S. P. Yukna, On an entropic method for obtaining lower bounds on the complexity of Boolean functions, *Dokl. Akad. Nauk SSSR*, 1988, Volume 298, Number 3, 556–559

ЛИТЕРАТУРА

1. *Bestvina M.* Characterizing k-dimensional universal Menger compacta. Dissertation. Knoxville. Univ. Tennessee, 1984. 2. *Engelking R.* Dimension Theory. Warszawa: PWN, 1978. 3. *Chapman T.A.* – Fund. Math., 1972, vol. 76, p. 181. 4. *Chapman T.A.* – Ibid., 1972, vol. 76, p. 261. 5. *Geoghegan R., Summerhill R.* – Trans. Amer. Math. Soc., 1973, vol. 179, p. 281. 6. *Borsuk K.* Theory of Shape. Warszawa: PWN, 1975. 7. *Lacher R.C.* – Bull. Amer. Math. Soc., 1977, vol. 83, p. 495.

УДК 519.714 МАТЕМАТИКА

С.П. ЮКНА

ОБ ОДНОМ ЭНТРОПИЙНОМ МЕТОДЕ ПОЛУЧЕНИЯ НИЖНИХ ОЦЕНОК СЛОЖНОСТИ БУЛЕВЫХ ФУНКЦИЙ

(Представлено академиком А.Н. Тихоновым 25 IX 1986)

В силу известного эффекта Шеннона–Лупанова почти все булевы функции (БФ) при реализации обычными логическими схемами такими, как схемы из функциональных элементов (СФЭ), контактные схемы (КС) и др., требуют экспоненциального числа элементов. Тем не менее эффективно (т.е. без привлечения полного перебора всех БФ) строить сложнореализуемые БФ пока не удается: наиболее высокими эффективными нижними оценками (ЭНО) остаются оценки порядка $\Omega(n^2)$, где n – число переменных БФ, полученные Э.И. Нечипоруком [1] и В.М. Храпченко [2]. На принципиальность такого явления указывают также результаты С.В. Яблонского о неустранимости полного перебора при построении самых сложных БФ посредством так называемых правильных алгоритмов [3]. Поэтому для выяснения природы возникающих трудностей приходится так или иначе ограничивать класс схем.

Первый нетривиальный результат в этом направлении получил Э.И. Нечипорук в [4], где доказаны полиномиальные ЭНО для формул в некоторых специальных базисах. Затем Г.А. Ткачев [5] получил первую экспоненциальную ЭНО $\Omega(\exp(n^{1/4}))$ для СФЭ ограниченной глубины. А.К. Пулатов [6] и С.Е. Кузнецов [7] получили аналогичные оценки для схем без нулевых цепей. Для монотонных СФЭ*, т.е. СФЭ в базисе $\{\&, \vee, 0, 1\}$, первую экспоненциальную ЭНО порядка $\exp(n^{1/8-o(1)})$ удалось получить А.Е. Андрееву [9]. Независимо А.А. Разборов [10] для этого класса схем получил ЭНО $n^{c\log_2 n}$, $c > 0$. Следует заметить, что вводимые ограничения приводят к тому, что реализуемая подсхемой функция слабо зависит или вообще не зависит (как в случае монотонных схем или схем без нулевых цепей) от всей схемы, т.е. к определенной локальности вычислений.

В настоящей заметке предлагается новый метод получения ЭНО для контактных схем. В случае локальных схем он позволяет получать экспоненциальные ЭНО, рост которых достигает $n^{c\sqrt{n}}$, $c > 0$. Метод является подходящей конкретизацией

*Известно [8], что сложность самых сложных БФ в этом классе схем асимптотически равна $\sqrt{2/\pi}\cdot 2^n\cdot n^{-3/2}$.

(на случай булевых функций) предложенного ранее автором [11] более общего подхода к проблеме получения ЭНО сложности вычислений, основанного на введенном Ю.И. Яновым [12] понятии свертки алгоритмов. Общая идея метода достаточно проста. При заданном классе схем $\mathfrak{A}$ с мерой их сложности μ задача состоит в том, чтобы без привлечения понятия реализуемости определить нижнюю оценку для $L_\mu(f) = \min\{\mu(S): S$ реализует $f\}$. Каждую схему S отождествляем с некоторой совокупностью S^* ее "подсхем" и вводим подходящее отношение φ "подобия" таких подсхем. Под φ-э н т р о п и е й $H^\varphi(S)$ схемы S понимаем минимальное число покрывающих S^* φ-интервалов, т.е. множеств $A \subseteq S^*$ таких, что для любых $a, b \in A$ $a\varphi b$ или $b\varphi a$. Второй шаг состоит в построении сохраняющих энтропию вложений схем. При этом считаем, что схема S_1 (φ, ψ)-эпиморфна схеме S_2, если существует такая (возможно, частичная) сюръекция $\nu: S_1^* \to S_2^*$, что для любых $a, b \in \nu^{-1}(S_2^*)$ $a\varphi b$ влечет $\nu(a)\psi\nu(b)$. Тогда $H^\varphi(S_1) \geqslant H^\psi(S_2)$ (хотя возможно, что $\mu(S_1) < \mu(S_2)$). Для получения требуемой оценки выделяем некоторые промежуточные классы (более ограниченных) схем $\mathfrak{A} = \mathfrak{A}_0 \supset \mathfrak{A}_1 \supset \ldots \supset \mathfrak{A}_k$, где $\mathfrak{A}_k$ – класс исходных заданий БФ, и определяем отношения их подобия $\varphi_0, \varphi_1, \ldots, \varphi_k$ так, чтобы каждая реализующая f схема из $\mathfrak{A}_i$ была $(\varphi_i, \varphi_{i+1})$-эпиморфной некоторой реализующей f схеме из $\mathfrak{A}_{i+1}$. Если при этом φ_0 такое, что $H^{\varphi_0} \leqslant \mu$, то $L_\mu(f) \geqslant H^{\varphi_k}(f)$.

Используемые далее без пояснений понятия можно найти в [13]. Для КС S через S^v (через S_v) обозначаем дизъюнкцию всех ненулевых цепей из входа схемы S в вершину v (соответственно из v в выход S). Окрестность вершины v – это множество переменных x таких, что для некоторых цепей $K_0 \in S_v, K_1, K_2 \in S^v$ и $\alpha \in \{0, 1\}$ имеет место: $x^\alpha \in K_0$, $\overline{x}^\alpha \in K_1$ и $\overline{x}^\alpha \notin K_2$. Схему, окрестность любой вершины которой содержит не более чем $\lambda \geqslant 0$ переменных, называем λ-л о к а л ь н о й. Любая КС, реализующая БФ от n переменных, λ-локальна при некотором $0 \leqslant \lambda \leqslant n$. Примерами 0-локальных схем служат монотонные КС (т.е. КС из замыкающих контактов) и схемы без нулевых цепей. Помимо обычных КС, представляют также интерес детерминированные схемы (ДКС), т.е. схемы, любой двоичный вектор в которых реализует не более одной ветви. Частным случаем таких схем являются бинарные программы (см., например, [14, 15]). Пусть $L_\lambda(f)$ – минимальное число контактов, достаточное для реализации БФ f λ-локальной КС. В случае ДКС меру L_λ будем обозначать l_λ. Известно [14], что $l_n \leqslant L_n^{O(1)}$.

Контактное дерево (КД), каждая ветвь которого не содержит повторных вхождений переменных, называем б е с п о в т о р н ы м. Если V – множество вершин КД T и $\varphi \subseteq V \times V$, то φ-э н т р о п и е й $H^\varphi(T)$ д е р е в а T считаем минимальное число покрывающих V φ-интервалов. Э н т р о п и е й БФ f считаем число $H^\varphi(f) = \min\{H^\varphi(T): T$ – бесповторное КД и T реализует $f\}$. В случае ДКС энтропию f будем обозначать $h^\varphi(f)$. Для элементарных конъюкций K, M и ДНФ $D = K_1 \vee \ldots \vee K_q$ полагаем: $K \dot{-} M = \{x^\alpha \in K: \overline{x}^\alpha \notin M\}$ и $D\{K\} = \{K_1 \cdot K_1' \vee \ldots \vee K_q \cdot K_q': K_i' \subseteq K, i = 1, \ldots, q\}$. Для вершин v, u КД T полагаем:

$$v\psi u \iff (T^v \dot{-} T^u) \cdot T_v = (T^u \dot{-} T^v) \cdot T_u,$$
$$v\theta u \iff T_v\{T^v \dot{-} T^u\} \cap T_u\{T^u \dot{-} T^v\} \neq \phi.$$

Х э м м и н г о в о й называем любую БФ f такую, что любые два вектора из $f^{-1}(1)$ различаются не менее чем в двух координатах. Путем построения подходящих эпиморфных вложений схем доказывается

Т е о р е м а 1. *Для любой булевой функции f выполнены неравенства $L_\lambda(f) \geqslant H^\varphi(f) \cdot 3^{-\lambda}$ и $l_\lambda(f) \geqslant h^\varphi(f) \cdot 3^{-\lambda}$, где $\varphi = \psi$, если f хэммингова, и $\varphi = \theta$ в противном случае.*

Поскольку энтропия функций определяется энтропией их бесповторных КД, то в ряде случаев она оценивается достаточно просто. Сделаем это для трех классов булевых функций. Пусть $X = \{x_1, \ldots, x_n\}$ и $|A|$ – число элементов в множестве A. Отображение ρ: $X \to X \cup \{0, 1\}$ такое, что $\forall x \in X(\rho(x) \notin \{0, 1\} \Rightarrow \rho(x) = x)$ называем подстановкой; множество $\hat{\rho} = \rho^{-1}(0) \cup \rho^{-1}(1)$ – ее сигнатурой, а число $|\hat{\rho}|$ – ее рангом. Для БФ $f(X)$ полагаем $f^{\rho} = f(\rho(x_1), \ldots, \rho(x_n))$.

Функцию f называем (слабо) m-неоднородной, если для любых двух различных подстановок ρ и γ одной и той же сигнатуры ранга m выполнено: (либо $f^{\rho} = f^{\gamma} \equiv 0$, либо) $f^{\rho} \neq f^{\gamma}$. Класс таких функций достаточно богат: при любом $m \leqslant n - (1 + \epsilon)\log_2 n$, $\epsilon > 0$, почти все БФ от n переменных m-неоднородны. Пусть $Q_m(f)$ – минимальное число k подстановок $\rho_1, \ldots, \rho_k$ ранга m, достаточное для представления БФ f в виде $f = K_{\rho_1} \cdot f^{\rho_1} \vee \ldots \vee K_{\rho_k} \cdot f^{\rho_k}$, где $K_{\rho} = \{x^{\rho(x)} : x \in \hat{\rho}\}$.

Теорема 2. *Если f слабо $2m$-неоднородна, то $h^{\theta}(f) \geqslant Q_m(f)$. Если при этом f m-неоднородна, то $h^{\theta}(f) \geqslant 2^m$.*

Функцию $f(X)$ называем m-устойчивой, если для любой $x \in X$ и любого $Y \subseteq X - \{x\}$, $|Y| \leqslant m$, существует подстановка ρ сигнатуры $X - Y - \{x\}$ такая, что функция $f^{\rho}(x, Y)$ зависит только от переменной x, т.е. либо $f^{\rho}(x, Y) = x$, либо $f^{\rho}(x, Y) = \bar{x}$.

Теорема 3. *Если f $2m$-устойчива, то $h^{\theta}(f) \geqslant 2^m$.*

Пусть $|\tilde{\alpha}|$ – число единиц в $\tilde{\alpha} \in \{0, 1\}^n$. Функцию f называем (k, r)-равномерной, если для всех $\tilde{\alpha}$, $\tilde{\beta}$ из $f^{-1}(1)$ выполнено $|\tilde{\alpha}| = |\tilde{\beta}| \geqslant 2r$ и любые k векторов в $f^{-1}(1)$ имеют не более чем r общих единичных координат; k-равномерной, если она (k, r)-равномерна при некотором $r \geqslant 1$. Пусть $\|f\| = |f^{-1}(1)|$.

Теорема 4. *Если f k-равномерна, $k \geqslant 2$, то $h^{\psi}(f) \geqslant \|f\| \cdot (k-1)^{-2}$ и $H^{\psi}(f) \geqslant \|f\| \cdot (k-1)^{-3}$.*

Опираясь на полученные результаты, можно достаточно просто получать экспоненциальные ЭНО для локальных схем. При этом в ряде случаев получаются более высокие нижние оценки (и в более широких классах схем), чем оценки, даваемые наиболее сильными из известных специальными методами. Здесь приведем лишь некоторые из них.

Богатый класс примеров порождается задачей нахождения трансверсалей $(0, 1)$-матриц. Пусть $q \geqslant 2$ и $\bar{q} = \{0, 1, \ldots, q-1\}$. Пусть W_q – семейство всех одноместных функций σ: $\bar{q} \to \bar{q}$. Трансверсаль $(0, 1)$-матрицы $X = \{x_{i,j}: i, j \in \bar{q}\}$ – это функция $\sigma \in W_q$ такая, что $x_{i,\sigma(i)} = 1$ для всех $i \in \bar{q}$. Пусть $\mathrm{Tr}(X)$ – множество всех трансверсалей матрицы X. Для класса $F \subseteq W_q$ через $t_F(X)$ обозначим число трансверсалей X в F, т.е. $t_F(X) = |F \cap \mathrm{Tr}(X)|$. С любым классом $F \subseteq W_q$ связываем две булевы функции $F^0(X)$ и $F^1(X)$ (от $n = q^2$ переменных), полагая: $F^0(X) = 1 \Leftrightarrow t_F(X) > 0$ и $F^1(X) \equiv t_F(X) \pmod 2$. Пусть $\mathrm{gr}\,\sigma$ – график функции σ. Класс F называем m-плотным, если для любого $a \in \bar{q}^2$ и любого $A \subseteq \bar{q}^2 - \{a\}$, $|A| \leqslant m$, имеется $\sigma_0 \in F$ такая, что $a \in \mathrm{gr}\,\sigma_0$, $A \cap \mathrm{gr}\,\sigma_0 = \phi$ и $\mathrm{gr}\,\sigma - (A \cup \mathrm{gr}\,\sigma_0) \neq \phi$ для любой $\sigma \in F - \{\sigma_0\}$ такой, что $a \notin \mathrm{gr}\,\sigma$. Можно показать, что m-плотность класса $F \subseteq W_q$ влечет m-устойчивость обеих БФ F^0 и F^1. Отсюда

Следствие 1. *Для любого m-плотного класса $F \subseteq W_q$ и $\alpha \in \{0, 1\}$ выполнено неравенство $l_{\lambda}(F^{\alpha}) \geqslant 2^{m/2} \cdot 3^{-\lambda}$.*

Пусть $R = \{\sigma \in W_q: \forall i \in \bar{q}\,(\sigma^{-1}(i) \neq \phi \Rightarrow |\sigma^{-1}(i)| \geqslant 2)\}$. Класс R m-плотен при любом $m \leqslant q/2$. Отсюда

Следствие 2. *Пусть $\lambda \leqslant \sqrt{n}/20$ и $\alpha \in \{0, 1\}$. Тогда $l_{\lambda}(R^{\alpha}) \geqslant 2^{\sqrt{n}/5}$.*

Пусть $B \subseteq W_q$ – класс всех биекций и P – класс всех полиномов степени не выше $d = [q/2]$ над полем Галуа $GF(q)$ порядка q. Нетрудно видеть, что эти классы m-плотны при любом $m \leqslant d - 2$. Поэтому для порождаемых ими БФ P^{α} и B^{α}, $\alpha \in \{0, 1\}$, справедливы аналогичные оценки. Функции P^0 и B^0 рассматривались в

[9, 10], где для них в классе монотонных СФЭ доказаны оценки $\Omega(\exp(n^{1/8-o(1)}))$ и $\exp(\Omega(\log_2^2 n))$ соответственно. Что же касается близких к ним функций P^1 и B^1, то для них эти методы заведомо неприменимы (в силу немонотонности этих функций).

Через f_* обозначим характеристическую функцию множества нижних единиц монотонной БФ f. Ясно, что тогда f_* хэммингова.

Следствие 3. *Справедливы оценки*

$$l_\lambda(B_*^0) \geqslant \binom{\sqrt{n}}{\sqrt{n}/2} \cdot 3^{-\lambda}, \quad L_\lambda(P_*^0) \geqslant \sqrt{n}^{\sqrt{n}/2+1} \cdot 3^{-\lambda}.$$

Действительно, в силу теорем 1 и 4 достаточно заметить, что функция P_*^0 $(2, d)$-равномерна, функция B_*^0 $((q-r)!, r)$-равномерна при любом $1 \leqslant r \leqslant d$, причем $\| B_*^0 \| = q!$ и $\| P_*^0 \| = q^{d+1}$. Для сравнения приведем очевидную верхнюю оценку: $L_0(P_*^0) \leqslant \sqrt{n}^{\sqrt{n}/2+2}$.

Наконец, пусть f_n^s – монотонная БФ от $\binom{n}{2}$ переменных такая, что $f_n^s = 1 \iff$ когда n-вершинный граф, определяемый значениями переменных, содержит полный подграф на s вершинах. Пусть также $g_n = (f_n^s)_*$, где $s = n/2$. Эти функции рассматривались в [14, 15], где для них получены почти экспоненциальные нижние оценки в классе бесповторных (т. е. 0-локальных) бинарных программ. Наш метод прямо дает аналогичные оценки в более широком классе схем. Пусть $s = [\sqrt{n}]$, $f \in \{f_n^s, g_n\}$ и $\lambda \leqslant n/5$. Тогда $l_\lambda(f) \geqslant 2^{cn}$, где $c > 1/5$. Действительно, в силу теорем 1–3 достаточно лишь заметить, что функция g_n слабо $\binom{n/2}{2}$-неоднородна, а f_n^s m-устойчива при любом

$$m \leqslant \min\left\{\binom{s}{2}, (n-s)/2\right\} - 1.$$

Замечание. Известно, что функции B^0, B^1, P_*^0 и g в классе всех ДКС реализуемы с полиномиальной сложностью. Стало быть, переход от n-локальных схем к $n^{1/2-\epsilon}$-локальным влечет почти экспоненциальное увеличение их сложности.

В заключение автор приносит глубокую благодарность Ю.И. Янову за внимание к работе и полезные обсуждения.

Институт математики и кибернетики
Академии наук ЛитССР
Вильнюс

Поступило
28 V 1986

ЛИТЕРАТУРА

1. *Нечипорук Э.И.* – ДАН, 1966, т. 169, № 4, с. 765–767. 2. *Храпченко В.М.* – Матем. заметки, 1971, т. 10, № 1, с. 83–92. 3. *Яблонский С.В.* В сб.: Проблемы кибернетики. М., 1959, вып. 2, с. 75–121. 4. *Нечипорук Э.И.* Там же, 1970, вып. 23, с. 291–293. 5. *Ткачев Г.А.* В сб.: Комбинаторно-алгебраические методы в прикладной математике. Горький, 1980, с. 161–207. 6. *Пулатов А.К.* Там же, 1979, с. 81–95. 7. *Кузнецов С.Е.* – Изв. вузов. Математика, 1981, № 5, с. 56–63. 8. *Андреев А.Е.* – Вестн. МГУ. Математика, 1985, № 4, с. 83–87. 9. *Андреев А.Е.* – ДАН, 1985, т. 282, № 5, с. 1033–1037. 10. *Разборов А.А.* – ДАН, 1985, т. 281, № 4, с. 798–801. 11. *Jukna S.* – Cool. Math. Soc. J. Bolyai, 1984, vol. 44, p. 251–270. 12. *Янов Ю.И.* – ДАН, 1975, т. 224, № 2, с. 301–304. 13. *Нигматуллин Р.Г.* Сложность булевых функций. Казань: Изд-во Казан. ун-та, 1983. 208 с. 14. *Pudlak P., Žak S.* – Preprint, Univ. Prague, 1983. 30 p. 15. *Wegener I.* – Intern. Beriche, Univ. Frankfurt, 1985, № 5, 32 S.