КРАТКИЕ СООБЩЕНИЯ

УДК 519.7

Г. Г. Аманжаев

О ЗАМЫКАНИИ НЕНУЛЕВОГО ИНВАРИАНТНОГО КЛАССА ЯБЛОНСКОГО ПО ОПЕРАЦИИ ОТОЖДЕСТВЛЕНИЯ ПЕРЕМЕННЫХ

В данной работе доказывается, что замыкание любого ненулевого инвариантного класса булевых функций по операции отождествления переменных совпадает с множеством всех функций алгебры логики.

Класс Q функций алгебры логики называется *инвариантным* [1, 2], если он замкнут относительно операций подстановки констант, переименования (без отождествления) переменных и добавления или изъятия несущественных переменных. Пусть $Q_n \subset Q$ содержит функции от n переменных $x_1, ..., x_n$.

Понятие инвариантного класса было введено С. В. Яблонским [2]; было показано, что для любого инвариантного класса Q последовательность величин $2^{-n}\log_2|Q_n|$ является невозрастающей и имеет предел $\sigma=\sigma(Q)\in[0, 1]$. Инвариантные классы Q, для которых $\sigma(Q)=0$, называются *нулевыми*, а остальные *ненулевыми*.

В настоящей работе доказывается следующее утверждение.

Теорема 1. *Замыкание любого ненулевого инвариантного класса по операции отождествления переменных состоит из всех булевых функций.*

Пусть f — булева функция. Обозначим через Q^f множество всех тех булевых функций, из которых операциями подстановки констант, переименования (возможно, с отождествлением) переменных и добавления/изъятия несущественных переменных нельзя получить f. Очевидно, что Q^f — инвариантный класс, и теореме 1 равносильна

Теорема 1′. *Для любой булевой функции f класс Q^f — нулевой.*

Обозначим $E_m=\{0, 1, \ldots, m-1\}$. Пусть $f(x_1, \ldots, x_n)$ — булева функция. Функцию $F: E_{m_1}\times \ldots \times E_{m_n} \to \{0, 1\}$ назовем *f-свободной*, если ни для каких отображений $\mu_i:\{0, 1\}\to E_{m_i}$, таких, что $\mu_i(0)<\mu_i(1)$, суперпозиция $F(\mu_1(x_1), \ldots, \mu_n(x_n))$ не совпадает с f. Обозначим через $a_f(m_1, \ldots, m_n)$ число f-свободных функций $F: E_{m_1}\times \ldots \times E_{m_n} \to \{0, 1\}$. Пусть $\tau_f(N)=\sup\limits_{m_1\geqslant N,\ldots,m_n\geqslant N} \sqrt[m_1\ldots m_n]{a_f(m_1, \ldots, m_n)}$, $\tau(f)=\lim\limits_{N\to\infty}\tau_f(N)$ ($\tau(f)$ имеет значение из отрезка $[1, 2]$).

Теорема 1′ вытекает из двух следующих утверждений.

Теорема 2. *Если* $\tau(f)=1$, *то* $\sigma(Q^f)=0$.

Теорема 3. $\tau(f)=1$ *для любой булевой функции* f.

Доказательство теоремы 2. Назовем последовательность точек $(\tilde{x}_0, \ldots, \tilde{x}_{m-1})$, $\tilde{x}_i=(x_{i1}, \ldots, x_{in})$, двоичного куба $\{0, 1\}^n$ *цепью* длины m, если $x_{i,j}\leqslant x_{i+1,j}$ и точки $\tilde{x}_i$ и $\tilde{x}_{i+1}$ отличаются ровно по одной координате. Как показано в [3], куб $\{0, 1\}^t$ можно представить в виде объединения попарно не пересекающихся цепей так, чтобы число цепей длины $t-2p+1$ было равно $C_t^p-C_t^{p-1}$; здесь $0\leqslant p\leqslant[t/2]$.

Назовем *короткими* цепи длины $\leqslant\sqrt[3]{t}$. Тогда число точек куба, которые при указанном разбиении принадлежат коротким цепям, не превосходит $2^t/\sqrt[6]{t}$.

Пусть nr-местная булева функция $g \in Q^f$ задана на $K = \underbrace{\{0, 1\}^r \times \ldots \times \{0, 1\}^r}_{n}$; пусть $Ц_i$ — цепь в i-м сомножителе этого произведения. Пусть $f_i(j)$ есть j-й элемент цепи $Ц_i$ $(0 \leqslant j < |Ц_i|)$. Тогда можно утверждать, что функция $F(x_1, \ldots, x_n) = g(f_1(x_1), \ldots, f_n(x_n))$ является f-свободной.

Идея дальнейшего доказательства состоит в разбиении «почти всего» куба K на произведения цепей большой длины; для каждого такого произведения порождаемая им функция F является f-свободной, а их число ограничено сверху по условию теоремы.

Доказательство теоремы 3. Рассмотрим более общее понятие, чем f-свободные функции: вместо условия «$F(\mu_1(x_1), \ldots, \mu_n(x_n)) \neq f(x_1, \ldots, x_n)$ ни для каких $\mu_1, \ldots, \mu_n$» рассмотрим условие, в котором f, вообще говоря, зависит от $\mu_1, \ldots, \mu_n$.

Обозначим $\Pi_r = \{(\mu_1, \ldots, \mu_r) \mid \mu_i : \{0, 1\} \to \mathbf{Z}_+, \mu_i(0) < \mu_i(1)\}$, $\Pi(m_1, \ldots, m_r) = \{(\mu_1, \ldots, \mu_r) \in \Pi_r \mid \mu_i(1) \leqslant m_i\}$, $\Psi_r = \{L : \Pi_r \to P_2^{(r)}\}$, $\Psi(m_1, \ldots, m_r) = \{L : \Pi(m_1, \ldots, m_r) \to P_2^{(r)}\}$ ($P_2^{(r)}$ — множество всех функций $f : \{0, 1\}^r \to \{0, 1\}$).

Будем говорить, что функция $F : E_{m_1} \times \ldots \times E_{m_r} \to \{0, 1\}$ является *L-свободной* ($L \in \Psi(m_1, \ldots, m_r)$), если ни при каком выборе $(\mu_1, \ldots, \mu_r) \in \Pi(m_1, \ldots, m_r)$ не совпадут булевы функции $f_1(x_1, \ldots, x_r) = F(\mu_1(x_1), \ldots, \mu_r(x_r))$ и $f_2 = L(\mu_1, \ldots, \mu_r)$. Для записи утверждения „F является L-свободной“ введем обозначение $F \| L$. Заметим, что если оператор L — константа, т. е. любое его значение — одна и та же булева функция f, то $F \| L$ — это то же самое, что и условие „F является f-свободной“.

Обозначим через $W_L(m_1, \ldots, m_r)$ число L-свободных функций $F : E_{m_1} \times \ldots \times E_{m_r} \to \{0, 1\}$. Пусть также

$$W(m_1, \ldots, m_r) = \max_{L \in \Psi(m_1, \ldots, m_r)} W_L(m_1, \ldots, m_r),$$

$$\tau_r(N) = \sup_{m_1 \geqslant N, \ldots, m_r \geqslant N} \sqrt[m_1 \ldots m_r]{W(m_1, \ldots, m_r)}.$$

Заметим, что $1 \leqslant \tau_f(N) \leqslant \tau_r(N)$, где r — число переменных у булевой функции f, а также $a_f(m_1, \ldots, m_r) \leqslant W(m_1, \ldots, m_r)$.

Тем самым достаточно показать, что при любом $r \in \mathbf{N}$, $N \to \infty$ имеет место оценка $\tau_r(N) \leqslant 1 + o(1)$. При $r = 1$ она следует из неравенства $W(m) \leqslant m + 1$. Для $r > 1$ применяется индукция по r.

Пусть Ψ_r' и $\Psi'(m_1, \ldots, m_r)$ — подмножества Ψ_r и $\Psi(m_1, \ldots, m_r)$, состоящие из тех операторов, которые не зависят от μ_r. Пусть

$$W'(m_1, \ldots, m_r) = \max_{L \in \Psi'(m_1, \ldots, m_r)} W_L(m_1, \ldots, m_r).$$

Будем говорить, что за функцией $G' : E_{m_1} \times \ldots \times E_{m_{r-1}} \to \{0, 1\}$ может *L-следовать* функция $G'' : E_{m_1} \times \ldots \times E_{m_{r-1}} \to \{0, 1\}$, где $L \in \Psi_r'$ или $\Psi'(m_1, \ldots, m_r)$, если функция $\vec{G} : E_{m_1} \times \ldots \times E_{m_{r-1}} \times \{0, 1\} \to \{0, 1\}$, заданная следующим образом:

$$\vec{G}(x_1, \ldots, x_r) = \begin{cases} G'(x_1, \ldots, x_{r-1}), & x_r = 0; \\ G''(x_1, \ldots, x_{r-1}), & x_r = 1, \end{cases}$$

является L-свободной. Обозначим этот факт посредством $G' \xrightarrow{L} G''$.

Для того чтобы $F : E_{m_1} \times \ldots \times E_{m_r} \to \{0, 1\}$ была L-свободной ($L \in \Psi'$), необходимо и достаточно, чтобы в последовательности $\{F_0, \ldots, F_{m_r - 1}\}$, где $F_i(x_1, \ldots, x_{r-1}) = F(x_1, \ldots, x_{r-1}, i)$, при $p < q$ было выполнено $F_p \xrightarrow{L} F_q$, т. е. $W_L(m_1, \ldots, m_r)$ есть число последовательностей $\{F_0, \ldots, F_{m_r-1}\}$, где $F_i: E_{m_1} \times \ldots \times E_{m_{r-1}} \to \{0, 1\}$ и $F_p \xrightarrow{L} F_q$ при $0 \leqslant p < q < m_r$.

Можно показать, что при $L \in \Psi_r'$, $m_1, \ldots, m_{r-1} = \text{const}$, $m_r \to \infty$ имеет место оценка

$$\sqrt[m_r]{W_L(m_1, \ldots, m_r)} \leqslant W(m_1, \ldots, m_{r-1}) + o(1)$$

(если Φ_i — множество возможных функций F_i в последовательности $\{F_0, F_1, \ldots, F_i\}$, соответствующих $F \| L$, то «почти всегда» $\Phi_i = \Phi_{i+1}$, а в этом случае $F_i \| L'$, где $L' \in \Psi_{r-1}$ — некоторый новый оператор, зависящий от Φ_i).

Для завершения доказательства надо в последовательности $\{F_0, F_1, \ldots, F_{m_r-1}\}$ для $F \| L$, $L \in \Psi_r$, выделить подпоследовательность растущей длины, для которой соответствующий подоператор не зависит от μ_r; здесь применяется теорема Рамсея [4]. При этом устанавливается оценка

$$\sqrt[m_r]{W(m_1, \ldots, m_r)} \leqslant W(m_1, \ldots, m_{r-1}) + o(1),$$

где $m_r \to \infty$, $m_1, \ldots, m_{r-1} = \text{const}$. Из нее с использованием полуаддитивности $\log_2 W$ по всем параметрам выводится утверждение теоремы 3.

Наконец, приведем пример *нулевого* инвариантного класса, замыкание которого по операции отождествления переменных совпадает с множеством всех булевых функций.

Пусть $M' = \{f(x_1, \ldots, x_n) \mid (\exists \sigma_1, \ldots, \sigma_n \in \{0, 1\})(\exists g \in M)\ f(x_1, \ldots, x_n) = g(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n})\}$, где M — множество монотонных функций. Покажем, что M' — искомый нулевой инвариантный класс.

Инвариантность класса M' очевидна по определению. Поскольку число монотонных n-местных функций есть $2^{O(2^n/\sqrt{n})}$, класс M' содержит не более $2^n 2^{O(2^n/\sqrt{n})}$ функций от $x_1, \ldots, x_n$ и его параметр σ равен $\lim\limits_{n\to\infty} 2^{-n} \log_2 (2^n 2^{O(2^n/\sqrt{n})})$, т. е. нулю.

Наконец, покажем, что любая булева функция $h(x_1, \ldots, x_n)$ может быть получена отождествлением переменной из некоторой функции $f \in M'$. Разложим h в совершенную ДНФ:

$$h(x_1, \ldots, x_n) = \bigvee_{\substack{\sigma_1, \ldots, \sigma_n \\ h(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \ldots x_n^{\sigma_n},$$

Заменим в каждой элементарной конъюнкции этой ДНФ сомножители вида x_i^0 на y_i^0, а сомножители вида x_i^1 — на z_i^1. Получим выражение для некоторой функции $f(y_1, \ldots, y_n, z_1, \ldots, z_n)$, которая, очевидно, принадлежит M' (поскольку $f(\bar{y}_1, \ldots, \bar{y}_n, z_1, \ldots, z_n)$ — монотонная функция) и такая, что $h(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, x_1, \ldots, x_n)$.

Автор выражает благодарность профессору О. Б. Лупанову за обсуждение полученных результатов.

СПИСОК ЛИТЕРАТУРЫ

1. Яблонский С. В. О классах функций алгебры логики, допускающих простую схемную реализацию//Успехи матем. наук. 1957. 12, вып. 6. 189—196.
2. Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем//Проблемы кибернетики. 1959. Вып. 2. 75—121.

3. Hansel G. Sur le nombre des fonctions booleennes monotones de n variables// //C. r. Acad. sci. Paris. 1966. **262**, N 20. 1088—1090 Перевод: Ансель Ж. О числе монотонных булевых функций n переменных//Кибернет. сб. 1968. Вып. 5 (новая серия). 53—57.
4. Ramsey F. P. On a problem of formal logic//Proc. London Math. Soc. Ser. 2. 1930. **30**. 264—286.

Поступила в редакцию
16.12.94

ВЕСТН. МОСК. УН-ТА. СЕР. 1, МАТЕМАТИКА. МЕХАНИКА. 1995. № 3

УДК 519.6

О. М. Касим-Заде

О КЛАССАХ БУЛЕВЫХ ФУНКЦИЙ, ИНВАРИАНТНЫХ ОТНОСИТЕЛЬНО ПОДСТАНОВКИ ФУНКЦИЙ ОТ ОДНОЙ ПЕРЕМЕННОЙ

Понятие инвариантного класса введено С. В. Яблонским. Дескриптивные и метрические свойства инвариантных классов детально исследованы в [1]. Понятие инвариантного класса обобщено в [2] и [3]. Пусть F — произвольное подмножество множества P_2 всех булевых функций. Множество $Q \subseteq P_2$ назовем *F-инвариантным классом*, если оно замкнуто относительно операций добавления (изъятия) несущественных переменных, переименования переменных без отождествления и подстановки функций из множества F вместо некоторых переменных. Пусть $C=\{0, 1\}$, $G=\{0, 1, x\}$ и $H=\{0, 1, x, \bar{x}\}$. Нетрудно убедиться, что C-инвариантные классы — это инвариантные классы в обычном смысле [1], а G-инвариантные классы — это классы, инвариантные относительно подстановки констант и отождествления переменных. В данной работе рассматриваются метрические свойства G- и H-инвариантных классов.

Класс $Q \subseteq P_2$ называется *нулевым*, если

$$\limsup 2^{-n} \log_2 |Q_n| = 0,$$

где $n \to \infty$, а Q_n обозначает множество функций из Q от n переменных. Известна следующая гипотеза, о которой автор узнал от О. Б. Лупанова более двадцати лет тому назад: всякий класс булевых функций, инвариантный относительно подстановки констант и отождествления переменных, либо совпадает с P_2, либо является нулевым. В данной работе эта гипотеза доказана. На самом деле имеет место более сильное утверждение.

Теорема 1. *Если G-инвариантный класс Q не совпадает с P_2, то существует такая постоянная $\delta>0$, что при всех достаточно больших n выполняется неравенство*

$$\log_2 |Q_n| < 2^n/n^{\delta}.$$

Для H-инвариантных классов справедливо еще более сильное утверждение.

Теорема 2. *Если H-инвариантный класс Q не совпадает с P_2, то существует такая постоянная $\varepsilon>0$, что при всех достаточно больших n выполняется неравенство*

$$\log_2 |Q_n| < 2^{(1-\varepsilon)n}.$$

Следующее утверждение связано с одним известным свойством класса S всех симметрических булевых функций: замыкание класса