

О сложности алгоритмов*

В. Б. Кудрявцев, А. Е. Андреев

Излагаются некоторые результаты по теории сложности схемных и тьюринговых алгоритмов, полученные А. Е. Андреевым, Нгуен Ким Ань и Т. М. Игамбердыевым.

Введение

Алгоритмы применяются к двум основным объектам — конечным и бесконечным множествам.

В первом случае имеют дело со схемными вычислениями, во втором — с тьюринговыми или программными вычислениями.

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.

Тьюринговые вычисления используются, как правило, при анализе свойств счетных множеств. Особый интерес вызывают вычисления, связанные с анализом сложности строения семейств конечных множеств. Примерами таковых являются 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.

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

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

Здесь на основе обобщения метода Б. А. Субботовской (1961, [110]) и с использованием идеи универсальной функции Э. И. Нечипорука (1966, [111]) построен пример функции, имеющий 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, 1971, [112]).

Пусть

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

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

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

что

$$1 \leq j_{i,1} \leq j_{i,2} \leq \dots \leq j_{i,s} \leq l, \quad i = 1, 2, \dots, k;$$

$$\sigma_{i,t} \in \{0, 1\}, \quad i = 1, 2, \dots, k, \quad t = 1, 2, \dots, s.$$

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

Лемма 1.1 ([114]). *Если $k \geq 1$, $l \geq 5$, то для любой булевой функции $f(\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_k)$ такой, что $L(f) \geq 2$, существует $\tilde{\alpha}$ из $X_1^{k,l}$, такое, что*

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

где

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

Лемма 1.2 ([114]). Существует такая положительная константа c_0 , что если $k \geq 1$, $l \geq r \geq 4$, то для любой булевой функции $f(\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_k)$ существует $\tilde{\alpha}$ из $X_{l-r}^{k,l}$, такое, что

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

Лемма 1.3 ([114]). Если $k \geq 1$, $l \geq r \geq 4$, функции $g_1(\tilde{x}_1), \dots, g_k(\tilde{x}_k)$ не обращаются в константу ни на каком интервале размерности r и $f = g(g_1(\tilde{x}_1), \dots, g_k(\tilde{x}_k))$, то

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

Пусть k — натуральное, $k \geq 3$ и $l = \lceil 2^k/k \rceil$, $n = 2^k + k \cdot l$. Пусть набор \tilde{y} состоит из 2^k различных переменных $y_{\sigma_1, \dots, \sigma_k}$, $\sigma_1, \dots, \sigma_k \in \{0, 1\}$, не входящих в $\tilde{x}_1, \dots, \tilde{x}_k$. Полагаем

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

Теорема 1.1 ([114]). Имеет место

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

где C — положительная константа.

2. Эффективные нижние оценки сложности монотонных функций

Рассматривается задача 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 (А. А. Марков [95], Э. И. Нечипорук [96, 97], М. S. Paterson [98], V. R. Pratt [99], N. Pipenger [100], Z. Galil [101], К. Mehlohn [101, 102], I. Vegener [103], Е. А. Окольнішнікова [104]).

В 1984 году А. Е. Андреев предложил метод позволяющий получать почти экспоненциальные нижние оценки монотонной сложности ($2^{n^{\frac{1}{3}-o(1)}}$, где n — число переменных).

Одновременно А. А. Разборов [107, 108] предложил метод, позволивший получить оценку вида $2^{O(\log^2 n)}$.

В работе [109] А. Е. Андреев предложил усовершенствованный вариант своего метода. Основным результатом является общая оценка сложности монотонной булевой функции через некоторые ее комбинаторные характеристики. Приведен пример последовательности функций, для которых полученная оценка имеет рост $2^{n^{\frac{1}{3}-o(1)}}$, где n — число переменных. Эта оценка остается 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 называем схему в базисе $\{\&, \vee\}$, входным полюсам которой приписаны функции из множества \mathcal{A} . Через $L_{\mathcal{A}}(f)$ обозначаем 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

$$L_{\{\&, \vee, 0, 1\}}^c(f) \geq L_{\mathcal{A}}(f),$$

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

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

$$\begin{aligned} \rho(x, x) &= 0, \\ \rho(x, y) &= \rho(y, x), \end{aligned}$$

$$\rho(x, z) \leq \rho(x, y) + \rho(y, z).$$

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

$$\{\tilde{\alpha} | f_1(\tilde{\alpha}) \neq f_2(\tilde{\alpha})\} \subseteq \{\tilde{\alpha} | f_3(\tilde{\alpha}) \neq f_4(\tilde{\alpha})\} \implies \rho(f_1, f_2) \leq \rho(f_3, f_4).$$

Очевидно, что для любой монотонной псевдометрики ρ справедливо неравенство

$$\rho(F(u_1, \dots, u_n, f_1), F(u_1, \dots, u_n, f_2)) \leq \rho(f_1, f_2).$$

Полагаем

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

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

Последовательность функций f_1, f_2, \dots, f_k называем правильной, если для любого i из $\{1, 2, \dots, k-1\}$ либо $f_i \leq f_{i+1}$, либо $f_i \geq f_{i+1}$. Полагаем

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

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

Записываем

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

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

$$\rho_1^\uparrow(f_1, \dots, f_k) \leq a_1, \quad \rho_2^\downarrow(f_1, \dots, f_k) \leq a_2.$$

Если $\mathcal{B}_1, \mathcal{B}_2 \subseteq \mathcal{P}^{<n>}$ и для любой f из \mathcal{B}_1 существует g из \mathcal{B}_2 такая, что $[\rho_1, \rho_2](f, g) \leq (a_1, a_2)$, то записываем

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

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 ([109]). *Если*

$$f \in \mathcal{P}^{<n>}, \quad \mathcal{A} \subseteq \mathcal{P}^{<n>}, \quad L_{\mathcal{A}}(f) \geq 1,$$

и для монотонных псевдометрик ρ_1, ρ_2 выполнено

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

то существует g из $\mathcal{P}^{<n>}$ такая, что

$$\begin{aligned} L_{\mathcal{A}}(g) &\leq L_{\mathcal{A}}(f) - 1, \\ \rho_1(0, g) &\geq \rho_1(0, f) - a_1, \\ \rho_2(1, g) &\geq \rho_2(1, f) - a_2. \end{aligned}$$

Теорема 2.1 ([109]). *Если*

$$f \in \mathcal{P}^{<n>}, \quad \mathcal{A} \subseteq \mathcal{P}^{<n>}, \quad L_{\mathcal{A}}(f) \geq 0$$

и для монотонных псевдометрик ρ_1, ρ_2 выполнено

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

то

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

2.2. Лемма о системе конечных множеств

Лемма 2.2 ([109]). *Если \mathcal{R} — система непустых попарно невлости-мых множеств мощности не более s и*

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

то существуют такие различные V_1, V_2, \dots, V_r из \mathcal{R} и множество V_0 (быть может пустое), что $V_0 \subseteq V_1 \wedge V_2$ и множества $V_1 \setminus V_0, \dots, V_r \setminus V_0$ 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 $U_n = \{u_1, u_2, \dots, u_n\}$, причем

$$\begin{aligned}\mathcal{F}(\emptyset) &= \emptyset, \quad \mathcal{F}(W) = U_n, \\ \mathcal{F}(w_1) \cup \mathcal{F}(w_2) &= \mathcal{F}(w_1 \cup w_2), \\ \mathcal{F}(w_1) \cap \mathcal{F}(w_2) &= \mathcal{F}(w_1 \cap w_2).\end{aligned}$$

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

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

Если $f \in M^{<n>}$, 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 $\sum_f^{\mathcal{F}}$ обозначаем систему всех простых для f множеств. Ясно, что для всех f из $M(\mathcal{F})$ верно

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

(пустая дизъюнкция считается равной 0).

Через $l_s^{\mathcal{F}}$ обозначаем число непустых множеств из $\sum_f^{\mathcal{F}}$ мощности не более s , а через $R^{\mathcal{F}}(f)$ — максимальную мощность множеств из $\sum_f^{\mathcal{F}}$, где $f \in M^{<n>}$. Полагаем $R^{\mathcal{F}}(0) = 0$.

Через $M(\mathcal{F}, w, k, r)$ обозначаем множество всех таких f из $M(\mathcal{F})$, что все множества из $\sum_f^{\mathcal{F}}$ содержат w и выполнено

$$R^{\mathcal{F}}(f) \leq |w| + k,$$

$$l_{|w|+s}^{\mathcal{F}} \leq (r-1)^s, \quad s = 1, 2, \dots, k.$$

Полагаем

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

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

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

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

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

$$t(\mathcal{F}, k) = \max_{\substack{w_1 \subseteq w_2 \subseteq W \\ |w_1| \leq k, |w_2| \leq |w_1| + k}} |\mathcal{F}(w_2) \setminus \mathcal{F}(w_1)|,$$

$$B_{r,k}^{\mathcal{F}} = B_{r,t(\mathcal{F},k)}^{<n>}.$$

Лемма 2.3 ([109]). *Если ρ — монотонная псевдометрика на $M^{<n>}$, $r \geq 2$, $|w| \leq k$, то для любой f из $M(\mathcal{F}, w, k) \setminus M(\mathcal{F}, w, k, r)$ существует g из $M(\mathcal{F}, w, k)$ такая, что*

$$g \geq f,$$

$$l(g) \leq l(f) - 1,$$

$$\rho(f, g) \leq \rho(1, B_{r,k}).$$

Лемма 2.4 ([109]). *Если ρ — монотонная псевдометрика на $M^{<n>}$, $|w| \leq k$, $r \geq 2$, то для любой f из $M(\mathcal{F}, w, k) \setminus M(\mathcal{F}, w, k, r)$ существует такая g из $M(\mathcal{F}, w, k, r)$, что*

$$g \geq f,$$

$$\rho(f, g) \leq l(f) * \rho(1, B_{r,k}).$$

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

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

Полагаем

$$\begin{aligned} \mathfrak{M}(\mathcal{F}, k, r) &= M(\mathcal{F}, \emptyset, k, r), \quad \mathfrak{M}(\mathcal{F}, k) = M(\mathcal{F}, \emptyset, k). \\ \mathfrak{D}(\mathcal{F}, s) &= \{\mathcal{K}_w^{\mathcal{F}} \mid w \subseteq W, |w| = s\}. \end{aligned}$$

Лемма 2.5 ([109]). *Если ρ_1, ρ_2 — монотонные псевдометрики на $M^{<n>}$, ρ_1 — \mathcal{F} -правильная, $r \geq 2, k \geq 1$, то*

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

где

$$\begin{aligned} a_1 &= \sum_{s=k+1}^{2k} s \cdot (r-1)^s \cdot \rho_1(0, \mathfrak{D}(\mathcal{F}, s)), \\ a_2 &= 2k \cdot (r-1)^{2k} \cdot \rho_2(1, B_{r,k}^{\mathcal{F}}). \end{aligned}$$

Теорема 2.2 ([109]). *Если ρ_1, ρ_2 — монотонные псевдометрики на $M^{<n>}$, ρ_1 — \mathcal{F} -правильная $f \in M^{<n>}$, $r \geq 2, |W| \geq k \geq 1, L_{\mathcal{A}} \geq 0$, то для любого $\alpha > 0$*

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

где

$$\begin{aligned} a_1 &= \alpha + \sum_{s=k+1}^{2k} s \cdot (r-1)^s \cdot \rho_1(0, \mathfrak{D}(\mathcal{F}, s)), \\ a_2 &= \alpha + 2k \cdot (r-1)^{2k} \cdot \rho_2(1, B_{r,k}^{\mathcal{F}}). \\ \mathcal{A} &= \mathfrak{M}(\mathcal{F}, k, r). \end{aligned}$$

2.4. Оценки в случае специальных псевдометрик

Полагаем, что $\lambda_s^{\mathcal{F}}(f)$ — минимально возможное число множеств из $\Sigma_f^{\mathcal{F}}$ таких, что их пересечение 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 ([109]). *Если $p \in (0, 1)$, $|W| \geq k \geq 1$, $r \geq 2$, $f \in M(\mathcal{F})$, $L_{\mathcal{A}}(f) \leq 0$, $\lambda_{k+1}^{\mathcal{F}}(f) \geq 1$, $t(\mathcal{F}, k) \geq 1$, $\mathcal{A} = \mathfrak{M}(\mathcal{F}, k, r)$, то*

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

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

Теорема 2.4 ([109]). *Если $p \in (0, 1)$, $k \geq 1$, $r \geq 2$, $f \in M^{<n>}$, $R^*(f) \geq k + 1$, $\mathfrak{B} = \{\&, \vee, 0, 1\}$, то*

$$L_{\mathfrak{B}}(f) \geq \min \left(\frac{l(f)}{\sum_{s=k+1}^{2k} s(r-1)^s \lambda_s(f)}, \frac{1 - l(f)e^{-pR^*(f)} - pk}{2k(r-1)^{2k}(pk)^r} \right).$$

2.5. Примеры сложнореализуемых монотонных функций

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

Пусть $GF(q)$ — поле Галуа порядка q а $p(x) = x^2 + c_1x + c_2$, $c_1, c_2 \in GF(q)$, — неприводимый над $GF(q)$ многочлен. Рассмотрим расширение $GF(q)$, порождаемое присоединением корней $p(x)$. В этом случае операции на $GF(q)^2 = GF(q) \times GF(q)$ определяются следующим образом:

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2), \\ (a_1, a_2) * (b_1, b_2) &= (a_1b_1 - c_2a_2b_2, a_1b_2 + a_2b_1 - c_1a_2b_2). \end{aligned}$$

Данное расширение является, как известно, полем Галуа $GF(q^2)$. При этом множество всех пар вида $(a, 0)$ образует подполе $GF(q)$ и выполнено

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

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

$$\begin{aligned} \varphi_0(x, y), \varphi_1(x, y) = x, \varphi_2(x, y) = y, \\ (\varphi_{2k+1}(x, y), \varphi_{2k+2}(x, y)) = (\varphi_{2k-1}(x, y), \varphi_{2k}(x, y)) * (x, y), \quad k \geq 1. \end{aligned}$$

Пусть $n = q^3$ и

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

то есть мы индексировали тройками из $GF(q)^3$ все переменные из U_n . Полагаем

$$\begin{aligned} d(\tilde{\alpha}, a, b) &= \bigoplus_{i=0}^{2m} \alpha_i \varphi_i(a, b), \\ \tilde{\alpha} &= (\alpha_0, \alpha_1, \dots, \alpha_{2m}) \in GF(q)^{2m+1}, \quad a, b \in GF(q), \\ \mathcal{K}_{\tilde{\alpha}} &= \bigwedge_{a,b \in GF(q)} x_{a,b,d(\tilde{\alpha},a,b)}, \\ g_{n,m}(u_1, u_2, \dots, u_n) &= \bigvee_{\tilde{\alpha} \in GF(q)^{2m+1}} \mathcal{K}_{\tilde{\alpha}}. \end{aligned}$$

Следствие 2.1 ([109]). *Если m четное,*

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

то для любого полного монотонного базиса B выполнено

$$L_B(g_{n,m}) \geq C_B \frac{2^{m/2}}{m}.$$

где C_B — 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

$$L_B(g_{n,m}) \geq 2^{n^{1/3-o(1)}}.$$

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

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

Полагаем

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

Эти функции называем μ -симметрическими.

Следствие 2.2 ([109]). *Если $\mu \geq 2$ и*

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

то для любого полного монотонного базиса B выполнено

$$L_B(f_t^{n,\mu}) \geq 2^{n^{\frac{\mu-1}{\mu(2\mu-1)}-o(1)}}.$$

3. Сложность схемных алгоритмов

При проектировании управляющих систем, одной из основных задач является минимизация их параметров, обуславливающих стоимость, размеры и материалоемкость. Пусть, например, перед конструктором стоит задача разработки блока ЭВМ для умножения чисел заданных в двоичной записи. В целях обеспечения быстродействия и надежности желательно, чтобы этот блок состоял из одной микросхемы. Однако число транзисторов и других функциональных узлов, которое можно разместить на одном кристалле, ограничено,

вследствие причин 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} , сопоставляющий каждой схеме $u \in \mathcal{U}$, реализуемую ею булеву функцию $\mathcal{F}(u)$ (или оператор). В приведенном примере \mathcal{U} — это множество микросхем, а $\mathcal{F}(u)$ — преобразование входных наборов импульсов в выходные, осуществляемое микросхемой u . Задан неотрицательный, определенный 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 ее схему u минимально возможной сложности $L_{\mathcal{U}}(u)$, которая обозначается через $L_{\mathcal{U}}(f)$ и называется сложностью реализации f , схема же 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 при уже относительно небольшом числе переменных у функции этот перебор оказывается, как правило, неосуществимым в обозримое время. Например, для реализации умножения 100-рядных 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 [1] был предложен подход, заключающийся в следующем видоизменении задачи синтеза. Полагаем, что

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

где максимум берется по всем функциям от n переменных. Требуется получить возможно лучшие оценки для $L_{\mathcal{U}}(n)$ (в настоящее время она называется функцией Шеннона) и предложить метод синтеза, то есть построения, который по каждой функции от n переменных строит реализующую ее схему сложности, близкой 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, соответственно, оптимальный по порядку, в указанном выше смысле, метод синтеза контактных схем.

Асимптотически оптимальные методы синтеза были разработаны О. Б. Лупановым [2, 5]. 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, причем 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. То есть, если задан класс \mathfrak{A} булевых функций, то требуется для каждой функции из $\mathfrak{A}^{<n>}$ (где $\mathfrak{A}^{<n>}$ множество функций из \mathfrak{A} , зависящих от первых n переменных) построить реализующую ее схему, близкую по сложности к

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

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 [10, 11], 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 [12, 13]. 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 реальных управляющих систем в них 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 работе [14] была поставлена задача синтеза самокорректирующихся схем, то есть построения для каждой булевой функции f такой схемы, реализующей ее, 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 [15]. Наиболее глубокие результаты были достигнуты Э. И. Нечипорук [16]–[19], 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 [20, 21] Д. Улигом [22] 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 (Г. И. Кириенко [23, 24], Улиг [25], С. И. Ортюков [26]), однако в этом случае возникает необходимость использования абсолютно надежных 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. При этом эта ситуация является характерной. Это замечание относится и к методам синтеза асимптотически избыточных самокорректирующихся схем. Причем здесь погружение в специфику конкретных типов управляющих систем часто столь велико, что остается неясным, можно ли ожидать эффекта асимптотически избыточного корректирования нетривиальных классов неисправностей для новых типов управляющих систем, которые возможно еще возникнут.

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

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

Исследования, которые здесь излагаются, были проведены А. Е. Андреевым [30].

Разработка этих вопросов привела к необходимости

- фактического выхода за пределы двузначной логики, а именно рассмотрения недоопределенных булевых функций, которые понимаются как принимающие на наборах из нулей и единиц три значения — 0, 1 и * в точках их неопределенности;
- 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 (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 характеристики сложности компонент). При этом сложность операции учитывается с очень большим весом (растущим с ростом числа задействованных переменных). Вес компонент растет с уменьшением мощности области определения. Затем по обычной схеме определяется сложность реализации функции как минимум сложности по всем реализующим ее функциональным сетям, и функция Шеннона для класса \mathfrak{A} — как

максимальная сложность функций из $\mathfrak{A}^{<n>}$. В качестве неисправностей функциональных сетей рассматриваются замещения компонент — либо произвольные, либо на нули и единицы. Классы неисправностей описываются ограничениями на допустимое число замещений.

В качестве подхода к решению проблемы создания универсальных методов синтеза схем, предлагается рассматривать разработку асимптотически оптимальных методов 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 управляющих систем. Эта перестройка называется моделированием. Чтобы ее осуществить, надо реализовать компоненты функциональной сети с помощью асимптотически оптимального для класса частичных функций с данной величиной области определения методом синтеза схем. А 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 ее 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 определенном смысле включают этот класс операций. Поэтому степень универсальности методов синтеза функциональных сетей по от-

ношению к типам управляющих систем определяется тем, насколько узким является рассматриваемый класс операций.

Изучаются в основном два класса операций — неповторные и топологические. Операции из первого класса задаются двухполосными 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 операций является расширением класса неповторных операций. Поэтому множество типов управляющих систем, моделирующих топологические операции, сужается по сравнению с неповторными, оставаясь, тем не менее, достаточно широким. В классе неповторных функциональных сетей возможна лишь реализация функций, топологические же сети допускают и реализацию операторов.

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

- частичные функции с данной величиной области определения,
- функции с данным числом единиц,
- функции с ограниченной энтропией,
- ненулевые инвариантные классы С. В. Яблонского,
- классы Поста, не содержащиеся в D_3 , L_1 , S_6 и P_6 (обозначения из [27]).

Основным результатом относительно топологических функциональных сетей является теорема о дублях. В процессе доказательства этой теоремы им предложен метод одновременной реализации многих экземпляров частичной функции и ее отрицания со сложностью, асимптотически не превосходящей сложности самой функции (то есть величины ее 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:

- ненулевые инвариантные классы операторов,
- класс монотонных в арифметическом смысле операторов,
- классы операторов, вычисляющих значения функций на нескольких последовательных наборах.

Вопросы самокорректирования рассматриваются им также для неповторных и топологических функциональных сетей. Для обоих классов операций разработаны методы преобразования обычных функциональных сетей в самокорректирующиеся. При этих преобразованиях сложность в определенном 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 неповторных сетей этот список включает, например:

- 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 трех пунктов.

Моделирование функциональных сетей рассмотрено 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 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 неизбежно корректируемых неисправностей существенно выше, чем ранее известные. Так в случае класса всех булевых функций установлена возможность асимптотически неизбежного корректирования:

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

Развитые методы синтеза могут быть использованы при проектировании сложных управляющих систем. Они также могут быть полезны при создании систем автоматического проектирования, например, микросхем. Причем 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 \mathcal{M} — множество операций на P . Если операция \mathcal{F} из \mathcal{M} применима к набору (f_1, f_2, \dots, f_k) функций из P , где k — арность этой операции, то выражение

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

называется функциональной сетью. Через $[S]$ обозначается функция (оператор) разложением которой является функциональная сеть S . То есть $[S]$ — это результат применения порождающей операции к набору функций перечисленных в скобках.

Пусть

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

Функциональная сеть S реализует функцию f (оператор)

$$f \preceq [S],$$

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

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

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

Считается, что знаки \preceq и $\overset{\emptyset}{\preceq}$ совпадают, а выражения $f \overset{\Delta}{\preceq} [S]$ и $f \overset{\Delta}{\preceq} S$, $\Delta \in \{\emptyset, \xi, (a, b)\}$, означают одно и то же.

Вводим три класса операций:

- **СЛ** — слабые логические,
- **T** — топологические,
- **II** — неповторные.

Операция из класса **СЛ** задается ориентированным ациклическим графом. В графе выделены вершины, называемые полюсами, они занумерованы числами $1, 2, \dots, k$, где k — число полюсов. В полюса ребра 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 и занумерованы числами $1, 2, \dots, S$, где S — их число. Операция \mathcal{F} , задаваемая такой логической сетью, имеет арность k и ее результатом является S -компонентный оператор $[\mathcal{F}(f_1, f_2, \dots, f_k)]$, определяемый следующим образом. Пусть функции f_1, f_2, \dots, f_k — полностью определенные. Полюсу с номером i приписываем функцию f_i , $i = 1, 2, \dots, k$, 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 $[\mathcal{F}(f_1, f_2, \dots, f_k)]$ являются функции, приписанные выходным вершинам в соответствии с нумерацией последних. В общем случае, для определения оператора $[\mathcal{F}(f_1, f_2, \dots, f_k)]$ рассматриваются всевозможные наборы g_1, g_2, \dots, g_k такие, что g_i — полное доопределение f_i , зависящее от тех же переменных. Если на данном наборе значений переменных в i -ой выходной вершине при любом таком полном доопределении реализуется одно и то же значение, то оно является значением i -ой компоненты результата операции на данном наборе значений переменных, в противном случае это значение равно $*$.

Операция из класса \mathbf{T} задается конечным неориентированным графом без петель (кратные ребра допустимы) с выделенными вершинами, которые называются полюсами, то есть — сетью. Ребра графов занумерованы натуральными числами от 1 до k , где k — число ребер, а полюса — натуральными числами от 1 до p , где p — число полюсов. Арность операции — k , она применима к любому набору из k функций. Ее результат при применении к набору (f_1, f_2, \dots, f_k) является оператором с C_p^2 компонентами. Ребру с номером i приписывается функция f_i . Компонента результата с номером $C_{j-1}^2 + i$, $1 \leq i < j \leq p$, определяется следующим образом: на данном наборе значений переменных она равна 0, если нет цепей между i -ым и j -ым полюсами, либо, если в любой цепи между ними существует ребро помеченное функцией, обращающейся на выбранном наборе значений переменных в 0; равна 1, если существует цепь между рассматриваемыми полюсами такая, что все приписанные ее ребрам функции обращаются на выделенном наборе переменных в 1; в остальных случаях значение равно $*$.

Пусть \mathbf{II} — подкласс класса \mathbf{T} , соответствующий двухполюсным параллельно последовательным сетям. Он совпадает с подклассом класса $\mathbf{СЛ}$, порождаемым неповторными (то есть древовидными) логическими сетями.

Ясно, что

$$\mathbf{II} \subset \mathbf{T} \subset \mathbf{СЛ}.$$

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

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 \mathbf{III} , определенной, неотрицательной, монотонной и неограниченной на $[0, \infty)$;
- весовой функцией операции φ , определенной, неотрицательной на $[0, \infty)$ и $\varphi(a) \rightarrow \infty$ при $a \rightarrow \infty$.

Набор

$$\sigma = \langle \mathfrak{M}, L_{\mathfrak{M}}, \Phi, \mathbf{III} \rangle$$

называется сигнатурой. Для функциональной сети

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

полагаем

$$L_{\sigma, \varphi}(S) = \mathbf{III}^{-1} \left(\varphi(n) L_{\mathfrak{M}}(\mathcal{F}) + \sum_{i=1}^k \mathbf{III}(\Phi(f_i)) \right),$$

где n — число переменных задействованных в функциональной сети S и

$$\mathbf{III}^{-1}(a) = \sup\{b \mid \mathbf{III}(b) \leq a\}.$$

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

Если f — функция из P (оператор), то

$$L_{\sigma, \varphi}^{\Delta}(f) = \min_{S, f \stackrel{\Delta}{\leq} S} L_{\sigma, \varphi}(S),$$

$\Delta \in \{\emptyset, \xi, (a, b)\}$, — сложность реализации f функциональными сетями в сигнатуре σ с весовой функцией φ (корректирующими ξ неисправностей, a единичных и b ненулевых неисправностей).

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

$$L_{\sigma, \varphi}^{\Delta}(\mathfrak{A}^{<n>}) = \max_{f \in \mathfrak{A}^{<n>}} L_{\sigma, \varphi}^{\Delta}(f),$$

$\Delta \in \{\emptyset, \xi, (a, b)\}$, — соответствующая функция Шеннона.

В качестве основных функционалов характеристики 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 —

$\mathcal{H}(f)$ — энтропия f , то есть двоичный логарифм (\log) числа сочетаний из $m(f)$ по $m_1(f)$ — числу единичных точек функции f . В качестве нормировочных функций рассматриваются:

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

где

$$\overline{\log x} = \begin{cases} \log x, & \text{если } x \geq 4 \\ 2, & \text{если } 0 \leq x < 4 \end{cases}$$

Если соотношение

$$L_{\sigma, \varphi}^{\Delta}(\mathfrak{A}^{<n>}) \lesssim \psi(n)$$

выполнено при всех φ таких, что

$$\log \varphi(n) = o(\log \psi(n)),$$

то записываем

$$L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \lesssim \psi(n),$$

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

$$L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \dot{\lesssim} \psi(n).$$

Если соотношение

$$L_{\sigma, \varphi}^{\Delta}(\mathfrak{A}^{<n>}) \gtrsim \psi(n)$$

выполнено хотя бы для одной φ такой, что

$$\log \varphi(n) = o(\log \psi(n)),$$

то записываем

$$L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \gtrsim \psi(n),$$

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

$$L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \dot{\gtrsim} \psi(n).$$

Полагаем:

$$\begin{aligned} L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \sim \psi(n) &\leftrightarrow L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \lesssim \psi(n), L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \gtrsim \psi(n); \\ L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \dot{\sim} \psi(n) &\leftrightarrow L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \dot{\lesssim} \psi(n), L_{\sigma}^{\Delta}(\mathfrak{A}^{<n>}) \dot{\gtrsim} \psi(n). \end{aligned}$$

Для сигнатур σ_1, σ_2 записываем $\sigma_1 \leq \sigma_2$, если при всех допустимых f, φ, Δ выполнено

$$L_{\sigma_1, \varphi}^{\Delta}(f) \leq L_{\sigma_2, \varphi}^{\Delta}(f).$$

Так как $\mathbf{II} \subset \mathbf{T} \subset \mathbf{СЛ}$, то

$$\langle \mathbf{СЛ}, L_{\mathbf{СЛ}}, \Phi, \mathbf{III} \rangle \leq \langle \mathbf{T}, L_{\mathbf{T}}, \Phi, \mathbf{III} \rangle \leq \langle \mathbf{II}, L_{\mathbf{II}}, \Phi, \mathbf{III} \rangle$$

при любых допустимых Φ и \mathbf{III} .

Пусть

$$\mathbf{III}_1(x) = \frac{x}{\log x}, \quad \mathbf{III}_2(x) = \frac{x}{\log \log x}.$$

Показано, что

$$\langle \mathfrak{M}, L_{\mathfrak{M}}, \Phi, \mathbf{III}_2 \rangle \leq \langle \mathfrak{M}, L_{\mathfrak{M}}, \Phi, \mathbf{III}_1 \rangle$$

при любых допустимых \mathfrak{M} и Φ .

Для мощностных нижних оценок функции Шеннона имеет место утверждение.

Теорема 3.1 ([35]). *Если $\log n = o(\log \mathcal{H}(\mathfrak{A}^{<n>}))$, то*

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

а если $\log \log n = o(\log \log \mathcal{H}(\mathfrak{A}^{<n>}))$, то

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

где $\sigma_1 = \langle \mathcal{CЛ}, L_{\mathcal{CЛ}}, m, \frac{x}{\log \log x} \rangle$, а $\mathcal{H}(\mathfrak{A}^{<n>})$ — энтропия класса $\mathfrak{A}^{<n>}$, то есть двоичный логарифм минимально возможной мощности множества булевых функций (операторов), содержащего доопределения всех f из $\mathfrak{A}^{<n>}$.

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

Сначала рассматриваются классы с ограничениями на энтропию функций. На конструкции этого параграфа существенно опираются последующие главы. Следующая теорема является основным результатом для этих классов.

Теорема 3.2 ([35]). *Если \mathfrak{A} — класс булевых функций или операторов, $\mathfrak{M} \in \{\Pi, \mathbf{T}, \mathcal{CЛ}\}$, $\Delta(n) \in \{\emptyset, \xi(n), (a(n), b(n))\}$,*

$$L_{\sigma_1}^{\Delta(n)}(\mathfrak{A}^{<n>}) \lesssim \psi(n),$$

$\log^2 n = o(\log \psi(n))$, то

$$L_{\sigma_2}^{\Delta(n)}(\mathfrak{A}^{<n>}) \lesssim \psi(n),$$

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 обозначается множество всех таких f из P , что

$$\mathcal{H}(f) \leq r(N(f)),$$

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

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

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

Теорема 3.3 ([35]). Если $\log^2 n = o(\log r(n))$, $r(n) \leq 2^n$, то

$$L_\sigma(Q_r^{<n>}) \sim r(n),$$

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

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

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

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

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

Теорема 3.4 ([35]). Если $\log \log n = o(\log \log r(n))$, то

$$L_\sigma(\varepsilon_r^{<n>}) \sim r(n).$$

С помощью этой теоремы устанавливается такой факт.

Теорема 3.5 ([35]). Если $\mathfrak{A} \subseteq P$, $\Delta(n) \in \{\emptyset, \xi(n), (a(n), b(n))\}$,

$$L_{\sigma_0}^{\Delta(n)}(\mathfrak{A}^{<n>}) \lesssim \psi(n),$$

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

$$L_\sigma^{\Delta(n)}(\mathfrak{A}^{<n>}) \lesssim \psi(n),$$

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

Рассматриваются ненулевые инвариантные классы С. В. Яблонского. Пусть \mathcal{R}_α некоторый ненулевой инвариантный класс такой, что

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

Тогда справедлива теорема.

Теорема 3.6 ([35]).

$$L_\sigma(\mathcal{R}_\alpha^{<n>}) \sim \alpha 2^n,$$

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

Рассматриваются также классы 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*

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

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

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 , записываем $S_1 \preccurlyeq S_2$, 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 ее отрицание является компонентой этого набора,

$L_{\mathbf{T}}^*(S)$ — арность \mathcal{F} ,

$N(S)$ — число переменных, задействованных в S . Если r_1, r_2 — положительные последовательности, то через \mathbf{T}_{r_1, r_2}^* обозначаем множество всех таких топологических функциональных сетей S , что

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

Имеет место следующее утверждение.

Теорема 3.8 ([35]). *Если $1 \leq r_1(n) = r_2(n)^{o(1)}$, $\log^3 n = o(\log r_2(n))$, $r_2(n) \leq 2^{cn}$, то*

$$L_\sigma(\mathbf{T}_{r_1, r_2}^{* <n>}) \sim r_2(n),$$

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

Эта теорема позволяет переносить на топологические функциональные сети многие конструкции принципа локального кодирования О. Б. Лупанова.

Она может быть проиллюстрирована так. Рассматриваются 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 называется ненулевым, если

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

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

Теорема 3.9 ([35]). *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 $\sigma = \langle T, L_T, m, \frac{x}{\log x} \rangle$.

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



Рассматривается класс монотонных операторов. Для булевого набора $\tilde{a} = (a_1, a_2, \dots, a_n)$ полагаем

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

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

$$I(\tilde{a}) \leq I(\tilde{b}) \Rightarrow I(F(\tilde{a})) \leq I(F(\tilde{b})).$$

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

Теорема 3.10 ([35]).

$$L_\sigma(\{\langle \tilde{F} \rangle \mid \tilde{F} \in \text{MH}^{\langle n \rangle}\}) \sim 2^{n+1},$$

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

Рассматривается вопрос о вычислении значения функции на нескольких последовательных наборах.

Если $f \in P^{\langle n \rangle}$, то через f^{+k} обозначается такая функция из $P^{\langle n \rangle}$, что

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

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

Теорема 3.11 ([35]). Если $1 \leq t(n) \leq 2^{o(n)}$, то

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

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

Рассматриваются вопросы синтеза асимптотически неизбыточных самокорректирующихся функциональных сетей.

Теорема 3.12 ([35]). Если $\mathfrak{A} \subseteq P$, $\log^2 n = o(\log \psi(n))$,

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

$$1 \leq \log \xi(n) = o\left(\sqrt{\frac{\log \psi(n)}{\log n}}\right), \text{ то}$$

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

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

Изучается самокорректирование в топологических функциональных сетях, предполагается, что $\sigma = \langle \mathbf{T}, L_{\mathbf{T}}, m, \frac{x}{\log x} \rangle$. Основными результатами здесь являются следующие теоремы.

Теорема 3.13 ([35]). Если \mathfrak{A} — класс функций или операторов и

$$L_{\sigma}(\mathfrak{A}^{<n>}) \lesssim \psi(n),$$

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

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

Теорема 3.14 ([35]). Если \mathfrak{A} — класс функций или операторов и

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

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

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

где c — константа.

Теорема 3.15 ([35]). Если $\varepsilon \in (0, 1)$, $a(n) \geq 2$, $b(n) \geq 2$,

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

то

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

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

Рассматриваются формулы в полном базисе \mathfrak{B} , который состоит из надежной и ненадежной частей. При этом надежная часть базиса \mathfrak{B}_n полна. Формула, реализующая f корректирует ξ неисправностей, если при замене в ней не более ξ любых вхождений ненадежных функциональных символов на любые другие той же арности, получающаяся формула также реализует f . Через $L_{\mathfrak{B}, \Phi}^{\xi}(f)$ обозначается сложность реализации f формулами в базисе \mathfrak{B}_n , корректирующими

ξ неисправностей. Через $\rho(\mathcal{B})$ обозначается минимальный приведенный вес базиса \mathcal{B} .

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

- 1) $\varepsilon_r = \{f \mid m(f) \leq r(N(f))\}$, где r — любая натуральная монотонная последовательность;
- 2) $\varepsilon_{1,r} = \{f \mid m_1(f) = r(N(f))\}$, где r — любая натуральная последовательность;
- 3) $Q_r = \{f \mid \mathcal{H}(f) \leq r(N(f))\}$, 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 классов \mathfrak{A} семейства \mathfrak{N}_1 таких, что $\log \log \mathcal{H}(\mathfrak{A}^{<n>}) \sim \log n$, а также классов ε_r и Q_r таких, что $\log \log n = o(\log \log r(n))$.

Теорема 3.16 ([35]). *Если $\mathfrak{A} \in \hat{\mathfrak{N}}_1$, $\log \xi(n) = o\left(\sqrt{\frac{\log \mathcal{H}(\mathfrak{A}^{<n>})}{\log n}}\right)$, то для любого базиса \mathcal{B} с полной надежной частью*

$$L_{\mathcal{B},\Phi}^{\xi(n)}(\mathfrak{A}^{<n>}) \sim L_{\mathcal{B},\Phi}^0(\mathfrak{A}^{<n>}) \sim \rho(\mathcal{B}) \frac{\mathcal{H}(\mathfrak{A}^{<n>})}{\log \log \mathcal{H}(\mathfrak{A}^{<n>})}.$$

Это утверждение вытекает из изложенных выше результатов и результатов О. Б. Лупанова [28], в которой получена асимптотика функции Шеннона для формул.

Рассматриваются контактные схемы. Через $L_k(F)$ обозначается сложность реализации F обычными контактными схемами, а через $L_k^{\xi}(F)$ и $L_k^{(a,b)}(F)$ — 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 ([35]). *Если $f \in P^{<n>}$, то*

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

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

- 1) всех ненулевых инвариантных классов операторов;
- 2) класса МН монотонных операторов;
- 3) $\{(f, f^{+1}, \dots, f^{+r(N(f))}) \mid f \in P\}$, где r такая натуральная последовательность, что $1 \leq r(n) = 2^{o(n)}$;
- 4) $\{\underbrace{(f, \bar{f}, f, \bar{f}, \dots, f, \bar{f})}_{r(N(f))} \mid f \in P\}$, где r такая натуральная последовательность, что $1 \leq r(n) = 2^{o(n)}$;

Если \mathfrak{A} класс операторов, то полагаем $\hat{\mathfrak{A}} = \{\langle \tilde{F} \rangle \mid \tilde{F} \in \mathfrak{A}\}$.

Полагаем $\hat{\mathfrak{N}}_2 = \{\hat{\mathfrak{A}} \mid \mathfrak{A} \in \mathfrak{N}_2\}$.

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

Теорема 3.18 ([35]). *Если $\mathfrak{A} \in \mathfrak{N}_1 \cup \hat{\mathfrak{N}}_2$ и $\mathcal{H}(\mathfrak{A}^{<n>}) \geq 2^{\log^6 n}$,*

$$1 \leq \log \xi(n) = o(\log \mathcal{H}(\mathfrak{A}^{<n>})),$$

то

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

Теорема 3.19 ([35]). *Если $\varepsilon \in (0, 1)$, $a(n) \geq 2$, $b(n) \geq 2$,*

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

то

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

Изложенные результаты опубликованы в [29]–[34].

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 80-х годов не удавалось привести примеров булевых функций с нелинейной сложностью.

В работе [36] 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 $f(x_1, \dots, x_n)$, 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: упорядочиваются все д. н. ф. над переменными $\{x_1, \dots, x_n\}$ (их число 2^{3^n}) по порядку неубывания рассматриваемой сложности и выбирается первая д. н. ф., которая реализует данную функцию. Это решение с точки зрения практики слишком громоздко. Известно [44, 48], что кратчайшее д. н. ф. (к. д. н. ф.) и минимальное д. н. ф. (м. д. н. ф.) можно получить из сокращенной д. н. ф. (с. д. н. ф.) заданной функции путем удаления некоторых конъюнкций. Установлен достаточно эффективный критерий, позволяющий осуществлять это удаление (так называемый критерий поглощения) [41, 44]. Однако и при таком подходе решение задачи минимизации булевых функций встречает ряд серьезных препятствий. Последние были указаны в работах по алгоритмическим трудностям синтеза минимальных схем и в работах Ю. Л. Васильева и В. В. Глаголева [37, 38, 44]. Эти трудности проявляются прежде всего в том, что, переходя последовательно посредством упрощения от одной д. н. ф. для данной функции к другой с помощью критерия поглощения, приходят к далее неупрощаемой

тупиковой 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 выбрано искомое решение.

Подчеркивая большую трудоемкость процедур такого рода, Ю. И. Журавлев указывал на необходимость предварительного изучения свойств удаляемых конъюнкций и предложил в связи с этим подход, названный им локальными алгоритмами [41, 42, 43]. 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, они позволяют 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 [43, 44]. 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 [37], а, с другой стороны, мощность областей перебора обычно очень велика. Как отмечено в [38, 44], максимальное число т. д. н. ф. функции от n переменных имеет порядок, больший, чем 2^{2^n} .

В работе Нгуен Ким Ань [50] изучаются 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.

Изучается процесс построения всех т. д. н. ф. булевой функции в геометрическом плане и исследуется поведение указанных функций Шеннона. Граф интервалов был введен А. А. Сапоженко [46]. Здесь исследуются новые качественные и количественные проблемы, связанные с этим графом. Описаны алгоритмы нахождения к. д. н. ф. и м. д. н. ф. для класса булевых функций, так называемый упрощенный граф интервалов каждой из которых является деревом. Сложность построенных алгоритмов оказалась линейно зависящей от числа вершин-конъюнкций в исходном графе.

Полученные ею результаты по первым двум из вышеуказанных вопросов позволяют лучше понять сложную структуру взаимосвязи 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. Введем основные понятия и обозначения, используемые далее. Пусть A — некоторое множество. $|A|$ — его мощность, 2^A — множество всех его подмножеств и A^n — декартово произведение $\underbrace{A \times \dots \times A}_{n \text{ раз}}$. Если $|A| = n$, то A называем n -мно-

жеством. Используем символ ξ_n для множества $\{1, \dots, n\}$, ($n \geq 1$) и символ E_2 — для множества $\{0, 1\}$. E_2^n есть множество всех точек $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$, где $\alpha_i \in E_2$ для любого $i \in \xi_n$. При фиксированном n положим $\hat{1} = \underbrace{(1, \dots, 1)}_{n \text{ раз}}$ и $\hat{0} = \underbrace{(0, \dots, 0)}_{n \text{ раз}}$. Для точки $\tilde{\alpha}$ из E_2^n обозначим

через $I_{\tilde{\alpha}}^1$ (соответственно, $I_{\tilde{\alpha}}^0$) множество всех номеров i из ξ_n , таких, что $\alpha_i = 1$ (соответственно $\alpha_i = 0$). Нормой точки $\tilde{\alpha}$ (обозначается $|\tilde{\alpha}|$) называется 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 $\tilde{\alpha} \leq \tilde{\beta}$), если имеет место соотношение $I_{\tilde{\alpha}}^1 \subseteq I_{\tilde{\beta}}^1$, что $\tilde{\alpha}$ и $\tilde{\beta}$ несравнимы, если не выполняется ни $\tilde{\alpha} \leq \tilde{\beta}$, ни $\tilde{\beta} \leq \tilde{\alpha}$.

Граф Γ с множеством вершин V и множеством ребер 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, то есть 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 $\{x_1, \dots, x_n\}$. Элементарной конъюнкцией ранга r называется логическое произведение $x_{i_1}^{\sigma_1} \dots x_{i_r}^{\sigma_r}$, где $x_i^{\sigma_i} = x_i$, если $\sigma_i = 1$, и $x_i^{\sigma_i} = \bar{x}_i$, если $\sigma_i = 0$, а все x_{i_j} различны. Д. н. ф. есть логическая сумма $D = K_1 \vee \dots \vee K_m$ различных элементарных конъюнкций K_j . Для д. н. ф. D обозначим через $M(D)$ множество всех ее элементарных конъюнкций. Если булева функция представляется в виде д. н. ф., то говорят, что последняя реализует данную функцию. К. д. н. ф. (соответственно м. д. н. ф.) для функции $f(x_1, \dots, x_n)$ являются те д. н. ф., которые реализуют $f(x_1, \dots, x_n)$ и содержат наименьшее число элементарных конъюнкций (соответственно, наименьшее число вхождений символов переменных) по сравнению с другими реализующими $f(x_1, \dots, x_n)$ д. н. ф. Каждой булевой функции $f(x_1, \dots, x_n)$ сопоставим в соответствие подмножество \mathcal{N}_f множества E_2^n все точек $\tilde{\alpha}$ таких, что $f(\tilde{\alpha}) = 1$. Для элементарной конъюнкции K r -го ранга множество $\mathcal{N}_K \subseteq E_2^n$ ($n \geq r$) называется интервалом r -го ранга, а \mathcal{N}_K — граф — $(n - r)$ -мерной гранью единичного n -мерного куба. Элементарная конъюнкция K называется простой, а соответствующий интервал — максимальным для функции $f(x_1, \dots, x_n)$, если имеет место $\mathcal{N}_K \subseteq \mathcal{N}_f$ и не существует конъюнкции K' , такой, что $\mathcal{N}_K \subseteq \mathcal{N}_{K'} \subseteq \mathcal{N}_f$. Дизъюнкция всех простых конъюнкций функции $f(x_1, \dots, x_n)$ 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

$M(D_{\cap T}(f))$ называется множеством ядровых конъюнкций, а множество $M(D_C(f)) \setminus M(D_{\cap T}(f))$ — множеством неядровых конъюнкций функции f . Две функции $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n)$ считаются равными, если $\mathcal{N}_f = \mathcal{N}_g$, а две д. н. ф. D_1, D_2 — конъюнктивно равными (обозначаем $D_1 = D_2$), 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 $C = (X_1, \dots, X_s)$ — 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 имеет место $X_i \cap Y \neq \emptyset$. Покрытие Y называется приведенным для C , если любое его собственное подмножество не является покрытием для C . Множество всех приведенных покрытий для C обозначается через $\mathcal{P}(C)$.

Изучается алгоритм минимизации булевых функций, в основе которого лежит процедура сравнения на поглощаемость одного набора конъюнкций другими [40, 48]. Предполагается, что булева функция задается с помощью с. д. н. ф. Тогда этот алгоритм состоит в последовательном получении 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 ребрами — пары указанных д. н. ф., отличающихся друг от друга ровно одним дизъюнктивным членом.

Назовем поликубом любой $\Pi(l, k)$ — граф, где $\Pi(l, k)$ состоит из некоторых k попарно несравнимых точек $\tilde{\alpha}^1, \dots, \tilde{\alpha}^k$ из E_2^l удовлетворяющих условию $|\bigcup_{i=1}^k I_{\tilde{\alpha}^i}^0| = l$, и из всех точек $\tilde{\beta}$ из E_2^l таких, что имеет место $\tilde{\alpha}^i \leq \tilde{\beta}$ 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 ее 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 $\mathcal{J}(\Pi(l, k)) = \{I_{\tilde{\alpha}^1}^1, \dots, I_{\tilde{\alpha}^k}^1\}$. Пусть $\gamma: \xi_l \rightarrow M$ — некоторое отображение множества ξ_l в множество конъюнкций M , $\beta = \{i_1, \dots, i_s\}$, ($s \leq l$) — 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 $\mathcal{F}(\Pi(l, k))$. Справедливо утверждение.

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

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

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

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

Пусть π^l , $\pi^{l,k}$ и π_s^l соответственно есть 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 $\overline{n}(l) = \max_{\Pi \in \pi^l} n(\Pi)$; $\underline{n}(l) = \min_{\Pi \in \pi^l} n(\Pi)$; $\overline{n}(l, k) = \max_{\Pi \in \pi^{l,k}} n(\Pi)$; $\overline{n}_s(l) = \max_{\Pi \in \pi_s^l} n(\Pi)$.

Показывается, что для любого $l \geq 1$ имеет место $\overline{n}(l) = l + 2$, что $\underline{n}(l)$ имеет порядок $\log_3 l$, и что $l + 1 \leq \overline{n}_s(l) \leq l + 2$ при всех l, s , удовлетворяющих соотношениям $l \geq 1, 1 \leq s \leq C_l^{\lfloor \frac{l}{2} \rfloor}$.

Теорема 4.2. *Справедливы следующие оценки:*

- 1) $l + 1 \leq \overline{n}(l, k) \leq l + 2$, при $C_l^2 \leq k \leq C_l^{\lfloor \frac{l}{2} \rfloor}$, причем $\overline{n}(l, k) = l + 2$, при $k = C_l^2, \dots, C_l^{\lfloor \frac{l}{2} \rfloor}$;

2) $l \leq \bar{n}(l, k) \leq l + 2$, при $l \leq k < C_l^2$;

3) $\max(k, k \cdot \log_2(\lceil \frac{l}{k} \rceil)) \leq \bar{n}(l, k) \leq \min(l + 2, A)$, где

$$A = C_k^{\lceil \frac{k}{2} \rceil} \log_2 \left(\frac{l}{\min(l, C_k^{\lceil \frac{k}{2} \rceil})} \right) + 2C_k^{\lceil \frac{k}{2} \rceil} + 3, \text{ при } 2 \leq k \leq l;$$

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

Как вытекает из этой теоремы, величина $\bar{n}(l, k)$ не более чем на 2 отличается от l при $k \geq l$, 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 $1 \leq s \leq k \leq C_l^{\lceil \frac{l}{2} \rceil}$ 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 $1 \leq s \leq C_l^{\lceil \frac{l}{2} \rceil}$, и обозначим через $K(l, s)$ максимальную разность $k - s$ по всем числам k таким, что $s \leq k \leq C_l^{\lceil \frac{l}{2} \rceil}$ и

$\pi_s^{l,k}$ не пусто. Положим $\varphi_l(\lambda) = \frac{K(l, \lambda C_l^{\lceil \frac{l}{2} \rceil})}{C_l^{\lceil \frac{l}{2} \rceil}}$, где $0 \leq \lambda \leq 1$.

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 $\bar{n}_s(l, k)$, где $\bar{n}_s(l, k) = \max_{\Pi \in \pi_s^{l,k}} n(\Pi)$, также выяснено, что при всех k , больших некоторой величины $\eta(l, s)$, имеет место $l + 1 \leq \bar{n}_s(l, k) \leq l + 2$.

Изучаются некоторые метрические свойства графа перебора такие, как высота, ширина, объем.

Изучается структура графа интервалов. Вершинами графа интервалов булевой функции являются ее простые конъюнкции, а ребрами — пары простых конъюнкций, интервалы которых пересекаются. Установлено что любой граф без петель и кратных ребер может служить графом интервалов для булевой функции.

Пусть \mathcal{T}^m (соответственно \mathcal{G}^m) — множество всех графов (соответственно, деревьев) с m вершинами без петель и кратных ребер. Положим $\bar{n}(\mathcal{T}^m) = \max_{\Gamma \in \mathcal{T}^m} n(\Gamma)$; $\underline{n}(\mathcal{T}^m) = \min_{\Gamma \in \mathcal{T}^m} n(\Gamma)$; $\bar{n}(\mathcal{G}^m) = \max_{\Gamma \in \mathcal{G}^m} n(\Gamma)$; $\underline{n}(\mathcal{G}^m) = \min_{\Gamma \in \mathcal{G}^m} n(\Gamma)$, $n(\Gamma)$ — 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 $m \geq 2$ справедлива оценка $\bar{n}(\mathcal{T}^m) = m$.*

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

- 1) $\lceil \log_2(m+1) \rceil + 2 \leq \bar{n}(\mathcal{G}^m) \leq (\log_2 m)^2 + c_1 \log_2 m + c_2$, где $c_1 = 16$, $c_2 = 39$.
- 2) $\log_2(m+1) \leq \underline{n}(\mathcal{G}^m) \leq \lceil \log_2(m-1) \rceil + 2$.

В ряде специальных случаев возможен переход от известных локальных процедур [40, 41, 42] к улучшающим их нелокальным, но логически простым процедурам минимизации булевых функций. Приводится пример реализации этой идеи для класса \mathcal{F}_3^y всех булевых функций таких, что упрощенный граф интервалов для каждой из них, полученный из графа интервалов после удаления некоторых специальных конъюнкций, является лесом, то есть 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 упрощенного графа интервалов. Сложность описанных алгоритмов линейно зависит от числа вершин в упрощенном графе интервалов для исходной функции.

Проблема минимизации дизъюнктивных нормальных форм, 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. с 50-х годов прошлого века привлекает внимание, 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, причем описывается в основном типичное поведение соответствующих параметров. В этой постановке получены окончательные или близкие к окончательным результаты по следующим вопросам: сложность сокращенной д. н. ф., сложность самокорректирующихся д. н. ф., сложность реализации булевых операторов, протяженность сокращенной 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 A -алгоритма, кроме того, распознавание предиката «вхождение в сумму минимальных» по сложности полиномиально эквивалентно нахождению минимальной д. н. ф. Разработанные методы применяются к задачам из других разделов теории дискретной оптимизации.

Общеизвестные понятия, не определяемые здесь, можно найти в [116]. Через l_C , $l_{\cap T}$, l_Q , l_{kp} , l_{kp}^s , l_{ko} и l_A обозначим число элементарных конъюнкций соответственно в д. н. ф.: сокращенной, объединение и пересечение тупиковых, Квайна, кратчайшей, кратчайшей из корректирующих s отбрасываний элементарных конъюнкций, получающихся в результате применения к сокращенной д. н. ф. кольцевого алгоритма ранга 2 и A -алгоритма; а через l_{\min} — число букв в минимальной д. н. ф. Пусть ρ — протяженность, Y — разброс, τ — число тупиковых д. н. ф. Через l_C^k обозначим число интервалов размерности k в сокращенной д. н. ф. Пусть P^n — множество всех булевых функций, определенных на $\{0, 1\}^n$; \hat{P}^n — соответствующее множество ча-

стичных булевых функций; $P_{\alpha, m}^n$ — множество всех булевых функций из P^n , принимающих значение α на m наборах; P_m^n — множество всех частичных булевых функций, определенных на m наборах из $\{0, 1\}^n$; $P_m^{n, t}$ — множество всех частичных (n, t) -операторов, определенных на m наборах из $\{0, 1\}^n$; \tilde{P}_{m_1, m_2}^n — множество всех частичных булевых функций из $P_{m_1 + m_2}^n$, принимающих значение 1 на m_2 наборах.

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

Теорема 4.7 ([115]). *Для почти всех булевых функций f из $P_{0, m}^n$ имеет место*

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

если $\log^3 n \leq m \leq 2^n - 1$;

$$l_C(f) \sim \sum_{r=1}^{2^{\lfloor \log n \rfloor}} \binom{m}{r} \cdot 2^r (n \cdot 2^{-r})^r,$$

если $1 = o(m)$, $m \leq \log^3 n$;

$$l_C(f) \sim 2^m \cdot (n \cdot 2^{-m})^m,$$

если $1 \leq m = O(1)$.

Асимптотика получена также для классов \tilde{P}_{m_1, m_2}^n при всех возможных соотношениях между n , m_1 и m_2 . Ранее была известна лишь асимптотика логарифма l_C [117].

Теорема 4.8 ([115]). *Для почти всех булевых функций f из $P_{0, m}^n$ верно:*

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

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

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

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

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

если $2 \leq m \leq 2^{n/2}$.

При $m \sim 2^{n-1}$ отсюда следует результат А. А. Сапоженко [118].

Теорема 4.9 ([115]). *Для почти всех булевых функций f из P_{m_1, m_2}^n верно, что*

$$l_{kp}^s(f) \asymp \left(1 + \frac{s+1}{\beta+1}\right) \cdot l_{kp}(f),$$

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

В ряде случаев можно получить явную асимптотику, например, для почти всех булевых функций из P^n , если $s \rightarrow \infty$, а n специального вида. При $m_1 \sim m_2 \sim 2^{n-1}$, $s \gg \log \log n$ из этой теоремы вытекает результат Н. Н. Кузюрина [119].

Теорема 4.10 ([115]). *Для почти всех операторов F из $P_m^{n,t}$ выполнено:*

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

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 ее элементарных конъюнкций, код булевой функции — из кодов совершенной д. н. ф. и совершенной д. н. ф. ее отрицания. Пусть $T(f)$ — время работы машины T на коде булевой функций f .

Положим

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

Теорема 4.11 ([115]). *Можно указать машины T_{\min} и T_{kp} , вычисляющие по коду булевой функции f код ее минимальной и, соответственно, кратчайшей д. н. ф., и константу c такие, что:*

$$\begin{aligned} T_{\min}(n) + T_{kp}(n) &\leq 2^{c \cdot n} \cdot 2^{2^{n+1}}, \\ T_{kp}(n, m_1, m_2) &\leq (n \cdot (m_1 + m_2))^c \cdot 2^{2 \cdot m_2} \cdot \min \{2^n, 2^{m_2}\}, \\ T_{\min}(n, m_1, m_2) &\leq (n \cdot (m_1 + m_2))^c \cdot 2^{2 \cdot m_2} \cdot \\ &\quad \cdot (\min \{2^n, 2^{m_2}\} + 2^{-m_2} \cdot \min \{2^n, 2^{2 \cdot m_1}\}). \end{aligned}$$

Сравнение полученных оценок с оценками для числа тупиковых д. н. ф. (см. [116]) показывает, что последнее, как правило, растет 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 назовем полиномиально эквивалентными, если для любой машины T_A , решающей задачу A , найдется машина T_B , решающая задачу B , и константа c такие, что $T_B(n) \leq 2^{cn} T_A(n)$, и наоборот.

Теорема 4.12 ([115]). *Следующие задачи полиномиально эквивалентны:*

- 1) по частичной булевой функции f найти некоторую ее минимальную 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 ее элементарной конъюнкции K вычислить значение предиката «элементарная конъюнкция принадлежит д. н. ф. сумма минимальных»;
- 4) по частичной булевой функции f найти длину ее минимальной д. н. ф.

Эта теорема объясняет обнаруженное Ю.И. Журавлевым [116] 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 ([115]).

а) Для почти всех булевых функций f из P^n имеет место:

$$l_{\cup T}(f) = l_Q(f) = l_C(f) \sim l_A(f) \sim l_{ko}(f),$$

$$l_{\cap T}(f) \sim \sum_{r=\lceil \log \log n \rceil}^{\lceil \log \log n \rceil + 1} \binom{n}{r} \cdot 2^r \cdot 2^{-2^r}.$$

б) При $1 \leq m \leq 2^n - 2$ для почти всех булевых функций f из $\tilde{P}_{1,m}^n$ верно:

$$\begin{aligned} & - l_Q(f) \sim l_{\cup T}(f) \sim l_A(f), \quad l_C(f) = O(l_A(f)), \\ & - l_C(f) \sim l_C^0(f) + l_C^1(f), \text{ если } m = O(2^n/n), \\ & - l_{\cup T} = l_Q(f) = l_C(f), \text{ если } m \geq (1 + \varepsilon) \cdot 2^n(\sqrt{2} - 1)/\sqrt{2}, \\ & - l_A(f) = l_C(f), \text{ если } m \geq (1 + \varepsilon) \cdot 2^{n-1}, \\ & - l_{\cap T}(f) = 0, \text{ если } \log n \ll 2^n - m \leq 2^{n-1}(1 - \varepsilon), \end{aligned}$$

где $\varepsilon \in (0, 1/2)$.

в) Если $m \sim 2^{\varepsilon n}$, $\varepsilon \in [1/2, 1)$ то для почти всех булевых функций f из $P_{0,m}^n$ имеет место:

$$\log \log \tau(f) \sim n, \quad \rho(f) = \left\lceil \frac{1}{1 - \varepsilon} \right\rceil,$$

$$\log Y(f) \sim (1 - \varepsilon)n \sim \dim f,$$

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

Ранее полученные результаты [116] следуют из п. а) Теоремы 4.13. Отметим, что при $m \sim 2^{\varepsilon n}$, $\varepsilon \in [1/2, 2/3]$, мы получаем из $P_{0,m}^n$ примеры массивных классов плотных булевых функций, причем существенно более простые, чем у Ю. Л. Васильева [120, 121]. 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 минимальной д. н. ф. Однако реализация кольцевого алгоритма требует анализа существенно большего числа частичных булевых функций. Следовательно, в этом случае трудоемкость 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 приведенный вес элементов этого базиса.

Теорема 4.14 ([115]). *Для почти всех булевых функций f из P_m^n выполнено:*

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

если $\log n \ll m \leq n^{1+o(1)}$.

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 [122] эта теорема дает 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 ([115]). *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 $1 \leq C(m, n) \leq 2$, если $\log n \ll m \leq n^{o(1)}$. Константа может быть вычислена эффективно.

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

Теорема 4.16 ([115]). Для почти всех графов g с n вершинами и t ребрами верно:

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

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

При $\lambda \sim 1$ из этой теоремы следует результат А. Д. Коршунова [123].

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

Теорема 4.17 ([115]). Для почти всех булевых функций f из P^n имеет место:

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

Эта оценка совпадает по порядку с полученной С. Е. Кузнецовым [124] нижней оценкой.

5. Булевы уравнения

Многие задачи теории управляющих систем, дискретной оптимизации, распознавания образов, технической диагностики и др. [53, 63] 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 — дизъюнктивная нормальная форма (д. н. ф.) Так, например, задача построения тупиковых тестов приводит к исследованию систем булевых уравнений вида

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

Проверка разрешимости системы булевых уравнений является одной из NP -полных проблем, причем NP -полнота сохраняется даже в случае, если каждое уравнение является дизъюнкцией трех 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 работах [64]–[67] исследовались вопросы классификации систем булевых уравнений, существования и единственности их решений, представления решений в параметрическом виде. Однако весьма актуальной остается 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. Все существующие универсальные методы решения систем булевых уравнений [57, 63, 68]–[78] не позволяют элиминировать этот перебор. При этом остается открытым вопрос о принципиальной возможности такой элиминации.

Для обхода этих трудностей существует два традиционных пути. Первый из них заключается в разработке алгоритмов, ориентированных на достаточно узкие классы систем. Это направление активно развивается разными авторами [61, 63, 79]–[84]. Второй путь элиминации перебора состоит в построении алгоритмов малой трудоемкости, находящих приближенное 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 [85].

Очевидно, что естественной нижней оценкой сложности любого алгоритма может служить число решений. Такой подход был применен, например, в работах [86]–[89] при решении задачи поиска всех тупиковых тестов, где были разработаны алгоритмы, имеющие слож-

ность, 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 эквивалентных 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 еще трудно сделать. Это связано также и с тем, что список разработанных алгоритмов решения булевых уравнений не широк и разнороден.

В связи с этим актуальной является задача оценивания числа решений систем булевых уравнений, которое служит естественной нижней оценкой сложности соответствующих алгоритмов.

В работах [90, 91] исследовался вопрос о типичном значении числа решений таких систем булевых уравнений, где каждому уравнению соответствует случайная булева функция, без учета того, в каком виде она задана.

Целью исследований Т. И. Игамбердыева является исследование систем булевых уравнений заданных в конкретных базисах, получение для них точных и асимптотических оценок числа решений и построение на основе этих оценок приближенных алгоритмов решения систем булевых уравнений.

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.

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

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

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

Определим ряд понятий, необходимых для изложения основных результатов.

Пусть M — некоторое множество. Через $|M|$ обозначим число его элементов, называемое мощностью множества M .

Символом E_2 обозначим множество $\{0, 1\}$, а E_2^n — множество всех точек $\tilde{a} = (a_1, \dots, a_n)$, где $a_i \in E_2$ ($i = 1, \dots, n$).

Значит, E_2^n — это множество всех вершин единичного n -мерного куба B^n .

Через P_2 обозначим множество всех булевых функций, то есть таких функций, у которых переменные и сами функции принимают значения из E_2 .

Пусть

$$x^\sigma = \begin{cases} x, & \text{если } \sigma = 1 \\ \bar{x}, & \text{если } \sigma = 0 \end{cases}$$

Элементарной конъюнкцией ранга r называется логическое произведение $x_{i_1}^{\sigma_1} \& x_{i_2}^{\sigma_2} \& \dots \& x_{i_r}^{\sigma_r}$, где все x_{i_j} различны.

Дизъюнктивная нормальная форма (д. н. ф.) есть логическая сумма $D(x_1, \dots, x_n) = K_1 \vee \dots \vee K_t$ различных элементарных конъюнкций K_j . Число элементарных конъюнкций в д. н. ф. называется ее длиной и обозначается $\|d\|$.

Если булева функция представима в виде д. н. ф., то говорят, что последняя реализует данную функцию.

Каждой булевой функции $f(x_1, \dots, x_n)$ поставим в соответствие подмножество N_f множества E_2^n всех \tilde{a} таких, что $f(\tilde{a}) = 1$.

Подмножество $N_k \subset E^n$, соответствующее элементарной конъюнкции K ранга r , называется интервалом размерности $n - r$.

Пусть $f(x_1, \dots, x_n)$ и $\hat{f}(x_1, \dots, x_n)$ — булевы функции, причем $N_f \subseteq N_{\hat{f}}$. Говорят, что функция $\hat{f}(x_1, \dots, x_n)$ аппроксимирует сверху функцию $f(x_1, \dots, x_n)$.

В дальнейшем величину $|N_{\hat{f}} \setminus N_f|$ будем называть погрешностью, а

$$\Pi(\hat{f}, f) \geq |N_{\hat{f}} \setminus N_f|$$

— оценкой погрешности аппроксимации.

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

Обозначим через

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

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

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

— дисперсию, или среднеквадратичное отклонение функции φ .

Пусть $A_s = \{a_1, \dots, a_s\}$ — 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 $s \rightarrow \infty$ обладают свойством Q , если $\lim_{s \rightarrow \infty} \frac{P_s(Q)}{|A_s|} = 1$.

Пусть

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

— система булевых уравнений.

Рассматривается 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 систем m , число элементарных конъюнкций во всех д. н. ф., соответствующих уравнениям, одинаково и равно t , и число букв во всех элементарных конъюнкциях одинаково и равно r . Изучен 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 $r \rightarrow \infty$, $MG \rightarrow \infty$, $t2^{-r} - n \ln n \gg n$, или условий $r \rightarrow \infty$, $MG > 2^{\delta n}$, 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

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

Рассматривается 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 , и число букв в каждом слагаемом равно r . Изучен 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 $n \rightarrow \infty$, и все параметры являются функциями от n .

Теорема 5.3. *Для любого $\delta \in (0, 1)$ найдется 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} .*

Известно, что одной из наиболее удобных и часто применяемых форм задания булевых функций является д. н. ф. В частности, булевы уравнения, возникающие на практике, как правило задаются в виде д. н. ф., то есть $D(x_1 \dots x_n) = K_1 \vee K_2 \vee \dots \vee K_t$, где K_i ($1 \leq i \leq t$) — элементарные конъюнкции, t называем длиной D .

Нетрудно видеть, что сложность решения системы таких уравнений

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

с помощью алгоритмов, предлагаемых, например, в [71], зависит от длин уравнений t_i ($1 \leq i \leq m$), уменьшая которые, можно существенно упростить решение. В связи с этим возникает задача аппроксимации булевых функций.

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

Сопоставим д. н. ф. $D(x_1, \dots, x_n)$ граф $G(D)$, вершинами которого являются элементарные конъюнкции из д. н. ф. $D(x_1, \dots, x_n)$, причем две вершины графа соединены только тогда, когда они имеют общие переменные.

Назовем д. н. ф. $D(x_1, \dots, x_n)$ ациклической, если граф $G(D)$ является лесом.

Пусть $\alpha(f) = \frac{2^n - |N_f|}{2^n}$, где n — число переменных функции f , то есть 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 $a = (1 - 2^{\sigma-R})$, $b = 2^{\sigma-R} - 2^{-R}$, $\beta_1 = \frac{a}{2} + \sqrt{\frac{a^2}{4} + b}$, $\beta_2 = \frac{a}{2} - \sqrt{\frac{a^2}{4} + b}$.

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

Теорема 5.4. *Имеет место соотношение*

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

Следствие 5.2. Пусть R и σ — функции от t , причем $\sigma \rightarrow \infty$ и $R - \sigma \rightarrow \infty$ при $t \rightarrow \infty$. 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. $D \in \bigcup_{t=0}^{\infty} D(R, t)$ найдется д. н. ф. \hat{D} длины не более t_0 такая, что $N_D \subseteq N_{\hat{D}}$, причем

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

Предлагаются конкретные алгоритмы аппроксимации булевых функций и алгоритм решения систем булевых уравнений.

Пусть дана булева функция $f(x_1, \dots, x_n)$, заданная с помощью д. н. ф. $D(x_1, \dots, x_n) = K_1 \vee K_2 \vee \dots \vee K_t$, где $K_i (1 \leq i \leq t)$ — элементарная конъюнкция ранга R .

Предлагаются алгоритмы \mathfrak{U}_1 и \mathfrak{U}_2 , строящие аппроксимирующую функцию $\hat{f}(x_1, \dots, x_n)$, заданную с помощью д. н. ф. $\hat{D}(x_1, \dots, x_n) = \hat{K}_1 \vee \hat{K}_2 \vee \dots \vee \hat{K}_{t_0}$, такую, что $N_f \subseteq N_{\hat{f}}$, причем $t_0 \leq \hat{t}$, где \hat{t} — фиксированный наперед заданный параметр, и по ходу работы алгоритма производится подсчет оценки величины возможной погрешности $\Pi(D, \hat{D}) \geq (|N_{\hat{f}}| - |N_f|)$.

Идеи алгоритмов \mathfrak{U}_1 и \mathfrak{U}_2 основаны на результатах, изложенных выше. Они отличаются друг от друга сложностью реализации и точностью приближения.

Описывается алгоритм, основанный на применении аппроксимации булевых функций с помощью одного из описанных алгоритмов \mathfrak{U}_1 или \mathfrak{U}_2 .

Пусть дана система булевых уравнений, заданных в виде д. н. ф.

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

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

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

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 путем проверки.

Список литературы

- [1] Shannon C. E. The synthesis of two-terminal swithing circuits // Bell Syst. Techn. J. 1949. V. 28. N 1. P. 59–98.
- [2] Лупанов О. Б. О вентильных и контактно-вентильных схемах // Доклады АН СССР. 1956. Т. 111. № 6. С. 1171–1174.
- [3] Лупанов О. Б. О синтезе контактных схем // Доклады АН СССР. 1958. Т. 119. № 1. С. 23–26.
- [4] Лупанов О. Б. Об одном методе синтеза схем // Известия вузов. Радиофизика. 1958. Т. 1. № 1. С. 120–140.
- [5] Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. 1960. Вып. 3. С. 61–80.
- [6] Лупанов О. Б. Об одном классе схем из функциональных элементов (формулы с конечной памятью) // Проблемы кибернетики. 1962. Вып. 7. С. 61–114.
- [7] Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. 1963. Вып. 10. С. 63–97.

- [8] Лупанов О. Б. О сложности реализации функций алгебры логики релейно-контактными схемами // Проблемы кибернетики. 1964. Вып. 11. С. 25–47.
- [9] Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. 1970. Вып. 23. С. 43–81.
- [10] Яблонский С. В. О классах функций алгебры логики, допускающих простую схемную реализацию // Успехи математических наук. 1957. Т. 12. Вып. 6. С. 189–196.
- [11] Яблонский С. В. Об алгоритмических трудностях синтеза минимальных контактных схем // Проблемы кибернетики. 1959. Вып. 2. С. 75–121.
- [12] Лупанов О. Б. О принципе локального кодирования и реализации функций из некоторых классов схемами из функциональных элементов // Доклады АН СССР. 1961. Т. 140. № 2. С. 322–325.
- [13] Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. 1965. Вып. 14. С. 31–110.
- [14] Потапов Ю. Г., Яблонский С. В. О синтезе самокорректирующихся контактных схем // Доклады АН СССР. 1960. Т. 134. № 3. С. 543–547.
- [15] Мадатян Х. А. О синтезе схем корректирующих размыканий контактов // Доклады АН СССР. 1964. Т. 159. № 2. С. 290–293.
- [16] Нечипорук Э. И. О топологических принципах самокорректирования // Доклады АН СССР. 1968. Т. 179. № 4. С. 786–789.
- [17] Нечипорук Э. И. О корректировании обрывов в вентильных и контактных схемах // Кибернетика. 1968. № 5. С. 40–48.
- [18] Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. 1969. Вып. 21. С. 5–102.
- [19] Нечипорук Э. И. О топологических принципах самокорректирования // Проблемы кибернетики. 1973. Вып. 26. С. 19–26.
- [20] Редькин Н. П. О самокорректировании контактных схем // Проблемы кибернетики. 1978. Вып. 33. С. 119–138.

- [21] Редькин Н. П. О самокорректировании контактных схем, II // Проблемы кибернетики. 1979. Вып. 36. С. 195–208.
- [22] Улиг Д. Самокорректирующиеся контактные схемы исправляющие большое число ошибок // Доклады АН СССР. 1978. Т. 241. № 6. С. 1273–1276.
- [23] Кириенко Г. И. О самокорректирующихся схемах из функциональных элементов // Проблемы кибернетики. 1964. Вып. 12. С. 29–37.
- [24] Кириенко Г. И. Синтез самокорректирующихся схем из функциональных элементов для случая растущего числа ошибок в схеме // Дискретный анализ. 1970. Вып. 16. С. 38–43.
- [25] Улиг Д. О синтезе самокорректирующихся схем из функциональных элементов с малым числом ненадежных элементов // Математические заметки. 1974. Т. 15. № 6. С. 937–944.
- [26] Ортюков С. И. Об оценках функции Шеннона для схем из ненадежных функциональных элементов // Проблемы кибернетики. 1983. Вып. 40. С. 269.
- [27] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. М.: Наука, 1966.
- [28] Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. 1960. Вып. 3. С. 61–80.
- [29] Андреев А. Е. О синтезе самокорректирующихся управляющих систем // Доклады АН СССР. 1984. Т. 277. № 3. С. 521–525.
- [30] Андреев А. Е. Универсальный принцип самокорректирования // Математический сборник. 1985. Т. 127 (169). № 6. С. 147–172.
- [31] Андреев А. Е. О сложности монотонных функций // Вестник Московского университета. Серия 1: Математика, механика. 1985. № 4. С. 83–87.
- [32] Андреев А. Е. Метод бесповторной редукции синтеза самокорректирующихся схем // Доклады АН СССР. 1985. Т. 283. № 2. С. 265–269.

- [33] Андреев А. Е. О синтезе топологических функциональных сетей / Препринт № 259 ИПМех АН СССР и МГУ им. М. В. Ломоносова. 1985. С. 1–67.
- [34] Андреев А. Е. О синтезе контактных многополюсников // 7-я Всесоюзная конференция «Проблемы теоретической кибернетики», тезисы докладов. Иркутск, 1985. С. 9–10.
- [35] Андреев А. Е. О синтезе функциональных сетей / Докторская диссертация. МГУ. 1985.
- [36] Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // ДАН СССР. 1985. Т. 281. № 2. С. 1033–1037.
- [37] Васильев Ю. Л. О сравнении сложности тупиковых и минимальных дизъюнктивных нормальных форм // Проблемы кибернетики. Вып. 10. М.: Физматгиз, 1963. С. 5–61.
- [38] Васильев Ю. Л. К вопросу о числе тупиковых и минимальных дизъюнктивных нормальных форм // Дискретный анализ. Вып. 2. Новосибирск: ИМ СО АН СССР, 1964. С. 3–9.
- [39] Викулин А. П. Оценка числа конъюнкций в сокращенной д. н. ф. // Проблемы кибернетики. Вып. 19. М.: Наука, 1974. С. 151–166.
- [40] Журавлев Ю. И. Теоретико-множественные методы алгебры логики // Проблемы кибернетики. Вып. 8. М.: Физматгиз, 1962. С. 5–14.
- [41] Журавлев Ю. И. Алгоритмы упрощения дизъюнктивных нормальных форм конечного индекса // ДАН СССР. 139. № 6. 1961. С. 1329–1331.
- [42] Журавлев Ю. И. Локальные алгоритмы вычисления информации // Кибернетика. № 1. 1965. С. 12–19.
- [43] Журавлев Ю. И. Оценка сложности локальных алгоритмов для некоторых экстремальных задач на конечных множествах // ДАН СССР. 158. № 5. 1964. С. 1018–1021.
- [44] Дискретная математика и математические вопросы кибернетики. Т. 1. М.: Наука, 1974. С. 67–148.
- [45] Коршунов А. Д. О числе монотонных булевых функций // Проблемы кибернетики. Вып. 38. М.: Наука, 1981. С. 5–108.

- [46] Сапоженко А. А. Метрические свойства почти всех функций алгебры логики // Дискретный анализ. Вып. 10. Новосибирск: ИМ СО АН СССР, 1967. С. 91–119.
- [47] Холл М. Комбинаторика. М.: Мир, 1970.
- [48] Яблонский С. В. Функциональные построения в k -значной логике // Труды МИ АН СССР. 51. М.: АН СССР, 1958. С. 5–142.
- [49] Katona G. A theorem of finite sets, Theory of Graph. New York, London, 1969. P. 187–208.
- [50] Нгуен Ким Ань. О некоторых характеристиках алгоритмов минимизации булевых функций // ДАН СССР.
- [51] Нгуен Ким Ань. Некоторые характеристики алгоритмов минимизации булевых функций // Тезисы докладов IV Всесоюзной конференции по математической логике. Тбилиси, 1982.
- [52] Нгуен Ким Ань. О некоторых характеристиках алгоритмов минимизации булевых функций // Проблемы кибернетики.
- [53] Бибило П. Н., Енин С. В. Декомпозиция булевой функции с минимальным числом существенных аргументов подфункций // Известия АН СССР. Техн. киб. 1980. № 3. С. 123–129.
- [54] Menicon G. Umfassende Rechnerprogramme Losung vielschichtiger Luverlassigkeitsprobleme // Elek.-Nachr. 1973. N 3. S. 267–276.
- [55] Закревский А. Д. Алгоритмы синтеза дискретных автоматов. М.: Наука, 1971.
- [56] Амбарцумян А. А., Малевич А. Н. Синтез программ логического управления по алгоритму, заданному системой функций возбуждения и выходов // Проектирование устройств логического управления. М.: Наука. С. 41–52.
- [57] Горелик А. Л., Скрипкин В. А. Методы распознавания. М.: Высшая школа, 1984.
- [58] Яблонский С. В., Демидова Н. Г., Константинов Р. М., Королева 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.
- [59] Соловьев Н. А. Тесты. Новосибирск: Наука, 1978.

- [60] Константинов Р. М., Королева З. Е. Применение тестовых алгоритмов к задачам геологического прогнозирования // Распознавание образов. Труды Международного симпозиума 1971 г. по практическим применениям методов распознавания образов ВЦ АН СССР. М., 1973. С. 194–204.
- [61] Сафарян А. А. О решении систем булевых уравнений, возникающих при построении тестов и систем нельсоновского типа // Журнал выч. мат. и мат. физ. 24. № 10. С. 1590–1595.
- [62] Яблонский С. В. Функциональные построения в k -значной логике // Труды МИАН им. Стеклова. 1958. Т. 51. С. 5–142.
- [63] Кабулов А. В. Приложения дискретной математики к кибернетике. Ташкент: ФАН, 1982.
- [64] Коваленко И. Н. К вычислению вероятности единственности решения системы случайных нелинейных булевых уравнений // Кибернетика. 1973. № 3. С. 12–15.
- [65] Skala Helen. The general solution of an arbitrary Boolean equations // Amer. Math. Monthly. 1967. 74. N 9. P. 1074–1077.
- [66] Bochman D., Posthoff Ch. Die Behandlung Booleischer Gleichungen mit Hilfe des Booleschen Differentialkalküls // Sitzungsber Akad. Wiss. DDR. Math.-Naturwiss.-Tech. 1979. N 12. S. 5–25.
- [67] Bankovic Dragic. Solving systems of arbitrary equations // Discrete Math. 1983. 46. N 3. P. 305–309.
- [68] Antoniu Svoboda. An Algorithm for solving Boolean Equations // IEEE Trans. compt. Vol. EC-12. Oct. 1963. N 5. P. 557–560.
- [69] Уткин А. А. Решение логических уравнений // Автоматизация логического проектирования. Минск: ИТК АН БССР, 1982. С. 41–58.
- [70] Кабулов А. В. Игамбердыев Т. М. Об одном подходе к решению систем логических уравнений // Вопросы вычислительной и прикладной математики. Ташкент, 1984. Вып. 74. С. 68–73.
- [71] Закревский А. Д. Логические уравнения. Минск: Наука и техника, 1975.
- [72] Григорян Ю. Г. Алгоритм решения системы логических уравнений // Журнал выч. мат. и мат. физ. 1962. Т. 2. № 1. С. 186–189.

- [73] Tapia Moier A., Tucker Jerry H. Complete solution of Boolean equations // IEEE Trans comput. 1980. 29. N 7. P. 662–665.
- [74] Vaquero A., Iglesias M. Aplicacion del metodo de resolution de S.E.B. de Tagia and Tucker a la sintesis de funkiones multiples // Revista inf. y autom. 1983. 16. N 58. P. 35–39.
- [75] Brown F. M. Reduced solution of Boolean equations // IEEE Trans. comput. Vol. C–19. Oct. 1970. P. 970–981.
- [76] Свобода А., Чулик К. Алгоритм для решения булевых уравнений // Автоматика и телемеханика. 1964. 25. № 3. С. 374–381.
- [77] Сериков Ю. А. Алгебраический метод решения логических уравнений // Изв. АН СССР. Техн. киб. 1972. № 2. С. 114–124.
- [78] Follinger Otto. Die Losung Boolischer Gleichungen // Elektron Datenverard. 1965. 5. N 6. S. 253–260.
- [79] Егиазарян Э. В. Об одном классе систем булевых уравнений // Журнал выч. мат. и мат. физ. 1976. № 4. С. 1073–1077.
- [80] Сафарян А. А. NP-полнота задачи разбиения систем булевых уравнений на минимальные блоки. М.: ВЦ АН СССР, 1984.
- [81] Чистов В. П. О системах логических уравнений // Деп. ин-т мат. и мех. Урал. науч. центра АН СССР. Свердловск, 1984.
- [82] Нечепуренко М. Н. Элементы булева интервального анализа // Системное моделирование в информатике. Новосибирск: ВЦ СО АН СССР, 1985. С. 37–61.
- [83] Peeva K. Sistsms of linear equations over a bounded chain // Acta Cybernetica. 7. Fas. 2. Forum centre publ. cybern. Hungaricum Szeged. 1985. P. 195–202.
- [84] Леонтьев В. К. Нурлыбаев А. Н. Об одном классе систем булевых уравнений // Журнал выч. мат. и мат. физ. 1975. 15. № 6. С. 1568–1579.
- [85] Матросова А. Ю. Об объеме вычислений при решении булевых уравнений // Мат. сб. Томского ун-та. 1975. Вып. 2. С. 120–128.
- [86] Андреев А. Е. О тупиковых и минимальных тестах // ДАН СССР. 1981. 256. № 3. С. 521–524.

- [87] Андреев А. Е. О качественных и метрических свойствах тестовых алгоритмов / Автореф. дис. канд. физ.-мат. наук. М.: ВЦ АН СССР, 1981.
- [88] Андреев А. Е. Об асимптотическом поведении числа тупиковых тестов и минимальной длины теста для почти всех таблиц // Проблемы кибернетики. Вып. 41. С. 117–141. М.: Наука, 1984.
- [89] Дюкова Е. В. Об асимптотически оптимальном алгоритме построения тупиковых тестов для бинарных таблиц // Проблемы кибернетики. Вып. 34. С. 169–186. М.: Наука, 1978.
- [90] Егиазарян Э. В. Метрические свойства систем булевых уравнений // Доклады АН Арм. ССР. 1981. 72. № 2. С. 67–72.
- [91] Егиазарян Э. В. Оценки, связанные с числом решений систем булевых уравнений // Вопросы кибернетики, комбинаторный анализ и теория графов. М., 1980. Вып. 64. С. 124–130.
- [92] Феллер В. Введение в теорию вероятностей и ее приложения. Т. 1. М.: Мир, 1984.
- [93] Дискретная математика и математические вопросы кибернетики / Под общей редакцией Яблонского С. В. и Лупанова О. Б. Т. 1. М.: Наука, 1974.
- [94] Курош А. Г. Курс высшей алгебры. М.: Наука, 1975.
- [95] Марков А. А. О минимальных контактно-вентильных двуполосниках для монотонных симметрических функций // Проблемы кибернетики. 1962. Вып. 8. С. 117–122.
- [96] Нечипорук Э. И. Об одной булевской матрице // Проблемы кибернетики. 1969. Вып. 21. С. 237–240.
- [97] Нечипорук Э. И. О реализации дизъюнкции и конъюнкции в некоторых монотонных базисах // Проблемы кибернетики. 1970. Вып. 23. С. 291–294.
- [98] Paterson M. S. Complexity of monotone networks for boolean matrix product // Theoretic Computer Science. 1975. V. 1. P. 13–20.
- [99] Pratt V. P. The effect of basis on size of Boolean expressions // Proc. of 16th Ann. Symp. Found. of Comp. Sci. New York, 1975. P. 119–121.

- [100] Pipendger N. On another Boolean matrix // IBM Research Report RC-6914. 1977.
- [101] Mehlhorn K., Galil Z. Monotone switching circuits and Boolean matrix product // Computing. 1976. V. 16. P. 99–111.
- [102] Mehlhorn K. Some remarks on Boolean sums // Acta Informatica. 1979. V. 12. P. 371–375.
- [103] Wegener I. Switching functions whose monotone complexity is nearly quadratic // Theoretical Computer Science. 1979. V. 9. P. 83–97.
- [104] Окольнішнікова Е. А. Монотонна булева система з квадратичною складністю реалізації в базисі $\{\&, \vee, 0, 1\}$ // Дискретний аналіз. 1984. Вып. 41. С. 81–98.
- [105] Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // Препринт № 248 ИПМех АН СССР и МГУ. 1985. С. 1–15.
- [106] Андреев А. Е. Об одном методе получения нижних оценок сложности индивидуальных монотонных функций // ДАН СССР. 1985. Т. 282. С. 1033–1037.
- [107] Разборов А. А. Нижние оценки монотонной сложности некоторых булевых функций // ДАН СССР. 1985. Т. 281. № 4. С. 798–801.
- [108] Разборов А. А. Нижние оценки монотонной сложности логического перманента // Матем. заметки. 1985. Т. 37. № 6. С. 887–908.
- [109] Андреев А. Е. Об одном методе получения эффективных нижних оценок монотонной сложности // Алгебра и логика. 1987. № 1. С. 3–26.
- [110] Субботовская Б. А. О реализации линейных функций формулами в базисе $\{\&, \vee, \neg\}$ // ДАН СССР. 1961. Т. 136. № 3. С. 553–555.
- [111] Нечипорук Э. И. Об одной булевой функции // ДАН СССР. 1966. Т. 169. № 4. С. 765–767.
- [112] Храпченко В. М. Об одном методе получения нижних оценок сложности π -схем // Математические заметки. 1971. Т. 10. № 1. С. 83–92.

- [113] Храпченко В. М. Нижние оценки сложности схем из функциональных элементов (обзор) // Кибернетический сборник. 1984. Вып. 21. С. 3–54.
- [114] Андреев А. Е. Об одном методе получения более чем квадратичных эффективных нижних оценок сложности π -схем // Вестник Моск. Ун-та. Сер. 1: Математика, механика. 1987. № 1. С. 70–73.
- [115] Андреев А. Е. К проблеме минимизации дизъюнктивных нормальных форм // ДАН. 1984. Т. 274. № 2. С. 265–269.
- [116] Яблонский С. В. и др. Дискретная математика и математические вопросы кибернетики // М.: Наука, 1974.
- [117] Глаголев В. В. // ДАН. 1964. Т. 158. № 4. С. 770–773.
- [118] Сапоженко А. А. // ДАН. 1968. Т. 180. № 1. С. 32–35.
- [119] Кузюрин Н. Н. // Комбинаторно-алгебраические методы в прикладной математике. Горький, 1980. С. 88–98.
- [120] Васильев Ю. Л. // ДАН. 1966. Т. 171. № 1. С. 13–16.
- [121] Васильев Ю. Л. // Дискретный анализ. Новосибирск, 1978. Вып. 32. С. 21–33.
- [122] Шоломов Л. А. // Проблемы кибернетики. М.: Наука, 1969. Вып. 21. С. 215–226.
- [123] Коршунов А. Д. // Дискретный анализ. Новосибирск, 1980. Вып. 35. С. 15–44.
- [124] Кузнецов С. Е. // Дискретный анализ. Новосибирск, 1981. Вып. 37. С. 51–64.