Московский государственный университет имени

М. В. Ломоносова

Факультет вычислительной математики и кибернетики

С. А. Ложкин

Дополнительные главы кибернетики

Москва 2013

Оглавление

1 Асимптотически оптимальные методы синтеза схем и оценки высокой степени точности для ряда функций Шеннона. Синтез схем для функций из специальных классов 4

§1 Некоторые модификации контактных схем. Итеративные контактные схемы. Верхние оценки числа схем контактного типа, нижние мощностные оценки функций Шеннона 4

§2 Формулы и СФЭ в произвольном базисе, усилительные СФЭ. Верхние оценки числа формул и СФЭ, нижние мощностные оценки функций Шеннона 12

§3 Универсальные системы ФАЛ и их построение на основе селекторных разбиений БП 18

§4 Асимптотические оценки высокой степени точности для сложности итеративных контактных схем и контактных схем из ориентированных контактов 23

§5 Асимптотически наилучший метод синтеза СФЭ в произвольном базисе. Асимптотические оценки высокой степени точности для сложности усилительных СФЭ в некоторых базисах 28

§6 Асимптотически наилучший метод синтеза формул в произвольном базисе. Асимптотические оценки высокой степени точности для сложности формул в некоторых базисах 33

§7 Мультиплексорные ФАЛ и обобщённое разложение. Оптимальная по задержке реализация мультиплексорных ФАЛ в произвольном базисе 37

§8 Задача синтеза схем для функций из специальных классов, примеры её решения и мощностные нижние оценки. Инвариантные классы С. В. Яблонского, теорема о числе инвариантных классов 42

§9 Принцип локального кодирования О. Б. Лупанова и примеры его применения. 48

§10 Синтез схем для не всюду определённых функций 53

2 Синтез схем для индивидуальных функций и оценки их сложности 59

§1 Средняя проводимость схемы. Асимптотика контактной сложности универсальных систем функций 59

§2 Забивание переменных константами. Сложность линейной функции в классе схем из функциональных элементов 61

§3 Незабиваемые множества переменных. Асимптотика сложности мультиплексора в некоторых классах схем 65
§4 Сферические функции. Сложность линейной и других функций в классе контактных схем и самокорректирующихся контактных схем 68
§5 Теорема Храпченко. Сложность линейной функции в классе π–схем . 71

Литература **75**

Глава 1

Асимптотически оптимальные методы синтеза схем и оценки высокой степени точности для ряда функций Шеннона. Синтез схем для функций из специальных классов[1]

§1 Некоторые модификации контактных схем. Итеративные контактные схемы. Верхние оценки числа схем контактного типа, нижние мощностные оценки функций Шеннона

Рассмотрим одну модификацию контактных схем (КС), которая является, по существу, частным случаем т.н. релейно-контактных схем (см., например, [4]) и связана с операцией присоединения управляющих булевых переменных (БП) или, иначе, управляющих входов КС к ее выходам.

Для КС $\Sigma = \Sigma(x_1, \ldots, x_n;\ 1;\ z_1, \ldots, z_m)$ определим операцию *присоединения её управляющей БП x_i к выходу z_j*, которая применима, если БП x_i входит в Σ без отрицаний, и в результате выполнения которой в графе КС Σ происходит снятие БП z_j, сопоставление связанной с ней вершине внутренней БП y и замена всех пометок x_i на пометку y. Аналогично определяется операция (одновременного) присоединения нескольких управляющих БП КС Σ к её выходам, при выполнении которой каждой участвующей в присоединениях выходной вершине Σ сопоставляется только одна внутренняя БП, причём разным вершинам сопоставляются разные БП. Любая из полученных таким образом схем называется *итеративной контактной схемой (ИКС) на базе КС* Σ. Под сложностью $L(\Sigma')$ ИКС Σ' на базе КС Σ понимается сложность $L(\Sigma)$.

Функционированние итеративной контактной схемы $\Sigma(x_1, \ldots, x_n;\ z_1, \ldots, z_m)$ на базе КС вида $\widehat{\Sigma}(x_1, \ldots, x_n,\ y'_1, \ldots, y'_l;\ 1;\ y''_1, \ldots, y''_l, z_1, \ldots, z_m)$ с внутренними БП $y_i = y'_i = y''_i$, $i = 1, \ldots, l$, рассматривается в дискретные моменты времени t, $t = 0, 1, \ldots$. Для любого входного набора $\alpha = (\alpha_1, \ldots, \alpha_n) \in B^n$ при $t = 0, 1, \ldots$ происходит последовательное установление в различных вершинах значения 1 в результате образования цепей, соединяющих эти вершины с входом 1 и состоящих из проводящих к данному моменту контактов, а также значение 0 в результате образования разрезов, отделяющих рассматриваемые вершины от входа 1 и состоящих

[1] Те понятия и обозначения, которые здесь не определяются могут быть найдены в [3], гл. 2, §3

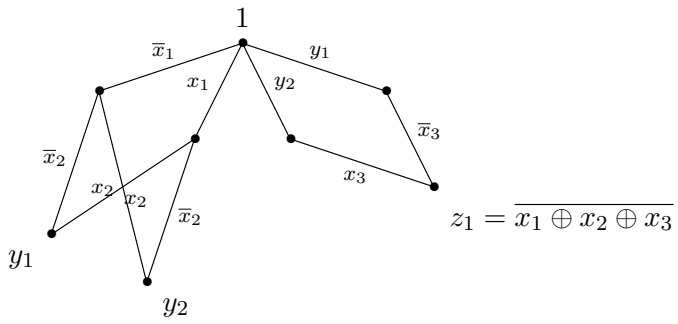

Рис. 1.1: Пример комбинационной ИКС

из непроводящих к данному моменту контактов. При этом вершина u_i, связанная с БП y_i, $1 \leqslant i \leqslant l$, в которой установилось значение σ, начинает в следующий момент времени управлять проводимостью контактов y_i и т.д. Обозначим через $V^{(\sigma)}(\Sigma, \alpha, t)$, $\sigma \in B$, множество тех вершин Σ, в которых к моменту времени t установилось значение σ, а через $V^{(2)}(\Sigma, \alpha, t)$ — множество всех остальных вершин Σ, и заметим, что

$$V^{(\sigma)}(\Sigma, \alpha, t) \subseteq V^{(\sigma)}(\Sigma, \alpha, t+1), \qquad V^{(\gamma)}(\Sigma, \alpha, t) \cap V^{(\delta)}(\Sigma, \alpha, t) = \varnothing \tag{1.1}$$

для любого σ, $\sigma \in B$, и любых $\gamma \neq \delta$ из $[0, 2]$. Будем считать, что в момент времени t в вершинах множества $V^{(2)}(\Sigma, \alpha, t)$ имеется неопределенное значение 2.

Из (1.1) следует, что, начиная с некоторого T, $T \geqslant 0$, множества $V^{(\sigma)}(\Sigma, \alpha, t)$, $\sigma \in [0, 2]$, стабилизируются, то есть $V^{(\sigma)}(\Sigma, \alpha, t+1) = V^{(\sigma)}(\Sigma, \alpha, t) = V^{(\sigma)}(\Sigma, \alpha)$, при $t \geqslant T$, и будем говорить, что в момент времени T процесс функционирования ИКС Σ на наборе α завершается, причем завершается он установлением значения σ, $\sigma \in [0, 2]$, во всех вершинах множества $V^{(\sigma)}(\Sigma, \alpha)$. При этом ИКС Σ называется *комбинационной схемой* (*схемой без памяти*), если для любого входного набора α, $\alpha \in B^n$, её функционирование на наборе α завершается определёнными значениями во всех выходных вершинах $z_1, \ldots, z_m$, которые определяют значения $f_1(\alpha), \ldots, f_m(\alpha)$ ФАЛ $f_1, \ldots, f_m$ от БП $x_1, \ldots, x_n$, реализуемых Σ.

На рис. 1.1 показана комбинационная ИКС, реализующая ФАЛ $x_1 \oplus x_2 \oplus x_3 \oplus 1$, а на рис. 1.2 — некомбинационная ИКС, которая реализует систему функций (f_1, f_2), где $f_1 = f_2 = 2x_1 \cdot x_2$. Будем называть ИКС $\Sigma(x_1, \ldots, x_n;\ z_1, \ldots, z_m)$ на базе КС $\widehat{\Sigma}(x_1, \ldots, x_n,\ y'_1, \ldots, y'_l;\ 1;\ y''_1, \ldots, y''_l,\ z_1, \ldots, z_m)$ *упорядоченой*, если существует такая перестановка $j_1, \ldots, j_l$ чисел $1, \ldots, l$, при которой для любого i, $i \in [1, l]$, ФАЛ проводимости от 1 к y_{j_i} в КС $\widehat{\Sigma}$ может существенно зависеть только от БП $x_1, \ldots, x_n$, $y_{j_1}, \ldots, y_{j_{i-1}}$. Заметим, что упорядоченная ИКС Σ является комбинационной и что ИКС, показанная на рис. 1.1, является упорядоченной.

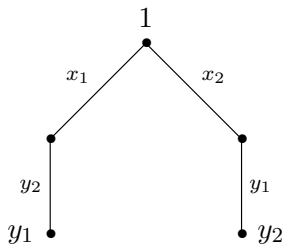

Рис. 1.2: Пример некомбинационной ИКС

По аналогии с классами $\mathcal{U}^{\text{КС}}$ и $\mathcal{U}^{\overrightarrow{\text{КС}}}$ (см. [3]) контактных схем из неориентированных и ориентированных контактов соответственно обозначим через $\mathcal{U}^{\text{ИКС}}$ класс всех комбинационных ИКС из неориентированных контактов, а через $\mathcal{U}^{A}(L,n)$, где $A \in \{\text{КС}, \overrightarrow{\text{КС}}, \text{ИКС}\}$ — множество схем от БП $X(n) = \{x_1, \ldots, x_n\}$ из $\mathcal{U}^{A}$, которые представляют собой связный граф, имеют один выход, один вход и сложность не более L. В соответствии с [3] для конечного множества $\mathfrak{G}$, состоящего из графов, сетей или схем, через $|\mathfrak{G}|$ и $\|\mathfrak{G}\|$ обозначим число попарно не изоморфных и попарно не эквивалентных элементов в $\mathfrak{G}$. В частности, число попарно неэквивалентных ИКС из $\mathcal{U}^{\text{ИКС}}(L,n)$ будем обозначать через $\left\|\mathcal{U}^{\text{ИКС}}(L,n)\right\|$.

Лемма 1.1. *Число попарно неизоморфных связных графов с параллельными рёбрами, содержащих p вершин и q, $q \geqslant p-1$, рёбер, не больше, чем $4^{p-1}\left(\frac{3p^2}{q-p+1}\right)^{q-p+1}$, если*

$$p-1 < q \leqslant \frac{p(p+1)}{2} - 2, \tag{1.2}$$

и не больше, чем $4^{p-1} \cdot 6^{q-p+1}$, в остальных случаях.

Доказательство. Подсчёт указанных графов можно организовать следующим образом: сначала выбирается остовное дерево, а потом оставшиеся рёбра распределяются по всевозможным парам вершин с возможными повторениями. Остовное дерево можно выбрать 4^{p-1} способами, а число возможных распределений оставшихся рёбер по парам вершин можно оценить сверху числом сочетаний с повторениями, при условии, что число пар вершин равно $\frac{p(p-1)}{2}$. Так как число сочетаний с повторениями из n элементов по k равно $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$, то, используя известное неравенство

$$\binom{n}{m} \leqslant \left(\frac{3m}{n}\right)^{n},$$

получим при условии $q > p-1$ следующее неравенство:

$$4^{p-1} \cdot \binom{\frac{p(p-1)}{2} + q - p}{q-p+1} \leqslant 4^{p-1} \cdot \left(3\left(1 + \frac{\frac{p(p-1)}{2} - 1}{q-p+1}\right)\right)^{q-p+1}. \tag{1.3}$$

Из неравенства (1.2) вытекает, что

$$\frac{\frac{p(p-1)}{2}-1}{q-p+1} \geqslant 1$$

и поэтому неравенство (1.3) можно продолжить в случае (1.2) следующим образом:

$$4^{p-1}\cdot\left(3\left(1+\frac{\frac{p(p-1)}{2}-1}{q-p+1}\right)\right)^{q-p+1} \leqslant 4^{p-1}\cdot\left(3\left(\frac{p^2}{2(q-p+1)}+\frac{p^2}{2(q-p+1)}\right)\right)^{q-p+1} \leqslant$$
$$\leqslant 4^{p-1}\cdot\left(\frac{3p^2}{q-p+1}\right)^{q-p+1}.$$

В случае $q=p-1$ рассматриваемые графы являются деревьями, число которых не больше, чем $4^{p-1}=4^{p-1}\cdot 6^{q-p+1}$. В остальных случаях, неравенство (1.3) можно продолжить следующим образом:

$$4^{p-1}\cdot\left(3\left(1+\frac{\frac{p(p-1)}{2}-1}{q-p+1}\right)\right)^{q-p+1} \leqslant 4^{p-1}\cdot(3(1+1))^{q-p+1} \leqslant 4^{p-1}\cdot 6^{q-p+1},$$

что завершает доказательство.

Лемма доказана. □

Следствие. *В случае ориентированных графов, оценки леммы умножаются на* 2^q.

Лемма 1.2. *Если* a, m, τ, α *— действительные параметры такие, что*

$$a \geqslant 2, \quad m \geqslant 1, \quad \tau \geqslant 1, \quad \alpha \geqslant 0,$$

то выполняется неравенство

$$\max_{0\leqslant y\leqslant m}\left(\frac{ay^\tau}{m-y}\right)^{m-y} y^{\alpha m} \leqslant \left(\beta t m^\alpha (\log t)^{-\alpha-\tau}\right)^m,$$

где $\beta=\beta(\alpha,\ \tau)$, $t=am^{\tau-1}$.

Доказательство. Введём обозначения:

$$F(y)=\left(\frac{ay^\tau}{m-y}\right)^{m-y} y^{\alpha m},$$
$$f(y)=\ln F(y)=(m-y)\ln\left(\frac{ay^\tau}{m-y}\right)+\alpha m\ln y.$$

Далее, через $\beta_1, \beta_2, \ldots$ будем обозначать некоторые функции величин α и τ. Пусть $y = z \cdot m$, где $z \in [0,1]$. Тогда, дифференцируя $f(y)$, получим

$$f'(y) = \frac{m(\tau+\alpha)}{y} - \ln\left(\frac{ay^\tau}{m-y}\right) - \tau + 1 =$$
$$= \underbrace{\frac{\tau+\alpha}{z} - \ln\left(\frac{z^\tau}{1-z}\right) - \tau + 1}_{\delta(z)} - \underbrace{\ln\left(am^{\tau-1}\right)}_{>0}.$$

Заметим, что $\delta(z) \to -\infty$ при $z \to 1$, и существует $\beta_1 < 1$ такое, что $f'(y) < 0$ при $y > \beta_1 m$. Пусть ξ является точкой максимума функции f, тогда $f'(\xi) = 0$ и $\xi \leqslant \beta_1 m$. Если обе части последнего неравенства умножить на -1, прибавить m, разделить на $(1-\beta_1)$, и возвести в степень $\frac{1}{\tau}$, то получим неравенство

$$m^{\frac{1}{\tau}} \leqslant \beta_2 (m-\xi)^{\frac{1}{\tau}}. \tag{1.4}$$

В точке максимума выполняется условие $f'(\xi) = 0$, из которого следует, что

$$\frac{m(\tau+\alpha)}{\xi} - \tau \ln\left(\frac{e^{\left(1-\frac{1}{\tau}\right)} a^{\frac{1}{\tau}} \xi}{(m-\xi)^{\frac{1}{\tau}}}\right) = 0. \tag{1.5}$$

Обозначив $e^{1-\frac{1}{\tau}}$ через β_3, из (1.5) и (1.4) получаем

$$\ln\left(\beta_3 \frac{a^{\frac{1}{\tau}}\xi}{(m-\xi)^{\frac{1}{\tau}}}\right) \cdot \beta_3 \frac{a^{\frac{1}{\tau}}\xi}{(m-\xi)^{\frac{1}{\tau}}} = \frac{m(\tau+\alpha)}{\xi\tau} \cdot \beta_3 \frac{a^{\frac{1}{\tau}}\xi}{(m-\xi)^{\frac{1}{\tau}}} =$$
$$= \beta_3 \frac{\tau+\alpha}{\tau} \cdot \underbrace{\frac{ma^{\frac{1}{\tau}}}{(m-\xi)^{\frac{1}{\tau}}}}_{\geqslant m^{\frac{1}{\tau}}/\beta_2} \leqslant \beta_4 m^{1-\frac{1}{\tau}} a^{\frac{1}{\tau}},$$

где $\beta_4 = \beta_2\beta_3\frac{\tau+\alpha}{\tau}$. Положим $w = \beta_4 a^{\frac{1}{\tau}} m^{1-\frac{1}{\tau}}$, $u = \beta_3 \frac{a^{\frac{1}{\tau}}\xi}{(m-\xi)^{\frac{1}{\tau}}}$. Тогда, как показано выше, $w \geqslant u \ln u$, откуда $u \leqslant r\frac{w}{\ln w}$ для некоторой константы r (можно взять $r = 2$). Отсюда, положив $\beta_5 = r\beta_4^{-1}$, имеем

$$\frac{a^{\frac{1}{\tau}}\xi}{(m-\xi)^{\frac{1}{\tau}}} \leqslant \beta_5 a^{\frac{1}{\tau}} m^{1-\frac{1}{\tau}} \cdot \left(\ln\left(\beta_4 a^{\frac{1}{\tau}} m^{1-\frac{1}{\tau}}\right)\right)^{-1} = \frac{\beta_5}{\tau} \cdot \frac{(am^{\tau-1})^{1/\tau}}{\ln\left(\beta_4 (am^{\tau-1})^{1/\tau}\right)} \leqslant \frac{\beta_6 t^{\frac{1}{\tau}}}{\log t}, \tag{1.6}$$

где $t = am^{\tau-1}$. Из последнего неравенства следует, что

$$\xi \leqslant \frac{(m-\xi)^{1/\tau}}{a^{1/\tau}} \cdot \frac{\beta_6 t^{1/\tau}}{\log t} = \frac{\beta_6 m}{\log t} \cdot \left(\frac{m-\xi}{m}\right)^{1/\tau} \leqslant \frac{\beta_7 m}{\log t}. \tag{1.7}$$

Пользуясь неравенствами (1.6) и (1.7), получаем

$$\max_{0\leqslant y\leqslant m} F(y) = F(\xi) \leqslant \left(\frac{a^{\frac{1}{\tau}}\xi}{(m-y)^{\frac{1}{\tau}}}\right)^{\tau m} \xi^{\alpha m} \leqslant \left(\beta t m^{\alpha}(\log t)^{-\alpha-\tau}\right)^{m}.$$

Лемма доказана. □

Теорема 1.1. *Для любых натуральных n и L выполняются неравенства*[1]

$$\left\|\mathcal{U}^{\text{КС}}(L,n)\right\| \leqslant \left(\frac{e_1 nL}{\log^2 L}\right)^{L}, \tag{1.8}$$

$$\left\|\mathcal{U}^{\overrightarrow{\text{КС}}}(L,n)\right\| \leqslant \left(\frac{e_2 nL}{\log^2 L}\right)^{L}, \tag{1.9}$$

$$\left\|\mathcal{U}^{\text{ИКС}}(L,n)\right\| \leqslant \left(\frac{e_3 (n+L)^2}{\log^3 (n+L)}\right)^{L+2n}. \tag{1.10}$$

Доказательство. Введём сначала некоторые вспомогательные величины и установим для них верхние оценки на основе лемм 1.1, 1.2. Пусть $\mathcal{N}(q)$ — число попарно не изоморфных связных неориентированных графов с не более чем q (возможно, параллельными) ребрами, а $\widehat{\mathcal{N}}(q)$ — число аналогичных графов, в каждом из которых любое ребро помечено либо одним из s специальных символов, либо одной из вершин данного графа.

Заметим, что

$$\mathcal{N}(q) = \sum_{t=1}^{q}\sum_{p=1}^{t+1}\mathcal{N}(p,t), \quad \text{и} \quad \widehat{\mathcal{N}}(q) \leqslant \sum_{t=1}^{q}\sum_{p=1}^{t+1}\mathcal{N}(p,t)\cdot(p+s)^t, \tag{1.11}$$

где $\mathcal{N}(q,t)$ — число попарно неизоморфных связных неориентированных графов с p вершинами и t (возможно, параллельными) ребрами, которое оценивалось в лемме 1.1. Для удобства работы с этими оценками введем функции $Q(t)$ и $\widehat{Q}(t,s)$ натуральных аргументов t и s вида

$$Q(t) = \max_{1\leqslant p\leqslant t}\left\{\left(\frac{3p^2}{q-p+1}\right)^{t-p+1}\right\}, \quad \widehat{Q}(t,s) = \max_{1\leqslant p\leqslant t}\left\{\left(\frac{3p^2}{q-p+1}\right)^{q-p+1}\cdot(p+s)^t\right\}, \tag{1.12}$$

где максимум берется по всем действительным значениям параметра p из отрезка $[1,t]$.

Из (1.12) следует, что

$$\widehat{Q}(t,s) \leqslant Q(t)\cdot(t+s)^t, \tag{1.13}$$

[1]Буквой e с различными индексами обозначаются некоторые положительные константы.

и что функции $Q(t)$, $\widehat{Q}(t,s)$ монотонно не убывают по t, так как при $t' \geqslant t$ и $p' = p + (t' - t)$ выполняются неравенства

$$\left(\frac{3(p')^2}{t'-p'+1}\right)^{t'-p'+1} \geqslant \left(\frac{3p^2}{t-p+1}\right)^{t-p+1} \qquad \text{и} \qquad (p'+s)^{t'} \geqslant (p+s)^t.$$

Заметим также, что

$$Q(t) \geqslant 3^t \qquad \text{и} \qquad \widehat{Q}(t,s) \geqslant \left(\frac{3}{2}\right)^t \cdot (t+s)^t. \tag{1.14}$$

Действительно, в случае $t \geqslant 4$ и $p = \frac{t}{2} + 1$ выполняются неравенства

$$Q(t) \geqslant \left(\frac{3\left(\frac{t}{2}+1\right)^2}{\frac{t}{2}}\right)^{\frac{t}{2}} \geqslant 9^{\frac{t}{2}} = 3^t, \qquad \widehat{Q}(t,s) \geqslant 3^t \cdot \left(\frac{t}{2}+s+1\right)^t \geqslant \left(\frac{3}{2}\right)^t \cdot (t+s)^t,$$

а в случае $1 \leqslant t \leqslant 3$ и $p = t$ — неравенства

$$Q(t) \geqslant 3t^2 \geqslant 3^t, \qquad \widehat{Q}(t,s) \geqslant 3^t \cdot (t+s)^t,$$

которые в совокупности доказывают (1.14).

Опираясь на лемму 1.1, соотношения (1.11)–(1.14) и монотонность функций $Q(t), \widehat{Q}(t,s)$ по t, докажем, что

$$\mathcal{N}(q) \leqslant 5 \cdot 4^q \cdot Q(q), \qquad \widehat{\mathcal{N}}(q,s) \leqslant 5 \cdot 4^q \cdot \widehat{Q}(q,s)(q+s)^q, \tag{1.15}$$

Действительно, используя оценки леммы 1.1 и первые части соотношений (1.11), (1.12), получим

$$\mathcal{N}(q) = \sum_{t=1}^{q}\sum_{p=1}^{t+1}\mathcal{N}(p,t) \leqslant \sum_{t=1}^{q}\sum_{p=1}^{t+1}4^{p-1}6^{t-p+1} + \sum_{t=2}^{q}\sum_{p=2}^{t}4^{p-1}Q(t) =$$
$$= \sum_{t=1}^{q}6^t\sum_{p=1}^{t+1}\left(\frac{2}{3}\right)^{p-1} + \sum_{t=2}^{q}Q(t)\left(\frac{4^t-1}{3}\right),$$

откуда в силу монотонности $Q(t)$ и первого из неравенств (1.14) следует, что

$$\mathcal{N}(q) \leqslant \frac{18}{5} \cdot 6^q + \frac{4}{9} \cdot 4^q \cdot Q(q) \leqslant 5 \cdot 4^q \cdot Q(q).$$

Второе из неравенств (1.15) устанавливается аналогично с использованием вторых частей соотношений (1.11), (1.12), (1.14), а также неравенства (1.13).

Неравенства

$$\mathcal{N}(q) \leqslant \left(e_0\frac{q}{\log^2 q}\right)^q, \qquad \text{и} \qquad \widehat{\mathcal{N}}(q,s) \leqslant \left(e_0\frac{q+s}{\log^3(q+s)}\right)^{q+s} \tag{1.16}$$

вытекают, с учетом (1.12), (1.15), из леммы 1.2, где

$$a = 3, m = q + 1, \tau = 2, \alpha = 0, y = p \quad \text{и} \quad a = 3, m = q + s + 1, \tau = 2, \alpha = 1, y = p + s$$

соответственно.

Оценки (1.8) и (1.9) получаются, с учетом леммы 1.1 и её следствия, из первого неравенства (1.16) при $q = L$, так как число попарно неэквивалентных КС рассматриваемого вида из неориентированных контактов можно оценить сверху произведением числа попарно неизоморфных связных неориентированных графов с не более чем L рёбрами и двумя полюсами на число возможных способов выбора пометок их рёбер БП $x_1, \ldots, x_n$ или отрицаниями этих БП.

Для доказательства (1.10) заметим, что число возможных способов выбора пометок рёбер для ИКС рассматриваемого вида с p вершинами не превосходит $(2n + p)^L$. Следовательно, справедливо неравенство:

$$\left\| \mathcal{U}^{\text{ИКС}}(L, n) \right\| \leqslant \widehat{\mathcal{N}}(L, 2n) \cdot L^2,$$

из которого неравенство (1.10) вытекает в силу второго неравенства (1.16).

Теорема доказана. □

На основе теоремы 1.1 с помощью мощностного метода Шеннона обычным образом (см., например, [3]) устанавливаются нижние мощностные оценки функций Шеннона $L^{\text{КС}}(n)$, $L^{\overrightarrow{\text{КС}}}(n)$, $L^{\text{ИКС}}(n)$ для классов $\mathcal{U}^{\text{КС}}$, $\mathcal{U}^{\overrightarrow{\text{КС}}}$ и $\mathcal{U}^{\text{ИКС}}$ соответственно.

Теорема 1.2. *Для натуральных $n = 1, 2, \ldots$ выполняются неравенства*

$$L^{\text{КС}}(n) \geqslant \frac{2^n}{n} \left(1 + \frac{2 \log n - O(1)}{n} \right), \tag{1.17}$$

$$L^{\overrightarrow{\text{КС}}}(n) \geqslant \frac{2^n}{n} \left(1 + \frac{2 \log n - O(1)}{n} \right), \tag{1.18}$$

$$L^{\text{ИКС}}(n) \geqslant \frac{2^{n-1}}{n} \left(1 + \frac{\frac{5}{2} \log n - O(1)}{n} \right). \tag{1.19}$$

Доказательство. Неравенства (1.17)–(1.19) могут быть получены в результате применения соотношения (4.1) и леммы 4.1 из §4 гл. 4 пособия [3] к (1.8)–(1.10). Приведём, тем не менее, технически более простой вариант доказательства (1.17)–(1.19), опирающийся на тот факт, что все рассматриваемые функции Шеннона имеют порядок роста $\frac{2^n}{n}$, то есть, в частности,

$$L^A(n) \leqslant c \frac{2^n}{n}, \tag{1.20}$$

где $A \in \{ \text{КС}, \overrightarrow{\text{КС}}, \text{ИКС} \}$, а c — некоторая константа, не зависящая от n.

В силу (1.20) и равенства Шеннона (см. [3])

$$\left\|\mathcal{U}^A\left(L^A(n),n\right)\right\| = 2^{2^n}$$

из (1.8)–(1.10) следует, что

$$\begin{aligned}
2^n &= \log\left\|\mathcal{U}^{\text{КС}}\big(L^{\text{КС}}(n),n\big)\right\| \leqslant L^{\text{КС}}(n)\cdot(n-2\log n+O(1)),\\
2^n &= \log\left\|\mathcal{U}^{\overrightarrow{\text{КС}}}\big(L^{\overrightarrow{\text{КС}}}(n),n\big)\right\| \leqslant L^{\overrightarrow{\text{КС}}}(n)\cdot(n-2\log n+O(1)),\\
2^n &= \log\left\|\mathcal{U}^{\text{ИКС}}\big(L^{\text{ИКС}}(n),n\big)\right\| \leqslant \big(L^{\text{ИКС}}(n)+2n\big)\cdot(2n-5\log n+O(1)).
\end{aligned}$$

Решение полученных неравенств относительно соответствующих функций Шеннона даёт (1.17)–(1.19).

Теорема доказана. □

§2 Формулы и СФЭ в произвольном базисе, усилительные СФЭ. Верхние оценки числа формул и СФЭ, нижние мощностные оценки функций Шеннона

Продолжим начатое в [3] (см. гл. 2, 4) изучение формул и схем из функциональных элементов (СФЭ) над произвольным конечным полным базисом $\text{Б} = \{\mathcal{E}_i\}_{i=1}^b$, где функциональный элемент (ФЭ) $\mathcal{E}_i$ реализует ФАЛ $\varphi_i(x_1,\dots,x_{k_i})$, которая в случае $k_i \geqslant 2$ существенно зависит от всех своих переменных.

Будем по-прежнему (ср. с §3 главы 2 пособия [3]) представлять СФЭ Σ в виде $\Sigma = \Sigma(x;\,z)$, если $x = (x_{i_1},\dots,x_{i_n})$ и $z = (z_{j_1},\dots,z_{j_n})$ — наборы, составленные из всех её различных входных и выходных булевых переменных (БП), перечисленных в порядке возрастания их номеров в алфавитах $X = \{x_1,x_2,\dots,x_n,\dots\}$ и $Z = \{z_1,z_2,\dots,z_m,\dots\}$, соответственно. Сложность, то есть число ФЭ, глубину, то есть максимальное число последовательно соединённых ФЭ, и ранг, то есть число дуг, исходящих из входов, в схеме Σ, следуя [3], будем обозначать через $L(\Sigma)$, $D(\Sigma)$ и $R(\Sigma)$ соответственно.

Будем рассматривать формулы и СФЭ с различными ограничениями на соединения ФЭ. Так, для базисов, имеющих одновходовые неконстантные ФЭ, введём понятие *усилительной* СФЭ — СФЭ, в которой «ветвятся» выходы только указанных ФЭ. Заметим, что данное ограничение выполняется во многих классах электронных схем, причем в соответствующих базисах имеются специальные «усилительные» ФЭ, реализующие тождественную ФАЛ.

Введём теперь «взвешенные» функционалы сложности и глубины СФЭ. Будем считать, что каждому функциональному элементу $\mathcal{E}_i$, $i = 1,\dots,b$, сопоставлены положительные действительные числа $\mathcal{L}_i$ и T_i, называемые его «весом» и «задержкой», которые характеризуют сложность («размер») и время срабатывания $\mathcal{E}_1$ соответственно. Предполагается, что «вес» и «задержка» любого ФЭ стандартного базиса $\text{Б}_0 = \{\&,\vee,\neg\}$ равны 1. Если (v_0,v_t)-цепь C длины t в СФЭ Σ проходит

через вершины $v_1, \ldots, v_{t-1}$, и вершине v_j, $j = 1, \ldots, t$, при этом соответствует ФЭ $\mathcal{E}_{i_j}$ базиса Б, то число $T(C) = T_{i_1} + \cdots + T_{i_t}$ будем называть *задержкой* этой цепи.

По аналогии с глубиной определим *задержку* вершины v СФЭ Σ как максимальную задержку тех цепей Σ, которые начинаются в одной из ее входных вершин и заканчиваются в вершине v. Для каждой СФЭ Σ над базисом Б помимо сложности $L(\Sigma)$, глубины $D(\Sigma)$ и ранга $R(\Sigma)$ определим следующие параметры (функционалы сложности):

1) $\mathcal{L}(\Sigma)$ — *размер* Σ, то есть сумма «весов» всех её ФЭ;

2) $T(\Sigma)$ — *задержка* Σ, то есть максимальная задержка её вершин.

Заметим, что функционал L (D) является частным случаем функционала $\mathcal{L}$ (соответственно T), когда веса (соответственно задержки) всех ФЭ базиса Б равны 1. Введем также «частичный» размер $\mathcal{L}_{Б'}(\Sigma)$ (задержку $T_{Б'}(\Sigma)$), который равен сумме весов ФЭ Σ типа $\mathcal{E}_i$, где $\mathcal{E}_i \in Б'$, в СФЭ Σ (соответственно максимальной сумме задержек ФЭ указанного вида, лежащих на одной цепи Σ). Аналогичным образом вводится «частичная» сложность $L_{Б'}(\Sigma)$ и «частичная» глубина $D_{Б'}(\Sigma)$ для СФЭ Σ.

Напомним (см. [3]), что СФЭ называется *приведённой*, если выход любого её ФЭ, не являющийся выходом схемы, поступает на вход другого ФЭ этой схемы. Приведённая СФЭ (системы формул) считается *строго приведённой*, если в ней нет эквивалентных вершин, то есть вершин, в которых реализуются равные ФАЛ (соответственно нет эквивалентных вершин, лежащих на одно цепи). Заметим, что для любой СФЭ (системы формул) Σ существует эквивалентная ей строго приведённая СФЭ (соответственно система формул) Σ', для которой

$$\mathcal{L}_{Б'}(\Sigma') \leqslant \mathcal{L}_{Б'}(\Sigma) \quad \text{и} \quad T_{Б'}(\Sigma') \leqslant T_{Б'}(\Sigma)$$

при любом $Б' \subseteq Б$. Легко видеть также, что в строго приведённой формуле или СФЭ нет трёх или более последовательно соединённых одновходовых ФЭ.

Для базиса $Б = \{\mathcal{E}_i\}_{i=1}^{b}$ положим $\widehat{Б} = \{\, \mathcal{E}_i \mid k_i \geqslant 2 \,\}$ и заметим, что множество $\widehat{Б}$ не пусто в силу полноты базиса Б. Для ФЭ $\mathcal{E}_i$, $\mathcal{E}_i \in \widehat{Б}$, определим его *приведённый вес* ρ_i и *приведённую задержку* τ_i следующим образом:

$$\rho_i = \frac{\mathcal{L}_i}{k_i - 1}, \qquad \tau_i = \frac{T_i}{\log k_i}.$$

Введём, далее, величины

$$\rho_Б = \min_{\mathcal{E}_i \in \widehat{Б}} \rho_i \quad \text{и} \quad \tau_Б = \min_{\mathcal{E}_i \in \widehat{Б}} \tau_i,$$

которые назовём *приведённым весом* и *приведённой задержкой базиса* Б соответственно. Для стандартного базиса $Б_0 = \{\&, \vee, \neg\}$, очевидно,

$$\widehat{Б}_0 = \{\&, \vee\}, \quad \rho_{Б_0} = \tau_{Б_0} = 1.$$

Для функционала сложности ψ типа L, $\mathcal{L}$, D, T через $\widehat{\psi}(\Sigma)$ будем обозначать величину $\psi_{\widehat{\text{Б}}}(\Sigma)$.

Следуя [3] обозначим через $\mathcal{U}_{\text{Б}}^{\text{С}}$, $\mathcal{U}_{\text{Б}}^{\text{УС}}$ и $\mathcal{U}_{\text{Б}}^{\Phi}$ множество СФЭ над базисом Б, множество усилительных СФЭ над Б и множество формул над Б соответственно. При этом для каждого A, $A \in \{\text{С}, \text{УС}, \Phi\}$ определим размер $\mathcal{L}_{\text{Б}}^{A}(F)$ ФАЛ или системы ФАЛ F в классе $\mathcal{U}_{\text{Б}}^{A}$ и её задержку $T_{\text{Б}}(F)$ обычным образом, а через $\mathcal{L}_{\text{Б}}^{A}(n)$ и $T_{\text{Б}}(n)$ обозначим соответствующие функции Шеннона.

Лемма 2.1. *Для любой формулы $\mathcal{F}$, $\mathcal{F} \in \mathcal{U}_{\text{Б}}^{\Phi}$, выполняются неравенства*

$$R(\mathcal{F}) \leqslant \frac{1}{\rho_{\text{Б}}}\widehat{\mathcal{L}}(\mathcal{F}) + 1, \qquad R(\mathcal{F}) \leqslant 2^{\frac{\widehat{T}(\mathcal{F})}{\tau_{\text{Б}}}}. \tag{2.1}$$

Доказательство. Пусть для каждого i, $i = 1, \ldots, b$, формула $\mathcal{F}$ содержит s_i ФЭ $\mathcal{E}_i$. При этом для числа ребер квазидерева $\mathcal{F}$ будут выполняться равенства

$$|E(\mathcal{F})| = \sum_{i=1}^{b} s_i \cdot k_i = R(\mathcal{F}) + \sum_{i=1}^{b} s_i - 1.$$

Следовательно,

$$R(\mathcal{F}) = \sum_{i=1}^{b} s_i(k_i - 1) + 1 = \sum_{k_i \geqslant 2} \frac{k_i - 1}{\mathcal{L}_i} \cdot \mathcal{L}_i s_i + 1 \leqslant \frac{1}{\rho_{\text{Б}}} \sum_{k_i \geqslant 2} \mathcal{L}_i s_i + 1 = \frac{1}{\rho_{\text{Б}}}\widehat{\mathcal{L}}(\mathcal{F}) + 1$$

и первое неравенство (2.1) доказано.

Второе неравенство (2.1) доказывается индукцией по $D(\mathcal{F})$. Действительно, при $D(\mathcal{F}) = 0$, когда $\mathcal{F} = x_j$, оно, очевидно, выполняется. Пусть теперь второе неравенство (2.1) верно для любой формулы глубины меньше, чем d, и пусть $\mathcal{F} = \varphi_i(\mathcal{F}_1, \ldots, \mathcal{F}_{k_i})$, где $D(\mathcal{F}) = d$ и $D(\mathcal{F}_j) < d$, $\widehat{T}(\mathcal{F}_j) = t_j$ при всех $j = 1, \ldots, k_i$. Тогда

$$R(\mathcal{F}) = \sum_{j=1}^{k_i} R(\mathcal{F}_j) \leqslant k_i \cdot 2^{\frac{t}{\tau_{\text{Б}}}},$$

где $t = \max_{1 \leqslant j \leqslant k_i} t_j$. Следовательно, при $k_i = 1$ формула $\mathcal{F}$ удовлетворяет второму неравенству (2.1), так как в этом случае $\widehat{T}(\mathcal{F}) = t$. При $k_i \geqslant 2$ в соответствии с определением $\tau_{\text{Б}}$ выполняется неравенство

$$k_i \leqslant 2^{\frac{T_i}{\tau_{\text{Б}}}},$$

используя которое и учитывая, что в данном случае $\widehat{T}(\mathcal{F}) = t + T_i$, получим

$$R(\mathcal{F}) \leqslant k_i \cdot 2^{\frac{t}{\tau_{\text{Б}}}} \leqslant 2^{\frac{t+T_i}{\tau_{\text{Б}}}} = 2^{\frac{\widehat{T}(\mathcal{F})}{\tau_{\text{Б}}}}.$$

Лемма доказана. □

Замечание. Аналогично первому неравенству (2.1) доказывается, что число рёбер дерева, соответствующего формуле $\mathcal{F}$, в которой нет трёх и более последовательно соединённых одновходовых ФЭ, удовлетворяет неравенству

$$|E(\mathcal{F})| \leqslant 6(R(\mathcal{F}) - 1). \tag{2.2}$$

Действительно, если $\mathcal{F}$ содержит s_i ФЭ $\mathcal{E}_i$, $i = 1, \ldots, b$, то

$$R(\mathcal{F}) = \sum_{i=1}^{b} s_i(k_i - 1) + 1 \geqslant \widehat{L}(\mathcal{F}) + 1,$$
$$|E(\mathcal{F})| \leqslant 3\left(R(\mathcal{F}) + \widehat{L}(\mathcal{F}) - 1\right) \leqslant 3(2R(\mathcal{F}) - 2) = 6(R(\mathcal{F}) - 1).$$

Неравенство (2.2) выполняется, в частности, для строго приведённой формулы $\mathcal{F}$.

Для приведённой одновыходной СФЭ Σ на базисом Б её *остовом* будем называть такую формулу $\mathcal{F}(x_1)$ над Б, дерево которой получается в результате применения к каждой вершине Σ операций отсоединения всех исходящих дуг, кроме одной, и объявления начальных вершин этих дуг листьями указанного дерева.

Пусть для $A \in \{\text{С}, \text{УС}\}$ $\mathcal{U}_{\text{Б}}^{A}\langle \mathcal{L}, n\rangle$ ($\mathcal{U}_{\text{Б}}^{\Phi}\langle \mathcal{L}, n\rangle$, $\mathcal{U}_{\text{Б}}^{\Phi}\{T, n\}$) — множество всех строго приведённых схем из функциональных элементов вида $\Sigma(x_1, \ldots, x_n;\, z_1)$ из $\mathcal{U}_{\text{Б}}^{A}$ (соответственно формул $\mathcal{F}(x_1, \ldots, x_n)$) из $\mathcal{U}_{\text{Б}}^{\Phi}$, для которых $\mathcal{L}(\Sigma) \leqslant \mathcal{L}$ (соответственно $\mathcal{L}(\mathcal{F}) \leqslant \mathcal{L}$, $T(\mathcal{F}) \leqslant T$).

Лемма 2.2. *Для любых $\mathcal{L} \geqslant 0$, $T \geqslant 0$ и любого натурального n справедливы неравенства*[1]*:*

$$\left\|\mathcal{U}_{\text{Б}}^{\text{С}}\langle \mathcal{L}, n\rangle\right\| \leqslant (c_1(\mathcal{L} + n))^{\frac{1}{\rho_{\text{Б}}}\mathcal{L}+1}, \tag{2.3}$$

$$\left\|\mathcal{U}_{\text{Б}}^{\Phi}\langle \mathcal{L}, n\rangle\right\| \leqslant (c_2 n)^{\frac{1}{\rho_{\text{Б}}}\mathcal{L}+1}, \tag{2.4}$$

$$\left\|\mathcal{U}_{\text{Б}}^{\Phi}\{T, n\}\right\| \leqslant (c_2 n)^{2^{\frac{T}{\tau_{\text{Б}}}}}. \tag{2.5}$$

Доказательство. Пусть $\Sigma \in \mathcal{U}^{\text{С}}\langle \mathcal{L}, n\rangle$, а $\check{\mathcal{F}}$ — остов Σ. В силу леммы 2.1 и замечания к ней число рёбер в дереве формулы $\check{\mathcal{F}}$ не больше, чем $\widehat{c}_1\mathcal{L}$, где $\widehat{c}_1 = \frac{6}{\rho_{\text{Б}}}$, а число таких попарно не изоморфных формул не превосходит $c_2^{\mathcal{L}/\rho_{\text{Б}}}$, где $c_2 \leqslant 4^6$. Любая формула $\mathcal{F}$ (СФЭ Σ) из $\mathcal{U}^{\text{С}}\langle \mathcal{L}, n\rangle$ может быть получена в результате присоединения каждого из $R(\check{\mathcal{F}}) \leqslant \frac{1}{\rho_{\text{Б}}}\mathcal{L}(\check{\mathcal{F}}) + 1$ (в силу леммы 2.1) листьев дерева формулы $\check{\mathcal{F}}$, являющейся её остовом, к входам $x_1, \ldots, x_n$ (соответственно к входам $x_1, \ldots, x_n$ и внутренним вершинам $\check{\mathcal{F}}$), которое можно осуществить не более, чем $n^{R(\check{\mathcal{F}})}$ (соответственно $(\widehat{c}_1 \cdot \mathcal{L} + n)^{R(\check{\mathcal{F}})}$) способами. Перемножая полученные оценки и учитывая (2.1) приходим к (2.3) с константой $c_1 = c_2 \max\{\widehat{c}_1, 1\}$ и (2.4).

[1] Буквой c с различными индексами будем обозначать константы, зависящие только от базиса Б

В случае $\Sigma = \mathcal{F} \in \mathfrak{U}_{\text{Б}}^{\Phi}\{T, n\}$, рассуждая аналогично, приходим к (2.5) с учётом того, что число рёбер в формуле $\check{\mathcal{F}}$ не больше, чем $6 \cdot 2^{T/\tau_{\text{Б}}}$, число таких формул не превосходит $(c_2)^{2^{T/\tau_{\text{Б}}}}$, а их ранг ограничен сверху в силу (2.1) числом $2^{T/\tau_{\text{Б}}}$.

Лемма доказана. □

Лемма 2.3. *Для любого $\mathcal{L} \geqslant 0$ и любого натурального n выполняется неравенство*

$$\left\|\mathfrak{U}_{\text{Б}}^{\text{УС}}\langle \mathcal{L}, n\rangle\right\| \leqslant \left(\frac{c_3(\mathcal{L}+n)}{\log(\mathcal{L}+n)}\right)^{\frac{1}{\rho_{\text{Б}}}(\widehat{\mathcal{L}}+n)+1}. \tag{2.6}$$

Доказательство. На основе рассуждений из доказательства леммы 2.2 и с учетом (2.1)–(2.3) можно показать, что число СФЭ Σ, $\Sigma \in \mathfrak{U}_{\text{Б}}^{\text{УС}}\langle \mathcal{L}, n\rangle$, для которых $\widehat{\mathcal{L}}(\Sigma) = \widehat{\mathcal{L}}$, не больше, чем

$$c_2^{\frac{\mathcal{L}}{\rho_{\text{Б}}}}\left(\frac{1}{c_4}(\mathcal{L}-\widehat{\mathcal{L}})+n\right)^{\frac{\widehat{\mathcal{L}}}{\rho_{\text{Б}}}+1} \leqslant c_5^{\mathcal{L}}\left(\mathcal{L}-\widehat{\mathcal{L}}+n\right)^{\frac{\widehat{\mathcal{L}}}{\rho_{\text{Б}}}+1},$$

где c_4 — минимальный «вес» одновходовых ФЭ базиса Б. Отсюда следует, что

$$\left\|\mathfrak{U}_{\text{Б}}^{\text{УС}}\langle \mathcal{L}, n\rangle\right\| \leqslant c_6^{\mathcal{L}} \max_{\widehat{\mathcal{L}}\in[0,\mathcal{L}]} (\mathcal{L}-\widehat{\mathcal{L}}+n)^{\frac{\widehat{\mathcal{L}}}{\rho_{\text{Б}}}+1}.$$

Находя максимум правой части полученного неравенства как функции параметра $\widehat{\mathcal{L}}$, принимающего значения из действительного отрезка $[0, \mathcal{L}]$, с помощью леммы 1.2, где

$$m = \frac{1}{\rho_{\text{Б}}}(\mathcal{L}+n)+1, \quad y = \frac{1}{\rho_{\text{Б}}}(\mathcal{L}-\widehat{\mathcal{L}}+n), \quad a = m, \quad \tau = 1, \quad \alpha = 0,$$

получим (2.6).

Лемма доказана. □

Из лемм 2.2, 2.3 с помощью мощностного метода (см. (1.20) и (1.14')) выводится следующая теорема.

Теорема 2.1. *Для натуральных $n = 1, 2, \ldots$ выполняются неравенства*

$$\mathcal{L}_{\text{Б}}^{\text{С}}(n) \geqslant \rho_{\text{Б}}\frac{2^n}{n}\left(1+\frac{\log n - O(n)}{n}\right), \tag{2.7}$$

$$\mathcal{L}_{\text{Б}}^{\text{УС}}(n) \geqslant \rho_{\text{Б}}\frac{2^n}{n}\left(1+\frac{2\log n - O(1)}{n}\right), \tag{2.8}$$

$$\mathcal{L}_{\text{Б}}^{\Phi}(n) \geqslant \rho_{\text{Б}}\frac{2^n}{\log n}\left(1-O\left(\frac{1}{\log n}\right)\right), \tag{2.9}$$

$$T_{\text{Б}}(n) \geqslant \tau_{\text{Б}}(n - \log\log n) - O(1). \tag{2.10}$$

Для базиса $Б_0' = \{x_1 \cdot x_2, \neg x_1\}$, в котором $L_\& = L_\neg = 1$ и $T_\& = T_\neg = 1$, оценки лемм 2.2, 2.3 можно уточнить следующим образом.

Лемма 2.4. *Для любого $L \geqslant 0$ и любого натурального n выполняются неравенства*

$$\left\| \mathcal{U}^{\Phi}_{Б_0'}(L,n) \right\| \leqslant \left(\frac{e_4 n}{\log n} \right)^{L+2}, \tag{2.11}$$

$$\left\| \mathcal{U}^{УС}_{Б_0'}(L,n) \right\| \leqslant \left(\frac{e_5 (L+n)}{\log^2 (L+n)} \right)^{L+n+2}. \tag{2.12}$$

Доказательство. Пусть $\mathcal{F}(x_1)$ — остов какой-либо СФЭ (формулы) Σ, $\Sigma \in \mathcal{U}^{УС}_{Б_0'}$, и пусть

$$p = L_1(\Sigma) + 1, \qquad R(\mathcal{F}) = R \leqslant -p + 2,$$

а M, $M \leqslant L - p + 2$ (соответственно $M \leqslant n$), — число тех вершин Σ, от которых при переходе от Σ к $\mathcal{F}$ были отсоединены исходящие дуги. Разобьём множество листьев дерева $\mathcal{F}$ на p групп, включив в i-ую группу, $i = 1, \ldots, p$, все те t_i, $t_i \geqslant 0$, листьев, которые связаны цепочкой из ФЭ & с i-м ФЭ $\neg$, если $i < p$, и связаны аналогичным образом с выходом Σ, если $i = p$.

Заметим, что число способов выбора остова $\mathcal{F}$ схемы (формулы) Σ не больше, чем 4^{2L}, и что выбор формулы $\mathcal{F}$ однозначно определяет описанное выше разбиение листьев дерева $\mathcal{F}$ на группы. Заметим также, что число тех попарно не эквивалентных схем (формул) Σ указанного вида, которые можно получить из одного и того же остова в результате соответствующего присоединения его листьев, не больше, чем

$$\max_{1 \leqslant t_1 + \cdots + t_p \leqslant R} \left\{ C_M^{t_1} \cdot \ldots \cdot C_M^{t_p} \right\} \leqslant$$
$$\leqslant \max_{1 \leqslant t_1 + \cdots + t_p \leqslant R} \left\{ \left(\frac{3M}{t_1} \right)^{t_1} \cdot \ldots \cdot \left(\frac{3M}{t_p} \right)^{t_p} \right\} \leqslant \max_{1 \leqslant p \leqslant L+2} \left(\frac{3Mp}{L-p+2} \right)^{L-p+2}.$$

Следовательно, в силу леммы 1.2, где $a = 3n$, $\tau = 1$, $\alpha = 0$, $m = L + 2$ и $y = p$, получим неравенство

$$\left\| \mathcal{U}^{\mathcal{F}}_{Б_0'}(L,n) \right\| \leqslant 16^L \max_{1 \leqslant p \leqslant L+2} \left(\frac{3np}{L-p+2} \right)^{L-p+2} \leqslant \left(\frac{e_4 n}{\log n} \right)^{L+2},$$

а при $a = 3$, $\tau = 2$, $\alpha = 0$, $m = L+n+2$, $y = n+p$ и с учётом числа способов выбора тех вершин остова, от которых отсоединялись исходящие дуги, — неравенство

$$\left\| \mathcal{U}^{УС}_{Б_0'}(L,n) \right\| \leqslant 32^L \max_{1 \leqslant p \leqslant L+2} \left(\frac{3(n+p) \cdot p}{L-p+2} \right)^{L-p+2} \leqslant \left(\frac{e_5 (L+n)}{\log^2 (L+n)} \right)^{L+n+2}.$$

Лемма доказана. □

Из леммы 2.4 на основе мощностных соображений выводится следующая теорема.

Теорема 2.2. *Для натуральных* $n = 1, 2, \ldots$ *выполняются неравенства*

$$\mathcal{L}^{\Phi}_{\text{Б}'_0}(n) \geqslant \rho_{\text{Б}} \frac{2^n}{\log n} \left(1 + \frac{\log\log n - O(1)}{\log n}\right), \tag{2.13}$$

$$\mathcal{L}^{\text{УС}}_{\text{Б}'_0}(n) \geqslant \rho_{\text{Б}} \frac{2^n}{n} \left(1 + \frac{3\log n - O(1)}{n}\right). \tag{2.14}$$

Замечание. Аналогичным образом, с учётом теоремы 2.1 для произвольного базиса Б устанавливаются следующие мощностные нижние оценки

$$\mathcal{L}^{\Phi}_{\text{Б}}(n) \geqslant \rho_{\text{Б}} \frac{2^n}{\log n} \left(1 + \frac{æ_{\text{Б}} \log\log n - O(1)}{\log n}\right),$$

$$\mathcal{L}^{\text{УС}}_{\text{Б}}(n) \geqslant \rho_{\text{Б}} \frac{2^n}{n} \left(1 + \frac{(2 + æ_{\text{Б}}) \log n - O(1)}{n}\right),$$

где $æ_{\text{Б}} \in \{0, 1\}$ и $æ_{\text{Б}} = 1$ тогда и только тогда, когда все ФЭ $\mathcal{E}_i \in$ Б, для которых $\rho_i = \rho_{\text{Б}}$, реализуют либо только монотонные ЭК, либо только монотонные ЭД, либо только линейные ФАЛ.

§3 Универсальные системы ФАЛ и их построение на основе селекторных разбиений БП

Напомним (см. [3]), что множество ФАЛ G называется дизъюнктивно-универсальным множеством (ДУМ) ФАЛ порядка m и ранга p, тогда и только тогда, когда $G \subseteq P_2(m)$ и для любой ФАЛ g, $g \in P_2(m)$, найдутся функции $g_1, \ldots, g_p$ из G для которых $g = g_1 \vee \cdots \vee g_p$.

Обобщим понятие ДУМ ФАЛ следующим образом. Пусть $\varphi(y_1, \ldots, y_p)$ — существенная ФАЛ, то есть ФАЛ, существенно зависящая от всех своих БП. Множество ФАЛ G, $G \in P_2(m)$, называется *φ–универсальным множеством (φ–УМ) порядка* m, если любая ФАЛ g, $g \in P_2(m)$, может быть представлена в виде

$$g = \varphi(g_1, \ldots, g_p), \tag{3.1}$$

где $g_i \in G$ при всех i, $i = 1, \ldots, p$. Заметим, что в случае $\varphi(y_1, \ldots, y_p) = y_1 \vee \cdots \vee y_p$ понятие φ–УМ совпадает с понятием ДУМ ранга p.

Так же, как и ДУМ (см. [3]), будем строить φ–УМ порядка m на основе разбиения $\Delta = (\delta_1, \ldots, \delta_p)$ единичного куба B^m. Для каждого i, $i = 1, \ldots, p$, в силу существенной зависимости ФАЛ φ от БП y_i найдётся набор двоичных констант $\alpha_{i,1}, \ldots, \alpha_{i,p}$ такой, что

$$\varphi(\alpha_{i,1}, \ldots, \alpha_{i,i-1},\ y_i,\ \alpha_{i,i+1}, \ldots, \alpha_{i,p}) = y_i \oplus \alpha_{i,i}. \tag{3.2}$$

Обозначим через $G^{(j)}$, $j = 1, \ldots, p$, множество всех тех ФАЛ из $P_2(m)$, которые при любом i, $1 \leqslant i \leqslant p$ и $j \neq i$, равны $\alpha_{i,j}$ на множестве наборов δ_i, и пусть

$$G = G^{(1)} \cup \cdots \cup G^{(p)}. \tag{3.3}$$

Нетрудно убедиться в том, что равенство (3.1) имеет место для любой функции g, $g \in P_2(m)$, если g_i, $i = 1, \ldots, p$, — ФАЛ из $G^{(i)}$, совпадающая на δ_i с ФАЛ $g \oplus \alpha_{i,i}$. Действительно, для любого i, $i = 1, \ldots, p$, и любого набора β, $\beta \in \delta_i$, в силу (3.2), получим:

$$\varphi(g_1(\beta), \ldots, g_p(\beta)) = \varphi(\alpha_{i,1}, \ldots, \alpha_{i,i-1},\ g(\beta) \oplus \alpha_{i,i},\ \alpha_{i,i+1}, \ldots, \alpha_{i,p}) = g(\beta).$$

Следовательно, множество G представляет собой φ–УМ порядка m, которое будем называть *стандартным φ–УМ, связанным с разбиением* Δ.

Приведём пример стандартного φ–УМ для функции $\varphi(y_1, \ldots, y_p) = y_1 y_{t+1} \vee \vee y_2 y_{t+2} \vee \cdots \vee y_t y_{2t}$, где $p = 2t$, связанного с разбиением куба B^m на последовательные отрезки $\delta_1, \ldots, \delta_p$ длины $s_1, \ldots, s_p$ соответственно, где $s_1 + \cdots + s_p = 2^m$. Если при этом константы в (3.2) выбрать так, что $\alpha_{i,j} = 1$ только тогда, когда $|i - j| = t$, то соответствующее стандартное φ–УМ $\widetilde{G}$ порядка m будет иметь вид (3.3), где $G^{(j)}$ состоит из таких ФАЛ g, $g \in P_2(m)$, для которых $g(\alpha) = 1$ при $\alpha \in \delta_i$, если $|i - j| = t$, и $g(\alpha) = 0$ на остальных отрезках δ_i, за исключением δ_j. Заметим, что полученное φ–УМ $\widetilde{G}$ имеет мощность $t(2^{s'} + 2^{s''})$, если $|s_1| = \cdots = |s_t| = s'$ и $s_{t+1} = \cdots = |s_{2t}| = s''$, где $t(s' + s'') = 2^m$.

Заметим также, что в указанном случае можно построить и более компактное φ–УМ порядка m для рассматриваемой функции φ. Введём множество $\check{G}$, $\check{G} \subset P_2(m)$, которое состоит из $2^{s''}$ функций, равных единице на множестве $\delta_1 \cup \cdots \cup \delta_t$ и принимающих одинаковые значения на наборах с одинаковыми номерами внутри компонент $\delta_{t+1}, \ldots, \delta_{2t}$. Из определения множеств $G^{(1)}, \ldots, G^{(t)}$ и того факта, что при $1 \leqslant i \leqslant t$ выполнены тождества

$$\varphi(0, \ldots, 0,\ y_i,\ 0, \ldots, 0, \underbrace{1, \ldots, 1}_{t}) \equiv y_i;$$

$$\varphi(\underbrace{0, \ldots, 0}_{i},\ 1,\ 0, \ldots, 0, y_{t+1}, \ldots, y_{2t}) \equiv y_{t+i},$$

следует, что множество $\widehat{G} = G^{(1)} \cup \cdots \cup G^{(t)} \cup \check{G}$ является φ–УМ мощности $t \cdot 2^{s'} + 2^{s''}$ и что любые две ФАЛ из различных множеств $G^{(i)}$, $i = 1, \ldots, t$, ортогональны.

Определение. Разбиение $D = (Y_1, \ldots, Y_d)$ множества $Y = \{y_1, \ldots, y_p\}$ называется *селекторным разбиением БП функции* $\varphi(y_1, \ldots, y_p)$ тогда и только тогда, когда для всякого i, $i = 1, \ldots, d$, и для любой переменной $y \in Y_i$ найдутся константы $\alpha_1, \ldots, \alpha_d$ такие, что при подстановке $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_d$ вместо переменных из $Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_d$ соответственно, выполняется равенство $\varphi = y \oplus \alpha_i$.

Отметим, что если $\varphi(y_1,\dots,y_p)$ существенно зависит от всех своих БП, то тривиальное разбиение D, при котором $Y_i=\{y_i\}$, $i=1,\dots,p$, является селекторным. Заметим также, что если функция φ симметрична по переменным y_i,y_j, то они не могут входить в одну и ту же компоненту селекторного разбиения. Отсюда следует, что у функции $\varphi(y_1,\dots,y_p)=y_1\vee\dots\vee y_p$ нет нетривиальных селекторных разбиений БП. В то же время функция $\varphi(y_1,\dots,y_p)=y_1y_{t+1}\vee y_2y_{t+2}\vee\dots\vee y_ty_{2t}$ имеет селекторное разбиение с компонентами $Y_1=\{y_1\},\dots,Y_t=\{y_t\},Y_{t+1}=\{y_{t+1},\dots,y_{2t}\}$.

Лемма 3.1. *Пусть $D=(Y_1,\dots,Y_d)$ селекторное разбиение множества переменных $Y=\{y_1,\dots,y_p\}$ ФАЛ $\varphi(y_1,\dots,y_p)$, где $|Y_i|=p_i$, $i=1,\dots,p$, и пусть $s_1,\dots,s_d$ — чётные числа, удовлетворяющие условию $s_1p_1+\dots+s_dp_d\geqslant 2^m$. Тогда существует φ–УМ G порядка m такое, что*

$$|G|\leqslant 2^{s_1}+\dots+2^{s_d}, \tag{3.4}$$

$$L^A(\vec{G})\leqslant e_A|G|+O(d\cdot 2^{m+s/2}), \tag{3.5}$$

где $A\in\{\mathrm{K},\mathrm{C}\}$, $s=\max_{1\leqslant i\leqslant d}s_i$ и $e_{\mathrm{K}}=2$, $e_{\mathrm{C}}=4$.

Доказательство. Будем считать, что для каждого j, $j=1,\dots,d$, множество номеров БП из Y_j составляет отрезок $I_j=[a_j,a_{j+1})$, где $a_1=1$, $a_{d+1}=p+1$ и $|I_j|=a_{j+1}-a_j=p_j$ при любом j, $j\in[1,d]$. Данное предположение не ограничивает, очевидно, общность проводимых рассуждений. Рассмотрим сначала случай, когда

$$p_1s_1+\dots+p_ds_d=2^m.$$

Пусть $\Delta=(\delta_1,\dots,\delta_p)$ — разбиение куба B^m на последовательные отрезки длины $\underbrace{s_1,\dots,s_1}_{p_1},\dots,\underbrace{s_d,\dots,s_d}_{p_d}$ соответственно и пусть i–й отрезок Δ, $i=1,\dots,p$, связан с БП y_i ФАЛ φ. При этом для каждого j, $j=1,\dots,d$, отрезки длины s_j с номерами из I_j будут соответствовать БП из Y_j. Из селекторности разбиения D следует, что для каждого j, $j=1,\dots,d$, и каждого i, $i\in I_j$, существуют константы $\alpha_{i,1},\dots,\alpha_{i,j-1},\alpha_{i,j+1},\dots,\alpha_{i,d}$ при подстановке которых вместо БП из $Y_1,\dots,Y_{j-1},Y_{j+1},\dots,Y_d$ соответственно ФАЛ φ переходит в ФАЛ вида $y_i\oplus\beta_i$, где $\beta_i\in B$.

Определим (см. рис. 3.1) для каждого j, $j=1,\dots,d$, множество $G^{(j)}$ как множество всех тех ФАЛ из $P_2(m)$, которые:

1) принимают на любом отрезке δ_i, $i\in([1,p]\setminus I_j)$, значение $\alpha_{i,j}$;

2) принимают одинаковые значения на любых двух наборах с одинаковыми «внутренними» номерами из различных отрезков Δ, соответствующих БП из Y_j.

Заметим, что у любой ФАЛ из $G^{(i)}$, $i\in[1,d]$, те части столбца её значений которые соответствуют отрезкам разбиения Δ с номерами из I_i и рассматриваются

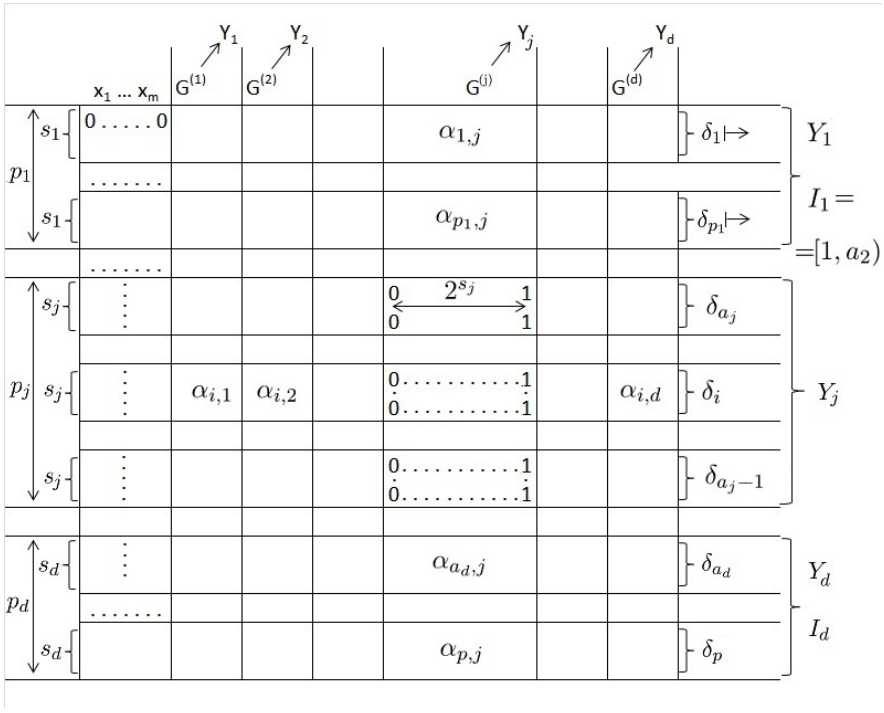

Рис. 3.1: Таблица ФАЛ из φ–УМ G

как наборы «высоты» s_i, совпадают между собой и что в качестве указанных наборов у различных ФАЛ из $G^{(i)}$ встречаются все 2^{s_i} различных наборов. Отсюда следует, что $\left|G^{(i)}\right| = 2^{s_i}$, так как на остальных отрезках разбиения Δ все ФАЛ из $G^{(i)}$ ведут себя одинаково.

Из построения следует, что множество (ср. с (3.3))

$$G = G^{(1)} \cup \cdots \cup G^{(d)}$$

является φ–УМ порядка m. Действительно, для любой ФАЛ g, $g \in P_2(m)$, справедливо представление

$$g = \varphi(g_1, \ldots, g_p),$$

где для каждого i, $i = 1, \ldots, d$, и каждого j, $j \in I_i$, в качестве ФАЛ g_j берётся та ФАЛ из $G^{(i)}$, которая совпадает с ФАЛ $g \oplus \beta_j$ на отрезке δ_j. Кроме того, множество G удовлетворяет (3.4), так как

$$|G| \leqslant \sum_{i=1}^{d} |G^{(i)}| \leqslant 2^{s_1} + \cdots + 2^{s_d}.$$

Убедимся в том, что множество G удовлетворяет (3.5), то есть является искомым φ–УМ порядка m. Для каждого i, $i = 1, \ldots, d$, и каждого σ, $\sigma \in B$, рассмотрим

множество ФАЛ $G_\sigma^{(i)}$, $G_\sigma^{(i)} \subseteq P_2(m-1)$, которые состоят из всех различных ФАЛ, получающихся из ФАЛ множества $G^{(i)}$ в результате подстановки константы σ вместо БП x_m. При этом из чётности чисел $s_1, \ldots, s_i$ вытекает, что $G_0^{(i)} = G_1^{(i)}$ и что $\left|G_0^{(i)}\right| = \left|G_1^{(i)}\right| \leqslant 2^{s_i/2}$. Следовательно, для каждого A, $A \in \{\mathrm{C}, \mathrm{K}\}$, и каждого i, $i \in [1, d]$, сложность схемы $\Sigma_i^{(A)}$ из $\mathcal{U}^A$, построенной для системы ФАЛ $\overrightarrow{G}^{(i)}$ по методу каскадов (см. [3]) с разложением реализуемых ФАЛ по БП $x_m, x_{m-1}, \ldots, x_1$ удовлетворяет неравенству

$$L(\Sigma_i^{(A)}) \leqslant e_A \cdot \left|G^{(i)}\right| + O(2^{m+s_i/2}).$$

Суммируя данные неравенства для всех i, $i = 1, \ldots, d$, получим (3.5).

Осталось рассмотреть случай, когда

$$h = p_1 s_1 + \cdots + p_d s_d > 2^m.$$

Положим $q = \lceil \log h \rceil$ и рассмотрим в кубе B^q от набора БП $\widehat{x} = (u_1, \ldots, u_t, x_1, \ldots, x_m)$, где $t = q - m > 0$, отрезок I, состоящий из первых h наборов этого куба. Построим множество ФАЛ G, $G \subseteq P_2(\widehat{x})$, так же, как строилось множество G в предыдущем случае, полагая, что все рассматриваемые ФАЛ от БП $\widehat{x}$ равны 0 вне отрезка I. При этом множество G будет обладать свойством φ–универсальности на отрезке I, то есть любая ФАЛ g, $g \in P_2(\widehat{x})$, будет совпадать на I с некоторыой ФАЛ вида $\varphi(g_1, \ldots, g_p)$, где $g_j \in G$ при всех j, $j \in [1, p]$. Следовательно, множество G, которое получается из множества $\widehat{G}$ при подстановке константы 0 вместо БП $u_1, \ldots, u_t$, является φ–УМ порядка m и удовлетворяет (3.4), (3.5).

Лемма доказана. □

Замечание 1. В условии леммы 3.1 допустимо равенство $s_i = 0$, которое означает, что построенное при доказательстве множество I_i пусто, а множество $G^{(i)}$ состоит из одной ФАЛ, принимающей на каждой из непустых полос δ_j, $1 \leqslant j \leqslant p$, постоянные значения.

Замечание 2. Построенное в начале §3 для ФАЛ $\varphi(y_1, \ldots, y_{2t}) = y_1 y_{t+1} \vee \cdots \vee y_t y_{2t}$ «компактное» φ-УМ $\widehat{G}$, является частным случаем φ–УМ $G = G^{(1)} \cup \cdots \cup G^{(t+1)}$, полученного по лемме 3.1 для этой же ФАЛ на основе указанного ранее селекторного разбиения $D = (\{y_1\}, \ldots, \{y_t\}, \{y_{t+1}, \ldots, y_{2t}\})$ её БП, где

$$s_1 = \cdots = s_t = s', \quad s_{t+1} = s'', \quad G^{(t+1)} = \check{G} \quad \text{и} \quad t(s' + s'') \geqslant 2^m.$$

Определение. *Энтропией разбиения* D, $D = (Y_1, \ldots, Y_d)$, множества Y называется величина

$$H(D) = -\sum_{i=1}^{d} \frac{|Y_i|}{|Y|} \log \frac{|Y_i|}{|Y|}.$$

Заметим, что энтропия вырожденного разбиения, при котором $d = 1$, равна нулю, а энтропия тривиального разбиения, при котором $d = p$, равна $\log p$. Можно показать, что $0 \leqslant H(D) \leqslant \log d$ для любого разбиения D множества Y на d компонент.

Отметим также, что энтропия разбиения D из замечания 2 к лемме 3.1 равна

$$\sum_{i=1}^{t} \frac{\log(2t)}{2t} + \frac{\log 2}{2} = \frac{\log t}{2} + 1.$$

Теорема 3.1. *Если $D = (Y_1, \ldots, Y_d)$ — селекторное разбиение БП ФАЛ $\varphi(y_1, \ldots, y_p)$, и $s > \log p$, а $p(s - H(D)) \geqslant 2^m$, то найдётся φ–УМ G порядка m такое, что*

1) $|G| \leqslant 2^{s+2}$;

2) $L^A(\overrightarrow{G}) \leqslant e_A \cdot |G| + O(d \cdot 2^{m+s/2})$, *где* $A \in \{\mathrm{K}, \mathrm{C}\}$.

Доказательство. Выберем для каждого i, $1 \leqslant i \leqslant d$, чётное число s_i такое, что

$$s + \log \frac{p_i}{p} \leqslant s_i \leqslant s + \log \frac{p_i}{p} + 2,$$

где $p_i = |Y_i|$, и убедимся в том, что выполнено неравенство $s_1 p_1 + \cdots + s_d p_d \geqslant 2^m$. Действительно,

$$s_i p_i \geqslant p_i(s + \log \frac{p_i}{p}) = p_i s + p \cdot \frac{p_i}{p} \log \frac{p_i}{p}$$

и, следовательно,

$$\sum_{i=1}^{d} s_i p_i \geqslant \sum_{i=1}^{d} p_i s + p \cdot \sum_{i=1}^{d} \frac{p_i}{p} \log \frac{p_i}{p} = p(s - H(D)) \geqslant 2^m.$$

Осталось воспользоваться леммой 3.1 и построить φ–УМ G, удовлетворяющее неравенствам (3.4) и (3.5), из которых следует, что

$$|G| \leqslant 2^{s_1} + \cdots + 2^{s_p} \leqslant 2^{s+2} \sum_{i=1}^{d} \frac{p_i}{p} = 2^{s+2}$$

и что сложность $L^A(\overrightarrow{G})$ удовлетворяет второму условию теоремы.

Теорема доказана. □

§4 Асимптотические оценки высокой степени точности для сложности итеративных контактных схем и контактных схем из ориентированных контактов

Используем приведённые в §3 φ–УМ и схемы, которые их реализуют, для синтеза ИКС и КС из ориентированных контактов.

Рис. 4.1: Реализация ФАЛ $\varphi(y_1, \ldots, y_p)$ с помощью ИКС и КС из ориентированных контактов

Теорема 4.1. *Для любой ФАЛ f, $f \in P_2(n)$, существует реализующая её ИКС Σ_f такая, что*

$$L(\Sigma_f) \leqslant \frac{2^{n-1}}{n}\left(1 + \frac{\frac{5}{2}\log n + O(1)}{n}\right). \tag{4.1}$$

Доказательство. Выберем натуральный параметр q, $q < n$, выделим из набора БП $x = (x_1, \ldots, x_n)$ поднаборы $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$ и рассмотрим разложение ФАЛ $f(x)$ по БП x'' (разложение Шеннона)

$$f(x) = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') \cdot f_{\sigma''}(x'), \tag{4.2}$$

где $f_{\sigma''}(x') = f(x', \sigma'')$ для любого набора σ'' из B^{n-q}.

Положим $p = 2t$ и рассмотрим введённую в §3 ФАЛ $\varphi(y_1, \ldots, y_p) = y_1 y_{t+1} \vee \ldots \vee$ $\vee\, y_t y_{2t}$ с селекторным разбиением $D = (\{y_1\}, \ldots, \{y_t\}, \{y_{t+1}, \ldots y_{2t}\})$ её БП, энтропия которого равна $1 + (\log t)/2$. Выберем, далее, параметры s и t такие, что

$$2t\left(s - \frac{\log t}{2} - 1\right) \geqslant 2^q, \tag{4.3}$$

и по теореме 3.1 построим на основе разбиения D φ–УМ $G = G^{(1)} \cup \cdots \cup G^{(t+1)}$ порядка q такое, что

$$|G| \leqslant 2^{s+2}, \qquad L^{\mathrm{K}}\big(\overrightarrow{G}\big) \leqslant 2|G| + O\big(t \cdot 2^{q+s/2}\big) \tag{4.4}$$

и что любые две ФАЛ из различных множеств $G^{(j)}$, $j = 1, \ldots, t$, ортогональны.

Пусть $(1, |G|)$–КС Σ_G реализует систему ФАЛ G со сложностью, удовлетворяющей (4.4). Для реализации ФАЛ φ будем использовать $(t, 1)$–КС $\widehat{\Sigma}_t$, $\widehat{\Sigma}_t = \widehat{\Sigma}_t(y_1, \ldots, y_t;\, y_{t+1}, \ldots, y_{2t};\, z)$ с «управляющими» итеративными входами $y_1, \ldots, y_t$, «проводящими» входами $y_{t+1}, \ldots, y_{2t}$ и выходом z, которая представляет собой «звезду» из t контактов, где контакт с номером j, $j = 1, \ldots, t$, соединяет вход y_{t+j} с выходом z и управляется входной БП y_j (см. рис. 4.1а).

В силу φ–универсальности множества ФАЛ G и особенностей его структуры для любой ФАЛ $g(x')$ справедливо представление

$$g\big(x'\big) = \varphi\big(g^{(1)}, \ldots, g^{(p)}\big) \tag{4.5}$$

где $g^{(j)} \in G^{(j)}$ для всех j, $j = 1, \ldots, t$, и $g^{(j)} \in G^{(t+1)}$, если $j \geqslant t+1$. Заметим, что для реализации данного представления достаточно входы $y_1, \ldots, y_p$ КС $\widehat{\Sigma}_t$ присоединить к выходам КС Σ_G в соответствии с (4.5) и что указанная реализация является корректной суперпозицией соответствующих схем в силу ортогональности ФАЛ из различных множеств $G^{(j)}$, $j = 1, \ldots, t$.

Пусть ИКС Σ' от БП x' содержит в качестве подсхемы КС Σ_G и реализует каждую ФАЛ $f_{\sigma''}(x')$, $\sigma'' \in B^{n-q}$, на одном из своих 2^{n-q} выходов согласно (4.5), используя для этого схему $\widehat{\Sigma}_t$, входы которой присоединены к выходам Σ_G соответствующим образом.

Искомая ИКС Σ_f, содержит ИКС Σ' в качестве подсхемы и представляет собой результат корректной суперпозиции вида $\Sigma_f = \Sigma''(\Sigma')$, где Σ'' — $(2^{n-q}, 1)$–контактное дерево от БП x'' входы (листья) которого присоединены к выходам Σ' в соответствии с (4.2).

Сложности ИКС Σ' и КС Σ'' удовлетворяют неравенствам

$$L\big(\Sigma'\big) \leqslant L(\Sigma_G) + 2^{n-q} \cdot t, \qquad L\big(\Sigma''\big) \leqslant 2^{n-q+1}$$

и, следовательно, в силу (4.4)

$$L\big(\Sigma_f\big) \leqslant 2^{n-q} \cdot t + O\big(2^{n-q}\big) + O\big(2^s + t \cdot 2^{q+s/2}\big).$$

Оценка (4.1) получается из последнего неравенства при следующих значениях параметров

$$q = \lceil 2 \log n \rceil, \quad s = \lceil n - 2 \log n \rceil, \quad t = \left\lceil \frac{2^{q-1}}{s - \frac{\log n}{2} - 1} \right\rceil,$$

при которых, начиная с достаточно большого n, выполнены все необходимые соотношения и, в частности, неравенство (4.3).

Теорема доказана. □

Следствие. *Из* (4.1) *с учётом нижней оценки* (1.19) *вытекает соотношение*

$$L^{\text{ИКС}}(n) = \frac{2^{n-1}}{n} \left(1 + \frac{\frac{5}{2} \log n \pm O(1)}{n} \right)$$

Напомним, далее, что (см., например, [ ]) множество δ, $\delta \subseteq B^q$ называется *m-регулярным* множеством наборов куба B^q, если $m < q$, $|\delta| = 2^m$ и все префиксы[1] длины m наборов из δ различны. Заметим, что m-регулярному множеству δ, $\delta \subseteq B^q$, можно взаимнооднозначно сопоставить систему ФАЛ $\psi = (\psi_1, \ldots, \psi_{q-m})$ из $P_2^{q-m}(m)$ так, что набор $\alpha = (\beta, \gamma)$, где $\beta \in B^m$ и $\gamma \in B^{q-m}$, принадлежит δ тогда

[1] Для слова (набора) α вида $\alpha = \beta\gamma$ слово β (γ) считается его *префиксом* (соответственно *суффиксом*).

и только тогда, когда $\psi(\beta) = \gamma$. Заметим также, что любая ФАЛ g, $g \in P_2(q)$, совпадает на m-регулярном множестве наборов δ, $\delta \subseteq B^q$, с некоторой ФАЛ из $P_2(m)$, если рассматривать $P_2(m)$ как множество всех ФАЛ из $P_2(q)$ с несущественными БП $x_{m+1}, \ldots, x_q$. При этом любая ФАЛ из связанной с δ системы функций совпадает на δ с соответствующей БП куба B^q.

Для наборов $\beta = (\beta_1, \ldots, \beta_q)$ и $\alpha = (\alpha_1, \ldots, \alpha_q)$ через $\beta \oplus \alpha$ будем обозначать набор вида $(\beta_1 \oplus \alpha_1, \ldots, \beta_q \oplus \alpha_q)$. Для множества δ, $\delta \subseteq B^q$, и набора α, $\alpha \in B^q$, определим множество $\delta \oplus \alpha$ как множество различных наборов вида $\beta \oplus \alpha$, где $\beta \in \delta$, то есть множество, получающееся из δ сдвигом (параллельным переносом) на набор α. Заметим, что для m-регулярного множества δ, $\delta \subseteq B^q$, и любого набора α, $\alpha \in B^q$, множество $\delta \oplus \alpha$ также является m-регулярным. Если при этом $\nu(\alpha) < 2^{q-m}$, то есть

$$\alpha = (\underbrace{0, \ldots, 0}_{m}, \gamma),$$

где $\gamma = (\gamma_1, \ldots, \gamma_{q-m})$ и $\nu(\gamma) = \nu(\alpha)$, а множество наборов δ соответствует системе ФАЛ $g = (g_1, \ldots, g_{q-m})$, то множество наборов $\delta \oplus \alpha$ будет соответствовать системе ФАЛ $g \oplus \gamma = (g_1 \oplus \gamma_1, \ldots, g_{q-m} \oplus \gamma_{q-m})$, получающейся из системы g инвертированием некоторых ФАЛ.

Напомним (см. []), что для любой системы ФАЛ $g = (g_1, \ldots, g_\lambda)$, $g \in P_2(m)$, и $q = m + \lambda$ система $\Delta = (\delta_1, \ldots, \delta_{2^\lambda})$ подмножеств единичного куба B^q, где при любом i, $i \in [1, 2^\lambda]$, и $\gamma = \nu^{-1}(i-1)$ множество δ_i соответствует системе ФАЛ $g \oplus \gamma$, является разбиением данного куба. При этом, очевидно, ФАЛ g, $j = 1, \ldots, \lambda$, на компоненте δ_i, $1 \leqslant i = \nu^{-1}(\alpha_1, \ldots, \alpha_\lambda) + 1 \leqslant 2^\lambda$, совпадает с буквой $x_{m+j}^{\overline{\alpha}_j}$.

Теорема 4.2. *Для любой ФАЛ f, $f \in P_2(n)$, существует реализующая её КС Σ_f из ориентированных контактов такая, что*

$$L(\Sigma_f) \leqslant \frac{2^n}{n}\left(1 + \frac{2\log n + O(1)}{n}\right). \tag{4.6}$$

Доказательство. Выберем натуральные параметры m, t, q и чётное число s так, что

$$s \leqslant 2^m, \qquad t = \left\lceil \frac{2^m}{s} \right\rceil, \qquad q = m + t \leqslant n \tag{4.7}$$

Для $p = 2t$ и указанной в доказательстве теоремы 4.1 ФАЛ $\varphi(y_1, \ldots, y_p)$ с селекторным разбиением $D = (\{y_1\}, \ldots, \{y_t\}, \{y_{t+1}, \ldots, y_{2t}\})$ её БП построим по лемме 3.1, где $s_1 = \cdots = s_t = 0$ и $s_{t+1} = s$, φ–УМ $G = G^{(1)} \cup \cdots \cup G^{(t)} \cup G^{(t+1)}$ порядка m.

Из замечания 1 к лемме 3.1 следует, что множество $G^{(j)}$, $j = 1, \ldots, t$, состоит из единственной ФАЛ ψ_j, а для множества ФАЛ $H = G^{(t+1)}$ в силу (3.4), (3.5) существует $(1, \lambda)$–КС Σ_H, где $\lambda = |H| \leqslant 2^s$, которая реализует систему ФАЛ $\overrightarrow{H}$ и для которой

$$L(\Sigma_H) \leqslant 2^{s+1} + O(t \cdot 2^{m+s/2}). \tag{4.8}$$

При этом в силу φ–универсальности множества ФАЛ G для любой ФАЛ g из $P_2(m)$ справедливо представление

$$g = \varphi\big(\psi_1, \ldots, \psi_t, , \ h^{(t+1)}, \ldots, h^{(2t)}\big), \tag{4.9}$$

где ФАЛ $h^{(t+1)}, \ldots, h^{(2t)}$ берутся из H.

Пусть, по-прежнему, $x' = (x_1, \ldots, x_q)$, а $\Delta = (\delta_1, \ldots, \delta_{2^t})$ — разбиение куба B^q от БП x', связанное с «моделированием» системы ФАЛ $\psi = (\psi_1, \ldots, \psi_t)$, для которого при любом i, $1 \leqslant i = \nu^{-1}(\alpha_1, \ldots, \alpha_t) + 1 \leqslant 2^t$, и любом j, $1 \leqslant j \leqslant t$, ФАЛ ψ_j совпадает на δ_i с буквой $x_{m+j}^{\overline{\alpha}_j}$. Следовательно, любоая ФАЛ $g(x')$ в силу (4.9) и в силу m–регулярности при любом i, $1 \leqslant i \leqslant \nu{-}1(\alpha_1, \ldots, \alpha_t) + 1 \leqslant 2^t$, компоненты δ_i совпадает на ней с ФАЛ

$$g_i\big(x'\big) = \varphi\big(x_{m+1}^{\alpha_1}, \ldots, x_{m+t}^{\alpha_t}, \, h_i^{(t+1)}, \ldots, h_i^{(2t)}\big), \tag{4.10}$$

где все ФАЛ $h_i^{(t+1)}, \ldots, h_i^{(2t)}$ принадлежат множеству H.

Полагая, как и раньше, $x'' = (x_{q+1}, \ldots, x_n)$, продолжим разложение (4.3) ФАЛ $f(x', x'')$ следующим образом

$$f(x', x'') = \bigvee_{i=1}^{2^t} \chi_i(x')\big(\bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') \cdot f_{\sigma'',i}(x')\big), \tag{4.11}$$

где $\chi_i(x')$ — характеристическая ФАЛ компоненты δ_i, $i = 1, \ldots, 2^t$, а ФАЛ $f_{\sigma'',i}(x')$, $\sigma'' \in B^{n-q}$, имеет вид правой части равенства (4.10) для ФАЛ $f_{\sigma''}(x')$.

Пусть $(1, 2^{t+n-q})$–КС Σ' от БП x' содержит в качестве подсхемы КС Σ_H и реализует каждую ФАЛ $f_{\sigma'',i}$ на одном из своих выходов согласно (4.10), используя для этого ориентированную КС $\check{\Sigma}_t$ (см. рис. 4.1б), контакты которой управляются буквами $x_{m+1}^{\overline{\alpha}_1}, \ldots, x_{m+t}^{\overline{\alpha}_t}$, а проводящие входы $y_{t+1}, \ldots, y_{2t}$ присоединены к соответствующим входам КС Σ_H. Заметим, что правильность и корректность всех указанных суперпозиций КС обеспечивается разделительностью КС $\check{\Sigma}_t$ по входам.

Пусть, далее, $(2^t, 1)$–КС $\widetilde{\Sigma}$ получается из $(2^q, 1)$–КД от БП x' отождествлением для каждого i, $i = 1, \ldots, 2^t$, тех его листьев, которые соответствуют конъюнкциям вида $x_1^{\sigma_1} \cdot \cdots \cdot x_q^{\sigma_q}$, где $(\sigma_1, \ldots, \sigma_q) \in \delta_i$. Построим, наконец, $(2^{t+n-q}, 1)$–КС Σ'', которая получается в результате присоединения к каждому входу КС $\widetilde{\Sigma}$ выхода (корня) $(2^{n-q}, 1)$–контактного дерева от БП x''. Заметим, что все операции суперпозиции, использованные при построении КС Σ'', являются корректными и поэтому Σ'' разделительна по входам, а система ФАЛ проводимости между её входами и выходом состоит из всех ФАЛ вида $\chi_i(x') \cdot K_{\sigma''}(x'')$, где $i \in [1, 2^t]$ и $\sigma'' \in B^{n-q}$.

Искомая КС Σ_f содержит КС Σ' в качестве подсхемы и представляет собой результат суперпозиции вида $\Sigma_f = \Sigma''(\Sigma')$, при выполнении которой входы Σ'' присоединяются к выходам Σ' в соответствии с (4.11). В силу разделительности

КС Σ'' по входам указанная суперпозиция является корректной и поэтому КС Σ_f действительно реализует ФАЛ f.

Из (4.8) с учётом того, что число контактов в контактном дереве от r БП равно $2^{r+1}-2$, вытекает неравенство

$$L\big(\Sigma_f\big) \leqslant 2^{n-q+1} + 2^{t+n-q+1} + t\cdot 2^{t+n-q} + 2^{s+1} + O\big(t\cdot 2^{m+s/2}\big).$$

Оценка (4.6) получается из последнего неравенства при следующих значениях параметров

$$m = \lfloor 2\log n\rfloor - 1, \qquad s = 2\left\lceil \frac{n-2\log n}{2}\right\rceil,$$

при которых, начиная с достаточно большого n, выполнены все необходимые соотношения и, в частности, неравенства (4.7).

Теорема доказана. □

Следствие. *Из* (4.6) *с учётом нижней оценки* (1.18) *вытекает соотношение*

$$L^{\overrightarrow{\text{КС}}}\big(n\big) = \frac{2^n}{n}\left(1 + \frac{2\log n \pm O(1)}{n}\right).$$

§5 Асимптотически наилучший метод синтеза СФЭ в произвольном базисе. Асимптотические оценки высокой степени точности для сложности усилительных СФЭ в некоторых базисах

Используем построенные в §3 φ–УМ для синтеза усилительных СФЭ в базисе Б, Б $=\{\mathcal{E}_i\}_{i=1}^b$. В силу полноты базиса Б в $\mathfrak{U}_{\text{Б}}^{\text{Ф}}$ существуют формулы $\mathcal{F}_{\&}$, $\mathcal{F}_{\vee}$ и $\mathcal{F}_{\neg}$, реализующие ФАЛ $x_1\cdot x_2$, $x_1\vee x_2$ и $\overline{x}_1$ соответственно, которыми мы будем заменять ФЭ базиса Б$_0$ при синтезе схем на основе конъюнктивных и дизъюнктивных представлений.

Теорема 5.1 (ср. [3]). *Для любой ФАЛ f, $f\in\mathfrak{U}_{\text{Б}}^{\text{УС}}$, существует реализующая её СФЭ Σ_f, $\Sigma_f\in\mathfrak{U}_{\text{Б}}^{\text{УС}}$, такая, что*

$$\mathcal{L}(\Sigma_f) \leqslant \rho_{\text{Б}}\frac{2^n}{n}\left(1 + \frac{3\log n + O(1)}{n}\right). \tag{5.1}$$

Доказательство. Найдём среди ФЭ базиса Б, Б $=\{\mathcal{E}_i\}_{i=1}^b$, элемент $\mathcal{E}_j$, на котором достигается приведённый вес $\rho_j=\rho_{\text{Б}}$ (см. §2), то есть

$$\rho_j = \frac{\mathcal{L}_j}{k_j-1} = \min_{k_i\geqslant 2}\rho_i = \rho_{\text{Б}}. \tag{5.2}$$

Пусть, далее, m,s,t,p — натуральные числа такие, что s — чётное,

$$p = t(k_j-1)+1, \tag{5.3}$$

$$k_j \leqslant \frac{2^m}{s} \leqslant p < \frac{2^m}{s} + (k_j-1), \tag{5.4}$$

а $\Pi = (\pi_1, \ldots, \pi_p)$ — такое разбиение куба B^m на последовательные отрезки, что

$$|\pi_i| = s_i \leqslant s. \tag{5.5}$$

Построим из t ФЭ $\mathcal{E}_j$ бесповторную формулу $\mathcal{F}_t$ с p входами, которая имеет вид квазиполного l–ярусного, $l = \lceil \log_k p \rceil$, дерева и реализует ФАЛ $\varphi(y_1, \ldots, y_p)$. Пусть G, $G \subseteq P_2(m)$, — стандартное φ–УМ порядка m, связанное с разбиением Π (см. §3), для которого в силу (5.3)–(5.5)

$$|G| = \lambda \leqslant p \cdot 2^s. \tag{5.6}$$

Искомая СФЭ Σ_f строится, как обычно, на основе разложения ФАЛ $f(x_1, \ldots, x_n)$ по переменным $x'' = (x_{q+1}, \ldots, x_n)$

$$f(x', x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') \cdot f_{\sigma''}(x'), \tag{5.7}$$

где $q = m$, $x' = (x_1, \ldots, x_q)$, а $f_{\sigma''}(x') = f(x', \sigma'')$. При этом для реализации каждой ФАЛ $f_{\sigma''}(x')$, $\sigma'' \in B^{n-q}$, используется её представление

$$f_{\sigma''}(x') = \varphi(g_{\sigma'',1}, \ldots, g_{\sigma'',p}), \tag{5.8}$$

где ФАЛ $g_{\sigma'',1}, \ldots, g_{\sigma'',p}$ берутся из множества G.

Из леммы 3.1 следует, что для системы ФАЛ $\overrightarrow{G}$ можно построить реализующую её СФЭ Σ_G, $\Sigma_G \in \mathfrak{U}_{\text{Б}}^{\text{УС}}$, сложности не более чем $c \cdot p \cdot 2^{m+s/2}$, выходами которой являются выходы усилительных ФЭ базиса Б.

Пусть, далее, СФЭ Σ' содержит СФЭ Σ_G в качестве подсхемы и для каждого σ'', $\sigma'' \in B^{n-q}$, реализует ФАЛ $f_{\sigma''}(x')$ в соответствии с (5.8), используя для этого формулу $\mathcal{F}_p$. Схема Σ_f представляет собой суперпозицию вида $\Sigma_f = \Sigma'(\Sigma'')$, где усилительная СФЭ Σ'' — мультиплексор порядка $n-q$ от БП x'', и реализует ФАЛ f в соответствии с (5.7). Сложность построенной СФЭ Σ_f, $\Sigma_f \in \mathfrak{U}_{\text{Б}}^{\text{УС}}$, с учётом (5.2)–(5.6) будет удовлетворять неравенству

$$\mathcal{L}(\Sigma_f) \leqslant \mathcal{L}_j \cdot t \cdot 2^{n-m} + O(2^{n-m} + p \cdot 2^s + p \cdot 2^{s/2+m}), \tag{5.9}$$

из которого при

$$m = q = \lceil 2 \log n \rceil, \quad s = 2 \left\lceil \frac{n - 3 \log n}{2} \right\rceil \tag{5.10}$$

и при значениях остальных параметров, определённых из (5.3)–(5.4), следует (5.1).

Теорема доказана. □

Следствие 1.

$$\mathcal{L}_{\text{Б}}^{\text{С}}(n) \sim \mathcal{L}_{\text{Б}}^{\text{УС}}(n) \sim \rho_{\text{Б}} \frac{2^n}{n}.$$

Следствие 2.

$$\mathcal{L}^{\text{УС}}_{\text{Б}'_0}(n) = \frac{2^n}{n}\left(1 + \frac{3\log n + O(1)}{n}\right).$$

Будем говорить, что разбиение Δ является *подразбиением разбиения* D, $D = (Y_1, \ldots, Y_d)$, множества Y, если оно получается из D в результате замены каждой его компоненты Y_i, $i = 1, \ldots, d$, её разбинием $\delta_i = (Y_{i,1}, \ldots, Y_{i,d_i})$. При этом

$$\begin{aligned} H(\Delta) &= -\sum_{i=1}^{d}\sum_{j=1}^{d_i} \frac{|Y_{i,j}|}{|Y|} \cdot \log \frac{|Y_{i,j}|}{|Y|} = \\ &= -\sum_{i=1}^{d}\sum_{j=1}^{d_i} \frac{|Y_i|}{|Y|} \cdot \frac{|Y_{i,j}|}{|Y_i|}\left(\log \frac{|Y_i|}{|Y|} + \log \frac{|Y_{i,j}|}{|Y_i|}\right) = \\ &= \sum_{i=1}^{d} \frac{|Y_i|}{|Y|}\left(\log \frac{|Y_i|}{|Y|} + \sum_{j=1}^{d_i} \frac{|Y_{i,j}|}{|Y_i|} \log \frac{|Y_{i,j}|}{|Y_i|}\right) \end{aligned}$$

и, следовательно, справедливо равенство

$$H(\Delta) = H(D) + \sum_{i=1}^{d} \frac{|Y_i|}{|Y|} H(\delta_i), \tag{5.11}$$

из которого вытекает неравенство

$$H(\Delta) \leqslant \log d + \max_{1 \leqslant i \leqslant d} H(\delta_i). \tag{5.12}$$

Для разбиения $D = (Y_1, \ldots, Y_d)$ множества Y его *спектром* будем называть множество (сочетание), состоящее из чисел $|Y_1|, \ldots, |Y_d|$. Заметим, что два разбиения, спектры которых получаются друг из друга умножением на одно и то же число, имеет одинаковую энтропию.

Разбиение, спектр которого имеет вид $1, 1, 2, 4, \ldots, 2^{t-1}$, где $t \geqslant 1$, будем называть *двоично-геометрическим разбиением высоты* t.

При $t \geqslant 2$ указанное разбиение является, очевидно, подразбиением разбиения со спектром $2^{t-1}, 2^{t-1}$ и получается из него заменой одной из компонент двоично-геометрическим разбиением высоты $(t-1)$. В силу (5.11) отсюда следует, что энтропия данного разбиения задаётся формулой

$$1 + \frac{1}{2}\left(1 + \frac{1}{2}\left(\ldots\left(1 + \frac{1}{2}\right)\right)\ldots\right),$$

где число вложенных пар скобок равно $(t-2)$, и, таким образом, энтропия двоично-геометрического разбиения высоты t, $t \geqslant 1$, равна

$$1 + \frac{1}{2} + \cdots + \frac{1}{2^{t-1}} = 2 - \frac{1}{2^{t-1}}.$$

Рис. 5.1: Структура КС $\widetilde{\Sigma}_t$ и её связь с формулой $\widetilde{F}_t$

Теорема 5.2. *Для любой ФАЛ f, $f \in P_2(n)$, существует реализующая её СФЭ Σ_f, $\Sigma_f \in \mathfrak{U}^{\text{УС}}$, такая, что*

$$L(\Sigma_f) \leqslant \frac{2^n}{n}\left(1 + \frac{2\log n + O(1)}{n}\right). \tag{5.13}$$

Доказательство. Пусть $\widetilde{\text{Б}} = \{\mathcal{E}_1, \mathcal{E}_2\}$ — базис, где $\varphi_1(x_1) = \overline{x}_1$, $\varphi_2(x_1, x_2, x_3, x_4) = x_1x_3 \vee x_2x_4$ и $\mathcal{L}_1 = 1$, $\mathcal{L}_2 = 3$. Заметим, что для любой СФЭ $\widetilde{\Sigma}$, $\widetilde{\Sigma} \in \mathfrak{U}^{\text{УС}}_{\widetilde{\text{Б}}}$, существует эквивалентная ей СФЭ Σ, $\Sigma \in \mathfrak{U}^{\text{УС}}$, такая, что $L(\Sigma) = L(\widetilde{\Sigma})$. Следовательно, для доказательства теоремы достаточно построить СФЭ $\widetilde{\Sigma}_f$, $\widetilde{\Sigma}_f \in \mathfrak{U}^{\text{УС}}_{\widetilde{\text{Б}}}$, которая реализует заданную ФАЛ f и сложность которой не превосходит правой части (5.13).

Пусть параметры t и p выбраны для базиса $\widetilde{\text{Б}}$ в соответствии с (5.2), где $k_j = 4$, то есть $p = 3t + 1$. Построим из t ФЭ $\mathcal{E}_2$, соединённых между собой по двум последним входам, бесповторную формулу $\widetilde{\mathcal{F}}_t$ с p входами, которая представляет собой l–ярустное, $l = \lceil \log(t+1) \rceil$, квазиполное двоичное дерево и реализует ФАЛ $\widetilde{\varphi}(y_1, \ldots, y_p)$. Будем считать, что все $\hat{t}$, $\hat{t} = t - 2^{l-1} + 1$, ФЭ l-го яруса формулы $\widetilde{\mathcal{F}}_t$ присоединены к первым $\hat{t}$ листьям полного $(l-1)$–ярусного поддерева $\widehat{D}$ при их естественной нумерации.

Заметим, что формула $\widetilde{\mathcal{F}}_t$ как структурно, так и функционально моделируется ориентированной КС $\widetilde{\Sigma}_t$, имеющей вид квазиполного двоичного l-ярусного дерева с $(p - 2t)$ листьями, которые являются «проводящими» входами $\widetilde{\Sigma}_t$, с $2t$ контактами, которые помечены $2t$ «управляющими» входами этой КС, и корнем z, который является выходом КС (см. рис. 5.1а). При указанном моделировании каждая вершина v КС $\widetilde{\Sigma}_t$ взаимно однозначно сопоставляется эквивалентной ей вершине $\check{v}$ дерева формулы $\widetilde{\mathcal{F}}_t$ так, как это показано на рис. 5.1б.

Пусть для каждого i, $i = 1, \ldots, l$, Y'_i и Y''_i — множество тех БП из $Y = \{y_1, \ldots, y_p\}$, которые связаны с двумя первыми и двумя последними входами ФЭ $\mathcal{E}_2$ относящихся к i-му ярусу, соответственно. Заметим, что

$$|Y'_l| = |Y''_l| = 2(t - 2^{l-1} + 1), \qquad |Y''_{l-1}| = t + 1 - |Y'_l| \quad \text{и} \quad Y''_i = \varnothing, \qquad |Y'_v| = 2^v$$

при всех i, $i < (l-1)$, $v \leqslant l - 1$.

Пусть, далее, $Y'_{i,0}$ и $Y'_{i,1}$ — равномощные подмножества, состоящие из тех БП множества Y'_i, $i \in [1, l]$, которые связаны с первыми и вторыми входами ФЭ $\mathcal{E}_2$ соответственно, а $Y'' = Y''_{l-1} \cup Y''_l$.

Из построения следует, что разбиение D множества Y, где

$$D = (Y'_{1,0}, Y'_{1,1}, \ldots, Y'_{l,0}, Y'_{l,1}, Y'')$$

является селекторным разбиением БП Y ФАЛ $\widetilde{\varphi}$. Действительно, для получения на выходе $\widetilde{\Sigma}_t$ БП y'' из Y'' достаточно для каждого i, $i = 1, \ldots, l$, выбрать такие значения σ_i и $\overline{\sigma}_i$ для БП из $Y'_{i,0}$ и $Y'_{i,1}$ соответственно, при которых в $\widetilde{\Sigma}_t$ образуется только одна проводящая цепь, соединяющая листья дерева с его корнем, и эта цепь начинается в листовой вершине с пометкой y''. Заметим, что при любом i, $i \in [1, l]$, и выбранных значениях всех групп БП, за исключением группы Y'_{i,σ_i}, для получения на выходе КС $\widetilde{\Sigma}_t$ той БП y_j из Y'_i, контакт которой лежит на построенной цепи, достаточно присвоить всем БП из Y'' значение 1.

Рассмотрим подразбиение $\widehat{D}$ разбиения D, которое получается из него заменой компоненты Y'' её произвольным разбиением вида $(Y'_{0,0}, Y'_{0,1}, \widehat{Y}'')$, где $\left|Y'_{0,0}\right| = \left|Y'_{0,1}\right| = 1$. Положим, далее,

$$\widehat{Y}'_0 = \bigcup_{i=0}^{l-1} Y'_{i,0}, \qquad \widehat{Y}'_1 = \bigcup_{i=0}^{l-1} Y'_{i,1}$$

и пусть $\check{D}$ — разбиение множества Y на компоненты $(\widehat{Y}'_0, \widehat{Y}'_1, Y'_{l,0}, Y'_{l,1}, \widehat{Y}'')$.

Поскольку, как это следует из сказанного выше,

$$\left|Y'_{i,0}\right| = \left|Y'_{i,1}\right| = 2^{i-1}$$

для всех i, $i = 1, \ldots, l-1$, то $\widehat{D}$ является подразбиением разбиения $\check{D}$ и получается заменой двух первых компонент последнего двоично-геометрическими разбиениями высоты $(l-1)$. Следовательно, в силу (5.11), (5.12) и с учетом того, что энтропия двоично-геометрических разбиений не более 2, получим

$$H(D) \leqslant H(\widehat{D}) \leqslant \log 5 + 2 \leqslant 5.$$

Искомая СФЭ $\widetilde{\Sigma}_f$ строится аналогично тому, как строилась СФЭ Σ_f, при доказательстве теоремы 5.1, с той лишь разницей, что вместо формулы $\mathcal{F}_t$ используется формула $\widetilde{\mathcal{F}}_t$, а $\widetilde{\varphi}$–УМ G порядка m и схема Σ_G находятся с использованием разбиения D по теореме 3.1 при значениях параметров p и s, удовлетворяющих её условиям. При этом для сложности СФЭ $\widetilde{\Sigma}_f$ справедливо неравенство

$$\mathcal{L}(\widetilde{\Sigma}_f) \leqslant 3t2^{n-m} + O(2^s + 2^{m+s/2} \cdot \log t)$$

из которого при следующих значениях параметров:

$$m = \lceil 2\log n \rceil, \quad s = \lceil n - 2\log n \rceil, \quad t = \left\lceil \frac{2^m}{3(s-5)} \right\rceil, \quad p = 3t + 1,$$

обеспечивающих выполнение условий теоремы 3.1, вытекает (5.13)

Теорема доказана. □

Следствие.

$$L^{\text{УС}}(n) = \frac{2^n}{n}\left(1 + \frac{2\log n \pm O(1)}{n}\right).$$

§6 Асимптотически наилучший метод синтеза формул в произвольном базисе. Асимптотические оценки высокой степени точности для сложности формул в некоторых базисах

При синтезе СФЭ с базисе Б $= \{\varphi_i\}_{i=1}^b$ мы использовали (см. §5) некоторые формулы $\mathcal{F}_\&$, $\mathcal{F}_\vee$ и $\mathcal{F}_\neg$ из $\mathcal{U}_{\text{Б}}^{\Phi}$, реализующие ФАЛ $x_1 \cdot x_2$, $x_1 \vee x_2$ и $\overline{x}_1$ соответственно, для моделирования конъюнктивных и дизъюнктивных представлений ФАЛ. При этом возможность такого моделирования и его сложность не налагали на данные формулы каких-либо структурных или параметрических ограничений. В то же время при использовании формул $\mathcal{F}_\&$, $\mathcal{F}_\vee$, $\mathcal{F}_\neg$ для аналогичного моделирования конъюнктивных и дизъюнктивных представлений ФАЛ в классе $\mathcal{U}_{\text{Б}}^{\Phi}$ необходимо обеспечить отсутствие «внутренних» ветвлений в получающихся схемах за счёт определенных ограничений на их структуру.

Напомним, что БП, встречающаяся в записи формулы только один раз, считается *бесповторной* БП этой формулы и что формула, все БП (соответственно, все существенные БП) которой бесповторны, называется *бесповторной* (соответсвенно, *квазибеспоторной*).

Лемма 6.1. *Существуют квазибесповторные формулы $\mathcal{F}_\neg$, $\mathcal{F}_\&$ и $\mathcal{F}_\vee$ над базисом* Б*, которые реализуют ФАЛ $\overline{x}_1$, $x_1 \cdot x_2$ и $x_1 \vee x_2$ соответственно.*

Доказательство. В силу полноты системы ФАЛ $\{\varphi_i\}_{i=1}^b$ можно построить формулы $\mathcal{F}_0$, $\mathcal{F}_1$ от БП y над Б, которые реализуют константы 0, 1 и являются квазибесповторными в связи с отсутствием существенных БП. Из полноты следует также, что среди базисных ФАЛ есть немонотонная ФАЛ $\varphi'(x_1, \ldots, x_{k'})$ и нелинейная ФАЛ $\varphi''(x_1, \ldots, x_{k''})$. В силу леммы о немонотонной ФАЛ найдётся набор $(\alpha_1, \alpha_2, \ldots, \alpha_{k'})$ из $B^{k'}$ и число i, $1 \leqslant i \leqslant k'$, такие, что

$$\varphi'\big(\alpha_1, \ldots, \alpha_{i-1}, x_i, \alpha_{i+1}, \ldots, \alpha_{k'}\big) = \overline{x}_i.$$

Следовательно, формула

$$\mathcal{F}_\neg\big(x\big) = \mathcal{F}_\neg\big(x, y\big) = \varphi'\big(\mathcal{F}_{\alpha_1}, \ldots, \mathcal{F}_{\alpha_{i-1}}, x, \mathcal{F}_{\alpha_{i+1}}, \ldots, \mathcal{F}_{\alpha_{k'}}\big)$$

является бесповторной формулой над Б, реализующей ФАЛ $\overline{x}$. Положим:

$$\mathcal{F}_\neg^{(1)}(x, y) = \mathcal{F}_\neg(x) \quad \text{и} \quad \mathcal{F}_\neg^{(0)}(x, y) = x.$$

Из доказательства леммы о нелинейной ФАЛ следует, что найдётся такой набор $\beta = (\beta_1, \ldots, \beta_{k''})$ из $B^{k''}$, натуральные числа i и j, $1 \leqslant i < j \leqslant k''$, а также константа γ, $\gamma \in B$, для которых

$$\varphi''\big(\beta_1, \ldots, \beta_{i-1}, x_i \oplus \beta_i, \beta_{i+1}, \ldots, \beta_{j-1}, x_j \oplus \beta_j, \beta_{j+1}, \ldots, \beta_{k''}\big) = x_i \cdot x_j \oplus \gamma.$$

Тогда формула $\mathcal{F}_{\&}$ вида

$$\mathcal{F}_{\&}\big(x_1, x_2, y\big) = \mathcal{F}_{\neg}^{(\gamma)}\big(\varphi''\big(\mathcal{F}_{\beta_1}, \ldots, \mathcal{F}_{\beta_{i-1}}, \mathcal{F}_{\neg}^{(\beta_i)}(x_1, y), \\ \mathcal{F}_{\beta_{i+1}}, \ldots, \mathcal{F}_{\beta_{j-1}}, \mathcal{F}_{\neg}^{(\beta_j)}(x_2, y), \mathcal{F}_{\beta_{j+1}}, \ldots, \mathcal{F}_{\beta_{k''}}\big), y\big)$$

является квазибесповторной формулой над Б и реализует ФАЛ $x_1 \cdot x_2$. Квазибесповторная формула $\mathcal{F}_{\vee}(x_1, x_2, y)$, которая реализует ФАЛ $x_1 \vee x_2$, получается из формулы

$$\mathcal{F}_{\neg}\big(\mathcal{F}_{\&}\big(\mathcal{F}_{\neg}\big(x_1, y\big), \mathcal{F}_{\neg}\big(x_2, y\big), y\big), y\big)$$

«удалением» всех вхождений двух последовательных формул $\mathcal{F}_{\neg}$.

Лемма доказана. □

Распространим операцию сложения двоичных наборов (слов) по модулю 2 (см. §4) на тот случай, когда длина второго слагаемого может быть больше длины первого. Для наборов $\alpha = (\alpha_1, \ldots, \alpha_m) \in B^m$ и $\beta = (\beta_1, \ldots, \beta_n) \in B^n$, где $n \geqslant m$, определим их сумму $\alpha \oplus \beta$ как набор $\gamma = (\gamma_1, \ldots, \gamma_n) \in B^n$, который в случае $n = m$ представляет собой введённую ранее поразрядную сумму по модулю 2 этих наборов.

В случае $n > m$ разобьём слово β на последовательно (слева направо) расположенные и составленные из подряд идущих символов непустые слова $\beta^{(1)}, \ldots, \beta^{(k)}$, где $k \geqslant 2$ и $\beta^{(j)} \in B^{\lambda_j}$ для всех j, $j = 1, \ldots, k$, такие, что:

1) $\lambda_1 = m$ и при любом j, $j \in [2, k-1]$, число λ_j равно числу 1 в слове $\beta^{(j-1)}$;

2) число 1 в слове $\beta^{(k-1)}$ либо равно 0, либо больше, чем $\lambda_k = (n-m) - \lambda_1 - \lambda_2 - \cdots - \lambda_{k-1}$.

Заметим, что указанное разбиение набора β однозначно определяется числом m, $m < n$.

Сопоставим построенной последовательности слов $\beta^{(1)}, \ldots, \beta^{(k)}$ последовательность слов $\alpha^{(1)}, \ldots, \alpha^{(k)}$, где $\alpha^{(j)} \in B^{\lambda_j}$ при всех j, $j \in [1, k]$, такую, что:

1) $\alpha^{(1)} = \alpha$ и при любом j, $j \in [2, k-1]$, слово $\alpha^{(j)}$ состоит из тех и только тех, расположенных в порядке возрастания их номеров, λ_j разрядов $\alpha_t^{(j-1)}$, $1 \leqslant t \leqslant \lambda_{j-1}$, вектора $\alpha^{(j-1)} = \big(\alpha_1^{(j-1)}, \ldots, \alpha_{\lambda_{j-1}}^{(j-1)}\big)$, для которых соответствующие им разряды $\beta_t^{(j-1)}$ вектора $\big(\beta_1^{(j-1)}, \ldots, \beta_{\lambda_{j-1}}^{(j-1)}\big) = \beta^{(j-1)}$ равны 1;

2) вектор $\alpha^{(k)}$ состоит из λ_k нулей.

Определим искомый вектор $\gamma = \alpha \oplus \beta$ как конкатенацию (последовательность) векторов $\alpha^{(1)} \oplus \beta^{(1)}, \ldots, \alpha^{(k)} \oplus \beta^{(k)}$ и заметим, что при этом уравнение $\alpha \oplus \beta = \gamma$ имеет единственное относительно β решение при любых α, $\alpha \in B^m$, и γ, $\gamma \in B^n$.

На основе введённой операции при любых β, $\beta \in B^t$, и $\lambda \leqslant t$ обычным образом определяется сумма $\delta \oplus \beta$, где $\delta \subseteq B^\lambda$, а также сумма $g \oplus \beta$, где $g = (g_1, \ldots, g_\lambda) \in P_2^\lambda(m)$. При этом последняя сумма является набором длины t, который по-прежнему состоит из ФАЛ системы g или их отрицаний и задаёт m–регулярное множество наборов куба B^t. Заметим также, что любая ФАЛ системы g хотя бы один раз входит в систему $g \oplus \beta$ без отрицания, если число 1 в наборе β больше или равно λ.

Пусть $G \subseteq P_2(m)$ и $|G| = \lambda$, а $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$, где $q > m$, — разбиение куба B^q на m–регулярные компоненты. Будем говорить, что разбиение Δ *моделирует ФАЛ из G с помощью БП или их отрицаний*, если для любого i, $i \in [1, 2^{q-m}]$, любая ФАЛ g, $g \in G$, совпадает на δ_i с некоторой буквой x_j^σ, где $1 \leqslant j \leqslant q$ и $\sigma \in B$. Компонента δ_i считается при этом *хорошей компонентой* разбиения Δ (относительно множества G) в том случае, когда для любой ФАЛ g, $g \in G$ указанное совпадение имеет место при $\sigma = 1$.

Лемма 6.2. *Пусть $G \subseteq P_2(m)$, $|G| = \lambda$, $q \geqslant m + \lambda$ и пусть δ_i, $i = 1, \ldots, 2^{q-m}$, — m–регулярное разбиение куба B^q, которое соответствует системе ФАЛ $\overrightarrow{G} \oplus \beta$, где $\beta \in B^{q-m}$ и $\nu(\beta) = i-1$. Тогда система множеств $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ образует m–регулярное разбиение куба B^q, которое моделирует ФАЛ из G с помощью БП или их отрицаний и имеет при этом $C_{q-m}^0 + \cdots + C_{q-m}^{\lambda-1}$ «плохих» компонент.*

Доказательство. Покажем сначала, что система множеств Δ является разбиением куба B^q. Для этого в силу того, что мощность каждого из них равна 2^m, достаточно убедиться в том, что Δ — покрытие куба B^q, то есть любой набор γ, $\gamma \in B^q$, входит хотя бы в одно из множеств δ_i, $i \in [1, 2^{q-m}]$.

Действительно, представим набор γ в виде $\gamma = (\alpha, \hat{\gamma})$, где $\alpha \in B^m$, и найдём набор β, $\beta \in B^{q-m}$, который является единственным решением уравнения $\overrightarrow{G}(\alpha) \oplus \beta = \hat{\gamma}$. Следовательно, $\gamma \in \delta_i$, где $\nu(\beta) = i - 1$, и система множеств Δ является разбиением куба B^q.

Заметим, что в силу отмеченных выше свойств операции сложения по модулю 2, разбиение Δ обладает всеми необходимыми для моделирования множества ФАЛ G свойствами, и что при этом число его «плохих» компонент не больше, чем

$$C_{q-m}^0 + \cdots + C_{q-m}^{\lambda-1}.$$

Лемма доказана. □

Следствие. *В случае $q \geqslant m+3\lambda$ число плохих компонент разбиения Δ не больше, чем $(2e_6)^{q-m}$, где $e_6 < 1$.*

Теорема 6.1. *Для любой ФАЛ f, $f \in P_2(n)$ существует реализующая её формула $\mathcal{F}_f$, $\mathcal{F}_f \in \mathcal{U}_{\text{Б}}^{\Phi}$, такая, что*

$$\mathcal{L}\big(\mathcal{F}_f\big) \leqslant \rho_{\text{Б}} \frac{2^n}{\log n}\Big(1 + \frac{\log\log n \pm O(1)}{\log n}\Big). \tag{6.1}$$

Доказательство. Выберем ФЭ $\mathcal{E}_j$, введём натуральные параметры m, s, t, p, l, λ и определим разбиение Π, формулу $\mathcal{F}_p$, ФАЛ φ, φ–УМ G порядка m так, как это было сделано в доказательстве теоремы 5.1 и так, чтобы выполнялись соотношения (5.2)–(5.6).

Выберем, далее, натуральный параметр q так, что

$$m + 3\lambda \leqslant q \leqslant n \tag{6.2}$$

и построим по лемме 6.2 для множества ФАЛ G соответствующее m–регулярное разбиение $\Delta = (\delta_1, \ldots, \delta_{2^{q-m}})$ куба B^q от БП $x' = (x_1 \ldots x_q)$. Заметим, что для произвольной ФАЛ $g(x')$ и любого i, $i \in [1, 2^{q-m}]$, в силу φ–универсальности множества G, m–регулярности разбиения Δ и возможности моделировать ФАЛ из G на компонентах Δ с помощью БП или их отрицаний всегда найдутся такие натуральные числа $j_1, \ldots, j_p$ из $[m+1, q]$ и булевы константы $\alpha_1, \ldots, \alpha_p$, для которых равенство

$$g(x') = \varphi\big(x_{j_1}^{\alpha_1}, \ldots, x_{j_p}^{\alpha_p}\big) \tag{6.3}$$

выполняется на любом наборе из δ_i.

Возьмём (см. (5.7)) разложение ФАЛ f по БП $x'' = (x_{q+1} \ldots x_n)$ и продолжим его на основе (6.3) так, что

$$f(x', x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') \cdot f_{\sigma''}(x') = \bigvee_{i=1}^{2^{q-m}} \chi_i(x_i) \cdot \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') \cdot \varphi\big(x_{j_{1,i,\sigma''}}^{\alpha_{1,i,\sigma''}}, \ldots, x_{j_{j,i,\sigma''}}^{\alpha_{p,i,\sigma''}}\big), \tag{6.4}$$

где $\chi_i(x')$ — характеристическая ФАЛ компоненты δ_i разбиения Δ. Искомая формула $\mathcal{F}_f$ получается из последнего представления (6.4) ФАЛ f следующим образом:

1) характеристическая ФАЛ χ_i, $i \in [1, 2^{q-m}]$, реализуется по своей совершенной ДНФ;

2) мультиплексорная ФАЛ μ_{n-q} порядка $(n-q)$ от адресных БП x'', связанная с разложением f по этим БП, реализуется с помощью бесповторной по информационным БП формулы из $\mathcal{U}^{\mathrm{C}}$ сложности не больше, чем $4 \cdot 2^{n-q}$ (см. [ ]);

3) каждая ФАЛ вида (6.3) реализуется одной формулой $\mathcal{F}_p$ с необходимыми инверсиями её БП в случае «плохой» компоненты δ_i;

4) все используемые при реализации формул из пунктов 1-3 элементы базиса Б_0 заменяются соответствующими им бесповторными формулами $\mathcal{F}_{\&}$, $\mathcal{F}_{\vee}$, $\mathcal{F}_{\neg}$ из леммы 6.1.

Для сложности построенной таким образом формулы $\mathcal{F}_f$ будет (ср. с (5.7)) справедливо неравенство

$$\mathcal{L}(\mathcal{F}_f) \leqslant \mathcal{L}_j \cdot t \cdot 2^{n-m} + O\big(2^{n-m}\big(1 + t \cdot e_6^{q-m}\big) + q \cdot 2^q\big), \tag{6.5}$$

которое при значениях параметров

$$m = \lfloor 2\log\log n \rfloor, \qquad s = \lfloor \log n - \log\log n \rfloor - 2,$$

удовлетворяющих при достаточно больших n условиям (6.2), даёт оценку (6.1).

Теорема доказана. □

Теорема 6.2. *Для любой ФАЛ f, $f \in P_2(n)$, существует реализующая её формула $\mathcal{F}_f$, $\mathcal{F}_f \in \mathfrak{U}^{\Phi}$, такая, что*

$$L(\mathcal{F}_f) \leqslant \frac{2^n}{\log n}\left(1 + O\left(\frac{1}{\log n}\right)\right). \tag{6.6}$$

Доказательство. Искомая формула $\mathcal{F}_f$ строится, как и при доказательстве теоремы 6.1, на основе представления (6.4). При этом вместо ФЭ $\mathcal{E}_j$ необходимо взять ФЭ $\widetilde{\mathcal{E}}$ базиса $\widetilde{\text{Б}}$, а вместо формулы $\mathcal{F}_t$, ФАЛ $\varphi(y_1, \ldots, y_p)$ и φ–УМ G необходимо использовать формулу $\widetilde{\mathcal{F}}_t$, ФАЛ $\widetilde{\varphi}(y_1, \ldots, y_p)$ и $\widetilde{\varphi}$–УМ G из доказательства теоремы 5.2 соответственно. Заметим, что в данном случае отпадает необходимость моделирования базисных ФАЛ бесповторными формулами из леммы 6.1.

Сложность построенной таким образом формулы $\mathcal{F}_f$ по-прежнему удовлетворяет неравенству (6.5), из которого при следующих значениях параметров

$$m = \lfloor 2\log\log n \rfloor, \quad s = \lfloor \log n \rfloor - 3, \quad t = \left\lceil \frac{2^m}{3(s-5)} \right\rceil, \quad p = 3t + 1,$$

удовлетворяющих при достаточно больших n всем необходимым условиям, вытекает (6.6).

Теорема доказана. □

Следствие.

$$L^{\Phi}(n) = \frac{2^n}{\log n}\left(1 \pm O\left(\frac{1}{\log n}\right)\right).$$

§7 Мультиплексорные ФАЛ и обобщённое разложение. Оптимальная по задержке реализация мультиплексорных ФАЛ в произвольном базисе

Пусть $\Delta = (\delta_1, \ldots, \delta_p)$ — разбиение куба B^n от БП $x = (x_1, \ldots, x_n)$. Определим *мультиплексорную ФАЛ μ_Δ, соответствующую разбиению* Δ, равенством

$$\mu_\Delta(x,\, u_1, \ldots, u_p) = \bigvee_{i=1}^{p} \chi_{\delta_i}(x) u_i, \tag{7.1}$$

где χ_{δ_i} — характеристическая ФАЛ компоненты δ_i. Тогда стандартную мультиплексорную ФАЛ порядка n

$$\mu_n(x,\ u_0,\dots,u_{2^n-1}) = \bigvee_{\sigma=(\sigma_1,\dots,\sigma_n)\in B^n} K_\sigma(x)u_{\nu(\sigma)} \tag{7.2}$$

можно рассматривать как обобщённую мультиплексорную ФАЛ μ_Δ с тривиальным разбиением Δ таким, что $\delta_{\nu(\sigma)} = \{\sigma\}$ для каждого σ, $\sigma \in B^n$.

Напомним, что БП $x_1,\dots,x_n$ считаются *адресными* БП указанных выше мультиплексорных ФАЛ, а БП $u_1,\dots,u_p$ и $u_0,\dots,u_{2^n-1}$ называются *информационными* БП ФАЛ μ_Δ и μ_n соответственно. С содержательной точки зрения поведение мультиплексорной ФАЛ μ_Δ определяется тем, что на любом наборе значений адресных БП из компоненты δ_i, $i \in [1,p]$, она совпадает с информационной БП u_i.

Заметим, что правые части равенств (7.1) и (7.2) представляют собой результат суперпозиции, внешней ФАЛ, которой является дизъюнкция вида $y_1 \vee \dots \vee y_p$ и $y_0 \vee \dots \vee y_{2^n-1}$ соответственно, а каждая внутренняя ФАЛ этой суперпозиции зависит от адресных БП и не более, чем от одной, из информационных БП. Обобщим указанные представления на тот случай, когда в качестве внешней ФАЛ используется, вообще говоря, произвольная ФАЛ от достаточно большого числа БП.

Лемма 7.1. *Для любой существенной ФАЛ $\varphi(y_1,\dots,y_p)$ и любого разбиения $\Delta = (\delta_1,\dots,\delta_p)$ куба B^n от БП $x = (x_1,\dots,x_n)$ существуют ФАЛ $g_i(x,u_i)$, $i = 1,\dots,p$, которые монотонно или антимонотонно зависят от БП $u_1,\dots,u_p$, и для которых*

$$\mu_\Delta(x,\ y_1,\dots,y_p) = \varphi(g_1,\dots,g_p). \tag{7.3}$$

Доказательство. Существенность ФАЛ φ означает, что для любого i, $i = 1,\dots,p$, найдутся булевские константы $\alpha_{i,1},\dots,\alpha_{i,p}$ такие, что (ср. с. (3.2))

$$\varphi(\alpha_{i,1},\dots,\alpha_{i,i-1},\ y_i,\ \alpha_{i,i+1},\dots,\alpha_{i,p}) = y_i \oplus \alpha_{i,i}.$$

Значит, определив ФАЛ g_i так, что

$$g_j(\beta,u_j) = \begin{cases} \alpha_{i,j}, & \text{если } \beta \in \delta_i \text{ при } j \neq i; \\ y_j \oplus \alpha_{j,j}, & \text{если } \beta \in \delta_j; \end{cases} \tag{7.4}$$

для произвольного набора β, $\beta \in \delta_i$, будем иметь

$$\begin{aligned} &\varphi(g_1(\beta,y_1),\dots,g_{i-1}(\beta,y_{i-1}),\ g_i(\beta,y_i),\ g_{i+1}(\beta,y_{i+1}),\dots,g_p(\beta,y_p)) = \\ &\quad = \varphi(\alpha_{i,1},\dots,\alpha_{i,i-1},\ y_i \oplus \alpha_{i,i},\ \alpha_{i,i+1},\dots,\alpha_{i,p}) = (y_i \oplus \alpha_{i,i}) \oplus \alpha_{i,i} = y_i = \\ &\qquad = \mu_\Delta(\beta,\ y_1,\dots,y_p). \end{aligned} \tag{7.5}$$

Из (7.4) следует, что каждая ФАЛ g_j зависит от БП u_j только на компоненте δ_j, на которой $g_j = u_j \oplus \alpha_{j,j}$. Следовательно, каждая ФАЛ g_j либо монотонно, либо антимонотонно зависит от БП u_j.

Лемма доказана. □

Замечание. Лемма 7.1 остаётся справедливой и в том случае, когда число компонент разбиения Δ равно t и $t < p$, если при этом формально считать все недостающие компоненты $\delta_{t+1}, \ldots, \delta_p$ разбиения Δ пустыми, а соответствующие им информационные БП $u_{d+1}, \ldots, u_p$ — фиктивными БП ФАЛ $g_{t+1}, \ldots, g_p, \mu_\Delta$.

В дальнейшем представление (7.3) мультиплексорной ФАЛ μ_Δ будем называть её *φ–разложением* или, иначе, *обобщенным разложением* μ_Δ с *внешней* ФАЛ φ. При этом ФАЛ системы $(g_1, \ldots, g_p)$ будем считать *внутренними* ФАЛ указанного разложения, а все различные ФАЛ вида $g_j(x, \sigma)$, где $j \in [1, p]$, и $\sigma \in B$, — его *вспомогательными* ФАЛ. Так ФАЛ вида $\chi_i(x) \cdot u_i$, $i \in [1, p]$, и $K_\sigma(x) \cdot u_{\nu(\sigma)}$, $\sigma \in B^n$, являются внутренними ФАЛ разложений (7.1) и (7.2) соответственно, а ФАЛ вида $\chi_i(x)$, $i \in [1, p]$, и 0 (вида $K_\sigma(x)$, $\sigma \in B^n$, и 0) — внутренними ФАЛ разложения (7.1) (соответственно (7.2)).

Заметим, что обобщённое разложение (7.3) стандартной мультиплексорной ФАЛ μ_n с внешней ФАЛ $\varphi(y_1, \ldots, y_p)$, где $p \geqslant 2^n$, можно использовать для соответствующего обобщённого разложения по БП $x = (x_1, \ldots, x_n)$ произвольной ФАЛ $\psi(x, z)$, где $z = (z_1, \ldots, z_m)$, следующим образом:

$$\psi(x, z) = \varphi(g_0(x, \psi(\tilde{0}, z)), \ldots, g_{2^n-1}(x, \psi(\tilde{1}, z)), g_{2^n}(x), \ldots, g_{p-1}(x))$$

Установим, далее, верхние оценки некоторых «мощностных» и «сложностных» характеристик внутренних и вспомогательных ФАЛ обобщённого разложения (7.3) в тех случаях, когда ФАЛ φ обладает определёнными свойствами и, в частности, когда она реализуется бесповторной формулой базиса Б.

Отметим, сначала, что при $n = m$ имеется явная связь между вспомогательными (внутренними) ФАЛ обобщённого разложения (7.3) и построенным в §3 на основе разбиения Δ «диагональным» φ–УМ G порядка m, которое имеет вид $G = G^{(1)} \cup \cdots \cup G^{(p)}$. Действительно, если и в том и в другом случае используется один и тот же набор констант $\alpha_{i,j}$ — констант существенной зависимости ФАЛ φ от её БП, — то в силу (3.2), (3.3), (7.3), (7.4) ФАЛ $g_j(x, 1)$ и $g_j(x, 0)$, где $j \in [1, p]$, являются единственным максимальным и единственным минимальным элементами частично упорядоченного отношением «поразрядного» сравнения $\leqslant$ множества ФАЛ $G^{(j)}$ соответственно.

Аналогичное соответствие сохраняется и тогда, когда φ–УМ G порядка m строится для (произвольного) разбиения $\Delta = (\delta_1, \ldots, \delta_p)$ на базе селекторного разбиения Δ БП ФАЛ $\varphi(y_1, \ldots, y_p)$ (см. доказательство леммы 3.1). При этом построение указанного множества G возможно и в тех случаях, когда условия леммы 3.1, связанные с чётностью мощностей компонент разбиения Δ, а также с совпадением мощностей тех компонент Δ, которые соответствуют БП из одной и той же компоненты разбиения Δ, не выполняются. С учётом вышесказанного из доказательства леммы 3.1 вытекает справедливость следующего утверждения.

Лемма 7.2. *Пусть в условиях леммы 7.1 ФАЛ φ имеет селекторное разбиение множества своих БП на d компонент. Тогда внутренние ФАЛ φ–разложения* (7.3) *ФАЛ μ_Δ можно выбрать так, что число различных вспомогательных ФАЛ этого разложения будет не больше, чем $2d$.*

Назовём *альтернированием набора* α, $\alpha = (\alpha_1, \ldots, \alpha_n)$, число изменений значений α_i в нём, при их просмотре в порядке возрастания номера i, $i = 1, \ldots, n$, и обозначим это число через $\mathrm{alt}\,(\alpha)$. Другими словами

$$\mathrm{alt}\,(\alpha) = \sum_{i=1}^{n-1} (\alpha_i \oplus \alpha_{i+1}).$$

Альтернирование набора равно минимальному числу отрезков постоянства, на которые он распадается, уменьшенному на единицу. Определим *альтернирование ФАЛ f* как альтернированию столбца её значений и обозначим эту величину через $\mathrm{alt}\,(f)$. Назовём ФАЛ h *ступенчатой*, если $\mathrm{alt}\,(h) \leqslant 1$. Нетрудно видеть, что ступечантая ФАЛ является либо монотонной, либо антимонотонной ФАЛ. Функцию h_i, $h_i \in P_2(n)$, назовём *i-ой ступенчатой* ФАЛ ($0 \leqslant i \leqslant 2^n$), если для всякого β, $\beta \in B^n$,

$$h_i(\beta) = \begin{cases} 0, & \text{при } \nu(\beta) < i; \\ 1, & \text{при } \nu(\beta) \geqslant i. \end{cases}$$

Лемма 7.3. *При $n \geqslant 2$ глубина в базисе* Б_0 *любой ФАЛ g, $g \in P_2(n)$, удовлетворяет неравенству*

$$D(g) \leqslant 2\lceil \log n \rceil + \lceil \log(\mathrm{alt}\,(g) + 1) \rceil. \tag{7.6}$$

Доказательство. Если $\mathrm{alt}\,(g) = 0$, то есть ФАЛ g — константа, то неравенство (7.6) выполняется, поскольку любую константу можно реализовать одной из формул вида $x_1 \vee \overline{x}_1$, $x_1 \cdot \overline{x}_1$, которые имеют глубину 2.

Индукцией по k, $k \geqslant 1$ докажем, что при любом n, $n \in [2, 2^k]$ и любом i, $i \in [1, 2^n)$, выполняется неравенство

$$D(h_i(x_1, \ldots, x_n)) \leqslant 2\lceil \log n \rceil - 1. \tag{7.7}$$

Базис индукции составляет случай $k = 1$, в котором $h_1(x_1, x_2) = x_1 \vee x_2$, $h_2(x_1, x_2) = x_1$, $h_3(x_1, x_2) = x_1 \cdot x_2$, и, следовательно, неравенство (7.7) справедливо.

Пусть для некоторого натурального k неравенство (7.7) выполняется при любом n', $n' \in (2^{k-1}, 2^k]$, и любом i', $i \in [1, 2^n)$. Для обоснования индуктивного перехода достаточно доказать (7.7) для любого n, $n \in (2^k, 2^{k+1}]$, то есть для любого n, удовлетворяющего соотношению $\lceil \log n \rceil = k + 1$, и любого i, $i \in [1, 2^n)$.

Рассмотрим ФАЛ h_i, $h_i \in P_2(n)$, как ФАЛ, зависящую от всех 2^{k+1} БП $x_1, \ldots, x_{2^{k+1}}$ (при $n < 2^{k+1}$ от последних БП зависимость фиктивная), и обозначим $x = (x_1, \ldots, x_{2^k})$, $x'' = (x_{2^k+1}, \ldots, x_{2^{k+1}})$. Представим число i, $1 \leqslant i \leqslant 2^n - 1 \leqslant 2^{2^{k+1}} - 1$, в виде

$$i = 2^{2^k} i' + i'',$$

где $0 \leqslant i', i'' \leqslant 2^{2^k} - 1$, причём i' и i'' не равны нулю одновременно. Заметим, что при этом

$$h_i(x', x'') = h_{i+1}(x') \vee K_{i'}^{+}(x') \cdot h_{i''}(x''), \tag{7.8}$$

где $K_0^+ \equiv 1$ и $K_{i'}^+(x')$ — конъюнкция тех БП набора x', которым в наборе $\nu^{-1}(i')$ значений этих БП соответствуют единицы, если $i' > 0$.

Пусть $i' \in (0, 2^{2^k} - 1)$, $i'' \neq 0$ и пусть формулы $\mathcal{F}_{i'+1}(x')$, $\mathcal{F}_{i''}(x'')$ построены по индуктивному предположению для ФАЛ $h_{i'+1}(x')$, $h_{i''}(x'')$ соответственно, а формула $\mathcal{K}_{i'}^+(x')$ реализует ЭК $K_{i'}^+(x')$ на основе двоичного дерева глубины не больше, чем k, состоящего из ФЭ &. Тогда в силу (7.8) формула

$$\mathcal{F}_i(x', x'') = \mathcal{F}_{i'+1}(x') \vee \mathcal{K}_{i'}^+(x') \cdot \mathcal{F}_{i''}(x'')$$

реализует ФАЛ $h_i(x', x'')$ с глубиной

$$D(\mathcal{F}_i) \leqslant \max\{2k - 1, \max\{k, 2k - 1\} + 1\} + 1 \leqslant 2(k + 1) - 1,$$

удовлетворяющей (7.7).

В остальных случаях, используя введённые выше обозначения, определим искомую формулу $\mathcal{F}_i$, удовлетворяющую (7.7), следующим образом:

$$\mathcal{F}_i = \begin{cases} \mathcal{F}_1(x') \vee \mathcal{F}_{i''}(x''), & \text{если } i' = 0; \\ x_1 \cdot \ldots \cdot x_{2^k} \cdot \mathcal{F}_{i''}(x''), & \text{если } i' = 2^{2^k} - 1 \text{ и } i'' > 0; \\ \mathcal{F}_{i'}(x'), & \text{если } i'' = 0. \end{cases}$$

Неравенство (7.7), таким образом, полностью доказано.

Заметим, что альтернирование 1 и 2 в $P_2(n)$ имеют только ФАЛ вида h_i, $\overline{h}_i$, где $i \in (0, 2^n)$, и ФАЛ вида $\overline{h}_i \vee h_j$, $h_i \cdot \overline{h}_j$, где $0 < i < j < 2^n$ соответственно. Следовательно, в силу (7.7) для любой ФАЛ g, $g \in P_2(n)$, такой, что $1 \leqslant \mathrm{alt}\,(g) \leqslant 2$, справедливо неравенство

$$D(g) \leqslant 2\lceil \log n \rceil + \lceil \log(\mathrm{alt}\,(g)) \rceil, \tag{7.9}$$

из которого для указанной ФАЛ g вытекает (7.6). Заметим также, что приведённые выше ФАЛ $h_i \cdot \overline{h}_j$ и $\overline{h}_i \vee h_j$ являются характеристической ФАЛ отрезка $[i, j)$ куба B^n и её отрицанием соответственно.

Пусть, далее, g — произвольная ФАЛ из $P_2(n)$ и пусть $\mathrm{alt}\,(g) = g \geqslant 3$. Из определений следует, что куб B^n разбивается на последовательные отрезки «постоянства» ФАЛ g, то есть отрезки $I_0, I_1, \ldots, I_q$ такие, что ФАЛ g равна $g(0, \ldots, 0) + i \pmod 2$ на отрезке I_i, $i \in [0, q]$. При этом ФАЛ g представляет собой дизъюнкцию характеристических ФАЛ t, $t = \lfloor (q + 1)/2 \rfloor \geqslant 2$, «нечётных» отрезков её постоянства $I_1, I_3, \ldots, I_{2t-1}$, если $g(0, \ldots, 0) = 0$, и конъюнкцию отрицаний этих ФАЛ, если $g(0, \ldots, 0) = 1$.

Следовательно, формула $\mathcal{F}_g$, которая реализует ФАЛ g, $g(0,\ldots,0)=\sigma$, с глубиной, удовлетворяющей (7.6), получается в результате подстановки t удовлетворяющих (7.9) формул для $\overline{\sigma}$–степеней характеристических ФАЛ отрезков $I_1,\ldots,I_{2t-1}$ вместо t БП бесповторной формулы, дерево которой представляет собой квазиполное двоичное дерево глубины $\lceil\log t\rceil$ из ФЭ &, если $\sigma=1$, и ФЭ $\vee$, если $\sigma=0$. Действительно,

$$D(\mathcal{F}_g)\leqslant 2\lceil\log n\rceil+1+\lceil\log t\rceil=$$
$$=2\lceil\log n\rceil+\lceil\log(2\lfloor(q+1)/2\rfloor)\rceil\leqslant 2\lceil\log n\rceil+\lceil\log(q+1)\rceil\,.$$

Лемма доказана. □

§8 Задача синтеза схем для функций из специальных классов, примеры её решения и мощностные нижние оценки. Инвариантные классы С. В. Яблонского, теорема о числе инвариантных классов

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. Для класса ФАЛ или операторов Q' и класса ФАЛ Q'' введём такие 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 из определения следует, что $0\leqslant\sigma_Q(n)\leqslant 1$ для всех n, $n=1,2,\ldots$.

Класс ФАЛ (операторов) Q называется:

1) *невырожденным*, если $n+m_Q(n)=o\big(\mathcal{J}\big(Q(n)\big)\big)$;

2) *строго невырожденным* классом ФАЛ, если $\log n = o\big(\log|Q(n)|\big)$;

3) *ненулевым классом ФАЛ*, если $\varliminf_{n\to\infty} \sigma_Q(n) > 0$.

На основе стандартного мощностного метода получения нижних оценок можно установить справедливость следующего утверждения.

Лемма 8.1. *Если Q — невырожденный класс ФАЛ (операторов), то*

$$\mathcal{L}^{\mathrm{C}}_{\text{Б}}\big(Q(n)\big) \gtrsim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big), \qquad L^{\text{ИКС}}\big(Q(n)\big) \gtrsim \frac{1}{2} \cdot \mathcal{J}\big(Q(n)\big),$$

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 выполнены асимптотические неравенства*

$$\mathcal{L}^{\mathrm{C}}_{\text{Б}}\big(Q(n)\big) \gtrsim \rho_{\text{Б}} \cdot \sigma_Q(n)\frac{2^n}{n},$$
$$L^{\text{ИКС}}\big(Q(n)\big) \gtrsim \frac{1}{2} \cdot \sigma_Q(n)\frac{\log|Q(n)|}{n},$$
$$L^{\mathrm{K}}\big(Q(n)\big) \gtrsim \sigma_Q(n)\frac{2^n}{n}.$$

Класс ФАЛ (операторов) Q называется *стандартным относительно функционала сложности $\mathcal{L}$ класса схем* $\mathfrak{U}^{\mathrm{C}}_{\text{Б}}$, если выполнено асимптотическое неравенство

$$\mathcal{L}^{\mathrm{C}}_{\text{Б}}\big(Q(n)\big) \lesssim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big) + O\big(n + m(n)\big).$$

Аналогично вводится определения стандартного класса операторов относительно других классов схем и функционалов их сложности, если соответствующая функция Шеннона имеет порядок роста $2^n/n$. Отметим, что при этом для невырожденного стандартного класса ФАЛ Q имеет место асимптотическое равенство

$$\mathcal{L}^{\mathrm{C}}_{\text{Б}}\big(Q(n)\big) \sim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big).$$

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 8.2. *Для любой функции $r = r(n) \geqslant 1$ соответствующий класс $Q(n) = P_2(n, r(n))$ является стандартным относительно функционала сложности $\mathcal{L}$ схем класса $\mathfrak{U}^{\mathrm{C}}_{\text{Б}}$, то есть*

$$\mathcal{L}^{\mathrm{C}}_{\text{Б}}\big(Q(n)\big) \lesssim \rho_{\text{Б}}\frac{r}{\log r} + O(n).$$

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). 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 $\mathcal{F}_t$. Из принадлежности ФАЛ f классу $P_2(n, r)$ следует, что при $\nu(\sigma'') > \lceil r/2^q \rceil$ 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 (5.9) будет выполняться неравенство

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

из которого при значениях параметров (5.10) следует, что

$$\mathcal{L}\big(\widetilde{\Sigma}_f\big) \lesssim \rho_{\text{Б}} \frac{r}{\log r}. \tag{8.1}$$

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,

$$f(x_1, \ldots, x_n) = \overline{x}_{k+1} \cdot \ldots \cdot \overline{x}_n \cdot f'(x_1, \ldots, x_k). \tag{8.2}$$

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 (8.1). Искомая СФЭ $\widetilde{\Sigma}_f$ строится на основе (8.2) так, что

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

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*

$$\mathcal{L}_{\text{Б}}^{\text{С}}\big(Q(n)\big) \sim \rho_{\text{Б}} \frac{r}{\log r}.$$

Замечание. Аналогично доказывается стандартность класса $Q(n) = P_2(n, r(n))$ относительно функционала «обычной» сложности и классов схем $\mathcal{U}^{\text{ИКС}}, \mathcal{U}^{\text{К}}$.

Рассмотрим теперь 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 операций 1–3, то говорят, что g является *квазиподфункцией* ФАЛ f, а f — *квазинадфункцией* ФАЛ g. Для множества функций F через $F^{\urcorner}$ и $F_{\lrcorner}$ будем обозначать множества всех квазинадфункций и квазиподфункций 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 $Q \supseteq \{0, 1\}$, поскольку Q содержит неконстантую 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 $\widehat{L}$ всех монотонных и всех линейных ФАЛ соответственно. При этом 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 всех симметрических ФАЛ также не является инвариантным, так как он не замкнут относительно операции 1. При этом инвариантным является класс $\widehat{S}$ — класс *квазисимметрических* ФАЛ, то есть функций, симметрических по всем своим существенным переменным.

Лемма 8.3. *Пусть Q — инвариантный 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 последовтельности $\sigma_Q(n)$ следует, что для каждого n выполнено неравенство $0 \leqslant \sigma_Q(n) \leqslant 1$, то есть эта последовательность $\sigma_Q(n)$ ограничена. Покажем, что она монотонно не возрастает, откуда будет следовать её сходимость. В силу инвариантности класса Q, всякую функцию f из множества $Q(n+1)$ 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 $f_\sigma(x_1,\dots,x_n) = f(x_1,\dots,x_n,\sigma)$, $\sigma \in B$, 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 $\sigma_Q(n)$, $n = 1, 2, \dots$, 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.

Инвариантный класс Q с характеристикой $\sigma_Q = 0$ называется *нулевым*. Покажем, 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 $\sigma_Q(n)$, $n = 1, 2, \dots$, и её сходимости к пределу σ_Q следует, что $\sigma_Q \leqslant \sigma_Q(m) < 1$.

Найдём значение характеристик инвариантных классов M, $\widehat{L}$ и $\widehat{S}$. Известно [], что

$$\log|M(n)| \sim C_n^{\lceil n/2 \rceil} \sim \frac{2^n}{\sqrt{2\pi n}},$$

откуда следует, что $\sigma_M = 0$. Для класса линейных функций, очевидно, при любом n выполняется равенство $|\widehat{L}(n)| = 2^{n+1}$ и, значит, $\sigma_L = 0$. Всякую функцию из множества $\widehat{S}(n)$ 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

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

и поэтому $\sigma_{\widehat{S}} = 0$. Таким образом, все три класса M, $\widehat{L}$, $\widehat{S}$ являются нулевыми. Примером ненулевого инвариантного класса, отличного от P_2, является класс Q, состоящий из всех ФАЛ вида $f(x_{i_1},\dots,x_{i_r})(x_{i_1} \oplus \dots \oplus x_{i_r} \oplus \sigma)$, где $1 \leqslant i_1 < \dots < i_r$ 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 8.4. *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 $\widehat{S}$, 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

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

следует, что порождающий элемент нетривиального инвариантного класса является существенной функцией и что никакие два различных порождающих элемента не являются квазиподфункциями 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 8.5. *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.*

§9 Принцип локального кодирования О. Б. Лупанова и примеры его применения.

Рассмотрим достаточно общий подход к решению задачи синтеза СФЭ для ФАЛ из специальных классов, предложенный в работе [5] О. Б. Лупанова и названный им принципом локального кодирования.

Основаная идея этого подхода состоит в том, чтобы с помощью определённого «кодирования» свести задачу синтеза СФЭ для ФАЛ или операторов из заданного класса Q к аналогичной задаче синтеза для класса произвольных или близких к ним операторов соответствующей размерности. В [5] был предложен ряд условий, налагаемых как на класс Q, так и на его кодирование, при выполнении которых получаемые указанным способом схемы могли оказаться асимптотически наилучшими как для самых «плохих» ФАЛ (систем ФАЛ) из $Q(n)$, так и для почти всех

ФАЛ (систем ФАЛ) из $Q(n)$, $n = 1, 2, \ldots$. Следующее утверждение и его доказательство дают пример решения задачи синтеза СФЭ для ФАЛ из инвариантного класса Q с помощью принципа локального кодирования.

Лемма 9.1. *Для всякого инвариантного класса Q и $n = 1, 2, \ldots$*

$$L^{\mathrm{C}}\big(Q(n)\big) \sim \sigma_Q \frac{2^n}{n} \qquad \text{при } \sigma_Q > 0, \tag{9.1}$$

$$L^{\mathrm{C}}\big(Q(n)\big) = o\Big(\sigma_Q \frac{2^n}{n}\Big) \qquad \text{при } \sigma_Q = 0. \tag{9.2}$$

Доказательство. Рассмотрим сначала случай $\sigma_Q > 0$. В этом случае в соответствии с введёнными в §8 обозначениями и в силу леммы 8.3 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 8.1 следует нижняя оценка (9.1).

Перейдём к получению верхней оценки (9.1). 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

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

получим верхнюю оценку

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

В случае $\sigma_Q > 0$ отсюда, с учётом нижней оценки, вытекает (9.1).

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

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

что доказывает (9.2).

Лемма доказана. □

Как уже говорилось, при доказательстве верхней оценки леммы 9.1 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 $A^{(1)} = A_n^{(1)}$ по набору σ вычисляет координаты куска кода $\pi_{i(\sigma)}$, а оператор декодирования $A^{(2)} = A_n^{(2)}$ 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 $O = O_n$, который по координатам куска $\pi_{i(\sigma)}$ выдаёт сам этот кусок.

Если при этом сложность указанных выше операторов $A_n^{(1)}$, $A_n^{(2)}$ и O_n удовлетворяет соотношениям

$$\mathcal{L}_{\text{Б}}^{\text{С}}\big(A_n^{(1)}\big) = o\big(\mathcal{J}\big(Q(n)\big)\big), \qquad \mathcal{L}_{\text{Б}}^{\text{С}}\big(A_n^{(2)}\big) = o\big(\mathcal{J}\big(Q(n)\big)\big), \tag{9.3}$$

$$\mathcal{L}_{\text{Б}}^{\text{С}}\big(O_n\big) \lesssim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big), \tag{9.4}$$

то искомая СФЭ Σ_n может быть выбрана так, что

$$\mathcal{L}\big(\Sigma_n\big) \lesssim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big).$$

Отсюда вытекает, что

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \lesssim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big),$$

и, следовательно, в силу леммы 8.1 в случае невырожденности класса Q выполняется асимптотическое равенство

$$\mathcal{L}_{\text{Б}}^{\text{C}}\big(Q(n)\big) \sim \rho_{\text{Б}} \cdot \mathcal{J}\big(Q(n)\big),$$

которое означает стандартность класса Q относительно функционала сложности $\mathcal{L}$ класса схем $\mathcal{U}_{\text{Б}}^{\text{C}}$.

Заметим, что в случае асимптотической неизбыточности кодирования $\Pi = \Pi_n$, когда

$$d(n) \sim \log |Q(n)|,$$

при построении схемы, которая реализует оператор O_n со сложностью, удовлетворяющей (9.4), достаточно, как правило, использовать асимптотически наилучший метод синтеза СФЭ для произвольных систем ФАЛ подходящей размерности или некоторые его модификации (см., например, лемму 8.2).

Заметим также, что соотношение (9.3) означает возможность существенно более простой по сравнению с оператором O_n реализации операторов $A_n^{(1)}$ и $A_n^{(2)}$ в классе $\mathcal{U}_{\text{Б}}^{\text{C}}$.

Покажем, что описанный в доказательстве леммы 9.1 асимптотически наилучший метод синтеза СФЭ над базисом Б 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 O совпадает с оператором $\mathcal{O}$, а оператор $A^{(2)}$ — с ФАЛ h.

Рассмотрим ещё два класса операторов и с помощью принципа локального кодирования докажем (при некоторых условиях) их стандартность. Обозначим через S класс всех симметрических ФАЛ, а под (n, m)-оператором будем понимать систему ФАЛ $F = (f_1, \ldots, f_m)$ из $P_2^m(n)$.

Лемма 9.2. *Если натуральная последовательность $m = m(n)$, $n = 1, 2, \ldots$, такова, что*

$$\log n = o(m) \quad \text{и} \quad \log m = o(n), \tag{9.5}$$

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

$$\mathcal{J}\big((Q(n)\big) = \frac{m(n+1)}{\log m + \log(n+1)}. \tag{9.6}$$

Из (9.6), 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 (9.5) 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 8.1 с учётом (9.5) получаем нижнюю оценку

$$L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \mathcal{J}\big(Q(n)\big) \sim \frac{m \cdot n}{\log n}. \tag{9.7}$$

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 $\pi = (\,F(0,\ldots,0), F(0,\ldots,0,1), F(0,\ldots,0,1,1), \ldots, F(1,\ldots,1)\,)$, разбитый на $(n+1)$ непересекающихся кусков длины $\lambda = m$. При этом «координатами» i-го, $i \in [0,n]$, куска кода $\pi_i = F(\,(0,\ldots,0,\underbrace{1,\ldots,1}_{i})\,)$ 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 $\alpha = (\alpha_1, \ldots, \alpha_n) \in B^n$ переводит в набор β, $\beta \in B^t$, такой, что $\nu(\beta) = \alpha_1 + \cdots + \alpha_n$, и имеет сложность [1]

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

Заметим, что основной оператор O_n может быть при этом выбран из множества $P_2^m(t, n+1)$, а его сложность в силу леммы 8.2 удовлетворяет неравенству

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

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 (9.7).

Лемма доказана. □

Лемма 9.3. *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 8.1 непосредственно вытекает необходимая нижняя оценка

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

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 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

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

из которых следует, что

$$L^{\mathrm{C}}\big(F_n\big) \lesssim \frac{2^n}{n}.$$

Лемма доказана. □

§10 Синтез схем для не всюду определённых функций

В заключение части I рассмотрим задачу синтеза схем для не всюду определённых функций, которая близка к задаче синтеза схем для ФАЛ из специальных классов.

Отображение $f\colon B^n \overset{f}{\mapsto} [0,2]$ 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:

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

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

Лемма 10.1. *Если* $n \log n = o(t(n))$, *то*

$$L^{\mathrm{C}}\bigl(\widehat{P}_2(n, t(n))\bigr) \gtrsim \frac{t(n)}{\log t(n)}. \tag{10.1}$$

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, что $n = o\bigl(\mathcal{J}(|Q(n)|)\bigr)$, то есть класс ФАЛ $Q(1), \ldots, Q(n)$, является невырожденным. Из этой невырожденности, леммы 8.1 и очевидных соотношений

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

вытекает оценка (10.1).

Лемма доказана. □

Рассмотрим, далее, несколько утверждений, позволяющих установить для исследуемой функции Шеннона верхнюю оценку вида правой части (10.1) при последовательно ослабляемых ограничениях на рост функции $t = t(n)$.

Лемма 10.2. *Если* $t = t(n) \sim n$, *то*

$$L^{\mathrm{C}}\big(\widehat{P}_2(n,t)\big) \lesssim \frac{t(n)}{\log t(n)}. \tag{10.2}$$

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 μ, $\mu \leqslant 2^q$, и для любого s, $s \leqslant 2^q$, построим такое множество наборов $\mathfrak{A}_s$ куба B^s, которое «протыкает» (см. [3]) все грани ранга не больше чем μ, этого куба и состоит не более, чем из $s \cdot 2^\mu$ 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

$$|G| \leqslant 2^{\mu+3q}, \qquad L^{\mathrm{C}}\big(\overrightarrow{G}\big) \leqslant 2^{\mu+4q}. \tag{10.3}$$

Заметим также, что любая ФАЛ $\widehat{g}$ из $\widehat{P}_2(q,t')$, где $t' \leqslant \mu$, 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'':

$$f(x', x'') = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''}(x'') f_{\sigma''}(x'), \tag{10.4}$$

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 $p_{\sigma''} = \lceil t_{\sigma''}/\mu \rceil$ и розобьём 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 μ (соответственно не больше, чем μ) 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

$$f_{\sigma''} = f^{(1)}_{\sigma''} \vee \cdots \vee f^{(p_{\sigma''})}_{\sigma''} \tag{10.5}$$

и поэтому её доопределением является ФАЛ

$$g_{\sigma''} = g^{(1)}_{\sigma''} \vee \cdots \vee g^{(p_{\sigma''})}_{\sigma''}. \tag{10.6}$$

Из (10.3)–(10.6) следует, что ФАЛ $g(x)$ вида

$$g(x) = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''} \Bigg(\bigvee_{i=1}^{p_{\sigma''}} g^{(i)}_{\sigma''}(x') \Bigg), \tag{10.7}$$

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 (10.7) можно построить СФЭ Σ, которая реализует ФАЛ g со сложностью

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

Из последнего неравенства при

$$q = \lceil n - \log t + 2\log n \rceil, \qquad \mu = \lceil \log t - 4q - 2\log n \rceil$$

получаем требуемую оценку

$$L^{\mathrm{C}}(g) \lesssim \frac{t}{\log t}.$$

Лемма доказана. □

Замечание. Из леммы 10.2 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 8.1 отсюда следует, что

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

в то время как

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

Введём некоторые понятия и рассмотрим связанные с ними конструкции, позволяющие ослабить условия леммы 10.2.

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 10.3. *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 $r \leqslant t(t-1)/2$.

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 10.4. *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

$$s \leqslant n, \qquad s \sim \log t, \qquad nt\log t = o(2^s). \tag{10.8}$$

Возьмём произвольную фунцию f, $f \in \widehat{P}_2(n,t)$, и пусть $A = \delta(f)$, $|A| = t$. Построим по лемме 10.3 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 (10.8) $t' \sim t$, $s \sim \log t'$, 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 10.2. Найдём по этому утверждению такое доопределение $\widetilde{g}'(y)$ ФАЛ $\widetilde{f}'(y)$, для которого

$$L^{\mathrm{C}}(\widetilde{g}') \lesssim \frac{t'}{\log t'} \sim \frac{t}{\log t}. \tag{10.9}$$

Легко видеть, что ФАЛ вида

$$g(x) = \widetilde{g}'(\psi(x)) \cdot \overline{\chi}''(x) \vee g''(x), \tag{10.10}$$

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 (10.8) вытекает оценка

$$L^{\mathrm{C}}(\chi'') + L^{\mathrm{C}}(g'') + L^{\mathrm{C}}(\psi) = o(t/\log t). \tag{10.11}$$

Таким образом, реализуя ФАЛ $g(x)$ в соответствии с (10.10) и учитывая (10.9), (10.11), получим

$$L^{\mathrm{C}}(f) \lesssim \frac{t}{\log t}.$$

Лемма доказана. □

Лемма 10.5. *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 10.4, 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 следующий основной результат.

Теорема 10.1. *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 $n \log n = o(t)$ [2].

Глава 2

Синтез схем для индивидуальных функций и оценки их сложности

§1 Средняя проводимость схемы. Асимптотика контактной сложности универсальных систем функций

Использование так называемой средней проводимости контактов схемы позволяет в некоторых случаях получать более высокие по сравнению с леммой 2.3 [3, глава 4] нижние оценки сложности реализации систем ФАЛ в классе $\mathfrak{U}^{\mathrm{K}}$. Этот метод уже применялся, по существу, при доказательстве минимальности контактного дерева в классе разделительных КС (см. лемму 2.5 [3, глава 4]).

Будем называть множество δ, $\delta \subseteq B^n$, *равномерным*, если для каждого i, $i \in [1, n]$, число тех наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$ из δ, у которых $\alpha_i = 1$, равно $\frac{|\delta|}{2}$. Заметим, что каждый контакт КС $\Sigma = \Sigma(\alpha_1, \ldots, \alpha_n)$ проводит (не проводит) ровно на половине всех наборов равномерного множества δ, $\delta \subseteq B^n$, и, следовательно, в обозначениях §§1, 5 [3, глава 2] выполняются равенства

$$\frac{1}{|\delta|} \sum_{\alpha \in \delta} |E(\Sigma|_\alpha)| = \frac{1}{|\delta|} \sum_{\alpha \in \delta} |E(\Sigma|_{\overline{\alpha}})| = \frac{1}{2} L(\Sigma) \tag{1.1}$$

которые и задают «среднюю» проводимость (непроводимость) контактов Σ на наборах множества δ. В качестве множества δ мы, чаще всего, будем выбирать весь единичный куб B^n , а для получения нижних оценок сумм (1.1) — использовать неравенства

$$|E(\Sigma|_\alpha)| \geqslant |V(\Sigma)| - |c(\Sigma|_\alpha)|, \tag{1.2}$$

$$|E(\Sigma|_{\overline{\alpha}})| \geqslant |c(\Sigma|_\alpha)| - |C(\Sigma)|, \tag{1.3}$$

которые вытекают из неравенства (1.2) [3, глава 2]. Напомним, что в [3, глава 4] было доказано следующее утверждение.

Лемма 1.1. *Если система ФАЛ $F = (f_1, \ldots, f_m)$ состоит из попарно различных и отличных от констант ФАЛ от БП $X(n)$, то*

$$L^{\mathrm{K}}(F) \geqslant 2^{1-n} \sum_{j=1}^{m} \left| N_{f_j} \right| .$$

Следствие 1.

$$L^{\mathrm{K}}(J_n) \geqslant 2^{n+1} - 2$$

Следствие 2. *Оценки следствия 1 и леммы 7.3 из [3, глава 4] дают асимптотическое равенство*

$$L^{\mathrm{K}}(\overrightarrow{J}_n) \sim 2^{n+1}$$

Теорема 1.1. *Для любого множества ФАЛ Q, $Q \subseteq P_2(n)$, и любого натурального r, $r \leqslant n$, справедливо неравенство*

$$L^{\mathrm{K}}(\overrightarrow{Q}) \geqslant 2|Q|\left(1 - \frac{5}{\sqrt{r}}\right) - 2|\widehat{Q}|, \tag{1.4}$$

где множество $\widehat{Q}$ состоит из тех ФАЛ f, $f \in Q$, у которых во множестве $\overline{N}_f$ есть грани размерности больше, чем $(n-r)$.

Доказательство. Пусть Σ — минимальная приведённая $(1, |Q|)$–КС, реализующая систему ФАЛ $\overrightarrow{Q}$, и пусть V — множество её выходных вершин. Пусть, далее, s и t — натуральные параметры, для которых $(s-1)(t-1) \leqslant r$, а V' — множество тех выходных вершин Σ, степень которых не меньше, чем s. Достаточно рассмотреть случай, когда

$$|V'| \leqslant 4\frac{|Q|}{s}, \tag{1.5}$$

так как иначе число контактов Σ инцидентных вершинам из V' уже было бы не меньше, чем $2|Q|$.

Для произвольного набора α, $\alpha \in B^n$, множество $c(\alpha)$ связанных компонент сети $\Sigma|_\alpha$ разобьём на непересекающиеся подмножества $c_i(\alpha)$, $i \in [1, 4]$, так, что связная компонента G, $G \in c(\alpha)$, входит в подмножество:

1. $c_1(\alpha)$, если $V(G) \nsubseteq V$;
2. $c_2(\alpha)$, если $G \notin c_1(\alpha)$ и $V(G) \cap V' \neq \varnothing$;
3. $c_3(\alpha)$, если $G \notin (c_1(\alpha) \cup c_2(\alpha))$ и $|V(G)| \geqslant t$;
4. $c_4(\alpha)$ в остальных случаях.

Заметим, что произвольная связная компонента G из $c_i(\alpha)$ удовлетворяет неравенству

$$|E(G)| \geqslant |V \cap V(G)|, \tag{1.6}$$

если $i = 1$ и состоит только из выходных вершин Σ в остальных случаях. При этом в случае $i = 2$ она содержит хотя бы одну вершину из V', в случае $i = 3$ — состоит не менее, чем из t вершин, а в случае $i = 4$ включает в себя не более $(t-1)$ вершин, которые отделяются от остальных вершин сети $\Sigma|_\alpha$ сечением, состоящим не более,

чем из $(s-1)(t-1) \leqslant r$, контактов множества $E|\Sigma|_{\overline{\alpha}}|$. Таким образом, в каждой вершине компоненты G из множества $c_4(\alpha)$ реализуется ФАЛ из множества $\widehat{Q}$, и, учитывая все вышесказанное, получим

$$|c_2(\alpha)| \leqslant |V'|, \quad |c_3(\alpha)| \leqslant \frac{|Q|}{t}, \quad |c_4(\alpha)| \leqslant |\widehat{Q}|. \tag{1.7}$$

Из (1.5)–(1.7) в силу (1.2) вытекает неравенство

$$|E(\Sigma|_\alpha)| \geqslant |Q| - \frac{4|Q|}{s} - \frac{|Q|}{t} - |\widehat{Q}|,$$

из которого в соответсвии с 1.1 при $\delta = B^n$ и $s = t = \lceil \sqrt{r} \rceil$ следует (1.4).

Теорема доказана. □

Следствие 1. *Полагая $Q = P_2(n)$ и учитывая то, что при $r = \left\lceil \frac{n}{2} \right\rceil$ множество $\widehat{Q} = \widehat{P}_2(n)$ удовлетворяет соотношению $\left|\widehat{P}_2(n)\right| = o\big(2^{2^n}/\sqrt{n}\big)$, получим*

$$L^{\mathrm{K}}\big(\overrightarrow{P}_2(n)\big) \geqslant 2 \cdot 2^{2^n} \left(1 - O\left(\frac{1}{\sqrt{n}}\right)\right).$$

Следствие 2. *Оценки следствия 1 и леммы 3.1 из[3, глава 4] дают асимптотическое неравенство*

$$L^{\mathrm{K}}\big(\overrightarrow{P}_2(n)\big) \sim 2 \cdot 2^{2^n}.$$

§2 Забивание переменных константами. Сложность линейной функции в классе схем из функциональных элементов

Определим сначала операцию подстановки констант вместо переменных в функции и схемы. Будем считать, что любая ЭК K ранга r от БП $X(n)$ вида $K = x_{i_1}^{\sigma_1} \dots x_{i_r}^{\sigma_r}$ задаёт подстановку констант $x_{i_1} = \sigma_1, \dots, x_{i_r} = \sigma_r$. Результат применения указанной подстановки к системе ФАЛ F, $F \in P_2^m(n)$, и схеме Σ от БП $X(n)$ будем обозначать через $F|_K$ и $\Sigma|_K$ соответственно. При этом система ФАЛ $F|_K$ определяется обычным образом, а преобразование схемы Σ в схему $\Sigma|_K$ в классе $\mathcal{U}^{\mathrm{C}}$ ($\mathcal{U}^{\mathrm{K}}$) связано с заменой вершин x_{i_j}, $j = 1, \dots, r$, константой σ_j и применением, до тех пор, пока это возможно, тождеств подстановки констант из §§ 1–2 [3, глава 3] (соответственно отождествлением концевых вершин контактов вида $x_{i_j}^{\sigma_j}$ и удалением контактов вида $x_{i_j}^{\overline{\sigma}_j}$, $j = 1, \dots, r$) с последующим переходом к эквивалентной приведённой схеме. Заметим, что

$$K \cdot f = K \cdot f|_K$$

для любой ФАЛ f и что схема $\Sigma|_K$ реализует систему ФАЛ $F|_K$, если схема Σ реализует систему ФАЛ F. Заметим также, что для КС Σ от БП $X(n)$ и набора

$\alpha = (\alpha_1, \ldots, \alpha_n)$ схема $\Sigma|_{x_1^{\alpha_1} \ldots x_n^{\alpha_n}}$ в отличие от сети $\Sigma|_\alpha$ (см. §§ 1,5 из [3, глава 2]) состоит из (кратных) изолированных полюсов.

Те СФЭ из класса $\mathcal{U}^{\mathrm{C}}$, которые реализуют линейные ФАЛ l_n или $\bar{l}_n$, будем называть *линейными схемами порядка* n. Положим

$$\mathcal{L}(n) = \min\{L^{\mathrm{C}}(l_n),\ L^{\mathrm{C}}(\bar{l}_n)\},$$

а линейные СФЭ порядка n и сложности $\mathcal{L}(n)$ будем называть *минимальными* линейными СФЭ. Из [3] (см. лемму 3.1 гл. 4) следует, что если $n \geqslant 2$, то

$$\mathcal{L}(n) \leqslant \min\{L^{\mathrm{C}}(l_n),\ L^{\mathrm{C}}(\bar{l}_n)\} \leqslant 4n - 4, \tag{2.1}$$

а из теоремы 3.1 в силу незабиваемости множества всех БП линейной ФАЛ вытекает, что

$$\mathcal{L}(n) \geqslant 2n - 2.$$

Докажем, что верхняя оценка (2.1) даёт точные значения сложностей $L^{\mathrm{C}}(l_n)$ и $L^{\mathrm{C}}(\bar{l}_n)$.

Лемма 2.1. *Пусть Σ — линейная СФЭ порядка n от БП $X(n)$ и пусть её БП x_i поступает только на вход ФЭ $\mathcal{E}$ СФЭ Σ, связанного с вершиной v. Тогда в случае $\mathcal{E} = \&$ ($\mathcal{E} = \vee$) на второй вход ФЭ $\mathcal{E}$ поступает ФАЛ 1 (соответственно 0), а в случае $\mathcal{E} = \neg$ СФЭ Σ', которая получается из Σ удалением $\mathcal{E}$ и объявлением v входной вершиной БП x_i, также является линейной СФЭ порядка n.*

Доказательство. Из свойств линейной ФАЛ следует, что СФЭ Σ' отрицание той ФАЛ, которую реализует СФЭ Σ, и потому СФЭ Σ' тоже является линейной СФЭ порядка n.

Пусть теперь $\mathcal{E}$ — двухвходовой ФЭ, который соответствует ФАЛ $\varphi(y_1,\ y_2)$, и пусть на второй вход $\mathcal{E}$ поступает дуга из вершины w. При этом ФАЛ g, которая реализуется в вершине w, не зависит, очевидно, от БП x_i. Предположим, что $g \not\equiv \overline{\sigma}$, где $\sigma = 0$ в случае $\varphi = y_1 \cdot y_2$ и $\sigma = 1$ в случае $\varphi = y_1 \vee y_2$, то есть $g|_K = \sigma$ для некоторой ЭК K вида $x_1^{\alpha_1} \ldots x_{i-1}^{\alpha_{i-1}} x_{i+1}^{\alpha_{i+1}} \ldots x_n^{\alpha_n}$. Тогда в силу особенностей структуры СФЭ Σ и в силу тождества $\varphi(\sigma,\ x_i) = \sigma$ СФЭ $\Sigma|_K$ реализует константу, что противоречит линейности Σ.

Лемма доказана. □

Следствие 1. *Степень любого входа минимальной линейной СФЭ порядка n, $n \geqslant 2$, не меньше двух.*

Следствие 2. *Справедливы равенства*

$$\mathcal{L}(2) = L^{\mathrm{C}}(l_2) = L^{\mathrm{C}}(\bar{l}_2) = 4. \tag{2.2}$$

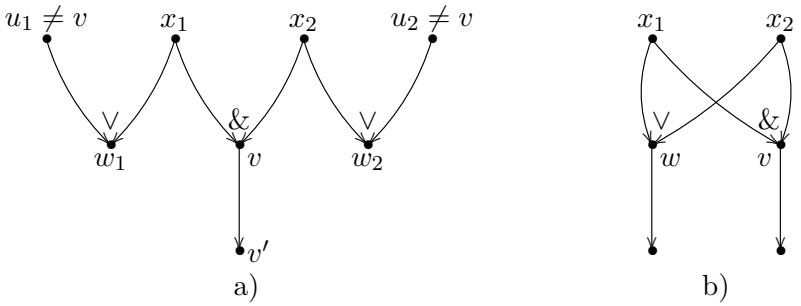

Рис. 2.1:

Действительно, в соответствии со следствием 1 ранг любой линейной СФЭ порядка 2 не меньше четырех. Поэтому в силу того, что в Σ есть хотя бы один ФЭ $\neg$, справедливо неравенство $L(\Sigma) \geqslant 4$, из которого в соответствии с (2.1) вытекает (2.2).

Теорема 2.1. *Для любого натурального n, $n \geqslant 2$, выполняются равенства*

$$\mathcal{L}(n) = L^{\mathrm{C}}(l_n) = L^{\mathrm{C}}(\bar{l}_n) = 4n - 4. \tag{2.3}$$

Доказательство. В силу (2.1) для доказательства (2.3) достаточно убедиться в том, что

$$\mathcal{L}(n) \geqslant 4n - 4. \tag{2.4}$$

Установим справедливость (2.4) индукцией по n, $n = 2, 3, \ldots$.

При $n = 2$ неравенство (2.4) выполняется в силу (2.2), что составляет базис рассматриваемой индукции. Для обоснования индуктивного перехода возьмем произвольную минимальную линейную СФЭ Σ порядка n, $n \geqslant 3$, от БП $X(n)$ и покажем, что для некоторых i, $i \in [1, n]$, и σ, $\sigma \in B$, выполняется неравенство

$$L(\Sigma) \geqslant L(\Sigma|_{x_i^\sigma}) + 4. \tag{2.5}$$

Будем считать, что на каждом шаге преобразования СФЭ Σ в СФЭ $\Sigma''_{i,\sigma} = \Sigma|_{x_i^\sigma}$ удаляется один ФЭ $\mathcal{E}$ с константой на входе. При этом вершина, с которой связан ФЭ $\mathcal{E}$, обьявляется константной входной вершиной типа σ новой схемы, если на выходе $\mathcal{E}$ реализуется константа σ, $\sigma \in B$, и удаляется вместе с $\mathcal{E}$ в остальных случаях. Заметим, что для любой промежуточной схемы Σ' указанного преобразования выполняется неравенство

$$L(\Sigma''_{i,\sigma}) \leqslant L(\Sigma') - \mathrm{IC}(\Sigma'), \tag{2.6}$$

где $\mathrm{IC}(\Sigma')$ — число дуг Σ', исходящих из её константных входов. Будем предполагать также, что в любой вершине СФЭ $\Sigma''_{i,\sigma}$ реализуется неконстантная ФАЛ.

Полустепень исхода, то есть число исходящих дуг вершины v СФЭ Σ будем обозначать через $d^+(v)$, а число исходящих из v дуг, которые ведут в вершины, связанные с ФЭ типа Φ, $\Phi \subseteq Б_0$, — через $d^+_\Phi(v)$. Заметим, что для любой вершины v СФЭ Σ и для любого любого i, $i \in [1, n]$, выполняются неравенства

$$d^+_\neg(v) \leqslant 1, \qquad d^+(x_i) = d^+_\&(x_i) + d^+_\vee(x_i) + d^+_\neg(x_i) \geqslant 2, \tag{2.7}$$

первое из которых вытекает непосредственно из минимальности Σ, а второе — из следствия 1 леммы 2.1. Нетрудно убедиться в том, что неравенство (2.5) выполняется в следующих случаях:

1. $d^+(x_i) \geqslant 4$ — при любом σ;
2. $d^+_\&(x_i) \geqslant 2$ или $d^+_\&(x_i) = d^+_\neg(x_i) = 1$ — при $\sigma = 0$;
3. $d^+_\vee(x_i) \geqslant 2$ или $d^+_\vee(x_i) = d^+_\neg(x_i) = 1$ — при $\sigma = 1$.

Действительно, в каждом из этих случаев СФЭ Σ', которая получается при переходе от СФЭ Σ к СФЭ $\Sigma''_{i,\sigma}$ в результате удаления $d^+(x_i)$ ФЭ, связанных с входом x_i, имеет при $d^+(x_i) < 4$ не меньше, чем $(4 - d^+(x_i))$, константных входных дуг и, следовательно, в силу (2.6) выполняется (2.5).

Таким образом, с учётом (2.7) осталось рассмотреть основной случай — случай, когда $d^+_\&(x_i) = d^+_\vee(x_i) = 1$ и $d^+_\neg(x_i) = 0$ для каждого i, $i \in [1, n]$. В этом случае в СФЭ Σ найдутся два входа, связанные с одним и тем же ФЭ типа & или $\vee$. Пусть для определённости, данными входами Σ будут БП x_1 и x_2, котороые поступают на входы одного и того же ФЭ &, связанного с вершиной v. Пусть при этом вторая дуга, исходящая из вершины x_i, $i = 1, 2$, идёт в вершину w_i, связанную с ФЭ $\vee$, на другой вход которого поступает дуга из вершины u_i. Заметим, что в силу минимальности Σ для любого i, $i = 1, 2$, вершина u_i отлична от вершины v, так как при $v = u_i$ в вершине w_i реализуется ФАЛ x_i.

Покажем, что в случае $w_1 \neq w_2$ неравенство (2.5) выполняется. Действительно,рассмотрим в этом случае СФЭ Σ', которая пролучается при переходе от СФЭ Σ к СФЭ $\Sigma''_{1,0}$ в результате удаления двух ФЭ, связанных с вершинами w_1 и v, а также одного ФЭ, связанного с какой-либо вершиной v', в котороую идет дуга из v. Так как $u_2 \neq v$ и, следовательно, $v' \neq w_2$, то вход x_2 схемы Σ' поступает только на вход ФЭ $\vee$, связанного с вершиной w_2. Из леммы 2.1 вытекает, что при этом в вершине u_2 СФЭ Σ' реализуется ФАЛ 0, то есть при переходе от Σ' к $\Sigma''_{1,0}$ ещё один ФЭ — ФЭ $\vee$, связанный с вершиной w_2, — будет удалён. Неравенство (2.5) в случае $w_1 \neq w_2$ доказано.

Пусть, наконец, $w_1 = w_2$ и, следовательно, $x_1 = u_2$, $x_2 = u_1$ и пусть, для определённости, либо $d^+(v) \geqslant 2$, либо $d^+(v) = d^+(w) = 1$ и $d^+_{\&,\vee}(v) \geqslant d^+_{\vee,\neg}(w)$. Рассмотрим СФЭ Σ', которая получается при переходе от СФЭ Σ к СФЭ $\Sigma''_{1,0}$ в результате удаления двух ФЭ, связанных с вершинами v и w, а также всех тех ФЭ, входы коорых присоединены к v (число таких ФЭ равно $d^+(v)$). Заметим, что в случае

$d^+(v) \geqslant 2$ неравенство (2.5) вытекает из неравенства $L(\Sigma) - L(\Sigma') \geqslant 4$, а в случае $d^+(v) = d^+_{\&,\vee}(v) = 1$ — из неравенства $L(\Sigma) = L(\Sigma') + 3$ и неравенства (2.6), где $\mathrm{IC}(\Sigma) \geqslant 1$. В оставшемся случае $d^+(v) = d^+_{\vee}(v) = d^+(w) = d^+_{\&}(w) = 1$ из вершины v (w) исходит единственная дуга, ведущая в вершину v' (соответственно w'), связанную с ФЭ $\vee$ (соответственно &). В этом случае СФЭ Σ' имеет в вершине w_2 вход x_2 степени 1, поступающий на вход ФЭ &, и, следовательно, в силу леммы 2.1 удовлетворяет неравенству $L(\Sigma') - L(\Sigma''_{1,0}) \geqslant 1$, из которого, с учётом равенства $L(\Sigma) - L(\Sigma') = 3$, вытекает (2.5).

Теорема доказана. □

§3 Незабиваемые множества переменных. Асимптотика сложности мультиплексора в некоторых классах схем

Будем говорить, что подмножество U множества X, состоящего из всех БП ФАЛ f, *забивает* БП x, $x \in X \setminus U$, этой ФАЛ, если существует ЭК K от БП U такая, что ФАЛ $f|_K$ не зависит существенно от x. При этом будем считать, по определению, что пустое множество $U = \varnothing$ забивает любую несущественную БП ФАЛ f и не забивает её существенные БП. Непустое подмножество Y множества БП ФАЛ f называется *незабиваемым множеством переменных* этой ФАЛ, если для любой БП y, $y \in Y$, множество $Y \setminus \{y\}$ не забивает y. Заметим, что если Y — незабиваемое множество БП ФАЛ f, то:

1. любая БП из Y является существенной БП ФАЛ f;

2. для любой ЭК K от БП Y множество её несущественных БП является незабиваемым множеством БП ФАЛ $f|_K$. Заметим также, что примером незабиваемого множества БП является множество всех существенных (информационных) БП линейной (соответственно мультиплексорной) ФАЛ.

Теорема 3.1. *Если ФАЛ f имеет незабиваемое множество, состоящее из n её БП, то*

$$L^{\mathrm{C}}(f) \geqslant 2n - 2, \qquad L^{\mathrm{K}}(f) \geqslant 2n - 1 \tag{3.1}$$

Доказательство. Первое из равенств (3.1) докажем индукцией по n, $n = 1, 2, \ldots$. При $n = 1$ это неравенство, очевидно, выполняется. Пусть оно верно для любой ФАЛ f', которая имеет незабиваемое множество, состоящее из n', $n' \leqslant (n-1)$, её БП, и пусть $Y = \{y_1, \ldots, y_n\}$ — незабиваемое множество БП ФАЛ f, где $n \geqslant 2$.

Возьмём миниимальную приведённую СФЭ Σ в базисе $\mathrm{Б}_0$, которая реализует ФАЛ f со сложностью $L^{\mathrm{C}}(f)$. В силу существенной зависимости ФАЛ f от БП y_1 в СФЭ имеется цепь из последовательно соединённых вершин $v_1, \ldots, v_t$, где v_1 — вход y_1 СФЭ Σ, а v_t — выход Σ. При этом в вершине v_1 реализуется ФАЛ y_1 и, так как $f \neq y_1$, то, следовательно, $t \geqslant 2$. Для $\sigma_1 \in B$ и $\sigma_1 = 0$ тогда и только тогда, когда вершина v_2 связана с ФЭ &, рассмотрим СФЭ $\Sigma' = \Sigma|_{y_1^{\sigma_1}}$ и реализуемую

ею ФАЛ $f' = f|_{y_1^{\sigma_1}}$, которая имеет незабиваемое множество БП $Y' = Y \setminus \{y_1\}$ и поэтому отлична от констант.

Заметим, что в вершинах v_1 и v_2 СФЭ Σ при $y_1 = \sigma_1$ реализуются константы σ_1 и σ_2 соответственно, а так как $f' \neq \sigma_2$, то значит $t \geqslant 3$. При этом константа σ_2 из вершины v_2 поступает на вход ФЭ вершины v_3 и, следовательно, при переходе от СФЭ Σ к СФЭ Σ' элементы, связанные с вершинами v_2 и v_3 будут устранены («забиты»). Таким образом, выполняются неравенства

$$L^{\mathrm{C}}(f) = L(\Sigma) \geqslant L(\Sigma') + 2 \geqslant L^{\mathrm{C}}(f') + 2,$$

которые устанавливают справедливость рассматриваемого индуктивного перехода и доказывают первое из равенств (3.1).

Докажем теперь второе из равенств (3.1). Пусть, по-прежнему, $Y = \{y_1, \ldots, y_n\}$ — незабиваемое множество БП ФАЛ f и пусть Σ — минимальная приведённая $(1,1)$–КС, реализующая ФАЛ f со сложностью $L(\Sigma) = L^{\mathrm{K}}(f)$. Если каждая из БП y_i, $i \in [1,n]$, имеет в КС Σ не менее двух контактов, то второе неравенство (3.1), очевидно, выполняется. Таким образом, достаточно рассмотреть случай, когда множество Y', состоящее из тех БП y_i, $i \in [1,n]$, которым в Σ соответствует ровно один контакт, не пусто. Пусть, для определённости, $Y' = \{y_1, \ldots, y_m\}$, $1 \leqslant m \leqslant n$, и пусть каждая из БП y_i, $i \in [1,m]$, имеет в Σ только один замыкающий контакт (это предположение не ограничивает, очевидно, общности рассуждений).

Рассмотрим КС $\Sigma' = \Sigma|_{\overline{y}_{m+1} \cdot \ldots \cdot \overline{y}_n}$, которая реализует ФАЛ $f' = f|_{\overline{y}_{m+1} \cdot \ldots \cdot \overline{y}_n}$ с незабиваемым множеством БП Y' и для которой в силу выбора Y' выполняется неравенство

$$L(\Sigma') \leqslant L(\Sigma) - 2(n-m). \tag{3.2}$$

Схема Σ' по построению является связным графом и для каждого i, $i \in [1,m]$, содержит ровно один (замыкающий) контакт БП y_i. Пусть, далее, КС Σ'' является остовной подсхемой КС Σ', содержащей все контакты БП Y' и только их, а остовная подсхема $\overline{\Sigma}''$ схемы Σ' служит дополнением Σ'', то есть $\overline{\Sigma}'' = \Sigma' \setminus \Sigma''$.

Покажем, что в КС Σ'' нет циклов, то есть Σ'' представляет собой систему деревьев, и что $|c(\overline{\Sigma}'')| \leqslant 2$. Действительно, если бы в КС Σ'' контакт БП y', $y' \in Y'$, принадлежал циклу, то множество БП $Y' \setminus \{y'\}$ при подстановке константы 1 забивало бы БП y' в КС Σ', что противоречит незабиваемости множества БП Y' ФАЛ f'. Аналогичное противоречие в случае $|c(\overline{\Sigma}'')| \geqslant 3$ связано с тем, что при этом в Σ' найдётся контакт БП y', $y' \in Y'$, соединяющий между собой две различные компоненты $\overline{\Sigma}''$, одна из которых не содержит полюсов Σ, и, следовательно, множество БП $Y' \setminus \{y'\}$ вновь забивает БП y' при подстановке константы 0.

Учитывая установлённые свойства схем Σ'' и $\overline{\Sigma}''$, а также соотношения (1.2) и (1.3) из [3, глава 2], получим:

$$L(\overline{\Sigma}'') + 2 \geqslant |V(\overline{\Sigma}'')| = |V(\Sigma')| = |V(\Sigma'')| \geqslant m + 1.$$

Следовательно, выполняется неравенство

$$L(\Sigma') = L(\overline{\Sigma}'') + m \geqslant 2m - 1,$$

из которого, в силу (3.2) вытекает второе неравенство (3.1).

Теорема доказана. □

Следствие.

$$L^{\mathrm{C}(\mu_n)} \geqslant 2^{n+1} - 2, \qquad L^{\mathrm{K}}(\mu_n) \geqslant 2^{n+1} - 1.$$

Установим теперь верхние оценки сложности реализации мультиплексорной ФАЛ μ_n в классах схем $\mathcal{U}^{\mathrm{C}}$, $\mathcal{U}^{\Phi}$, $\mathcal{U}^{\mathrm{K}}$, $\mathcal{U}^{\overrightarrow{\mathrm{K}}}$.

Теорема 3.2. *Для $n = 1, 2, \ldots$ справедливы неравенства:*

$$L^{\mathrm{C}}(\mu_n) \leqslant L^{\Phi}(\mu_n) \leqslant 2^{n+1} + O\big(2^{\frac{n}{2}}\big), \tag{3.3}$$

$$L^{\mathrm{K}}(\mu_n) \leqslant 2^{n+1} + O\big(2^n/\sqrt{n}\big), \tag{3.4}$$

$$L^{\overrightarrow{\mathrm{K}}}(\mu_n) \leqslant 2^n + O\big(2^{\frac{n}{2}}\big). \tag{3.5}$$

Доказательство. Построим в классе $\mathcal{U}^{\mathrm{C}}$ схемный мультиплексор Σ_n порядка n, сложность которого даёт оценку (3.3) для $L^{\mathrm{C}}(\mu_n)$, следующим образом:

1. разобьём набор БП $X(n)$ на группы $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$, где $q = \lceil n/2 \rceil$, а набор БП $y = (y_0, \ldots, y_{2^n-1})$ — на 2^q последовательных наборов $y^{(0)}, \ldots, y^{(2^q-1)}$ длины 2^{n-q} каждый;

2. возьмём дешифраторы Σ' и Σ'' от БП x' и x'' порядка q и $n-q$, построенные по лемме ? главы ?;

3. построим схему $\widehat{\Sigma}''$, которая содержит дешифратор Σ'' в качестве подсхемы и для каждого σ'', $\sigma'' \in B^{n-q}$, на выходе z_j, где $j = \nu(\sigma'')$, реализует ФАЛ $\mu_{n-q}(x'', z^{(j)})$ по её сокращённой ДНФ, используя для этого 2^{n-q} ФЭ & и $(2^{n-q} - 1)$ ФЭ $\vee$;

4. искомая схема Σ_n содержит СФЭ Σ' и $\widehat{\Sigma}''$ в качестве подсхем и реализует ФАЛ $\mu_n(x', x'', y) = \mu_q(x', z_0, \ldots, z_{2^q-1})$ на основе сокращённой ДНФ μ_q, используя для этого 2^q ФЭ & и $(2^q - 1)$ ФЭ $\vee$.

Оценка (3.4) достигается на контактном мультиплексоре $\widehat{\Sigma}_n$ порядка n, который получается в результате стыковки асимптотически наилучшего контактного дешифратора $\Sigma_n^{(\&)}$ порядка n (см. лемму 7.2 из [3, глава 4]) с $(2^n, 1)$–контактной звездой из 2^n контактов БП $y_0, \ldots, y_{2^n-1}$ (см. рис. 5.7 в [3, глава 2]).

Аналогичным образом можно построить π–схему $\widetilde{\Sigma}_n$, которая реализует ФАЛ μ_n со сложностью $L(\widetilde{\Sigma}_n) \sim 2^{n+1}$ и содержит $o(2^n)$ размыкающих контактов. Для этого достаточно (см. доказательство леммы 7.2 из [3, глава 4]) каждую

из характеристических ФАЛ $\chi_1, \ldots, \chi_{2^p}$ реализовать соответствующей канонической π–схемой. Кроме того, для построения m–регулярного разбиения единичного куба от БП $x' = (x_1, \ldots, x_q)$, на компонентах которого ЭК от БП x' моделируются, как правило, с помощью БП, а не их отрицаниями, достаточно использовать технику [**?**]. Искомая формула, удовлетворяющая (3.3), получается моделированием π–схемы $\widetilde{\Sigma}_n$.

Контактный мультиплексор $\check{\Sigma}$ порядка n из ориентированных контактов, сложность которого даёт оценку (3.5) имеет вид $\check{\Sigma} = \Sigma''(\Sigma')$, где для $q = \lceil n/2 \rceil$ Σ' и Σ'' — $(1, 2^q)$– и $(2^{n-q}, 1)$–контактные деревья от БП $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$ соответственно, построенные из контактов, ориентированных от входов к выходам. При этом каждый выход $z_{\nu(\sigma')}$, где $\sigma' = (\sigma_1, \ldots, \sigma_q) \in B^q$ КС Σ', на котором реализуется ЭК $K' = x_1^{\sigma_1} \ldots x_q^{\sigma_q}$, соединяется с каждым входом $u_{\nu(\sigma'')}$, где $\sigma'' = (\sigma_{q+1}, \ldots, \sigma_n) \in B^{n-q}$, КС Σ'', для которого функция проводимости от $u_{\nu(\sigma'')}$ к выходу Σ'' равна $K'' = x_{q+1}^{\sigma_{q+1}} \ldots x_n^{\sigma_n}$, контактом БП $y_{\nu(\sigma', \sigma'')}$, ориентированным по направлению от $z_{\nu(\sigma')}$ к $u_{\nu(\sigma'')}$.

Теорема доказана. □

§4 Сферические функции. Сложность линейной и других функций в классе контактных схем и самокорректирующихся контактных схем

Функцию f из $P_2(n)$ будем называть *α–сферической*, где $\alpha \in B^n$, если для любых наборов β и γ из B^n, отличающихся от α ровно в одном и ровно в двух разрядах соответственно, $f(\beta) = 0$ и $f(\gamma) = 1$. При этом $\tilde{0}$–сферическую ФАЛ, будем называть просто сферической. Пусть s_n^i, где $0 \leqslant i \leqslant n$, — элементарная симметрическая ФАЛ с рабочим числом i, то есть ФАЛ от БП $x_1, \ldots, x_n$, обращающаяся в 1 на всех тех наборах, которые содержат ровно i единиц. Заметим, что ФАЛ s_3^2 является сферической, а ФАЛ s_3^1 — $\tilde{1}$–сферической и что ФАЛ $\bar{l}_n$ (l_n) является α–сферической для всех наборов α из множества $B^n_{\text{чёт.}}$ $(B^n_{\text{неч.}})$, содержащего все наборы B^n с чётным (соответственно нечётным) числом единиц.

Наряду с КС из «обычных» (абсолютно надёжных) контактов будем рассматривать КС из ненадёжных контактов, которые могут выходить из строя в результате *обрыва*, когда ФАЛ проводимости контакта становится равной 0 или *замыкания*, когда эта ФАЛ становится равной 1. Будем говорить, что КС Σ *корректирует p, $p \geqslant 0$, обрывов и q, $q \geqslant 0$, замыканий, если она эквивалентна любой КС, получающейся из Σ в результате обрыва не более чем p, и замыкания не более чем q контактов.*

Лемма 4.1. *Если КС Σ реализует сферическую ФАЛ f из $P_2(n)$, то в Σ встречаются замыкающие контакты всех БП $x_1, \ldots, x_n$, причём контакты всех этих типов, за исключением, быть может, двух, встречаются в ней не менее двух раз.*

Доказательство. Из сферичности ФАЛ f следует, что она существенно зависит от всех своих БП и не является антимонотонной ни по одной из них. Следовательно, в Σ имеются замыкающие контакты всех БП $x_1, \ldots, x_n$. Обозначим через a_1 и a_2 полюса КС Σ, а через E_1 (E_2) — множество тех её контактов, каждый из которых является первым (соответственно последним) замыкающим контактом для какой-либо проводящей цепи КС Σ идущей от a_1 к a_2.

Докажем, сначала, что $E_1 \cap E_2 = \varnothing$. Действительно, пусть $E_1 \cap E_2 \neq \varnothing$ и поэтому в КС Σ имеется контакт K вида x_i, $1 \leqslant i \leqslant n$, который является первым (последним) замыкающим контактом проводящей цепи C_1 (соответственно C_2), идущей от a_1 к a_2. Для $j = 1, 2$ обозначим через C'_j и C''_j начальную (до контакта K) и заключительную (после контакта K) подцепи цепи C_j. Пусть, далее, цепь C состоит из начальной подцепи C'_1, контакта K и заключительной подцепи C''_2, если цепи C_1 и C_2 проходят контакт K в одном направлении и состоит из начальной подцепи C'_1, которая сразу переходит в заключительную подцепь C''_2 в противном случае. Заметим, что подцепи C'_1 и C''_2 по построению состоят только из размыкающих контактов, среди которых нет контактов вида $\overline{x}_i$ и поэтому цепь C будет проводить на наборе

$$\beta = (\underbrace{0, \ldots, 0}_{i}, 1, 0, \ldots, 0),$$

что противоречит сферичности ФАЛ f.

Докажем теперь, что каждое из множеств E_s, $s = 1, 2$, содержит замыкающие контакты всех БП $x_1, \ldots, x_n$ за исключением, быть может, одной. Действительно, из сферичности ФАЛ f следует, что для любых i и j, $1 \leqslant i < j \leqslant n$, в КС Σ имеется цепь C, идущая из a_1 в a_2, которая проводит на наборе

$$\gamma = (\underbrace{0, \ldots, 0, 1}_{i}, 0, \ldots 0, \underbrace{1, 0, \ldots, 0}_{n-j+1})$$

и состоит из замыкающих контактов БП x_i, x_j, а также размыкающих контактов остальных БП. Заметим, что в C не могут отсутствовать замыкающие контакты ни одной из БП x_i, x_j, так как иначе ФАЛ f обращалась бы в 1 на некотором наборе β, содержащем ровно одну 1. Следовательно, первый из контактов вида x_i, x_j на цепи C войдёт в E_1, а последний — в E_2 и поэтому как в E_1, так и в E_2 контакты вида x_i, x_j не могут отсутвствовать одновременно. Таким образом, во множестве $E_1 \cup E_2$ не могут отсутствовать замыкающие контакты трёх и более БП.

Лемма доказана. □

Следствие 1. *Если КС Σ реализует α–сферическую ФАЛ f из $P_2(n)$, где $\alpha = (\alpha_1, \ldots, \alpha_n)$, то контакты всех типов $x_1^{\overline{\alpha}_1}, \ldots, x_n^{\overline{\alpha}_n}$ встречаются в Σ по крайней мере $t = 1$ раз, причём контакты всех этих типов за исключением, быть может, двух встречаются в Σ не менее $r = 2$ раз.*

Следствие 2. *Если КС Σ корректирует p, $p \geqslant 0$ обрывов, то в условиях следствия 1 имеем $t \geqslant p+1$ и $r \geqslant 2\lceil (p+1)/2 \rceil$, то есть*

$$L(\Sigma) \geqslant 2(p+1) + 2\left\lceil \frac{p+1}{2} \right\rceil (n-2).$$

Теорема 4.1. *При любом натуральном n имеют место равенства*

$$L^{\mathrm{K}}(s_n^1) = L^{\mathrm{K}}(s_n^{n-1}) = 3n-2,$$

а если $n \geqslant 2$, то

$$L^{\mathrm{K}}(l_n) = L^{\mathrm{K}}(\bar{l}_n) = 4n-4. \tag{4.1}$$

Доказательство. Все необходимые верхние оценки могут быть получены с помощью метода каскадов (см., например, § 3 из [3, гл. 4]).

Пусть КС Σ реализует ФАЛ $f = s_n^{n-1}$. Из того, что ФАЛ s_n^{n-1} не является ни монотонной ни антимонотонной ни по одной из своих БП, следует что в КС Σ встречаются константы всех типов $x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n$. Заметим, что при этом контакты всех типов $x_1, \ldots, x_n$ за исключением, быть может, двух встречаются в Σ не менее двух раз. Действительно, пусть, например, контакты типов x_1, x_2, x_3 встречаются в Σ только по одному разу. Тогда, подставив константу 1 вместо всех БП $x_4, \ldots, x_n$, мы получим КС Σ', которая реализует сферическую ФАЛ s_3^2 и содержит только по одному замыкающему контакту своих БП, что противоречит лемме 4.1. Следовательно,

$$L(\Sigma) \geqslant 3n-2.$$

Случай, когда КС Σ реализует ФАЛ $f = s_n^1$, сводится к рассмотренному случаю инвертированием БП.

Пусть теперь $n \geqslant 2$ и КС Σ реализует ФАЛ $f = l_n$. Из того, что ФАЛ f является α–сферической при любом α из $B^n_{\text{неч.}}$, в силу (1.1) и следствия 1 из леммы 4.1 вытекает неравенство:

$$2^{n-2}L(\Sigma) \geqslant 2^{n-1}(2n-2),$$

из которого следует, что

$$L(\Sigma) \geqslant 4n-4.$$

Случай, когда $f = \bar{l}_n$, рассматривается аналогично.

Теорема доказана. □

Для ФАЛ f и $p \geqslant 0$, $q \geqslant 0$ определим «самокорректирующуюся» сложность $L^{\mathrm{K}}_{(p,q)}(f)$ как минимальную из сложностей тех КС, реализующих ФАЛ f, которые корректируют p обрывов и q замыканий.

Теорема 4.2. *При любоых натуральных p и n, $n \geqslant 2$, имеют место равенства*

$$L^{\mathrm{K}}_{(p,0)}(l_n) = 4(p+1) + 4\left\lceil \frac{p+1}{2} \right\rceil (n-2), \tag{4.2}$$

$$L^{\mathrm{K}}_{(1,1)}(l_n) = 8n. \tag{4.3}$$

Доказательство. Нижняя оценка в (4.2) доказывается аналогично нижней оценке (4.1) с использованием следствия 2 леммы 4.1. Верхнюю оценку (4.2) в случае $p = 1$ даёт схема из [**?**, гл. 3, § 1], которая получается из КС, построенной для линейной ФАЛ по методу каскадов, добавлением 4 контактов. В общем случае $p \geqslant 1$ искомая КС представляет собой результат параллельного соединения $\lceil \lfloor p+1 \rfloor 2 \rceil$ указанных выше самокорректирующихся КС и $((p+1) - 2\lfloor (p+1)/2 \rfloor)$ КС, построенных по методу каскадов.

Верхнюю оценку в (4.3) даёт КС, которая получается в результате последовательного соединения двух упомянутых выше КС для линейной ФАЛ, корректирующих 1 обрыв. Для доказательства нижней оценки заметим, что в силу теоремы о максимальном потоке и минимальном разрезе в КС Σ, которая реализует ФАЛ f и корректирует p обрывов, для любого набора α, $\alpha \in N_f$, существует не менее, чем $(p+1)$ не пересекающихся по контактами проводящих на наборе α цепей, соединяющих полюса Σ. Если при этом $f = l^{\sigma}_n$ и КС Σ корректирует q замыканий, то каждая из указанных цепей иемет длину не меньше чем $(q+1)n$, и следовательно,

$$|E(\Sigma|_{\alpha})| \geqslant (p+1)(q+1)n \tag{4.4}$$

для любого набора α, $\alpha \in N_f$. Из (4.4) в силу (1.1) при $\delta = N_f$ вытекает, что

$$L^{\mathrm{K}}_{(p,q)}(l^{\sigma}_n) \geqslant (p+1)(q+1)n.$$

Теорема доказана. □

§5 Теорема Храпченко. Сложность линейной функции 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 $x^{\sigma_1}_{j_1}, \ldots, x^{\sigma_t}_{j_t}$, положим

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

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. [3, §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 $x^{\alpha_1}_1, \ldots, x^{\alpha_n}_n$, 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 $x^{\overline{\beta}_1}_1, \ldots, x^{\overline{\beta}_n}_n$. Заметим, что множество $S \cap C$, то есть множество общих для S и C контактов не пусто и состоит из контактов вида $x^{\alpha_i}_i$, где $\alpha_i = \beta_i$.

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 5.1. *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 стороению 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:

$$\mathcal{C}(\Sigma_1 \cdot \Sigma_2) = \{\, C \mid C = C_1 \cdot C_2, \text{ где } K(C) \neq 0 \text{ и } C_i \in \mathcal{C}(\Sigma_i),\ i = 1, 2 \,\},$$
$$\mathcal{S}(\Sigma_1 \cdot \Sigma_2) = \mathcal{S}(\Sigma_1) \cup \mathcal{S}(\Sigma_2),$$
$$\mathcal{C}(\Sigma_1 \parallel \Sigma_2) = \mathcal{C}(\Sigma_1) \cup \mathcal{C}(\Sigma_2) \tag{5.1}$$
$$\mathcal{S}(\Sigma_1 \parallel \Sigma_2) = \{\, S \mid S = S_1 \cup S_2, \text{ где } J(S) \neq 1 \text{ и } S_i \in \mathcal{S}(\Sigma_i),\ i = 1, 2 \,\}. \tag{5.2}$$

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 (5.1), (5.2), и устанавливается справедливость индуктивного перехода в случае π–схемы вида $\Sigma_1 \parallel \Sigma_2$.

Лемма доказана. □

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 §1, $L^\pi(f)$ — сложность реализации ФАЛ f в классе $\mathcal{U}^\pi$.

Теорема 5.1. *Для любой ФАЛ f из $P_2(n)$ и любых множеств $\mathcal{N}', \mathcal{N}''$ таких, что $\mathcal{N}' \subseteq N_f$ и $\mathcal{N}'' \subseteq \overline{N}_f$, справедливо неравенство:*

$$L^\pi(f) \geqslant \frac{|\mathcal{R}(\mathcal{N}', \mathcal{N}'')|^2}{|\mathcal{N}'| \cdot |\mathcal{N}''|} \tag{5.3}$$

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 5.1 множество $C_\alpha \cap S_\beta$ состоит из одного контакта вида $x_s^{\alpha_s}$, где $\alpha_s \neq \beta_s$. Рассмотрим следующие множества:

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

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

$$|\mathcal{R}_i| \leqslant |\mathcal{N}'_i| \quad \text{и} \quad |\mathcal{R}_i| \leqslant |\mathcal{N}''_i| \tag{5.4}$$

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 (5.4) 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. □

Теорема 5.2. *При $n \geqslant 1$ для линейной ФАЛ l_n^σ, $\sigma \in \{0, 1\}$, выполнены неравенства*

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

Доказательство. Требуемая нижняя оценка вытекает из (5.3) при $f = l_n^\sigma$ и $\mathcal{N}' = N_f$, $\mathcal{N}'' = \overline{N}_f$ так как в данном случае

$$|\mathcal{N}'| = |\mathcal{N}''| = 2^{n-1}, \qquad |\mathcal{R}(\mathcal{N}', \mathcal{N}'')| = n \cdot 2^{n-1}$$

и поэтому $L^\pi(f) \geqslant n^2$.

При получении верхней 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 $x_{n+1}, \ldots, x_{2^k}$.

Теорема доказана. □

Напомним (см. [?, § 3, 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 3 из леммы 1.1 работы [?],

$$T(l_n^\sigma) = D(l_n^\sigma) \geqslant]2 \log n[$$

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 теоремы 5.2, имеют глубину не более, чем $(2 \log n + 3)$, и потому

$$T(l_n^\sigma) \leqslant 2 \log n + 3.$$

Литература

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

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

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

[4] *Лупанов О. Б.* О сложности реализации функций алгебры логики релейно-контактными схемами // Проблемы кибернетики. Вып. 11. М.: Наука, 1964. С. 25–48.

[5] *Лупанов О. Б.* Об одном подходе к синтезу управляющих систем — принципе локального кодирования. // Проблемы кибернетики. Вып. 14. М.: Наука, 1965. С. 31–110.

[6] *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. М.: МГУ, 1984.

[7] *Нигматулин Р. Г.* Сложность булевых функций. М.: Наука, 1991.

[8] *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.).

[9] *Яблонский С. В.* Надежность управляющих систем. М.: Изд-во МГУ, 1991.

[10] *Кричевский Р. Е.* О сложности параллельно-последовательных контактных схем, реализующих одну последовательность булевых функций. Проблемы кибернетики, вып. 12. М.: Наука, 1964. С. 45-55.

[11] *Ложкин С. А.* Об одном методе получения нижних оценок сложности контактных схем и о некоторых минимальных схемах для линейных функций. Сб. трудов семинара по дискретной математике и ее приложениям. М.: Изд-во механико-математического ф-та МГУ, 1997. С. 113-115.

[12] *Ложкин С. А.* Оценки высокой степени точности для сложности управляющих систем из некоторых классов. Математические вопросы кибернетики, вып. 6 М.: Наука, 1996. С. 189 - 214.

[13] *Ложкин С. А.* О глубине функций алгебры логики в произвольном полном базисе. Вестник МГУ. Математика. Механика, 1996, №2. С. 80-82.

[14] *Ложкин С. А., Кошкин М.* А. О сложности реализации некоторых систем функций алгебры логики контактными многополюсниками. ДАН СССР, т. 298 (1988), №4. С. 807-811.

[15] *Шоломов Л. А.* О реализации недоопределенных булевых функций схемами их функциональных элементов. Проблемы кибернетики, вып. 21. М.: Наука, 1969. С. 215 - 226.