающую цепь в M_1 , т. е. множество M_1 является коротким, что противоречит условию леммы.

Пусть теперь M' не узко. Тогда в нём найдётся бесконечное множество несравнимых пар $\{m_j^i = (m_j^3, m_j^4) \mid j = 1, 2, \dots\}$. Рассмотрим множество $Q_3 = \{m_j^3 \mid j = 1, 2, \dots\}$. Если оно конечно, то, начиная с некоторого N , имеем $m_N^3 = m_{N+1}^3 = \dots$. Поэтому множество $\{m_j^4 \mid j \geq N\} \subseteq M_2$ является примером бесконечного множества, состоящего из попарно несравнимых элементов, чего быть не может. Следовательно, Q_3 бесконечно. Тогда по утверждению 2 из Q_3 можно выбрать бесконечно возрастающую цепь $m_{i(1)}^3 < m_{i(2)}^3 < \dots$ (множество Q_3 является узким и коротким как подмножество множества M_1). Рассмотрим множество элементов $Q_4 = \{m_{i(1)}^4, m_{i(2)}^4, \dots\}$ (парных к элементам выбранной бесконечно возрастающей цепи). Если Q_4 конечно, то для некоторого N' имеем $m_{i(N')}^4 = m_{i(N'+1)}^4$. Следовательно, $m'_{i(N')} < m'_{i(N'+1)}$, что противоречит несравнимости этих пар. Остаётся рассмотреть случай, когда Q_4 бесконечно. В этом случае по утверждению 2 из Q_4 можно выбрать бесконечно возрастающую последовательность $m_{i(j(1))}^4 < m_{i(j(2))}^4 < \dots$

Числа $j(1), j(2), \dots$ попарно различны. Следовательно, найдётся такое N'' , что $j(N'') < j(N'' + 1)$. Поэтому $m'_{i(j(N''))} < m'_{i(j(N''+1))}$, что противоречит несравнимости этих пар. Лемма 2 доказана.

Утверждение 3. Если M является узким и коротким ЧУМ, то множество $I(M)$ коротко.

Доказательство. Пусть, напротив, в M существует бесконечно убывающая последовательность инвариантных классов $K_1 \supset K_2 \supset \dots$. Тогда существует последовательность элементов $m_1 \in K_1 \setminus K_2$, $m_2 \in K_2 \setminus K_3, \dots$. Ни для каких $i < j$ не выполнено неравенство $m_i \leq m_j$, иначе $m_i \in K_j$, что противоречит включению $m_i \in K_i \setminus K_{i+1} \subseteq K_i \setminus K_j$. Множество $Q = \{m_1, m_2, \dots\}$ бесконечно; оно коротко и узко как подмножество множества M . Согласно утверждению 2 в Q существует бесконечно возрастающая цепь $m_{i(1)} < m_{i(2)} < \dots$. Числа $i(1), i(2), \dots$ попарно различны. Поэтому найдётся N такое, что $i(N) < i(N + 1)$. Тогда $m_{i(N)} < m_{i(N+1)}$, что противоречит выбору элементов m_1, m_2, \dots . Утверждение 3 доказано.

3. Формулы над сигнатурами

Зафиксируем целое неотрицательное число n . Пусть M_0, \dots, M_n — короткие, не более чем счётные ЧУМ. Набор $\Sigma = (M_0, \dots, M_n)$ назовём *сигнатурой*. Индуктивно определим *формулы над сигнатурой* Σ . Формулами являются выражения, имеющие вид m_0 , где $m_0 \in M_0$, или $m_s(F_1, \dots, F_s)$, где $m_s \in M_s$, $1 \leq s \leq n$, и каждое выражение F_1, \dots, F_s является ранее построенной формулой над Σ . Примером сигнатуры является набор $\Sigma_0(B) = (B(0) \cup \{x_1, x_2, \dots\}, B(1), \dots, B(n))$, где $B(i)$ — множество всех i -местных функций из базиса B (все функции и переменные попарно несравнимы, n равно наибольшему числу переменных у функций из B). Формулами над $\Sigma_0(B)$ являются формулы в базисе B . Другой пример — сигнатура $\Sigma(B) = (\{y^0, y^1\}, \emptyset, B'(2), \dots, B'(n))$, формулами над которой являются формулы вида $F'_B(g)$. Сигнатуру (M_0, \dots, M_n) назовём *узкой*, если множества M_0, \dots, M_n узки. Сигнатура $\Sigma(B)$ является узкой, а $\Sigma_0(B)$ не является.

Пусть F — формула над Σ . *Подформулой* формулы F называется произвольная формула (включая F), возникшая в процессе индуктивного построения формулы F по определению. Введём понятие *предшествования* формул. Для этого определим элементарные операции *горизонтального* и *вертикального сжатия* формулы. Пусть F — формула над Σ , G — её подформула и G имеет вид $m_s(G_1, \dots, G_s)$, где $m_s \in M_s$, G_1, \dots, G_s — формулы. Обозначим через $F_{G \rightarrow G_i}$ формулу, полученную из F заменой подформулы G (точнее, её рассматриваемого экземпляра) на формулу G_i , $1 \leq i \leq s$. Переход от F к $F_{G \rightarrow G_i}$ назовём элементарной

операцией горизонтального сжатия формулы. Элементарной операцией вертикального сжатия назовём замену в формуле одного вхождения символа $m_s \in M_s$, $0 \leq s \leq n$, (являющегося началом подформулы с s аргументами) на символ $m'_s \in M_s$ такой, что $m'_s < m_s$. Будем говорить, что формула H предшествует формуле F , если H может быть получена из F за конечное (возможно, нулевое) число применений элементарных операций горизонтального и вертикального сжатия. Обозначим через $\mathcal{F}(\Sigma)$ частично упорядоченное множество формул в сигнатуре Σ с отношением предшествования формул.

Утверждение 4. Для любой сигнатуры Σ множество $\mathcal{F}(\Sigma)$ коротко и не более чем счётно.

Доказательство. Не более чем счётность множества $\mathcal{F}(\Sigma)$ следует из того, что формулы являются словами не более чем в счётном алфавите $\{(' , ') , ', '\} \cup M_0 \cup \dots \cup M_n$, а множество всех таких слов не более чем счётно. Докажем короткость множества $\mathcal{F}(\Sigma)$. Действительно, в противном случае существует бесконечная цепь формул $F_1 > F_2 > \dots$ такая, что F_{i+1} получена из F_i элементарной операцией горизонтального или вертикального сжатия. К любой формуле операцию горизонтального сжатия можно применить лишь конечное число раз, так как длина формулы каждый раз уменьшается. Поэтому начиная с некоторого N в последовательности F_N, F_{N+1}, \dots применяется только операция вертикального сжатия. Найдётся такое j и такое вхождение в формулу F_N символа из множества M_j , к которому операция вертикального сжатия применяется в последовательности F_N, F_{N+1}, \dots бесконечное число раз. Следовательно, в множестве M_j существует бесконечно убывающая цепь элементов, что противоречит его короткости, требуемой в определении сигнатуры. Утверждение 4 доказано.

Расширенной сигнатурой назовём пару $\Sigma' = (\Sigma, R)$, где Σ — сигнатура, $R \subseteq \mathcal{F}(\Sigma)$ и $|R| \leq 1$, т. е. R либо пусто, либо содержит одну формулу над Σ . Положим $\mathcal{F}(\Sigma') := Z(\mathcal{F}(\Sigma); R)$. Пусть Σ_1 и Σ_2 — сигнатуры, $\Sigma_i = (M_0^i, \dots, M_n^i)$, $i = 1, 2$. Скажем, что Σ_1 *строго предшествует* сигнатуре Σ_2 ($\Sigma_1 \prec \Sigma_2$), если для некоторого i , $0 \leq i \leq n$, выполнены равенства $M_n^1 = M_n^2, \dots, M_{i+1}^1 = M_{i+1}^2$, но $M_i^1 \subset M_i^2$, причём M_i^1 является инвариантным классом в M_i^2 . Пусть теперь Σ'_1 и Σ'_2 — расширенные сигнатуры, $\Sigma'_i = (\Sigma_i, R_i)$, $i = 1, 2$. Скажем, что Σ'_1 *строго предшествует* сигнатуре Σ'_2 ($\Sigma'_1 \prec \Sigma'_2$), если либо $\Sigma_1 \prec \Sigma_2$, либо $\Sigma_1 = \Sigma_2$ и реализуется один из двух случаев: 1) $R_2 = \emptyset$, $R_1 \neq \emptyset$; 2) $R_2 = \{F_2\}$, $R_1 = \{F_1\}$, и F_1 является собственной подформулой формулы F_2 (*собственная подформула* — подформула, отличная от самой формулы). Расширенную сигнатуру назовём *узкой*, если входящая в неё сигнатура узка.

Лемма 3. *Не существует бесконечной последовательности узких расширенных сигнатур $\Sigma'_1, \Sigma'_2, \dots$, в которой каждая следующая сигнатура строго предшествует предыдущей (другими словами, класс *) узких расширенных сигнатур короток).*

ДОКАЗАТЕЛЬСТВО. Пусть, напротив, существует такая последовательность: $\dots \prec \Sigma'_2 \prec \Sigma'_1$, $\Sigma'_i = (\Sigma_i, R_i)$, $\Sigma_i = (M_0^i, \dots, M_n^i)$, $i = 1, 2, \dots$. Возможны два случая: 1) в последовательности $\Sigma_1, \Sigma_2, \dots$ имеется бесконечное число различных сигнатур; 2) среди $\Sigma_1, \Sigma_2, \dots$ число различных сигнатур конечно.

В первом случае обозначим через i наименьшее из чисел $0, \dots, n$, удовлетворяющее условию: для любого $j > i$ найдётся такое N_j , что $M_j^{N_j} = M_j^{N_j+1} = \dots$. Если такого числа i нет, то начиная с некоторого N^j имеем $\Sigma_{N^j} = \Sigma_{N^j+1} = \dots$, что противоречит условию случая 1). Обозначим через N максимальное из чисел $N_{i+1}, \dots, N_n, 1$. Тогда последовательность множеств M_i^N, M_i^{N+1}, \dots , с одной стороны, монотонно (нестрого) убывает по включению, а с другой — в силу выбора i число различных элементов в ней бесконечно. Поэтому в ней существует строго убывающая подпоследовательность $M_i^N = Q_1 \supset Q_2 \supset \dots$. Каждое множество Q_i является инвариантным классом в Q_{i-1} , т. е. Q_1, Q_2, \dots — бесконечно убывающая последовательность инвариантных классов в узком (по условию леммы) и коротком (по определению сигнатуры) множестве M_i^N , чего не может быть согласно утверждению 3.

Во втором случае найдётся номер N такой, что $\Sigma_N = \Sigma_{N+1} = \dots$. Рассмотрим последовательность R_{N+1}, R_{N+2}, \dots (возможно, $R_N = \emptyset$). Каждое множество R_i содержит формулу F_i над Σ_N , причём F_{i+1} является собственной подформулой формулы F_i , $i = N+1, N+2, \dots$. При переходе от формулы к её подформуле длина формулы уменьшается. Поэтому описанная бесконечная последовательность формул невозможна. Полученное противоречие доказывает лемму 3.

Положим $\Sigma_\emptyset = (\emptyset, \dots, \emptyset)$, $\Sigma'_\emptyset = (\Sigma_\emptyset, \emptyset)$; сигнатура Σ'_\emptyset называется *пустой*.

Утверждение 5 (об индукции по короткому классу) Пусть P — предикат, заданный на расширенных сигнатурах, для которого выполнены условия:

- а) $P(\Sigma'_\emptyset)$ истинно;
- б) если Σ' — непустая узкая расширенная сигнатура и для любой узкой расширенной сигнатуры Σ'_1 , строго предшествующей сигнатуре Σ' , выражение $P(\Sigma'_1)$ истинно, то $P(\Sigma')$ истинно.

*) В смысле аксиоматики теории множеств Гёделя — Бернайса.

Тогда для любой узкой расширенной сигнатуры Σ' выражение $P(\Sigma')$ истинно.

Доказательство. Предположим противное, т. е. для некоторой узкой расширенной сигнатуры Σ'_1 выражение $P(\Sigma'_1)$ ложно. Очевидно, что $\Sigma'_1 \neq \Sigma'_\emptyset$. Поэтому согласно отрицанию свойства б) существует такая узкая расширенная сигнатура Σ'_2 , строго предшествующая сигнатуре Σ'_1 , что выражение $P(\Sigma'_2)$ ложно. Действуя так далее, получим бесконечно убывающую последовательность узких расширенных сигнатур $\dots \prec \Sigma'_2 \prec \Sigma'_1$, что противоречит лемме 3. Утверждение 5 доказано.

Лемма 4 (основная). Для любой узкой расширенной сигнатуры Σ' множество $\mathcal{F}(\Sigma')$ узко.

Доказательство. Проведём индукцию, опираясь на утверждение 5. В качестве предиката P возьмём утверждение об узости множества $\mathcal{F}(\Sigma')$. Так как множество $\mathcal{F}(\Sigma'_\emptyset)$ пусто, то оно узко. Следовательно, условие а) утверждения 5 выполнено. Проверим условие б). Пусть $\Sigma' = (\Sigma, R)$ — произвольная непустая узкая расширенная сигнатура, $\Sigma = (M_0, \dots, M_n)$. Рассмотрим два случая: 1) $R = \emptyset$; 2) $R \neq \emptyset$.

Случай 1. Докажем, что множество $I(\mathcal{F}(\Sigma))$ не более чем счётно. Пусть $K \subset \mathcal{F}(\Sigma)$ — произвольный инвариантный класс, отличный от множества $\mathcal{F}(\Sigma)$. Тогда существует формула $F \in \mathcal{F}(\Sigma)$, не принадлежащая K . Имеем $K \subseteq Z(\mathcal{F}(\Sigma); \{F\}) = \mathcal{F}(\Sigma'_F)$, где $\Sigma'_F = (\Sigma, \{F\})$. Очевидно, что K является инвариантным классом в множестве $\mathcal{F}(\Sigma'_F)$. Следовательно,

$$I(\mathcal{F}(\Sigma)) = \{\mathcal{F}(\Sigma)\} \cup \bigcup_{F \in \mathcal{F}(\Sigma)} I(\mathcal{F}(\Sigma'_F)). \quad (2)$$

По определению, каждая сигнатура Σ'_F строго предшествует сигнатуре Σ' , кроме того, Σ'_F узка (в силу узости сигнатуры Σ). По предположению индукции множество $\mathcal{F}(\Sigma'_F)$ узко. Следовательно, по лемме 1 число инвариантных классов в $\mathcal{F}(\Sigma'_F)$ не более чем счётно (короткость и не более чем счётность множества $\mathcal{F}(\Sigma)$, а значит, и его подмножества $\mathcal{F}(\Sigma'_F)$ следует из утверждения 4). В силу равенства (2) множество $I(\mathcal{F}(\Sigma))$ не более чем счётно как объединение не более чем счётного числа не более чем счётных множеств. Опять же по лемме 1 множество $\mathcal{F}(\Sigma)$ узко. Случай 1 в силу равенства $\mathcal{F}(\Sigma') = \mathcal{F}(\Sigma)$ рассмотрен.

Случай 2. Пусть $R = \{F\}$. Если формула F имеет вид m_0 , $m_0 \in M_0$, то инвариантный класс $\mathcal{F}(\Sigma')$, равный $Z(\mathcal{F}(\Sigma); \{F\})$, состоит из тех и только тех формул над Σ , в которых нет подформулы вида m , где $m \in M_0$ и $m \geq m_0$. Таким образом, справедливо равенство $\mathcal{F}(\Sigma') = \mathcal{F}(\Sigma'_0)$,

где $\Sigma'_0 = (\Sigma_0, \emptyset)$, $\Sigma_0 = (Z(M_0; \{m_0\}), M_1, \dots, M_n)$. По определению, сигнатура Σ'_0 строго предшествует сигнатуре Σ' и узка в силу узости сигнатуры Σ' . Следовательно, по предположению индукции множество $\mathcal{F}(\Sigma'_0)$ узко. Тогда множество $\mathcal{F}(\Sigma')$ узко.

Наконец, рассмотрим случай, когда формула F имеет вид $m_s(F_1, \dots, F_s)$, где $m_s \in M_s$ и F_1, \dots, F_s — формулы над Σ . Обозначим через Σ'_i , $1 \leq i \leq s$, расширенную сигнатуру $(\Sigma, \{F_i\})$. Так как формула F_i является подформулой формулы F , то сигнатура Σ'_i предшествует сигнатуре Σ' . Кроме того, Σ'_i узка в силу узости сигнатуры Σ . Применив к Σ'_i предположение индукции, получим, что множество $\mathcal{F}(\Sigma'_i)$ узко.

Рассмотрим произвольную формулу G из множества $\varphi(\Sigma')$ и её произвольную подформулу H вида

$$m'(H_1, \dots, H_s), \text{ где } m' \in M_s \text{ и } H_1, \dots, H_s \text{ — формулы.} \quad (3)$$

Множество $\mathcal{F}(\Sigma')$ состоит только из таких формул G над Σ , что для каждой подформулы H вида (3) формулы G либо $m' \not\geq m_s$, либо для некоторого i формула H_i не предшествует формуле F_i , т. е. $H_i \in \mathcal{F}(\Sigma'_i)$.

Пусть $K_0 = \{(0, m) \mid m \in M_{s-1}\}$, $K_i = \{(i, m, H'_i) \mid m \in M_s, H'_i \in \mathcal{F}(\Sigma'_i)\}$, $1 \leq i \leq s$, и $M'_s = K_0 \cup K_1 \cup \dots \cup K_s$. На множестве K_0 введём частичный порядок: $(0, m) \leq (0, m'') \iff m \leq m''$. При этом K_0 изоморфно множеству M_{s-1} . На K_i при $i > 0$ также введём частичный порядок: $(i, m, H'_i) \leq (i, m'', H''_i) \iff m \leq m''$ и H'_i предшествует формуле H''_i . ЧУМ K_i изоморфно произведению $M_s \times \mathcal{F}(\Sigma'_i)$. Множество M'_s узко, коротко (в силу леммы 2 как конечное объединение произведений узких, коротких ЧУМ); узость множеств $\mathcal{F}(\Sigma'_i)$ мы уже показали, их короткость следует из утверждения 4) и не более чем счётно.

Введём сигнатуру $\Sigma_\bullet = (M_0, \dots, M_{s-2}, M'_{s-1}, Z(M_s; \{m_s\}), M_{s+1}, \dots, M_n)$ и расширенную сигнатуру $\Sigma'_\bullet = (\Sigma_\bullet, \emptyset)$. Построим отображение $\varphi : \mathcal{F}(\Sigma') \rightarrow \mathcal{F}(\Sigma_\bullet)$. Пусть $G \in \mathcal{F}(\Sigma')$. Построим последовательность таких формул $G = G_0, G_1, \dots, G_r$, что каждая следующая формула получена из предыдущей описанным ниже преобразованием, а к G_r это преобразование не применимо. Обозначим через H самую левую максимальную по включению подформулу формулы G_t ($t = 0, \dots, r-1$) среди тех подформул вида (3), в которых $m' \geq m_s$. Если таких подформул нет, то преобразование не применимо. Пусть i такой минимальный индекс, что $H_i \in \mathcal{F}(\Sigma'_i)$. Подформулу H в G_t заменим формулой $(i, m', H_i)(H_1, \dots, H_{i-1}, H_{i+1}, \dots, H_s)$ (другими словами, включим подформулу H_i в имя функции) и полученную формулу примем за G_{t+1} . Так как каждый раз H выбирается максимальной, то к формуле H и её

подформулам ранее не были применены никакие преобразования. Поэтому $H \in \mathcal{F}(\Sigma')$, что необходимо для наличия требуемой подформулы H_i .

Наконец, каждую подформулу H' формулы G_r вида $m_{s-1}(H'_1, \dots, H'_{s-1})$, где $m_{s-1} \in M_{s-1}$ и H'_1, \dots, H'_{s-1} — формулы, заменим формулой $(0, m_{s-1})(H'_1, \dots, H'_{s-1})$. В результате получим формулу над сигнатурой Σ_\bullet , которую и примем за $\varphi(G)$. Заметим, что формула G восстанавливается по своему образу $\varphi(G)$ однозначно, т. е. φ — инъекция. Заметим также, что обратное отображение φ^{-1} (определённое на образе отображения φ) сохраняет отношение частичного порядка, т. е. если $\varphi(G') \leq \varphi(G'')$, то $G' \leq G''$ (операции вертикального сжатия формул над Σ_\bullet , производимой с третьей координатой набора из множества $K_1 \cup \dots \cup K_s$, соответствует операция горизонтального сжатия формул над Σ). Следовательно, если формулы G' и G'' не сравнимы, то и формулы $\varphi(G')$ и $\varphi(G'')$ не сравнимы.

Сигнатура Σ'_\bullet строго предшествует сигнатуре Σ' и узко (ранее мы показали, что множество M'_{s-1} узко). Применив к Σ'_\bullet предположение индукции, получим, что множество $\mathcal{F}(\Sigma'_\bullet)$ узко. Поэтому множество $\mathcal{F}(\Sigma')$ узко. Действительно, если $\mathcal{F}(\Sigma')$ не узко, то в нём найдётся бесконечное множество попарно несравнимых элементов $\{G_1, G_2, \dots\}$. Тогда множество формул $\{\varphi(G_1), \varphi(G_2), \dots\}$ в сигнатуре $\mathcal{F}(\Sigma'_\bullet)$ бесконечно и состоит из попарно несравнимых элементов, что невозможно. Лемма 4 доказана.

4. Доказательство основных утверждений

Пусть $K \subseteq \mathcal{E}(B)$ — произвольный инвариантный класс. Обозначим через K^* множество всех функций из K , тождественно не равных константе. Классу $K \subseteq \mathcal{E}(B)$ поставим в соответствие множество формул $\psi_B(K) \subseteq \mathcal{F}(\Sigma(B))$, а именно $\psi_B(K)$ состоит из всевозможных формул $F'_B(g)$ для функций $g \in K^*$.

Лемма 5. Для любого инвариантного класса $K \subseteq \mathcal{E}(B)$ множество $\psi_B(K)$ является инвариантным классом в $\mathcal{F}(\Sigma(B))$, причём множество K^* однозначно восстанавливается по $\psi_B(K)$.

Доказательство. Пусть $K' = \psi_B(K)$. Покажем, что K' — инвариантный класс в $\mathcal{F}(\Sigma(B))$. Рассмотрим произвольную формулу $F'_B(g) \in K'$ и связанную с ней формулу $F_B(g)$. Пусть формула F'_1 над $\Sigma(B)$ предшествует формуле $F'_B(g)$; для простоты будем считать, что F'_1 получена из $F'_B(g)$ за одну операцию горизонтального сжатия, а именно $F'_1 = (F'_B(g))_{G' \rightarrow G'_i}$ (вертикальное сжатие неприменимо, так как все элементы множеств сигнатуры $\Sigma(B)$ попарно несравнимы).

Рассмотрим соответствующую формуле G' подформулу G формулы $F_B(g)$. Пусть $G = f'(G_1, \dots, G_s)$, где $f' \in B'$ и формулы G_1, \dots, G_s соответствуют подформулам G'_1, \dots, G'_s формулы G' . В силу неубывания функции f' ни по одной переменной существуют такие константы $c_1, \dots, c_{i-1}, c_{i+1}, \dots, c_s$, что выполнено тождество (1). Далее, функция, реализуемая формулой G_j , $j = 1, \dots, i-1, i+1, \dots, n$, существенно зависит хотя бы от одной переменной (как неповторная суперпозиция функций, отличных от констант). Поэтому при некоторой подстановке констант вместо её переменных получится формула, тождественно равная c_j .

Таким образом, при некоторой подстановке констант вместо переменных формула G становится тождественно равной формуле G_i . Обозначим через F_1 формулу, полученную из $F_B(g)$ заменой подформулы G на G_i . Формула F_1 реализует некоторую подфункцию g' функции g и является своим неубывающим представителем. Поэтому $F_1 = F_B(g')$, а значит, $F'_1 = F'_B(g')$. Так как функция g' принадлежит множеству K^* , то $F'_1 \in K'$.

Итак, K' является инвариантным классом в $\mathcal{F}(\Sigma(B))$. Покажем, что класс K' однозначно восстанавливается по множеству K^* . Предположим противное, т. е. в $\mathcal{E}(B)$ существуют два класса K_1 и K_2 , соответствующие одному и тому же классу K' , но имеющие разные множества K_1^* и K_2^* . Пусть, например, существует функция $h_1 \in K_1^* \setminus K_2^*$. Тогда $F'_B(h_1) \in K'$. Поэтому существует такая функция $h_2 \in K_2^*$, что $F'_B(h_2) = F'_B(h_1)$. Из последнего равенства следует, что функции h_1 и h_2 различаются, может быть, несущественными переменными и порядком следования переменных. Значит, $h_1 \in K_2^*$. Противоречие. Лемма 5 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Из леммы 4 следует, что множество $\mathcal{F}(\Sigma(B))$ узко. Поэтому в силу леммы 1 множество $I(\mathcal{F}(\Sigma(B)))$ не более чем счётно. Пусть K — произвольный инвариантный класс из $\mathcal{E}(B)$. Заметим, что если множество K^* непусто, то класс K содержит обе константы. Следовательно, различным непустым множествам K^* соответствуют различные классы K . Тогда в силу леммы 5 ограничение отображения ψ на множество классов K , для которых $K^* \neq \emptyset$, является инъекцией. Образ этого отображения не более чем счётен, а значит, и число классов K с непустым множеством K^* не более чем счётно. Классов, состоящих только из констант, ровно четыре, поэтому число всех инвариантных классов в $\mathcal{E}(B)$ не более чем счётно. Это число не менее чем счётно, так как функции $x_1 \& \dots \& x_m$, $m = 1, 2, \dots$, неповторно выразимы в любом полном базисе, следовательно, инвариантные классы $K_m = \{0, 1, x_{i_1} \& \dots \& x_{i_j}, j \leq m\}$ составляют счётное его подмножество. Теорема 1 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Для произвольных $k > 2$ и $m \geq 1$ определим функцию

$$f_k^m(x_1, \dots, x_m) = \begin{cases} x_1, & \text{если } x_1 = x_2 = \dots = x_m; \\ 0, & \text{если среди } x_1, \dots, x_m \text{ есть различные.} \end{cases}$$

Положим $B_k = \{f_k^2, 0, 1, \dots, k-1\}$. Из тождества

$$f_k^m(x_1, \dots, x_{m-1}, f_k^2(x_m, x_{m+1})) = f_k^{m+1}(x_1, \dots, x_{m+1})$$

следует, что функция f_k^m бесповторно выразима в базисе B_k . При подстановке в функцию f_k^m хотя бы одной константы вместо переменной получится функция, не принимающая всех k значений. Так, при подстановке константы c вместо любой переменной полученная функция будет принимать только значения 0 и c . Следовательно, ни одна собственная подфункция функции f_k^m не является функцией вида $f_k^{m'}$, $m' \neq m$. Тогда минимальный инвариантный класс K_M , содержащий множество $\{f_k^m \mid m \in M\}$ (M — подмножество множества натуральных чисел), не содержит функций вида $f_k^{m'}$, $m' \notin M$. Поэтому если $M_1 \neq M_2$, то $K_{M_1} \neq K_{M_2}$. Следовательно, мощность множества инвариантных классов не меньше мощности множества всех подмножеств множества натуральных чисел, которое равно континууму. Искомая мощность также не больше континуума, так как мощность множества всевозможных подмножеств множества P_k равна континууму. Теорема 2 доказана.

Теперь рассмотрим способы задания инвариантных классов из множества $\mathcal{E}(B)$ для булева базиса B . Следующая теорема 3 позволяет произвольный такой класс породить в $\mathcal{E}(B)$ конечным множеством запрещённых подфункций.

Теорема 3. Пусть B — булев базис и $K \subseteq \mathcal{E}(B)$ — инвариантный класс. Тогда существует конечное множество функций $Q \subseteq \mathcal{E}(B)$ таких, что произвольная функция $g \in \mathcal{E}(B)$ принадлежит классу K тогда и только тогда, когда g не содержит в качестве подфункций ни одной функции из Q .

ДОКАЗАТЕЛЬСТВО. На множестве P_2 рассмотрим следующее отношение эквивалентности \sim : две функции эквивалентны, если одну из них можно получить из другой путём перестановки переменных, а также добавления и изъятия несущественных переменных. На фактор-множестве P_2/\sim введём отношение частичного порядка: класс функции g_1 предшествует классу функции g_2 , если g_1 эквивалентна некоторой подфункции функции g_2 . При этом имеется взаимно однозначное соответствие инвариантных классов в P_2 и инвариантных классов в P_2/\sim , рассматриваемом в смысле частично упорядоченного множества. Тогда в силу теоремы 1 число инвариантных классов в $\mathcal{E}(B)/\sim$ счётно, а значит, по

лемме 1 каждый такой класс порождён конечным множеством запретов Q' . В каждом классе эквивалентности из Q' выберем по одной функции и образуем множество Q , состоящее из всех выбранных функций и всех функций, полученных из выбранных путём перестановки переменных. Очевидно, что Q удовлетворяет условиям теоремы. Теорема 3 доказана.

Так как в силу результата В. А. Стеценко [2] класс $\mathcal{E}(\{\&, \vee, \neg\})$ нельзя породить в P_2 конечным множеством запрещённых подфункций, то в теореме 3 условие $g \in \mathcal{E}(B)$ нельзя заменить условием $g \in P_2$. Покажем, что каждый инвариантный класс из $\mathcal{E}(B)$ можно задать другим конечным способом — множеством формул, порождаемых некоторой контекстно-свободной грамматикой.

5. Контекстно-свободные грамматики

Сигнатуру $\Sigma = (M_0, \dots, M_n)$ назовём *простой*, если множества M_0, \dots, M_n конечны и все их элементы попарно не сравнимы. Пусть Σ — простая сигнатура и $A = \{\alpha_0, \alpha_1, \dots\}$ — счётный алфавит, буквы которого будем называть *метасимволами*. *Контекстно-свободной (КС) грамматикой формульного типа* над Σ назовём конечную систему \mathcal{G} правил вида

$$\alpha_i \rightarrow m_0, \quad \text{где } m_0 \in M_0, \quad (4)$$

или

$$\alpha_i \rightarrow m_s(\alpha_{i_1}, \dots, \alpha_{i_s}), \quad \text{где } m_s \in M_s, \quad s > 0, \quad i_1 \geq i, \dots, i_s \geq i. \quad (5)$$

Положим $M = M_0 \cup \dots \cup M_n \cup \{(' , ' '), (' , ' '), (' , ' ')\}$ и $M' = M \cup A$. Пусть v и w — слова в алфавите M' . Скажем, что слово w получено из v *применением* правила грамматики \mathcal{G} вида (4) или (5), если w получено заменой некоторого метасимвола α_i в слове v на соответствующую правую часть правила. Скажем, что слово w в алфавите M *выводимо* в грамматике \mathcal{G} , если существует последовательность слов $w_0 = \alpha_0, w_1, \dots, w_t = w$ в алфавите M' , в которой каждое следующее слово получено из предыдущего применением правила грамматики \mathcal{G} . Множество слов, выводимых в \mathcal{G} , обозначим через \mathcal{G}^* . Нетрудно видеть, что в \mathcal{G} можно вывести только формулы над Σ .

Обозначим через $\mathcal{G}(\alpha_j)$ грамматику, полученную из \mathcal{G} удалением всех правил вида (4) или (5), в которых $i < j$, и заменой каждого метасимвола $\alpha_{i'}$ в оставшихся правилах на символ $\alpha_{i'-j}$ (эта операция корректна в силу условий $i_1 \geq i, \dots, i_s \geq i$ в (5)). Слова, выводимые в грамматике $\mathcal{G}(\alpha_j)$, будем также называть словами, *выводимыми* в \mathcal{G} из символа α_j . Заметим, что грамматике \mathcal{G} можно поставить в соответствие ориентированный граф \mathcal{G}' , вершинами которого являются метасимволы,

а дуга, ориентированная от α_i в α_j , присутствует тогда и только тогда, когда для некоторого правила вида (5) метасимвол α_j входит в его правую часть. Согласно определению \mathcal{G} не содержит ориентированных циклов, за исключением петель. Можно было бы потребовать, чтобы этот граф являлся деревом с петлями, что равносильно данному выше определению (в смысле совпадения класса реализуемых языков): любой граф без ориентированных циклов, отличных от петель, можно привести к дереву с петлями дублированием отдельных фрагментов.

Лемма 6. Пусть \mathcal{G} — КС-грамматика формульного типа над Σ и F — формула над Σ . Тогда существует такая КС-грамматика формульного типа \mathcal{G}_F , что $\mathcal{G}_F^* = Z(\mathcal{G}^*; \{F\})$.

Доказательство. Проведём индукцию по длине формулы F .

БАЗИС ИНДУКЦИИ: $F = m_0$, где $m_0 \in M_0$. Для получения грамматики \mathcal{G}_F необходимо и достаточно удалить из \mathcal{G} все правила вида (4) с символом m_0 в правой части.

ИНДУКТИВНЫЙ ПЕРЕХОД: $F = m_s(F_1, \dots, F_s)$, где $m_s \in M_s$ и F_1, \dots, F_s — формулы над Σ . Пусть Π_1, \dots, Π_r — все правила вида (5) грамматики \mathcal{G} с начальным символом m_s в правой части. Рассмотрим произвольное из них — Π_l . По предположению индукции, применённому к грамматике $\mathcal{G}(\alpha_{i_j})$, $1 \leq j \leq s$, и формуле F_j , существует грамматика $\mathcal{G}_j = \mathcal{G}(\alpha_{i_j})_{F_j}$, в которой множество выводимых формул совпадает с множеством $Z(\mathcal{G}(\alpha_{i_j})^*; \{F_j\})$. Пусть N, N_1, \dots, N_s — наибольшие номера метасимволов, встречающихся в грамматиках $\mathcal{G}, \mathcal{G}_1, \dots, \mathcal{G}_s$ соответственно. Увеличим номера всех метасимволов грамматики \mathcal{G}_j , $1 \leq j \leq s$, на $N + N_1 + \dots + N_{j-1} + j$ (так, чтобы метасимволы разных грамматик не пересекались), полученные грамматики добавим к \mathcal{G} , удалим из неё правило Π_l и введём правила $\alpha_i \rightarrow m_s(\alpha_{N+1}, \alpha_{i_2}, \dots, \alpha_{i_s})$, $\alpha_i \rightarrow m_s(\alpha_{i_1}, \alpha_{N+N_1+2}, \alpha_{i_3}, \dots, \alpha_{i_s})$, \dots , $\alpha_i \rightarrow m_s(\alpha_{i_1}, \dots, \alpha_{i_{s-1}}, \alpha_{N+N_1+\dots+N_{s-1}+s})$, которые обозначим через Π_l^1, \dots, Π_l^s .

Описанную процедуру проделаем последовательно для всех правил Π_1, \dots, Π_l (грамматика \mathcal{G} при этом будет меняться, однако список Π_1, \dots, Π_l остаётся первоначальным). Полученную в результате грамматику обозначим через \mathcal{G}'_F . Далее удалим из \mathcal{G}'_F все правила, которые не могут быть применены ни в одном выводе, и оставшуюся грамматику примем за \mathcal{G}_F .

Пусть G — произвольная формула, которой предшествует F . Заметим, что если для любого правила вида (5) грамматики \mathcal{G}_F (с тем же начальным символом m_s) такого, что хотя бы из одного символа α_{i_j} не может быть выведена никакая формула, которой предшествует F_j , то G не может быть выведена в \mathcal{G}_F . Пусть Π — такое правило. Тогда либо $\Pi = \Pi_l^j$ для некоторых l, j , либо Π — правило некоторой грамматики \mathcal{G}_j ,

(с переименованными метасимволами). В первом случае из символа α_{i_j} не может быть выведена формула F_j . Во втором случае в грамматике $\mathcal{G}_{j'}$ не может быть выведена формула $F_{j'}$. Следовательно, формула $F_{j'}$ не может быть выведена ни из одного метасимвола, имеющегося в правой части правила Π . Таким образом, мы показали, что G не может быть выведена в грамматике \mathcal{G}_F .

С другой стороны, в \mathcal{G}_F может быть выведена любая формула из \mathcal{G}^* , которой не предшествует F . Действительно, пусть F не предшествует формуле G' . Будем выводить формулу G' в грамматике \mathcal{G}_F так же, как она выводилась в \mathcal{G} , до тех пор, пока не встретится применение правила Π_i вида (5) с данным начальным символом m_s . Далее вывод в \mathcal{G} формулы G' шёл таким образом, что хотя бы из одного символа α_{i_j} была выведена некоторая формула G'_j , которой не предшествует F_j . В противном случае формуле G' предшествовала бы F . Тогда вместо правила Π_i применим правило Π_j^j . По предположению индукции из символа $\alpha_{N+N_1+\dots+N_{j-1}+j}$ можно вывести требуемую формулу G'_j . К остальным символам $\alpha_{i_{j'}}$, $j' \neq j$, применимы прежние рассуждения. Лемма 6 доказана.

Лемма 7. Пусть Σ — простая сигнатура и K — инвариантный класс в $\mathcal{F}(\Sigma)$. Тогда существует такая КС-грамматика формульного типа \mathcal{G} над сигнатурой Σ , что $\mathcal{G}^* = K$.

Доказательство. Согласно лемме 4 множество $\mathcal{F}(\Sigma)$ узко. Поэтому в силу леммы 1 класс K может быть задан в $\mathcal{F}(\Sigma)$ конечным множеством запретов: $K = Z(\mathcal{F}(\Sigma); \{F_1, \dots, F_p\})$. Проведём индукцию по числу p .

Базис индукции: $p = 0$. В этом случае $K = \mathcal{F}(\Sigma)$. Очевидно, что множество всех формул над Σ задаётся следующей грамматикой:

$$\{\alpha_0 \rightarrow m_0 \mid m_0 \in M_0\} \cup \{\alpha_0 \rightarrow m_s(\alpha_0, \dots, \alpha_0) \mid m_s \in M_s, 1 \leq s \leq n\}.$$

Индуктивный переход: $p \geq 1$. По предположению индукции класс $K_1 = Z(\mathcal{F}(\Sigma); \{F_1, \dots, F_{p-1}\})$ задаётся некоторой грамматикой \mathcal{G}_1 . Очевидно, что $K = Z(K_1; \{F_p\})$. Поэтому в силу леммы 6 класс K также задаётся некоторой грамматикой \mathcal{G} . Лемма 7 доказана.

Теорема 4. Пусть K — инвариантный класс булевых функций и $K \subseteq \mathcal{E}(B)$. Тогда существует КС-грамматика формульного типа \mathcal{G} над сигнатурой $\Sigma(B)$ такая, что множество K^* содержит только такие функции, которые можно задать формулами, получающимися из формул множества \mathcal{G}^* посредством замены символов y^1 (y^0) на попарно различные переменные (их отрицания).

Доказательство. Рассмотрим класс $K' = \psi_B(K) \subseteq \mathcal{F}(\Sigma(B))$. Согласно лемме 5 он инвариантен. Поэтому в силу леммы 7 его можно

задать некоторой КС-грамматикой \mathcal{G} формульного типа (т. е. $K' = \mathcal{G}^*$). Пусть $g \in K^*$. Формулу $F_B(g)$ можно получить из соответствующей формулы $F'_B(g)$ путём замены символов y^1 (y^0) на попарно различные переменные (с отрицаниями). Любая другая формула, полученная из $F'_B(g)$ тем же способом, реализует некоторую функцию g' , которая может быть получена из g перестановкой переменных, добавлением и отбрасыванием несущественных переменных. Поэтому $g' \in K^*$. Теорема 4 доказана.

ЛИТЕРАТУРА

1. **Кузнецов А. В.** О неповторных контактных схемах и неповторных суперпозициях функций алгебры логики // Сборник статей по математической логике и её приложениям к некоторым вопросам кибернетики. М.: Изд-во АН СССР, 1958. С. 186-225. (Тр. Мат. ин-та им. В. А. Стеклова; Т. 51).
2. **Стеценко В. А.** О предположих базисах в P_2 // Мат. вопросы кибернетики. Вып. 4. М.: Наука, 1992. С. 139-177.
3. **Яблонский С. В.** Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. Вып. 2. М.: Физматгиз, 1959. С. 75-121.

Адрес автора:
МГУ, мех.-мат. факультет,
Воробьевы горы,
119992 Москва, Россия.

Статья поступила
6 мая 2002 г.