«Дополнительные главы дискретной математики и кибернетики»

Лекторы —
профессор С. С. Марченков,
профессор С. А. Ложкин

Информационная поддержка курса:
http://mk.cs.msu.ru/index.php/Дополнительные_главы_дискретной_математики_и_кибернетики_(2-й_поток,_4_курс)

Осенний семестр 2020–2021 уч. г.
группы 411–419

1. III. Сложность реализации ФАЛ из некоторых классов
   - 26. Задача синтеза схем для ФАЛ из специального класса
   - 27. Теорема о числе инвариантных классов
   - 28. Стандартные классы
   - 29. Ненулевые квазиинвариантные классы
   - 30. Принцип локального кодирования
   - 31. Стандартность некоторых невырожденных классов операторов
   - 32. Синтез схем для не всюду определенных функций
   - 33. Случай «сильной» определенности функций
   - 34. Случай «средней» и «слабой» определенности функций
   - 35. Лемма о цепях и сечениях для π-схем
   - 36. Теорема Храпченко
   - 37. Теорема Дж. Сэвиджа

III. Сложность структурной реализации функций алгебры логики из некоторых классов

III часть курса ДГДМиК продолжает курс ОК (6 семестр) и посвящена задаче синтеза схем для функций алгебры логики (ФАЛ) из специальных классов. Рассмотренные в курсе ОК методы синтеза ориентированы, вообще говоря, на «произвольную» или самую «сложную» ФАЛ, тогда как в реальных задачах схемной реализации встречаются далеко не «случайные» ФАЛ. Кроме того, в реальных задачах чаще всего приходится иметь дело с системами ФАЛ или, иначе, операторами, для которых возможна эффективная совместная реализация.

Целью данного раздела курса ДГДМиК является рассмотрение ряда вопросов, связанных с задачей синтеза схем для ФАЛ (операторов) из специальных классов. Мы рассмотрим общие подходы к решению данной задачи, основанные на ее сведении к задаче синтеза схем для «произвольной» ФАЛ меньшей «размерности» с помощью специального «кодирования». Рассмотрим также эту задачу для некоторых очень «узких» классов ФАЛ, то есть классов, связанных с задачей «индивидуального» синтеза.

Для изучения настоящего раздела необходимо повторить материал III раздела курса ОК, посвященный задаче синтеза и оценкам сложности ФАЛ.

26. Задача синтеза схем для ФАЛ (операторов) из специального класса, нижние мощностные оценки функции Шеннона для их сложности в случае невырожденного (ненулевого, квазиинвариантного) класса

Некоторые определения и обозначения из курса ОК, связанные с задачей синтеза:

$B = \{0, 1\}, B^n = \underbrace{B \times \cdots \times B}_{n} = \{\beta = (\beta_1, \ldots, \beta_n) : \beta_i \in B\}$ — **единичный n-мерный куб**;

отображение $f : B^n \to B$ — **функция алгебры логики (ФАЛ)**;

$\mathfrak{X} = \{x_1, \ldots, x_n, \ldots\}$ — **счетный упоряд. алфавит входных БП**;

$\mathfrak{Z} = \{z_1, \ldots, x_m, \ldots\}$ — **счетный упоряд. алфавит выходных БП**;

$P_2(X)$ — **множество ФАЛ $f(x)$ от конечного множества БП из X, $X \subseteq \mathfrak{X}$**;

$P_2 = P_2(\mathfrak{X})$, $P_2(n) = P_2(X(n))$, где $X(n) = \{x_1, \ldots, x_n\}$.

$P_2^m(n)$ — **множество** (n, m)-**операторов**, т.е. систем ФАЛ вида $F = (f_1, \ldots, f_m)$, где $f_i \in P_2(n)$, или, иначе, систем уравнений вида $(z_{j_1} = f_1, \ldots, z_{j_m} = f_m)$.

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, $|Q(n)| \geqslant 3$.

Для класса ФАЛ или операторов Q' и класса ФАЛ Q'' введём функции

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

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

Класс ФАЛ (операторов) Q называется **невырожденным**,
если $n + m_Q(n) = o\big(\jmath\big(|Q(n)|\big)\big)$ при $n = 1, 2, \ldots$.
Класс ФАЛ Q считается **строго невырожденным**,
если $\log n = o\big(\log\log|Q(n)|\big)$, **ненулевым (нулевым)**, если $\varliminf\limits_{n\to\infty} \sigma_Q(n) > 0$
(соответственно $\overline{\lim\limits_{n\to\infty}} \sigma_Q(n) = \lim\limits_{n\to\infty} \sigma_Q(n) = 0$), и **стабильным**,
если $\sigma_Q(n+1) = \sigma_Q(n)$, начиная с некоторого $n = n_0$.
Заметим, что ненулевой класс ФАЛ является строго невырожденным, строго невырожденный класс — невырожденным, а стабильный класс Q — ненулевым, если $|Q(n)| \geqslant 2$ при $n \geqslant n_0$.

Пусть D, M, S и $\mathcal{L}$ — классы самодвойственных, монотонных, симметричных и линейных ФАЛ соответственно, а P_2, как обычно, класс всех ФАЛ.

Напомним, что

1. $|P_2(n)| = 2^{2^n}$, т. е. $\sigma_{P_2}(n) = 1$, $\mathcal{J}\big(|P_2(n)|\big) = \frac{2^n}{n}$;
2. $f \in D(n)$, если $\overline{f}(\overline{x}_1, \ldots, \overline{x}_n) = f(x_1, \ldots, x_n)$, и, следовательно, $|D(n)| = 2^{2^{n-1}}$, т. е. $\sigma_D(n) = \frac{1}{2}$, $\mathcal{J}\big(|D(n)|\big) = \frac{2^{n-1}}{n-1}$;
3. $f \in M(n)$, если в случае, когда $\alpha_1 \leqslant \beta_1, \ldots, \alpha_n \leqslant \beta_n$, верно неравенство $f(\alpha_1, \ldots, \alpha_n) \leqslant f(\beta_1, \ldots, \beta_n)$ и что при этом, как известно[1], $\log |M(n)| \sim C_n^{\left\lceil \frac{n}{2} \right\rceil} \sim \frac{2^n}{\sqrt{2\pi n}}$, т. е. $\sigma_M(n) \sim \frac{1}{\sqrt{2\pi n}}$, $\mathcal{J}\big(|M(n)|\big) \sim \frac{2^n}{\sqrt{2\pi n^3}}$;

[1] Полагаем, что $a(n) \lesssim b(n)$ для последовательностей $a(n)$ и $b(n)$, где $n = 1, 2, \ldots$, если $a(n) \leqslant (1 + \overline{o}(1))b(n)$, и что $a(n) \sim b(n)$ тогда и только тогда, когда $a(n) \lesssim b(n)$ и $b(n) \lesssim a(n)$.

4. $f \in S(n)$, если для каждого $i, i \in [0, n]$, и любых двух наборов α, β из множества $B_i^n = \{\gamma = (\gamma_1, \ldots, \gamma_n) : \gamma_1 + \cdots + \gamma_n = i\}$ — т. н. i-го слоя куба B^n, — выполняется равенство $f(\alpha) = f(\beta)$, т. е. $|S(n)| = 2^{n+1}, \sigma_S(n) = \frac{n+1}{2^n}, \mathcal{J}(|S(n)|) = \frac{n+1}{\log(n+1)}$;
5. $f \in \mathcal{L}(n)$, если $f = \alpha_1 x_1 \oplus \cdots \oplus \alpha_n x_n \oplus \alpha_0$, т. е. $|\mathcal{L}(n)| = 2^{n+1}, \sigma_{\mathcal{L}}(n) = \frac{n+1}{2^n}, \mathcal{J}(|\mathcal{L}(n)|) = \frac{n+1}{\log(n+1)}$.

Таким образом, классы P_2, D являются ненулевыми и стабильными, класс M — нулевым и строго невырожденным, а классы S, $\mathcal{L}$ — нулевыми и вырожденными.

Пусть заданы класс ФАЛ или операторов Q, класс схем $\mathcal{U}$ и функционал их сложности Ψ. Тогда под **Ψ-сложностью** $\Psi(F)$ оператора (ФАЛ) F, $F \in Q(n)$, понимается, как обычно, минимальное по всем реализующим F схемам Σ из $\mathcal{U}$ значение величины $\Psi(\Sigma)$. При этом **функцией Шеннона для класса ФАЛ или операторов Q при их реализации в классе схем $\mathcal{U}$ относительно функционала сложности Ψ** называется функция натурального аргумента

$$\Psi(Q(n)) = \max_{f \in Q(n)} \Psi(f).$$

В дальнейшем будем, как правило, рассматривать в качестве $\mathcal{U}$ класс $\mathcal{U}^{\mathrm{C}}$ — класс СФЭ над базисом $\mathrm{Б}_0 = \{\&, \vee, \neg\}$, а в качестве $\Psi(\Sigma)$ — функционал $L(\Sigma)$, равный числу элементов в СФЭ Σ.

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

Утверждение 26.1

Если Q — невырожденный класс ФАЛ (операторов), то

$$L^{\mathrm{C}}(Q(n)) \gtrsim \frac{\log|Q(n)|}{\log\log|Q(n)|} = \mathcal{J}(|Q(n)|),$$

а если Q — строго невырожденный класс ФАЛ, то

$$L^{\mathrm{K}}(Q(n)) \gtrsim \frac{\log|Q(n)|}{\log\log|Q(n)|} = \mathcal{J}(|Q(n)|).$$

Следствие

Для всякого ненулевого класса ФАЛ Q выполняются асимптотические неравенства:

$$L^{\mathrm{C}}(Q(n)) \gtrsim \sigma_Q(n)2^n/n, L^{\mathrm{K}}(Q(n)) \gtrsim \sigma_Q(n)2^n/n.$$

Действительно, Q — невырожденный класс ФАЛ, для которого $\log|Q(n)| = \sigma_Q(n) \cdot 2^n$ и $\log\log|Q(n)| = n + \log\sigma_Q(n) \sim n$, так как $\varliminf\limits_{n\to\infty} \sigma_Q(n) > 0$

Схема доказательства.

Пусть $Q = Q(1), \ldots, Q(n), \ldots$ — невырожденный класс (n, m)-операторов, где $m = m(n)$, $n = 1, 2, \ldots$, и $Q(n) \subseteq P_2^{m(n)}(n)$, для которого $m + n = \overline{o}(\mathcal{J}(Q(n)))$.

Рассмотрим множество $\mathcal{U}^{\mathrm{C}}(L, n, m)$ — множество приведенных СФЭ $\Sigma = \Sigma(x_1, \ldots, x_n; z_1, \ldots, z_m)$ из $\mathcal{U}^{\mathrm{C}}$ таких, что $L(\Sigma) \leqslant L$ и докажем неравенство

$$\left\|\mathcal{U}^{\mathrm{C}}(L, n, m)\right\| \leqslant (8(L + n))^{L+m}, \tag{3.1}$$

которое обобщает следующую оценку из курса ОК

$$\left\|\mathcal{U}^{\mathrm{C}}(L, n)\right\| \leqslant (8(L + n))^{L+1}.$$

Для этого достаточно учесть то, что:

1. число т. н. «каркасов», т. е. систем формул $\mathcal{F}(x_1) = (\mathcal{F}_1(x_1), \ldots, \mathcal{F}_m(x_1))$, которые получаются из Σ отсоединением кратных дуг, исходящих из входов Σ и выходов ее ФЭ, а также нанесением пометки x_1 на все листья получившейся системы из m деревьев, по прежнему не превосходит 8^L;
2. $R(\mathcal{F}) = R(\mathcal{F}_1) + \cdots + R(\mathcal{F}_m) \leqslant L + m$;
3. СФЭ Σ получается из системы формул $\mathcal{F}$ путем присоединения каждой исходящей из ее входа x_1 дуги, либо к одной из БП $x_1, \ldots, x_n$, либо к выходу какого-либо элемента $\mathcal{F}$.

Полагая, далее, что

$$L^{\mathrm{C}}(Q(n)) < (1-\epsilon(n))\mathcal{J}\big(|Q(n)|\big),$$

где $0 < \epsilon = \epsilon(n) < 1$, учитывая (3.1) и то, что $m+n = \overline{o}(\mathcal{J}\big(|Q(n)|\big))$, подбираем такое $\epsilon(n) = \overline{o}(1)$, при котором не будет выполняться (обобщенное мощностное неравенство Шеннона)

$$\big\|\mathcal{U}^{\mathrm{C}}(L^{\mathrm{C}}(Q(n)), n, m(n))\big\| \geqslant |Q(n)|.$$

Отсюда следует, что

$$L^{\mathrm{C}}(Q(n)) \geqslant (1-\epsilon(n))\mathcal{J}\big(|Q(n)|\big) \sim \mathcal{J}\big(|Q(n)|\big).$$

Второе неравенство доказывается аналогично, но с учетом сильной невырожденности класса Q. Утверждение доказано. $\square$

Класс ФАЛ Q называется **квазиинвариантным** классом, если для некоторого n_0, $n_0 \geqslant 2$, и любого n, $n \geqslant n_0$, для произвольной ФАЛ f, $f \in Q(n)$, при любом σ, $\sigma \in B$, ФАЛ $f(x_1, \ldots, x_{n-1}, \sigma)$ принадлежит $Q(n-1)$.
Минимальное число n_0, для которого указанное соотношение выполняется, будем считать **порогом** квазиинвариантного класса Q.
Из введенных выше классов P_2, D, M, S и $\mathcal{L}$ только класс D не является квазиинвариантным.

Утверждение 26.2

Пусть Q — квазиинвариантный класс ФАЛ. Тогда существует предел

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

где $0 \leqslant \sigma_Q \leqslant 1$.

Замечание

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

Доказательство.

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

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

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

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

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

из которого, в свою очередь, следует, что

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

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

Из определений и утв. 26.2 вытекает, что квазиинвариантный класс Q является нулевым (ненулевым) классом ФАЛ тогда и только тогда, когда $\sigma_Q = 0$ (соответственно $\sigma_Q > 0$). При этом в силу следствия из утв. 26.1 справедливо следующее утверждение.

Утверждение 26.3

Для всякого ненулевого квазиинвариантного класса Q и $n = 1, 2, \ldots$

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

27. Инвариантные классы функций С. В. Яблонского, их описание на языке базовых множеств и порождающих элементов. Теорема о числе инвариантных классов и фрагменты её доказательства

Рассмотрим некоторое более узкое по сравнению с введённым в вопросе 26 семейством квазиинвариантных классов — предложенное С. В. Яблонским семейство т. н. инвариантных классов ФАЛ.

Для этого определим 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).

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 неконстантную функцию, из которой при помощи операции 3 можно получить обе константы. Отметим, что если класс Q замкнут по суперпозиции и $\{0,1\} \subseteq Q$, то класс Q является инвариантным.

Примерами таких инвариантных классов являются классы M и $\mathcal{L}$ всех монотонных и всех линейных ФАЛ соответственно.

С другой стороны класс D — 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 S — 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.

Заметим, что инвариантный класс Q является квазиинвариантным классом с порогом 2 и поэтому в силу утв. 26.2 его мощностная последовательность $\sigma_Q(n)$ является монотонно не возрастающей при всех $n = 1, 2, \ldots$.

Напомним, что инвариантные классы M, $\mathcal{L}$ являются ненулевыми классами и найдем мощностную характеристику класса $\widehat{S}$.

Произвольную 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). Следовательно

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

и поэтому $\sigma_{\widehat{S}} = 0$. Таким образом, все три инвариантных класса M, $\mathcal{L}$, $\widehat{S}$ являются нулевыми.

Построим пример ненулевого инвариантного класса, отличного от P_2.

Рассмотрим инвариантный класс Q, состоящий из всех ФАЛ вида $f(x_{i_1}, \ldots, x_{i_r})(x_{i_1} \oplus \cdots \oplus x_{i_r} \oplus \sigma)$, где $1 \leqslant i_1 < \cdots < i_r$ и $\sigma \in B$, который 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, $\sigma_Q = \frac{1}{2}$.

Докажем, что существует только один инвариантный класс Q с характеристикой $\sigma_Q = 1$ — это класс P_2 и что существует континуум инвариантных классов с нулевой мощностной константой. На самом деле справедливо следующее утверждение:

Утверждение 27.1

Класс P_2 является единственным инвариантным классом ФАЛ Q, для которого $\sigma_Q = 1$. Для любого действительного σ, $\sigma \in [0, 1)$, существует континуум инвариантных классов Q, для которых $\sigma_Q = \sigma$.

Доказательство.

1. Если инвариантный класс Q не совпадает с P_2, то для некоторого m будет выполнено неравенство $|Q(m)| < |P_2(m)|$, которое равносильно неравенству $\sigma_Q(m) < 1$. Из последнего неравенства в силу монотонного невозрастания последовательности $\sigma_Q(n)$, $n = 1, 2, \ldots$, и её сходимости к пределу σ_Q следует, что $\sigma_Q \leqslant \sigma_Q(m) < 1$.
2. Отметим, что число различных инвариантных классов не может быть больше континуума, поскольку множество P_2 счётно и докажем, что существует континуум различных инвариантных классов с характеристикой 0.

Для этого введем некоторые определения и обозначения.

Если функция g получена из функции f применением операции 3 (соответственно операций 1–3), то говорят, что g является **подфункцией** (соответственно **псевдоподфункцией**) ФАЛ f, а f — **надфункцией** (соответственно **псевдонадфункцией**) ФАЛ g.

При этом подфункция, полученная при «реальной» подстановке констант в исходную ФАЛ, считается ее **собственной** подфункцией.

Для множества функций F через $F^{\urcorner}$ и $F_{\llcorner}$ будем обозначать множества всех псевдонадфункций и псевдоподфункций для функций из F соответственно.

Множество F называется **базовым множеством** инвариантного класса Q, если $F_{\lrcorner} = Q$. Для задания всякого инвариантного класса достаточно задать, очевидно, его базовое множество.

Возвращаясь к доказательству утверждения, рассмотрим симметрические функции $s_m^{\{0,m\}}$, определяемые при $m > 1$ следующим образом:

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

и для любого J, $J \subseteq \mathbb{N} \setminus \{1\}$, определим соответствующи ему инвариантный класс $Q_J = \{ s_m^{\{0,m\}} \mid m \in J \}_{\lrcorner}$.

Заметим, что $s^{\{0,m'\}} \notin \{s^{\{0,m''\}}\}_{\lrcorner}$ при $m' \neq m''$, и, следовательно, для любых различных множеств J' и J'' из $\mathbb{N} \setminus \{1\}$, соответствующие им классы $Q_{J'}$ и $Q_{J''}$ 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.

Доказательство того факта, что для любого σ, $\sigma \in (0, 1)$, существует континуум инвариантных классов Q таких, что $\sigma_Q = \sigma$ является очень сложным и мы его опускаем.

Утверждение доказано. $\square$

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 J, состоящий из констант 0, 1 и всех монотонных элементарных дизъюнкций (ЭД), то есть функций вида $x_{i_1} \vee \cdots \vee x_{i_s}$, имеет счётное базовое множество, но не имеет базы.

Действительно, любое базовое множество A класса J должно содержать ЭД, существенно зависящие от счетного числа БП. При этом ЭД из A с минимальным числом существенных БП является псевдоподФАЛ любой другой ЭД из A.

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 g принадлежат Q. Из определения следует, что порождающий элемент нетривиального инвариантного класса является существенной функцией и что никакие два попарно не конгруэнтных порождающих элемента не являются псевдоподфункциями друг друга.

Приведём примеры порождающих элементов. Класс M монотонных ФАЛ имеет единственный с точностью до конгруэнтности порождающий элемент — функцию $\overline{x}_1$. Порождающими элементами класса $\mathcal{L}$ являются, например, ФАЛ $x_1 \cdot x_2$ и $x_1 \vee x_2$.

Для инвариантного класса Q его **порождающим множеством** называется всякое максимальное по включению множество попарно не конгруэнтных порождающих элементов Q. Так, порождающее множество класса M состоит из ФАЛ $\overline{x}_1$, а класса, состоящего из констант и монотонных элементарных дизъюнкций, суть $\{\overline{x}_1, x_1 x_2\}$.

Утверждение 27.2

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

Следствие

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

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 свойство существенной ФАЛ f из $P_2 \setminus Q$ верно, в том случае, когда любая собственная подФАЛ ФАЛ f принадлежит 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 рассматриваемое свойство верно для всех существенных ФАЛ из $P_2 \setminus Q$, зависящих от n, $n \in [1, k)$, где $k \geqslant 2$, БП 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.

Утверждение доказано. $\square$

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

Заметим, что асимптотическое совпадение функций Шеннона $L^{\mathrm{C}}\big(Q(n)\big)$ с её нижней мощностной оценкой из утв. 26.1 является типичным для абсолютного большинства невырожденных «естественных» классов ФАЛ (операторов). В связи с этим введём следующее определение.

Класс ФАЛ (операторов) Q называется **стандартным**, если выполнено асимптотическое неравенство

$$L^{\mathrm{C}}\big(Q(n)\big) \lesssim \mathcal{J}\big(|Q(n)|\big) + O\big(n + m(n)\big).$$

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

Утверждение 28.1

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

Доказательство.

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

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

Напомним основные этапы построения СФЭ Σ_f и оценки сложности составляющих ее подсхем.

Пусть $x' = (x_1, \ldots, x_q)$, $x'' = (x_{q+1}, \ldots, x_n)$ и $f_{\sigma''}(x') = f(x', \sigma'')$ для всех σ'' из B^{n-q}. Пусть, далее, Σ'' — мультиплексор порядка $(n-q)$ от адресных БП x'' и информационных БП $y = (y_0, \ldots, y_{2^{n-q}-1})$, который был построен в курсе ОК, представляет собой формулу $\mathcal{F}_{n-q}$ сложности не больше, чем $4 \cdot 2^{n-q}$, и реализует мультиплексорную ФАЛ $\mu_{n-q}(x'', y)$.

Пусть s, $s < 2^m$, — некоторый параметр, а G — стандартное ДУМ порядка q и высоты s такое, что $|G| \leqslant p \cdot 2^s$, где $p = \left\lceil \frac{2^q}{s} \right\rceil$. Обозначим через Σ_G СФЭ, которая реализует систему ФАЛ $\overrightarrow{G}$ и представляет собой объединение схем сложности не больше, чем $3 \cdot 2^q$, построенных для каждой из них по совершенной ДНФ на базе контактного дерева. Тогда

$$L(\Sigma'') \leqslant 4 \cdot 2^{n-q}, \; L(\Sigma_G) \leqslant 3p \cdot 2^{s+q}.$$

Напомним, что при этом ФАЛ f разлагается по БП x'' следующим образом:

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

и что для реализации каждой ФАЛ $f_{\sigma''}(x')$ в СФЭ Σ_f используется формула $g^{(1)}_{\sigma''} \vee \ldots \vee g^{(p)}_{\sigma''}$, где $g^{(j)}_{\sigma''} \in G$ при всех j, $j = 1, \ldots, p$. Из принадлежности ФАЛ f классу $P_2(n, r)$ следует, что при $\nu(\sigma'') > \left\lceil \frac{r}{2^q} \right\rceil$ функция $f_{\sigma''}(x')$ тождественно равна нулю, и, таким образом, из схемы Σ_f можно удалить подсхемы, реализующие все указанные подфункции.

Для сложности полученной при этом СФЭ $\widetilde{\Sigma}_f$ будет выполняться неравенство

$$L(\widetilde{\Sigma}_f) \leqslant \left\lceil \frac{r}{2^q} \right\rceil (p-1) + 4 \cdot 2^{n-q} + 3p \cdot 2^{s+q},$$

из которого при тех же значениях параметров, что и в курсе ОК, где $s = \lceil n - 5 \log n \rceil$ и $q = \lceil 2 \log n \rceil$, следует, что

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

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,

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

Заметим, что функция f' принадлежит классу $P_2(k, r)$, где $r > 2^{k-1}$, и для неё по предыдущему случаю можно построить СФЭ $\widetilde{\Sigma}_{f'}$, сложность которой асимптотически не больше, чем $\frac{r}{\log r}$.

Искомая СФЭ $\widetilde{\Sigma}_f$ строится на основе указанного выше разложения так, что

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

Утверждение доказано. $\square$

Следствие

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

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

29. Асимптотически наилучший метод синтеза схем для ненулевых квазиинвариантных классов, их стандартность

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

Утверждение 29.1

Для всякого квазиинвариантного класса Q и $n = 1, 2, \ldots$

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

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

Доказательство.

Рассмотрим сначала случай $\sigma_Q > 0$. В этом случае в соответствии с введёнными ранее обозначениями и в силу утв. 26.2 получим

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

откуда по утв. 26.3 следует требуемая нижняя оценка.

Перейдём к получению необходимой верхней оценки. 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 квазиинвариантности класса Q.

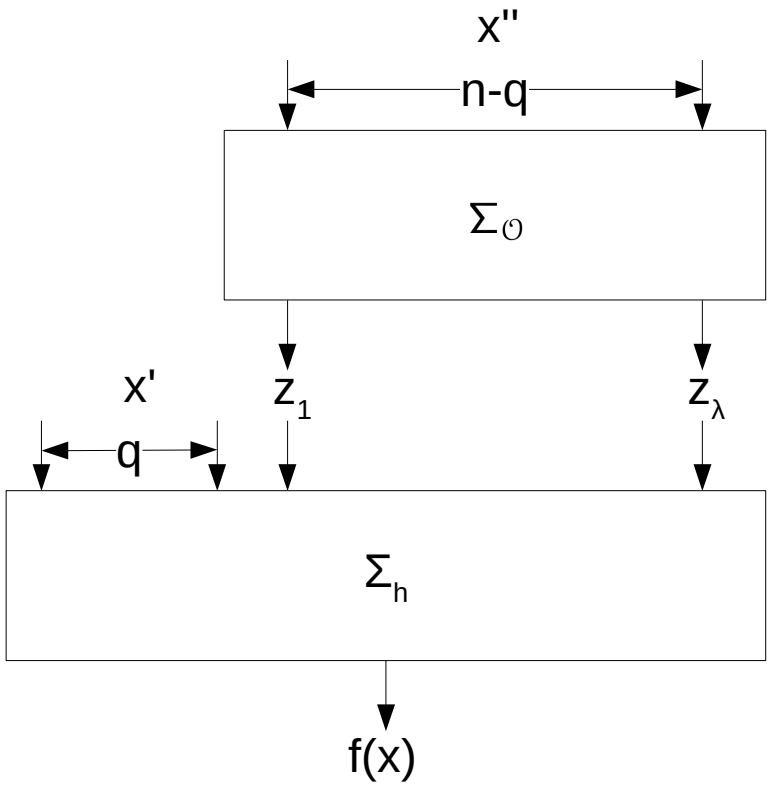
Положим $\lambda = \lceil \log |Q(q)| \rceil$ и пусть Π' — произвольное инъективное отображение (кодирование) ФАЛ множества $Q(q)$ двоичными наборами куба B^λ от БП $y = (y_1, \ldots, y_\lambda)$, то есть $\Pi' \colon Q(q) \mapsto B^\lambda(y)$, которое существует, так как $2^\lambda \geqslant |Q(q)|$. 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 $\mathfrak{O} = (\mathfrak{O}_1, \ldots, \mathfrak{O}_\lambda) \in P_2^\lambda(n-q)$ — система ФАЛ, которая сопоставляет произвольному набору σ'', $\sigma'' \in B^{n-q}$, набор («код») $\pi_{\sigma''}$ и пусть СФЭ $\Sigma_{\mathfrak{O}}$ из $\mathcal{U}^c$, построенная асимптотически наилучшим методом, реализует эту систему ФАЛ со сложностью

$$L(\Sigma_{\mathfrak{O}}) \leqslant \lambda \frac{2^{n-q}}{n-q} + o\left(\frac{2^{n-q}}{n-q}\right).$$



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 $q = \left\lceil \frac{1}{2} \log n \right\rceil$, и учитывая, что

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

получим верхнюю оценку

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

В случае $\sigma_Q > 0$ отсюда, с учётом нижней оценки, вытекает искомая асимптотика вида $\sigma_Q \frac{2^n}{n}$ для функции Шеннона $L^C(Q(n))$.

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

$$L(\Sigma_f) = o\left(\frac{2^n}{n}\right),$$

что доказывает второе соотношение утверждения.

Утверждение 29.1 доказано. □

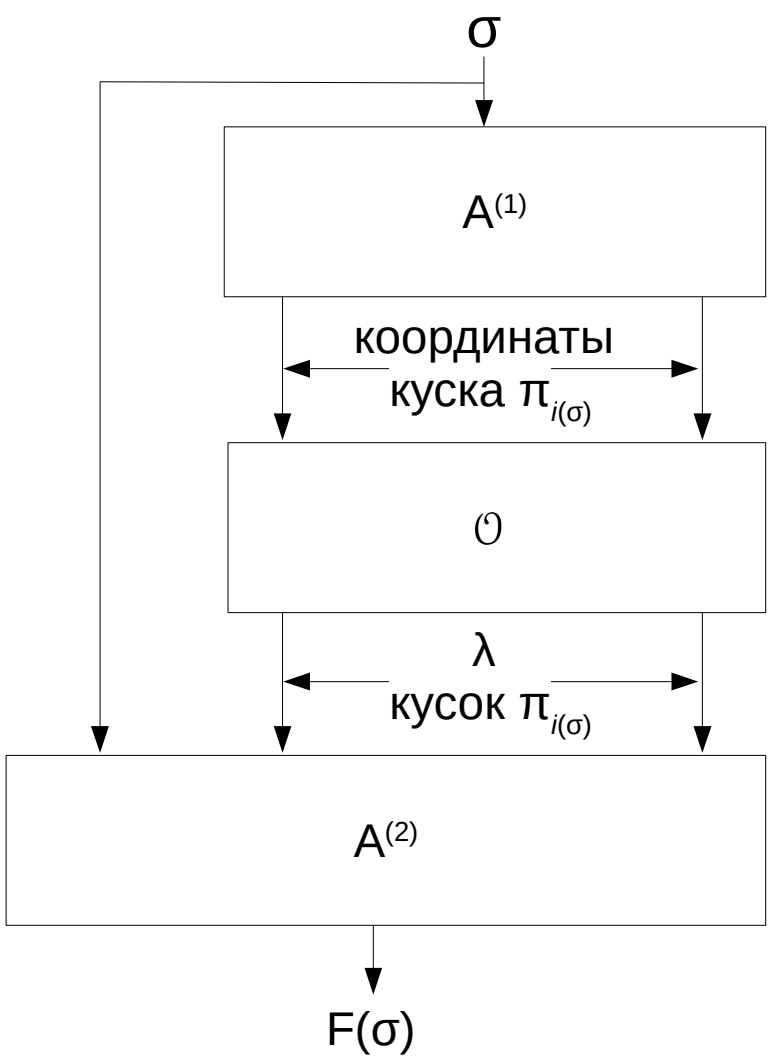
30. Общее описание принципа локального кодирования, его применение для доказательства стандартности класса самодвойственных функций

При доказательстве верхней оценки утв. 29.1 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 $\pi_{i(\sigma)}$.

Будем предполагать, что «положение» куска кода задается его «координатами» (например, позицией его первого разряда в коде и длиной, или номером куска, если куски кода не пересекаются и имеют одинаковую длину, и т. п.).



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

$$L^{\mathrm{C}}\bigl(A_n^{(1)}\bigr) = o\bigl(\mathcal{J}\bigl(|Q(n)|\bigr)\bigr),\ L^{\mathrm{C}}\bigl(A_n^{(2)}\bigr) = o\bigl(\mathcal{J}\bigl(|Q(n)|\bigr)\bigr),\ L^{\mathrm{C}}\bigl(\mathcal{O}_n\bigr) \lesssim \mathcal{J}\bigl(|Q(n)|\bigr),$$

то искомая СФЭ Σ_n может быть выбрана так, что $L\bigl(\Sigma_n\bigr) \lesssim \mathcal{J}\bigl(|Q(n)|\bigr)$. Отсюда вытекает, что $L^{\mathrm{C}}\bigl(Q(n)\bigr) \lesssim \mathcal{J}\bigl(|Q(n)|\bigr)$, и, следовательно, в силу утв. 26.1 в случае невырожденности класса Q выполняется асимптотическое равенство $L^{\mathrm{C}}\bigl(Q(n)\bigr) \sim \mathcal{J}\bigl(|Q(n)|\bigr)$, которое означает стандартность класса Q относительно функционала сложности L класса схем $\mathcal{U}^{\mathrm{C}}$.

Заметим, что в случае асимптотической неизбыточности кодирования $\Pi = \Pi_n$, когда $d(n) \sim \log |Q(n)|$, при построении схемы, которая реализует оператор $\mathcal{O}_n$ со сложностью, $L^{\mathrm{C}}(\mathcal{O}_n) \lesssim \mathcal{J}(|Q(n)|)$, достаточно, как правило, использовать асимптотически наилучший метод синтеза СФЭ для произвольных систем ФАЛ подходящей размерности или некоторые его модификации (см., например, утв. 28.1).

Заметим также, что соотношения $L^{\mathrm{C}}(A_n^{(1)}) = o(\mathcal{J}(|Q(n)|))$, $L^{\mathrm{C}}(A_n^{(2)}) = o(\mathcal{J}(|Q(n)|))$ означают возможность существенно более простой по сравнению с оператором $\mathcal{O}_n$ реализации операторов $A_n^{(1)}$ и $A_n^{(2)}$ в классе $\mathcal{U}^{\mathrm{C}}$.

Описанный выше асимптотически наилучший метод синтеза СФЭ над базисом $Б_0$ для ФАЛ из ненулевых инвариантных классов является примером применения принципа локального кодирования.

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

Утверждение 30.1

Класс самодвойственных ФАЛ является невырожденным стандратным классом ФАЛ и, тем самым,

$$L^{\mathrm{C}}\big(D(n)\big) \sim \frac{2^{n-1}}{n}.$$

Доказательство.

Невырожденность класса D и требуемая нижняя мощностная оценка вытекают из того, что $|D(n)| = 2^{2^{n-1}}$, т. е. $\mathcal{J}\big(|D(n)|\big) = \frac{2^{n-1}}{n-1}$, в силу утв.26.1, так как при этом $n = o\big(\mathcal{J}(|D(n)|)\big)$.

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

Далее, выберем в качестве основного оператора $\mathfrak{O}$ ФАЛ $h(y_1, \ldots, y_{n-1})$ со столбцом значений π, а в качестве оператора $A_n^{(2)}$ — ФАЛ $x_1 \oplus z$, где $z = h(y_1, \ldots, y_{n-1})$ и $y_i = g_i(x_1, \ldots, x_n)$ для всех i, $i = 1, \ldots, n-1$.

Действительно, в силу самодвойственности ФАЛ f:

$f(0, \sigma_2, \ldots, \sigma_n) = h(\sigma_2, \ldots, \sigma_n)$, $f(1, \sigma_2, \ldots, \sigma_n) = \overline{h}(\overline{\sigma}_2, \ldots, \overline{\sigma}_n)$. Таким образом, $L^{\mathrm{C}}(f) \leqslant L^{\mathrm{C}}(h) + 4n \lesssim \frac{2^{n-1}}{n}$, что доказывает верхнюю оценку утв. 30.1.

Утверждение доказано. $\square$

31. Применение принципа локального кодирования для доказательства стандартности некоторых невырожденных классов операторов

Рассмотрим два класса операторов и с помощью принципа локального кодирования докажем (при некоторых условиях) их стандартность. Пусть, по-прежнему, S — класс всех симметрических ФАЛ.

Утверждение 31.1

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

$$\log n = o(m) \quad \textit{и} \quad \log m = o(\log n), \tag{3.2}$$

то класс операторов Q, для которого $Q(n) = S^m(n)$, является невырожденным и стандартным 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

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

Из данного соотношения, 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 условий утверждения стремятся к 0 при n стремящемся к бесконечности.

Следовательно, $m + n = o(\mathcal{J}(|Q(n)|)$, то есть $Q(n)$ — невырожденный класс операторов. Отсюда по утв. 26.1 с учётом того, что $\log m = o(\log n)$ получаем нижнюю оценку

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

Для получения аналогичной верхней 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, как известно, имеет сложность

$$L^{\mathsf{C}}\left(A_n^{(1)}\right) \leqslant 9n.$$

Заметим, что основной оператор $\mathfrak{O}_n$ может быть при этом выбран из множества $P_2^m(t, n+1)$, а его сложность в силу утв. 28.1 удовлетворяет неравенству

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

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 полученной ранее нижней оценкой. Утверждение доказано. $\square$

Следствие

$$L^{\mathrm{C}}(S(n)) = o(n).$$

Утверждение 31.2

Для постоянной последовательности $m = m(n) \geqslant 2$, $n = 1, 2, \ldots$, класс операторов Q, для которого множество $Q(n)$ состоит из всех (n, m)-операторов $F = (f_1, \ldots, f_m)$ таких, что $f_i(\beta) = f_1(\alpha)$ при любом i, $i \in [2, m]$, любом α, $\alpha \in B^n$, и $\nu(\beta) - \nu(\alpha) \equiv i - 1 \pmod{2^n}$, является стандартным 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 утв. 26.1 непосредственно вытекает необходимая нижняя оценка $L^{\mathrm{C}}\big(Q(n)\big) \gtrsim \dfrac{2^n}{n}$.

Для получения аналогичной верхней оценки возьмём произвольное натуральное n и натуральное q, $q \leqslant n$, а затем обычным образом разобьём набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$. Выберем из $Q(n)$ произвольный оператор $F = (f_1, \ldots, f_m)$ и положим $f = f_1$. Рассмотрим кодирование $\Pi = \Pi_n$, которое сопоставляет оператору $F = F_n$ набор π длины $d = 2^n + (m-1)$, получающийся удлинением столбца значений $\tilde{\alpha}_f$ ФАЛ f первыми $(m-1)$ разрядами этого же столбца. Выделим в этом наборе 2^{n-q} кусков $\pi_{\sigma''}$, $\sigma'' \in B^{n-q}$, длины $\lambda = 2^q + (m-1)$, где кусок $\pi_{\sigma''}$ получается удлинением той части столбца $\tilde{\alpha}_f$, которая соответствует ФАЛ $f(x', \sigma'')$, на $(m-1)$ следующий за ней разряд.

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

$$L^{\mathrm{C}}\left(A_n^{(1)}\right) = 0, \qquad L^{\mathrm{C}}\left(A_n^{(2)}\right) \lesssim m \cdot \frac{2^{q+\lambda}}{q+\lambda} = o\left(\frac{2^n}{n}\right),$$

$$L^{\mathrm{C}}\left(\mathcal{O}_n\right) \lesssim \left(2^q + (m-1)\right) \cdot \frac{2^{n-q}}{n-q} \sim \frac{2^n}{n},$$

из которых следует, что $L^{\mathrm{C}}\left(Q(n)\right) \lesssim \frac{2^n}{n}$.

Утверждение доказано. $\square$

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

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

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

Функция Шеннона для этого класса определяется стандартным образом:

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

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

Пусть функция $g(x_1, x_2)$ из $\widehat{P}_2(2)$ имеет столбец значений $\tilde{\alpha}_g = (0122)$ и, следовательно, $g \in \widehat{P}_2(2,2)$. Тогда доопределениями g будут ФАЛ $(0100) = \overline{x}_1 x_2$, $(0110) = x_1 \oplus x_2$, $(0101) = x_2$ и $(0111) = x_1 \vee x_2$, то есть $L^{\mathrm{C}}(g) = 0$.

Положим $\widehat{P}_2(n, 2^n) = \widehat{P}_2(n)$ и заметим, что $|\widehat{P}_2(n)| = 3^n$, то есть $\mathcal{J}(|\widehat{P}_2(n)|) = \frac{\log 3 \cdot 2^n}{n + \log\log 3} \sim \log 3 \frac{2^n}{n}$, хотя при этом, очевидно, $L^{\mathrm{C}}(\widehat{P}_2(n)) \leqslant L^{\mathrm{C}}(n)$.

Утверждение 32.1

Если $n \log n = o(t(n))$, *то*

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

Замечание

Нетрудно показать, что для $t = t(n)$ и $n = 1, 2, \ldots$, условие $n \log n = o(t)$ и $n = o(\frac{t}{\log t})$ равносильны.

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

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

Из последнего равенства и условий утверждения (см. замечание) следует, что $n = o\big(\mathcal{J}(|Q(n)|)\big)$, то есть класс ФАЛ $Q(1), \ldots, Q(n)$, является невырожденным. Из этой невырожденности, утв. 26.1 и очевидных соотношений

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

вытекает оценка утверждения.

Утверждение доказано. $\square$

Утверждение 32.2

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

Замечание 1

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

Замечание 2

Из утв. 32.2 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, которое содержит, очевидно, все ФАЛ f, $f \in P_2(n)$, такие, что $|N_f| = \left\lceil \frac{2^n}{3} \right\rceil$. Следовательно,

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

В силу утв. 26.1 отсюда следует, что

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

в то время как

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

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

Рассмотрим, далее (вопросы 33, 34), несколько утверждений, позволяющих установить для исследуемой функции Шеннона верхнюю оценку вида правой части утв. 32.2 при последовательно ослабляемых ограничениях на рост функции $t = t(n)$, то есть доказать, в итоге, утв. 32.2 полностью.

Замечание. При $t = 2^n/n^5$ условие утв. 33.1 выполнено.

Утверждение 33.1

Если $\log t = \log t(n) \sim n$, *то*

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

Доказательство.

Для произвольного натурального n и натурального q, $1 \leqslant q < n$, разобъём, как обычно, набор БП $x = (x_1, \ldots, x_n)$ на поднаборы $x' = (x_1, \ldots, x_q)$ и $x'' = (x_{q+1}, \ldots, x_n)$.

Выберем натуральный параметр m, $m \leqslant 2^q$, и для любого s, $s \leqslant 2^q$, построим такое множество наборов $\mathfrak{A}_s$ куба B^s, которое «протыкает» (лемма о «протыкающем» множестве наборов в кубе из курса ОК) все грани ранга не больше, чем m, этого куба и состоит не более, чем из $s \cdot 2^m$ наборов. Для каждого отрезка I, т. е. множества наборов с подряд идущими номерами, куба B^q от БП x' рассмотрим множество G_I, состоящее из тех равных 0 вне I ФАЛ $P_2(x')$, «проекции» столбцов значений которых на I принадлежат множеству $\mathfrak{A}_s$, где $s = |I|$.

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

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

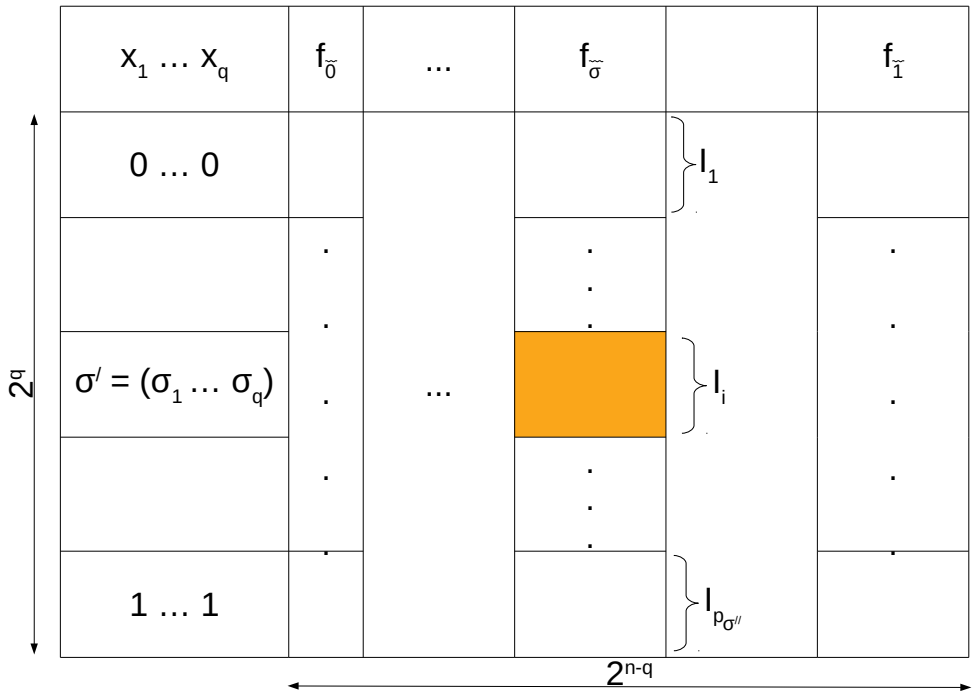
Действительно, отрезок I задается выбором его начала и конца, причем выбор каждого из них возможен не более, чем 2^q способами. После этого для задания ФАЛ из G_I достаточно не более, чем $s \cdot 2^m \leqslant 2^{q+m}$ способами, выбрать из $\mathfrak{A}_s$ «проекцию» ее столбца значений на I. Реализуем каждую ФАЛ из G по совершенной ДНФ на базе КД, получим искомую оценку для $L^{\mathrm{C}}\left(\overrightarrow{G}\right)$.

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

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

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

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



Для каждого набора σ'', $\sigma'' \in B^{n-q}$, положим $p_{\sigma''} = \lceil t_{\sigma''}/m \rceil$ и разобьём куб B^q от БП x' на последовательные отрезки $I_1, \ldots, I_{p_{\sigma''}}$ так, чтобы при любом i, $i \in [1, p_{\sigma''}]$, та часть столбца значений функции $f_{\sigma''}(x')$, которая связана с отрезком I_i, содержала m (соответственно не больше, чем m) булевских значений, если $i < p_{\sigma''}$ (соответственно $i = p_{\sigma''}$).

Пусть, далее, функция $f^{(i)}_{\sigma''}(x')$, $i = 1, 2, \ldots, p_{\sigma''}$, совпадает с функцией $f_{\sigma''}$ на отрезке I_i и равна 0 вне его, а ФАЛ $g^{(i)}_{\sigma''}$ из G_{I_i} является её доопределением. Отсюда следует, что функция $f_{\sigma''}$ может быть представлена в виде

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

и поэтому её доопределением является ФАЛ

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

Из полученных выше соотношений следует, что ФАЛ $g(x)$ вида

$$g(x) = \bigvee_{\sigma'' \in B^{n-q}} K_{\sigma''} \left(\bigvee_{i=1}^{p_{\sigma''}} g_{\sigma''}^{(i)}(x') \right),$$

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

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

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

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

Введём некоторые понятия и рассмотрим связанные с ними конструкции, позволяющие ослабить условия утв. 33.1.

Пусть n и s, $s \leqslant n$, — натуральные числа, а A — произвольное множество наборов куба B^n и $|A| \leqslant 2^s$. Будем говорить, что (n, s)-оператор ψ, $\psi \in P_2^s(n)$, является **оператором разделения** или, иначе, **оператором хэширования** для A, если $\psi(\alpha) \neq \psi(\beta)$ для любых различных наборов α и β из A.

Обозначим через Λ класс линейных ФАЛ с нулевым свободным членом и будем выбирать нужные нам операторы разделения из множества $\Lambda^s(n)$, т. е. множества наборов вида $(f_1, \ldots, f_s)$, где для всех j, $j = 1, \ldots, s$, ФАЛ $f_j = \gamma_1^{(j)} x_1 \oplus \ldots \oplus \gamma_n^{(j)} x_n$ при некоторых $\gamma_1^{(j)}, \ldots, \gamma_n^{(j)}$ из B.

Утверждение 34.1

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

Доказательство.

Рассмотрим множество $\Lambda^s(n)$ как вероятностное пространство, в котором вероятность выбора любого из 2^{ns} операторов равна 2^{-ns}. В этой модели для любых различных наборов α и β из B^n вероятность того, что случайный оператор из $\Lambda^s(n)$ их не разделит, равна 2^{-s}.

Действительно, для наборов $\alpha = (\alpha_1, \ldots, \alpha_n) \neq \beta = (\beta_1, \ldots, \beta_n)$ число не разделяющих их линейных ФАЛ вида $\gamma_1 x_1 \oplus \ldots \oplus \gamma_n x_n$ равно числу тех наборов $\gamma = (\gamma_1, \ldots, \gamma_n)$ из B^n, для которых $\gamma_1(\alpha_1 \oplus \beta_1) \oplus \ldots \oplus \gamma_n(\alpha_n \oplus \beta_n) = 0$, 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 $\mathbb{E}\xi_{\alpha,\beta}$ случайной величины $\xi_{\alpha,\beta}$, которая принимает значение из B и равна 1 с вероятностью того, что случайный оператор из Λ^s не разделит α и β, т. е. с вероятностью 2^{-s}, равно 2^{-s}. Тогда для случайной величины ξ_A, которая равна числу не разделённых случайным оператором из $\Lambda^s(n)$ неупорядоченных пар различных наборов из A, справедливы соотношения

$$\xi_A = \sum_{\substack{\alpha,\beta\in A \\ \nu(\alpha)<\nu(\beta)}} \xi_{\alpha,\beta} \qquad \text{и} \qquad \mathbb{E}\xi_A = \frac{t(t-1)}{2^{s+1}}.$$

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 $r \leqslant t(t-1)/2^{s+1}$.

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.

Утверждение доказано. $\square$

Следствие

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

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

Утверждение 34.2

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

Доказательство.

Положим

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

и заметим, что в силу условий утверждения выполняются соотношения

$$s \leqslant n, \qquad s \sim \log t, \qquad nt\log t = o(2^s). \tag{34.1}$$

Возьмём произвольную функцию f, $f \in \widehat{P}_2(n,t)$, и пусть $A = \delta(f)$, $|A| = t$. Построим по утв. 34.1 для множества A, $A \subset B^n$, оператор ψ, который отображает куб B^n от БП $x = (x_1, \ldots, x_n)$ в куб B^s от БП $y = (y_1, \ldots, y_s)$ и разделяет подмножество A', $A' \subseteq A$, такое, что

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

Заметим, что при этом в силу соотношений (34.1) $t' \sim t$, $s \sim \log t'$, и, следовательно, для множества $\widehat{P}_2(s, t')$, которому принадлежит функция $\widetilde{f}'(y)$ такая, что $\delta(\widetilde{f}') = \psi(A')$ и $\widetilde{f}'(\psi(\alpha)) = f(\alpha)$ при любом α, $\alpha \in A'$, выполнены условия утв. 33.1. Найдём по этому утверждению такое доопределение $\widetilde{g}'(y)$ ФАЛ $\widetilde{f}'(y)$, для которого

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

Легко видеть, что ФАЛ вида

$$g(x) = \widetilde{g}'(\psi(x)) \cdot \overline{\chi}''(x) \vee g''(x), \tag{34.2}$$

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

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

а известная оптимальная реализация линейной ФАЛ — оценку $L^{\mathrm{C}}(\psi) \leqslant 4ns$, из которых в силу соотношений (34.1) вытекает оценка

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

Таким образом, реализуя ФАЛ $g(x)$ в соответствии с равенством (34.2) и учитывая оценки сложности построенных схем, получим $L^{\mathrm{C}}(f) \lesssim \frac{t}{\log t}$.

Утверждение доказано. $\square$

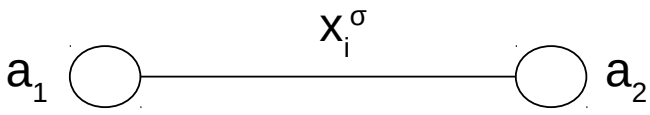
Утверждение 34.3

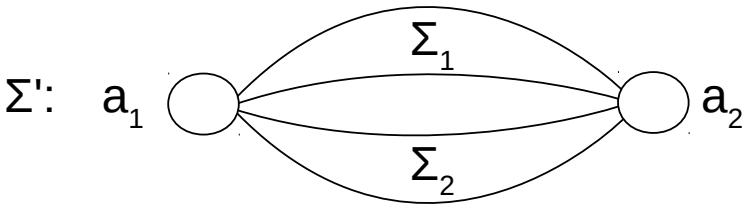
Если $t \leqslant 2^{n/3}$ *и* $n \log^2 n = o(t)$, *то* $L^{\mathrm{C}}\left(\widehat{P}_2(n,t)\right) \lesssim \frac{t}{\log t}$.

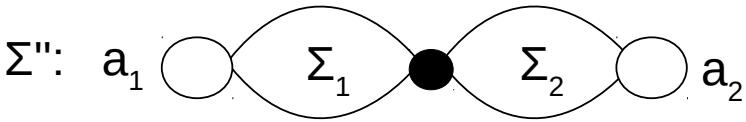
Доказательство этого утверждения представляет собой упрощённый вариант доказательства утв. 34.2, при котором $s = \lfloor 2 \log t \rfloor$ и, следовательно, $A' = A$, то есть вариант, не требующий реализации ФАЛ χ'', g''.

Суммируя доказанные утверждения, получаем основной результат — утв. 32.1.

35. Лемма о цепях и сечениях для π-схем; верхние оценки сложности реализации линейных функций в классе π-схем





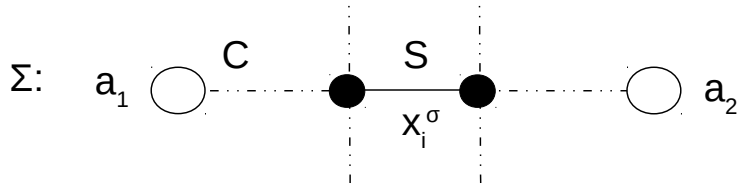


Под контактной схемой (КС) в данном вопросе будем понимать $(1,1)$-КС из неориентированных контактов. Результат последовательного (параллельного) соединения КС Σ_1 и Σ_2 будем обозначать через $\Sigma'' = \Sigma_1 \cdot \Sigma_2$ (соответственно $\Sigma' = \Sigma_1 \parallel \Sigma_2$). Назовём **простейшей 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.

Для множества C, состоящего из t контактов вида $x_{j_1}^{\sigma_1}, \ldots, x_{j_t}^{\sigma_t}$, положим

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

и будем считать его *проводящим* (*отделимым*), если $K(C) \not\equiv 0$ (соответственно $J(C) \not\equiv 1$). Для КС Σ, реализующей ФАЛ f из $P_2(n)$, через $\mathcal{C}(\Sigma)$ и $\widehat{\mathcal{C}}(\Sigma)$ будем обозначать множество всех и, соответственно, всех проводящих простых цепей Σ, соединяющих её полюса, а через $\mathcal{S}(\Sigma)$ и $\widehat{\mathcal{S}}(\Sigma)$ — множество всех и, соответственно, всех отделимых тупиковых сечений Σ, разделяющих её полюса (см. материалы курса ОК).



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

Утверждение 35.1

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

Доказательство.

Как уже отмечалось, любая цепь из $\widehat{\mathcal{C}}(\Sigma)$ и любое сечение из $\widehat{\mathcal{S}}(\Sigma)$ имеют хотя бы один общий контакт. Следовательно, достаточно убедиться в том, что $|C \cap S| = 1$ для любой цепи C из $\mathcal{C}(\Sigma)$ и любого сечения S из $\mathcal{S}(\Sigma)$.

Проведём индукцию по строению π-схемы Σ от БП $X(n) = \{x_1, \ldots, x_n\}$.

В случае, когда Σ — простейшая π-схема, состоящая из одного контакта, данное свойство, очевидно, выполняется. Докажем его справедливость при индуктивном переходе.

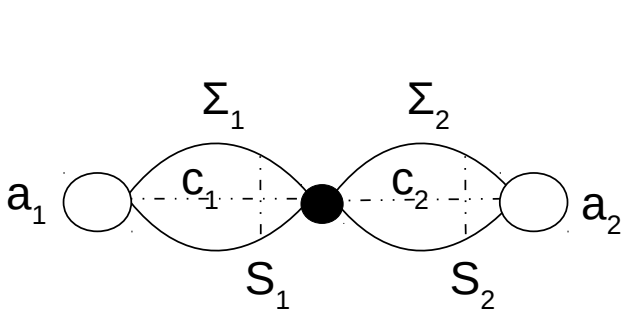
Отметим, сначала, что для произвольных КС Σ_1 и Σ_2 выполняются равенства:

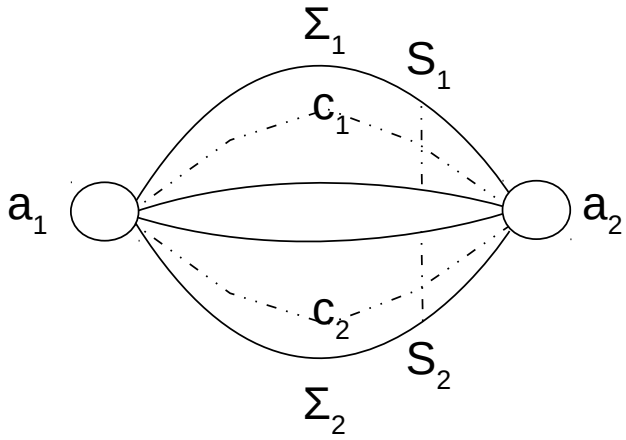
$$\mathcal{C}(\Sigma_1 \cdot \Sigma_2) = \{\, C \mid C = C_1 \cdot C_2, \text{ где } C_i \in \mathcal{C}(\Sigma_i), i = 1, 2 \,\},$$

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

$$\mathcal{C}(\Sigma_1 \parallel \Sigma_2) = \mathcal{C}(\Sigma_1) \cup \mathcal{C}(\Sigma_2), \tag{35.1}$$

$$\mathcal{S}(\Sigma_1 \parallel \Sigma_2) = \{\, S \mid S = S_1 \cup S_2, \text{ где } S_i \in \mathcal{S}(\Sigma_i), i = 1, 2 \,\}. \tag{35.2}$$





Действительно, любая цепь C из $\mathcal{C}(\Sigma_1 \cdot \Sigma_2)$ имеет вид $C = C_1 \cdot C_2$, где $C_i \in \mathcal{C}(\Sigma_i)$, $i = 1, 2$, а любое сечение S из $\mathcal{S}(\Sigma_1 \cdot \Sigma_2)$ должно быть либо сечением Σ_1, либо сечением Σ_2 и поэтому в силу своей тупиковости 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, обладающими данным свойством, то π-схема $\Sigma_1 \cdot \Sigma_2$ тоже будет ими обладать.

Аналогичным образом доказываются равенства (35.1), (35.2), и устанавливается справедливость индуктивного перехода в случае π-схемы вида $\Sigma_1 \parallel \Sigma_2$.

Утверждение доказано. $\square$

Утверждение 35.2

При $n \geqslant 1$ для линейной ФАЛ $l_n^\sigma = x_1 \oplus \ldots \oplus x_n \oplus \sigma$, $\sigma \in B$, выполнено неравенство

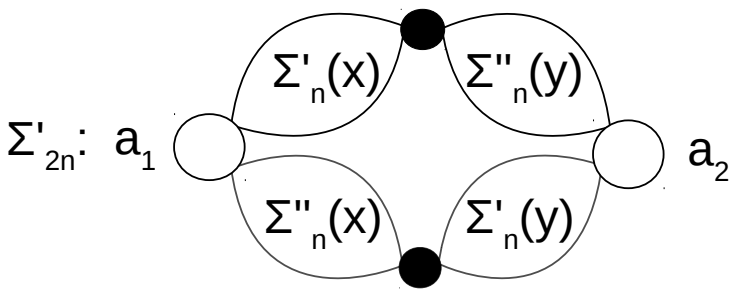
$$L^\pi(l_n^\sigma) \leqslant 4n^2.$$

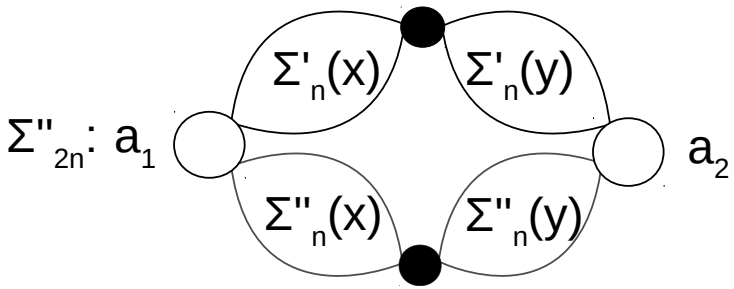
Доказательство.

Для получения требуемой оценки рассмотрим случай $n = 2^k$, $k = 1, 2, \ldots$.

Для $n = 2$ искомые π-схемы Σ_2' и Σ_2'' реализующие со сложностью 4 ФАЛ l_2 и $\bar{l}_2$ соответственно, строятся на основе их совершенных ДНФ:

$l_2 = x_1\overline{x}_2 \vee \overline{x}_1 x_2$, $\bar{l}_2 = x_1 x_2 \vee \overline{x}_1\overline{x}_2$.





Пусть для $n = 2^k$ искомые π-схемы Σ'_n и Σ''_n, реализующие со сложностью 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 $\bar{l}_{2n}$ от БП (x, y), где $x = (x_1, \ldots, x_n)$ и $y = (x_{n+1}, \ldots, x_{2n})$, могут быть построены на основе разложений:

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

$$\bar{l}_{2n}(x, y) = l_n(x) \cdot l_n(y) \vee \bar{l}_n(x) \cdot \bar{l}_n(y).$$

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

Утверждение доказано. $\square$

Замечание 1

Аналогичным образом можно строить π-схему для $l_n^{\sigma}(x_1, \ldots, x_n)$ при разбиении набора ее БП на два поднабора разной длины.

Замечание 2

Если $n = 2^k$, то $L^{\pi}(l_n^{\sigma}) \leqslant n^2$.

36. Теорема Храпченко, нижние оценки сложности линейной функции в классе π-схем

Для пересекающихся подмножеств $\mathcal{N}'$ и $\mathcal{N}''$ множества B^n обозначим через $\mathcal{R}(\mathcal{N}', \mathcal{N}'')$ множество всех пар (α, β), состоящих из соседних по какой-либо БП $x_1, \ldots, x_n$ наборов α и β куба B^n таких, что $\alpha \in \mathcal{N}'$ и $\beta \in \mathcal{N}''$. Пусть, как обычно, $\mathcal{U}^\pi$ — класс π-схем и, в соответствии с общими правилами, $L^\pi(f)$ — сложность реализации ФАЛ f в классе $\mathcal{U}^\pi$.

Утверждение 36.1

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:

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

Следствие

При $n \geqslant 1$ для линейной ФАЛ l_n^{σ}, $\sigma \in B$, выполнены неравенства

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

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 $x_{j_i}^{\sigma_i}$, $i = 1, \ldots, L$. Каждому набору $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\alpha \in N_f$, сопоставим цепь C_α из множества $\widehat{\mathfrak{C}}(\Sigma)$, 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 $\widehat{\mathfrak{S}}(\Sigma)$, состоящее из контактов вида $x_1^{\beta_1}, \ldots, x_n^{\beta_n}$. При этом в соответствии с утв. 35.1 множество $C_\alpha \cap S_\beta$ состоит из одного контакта вида $x_s^{\alpha_s}$, где $\alpha_s \neq \beta_s$.

Рассмотрим для $i = 1, \ldots, L$ следующие множества:

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

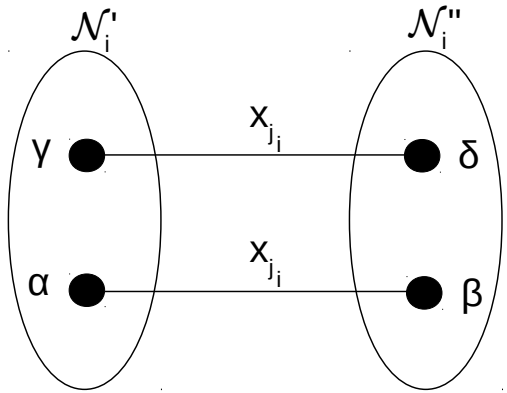
Заметим, что при $i \neq j$ множества Π_i и Π_j ($\mathcal{R}_i$ и $\mathcal{R}_j$) не пересекаются, а объединение всех таких множеств равно множеству Π (соответственно $\mathcal{R}$).

Действительно, любая пара (α, β) из П 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

$$|\mathcal{R}_i| \leqslant |\mathcal{N}'_i| \quad \text{и} \quad |\mathcal{R}_i| \leqslant |\mathcal{N}''_i| \tag{36.1}$$

для всех i, $i = 1, \ldots, L$.



Для этого достаточно убедиться в том, 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_{j_i} и поэтому в случае $\alpha = \gamma$ или $\beta = \delta$ было бы выполнено равенство $(\alpha, \beta) = (\gamma, \delta)$, которое противоречит выбору данных пар.

Из определения и свойств введённых выше множеств, а также неравенств (36.1) следует, что

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

Для последней суммы в силу неравенства Коши-Буняковского

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

и предыдущих соотношений получим

$$|\mathcal{N}'| \cdot |\mathcal{N}''| \geqslant \sum_{i=1}^{L} |\mathcal{R}_i|^2 \geqslant \frac{1}{L} |\mathcal{R}_i|^2, \text{ т.е. } L \geqslant \frac{|\mathcal{R}|^2}{|\mathcal{N}'| \cdot |\mathcal{N}''|}.$$

Утверждение доказано. □

Завершая данный вопрос, докажем следствие из утв. 36.1, то есть докажем для линейной ФАЛ $l_n = x_1 \oplus \ldots \oplus x_n$ нижнюю оценку $L^{\pi}(l_n) \geqslant n^2$.
Напомним, что $N_{l_n} = B^n_{\text{неч.}}$, $\overline{N}_{l_n} = B^n_{\text{чет.}}$ и что любое ребро куба B^n соединяет вершину из $B^n_{\text{неч.}}$ с вершиной из $B^n_{\text{чет.}}$. Напомним также, что $|B^n_{\text{чет.}}| = |B^n_{\text{неч.}}| = 2^{n-1}$ и что число ребер в B^n равно $n \cdot 2^{n-1}$.
Тогда, полагая в утв. 36.1 $f = l_n$, $\mathcal{N}' = B^n_{\text{неч.}}$ и $\mathcal{N}'' = B^n_{\text{чет.}}$, получим

$$L^{\pi}(l_n) \geqslant \frac{(n \cdot 2^{n-1})^2}{2^{n-1} \cdot 2^{n-1}} = n^2.$$

При этом в случае $n = 2^k$ в соответствии с замечанием 2 к утв. 35.2 будет выполняться равенство $L^{\pi}(l_n) = n^2$.

Можно доказать, что $L^{\pi}(l_n) > n^2$, если n не является степенью 2 (задача).

Отсюда следует, в частности, что $L^{\pi}(l_3) = 10$, так как верхняя оценка $L^{\pi}(l_3) \leqslant 10$ доказывается разбиением набора БП (x_1, x_2, x_3) на части длины 1 и 2 с последующим применением замечания 1 к утв. 35.2.

Известно также, что для произвольного натурального n верхнюю оценку $4n^2$ из утв. 35.2 можно понизить до $\frac{9}{8}n^2$.

37. Схемная и алгоритмическая сложность функций, теорема Дж. Сэвиджа. Построение сложно реализуемых функций, гипотеза С. В. Яблонского.

Рассмотрим сначала вопрос о соотношениях между схемной сложностью ФАЛ, то есть сложностью их реализации в каком-либо классе схем, и временно́й сложностью ФАЛ, то есть сложностью их вычисления на машине Тьюринга (МТ).

Возьмем, для примера, ФАЛ $f_n(x_1, \ldots, x_n)$, которая равна 1 на наборе $\alpha = (\alpha_1, \ldots, \alpha_n)$ тогда и только тогда, когда $\alpha_1 = \alpha_n$, $\alpha_2 = \alpha_{n-1}$, $\ldots$, $\alpha_{\lfloor \frac{n}{2} \rfloor} = \alpha_{n-\lfloor \frac{n}{2} \rfloor+1}$ и которая называется ФАЛ **распознавания симметрии** входного набора. Она может быть задана формулой (КНФ) вида

$$f_n(x_1, \ldots, x_n) = \bigwedge_{i=1}^{\lfloor \frac{n}{2} \rfloor} (x_i x_{n-i+1} \vee \overline{x}_i \overline{x}_{n-i+1}),$$

и для нее, очевидно,

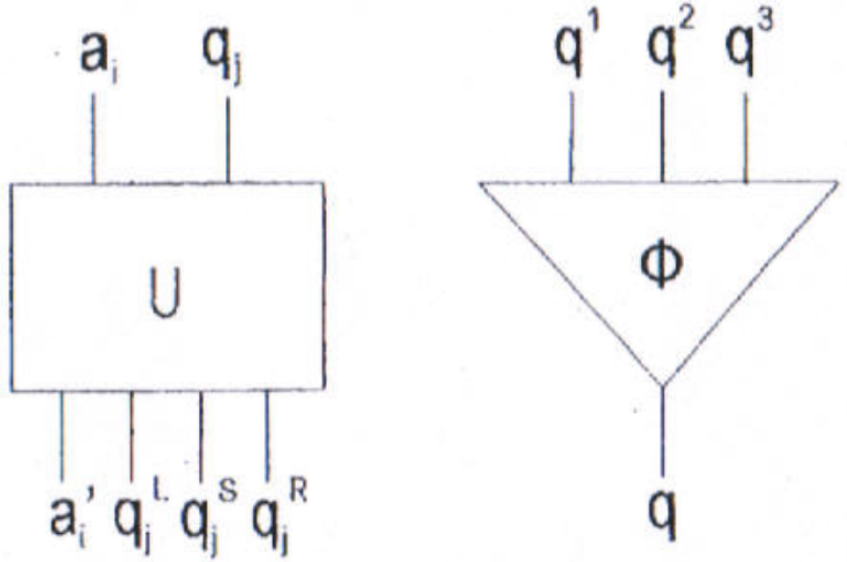
$$L^{\mathrm{C}}(f_n) \leqslant 4 \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor - 1 \leqslant \frac{5}{2} n.$$

С другой стороны, известно, что сложность распознавания симметрии на МТ не меньше, чем $\frac{n^2}{4}$, и не больше, чем $2n^2$.

Установим теперь формальную связь между сложностью ФАЛ и временно́й сложностью машинных вычислений. Наличие такой связи может показаться неожиданным, поскольку схемная сложность ассоциируется скорее с описательной сложностью, нежели со сложностью вычислений. Тем не менее, сложность СФЭ хорошо мажорирует время работы МТ как это утверждает теорема Дж. Сэвиджа.

Рассматриваются обычные (детерминированные) МТ с односторонней бесконечной вправо лентой, алфавитом ленты $A = \{a_1, \ldots, a_m\}$ и алфавитом состояний $Q = \{q_0, \ldots, q_k\}$. **Начальное** состояние обозначается через q_0, а **заключительное** — через q_k. Один из символов ленты называется **пустым** и обозначается через Λ. Он обозначает отсутствие значащего символа в ячейке ленты. В начальный момент на ленте записано исходное слово $x_1, x_2, \ldots, x_n$ и головка МТ обозревает самый левый символ этого слова в состоянии q_0. Все остальные ячейки заполнены символом Λ.

Мы будем применять для моделирования обобщенные СФЭ, у которых на входах и выходах элементов — символы алфавитов A и $\tilde{Q}$, где $\tilde{Q} = Q \cup \{\tilde{q}\}$, а $\tilde{q}$ — новый символ, который называется **холостым** состоянием.
Ясно, что каждый такой элемент можно моделировать обычной (двоичной) СФЭ константной сложности после предварительного кодирования букв алфавитов A и $\tilde{Q}$ конечными двоичными последовательностями. Поэтому переход от обобщенных СФЭ к обычным связан с увеличением сложности лишь в константу раз.



Итак, пусть машина Тьюринга M работает на каждом слове длины n не более T тактов. Построим обобщенную СФЭ, которая моделирует работу M на словах длины n, из преобразующих элементов U и фильтрующих элементов Ф.

Элемент U имеет два входа и четыре выхода. На левый вход U подаются символы $a_i \in A$, на правый $q_j \in \tilde{Q}$. Если $q_j = \tilde{q}$, то элемент U производит тождественное преобразование, то есть

$$a'_i = a_i, q_j^R = q_j^L = q_j^S = \tilde{q}.$$

Если $q_j \neq \tilde{q}$, то в системе команд машины M отыскиваем команду с левой частью $a_i q_j$ и правой частью $a_l q_m L$. Тогда на выходе элемента U появляются значения

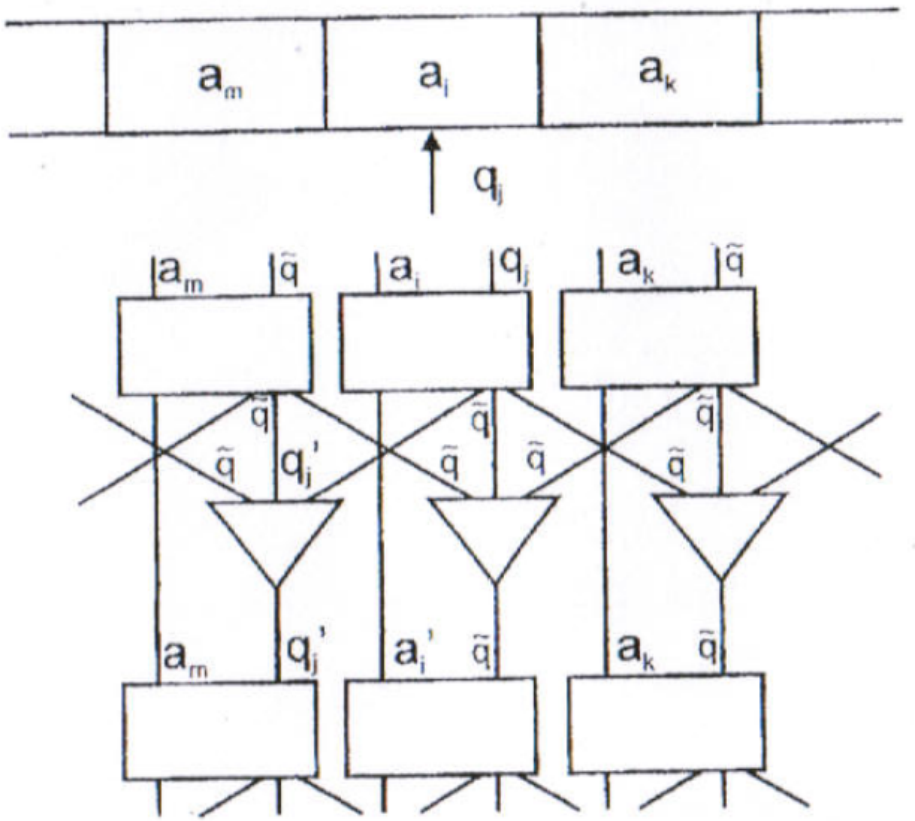
$$a'_i = a_l, q_j^L = q'_m, q_j^R = q_j^S = \tilde{q}.$$

Если символ движения головки L заменить на S или R, то, соответственно, будет $q_j^S = q_m$ или $q_j^R = q_m$, а на других q-выходах $\tilde{q}$.

На входах и выходе элемента Ф возникают только символы алфавита $\tilde{Q}$. Если на одном из входов q^1, q^2, q^3 появляется символ, отличный от $\tilde{q}$, то он проходит на выход (случай, когда несколько входов отличны от $\tilde{q}$, невозможен), а если на всех входах появляется $\tilde{q}$, то выход равен $\tilde{q}$.

Заметим, что если время работы МТ над словом $x_1 \dots x_n$ не превосходит T, то головка может уйти вправо от начального положения не далее, чем на T ячеек. Поэтому достаточно держать в поле зрения зону ленты из T ячеек, которые мы будем нумеровать числами от 1 до T. Схема, которую мы построим, имеет прямоугольный вид. У нее T (двухъярусных) строк и T столбцов. При этом i-я строка ($i = 1, 2, \dots, T$) выходами своит T элементов представляет i-ую конфигурацию машины M, а именно, элемент U j-го ($1 \leqslant j \leqslant T$) столбца — символ, содержащийся в j-ой ячейке, а элемент Ф — состояние машины, обозревающей j-ю ячейку.

При всяком i в точности для одного j состояние отлично от $\tilde{q}$ (а именно, для той ячейки, которая действительно обозревается головкой в i-й конфигурации). На пересечении i-й строки и j-ого столбца в схеме один элемент U и один элемент Ф. Мы будем изображать их один под другим, тем самым каждая строка будет двухъярусной.



Для наглядности сверху показан фрагмент текущей конфигурации, а на входах элементов — соответствующие значения схемы в предположении, что команда машины M имеет вид $a_i q_j \to a'_i q'_j L$.

Утверждение 37.1 (Дж. Сэвидж)

Пусть машина Тьюринга M работает на словах длины n не больше, чем $T_M(n)$ тактов. Тогда ее можно моделировать СФЭ сложности не больше, чем $O(T_M^2(n))$.

Доказательство.

Построенная нами СФЭ моделирует работу машины M. Фактически она воспроизводит последовательность конфигураций при работе машины над входным словом. Из построения ясно, что схема содержит $2T^2$ обобщенных элементов. После замены каждого такого элемента схемой из двоичных элементов сложность возрастает только в константу раз.

Утверждение доказано. □

Легко видеть, что в построенной схеме много «лишних» элементов. Это, например, элементы правого верхнего угла схемы, где длительное время состояние остается холостым. И в оставшейся части схемы существенны только элементы в окрестности нехолостого значения состояния. Это предоставляет большие возможности для упрощения схемы. К. П. Шнорр понизил верхнюю оценку до $O(T_M(n) \log S_M(n) + ||M||)$, где $T_M(n)$ и $S_M(n)$ соответственно число тактов и число ячеек, достаточное для обработки слова длины n машиной Тьюринга, а $||M||$ — число команд машины M.

Рассмотрим теперь вопрос о конструктивном построении сложно реализуемых ФАЛ. Будем говорить, что последовательность ФАЛ $\{f_n\}_{n\geqslant 1}$, где $f_n \in P_2(n)$, является **сложной** (**асимптотически сложной**) тогда и только тогда, когда $L^{\mathrm{C}}(f_n) = L^{\mathrm{C}}(n)$ (соответственно $L^{\mathrm{C}}(f_n) \sim L^{\mathrm{C}}(n)$).

Утверждение 37.2

Для любой асимптотически сложной последовательности ФАЛ $f_1, f_2, \ldots, f_n, \ldots$, содержащий ее инвариантный класс совпадает с классом всех ФАЛ.

Доказательство.

Пусть Q — инвариантный класс ФАЛ такой, что $f_n \in Q(n)$ при всех $n = 1, 2, \ldots$. Из утв. 29.1 следует, что в этом случае

$$L^{\mathrm{C}}(f_n) \lesssim L^{\mathrm{C}}(Q(n)) \lesssim \sigma_Q \frac{2^n}{n},$$

то есть $\sigma_Q = 1$ в силу асимптотической сложности последовательности ФАЛ $f_1, f_2, \ldots$.

Тогда из утв. 27.1, в свою очередь, вытекает, что $Q = P_2$.

Утверждение доказано. $\square$

Алгоритм, который строит последовательность ФАЛ, называется правильным, если наряду с каждой из ее ФАЛ f он строит все ФАЛ из ее «инвариантного» замыкания $\{f\}\rfloor$.

Гипотеза С. В. Яблонского: правильный алгоритм, который строит сложную последовательность ФАЛ, осуществляет перебор всех ФАЛ.