Московский государственный университет имени М. В. Ломоносова

Факультет вычислительной математики и кибернетики

С. А. Ложкин

Дополнительные главы кибернетики

(группы 411–419, 2018–2019 уч. год)

Москва 2019

Оглавление

§1 Задача синтеза схем для функций (операторов) из специального класса, мощностные нижние оценки функции Шеннона для их сложности в случае невырожденного (ненулевого, квазиинвариантного) класса

Для множества ФАЛ Q, $Q \subseteq P_2$, и натурального n через $Q(n)$ будем обозначать множество $Q \cap P_2(n)$. При этом, как само множество Q, так и связанную с ним последовательность $Q(1), Q(2), \ldots$ будем называть *классом ФАЛ*. Аналогичным образом последовательность $Q(1), \ldots, Q(n), \ldots$, где $Q(n) \subseteq P_2^m(n)$ и $m = m_Q(n)$, а также их объединение называется *классом операторов*. Будем предполагать, что ни одно из множеств $Q(n)$, $n = 1, 2, \ldots$, рассматриваемого класса ФАЛ или операторов Q не является пустым и, как правило, $|Q(n)| \geqslant 3$.

Пусть заданы класс ФАЛ или операторов Q, класс схем $\mathcal{U}$ и функционал сложности $\mathcal{L}$. Тогда *функцией Шеннона для класса ФАЛ или операторов Q при их реализации в классе схем $\mathcal{U}$ относительно функционала сложности $\mathcal{L}$* называется функция натурального аргумента

$$\mathcal{L}(Q(n)) = \max_{f \in Q(n)} \mathcal{L}(f),$$

где $\mathcal{L}(f)$ — минимальная $\mathcal{L}$–сложность схем из $\mathcal{U}$, реализующих (систему) ФАЛ f. В дальнейшем будем, для простоты, рассматривать в качестве $\mathcal{U}$ класс $\mathcal{U}^{\mathrm{C}}$ — класс СФЭ над базисом $\text{Б}_0 = \{\&, \vee, \neg\}$, а в качестве $\mathcal{L}(\Sigma)$ — функционал $L(\Sigma)$, равный числу элементов в СФЭ Σ. Для класса ФАЛ или операторов Q' и класса ФАЛ Q'' введём функции

$$\mathcal{J}\big(|Q'(n)|\big) = \frac{\log |Q'(n)|}{\log\log |Q'(n)|} \quad \text{и} \quad \sigma_{Q''}(n) = \frac{\log |Q''(n)|}{2^n},$$

где $n = 1, 2, \ldots$. При этом последовательность $\sigma_{Q''}(n)$, $n = 1, 2, \ldots$, будем называть *мощностной последовательностью* класса Q'', а из её определения следует, что $0 \leqslant \sigma_{Q''}(n) \leqslant 1$ для всех n.

Класс ФАЛ (операторов) Q называется: 1) *невырожденным*, если $n + m_Q(n) = o\big(\mathcal{J}\big(|Q(n)|\big)\big)$, 2) *строго невырожденным*, если $\log n = o\big(\log |Q(n)|\big)$, 3) *ненулевым* (*нулевым*), если $\varliminf\limits_{n\to\infty} \sigma_Q(n) > 0$ (соответственно $\varlimsup\limits_{n\to\infty} \sigma_Q(n) = \lim\limits_{n\to\infty} \sigma_Q(n) = 0$).

На основе стандартного мощностного метода получения нижних оценок (см. [1, §4 гл. 4]) можно установить справедливость следующего утверждения.

Лемма 1.1 (ср. с леммой 4.2 из [1]). *Если Q — невырожденный класс ФАЛ (операторов), то $L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \mathcal{J}\big(|Q(n)|\big)$, а если Q — строго невырожденный класс ФАЛ, то $L^{\mathrm{K}}\big(Q(n)\big) \gtrsim \mathcal{J}\big(|Q(n)|\big)$.*

Следствие. *Для всякого ненулевого класса ФАЛ Q выполнено асимптотическое неравенство $L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \sigma_Q(n)\frac{2^n}{n}$.*

Класс ФАЛ Q называется *квазиинвариантным* классом, если для некоторого n_0, $n_0 \geqslant 2$, и любого n, $n \geqslant n_0$, для произвольной ФАЛ f, $f \in Q(n)$, при любом σ, $\sigma \in B$, ФАЛ $f(x_1, \ldots, x_{n-1}, \sigma)$ принадлежит $Q(n-1)$. Минимальное число n_0, для которого указанное соотношение выполняется, будем считать *порогом* квазиинвариантного класса Q.

Лемма 1.2. *Пусть Q — квазиинвариантный класс ФАЛ. Тогда существует предел*

$$\sigma_Q = \lim_{n\to\infty} \sigma_Q(n) = \lim_{n\to\infty} \frac{\log |Q(n)|}{2^n},$$

где число σ_Q удовлетворяет неравенствам $0 \leqslant \sigma_Q \leqslant 1$.

Доказательство. Из определения последовательности $\sigma_Q(n)$ следует, что для каждого n выполнено неравенство $0 \leqslant \sigma_Q(n) \leqslant 1$, то есть эта последовательность $\sigma_Q(n)$ ограничена. Покажем, что при $n \geqslant n_0$, где n_0 — порог класса Q, она монотонно не возрастает, откуда будет следовать её сходимость.

В силу квазиинвариантности класса Q, всякую функцию f из множества $Q(n+1)$, где $n \geqslant n_0$, можно представить в виде

$$f(x_1, \ldots, x_{n+1}) = \overline{x}_{n+1} f_0(x_1, \ldots, x_n) \vee x_{n+1} f_1(x_1, \ldots, x_n),$$

где $f_\sigma(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, \sigma)$, $\sigma \in B$, и обе ФАЛ f_0, f_1 принадлежат множеству $Q(n)$. Отсюда сразу вытекает неравенство

$$|Q(n+1)| \leqslant |Q(n)|^2,$$

из которого, в свою очередь, следует, что

$$\sigma_Q(n+1) = \frac{\log |Q(n+1)|}{2^{n+1}} \leqslant \frac{\log |Q(n)|}{2^n} = \sigma_Q(n).$$

Сходимость последовательности $\sigma_Q(n)$, $n = 1, 2, \ldots$, доказана, а принадлежность её предела σ_Q действительному отрезку $[0, 1]$ следует из того, что ему принадлежат все члены данной последовательности.

Лемма доказана. □

Замечание. Предел σ_Q будем называть *мощностной* характеристикой класса Q.

Из определений и леммы 1.2 вытекает, что квазиинвариантный класс Q является нулевым (ненулевым) классом ФАЛ тогда и только тогда, когда $\sigma_Q = 0$ (соответственно $\sigma_Q > 0$). При этом в силу следствия из леммы 1.1 справедливо следующее утверждение.

Лемма 1.3. *Для ненулевого квазиинвариантного класса ФАЛ Q выполняется асмптотическое неравенство $L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \sigma_Q \cdot \frac{2^n}{n}$.*

§2 Синтез схем для функций из специальных классов на основе модификации асимптотически наилучшего метода. Стандартные классы и стандартность класса функций равных нулю на всех наборах значений переменных, номера которых больше заданного числа

Предварительно заметим, что асимптотическое совпадение функций Шеннона $L^{\mathrm{C}}\big(Q(n)\big)$ с её нижней мощностной оценкой из леммы 1.1 является типичным для абсолютного большинства невырожденных «естественных» классов ФАЛ (операторов). В связи с этим введём следующее определение.

Класс ФАЛ (операторов) Q называется *стандартным*, если выполнено асимптотическое неравенство $L^{\mathrm{C}}\big(Q(n)\big) \lesssim \jmath\big(|Q(n)|\big) + O\big(n + m(n)\big)$.

Для $n = 1, 2, \ldots$ и $r = r(n) \geqslant 1$ рассмотрим множество ФАЛ $P_2(n, t)$, которое включает в себя все ФАЛ из $P_2(n)$, обращающиеся в 0 на наборах с номерами $t, t+1, \ldots, 2^n - 1$, и мощность которого равна, очевидно, 2^t. Для любой функции $r = r(n) \geqslant 1$ рассмотрим класс ФАЛ Q, определённый равенствами $Q(n) = P_2(n, r(n))$, $n = 1, 2, \ldots$.

Лемма 2.1. *Для любой функции $r = r(n) \geqslant 1$ соответствующий класс $Q(n) = P_2(n, r(n))$ является стандартным относительно функционала сложности L схем класса $\mathfrak{U}^{\mathrm{C}}$, то есть $L^{\mathrm{C}}\big(Q(n)\big) \lesssim \frac{r}{\log r} + O(n)$.*

Доказательство. Будем считать, для удобства, что при лексикографической ν-нумерации наборов куба B^n от БП $X(n)$, $n = 1, 2, \ldots$, БП x_i «старше» БП x_j, если $i > j$. Полученные при этом предположении оценки сложности будут справедливы, очевидно, и для «обычного» порядка «старшинства» БП.

Рассмотрим сначала случай, когда $r > 2^{n-1}$. Выберем из множества $P_2(n, r)$ произвольую ФАЛ f и построим для неё СФЭ Σ_f с помощью асимптотически наилучшего

метода синтеза (см. §5 гл. 4 из [1]). Напомним, что при этом ФАЛ f (см. доказательство теоремы 5.1) разлагается по БП $x'' = (x_{q+1}, \ldots, x_n)$ следующим образом:

$$f(x',\, x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') f_{\sigma''}(x'),$$

где $x' = (x_1, \ldots, x_q)$, и что для реализации каждой ФАЛ $f_{\sigma''}(x')$ в СФЭ Σ_f используется одна формула $\mathcal{F}_p = y_1 \vee \ldots \vee y_p$, где $p = \left\lceil \frac{2^q}{s} \right\rceil$. Из принадлежности ФАЛ f классу $P_2(n, r)$ следует, что при $\nu(\sigma'') > \left\lceil \frac{r}{2^q} \right\rceil$ функция $f_{\sigma''}(x')$ тождественно равна нулю, и, таким образом, из схемы Σ_f можно удалить подсхемы, реализующие все указанные подфункции. Для сложности полученной при этом СФЭ $\widetilde{\Sigma}_f$ в силу (5.6) (см. §5 гл. 4 из [1]) будет выполняться неравенство

$$L\big(\widetilde{\Sigma}_f\big) \leqslant \left\lceil \frac{r}{2^q} \right\rceil p + O\big(2^{n-q} + p \cdot 2^{s+q}\big),$$

из которого при тех же значениях параметров, что и в указанной выше теореме 5.1, следует, что

$$L\big(\Sigma_f\big) \lesssim \frac{r}{\log r}. \tag{2.1}$$

Пусть теперь $r \leqslant 2^{n-1}$. В этом случае найдём число k такое, что

$$k < n, \qquad 2^{k-1} < r \leqslant 2^k$$

и, следовательно,

$$f(x_1, \ldots, x_n) = \overline{x}_{k+1} \cdot \ldots \cdot \overline{x}_n \cdot f'(x_1, \ldots, x_k). \tag{2.2}$$

Заметим, что функция f' принадлежит классу $P_2(k, r)$, где $r > 2^{k-1}$, и для неё по предыдущему случаю можно построить СФЭ $\widetilde{\Sigma}_{f'}$, удовлетворяющую (2.1). Искомая СФЭ $\widetilde{\Sigma}_f$ строится на основе (2.2) так, что

$$L\big(\widetilde{\Sigma}_f\big) \leqslant L\big(\widetilde{\Sigma}_{f'}\big) + O(n) \lesssim \frac{r}{\log r} + O(n).$$

Лемма доказана. □

Следствие. *Если $n = o\big(\frac{r}{\log r}\big)$, то $Q(n) = P_2(n, r(n))$ — стандартный невырожденный класс ФАЛ, для которого выполнено асимптотическое равенство*

$$L^{\mathrm{C}}\big(Q(n)\big) \sim \frac{r}{\log r}.$$

§3 Асимптотически наилучший метод синтеза схем для ненулевых квазиинвариантных классов, их стандартность

Рассмотрим асимптотически оптимальный метод синтеза СФЭ для ФАЛ из ненулевых квазиинвариантных классов, основанный на их специальном кодировании.

Лемма 3.1. *Для всякого квазиинвариантного класса Q и $n = 1, 2, \ldots$*

$$L^{\mathrm{C}}\big(Q(n)\big) \sim \sigma_Q \frac{2^n}{n} \qquad \text{при } \sigma_Q > 0, \tag{3.1}$$

$$L^{\mathrm{C}}\big(Q(n)\big) = o\Big(\sigma_Q \frac{2^n}{n}\Big) \qquad \text{при } \sigma_Q = 0. \tag{3.2}$$

Доказательство. Рассмотрим сначала случай $\sigma_Q > 0$. В этом случае в соответствии с введёнными в §1 обозначениями и в силу леммы 1.1 получим

$$\mathcal{J}\big(|Q(n)|\big) = \frac{\log |Q(n)|}{\log\log |Q(n)|} = \frac{\sigma_Q(n) \cdot 2^n}{\log(\sigma_Q(n) \cdot 2^n)} \sim \sigma_Q \frac{2^n}{n},$$

откуда по лемме 1.3 следует нижняя оценка (3.1).

Перейдём к получению верхней оценки (3.1). Для этого возьмём произвольное натуральное n и натуральное q, $q \leqslant n$, а затем обычным образом разобьём набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$. Выберем из множества $Q(n)$ произвольную ФАЛ f и для каждого набора σ'', $\sigma'' \in B^{n-q}(x'')$, положим как обычно, $f_{\sigma''}(x') = f(x', \sigma'')$, причём в данном случае $f_{\sigma''}(x') \in Q(q)$ в силу инвариантности класса Q.

Положим $\lambda = \lceil \log |Q(q)| \rceil$ и пусть Π' — произвольное инъективное отображение (кодирование) ФАЛ множества $Q(q)$ двоичными наборами куба B^λ от БП $y = (y_1, \ldots, y_\lambda)$, то есть $\Pi' \colon Q(q) \mapsto B^\lambda(y)$, которое существует, так как $2^\lambda \geqslant |Q(q)|$. Заметим, что ФАЛ $f_{\sigma''}(x')$ однозначно определяется своим «кодом» $\pi_{\sigma''} = \Pi'(f_{\sigma''}(x'))$ и поэтому существует ФАЛ $h(x', y)$, $h \in P_2(q + \lambda)$, такая что

$$f(\sigma', \sigma'') = h(\sigma', \pi_{\sigma''})$$

при любых σ' и σ'' из $B^q(x')$ и $B^{n-q}(x'')$ соответственно.

Пусть $\mathcal{O} = (\mathcal{O}_1, \ldots, \mathcal{O}_\lambda) \in P_2^\lambda(n-q)$ — система ФАЛ, которая сопоставляет произвольному набору σ'', $\sigma'' \in B^{n-q}$, набор («код») $\pi_{\sigma''}$ и пусть СФЭ $\Sigma_{\mathcal{O}}$ из $\mathcal{U}^{\mathrm{C}}$, построенная асимптотически наилучшим методом, реализует эту систему ФАЛ со сложностью

$$L\big(\Sigma_{\mathcal{O}}\big) \leqslant \lambda \frac{2^{n-q}}{n-q} + o\Big(\frac{2^{n-q}}{n-q}\Big).$$

Искомая СФЭ Σ_f реализует ФАЛ f в соответствии с представлением

$$f(x', x'') = h(x', \mathcal{O}(x''))$$

и содержит в качестве подсхемы СФЭ $\Sigma_{\mathcal{O}}(x'', y)$, а также построенную асимптотически наилучшим методом СФЭ Σ_h, которая реализует ФАЛ $h(x', y)$.

Полагая $q = \lceil \log n \rceil$, и учитывая, что

$$\lambda \leqslant \sigma_Q(q) \cdot 2^q + 1 \lesssim \sigma_Q \cdot 2^q,$$

получим верхнюю оценку

$$L\big(\Sigma_f\big) \lesssim \sigma_Q \cdot 2^q \frac{2^{n-q}}{n-q} \lesssim \sigma_Q \frac{2^n}{n}.$$

В случае $\sigma_Q > 0$ отсюда, с учётом нижней оценки, вытекает (3.1).

В случае $\sigma_Q = 0$ искомая СФЭ Σ_f строится аналогично, но так как при этом последовательность $\sigma_Q(q)$ стремится к нулю, то

$$L\big(\Sigma_f\big) = o\Big(\frac{2^n}{n}\Big),$$

что доказывает (3.2).

Лемма доказана. □

§4 Общее описание принципа локального кодирования, его применение для доказательства стандартности класса самодвойственных функций

Как уже говорилось, при доказательстве верхней оценки леммы 3.1 мы фактически использовали приём, называемый *принципом локального кодирования*, предложенный О. Б. Лупановым, который состоит в следующем. Пусть Q — класс операторов, и пусть для каждого натурального n определено кодирование $\Pi = \Pi_n$, ставящее в соответствие произвольному оператору $F = F_n$, $F \in Q(n)$, двоичный набор («код») $\pi = \pi(F)$ длины $d = d(n)$, в котором выделены «куски» π_i, $i \in [1, t]$, составленные из подряд идущих

разрядов кода π и имеющие длину не больше, чем $\lambda = \lambda(n)$. Пусть указанное кодирование обладает свойством «локальности»: для вычисления значения оператора F на произвольном фиксированном наборе σ достаточно знать лишь один кусок кода $\pi_{i(\sigma)}$, задаваемый своими «координатами» (например, позицией его первого разряда в коде и длиной, или номером куска, если куски кода не пересекаются и имеют одинаковую длину, и т. п.).

Пусть, далее, оператор кодирования $A^{(1)} = A^{(1)}_n$ по набору σ вычисляет координаты куска кода $\pi_{i(\sigma)}$, а оператор декодирования $A^{(2)} = A^{(2)}_n$ по куску $\pi_{i(\sigma)}$ и, возможно, набору σ, вычисляет $F(\sigma)$. Искомая схема $\Sigma = \Sigma_n$, реализующая оператор F и построенная на основе локального кодирования Π, состоит из подсхем $A^{(1)}$, $A^{(2)}$ и «основного» блока $\mathcal{O} = \mathcal{O}_n$, который по координатам куска $\pi_{i(\sigma)}$ выдаёт сам этот кусок.

Если при этом сложность указанных выше операторов $A^{(1)}_n$, $A^{(2)}_n$ и $\mathcal{O}_n$ удовлетворяет соотношениям

$$L^{\mathrm{C}}\big(A^{(1)}_n\big) = o\big(\mathcal{J}\big(|Q(n)|\big)\big), \qquad L^{\mathrm{C}}\big(A^{(2)}_n\big) = o\big(\mathcal{J}\big(|Q(n)|\big)\big), \tag{4.1}$$

$$L^{\mathrm{C}}\big(\mathcal{O}_n\big) \lesssim \mathcal{J}\big(|Q(n)|\big), \tag{4.2}$$

то искомая СФЭ Σ_n может быть выбрана так, что $L\big(\Sigma_n\big) \lesssim \mathcal{J}\big(|Q(n)|\big)$. Отсюда вытекает, что $L^{\mathrm{C}}\big(Q(n)\big) \lesssim \mathcal{J}\big(|Q(n)|\big)$, и, следовательно, в силу леммы 1.1 в случае невырожденности класса Q выполняется асимптотическое равенство $L^{\mathrm{C}}\big(Q(n)\big) \sim \mathcal{J}\big(|Q(n)|\big)$, которое означает стандартность класса Q относительно функционала сложности L класса схем $\mathcal{U}^{\mathrm{C}}$.

Заметим, что в случае асимптотической неизбыточности кодирования $\Pi = \Pi_n$, когда $d(n) \sim \log |Q(n)|$, при построении схемы, которая реализует оператор $\mathcal{O}_n$ со сложностью, удовлетворяющей (4.2), достаточно, как правило, использовать асимптотически наилучший метод синтеза СФЭ для произвольных систем ФАЛ подходящей размерности или некоторые его модификации (см., например, лемму 2.1).

Заметим также, что соотношение (4.1) означает возможность существенно более простой по сравнению с оператором $\mathcal{O}_n$ реализации операторов $A^{(1)}_n$ и $A^{(2)}_n$ в классе $\mathcal{U}^{\mathrm{C}}$.

Покажем, что описанный в доказательстве леммы 3.1 асимптотически наилучший метод синтеза СФЭ над базисом $\mathrm{Б}_0$ является примером применения принципа локального кодирования.

Действительно, в обозначениях данного доказательства, локальное кодирование Π сопоставляет произвольной ФАЛ f, $f \in Q(n)$, код π длины $d = \lambda \cdot 2^{n-q}$, разбитый на 2^{n-q} непересекающихся кусков длины λ и вида $\pi_{\sigma''}$, где $\sigma'' \in B^{n-q}$. При этом оператор кодирования $A^{(1)}$ представляет собой оператор выбора поднабора x'' из набора x, оператор $\mathcal{O}$ является основным, а оператор $A^{(2)}$ связан с вычислением ФАЛ h.

Рассмотрим теперь пример применения принципа локального кодирования для доказательства стандартности класса $\mathcal{S}$ — класса самодвойственных ФАЛ.

Лемма 4.1. *Класс самодвойственных ФАЛ является невырожденным стандратным классом ФАЛ и, тем самым,*

$$L^{\mathrm{C}}\big(\mathcal{S}(n)\big) \sim \frac{2^{n-1}}{n}. \tag{4.3}$$

Доказательство. Невырожденность класса $\mathcal{S}$ и нижняя мощностная оценка в (4.3) вытекают из того, что $|\mathcal{S}(n)| = 2^{2^{n-1}}$, т. е. $\mathcal{J}\big(|\mathcal{S}(n)|\big) = \frac{2^{n-1}}{n-1}$, в силу леммы 1.1, так как при этом $n = o\big(\mathcal{J}(|\mathcal{S}(n)|)\big)$.

Возьмём произвольную ФАЛ f, $f \in \mathcal{S}(n)$, и сопоставим ей код $\pi = (\alpha_0, \ldots, \alpha_{2^{n-1}-1})$ длины $d = 2^{n-1}$, который представляет собой первую половину столбца значений $\tilde{\alpha}_f$ ФАЛ f, «разбитую» на 2^{n-1} «кусков» длины $\lambda = 1$. При этом оператор $A^{(1)}_n$ будет представлять собой $(n, n-1)$-оператор $G = (g_1, \ldots, g_{n-1})$, где $g_i(x_1, \ldots, x_n) = x_1 \oplus x_{i+1}$ для всех i, $i = 1, \ldots, n-1$, а его сложность $L^{\mathrm{C}}(G)$ будет не больше, чем $4(n-1)$.

Далее, выберем в качестве основного оператора $\mathcal{O}$ ФАЛ $h(y_1,\dots,y_{n-1})$ со столбцом значений π, а в качестве оператора $A_n^{(2)}$ — ФАЛ $x_1 \oplus z$, где $z = h(y_1,\dots,y_{n-1})$ и $y_i = g_i(x_1,\dots,x_n)$ для всех i, $i = 1,\dots,n-1$. Действительно, в силу самодвойственности ФАЛ f: $f(0,\sigma_2,\dots,\sigma_n) = h(\sigma_2,\dots,\sigma_n)$, $f(1,\sigma_2,\dots,\sigma_n) = \overline{h}(\overline{\sigma}_2,\dots,\overline{\sigma}_n)$. Таким образом, $L^{\mathrm{C}}(f) \leqslant L^{\mathrm{C}}(h) + 4n \lesssim \frac{2^{n-1}}{n}$, что доказывает верхнюю оценку (4.3).

Лемма доказана. □

§5 Применение принципа локального кодирования для доказательства стандартности невырожденных классов симметрических операторов и операторов, связанных с вычислением функции на нескольких последовательных наборах

Рассмотрим теперь два класса операторов[1] и с помощью принципа локального кодирования докажем (при некоторых условиях) их стандартность. Обозначим через S класс всех симметрических ФАЛ.

Лемма 5.1. *Если натуральная последовательность $m = m(n)$, $n = 1, 2, \dots$, такова, что*

$$\log n = o(m) \quad \textit{и} \quad \log m = o(\log n), \tag{5.1}$$

то класс операторов Q, для которого $Q(n) = S^m(n)$, является невырожденным и стандартным (относительно функционала сложности L СФЭ из $\mathcal{U}^{\mathrm{C}}$) классом операторов.

Доказательство. Для рассматриваемого класса операторов Q при любых натуральных n и m выполняется равенство $|Q(n)| = 2^{m(n+1)}$, из которого следует, что

$$\mathcal{J}\big(|Q(n)|\big) = \frac{m(n+1)}{\log m + \log(n+1)}. \tag{5.2}$$

Из (5.2), в свою очередь, вытекает, что последовательности

$$\frac{m}{\mathcal{J}\big(|Q(n)|\big)} = \frac{\log m + \log(n+1)}{n+1} \leqslant \frac{\log m}{n} + o(1),$$
$$\frac{n}{\mathcal{J}\big(|Q(n)|\big)} \leqslant \frac{\log m + \log(n+1)}{m} \leqslant \frac{\log n}{m} + o(1)$$

в силу (5.1) стремятся к 0 при n стремящемся к бесконечности и, следовательно, $m+n = o(\mathcal{J}(|Q(n)|)$, то есть $Q(n)$ — невырожденный класс операторов. Отсюда по лемме 1.1 с учётом (5.1) получаем нижнюю оценку

$$L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \mathcal{J}\big(|Q(n)|\big) \sim \frac{m \cdot n}{\log n}. \tag{5.3}$$

Для получения аналогичной вехней оценки рассмотрим кодирование $\Pi = \Pi_n$, которое оператору F, $F \in Q(n)$, сопоставляет набор $\pi(F) = \pi$ длины $d = m(n+1)$ и вида $\pi = (\, F(0,\dots,0), F(0,\dots,0,1), F(0,\dots,0,1,1), \dots, F(1,\dots,1)\,)$, разбитый на $(n+1)$ непересекающихся кусков длины $\lambda = m$. При этом «координатами» i-го, $i \in [0,n]$, куска кода $\pi_i = F(\,(0,\dots,0,\underbrace{1,\dots,1}_{i})\,)$ будем считать набор $\nu_t^{-1}(i)$, где $t = \lceil \log(n+1) \rceil$.

Следовательно, оператор декодирования $A_n^{(2)}$ является тождественным оператором, а оператор кодирования $A_n^{(1)}$ представляет собой счётчик числа единиц, который набор $\alpha = (\alpha_1,\dots,\alpha_n) \in B^n$ переводит в набор β, $\beta \in B^t$, такой, что $\nu(\beta) = \alpha_1 + \dots + \alpha_n$, и имеет сложность [2]

$$L^{\mathrm{C}}\big(A_n^{(1)}\big) \leqslant 9n.$$

[1] Под (n,m)-оператором будем понимать систему ФАЛ $F = (f_1,\dots,f_m)$ из $P_2^m(n)$.

Заметим, что основной оператор $\mathcal{O}_n$ может быть при этом выбран из множества $P_2^m(t, n+1)$, а его сложность в силу леммы 2.1 удовлетворяет неравенству

$$L^{\mathrm{C}}\big(\mathcal{O}_n\big) \lesssim \frac{t \cdot m}{\log t} + O(n).$$

Таким образом, СФЭ Σ, реализующая оператор F и построенная на основе описанного выше локального кодирования, имеет сложность

$$L(\Sigma) \lesssim \frac{m \cdot n}{\log n} + O(n),$$

которая асимптотически совпадает с нижней оценкой (5.3).

Лемма доказана. □

Лемма 5.2. *Для постоянной последовательности $m = m(n) \geqslant 2$, $n = 1, 2, \ldots$, класс операторов Q, для которого множество $Q(n)$ состоит из всех (n, m)-операторов $F = (f_1, \ldots, f_m)$ таких, что $f_i(\beta) = f_1(\alpha)$ при любом i, $i \in [2, m]$, любом α, $\alpha \in B^n$, и $\nu(\beta) - \nu(\alpha) \equiv i - 1 \pmod{2^n}$, является стандартным (относительно функционала сложности схем из $\mathfrak{U}^{\mathrm{C}}$) классом.*

Доказательство. Так как $|Q(n)| = 2^{2^n}$ и, следовательно, $\mathcal{J}(|Q(n)|) = 2^n/n$, то $n = o(\mathcal{J}(|Q(n)|))$ и Q — невырожденный класс операторов, а из леммы 1.1 непосредственно вытекает необходимая нижняя оценка $L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \dfrac{2^n}{n}$.

Для получения аналогичной верхней оценки возьмём произвольное натуральное n и натуральное q, $q \leqslant n$, а затем обычным образом разобьём набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$. Выберем из $Q(n)$ произвольный оператор $F = (f_1, \ldots, f_m)$ и положим $f = f_1$.

Рассмотрим кодирование $\Pi = \Pi_n$, которое сопоставляет оператору $F = F_n$ набор π длины $d = 2^n + (m-1)$, получающийся удлинением столбца значений $\tilde{\alpha}_f$ ФАЛ f первыми $(m-1)$ разрядами этого же столбца. Выделим в этом наборе 2^{n-q} кусков $\pi_{\sigma''}$, $\sigma'' \in B^{n-q}$, длины $\lambda = 2^q + (m-1)$, где кусок $\pi_{\sigma''}$ получается удлинением той части столбца $\tilde{\alpha}_f$, которая соответствует ФАЛ $f(x', \sigma'')$, на $(m-1)$ следующий за ней разряд.

Легко видеть, что построенное кодирование обладает свойством локальности и что координатами куска кода $\pi_{\sigma''}$ можно считать индексирующий его набор σ'', $\sigma'' \in B^{n-q}$. При этом оператор кодирования $A_n^{(1)}$ является оператором выбора поднабора x'' из набора x, а оператор декодирования $A_n^{(2)}$ и основной оператор $\mathcal{O}_n$ принадлежат множествам $P_2^m(q+\lambda)$ и $P_2^{\lambda}(n-q)$ соответственно. При $q = \left\lceil \frac{1}{2} \log n \right\rceil$ для сложности указанных операторов будут выполняться соотношения

$$L^{\mathrm{C}}\big(A_n^{(1)}\big) = 0, \qquad L^{\mathrm{C}}\big(A_n^{(2)}\big) \lesssim m \cdot \frac{2^{q+\lambda}}{q+\lambda} = o\Big(\frac{2^n}{n}\Big),$$
$$L^{\mathrm{C}}\big(\mathcal{O}_n\big) \lesssim \big(2^q + (m-1)\big) \cdot \frac{2^{n-q}}{n-q} \sim \frac{2^n}{n},$$

из которых следует, что $L^{\mathrm{C}}\big(F_n\big) \lesssim \dfrac{2^n}{n}$.

Лемма доказана. □

§6 Задача синтеза схем для не всюду определённых функций. Особенности получения нижней мощностной оценки соответствующей функции Шеннона, формулировка теоремы о её асимптотическом поведении

Рассмотрим задачу синтеза схем для не всюду определённых функций, которая близка к задаче синтеза схем для ФАЛ из специальных классов.

Отображение $f\colon B^n \mapsto [0,2]$ будем называть *не всюду определённой* ФАЛ от n БП, а множество $f^{-1}(\{0,1\})$ будем считать её *областью определённости* и обозначать через $\delta(f)$. При этом *доопределением* указанной функции f считается любая ФАЛ из $P_2(n)$, совпадающая с f на множестве $\delta(f)$, а под сложностью $L^{\mathrm{C}}(f)$ реализации функции f в классе $\mathcal{U}^{\mathrm{C}}$ понимается наименьшая из соответствующих сложностей её доопределений.

Обозначим через $\widehat{P}_2(n)$ множество всех не всюду определённых ФАЛ от БП $X(n) = \{x_1, \ldots, x_n\}$ и для любого t, $t \in [0, 2^n]$, введём его подкласс $\widehat{P}_2(n,t)$, состоящий из всех тех функций f, $f \in \widehat{P}_2(n)$, для которых $|\delta(f)| = t$.

Функция Шеннона для этого класса определяется стандартным образом:

$$L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) = \max_{f \in \widehat{P}_2(n,t)} L^{\mathrm{C}}(f),$$

причём считается, как обычно, что $t = t(n)$, $n = 1, 2, \ldots$.

Лемма 6.1. *Если* $n \log n = o(t(n))$, *то*

$$L^{\mathrm{C}}\big(\widehat{P}_2(n, t(n))\big) \gtrsim \frac{t(n)}{\log t(n)}. \tag{6.1}$$

Доказательство. Для $n = 1, 2, \ldots$ рассмотрим множество

$$\check{P}_2(n,t) = \{f \in \widehat{P}_2(n,t) \mid \delta(f) = [0,t)\},$$

для каждой из 2^t его функций выберем одно доопределение с минимальной сложностью, и множество этих доопределений обозначим через $Q(n) = Q$. Так как различные функции из $\check{P}_2(n,t)$ не могут иметь общих доопределений, то

$$|\check{P}_2(n,t)| = |Q| = 2^t, \qquad \mathcal{J}(|Q|) = \frac{t}{\log t}.$$

Из последнего равенства и условий леммы следует[1], что $n = o\big(\mathcal{J}(|Q(n)|)\big)$, то есть класс ФАЛ $Q(1), \ldots, Q(n)$, является невырожденным. Из этой невырожденности, леммы 1.1 и очевидных соотношений

$$L^{\mathrm{C}}\big(Q(n)\big) = L^{\mathrm{C}}\big(\check{P}_2(n,t)\big) \leqslant L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big)$$

вытекает оценка (6.1).

Лемма доказана. □

Теорема 6.1. *Если* $n \log^2 n = o(t)$, *то* $L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) \sim \frac{t}{\log t}$.

Замечание. Оценка теоремы верна и при более слабом условии $n \log n = o(t)$ [3].

§7 Асимптотически наилучший метод синтеза схем для не всюду определённых функций в случае их «сильной» определённости

Рассмотрим, далее (см. §7, §8), несколько утверждений, позволяющих установить для исследуемой функции Шеннона верхнюю оценку вида правой части (6.1) при последовательно ослабляемых ограничениях на рост функции $t = t(n)$, то есть доказать теорему 6.1.

Лемма 7.1. *Если* $t = t(n) \sim n$, *то*

$$L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) \lesssim \frac{t(n)}{\log t(n)}. \tag{7.1}$$

[1] Нетрудно показать, что для $t = t(n)$ и $n = 1, 2, \ldots$, условие $n \log n = o(t)$ и $n = o(t/\log t)$ равносильны.

Доказательство. Для произвольного натурального n и натурального q, $1 \leqslant q < n$, разобъём, как обычно, набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$. Выберем натуральный параметр m, $m \leqslant 2^q$, и для любого s, $s \leqslant 2^q$, построим такое множество наборов $\mathfrak{A}_s$ куба B^s, которое «протыкает» (см. [1], лемма 6.2 из §6 гл. 1) все грани ранга не больше чем m, этого куба и состоит не более, чем из $s \cdot 2^m$ наборов. Для каждого отрезка I куба B^q от БП x' рассмотрим множество G_I, состоящее из тех равных 0 вне I ФАЛ $P_2(x')$, «проекции» столбцов значений которых на I принадлежат множеству $\mathfrak{A}_s$, где $s = |I|$.

Определим множество ФАЛ G как объединение множеств G_I по всем отрезкам куба $B^q(x')$ и заметим, что

$$|G| \leqslant 2^{m+3q}, \qquad L^{\mathrm{C}}\big(\overrightarrow{G}\big) \leqslant 2^{m+4q}. \tag{7.2}$$

Заметим также, что любая ФАЛ $\widehat{g}$ из $\widehat{P}_2(q, t')$, где $t' \leqslant m$, равная 0 вне отрезка I куба B^q от БП x', имеет в G_I доопределение.

Возьмём произвольную функцию f, $f \in \widehat{P}_2(n, t)$, и разложим её по БП x'':

$$f(x', x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') f_{\sigma''}(x'), \tag{7.3}$$

где при любом σ'', $\sigma'' \in B^{n-q}$, функция $f_{\sigma''}(x')$ принадлежит множеству $\widehat{P}_2(x', t_{\sigma''})$, причём $\Sigma_{\sigma''} t_{\sigma''} = t$.

Для каждого набора σ'', $\sigma'' \in B^{n-q}$, положим $p_{\sigma''} = \lceil t_{\sigma''}/m \rceil$ и разобьём куб B^q от БП x' на последовательные отрезки $I_1, \ldots, I_{p_{\sigma''}}$ так, чтобы при любом i, $i \in [1, p_{\sigma''}]$, та часть столбца значений функции $f_{\sigma''}(x')$, которая связана с отрезком I_i, содержала m (соответственно не больше, чем m) булевских значений, если $i < p_{\sigma''}$ (соответственно $i = p_{\sigma''}$). Пусть, далее, функция $f^{(i)}_{\sigma''}(x')$, $i = 1, 2, \ldots, p_{\sigma''}$, совпадает с функцией $f_{\sigma''}$ на отрезке I_i и равна 0 вне его, а ФАЛ $g^{(i)}_{\sigma''}$ из G_{I_i} является её доопределением. Отсюда следует, что функция $f_{\sigma''}$ может быть представлена в виде

$$f_{\sigma''} = f^{(1)}_{\sigma''} \vee \cdots \vee f^{(p_{\sigma''})}_{\sigma''} \tag{7.4}$$

и поэтому её доопределением является ФАЛ

$$g_{\sigma''} = g^{(1)}_{\sigma''} \vee \cdots \vee g^{(p_{\sigma''})}_{\sigma''}. \tag{7.5}$$

Из (7.2)–(7.5) следует, что ФАЛ $g(x)$ вида

$$g(x) = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}\Bigg(\bigvee_{i=1}^{p_{\sigma''}} g^{(i)}_{\sigma''}(x') \Bigg), \tag{7.6}$$

где $g^{(i)}_{\sigma''} \in G$ при любых σ'', $\sigma'' \in B^{n-q}$, и i, $i \in [1, p_{\sigma''}]$, является доопределением ФАЛ f и что на основе (7.6) можно построить СФЭ Σ, которая реализует ФАЛ g со сложностью

$$L(\Sigma) \leqslant 2^{4q+m} + t/m + O(2^{n-q}).$$

Из последнего неравенства при $q = \lceil n - \log t + 2 \log n \rceil$, $m = \lceil \log t - 4q - 2 \log n \rceil$ получаем требуемую оценку $L^{\mathrm{C}}(g) \lesssim \frac{t}{\log t}$.

Лемма доказана. □

Замечание. Из леммы 7.1 вытекает что, при построении оптимальной схемы для не всюду определённой функции f, $f \in \widehat{P}_2(n, t)$, в общем случае невыгодно доопределять её нулями на множестве $B^n \setminus \delta(f)$. Действительно, полагая $t = \lceil 2^n/3 \rceil$ и доопределяя функции из $\widehat{P}_2(n, t)$ нулями, получим множество $Q(n)$ всюду определённых функций, для которого

$$\log |Q(n)| \sim \log C_{2^n}^{\lceil 2^n/3 \rceil} \sim 2^n \left(\frac{\log 3}{3} + \frac{2}{3} \log \frac{3}{2} \right) = 2^n \cdot \log \frac{3}{\sqrt[3]{4}} > 2^n \cdot \frac{2}{3}.$$

В силу леммы 1.1 отсюда следует, что

$$L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \frac{2}{3} \cdot \frac{2^n}{n},$$

в то время как

$$L^{\mathrm{C}}\big(\widehat{P}_2(n, \lceil 2^n/3 \rceil)\big) \sim \frac{1}{3} \cdot 2^n.$$

§8 Лемма о линейном разделяющем операторе. Асимптотически наилучший метод синтеза схем для не всюду определённых функций в случае их «средней» и «слабой» определённости

Введём некоторые понятия и рассмотрим связанные с ними конструкции, позволяющие ослабить условия леммы 7.1.

Пусть n и s, $s \leqslant n$, — натуральные числа, а A — произвольное множество наборов куба B^n и $|A| \leqslant 2^s$. Будем говорить, что (n, s)-оператор ψ, $\psi \in P_2^s(n)$, является *оператором разделения* или, иначе, *оператором хэширования* для A, если $\psi(\alpha) \neq \psi(\beta)$ для любых различных наборов α и β из A. Обозначим через Λ класс линейных ФАЛ с нулевым свободным членом и будем выбирать нужные нам операторы разделения из множества $\Lambda^s(n)$.

Лемма 8.1. *Для любого множества A, $A \subseteq B^n$, и любого s, $s \leqslant n$, существует оператор ψ, $\psi \in \Lambda^s(n)$, разделяющий некоторое множество A', $A' \subseteq A$, такое, что $|A'| \geqslant t - \frac{t(t-1)}{2^{s+1}}$, где $t = |A|$.*

Доказательство. Рассмотрим множество $\Lambda^s(n)$ как вероятностное пространство, в котором вероятность выбора любого из 2^{ns} операторов равна 2^{-ns}. В этой модели для любых различных наборов α и β из B^n вероятность того, что случайный оператор из $\Lambda^s(n)$ их не разделит, равна 2^{-s}. Действительно, для наборов $\alpha = (\alpha_1, \ldots, \alpha_n) \neq \beta = (\beta_1, \ldots, \beta_n)$ число не разделяющих их линейных ФАЛ вида $\gamma_1 x_1 \oplus \cdots \oplus \gamma_n x_n$ равно числу тех наборов $\gamma = (\gamma_1, \ldots, \gamma_n)$ из B^n, для которых $\gamma_1(\alpha_1 \oplus \beta_1) \oplus \cdots \oplus \gamma_n(\alpha_n \oplus \beta_n) = 0$, то есть равно 2^{n-1}, а значит число тех операторов из $\Lambda^s(n)$, которое не разделяют α и β, равно $2^{s(n-1)}$.

Отсюда следует, что математическое ожидание числа не разделённых случайным оператором из $\Lambda^s(n)$ неупорядоченных пар различных наборов из A равна $t(t-1)/2^{s+1}$. Это означает, что найдётся такой оператор ψ, $\psi \in \Lambda^s(n)$, для которого множество R, состоящее из не разделённых им пар наборов указанного вида имеет мощность r, где $r \leqslant$ $\leqslant t(t-1)/2$.

Индукцией по r легко показать, что мощность минимального по включению подмножества A'' множества A, которое «протыкает» все пары из R, то есть имеет с каждой из них непустое пересечение, не больше, чем r. Действительно, при $r = 1$ это очевидно, а при увеличении числа r на 1 мощность множества A'' увеличивается не больше, чем на 1. Таким образом, множество $A' = A \setminus A''$ разделяется оператором ψ и имеет требуемую мощность.

Лемма доказана. □

Следствие. *Если в условиях леммы $s \geqslant \lfloor 2 \log t \rfloor$, то $A' = A$, так как*

$$|A'| \geqslant t - \frac{t(t-1)}{2^{s+1}} > t - 1.$$

Лемма 8.2. *Если $2^{n/3} \leqslant t \leqslant 2^n/n^5$, то $L^{\mathrm{C}}\big(\widehat{P}_2(n, t)\big) \lesssim \frac{t}{\log t}$.*

Доказательство. Положим

$$s = \lfloor \log t + 2 \log n + \log \log t \rfloor$$

и заметим, что в силу условий леммы выполняются соотношения

$$s \leqslant n, \qquad s \sim \log t, \qquad nt \log t = o(2^s). \tag{8.1}$$

Возьмём произвольную фунцию f, $f \in \widehat{P}_2(n,t)$, и пусть $A = \delta(f)$, $|A| = t$. Построим по лемме 8.1 для множества A, $A \subset B^n$, оператор ψ, который отображает куб B^n от БП $x = (x_1, \ldots, x_n)$ в куб B^s от БП $y = (y_1, \ldots, y_s)$ и разделяет подмножество A', $A' \subseteq A$, такое, что

$$|A'| = t' \geqslant t - \frac{t(t-1)}{2^{s+1}}.$$

Заметим, что при этом в силу (8.1) $t' \sim t$, $s \sim \log t'$, и, следовательно, для множества $\widehat{P}_2(s,t')$, которому принадлежит функция $\widetilde{f}'(y)$ такая, что $\delta(\widetilde{f}') = \psi(A')$ и $\widetilde{f}'(\psi(\alpha)) = f(\alpha)$ при любом α, $\alpha \in A'$, выполнены условия леммы 7.1. Найдём по этому утверждению такое доопределение $\widetilde{g}'(y)$ ФАЛ $\widetilde{f}'(y)$, для которого

$$L^{\mathrm{C}}(\widetilde{g}') \lesssim \frac{t'}{\log t'} \sim \frac{t}{\log t}. \tag{8.2}$$

Легко видеть, что ФАЛ вида

$$g(x) = \widetilde{g}'(\psi(x)) \cdot \overline{\chi}''(x) \vee g''(x), \tag{8.3}$$

где χ'' — характеристическая ФАЛ множества $A'' = A \setminus A'$, а g'' — ФАЛ, совпадающая с f на A'' и равная 0 вне его, является доопределением ФАЛ f. Заметим, что реализация ФАЛ χ'' и g'' по их совершенным ДНФ даёт следующую суммарную оценку их сложности

$$L^{\mathrm{C}}(\chi'') + L^{\mathrm{C}}(g'') = O(nt^2/2^s),$$

а известная оптимальная реализация линейной ФАЛ — оценку $L^{\mathrm{C}}(\psi) \leqslant 4ns$, из которых в силу (8.1) вытекает оценка

$$L^{\mathrm{C}}(\chi'') + L^{\mathrm{C}}(g'') + L^{\mathrm{C}}(\psi) = o(t/\log t). \tag{8.4}$$

Таким образом, реализуя ФАЛ $g(x)$ в соответствии с (8.3) и учитывая (8.2), (8.4), получим $L^{\mathrm{C}}(f) \lesssim \frac{t}{\log t}$.

Лемма доказана. □

Лемма 8.3. *Если* $t \leqslant 2^{n/3}$ *и* $n \log^2 n = o(t)$, *то* $L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) \lesssim \frac{t}{\log t}$.

Доказательство этого утверждения представляет собой упрощённый вариант доказательства леммы 8.2, при котором $s = \lfloor 2 \log t \rfloor$ и, следовательно, $A' = A$, то есть вариант, не требующий реализации ФАЛ χ'', g''.

Суммируя доказанные утверждения, получаем основной результат — теорему 6.1.

§9 Лемма оцепях и сечениях для π-схем; верхние оценки сложности реализации линейных функций в классе π-схем

Под контактной схемой (КС) в данном параграфе будем понимать $(1,1)$-КС из неориентированных контактов. Для множества C, состоящего из t контактов вида $x_{j_1}^{\sigma_1}, \ldots, x_{j_t}^{\sigma_t}$, положим

$$K(C) = x_{j_1}^{\sigma_1} \cdot \ldots \cdot x_{j_t}^{\sigma_t}, \qquad J(C) = x_{j_1}^{\sigma_1} \vee \ldots \vee x_{j_t}^{\sigma_t}.$$

Для КС Σ, реализующей ФАЛ f из $P_2(n)$, через $\mathcal{C}(\Sigma)$ будем обозначать множество проводящих простых цепей Σ, соединяющих её полюса, а через $\mathcal{S}(\Sigma)$ — множество отделимых тупиковых сечений Σ, разделяющих её полюса (см. [1, §5 гл. 2]). При этом каждому набору $\alpha = (\alpha_1, \ldots, \alpha_n)$ из N_f соответствует цепь C, $C \in \mathcal{C}(\Sigma)$, состоящая

из проводящих на наборе α контактов вида $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$, а набору $\beta = (\beta_1, \ldots, \beta_n)$ из $\overline{N}_f = B^n \setminus N_f$ — сечение S, $S \in \mathcal{S}(\Sigma)$, состоящее из разомкнутых на наборе β контактов вида $x_1^{\overline{\beta}_1}, \ldots, x_n^{\overline{\beta}_n}$. Заметим, что множество $S \cap C$, то есть множество общих для S и C контактов не пусто и состоит из контактов вида $x_i^{\alpha_i}$, где $\alpha_i = \overline{\beta}_i$.

Результат последовательного (параллельного) соединения КС Σ_1 и Σ_2 будем обозначать через $\Sigma_1 \cdot \Sigma_2$ (соответственно $\Sigma_1 \parallel \Sigma_2$). Назовём *простейшей π-схемой* любую КС, состоящую из одного контакта, а затем индукцией по сложности определим *π-схему* Σ как КС вида $\Sigma_1 \cdot \Sigma_2$ или $\Sigma_1 \parallel \Sigma_2$, где Σ_1, Σ_2 — π-схемы.

Лемма 9.1. *Для π-схемы Σ любая цепь C, $C \in \mathcal{C}(\Sigma)$, и любое сечение S, $S \in \mathcal{S}(\Sigma)$ имеют ровно один общий контакт.*

Доказательство. Проведём индукцию по строению π-схемы Σ. В случае, когда Σ — простейшая π-схема, состоящая из одного контакта, утверждение леммы, очевидно, выполняется. Докажем справедливость индуктивного перехода.

Отметим, сначала, что для произвольных КС Σ_1 и Σ_2 выполняются равенства:

$$\mathcal{C}(\Sigma_1 \cdot \Sigma_2) = \{\, C \mid C = C_1 \cdot C_2, \text{ где } K(C) \neq 0 \text{ и } C_i \in \mathcal{C}(\Sigma_i),\ i = 1, 2 \,\},$$

$$\mathcal{S}(\Sigma_1 \cdot \Sigma_2) = \mathcal{S}(\Sigma_1) \cup \mathcal{S}(\Sigma_2),$$

$$\mathcal{C}(\Sigma_1 \parallel \Sigma_2) = \mathcal{C}(\Sigma_1) \cup \mathcal{C}(\Sigma_2) \tag{9.1}$$

$$\mathcal{S}(\Sigma_1 \parallel \Sigma_2) = \{\, S \mid S = S_1 \cup S_2, \text{ где } J(S) \neq 1 \text{ и } S_i \in \mathcal{S}(\Sigma_i),\ i = 1, 2 \,\}. \tag{9.2}$$

Действительно, любая цепь C из $\mathcal{C}(\Sigma_1 \cdot \Sigma_2)$ имеет вид $C = C_1 \cdot C_2$, где $C_i \in \mathcal{C}(\Sigma_i)$, $i = 1, 2$, и $K(C_1) \cdot K(C_2) \neq 0$, а любое сечение S из $\mathcal{S}(\Sigma_1 \cdot \Sigma_2)$ совпадает либо с некоторым сечением S_1 из $\mathcal{S}(\Sigma_1)$, либо с некоторым сечением S_2 из $\mathcal{S}(\Sigma_2)$.

Заметим, что при этом $C \cap S = C_i \cap S_i$, где $S = S_i$, и, следовательно, если КС Σ_1, Σ_2 являются π-схемами, удовлетворяющими условиям леммы, то π-схема $\Sigma_1 \cdot \Sigma_2$ тоже будет им удовлетворять. Аналогичным образом доказываются равенства (9.1), (9.2), и устанавливается справедливость индуктивного перехода в случае π-схемы вида $\Sigma_1 \parallel \Sigma_2$.

Лемма доказана. □

Лемма 9.2. *При $n \geqslant 1$ для линейной ФАЛ l_n^σ, $\sigma \in B$, выполнено неравенство*

$$L^\pi(l_n^\sigma) \leqslant 4n^2.$$

Доказательство. Для получения требуемой оценки рассмотрим случай $n = 2^k$, $k = 1, 2, \ldots$. Для $n = 2$ искомые π-схемы Σ_2' и Σ_2'' реализующие со сложностью 4 ФАЛ l_2 и $\bar{l}_2$ соответственно, строятся на основе совершенных ДНФ. Пусть для $n = 2^k$ искомые π-схемы Σ_n' и Σ_n'', реализующие со солжностью n^2 ФАЛ l_n и $\bar{l}_n$ уже построены. Тогда π-схемы Σ_{2n}' и Σ_{2n}'', реализующие со сложностью $4n^2$ ФАЛ l_{2n} и $\bar{l}_{2n}$ могут быть построены на основе разложений:

$$l_{2n}(x, y) = l_n(x) \cdot \bar{l}_n(y) \vee \bar{l}_n(x) \cdot l_n(y) \quad \text{и} \quad \bar{l}_{2n}(x, y) = l_n(x) \cdot l_n(y) \vee \bar{l}_n(x) \cdot \bar{l}_n(y),$$

где $x = (x_1, \ldots, x_n)$ и $y = (x_{n+1}, \ldots, x_{2n})$. Таким образом, $L^\pi(l_n^\sigma) \leqslant n^2$, если $n = 2^k$, $k = 1, 2, \ldots$. В общем случае, когда $2^{k-1} < n \leqslant 2^k$, для построения π-схем Σ_n' и Σ_n'', реализующих со сложностью не более, чем $4n^2$, ФАЛ l_n и $\bar{l}_n$ соответственно, достаточно взять построенные выше π-схемы Σ_{2^k}' и Σ_{2^k}'', а затем подставить константу 0 вместо всех БП $x_{n+1}, \ldots, x_{2^k}$.

Лемма доказана. □

§10 Теорема Храпченко, нижние оценки сложности линейной функции в классе π-схем

Для пересекающихся подмножеств $\mathcal{N}'$ и $\mathcal{N}''$ множества B^n обозначим через $\mathcal{R}(\mathcal{N}', \mathcal{N}'')$ множество всех пар (α, β), состоящих из соседних по какой-либо БП $x_1, \ldots, x_n$ наборов α

и β куба B^n таких, что $\alpha \in \mathcal{N}'$ и $\beta \in \mathcal{N}''$. Пусть, как обычно, $\mathcal{U}^\pi$ — класс π-схем и, в соответствии с общими правилами, $L^\pi(f)$ — сложность реализации ФАЛ f в классе $\mathcal{U}^\pi$.

Теорема 10.1. *Для любой ФАЛ f из $P_2(n)$ и любых множеств $\mathcal{N}'$, $\mathcal{N}''$ таких, что $\mathcal{N}' \subseteq \subseteq N_f$ и $\mathcal{N}'' \subseteq \overline{N}_f$, справедливо неравенство:*

$$L^\pi(f) \geqslant \frac{|\mathcal{R}(\mathcal{N}', \mathcal{N}'')|^2}{|\mathcal{N}'| \cdot |\mathcal{N}''|} \tag{10.1}$$

Доказательство. Пусть π-схема Σ сложности L реализует ФАЛ f и состоит из контактов $\mathcal{K}_1, \ldots, \mathcal{K}_L$, где $\mathcal{K}_i$ — контакт вида $x_{ji}^{\sigma_i}$, $i = 1, \ldots, L$. Каждому набору $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\alpha \in N_f$, сопоставим цепь C_α из множества $\mathcal{C}(\Sigma)$, состоящую из контактов вида $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$, а каждому набору $\beta = (\beta_1, \ldots, \beta_n)$, $\beta \in \overline{N}_f$, — сечение S_β из множества $\mathcal{S}(\Sigma)$, состоящее из контактов вида $x_1^{\beta_1}, \ldots, x_n^{\beta_n}$. При этом в соответствии с леммой 9.1 множество $C_\alpha \cap S_\beta$ состоит из одного контакта вида $x_s^{\alpha_s}$, где $\alpha_s \neq \beta_s$. Рассмотрим следующие множества:

$$\begin{gathered}
\Pi = \mathcal{N}' \times \mathcal{N}'', \quad \mathcal{R} = \mathcal{R}(\mathcal{N}', \mathcal{N}''), \\
\mathcal{N}_i' = \{\, \alpha \in \mathcal{N}' \mid S_\alpha \ni \mathcal{K}_i \,\}, \\
\mathcal{N}_i'' = \{\, \beta \in \mathcal{N}'' \mid S_\beta \ni \mathcal{K}_i \,\}, \\
\Pi_i = \mathcal{N}_i' \times \mathcal{N}_i'', \quad \mathcal{R}_i = \mathcal{R} \cap \Pi_i,
\end{gathered}$$

где $i = 1, \ldots, L$. Заметим, что при $i \neq j$ множества Π_i и Π_j ($\mathcal{R}_i$ и $\mathcal{R}_j$) не пересекаются, а объединение всех таких множеств равно множеству Π (соответственно $\mathcal{R}$). Действительно, любая пара (α, β) из Π принадлежит тому и только тому из множеств $\mathcal{N}_i' \times \mathcal{N}_i''$, $1 \leqslant i \leqslant L$, для которого контакт $\mathcal{K}_i$ является единственным общим контактом цепи C_α и сечения S_β. При этом пара (α, β) принадлежит соответствующему множеству $\mathcal{R}_i$ тогда и только тогда, когда наборы α и β являются соседними.

Докажем теперь, что

$$|\mathcal{R}_i| \leqslant |\mathcal{N}_i'| \quad \text{и} \quad |\mathcal{R}_i| \leqslant |\mathcal{N}_i''| \tag{10.2}$$

для всех i, $i = 1, \ldots, L$. Для этого достаточно доказать, что для любых двух различных пар (α, β) и (γ, δ) из $\mathcal{R}_i$ выполнены соотношения: $\alpha \neq \gamma$ и $\beta \neq \delta$. Действительно, наборы α и β, а также наборы γ и δ являются соседними по БП x_{ji} и поэтому в случае $\alpha = \gamma$ или $\beta = \delta$ было бы выполнено равенство $(\alpha, \beta) = (\gamma, \delta)$, которое противоречит выборц данных пар.

Из определения и свойств введённых выше множеств, а также неравенств (10.2) и неравенства Коши-Буняковского

$$\sum_{i=1}^{m} {a_i}^2 \geqslant \frac{1}{m} \left(\sum_{i=1}^{m} |a_i| \right)^2$$

следует, что

$$|\mathcal{N}'| \cdot |\mathcal{N}''| = |\Pi| = \sum_{i=1}^{L} |\Pi_i| = \sum_{i=1}^{L} |\mathcal{N}_i'| \cdot |\mathcal{N}_i''| \geqslant \sum_{i=1}^{L} |\mathcal{R}_i|^2 \geqslant \frac{1}{L} \left(\sum_{i=1}^{L} |\mathcal{R}_i| \right) \geqslant \frac{1}{L} |\mathcal{R}|^2.$$

Таким образом,

$$L \geqslant \frac{|\mathcal{R}|^2}{|\mathcal{N}'| \cdot |\mathcal{N}''|}.$$

Теорема доказана. □

Следствие. *При $n \geqslant 1$ для линейной ФАЛ l_n^σ, $\sigma \in B$, выполнены неравенства*

$$n^2 \leqslant L^\pi(l_n^\sigma) \leqslant 4n^2$$

Доказательство. Требуемая нижняя оценка вытекает из (10.1) при $f = l_n^\sigma$ и $\mathcal{N}' = N_f$, $\mathcal{N}'' = \overline{N}_f$ так как в данном случае $|\mathcal{N}'| = |\mathcal{N}''| = 2^{n-1}$, $|\mathcal{R}(\mathcal{N}', \mathcal{N}'')| = n \cdot 2^{n-1}$ и поэтому $L^\pi(f) \geqslant n^2$. □

Напомним (см. [1, §2 гл. 4]), что любой π-схеме Σ можно сопоставить эквивалентную формулу $\mathcal{F}$ с поднятыми отрицаниями из класса $\mathcal{U}^\Phi$, для которой $\mathcal{R}(\mathcal{F}) = L(\Sigma)$, и что при поднятии отрицаний ранг формулы не изменится. Следовательно, $\mathcal{R}^\Phi(l_n^\sigma) \geqslant n^2$ и в соответствии со следствием из леммы 2.1 [1, гл.2] $D(l_n^\sigma) \geqslant \lceil 2 \log n \rceil$. С другой стороны, формулы $\mathcal{F}'_n$ и $\mathcal{F}''_n$ с поднятыми отрицаниями, которые соответствуют π-схемам Σ'_n и Σ''_n, построенными при доказательстве леммы 9.2, имеют глубину не более, чем $(2 \log n + 3)$, и потому $D(l_n^\sigma) \leqslant 2 \log n + 3$.

§11 Инвариантные классы функций, их описание на языке базовых множеств и порождающих элементов. Теорема о числе инвариантных классов и фрагменты её доказательства

Рассмотрим некоторое более узкое по сравнению с введённым в §1 семейством квазиинвариантных классов — введённое С. В. Яблонским [4] семейство т. н. инвариантных классов ФАЛ.

Для этого рассмотрим следующие операции над ФАЛ:

1) добавление и изъятие фиктивных БП (переход к равной ФАЛ),

2) переименование БП без отождествления (переход к конгруэнтной ФАЛ),

3) подстановка констант 0, 1 вместо БП (переход к подфункции).

Если функция g получена из функции f применением операции 1 (соответственно операций 1–3), то говорят, что g является *подфункцией* (соответственно *псевдоподфункцией*) ФАЛ f, а f — *надфункцией* (соответственно *псевдонадфункцией*) ФАЛ g. Для множества функций F через $F^\urcorner$ и $F_\llcorner$ будем обозначать множества всех псевдонадфункций и псевдоподфункций для функций из F соответственно.

Множество ФАЛ Q, $Q \subseteq P_2$, называется *инвариантным классом ФАЛ*, если оно замкнуто относительно трёх указанных операций. Множества $\{0\}$, $\{1\}$, $\{0, 1\}$ называются *тривиальными инвариантными классами*. Если инвариантный класс Q не является тривиальным, то $Q \supsetneq \{0, 1\}$, поскольку Q содержит неконстантную функцию, из которой при помощи операции 3 можно получить обе константы. Отметим, что если класс Q замкнут по суперпозиции и $\{0, 1\} \subseteq Q$, то класс Q является инвариантным. Примерами инвариантных классов могут, следовательно, служить классы M и $\mathcal{L}$ всех монотонных и всех линейных ФАЛ соответственно. При этом класс S — класс самодвойственных функций, а также классы T_0 и T_1 — классы сохранения констант 0 и 1 соответственно, — не являются инвариантными (они не замкнуты относительно операции 3). Класс $\mathcal{S}$ — класс всех симметрических ФАЛ также не является инвариантным, так как он не замкнут относительно операции 1. При этом инвариантным является класс $\widehat{\mathcal{S}}$ — класс *квазисимметрических* ФАЛ, то есть функций, симметрических по всем своим существенным переменным.

Заметим, что инвариантный класс Q является квазиинвариантным классом с порогом 2 и поэтому в силу леммы 1.2 его мощностная последовательность $\sigma_Q(n)$ является монотонно не возрастающей при всех $n = 1, 2, \ldots$. Докажем, что существует только один инвариантный класс Q с характеристикой $\sigma_Q = 1$ — это класс P_2.

Действительно, если инвариантный класс Q не совпадает с P_2, то для некоторого m будет выполнено неравенство $|Q(m)| < |P_2(m)|$, которое равносильно неравенству $\sigma_Q(m) < 1$. Из последнего неравенства в силу монотонного невозрастания последовательности $\sigma_Q(n)$, $n = 1, 2, \ldots$, и её сходимости к пределу σ_Q следует, что $\sigma_Q \leqslant \sigma_Q(m) < 1$.

Найдём значение характеристик инвариантных классов M, $\mathcal{L}$ и $\widehat{\mathcal{S}}$. Известно [5], что $\log|M(n)| \sim C_n^{\lceil n/2\rceil} \sim \frac{2^n}{\sqrt{2\pi n}}$, откуда следует $\sigma_M = 0$. Для класса линейных функций, очевидно, при любом n выполняется равенство $|\mathcal{L}(n)| = 2^{n+1}$, значит $\sigma_L = 0$. Всякую функцию из множества $\widehat{\mathcal{S}}(n)$ можно получить так: сначала выбираем k её существенных БП, а затем не более чем 2^{k+1} способами определяем значение этой функции на каждом слое куба B^k (в пределах одного слоя значение функции одно и то же). Отсюда следует, что

$$|\widehat{\mathcal{S}}(n)| \leqslant \sum_{k=0}^{n} C_n^k \cdot 2^{k+1} = 2 \cdot 3^n,$$

и поэтому $\sigma_{\widehat{\mathcal{S}}} = 0$. Таким образом, все три класса M, $\mathcal{L}$, $\widehat{\mathcal{S}}$ являются нулевыми. Примером ненулевого инвариантного класса, отличного от P_2, является класс Q, состоящий из всех ФАЛ вида $f(x_{i_1}, \ldots, x_{i_r})(x_{i_1} \oplus \cdots \oplus x_{i_r} \oplus \sigma)$, где $1 \leqslant i_1 < \cdots < i_r$ и $\sigma \in B$. Действительно, класс Q замкнут относительно операций 1–3. При этом любая ФАЛ из $Q(n)$ однозначно определяется множеством X её существенных БП, $X \subseteq X(n)$, и своими значениями на множестве тех наборов единичного куба от БП X, которые имеют либо чётное, если $\sigma = 1$, либо нечётное, если $\sigma = 0$, число единиц. Таким образом,

$$2 \cdot 2^{2^{n-1}} \leqslant |Q(n)| \leqslant \sum_{r=0}^{n} 2 \cdot C_n^r \cdot 2^{2^{r-1}} \leqslant 2^{2^{n-1}+n+1}$$

и, следовательно, $\sigma_Q = \frac{1}{2}$.

Выше было установлено, что существует единственный инвариантный класс с характеристикой 1. Можно доказать, что при при любом σ, $0 \leqslant \sigma < 1$ существует континуум инвариантных классов с характеристикой σ. Докажем это в частном случае $\sigma = 0$.

Лемма 11.1. *Существует континуум различных инвариантных классов с характеристикой* 0.

Доказательство. Отметим, что число различных инвариантных классов не может быть больше континуума, поскольку множество P_2 счётно.

Рассмотрим симметрические функции $s_m^{\{0,m\}}$, определяемые при $m > 1$ следующим образом:

$$s_m^{\{0,m\}}(x_1, \ldots, x_m) = x_1 \cdot \ldots \cdot x_m \vee \overline{x}_1 \cdot \ldots \cdot \overline{x}_m.$$

Заметим, что $s^{\{0,m'\}} \notin \{s^{\{0,m''\}}\}_{\lrcorner}$ при $m' \neq m''$, и, следовательно, для различных множеств J, $J \subseteq \mathbb{N} \setminus \{1\}$, соответствующие им множества функций $Q_J = \{\, s_m^{\{0,m\}} \mid m \in J \,\}_{\lrcorner}$ будут различны. Очевидно, что каждое из указанных множеств является инвариантным классом, содержащимся в классе $\widehat{\mathcal{S}}$, и, следовательно, имеет характеристику 0. Классов Q_J будет столько же, сколько подмножеств имеет множество $\mathbb{N} \setminus \{1\}$, то есть континуум.

Лемма доказана. □

Множество F называется *базовым множеством* инвариантного класса Q, если $F_{\lrcorner} = Q$. Базовое множество класса Q называется *базой*, если любое его собственное подмножество уже не является базовым множеством для Q. Существуют инвариантные классы, не имеющие базы. Например, класс, состоящий из констант 0, 1 и всех монотонных элементарных дизъюнкций (функций вида $x_{i_1} \vee \cdots \vee x_{i_s}$), имеет счётное базовое множество, но не имеет базы.

Для задания всякого инвариантного класса достаточно задать, таким образом, его базовое множество. Существует и другой способ задания инвариантных классов. Пусть Q — нетривиальный отличный от P_2 инвариантный класс. Функция $g \in P_2$ называется *порождающим элементом* класса Q тогда и только тогда, когда $g \notin Q$, а все

собственные подфункции[1] g принадлежат Q. Из определения следует, что порождающий элемент нетривиального инвариантного класса является существенной функцией и что никакие два различных порождающих элемента не являются псевдоподфункциями друг друга. Приведём примеры порождающих элементов. Класс M монотонных ФАЛ имеет единственный с точностью до конгруэнтности порождающий элемент — функцию $\overline{x}_1$. Для инвариантного класса Q его *порождающим множеством* называется всякое максимальное по включению множество попарно не конгруэнтных порождающих элементов Q. Так, порождающее множество класса, состоящего из констант и монотонных элементарных дизъюнкций, суть $\{\overline{x}_1, x_1x_2\}$.

Лемма 11.2. *Пусть Q — нетривиальный отличный от P_2 инвариантный класс, а G — его порождающее множество. Тогда $Q = P_2 \setminus (G^{\urcorner})$.*

Доказательство. Индукцией по n, $n = 1, 2, \ldots$, докажем, что если f — существенная ФАЛ от n БП и $f \notin Q$, то $G \cap (\{f\}_{\lrcorner}) \neq \varnothing$. Заметим, что данное утверждение верно, если любая собственная подФАЛ ФАЛ f прининадлежит Q. Действительно, в указанном случае ФАЛ f является порождающим элементом Q и в G имеется конгруэнтная ей ФАЛ. Это верно, в частности, для случая $n = 1$, который составляет базис рассматриваемой индукции.

Пусть сформулированное утверждение верно для всех n, $n \in [1, k)$, где $k \geqslant 2$, и пусть f — существенная ФАЛ из $P_2(k) \setminus Q(k)$, которая (см. разобранный выше случай) имеет собственную подФАЛ f', $f' \notin Q$. Тогда, по индуктивному предположению $G \cap (\{f'\}_{\lrcorner}) \neq \varnothing$ и, следовательно, $G \cap (\{f\}_{\lrcorner}) \neq \varnothing$, так как первое из этих множеств содержится во втором.

Лемма доказана. □

Следствие. *Пусть множество G состоит из ФАЛ, не являющихся квазиподфункциями друг друга. Тогда $P_2 \setminus (G^{\urcorner})$ — инвариантный класс с порождающим множеством G.*

[1] Под собственной подфункцией функции g понимается её произвольная подфункция, не совпадающая с g.

Литература

[1] *Ложкин С. А.* Лекции по основам кибернетики. М.: МГУ, 2004

[2] *Алексеев В. Б., Ложкин С. А.* Элементы теории графов, схем и автоматов. М.: Издательский отдел ф-та ВМиК МГУ, 2000.

[3] *Андреев А. Е.* О сложности реализации частичных булевых функций схемами из функциональных элементов. Дискретная математика, т. 1 (1989), №4. С. 36-45.

[4] *Яблонский С. В.* Об алгоритмических трудностях синтеза минимальных контактных схем. Проблемы кибернетики, вып. 2. - М.:Физматгиз, 1959. С. 75-121 (См. также Избранные труды С.В. Яблонского. М.: МАКС Пресс, 2004.).

[5] *Клейтмен Д.* О проблеме Дедекинда: число монотонных булевых функций // Кибернетический сборник. Новая серия, вып. 7. М.: Мир, 1970. С. 43-52.