

# Теоретический минимум по «основам кибернетики», 3 курс, 6 семестр

## Часть I

### Минимизация дизъюнктивных нормальных форм и связанные с ней задачи

#### 1. Представление функций алгебры логики (ФАЛ) дизъюнктивными нормальными формами (ДНФ) и его «геометрическая» интерпретация. Совершенная ДНФ и критерий единственности ДНФ.

См. §2 методички, он почти целиком состоит из определений. Список:

- единичный куб (гиперкуб) размерности  $n$ ;
- $i$ -й слой куба  $B^n$ ;
- отношение лексикографического линейного порядка на множестве  $B^n$ ;
- отрезок куба  $B^n$ ;
- расстояние Хэмминга;
- противоположные, соседние (соседние по  $i$ -й переменной) наборы;
- сфера и шар радиуса  $t$  с центром  $\alpha$ ;
- отношение частичного порядка  $\leq$  на  $B^n$ ;
- сравнимые и несравнимые наборы;
- грань куба  $B^n$ , её размерность и ранг;
- обозначения  $\mathcal{X}, P_2(\mathcal{X})$  или  $P_2, X \subset \mathcal{X}, P_2(X), P_2^m(X), X(n), P_2(n), P_2^m(n)$ ;
- таблица значений и столбец значений ФАЛ;
- характеристическое множество ФАЛ  $f$  и характеристическая функция множества  $N_f$ ;
- $P_2(1)$  и «основные» ФАЛ из  $P_2(2)$ , функция голосования;
- ассоциативность, коммутативность, дистрибутивность (в т. ч.  $\&$  относительно  $\vee$  и  $\oplus$ );
- тождества приведения подобных (в т. ч. тождество поглощения);
- линейная функция;
- множество  $B_0$ , буквы, ЭК и ЭД ранга  $r$  от БП  $X(n)$ ;
- ДНФ, КНФ, совершенные ДНФ и КНФ;
- длина ДНФ или КНФ  $\lambda(\mathfrak{A})$ ;
- разложение Шеннона;
- геометрическая интерпретация ДНФ и КНФ, а также совершенных ДНФ и КНФ.

**Лемма.** Совершенная ДНФ ФАЛ  $f \in P_2(n)$  является единственной ДНФ от БП  $X(n)$ , которая реализует эту ФАЛ  $\Leftrightarrow$  когда во множестве  $N_f$  нет соседних наборов.

**Следствие.** Совершенные ДНФ ФАЛ  $\ell_n, \bar{\ell}_n$  являются единственными ДНФ этих ФАЛ от БП  $X(n)$ .

## 2. Сокращённая ДНФ и способы её построения

ФАЛ  $f'$  имплицирует ФАЛ  $f''$  ( $(f' \rightarrow f'') \equiv 1$ ), если  $N_{f'} \subseteq N_{f''}$ .

ФАЛ  $f''$  поглощает ФАЛ  $f'$ , если  $N_{f'} \subseteq N_{f''}$ .

ФАЛ  $f'$  имплицирует ФАЛ  $f'' \Leftrightarrow f'' = f' \vee f''$  или  $f' = f' \cdot f''$ .

ЭК  $K'$  имплицирует ЭК  $K'' \Leftrightarrow K' = K'' \cdot K$ , где  $K$  не имеет общих букв с  $K''$ .

ЭК  $K$  является импликантой ФАЛ  $f$ , если  $K$  имплицирует  $f$ .

ДНФ  $\mathfrak{A}$  называется *ДНФ без поглощений ЭК*, если ни одна из граней  $N_{K_1}, \dots, N_{K_s}$  не содержится ни в одной из других граней покрытия  $N_f = N_{K_1} \cup \dots \cup N_{K_s}$ . Или, другими словами, ни одна ЭК не является импликантой другой ЭК.

Импликанта  $K$  ФАЛ  $f$  называется *простой импликантой  $f$* , если она не поглощается никакой другой отличной от неё импликантой  $f$  (т. е. не имплицирует никакую другую импликанту  $f$ ). С «геометрической» т. з. простые импликанты  $f$  соответствуют максимальным по включению граням множества  $N_f$ .

Дизъюнкция всех простых импликант ФАЛ  $f$  называется её *сокращённой ДНФ*.

Сокращённая ДНФ является ДНФ без поглощений.

**Теорема.** Пусть  $\mathfrak{A}'$  и  $\mathfrak{A}''$  – сокращённые ДНФ ФАЛ  $f'$  и  $f''$  соответственно, а ДНФ  $\mathfrak{A}$  без поглощений получается из формулы  $\mathfrak{A}' \cdot \mathfrak{A}''$  в результате раскрытия скобок и приведения подобных. Тогда  $\mathfrak{A}$  – сокращённая ДНФ ФАЛ  $f = f' \cdot f''$ .

**Следствие.** Если ДНФ  $\mathfrak{A}$  без поглощений получается из КНФ  $\mathfrak{B}$  ФАЛ  $f$  в результате раскрытия скобок и приведения подобных, то  $\mathfrak{A}$  – сокращённая ДНФ ФАЛ  $f$ .

Метод Блейка позволяет получить сокращённую ДНФ ФАЛ  $f$  из произвольной ДНФ  $f$ .

ДНФ  $\mathfrak{A}'$  называется *расширением ДНФ  $\mathfrak{A}$* , если она получена путём выделения с помощью тождеств ассоциативности и коммутативности подформул вида  $x_i K' \vee \bar{x}_i K''$ , применением к ним *тождества обобщённого склеивания* ( $x_i K' \vee \bar{x}_i K'' = x_i K' \vee \bar{x}_i K'' \vee K' K''$ ) и последующим приведением подобных.

ДНФ  $\mathfrak{A}'$  называется *строгим расширением ДНФ  $\mathfrak{A}$* , если она является расширением  $\mathfrak{A}$  и содержит ЭК, не являющуюся импликантой ни одной ЭК из  $\mathfrak{A}$ .

**Теорема.** ДНФ без поглощений ЭК является сокращённой ДНФ  $\Leftrightarrow$  когда она не имеет строгих расширений.

**Следствие.** Из любой ДНФ  $\mathfrak{A}$  ФАЛ  $f$  можно получить сокращённую ДНФ этой ФАЛ в результате построения последовательных строгих расширений и приведения подобных до получения ДНФ без поглощений ЭК, не имеющей строгих расширений.

### 3. Тупиковая ДНФ, ядро и ДНФ пересечение тупиковых. ДНФ Квайна, критерий вхождения простых импликант в тупиковые ДНФ и его локальность.

ДНФ  $\mathfrak{A}$ , реализующая ФАЛ  $f$ , называется *тупиковой ДНФ*, если  $f \neq \mathfrak{A}'$  для любой ДНФ  $\mathfrak{A}'$ , полученной из  $\mathfrak{A}$  в результате удаления некоторых букв или целых ЭК.

В тупиковую ДНФ ФАЛ  $f$  могут входить только простые импликанты  $f$ . Она является ДНФ без поглощений ЭК. С «геометрической» т. з. тупиковая ДНФ ФАЛ  $f$  задаёт тупиковое покрытие множества  $N_f$  максимальными гранями  $f$  и обратно.

Минимальная ДНФ — ДНФ, имеющая минимальный ранг среди ДНФ реализующих  $f$ .

Кратчайшая ДНФ — ДНФ, имеющая минимальную длину среди ДНФ реализующих  $f$ .

Минимальная ДНФ всегда является тупиковой, среди кратчайших обязательно найдётся тупиковая.

Набор  $\alpha$  называется *ядровой точкой* ФАЛ  $f$ , если  $\alpha \in N_f$  и  $\alpha$  входит только в одну максимальную грань ФАЛ  $f$ . При этом грань  $N_K$ , являющаяся максимальной гранью ФАЛ  $f$  и содержащая точку  $\alpha$ , называется *ядровой гранью* ФАЛ  $f$ . Совокупность всех различных ядровых граней ФАЛ  $f$  называется *ядром* ФАЛ  $f$ .

**Лемма.** ДНФ  $\cap T$  ФАЛ  $f$  состоит из тех простых импликант ФАЛ  $f$ , которые соответствуют ядровым граням этой ФАЛ  $f$ .

ДНФ  $\cap T$  в общем случае не реализует саму ФАЛ  $f$  и может быть пустой. ДНФ  $\Sigma T$  всегда реализует ФАЛ  $f$ .

ФАЛ называется *ядровой*, если все её максимальные грани являются ядровыми.

**Следствие.** Сокращённая ДНФ ядровой ФАЛ является её единственной тупиковой ДНФ.

ДНФ, получающаяся из сокращённой ДНФ ФАЛ  $f$  удалением тех ЭК  $K$ , для которых грань  $N_K$  покрывается ядром ФАЛ  $f$ , но не входит в него, называется *ДНФ Квайна* этой ФАЛ.

ДНФ  $\cap T \subseteq$  ДНФ  $\Sigma T \subseteq$  ДНФ Квайна  $\subseteq$  сокращённая ДНФ.

Для  $\alpha \in N_f$  обозначим через  $\Pi_\alpha(f)$  множество всех проходящих через  $\alpha$  максимальных граней ФАЛ  $f$ , будем называть его *пучком ФАЛ  $f$  через точку  $\alpha$* .

Точку  $\alpha$  будем называть *регулярной точкой* ФАЛ  $f$ , если найдётся точка  $\beta \in N_f$ , для которой имеет место строгое включение  $\Pi_\beta(f) \subset \Pi_\alpha(f)$ .

Грань  $N_K$  ФАЛ  $f$  называется *регулярной гранью* этой ФАЛ, если все точки  $N_K$  регулярны.

Любая неядровая точка ядровой грани регулярна. Грань, которая не входит в ядро, но покрывается им, регулярна.

**Теорема.** Простая импликанта  $K$  ФАЛ  $f$  входит в ДНФ  $\Sigma T \Leftrightarrow$  когда грань  $N_K$  не является регулярной гранью этой ФАЛ.

Для каждой максимальной грани  $\mathcal{N}$  ФАЛ  $f$  положим  $S_0(\mathcal{N}, f) = \{\mathcal{N}\}$ , затем индукцией по  $r$  определим *окрестность порядка  $r$  грани  $\mathcal{N}$  функции  $f$*   $S_r(\mathcal{N}, f)$  как множество всех тех максимальных граней ФАЛ  $f$ , которые имеют непустое пересечение хотя бы с одной гранью из  $S_{r-1}(\mathcal{N}, f)$ .

Вопрос о вхождении простой импликанты  $K$  в ДНФ  $\cap T$  (ДНФ  $\Sigma T$ ) этой ФАЛ можно решить, рассматривая окрестность  $S_1(N_K, f)$  (соответственно  $S_2(N_K, f)$ ).

#### 4. Особенности ДНФ линейных и монотонных ФАЛ. Функция покрытия, таблица Квайна и построение всех тупиковых ДНФ.

ФАЛ  $f$  *линейно зависит от БП  $x_i$*  ( $x_i$  является *линейной БП*  $f$ ), если  $f(\alpha) \neq f(\beta)$  для любых соседних по  $x_i$  наборов  $\alpha$  и  $\beta$ .

Равенство  $f(x_1, \dots, x_n) = x_i \oplus f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$  равносильно линейности по БП  $x_i$  ФАЛ  $f$ .

ФАЛ  $f$  является линейной  $\Leftrightarrow$  когда она линейно зависит от всех своих существенных БП.

Если ФАЛ  $f$  линейно зависит от БП  $x_i$ , то в любую импликанту этой ФАЛ входит одна из букв  $x_i, \bar{x}_i$ .

ФАЛ  $f$  называется *монотонной*, если  $f(\alpha) \leq f(\beta)$  для любых наборов  $\alpha$  и  $\beta$  таких, что  $\alpha \leq \beta$ .

ФАЛ  $f$  *монотонно зависит от БП  $x_i$*  ( $x_i$  является *монотонной БП* ФАЛ  $f$ ), если  $f(\alpha) \leq f(\beta)$  для любых соседних по  $x_i$  наборов  $\alpha$  и  $\beta$  таких, что  $\alpha \leq \beta$ .

ФАЛ является монотонной  $\Leftrightarrow$  когда она монотонно зависит от всех своих БП.

Если ФАЛ  $f$  монотонно зависит от БП  $x_i$ , то ни одна из её простых импликант не содержит букву  $\bar{x}_i$ .

Частные случаи монотонной зависимости  $f$  от  $x_i$ : конъюнктивная ( $f = x_i \cdot g$ ) и дизъюнктивная ( $f = x_i \vee g$ ), где ФАЛ  $g$  получается подстановкой вместо  $x_i$  константы 1 или 0 соответственно.

При конъюнктивной зависимости буква  $x_i$  входит в любую простую импликанту ФАЛ  $f$ , в случае дизъюнктивной зависимости буква  $x_i$  не входит ни в одну простую импликанту  $f$ , отличную от  $x_i$ .

ФАЛ  $f(x_1, \dots, x_n)$  зависит от БП  $x_i$  *инмонотонно* (инконъюнктивно, индизъюнктивно), если ФАЛ  $f(x_1, \dots, x_{i-1}, \bar{x}_i, x_{i+1}, \dots, x_n)$  зависит от  $x_i$  монотонно (соответственно

конъюнктивно, дизъюнктивно).

Сопоставим каждому набору  $\beta \in B^n$  монотонную ЭК  $K_\beta^+$ , состоящую только из тех букв  $x_j$ , для которых  $\beta\langle j \rangle = 1$ . Любая монотонная ЭК может быть представлена в таком виде.

Набор  $\alpha$  называется *нижней единицей* монотонной ФАЛ  $f$ , если  $\alpha \in N_f$  и  $\forall \beta \neq \alpha, \beta \leq \alpha$  выполняется  $f(\beta) = 0$ . Множество всех нижних единиц монотонной ФАЛ  $f$  обозначается  $N_f^+$ .

**Лемма.** *Сокращённая ДНФ  $\mathfrak{A}$  монотонной ФАЛ  $f$  является единственной тупиковой ДНФ этой ФАЛ и имеет вид*

$$\mathfrak{A} = \bigvee_{\beta \in N_f^+} K_\beta^+.$$

При этом все наборы из  $N_f^+$  являются ядровыми точками ФАЛ  $f$ .

**Замечание.** *Можно сказать, что сокращённая ДНФ монотонной ФАЛ состоит из её простых импликант, не содержащих отрицаний и соответствующих нижним единицам.*

**Следствие.** *Монотонная ФАЛ является ядровой ФАЛ.*

Пусть  $\mathcal{N} = \{\alpha_1, \dots, \alpha_s\}$  — конечное множество, а  $\mathfrak{N} = \{\mathcal{N}_1, \dots, \mathcal{N}_p\}$  — система его подмножеств, образующих покрытие  $\mathcal{N}$ . Сопоставим паре  $(\mathcal{N}, \mathfrak{N})$  матрицу  $M \in M^{p,s}$ , для которой  $M\langle i, j \rangle = 1 \Leftrightarrow \alpha_j \in \mathcal{N}_i$ .

Считаем, что  $i$ -я строка соответствует подмножеству  $\mathcal{N}_i$  системы  $\mathfrak{N}$ , а  $j$ -й столбец — элементу  $\alpha_j$  множества  $\mathcal{N}$ .

$i$ -я строка  $M$  покрывает её  $j$ -й столбец, если  $M\langle i, j \rangle = 1$ .

Система строк с номерами из  $I$  образует *покрытие матрицы  $M$* , если каждый её столбец покрывается хотя бы одной строкой с номером из  $I$ . Аналогично понимается покрытие одного множества строк  $M$  другим множеством строк.

Покрытие матрицы  $M$ , в котором ни одна строка не покрывается другой строкой называется *неприводимым*. Покрытие, не имеющее собственных подпокрытий, называется *тупиковым*.

ФАЛ  $F(y)$  называется *функцией покрытия* матрицы  $M$  без нулевых столбцов, если  $F(\beta) = 1 \Leftrightarrow$  когда система строк матрицы  $M$  с номерами из  $I(\beta) = \{i | \beta\langle i \rangle = 1\}$  образует её покрытие.

**Лемма.** *Функция покрытия  $F(y_1, \dots, y_p)$  матрицы  $M \in B^{p,s}$  без нулевых столбцов задаётся КНФ вида*

$$F(y_1, \dots, y_p) = \bigwedge_{j=1}^s \left( \bigvee_{\substack{1 \leq i \leq p \\ M\langle i, j \rangle = 1}} y_i \right).$$

**Следствие.** В результате раскрытия скобок и приведения пободных из КНФ для  $F$  (см. лемму) можно получить сокращённую ДНФ ФАЛ  $F(y)$ , простые импликанты которой взаимно однозначно соответствуют тупиковым покрытиям матрицы  $M$ .

Задача построения всех тупиковых ДНФ ФАЛ  $f$  на основе её сокращённой ДНФ сводится к рассмотренной выше задаче о покрытии, если  $\mathcal{N} = N_f$ , а  $\mathfrak{A}$  — система всех максимальных граней  $f$ .

## 5. Градиентный алгоритм и оценка длины градиентного покрытия, лемма о «протыкающих» наборах. Использование градиентного алгоритма для построения ДНФ.

Градиентный алгоритм ориентирован на выделение из заданного покрытия достаточно «коротких» подпокрытий или, иначе, на построение достаточно «коротких» покрытий для заданной матрицы.

Шаг: в матрице выбирается и включается в покрытие такая строка, которая покрывает наибольшее число ещё не покрытых столбцов (если таких строк несколько, из них выбирается строка с наименьшим номером).

Останов: после того шага, на котором получилось покрытие.

**Теорема.** Пусть для действительного  $\gamma$ ,  $0 < \gamma \leq 1$ , в каждом столбце матрицы  $M \in M^{p,s}$  имеется не меньше чем  $\gamma \cdot p$  единиц. Тогда покрытие матрицы  $M$ , получаемое с помощью градиентного алгоритма, имеет длину не больше чем  $\lceil \frac{1}{\gamma} \ln^+(\gamma s) \rceil + \frac{1}{\gamma}$ , где  $\ln^+(x) = 0$  при  $0 < x < 1$  и  $\ln^+(x) = \ln(x)$  при  $x \geq 1$ .

Задача о «протыкании» системы  $\mathfrak{A}$ , состоящей из подмножеств  $\mathcal{N}_1, \dots, \mathcal{N}_p$  множества  $\mathcal{N} = \{\alpha_1, \dots, \alpha_s\}$ , заключается в нахождении такого подмножества множества  $\mathcal{N}$ , в котором  $\forall i \in [1, p]$  имеется хотя бы один элемент из  $\mathcal{N}_i$ .

**Лемма.**  $\forall m, n \in \mathbb{N}$ ,  $m \leq n$  в кубе  $B^n$  всегда найдётся подмножество мощности не более чем  $n \cdot 2^m$ , протыкающее все грани ранга  $m$ .

## 6. Задача минимизации ДНФ. Поведение функции Шеннона и оценки типичных значений для ранга и длины ДНФ.

На множестве ДНФ задаётся неотрицательный функционал сложности  $\psi$ , обладающий свойством монотонности, т. е.  $\forall \text{ДНФ } \mathfrak{A} \exists \psi(\mathfrak{A}) \geq 0 : \psi(\mathfrak{A}') \geq \psi(\mathfrak{A}'')$ , если ДНФ  $\mathfrak{A}''$  получается из ДНФ  $\mathfrak{A}'$  удалением букв или ЭК.

Примеры: длина  $\lambda(\mathfrak{A})$ , ранг  $R(\mathfrak{A})$ , «формульная» сложность  $L(\mathfrak{A})$ .

Задача минимизации ДНФ относительно функционала сложности  $\psi$  состоит в нахождении для заданной ФАЛ  $f$  ДНФ  $\mathfrak{A}$ , такую что  $\psi(\mathfrak{A}) = \min \psi(\mathfrak{A}')$ , где минимум берётся по всем ДНФ  $\mathfrak{A}'$  ФАЛ  $f$ .

При этом ДНФ  $\mathfrak{A}$  называется *минимальной относительно функционала  $\psi$*  или  *$\psi$ -минимальной ДНФ*. Значение  $\psi(\mathfrak{A})$  называется *сложностью ФАЛ  $f$  относительно функционала  $\psi$*  или  *$\psi$ -сложностью ФАЛ  $f$*  в классе ДНФ.

$\lambda$ -минимальную (по длине) ДНФ будем называть *кратчайшей*, а  $R$ -минимальную (по рангу) — просто *минимальной*.

*Функция Шеннона* для класса ДНФ относительно функционала  $\psi$ :

$$\psi(n) = \max_{f \in P_2(n)} \psi(f).$$

**Лемма.**  $\forall n \in \mathbb{N}$  имеют место соотношения  $\lambda(n) = 2^{n-1}$ ,  $R(n) = n \cdot 2^{n-1}$ .

Рассмотрим отрезок  $[\psi'(n), \psi''(n)]$ , в который попадают значения  $\psi(n)$  для почти всех ФАЛ  $f \in P_2(n)$ . Если границы  $\psi'(n)$  и  $\psi''(n)$  асимптотически равны  $\psi(n)$ , то говорят, что для параметра  $\psi$  имеет место *эффект Шеннона*.

Для параметров  $\lambda$  и  $R$  эффект Шеннона отсутствует.

**Попытка интерпретации стр. 50—51. Вообще, вряд ли это будет в теореме на «3».**

Введём дискретную векторную случайную величину  $\xi$  состоящую из  $2^n$  случайных величин, принимающих с равной вероятностью значение 0 или 1. Введём дискретную случайную величину  $\tilde{\xi}$ , равную сумме элементов  $\xi$ .

Каждая реализация  $\xi$  соответствует какой-либо ФАЛ  $f$  от  $n$  переменных (равна её вектору значений). Если зафиксировать реализацию  $\xi$  и соответствующую ФАЛ  $f$ , то соответствующая реализация  $\tilde{\xi}$  будет равна мощности множества  $N_f$  для ФАЛ  $f$ .

$\mathbb{E}\tilde{\xi} = 2^{n-1}$ , отступим влево и вправо на  $t = \lceil n \cdot 2^{n/2} \rceil$ , получим интервал  $I = (2^{n-1} - t, 2^{n-1} + t)$ .

Применяем к случайной величине  $\tilde{\xi}$  неравенство Чебышева и устанавливаем, что доля тех ФАЛ  $f \in P_2(n)$ , для которых  $|N_f| \notin I$  стремится к 0 при  $n \rightarrow \infty$ .

Это означает, что для почти всех ФАЛ  $f \in P_2(n)$  выполнено (для проверки раскрыть скобки)

$$|N_f| = 2^{n-1}(1 \pm O(n \cdot 2^{-n/2})).$$

То есть длина совершенной ДНФ у почти всех ФАЛ из  $P_2(n)$  асимптотически равна  $2^{n-1}$ .

**Лемма.** Для почти всех ФАЛ  $f \in P_2(n)$  выполняются неравенства

$$\lambda(f) \leq \frac{3}{4} \cdot 2^{n-1}(1 + O(n \cdot 2^{-n/2})),$$

$$R(f) \leq \frac{3}{4} n \cdot 2^{n-1}(1 + O(n \cdot 2^{-n/2})).$$

## 7. Алгоритмические трудности минимизации ДНФ и оценки максимальных значений некоторых связанных с ней параметров. Теорема Ю. И. Журавлёва о ДНФ сумма минимальных.

Функция Шеннона для параметра  $\psi$  в классе ДНФ:  $\psi(n) = \max_{f \in P_2(n)} \psi(f)$ .

Обозначим значение функции Шеннона для следующих параметров: число тупиковых ДНФ —  $\tau(n)$ , число минимальных ДНФ —  $\mu(n)$  и длина сокращённой ДНФ у ФАЛ из  $P_2(n)$  —  $\lambda_{\text{сокр.}}(n)$  (ДНФ рассматриваются с точностью до перестановки ЭК и букв в них).

**Лемма.** Для ФАЛ  $f$  из  $P_2(n)$ ,  $n \geq 4$ , вида  $f(x_1, \dots, x_n) = g(x_1, x_2, x_3) \cdot (x_4 \oplus \dots \oplus x_n)$ , где  $\bar{N}_g = \{(000), (111)\}$ , число тупиковых (минимальных) ДНФ равно  $5^{2^{n-4}}$  (соответственно  $2^{2^{n-4}}$ ).

**Следствие.**  $\tau(n) \geq 5^{2^{n-4}}$ ,  $\mu(n) \geq 2^{2^{n-4}}$ .

Выберем множество номеров  $I \subseteq [0, n]$ , зафиксируем объединение всех слоёв куба  $B^n$  с номерами из  $I$ , обозначим характеристическую функцию этого объединения как  $\mathfrak{s}_n^I$ . Числа из  $I$  назовём *рабочими числами* ФАЛ  $\mathfrak{s}_n^I$ .

ФАЛ  $\mathfrak{s}_n^I$  является *симметрической*, т. е. не изменяет своё значение при любой перестановке аргументов. Наоборот тоже верно: любая симметрическая ФАЛ совпадает с одной из ФАЛ вида  $\mathfrak{s}_n^I$ .

Симметрическая ФАЛ, отличная от константы, является существенной. Рабочими числами симметрических ФАЛ  $\ell_n$  и  $\bar{\ell}_n$  являются все нечётные и все чётные числа отрезка  $[0, n]$  соответственно.

Симметрическая ФАЛ является *поясковой*, если её рабочие числа образуют отрезок. Вид её сокращённой ДНФ:

$$\mathfrak{s}_n^{[r,p]}(x_1, \dots, x_n) = \bigvee_{\substack{1 \leq i_1 < \dots < i_{n+r-p} \leq n \\ \sigma_1 + \dots + \sigma_{n+r-p} = r}} x_{i_1}^{\sigma_1} \dots x_{i_{n+r-p}}^{\sigma_{n+r-p}}.$$

**Лемма.**  $\lambda_{\text{сокр.}}(n) \geq e_1 \frac{3^n}{n}$ , где  $e_1$  — некоторая константа.

Функция  $f(x_1, \dots, x_n)$  называется *цепной* (циклической) *функцией длины  $t$* , если её сокращённая ДНФ с «геометрической» т. з. представляет собой цепь (соответственно цикл) из  $t$  последовательно соединённых рёбер  $\mathcal{N}_1, \dots, \mathcal{N}_t$  куба  $B^n$ .

**Теорема.**  $\forall n \in \mathbb{N}, n \geq 3$ , в  $P_2(n)$  существуют ФАЛ  $f'$  и  $f''$ , имеющие общую простую импликанту  $K$ , которая входит в ДНФ  $\Sigma M$  одной, но не входит в ДНФ  $\Sigma M$  другой из этих ФАЛ и для которой  $S_{n-3}(N_K, f') = S_{n-3}(N_K, f'')$ .

## Недостающее

- Часть II (вопросы 8–16) в данном файле отсутствует.



- Вопрос 16 не должен быть в билетах (только как дополнительный вопрос).

## Часть III

# Синтез и сложность управляющих систем

## 17. Задача синтеза. Методы синтеза схем на основе ДНФ и связанные с ними верхние оценки сложности функций.

Введём обозначения:  $\mathcal{U}$  — некоторый полный класс схем (из рассмотренных во II части),  $\Psi \geq 0$  — функционал сложности схем класса  $\mathcal{U}$  со свойством монотонности.

Сложность системы ФАЛ  $F$  относительно функционала  $\Psi$  в классе  $\mathcal{U}$ :  $\Psi(F) = \min_{\Sigma \in \mathcal{U} \text{ реализ. } F} \Psi(\Sigma)$ . При этом схема  $\Sigma$ , реализующая  $F$ , для которой  $\Psi(\Sigma) = \Psi(F)$ , называется *минимальной схемой* в классе  $\mathcal{U}$  относительно  $\Psi$ .

Если функционал  $\Psi$  совпадает с  $L$ ,  $D$ ,  $R$  (введены во II части), будем называть его *сложностью, глубиной, рангом* системы ФАЛ  $F$  соответственно.

*Функция Шеннона* для класса  $\mathcal{U}$  относительно функционала сложности  $\Psi$ :  $\Psi(n) = \max_{f \in P_2(n)} \Psi(f)$ .

Будем обозначать сложность и функцию Шеннона для некоторого класса  $A$  как  $\Psi_B^A(F)$  и  $\Psi_B^A(n)$  соответственно, будем опускать нижний индекс  $B$ , если  $B = B_0$ .

Если  $\mathcal{U}' \supseteq \mathcal{U}''$ , то  $\Psi'(F) \leq \Psi''(F)$ . В частности  $\Psi_B^C(F) \leq \Psi_B^D(F)$  и  $\Psi_B^K(F) \leq \Psi_B^\pi(F)$ .

Для сложности системы ФАЛ  $F = (f_1, \dots, f_m)$  в любом из рассматриваемых классов схем выполняется  $\max_{1 \leq i \leq m} L(f_i) \leq L(F) \leq \sum_{i=1}^m L(f_i)$ .

**Лемма** (моделирование совершенной ДНФ).  $\forall$  ФАЛ  $f(x_1, \dots, x_n) \neq 0 \exists$  формула  $\mathcal{F}_f \in \mathcal{U}^\Phi$  и  $\pi$ -схема  $\Sigma_f \in \mathcal{U}^\pi$ , реализующие ФАЛ  $f$ , для которых выполняется

$$L(\mathcal{F}_f) \leq 2n \cdot |N_f| - 1,$$

$$L(\Sigma_f) \leq n \cdot |N_f|.$$

**Следствие.** Если учесть, что ФАЛ 0 можно реализовать  $\pi$ -схемой и формулой из  $\mathcal{U}^\Phi$ , имеющими сложность 2, то выполняется

$$L^C(n) \leq L^\Phi(n) \leq n \cdot 2^{n+1} - 1,$$

$$L^K(n) \leq L^\pi(n) \leq n \cdot 2^n.$$

**Следствие.**  $D(n) \leq n + \lceil \log_2(n) \rceil + 2$ .

Получается из доказанного в части II соотношения для подобных формул с поднятыми отрицаниями  $D(\mathcal{F}) \leq \lceil \log_2(L(\mathcal{F}) + 1) \rceil + \text{Alt}(\mathcal{F})$ .

**Лемма** (моделирование совершенной ДНФ с использованием КД).  $\forall$  ФАЛ  $f(x_1, \dots, x_n) \neq 0$   $\exists$  формула  $\mathcal{F}_f \in \mathcal{U}^\Phi$  и  $\pi$ -схема  $\Sigma_f \in \mathcal{U}^\pi$ , реализующие ФАЛ  $f$ , для которых выполняется

$$L(\mathcal{F}_f) \leq 2^{n+1} + |N_f| - 4,$$

$$L(\Sigma_f) \leq 2^n + |N_f| - 2.$$

**Следствие.**

$$L^\Phi(n) \leq 3 \cdot 2^n - 4.$$

$$L^\pi(n) \leq 2^{n+1} - 2,$$

Результатом применения операции присоединения вершины  $v$  к вершине  $w$  называется СФЭ  $\Sigma'$ , получаемая из СФЭ  $\Sigma$  в результате удаления вершины  $v$ , переноса начала исходивших из  $v$  дуг в  $w$  и переноса всех выходных БП  $v$  в  $w$ .

Две вершины СФЭ называются эквивалентными, если в них реализуются равные ФАЛ.

Приведённая (т. е. без висячих вершин) схема называется строго приведённой, если в ней нет эквивалентных вершин. Из любой СФЭ можно получить эквивалентную ей строго приведённую СФЭ с помощью операции присоединения эквивалентных вершин и операции удаления висячих вершин.

Аналогичным образом определяется операция присоединения вершин в КС, с той лишь разницей, что на неё не накладываются какие-либо ограничения, связанные с достижимостью вершин.

Для множества ФАЛ  $G \subseteq P_2(n)$  через  $\vec{G}$  будем обозначать систему, состоящую из различных ФАЛ множества  $G$ , упорядоченных в соответствии с номерами их столбцов значений.

Обозначения для некоторых функций порядка  $n$ :

- $\ell_n$  и  $\bar{\ell}_n$  — линейные ФАЛ;
- $\mu_n$  — мультиплексорная ФАЛ;
- $\bar{Q}_n$  и  $\bar{J}_n$  — дешифратор и дизъюнктивный дешифратор;
- $\vec{P}_2(n)$  — универсальная система.

**Лемма.**  $\forall n \in \mathbb{N} \exists$  СФЭ  $U_n \in \mathcal{U}_B^C$ , которая реализует систему ФАЛ  $\vec{P}_2(n)$ , сложности  $2^{2^n} - n$ .

**Следствие.**  $L_B^C(\vec{P}_2(n)) \leq 2^{2^n} - n$ .

## 18. Нижние оценки сложности ФАЛ, реализация некоторых ФАЛ и минимальность некоторых схем.

**Лемма.** Если ФАЛ  $f(x_1, \dots, x_n)$  существенно зависит от всех своих БП, то

$$L^C(f) \geq n - 1,$$

$$L^K(f) \geq n.$$

Если при этом ФАЛ  $f$  не является монотонной ФАЛ, то

$$L^C(f) \geq n,$$

Если есть существенная зависимость от всех своих БП и каждая БП  $x_i$ ,  $i \in [1, k]$ , не является ни монотонной, ни немонотонной БП ФАЛ  $f$ , то

$$L^K(f) \geq n + k.$$

**Следствие.**

$$L^C(\ell_n) \geq n, \quad L^C(\mu_n) \geq 2^n + n,$$

$$L^K(\ell_n) \geq 2n, \quad L^K(\mu_n) \geq 2^n + 2n.$$

**Замечание.** Формула  $f = \overline{(x_1 \cdots x_n)}$  и  $\pi$ -схема, моделирующая ЭД  $f = \bar{x}_1 \vee \cdots \vee \bar{x}_n$ , являются минимальными в классах СФЭ и КС соответственно, при этом  $L^C(f) = n$ ,  $L^K(f) = n$ .

**Лемма.** Для системы  $F = (f_1, \dots, f_m)$ , состоящей из попарно различных ФАЛ от переменных (от констант), справедливо

$$L^C(F) \geq m \quad (\text{соответственно } L^K(F) \geq m).$$

**Следствие.**

$$L^C(\vec{Q}_n) \geq 2^n, \quad L^C(\vec{J}_n) \geq 2^n, \quad L^C(\vec{P}_2(n)) \geq 2^{2^n} - n,$$

$$L^K(\vec{Q}_n) \geq 2^n, \quad L^K(\vec{J}_n) \geq 2^n, \quad L^K(\vec{P}_2(n)) \geq 2^{2^n} - 2.$$

**Лемма.**  $\forall n \in \mathbb{N}$  выполняются неравенства [здесь было много верхних оценок для  $\vec{Q}_n$ ,  $\vec{J}_n$ ,  $\mu_n$ ,  $\ell_n$  и  $\bar{\ell}_n$  в разных классах, но формулировка билета не предусматривает верхних оценок.]

**Следствие.**  $L^C(\vec{Q}_n) \sim L^C(\vec{J}_n) \sim 2^n$ .

**Лемма.** Если система ФАЛ  $F = (f_1, \dots, f_m)$  состоит из попарно различных ФАЛ от БП  $X(n)$ , отличных от 0 и 1, то  $L^K(F) \geq 2^{1-n} \sum_{j=1}^m |N_{f_j}|$ .

**Следствие.**  $L^K(J_n) \geq 2^{n+1} - 2$ .

**Замечание.** (1, 4)-КС с входом  $a$  из двух непересекающихся  $(a-a)$ -цепей (т. е. циклов) с ЭК проводимости  $\bar{x}_1 x_2 x_1$  и  $\bar{x}_1 \bar{x}_2 x_1$  является минимальным дизъюнктивным контактным дешифратором порядка 2.

**Лемма.** Если для ФАЛ  $f \in P_2(n)$  и  $\forall \sigma \in \{0, 1\}$  ФАЛ  $f_\sigma(x_1, \dots, x_{n-1}, \sigma) \neq \text{const}$ , то  $L_{\&, \vee}^C(f) = \min\{L_{\&, \vee}^C(f_0), L_{\&, \vee}^C(f_1)\} + 2$ .

**Следствие.**  $L^C(\mu_n) \geq 2^{n+1} + n - 1$ .

**Замечание.** Формула  $\bar{x}_1 y_0 \vee x_1 y_1$  является минимальной СФЭ, реализующей ФАЛ  $\mu_1$  и  $L^C(\mu_1) = 4$ .

**Следствие.**  $D(\mu_n) \geq n + 1$ .

## 19. Метод каскадов для КС и СФЭ, примеры его применения. Метод Шеннона.

Метод каскадов позволяет строить КС и СФЭ, многократно использующие «промежуточные результаты».

**Лемма.**  $\forall n \in \mathbb{N}$  и  $\forall \sigma \in \{0, 1\}$  выполняются неравенства

$$L^K(\ell_n^\sigma) \leq 4n - 4 + \left\lfloor \frac{1}{n} \right\rfloor,$$

$$L^K(\vec{P}_2(n)) \leq 2 \cdot 2^{2^n},$$

$$L^K(\vec{J}_n) \leq 2^{n+2} - 6.$$

Метод Шеннона позволяет строить КС и СФЭ и установить порядок роста функций Шеннона  $L^C(n)$  и  $L^K(n)$ .

Метод Шеннона основан на разложении Шеннона по  $q$  переменным. При этом мы раскладываем функцию на подфункции от  $q$  переменных, которые в разложении домножаются на функции вида  $x_{q+1}^{\sigma_{q+1}} \cdots x_n^{\sigma_n}$  от  $(n - q)$  переменных. Все указанные подфункции от  $q$  переменных мы реализуем с помощью универсального многополюсника порядка  $q$  (т. е. схемы, которая реализует все функции от  $q$  переменных). Потом присоединяем к выходам универсального многополюсника, к  $q$  информационным входам мультиплексора порядка  $(n - q)$ , т. е. у него  $(n - q)$  адресных переменных, с помощью которых «адресуются» конкретные функции, реализуемые универсальным многополюсником.

Полагаем  $q = \lfloor \log_2(n - 2 \log_2 n) \rfloor$ .

**Теорема.** Для функций Шеннона в классах СФЭ и КС выполняется:

$$L^C(n) \lesssim 8 \frac{2^n}{n},$$

$$L^K(n) \lesssim 4 \frac{2^n}{n}.$$

## 20. Нижние мощностные оценки функций Шеннона

Мощностной метод Шеннона основан на том, что число ФАЛ от БП  $x_1, \dots, x_n$  не меньше числа попарно неэквивалентных схем, сложность которых не превосходит соответствующего значения функции Шеннона от  $n$ .

Обозначим через  $\mathcal{U}(\Psi, n)$  множество тех схем  $\Sigma \in \mathcal{U}$ , которые реализуют одну ФАЛ  $f$  из  $P_2(n)$  и для которых  $\Psi(\Sigma) \leq \Psi(f)$ .

Имеет место «мощностное» равенство  $|\mathcal{U}(\Psi(n), n)| = 2^{2^n}$ .

Верхние оценки, установленные ранее (в части II):

$$\|\mathcal{U}^C(L, n)\| \leq (8(L + n))^{L+1},$$

$$\|\mathcal{U}^\Phi(L, n)\| \leq (8n)^{L+1},$$

$$\|\mathcal{U}^K(L, n)\| \leq (8nL)^L,$$

$$\|\mathcal{U}^\pi(L, n)\| \leq (12n)^L,$$

$$\|\mathcal{U}^\Phi[D, n]\| \leq (8n)^{2^D}.$$

**Лемма.**  $\forall a, y, q \in \mathbb{R}^+(\geq 0) : a \log q > 1, (ay)^y \geq q \Rightarrow$

$$y \geq \frac{\log q}{\log(a \log q)} \left( 1 + \frac{\log \log(a \log q)}{\log(ae \log q)} \right),$$

где  $e$  — основание натурального логарифма.

$\forall a, y, q \in \mathbb{R}^+(\geq 0) : a > 1, a^y \geq q \Rightarrow$

$$y \geq \frac{\log q}{\log a}.$$

**Теорема.** Для некоторых последовательностей  $\varepsilon_i = \varepsilon_i(n)$ , где  $i = \overline{1, 5}$  и  $n \in \mathbb{N} : (\varepsilon_i(n) \geq 0$  при  $n \geq n_0$ ),  $(\varepsilon_i(n) \rightarrow 0$  при  $n \rightarrow \infty)$  для почти всех ФАЛ  $f \in P_2(n)$  выполняются неравенства

$$L^C(f) \geq (1 + \varepsilon_1(n)) \frac{2^n}{n},$$

$$L^\Phi(f) \geq (1 - \varepsilon_2(n)) \frac{2^n}{\log n},$$

$$L^K(f) \geq (1 - \varepsilon_3(n)) \frac{2^n}{n},$$

$$L^\pi(f) \geq (1 - \varepsilon_4(n)) \frac{2^n}{\log n},$$

$$D(f) \geq n - \log \log n - \varepsilon_5(n).$$

**Следствие.**

$$L^C(n) \gtrsim \frac{2^n}{n},$$

$$L^\Phi(n) \gtrsim \frac{2^n}{\log n},$$

$$L^K(n) \gtrsim \frac{2^n}{n},$$

$$L^\pi(n) \gtrsim \frac{2^n}{\log n}.$$

## 21. Дизъюнктивно-универсальные множества ФАЛ. Асимптотически наилучший метод О. Б. Лупанова для синтеза СФЭ в базисе $B_0$ .

Метод О. Б. Лупанова позволяет строить СФЭ и устанавливать асимптотику функции Шеннона  $L^C(n)$ .

Множество ФАЛ  $G \in P_2(m)$  называется *дизъюнктивно-универсальным множеством* (ДУМ) порядка  $m$  и ранга  $p$ , если любая ФАЛ  $g \in P_2(m)$  м. б. представлена в виде  $g = g_1 \vee \dots \vee g_p$ , где  $g_i \in G$ .

Метод О. Б. Лупанова также основан на разложении Шеннона по  $q$  переменным и также использует мультиплексор порядка  $(n - q)$ . Но подфункции от  $q$  переменных из разложения реализуются не универсальным многополюсником, а как дизъюнкция функций из ДУМ порядка  $q$ .

TODO: построение ДУМ, связанные определения, методичка III часть, стр. 35.

**Лемма.**  $\forall m, s \in \mathbb{N}$  и  $p = \lceil \frac{2^m}{s} \rceil$  существует стандартное ДУМ порядка  $m$  и высоты  $s$ , которое является ДУМ ранга  $p$  и для которого:

- 1)  $\lambda = |G| \leq p \cdot 2^s$ ;
- 2) система из  $p$  характеристических ФАЛ  $\psi_1, \dots, \psi_p$  ДУМ  $G$  обладает тем свойством, что  $\forall$  ФАЛ  $g \in P_2(m)$  и соответствующих ФАЛ  $g_1, \dots, g_p$  из  $G$  справедливо не только представление  $g = g_1 \vee \dots \vee g_p$ , но и  $g = \psi_1 g_1 \vee \dots \vee \psi_p g_p$ .

**Теорема.**  $\forall$  ФАЛ  $f \in P_2(n)$   $\exists$  СФЭ  $\Sigma_f \in \mathcal{U}^C$ , реализующая  $f$  и такая, что

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

**Следствие.**  $L^C \sim \frac{2^n}{n}$ .

В классе СФЭ, в отличие от класса ДНФ, имеет место эффект Шеннона, т. к. сложность  $L^C(f) \in P_2(n)$  для почти всех ФАЛ  $f \in P_2(n)$  асимптотически равна функции Шеннона  $L^C(n)$ , то есть сложности самой сложной ФАЛ из  $P_2(n)$ .

## Недостающее

- Вопросы 22—26 в данном файле отсутствуют.
- Вопросы 25—26 не должны быть в билетах (только как дополнительные вопросы).
- Частей IV и V (вопросы 27—30) в данном файле нет.
- Часть V (вопросы 29—30) не должна быть в билетах (только как дополнительные вопросы).