Основы Кибернетики. Ответы к экзамену

10 января 2011 г.

Аннотация

Печатная версия файла [2]$OK\_all\_answers.pdf$

За основу взят документ $OK\_all\_answers.s04e07.x13{+}x16.v3.0$ с рукописными ответами на вопросы программы.

Содержание

1 Введение

Используемые в рукописной версии материалы:

1. http://mathcyb.ru/wiki
2. Лекции 2007 года

Составители рукописной версии: $Nimbler(x13), Shelt(x13), Dragonizer(x13), l_andgraf(x16)$

Набор текущей версии в TeX: $LuarSoll(x17(2009 - 2012))$

Ежели вам захочется внести в файл исправления или дополнения, стучитесь в мыло luarsoll@yandex.ru , если к тому времени исходники не продолбаю в недрах компа - выдам=)

1.1 Разбивка по вопросам

В смысле какой вопрос где читать подробно

1. Некоторые вопросы сложности алгоритмов (Сапоженко).pdf с. $2 - 3$
2. Некоторые вопросы сложности алгоритмов (Сапоженко).pdf с. $3 - 5$
3. Преобразования управляющих систем.pdf с. $7 - 14$
4. Преобразования управляющих систем.pdf с. $14 - 17$
5. Преобразования управляющих систем.pdf с. $17 - 18$
6. Преобразования управляющих систем.pdf с. $19 - 22$
7. Преобразования управляющих систем.pdf с. $22 - 29$
8. Преобразования управляющих систем.pdf с. $29 - 31$
9. Sapogenko-Nekotorie voprosi slognosti algoritmov.pdf с. $22 - 25, 28 - 30$
10. Sapogenko-Nekotorie voprosi slognosti algoritmov.pdf с. $25 - 27$
11. Sapogenko-Nekotorie voprosi slognosti algoritmov.pdf с. $32, 34 - 36$
12. Sapogenko-Nekotorie voprosi slognosti algoritmov.pdf с. $36 - 39$
13. Sapogenko-Nekotorie voprosi slognosti algoritmov.pdf с. $39 - 41$
14. Sapogenko-Nekotorie voprosi slognosti algoritmov.pdf с. $42 - 45$
15. Яблонский - Надежность управляющих систем с. $31 - 33$
16. Яблонский - Надежность управляющих систем с. $33 - 36$
17. Лекции Ложкина.pdf с. $46 - 51$
18. В методичках отсутствует
19. Яблонский - Надежность управляющих систем с. $6 - 7, 13 - 14, 18 - 19$
20. Яблонский - Надежность управляющих систем с. $18 - 21$
21. Яблонский - Надежность управляющих систем с. $14 - 16, 21 - 24$

22. Яблонский - Надежность управляющих систем с. $24-25$

23. Яблонский - Надежность управляющих систем с. $26-29$

24. Яблонский - Надежность управляющих систем с. $29-31$

25. Sapozhenko_dnf.pdf с. $1-6$

2 Билет 1. Инвариантные классы (ИК). Примеры и свойства. Существование ИК характеристик 0, 0.5, 1

Опр. *Инвариантный класс - подмножество функций из P_2 ($Q \subseteq P_2$) такое, что если $f \in Q$, то Q принадлежат функции:*

- *получаемые из f добавлением/изъятием фиктивных переменных*
- *получаемые переименованием переменных (без отождествления)*
- *получаемые из f подстановкой констант вместо некоторых переменных*

Примеры

Класс линейных функций, класс монотонных функций - инвариантные классы

T_0, T_1, класс самодвойственных функций - не инвариантные классы (не замкнуты относительно подстановки констант)

Опр. *Тривиальные инвариантные классы - множество всех функций P_2 и пустое множество*

Пусть $Q(n)$ - множество всех $f \in Q$, зависящих (не обязательно существено) от переменных $x_1, x_2, ..., x_n$

Теорема Пусть $Q \neq \varnothing$. Тогда последовательность

$$\sqrt[2^n]{|Q(n)|}$$

не возрастает и существует предел:

$$1 \leq \lim_{n\to\infty} \sqrt[2^n]{|Q(n)|} \leq 2$$

Опр. Если $2^\sigma = \lim_{n\to\infty} \sqrt[2^n]{|Q(n)|}, \sigma \in [0,1]$, то σ - характеристика

$|Q_\sigma(n)| = 2^{\sigma 2^n(1+\Sigma_n)}$, $\Sigma_n \to 0$ при $n \to \infty$

Следствие Если Q_σ не совпадает с $P_2 \Rightarrow \sigma < 1$

Теорема (Яблонский) Для $\forall \sigma \in [0,1) \exists$ континуум попарно различных инвариантных классов Q с характеристикой σ

3 Билет 2. Оценки сложности функции Шенноне в классе СФЭ для ИК. Сложные множества. Правильные алгоритмы. Теорема С.В.Яблонского о неустранимости перебора

Пусть $L(f)$ - сложность минимальной схемы из СФЭ, реализующей функцию f.

$$L(n) = \max_{f \in P_2(n)} L(f); L_Q(n) = \max_{f \in Q(n)} L(f)$$

Теорема 1 (Лупанов) $L(n) = \frac{2^n}{n}(1 + \delta_n)$

Теорема 2 (Лупанов) Пусть Q - инвариантный класс с характеристикой σ. Тогда $L_Q(n) \leq \sigma \frac{2^n}{n}(1 + \Delta_n)$, $\Delta_n \to 0$ при $n \to \infty$

Опр. *Функция $f_n(x_1, ..., x_n)$ - сложная, если $L(f_n) = L(n)$*

Опр. *Бесконечная последовательность булевых функций $\{f_n(x_1, ..., x_n)\}_{n=1}^{\infty}$ - сложная, если $\forall N \exists n \geq N : f_n(x_1, ..., x_n)$ - сложная*

Опр. *Алгоритм, строящий бесконечную последовательность булевых функций $\{f_n(x_1, ..., x_n)\}_{n=1}^{\infty}$ из P_2 называетя правильным, если он строит все функции минимального инвариантного класса, содержащего эту последовательность*

Теорема (С.В. Яблонский) Любой правильный алгоритм, строящий сложную последовательность функций $\{f_n(x_1, ..., x_n)\}_{n=1}^{\infty}$ из P_2 строит все множество P_2.

4 Билет 3. Существование конечной полной системы тождеств для формул алгебры логики

4.1 Эквивалентные преобразования формул в P_2

Опр. *Формулы $\mathfrak{A}'$ и $\mathfrak{A}''$ называются равными (эквивалентными), если соответствующие им функции $f_{\mathfrak{A}'}$ и $f_{\mathfrak{A}''}$ равны*

Опр. *Если $\mathfrak{A}_1$ - часть формулы $\mathfrak{A}'$ - является формулой, то она называется подформулой формулы $\mathfrak{A}'$*

Опр. *Пусть $\mathfrak{A}_1$ подформула формулы $\mathfrak{A}'$, $\mathfrak{A}_2$ - произвольная формула. Замена формулы $\mathfrak{A}_1$ на $\mathfrak{A}_2$ в $\mathfrak{A}'$ называется подстановкой $\mathfrak{A}_2$ вместо $\mathfrak{A}_1$. Если $\mathfrak{A}_1 = \mathfrak{A}_2$, то подстановка эквивалентная*

Опр. *$\mathfrak{A}_1(x_1, ..., x_n) = \mathfrak{A}_2(x_1, ..., x_n)$ задает все тождества вида $\mathfrak{A}_1(\alpha_1, ..., \alpha_n) = \mathfrak{A}_2(\alpha_1, ..., \alpha_n)$, где $\alpha_1, ..., \alpha_n$ - произвольные формулы в данном базисе.*

Опр. *Последовательность формул $\mathfrak{A}^{(1)} \to \mathfrak{A}^{(2)} \to ... \to \mathfrak{A}^{(p)}$ - эквивалентное преобразование, если каждая последующая формула получается из предыдущей эквивалентной подстановкой с использованием тождеств системы $\{\mathfrak{A}_1 = \mathfrak{A}_2\}$*

Опр. *Система тождеств $\{\mathfrak{A}_1 = \mathfrak{A}_2\}$ - полная, если для любых двух эквивалентных формул существует эквивалентное преобразование при помощи формул этой системы*

Теорема Для системы формул алгебры логики в базисе $\{\neg, \&, \vee\}$ существует конечная полная система тождеств.

Теорема (Линдон) Для каждого замкнутого класса $\mathcal{P}$ из P_2 система формул в его специальном базисе имеет конечную полную систему тождеств.

Пример системы тождеств(в P_k (?)):

1. $\overline{x_1 \vee x_2} = \overline{x_1} \& \overline{x_2}$
2. $\overline{x_1 x_2} = \overline{x_1} \vee \overline{x_2}$
3. $\overline{\overline{x}} = x$
4. $(x_1 \vee x_2) \& x_3 = (x_1 \& x_3) \vee (x_2 \& x_3)$
5. $x_1 \& x_2 = x_2 \& x_1$
6. $(x_1 \& x_2) \& x_3 = x_1 \& (x_2 \& x_3)$
7. $x \& x = x$
8. $(x_1 \& \overline{x_1}) \& x_2 = x_1 \& \overline{x_1}$
9. $(x_1 \& \overline{x_1}) \vee x_2 = x_2$
10. $x_1 \vee x_2 = x_2 \vee x_1$
11. $(x_1 \vee \overline{x_1}) \& x_2 = x_2$
12. $(x_1 \vee x_2) \vee x_3 = x_1 \vee (x_2 \vee x_3)$
13. $x \vee x = x$
14. $x_1 \& \overline{x_1} = x_2 \& \overline{x_2}$

5 Билет 4. Функция Линдона. Основные тождества $A_{1,2,3}, B_m, C_m$. Полнота системы T_∞

В P_2 для любого замкнутого класса можно выбрать конечный базис. При переходе к P_k $(k \geq 3)$ ситуация становится более сложной - не каждый замкнутый класс имеет конечный базис.

Первый такой пример в P_7 был построен Линдоном. Возьмем функцию $\phi(x_1, x_2) \in P_7$. Обозначим $\phi(x_1, x_2) = x_1 \cdot x_2$. $B = \{\phi\}$. K_ϕ - класс, образованный замыканием функции Линдона.

Функция задается таблицей

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	0	1	5	6	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	5	5	5	0	0
6	0	0	6	6	6	0	0

Тождества:

- $A_{1,2,3} : 0 \cdot x_1 = 0; x_1 \cdot 0 = 0; x_1 \cdot (x_2 \cdot x_3)$
- $B_m : (...((x1 \cdot x_2) \cdot x_3)... \cdot x_m) \cdot x_1 = 0; m = 1, 2...$
- $C_m : (...((x1 \cdot x_2) \cdot x_3)... \cdot x_m) \cdot x_2 = (...(x1 \cdot x_2) \cdot x_3...) \cdot x_m; m = 2, 3, ...$

Рассмотрим систему тождеств $T_m = \{A_{1,2,3}, B_i, C_i, i = \overline{1, m}\}$

Теорема Пусть $A[x_1, ..., x_k], B[x_1, ..., x_k]$ - две произвольные эквивалентные формулы. Тогда существует эквивалентное преобразование из A в B при помощи T_m, где $m \leq k$

Следствие Система

$$T_\infty = \bigcup_{m=1}^{\infty} T_m$$

полна в классе K_ϕ

6 Билет 5. Свойство C^n. Лемма о сохранении свойства C^n. Теорема Линдона.

K_ϕ - класс, образованный замыканием функции Линдона.

$B = \phi$

Опр. *Формула $\mathfrak{A}$ обладает свойством C^n, если:*

- *$\mathfrak{A}$ содержит $x_1, x_2, ..., x_n$*
- *$\mathfrak{A}$ не содержит нулей и умножений слева*
- *если некоторые переменные встречаются 2 раза, то между этими вхождениями есть все остальные переменные*

Лемма Пусть формула $\mathfrak{A}$ обладает свойством C^n, а $\mathfrak{B}$ получена из $\mathfrak{A}$ при помощи тождеств $A_{1,2,3}, B_m, C_m$, где $m < n$. Тогда формула $\mathfrak{B}$ тоже удовлетворяет свойству C^n

Следствие Эквивалентность B_n не может быть получена при помощи тождеств $A_{1,2,3}, B_m, C_m, m < n$

Теорема (Линдона) В классе формул K_ϕ не существует конечной полной системы тождеств.

Д-во

Пусть в K_ϕ есть КПСТ.

$$\begin{cases} \mathfrak{A}'_1 = & \mathfrak{A}''_1 \\ ... & \\ \mathfrak{A}'_r = & \mathfrak{A}''_r \end{cases}$$

Обозначим через n наибольший номер переменной x, встречающийся в этих тождествах. На основании теоремы данная система тождеств может быть получена из системы $\{A_{1,2,3}, B_m, C_m, m \leq n\}$

В то же время она полная, значит, из нее можно вывести тождество B_{n+1}, что противоречит следствию пред. леммы.

7 Существование КПСТ для СФЭ

Опр. *Схемы* $\Sigma' = \Sigma'(x_1, ..., x_n, z_1, ..., z_p)$ *и* $\Sigma'' = \Sigma''(x_1, ..., x_n, z_1, ..., z_p)$ *называются эквивалентными, если уравнения*

$$\begin{cases} z_1 = & f_1'(x_1, ..., x_n) \\ ... & \\ z_p = & f_p'(x_1, ..., x_n) \end{cases}$$

и

$$\begin{cases} z_1 = & f_1''(x_1, ..., x_n) \\ ... & \\ z_p = & f_p''(x_1, ..., x_n) \end{cases}$$

описывающие их функционирование имеют равные правые части.

Схемы с одинаковыми входами и без выходных полюсов считаются эквивалентными

Опр. *Пусть* Σ_1 *- часть схемы* Σ*, которая является СФЭ. Тогда она называется подсхемой схемы* Σ*. При этом полюсами (входными и выходными) подсхемы* Σ_1 *являются полюса исходной схемы* Σ*, попавшие в* Σ_1*, а также вершины (связи), соединяющие* Σ_1 *с остальной частью схемы, и некоторые выходы эл-тов из* Σ_1

Опр. *Операция подстановки состоит в замене подсхемы* Σ_1 *на* Σ_2*, у которой столько же входов и выходов, как и у* Σ_1

Опр. *Если* Σ_2 *эквивалентна* Σ_1 *и подстановка согласована с соответствием полюсов при их эквивалентности, то мы имеем эквивалентную подстановку. Для СФЭ справедлив принцип эквивалентной замены*

Опр. *Тождество* Σ_1 Σ_2 *понимается с точностью до переименования переменных из алфавитов* X *и* Z

Теорема (Горбовицкая) Для СФЭ в базисе из инверторов, конъюнкторов и дизъюнкторов существует конечная полная система тождеств

8 Билет 7. Тождества в КС. Доказательство тождеств I-VII. Лемма о звездах. Теорема Мурского о полноте системы T_∞

Опр. *КС* Σ' *и* Σ'' *называются эквивалентными, если существует взаимнооднозначное соответствие* T *между их полюсами, такое, что матрицы* $\left\| f'_{ij} \right\|$ *и* $T \left\| f''_{ij} \right\| T^{-1}$ *равны, т.е. состоят из соотв. равных функций*

Опр. *Подмножество* Σ_1*, состоящее из некоторых вершин схемы* Σ *и части контактов их соединяющих называется подсхемой схемы* Σ*, если в нем выделены полюса так, что*

- *Если вершина из* Σ_1 *является полюсом в* Σ*, то она является также полюсом в* Σ_1

- *Если вершина из* Σ_1 *инцидентна контакту из* $\Sigma \backslash \Sigma_1$*, то она является полюсом в* Σ_1

- *Некоторое подмножество вершин из Σ_1 (возможно, и пустое) считается полюсами Σ_1*

Опр. *Если КС Σ_1 и Σ_2 эквивалентны и T - взаимнооднозначное соответствие их полюсов, обеспечивающее эквивалентность, и Σ_1 - подсхема схемы Σ, то подстановка вместо Σ_1 схемы Σ_2, согласованная с T, будет эквивалентной подстановкой.*

Тождества - Рис.1

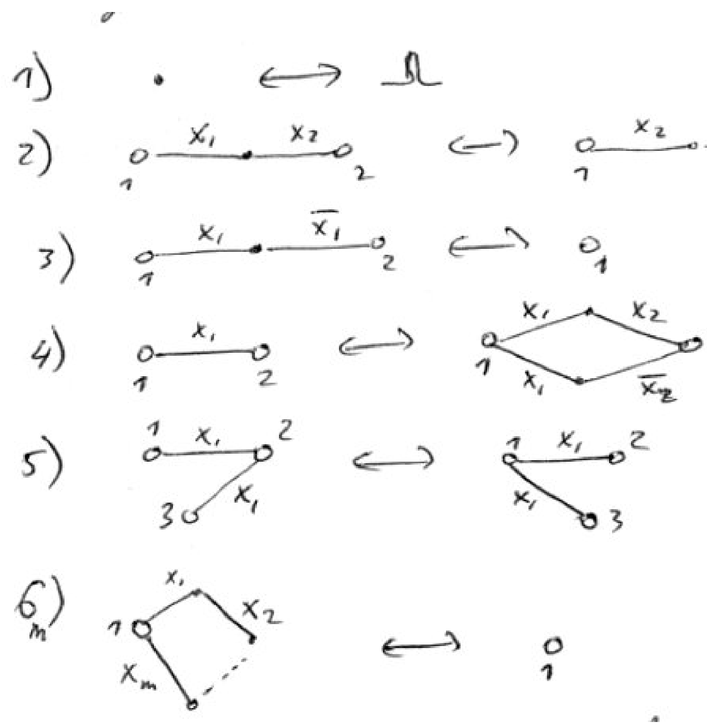

Рис. 1: Тождества $ti - tvi_m$

Пусть I - цепочка, соответствующая конъюнкции $x_1 \& ... \& x_n$.
Тождества - Рис.2

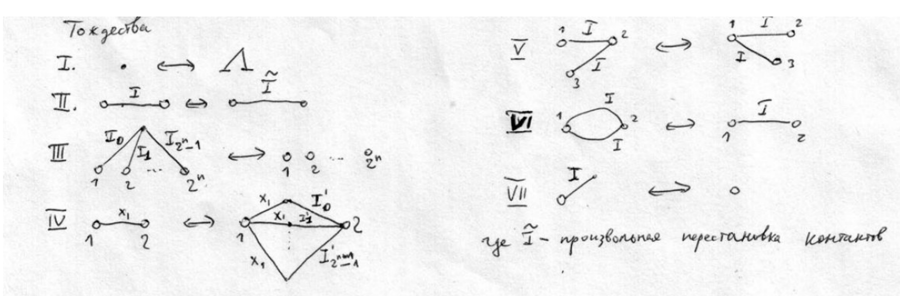

Рис. 2: Тождества $TI - TVII$

Лемма Тождества TI - TVII могут быть получены из тождеств ti - tvi *mleqn* при помощи эквивалентных преобразований

Лемма (о звезде) Тождества (*) (Рис.3) выводимы из TI-TVII

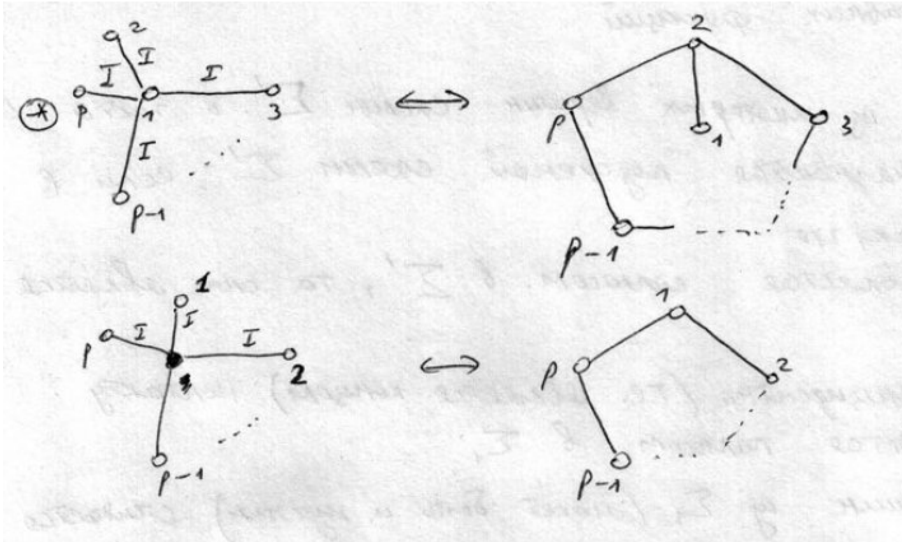

Рис. 3: Тождества (*)

Теорема Если Σ' и Σ'' две эквивалентные s-полюсные КС над $x_1, ..., x_n, \overline{x_1}, ..., \overline{x_n}$, то существует эквивалентное преобразование из Σ' в Σ'' при помощи тождеств ti-tvi $(m \leq n)$

Следствие Система тождеств ti-tvi (m=1, 2...) является полной в классе КС

9 Билет 8. Индекс схемы. Невыводимость тождества tvi_n из тождеств $ti - tvi_m(m < n)$. Теорема о несуществовании КПСТ для КС

Пусть Σ - КС над $x_1, ...x_n, \overline{x_1}, ..., \overline{x_n}$

Введем функцию $\phi_\Sigma(\alpha_1, ..., \alpha_n) = p - b + k$, где p - числе ребер в графе, получающемся из Σ при подстановке $x_1 = \alpha_1, ..., x_n = \alpha_n$ (контакт x^σ переходит в ребро при $x^\sigma = 1$ и выбрасывается при $x^\sigma = 0$); b - число вершин данного графа, k - число связных компонент получившегося графа.

Введем $Ind\Sigma = \sum_{(}\alpha_1, ..., \alpha_n)(mod2)$

Лемма Если схемы Σ' и Σ'' над алфавитом $x_1, ..., x_n, \overline{x_1}, ..., \overline{x_n}$, и Σ'' получена из Σ' эквивалентными преобразованиями $ti - tvi_m(m < n)$, то $Ind\Sigma' = Ind\Sigma''$

Следствие Тождество tvi_{n+1} невыводимо из $ti - tvi_m(m \leq n)$

Теорема Для КС не существует КПСТ

10 Билет 9. Полиномиальная сводимость языков. Классы P и NP. Язык 2-выполнимости. NP-полные языки

Опр.*Машина Тьюринга (МТ) - абстрактная вычислительная машина. В данном случае рассматриваем МТ с односторонней лентой, бесконечной вправо. Алфавит*

МТ - А. Множество состояний - Q. A, Q - конечны. q_1 *- начальное состояние.* a_1 *- пустой символ.*

Считается, что в начальный момент времени слово $\omega = b_1 b_2 ... b_n$ обрабатывается МТ, записано в первых n ячейках ленты, все остальные ячейки содержат символ a_1.

Опр. *Детерминированная МТ - для каждой пары вида (a, q), где a - символ входного алфавита, q - символ состояния, в программе МТ присутствует не более одной команды вида* $aq \to a'q'd$

Опр. *Конфигурацией (мгновенным описанием), соответствующим такту t (в это время в процессе работы МТ на ленте записано слово* $\omega = b_1 b_2 ... b_m$*) называется слово вида* $C_t = b_1 ... b_{k-1} q_j b_k ... b_m$.

Конфигурация, соответствующая первому тексту - начальная, последнему (если МТ остановилась) - заключительная

Опр. *Вычислением МТ М на входе* ω *называется последовательность конфигураций* $C_1, C_2, ..., C_t, ...$*, возникающая при работенад словом* ω

Если вычисление бесконечно, $t_m(\omega) = \infty$.

Среди состояний МТ имеются выделенные заключительные состояния. Они бывают принимающие и отвергающие, соответственно результат вычислений может быть „принять“ или „отвергнуть“.

Опр. *Недетерминированная МТ (НМТ) - для пары вида (a, q) в программе МТ может присутствовать несколько команд, начинающихся с aq, поэтому МТ, находясь в состоянии q может выбрать любую команду из возможных (при этом считается, что МТ создает две копии самой себя и прослеживает последовательность вычислений обоих способов действия)*

Опр. *Вычислением НМТ на входе* ω *называется последовательность конфигураций* $C_1, ..., C_t, ...$*, в которой* $C_1 = q_1\omega$*, а* C_{t+1} *получается из* C_t *с помощью одной из команд, соответствующих a(t)q(t)*

Всякое вычисление можно изобразить ориентированной цепью, где вершины - конфигурации, дуга - соединяет две последовательные вершины. Детерминированная МТ - вычисление однозначно определяется входом. НМТ - объединение цепей, соответствующих вычислениям с ω на входе; представляет собой ориентированное дерево (от корня) с корнем $C_1 = q_1\omega$

10.1 Распознавание языков

А - конечный алфавит

A^ω - множество всех слов конечной длины в алфавите А

$\|\omega\|$ - длина слова

$L \subset A^\omega$ - язык в алфавите А.

Опр. *МТ (НМТ) с двумя заключительными состояниями (принимающим и отвергающим) распознает язык L, если для любого слова* $\omega \in A^\omega$ *принимающее вычисление M с* ω *на входе существует тогда и только тогда, когда* $\omega \in L$.

Если $\omega \notin L$ *- либо вычисление бесконечное, либо отвергающее*

Опр. *МТ(НМТ) распознает язык L за полиномиальное время, если она распознает L и* $\exists p : \forall \omega \in L \exists$ *принимающее вычисление длины, не превышающей* $p(\|\omega\|)$

Опр. *P - класс языков, распознаваемых МТ за полиномиальное время*

П - мн-во отображений вида $f : A^\omega \to A^\omega$*, вычислимых МТ за полиномиальное* *время*

Опр.L *и* K *- языки. Тогда* L *полиномиально сводится к* K $(L \prec K)$, *если существует* $f \in \Pi : f(\omega) \in K \Leftrightarrow \omega \in L$

Опр.*Языки* L *и* K *полиномиально эквивалентны, если* $L \prec K$ *и* $K \prec L$

Опр.*NP - класс языков, распознаваемых НМТ за полиномиальное время*

Опр.*Язык* L *- NP-полный, если* $L \in NPK \prec L \Rightarrow K \in NP$

Опр.*Язык выполнимости (ВЫП) состоит из слов в алфавите* $A = \{(,), \&, \vee, /, x_i, i = 1, 2...\}$, *представляющий собой выполнимые КНФ (т.е. КНФ не равные тождественно 0)*

Опр.*Пусть буква - произвольная булева переменная или ее отрицание; скобка - формула вида* $(y_1 \vee ... \vee y_r$, *где* y_i *- буква, r>1. K-КНФ - конъюнкция скобок, каждая из которых есть дизъюнкция не более к букв. Задача k-выполнимости - распознавание выполнимости k-КНФ*

Теорема Задача 2-ВЫП распознается детерминированной МТ за полиномиальное время

11 Билет 10. Теорема С.Кука

Теорема. Если язык $L \in NP$, то L сводится к задаче выполнимости

Д-во

Т.к. $L \in NP$, существует НМТ, распознающая язык L за полиномиальное время. Пусть p(x) - полином и НМТ M такова, что M разпознает L и $t_M(\omega) \leq p(\|\omega\|)$ для любого слова $\omega \in L$

Построим по произвольному слову ω КНФ $A(\omega) = A(\omega, H, p)$ выполнимой тогда и только тогда, когда $\omega \in L$.

Пусть $A = \{a_1, ..., a_l\}$ - алфавит, a_1 - пустой символ

$Q = \{q_1, ..., q_r\}$ - множество состояний. q_1 - начальное состояние, q_r - принимающее.

Введем переменные, от которых будет зависеть строящаяся КНФ $A(\omega)$:

- $P^i_{s,t}; 1 \leq i \leq l; 1 \leq s, t \leq T$

  $P^i_{s,t} = 1 \Leftrightarrow$ ячейка с номером s на шаге t содержит символ a_i

- $Q^j_t; 1 \leq j \leq r; 1 \leq t \leq T$

  $Q^j_t = 1 \Leftrightarrow$ на шаге t МТ находится в состоянии q_j

- $S_{s,t}; 1 \leq s, t \leq T$

  $S_{s,t} = 1 \Leftrightarrow$ на шаге t головка обозревает s-ю ячейку.

Строим КНФ $A(\omega) = B\&C\&D\&E\&F\&G$, где

$$B = \bigcap_{t=1}^{T} B_t$$

B_t - на шаге t обозревается одна и только одна ячейка:

$$B_t = \overbrace{(S_{1,t} \vee ... \vee S_{T,t})}^{obozrevaetsia} \& \overbrace{\bigcap_{1 \leq i < j \leq T} (\overline{S_{i,t}} \vee \overline{S_{j,t}})}^{tol'ko\ odna}$$

$$C = \bigcap_{s=1}^{T} \bigcap_{t=1}^{T} C_{s,t}$$

, где $C_{s,t}$ - на шаге t в ячейке s находится один и только один символ

$$D = \bigcap_{t=1}^{t} D_t$$

, где D_t - в момент времени T МТ находится в одном и только одном состоянии.

$$E = Q_1^1 \& S_{1,1} \& P_{1,1}^{i_1} \& P_{2,1}^{i_2} \& ... \& P_{n,1}^{i_n} \& P_{n+1,1} \& ... \& P_{T,1}^1$$

Примечание - $\omega = \underbrace{a_{i_1}, ..., a_{i_n}}_{n} \underbrace{\quad}_{T-n}$. Всего T символов, т.к. дальше не уйдем за T шагов

$$F = \bigcap_{s=1}^{T} \bigcap_{t=1}^{T} F_{s,t}$$

, где $F_{s,t}$ а) если ячейка с номером s не обозревается на шаге t, то символ в ней не меняется; б) если ячейка с номером s обозревается на шаге t, то изменение символа в ней происходит в соответствии с программой.

Пусть $R_{s,t,i,j} = 1 \Leftrightarrow$ на шаге t обозревается ячейка s и из того, что в ячейке находится символ a_i и M находится в состоянии q_j следует, что M действует в соответствии хотя бы с одной из команд, начинающихся с пары $a_i q_j$.

Пример (в программе НМТ две команды)
$a_i q_j \to a_{i_1} q j_1 L$
$a_i q_j \to a_{i_2} q j_2 R$
Тогда $R_{s,t,i,j} = \overline{P_{s,t}^i} \vee \overline{Q_t^j} \vee P_{s,t+1}^{i_1} \& Q_{t+1}^{j_1} \& S_{s-1,t+1} \vee P_{s,t+1}^{i_2} \& Q_{t+1}^{j_2} \& S_{s+1,t+1}$

$$F_{s,t} = \overline{S_{s,t}} \& (\bigcap_{i=1}^{l} (\overline{P_{s,t}^i} \vee P_{s,t+1}^i)) \vee S_{s,t} \& (\bigvee_{i=1}^{l} \bigvee_{j=1}^{r} R_{s,t,i,j})$$

G - МТ обязательно придет в принимающее состояние
$G = Q_1^r \vee ... \vee Q_T^r$
Представим каждый множитель B, C, D, E, F, G в виде КНФ, тогда $A(\omega) = 1 \Leftrightarrow \omega \in L$

Следствие Язык ВЫП - NP-полный.

12 Вопрос 11. NP-трудная задача 3-ВЫП, (0,1)-целочисленное программирование

Теорема 3-ВЫП является NP-полной

Опр. *Задача называется NP-трудной, если любой язык из NP сводится к этой задаче.*

Опр. *Задача называется NP-полной, если она NP-трудная и принадлежит классу NP*

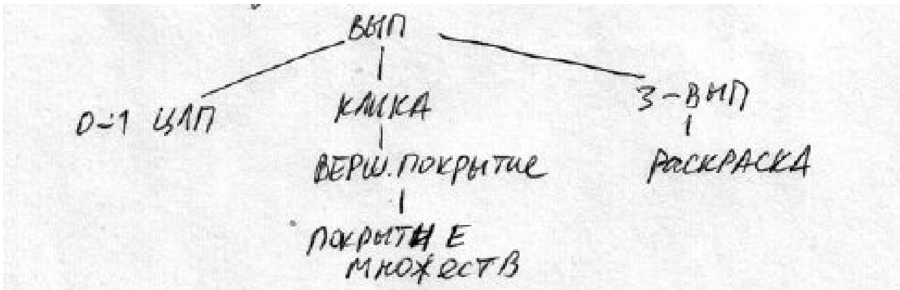

Рис. 4: Схема сведения задач

Схема сведения задач - Рис.5
Задача ВЫП:
Вход: КНФ
Св-во: выполнимость
Задача 0-1 ЦЛП:
Вход: м-ца $A \in R^{p \times n}$, целочисленный вектор $b = (b_1, ..., b_p)$
Св-во: существует (0,1)-вектор $x = (x_1, ..., x_n) : Ax^T \geq b^T$
Теорема Задача ВЫП сводится к 0-1 ЦЛП

13 Билет 12. NP-трудные задачи: Клика, Вершинное покрытие, Покрытие множества

Задача Клика
Вход: граф $G = (V, E)$, число k
Свойство: в G существует полный подграф с k-вершинами
Теорема ВЫП сводима к Клика
Задача вершинное покрытие
Вход: граф $G' = (V', E')$, число l.
Свойство: существует множество вершин R такое, что $|R| \leq l$ и при этом каждое ребро графа G инцидентно некоторой вершине из R.
Теорема Задача Клика сводима к задаче вершинное покрытие
Покрытие множеств
Вход: Семейство $F = S_1, ..., S_m$ подмножеств множества S такое, что

$$\bigcup_{S_j \in F} S_j = S$$

, число h
Свойство: существует подсемейство $T \subset F : |T| \leq h$ и при этом

$$\bigcup_{S_j \in T} S_j = S$$

Теорема Вершинное покрытие сводимо к покрытию множеств

14 Билет 13. NP-трудная задача Раскраска

Задача Раскраска

Вход: граф $G = (V, E)$, число k

Свойство: существует функция $\phi : V \to Z_k : \phi(u) \neq \phi(v)$ для всех $(u, v) \in E$

Теорема Задача 3-ВЫП сводится к задаче Раскраска

Д-во

Пусть К - 3-КНФ с n переменными и t скобками. Построим за время, ограниченное полиномом от $max(n, t)$ граф $G = (V, E)$ с $3n + t$ вершинами, который можно раскрасить в $n + 1$ цветов тогда и только тогда, когда К выполнима.

Пусть $x_1, ..., x_n$ - переменные; $C_1, ..., C_t$ - сомножители КНФ К.

Пусть $v_1, ..., v_n$ - новые символы. $n \geq 4$.

Вершины графа G:

- $x_i, \overline{x_i}, v_i$ для $1 \leq i \leq n$
- c_i для $1 \leq i \leq t$

Ребра графа G:

- Все $(v_i, v_j), i \neq j$
- Все (v_i, x_j) и $(v_i, \overline{x_j}), i \neq j$
- $(x_i, \overline{x_i}), 1 \leq i \leq n$
- (x_i, c_j), если x_i не входит в c_j и $(\overline{x_i}), c_j)$, если $\overline{x_i}$ не входит в скобку c_j

Вершины $v_1, ..., v_n$ образуют полный граф с n вершинами, значит, для их раскраски требуется n цветов. Каждая из вершин $x_j, \overline{x_j}$ соединена с каждой вершиной $v_i, i \neq j$, значит, $x_j, \overline{x_j}$ не могут быть одного цвета с v_i. Т.к. x_j и $\overline{x_j}$ смежны, они не могут быть раскрашены в один цвет. Значит, весь граф нельзя раскрасить меньше, чем в n+1 цвет. Граф G можно раскрасить ровно в n+1 цвет тогда и только тогда, когда одна из вершин $x_j, \overline{x_j}$ имеет тот же цвет, что и v_j, а другая имеет новый цвет (специальный).

Пусть той из вершин $x_j, \overline{x_j}$, которая раскрашена в специальный цвет, приписано значение 0.

Рассмотрим цвет, приписанный вершине c_j. Вершина c_j смежна по краней мере с $2n - 3$ из $2n$ вершин $x_1, ..., x_n, \overline{x_1}, ..., \overline{x_n}$. Т.к. $n \geq 4$, для каждой j найдется тако i, что c_j смежна как с x_i, так и с $\overline{x_i}$. Поскольку одна из этих вершин раскрашена в специальный цвет, то c_j не может быть раскрашена в специальный цвет.

Если скобка c_j содержит такой символ g, что вершине $\overline{g}$ приписан специальный цвет, то вершина c_j не смежна ни с какой вершиной, раскрашенной так же, как и g, значит, ей можно приписать тот же цвет, что и g. Иначе нужен новый цвет, а запаса уже нет=)

Таким образом, все вершины c_i можно раскрасить тогда и только тогда, когда символам можно так приписать специальный цвет, чтобы каждый сомножитель содержали такой символ g, чтобы символ $\overline{g}$ был раскрашен в специальный цвет, т.е. когда переменным можно так присвоить значения, чтобы в каждом сомножителе оказался g со значением 1, то есть когда КНФ выполнима

15 Билет 14. Моделирование МТ схемами. Теорема Севиджа о моделировании вычисления (n,m)-операторов

Рассмотрим детерминированную МТ с односторонней бесконечной лентой вправо.

$A = \{a_1, ..., a_m\}$ - алфавит ленты

$Q = \{q_0, ..., q_k\}$ - алфавит состояний, q_0 - начальное, q_k - заключительное

Λ - пустой символ.

В начальный момент времени на ленте записано слово $x_1, ..., x_n$.

Для моделирования будем применять обобщение СФЭ.

На входе: A - ленточный алфавит

На выходе: $\widetilde{Q} = Q \cup \{\widetilde{q}\}, \widetilde{q}$ - холостое состояние

Переход от обобщенных схем к обычным (двоичным) связан с увеличением сложности в константу раз (после предварительного кодирования букв алфавитов A и Q конечными двоичными последовательностями).

Пусть МТ M работает на каждом слове длины n не более T тактов.

Построим обобщенную схему, к-рая моделирует работу M на словах длины n. Схема состоит из преобразующих элементов U и фильтрующих элементов Ф.

Элемент U: 2 входа $(a_i \in A, q_j \in Q)$, 4 выхода $(a_i', q_i^L, q_i^R, q_i^S)$, производит тождественное преобразование.

- Если $q_j = \widetilde{q}$, то $a_i' = a_i; q_j^R = q_j^L = q_j^S = \widetilde{q}$
- Если $q_j \neq \widetilde{q}$, M отыскивает команду с левой частью $a_i q_j$ (пусть правая часть a_l, q_m, L). Тогда $a_i' = a_l; q_j^L = q_m, q_j^R = q_j^S = \widetilde{q}$

Элемент Ф: входы (3 шт.(?)) и выход - символы алфавита $\widetilde{Q}$

- Если на одном из входов появляется символ, отличный от $\widetilde{q}$, он проходит на выход
- Если на всех входах $\widetilde{q}$, то выход $\widetilde{q}$

Случай, когда несколько входов отличны от $\widetilde{q}$ невозможен.

Время работы МТ над словом $x_1, ..., x_n$ не превосходит T, то есть головка может уйти вправо от начального положения не более, чем на T ячеек. Значит, достаточно держать в поле зрения зону ленты в T ячеек, пронумерованных числами от 1 до T. Схема имеет прямоугольный вид: T двухъярусных строк и T столбцов. При этом i-я строка выходами своих T элементов представляет i-ю конфигурацию МТ.

Теорема (Дж. Сэвидж). Пусть МТ M работает на словах длины n не более $T_M(n)$ тактов. Тогда ее можно моделировать СФЭ сложности $O(T_M^2(n))$

16 Билет 15. Самокоррекция КС. Тривиальная самокоррекция. Примеры нетривиальной самокоррекции КС

Пусть $\mathfrak{U}$ - класс управляющих систем. H - источник неисправностей. Возьмем управляющую систему $U \in \mathfrak{U}$, где $U = (\Sigma, f)$. $f_1, ..., f_r (f_1 = f)$ - функции неисправностей, вызываемые источником H

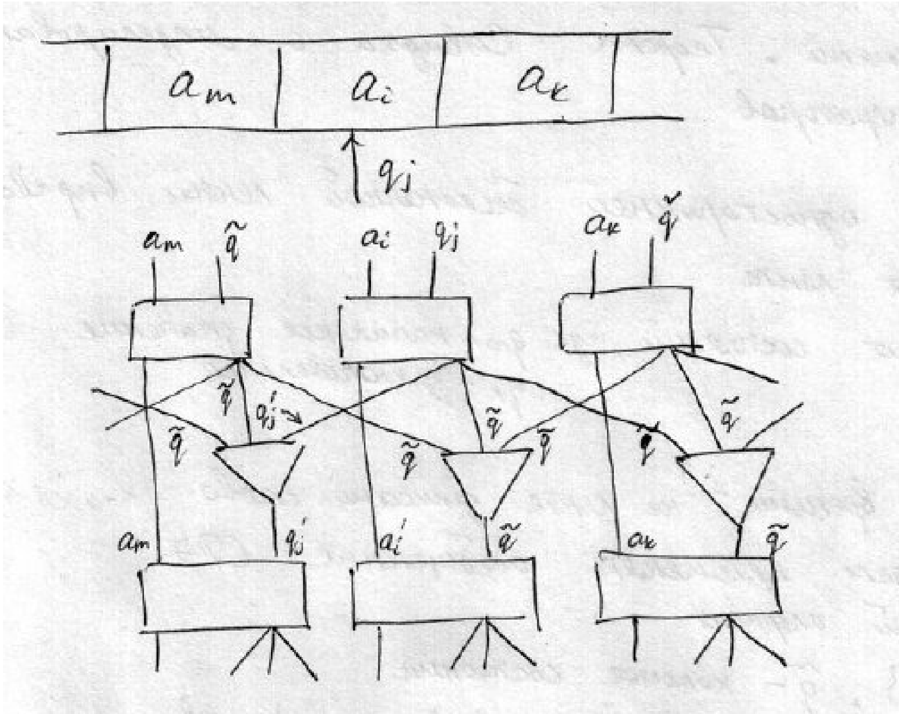

Рис. 5: часть СФЭ для МТ

Опр. *Схема Σ называется самокорректирующейся (относительно источника H), если для всех i $f_i = f$*

В качестве источника неисправностей возьмем $H_{a,b}$, вызывающий не более a разрывов и b замыканий в контактной схеме.

Пример

Тривиальная самокоррекция КС: f=x, a обрывов, b замыканий: Рис.6

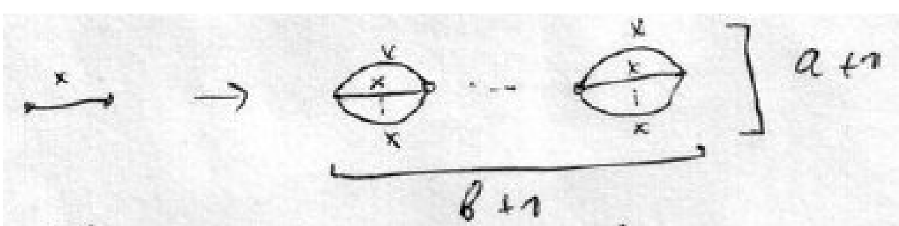

Рис. 6: тривиальная самокоррекция

Пример

Нетривиальная самокоррекция КС: $h(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$: Рис.7

сюда же добавить то, что было на семинарах

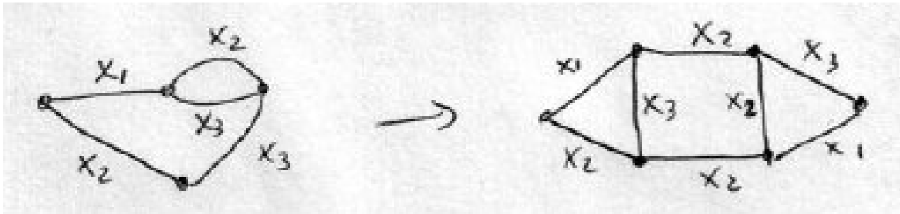

Рис. 7: нетривиальная самокоррекция

17 Билет 16. Асимптотика функции Шеннона для КС, корректирующих одно замыкание (или один обрыв) контакта

Пусть $L_{a,b}(f)$ - сложность минимальной самокорректирующейся схемы относительно $H_{a,b}$, реализующей ф-ю f. $L_{a,b}(n)$ - соответствующая функция Шеннона.

Теорема (Потапов, Яблонский) Существует метод синтеза, позволяющий для каждой булевой ф-и $f(x_1, ..., x_n)$ строить самокорректирующуюся относительно $H_{0,1}$ схему Σ_f^c такую, что $L(\Sigma^c_{f(x_1,...,x_n)}) \lesssim \frac{2^n}{n}$

Как-то тут мало букв, может, что еще стоит написать

18 Билет 17. Тесты. Алгоритмы построения всех тупиковых тестов. Нижние оценки длины тестов для таблиц. Верхняя оценка длины теста для почти всех таблиц

Опр. *Тест - множество наборов значений переменных, которое позволяет установить, какая неисправность произошла или определить, исправна ли схема*

Опр. *Тупиковый тест - тест, который перестает быть тестом при удалении любого набора*

Опр. *Минимальный тест - тест, который имеет минимальную мощность*

Опр. *Проверяющий тест - множество наборов, позволяющее отличить исходную функцию от неисправных*

Опр. *Диагностический тест - множество наборов, различающих все неисправности*

Задача сводится к тестам для таблицы A (таблица m x n, из нулей и единиц).

Диагностический тест для таблицы A - такое множество строк, что в подматрице A'_T, образованной этими строками все столбцы различны между собой.

Проверяющий тест для таблицы A - такое множество строк, что в подматрице A'_T все столбцы, начиная со 2го отличаются от 1го.

Найдем таблицу с максимальным размером минимального теста. При m=n рассмотрим диагональную таблицу. Размер ее диагностического теста будет n-1. Тривиальная оценка размера теста - n

Теорема (нижняя оценка длины тестов (каких?))

A - матрица m x n. Все столбцы A попарно различны. Пусть l(A) - длина минимального теста. Тогда $l(A) \geq \log_2 n$.

Оценим сверху длину минимального теста для почти всех таблиц

Опр. Почти все таблицы A размера m x n обладают свойством q, если доля тех A, к-рые обладают этим св-вом стремится 1 при $n \to \infty$

Теорема

Пусть $K_0(n) = 2\log_2 n + \phi(n)$, где $\phi(n) \to \infty$ при $n \to \infty$

Пусть $m \geq K_0(n)$

Тогда почти все таблицы A размена m x n обладают тестом длины $K_0(n)$

18.1 Алгоритм построения всех тупиковых тестов для таблиц

Задана A размера m x n.

По ней строим матрицу $A^{(2)}$, состоящую из сумм по модулю 2 всех пар столбцов матрицы A

Утв. Пусть подмн-во строк T - это тест для A. Тогда соответствующее мн-во T' - покрытие для $A^{(2)}$

Опр. *Покрытие матрицы - это подмножество ее строк такое, что в каждом столбце окажется хотя бы одна единица*

Если тест тупиковый, то соответствующее покрытие тупиковое.

Для построения тупикового (диагностического?) теста:

- Матрице $A(2)$ сопоставляем КНФ (i-й скобке соответствует i столбец A, в скобке используются переменные, соответствующие тем строкам, где в этом столбце единица)
- По КНФ построить сокращенную ДНФ. Каждое слагаемое ДНФ - тупиковый тест

19 Оценки длины теста для КС, реализующей счетчик четности

Что это за КС такая?

Теорема Существует тест T для Σ_f, диагностирующий обрыв не более одного контакта и такой, что $|T| \leq 5 + \lceil \log_2(n-2) \rceil$

Д-во

Тест (Рис.8) будет состоять из двух частей. Первая состоит из 4х наборов если n нечетно и из 5, если четно.

γ_i выбирается так, что в iй строке нечетное кол-во единиц. В M (внутренняя часть таблицы) все столбцы попарно различны.

Каждая цепь соответствует некоторому набору.

Выберем 4 цепи (Рис.9):

В верхней части таблицы будут наборы $\widetilde{\alpha_1}, \widetilde{\alpha_2}, \widetilde{\alpha_3}, \widetilde{\alpha_4}$ и еще одна строка при четных n.

Свойства:

- z_1, z_2, z_3, z_4 охватывает все внутренние контакты ровно 1 раз, т.е. узнаем, произошел ли обрыв контакта

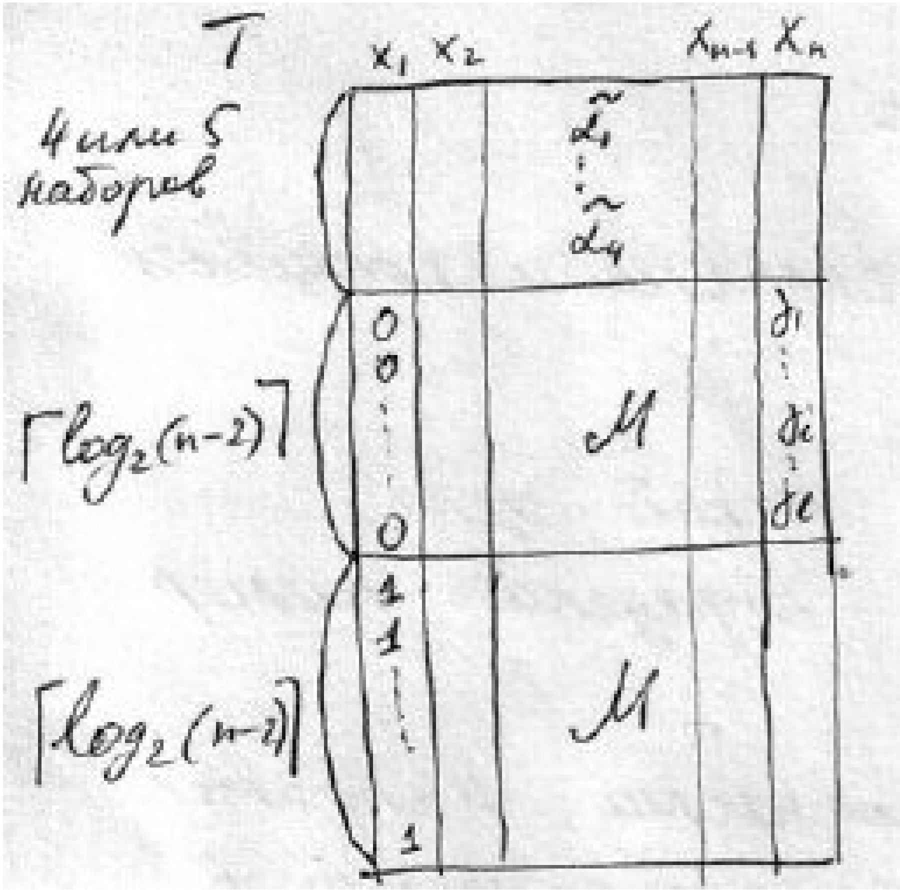

Рис. 8: Тест

- любой концевой контакт входит в эти цепи 2 раза, то есть подача на вход первых четырех наборов проверяет, произошел ли обрыв концевого или внутреннего контакта

- все внутренние контакты можно разбить на 4 класса (в какую из цепей они входят). Первые 4 набора позволяют определить, в какой из них они входят.

  Рассмотрим распознавание неисправностей в концевых контактах(Рис.10)

  При нечетных n все столбцы попарно различны. При четных n не различаются столбцы для $\overline{x_1}$ и x_n, поэтому добавляется 5й набор. В качестве 5го набора берется набор, соотв. цепи, проходящей через один из неразличимых контактов и не проходящий через другой.

- 5 первых наборов тогда диагностируют все неисправности концевых контактов. По реакции на первые 4 набора мы узнаем, в какой цепи находится неисправный внутренний контакт. Осталось определить номер переменной, которой помечен оборванных контакт.

В M все столбцы должны быть попарно различными, например, для ее построения можно воспользоваться наборами, записанными в лексикографическом порядке. Надо подобрать l строк, чтбы все столбцы были различны (Рис.11)

Таблица T позволяет установить, в каком контакте произошел обрыв.

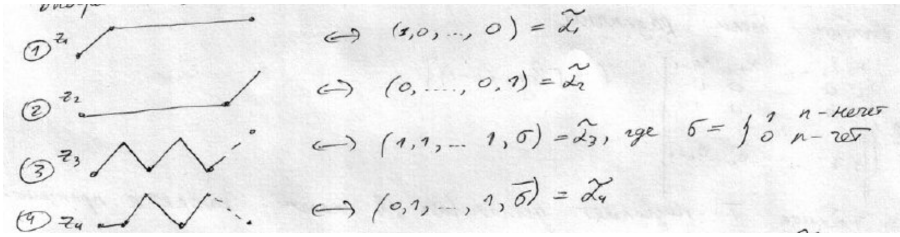

Рис. 9: 4 цепи

	x_1	$\overline{x}_1$	x_n (при нечет n)	$\overline{x}_n$ (при нечет n)	x_n (при четн. n)	$\overline{x}_n$ (при четн. n)
$\tilde{Z}_1$	0	1	1	0	1	0
$\tilde{Z}_2$	1	0	0	1	0	1
$\tilde{Z}_3$	0	1	0	1	1	0
$\tilde{Z}_4$	1	0	1	0	0	1

Рис. 10: табличка

20 Синтез СФЭ из надежных элементов. Оценка вероятности неправильного срабатывания СФЭ. Невозможность построения сколь угодно надежных схем. Пример нарастания ненадежности

Опр. *Вероятность $P(\Sigma)$ (фактической) неисправности схемы (элемента) Σ является важнейшей характеристикой надежности схемы.*

Пусть p_i - вероятность выхода из строя (неправильного срабатывания) элемента. $F_i \in \Phi$, т.е. $p_i = P(F_i)$. Пусть $\nu(i)(i = 1, 2...l)$ указывает тип элемента с номером i

Теорема

$$P(\Sigma) \leq 1 - \prod_{i=1}^{l}(1 - p_{\nu(i)})$$

Распределение вероятностей появления для схемы Σ режимов $g_1, ..., g_m$, где $g_1 = f(x_1, ..., x_n)$ и $1 \leq m \leq 2^{2^n}$ определяется указанием вероятностей $q^{(1)}, ..., q^{(m)}$

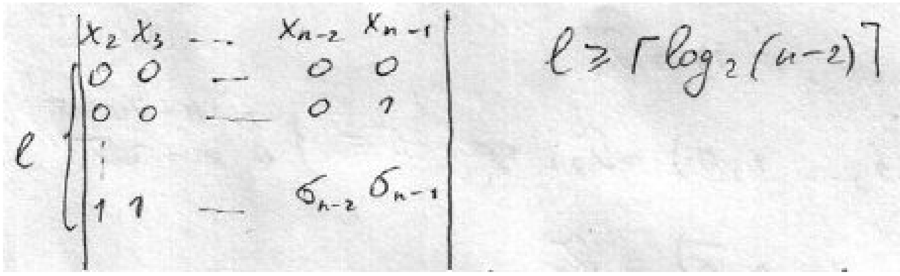

Рис. 11: табличка

их появления, для которых $\Sigma q^{(i)} = 1$. Поэтому

$$P(\Sigma) = 1 - q^{(1)} = \sum q^{(i)}{}^{m}_{i=2}$$

Для элементов F_i распределние вероятностей имеет вид

$$\begin{pmatrix} f_i^{(1)} & \dots & f_i^{(r_i)} \\ p_i^{(1)} & \dots & p_i^{(r_i)} \end{pmatrix}$$

$$\sum p_i^{(j)}{}^{m}_{j=1} = 1 f_i^{(1)} = f_i^0(x_1, ..., x_n) 2 \leq r_i \leq 2^{2^{n_i}}$$

Зная распределение для элементов F_i можно построить распределение для схемы Σ, реализующей функцию $f(x_1, ..., x_n)$

Для этого для каждого элемента схемы выбираем одну из возможных функций неисправности и вычисляем вероятность этой выборки как произведение вероятностей появления выбранных неисправностей для отдельных элементов. Затем находим режим схемы Σ, соответствующий данному выбору. Эту процедуру проделываем для всевозможных комбинаций выборов.

Суммируя все вероятности, соответствующие режиму g_i, находим величину $q^{(i)}$. Закон распределение вероятностей для базисных элементов является полной характеристикой источника Н

Влияние ошибок на надежность схемы

Эффект нарастания ненадежности.

Базис состоит из одного ненадежного элемента конъюнктора; источник Н.

Конъюнктор реализует $f_1 = x_1 \& x_2$ с вероятностью 1-p и $f_2 \equiv 0$ с вероятностью p.

Рассмотрим схему Рис.12

Эта схема должна реализовывать $f = x_1 \& x_2 \& ... \& x_n$

$P(\Sigma_n) = 1 - (1-p)^{n-1}$, т.к. если хоть один из элементов превратится в 0, то на выходе будет 0. При $n \to \infty P(\Sigma_n) \to 1$ - нарастание ошибки

Теорема Для того. чтобы в базисе Б с источником Н для любой булевой функции можно было построить сколь угодно надежную схему, необходимо и достаточно, чтобы можно было построить сколь угодно надежную схему для каждой функции некоторой полной системы.

Д-во

Необходимость очевидна.

Достаточность: рассмотрим некоторую полную систему $\phi_1, ..., \phi_l$, все ф-и к-рой допускают сколь угодно надежную реализацию в базисе В. Пусть $f(x_1, ..., x_n)$ - произвольная булева функция и $\epsilon > 0$ - произвольное число.

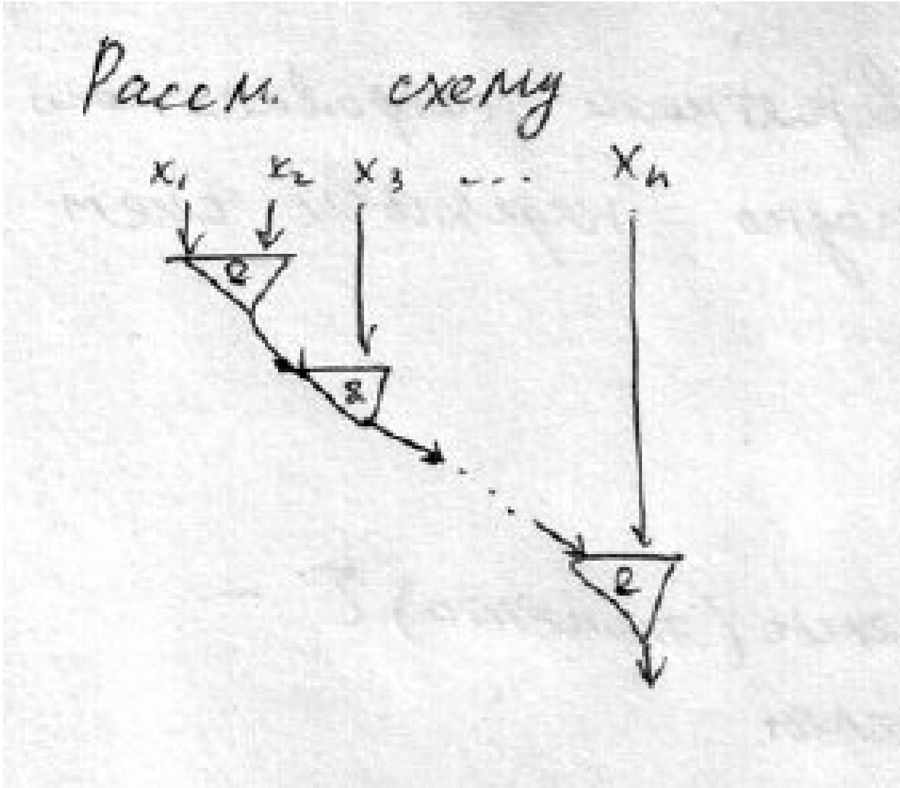

Рис. 12: схема

Рассмотрим реализацию f в базисе $\{F_{\phi_1}, ..., F_{\phi_l}\} = B'$. Соответствующая схема Σ, $L(\Sigma)$ - число элементов в ней. Пусть $\delta = \frac{\epsilon}{L(\Sigma)}$. Построим реализацию функций $\phi_1, ..., \phi_l$ в базисе B с ненадежностью, не превосходящей δ.

Если в схеме Σ заменить эл-ты $F_{\phi_1}, ..., F_{\phi_l}$ через указанные реализации, то получим схему Σ^ϵ и $P(\Sigma^\epsilon) \leq \frac{\epsilon}{L(\Sigma)} L(\Sigma) = \epsilon$

Пусть H_n - неймановский источник, если для каждого $F_i \in B_2$ распределение вероятностей имеет вид

$$\begin{pmatrix} f_i^{(1)}(x_1, ..., x_{n_i}) & \dots & f^{(}2^{2^{n_i}})_i(x_1, ..., x_{n_i}) \\ p_i^{(1)} & \dots & p^{(}2^{2^{n_i}})_i \end{pmatrix}$$

где

$$f_i^{(1)} = f_i^0(x_1, ..., x_{n_i}); \sum p_i^{(j)}{}^{2^{2^{n_i}}}_{j=1} = 1; p_i^{(j)} > 0$$

то есть у ненадежных элементов неймановский источник вызывает всевозможные функциональные повреждения. Обозначим для $F_i \in B_2$ через

$$p_{min}^{(i)} = \min_{1 \leq j \leq 2^{2^{n_i}}} p_i^{(j)}$$

и

$$p_{min} = \min_{i, F_i, B_2} p_{min}^{(i)}$$

Теорема Для неймановского источника H_n и $B_1 = \wedge$ $P(\Sigma) \geq p_{min}$

21 Вопрос 20. Пример изменения выразительной способности СФЭ. Критерий возможности сколь угодно надежной реализации булевых функций

Для произвольных источников U можно дать следующий критерий

Теорема Для того, чтобы в базисе $B = B_1 \cup B_2$ с источником Н для любой булевой функции можно было построить сколь угодно надежную схему, необходимо и достаточно, чтобы можно было построить сколь угодно надежную схему для каждой функции некоторой полной системы

См. пред. вопрос.

Пример

Пусть $B = B_2 = \{F_1\}$, где F_1 - элемент, реализующий в исправном состоянии функцию $f = x_1 \oplus x_2$. Пусть Н - источник, действующий на F_1

$f_1 = x_1 \oplus x_2; p_1 = 1 - p;$

$f_2 = \overline{x_1} \vee \overline{x_2}; p_2 = p; 0 < p < 0.5$

Функции f_1 и f_2 совпадают на всех наборах, кроме (0, 0)

Функции, реализуемые Σ_n: Рис.13 и их вероятностные параметры: Рис.14

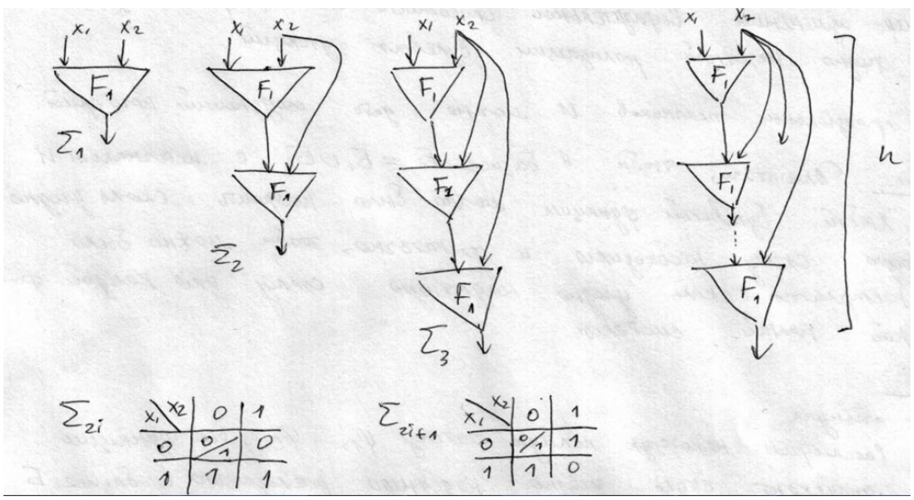

Рис. 13: Функции

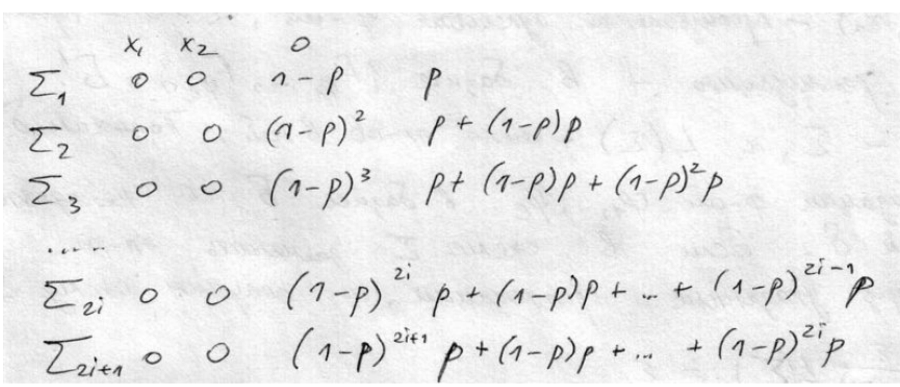

Рис. 14: Параметры

То есть $\{\Sigma_{2i+1}\}$ реализует штрих Шеффера сколь угодно надежно. Значит, в силу пред. теоремы этот базис позволяет реализовать любую функцию сколь угодно надежно.

Замечания:

- Базис B состоит только из ненадежных элементов
- Базис B в исправном состоянии не является полным
- Наличие источника неисправностей иногда может давать дополнительные возможности для реализации булевских функций

22 Повышение надежность с помощью функции голосования. Однородные деревья. Число внутренних вершин однородного дерева с q висячими вершинами

Функция голосования: $h(x_1, x_2, x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$

Пусть на входе одна и та же величина x с соответствующими вероятностями $0 \leq p_1, p_2, p_3 \leq 1$. Тогда вероятность θ ошибки на выходе этого элемента (в предположении, что его реализация абсолютно надежна) $\theta = p_1p_2 + p_1p_3 + p_2p_3 - 2p_1p_2p_3$.

θ неубывающая функция. Пусть $p = maxp_1, p_2, p_3$. Тогда $\theta \leq 3p^2 - 2p^3 = \theta_1(p)$. Значит, при $p < 0.5\theta(p) < p$, то есть элемент голосования позволяет увеличить надежность входного сигнала.

Рассмотрим схему Рис.15

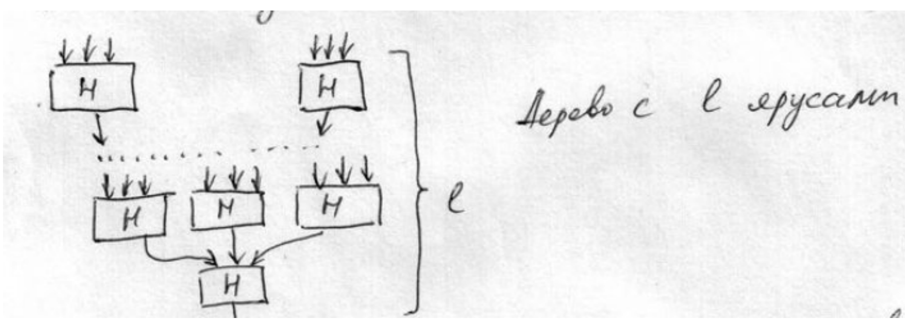

Рис. 15: Схема

Если на входы этой схемы передавать независимым образом величину x с вероятностью ошибки не большей p то ошибка на выходе $\theta_l(p) = \underbrace{\theta_1(\theta_1(...\theta_1}_{l}(p)...))$.

$\theta_l(p)$ может быть сделана сколь угодно малой при увеличении l

Лемма Если вероятность неправильного срабатывания элемента p<0.5, то можно построить схему с вероятностью неисправности $\theta_l \leq O(\frac{1}{2^{2^l}})$

Опр._Дерево назовем k-однородным, если это корневое дерево и на каждом уровне i<l степень исхода вверх из каждой вершины k (присутствуют все вершины яруса) на l-м уровне исходит q ребер, причем из всех (кроме одной возможной) вершины l-го яруса исходит k ребер или ни одного_

Лемма Пусть k=3. Для любого q существует 3-однородное дерево с q висячими вершинами, и число внутренних вершин $\lfloor q/2 \rfloor$

23 Вопрос 22. Реализация подфункций $f(x_1, ..., x_k, \sigma_{k+1}, ..., \sigma_n)$ с полностью однородных схем

Опр. *Полузвезда - совокупность ребер, исходящих из внутренней вершины.*

Сопоставим дереву D функцию $H(z_1, ..., z_q)$, считая, что каждой полузвезде порядка 3 соответствует функция $h(u, v, w)$, полузвезде $h(u, v, 0)$, концевым вершинам $1, ..., q$ - переменные $z_1, ..., z_q$

Лемма $f(x_1, ..., x_k, \sigma_{k+1}, ..., \sigma_n) = H(G^1_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k), ..., G^q_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k))$

Д-во

Пусть $x_1 = \sigma_1, ..., x_k = \sigma_k$. Найдем значения $G^1_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k), ..., G^q_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k)$

Пусть $(\sigma_1, ..., \sigma_k)$ лежит в i-й полосе (Π_i). Тогда

$$G^\nu_{\sigma_{k+1},...,\sigma_n}(\sigma_1, ..., \sigma_k) = \begin{cases} f(\sigma_1, ..., \sigma_n), & \text{если } \nu = i; \\ 0, & \text{если } \nu \neq i; i \notin \Pi_i; \\ 1, & \text{если } \nu \neq i; i \in \Pi_i. \end{cases}$$

В последнем выражении условия $i \in \Pi_i, i \notin \Pi_i$ эквивалентны $\nu \in D_i, \nu \notin D_i \Rightarrow$ при $x_1 = \sigma_1, ..., x_k = \sigma_k$ $H(G^1_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k), ..., G^q_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k)) = H(\gamma_1, ..., \gamma_q)$, где $\gamma_1, ..., \gamma_q$ - набор на входах, соответствующих концевым вершинам из $D \backslash D_i$, дает 0, на входах дерева D_i дает всюду 1, кроме выхода под номером i, на к-рый поступает $f(\sigma_1, ..., \sigma_k)$

Опускаясь по дереву, голосование дает на выходе значение $f(\sigma_1, ..., \sigma_k)$, то есть $H(\gamma_1, ..., \gamma_q) = f(\sigma_1, ..., \sigma_k)$

24 Билет 23. Верхняя оценка сложности реализации произвольной булевой функции схемами в базисе $\{H, \&, \vee, /\}$

Пусть Σ - схема из ФЭ в базисе B

Пусть $L^{\&,\vee}_B(\Sigma)$ и $L^h_B(\Sigma)$ - соответственно число элементов $F_{/} F_\&, F_\vee$ и F_h в схеме Σ.

Теорема Для $\forall m \in N$, где $m = m(n) = o(\mathfrak{n} \log n)$, существует алгоритм, который для каждой булевой функции $f(x_1, ..., x_n)$ строит схему $\Sigma_{f(x_1,...,x_n)}$ над базисом B так, что $L_b(\Sigma_{f(x_1,...,x_n)}) \lesssim \mathfrak{1}2\mathfrak{2}^{\mathfrak{n}} n$

$$\mathfrak{L}^{,\&,\vee}(\mathfrak{t}_{\mathfrak{f}(\mathfrak{x}_1,...,\mathfrak{x}_\mathfrak{n})}) L^h(\Sigma_{f(x_1,...,x_n)}) = o(\mathfrak{1} n^m)$$

Д-во

Построим исходную схему Σ_f из блоков A, B, C, C', D, E, F (Рис.16)

q - число полос, s - i-я полоса

- Блок A реализует все конъюнкции $x_1^{\sigma_1}, ..., x_k^{\sigma_k}$; $L_B(A) \leq k + k * 2^k$

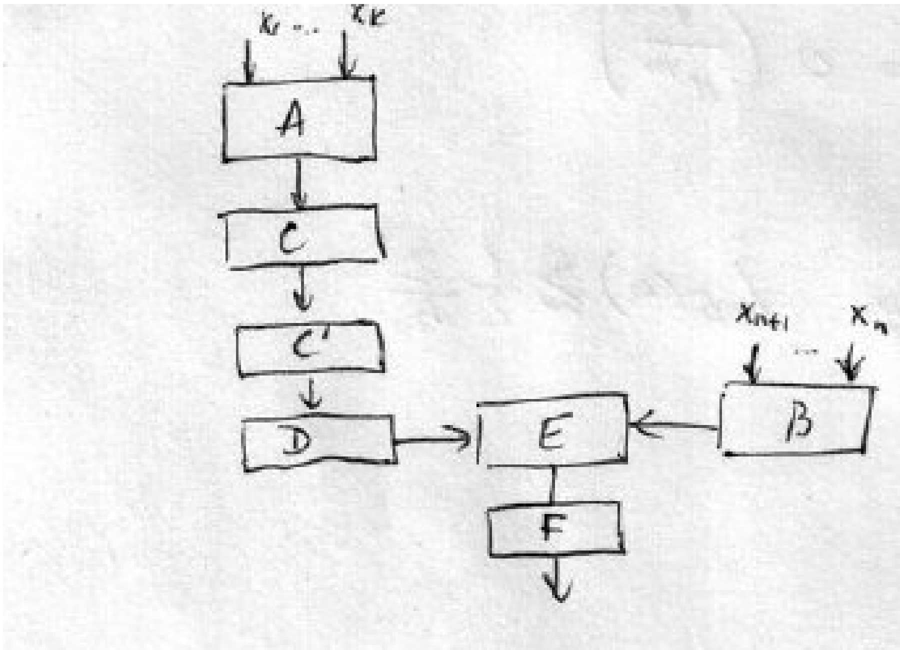

Рис. 16: Схема

- Блок B реализует все конъюнкции $x_{k+1}^{\sigma_{k+1}}, ..., x_n^{\sigma_n}$; $L_B(B) \leq (n-k) + (n-k) * 2^{n-k}$
- Блок C реализует в виде совершенной ДНФ все короткие столбцы и функции ψ_j; $L_B(C) \leq sq * 2^s$
- Блок C' реализует с помощью дизъюнкторов все „удлинненные“ столбцы. $L_B(C') \leq 2^s * q^{s/2}$
- Блок D реализует все функции $f(x_1, ..., x_k, \sigma_{k+1}, ..., \sigma_n)$, исходя из формул $H(G^1_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k), ..., G^q_{\sigma_{k+1},...,\sigma_n}(x_1, ..., x_k))$. Для этого требуется $[q/2]$ элементов F_h на каждую формулу и, может быть, нужно реализовать 0 (требует 2 элемента). $L_B(D) = [q/2]2n - k + \Delta$; Δ равно 0 или 2.
- Блок E реализует функции вида $x_{k+1}^{\sigma_{k+1}}, ..., x_n^{\sigma_n} f(x_1, ..., x_k, \sigma_{k+1}, ..., \sigma_n)$; $L_B(E) \leq 2^{n-k}$
- Блок F реализует функцию $f(x_1, ..., x_n)$; $L_B(F) \leq 2^{n-k}$

Пусть $k = [(m+3)\log_2 n], s = [n - (3m+6)\log_2 n]$
Тогда

$$L_B(A) \lesssim 2^{\mathfrak{n}} * 2^{\mathfrak{O}(\mathfrak{n})} n^{m+1} 2^n = o(2^{\mathfrak{n}} n^{m+1}) L_B(B) \lesssim 2\mathfrak{n} * 2^{\mathfrak{n}} n^{m+3} = o(2^{\mathfrak{n}} n^{m+1}) L_B(C) \lesssim 2^{s+k}\, 2^{\mathfrak{n}} n^{2m+3} = o(2^{\mathfrak{n}} n^{n}$$

Отсюда $L_B(n) \leq L_B(\Sigma_{f(x_1,...,x_n)})\ \frac{2^n}{2n}$
и

$$\frac{L^{\&,\vee}(\Sigma_{f(x_1,...,x_n)})}{L^h(\Sigma_{f(x_1,...,x_n)})} = o(\frac{1}{n^m})$$

Нижняя оценка для $L_B(n)$: $L_B(n) \gtrsim \frac{2^n}{2n}$, значит, $L_B(n)\ \frac{2^n}{2n}$

25 Билет 24. Теорема о сколь угодно надежной реализации произвольной БФ схемой в базисе $\{H, \&, \vee, /\}$

Рассмотрим СФЭ в базисе $B_p = B_1 \cup B_2$, где $B_1 = \{F_h\}, B_2 = \{F_/ F_\&, F_\vee\}$

$p = \max\{P(F_/), P(F_\&), P(F_\vee)\} \in (0, 0.5)$

Пусть $\epsilon > 0$ - некоторое число, γ^ϵ - класс всех схем Σ в базисе $B_p : P(\Sigma) < \epsilon$. γ^ϵ содержит все схемы, реализующие любые булевские функции. Пусть $L_{B_p}(f, \epsilon) = \min_\Sigma L_{B_p}(\Sigma); L_{B_p}(n, \epsilon) = \max_{f \in P_2^n} L_{B_p}(f, \Sigma)$, где Σ реализует f так, что $P(\Sigma) < \epsilon$

$L_{B_p}(n, \epsilon)$ - функция Шеннона, характеризующая сложность реализации булевских функций от n переменных в классе γ^ϵ

Теорема Существует алгоритм, который для каждой булевой функции $f(x_1, ..., x_n)$ строит схему $\Sigma_{f(x_1,...,x_n)}$ из γ^ϵ такую, что

- $L_{B_p}(\Sigma_{f(x_1,...,x_n)}) \leq \frac{2^n}{2n}$
- Для любого $\epsilon > 0$ существует $N(\epsilon)$ такое, что при $n > N(\epsilon)$ $P(\Sigma_{f(x_1,...,x_n)}) < \epsilon)$

Д-во

1) Пусть m=2. Построим последовательность $\{\Sigma'_{f(x_1,...,x_n)}\}$ схем над базисом B, для которой $L_B(\Sigma'_{f(x_1,...,x_n)})$ $\frac{2^n}{2n}$

$$\frac{L^{/,\&,\vee}(\Sigma'_{f(x_1,...,x_n)})}{L^h(\Sigma'_{f(x_1,...,x_n)})} = o(\frac{1}{n^2})$$

2) Построим элементы $\widetilde{F_/} = F_/^{(l)}, \widetilde{F_\&} = F_\&^{(l)}, \widetilde{F_\vee} = F_\vee^{(l)}$ из элементов базиса B_p так, чтобы $\max\{P(\widetilde{F_/}), P(\widetilde{F_\&}), P(\widetilde{F_\vee})\} < 1/6$.

Пусть $c = \max\{L_{B_p}(\widetilde{F_/}), L_{B_p}(\widetilde{F_\&}), L_{B_p}(\widetilde{F_\vee})\}$

3) Для каждой схемы F рассмотрим схему (Рис.17) $\Sigma_F^{(l)}$, содержащую l ярусов элементов голосования, где $l =]\log_2 n[$

Схема в исправном состоянии реализует ту же функцию, что и F. взяв в качестве F - $\widetilde{F_/}, P(\widetilde{F_\&}), P(\widetilde{F_\vee}$, получаем схемы $\Sigma_/ \Sigma_\&, \Sigma_\vee$. В этом случае $L_{B_p} \leq 3(c+1)n^2$

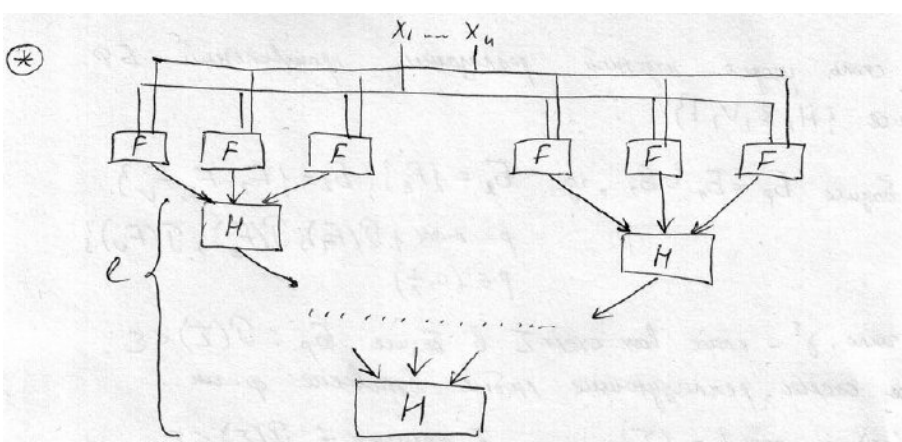

Рис. 17: Схема

Заменив в схеме $\Sigma'_{f(x_1,\ldots,x_n)}$ элементы $F_{/}F_{\&}, F_{\vee}$ на $\Sigma_{/}\Sigma_{\&}, \Sigma_{\vee}$, получаем схему $\Sigma_{f(x_1,\ldots,x_n)}$ над B_p.

$L_{B_p}(\Sigma_p) \leq L^h_B(\Sigma'_f) + L^{/,\&,\vee}_B(\Sigma'_f) * \max\{L_{B_p}(\Sigma_{/}), L_{B_p}(\Sigma_{\&}), L_{B_p}(\Sigma_{\vee})\} \lesssim \frac{2^n}{2n}$

$P(\Sigma_f) \leq L^{/,\&,\vee}_B(\Sigma'_f) * \max\{P(\Sigma_{/}), P(\Sigma_{\&}), P(\Sigma_{\vee})\} = o(\frac{1}{n^3}$. Т.к. $l \geq \log_2 n$, $o(\frac{1}{2^{2^l}}) = o(\frac{1}{2^n})$, то п. 2 вывода теоремы верен

Следствие $L_{B_p}(n, \epsilon)\ \frac{2^n}{2n}$

Из св-в нижней оценки и данной асимптотики вытекает также, что при фиксированном $\epsilon > 0$ для почти всех булевских функций минимальная ϵ-надежная схема имеет сложность, асимптотически равную $\frac{2^n}{2n}$, т.е. сложность минимальной схемы без требования надежности. Для указанного класса ф-й удается достичь надежной реализации без существенного усложнения схемы

Список литературы