О сложности алгоритмов*

В. Б. КУДРЯВЦЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: vbk@lsili.ru

А. Е. АНДРЕЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: andreev@lsi.com

УДК 519.95

Ключевые слова: схемы функциональных элементов, функция Шеннона, нижние оценки.

Аннотация

В работе представлен обзор результатов авторов по теории сложности алгоритмов. Описаны результаты по методам получения нижних оценок (приводятся почти экспоненциальные нижние оценки монотонной сложности монотонных функций) и асимптотически оптимальному синтезу функциональных сетей, по минимизации булевых функций и решению булевых уравнений.

Abstract

V. B. Kudryavtsev, A. E. Andreev, On algorithm complexity, Fundamentalnaya i prikladnaya matematika, vol. 15 (2009), no. 3, pp. 135—181.

This paper contains review of the authors' results in the theory of algorithm complexity. The results described concern the methods for obtaining lower bounds (containing almost all exponential lower bounds on monotone complexity of monotone functions), asymptotically optimal functional networks' synthesis, Boolean functions minimization, and the problems of solving Boolean equations.

Введение

Алгоритмы применяются к двум основным объектам — конечным и бесконечным множествам. В первом случае используются схемные вычисления, во втором — тьюринговы, или программные, вычисления.

Схемные вычисления оперируют с функциями k-значной логики. Накоплена целая коллекция конкретных схем вычислений: формулы, контактные схемы, схемы из функциональных элементов и др. При этом обычно предполагается, что вычисляются булевы функции.

*Работа поддерживалась грантом РФФИ № 06-01-00240.

Фундаментальная и прикладная математика, 2009, том 15, № 3, с. 135—181.

Тьюринговы вычисления используются, как правило, при анализе свойств счётных множеств. Особый интерес вызывают вычисления, связанные с анализом сложности строения семейств конечных множеств, например задачи поиска минимальных дизъюнктивных нормальных форм для булевых функций, решения булевых уравнений и др.

Здесь мы опишем результаты А. Е. Андреева по схемным вычислениям и результаты Нгуен Ким Ань, Т. М. Игамбердыева и А. Е. Андреева по минимизации булевых функций и решению булевых уравнений.

1. Более чем квадратичные эффективные нижние оценки сложности π-схем

На основе обобщения метода Б. А. Субботовской [84] и с использованием идеи универсальной функции Э. И. Нечипорука [63] мы построим пример функции, имеющей в классе π-схем сложность реализации по порядку не менее чем

$$\frac{n^{5/2}}{(\log n)^{3/2}\log\log n},$$

где n — число переменных. Самые высокие из известных ранее нижние оценки сложности реализации π-схемами индивидуальных функций имели рост n^2 (В. М. Храпченко [90]).

Пусть

$$\tilde{x}_1 = (x_1^1,\ldots,x_l^1),\ \tilde{x}_2(x_1^2,\ldots,x_l^2),\ldots,\ \tilde{x}_k(x_1^k,\ldots,x_l^k) -$$

попарно не пересекающиеся наборы различных переменных. Через $X_s^{k,l}$ обозначим множество всех таких наборов

$$\tilde{\alpha} = (j_{1,1},\ldots,j_{1,s},\ldots,j_{k,1},\ldots,j_{k,s},\sigma_{1,1},\ldots,\sigma_{1,s},\ldots,\sigma_{k,1},\ldots,\sigma_{k,s}),$$

что

$$1 \leqslant j_{i,1} \leqslant j_{i,2} \leqslant \ldots \leqslant j_{i,s} \leqslant l, \quad i = 1,2,\ldots,k;$$
$$\sigma_{i,t} \in \{0,1\}, \quad i = 1,2,\ldots,k, \quad t = 1,2,\ldots,s.$$

Для $f(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_k)$ через $f^{\tilde{\alpha}}$ обозначим функцию, которая получается из f подстановкой вместо переменных $x^i_{j_{i,t}}$ констант $\sigma_{i,t}$, $i = 1,2,\ldots,k$, $t = 1,2,\ldots,s$. Пусть $L(F)$ — сложность реализации функции f посредством π-схем.

Лемма 1.1 [14]. *Если $k \geqslant 1$, $l \geqslant 5$, то для любой булевой функции $f(\tilde{x}_1,\tilde{x}_2,\ldots,\tilde{x}_k)$, для которой $L(f) \geqslant 2$, существует такой набор $\tilde{\alpha}$ из $X_1^{k,l}$, что*

$$L(f^{\tilde{\alpha}}) \leqslant \varphi\left(\frac{1}{l}\right) L(f),$$

где

$$\varphi(x) = 1 - \frac{3}{2}x + \frac{1}{2}x^2.$$

Лемма 1.2 [14]. *Существует такая положительная константа c_0, что если $k \geqslant 1$, $l \geqslant r \geqslant 4$, то для любой булевой функции $f(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_k)$ существует такой набор $\tilde{\alpha}$ из $X_{l-r}^{k,l}$, что*

$$L(f^{\tilde{\alpha}}) \leqslant c_0 \left(\frac{l}{r}\right)^{-3/2} L(f).$$

Лемма 1.3 [14]. *Если $k \geqslant 1$, $l \geqslant r \geqslant 4$, функции $g_1(\tilde{x}_1), \ldots, g_k(\tilde{x}_k)$ не обращаются в константу ни на каком интервале размерности r и $f = g\big(g_1(\tilde{x}_1), \ldots, g_k(\tilde{x}_k)\big)$, то*

$$L(f) \geqslant \frac{1}{c_0} \left(\frac{l}{r}\right)^{3/2} L(g).$$

Пусть k — натуральное число, $k \geqslant 3$, $l =]2^k/k[$, $n = 2^k + k \cdot l$. Пусть набор $\tilde{y}$ состоит из 2^k различных переменных $y_{\sigma_1,\ldots,\sigma_k}$, $\sigma_1, \ldots, \sigma_k \in \{0,1\}$, не входящих в $\tilde{x}_1, \ldots, \tilde{x}_k$. Полагаем

$$F_n(\tilde{y}, \tilde{x}_1, \ldots, \tilde{x}_k) = \bigvee_{\sigma_1,\ldots,\sigma_k \in \{0,1\}} y_{\sigma_1,\ldots,\sigma_k} \wedge \left(\bigwedge_{i=1}^{k} (x_1^i \oplus \ldots \oplus x_l^i)^{\sigma_i} \right).$$

Теорема 1.1 [14]. *Имеет место оценка*

$$L(F_n) \geqslant C \cdot \frac{n^{5/2}}{(\log n)^{3/2} \log\log n},$$

где C — положительная константа.

2. Эффективные нижние оценки сложности монотонных функций

Рассмотрим задачу получения нижних оценок для сложности реализации индивидуальных монотонных функций схемами из функциональных элементов в монотонных базисах. Этой проблематике посвящено большое число работ.

До недавнего времени имелись лишь методы, которые позволяли получать относительно числа переменных только полиномиальные оценки [58, 67, 68, 70, 104—106, 108, 109, 115]. В 1984 г. А. Е. Андреев предложил метод, позволяющий получать почти экспоненциальные нижние оценки монотонной сложности ($2^{n^{1/3-o(1)}}$, где n — число переменных). Одновременно А. А. Разборов [73, 74] предложил метод, позволивший получить оценку вида $2^{O(\log^2 n)}$.

В [15] А. Е. Андреев предложил усовершенствованный вариант своего метода. Основным результатом является общая оценка сложности монотонной булевой функции через некоторые её комбинаторные характеристики. Был приведён пример последовательности функций, для которых полученная оценка имеет рост $2^{n^{1/3-o(1)}}$, где n — число переменных. Эта оценка остаётся самой высокой и в настоящее время.

2.1. Метрический критерий сложности $\mathcal{A}$-схем

Если $\mathcal{A} \subseteq \mathcal{P}$, где $\mathcal{P}$ — множество всех булевых функций, то $\mathcal{A}$-схемой будем называть схему в базисе $\{\&, \vee\}$, входным полюсам которой приписаны функции из множества $\mathcal{A}$. Через $L_{\mathcal{A}}(f)$ обозначим наименьшее число функциональных элементов, достаточное для реализации $\mathcal{A}$-схемой функции f. Ясно, что

$$L_{\mathcal{A}}(f) = 0 \iff f \in \mathcal{A},$$

и если $\mathcal{A}$ содержит константы 0, 1 и все переменные монотонной функции f, то

$$L^c_{\{\&,\vee,0,1\}}(f) \geqslant L_{\mathcal{A}}(f),$$

где $L^c_B(f)$ — сложность реализации f схемами из функциональных элементов в базисе B.

Неотрицательная функция $\rho(x, y)$ называется псевдометрикой, если она удовлетворяет следующим соотношениям:

$$\rho(x, x) = 0, \quad \rho(x, y) = \rho(y, x), \quad \rho(x, z) \leqslant \rho(x, y) + \rho(y, z).$$

Далее мы будем рассматривать псевдометрики на $\mathcal{P}^{\langle n\rangle}$, где $\mathfrak{A}^{\langle n\rangle}$ — множество всех булевых функций из $\mathfrak{A}$, зависящих от первых n переменных алфавита $\{u_1, u_2, \ldots, u_n, \ldots\}$. Псевдометрику ρ на $\mathcal{P}^{\langle n\rangle}$ будем называть монотонной, если

$$\{\tilde{\alpha} \mid f_1(\tilde{\alpha}) \neq f_2(\tilde{\alpha})\} \subseteq \{\tilde{\alpha} \mid f_3(\tilde{\alpha}) \neq f_4(\tilde{\alpha})\} \Longrightarrow \rho(f_1, f_2) \leqslant \rho(f_3, f_4).$$

Очевидно, что для любой монотонной псевдометрики ρ справедливо неравенство

$$\rho\big(F(u_1, \ldots, u_n, f_1), F(u_1, \ldots, u_n, f_2)\big) \leqslant \rho(f_1, f_2).$$

Полагаем

$$\rho(f, \mathcal{B}) = \max_{g \in \mathcal{B}} \rho(f, g), \quad f \in \mathcal{P}^{\langle n\rangle}, \quad \mathcal{B} \subseteq \mathcal{P}^{\langle n\rangle},$$

$$\rho(\mathcal{B}_1, \mathcal{B}_2) = \max_{f_1 \in \mathcal{B}_1} \max_{f_2 \in \mathcal{B}_2} \rho(f_1, f_2), \quad \mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{P}^{\langle n\rangle}.$$

Последовательность функций $f_1, f_2, \ldots, f_k$ будем называть правильной, если для любого i из $\{1, 2, \ldots, k-1\}$ либо $f_i \leqslant f_{i+1}$, либо $f_i \geqslant f_{i+1}$. Полагаем

$$\rho^{\uparrow}(f_1, \ldots, f_k) = \sum_{i,\ f_i \leqslant f_{i+1}} \rho(f_i, f_{i+1}),$$

$$\rho^{\downarrow}(f_1, \ldots, f_k) = \sum_{i,\ f_i \geqslant f_{i+1}} \rho(f_i, f_{i+1}).$$

Будем писать

$$[\rho_1, \rho_2](f, g) \leqslant (a_1, a_2),$$

если существует такая правильная последовательность $f_1, \ldots, f_k$, что $f_1 = f_2$, $g = f_k$ и

$$\rho_1^{\downarrow}(f_1, \ldots, f_k) \leqslant a_1, \quad \rho_2^{\uparrow}(f_1, \ldots, f_k) \leqslant a_2.$$

Если $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{P}^{\langle n\rangle}$ и для любой функции f из $\mathcal{B}_1$ существует функция g из $\mathcal{B}_2$, такая что $[\rho_1, \rho_2](f, g) \leqslant (a_1, a_2)$, то будем писать

$$[\rho_1, \rho_2](\mathcal{B}_1, \mathcal{B}_2) \leqslant (a_1, a_2).$$

Через $\mathcal{A}_*$ обозначим класс функций, которые представимы в виде $f_1 \,\&\, f_2$ или $f_1 \vee f_2$, где $f_1, f_2 \in \mathcal{A}$.

Лемма 2.1 [15]. *Если $f \in \mathcal{P}^{\langle n\rangle}$, $\mathcal{A} \subseteq \mathcal{P}^{\langle n\rangle}$, $L_{\mathcal{A}}(f) \geqslant 1$ и для монотонных псевдометрик ρ_1, ρ_2 выполнено*

$$[\rho_1, \rho_2](\mathcal{A}_*, \mathcal{A}) \leqslant (a_1, a_2), \quad a_1, a_2 > 0,$$

то существует функция g из $\mathcal{P}^{\langle n\rangle}$, такая что

$$L_{\mathcal{A}}(g) \leqslant L_{\mathcal{A}}(f) - 1, \quad \rho_1(0, g) \geqslant \rho_1(0, f) - a_1, \quad \rho_2(1, g) \geqslant \rho_2(1, f) - a_2.$$

Теорема 2.1 [15]. *Если $f \in \mathcal{P}^{\langle n\rangle}$, $\mathcal{A} \subseteq \mathcal{P}^{\langle n\rangle}$, $L_{\mathcal{A}}(f) \geqslant 0$ и для монотонных псевдометрик ρ_1, ρ_2 выполнено*

$$[\rho_1, \rho_2](\mathcal{A}_*, \mathcal{A}) \leqslant (a_1, a_2), \quad a_1, a_2 > 0,$$

то

$$L_{\mathcal{A}}(f) \geqslant \min\left(\frac{\rho_1(0, f)}{a_1}, \frac{\rho_2(1, f) - \rho_2(1, \mathcal{A} \setminus \{0\})}{a_2}\right).$$

2.2. Лемма о системе конечных множеств

Лемма 2.2 [15]. *Если $\mathcal{R}$ — система непустых попарно невложимых множеств мощности не более s и*

$$|\mathcal{R}| \geqslant (r-1)^s + 1, \quad r \geqslant 2, \quad s \geqslant 1,$$

то существуют такие различные множества $V_1, V_2, \ldots, V_r$ из $\mathcal{R}$ и множество V_0 (быть может, пустое), что $V_0 \subseteq V_1 \wedge V_2$ и множества $V_1 \setminus V_0, \ldots, V_r \setminus V_0$ попарно не пересекаются.

2.3. Аппроксимация функций из некоторых специальных классов

Пусть W — непустое конечное множество и $\mathcal{F}$ — отображение, которое каждому подмножеству w множества W ставит в соответствие некоторое подмножество $\mathcal{F}(w)$ множества переменных $U_n = \{u_1, u_2, \ldots, u_n\}$, причём

$$\mathcal{F}(\varnothing) = \varnothing, \quad \mathcal{F}(W) = U_n,$$
$$\mathcal{F}(w_1) \cup \mathcal{F}(w_2) = \mathcal{F}(w_1 \cup w_2), \quad \mathcal{F}(w_1) \cap \mathcal{F}(w_2) = \mathcal{F}(w_1 \cap w_2).$$

Через $\mathcal{K}_w^{\mathcal{F}}$ обозначим конъюнкцию всех переменных из $\mathcal{F}(w)$, а если $w = \varnothing$, то $\mathcal{K}_w^{\mathcal{F}} = 1$. Пусть E^n — n-мерный бинарный куб. Через $\tilde{\alpha}_w^{\mathcal{F}}$ обозначим такой набор из E^n, в котором единичными являются все компоненты, соответствующие переменным из $\mathcal{F}(w)$, а остальные компоненты нулевые.

Через M обозначим множество всех монотонных функций алгебры логики, а через $M(\mathcal{F})$ — множество таких функций f из $M^{\langle n\rangle}$, что либо f — константа, либо любая её простая импликанта есть $\mathcal{K}_w^{\mathcal{F}}$ для некоторого $w \subseteq W$.

Если $f \in M^{\langle n\rangle}$, то множество $w \subseteq W$ называется простым для f, если не существует такого w_1, что $w_1 \subset w$ и $\mathcal{K}_{w_1}^{\mathcal{F}}$ — импликанта f, однако $\mathcal{K}_w^{\mathcal{F}}$ является импликантой f. Через $\sum\limits_f^{\mathcal{F}}$ обозначаем систему всех простых для f множеств. Ясно, что для всех функций f из $M(\mathcal{F})$ верно, что

$$f = \bigvee_{w \in \sum_f^{\mathcal{F}}} \mathcal{K}_w^{\mathcal{F}}$$

(пустая дизъюнкция считается равной 0).

Через $l_s^{\mathcal{F}}$ обозначим число непустых множеств из $\sum\limits_f^{\mathcal{F}}$ мощности не более s, а через $R^{\mathcal{F}}(f)$, где $f \in M^{\langle n\rangle}$, — максимальную мощность множеств из $\sum\limits_f^{\mathcal{F}}$. Полагаем $R^{\mathcal{F}}(0) = 0$.

Через $M(\mathcal{F}, w, k, r)$ обозначим множество всех таких функций f из $M(\mathcal{F})$, что все множества из $\sum\limits_f^{\mathcal{F}}$ содержат w и выполнены неравенства

$$R^{\mathcal{F}}(f) \leqslant |w| + k, \quad l_{|w|+s}^{\mathcal{F}} \leqslant (r-1)^s, \quad s = 1, 2, \ldots, k.$$

Полагаем

$$M(\mathcal{F}, w, k) = \bigcup_{i=1}^{\infty} M(\mathcal{F}, w, k, i), \quad M(\mathcal{F}, w) = \bigcup_{k=1}^{\infty} M(\mathcal{F}, w, k).$$

Через $l(f)$ обозначим число простых импликант f, а через $R(f)$ их максимальную длину. Через $Б_{r,k}$ обозначаем множество всех бесповторных функций f из M, таких что

$$l(f) = r, \quad 1 \leqslant R(f) \leqslant k.$$

Здесь функцию f мы называем бесповторной, если её простые импликанты не имеют общих переменных. Полагаем

$$t(\mathcal{F}, k) = \max_{\substack{w_1 \subseteq w_2 \subseteq W, \\ |w_1| \leqslant k,\ |w_2| \leqslant |w_1| + k}} |\mathcal{F}(w_2) \setminus \mathcal{F}(w_1)|, \quad Б_{r,k}^{\mathcal{F}} = Б_{r,t(\mathcal{F},k)}^{\langle n\rangle}.$$

Лемма 2.3 [15]. *Если ρ — монотонная псевдометрика на $M^{\langle n\rangle}$, $|w| \leqslant k$, $r \geqslant 2$, то для любой функции f из $M(\mathcal{F}, w, k) \setminus M(\mathcal{F}, w, k, r)$ существует такая функция g из $M(\mathcal{F}, w, k)$, что*

$$g \geqslant f, \quad l(g) \leqslant l(f) - 1, \quad \rho(f, g) \leqslant \rho(1, Б_{r,k}).$$

Лемма 2.4 [15]. *Если ρ — монотонная псевдометрика на $M^{\langle n\rangle}$, $|w| \leqslant k$, $r \geqslant 2$, то для любой функции f из $M(\mathcal{F}, w, k) \setminus M(\mathcal{F}, w, k, r)$ существует такая функция g из $M(\mathcal{F}, w, k, r)$, что*

$$g \geqslant f, \quad \rho(f, g) \leqslant l(f) * \rho(1, Б_{r,k}).$$

Псевдометрика ρ на $M^{\langle n\rangle}$ называется $\mathcal{F}$-правильной, если $\rho(f_1,f_2)=0$, как только для всех w, содержащихся в W, выполнено равенство

$$f_1(\tilde{\alpha}_w^{\mathcal{F}})=f_2(\tilde{\alpha}_w^{\mathcal{F}}).$$

Полагаем

$$\mathfrak{M}(\mathcal{F},k,r)=M(\mathcal{F},\varnothing,k,r),\quad \mathfrak{M}(\mathcal{F},k)=M(\mathcal{F},\varnothing,k),$$
$$\mathcal{Э}(\mathcal{F},s)=\{\mathcal{K}_w^{\mathcal{F}}\mid w\subseteq W,\ |w|=s\}.$$

Лемма 2.5 [15]. *Если ρ_1, ρ_2 — монотонные псевдометрики на $M^{\langle n\rangle}$, псевдометрика ρ_1 $\mathcal{F}$-правильная, $r\geqslant 2$, $k\geqslant 1$, то*

$$[\rho_1,\rho_2]\big(\mathfrak{M}(\mathcal{F},k,r)_*,\mathfrak{M}(\mathcal{F},k,r)\big)\leqslant(a_1,a_2),$$

где

$$a_1=\sum_{s=k+1}^{2k}s\cdot(r-1)^s\cdot\rho_1\big(0,\mathcal{Э}(\mathcal{F},s)\big),\quad a_2=2k\cdot(r-1)^{2k}\cdot\rho_2(1,Б_{r,k}^{\mathcal{F}}).$$

Теорема 2.2 [15]. *Если ρ_1, ρ_2 — монотонные псевдометрики на $M^{\langle n\rangle}$, псевдометрика ρ_1 $\mathcal{F}$-правильная, $f\in M^{\langle n\rangle}$, $r\geqslant 2$, $|W|\geqslant k\geqslant 1$, $L_{\mathcal{A}}\geqslant 0$, то для любого $\alpha>0$*

$$L_{\mathcal{A}}\geqslant\left(\frac{\rho_1(0,f)}{a_1},\frac{\rho_2(1,f)-\rho_2(1,\mathcal{Э}(\mathcal{F},k))}{a_2}\right),$$

где

$$a_1=\alpha+\sum_{s=k+1}^{2k}s\cdot(r-1)^s\cdot\rho_1\big(0,\mathcal{Э}(\mathcal{F},s)\big),\quad a_2=\alpha+2k\cdot(r-1)^{2k}\cdot\rho_2(1,Б_{r,k}^{\mathcal{F}}),$$
$$\mathcal{A}=\mathfrak{M}(\mathcal{F},k,r).$$

2.4. Оценки в случае специальных псевдометрик

Полагаем, что $\lambda_s^{\mathcal{F}}(f)$ — минимально возможное число множеств из $\Sigma_f^{\mathcal{F}}$, пересечение которых содержит не менее s элементов. Через $R^*(f)$ обозначаем минимальную длину импликант f. Полагаем

$$\beta(\mathcal{F},k)=\max_{\substack{w\subseteq W,\\ |w|=k}}|\mathcal{F}(w)|.$$

Теорема 2.3 [15]. *Если $p\in(0,1)$, $|W|\geqslant k\geqslant 1$, $r\geqslant 2$, $f\in M(\mathcal{F})$, $L_{\mathcal{A}}(f)\leqslant 0$, $\lambda_{k+1}^{\mathcal{F}}(f)\geqslant 1$, $t(\mathcal{F},k)\geqslant 1$, $\mathcal{A}=\mathfrak{M}(\mathcal{F},k,r)$, то*

$$L_{\mathcal{A}}(f)\geqslant\min\left(\frac{l(f)}{\sum\limits_{s=k+1}^{2k}s(r-1)^s\lambda_s^{\mathcal{F}}(f)},\frac{1-l(f)e^{-pR^*(f)}-p\beta(\mathcal{F},k)}{2k(r-1)^{2k}(pt(\mathcal{F},k))^r}\right).$$

Через $\lambda_s(f)$ обозначим максимально возможное число простых импликант f, имеющих не менее s общих переменных.

Теорема 2.4 [15]. *Если* $p \in (0,1)$, $k \geqslant 1$, $r \geqslant 2$, $f \in M^{\langle n \rangle}$, $R^*(f) \geqslant k+1$, $\text{Б} = \{\&, \vee, 0, 1\}$, *то*

$$L_{\text{Б}}(f) \geqslant \min\left(\frac{l(f)}{\sum\limits_{s=k+1}^{2k} s(r-1)^s \lambda_s(f)}, \frac{1 - l(f)e^{-pR^*(f)} - pk}{2k(r-1)^{2k}(pk)^r}\right).$$

2.5. Примеры сложнореализуемых монотонных функций

Через A^k обозначаем декартово произведение k экземпляров множества A.

Пусть $\mathrm{GF}(q)$ — поле Галуа порядка q, а $p(x) = x^2 + c_1 x + c_2$, $c_1, c_2 \in \mathrm{GF}(q)$, — неприводимый над $\mathrm{GF}(q)$ многочлен. Рассмотрим расширение $\mathrm{GF}(q)$, порождаемое присоединением корней $p(x)$. В этом случае операции на $\mathrm{GF}(q)^2 = \mathrm{GF}(q) \times \mathrm{GF}(q)$ определяются следующим образом:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$
$$(a_1, a_2) * (b_1, b_2) = (a_1 b_1 - c_2 a_2 b_2, a_1 b_2 + a_2 b_1 - c_1 a_2 b_2).$$

Данное расширение является, как известно, полем Галуа $\mathrm{GF}(q^2)$. При этом множество всех пар вида $(a, 0)$ образует подполе $\mathrm{GF}(q)$ и выполнены соотношения

$$(a, 0) * (a_1, b_1) = (a * a_1, a * b_1) = a * (a_1, b_1).$$

Рассмотрим следующую систему функций на $\mathrm{GF}(q)^2$ со значениями в $\mathrm{GF}(q)$:

$$\varphi_0(x, y), \quad \varphi_1(x, y) = x, \quad \varphi_2(x, y) = y,$$
$$\big(\varphi_{2k+1}(x, y), \varphi_{2k+2}(x, y)\big) = \big(\varphi_{2k-1}(x, y), \varphi_{2k}(x, y)\big) * (x, y), \quad k \geqslant 1.$$

Пусть $n = q^3$ и

$$\{x_{a,b,d} \mid a, b, d \in \mathrm{GF}(q)\} = U_n = \{u_1, u_2, \ldots, u_n\},$$

т. е. мы индексировали тройками из $\mathrm{GF}(q)^3$ все переменные из U_n. Полагаем

$$d(\tilde{\alpha}, a, b) = \bigoplus_{i=0}^{2m} \alpha_i \varphi_i(a, b), \quad \tilde{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_{2m}) \in \mathrm{GF}(q)^{2m+1}, \quad a, b \in \mathrm{GF}(q),$$

$$\mathcal{K}_{\tilde{\alpha}} = \bigwedge_{a,b \in \mathrm{GF}(q)} x_{a,b,d(\tilde{\alpha},a,b)}, \quad g_{n,m}(u_1, u_2, \ldots, u_n) = \bigvee_{\tilde{\alpha} \in \mathrm{GF}(q)^{2m+1}} \mathcal{K}_{\tilde{\alpha}}.$$

Следствие 2.1 [15]. *Если* m *чётное,*

$$2 \leqslant m \leqslant \frac{n^{1/3}}{8 \ln n^{1/3}},$$

то для любого полного монотонного базиса Б *выполнено неравенство*

$$L_{\text{Б}}(g_{n,m}) \geqslant C_{\text{Б}} \frac{2^{m/2}}{m},$$

где $C_{\text{Б}}$ *— константа, зависящая только от базиса.*

Максимальный рост этих оценок достигается при

$$m = 2\left[\frac{n^{1/3}}{16 \ln n^{1/3}}\right].$$

В этом случае

$$L_{\text{Б}}(g_{n,m}) \geqslant 2^{n^{1/3-o(1)}}.$$

Пусть μ, t, n_0 — натуральные числа, $2 \leqslant \mu \leqslant t \leqslant n_0$, $n = \binom{n_0}{t}$. Пусть W — некоторое множество мощности n_0, $w_1, w_2, \ldots, w_n$ — все его подмножества мощности μ. Если $w \subseteq W$, $i \in \{1, 2, \ldots, n\}$, то полагаем, что

$$u_i \in \mathcal{F} \iff w_i \subseteq W.$$

Полагаем

$$f_t^{n,\mu}(u_1, u_2, \ldots, u_n) = \bigvee_{w \subseteq W,\ |w|=t}.$$

Эти функции называем μ-симметрическими.

Следствие 2.2 [15]. *Если* $\mu \geqslant 2$ *и*

$$t = \left[n^{\frac{1}{2\mu-1}}\right],$$

то для любого полного монотонного базиса Б *выполнено неравенство*

$$L_{\text{Б}}(f_t^{n,\mu}) \geqslant 2^{n^{\frac{\mu-1}{\mu(2\mu-1)}-o(1)}}.$$

3. Сложность схемных алгоритмов

При проектировании управляющих систем одной из основных задач является минимизация их параметров, обусловливающих стоимость, размеры и материалоёмкость. Пусть, например, перед конструктором стоит задача разработки блока ЭВМ для умножения чисел, заданных в двоичной записи. В целях обеспечения быстродействия и надёжности желательно, чтобы этот блок состоял из одной микросхемы. Однако число транзисторов и других функциональных узлов, которое можно разместить на одном кристалле, ограничено по причинам технологического и физического характера. Кроме того, производство микросхем с меньшим числом функциональных узлов обходится дешевле. Поэтому разработчик блока стремится уменьшить число транзисторов и других элементов в проектируемой схеме для умножения чисел. В процессе изучения модельных задач описанного типа и сформировалась теория сложности булевых функций — один из основных разделов математической кибернетики.

Основная задача этой теории состоит в следующем. Задано множество схем $\mathcal{U}$ и оператор $\mathcal{F}$, ставящий в соответствие каждой схеме $u \in \mathcal{U}$ реализуемую ею булеву функцию $\mathcal{F}(u)$ (или оператор). В приведённом примере $\mathcal{U}$ — это множество микросхем, а $\mathcal{F}(u)$ — преобразование входных наборов импульсов в выходные, осуществляемое микросхемой u. Задан неотрицательный определённый на $\mathcal{U}$ функционал $L_{\mathcal{U}}$ сложности схем. Это может быть, например, число транзисторов в микросхеме или площадь кристалла, на котором она расположена. Схема u реализует функцию f (или оператор), если $f = \mathcal{F}(u)$. Требуется для каждой функции (оператора) f найти реализующую её схему u минимально возможной сложности $L_{\mathcal{U}}(u)$. Эта сложность обозначается через $L_{\mathcal{U}}(f)$ и называется сложностью реализации f, схема u называется минимальной. Эта задача называется задачей синтеза. Обычно для каждой функции f легко выделить конечное подмножество схем, в котором содержится минимальная схема, реализующая f. Поэтому задача нахождения последней может быть решена перебором схем из этого подмножества.

Однако уже при относительно небольшом числе переменных у функции этот перебор оказывается, как правило, неосуществимым в обозримое время. Например, для реализации умножения 100-разрядных чисел достаточно в силу известного алгоритма умножения столбиком нескольких десятков тысяч транзисторов и других элементов. Однако перебрать все микросхемы, состоящие не более чем из такого числа элементов, чтобы найти среди них минимальную схему для умножения, не представляется реальным.

В связи с этими трудностями в 1949 г. К. Э. Шенноном [111] был предложен подход, заключающийся в следующем видоизменении задачи синтеза. Полагаем, что

$$L_{\mathcal{U}}(n) = \max_{f} L_{\mathcal{U}}(f),$$

где максимум берётся по всем функциям от n переменных. Функция $L_{\mathcal{U}}(n)$ в настоящее время она называется функцией Шеннона. Требуется получить для неё возможно лучшие оценки и предложить метод синтеза, т. е. построения по каждой функции от n переменных реализующей её схемы, сложность которой близка к $L_{\mathcal{U}}(n)$.

В упомянутой работе К. Э. Шенноном был найден порядок функции $L_{\mathcal{U}}(n)$ в случае контактных схем и предложен оптимальный по порядку, в указанном выше смысле, метод синтеза контактных схем.

Асимптотически оптимальные методы синтеза были разработаны О. Б. Лупановым [47, 50]. В этих работах получена и асимптотика функции Шеннона для многих классов управляющих систем. Из результатов О. Б. Лупанова вытекает, что почти все булевы функции от данного числа переменных являются асимптотически самыми сложными, причём эта сложность очень велика. Так, например, в случае умножения 100-разрядных чисел шенноновская оценка составляет примерно 2^{200} элементов.

Возникает задача выделения классов функций, допускающих относительно простую реализацию, и разработки асимптотически оптимальных методов

синтеза схем для функций из этих классов, т. е. если задан класс $\mathfrak{A}$ булевых функций, то требуется для каждой функции из $\mathfrak{A}^{\langle n\rangle}$ (где $\mathfrak{A}^{\langle n\rangle}$ — множество функций из $\mathfrak{A}$, зависящих от первых n переменных) построить реализующую её схему, близкую по сложности к

$$L_{\mathcal{U}}(\mathfrak{A}^{\langle n\rangle}) = \max_{f\in\mathfrak{A}^{\langle n\rangle}} L_{\mathcal{U}}(f).$$

Последняя величина называется функцией Шеннона для сложности реализации функций из класса $\mathfrak{A}$.

Впервые этот вопрос был рассмотрен в упомянутой выше работе К. Э. Шеннона. Первый результат общего характера принадлежит С. В. Яблонскому [94, 96], который построил и изучил, в том числе с точки зрения сложности реализации, континуальное семейство классов булевых функций, инвариантных относительно переименования переменных и подстановок констант.

Общий подход, позволяющий решить эту задачу для очень многих классов булевых функций, — принцип локального кодирования — был предложен О. Б. Лупановым [51, 55]. Этот метод особенно удобен при синтезе схем из функциональных элементов и других типов управляющих систем, допускающих многократное использование результатов промежуточных вычислений.

В процессе производства и функционирования в реальных управляющих системах могут возникать различного рода неисправности. Если при этом изменяется функция, реализуемая устройством, то его дальнейшее использование может оказаться недопустимым. Например, при изготовлении микросхем, вследствие технологических дефектов, отдельные транзисторы могут превращаться в участки, всегда проводящие или не проводящие ток. Вследствие этого при подаче чисел на вход микросхемы для умножения на выходе вместо произведения этих чисел может возникнуть совсем другой код сигнала. В связи с этим С. В. Яблонским в [72] была поставлена задача синтеза самокорректирующихся схем, т. е. построения для каждой булевой функции f такой схемы, реализующей её, что в любом неисправном состоянии из заданного класса она также реализует f. При этом наибольший интерес представляет выяснение условий для классов, корректирование неисправностей из которых не приводит к увеличению асимптотики функции Шеннона.

Первый результат в этом направлении был получен С. В. Яблонским и Ю. Г. Потаповым в упомянутой выше работе, где была доказана возможность асимптотически неизбыточного корректирования одного замыкания контакта для контактных схем. Аналогичный результат для размыканий впоследствии был получен Х. А. Мадатяном [57]. Наиболее глубокие результаты были достигнуты Э. И. Нечипоруком [64—66, 69], который разработал метод асимптотически неизбыточного корректирования растущего числа обрывов в вентильных схемах. На его основе он установил возможность асимптотически неизбыточного корректирования растущего числа размыканий ($o(\frac{\log n}{\log\log n})$, где n — число переменных) в контактных схемах, а также одновременно растущего числа размыканий

и замыканий в контактно-вентильных и π-схемах. Возможность асимптотически неизбыточного корректирования одновременно растущего числа размыканий ($o(\frac{\log n}{\log\log n})$) и замыканий ($o(\frac{n}{\log n})$) в контактных схемах была затем установлена Н. П. Редькиным [75, 76]. Д. Улигом [86] было показано, что при увеличении асимптотики функции Шеннона не более чем в два раза в контактных схемах возможно одновременное корректирование $2^{o(\frac{n}{\log n})}$ замыканий и размыканий.

Вопросы самокорректирования рассматривались и для схем из функциональных элементов (см. [37, 38, 71, 85]), однако в этом случае возникает необходимость использования абсолютно надёжных элементов.

Основными модельными управляющими системами в теории сложности булевых функций являются схемы из функциональных элементов, контактные схемы и формулы. Схемы из функциональных элементов допускают многократное использование результатов промежуточных вычислений, формулы не допускают, а контактные схемы в этом отношении занимают промежуточное положение.

Методы синтеза, возникшие в теории сложности булевых функций, в большей или меньшей степени ориентированы на конкретные типы управляющих систем. Между функционалами сложности реализации булевых функций различными типами управляющих систем к настоящему времени явных связей (в нетривиальных случаях) не установлено. Более того, перенесение конструкций, дающих хорошие результаты для одного типа управляющих систем, на другие типы часто весьма затруднительно или вообще не представляется возможным. Об этом, в частности, свидетельствует наличие большого числа классов булевых функций, для которых с помощью принципа локального кодирования построены асимптотически оптимальные методы синтеза схем из функциональных элементов, однако в случаях контактных схем и формул аналогичные методы неизвестны, причём эта ситуация является характерной. Это замечание относится и к методам синтеза асимптотически неизбыточных самокорректирующихся схем. Здесь погружение в специфику конкретных типов управляющих систем часто столь велико, что остаётся неясным, можно ли ожидать эффекта асимптотически неизбыточного корректирования нетривиальных классов неисправностей для новых типов управляющих систем, которые, возможно, ещё возникнут.

Поэтому особую актуальность приобретает разработка методов синтеза, инвариантных относительно конкретных типов управляющих систем, и выявление внутренних сложностных свойств булевых функций, обусловливающих поведение функционалов сложности реализации булевых функций различными типами управляющих систем.

Важно разрабатывать универсальные по отношению к типу управляющих систем асимптотически оптимальные методы синтеза схем для функций из специальных классов асимптотически неизбыточных самокорректирующихся схем.

Исследования, результаты которые здесь излагаются, были проведены А. Е. Андреевым [13].

Разработка этих вопросов привела к необходимости

- фактического выхода за пределы двузначной логики, а именно рассмотрения недоопределённых булевых функций, которые понимаются как принимающие на наборах из нулей и единиц три значения: 0, 1 и $*$ в точках их неопределённости;
- введения новых функционалов сложности булевых функций, порождаемых объектами, называемых функциональными сетями, промежуточными по своей природе между булевыми функциями и управляющими системами, а именно разложениями булевых функций в специальных классах операций (при этом компонентами разложений являются частичные функции).

Функциональные сети становятся основным объектом изучения. Функциональная сеть реализует частичную булеву функцию, если она является разложением некоторого доопределения этой функции (функция f — доопределение g, если f и g совпадают в тех точках, где g определена). Сложность функциональной сети определяется исходя из сложности порождающей операции и числа наборов, на которых определены компоненты (рассматриваются и другие характеризации сложности компонент). При этом сложность операции учитывается с очень большим весом (растущим с ростом числа задействованных переменных). Вес компонент растёт с уменьшением мощности области определения. Затем по обычной схеме определяется сложность реализации функции как минимум сложности по всем реализующим её функциональным сетям и функция Шеннона для класса $\mathfrak{A}$ как максимальная сложность функций из $\mathfrak{A}^{\langle n\rangle}$. В качестве неисправностей функциональных сетей рассматриваются замещения компонент — либо произвольные, либо на нули и единицы. Классы неисправностей описываются ограничениями на допустимое число замещений.

Для решения проблемы создания универсальных методов синтеза схем было предложено разрабатывать асимптотически оптимальные методы синтеза функциональных сетей. Правомерность этого подхода обусловлена тем обстоятельством, что из асимптотически оптимальной функциональной сети посредством относительно несложных однотипных перестроек можно получить асимптотически оптимальные схемы для многих типов управлявших систем. Эта перестройка называется моделированием. Чтобы её осуществить, надо реализовать компоненты функциональной сети с помощью методом синтеза схем, асимптотически оптимального для класса частичных функций с данной величиной области определения. Затем из полученных блоков в соответствии с операцией, порождающей функциональную сеть, собирается схема. Асимптотическая оптимальность получаемых таким образом схем обеспечивается упомянутым выше определением сложности функциональных сетей. При этом самокорректирующаяся функциональная сеть порождает самокорректирующиеся схемы, и при реализации компонент не надо требовать самокорректирования, поскольку оно обеспечивается лишь структурой порождающей операции.

Для описанного моделирования функциональных сетей необходимо располагать асимптотически оптимальными методами синтеза схем для функций

с данной величиной области определения при достаточно общих предположениях о её росте в зависимости от числа переменных. Для некоторых типов управляющих систем такие методы были разработаны ранее, для других вновь найдены.

Моделирование функциональных сетей с порождающими операциями из заданного класса может быть осуществлено, если выразительные средства рассматриваемого типа управляющих систем в определённом смысле включают этот класс операций. Поэтому степень универсальности методов синтеза функциональных сетей по отношению к типам управляющих систем определяется тем, насколько узким является рассматриваемый класс операций.

Изучаются в основном два класса операций: бесповторные и топологические. Операции из первого класса задаются двухполюсными параллельно-последовательными неориентированными сетями, а из второго — неориентированными сетями без ограничений на топологию и число полюсов.

Бесповторные операции моделируются почти всеми известными нетривиальными типами управляющих систем. Класс топологических операции является расширением класса бесповторных операций, поэтому множество типов управляющих систем, моделирующих топологические операции, сужается по сравнению с бесповторными, оставаясь тем не менее достаточно широким. В классе бесповторных функциональных сетей возможна лишь реализация функций, топологические же сети допускают и реализацию операторов.

А. Е. Андреевым найдены асимптотически оптимальные методы синтеза бесповторных функциональных сетей для следующих семейств классов булевых функции:

- частичных функций с данной величиной области определения;
- функций с данным числом единиц;
- функций с ограниченной энтропией;
- ненулевых инвариантных классов С. В. Яблонского;
- классов Поста, не содержащихся в D_3, L_1, S_6 и P_6 (обозначения из [97]).

Основным результатом относительно топологических функциональных сетей является теорема о дублях. В процессе доказательства этой теоремы А. Е. Андреевым был предложен метод одновременной реализации многих экземпляров частичной функции и её отрицания со сложностью, асимптотически не превосходящей сложности самой функции (т. е. величины её области определения). Теорема о дублях позволяет переносить на топологические функциональные сети многие конструкции принципа локального кодирования О. Б. Лупанова. Эта возможность иллюстрируется на примерах следующих классов операторов:

- ненулевых инвариантных классах операторов;
- классе монотонных в арифметическом смысле операторов;
- классах операторов, вычисляющих значения функций на нескольких последовательных наборах.

Вопросы самокорректирования рассматривались также для бесповторных и топологических функциональных сетей. Для обоих классов операций разработаны методы преобразования обычных функциональных сетей в самокорректирующиеся. При этих преобразованиях сложность в определённом смысле асимптотически не увеличивается. Эти результаты позволили установить возможность синтеза корректирующих достаточно широкие классы неисправностей асимптотически неизбыточных функциональных сетей для функций и операторов из специальных классов при весьма общих предположениях о последних. Этим условиям удовлетворяют, в частности, перечисленные выше классы.

Как уже отмечалось, методы синтеза функциональных сетей из рассматриваемых классов являются универсальными по отношению ко многим типам управляющих систем. Для бесповторных сетей этот список включает, например, следующие:

- формулы;
- контактные π-схемы;
- бинарные программы без вычислительных команд;
- контактные схемы;
- контактно-вентильные схемы;
- релейно-контактные схемы;
- схемы из функциональных элементов;
- формулы с частичной памятью;
- схемы из многовыходных функциональных элементов;
- автоматы;
- бинарные программы общего вида.

В случае топологических сетей этот список сохраняется за исключением первых трёх пунктов.

Моделирование функциональных сетей рассматривалось на примерах контактных схем и формул. При этом в качестве следствий из основных результатов получены, в частности, асимптотики для сложности реализации функций из перечисленных выше классов самокорректирующимися контактными схемами и формулами и реализации операторов самокорректирующимися контактными схемами. Для большинства этих классов ранее не были известны асимптотики функции Шеннона даже в случаях обычных контактных схем и формул. Полученные оценки допустимого числа асимптотически неизбыточно корректируемых неисправностей существенно выше, чем ранее известные. Так, в случае класса всех булевых функций установлена возможность асимптотически неизбыточного корректирования:

- для контактных схем $2^{o(n)}$ произвольных неисправностей контактов, где n — число переменных,
- для формул $2^{o(\sqrt{\frac{n}{\log n}})}$ произвольных неисправностей ненадёжных элементов.

Развитые методы синтеза могут быть использованы при проектировании сложных управляющих систем. Они также могут быть полезны при создании систем автоматического проектирования, например микросхем. Универсальность разработанных методов делает сферу их возможного применения более широкой по сравнению с ранее известными методами синтеза конкретных типов управляющих систем.

Формализуем изложенное. Пусть P — множество всех частичных функций алгебры логики и $\mathfrak{M}$ — множество операций на P. Если операция $\mathcal{F}$ из $\mathfrak{M}$ применима к набору $(f_1, f_2, \ldots, f_k)$ функций из P, где k — арность этой операции, то выражение

$$\mathcal{F}(f_1, f_2, \ldots, f_k)$$

называется функциональной сетью. Через $[S]$ обозначим функцию (оператор), разложением которой является функциональная сеть S, т. е. $[S]$ — это результат применения порождающей операции к набору функций, перечисленных в скобках.

Пусть

$$S = \mathcal{F}(f_1, f_2, \ldots, f_k).$$

Функциональная сеть S реализует функцию f (оператор), если

$$f \preccurlyeq [S],$$

где $f \preccurlyeq g$, если g есть доопределение f. Сеть S корректирует ξ неисправностей (a единичных и b нулевых),

$$f \overset{\xi}{\preccurlyeq} [S] \quad (f \overset{(a,b)}{\preccurlyeq} [S]),$$

если любая функциональная сеть, которую можно получить из S произвольной заменой не более ξ функций в наборе $(f_1, f_2, \ldots, f_k)$ (заменой не более a функций на тождественную единицу и одновременно не более b функций — на тождественный ноль), также реализует f.

Считается, что обозначения $\preccurlyeq$ и $\overset{\varnothing}{\preccurlyeq}$ совпадают, а выражения $f \overset{\triangle}{\preccurlyeq} [S]$ и $f \overset{\triangle}{\preccurlyeq} S$, $\triangle \in \{\varnothing, \xi, (a,b)\}$, означают одно и то же.

Рассмотрим три класса операций:

- ***СЛ*** — слабые логические;
- ***Т*** — топологические;
- ***П*** — бесповторные.

Операция из класса ***СЛ*** задаётся ориентированным ациклическим графом. В графе выделены вершины, называемые полюсами, они занумерованы числами $1, 2, \ldots, k$, где k — число полюсов. В полюса рёбра не входят, а во все остальные вершины входят ровно по два ребра. Каждая вершина, не являющаяся полюсом, помечена либо символом $\&$, либо $\vee$. Выделены выходные вершины, они занумерованы числами $1, 2, \ldots, S$, где S — их число. Операция $\mathcal{F}$, задаваемая такой логической сетью, имеет арность k, и её результатом является S-компонентный оператор $[\mathcal{F}(f_1, f_2, \ldots, f_k)]$, определяемый следующим образом. Пусть

функции $f_1, f_2, \ldots, f_k$ полностью определённые. Полюсу с номером i приписываем функцию f_i, $i = 1, 2, \ldots, k$, а каждой вершине, не являющейся полюсом, приписываем функции так, что функция, приписанная данной вершине, является конъюнкцией или дизъюнкцией (в соответствии с тем символом $\&$ или $\vee$, которым помечена вершина) функций, приписанных вершинам, из которых в данную входят ребра. Компонентами оператора $[\mathcal{F}(f_1, f_2, \ldots, f_k)]$ являются функции, приписанные выходным вершинам в соответствии с нумерацией последних. В общем случае для определения оператора $[\mathcal{F}(f_1, f_2, \ldots, f_k)]$ рассматриваются всевозможные наборы $g_1, g_2, \ldots, g_k$, где g_i — полное доопределение f_i, зависящее от тех же переменных. Если на данном наборе значений переменных в i-й выходной вершине при любом таком полном доопределении реализуется одно и то же значение, то оно является значением i-й компоненты результата операции на данном наборе значений переменных, в противном случае это значение равно $*$.

Операция из класса $\boldsymbol{T}$ задаётся сетью — конечным неориентированным графом без петель (кратные рёбра допустимы) с выделенными вершинами, которые называются полюсами. Рёбра графов занумерованы натуральными числами от 1 до k, где k — число рёбер, а полюса — натуральными числами от 1 до p, где p — число полюсов. Арность операции — k, операция применима к любому набору из k функций. Её результат при применении к набору $(f_1, f_2, \ldots, f_k)$ — оператор с C_p^2 компонентами. Ребру с номером i приписывается функция f_i. Компонента результата с номером $C_{j-1}^2 + i$, $1 \leqslant i < j \leqslant p$, определяется следующим образом. На данном наборе значений переменных она равна 0, если нет цепей между i-м и j-м полюсами или в любой цепи между ними существует ребро, помеченное функцией, обращающейся на выбранном наборе значений переменных в 0; равна 1, если существует такая цепь между рассматриваемыми полюсами, что все приписанные её рёбрам функции обращаются на выделенном наборе переменных в 1; в остальных случаях значение равно $*$.

Пусть $\boldsymbol{П}$ — подкласс класса $\boldsymbol{T}$, соответствующий двухполюсным параллельно-последовательным сетям. Он совпадает с подклассом класса $\boldsymbol{СЛ}$, порождаемым бесповторными (т. е. древовидными) логическими сетями. Ясно, что

$$\boldsymbol{П} \subset \boldsymbol{T} \subset \boldsymbol{СЛ}.$$

Полагаем, что $L_{\boldsymbol{СЛ}}(\mathcal{F})$ — наименьшее возможное число вершин в логической сети, задающей операцию $\mathcal{F}$ из $\boldsymbol{СЛ}$. Функционалы $L_{\boldsymbol{T}}$ и $L_{\boldsymbol{П}}$ являются ограничениями функционала $L_{\boldsymbol{СЛ}}$ на множества операций $\boldsymbol{T}$ и соответственно $\boldsymbol{П}$.

Функционалы сложности функциональных сетей задаются:

- классом $\mathfrak{M}$;
- функционалом $L_{\mathfrak{M}}$ сложности операций;
- неотрицательным функционалом Φ на P, характеризующим априорную сложность компонент;
- нормировочной функцией $\boldsymbol{Ш}$, определённой, неотрицательной, монотонной и неограниченной на $[0, \infty)$;

- весовой функцией операции φ, определённой, неотрицательной на $[0,\infty)$, удовлетворяющей условию $\varphi(a)\to\infty$ при $a\to\infty$.

Набор

$$\sigma=\langle\mathfrak{M},L_{\mathfrak{M}},\Phi,\boldsymbol{Ш}\rangle$$

называется сигнатурой. Для функциональной сети

$$S=\mathcal{F}(f_1,f_2,\ldots,f_k),\quad \mathcal{F}\in\mathfrak{M},$$

полагаем

$$L_{\sigma,\varphi}(S)=\boldsymbol{Ш}^{-1}\biggl(\varphi(n)L_{\mathfrak{M}}(\mathcal{F})+\sum_{i=1}^{k}\boldsymbol{Ш}\bigl(\Phi(f_i)\bigr)\biggr),$$

где n — число переменных, задействованных в функциональной сети S, и

$$\boldsymbol{Ш}^{-1}(a)=\sup\{b\mid\boldsymbol{Ш}(b)\leqslant a\}.$$

Определённая величина называется сложностью функциональной сети S в сигнатуре σ с весовой функцией φ.

Если f — функция из P (оператор), то

$$L^{\triangle}_{\sigma,\varphi}(f)=\min_{S,f\overset{\triangle}{\preccurlyeq}S}L_{\sigma,\varphi}(S),\quad \triangle\in\{\varnothing,\xi,(a,b)\},\ -$$

сложность реализации f функциональными сетями в сигнатуре σ с весовой функцией φ (корректирующими ξ неисправностей, a единичных и b нулевых неисправностей).

Если $\mathfrak{A}$ — класс функций или операторов, то

$$L^{\triangle}_{\sigma,\varphi}(\mathfrak{A}^{\langle n\rangle})=\max_{f\in\mathfrak{A}^{\langle n\rangle}}L^{\triangle}_{\sigma,\varphi}(f),\quad \triangle\in\{\varnothing,\xi,(a,b)\},\ -$$

соответствующая функция Шеннона.

В качестве основных функционалов характеризации априорной сложности компонент рассматриваются $m(f)$ — число точек, на которых функция принимает значения ноль и один, $2^{N(f)}$ — число всевозможных наборов значений переменных функции. В качестве вспомогательного функционала рассматривается $\mathcal{H}(f)$ — энтропия f, т. е. двоичный логарифм (log) числа сочетаний из $m(f)$ по $m_1(f)$ — числу единичных точек функции f. В качестве нормировочных функций рассматриваются

$$\frac{x}{\overline{\log}\,\overline{\log}\,x}\quad\text{и}\quad\frac{x}{\overline{\log}\,x},$$

где

$$\overline{\log}\,x=\begin{cases}\log x, & \text{если } x\geqslant 4,\\ 2, & \text{если } 0\leqslant x<4.\end{cases}$$

Если соотношение

$$L^{\triangle}_{\sigma,\varphi}(\mathfrak{A}^{\langle n\rangle})\lesssim\psi(n)$$

выполнено при всех φ, таких что $\log\varphi(n) = o(\log\psi(n))$, то пишем

$$L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n),$$

а если при всех таких φ, что $\log\log\varphi(n) = o(\log\log\psi(n))$, то пишем

$$L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \dot{\lesssim} \psi(n).$$

Если соотношение

$$L^{\triangle}_{\sigma,\varphi}(\mathfrak{A}^{\langle n\rangle}) \gtrsim \psi(n)$$

выполнено хотя бы для одной φ, такой что $\log\varphi(n) = o(\log\psi(n))$, то пишем

$$L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \gtrsim \psi(n),$$

а если хотя бы для одной φ, такой что $\log\log\varphi(n) = o(\log\log\psi(n))$, то пишем

$$L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \dot{\gtrsim} \psi(n).$$

Полагаем

$$L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \sim \psi(n) \leftrightarrow L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n),\ L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \gtrsim \psi(n);$$
$$L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \dot{\sim} \psi(n) \leftrightarrow L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \dot{\lesssim} \psi(n),\ L^{\triangle}_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \dot{\gtrsim} \psi(n).$$

Для сигнатур σ_1, σ_2 пишем $\sigma_1 \leqslant \sigma_2$, если при всех допустимых f, φ, $\triangle$ выполнено

$$L^{\triangle}_{\sigma_1,\varphi}(f) \leqslant L^{\triangle}_{\sigma_2,\varphi}(f).$$

Так как $\boldsymbol{П} \subset \boldsymbol{Т} \subset \boldsymbol{СЛ}$, то

$$\langle \boldsymbol{СЛ}, L_{\boldsymbol{СЛ}}, \Phi, \boldsymbol{Ш}\rangle \leqslant \langle \boldsymbol{Т}, L_{\boldsymbol{Т}}, \Phi, \boldsymbol{Ш}\rangle \leqslant \langle \boldsymbol{П}, L_{\boldsymbol{П}}, \Phi, \boldsymbol{Ш}\rangle$$

при любых допустимых Φ и $\boldsymbol{Ш}$.

Пусть

$$\boldsymbol{Ш}_1(x) = \frac{x}{\overline{\log x}}, \quad \boldsymbol{Ш}_2(x) = \frac{x}{\overline{\log}\,\overline{\log x}}.$$

Было показано, что

$$\langle \mathfrak{M}, L_{\mathfrak{M}}, \Phi, \boldsymbol{Ш}_2\rangle \leqslant \langle \mathfrak{M}, L_{\mathfrak{M}}, \Phi, \boldsymbol{Ш}_1\rangle$$

при любых допустимых $\mathfrak{M}$ и Φ.

Для мощностных нижних оценок функции Шеннона имеет место следующее утверждение.

Теорема 3.1 [9]. *Если* $\log n = o\big(\log \mathcal{H}(\mathfrak{A}^{\langle n\rangle})\big)$, *то*

$$L_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \gtrsim \mathcal{H}(\mathfrak{A}^{\langle n\rangle}),$$

а если $\log\log n = o\big(\log\log \mathcal{H}(\mathfrak{A}^{\langle n\rangle})\big)$, *то*

$$L_{\sigma}(\mathfrak{A}^{\langle n\rangle}) \dot{\gtrsim} \mathcal{H}(\mathfrak{A}^{\langle n\rangle}),$$

где $\sigma_1 = \big\langle \boldsymbol{СЛ}, L_{\boldsymbol{СЛ}}, m, \frac{x}{\overline{\log}\,\overline{\log x}}\big\rangle$, *а* $\mathcal{H}(\mathfrak{A}^{\langle n\rangle})$ *— энтропия класса* $\mathfrak{A}^{\langle n\rangle}$, *т. е. двоичный логарифм минимально возможной мощности множества булевых функций* (*операторов*), *содержащего доопределения всех* f *из* $\mathfrak{A}^{\langle n\rangle}$.

А. Е. Андреевым разработан асимптотически оптимальный метод синтеза бесповторных функциональных сетей.

Теорема 3.2 является основным результатом для классов с ограничениями на энтропию функций.

Теорема 3.2 [9]. *Если* $\mathfrak{A}$ *— класс булевых функций или операторов,* $\mathfrak{M} \in \{\boldsymbol{\Pi}, \boldsymbol{T}, \boldsymbol{СЛ}\}$, $\triangle(n) \in \{\varnothing, \xi(n), (a(n), b(n))\}$,

$$L_{\sigma_1}^{\triangle(n)}(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n),$$

$\log^2 n = o(\log \psi(n))$, *то*

$$L_{\sigma_2}^{\triangle(n)}(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n),$$

где $\sigma_1 = \langle \mathfrak{M}, L_{\mathfrak{M}}, \mathcal{H}, \frac{x}{\log x}\rangle$, $\sigma_2 = \langle \mathfrak{M}, L_{\mathfrak{M}}, m, \frac{x}{\log x}\rangle$.

Через Q_r обозначим множество всех таких функций f из P, что

$$\mathcal{H}(f) \leqslant r(N(f))$$

(r — неотрицательная последовательность, $N(f)$ — число переменных f), а через $\varepsilon_{1,r}$ — множество всех таких функций f, что

$$m_1(f) = r(N(f))$$

(r — натуральная последовательность). Из теорем 3.1 и 3.2 вытекает следующий результат.

Теорема 3.3 [9]. *Если* $\log^2 n = o(\log r(n))$, $r(n) \leqslant 2^n$, *то*

$$L_\sigma(Q_r^{\langle n\rangle}) \sim r(n),$$

а если r *— натуральная последовательность и* $\log^2 n = o(\log r(n))$, $\log^2 n = o\Big(\log\big(2^n - r(n)\big)\Big)$, *то*

$$L_\sigma(\varepsilon_{1,r}^{\langle n\rangle}) \sim \log C_{2^n}^{r(n)},$$

где $\sigma = \langle \boldsymbol{\Pi}, L_{\boldsymbol{\Pi}}, m, \frac{x}{\log x}\rangle$.

Важно получить оценки сложности реализации частичных функций с данной величиной области определения функциональными сетями в сигнатуре $\sigma = \langle \boldsymbol{\Pi}, L_{\boldsymbol{\Pi}}, 2^N, \frac{x}{\log\log x}\rangle$.

Через ε_r обозначим множество всех таких функций f из P, что $m(f) \leqslant r(N(f))$, где r — натуральная последовательность. Имеет место следующее утверждение.

Теорема 3.4 [9]. *Если* $\log\log n = o(\log\log r(n))$, *то*

$$L_\sigma(\varepsilon_r^{\langle n\rangle}) \dot{\sim} r(n).$$

С помощью этой теоремы устанавливается следующий факт.

Теорема 3.5 [9]. *Если* $\mathfrak{A} \subseteq P$, $\triangle(n) \in \{\varnothing, \xi(n), (a(n), b(n))\}$,

$$L_{\sigma_0}^{\triangle(n)}(\mathfrak{A}^{\langle n\rangle}) \dot{\lesssim} \psi(n),$$

$\log\log n = o(\log\log\psi(n))$, *то*

$$L_{\sigma}^{\triangle(n)}(\mathfrak{A}^{\langle n\rangle}) \dot{\lesssim} \psi(n),$$

где σ *имеет тот же смысл, что и в предыдущей теореме,* $\sigma_0 = \langle \boldsymbol{\Pi}, L_{\boldsymbol{\Pi}}, m, \frac{x}{\overline{\log\log x}}\rangle$.

Рассмотрим ненулевые инвариантные классы С. В. Яблонского. Пусть $\mathcal{R}_\alpha$ — некоторый ненулевой инвариантный класс, такой что

$$\lim_{n\to\infty} \frac{\mathcal{H}(\mathcal{R}_\alpha^{\langle n\rangle})}{2^n} = \alpha > 0.$$

Справедлива следующая теорема.

Теорема 3.6 [9]. $L_\sigma(\mathcal{R}_\alpha^{\langle n\rangle}) \sim \alpha 2^n$, *где* $\sigma = \langle \boldsymbol{\Pi}, L_{\boldsymbol{\Pi}}, m, \frac{x}{\overline{\log x}}\rangle$.

Для классов Поста установлен следующий результат.

Теорема 3.7. *Для любого замкнутого класса* $\mathfrak{A}$ *функций алгебры логики, не содержащегося полностью ни в одном из классов* D_3, L_1, S_6, P_6, *имеет место соотношение*

$$L_\sigma(\mathfrak{A}^{\langle n\rangle}) \sim \mathcal{H}(\mathfrak{A}^{\langle n\rangle}),$$

где $\sigma = \langle \boldsymbol{\Pi}, L_{\boldsymbol{\Pi}}, m, \frac{x}{\overline{\log x}}\rangle$.

Были разработаны асимптотически оптимальные методы синтеза топологических функциональных сетей.

Наряду с реализацией функций и операторов рассматривается реализация и топологических функциональных сетей. При этом сеть S_2 реализует сеть S_1 (пишем $S_1 \preccurlyeq S_2$), если множества их полюсов совпадают и компонента $[S_2]$, отвечающая данной паре полюсов, является доопределением соответствующей компоненты $[S_1]$.

Если $S = \mathcal{F}(\tilde{F})$ — топологическая функциональная сеть, то полагаем, что $\mathcal{H}_{\text{пр}}(S)$ — минимально возможная суммарная энтропия такого набора функций, что любая компонента $\tilde{F}$ или её отрицание является компонентой этого набора, $L_{\boldsymbol{T}}^*(S)$ — арность $\mathcal{F}$, $N(S)$ — число переменных, задействованных в S. Если r_1, r_2 — положительные последовательности, то через $\boldsymbol{T}_{r_1,r_2}^*$ обозначим множество всех таких топологических функциональных сетей S, что

$$L_{\boldsymbol{T}}^*(S) \leqslant r_1\big(N(S)\big), \quad \mathcal{H}_{\text{пр}}(S) \leqslant r_2\big(N(S)\big).$$

Имеет место следующее утверждение.

Теорема 3.8 [9]. *Если* $1 \leqslant r_1(n) = r_2(n)^{o(1)}$, $\log^3 n = o(\log r_2(n))$, $r_2(n) \leqslant 2^{cn}$, *то*

$$L_\sigma(\boldsymbol{T}_{r_1,r_2}^{*\,\langle n\rangle}) \sim r_2(n),$$

где c — *константа, а* $\sigma = \langle \boldsymbol{T}, L_{\boldsymbol{T}}, m, \frac{x}{\overline{\log x}}\rangle$.

Эта теорема позволяет переносить на топологические функциональные сети многие конструкции принципа локального кодирования О. Б. Лупанова. Она может быть проиллюстрирована следующим образом. Рассмотрим инвариантные классы операторов. Они определяются аналогично инвариантным классам С. В. Яблонского. При этом число компонент у всех операторов из одного класса одинаково. Следуя С. В. Яблонскому, инвариантный класс $\mathfrak{A}$ операторов называем ненулевым, если

$$\lim_{n\to\infty} \frac{\mathcal{H}(\mathfrak{A}^{\langle n\rangle})}{2^n} > 0.$$

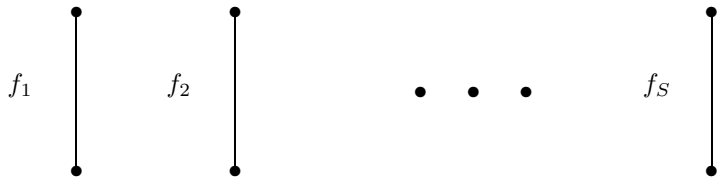
При помощи конструкции принципа локального кодирования О. Б. Лупанова для инвариантных классов и теоремы 3.8 получается следующий результат.

Теорема 3.9 [9]. *Если $\mathfrak{A}$ — ненулевой инвариантный класс операторов, то*

$$L_\sigma(\{\langle\tilde{F}\rangle \mid \tilde{F} \in \mathfrak{A}^{\langle n\rangle}\}) \sim \mathcal{H}(\mathfrak{A}^{\langle n\rangle}),$$

где $\sigma = \langle \boldsymbol{T}, L_{\boldsymbol{T}}, m, \frac{x}{\log x}\rangle$.

Здесь через $\langle\tilde{F}\rangle$, где $\tilde{F} = (f_1, f_2, \ldots, f_S)$, обозначается топологическая функциональная сеть вида



Рассмотрим класс монотонных операторов. Положим для булева набора $\tilde{a} = (a_1, a_2, \ldots, a_n)$

$$I(\tilde{a}) = 2^{n-1}a_1 + 2^{n-2}a_2 + \ldots + 2a_{n-1} + a_n.$$

Класс MH состоит из всех таких операторов F, у которых число компонент равно числу переменных и

$$I(\tilde{a}) \leqslant I(\tilde{b}) \implies I\big(F(\tilde{a})\big) \leqslant I\big(F(\tilde{b})\big).$$

С использованием конструкции О. Б. Лупанова для этого класса и теоремы 3.8 получается следующий результат.

Теорема 3.10 [9]. $L_\sigma(\{\langle\tilde{F}\rangle \mid \tilde{F} \in \mathsf{MH}^{\langle n\rangle}\}) \sim 2^{n+1}$, *где $\sigma = \langle \boldsymbol{T}, L_{\boldsymbol{T}}, m, \frac{x}{\log x}\rangle$.*

Рассмотрим вопрос о вычислении значения функции на нескольких последовательных наборах.

Если $f \in P^{\langle n\rangle}$, то через f^{+k} обозначим такую функцию из $P^{\langle n\rangle}$, что

$$I(\tilde{b}) = I(\tilde{a}) + k \pmod{2^n} \implies f^{+k}(\tilde{a}) = f^{+k}(\tilde{b}).$$

При помощи конструкции О. Б. Лупанова и теоремы 3.8 получается следующий результат.

Теорема 3.11 [9]. *Если* $1 \leqslant t(n) \leqslant 2^{o(n)}$, *то*

$$L_\sigma(\{\langle f, f^{+1}, \ldots, f^{+t(n)}\rangle \mid f \in P^{\langle n\rangle}\}) \sim 2^n,$$

где $\sigma = \langle \boldsymbol{T}, L_{\boldsymbol{T}}, m, \frac{x}{\overline{\log x}}\rangle$.

Рассмотрим вопросы синтеза асимптотически неизбыточных самокорректирующихся функциональных сетей.

Теорема 3.12 [9]. *Если* $\mathfrak{A} \subseteq P$, $\log^2 n = o\big(\log \psi(n)\big)$,

$$L_\sigma(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n),$$

$1 \leqslant \log \xi(n) = o\Big(\sqrt{\frac{\log \psi(n)}{\log n}}\Big)$, *то*

$$L_\sigma^{\xi(n)}(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n),$$

где $\sigma = \langle \boldsymbol{\Pi}, L_{\boldsymbol{\Pi}}, m, \frac{x}{\overline{\log x}}\rangle$.

Пусть $\sigma = \langle \boldsymbol{T}, L_{\boldsymbol{T}}, m, \frac{x}{\overline{\log x}}\rangle$. Основными результатами о самокорректировании в топологических функциональных сетях являются следующие теоремы.

Теорема 3.13 [9]. *Если* $\mathfrak{A}$ *— класс функций или операторов и*

$$L_\sigma(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n),$$

$\log^3 n = o(\log \psi(n))$, $1 \leqslant \log \xi(n) = o(\log \psi(n))$, *то*

$$L_\sigma^{\xi(n)}(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n).$$

Теорема 3.14 [9]. *Если* $\mathfrak{A}$ *— класс функций или операторов и*

$$L_\sigma(\mathfrak{A}^{\langle n\rangle}) \lesssim \psi(n) = \mathcal{H}(\mathfrak{A}^{\langle n\rangle}),$$

$\log^3 n = o\big(\log \psi(n)\big)$, $\psi(n) \leqslant 2^{cn}$, *то*

$$L_\sigma^{\xi(n)}(\mathfrak{A}^{\langle n\rangle}) \sim \psi(n) \leftrightarrow \log \xi(n) = o\big(\log \psi(n)\big),$$

где c *— константа.*

Теорема 3.15 [9]. *Если* $\varepsilon \in (0, 1)$, $a(n) \geqslant 2$, $b(n) \geqslant 2$,

$$\log a(n) + \log b(n) \leqslant \frac{n}{2}(1 - \varepsilon),$$

то

$$L_\sigma^{(a(n), b(n))}(P^{\langle n\rangle}) \lesssim \frac{1}{\varepsilon} 2^n.$$

Исследовались вопросы моделирования функциональных сетей. Были описаны условия, при которых асимптотически оптимальные в данной сигнатуре функциональные сети порождают при моделировании в данном типе управляющих систем асимптотически оптимальные схемы. Рассматривалось моделирование бесповторных функциональных сетей формулами и топологических функциональных сетей контактными схемами.

Рассмотрим формулы в полном базисе $\mathsf{Б}$, который состоит из надёжной и ненадёжной частей, причём надёжная часть базиса $\mathsf{Б}_{\text{н}}$ полна. Формула, реализующая f, корректирует ξ неисправностей, если при замене в ней не более ξ любых вхождений ненадёжных функциональных символов на любые другие той же арности получающаяся формула также реализует f. Через $L^{\xi}_{\mathsf{Б.Ф.}}(f)$ обозначается сложность реализации f формулами в базисе $\mathsf{Б}_{\text{н}}$, корректирующими ξ неисправностей. Через $\rho(\mathsf{Б})$ обозначается минимальный приведённый вес базиса $\mathsf{Б}$.

Пусть семейство $\mathfrak{N}_1$ состоит из следующих классов функций из P:

1) $\varepsilon_r = \{f \mid m(f) \leqslant r\big(N(f)\big)\}$, где r — любая натуральная монотонная последовательность;
2) $\varepsilon_{1,r} = \{f \mid m_1(f) = r\big(N(f)\big)\}$, где r — любая натуральная последовательность;
3) $Q_r = \{f \mid \mathcal{H}(f) \leqslant r\big(N(f)\big)\}$, где r — любая положительная монотонная последовательность;
4) всех ненулевых инвариантных классов С. В. Яблонского;
5) всех классов Поста, не содержащихся полностью в D_3, L_1, S_6, P_6.

Пусть семейство $\hat{\mathfrak{N}}_1$ состоит из всех таких классов $\mathfrak{A}$ семейства $\mathfrak{N}_1$, что $\log\log\mathcal{H}(\mathfrak{A}^{\langle n\rangle}) \sim \log n$, и таких классов ε_r и Q_r, что $\log\log n = o\big(\log\log r(n)\big)$.

Теорема 3.16 [9]. *Если* $\mathfrak{A} \in \hat{\mathfrak{N}}_1$, $\log\xi(n) = o\Big(\sqrt{\frac{\log\mathcal{H}(\mathfrak{A}^{\langle n\rangle})}{\log n}}\Big)$, *то для любого базиса* $\mathsf{Б}$ *с полной надёжной частью*

$$L^{\xi(n)}_{\mathsf{Б.Ф.}}(\mathfrak{A}^{\langle n\rangle}) \sim L^{0}_{\mathsf{Б.Ф.}}(\mathfrak{A}^{\langle n\rangle}) \sim \rho(\mathsf{Б})\frac{\mathcal{H}(\mathfrak{A}^{\langle n\rangle})}{\log\log\mathcal{H}(\mathfrak{A}^{\langle n\rangle})}.$$

Это утверждение вытекает из изложенных выше результатов и результатов О. Б. Лупанова [50], в которой получена асимптотика функции Шеннона для формул.

Рассмотрим контактные схемы. Через $L_k(F)$ обозначим сложность реализации F обычными контактными схемами, а через $L^{\xi}_k(F)$ и $L^{(a,b)}_k(F)$ — корректирующими ξ любых неисправностей контактов и соответственно a замыканий и b размыканий контактов одновременно. Получена верхняя оценка сложности реализации контактными схемами частичных функций с данной величиной области определения, которая необходима для асимптотически оптимального моделирования топологических функциональных сетей.

Теорема 3.17 [9]. *Если* $f \in P^{\langle n\rangle}$, *то*

$$L_k(f) \leqslant \frac{m(f)}{\overline{\log}\, m(f)}\left(1 + \frac{O(1)}{\overline{\log}\,\overline{\log}\, n}\right) + 2^{O(1)\log^5 n}.$$

Пусть семейство $\mathfrak{N}_2$ состоит из следующих классов операторов:

1) всех ненулевых инвариантных классов операторов;
2) класса $\mathsf{МН}$ монотонных операторов;
3) $\big\{\big(f, f^{+1}, \ldots, f^{+r(N(f))}\big) \mid f \in P\big\}$, где r — такая натуральная последовательность, что $1 \leqslant r(n) = 2^{o(n)}$;

4) $\Big\{(\underbrace{f,\bar{f},f,\bar{f},\ldots,f,\bar{f}}_{r(N(f))}) \mid f \in P\Big\}$, где r — такая натуральная последовательность, что $1 \leqslant r(n) = 2^{o(n)}$.

Если $\mathfrak{A}$ — класс операторов, положим $\hat{\mathfrak{A}} = \{\langle \tilde{F}\rangle \mid \tilde{F} \in \mathfrak{A}\}$. Положим $\hat{\mathfrak{N}}_2 = \{\hat{\mathfrak{A}} \mid \mathfrak{A} \in \mathfrak{N}_2\}$.

Считается, что контактная схема реализует функциональную сеть S, если она реализует $[S]$.

Теорема 3.18 [9]. *Если* $\mathfrak{A} \in \mathfrak{N}_1 \cup \hat{\mathfrak{N}}_2$ *и* $\mathcal{H}(\mathfrak{A}^{\langle n\rangle}) \geqslant 2^{\log^6 n}$,

$$1 \leqslant \log \xi(n) = o\big(\log \mathcal{H}(\mathfrak{A}^{\langle n\rangle})\big),$$

то

$$L_k^{\xi(n)}(\mathfrak{A}^{\langle n\rangle}) \sim L_k(\mathfrak{A}^{\langle n\rangle}) \sim \frac{\mathcal{H}(\mathfrak{A}^{\langle n\rangle})}{\log \mathcal{H}(\mathfrak{A}^{\langle n\rangle})}.$$

Теорема 3.19 [9]. *Если* $\varepsilon \in (0,1)$, $a(n) \geqslant 2$, $b(n) \geqslant 2$,

$$\log a(n) + \log b(n) \leqslant \frac{n}{2}(1-\varepsilon),$$

то

$$L_k^{(a(n),b(n))}(P^{\langle n\rangle}) \lesssim \frac{1}{\varepsilon}\frac{2^n}{n}.$$

Изложенные результаты опубликованы в [4, 6—8, 10, 13].

Одним из основных вопросов теории схемной сложности является нахождение высоких нижних оценок для классов булевых функций при реализации их конкретными видами схем. Особую роль здесь играют схемы из функциональных элементов, по отношению к которым до 1980-х годов не удавалось привести примеров булевых функций с нелинейной сложностью. В [12] впервые указана последовательность булевых функций, сложность которой в монотонном базисе является не только нелинейной, но почти экспоненциальной.

4. Минимизация булевых функций

Важное место в теории управляющих систем занимает теория дизъюнктивных нормальных форм. Булева функция $f(x_1,\ldots,x_n)$, описывающая функционирование управляющей системы, может быть реализована с помощью дизъюнктивной нормальной формы (д. н. ф.), которая в этом случае опишет схему соответствующей управляющей системы. Важная задача теории управляющих систем — нахождение оптимальной схемы с наименьшей затратой оборудования — выражается в теории д. н. ф. как задача нахождения среди всех д. н. ф., реализующих данную функцию, кратчайших или минимальных д. н. ф. Существует тривиальное решение указанной задачи: все д. н. ф. над переменными $\{x_1,\ldots,x_n\}$ (их число 2^{3^n}) упорядочиваются по порядку неубывания рассматриваемой сложности и выбирается первая д. н. ф., которая реализует данную

функцию. Это решение с точки зрения практики слишком громоздко. Известно [24, 95], что кратчайшую д. н. ф. (к. д. н. ф.) и минимальную д. н. ф. (м. д. н. ф.) можно получить из сокращённой д. н. ф. (с. д. н. ф.) заданной функции путём удаления некоторых конъюнкций. Установлен достаточно эффективный критерий, позволяющий осуществлять это удаление (так называемый критерий поглощения) [24, 29]. Однако и при таком подходе решение задачи минимизации булевых функций встречает ряд серьёзных препятствий. Последние были указаны в работах по алгоритмическим трудностям синтеза минимальных схем и в работах Ю. Л. Васильева и В. В. Глаголева [17, 18, 24]. Эти трудности проявляются прежде всего в том, что после ряда последовательных упрощений д. н. ф. для данной функции с помощью критерия поглощения получается неупрощаемая тупиковая д. н. ф. (т. д. н. ф.), которая может являться к. д. н. ф. или м. д. н. ф., а может и не быть таковой. Приходится снова проводить процесс упрощения с. д. н. ф., удаляя другие конъюнкции до тех пор, пока не будут получены все т. д. н. ф., и среди них выбирать искомое решение.

Подчёркивая большую трудоёмкость процедур такого рода, Ю. И. Журавлёв указывал на необходимость предварительного изучения свойств удаляемых конъюнкций и предложил в связи с этим подход, названный им локальными алгоритмами [29, 31, 32]. Главным достоинством таких алгоритмов является то, что, не прибегая к просмотру всех т. д. н. ф. и ограничиваясь лишь информацией о конъюнкциях, близких к рассматриваемой конъюнкции, можно иногда определить, входит или не входит последняя в некоторые (или во все) к. д. н. ф. (м. д. н. ф.) данной функции. Однако в общем случае утвердительного ответа на такой вопрос локальные алгоритмы дать не могут [24, 31]. Поэтому можно считать, что локальные алгоритмы играют лишь промежуточную роль в общей теории минимизации булевых функций. Характерная трудность изучаемой задачи заключается в том, что, с одной стороны, процедуры минимизации булевых функций не могут быть осуществлены без перебора [17], а с другой стороны, мощность областей перебора обычно очень велика. Как отмечено в [18, 24], максимальное число т. д. н. ф. функции от n переменных имеет порядок, больший, чем 2^{2^n}.

В [61] изучались качественные и количественные вопросы, связанные с алгоритмами минимизации булевых функций.

1. Описать процесс построения с помощью критерия поглощения всех т. д. н. ф. булевой функции в виде так называемого графа перебора и оценить для некоторых классов графов

   а) наименьшее число n, такое что для любого графа перебора из данного класса существует булева функция от n переменных, граф перебора для которой изоморфен данному графу;

   б) наименьшее число n, такое что существует булева функция от n переменных, граф перебора для которой принадлежит данному классу графов.

2. Описать взаимосвязь между конъюнкциями из с. д. н. ф. булевой функции в виде графа интервалов и оценить для некоторых классов графов аналогичные вышеуказанным функции Шеннона.
3. Разработать алгоритмы нахождения к. д. н. ф. и м. д. н. ф. для булевых функций из некоторых классов.

Изучался процесс построения всех т. д. н. ф. булевой функции в геометрическом плане и исследовалось поведение указанных функций Шеннона. Граф интервалов был введён А. А. Сапоженко [77]. Исследовались новые качественные и количественные проблемы, связанные с этим графом. Были описаны алгоритмы нахождения к. д. н. ф. и м. д. н. ф. для класса булевых функций, так называемый упрощённый граф интервалов каждой из которых является деревом. Сложность построенных алгоритмов оказалась линейно зависящей от числа вершин-конъюнкций в исходном графе.

Результаты, полученные по первым двум из вышеуказанных вопросов, позволяют лучше понять сложную взаимосвязь различных характеристик булевых функций. Выработанные алгоритмы осуществляют строго меньший перебор, чем алгоритм перебора среди всех т. д. н. ф. булевой функции из выбранного класса.

Формализуем изложенное. Введём основные понятия и обозначения, используемые далее. Пусть A — некоторые множество, $|A|$ — его мощность, 2^A — множество всех его подмножеств и A^n — декартово произведение $\underbrace{A \times \ldots \times A}_{n \text{ раз}}$. Если $|A| = n$, то A будем называть n-множеством. Будем использовать обозначение ξ_n для множества $\{1, \ldots, n\}$ ($n \geqslant 1$) и обозначение E_2 для множества $\{0, 1\}$. E_2^n есть множество всех точек $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, где $\alpha_i \in E_2$ для любого $i \in \xi_n$. При фиксированном n положим $\tilde{1} = (\underbrace{1, \ldots, 1}_{n \text{ раз}})$ и $\tilde{0} = (\underbrace{0, \ldots, 0}_{n \text{ раз}})$. Для точки $\tilde{\alpha}$ из E_2^n обозначим через $I_{\tilde{\alpha}}^1$ ($I_{\tilde{\alpha}}^0$) множество всех номеров i из ξ_n, таких что $\alpha_i = 1$ (соответственно $\alpha_i = 0$). Нормой точки $\tilde{\alpha}$ (обозначение $|\tilde{\alpha}|$) назовём мощность множества $I_{\tilde{\alpha}}^1$. Пусть $\tilde{\alpha}$, $\tilde{\beta}$ — две точки из E_2^n. Будем говорить, что $\tilde{\alpha}$ не превосходит $\tilde{\beta}$ (обозначение $\tilde{\alpha} \leqslant \tilde{\beta}$), если имеет место соотношение $I_{\tilde{\alpha}}^1 \subseteq I_{\tilde{\beta}}^1$, и что $\tilde{\alpha}$ и $\tilde{\beta}$ несравнимы, если не выполняется ни $\tilde{\alpha} \leqslant \tilde{\beta}$, ни $\tilde{\beta} \leqslant \tilde{\alpha}$.

Граф Γ с множеством вершин V и множеством рёбер U обозначается через $\Gamma = (V, U)$.

Если $V \subseteq E_2^n$, то под V-графом будем понимать граф $\Gamma = (V, U)$, где U состоит из всех пар вершин $\tilde{\alpha}$, $\tilde{\beta}$ из V, таких что $\tilde{\alpha}$, $\tilde{\beta}$ отличаются друг от друга ровно в одной координате. В частности, E_2^n-графом является единичный n-мерный куб.

Через P_2 обозначим множество всех булевых функций, т. е. таких функций, у которых переменные и сами функции принимают значения из E_2, а через $P_2(n)$ — множество всех булевых функций, зависящих от n переменных $\{x_1, \ldots, x_n\}$. Элементарной конъюнкцией ранга r называется логическое произведение $x_{i_1}^{\sigma_1} \ldots x_{i_r}^{\sigma_r}$, где $x_i^{\sigma_i} = x_i$, если $\sigma_i = 1$, и $x_i^{\sigma_i} = \overline{x_i}$, если $\sigma_i = 0$, а все x_{i_j} различны. Д. н. ф. есть логическая сумма $D = K_1 \vee \ldots \vee K_m$ различных эле-

ментарных конъюнкций K_j. Для д. н. ф. D обозначим через $M(D)$ множество всех её элементарных конъюнкций. Если булева функция представляется в виде д. н. ф., то говорят, что последняя реализует данную функцию. К. д. н. ф. (м. д. н. ф.) для функции $f(x_1,\ldots,x_n)$ являются те д. н. ф., которые реализуют $f(x_1,\ldots,x_n)$ и содержат наименьшее число элементарных конъюнкций (соответственно наименьшее число вхождений символов переменных) по сравнению с другими реализующими $f(x_1,\ldots,x_n)$ д. н. ф. Каждой булевой функции $f(x_1,\ldots,x_n)$ поставим в соответствие подмножество $\mathcal{N}_f$ множества E_2^n всех точек $\tilde{\alpha}$, таких что $f(\tilde{\alpha})=1$. Для элементарной конъюнкции K r-го ранга множество $\mathcal{N}_K \subseteq E_2^n$ $(n \geqslant r)$ называется интервалом r-го ранга, а граф $\mathcal{N}_K$ — $(n-r)$-мерной гранью единичного n-мерного куба. Элементарная конъюнкция K называется простой, а соответствующий интервал максимальным для функции $f(x_1,\ldots,x_n)$, если имеет место $\mathcal{N}_K \subseteq \mathcal{N}_f$ и не существует такой конъюнкции K', что $\mathcal{N}_K \subseteq \mathcal{N}_{K'} \subseteq \mathcal{N}_f$. Дизъюнкция всех простых конъюнкций функции $f(x_1,\ldots,x_n)$ называется с. д. н. ф. для данной функции и обозначается через $D_C(f)$. Любая дизъюнкция D простых конъюнкций функции f называется т. д. н. ф., если D реализует f и не существует другой реализующей f дизъюнкции D', такой что $M(D') \subset M(D)$. Логическую сумму всех т. д. н. ф. функции обозначаем через $D_{\cup T}(f)$, а логическую сумму всех простых конъюнкций функции f, каждая из которых входит во все т. д. н. ф. — через $D_{\cap T}(f)$. Множество $M\big(D_{\cap T}(f)\big)$ называется множеством ядровых конъюнкций, а множество $M\big(D_C(f)\big)\setminus M\big(D_{\cap T}(f)\big)$ — множеством неядровых конъюнкций функции f. Две функции $f(x_1,\ldots,x_n)$ и $g(x_1,\ldots,x_n)$ считаются равными, если $\mathcal{N}_f=\mathcal{N}_g$, а две д. н. ф. D_1, D_2 считаются конъюнктивно равными (обозначение $D_1=D_2$), если $M(D_1)=M(D_2)$.

Понятия булевых функций и д. н. ф. тесно связаны со многими понятиями комбинаторного анализа, в частности с понятием покрытия. Пусть $C=(X_1,\ldots,X_s)$ — некоторое семейство подмножеств множества X, и пусть $Y\subseteq X$. Будем говорить, что Y покрывает семейство C (или Y является покрытием для C), если для любого X_i из C выполнено $X_i\cap Y\neq\varnothing$. Покрытие Y называется приведённым для C, если любое его собственное подмножество не является покрытием для C. Множество всех приведённых покрытий для C обозначается через $\mathcal{P}(C)$.

Был изучен алгоритм минимизации булевых функций, в основе которого лежит процедура сравнения на поглощаемость одного набора конъюнкций другими [30, 95]. Предполагается, что булева функция задаётся с помощью с. д. н. ф. Тогда этот алгоритм состоит в последовательном построении наследственных д. н. ф., реализующих заданную функцию и получающихся друг из друга с помощью удаления дизъюнктивных членов. Эта процедура удобно представляется в виде так называемого графа перебора, вершинами которого является д. н. ф., состоящие из простых конъюнкций и реализующие заданную функцию, а рёбрами — пары указанных д. н. ф., отличающихся друг от друга ровно одним дизъюнктивным членом.

Назовём поликубом любой граф $\Pi(l,k)$, состоящий из некоторых k попарно несравнимых точек $\tilde{\alpha}^1,\dots,\tilde{\alpha}^k$ из E_2^l, удовлетворяющих условию $\Big|\bigcup\limits_{i=1}^{k} I^0_{\tilde{\alpha}^i}\Big| = l$, и из всех точек $\tilde{\beta}$ из E_2^l, таких что имеет место неравенство $\tilde{\alpha}^i \leqslant \tilde{\beta}$ для некоторых I из ξ_k. Число l называется размерностью поликуба, а число k — числом подкубов поликуба. Установлено, что если булева функция имеет l неядровых конъюнкций и k т. д. н. ф., то её граф перебора изоморфен некоторому поликубу $\Pi(l,k)$. Наоборот, показывается, что для любого поликуба размерности l существует булева функция от $l+2$ переменных, граф перебора для которой изоморфен данному поликубу.

Обозначим через $\{\tilde{\alpha}^1,\dots,\tilde{\alpha}^k\}$ k попарно несравнимых точек из E_2^l, которые определяют поликуб $\Pi(l,k)$. Положим $\mathcal{J}\big(\Pi(l,k)\big) = \{I^1_{\tilde{\alpha}^1},\dots,I^1_{\tilde{\alpha}^k}\}$. Пусть $\gamma\colon \xi_l \to M$ — некоторое отображение множества ξ_l в множество конъюнкций M, $\beta = \{i_1,\dots,i_s\}$ $(s \leqslant l)$ — произвольное подмножество множества ξ_l. Положим $\gamma^{\&}(\beta) = \gamma(i_1)\,\&\,\dots\,\&\,\gamma(i_s)$, $\gamma^{\vee}(\beta) = \gamma(i_1)\vee\dots\vee\gamma(i_s)$. Множество всех булевых функций с графом перебора, изоморфным поликубу $\Pi(l,k)$, обозначается через $\mathcal{F}\big(\Pi(l,k)\big)$.

Теорема 4.1. *Булева функция f содержится в $\mathcal{F}\big(\Pi(l,k)\big)$ тогда и только тогда, когда выполняются следующие условия*:

1) $\big|\bar{M}\big(D_{\cap T}(f)\big)\big| = l$, *где* $\bar{M}\big(D_{\cap T}(f)\big)$ — *множество неядровых конъюнкций функции* f;
2) *существует взаимно-однозначное отображение* $\gamma_f\colon \xi_l \leftrightarrow \bar{M}\big(D_{\cap T}(f)\big)$, *такое что для* β *из* $\mathcal{P}\Big(\mathcal{F}\big(\Pi(l,k)\big)\Big)$ *справедливо соотношение*

$$\mathcal{N}_{\gamma_f^{\&}(\beta)} \not\subset \bigcup_{K_i \in M(D_c(f))\setminus M(\gamma_f^{\vee}(\beta))} \mathcal{N}_{K_i},$$

причём для всех других множеств β $(\beta \subseteq \zeta_l)$, *не являющихся покрытием для* $\mathcal{F}\big(\Pi(l,k)\big)$, *это соотношение не выполняется.*

Пусть π^l, $\pi^{l,k}$ и π^l_s — это соответственно множество всех подкубов размерности l, всех поликубов размерности l с k подкубами и всех поликубов размерности l с s подкубами максимальной размерности. Пусть $n(\Pi)$ — наименьшее число переменных у всех таких функций, граф перебора для которых изоморфен поликубу Π. Положим

$$\overline{n}(l) = \max_{\Pi\in\pi^l} n(\Pi), \quad \underline{n}(l) = \min_{\Pi\in\pi^l} n(\Pi), \quad \overline{n}(l,k) = \max_{\Pi\in\pi^{l,k}} n(\Pi), \quad \overline{n}_s(l) = \max_{\Pi\in\pi^l_s} n(\Pi).$$

Можно показать, что для любого $l \geqslant 1$ имеет место равенство $\overline{n}(l) = l+2$, что $\underline{n}(l)$ имеет порядок $\log_3 l$ и что $l+1 \leqslant \overline{n}_s(l) \leqslant l+2$ при всех l, s, удовлетворяющих соотношениям $l \geqslant 1$, $1 \leqslant s \leqslant C_l^{[\frac{l}{2}]}$.

Теорема 4.2. *Справедливы следующие оценки*:

1) $l+1 \leqslant \overline{n}(l,k) \leqslant l+2$ *при* $C_l^2 \leqslant k \leqslant C_l^{[\frac{l}{2}]}$, *причём* $\overline{n}(l,k) = l+2$ *при* $k = C_l^2, \ldots, C_l^{[\frac{l}{2}]}$;
2) $l \leqslant \overline{n}(l,k) \leqslant l+2$ *при* $l \leqslant k < C_l^2$;
3) $\max\bigl(k, k \cdot \log_2([\frac{l}{k}])\bigr) \leqslant \overline{n}(l,k) \leqslant \min(l+2, A)$, *где*

$$A = C_k^{[\frac{k}{2}]} \log_2 \left(\frac{l}{\min(l, C_k^{[\frac{k}{2}]})} \right) + 2C_k^{[\frac{k}{2}]} + 3 \quad \textit{при} \quad 2 \leqslant k \leqslant l;$$

4) $\overline{n}(l,k) \asymp \log_3 l$ *при* $k = 1$.

Как вытекает из этой теоремы, величина $\overline{n}(l,k)$ не более чем на 2 отличается от l при $k \geqslant l$ и есть $o(l)$ при k, достаточно малых по сравнению с l.

Обозначим через $\pi_s^{l,k}$ множество всех поликубов из $\pi^{l,k}$, каждый из которых имеет ровно s подкубов максимальной размерности. Условие $1 \leqslant s \leqslant k \leqslant C_l^{[\frac{l}{2}]}$ является необходимым для непустоты $\pi_s^{l,k}$.

Очевидно, что существует тройка (l,k,s), удовлетворяющая необходимому условию, но не являющаяся набором соответствующих параметров некоторого поликуба. Однако, как показывает следующая теорема, число таких исключительных случаев сравнительно мало при росте l.

Фиксируем l, s, где $1 \leqslant s \leqslant C_l^{[\frac{l}{2}]}$, и обозначим через $K(l,s)$ максимальную разность $k-s$ по всем числам k, таким что $s \leqslant k \leqslant C_l^{[\frac{l}{2}]}$ и $\pi_s^{l,k}$ не пусто. Положим

$$\varphi_l(\lambda) = \frac{K\bigl(l, \lambda C_l^{[\frac{l}{2}]}\bigr)}{C_l^{[\frac{l}{2}]}},$$

где $0 \leqslant \lambda \leqslant 1$.

Теорема 4.3. $\varphi_l(\lambda)$ *равномерно сходится к* $1-\lambda$ *при* l, *стремящемся к бесконечности.*

На языке булевых функций непустота $\pi_s^{l,k}$ означает, что существует функция, которая имеет l неядровых конъюнкций и k т. д. н. ф., среди которых ровно s к. д. н. ф. При оценке функции $\overline{n}_s(l,k)$, где $\overline{n}_s(l,k) = \max\limits_{\Pi \in \pi_s^{l,k}} n(\Pi)$, также выяснено, что при всех k, бóльших некоторой величины $\eta(l,s)$, имеет место неравенство $l+1 \leqslant \overline{n}_s(l,k) \leqslant l+2$.

Изучались некоторые метрические свойства графа перебора, такие как высота, ширина, объём.

Изучалась структура графа интервалов. Вершинами графа интервалов булевой функции являются её простые конъюнкции, а рёбрами — пары простых конъюнкций, интервалы которых пересекаются. Установлено, что любой граф без петель и кратных рёбер может служить графом интервалов для булевой функции.

Пусть $\mathcal{T}^m$ ($\mathcal{G}^m$) — множество всех графов (соответственно деревьев) с m вершинами без петель и кратных рёбер. Положим

$$\overline{n}(\mathcal{T}^m) = \max_{\Gamma\in\mathcal{T}^m} n(\Gamma), \quad \underline{n}(\mathcal{T}^m) = \min_{\Gamma\in\mathcal{T}^m} n(\Gamma),$$
$$\overline{n}(\mathcal{G}^m) = \max_{\Gamma\in\mathcal{G}^m} n(\Gamma), \quad \underline{n}(\mathcal{G}^m) = \min_{\Gamma\in\mathcal{G}^m} n(\Gamma),$$

$n(\Gamma)$ — минимальное число переменных у всех булевых функций, граф интервалов у которых изоморфен графу Γ. Установлены следующие оценки этих величин.

Теорема 4.4. *Справедлива оценка* $\underline{n}(\mathcal{T}^m) \asymp \log_3 m$.

Теорема 4.5. *Для любого* $m \geqslant 2$ *справедлива оценка* $\overline{n}(\mathcal{T}^m) = m$.

Теорема 4.6. *Для любого* $m \geqslant 2$ *справедливы следующие оценки*:

1) $]\log_2(m+1)[+ 2 \leqslant \overline{n}(\mathcal{G}^m) \leqslant (\log_2 m)^2 + c_1 \log_2 m + c_2$, *где* $c_1 = 16$, $c_2 = 39$;
2) $\log_2(m+1) \leqslant \underline{n}(\mathcal{G}^m) \leqslant]\log_2(m-1)[+ 2$.

В ряде специальных случаев возможен переход от известных локальных процедур [29,30,32] к улучшающим их нелокальным, но логически простым процедурам минимизации булевых функций. Имеется пример реализации этой идеи для класса $\mathcal{F}^y_{\mathcal{G}}$ всех булевых функций, для которых упрощённый граф интервалов, полученный из графа интервалов после удаления некоторых специальных конъюнкций, является лесом, т. е. графом, каждая компонента связности которого является деревом. Особенностью построенных алгоритмов нахождения т. д. н. ф. и м. д. н. ф. является то, что благодаря специфике выбранного класса булевых функций они работают лишь с информацией о рангах конъюнкций, связанной с вершинами упрощённого графа интервалов. Сложность описанных алгоритмов линейно зависит от числа вершин в упрощённом графе интервалов для исходной функции.

Проблема минимизации д. н. ф., являясь одной из наиболее содержательно богатых многоэкстремальных комбинаторно-логических задач, в силу относительно простой структуры изучаемого объекта может рассматриваться в качестве модельной задачи многоэкстремальной дискретной оптимизации. Благодаря этому проблема минимизации д. н. ф. активно изучалась с 50-х годов прошлого века, однако некоторые важные вопросы теории д. н. ф. долгое время оставались открытыми.

Здесь излагаются результаты А. Е. Андреева, в которых изучается эволюция ряда свойств, характеризующих проблему минимизации д. н. ф. в зависимости от мощностных характеристик булевых функций, причём описывается в основном типичное поведение соответствующих параметров. В этой постановке получены окончательные или близкие к окончательным результаты по следующим вопросам: сложность сокращённой д. н. ф., сложность самокорректирующихся д. н. ф., сложность реализации булевых операторов, протяжённость сокращённой д. н. ф. и др. Получены оценки сложности минимизации д. н. ф. на машинах Тьюринга. Из этих результатов вытекает, что трудности минимизации нарастают

при уменьшении числа нулей булевых функций. В целом негативным является ответ на вопрос об эффективности локальных алгоритмов. При любом росте числа нулей д. н. ф. Квайна асимптотически не отличается от д. н. ф., являющейся результатом работы А-алгоритма, кроме того, распознавание предиката «вхождение в сумму минимальных» по сложности полиномиально эквивалентно нахождению минимальной д. н. ф. Разработанные методы могут быть применены к задачам из других разделов теории дискретной оптимизации.

Общеизвестные понятия, не определяемые здесь, можно найти в [24]. Через l_{C}, $l_{\cup T}$, $l_{\cap T}$, l_{Q}, $l_{\mathrm{кр}}$, $l^s_{\mathrm{кр}}$, $l_{\mathrm{ко}}$ и l_{A} обозначим число элементарных конъюнкций соответственно в следующих д. н. ф.: сокращённой, объединении и пересечении тупиковых, Квайна, кратчайшей, кратчайшей из корректирующих s отбрасываний элементарных конъюнкций, получающихся в результате применения к сокращённой д. н. ф. кольцевого алгоритма ранга 2 и А-алгоритма, а через $l_{\min}$ — число букв в минимальной д. н. ф. Пусть ρ — протяжённость, Y — разброс, τ — число тупиковых д. н. ф. Через l^k_{C} обозначим число интервалов размерности k в сокращённой д. н. ф. Пусть P^n — множество всех булевых функций, определённых на $\{0,1\}^n$; $\tilde{P}^n$ — соответствующее множество частичных булевых функций; $P^n_{\alpha,m}$ — множество всех булевых функций из P^n, принимающих значение α на m наборах; P^n_m — множество всех частичных булевых функций, определённых на m наборах из $\{0,1\}^n$; $P^{n,t}_m$ — множество всех частичных (n,t)-операторов, определённых на m наборах из $\{0,1\}^n$; $\tilde{P}^n_{m_1,m_2}$ — множество всех частичных булевых функций из $P^n_{m_1+m_2}$, принимающих значение 1 на m_2 наборах.

Во всех рассматриваемых далее асимптотических отношениях предполагается, что $n \to \infty$, это же относится к термину «для почти всех».

Теорема 4.7 [3]. *Для почти всех булевых функций f из $P^n_{0,m}$ справедливы следующие соотношения*:

$$l_{\mathrm{C}}(f) \sim \sum_{r=0}^{n-1} \binom{n}{r} 2^{n-r} (1 - m \cdot 2^{-n})^{2^r} \left(1 - (1 - m \cdot 2^{-n})^{2^r}\right)^{n-r},$$

если $\log^3 n \leqslant m \leqslant 2^n - 1$;

$$l_{\mathrm{C}}(f) \sim \sum_{r=1}^{2[\log n]} \binom{m}{r} 2^r (n \cdot 2^{-r})^r,$$

если $1 = o(m)$, $m \leqslant \log^3 n$;

$$l_{\mathrm{C}}(f) \sim 2^m (n \cdot 2^{-m})^m,$$

если $1 \leqslant m = O(1)$.

Асимптотика получена также для классов $\tilde{P}^n_{m_1,m_2}$ при всех возможных соотношениях между n, m_1 и m_2. Ранее была известна лишь асимптотика логарифма l_{C} [21].

Теорема 4.8 [3]. *Для почти всех булевых функций f из $P^n_{0,m}$ справедливы следующие соотношения*:

$$\rho(f) \sim \frac{n}{n - \log m + \log\log n},$$

если $n - \log m = o(n)$, $2^n = O(2^n - m)$;

$$\left]\frac{n}{n-\log m} - \delta\right[\leqslant \rho(f) \leqslant \left]\frac{n}{n-\log m}\right[,$$

если $2^{n/2} \leqslant m \leqslant 2^{n(1-\varepsilon)}$, *где* $\delta, \varepsilon \in (0, 1/2)$;

$$\rho(f) = 2,$$

если $2 \leqslant m \leqslant 2^{n/2}$.

При $m \sim 2^{n-1}$ отсюда следует результат А. А. Сапоженко [78].

Теорема 4.9 [3]. *Для почти всех булевых функций f из $P^n_{m_1,m_2}$ верно, что*

$$l^s_{\text{кр}}(f) \asymp \left(1 + \frac{s+1}{\beta+1}\right) \cdot l_{\text{кр}}(f),$$

где $2^\beta = \frac{m_1+m_2}{m_1}$, *если* $m_1 + m_2 \gg \log n$, $\log \frac{m_2}{\log n} \leqslant \big(1 + O(1)\big) \log \frac{m_1}{\log n}$.

В ряде случаев (например, для почти всех булевых функций из P^n, если $s \to \infty$, а n специального вида) можно получить явную асимптотику. При $m_1 \sim m_2 \sim 2^{n-1}$, $s \gg \log\log n$ из этой теоремы вытекает результат Н. Н. Кузюрина [44].

Теорема 4.10 [3]. *Для почти всех операторов F из $P^{n,t}_m$ выполнено*

$$\frac{l_{\min}(F)}{\log \frac{m}{\log n}} \sim l_{\text{кр}}(F) \sim \left(1 + o(1) + \frac{Q(1)}{t}\right) \min\left\{m, \frac{mt}{\log \binom{n}{[\log \frac{m}{\log n}]}}\right\},$$

если $m \gg \log n$.

Рассмотрим задачу минимизации д. н. ф. с помощью машины Тьюринга. При работе с булевыми функциями из $\tilde{P}^n$ элементарные конъюнкции кодируются стандартным образом наборами длины n, код д. н. ф. составляется из кодов её элементарных конъюнкций, код булевой функции — из кодов совершенной д. н. ф. и совершенной д. н. ф. её отрицания. Пусть $T(f)$ — время работы машины T на коде булевой функций f.

Положим

$$T(n) = \max_{f \in \tilde{P}^n} T(f), \quad T(n, m_1, m_2) = \max_{f \in \tilde{P}^n_{m_1,m_2}} T(f).$$

Теорема 4.11 [3]. *Можно указать машины $T_{\min}$ и $T_{\text{кр}}$, вычисляющие по коду булевой функции f коды её минимальной и кратчайшей д. н. ф., и константу c,*

такие что

$$T_{\min}(n) + T_{\text{кр}}(n) \leqslant 2^{c\cdot n} \cdot 2^{2^{n+1}},$$
$$T_{\text{кр}}(n, m_1, m_2) \leqslant \big(n \cdot (m_1 + m_2)\big)^c \cdot 2^{2\cdot m_2} \cdot \min\{2^n, 2^{m_2}\},$$
$$T_{\min}(n, m_1, m_2) \leqslant \big(n \cdot (m_1 + m_2)\big)^c \cdot 2^{2\cdot m_2} \times$$
$$\times \big(\min\{2^n, 2^{m_2}\} + 2^{-m_2} \cdot \min\{2^n, 2^{2\cdot m_1}\}\big).$$

Сравнение полученных оценок с оценками для числа тупиковых д. н. ф. (см. [24]) показывает, что последнее, как правило, растёт существенно быстрее. Следовательно, алгоритмы, включающие перебор тупиковых д. н. ф., нельзя рассматривать в качестве универсального метода минимизации. Из этих оценок также легко извлекается ряд случаев полиномиальности задачи минимизации, например при условии, что $m_1 + m_2 = O(\log n)$. Однако в этих же условиях рост числа тупиковых д. н. ф. не является полиномиальным.

Как обычно, задачи A и B назовём полиномиально эквивалентными, если для любой машины T_A, решающей задачу A, найдутся машина T_B, решающая задачу B, и константа c, такие что $T_B(n) \leqslant 2^{cn} T_A(n)$, и наоборот.

Теорема 4.12 [3]. *Следующие задачи полиномиально эквивалентны*:

1) *по частичной булевой функции f найти некоторую её м. д. н. ф.*;
2) *по частичной булевой функции f найти некоторую элементарную конъюнкцию, входящую в д. н. ф. «сумма минимальных»*;
3) *по частичной булевой функции f и её элементарной конъюнкции K вычислить значение предиката «элементарная конъюнкция принадлежит д. н. ф. „сумма минимальных“»*;
4) *по частичной булевой функции f найти длину её м. д. н. ф.*

Эта теорема объясняет обнаруженное Ю. И. Журавлёвым (см. [24]) отсутствие локального критерия распознавания предиката «вхождение в сумму минимальных». Поскольку указанное распознавание по сложности фактически совпадает с решением задачи минимизации, применение локальных алгоритмов, базирующихся на этом предикате, в общем случае либо почти не понижает сложности перебора, либо сводится к нему же. Следующее утверждение достаточно хорошо иллюстрирует эту закономерность.

Теорема 4.13 [3].

1. *Для почти всех булевых функций f из P^n справедливы соотношения*

$$l_{\cup T}(f) = l_{\text{Q}}(f) = l_{\text{C}}(f) \sim l_{\text{A}}(f) \sim l_{\text{ко}}(f),$$
$$l_{\cap T}(f) \sim \sum_{r=[\log\log n]}^{[\log\log n]+1} \binom{n}{r} \cdot 2^r \cdot 2^{-2^r}.$$

2. *При $1 \leqslant m \leqslant 2^n - 2$ для почти всех булевых функций f из $\tilde{P}^n_{1,m}$ справедливы соотношения*

$$l_{\mathrm{Q}}(f) \sim l_{\cup T}(f) \sim l_{\mathrm{A}}(f), \quad l_{\mathrm{C}}(f) = O\big(l_{\mathrm{A}}(f)\big),$$
$$l_{\mathrm{C}}(f) \sim l^0_{\mathrm{C}}(f) + l^1_{\mathrm{C}}(f), \quad \textit{если} \quad m = O(2^n/n),$$
$$l_{\cup T} = l_{\mathrm{Q}}(f) = l_{\mathrm{C}}(f), \quad \textit{если} \quad m \geqslant (1+\varepsilon)\cdot 2^n(\sqrt{2}-1)/\sqrt{2},$$
$$l_{\mathrm{A}}(f) = l_{\mathrm{C}}(f), \quad \textit{если} \quad m \geqslant (1+\varepsilon)\cdot 2^{n-1},$$
$$l_{\cap T}(f) = 0, \quad \textit{если} \quad \log n \ll 2^n - m \leqslant 2^{n-1}(1-\varepsilon),$$

где $\varepsilon \in (0, 1/2)$.

3. *Если* $m \sim 2^{\varepsilon n}$, $\varepsilon \in [1/2, 1)$ *то для почти всех булевых функций* f *из* $P^n_{0,m}$ *справедливы соотношения*

$$\log\log\tau(f) \sim n, \quad \rho(f) = \left]\frac{1}{1-\varepsilon}\right[,$$
$$\log Y(f) \sim (1-\varepsilon)n \sim \dim f,$$

причём последнее соотношение достигается на почти всех тупиковых д. н. ф.

Ранее полученные результаты [24] следуют из первого пункта теоремы 4.13. Отметим, что при $m \sim 2^{\varepsilon n}$, $\varepsilon \in [1/2, 2/3]$, мы получаем из $P^n_{0,m}$ примеры массивных классов плотных булевых функций, причём существенно более простые, чем у Ю. Л. Васильева [19]. Для этих классов простейшие локальные алгоритмы имеют почти всегда нулевой эффект, а анализ не более чем 2^n частичных функций из кольца ранга 2 приводит к построению м. д. н. ф. Однако реализация кольцевого алгоритма требует анализа существенно большего числа частичных булевых функций. Следовательно, в этом случае трудоёмкость кольцевого алгоритма неприемлема. В то же время алгоритм наискорейшего спуска является для этих классов асимптотически оптимальным по порядку.

Следующие далее утверждения иллюстрируют тезис о модельности проблемы минимизации д. н. ф. Они были получены соответствующей адаптацией алгоритмов синтеза асимптотически оптимальных д. н. ф.

Пусть L_B — сложность реализации схемами из функциональных элементов в базисе B, а $\rho(B)$ — минимальный приведённый вес элементов этого базиса.

Теорема 4.14 [3]. *Для почти всех булевых функций* f *из* P^n_m *выполнено*

$$L_B(f) \sim \rho(B)\frac{m}{\log n},$$

если $\log n \ll m \leqslant n^{1+o(1)}$.

Отметим, что при $m = O(\log n)$ задача вырождается, так как в этом случае сложность соответствующих схем ограничена константой. В совокупности с результатами Л. А. Шоломова [93] эта теорема даёт окончательное решение задачи о зависимости сложности булевой функции от величины области определения. В рассматриваемом нами случае наблюдается лишь незначительное отличие схем от д. н. ф., однако оно есть.

Теорема 4.15 [3]. *Для почти всех булевых функций f из P_m^n выполнено*

$$l_{\min}(f) \sim \frac{m}{\log n} \cdot C(m,n)$$

для некоторой константы $1 \leqslant C(m,n) \leqslant 2$, если $\log n \ll m \leqslant n^{o(1)}$. Константа может быть вычислена эффективно.

Пусть $\chi(g)$ — хроматическое число графа g.

Теорема 4.16 [3]. *Для почти всех графов g с n вершинами и m рёбрами верно*

$$\chi(g) \sim \frac{\lambda \cdot n}{2\log n},$$

если $m = n(n-1)(1-2^{-\lambda}/2$, $\lambda - \ln\lambda \ll \log n$.

При $\lambda \sim 1$ из этой теоремы следует результат А. Д. Коршунова [42].

Пусть L^* — сложность реализации контактными схемами, не имеющими цепей с нулевой проводимостью.

Теорема 4.17 [3]. *Для почти всех булевых функций f из P^n справедливо соотношение*

$$L^*(f) \leqslant \bigl(1+o(1)\bigr)\frac{2^{n+1}}{\log\log n}.$$

Эта оценка совпадает по порядку с полученной С. Е. Кузнецовым [43] нижней оценкой.

5. Булевы уравнения

Многие задачи теории управляющих систем, дискретной оптимизации, распознавания образов, технической диагностики и др. (см. [16, 35]) естественно сводятся к решению систем булевых уравнений. При этом требуется найти или все решения системы, или часть их со специальными свойствами, или хотя бы одно решение. Как правило, уравнения в возникающих системах имеют достаточно регулярную структуру. Чаще всего они имеют вид $D = 1$, где D — д. н. ф. Так, например, задача построения тупиковых тестов приводит к исследованию систем булевых уравнений вида

$$\begin{cases} \sigma_{11}x_1 \vee \sigma_{12}x_2 \vee \ldots \vee \sigma_{1n}x_n = 1, \\ \quad\vdots \\ \sigma_{m1}x_1 \vee \sigma_{m2}x_2 \vee \ldots \vee \sigma_{mn}x_n = 1. \end{cases}$$

Проверка разрешимости системы булевых уравнений — NP-полная проблема, причём NP-полнота сохраняется даже в случае, если каждое уравнение является дизъюнкцией трёх членов, каждый из которых есть переменная или отрицание переменной. Поэтому разработка методов решения, исследование систем булевых уравнений представляет интерес не только в связи с конкретными приложениями, но и для изучения NP-полных проблем.

В [39, 99, 100, 110] исследовались вопросы классификации систем булевых уравнений, существования и единственности их решений, представления решений в параметрическом виде. Однако весьма актуальной остаётся задача разработки эффективных алгоритмов решения систем булевых уравнений.

Как и многие другие дискретные проблемы, задача нахождения решений булевых уравнений может быть решена тривиальной проверкой всех комбинаций значений переменных, однако это требует большого перебора. Существующие универсальные методы решения систем булевых уравнений [22,23,34—36,81,82, 87,101,102,112—114] не позволяют элиминировать этот перебор, причём остаётся открытым вопрос о принципиальной возможности такой элиминации.

Для обхода этих трудностей есть два традиционных пути. Первый заключается в разработке алгоритмов, ориентированных на достаточно узкие классы систем. Это направление активно развивается разными авторами (см. [26, 35, 46, 62, 79, 80, 92, 107]. Второй путь элиминации перебора состоит в построении алгоритмов малой трудоёмкости, находящих приближённое решение задачи. Возможности алгоритмов второго типа применительно к задаче решения систем булевых уравнений остались мало исследованными. Разработке этого подхода посвящены исследования Т. А. Игамбердыева, которые излагаются здесь.

Представляется также актуальным оценить, насколько эффективен каждый конкретный алгоритм. Такие попытки предпринимались, например, в [59].

Очевидно, что естественной нижней оценкой сложности любого алгоритма может служить число решений. Такой подход был применён, например, в [1, 2, 5, 25] при решении задачи поиска всех тупиковых тестов, где были разработаны алгоритмы, имеющие сложность, асимптотически равную числу тупиковых тестов для почти всех таблиц. С точки зрения такого подхода применительно к рассматриваемой задаче целесообразно вести работу в направлении поиска асимптотически оптимальных алгоритмов, число шагов которых эквивалентно числу решений системы булевых уравнений. Однако такая постановка пока затруднительна, поскольку, в отличие от тестовой ситуации, она связана с выработкой точного понятия шага, что пока ещё трудно сделать. Это связано также и с тем, что список разработанных алгоритмов решения булевых уравнений неширок и разнороден.

В [27, 28] исследовался вопрос о типичном значении числа решений таких систем булевых уравнений, где каждому уравнению соответствует случайная булева функция, без учёта того, в каком виде она задана.

Цель исследований Т. И. Игамбердыева — исследование систем булевых уравнений заданных в конкретных базисах, получение для них точных и асимптотических оценок числа решений и построение на основе этих оценок приближённых алгоритмов решения систем булевых уравнений. Была найдена точная формула для среднего числа решений систем булевых уравнений, заданных в виде д. н. ф., и при довольно общих предположениях о поведении метрических параметров системы установлена асимптотика числа решений для почти всех систем с заданным ростом параметров.

Был рассмотрен класс систем булевых уравнений, заданных в виде суммы по модулю 2 элементарных конъюнкций, и получена точная формула для среднего числа решений систем из заданного класса и асимптотическая оценка числа решений для почти всех систем с заданным ростом параметров.

Было показано, что в ряде случаев булевы функции, задаваемые сложными д. н. ф., можно достаточно хорошо аппроксимировать более простыми функциями.

Были описаны конкретные алгоритмы аппроксимации булевых функций и их применение при решении систем булевых уравнений.

Определим ряд понятий, необходимых для изложения основных результатов (основные определения были даны в разделе 4).

Пусть $f(x_1,\ldots,x_n)$ и $\hat{f}(x_1,\ldots,x_n)$ — булевы функции, причём $\mathcal{N}_f \subseteq \mathcal{N}_{\hat{f}}$. В этом случае говорят, что функция $\hat{f}(x_1,\ldots,x_n)$ аппроксимирует сверху функцию $f(x_1,\ldots,x_n)$.

В дальнейшем величину $|\mathcal{N}_{\hat{f}} \setminus \mathcal{N}_f|$ будем называть погрешностью, а $\Pi(\hat{f},f) \geqslant |\mathcal{N}_{\hat{f}} \setminus \mathcal{N}_f|$ — оценкой погрешности аппроксимации.

Пусть A — конечное множество, а φ — функция, ставящая в соответствие каждому $a \in A$ неотрицательное число $\varphi(a)$. Обозначим через

$$M\varphi = \frac{\sum\limits_{a\in A} \varphi(a)}{|A|}$$

среднее значение (или математическое ожидание) функции φ на множестве A, а через

$$D\varphi = \frac{\sum\limits_{a\in A} (\varphi(a) - M\varphi)^2}{|A|} -$$

дисперсию, или среднеквадратичное отклонение функции φ.

Пусть $A_s = \{a_1,\ldots,a_s\}$ — последовательность конечных множеств, а $P_s(Q)$ — число множеств $a \in A_s$, обладающих свойством Q. Говорят, что почти все элементы множества A_s при $s \to \infty$ обладают свойством Q, если $\lim\limits_{s\to\infty} \frac{P_s(Q)}{|A_s|} = 1$.

Будем рассматривать систему булевых уравнений

$$\Sigma = \begin{cases} f_1(x_1,\ldots,x_n) = 1, \\ \quad \vdots \\ f_m(x_1,\ldots,x_n) = 1. \end{cases}$$

Рассмотрим класс $\Gamma(n,m,t,r)$ систем булевых уравнений, заданных в виде д. н. ф., со следующими параметрами: число переменных равно n, число уравнений в каждой системе равно m, число элементарных конъюнкций во всех д. н. ф., соответствующих уравнениям, одинаково и равно t, число букв во всех элементарных конъюнкциях одинаково и равно r. Изучался вопрос о типичном значении числа решений систем Σ из класса $\Gamma(n,m,t,r)$.

Пусть G — число решений системы $\Sigma \in \Gamma(n,m,t,r)$, а MG — среднее значение числа решений для систем из $\Gamma(n,m,t,r)$.

Справедливо следующее утверждение. Среднее значение числа решений системы булевых уравнений $\Sigma \in \Gamma(n,m,t,r)$ равно $MG = 2^n(1-(1-2^{-r})^t)^m$.

Теорема 5.1. *При выполнении условий $r \to \infty$, $MG \to \infty$, $t2^{-r} - n\ln n \gg n$ или условий $r \to \infty$, $MG > 2^{\delta n}$, где $\delta \in (0,1)$, $t2^{-r} \gg \ln n$, для почти всех систем булевых уравнений $\Sigma \in \Gamma(n,m,t,r)$ число решений асимптотически равно*

$$2^n(1-(1-2^{-r})^t)^m.$$

Рассмотрим класс $\Pi(n,m,t,r)$ систем булевых уравнений, заданных в виде суммы по модулю 2 элементарных конъюнкций, со следующими параметрами: число переменных равно n, число уравнений в каждой системе равно m, число слагаемых во всех суммах, соответствующих уравнениям, одинаково и равно t, число букв в каждом слагаемом равно r. Изучался вопрос о типичном значении числа решений систем T из класса $\Pi(n,m,t,r)$.

Пусть Q — число решений системы $T \in \Pi(n,m,t,r)$, а MQ — среднее значение числа решений для системы из $\Pi(n,m,t,r)$.

Теорема 5.2. *Среднее значение числа решений системы булевых уравнений $T \in \Pi(n,m,t,r)$ равно $MQ = 2^{n-m}(1-(1-2^{1-r})^t)^m$.*

Пусть $n \to \infty$ и все параметры являются функциями от n.

Теорема 5.3. *Для любого $\delta \in (0,1)$ найдётся такое $\varepsilon(\delta) \in (0,1)$, что при выполнении условий $t \ll \left(\frac{4}{1+\varepsilon(\delta)}\right)^r$, $m \ll \left(\frac{2}{1+\varepsilon(\delta)}\right)^r$, $MQ > 2^{\delta n}$ для почти всех систем булевых уравнений $T \in \Pi(n,m,t,r)$ число решений асимптотически равно*

$$2^{n-m}(1-(1-2^{1-r})^t)^m.$$

Следствие 5.1. *Если выполняются условия теоремы 5.2, то при $m(1-2^{1-r})^t = o(1)$ для почти всех булевых уравнений $T \in \Pi(n,m,t,r)$ число решений асимптотически равно 2^{n-m}.*

Сложность решения системы уравнений, где булевы функции заданы д. н. ф.,

$$\Sigma = \begin{cases} K_1^1 \vee K_2^1 \vee \ldots \vee K_{t_1}^1 = 1, \\ \quad \vdots \\ K_1^m \vee K_2^m \vee \ldots \vee K_{t_m}^m = 1, \end{cases}$$

с помощью алгоритмов, предлагаемых, например, в [34], зависит от длин уравнений t_i $(1 \leqslant i \leqslant m)$, уменьшая которые, можно существенно упростить решение. В связи с эти возникает задача аппроксимации булевых функций.

Можно показать, что в ряде случаев булевы функции, задаваемые сложными д. н. ф., можно достаточно хорошо аппроксимировать более простыми функциями.

Поставим в соответствие д. н. ф. $D(x_1,\ldots,x_n)$ граф $G(D)$, вершинами которого являются элементарные конъюнкции из д. н. ф. $D(x_1,\ldots,x_n)$, причём две вершины графа соединены только тогда, когда они имеют общие переменные. Назовём д. н. ф. $D(x_1,\ldots,x_n)$ ациклической, если граф $G(D)$ является лесом.

Пусть $\alpha(f)=\frac{2^n-|\mathcal{N}_f|}{2^n}$, где n — число переменных функции f, т. е. это доля нулей функции f.

Пусть $D(R,\sigma,t)$ — это множество всех ациклических д. н. ф. длины t, таких что число букв в каждой элементарной конъюнкции не более R и число букв, общих у двух элементарных конъюнкций, не более σ.

Пусть $\alpha(R,\sigma,t)$ — это максимальная доля нулей для д. н. ф. из класса $D(R,\sigma,t)$.

Пусть

$$a=(1-2^{\sigma-R}),\quad b=2^{\sigma-R}-2^{-R},\quad \beta_1=\frac{a}{2}+\sqrt{\frac{a^2}{4}+b},\quad \beta_2=\frac{a}{2}-\sqrt{\frac{a^2}{4}+b}.$$

Ясно, что

$$\alpha(R,\sigma,1)=1-2^{-R},\quad \alpha(R,\sigma,2)=1-2^{1-R}+2^{\sigma-2R}.$$

Теорема 5.4. *Имеет место соотношение*

$$\alpha(R,\sigma,t)=\frac{1}{\beta_1-\beta_2}\big((\alpha(R,\sigma,2)-\alpha(R,\sigma,1)\beta_2)\beta_1^{t-1}-(\alpha(R,\sigma,2)-\alpha(R,\sigma,1)\beta_1)\beta_2^{t-1}\big).$$

Следствие 5.2. *Пусть R и σ — функции от t, причём $\sigma\to\infty$ и $R-\sigma\to\infty$ при $t\to\infty$. Тогда $\alpha(R,\sigma,t)\sim(1-2^{\sigma-R})^t$.*

Пусть $D(R,t)$ — множество всех д. н. ф. длины t, у которых число букв в элементарных конъюнкциях не превышает R.

Теорема 5.5. *Для любой д. н. ф. $D\in\bigcup\limits_{t=0}^{\infty}D(R,t)$ найдётся д. н. ф. $\hat{D}$ длины не более t_0, такая что $\mathcal{N}_D\subseteq\mathcal{N}_{\hat{D}}$, причём*

$$\alpha(D)-\alpha(\hat{D})\leqslant t_0(1-2^{-R})^{\sqrt[R]{t_0-1}}2^{R^2}e^2\left(R!+\left(\frac{R}{e}\right)^R\right).$$

Были предложены конкретные алгоритмы аппроксимации булевых функций и алгоритм решения систем булевых уравнений. Пусть имеется булева функция $f(x_1,\ldots,x_n)$, заданная с помощью д. н. ф. $D(x_1,\ldots,x_n)=K_1\vee K_2\vee\ldots\vee K_t$, где K_i $(1\leqslant i\leqslant t)$ — элементарная конъюнкция ранга R. Алгоритмы $\mathfrak{U}_1$ и $\mathfrak{U}_2$ строят аппроксимирующую функцию $\hat{f}(x_1,\ldots,x_n)$, заданную с помощью д. н. ф. $\hat{D}(x_1,\ldots,x_n)=\hat{K}_1\vee\hat{K}_2\vee\ldots\vee\hat{K}_{t_0}$, такую что $\mathcal{N}_f\subseteq\mathcal{N}_{\hat{f}}$, причём $t_0\leqslant\hat{t}$, где $\hat{t}$ — фиксированный наперёд заданный параметр; по ходу работы алгоритма производится подсчёт оценки величины возможной погрешности $\Pi(D,\hat{D})\geqslant$ $\geqslant(|\mathcal{N}_{\hat{f}}|-|\mathcal{N}_f|)$. Алгоритмы $\mathfrak{U}_1$ и $\mathfrak{U}_2$ основаны на результатах, изложенных выше. Они отличаются друг от друга сложностью реализации и точностью приближения.

Был описан алгоритм, основанный на применении аппроксимации булевых функций с помощью одного из алгоритмов $\mathfrak{U}_1$ или $\mathfrak{U}_2$. Пусть имеется система булевых уравнений, заданных в виде д. н. ф.

$$\Sigma = \begin{cases} f_1(\tilde{x}) = 1, \\ \quad \vdots \\ f_m(\tilde{x}) = 1. \end{cases}$$

Аппроксимируя описанным выше способом функции f_i $(1 \leqslant i \leqslant m)$, можно получить систему

$$\hat{\Sigma} = \begin{cases} \hat{f}_1(\tilde{x}) = 1, \\ \quad \vdots \\ \hat{f}_m(\tilde{x}) = 1. \end{cases}$$

Число решений системы $\hat{\Sigma}$, которые могут не являться решениями Σ, оценивается с помощью теоремы 5.5. Трудоёмкость решения системы $\hat{\Sigma}$, ввиду меньших размеров, как правило, существенно ниже трудоёмкости решения системы Σ. Поэтому предлагается следующая процедура решения систем булевых уравнений:

1) по Σ строится $\hat{\Sigma}$;
2) решается $\hat{\Sigma}$;
3) из решений $\hat{\Sigma}$ отбираются решения Σ путём проверки.

Литература

[1] Андреев А. Е. О качественных и метрических свойствах тестовых алгоритмов: Автореф. дис.... канд. физ.-мат. наук. — М., 1981.

[2] Андреев А. Е. О тупиковых и минимальных тестах // ДАН СССР. — 1981. — Т. 256, № 3. — С. 521—524.

[3] Андреев А. Е. К проблеме минимизации дизъюнктивных нормальных форм // ДАН СССР. — 1984. — Т. 274, № 2. — С. 265—269.

[4] Андреев А. Е. О синтезе самокорректирующихся управляющих систем // ДАН СССР. — 1984. — Т. 277, № 3. — С. 521—525.

[5] Андреев А. Е. Об асимптотическом поведении числа тупиковых тестов и минимальной длины теста для почти всех таблиц // Проблемы кибернетики. — 1984. — Вып. 41. — С. 117—141.

[6] Андреев А. Е. Метод бесповторной редукции синтеза самокорректирующихся схем // ДАН СССР. — 1985. — Т. 283, № 2. — С. 265—269.

[7] Андреев А. Е. О синтезе контактных многополюсников // 7-я Всесоюзная конференция «Проблемы теоретической кибернетики», тезисы докладов. — Иркутск, 1985. — С. 9—10.

[8] Андреев А. Е. О синтезе топологических функциональных сетей: Препринт № 259 ИПМех АН СССР и МГУ им. М. В. Ломоносова. — 1985.

[9] Андреев А. Е. О синтезе функциональных сетей: Дис.... докт. физ.-мат. наук. — М., 1985.

[10] Андреев А. Е. О сложности монотонных функций // Вестн. Моск. ун-та. Сер. 1, Математика, механика. — 1985. — № 4. — С. 83—87.

[11] Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций: Препринт № 248 ИПМех АН СССР и МГУ. — 1985.

[12] Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // ДАН СССР. — 1985. — Т. 281, № 2. — С. 1033—1037.

[13] Андреев А. Е. Универсальный принцип самокорректирования // Мат. сб. — 1985. — Т. 127 (169), № 6. — С. 147—172.

[14] Андреев А. Е. Об одном методе получения более чем квадратичных эффективных нижних оценок сложности π-схем // Вестн. Моск. ун-та. Сер. 1, Математика, механика. — 1987. — № 1. — С. 70—73.

[15] Андреев А. Е. Об одном методе получения эффективных нижних оценок монотонной сложности // Алгебра и логика. — 1987. — № 1. — С. 3—26.

[16] Бибило П. Н., Енин С. В. Декомпозиция булевой функции с минимальным числом существенных аргументов подфункций // Изв. АН СССР. Техн. киб. — 1980. — № 3. — С. 123—129.

[17] Васильев Ю. Л. О сравнении сложности тупиковых и минимальных дизъюнктивных нормальных форм // Проблемы кибернетики. — 1963. — Вып. 10. — С. 5—61.

[18] Васильев Ю. Л. К вопросу о числе тупиковых и минимальных дизъюнктивных нормальных форм // Дискретный анализ. Вып. 2. — Новосибирск: Ин-т математики СО АН СССР, 1964. — С. 3—9.

[19] Васильев Ю. Л. Массивные классы плотных булевых функций // Методы дискретного анализа в синтезе управляющих систем. Вып. 32. — Новосибирск: Ин-т математики СО АН СССР, 1978. — С. 21—33.

[20] Викулин А. П. Оценка числа конъюнкций в сокращённой д. н. ф. // Проблемы кибернетики. — 1974. — Вып. 19. — С. 151—166.

[21] Глаголев В. В. Оценка сложности сокращённой дизъюнктивной нормальной формы для почти всех функций алгебры логики // ДАН СССР. — 1964. — Т. 158, № 4. — С. 770—773.

[22] Горелик А. Л., Скрипкин В. А. Методы распознавания. — М.: Высшая школа, 1984.

[23] Григорян Ю. Г. Алгоритм решения системы логических уравнений // ЖВМ и МФ. — 1962. — Т. 2, № 1. — С. 186—189.

[24] Дискретная математика и математические вопросы кибернетики. Т. 1 / Под общ. ред. С. В. Яблонского, О. Б. Лупанова. — М.: Наука, 1974.

[25] Дюкова Е. В. Об асимптотически оптимальном алгоритме построения тупиковых тестов для бинарных таблиц // Проблемы кибернетики. — 1978. — Вып. 34. — С. 169—186.

[26] Егиазарян Э. В. Об одном классе систем булевых уравнений // ЖВМ и МФ. — 1976. — № 4. — С. 1073—1077.

[27] Егиазарян Э. В. Оценки, связанные с числом решений систем булевых уравнений // Вопросы кибернетики, комбинаторный анализ и теория графов. — 1980. — Вып. 64. — С. 124—130.

[28] Егиазарян Э. В. Метрические свойства систем булевых уравнений // Докл. АН Арм. ССР. — 1981. — Т. 72. № 2. — С. 67—72.

[29] Журавлёв Ю. И. Алгоритмы упрощения дизъюнктивных нормальных форм конечного индекса // ДАН СССР. — 1961. — Т. 139, № 6. — С. 1329—1331.

[30] Журавлёв Ю. И. Теоретико-множественные методы алгебры логики // Проблемы кибернетики. — 1962. — Вып. 8. — С. 5—14.

[31] Журавлёв Ю. И. Оценка сложности локальных алгоритмов для некоторых экстремальных задач на конечных множествах // ДАН СССР. — 1964. — Т. 158, № 5. — С. 1018—1021.

[32] Журавлёв Ю. И. Локальные алгоритмы вычисления информации // Кибернетика. — 1965. — № 1. — С. 12—19.

[33] Закревский А. Д. Алгоритмы синтеза дискретных автоматов. — М.: Наука, 1971.

[34] Закревский А. Д. Логические уравнения. — Минск: Наука и техника, 1975.

[35] Кабулов А. В. Приложения дискретной математики к кибернетике. — Ташкент: ФАН, 1982.

[36] Кабулов А. В., Игамбердыев Т. М. Об одном подходе к решению систем логических уравнений // Вопросы вычислительной и прикладной математики. — 1984. — Вып. 74. — С. 68—73.

[37] Кириенко Г. И. О самокорректирующихся схемах из функциональных элементов // Проблемы кибернетики. — 1964. — Вып. 12. — С. 29—37.

[38] Кириенко Г. И. Синтез самокорректирующихся схем из функциональных элементов для случая растущего числа ошибок в схеме // Дискретный анализ. Вып. 16. — Новосибирск: Ин-т математики СО АН СССР, 1970. — С. 38—43.

[39] Коваленко И. Н. К вычислению вероятности единственности решения системы случайных нелинейных булевых уравнений // Кибернетика. — 1973. — № 3. — С. 12—15.

[40] Константинов Р. М., Королёва З. Е. Применение тестовых алгоритмов к задачам геологического прогнозирования // Распознавание образов. Труды Международного симпозиума 1971 г. по практическим применениям методов распознавания образцов ВЦ АН СССР. — М., 1973. — С. 194—204.

[41] Коршунов А. Д. О числе монотонных булевых функций // Проблемы кибернетики. — 1981. — Вып. 38. — С. 5—108.

[42] Коршунов А. Д. О хроматическом числе n-вершинных графов // Методы дискретного анализа в теории булевых функций. Вып. 35. — Новосибирск: Ин-т математики СО АН СССР, 1980. — С. 15—44.

[43] Кузнецов С. Е. // Дискретный анализ. Вып. 37. — Новосибирск: Ин-т математики СО АН СССР, 1981. — С. 51—64.

[44] Кузюрин Н. Н. // Комбинаторно-алгебраические методы в прикладной математике. — Горький, 1980. — С. 88—98.

[45] Курош А. Г. Курс высшей алгебры. — М.: Наука, 1975.

[46] Леонтьев В. К. Нурлыбаев А. Н. Об одном классе систем булевых уравнений // ЖВМ и МФ. — 1975. — Т. 15, № 6. — С. 1568—1579.

[47] Лупанов О. Б. О вентильных и контактно-вентильных схемах // ДАН СССР. — 1956. — Т. 111, № 6. — С. 1171—1174.

[48] Лупанов О. Б. О синтезе контактных схем // ДАН СССР. — 1958. — Т. 119, № 1. — С. 23—26.

[49] Лупанов О. Б. Об одном методе синтеза схем // Изв. высш. учебн. завед. Радиофизика. — 1958. — Т. 1, № 1. — С. 120—140.

[50] Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. — 1960. — Вып. 3. — С. 61—80.

[51] Лупанов О. Б. О принципе локального кодирования и реализации функций из некоторых классов схемами из функциональных элементов // ДАН СССР. — 1961. — Т. 140, № 2. — С. 322—325.

[52] Лупанов О. Б. Об одном классе схем из функциональных элементов (формулы с конечной памятью) // Проблемы кибернетики. — 1962. — Вып. 7. — С. 61—114.

[53] Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. — 1963. — Вып. 10. — С. 63—97.

[54] Лупанов О. Б. О сложности реализации функций алгебры логики релейно-контактными схемами // Проблемы кибернетики. — 1964. — Вып. 11. — С. 25—47.

[55] Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. — 1965. — Вып. 14. — С. 31—110.

[56] Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. — 1970. — Вып. 23. — С. 43—81.

[57] Мадатян Х. А. О синтезе схем корректирующих размыканий контактов // ДАН СССР. — 1964. — Т. 159, № 2. — С. 290—293.

[58] Марков А. А. О минимальных контактно-вентильных двуполюсниках для монотонных симметрических функций // Проблемы кибернетики. — 1962. — Вып. 8. — С. 117—122.

[59] Матросова А. Ю. Об объёме вычислений при решении булевых уравнений // Мат. сб. Томского ун-та. — 1975. — Вып. 2. — С. 120—128.

[60] Нгуен Ким Ань. Некоторые характеристики алгоритмов минимизации булевых функций // Тезисы докладов IV Всесоюзной конференции по математической логике. — Тбилиси, 1982.

[61] Нгуен Ким Ань. О некоторых характеристиках алгоритмов минимизации булевых функций // ДАН СССР. — 1982. — Т. 267. — С. 1058—1062.

[62] Нечепуренко М. Н. Элементы булева интервального анализа // Системное моделирование в информатике. — Новосибирск: ВЦ СО АН СССР, 1985. — С. 37—61.

[63] Нечипорук Э. И. Об одной булевской функции // ДАН СССР. — 1966. — Т. 169, № 4. — С. 765—767.

[64] Нечипорук Э. И. О корректировании обрывов в вентильных и контактных схемах // Кибернетика. — 1968. — № 5. — С. 40—48.

[65] Нечипорук Э. И. О топологических принципах самокорректирования // ДАН СССР. — 1968. — Т. 179, № 4. — С. 786—789.

[66] Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. — 1969. — Вып. 21. — С. 5—102.

[67] Нечипорук Э. И. Об одной булевской матрице // Проблемы кибернетики. — 1969. — Вып. 21. — С. 237—240.

[68] Нечипорук Э. И. О реализации дизъюнкции и конъюнкции в некоторых монотонных базисах // Проблемы кибернетики. — 1970. — Вып. 23. — С. 291—294.

[69] Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. — 1973. — Вып. 26. — С. 19—26.

[70] Окольнишникова Е. А. Монотонная булева система с квадратичной сложностью реализации в базисе $\{\&, \vee, 0, 1\}$ // Дискретный анализ. Вып. 41. — Новосибирск: Ин-т математики СО АН СССР, 1984. — С. 81—98.

[71] Ортюков С. И. Об оценках функции Шеннона для схем из ненадёжных функциональных элементов // Проблемы кибернетики. — 1983. — Вып. 40. — С. 269.

[72] Потапов Ю. Г., Яблонский С. В. О синтезе самокорректирующихся контактных схем // ДАН СССР. — 1960. — Т. 134, № 3. — С. 543—547.

[73] Разборов А. А. Нижние оценки монотонной сложности логического перманента // Мат. заметки. — 1985. — Т. 37, № 6. — С. 887—908.

[74] Разборов А. А. Нижние оценки монотонной сложности некоторых булевых функций // ДАН СССР. — 1985. — Т. 281, № 4. — С. 798—801.

[75] Редькин Н. П. О самокорректировании контактных схем // Проблемы кибернетики. — 1978. — Вып. 33. — С. 119—138.

[76] Редькин Н. П. О самокорректировании контактных схем. II // Проблемы кибернетики. — 1979. — Вып. 36. — С. 195—208.

[77] Сапоженко А. А. Метрические свойства почти всех функций алгебры логики // Дискретный анализ. Вып. 10. — Новосибирск: Ин-т математики СО АН СССР, 1967. — С. 91—119.

[78] Сапоженко А. А. Порядок окрестности максимальных интервалов у почти всех булевых функций // ДАН СССР. — 1968. — Т. 180, № 1. — С. 32—35.

[79] Сафарян А. А. NP-полнота задачи разбиения систем булевых уравнений на минимальные блоки. — М.: ВЦ АН СССР, 1984.

[80] Сафарян А. А. О решении систем булевых уравнений, возникающих при построении тестов и систем нельсоновского типа // ЖВМ и МФ. — 1984. — Т. 24, № 10. — С. 1590—1595.

[81] Свобода А., Чулик К. Алгоритм для решения булевых уравнений // Автоматика и телемеханика. — 1964. — Т. 25, № 3. — С. 374—381.

[82] Сериков Ю. А. Алгебраический метод решения логических уравнений // Изв. АН СССР. Техн. киб. — 1972. — № 2. — С. 114—124.

[83] Соловьёв Н. А. Тесты. — Новосибирск: Наука, 1978.

[84] Субботовская Б. А. О реализации линейных функций формулами в базисе $\&, \vee, \neg$ // ДАН СССР. — 1961. — Т. 136, № 3. — С. 553—555.

[85] Улиг Д. О синтезе самокорректирующихся схем из функциональных элементов с малым числом ненадёжных элементов // Мат. заметки. — 1974. — Т. 15, № 6. — С. 937—944.

[86] Улиг Д. Самокорректирующиеся контактные схемы, исправляющие большое число ошибок // ДАН СССР. — 1978. — Т. 241, № 6. — С. 1273—1276.

[87] Уткин А. А. Решение логических уравнений // Автоматизация логического проектирования. — Минск: ИТК АН БССР, 1982. — С. 41—58.

[88] Феллер В. Введение в теорию вероятностей и её приложения. Т. 1. — М.: Мир, 1984.

[89] Холл М. Комбинаторика. — М.: Мир, 1970.

[90] Храпченко В. М. Об одном методе получения нижних оценок сложности π-схем // Мат. заметки. — 1971. — Т. 10, № 1. — С. 83—92.

[91] Храпченко В. М. Нижние оценки сложности схем из функциональных элементов (обзор) // Кибернет. сборник. — 1984. — Вып. 21. — С. 3—54.

[92] Чистов В. П. О системах логических уравнений. — Свердловск, 1984. — Деп. в Ин-т мат. и мех. Урал. науч. центра АН СССР.

[93] Шоломов Л. А. О реализации недоопределённых булевых функций схемами из функциональных элементов // Проблемы кибернетики. — 1969. — Вып. 21. — С. 215—226.

[94] Яблонский С. В. О классах функций алгебры логики, допускающих простую схемную реализацию // Успехи мат. наук. — 1957. — Т. 12, № 6. — С. 189—196.

[95] Яблонский С. В. Функциональные построения в k-значной логике // Тр. МИАН СССР. — 1958. — Т. 51. — С. 5—142.

[96] Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. — 1959. — Вып. 2. — С. 75—121.

[97] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

[98] Яблонский С. В., Демидова Н. Г., Константинов Р. М., Королёва З. Е., Кудрявцев В. Б., Сиротская С. В. Тестовый подход к оценке геолого-структурных факторов и масштабов оруднения // Геология рудных месторождений. — 1971. — Т. 13, № 2. — С. 30—42.

[99] Banković D. Solving systems of arbitraty equations // Discrete Math. — 1983. — Vol. 46, no. 3. — P. 305—309.

[100] Bochman D., Posthoff Ch. Die Behandlung Boolescher Gleichungen mit Hilfe des Booleschen Differentialkalküls // Probleme und Ergebnisse aus der Arbeitsgruppe Kybernetik / Informationsverarbeitung der Klasse Mathematik 1977/78. — Berlin: Akademie, 1981.

[101] Brown F. M. Reduced solutions of Boolean equations // IEEE Trans. Comput. — 1970. — Vol. 19. — P. 976—981.

[102] Föllinger O. Boolesche Gleichungen, Lösung und Anwendungen. I. Die Lösung Boolescher Gleichungen // Elektron. Datenverarb. — 1963. — S. 253—260.

[103] Katona G. A theorem of finite sets // Theory of Graph. — New York, 1969. — P. 187—208.

[104] Mehlhorn K. Some remarks on Boolean sums // Acta Inform. — 1979. — Vol. 12. — P. 371—375.

[105] Mehlhorn K., Galil Z. Monotone switching circuits and Boolean matrix product // Computing. — 1976. — Vol. 16. — P. 99—111.

[106] Paterson M. S. Complexity of monotone networks for Boolean matrix product // Theor. Comput. Sci. — 1975. — Vol. 1. — P. 13—20.

[107] Peeva K. Systems of linear equations over a bounded chain // Acta Cybernet. — 1985. — Vol. 7, no. 2. — P. 195—202.

[108] Pipendger N. On another Boolean matrix: IBM Research Report RC-6914. — 1977.

[109] Pratt V. P. The effect of basis on size of Boolean expressions // Proc. of 16th Ann. Symp. Found. of Comput. Sci. — New York, 1975. — P. 119—121.

[110] Skala H. The general solution of an arbitrary Boolean equations // Amer. Math. Monthly. — 1967. — Vol. 74, no. 9. — P. 1074—1077.

[111] Shannon C. E. The synthesis of two-terminal swithing circuits // Bell System Tech. J. — 1949. — Vol. 28, no. 1. — P. 59—98.

[112] Svoboda A. An algorithm for solving Boolean equations // IEEE Trans. Electron. Comput. — 1963. — No. 12. — P. 557—559.

[113] Tapia M. A., Tucker J. H. Complete solution of Boolean equations // IEEE Trans. Comput. — 1980. — Vol. 29, no. 7. — P. 662—665.

[114] Vaquero A., Iglesias M. Aplicación del método de resolución de S.E.B. de Tapia & Tucker a la síntesis de funciones múltiples // Rev. Inform. Automát. — 1983. — Vol. 16. — P. 35—39.

[115] Wegener I. Switching functions whose monotone complexity in nearly quadratic // Theor. Comput. Sci. — 1979. — Vol. 9. — P. 83—97.