Д. А. Дагаев, О сложности псевдолинейных функций, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 2010, номер 2, 53–56

В заключение отметим, что с помощью более аккуратной оценки в неравенстве (5) результат теоремы может быть несколько улучшен:

$$T_k(n) = \sum_{1\leqslant m\leqslant n} \tau_k(m) \leqslant nc^{k-1} \sum_{j=0}^{\left[\frac{k}{2}\right]} \binom{k-1-j}{j} \frac{b^j}{c^{2j}} L_{k-1-2j}\left(-\frac{\ln n}{c}\right), \tag{7}$$

где $L_r(x)$ — многочлен Лагерра степени r, а $c = 1 - a$ и b — такие неотрицательные константы, что для всех целых $m \geqslant 1$ выполнено неравенство

$$a\left[\frac{n}{m}\right] - b \leqslant \sum_{\substack{1\leqslant d\leqslant n\\ d\equiv 0 \pmod m}} \left\{\frac{n}{d}\right\}.$$

Здесь константы могут быть выбраны следующим образом: $a = \ln 2 - 0{,}5$, $b = 6\ln 2 - 3{,}7$. Тогда неравенство (7) дает нам некоторое улучшение оценки (3). При $a = 0$ и $b = 0$ из неравенства (7) получаем (3).

Автор выражает благодарность научному руководителю профессору В. Н. Чубарикову за постановку задачи и внимание к работе.

СПИСОК ЛИТЕРАТУРЫ

1. *Марджанишвили К.К.* Оценка одной арифметической суммы // Докл. АН СССР. 1939. **22**, вып. 7. 391–393.
2. *Митькин Д.А.* Об оценке некоторых арифметических сумм с числом делителей // Матем. заметки. 2006. **80**, вып. 3. 471–472.

Поступила в редакцию
19.06.09

УДК 519.714

О СЛОЖНОСТИ ПСЕВДОЛИНЕЙНЫХ ФУНКЦИЙ

Д. А. Дагаев[1]

В работе получены верхние и нижние оценки сложности функций трехзначной логики, которые принимают значения из множества $\{0, 1\}$ и ограничения которых на множестве наборов из нулей и единиц являются линейными функциями.

Ключевые слова: функции трехзначной логики, формулы, сложность формул.

Upper and lower estimates for the complexity of functions of the 3-valued logic taking values from the set $\{0, 1\}$ with linear Boolean restrictions are derived.

Key words: functions of three-valued logic, formulas, complexity of formulas.

Рассматривается задача о реализации функций трехзначной логики формулами над конечными системами. О. Б. Лупанов [1] для любой полной системы булевых функций получил асимптотически точную оценку функции Шеннона. В работе [2] показано, что для произвольной конечной системы Ψ булевых функций всякая функция из $[\Psi]$ может быть реализована формулой со сложностью, имеющей не более чем экспоненциальный порядок роста от числа переменных. Пример последовательности функций четырехзначной логики, сложность которых в классе формул над некоторой конечной неполной системой имеет порядок роста “двойной экспоненты” от числа переменных, приведен в [3]. В [4, 5] для некоторых замкнутых классов трехзначной логики получены верхние оценки соответствующих функций Шеннона. В настоящей работе исследуется сложность функций трехзначной логики, которые принимают значения

[1] *Дагаев Дмитрий Александрович* — асп. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: ddagaev@gmail.com.

из множества $\{0,1\}$ и ограничения которых на множестве наборов из нулей и единиц являются линейными булевыми функциями. Все необходимые определения можно найти в [1–3, 6–9].

Пусть $E_k = \{0,1,\ldots,k-1\}$, $k \geqslant 2$. Обозначим через E_k^n множество всех наборов $\widetilde{\alpha} = (\alpha_1,\ldots,\alpha_n)$, таких, что $\alpha_1,\ldots,\alpha_n \in E_k$. Множество всех функций k-значной логики обозначим через P_k, а множество всех функций из P_3, принимающих значения только из множества E_2, — через $P_{3,2}$. Пусть $F \subseteq P_k$. Обозначим через $[F]$ замыкание множества F относительно операций суперпозиции и введения несущественной переменной (см. [6]), а через $F(n)$ — множество всех функций из F, зависящих от переменных $x_1,\ldots,x_n$, $n \geqslant 1$.

Определим следующие множества булевых функций: L — множество всех линейных функций, S — множество всех самодвойственных функций, T_i — множество всех функций, сохраняющих константу i, $i = 0,1$. Положим $L_i = L \cap T_i$, $i = 0,1$; $L_{01} = L_0 \cap L_1$; $SL = S \cap L$. Дизъюнкцию x_1 и x_2, конъюнкцию x_1 и x_2, сумму по модулю два x_1 и x_2 будем обозначать через $x_1 \vee x_2$, $x_1 \& x_2$, $x_1 \oplus x_2$ соответственно.

Пусть Ψ — конечная система функций из P_k, $f(x_1,\ldots,x_n) \in [\Psi]$, Φ — формула над Ψ, реализующая функцию f, а $F \subseteq [\Psi]$. Обозначим через $L(\Phi)$ число символов переменных и констант, входящих в формулу Φ (сложность формулы Φ), через $L_\Psi(f)$ — сложность функции f, а через $L_\Psi(F(n))$ — функцию Шеннона для множества F.

Пусть $f(x_1,\ldots,x_n) \in P_{3,2}$. Проекцией функции $f(x_1,\ldots,x_n)$ называется такая булева функция $(\mathrm{pr}\, f)(x_1,\ldots,x_n)$, значение которой на произвольном наборе $\widetilde{\alpha} \in E_2^n$ определяется равенством $(\mathrm{pr}\, f)(\widetilde{\alpha}) = f(\widetilde{\alpha})$. В дальнейшем функцию $(\mathrm{pr}\, f)(x_1,\ldots,x_n)$ будем обозначать через $\mathrm{pr}\, f(x_1,\ldots,x_n)$. Проекцией $\mathrm{pr}\, F$ множества функций $F \subseteq P_{3,2}$ называется множество $\bigcup\{\mathrm{pr}\, f\}$, где объединение берется по всем функциям $f \in F$. Нетрудно убедиться, что для любого замкнутого класса $F \subseteq P_{3,2}$ множество $\mathrm{pr}\, F$ является замкнутым классом булевых функций. Положим $\mathcal{L} = \{f \in P_{3,2} | \mathrm{pr}\, f \in L\}$. Функция $f(x_1,\ldots,x_n) \in P_{3,2}$ называется псевдолинейной, если $f \in \mathcal{L}$.

Пусть $f(x_1,\ldots,x_n) \in P_{3,2}$, $H \subseteq E_3^n$. Будем называть ограничением функции f на множество H такую функцию из $P_{3,2}$, значение которой на произвольном наборе $\widetilde{\alpha} \in E_3^n$ равно $f(\widetilde{\alpha})$, если $\widetilde{\alpha} \in H$, и равно 0, если $\widetilde{\alpha} \notin H$ (обозначение $f|_H$).

Обозначим через $j_i(x)$ функцию из $P_{3,2}$, равную 1 при $x = i$ и 0 в остальных случаях, $i \in E_3$, а через $x+y$ и $x \cdot y$ — функции из $P_{3,2}$, такие, что для любых $\alpha, \beta \in E_3$ выполняются равенства $\alpha+\beta = j_1(\alpha) \oplus j_1(\beta)$ и $\alpha \cdot \beta = j_1(\alpha) \& j_1(\beta)$ соответственно.

Приведем описание замкнутых классов $H \subseteq P_{3,2}$, таких, что $\mathrm{pr}\, H = L$. Пусть $f(x_1,\ldots,x_n)$ — произвольная псевдолинейная функция. Нетрудно видеть, что выполняется равенство

$$f(x_1,\ldots,x_n) = \sum j_{\sigma_1}(x_1)\ldots j_{\sigma_n}(x_n),$$

где суммирование производится по всем наборам $\widetilde{\sigma} = (\sigma_1,\ldots,\sigma_n) \in E_3^n$, таким, что $f(\widetilde{\sigma}) = 1$. Заменим каждое вхождение функции $j_0(y)$ в правой части этого равенства на равную ей функцию $1 + j_1(y) + j_2(y)$ и раскроем скобки. Получим представление функции $f(x_1,\ldots,x_n)$ в следующем виде:

$$f(x_1,\ldots,x_n) = \eta_f(x_1,\ldots,x_n) + \delta_f(x_1,\ldots,x_n), \tag{1}$$

где

$$\eta_f(x_1,\ldots,x_n) = a + \sum_{i=1}^{n} a_i j_1(x_i), \quad \delta_f(x_1,\ldots,x_n) = \sum_{I,J} a_{I,J} \varkappa_{I,J}(x_1,\ldots,x_n),$$

$$\varkappa_{I,J}(x_1,\ldots,x_n) = \left(\prod_{i\in I} j_1(x_i)\right)\left(\prod_{j\in J} j_2(x_j)\right),$$

$a, a_i, a_{I,J} \in \{0,1\}$, а суммирование в определении функции δ_f производится по всем множествам I, J, таким, что $I \cup J \subseteq \{1,\ldots,n\}$, $I \cap J = \varnothing$, $J \neq \varnothing$. Если $a_{I,J} = 1$, то функция $\varkappa_{I,J}(x_1,\ldots,x_n)$ называется компонентой функции f. Множество всех компонент функции f будем обозначать через K_f. Положим $K = \bigcup K_f$, где объединение берется по всем псевдолинейным функциям f. Легко видеть, что представление функции $f \in \mathcal{L}$ в виде (1) единственно (с точностью до перестановки слагаемых и порядка множителей в слагаемых). Обозначим через J_f множество всех функций $j_1(x_i)$, $1 \leqslant i \leqslant n$, таких, что $a_i = 1$ в представлении функции f в виде (1). Определим множество H_f следующим образом: если $a = 1$ в представлении функции f в виде (1), то $H_f = \{1\}$; в противном случае $H_f = \varnothing$. Положим $Y_f = K_f \cup J_f \cup H_f$.

Пусть $a \in E_2$. Определим подмножество $Z_{2,a}$ множества $P_{3,2}$, $a = 0, 1$. Функция $f(x_1, \ldots, x_n) \in P_{3,2}$ принадлежит множеству $Z_{2,a}$ в том и только в том случае, если она удовлетворяет следующему условию: если $\widetilde{\alpha} \in E_2^n$, $\widetilde{\beta} \in E_3^n$ и набор $\widetilde{\alpha}$ получается из набора $\widetilde{\beta}$ заменой всех двоек на a, то $f(\widetilde{\alpha}) = f(\widetilde{\beta})$, $n \geqslant 1$.

Определим следующие подмножества множества $\mathcal{L}$. Положим

$$L_2 = \{f \in \mathcal{L} | K_f \subseteq \{\varkappa_{I,J} \in K | \ |I| \leqslant 1\}\},$$

$$L_{2,r} = \{f \in \mathcal{L} | K_f \subseteq \{\varkappa_{I,J} \in K | \ I = \varnothing, |J| \leqslant r\}\}, \quad 1 \leqslant r < \infty,$$

$$L_{2,\infty} = \{f \in \mathcal{L} | K_f \subseteq \{\varkappa_{I,J} \in K | \ I = \varnothing\}\}.$$

В работе [7] показано, что множество всех замкнутых классов $F \subseteq \mathcal{L}$, таких, что $\operatorname{pr} F = L$, состоит из следующих классов: $\mathcal{L}$, L_2, $L_{2,\infty}$, $Z_{2,0} \cap \mathcal{L}$, $Z_{2,1} \cap \mathcal{L}$, $L_{2,r}$, где $1 \leqslant r < \infty$. При этом каждый из перечисленных замкнутых классов, кроме класса $L_{2,\infty}$, имеет конечный базис.

Положим $\lambda(x, y) = j_1(x) + j_1(y)$, $\mu(x, y) = j_1(x) j_2(y)$, $\nu_r(x_1, \ldots, x_r) = j_2(x_1) j_2(x_2) \ldots j_2(x_r)$, $r \geqslant 1$. Определим следующие системы функций из $\mathcal{L}$. Положим

$$\mathfrak{A} = \{1, \lambda(x, y)\}, \quad \mathfrak{B} = \mathfrak{A} \cup \{j_1(x) j_1(y) j_2(z), j_0(x), j_1(x), j_2(x)\}, \quad \mathfrak{C} = \mathfrak{A} \cup \{\mu(x, y)\},$$

$$\mathfrak{D}_r = \mathfrak{A} \cup \{\nu_r(x_1, \ldots, x_r)\}, \quad \mathfrak{E} = \{1, j_0(x) + j_0(y)\}.$$

Известно [7], что $[\mathfrak{A}] = Z_{2,0} \cap \mathcal{L}$, $[\mathfrak{B}] = \mathcal{L}$, $[\mathfrak{C}] = L_2$, $[\mathfrak{D}_r] = L_{2,r}$, $[\mathfrak{E}] = Z_{2,1} \cap \mathcal{L}$.

Ниже устанавливаются оценки функций Шеннона для всех конечно-порожденных замкнутых классов $F \subseteq P_{3,2}$, таких, что $\operatorname{pr} F = L$.

Теорема 1. *Пусть $Q = Z_{2,0} \cap \mathcal{L}$, $U = Z_{2,1} \cap \mathcal{L}$, $W = L_2$, $V_r = L_{2,r}$, где $1 \leqslant r < \infty$. Тогда имеют место следующие соотношения:*

$$L_{\mathfrak{A}}(Q(n)) = L_{\mathfrak{E}}(U(n)) = n + 1, \quad n \geqslant 2; \tag{2}$$

$$L_{\mathfrak{D}_r}(V_r(n)) = 1 + n + r(C_n^1 + C_n^2 + \ldots + C_n^r), \quad n \geqslant r; \tag{3}$$

$$L_{\mathfrak{C}}(W(n)) = n 2^{n-1} + 2^{n+1} - 1, \quad n \geqslant 2. \tag{4}$$

Теорема 2. *Справедливо соотношение*

$$L_{\mathfrak{B}}(\mathcal{L}(n)) \sim \frac{3^n}{\log_2 n}. \tag{5}$$

При доказательстве теоремы 1 используется следующая лемма.

Лемма. *Пусть $f(x_1, \ldots, x_n)$ — произвольная функция из $L_{2,r}$, существенно зависящая от n переменных, $n \geqslant 2$. Тогда $L_{\mathfrak{D}_r}(f) = |J_f| + |H_f| + r|K_f|$.*

Доказательство теоремы 1 проводится следующим образом. В (2) равенство $L_{\mathfrak{A}}(Q(n)) = n+1$ вытекает из того, что для любой функции $f(x_1, \ldots, x_n) \in Q$, существенно зависящей от n переменных, $n \geqslant 2$, выполняется соотношение $L_{\mathfrak{A}}(f) = L_{\{1, x+y\}}(\operatorname{pr} f) = n + 1$. Равенство $L_{\mathfrak{E}}(U(n)) = n + 1$ имеет место из соображений двойственности.

Докажем равенство (3). Если $n = r = 1$, то утверждение очевидно. Пусть $n \geqslant 2$, $n \geqslant r \geqslant 1$. Легко видеть, что для любой функции $f(x_1, \ldots, x_n) \in V_r(n)$ выполняются неравенства $|J_f| + |H_f| \leqslant 1 + n$, $|K_f| \leqslant C_n^1 + \ldots + C_n^r$. Поэтому в силу леммы $L_{\mathfrak{D}_r}(V_r(n)) \leqslant 1 + n + r(C_n^1 + C_n^2 + \ldots + C_n^r)$, что и доказывает верхнюю оценку.

Докажем нижнюю оценку. Обозначим через θ_n функцию из множества $V_r(n)$, у которой в представлении (1) все коэффициенты равны 1. Очевидно, что $|J_{\theta_n}| + |H_{\theta_n}| = 1 + n$ и $|K_{\theta_n}| = C_n^1 + \ldots + C_n^r$. Из леммы следует, что $L_{\mathfrak{D}_r}(\theta_n) = |J_{\theta_n}| + |H_{\theta_n}| + r|K_{\theta_n}| = 1 + n + r(C_n^1 + \ldots + C_n^r)$. Поэтому $L_{\mathfrak{D}_r}(V_r(n)) \geqslant L_{\mathfrak{D}_r}(\theta_n) = 1 + n + r(C_n^1 + C_n^2 + \ldots + C_n^r)$.

При доказательстве равенства (4) сначала для любой функции $f \in L_2$, существенно зависящей от n переменных, $n \geqslant 2$, устанавливается неравенство $L_{\mathfrak{C}}(f) \leqslant |Y_f| + B(f)$, где $B(f)$ — некоторая величина, которая однозначно вычисляется по функции f. Затем показывается, что $|Y_f| \leqslant n 2^{n-1} + 2^n$, $B(f) \leqslant 2^n - 1$, и поэтому выполняется неравенство $L_{\mathfrak{C}}(f) \leqslant n 2^{n-1} + 2^{n+1} - 1$. Наконец, рассматривается такая функция $\tau_n(x_1, \ldots, x_n)$ из L_2, у которой в представлении (1) все коэффициенты равны 1, и показывается, что ее сложность удовлетворяет неравенству $L_{\mathfrak{C}}(\tau_n) \geqslant n 2^{n-1} + 2^{n+1} - 1$.

Приведем план доказательства теоремы 2. Верхняя оценка в соотношении (5) получается с помощью модификации асимптотически оптимального метода синтеза формул над базисом $\{\&, \vee, \bar{\ }\}$ [8] (другие обобщения см. в [10, 11]). Доказательство опирается на существование специального разбиения $\mathfrak{Y}$ множества E_3^n, $n \geqslant 1$, на непересекающиеся подмножества $\Gamma_0, \Gamma_1, \ldots, \Gamma_t$ (где t — параметр, зависящий от n). Это разбиение получается на основе метода построения совершенных кодов Хэмминга [9] длины m, $m < n$, над полем $GF(3)$, где m — параметр вида $m = (3^r - 1)/2$, $r \in \mathbb{N}$. Разбиение $\mathfrak{Y}$ обладает следующими свойствами: число наборов, содержащихся в множестве Γ_0, "достаточно мало", и для каждого множества Γ_i, $i = 1, \ldots, t$, найдется номер $j_i \leqslant m$, такой, что для любого набора $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \Gamma_i$ выполняется равенство $\alpha_{j_i} = 2$.

Пусть $f(x_1, \ldots, x_n) \in \mathcal{L}$, $n \geqslant 3$, $f|_{\Gamma_i}$ — ограничение функции f на множество Γ_i, $i = 0, \ldots, t$, а $A = \Gamma_1 \cup \ldots \cup \Gamma_t$. Опишем основные этапы построения формулы Φ над $\mathfrak{B}$, реализующей функцию f. Сначала строятся формулы $\Phi_1, \ldots, \Phi_t$, реализующие функции $f|_{\Gamma_1}, \ldots, f|_{\Gamma_t}$ соответственно, методом, который аналогичен методу синтеза формул из [8]. При этом вместо функций $x \vee y$ и $x \& y$ используются функции $j_1(x) + j_1(y)$ и $j_1(x)j_1(y)j_2(x_{j_i})$ соответственно (см. свойства разбиения $\mathfrak{Y}$). Далее строится формула Φ_A, которая реализует функцию $f|_A$ и имеет сложность, не превышающую мощностную нижнюю оценку для функции $L_{\mathfrak{B}}(\mathcal{L}(n))$. Затем в качестве формулы Φ_0 для функции $f|_{\Gamma_0}$ берется формула, "аналогичная" совершенной дизъюнктивной нормальной форме этой функции. Наконец, рассматривается формула $\Phi = j_1(\Phi_0) + j_1(\Phi_A)$, которая реализует функцию f, причем ее сложность (в силу свойств разбиения $\mathfrak{Y}$) асимптотически равна сложности формулы Φ_A.

Нижняя оценка в соотношении (5) следует из мощностных соображений [8] и равенства

$$|\mathcal{L}(n)| = 2^{n+1} \cdot 2^{3^n - 2^n}.$$

Замечание. Для замкнутых классов $F \subseteq P_{3,2}$, таких, что $\mathrm{pr}\, F \in \{L_0, L_1, LS, L_{01}\}$, можно установить аналогичные соотношения.

Автор выражает благодарность профессору А.Б. Угольникову за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект № 08–01–00863), программы "Ведущие научные школы РФ" (проект НШ–4470.2008.1) и программы фундаментальных исследований ОМН РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Задачи оптимального синтеза управляющих систем").

СПИСОК ЛИТЕРАТУРЫ

1. *Лупанов О.Б.* О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. М.: Физматгиз, 1960. 61–80.
2. *Угольников А.Б.* О глубине формул в неполных базисах // Математические вопросы кибернетики. Вып. 1. М.: Наука, 1988. 242–245.
3. *Угольников А.Б.* О сложности реализации формулами одной последовательности функций 4-значной логики // Вестн. Моск. ун-та. Матем. Механ. 2004. № 3. 52–55.
4. *Дагаев Д.А.* Глубина и сложность реализации формулами функций из некоторых классов трехзначной логики // Тез. докл. XV Междунар. конф. "Проблемы теоретической кибернетики" (Казань, 2–7 июня 2008 г.). Казань: Отечество, 2008. 24.
5. *Дагаев Д.А.* О глубине формул, реализующих функции из некоторых классов трехзначной логики // Мат-лы IX Междунар. семинара "Дискретная математика и ее приложения" (Москва, 18–23 июня 2007 г.). М.: Изд-во ЦПИ при механико-математическом факультете МГУ, 2007. 84–87.
6. *Яблонский С.В.* Введение в дискретную математику. М.: Высшая школа, 2008.
7. *Lau D.* Function Algebras on Finite Sets. Berlin: Springer-Verlag, 2006.
8. *Лупанов О.Б.* О синтезе некоторых классов управляющих систем // Проблемы кибернетики. Вып. 10. М.: Наука, 1963. 63–97.
9. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
10. *Гашков С.Б.* О параллельном вычислении некоторых классов многочленов с растущим числом переменных // Вестн. Моск. ун-та. Матем. Механ. 1990. № 2. 88–92.
11. *Захарова Е.Ю.* Реализация функций из P_k формулами // Матем. заметки. 1972. **11**, № 1. 99–108.

Поступила в редакцию
18.09.2009