ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 1997. Серия 1. Том 4, № 4, 79–95

УДК 519.6

ОБ ОДНОЙ БЕСКОНЕЧНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ УЛУЧШАЮЩИХСЯ БУЛЕВЫХ БАЗИСОВ*)

Д. Ю. Черухин

Рассматривается сложность реализации булевых функций формулами в конечных полных базисах. Показано, что с точки зрения сложности базис, состоящий из всех $(k+1)$-местных функций, существенно лучше базиса, состоящего из всех k-местных функций (при каждом $k \geqslant 2$).

Существуют два подхода к сравнению классов управляющих систем — глобальный (с точки зрения сложности реализации почти всех функций) и локальный (учитывающий сложность реализации отдельных последовательностей функций). О. Б. Лупанов [1] показал, что при глобальном подходе все конечные базисы эквивалентны (функции Шеннона для них имеют одинаковый порядок). В то же время Б. А. Субботовская [4] установила, что в базисе $\{\&, \vee, \neg\}$ линейные булевы функции от n аргументов реализуются со сложностью, по порядку большей, чем в базисе $\{\&, \oplus, 1\}$. Таким образом, локальный подход к сравнению базисов представляет несомненный интерес. Именно он изучается в настоящей работе.

Введем точные определения. *Сложностью формулы* F (обозначение: $L(F)$) называется число вхождений в нее символов переменных. *Сложностью булевой функции* f в базисе Б (обозначение: $L_{\text{Б}}(f)$) называется минимальная из сложностей формул в базисе Б, реализующих функцию f. Говорят, что базис Б_1 *не хуже* базиса Б_2 (обозначение: $\text{Б}_1 \preccurlyeq \text{Б}_2$), если существует такая положительная константа C, что $L_{\text{Б}_1}(f) \leqslant C L_{\text{Б}_2}(f)$ для любой булевой функции f. Базисы Б_1 и Б_2 называются *эквивалентными* (обозначение: $\text{Б}_1 \sim \text{Б}_2$), если $\text{Б}_1 \preccurlyeq \text{Б}_2$ и $\text{Б}_2 \preccurlyeq \text{Б}_1$. Говорят, что базис Б_1 *лучше* базиса Б_2 (обозначение: $\text{Б}_1 \prec \text{Б}_2$), если $\text{Б}_1 \preccurlyeq \text{Б}_2$, а соотношение $\text{Б}_2 \preccurlyeq \text{Б}_1$ не выполняется.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 96-01-01068).

О. Б. Лупанов [1] показал, что произвольный базис не хуже базиса $Б_0 = \{\&, \vee, \neg\}$. Б. А. Субботовская [4] установила критерий эквивалентности базису $Б_0$ и показала существование неэквивалентных базисов, а именно, доказала, что базис $Б_1 = \{\&, \oplus, 1\}$ лучше базиса $Б_0$. В. А. Стеценко [3] описал ближайшее окружение базиса $Б_0$ — множество предплохих базисов. Б. А. Мучник [2] показала, что всякий нелинейный базис Б неэквивалентен базису $Б_1$ и $Б \cup Б_1 \prec Б$. Таким образом, если Б — нелинейный базис, неэквивалентный базису $Б_0$, то базисы $Б \cup Б_1$, Б и $Б_0$ образуют упорядоченную отношением $\prec$ последовательность длины 3, т. е. $Б \cup Б_1 \prec Б \prec Б_0$.

В настоящей работе устанавливается, что базисы $\{P_2(n) \mid n \geqslant 2\}$, состоящие из всех n-местных булевых функций, образуют бесконечную последовательность, упорядоченную отношением $\prec$, т. е. $P_2(n+1) \prec P_2(n)$ при каждом $n \geqslant 2$. Для доказательства основной теоремы будет предложена такая система функций $\{f_n^{(m_k)} \mid n \in N,\ k \in N\}$, что при каждом $n \geqslant 2$ справедливо соотношение

$$\frac{L_{P_2(n)}(f_{n+1}^{(m_k)})}{L_{P_2(n+1)}(f_{n+1}^{(m_k)})} \to \infty \quad \text{при} \quad k \to \infty.$$

Пусть F — произвольная формула в базисе Б. Индуктивно определим понятие *подформулы* формулы F:

1) если $F \equiv x_i$, то единственной подформулой формулы F является F;

2) если $F \equiv f(G_1, \ldots, G_s)$ и $f \in Б$, то подформулами формулы F являются F и все подформулы формул $G_1, \ldots, G_s$. В этом случае формулы $G_1, \ldots, G_s$ назовем *непосредственными подформулами* формулы F.

В дальнейшем формулу $\Lambda_n^c(G_1, \ldots, G_n)$ (где Λ_n^c — линейная функция от n аргументов, принимающая значение c на нулевом наборе) будем обозначать через $G_1 \oplus \ldots \oplus G_n \oplus c$. Формулу $F' \equiv F_1 \oplus F_2 \oplus c$ назовем *линейным представлением* формулы F, если F' реализует ту же функцию, что и F, $L(F') \leqslant L(F)$, и ни одна из формул F_1, F_2 не является константой.

Пусть F — произвольная формула в базисе $P_2(n)$. Проведем следующие преобразования формулы F:

1) каждую подформулу формулы F, имеющую линейное представление и не являющуюся своим линейным представлением, заменим ее линейным представлением;

2) каждую подформулу формулы F, реализующую линейную функцию $x_{i_1} \oplus \ldots \oplus x_{i_s} \oplus c$ и содержащую подформулу, реализующую нелинейную функцию, заменим подформулой $(\ldots(x_{i_1} \oplus x_{i_2}) \oplus \ldots) \oplus x_{i_s} \oplus c$;

3) каждую подформулу формулы F, имеющую вид $f(G_1, \ldots, G_i, c, G_{i+1}, \ldots, G_s)$, заменим подформулой $g(G_1, \ldots, G_s)$, где c — константа, а $g(x_1, \ldots, x_s) \equiv f(x_1, \ldots, x_i, c, x_{i+1}, \ldots, x_s)$.

В результате получим формулу F', обладающую следующими свойствами:

а) F' — формула в базисе $P_2(n)$;

б) F' реализует ту же функцию, что и F, причем $L(F') \leqslant L(F)$;

в) каждая подформула G формулы F' имеет один из двух видов:

(i) $G \equiv f(G_1, \ldots, G_s)$, где $2 \leqslant s \leqslant n$, G не имеет линейного представления и все формулы G_i отличны от констант;

(ii) $G \equiv G_1 \oplus \ldots \oplus G_s \oplus c$;

г) никакая подформула формулы F', реализующая линейную функцию, не содержит подформул, реализующих нелинейные функции.

Формулу F', обладающую свойствами а)–г), назовем *приведенной* для F. В дальнейшем, если не оговорено противное, рассматриваемые формулы будем считать приведенными.

Пусть G — произвольная формула вида (i). Непосредственную подформулу формулы G назовем *выделенной*, если все другие непосредственные подформулы формулы G реализуют линейные функции. Формулу G назовем *μ-формулой*, если в ней выделена некоторая непосредственная подформула. Формулу G назовем *центром*, если все непосредственные подформулы формулы G реализуют линейные функции (каждый центр является μ-формулой). *Подстановкой констант* будем называть отображение из некоторого конечного подмножества множества переменных в множество $\{0, 1\}$.

Введем следующие обозначения:

- $n(F)$ — число различных переменных, входящих в формулу F;
- $m(F)$ — наибольшее число вхождений одной переменной в формулу F;
- $\operatorname{nes}(f)$ — число существенных переменных функции f;
- $L_n(f)$ — сложность функции f в базисе $P_2(n)$;
- $\{\tilde{x} = \tilde{c}\}$ или $\{x_{i_1} = c_{i_1}, \cdots, x_{i_k} = c_{i_k}\}$ — подстановка констант, которая ставит в соответствие каждой переменной x_{i_j} из $\tilde{x} = (x_{i_1}, \ldots, x_{i_k})$ константу c_{i_j} из $\tilde{c} = (c_{i_1}, \ldots, c_{i_k})$;
- $|A|$ — мощность подстановки констант A, т. е. число переменных, с которыми она сопоставляет константы;
- $F|_A$ — формула, получающаяся из формулы F в результате замены в ней всех вхождений переменных из области определения подстановки констант A на соответствующие константы из A и последующего приведения;

• $f|_A$ — функция, получающаяся из функции f при фиксации в ней всех переменных из области определения подстановки констант A соответствующими константами из A (функцию $f|_A$ назовем *подфункцией* функции f);

• $\mu(F)$ — число подформул формулы F, являющихся μ-формулами (μ-подформул формулы F);

• $z(F)$ — число центров среди подформул формулы F (центров формулы F);

• $d(f)$ — степень полинома Жегалкина функции f (если $f \equiv 1$ или $f \equiv 0$, то $d(f) = 0$).

Отметим некоторые свойства степени. Пусть $g \in P_2(s)$, $g_1, \ldots, g_s$ — произвольные функции, а c — произвольная константа. Тогда

(d1) $d(g(g_1, \ldots, g_s)) \leqslant \sum\limits_{i=1}^{s} d(g_i)$;

(d2) $d(g_1 \oplus \ldots \oplus g_s \oplus c) \leqslant \max\limits_{1 \leqslant i \leqslant s} d(g_i)$;

(d3) если $d(g) = s$ и $g_1, \ldots, g_s$ существенно зависят от непустых, попарно не пересекающихся наборов переменных, то $d(g(g_1, \ldots, g_s)) = \sum\limits_{i=1}^{s} d(g_i)$.

Лемма 1. *Если F — формула в базисе $P_2(n)$, реализующая произвольную нелинейную функцию f, то*

$$\mu(F) \geqslant \frac{1}{2n} d(f) + \frac{1}{2}.$$

Доказательство. Проводится индукция по построению формулы F.

Базис индукции: все непосредственные подформулы формулы F реализуют линейные функции, а F — нелинейную. Тогда F — центр. Из (d1) следует, что $d(f) \leqslant n$. Поэтому

$$\mu(F) = 1 = \frac{1}{2n} n + \frac{1}{2} \geqslant \frac{1}{2n} d(f) + \frac{1}{2}.$$

Индуктивный переход: хотя бы одна непосредственная подформула формулы F реализует нелинейную функцию.

Пусть $G_1, \ldots, G_s$ — непосредственные подформулы формулы F, причем G_i реализует функцию g_i, и пусть, для определенности, функции $g_1, \ldots, g_k$ — нелинейные ($k \geqslant 1$), а $g_{k+1}, \ldots, g_s$ — линейные. По предположению индукции при любом i, $1 \leqslant i \leqslant k$, имеем

$$\mu(G_i) \geqslant \frac{1}{2n} d(g_i) + \frac{1}{2}.$$

Возможны два случая: 1) F имеет вид (i); 2) F имеет вид (ii).

Случай 1. Пусть $F \equiv g(G_1, \ldots, G_s)$. Тогда $f = g(g_1, \ldots, g_s)$. Поэтому из свойства (d1) и неравенства $s \leqslant n$ следует, что

$$d(f) \leqslant \sum_{i=1}^{s} d(g_i) = \sum_{i=1}^{k} d(g_i) + (s-k) \leqslant \sum_{i=1}^{k} d(g_i) + n.$$

Если $k = 1$, то F является μ-формулой. Поэтому

$$\mu(F) = \mu(G_1) + 1 \geqslant \frac{1}{2n} d(g_1) + \frac{1}{2} + 1 \geqslant \frac{1}{2n} d(g_1) + 1.$$

Если же $k \geqslant 2$, то F не является μ-формулой и

$$\mu(F) = \sum_{i=1}^{k} \mu(G_i) \geqslant \frac{1}{2n} \sum_{i=1}^{k} d(g_i) + \frac{k}{2} \geqslant \frac{1}{2n} \sum_{i=1}^{k} d(g_i) + 1.$$

Таким образом, при любом k имеем

$$\mu(F) \geqslant \frac{1}{2n} \sum_{i=1}^{k} d(g_i) + 1 = \frac{1}{2n} \left(\sum_{i=1}^{k} d(g_i) + n \right) + \frac{1}{2} \geqslant \frac{1}{2n} d(f) + \frac{1}{2}.$$

Случай 2. Пусть $F \equiv G_1 \oplus \ldots \oplus G_s \oplus c$. Используя (d2), получаем

$$\mu(F) = \sum_{i=1}^{k} \mu(G_i) \geqslant \frac{1}{2n} \sum_{i=1}^{k} d(g_i) + \frac{k}{2} \geqslant \frac{1}{2n} \max_{1 \leqslant i \leqslant k} d(g_i) + \frac{1}{2}$$

$$= \frac{1}{2n} \max_{1 \leqslant i \leqslant s} d(g_i) + \frac{1}{2} \geqslant \frac{1}{2n} d(f) + \frac{1}{2}.$$

Лемма 1 доказана.

Пусть F — формула, $\mu_1, \ldots, \mu_t$ — последовательность различных μ-формул, причем μ_i — подформула формулы μ_{i+1} при $1 \leqslant i \leqslant t-1$, а μ_t — подформула формулы F. Тогда последовательность $\mu_1, \ldots, \mu_t$ назовем *μ-цепью* формулы F. *Максимальной μ-цепью* формулы F назовем μ-цепь формулы F, в которую нельзя добавить ни одной другой μ-подформулы формулы F.

Лемма 2. *Пусть некоторые μ-подформулы формулы F помечены (каким-либо способом), число помеченных формул равно Q и каждая μ-цепь формулы F содержит не более T помеченных формул. Тогда*

$$T \cdot z(F) \geqslant Q.$$

Доказательство. Установим взаимно однозначное соответствие между максимальными μ-цепями формулы F и центрами формулы F.

Пусть $\mu_1, \ldots, \mu_t$ — произвольная максимальная μ-цепь формулы F. Покажем, что μ_1 — центр. Действительно, в противном случае в μ_1 нашлась бы непосредственная подформула, реализующая нелинейную функцию, а в ней нашелся бы некоторый центр μ_0 (легко видеть, что в каждой формуле, реализующей нелинейную функцию, найдется хотя бы один центр). Тогда последовательность $\mu_0, \mu_1, \ldots, \mu_t$ была бы μ-цепью формулы F, что противоречит максимальности исходной μ-цепи. Поставим μ-цепи $\mu_1, \ldots, \mu_t$ в соответствие центр μ_1. Это соответствие взаимно однозначно, так как по каждой μ-формуле $\mu_i, 1 \leqslant i \leqslant t-1$, однозначно восстанавливается следующая за ней μ-формула μ_{i+1}. Обозначив через M число максимальных μ-цепей формулы F, получим $z(F) = M$. Так как каждая μ-подформула формулы F является μ-цепью, то она содержится в некоторой максимальной μ-цепи формулы F. Из условия леммы следует, что в каждой максимальной μ-цепи формулы F содержится не более T помеченных формул. Поэтому общее число помеченных подформул формулы F не превосходит TM. Следовательно,

$$T \cdot z(F) = TM \geqslant Q.$$

Лемма 2 доказана.

Формулу G назовем *забиваемой*, если G является μ-формулой и в некоторой выделенной подформуле формулы G содержится переменная, не входящая в другие непосредственные подформулы формулы G.

Лемма 3. *Если в формуле F имеется μ-цепь, состоящая из t незабиваемых μ-формул, и $m(F) \geqslant 1$, то*

$$L(F) \geqslant \left(1 + \frac{1}{m(F)}\right)^t.$$

Доказательство. Проводится индукция по t. Если $t = 1$, то в F найдется μ-цепь длины 1, т. е. μ-подформула. Поэтому $L(F) \geqslant 2 \geqslant \left(1 + \frac{1}{m(F)}\right)$.

Предположим, что лемма верна при любом $i \leqslant t-1$, $t \geqslant 2$. Пусть $\mu_1, \ldots, \mu_{t-1}, \mu_t$ — такая μ-цепь в F, что никакая формула μ_i не забиваема. По предположению индукции имеем

$$L(\mu_{t-1}) \geqslant \left(1 + \frac{1}{m(F)}\right)^{t-1}.$$

Пусть $G_1, \ldots, G_s$ — непосредственные подформулы формулы μ_t и пусть, для определенности, G_1 выделена. Формулы $G_2, \ldots, G_s$ реализуют линейные функции, а μ_{t-1} — нелинейную. Поэтому из свойства г) приведенных формул следует, что μ_{t-1} — подформула формулы G_1, а значит,

$$L(G_1) \geqslant L(\mu_{t-1}).$$

Так как формула μ_t незабиваема, то каждая переменная, содержащаяся в G_1, входит хотя бы в одну из формул $G_2, \ldots, G_s$. Следовательно,

$$\sum_{i=2}^{s} n(G_i) \geqslant n(G_1).$$

Заметим, что $L(G_i) \geqslant n(G_i)$ при любом i, $2 \leqslant i \leqslant s$, и $L(G_1) \leqslant m(F)n(G_1)$. Из выписанных неравенств следует, что

$$L(F) \geqslant L(\mu_t) = L(G_1) + \sum_{i=2}^{s} L(G_i) \geqslant L(G_1) + \sum_{i=2}^{s} n(G_i)$$
$$\geqslant L(G_1) + n(G_1) \geqslant L(G_1)\Big(1 + \frac{1}{m(F)}\Big) \geqslant \Big(1 + \frac{1}{m(F)}\Big)^t.$$

Лемма 3 доказана.

Пусть функция f отлична от константы и $s = \operatorname{nes}(f)$. Индуктивно определим семейство формул $\{\langle f\rangle_i^{(m)} \mid i \in N,\ m \in N \cup \{0\}\}$. Положим

$$\langle f\rangle_i^{(0)} \equiv x_i, \quad \langle f\rangle_i^{(m+1)} \equiv f\left(\langle f\rangle_i^{(m)}, \langle f\rangle_{i+s^m}^{(m)}, \ldots, \langle f\rangle_{i+s^m(s-1)}^{(m)}\right).$$

При разных i формулы $\langle f\rangle_i^{(m)}$ получаются друг из друга заменой переменных без отождествления. Поэтому в дальнейшем через $\langle f\rangle^{(m)}$ будем обозначать любую из них. Функцию, реализуемую формулой $\langle f\rangle^{(m)}$, обозначим через $f^{(m)}$.

В отличие от общего правила будем считать, что формула вида $\langle f\rangle^{(m)}|_A$, где $A = \{\tilde{x} = \tilde{c}\}$, является результатом подстановки констант из $\tilde{c}$ вместо соответствующих переменных из $\tilde{x}$ в формулу $\langle f\rangle^{(m)}$ без каких-либо дальнейших преобразований.

Пусть $g = f^{(m)}|_A$, $m \geqslant 1$. Функции, реализуемые непосредственными подформулами формулы $\langle f\rangle^{(m)}|_A$, назовем *непосредственными подфункциями* функции g. Заметим, что непосредственные подфункции функции g являются подфункциями функции $f^{(m-1)}$ и наборы их переменных попарно не пересекаются.

Предложение 1. *Пусть $m \geqslant 1$, $\operatorname{nes}(f) = s$ и некоторые $(s-1)^m + 1$ переменных функции $f^{(m)}$ каким-либо способом помечены. Тогда в формуле $\langle f\rangle^{(m)}$ можно указать такую подформулу, в которой каждая непосредственная подформула содержит помеченную переменную.*

Доказательство. Проводится индукция по m.

Если $m = 1$, то $(s-1)^m + 1 = s$, и в качестве искомой формулы можно взять формулу $\langle f\rangle^{(1)}$.

Пусть $m \geqslant 2$. Возможны два случая:

1) в качестве искомой формулы можно взять формулу $\langle f\rangle^{(m)}$;

2) в $\langle f\rangle^{(m)}$ имеется непосредственная подформула, не содержащая помеченных переменных. Используя принцип Дирихле, легко видеть, что в $\langle f\rangle^{(m)}$ найдется другая непосредственная подформула, содержащая не менее $\left\lceil \frac{(s-1)^m+1}{s-1} \right\rceil = (s-1)^{m-1}+1$ помеченных переменных. Остается применить к ней предположение индукции.

Предложение 1 доказано.

Пусть формула F реализует функцию g. Число существенных переменных функции g, каждая из которых входит в F не более q раз, обозначим через $N(q,F)$.

Лемма 4. *Пусть g — подфункция функции $f^{(m)}$, $m \geqslant 1$, F — формула в базисе $P_2(n)$, реализующая функцию g, и $L_n(f) > q\,\mathrm{nes}(f)$ для некоторого $q \geqslant 0$. Тогда*

$$N(q,F) \leqslant (\mathrm{nes}(f)-1)^m.$$

Доказательство. Предположим противное, т. е. $N(q,F) > (\mathrm{nes}(f)-1)^m$. Тогда $N(q,F) \geqslant (s-1)^m+1$, где $s = \mathrm{nes}(f)$. Пусть $g = f^{(m)}|_A$. Пометим существенные переменные функции g (они же будут переменными функции $f^{(m)}$), каждая из которых входит в F не более q раз. Согласно предложению 1 в формуле $\langle f\rangle^{(m)}$ найдется такая подформула $G \equiv f(G_1,\ldots,G_s)$, что каждая формула G_i содержит некоторую помеченную переменную x_{k_i}. Так как формула $\langle f\rangle^{(m)}|_A$ реализует функцию g, то при каждом i формула $G_i|_A$ существенно зависит от x_{k_i}. Следовательно, найдутся подстановка констант A_i и константа σ_i такие, что $(G_i|_A)|_{A_i}$ реализует функцию $x_{k_i} \oplus \sigma_i$ и A_i определена только на переменных, входящих в G_i. Каждая переменная входит в $\langle f\rangle^{(m)}|_A$ не более одного раза и формула $\langle f\rangle^{(m)}|_A$ существенно зависит от подформулы $G|_A$. Поэтому найдутся подстановка констант A_0 и константа σ_0 такие, что формула $(\langle f\rangle^{(m)}|_A)|_{A_0}$ реализует ту же функцию, что и формула $G|_A \oplus \sigma_0$. Положим $B = \bigcup\limits_{i=0}^{s} A_i$. Формула $(\langle f\rangle^{(m)}|_A)|_B$ реализует функцию $g|_B = f(x_{k_1} \oplus \sigma_1,\ldots,x_{k_s} \oplus \sigma_s) \oplus \sigma_0$. Так как базис $P_2(n)$ содержит отрицание, то $L_n(g|_B) = L_n(f)$. Отсюда с использованием условия леммы следует, что $L_n(g|_B) > qs$. С другой стороны, в силу выбора помеченных переменных имеем $L_n(g|_B) \leqslant L(F|_B) \leqslant qs$. Противоречие. Лемма 4 доказана.

Пусть g — подфункция функции $f^{(m)}$, причем $g = f^{(m)}|_A$. Существенную переменную x_i функции g назовем *особой*, если в формуле $\langle f\rangle^{(m)}|_A$ имеется подформула, содержащая x_i, в которую непосредственно

входит формула, реализующая константу. Число особых переменных функции g обозначим через $I(g)$.

Лемма 5. *Пусть g — произвольная подфункция функции $f^{(m)}$. Тогда*

(a) $I(g) \leqslant (\mathrm{nes}(f) - 1)(\mathrm{nes}(f^{(m)}) - \mathrm{nes}(g))$;

(b) *если* $d(f) = \mathrm{nes}(f)$, *то* $d(g) \geqslant \mathrm{nes}(g) - I(g)$;

(c) *если* $I(g) = 0$ *и* $\mathrm{nes}(g) > 0$, *то* $g = f^{(m)}$.

Доказательство. Проводится индукция по m. Положим $s = \mathrm{nes}\,(f)$.

Если $m = 0$, то g — либо переменная, либо константа. Поэтому $I(g) = 0$. Следовательно,

(a) $I(g) = 0 \leqslant (s-1)(1 - \mathrm{nes}\,(g)) = (s-1)(\mathrm{nes}\,(f^{(0)}) - \mathrm{nes}\,(g))$;

(b) $d(g) = \mathrm{nes}\,(g) \geqslant \mathrm{nes}\,(g) - I(g)$;

(c) из $\mathrm{nes}\,(g) > 0$ следует $g = f^{(0)}$.

Пусть $m \geqslant 1$ и пусть $g_1, \ldots, g_s$ — непосредственные подфункции функции g. Возможны два случая: 1) среди g_i есть константа (т. е. функция, тождественно равная 0 или 1); 2) среди g_i нет констант.

Случай 1. Все существенные переменные функции g являются особыми, т. е. $\mathrm{nes}\,(g) = I(g)$. Поэтому

(a) $I(g) = \mathrm{nes}\,(g) \leqslant (s-1)\,\mathrm{nes}\,(f^{(m-1)}) = (s-1)s^{m-1} = (s-1)(s^m - (s-1)s^{m-1}) \leqslant (s-1)(s^m - \mathrm{nes}\,(g))$;

(b) $d(g) \geqslant 0 = \mathrm{nes}\,(g) - I(g)$;

(c) случай не реализуется.

Случай 2. В этом случае

$$\mathrm{nes}\,(g) = \sum_{i=1}^{s} \mathrm{nes}\,(g_i) \quad \text{и} \quad I(g) = \sum_{i=1}^{s} I(g_i).$$

Согласно индуктивному предположению имеем

(a) $I(g) = \sum\limits_{i=1}^{s} I(g_i) \leqslant \sum\limits_{i=1}^{s} (s-1)(s^{m-1} - \mathrm{nes}\,(g_i)) = (s-1)(s^m - \mathrm{nes}\,(g))$;

(b) из $d(f) = \mathrm{nes}\,(f)$ и свойства (d3) следует, что $d(g) = \sum\limits_{i=1}^{s} d(g_i) \geqslant \sum\limits_{i=1}^{s} (\mathrm{nes}\,(g_i) - I(g_i)) = \mathrm{nes}\,(g) - I(g)$;

(c) из $I(g) = 0$ следует $I(g_i) = 0$ при каждом i, поэтому $g_i = f^{(m-1)}$, а значит, $g = f(f^{(m-1)}, \ldots, f^{(m-1)}) = f^{(m)}$.

Лемма 5 доказана.

При каждом $s \geqslant 1$ положим

$$f_s(x_1, \ldots, x_s) = x_1 x_2 \ldots x_s \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_s.$$

Предложение 2. *Пусть g — подфункция функции $f_s^{(m)}$, где $s \geqslant 2$ и $m \geqslant 1$, а $g_1, \ldots, g_s$ — непосредственные подфункции функции g, среди которых не более $s-2$ тождественно равны единице. Тогда*

$$\operatorname{nes}(g) = \sum_{i=1}^{s} \operatorname{nes}(g_i).$$

Доказательство. Пусть, для определенности, $g_1, \ldots, g_k$ — тождественно не равны ни 0, ни 1, $g_{k+1} \equiv \ldots \equiv g_n \equiv 0$, $g_{n+1} \equiv \ldots \equiv g_s \equiv 1$. Заметим, что $f_i|_{\{x_i=1\}} = f_{i-1} \oplus 1$ и $f_i|_{\{x_i=0\}} = x_1 \oplus \ldots \oplus x_{i-1}$ при любом $i \geqslant 2$. Из условия предложения следует, что $n \geqslant 2$. Если $k = n$, то $g = f_s(g_1, \ldots, g_s) = f_k(g_1, \ldots, g_k) \oplus (s-n) \pmod 2$, а если $k < n$, то $g = g_1 \oplus \ldots \oplus g_k \oplus (s-n) \pmod 2$. Функции f_k при $k \geqslant 2$ и $x_1 \oplus \ldots \oplus x_k$ при любом k существенно зависят от всех своих переменных, а множества существенных переменных функций g_i попарно не пересекаются. Поэтому

$$\operatorname{nes}(g) = \sum_{i=1}^{k} \operatorname{nes}(g_i) = \sum_{i=1}^{s} \operatorname{nes}(g_i).$$

Предложение 2 доказано.

Замечание. Функция f_s обращается в константу при подстановке в нее $s-1$ единиц.

Лемма 6. *Пусть g — подфункция функции $f_s^{(m)}$, $s \geqslant 2$, и x_i — существенная переменная функции g. Тогда существует такая константа c, что*

$$\operatorname{nes}(g) = \operatorname{nes}(g|_{\{x_i=c\}}) + 1 \quad \text{и} \quad g|_{\{x_i=c\}} \not\equiv 1.$$

Доказательство. Проводится индукция по m.

Если $m = 0$, то достаточно положить $c = 0$.

Пусть $m \geqslant 1$. В случае $\operatorname{nes}(g) = 1$ достаточно выбрать такую константу c, что $g(c) = 0$.

Рассмотрим случай $\operatorname{nes}(g) > 1$. Пусть $g_1, \ldots, g_s$ — непосредственные подфункции функции g и, для определенности, x_i — переменная функции g_1. Из замечания следует, что не все функции $g_2, \ldots, g_s$ тождественно равны единице. Согласно предложению 2

$$\operatorname{nes}(g) = \sum_{i=1}^{s} \operatorname{nes}(g_i). \tag{1}$$

По предположению индукции для функции g_1 существует такая константа c, что

$$\operatorname{nes}(g_1) = \operatorname{nes}(g_1|_{\{x_i=c\}}) + 1 \quad \text{и} \quad g_1|_{\{x_i=c\}} \not\equiv 1. \tag{2}$$

Таким образом, среди функций $g_1|_{\{x_i=c\}}, g_2, \ldots, g_s$ (которые являются непосредственными подфункциями функции $g|_{\{x_i=c\}}$) не более $s-2$ тождественно равны единице. Отсюда и из предложения 2 следует, что

$$\operatorname{nes}(g|_{\{x_i=c\}}) = \operatorname{nes}(g_1|_{\{x_i=c\}}) + \sum_{i=2}^{s} \operatorname{nes}(g_i). \tag{3}$$

Из равенств (1)–(3) получаем $\operatorname{nes}(g) = \operatorname{nes}(g|_{\{x_i=c\}}) + 1$. Тогда из $\operatorname{nes}(g) > 1$ следует, что $\operatorname{nes}(g|_{\{x_i=c\}}) > 0$, а значит, $g|_{\{x_i=c\}} \not\equiv 1$. Лемма 6 доказана.

Лемма 7. *Пусть g — подфункция функции $f_s^{(m)}$, $s \geqslant 2$, A — подстановка констант, определенная на некоторых существенных неособых переменных функции g, и среди подставляемых в ней констант имеется не более $s-2$ единиц. Тогда*

$$\operatorname{nes}(g) = \operatorname{nes}(g|_A) + |A|. \tag{4}$$

Доказательство. Проводится индукция по m.

Если $m = 0$, то $\operatorname{nes}(g) \leqslant 1$ и равенство (4) справедливо.

Пусть $m \geqslant 1$ и пусть $g_1, \ldots, g_s$ — непосредственные подфункции функции g. Если хотя бы одна из функций g_i тождественно равна 0 или 1, то все переменные функции g особые, т. е. $A = \varnothing$ и равенство (4) справедливо.

Предположим, что $\operatorname{nes}(g_i) > 0$ при каждом i. Тогда

$$\operatorname{nes}(g) = \sum_{i=1}^{s} \operatorname{nes}(g_i). \tag{5}$$

Пусть A_i — сужение подстановки констант A на множество переменных функции g_i. Тогда

$$|A| = \sum_{i=1}^{s} |A_i|. \tag{6}$$

К функции g_i применимо предположение индукции, согласно которому

$$\operatorname{nes}(g_i) = \operatorname{nes}(g_i|_{A_i}) + |A_i|. \tag{7}$$

Среди подстановок констант A_i найдутся две (для определенности A_1 и A_2), не сопоставляющие с переменными константу 1. Пусть A_j, $1 \leqslant j \leqslant 2$, — любая из них. Покажем, что $g_j|_{A_j} \not\equiv 1$. В случае $\operatorname{nes}(g_j|_{A_j}) \geqslant 1$ это очевидно. Пусть $\operatorname{nes}(g_j|_{A_j}) = 0$. Тогда $\operatorname{nes}(g_j) = |A_j|$ и из условия леммы 7 следует, что все переменные функции g_j неособые, т. е. $I(g_j) = 0$. Из утверждения (c) леммы 5 следует, что $g_j = f_s^{(m-1)}$. Так как функция f_s сохраняет нуль, то $f_s^{(m-1)}$ сохраняет нуль, а значит,

$g_j|_{A_j} \equiv 0 \neq 1$. Итак, среди функций $g_i|_{A_i}$, $1 \leqslant i \leqslant s$, не более $s-2$ функций тождественно равны единице. Согласно предложению 2 имеем

$$\operatorname{nes}(g|_A) = \sum_{i=1}^{s} \operatorname{nes}(g_i|_{A_i}). \tag{8}$$

Из равенств (5)–(8) следует (4). Лемма 7 доказана.

Теорема 1. *При любом натуральном $n \geqslant 2$ существует такая последовательность натуральных чисел (m_k), что при $k \to \infty$ справедливо соотношение*

$$\frac{L_n(f_{n+1}^{(m_k)})}{L_{n+1}(f_{n+1}^{(m_k)})} \to \infty.$$

Доказательство. При каждом фиксированном n индукцией по k докажем, что для любого $k \in N \cup \{0\}$ найдется $m_k \in N$ такое, что

$$L_n(f_{n+1}^{(m_k)}) > k(n+1)^{m_k}.$$

Отсюда и из равенства $L_{n+1}(f_{n+1}^{(m)}) = (n+1)^m$, справедливого при любом $m \geqslant 0$, следует утверждение теоремы 1.

При $k = 0$ достаточно положить $m_0 = 1$.

Пусть $k \geqslant 1$. По предположению индукции имеем

$$L_n(f_{n+1}^{(m_{k-1})}) > (k-1)(n+1)^{m_{k-1}}. \tag{9}$$

Положим $p = (n+1)^{m_{k-1}}$. Тогда $p \geqslant 2$ и $\frac{1}{m}\left(\frac{p}{p-1}\right)^{m/2} \to \infty$ при $m \to \infty$. Поэтому найдется $m \in N$ такое, что

$$\frac{1}{m}\left(\frac{p}{p-1}\right)^{m/2} \geqslant 20k^4n^3m_{k-1}. \tag{10}$$

Положим $m_k = mm_{k-1}$, $R = (p(p-1))^{m/2}$ и $r = \left(\frac{p}{p-1}\right)^{m/2}$. Заметим, что $Rr = p^m$ и $R/r = (p-1)^m$. С учетом обозначений (10) примет вид

$$r \geqslant 20k^4n^3m_k. \tag{11}$$

Докажем следующее вспомогательное утверждение.

Утверждение 1. *Пусть g — подфункция функции $f_{n+1}^{(m_k)}$. Тогда*

$$L_n(g) > \left(k + \frac{1}{r}\right)\operatorname{nes}(g) - R.$$

Доказательство. Проводится индукция по $\operatorname{nes}(g)$.

Пусть $\operatorname{nes}(g) = 0$. Тогда из $R > 0$ следует, что $L_n(g) \geqslant 0 > 0 - R$.

Пусть $\operatorname{nes}(g) \geqslant 1$ и пусть F — формула в базисе $P_2(n)$, реализующая функцию g со сложностью $L(F) = L_n(g)$. В силу (9) к функциям $f = f_{n+1}^{(m_{k-1})}$, g (как к подфункции функции $f^{(m)} = f_{n+1}^{(m_k)}$) и числу $q = k-1$ можно применить лемму 4. В результате получаем

$$N(k-1, F) \leqslant (\operatorname{nes}(f_{n+1}^{(m_{k-1})}) - 1)^m = (p-1)^m. \tag{12}$$

Возможны два случая: 1) $\operatorname{nes}(g) < p^m - kR$; 2) $\operatorname{nes}(g) \geqslant p^m - kR$.

Случай 1. Число переменных, каждая из которых входит в F не менее k раз, равно $\operatorname{nes}(g) - N(k-1, F)$. Поэтому $L(F) \geqslant k(\operatorname{nes}(g) - N(k-1, F))$. Отсюда, а также из (12), условия случая 1 и свойств R и r следует, что

$$\begin{aligned} L_n(g) = L(F) &\geqslant k(\operatorname{nes}(g) - (p-1)^m) = k \cdot \operatorname{nes}(g) - k\frac{R}{r} + R - R \\ &= k \cdot \operatorname{nes}(g) + \frac{1}{r}(p^m - kR) - R > \left(k + \frac{1}{r}\right)\operatorname{nes}(g) - R. \end{aligned}$$

Случай 2. Введем вспомогательное понятие. Пусть G — произвольная μ-подформула формулы F и $G_1, \ldots, G_s$ — все ее непосредственные подформулы, реализующие линейные функции. Формулу G назовем *отмеченной*, если

все переменные из $G_1, \ldots, G_s$ — неособые для функции g; (13)

число вхождений каждой переменной из $G_1, \ldots, G_s$ в F равно k; (14)

общее число различных переменных в $G_1, \ldots, G_s$ не больше r. (15)

Допустим, что найдется подстановка констант A, удовлетворяющая условиям

$$\operatorname{nes}(g) = \operatorname{nes}(g|_A) + |A|; \tag{16}$$

$$L(F) \geqslant L(F|_A) + k|A| + 1; \tag{17}$$

$$|A| \leqslant r. \tag{18}$$

Тогда из (17) следует, что $A \neq \varnothing$, т. е. $\operatorname{nes}(g|_A) < \operatorname{nes}(g)$. Поэтому к функции $g|_A$ применимо предположение индукции, из которого и условий (16)–(18) получаем

$$\begin{aligned} L_n(g) = L(F) &\geqslant L(F|_A) + k|A| + 1 \geqslant L_n(g|_A) + k|A| + \frac{|A|}{r} \\ &> \left(k + \frac{1}{r}\right)\operatorname{nes}(g|_A) - R + \left(k + \frac{1}{r}\right)|A| = \left(k + \frac{1}{r}\right)\operatorname{nes}(g) - R, \end{aligned}$$

т. е. при нашем допущении утверждение 1 доказано.

Далее будут рассмотрены четыре случая, покрывающие все возможности:

(a) $m(F) > k$;

(b) в формуле F имеется отмеченная забиваемая μ-подформула;

(c) в формуле F имеется отмеченный центр;

(d) $m(F) \leqslant k$, все центры формулы F неотмечены и все отмеченные подформулы формулы F незабиваемы.

В случаях (a)–(c) будет предъявлена подстановка констант A, удовлетворяющая условиям (16)–(18), а в случае (d) утверждение будет доказано независимо.

Случай (a). Пусть число вхождений переменной x_i в F не меньше $k+1$. По лемме 6 найдется такая константа c, что $\operatorname{nes}(g) = \operatorname{nes}(g|_{\{x_i=c\}})+1$. Положим $A = \{x_i = c\}$. Тогда $|A| = 1$, т. е. (16) выполнено. Из выбора переменной x_i следует (17), а из (11) следует $|A| = 1 \leqslant r$, т. е. (18) выполнено.

Случай (b). Пусть $G \equiv h(G_1, \ldots, G_s)$ — отмеченная и забиваемая μ-подформула формулы F и, для определенности, G_1 — выделенная подформула формулы G, содержащая переменную, не входящую в $G_2, \ldots, G_s$. Пусть $\tilde{x}$ — набор, состоящий из всех переменных, входящих в формулы $G_2, \ldots, G_s$, и $\Lambda_i(\tilde{x})$ при $i = 2, \ldots, s$ — функция, реализуемая формулой G_i. Так как подформула G_1 выделена, то все функции Λ_i линейны.

Рассмотрим функцию $\varphi(\tilde{x}, y) = h(y, \Lambda_2(\tilde{x}), \ldots, \Lambda_s(\tilde{x}))$. Если при любой подстановке констант $B = \{\tilde{x} = \tilde{c}\}$ функция $\varphi|_B$ существенно зависит от y, то $\varphi(\tilde{x}, y) \equiv \varphi(\tilde{x}, 0) \oplus y$. Следовательно, формула $h(0, G_2, \ldots, G_s) \oplus G_1$ реализует ту же функцию, что и формула G, т. е. формула G имеет линейное представление, что противоречит свойству (в) приведенных формул. Отсюда следует, что существует такая подстановка констант $B_0 = \{\tilde{x} = \tilde{c}_0\}$, что $\varphi|_{B_0}$ не зависит от y.

Рассмотрим систему линейных уравнений

$$\Lambda_i(\tilde{x}) = \Lambda_i(\tilde{c}_0), \quad i = 2, \ldots, s.$$

Она совместна, и ранг матрицы этой системы не больше числа уравнений, равного $s-1$. Поэтому найдется решение $\tilde{c}_1$, среди координат которого имеется не более $s-1$ единиц. Положим $A = \{\tilde{x} = \tilde{c}_1\}$. Из $\varphi(\tilde{c}_1, y) \equiv \varphi(\tilde{c}_0, y)$ следует, что $\varphi|_A$ не зависит от y, а значит, формула $G|_A$ не зависит от подформулы $G_1|_A$. Так как подформула $G_1|_A$ содержит переменную, не входящую в $\tilde{x}$, то после приведения формула $F|_A$ упростится хотя бы на одно вхождение переменной. Отсюда и из (14) следует (17). Подстановка констант A сопоставляет с переменными не более $s-1 \leqslant n-1 = \operatorname{nes}(f_{n+1}) - 2$ единиц. Кроме того, согласно (13) все переменные из $\tilde{x}$ — неособые для g. Применяя лемму 7, получим (16). Из (15) следует $|A| \leqslant r$, т. е. (18) выполнено.

Случай (c). В формуле F имеется отмеченный центр, который обозначим через H. Если каждая переменная входит в H не более одного раза, то формула H забиваема и к ней применимы рассуждения случая (b). Пусть переменная x_i входит в H не менее двух раз. В качестве A выберем подстановку констант, определенную на всех переменных, входящих в H, кроме x_i, и сопоставляющую им константу 0. Используя (13), применяем лемму 7, из которой следует (16). Так как формула $H|_A$ зависит только от x_i, то после приведения она будет иметь сложность, не превосходящую 1. Итак, $F|_A$ упрощается хотя бы на одно вхождение переменной x_i и с учетом (14) имеем (17). Из (15) следует (18).

Случай (d). Все центры формулы F неотмечены, все ее отмеченные подформулы незабиваемы и $m(F) \leqslant k$. Предположим, что утверждение не выполнено, т. е. $L_n(g) \leqslant (k + 1/r)\operatorname{nes}(g) - R$. Так как функция g является подфункцией функции $f_{n+1}^{(m_k)}$, то $\operatorname{nes}(g) \leqslant (n+1)^{m_k} = p^m$. Отсюда и из равенства $1/r = R/p^m$ получаем

$$L(F) = L_n(g) \leqslant \Big(k + \frac{1}{r}\Big)\operatorname{nes}(g) - R \leqslant \Big(k + \frac{R}{p^m}\Big)p^m - R = kp^m. \qquad (19)$$

Из утверждения (a) леммы 5 и условия случая 2 ($\operatorname{nes}(g) \geqslant p^m - kR$) следует

$$I(g) \leqslant (\operatorname{nes}(f_{n+1})-1)(\operatorname{nes}(f_{n+1}^{(m_k)})-\operatorname{nes}(g)) = n(p^m - \operatorname{nes}(g)) \leqslant nkR. \qquad (20)$$

Из определения функции f_{n+1} следует, что $d(f_{n+1}) = \operatorname{nes}(f_{n+1})$. Применяя утверждение (b) леммы 5, неравенства $\operatorname{nes}(g) \geqslant p^m - kR$ и (20), равенство $Rr = p^m$ и (11), получаем

$$\begin{aligned} d(g) \geqslant \operatorname{nes}(g) - I(g) &\geqslant p^m - kR - nkR \geqslant rR - 2nkR \\ &\geqslant 20k^4n^3m_kR - 2nkR \geqslant 18k^4n^3m_kR. \end{aligned}$$

Отсюда и из $R \geqslant 1$ следует, что $d(g) \geqslant 2$, т. е. функция g нелинейна. Тогда по лемме 1 имеем

$$\mu(F) \geqslant \frac{1}{2n}d(g) + \frac{1}{2} \geqslant 9k^4n^2m_kR. \qquad (21)$$

Пусть V — число неотмеченных μ-подформул формулы F, а V_1, V_2, V_3 — число μ-подформул формулы F, не удовлетворяющих условиям (13), (14) и (15) соответственно. Так как непосредственные подформулы из разных μ-подформул формулы F, реализующие линейные функции, не пересекаются, то с учетом $m(F) \leqslant k$ получаем

$$V_1 \leqslant k \cdot I(g), \quad V_2 \leqslant (k-1) \cdot N(k-1, F), \quad V_3 \leqslant L(F)/r. \qquad (22)$$

Из (12) следует, что

$$N(k-1, F) \leqslant (p-1)^m \leqslant \Big(\sqrt{p(p-1)}\Big)^m = R. \qquad (23)$$

Из (19) и равенства $1/r = R/p^m$ следует, что

$$L(F)/r = L(F) \cdot R/p^m \leqslant kp^m R/p^m = kR. \tag{24}$$

Суммируя оценки (22) и учитывая (20), (23) и (24), получаем

$$V \leqslant V_1 + V_2 + V_3 \leqslant k^2 nR + (k-1)R + kR \leqslant 3k^2 nR. \tag{25}$$

Пусть T — наибольшая длина μ-цепей формулы F, состоящих только из отмеченных μ-формул. Так как число отмеченных μ-подформул формулы F равно $\mu(F) - V$, то из леммы 2 следует, что

$$T \cdot z(F) \geqslant \mu(F) - V.$$

Поскольку функция g нелинейна, $z(F) > 0$. Из условия случая (d) следует, что все центры формулы F неотмечены, а значит, $V \geqslant z(F)$. Таким образом, имеем

$$\begin{aligned}
T &\geqslant \frac{\mu(F) - V}{z(F)} \geqslant \frac{\mu(F) - V}{V} = \frac{\mu(F)}{V} - 1 \geqslant (\text{ см. (21) и (25)}) \\
&\geqslant \frac{9k^4 n^2 m_k R}{3k^2 nR} - 1 = 3k^2 n m_k - 1 \geqslant 2k^2 n m_k \\
&\geqslant (\text{пользуемся неравенствами } k \geqslant \ln k + 1 \text{ и } n \geqslant \ln(n+1) \geqslant 1) \\
&\geqslant 2k(\ln k + 1)m_k \ln(n+1) = 2k(\ln k \cdot \ln(n+1)^{m_k} + \ln(n+1)^{m_k}) \\
&\geqslant (k+1)(\ln k + \ln(n+1)^{m_k}) = (k+1)\ln(kp^m).
\end{aligned} \tag{26}$$

Из условия случая (d) следует, что все отмеченные μ-подформулы формулы F незабиваемы. Поэтому в F найдется μ-цепь длины T, состоящая из незабиваемых μ-подформул. Применяя лемму 3, условие $m(F) \leqslant k$, оценку (26) и неравенство $(1 + 1/k)^{k+1} > e$, получаем

$$L(F) \geqslant \Big(1 + \frac{1}{m(F)}\Big)^T \geqslant \Big(1 + \frac{1}{k}\Big)^{(k+1)\ln(kp^m)} > e^{\ln(kp^m)} = kp^m,$$

а это противоречит (19). Утверждение 1 доказано.

Применяя доказанное утверждение к функции $g = f_{n+1}^{(m_k)}$, используя определение p и равенство $1/r = R/p^m$, получаем

$$L_n(f_{n+1}^{(m_k)}) > \Big(k + \frac{1}{r}\Big)(n+1)^{m_k} - R = \Big(k + \frac{R}{p^m}\Big)p^m - R = k(n+1)^{m_k}.$$

Теорема 1 доказана.

Теорема 2. *$P_2(n+1) \prec P_2(n)$ при любом $n \geqslant 2$.*

Доказательство. Из вложения $P_2(n+1) \supset P_2(n)$ следует, что $L_{n+1}(f) \leqslant L_n(f)$ для любой f. Поэтому $P_2(n+1) \preccurlyeq P_2(n)$. Из теоремы 1 непосредственно следует, что обратное неравенство не выполнено, т. е. по определению $P_2(n+1) \prec P_2(n)$. Теорема 2 доказана.

Автор выражает благодарность своему научному руководителю О. Б. Лупанову, а также Н. А. Карповой и М. И. Гринчуку за большую помощь в подготовке этой работы.

ЛИТЕРАТУРА

1. **Лупанов О. Б.** О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. М.: Физматгиз, 1960. Вып. 3. С. 61–80.
2. **Мучник Б. А.** Оценка сложности реализации линейной функции в некоторых базисах // Кибернетика. 1970. № 4. С. 29–38.
3. **Стеценко В. А.** О предплохих базисах в P_2 // Математические вопросы кибернетики. М.: Наука, 1992. Вып. 4. С. 139–177.
4. **Субботовская Б. А.** О сравнении базисов при реализации функций алгебры логики формулами // Докл. АН СССР. 1963. Т. 149, № 4. С. 784–787.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва,
Россия

Статья поступила
28 апреля 1997 г.,
переработанный вариант —
10 сентября 1997 г.