Введение в дискретную математику
ВМК МГУ 2-й семестр 1996

1 поток, лектор - ***О.Б. Лупанов*** *(Мехмат МГУ)*

Другие источники:
С.В. Яблонский. Введение в дискретную математику.
В.Г. Болтянский, В.А. Ефремович. Наглядная топология.

Frequently Asked Questions

1. Функции алгебры логики. Равенство функций. Тождества для элементарных функций.

- Фиксируем исходный алфавит переменных $U = \{u_1, \dots, u_n, \dots\}$
- Будем рассматривать функции $f(u_1, \dots, u_n)$, аргументы которых определены на множестве $E^2 = \{0,1\}$ и такие, что $f(a_1, \dots, a_n) \in E^2$, когда $a_i \in E^2$.Эти функции будем называть *функциями алгебры логики* или *булевыми функциями*.
- Каждая f определяет отображение $f: E^2 \times E^2 \times \dots \times E^2 \to E^2$.
- Обозначим систему булевых функций через $\mathbf{P_2}$.
- Каждая функция однозначно определяется таблицей истинности. Число строк в таблице истинности для функции n аргументов равно $m = 2^n$. Число функций из $\mathbf{P_2}$, зависящих от n аргументов равно $p_2(n) = 2^m$.
- Функция f *существенно зависит* от переменной x_i, если существуют два набора ее аргументов $A = (a_1,\dots,a_i\ 0\ a_{i+1},\dots,a_n)$ и $A' = (a_1,\dots,a_i\ 1\ a_{i+1},\dots,a_n)$, отличающиеся только в значении x_i, такие, что значения функции на этих наборах различны: $fA \neq fA'$. Если x_i не является существенной, то она называется несущественной или фиктивной.
- Пусть x_i несущественна для f. Тогда обозначим через g функцию n-1 аргументов $(a_1,\dots,a_i\ a_{i+1},\dots,a_n)$, такую, что $g(a_1,\dots,a_i\ a_{i+1},\dots,a_n) = f(a_1,\dots,a_i\ 0\ a_{i+1},\dots,a_n) = f(a_1,\dots,a_i\ 1\ a_{i+1},\dots,a_n)$. Будем говорить, что g получена из f *путем удаления фиктивной* x_i и что f получена из g *путем введения фиктивной* x_i.
- f и g называются *равными*: $f \equiv g$ если f получается из g введением и удалением фиктивных переменных.
- Элементарные функции: (а) константы 0, 1
- (б) унарные связки: x, отрицание $\neg x$
- (в) бинарные связки: конъюнкция $xy \equiv x \,\&\, y \equiv x \wedge y \equiv \min(x,y)$, дизъюнкция $x \vee y \equiv \max(x,y)$, импликация $x \Rightarrow y \equiv (x \le y)$, сложение по модулю 2 (исключающее или) $x \oplus y = x + y \pmod 2$, ‘штрих’ Шеффера $x / y \equiv \neg(x \,\&\, y)$.
- Простейшие тождества

двойное отрицание $\neg(\neg x) = x$
$\neg(x \,\&\, y) = (\neg x) \vee (\neg y)$, $\neg(x \vee y) = (\neg x) \,\&\, (\neg y)$
коммутативность $x \,\&\, y = y \,\&\, x$, $x \vee y = y \vee x$
$x \,\&\, (\neg x) = 0$, $x \vee (\neg x) = x \oplus (\neg x) = 1$
$1 \,\&\, x = 0 \vee x = x$, $0 \,\&\, x = 0$, $1 \vee x = x$
$0 \Rightarrow x = 1$, $1 \Rightarrow x = x$
ассоциативность $(x \,\&\, y) \,\&\, z = x \,\&\, (y \,\&\, z) \equiv x \,\&\, y \,\&\, z$ - аналогично для связок $\vee$, $\oplus$.
дистрибутивность $(x \,\&\, y) \vee z = (x \vee z) \,\&\, (y \vee z)$, $(x \vee y) \,\&\, z = (x \,\&\, z) \vee (y \,\&\, z)$, $x \Rightarrow (y \,\&\, z) = (x \Rightarrow y) \,\&\, (x \Rightarrow z)$
$(x \Rightarrow y) = y \vee (\neg x)$

2. Теорема о разложении булевой функции по аргументам. Теорема о совершенной дизъюнктивной нормальной форме.

- Любую булеву функцию f можно представить в виде
$f(x_1, x_2,...,x_n) = \neg x_1 g_1(x_2,...,x_n) \vee x_1 g_2(x_2,...,x_n) = \neg x_1 f(0, x_2,...,x_n) \vee x_1 f(1, x_2,...,x_n)$ - разложением по первой переменной. Указанные функции g_1 и g_2 определены единственным образом.
- Обозначение $x^\sigma \equiv \{x$, если $\sigma = 1, \neg x$, если $\sigma = 0\}$
- Аналогично, f раскладывается по $m \le n$ переменным $x_1,...,x_m$ - единственным образом в дизъюнкцию 2^m формул вида
$x_1^{\sigma 1}...x_m^{\sigma m} f(\sigma_1,..,\sigma_m,x_{m+1},..., x_n)$.
- Разложение по всем n переменным называется СДНФ для функции f. СДНФ строится с помощью таблицы истинности.
- С помощью понятия СДНФ становится очевидно, что любая булева функция представима в виде формулы над множеством из трех элементарных связок $\{ \&, \vee, \neg \}$

3. Полные системы. Примеры полных систем (с доказательством).

- Система булевых функций $\{f_1, f_2, ... , f_n\}$ называется полной (в P_2), если любая булева функция может быть записана в виде формулы через функции этой системы.
- Множество из трех элементарных связок $\{\&, \vee, \neg\}$ является полной системой. При этом оно остается полным, если убрать одну из двух бинарных связок $\&, \vee$ выразив эту связку через другую и отрицание.
- **Теорема**. Если система **F** полна и все ее функции выражаются через функции системы G, то G также полна.
- Система из *одной функции* Шеффера $\{x/y\}$ является полной. В самом деле , $(x/x) = \neg x$ и $\neg(x/y) = x \& y$

4. Теорема Жегалкина о представимости булевой функции полиномом.

- Система $G = \{0, 1, x\&y, x \oplus y\}$ полна. Таким образом, любая f, представленная в виде формулы над G, после раскрытия скобок выражается в виде полинома по mod 2 (*полинома Жегалкина*)
- $f(x_1,\ldots,x_n) = \sum a(i_1,..,i_s)x_1\ldots x_s$, где суммирование производится по всем наборам переменных и по mod 2. Единственность такого представления доказывается подсчетом числа различных полиномов, которое оказывается равным мощности $\mathbf{P_2}$.

5. Понятие замкнутого класса. Замкнутость классов.

- Пусть $R \subseteq P_2$. Замыканием [R] класса R называется множество всех функций из P_2, представимых в виде формул над R.
- Очевидно, что $R \subseteq [R]$, $[[R]] = [R]$, если $R_1 \subseteq R_2$, то $[R_1] \subseteq [R_2]$
- Замыканием $\{1, \oplus\}$ является класс **L** линейных функций.
- R - полный класс $\Leftrightarrow [R] = P_2$.
- Класс R называется замкнутым, если $[R] = R$.
- Любой класс вида $R = [A]$ замкнут.
- Класс линейных функций $\mathbf{L} = [\{1, \oplus\}]$ замкнут.
- Через $\mathbf{T_0}$ и $\mathbf{T_1}$ обозначаются классы функций, сохраняющих соответственно константы 0 и 1, т.е. $f \in \mathbf{T_0} \Leftrightarrow f(0,0,...,0)=0$ и $g \in \mathbf{T_1} \Leftrightarrow f(1,1,...,1)=1$. Классы $\mathbf{T_0}$ и $\mathbf{T_1}$ замкнуты.

- Класс **S** самодвойственных функций ***(See also n.6)*** замкнут.
- Класс **M** монотонных функций ***(See also n.7)*** замкнут.

6. Двойственность. Класс самодвойственных функций, его замкнутость.

- Функция $f^* = \neg f(\neg x_1,..., \neg x_n)$ называется двойственной к $f(x_1,...,x_n)$. Таблица истинности для f^* получается из таблицы истинности для f инвертированием и переворачиванием столбца значений.
- Очевидно, что двойственными для функций 0, 1 являются соответственно 1, 0; двойственными для x, ¬x являются соответственно ¬x, x; двойственными для x & y, $x \vee y$ являются соответственно $x \vee y$, x & y.
- *Принцип двойственности*: пусть $f(x_1,...,x_n)$ представлена в виде формулы $C[f_1,..,f_n]$ над мн-вом функций $\{f_1,..,f_n\}$. Тогда формула $C^* = C[f_1^*,..,f_n^*]$, полученная заменой всех вхождений f_i соответственно на f_i^* представляет функцию $f^*(x_1,...,x_n)$, двойственную к f.
- Обозначим через **S** класс всех самодвойственных функций, т.е. всех булевых функций $f = f^*$. Такие f на противоположных наборах аргументов принимают противоположные значения.
- Мощность **S** = $\sqrt{2^{2^n}} = \sqrt{Card(P_2)}$
- Покажем, что класс **S** замкнут ***(See also n.5).*** Поскольку E(x) = x самодвойственна, то достаточно показать, что $F = f(f_1, f_2,...,f_n)$ самодвойственна, если только $\{f, f_1, f_2,...,f_n\} \subset \mathbf{S}$. В самом деле, согласно принципу двойственности, заменяя в формуле для F функцию f и каждую из функций f_i соответственно на $f^* = f$ и $f_i^* = f_i$, т.е. не изменяя формулу, получаем формулу для функции, двойственной к F. Таким образом, любая F - композиция самодвойственных - является самодвойственной.

7. Класс монотонных функций, его замкнутость.

- *Частичный порядок* на множестве двоичных наборов. Пусть $\alpha=(a_1,...,a_n)$ и $\beta=(b_1,...,b_n)$ - наборы из n битов. Будем писать $\alpha \le \beta$, если $a_1 \le b_1$, ... , $a_n \le b_n$.
- Булева функция f называется *монотонной*, если для любых наборов $\alpha \le \beta$ выполняется $f(\alpha) \le f(\beta)$. Примеры: x, x & y, $x \vee y$.
- Обозначим через **M** класс всех монотонных булевых функций.
- Класс **M** замкнут ***(See also n.5)***. Поскольку E(x) = x монотонна, то достаточно показать, что $F = f(f_1, f_2,...,f_n)$ монотонна, если только $\{f, f_1, f_2,...,f_n\} \subset \mathbf{M}$. В самом деле, если $\alpha \le \beta$, то в силу монотонности f_i имеем $f_1(\alpha) \le f_1(\beta)$, ... , $f_n(\alpha) \le f_n(\beta)$. Тогда $F(\alpha)= F(f_1(\alpha),$ ... , $f_n(\alpha)) \le F(f_1(\beta),$ ... , $f_n(\beta))$ в силу монотонности f. Таким образом, любая F - композиция монотонных - является монотонной.

8. Лемма о несамодвойственной функции.

- *Лемма*. Если $f = f(x_1, ...,x_n) \notin \mathbf{S}$, то путем подстановки вместо x_i либо x, либо ¬x, из нее можно получить константную (несамодвойственную) функцию g() одной переменной x.
- В самом деле, поскольку f несамодвойственна, то существует набор α такой, что $f(\alpha) = f(\neg\alpha)$. Положим $x_i = x$, если $\alpha_i = 1$, $x_i = \neg x$, если $\alpha_i = 0$. Тогда $g(0) = f(\neg\alpha_1,..., \neg\alpha_n) = f(\alpha_1,..., \alpha_n) = g(1)$. Таким образом, g - константа.

9. Лемма о немонотонной функции.

- *Лемма*. Если $f = f(x_1, ...,x_n) \notin \mathbf{M}$, то путем подстановки вместо x_i либо x, либо константы 0,1, из нее можно получить отрицание (немонотонную функцию) $g(x) = \neg x$ одной переменной x.
- Будем называть наборы α и β соседними (по i-й координате), если они отличаются только в i-й координате.

- В силу немонотонности f найдется пара соседних наборов $\alpha \le \beta$ таких, что $1 = f(\alpha) > f(\beta) = 0$. $\alpha = (a_1, \ldots a_{i-1}, 0, a_{i+1}, \ldots, a_n)$ и $\beta = (a_1, \ldots a_{i-1}, 1, a_{i+1}, \ldots, a_n)$. Рассмотрим функцию $g(x) = (a_1, \ldots a_{i-1}, x, a_{i+1}, \ldots, a_n)$. Очевидно , $g(0) = f(\alpha) = 1$ и $g(1) = f(\beta) = 0$. Таким образом, $g(x) = \neg x$.

10. Лемма о нелинейной функции.

- *Лемма.* Если $f = f(x_1, \ldots,x_n) \notin \mathbf{L}$, то путем подстановки вместо x_i либо x(y) либо $\neg x(\neg y)$ либо констант 0,1, а также, возможно, навешивания отрицания на f, из нее можно получить конъюнкцию (нелинейную функцию) g(x,y) = x&y двух переменных x и y.
- Рассмотрим полином Жегалкина для f.
- $f(x_1,\ldots,x_n) = \sum a(i_1,..,i_s)x_1 \ldots x_s$. В силу нелинейности полинома в нем найдется член, содержащий не менее двух переменных x_1 и x_2 с ненулевым коэффициентом.
- Тогда полином можно переписать следующим образом:
- $f(x_1, x_2, \ldots,x_n) = x_1x_2\, f_1(x_3, \ldots,x_n) + x_1\, f_2(x_3, \ldots,x_n) + x_2\, f_3(x_3, \ldots,x_n) + f_4(x_3, \ldots,x_n)$, где $f_1(x_3, \ldots,x_n) \neq 0$. Имеется набор $\alpha = (a_3, \ldots, a_n)$, такой, что $f(\alpha) = 1$.
- Тогда положим $h(x_1, x_2) = f(x_1, x_2, a_3, \ldots, a_n) = x_1x_2 + x_1b_2 + x_2\, b_3 + b_4$, где b_2 , b_3 , b_4 - константы.
- Рассмотрим функцию $g(x, y)= h(x+b_3,y+b_2)+b_2b_3+b_4$. Очевидно, что g(x,y) = x&y.

11. Теорема Поста о полноте системы булевых функций.

- *Теорема*. **Для полноты системы $G \subset P_2$ необходимо и достаточно, чтобы G не содержалась ни в одном из пяти классов T_0, T_1, S, M, L**.
- *Необходимость* очевидна. В самом деле, если бы полная G содержалась бы в замкнутом классе R, то $P_2 = [G] \subseteq [R] = R$, но все указанные классы замкнуты и не совпадают с P_2.
- *Достаточность*. Пусть в G имеются функции f_1, f_2, f_3, f_4, f_5, не лежащие соответственно в T_0, T_1, S, M, L. Положим $G' = \{f_1, f_2, f_3, f_4, f_5\}$ и будем считать, что эти функции зависят от одних и тех же переменных $(x_1, x_2, \ldots,x_n)$.
- (1) С помощью f_1, f_2, f_3 построим константы 0 и 1.
- Положим $q(x) = f_1(x, x, \ldots,x) \notin T_0$. Очевидно, q(0) = 1.
- (а) Если q(1) = 1, то q(x) есть константа 1. Тогда с помощью $f_2 \notin T_1$ имеем вторую константу $f_2(1,1,\ldots,1) = 0$.
- (б) Если q(1) = 0, то q(x) есть $\neg x$. Тогда в силу соотв. леммы ***(See also n.8)*** из несамодвойственной f_3 можем получить константу c, и, применяя отрицание, получаем вторую константу $\neg c$.
- (2) С помощью констант 0,1 и немонотонной f_4 по соотв. лемме ***(See also n.9)*** можно построить отрицание $\neg x$.
- (3) С помощью констант 0,1, отрицания и нелинейной f_5, можно по соотв. лемме ***(See also n.10)*** получить конъюнкцию x&y.
- Таким образом, с помощью G выражается полная система $\{0,1,\neg,\&\}$, откуда G также полна ***(See also n.3)***.

12. Теорема о максимальном числе функций в базисе системы булевых функций.

- *Теорема.* Любой базис $\mathbf{P_2}$ содержит не более четырех функций, т.е. из всякой системы G полной в $\mathbf{P_2}$, можно оставить не более четырех функций, образующих полную систему.
- Из G можно согласно 11 выделить полную подсистему, содержащую не более 5 функций - f_1, f_2, f_3, f_4, f_5. Как видно из доказательства 11, пункт (1) функция f_1 либо не самодвойственна (случай а),

либо не монотонна и не сохраняет 1 (случай б). Поэтому полной подсистемой G будет также либо $\{f_1, f_2, f_4, f_5\}$ либо $\{f_1, f_3, f_4\}$

- Тот факт, что максимальное число функций в базисе в самом деле равно $\mathbf{P_2}$, следует из рассмотрения примера G = {0, 1, x & y, x ⊕ y ⊕ z}. В самом деле , $G\backslash\{0\} \subset \mathbf{T_1}$, $G\backslash\{1\} \subset \mathbf{T_0}$, $G\backslash\{\&\} \subset \mathbf{L}$, $G\backslash\{x \oplus y \oplus z\} \subset \mathbf{M}$.

13. Теорема о предполных классах.

- Класс $R \subset \mathbf{P_2}$ называется *предполным*, если R не является полным (в $\mathbf{P_2}$), а для любой f из $\mathbf{P_2}\backslash R$ класс $R \cup \{f\}$ является полным.

- Из определения следует, что любой предполный класс замкнут.

- Из 11 следует, что в алгебре логики существует только пять предполных классов: T_0, T_1, S, M, L.

- В самом деле, пусть G - предполный класс. Тогда, поскольку G не полон, $G \subseteq A$, где A - один из пяти указанных выше классов. Предположим, что $G \neq A$. Тогда возьмем $f \in A\backslash G$. По определению предполного класса, система $G' = G \cup \{f\}$ полна. Но, с другой стороны, $G' \subseteq A \Rightarrow G'$ не может быть полной (противоречие). Следовательно, G = A, т.е. совпадает с одним из T_0, T_1, S, M, L.

14. k-значные функции. Теорема о существовании полной конечной системы в мн-ве k-значных функций.*

- $E^k = \{0, 1, ..., k-1\}$. Функции вида $f(x_1, x_2, ..., x_n)$, аргументы и значения которых принадлежат E^k, будем называть функциями k-значной логики.

- Через P_k обозначим множество всех таких функций над алфавитом переменных U. Число функций из P_k, зависящих от n аргументов равно $p_k(n) = k^{k^n}$

- Элементарные функции:

(1) 'Циклический сдвиг' $\neg x = x \oplus 1 \pmod k$ - обобщение отрицания.
(2) $\min(x,y) \equiv x \,\&\, y$ и
(3) $xy \pmod k$ - два обобщения коньюнкции.
(4) $\max(x,y) \equiv x \vee y$ - обобщение дизьюнкции.
(5) $x + y \pmod k$
(6) $I_\sigma(x) = \{k-1$, если $x = \sigma$; 0 если $x \neq \sigma\}$

- Простейшие свойства:

(1) функции min, max, ⊕ ассоциативны и коммутативны.
(2) ~~x = x.
(3) ~min(x, y) = max(~x, ~y)
(4) $f(x_1,\ldots,x_n) = \max_{(\sigma_1,\ldots,\sigma_n)} .(I_{\sigma_1}(x_1)\&\ldots\&I_{\sigma_n}(x_n)\&f(\sigma_1,\ldots,\sigma_n))$

- аналог СДНФ в k - значной логике, доказывается прямой проверкой.

- Аналогично вводится понятие полноты системы k - значных функций ***(See also n.3)***.

- Как видно из (4), система функций, содержащая константы, функции $I_\sigma(x)$, min, max является полной.

15. Основные понятия теории графов. Изоморфизм графов. Связность.

- Множество объектов-вершин $V = \{a_1, ..., a_n, ...\}$ и множество пар объектов из V (*ребер*) W образуют *граф* $\mathbf{\Gamma}=(V,W)$. Про ребро вида (a_k, a_m) говорят, что оно *соединяет* вершины a_k и a_m. Граф называется конечным, если множество V конечно.

- Если ребра считаются упорядоченными парами, т.е. $(a,b) \neq (b,a)$ при $b \neq a$, то граф называется *ориентированным*.

- Если в W каждому ребру (a,b) приписана кратность $k \in \mathbf{N}$, то говорят, что **Г** допускает *кратные ребра* или, что вершины a и b соединяют k ребер.
- Граф Г=(V,W) называется *полным*, если любые две вершины a_k, $a_m \in V$ соединены ребром (a_k, a_m) $\in W$. Любое ребро вида (b,b) называется петлей.
- *Степенью* вершины называется число ребер, содержащих эту вершину.
- Набор ребер графа вида (b_1,b_2) (b_2,b_3).... (b_{n-1},b_n), где b_i - какие-то вершины графа, называется *путем* из b_1 в b_n. Любой путь из b в b называется *циклом*.
- Граф называется *связным*, если для любых вершин a_k и a_m существует путь, их соединяющий.
- Графы Г = (V,W) и Г' = (V',W') называются *изоморфными* $\Gamma \cong \Gamma'$, если существует взаимно-однозначное соответствие между вершинами $f: V \to V'$ и взаимно-однозначное соответствие между ребрами $g: W \to W'$, причем g(a,b) = (fa,fb).
- *Подразделением* графа Г называется любой граф Г', полученный из Г путем применения конечного числа раз операции подразделения ребер (т.е. введения новой вершины c и замены подразделяемого ребра (a,b) на пару ребер (a,c) и (b,c)).
- Графы Γ_1 и Γ_2 называются гомеоморфными, если существуют такие их подразделения Γ_1' и Γ_2', которые изоморфны.

16. Деревья. Свойства деревьев.

- *Деревом* называется связный ациклический граф G.
- Имеет место соотношение: $\chi(G) = B - P = 1$, где B - число вершин и P - число ребер дерева G (доказывается индукцией по P).
- Для любого связного графа G существует остовное дерево - его подграф, содержащий все его вершины и являющийся деревом.

17. Корневые деревья. Верхняя оценка их числа.

- Корневым называется любое дерево с выделенной вершиной, именуемой *корнем.*

18. Геометрическая реализация графов. Теорема о реализации графов в трехмерном пространстве.

- Геометрической реализацией графа Г называется изоморфный ему граф Г', вершинами которого являются точки в пространстве (на плоскости или другой поверхности), а ребрами - соединяющие эти точки кривые, не пересекающиеся между собой.
- Теорема. Любой конечный граф допускает правильную реализацию в трехмерном пространстве.

19. Планарные (плоские) графы. Формула Эйлера.

- *Планарным* называется любой граф, допускающий реализацию на плоскости (или гомеоморфной ей поверхности).
- Гранями планарного графа называются связные области, на которые ребра графа разбивают плоскость.
- Обозначения: B - число вершин графа; Г - число граней; P - число ребер; *Формула Эйлера*: **B + Г - P = 2** для любого связного планарного графа G.
- Идея доказательства: (1) Рассмотрим G^* - остовное (максимальное) дерево G. (2) $B(G^*) = B(G)$; $P(G^*) \le P(G)$; и, очевидно, $\Gamma(G^*)=1$.

- (3) Согласно 16, $B(G^*) - P(G^*)=1 \Rightarrow$ для G^* формула верна. (4) Будем добавлять к G^* перемычки - ребра G, не принадлежащие G^*. При этом добавление одной перемычки увеличивает число граней на одну (поскольку перемычка не пересекает других ребер) $\Rightarrow$ формула каждый раз остается верной.

20. Доказательство непланарности графов K_5 и $K_{3,3}$. Теорема Понтрягина-Куратовского (доказательство в одну сторону).

- Обозначения. K_n - полный граф с n вершинами. $K_{m,n}$ - полный двудольный граф с m вершинами в одной доле и n вершинами в другой.
- *Теорема*. **Графы K_5 и $K_{3,3}$ непланарны** (доказывается с помощью 19).
- (а) Пусть имеется плоская реализация K_5. $B = 5$; $P = 10$; $\Gamma \le 6 \le 20/3$ (т.к. минимальная длина цикла в K_5 равна 3) $\Rightarrow B + \Gamma - P \le 1$ (противоречие).
- (б) Пусть имеется плоская реализация $K_{3,3}$. $B = 6$; $P = 9$; $\Gamma \le 4 \le 18/4$ (т.к. минимальная длина цикла в $K_{3,3}$ равна 3) $\Rightarrow B + \Gamma - P \le 1$ (противоречие).
- *Теорема Понтрягина-Куратовского*. G планарен $\Leftrightarrow$ G не содержит подграфов, гомеоморфных K_5 и $K_{3,3}$.

21. Теорема о раскраске планарных графов в 5 цветов.

- Будем говорить, что граф *правильно раскрашен в N цветов*, если его вершинам приписаны числа от 1 до N (*цвета*), причем никаким соседним вершинам не приписан один цвет.
- Лемма. Пусть G - планарный граф без петель и кратных ребер. Тогда в G имеется хотя бы одна вершина степени $k \le 5$ (доказывается от противного с помощью формулы Эйлера).
- *Теорема*. **Любой планарный граф G допускает раскраску в 5 цветов**.
- Индукция по числу вершин B. Для $B \le 5$ очевидно.
- Пусть существует раскраска для $B = 5,6,...,p$. Рассмотрим граф с $B = p+1$. Выделим вершину №0 степени $k \le 5$. (а) Если $k < 5$, то по предположению раскрасим G'=G\{№0} и №0 припишем цвет ε, отличный от цветов всех ее соседей. (б) Если $k = 5$, то соседние вершины обозначим №1...№5 и проведем ребра №1↔№2, №2↔№3, ... , №5↔№1. При этом хотя бы одно из других ребер между этими соседними вершинами отсутствует. Для определенности, №2↔№5. Склеим вершины №0,№2 и №5 и по предположению раскрасим полученный G'. Вершины №1, №3, №4, и {№0,№2,№5} оказались покрашенными в какие-то четыре цвета. Припишем №0 цвет ε, отличный от этих четырех цветов, и остальную раскраску G' перенесем на G. Граф G правильно раскрашен.

22. Схемы из функциональных элементов. Реализация функций алгебры логики схемами.

- *Схемой из функциональных элементов* (СФЭ) называется конечный ориентированный граф G без циклов, каждой вершине a которого приписан символ (или символ и *) в соответствии со следующими правилами:
- (1) Если в a ребра не входят, то a приписан символ переменной x_i из фиксированного алфавита; в этом случае a называется входом. (2) Если в a входит k ребер, то a может быть приписан только символ k-арной логической связки. Используются функциональные элементы, соответствующие элементарным связкам ¬,&,∨ (возможны и другие). (3) Кроме того, любая вершина может быть помечена символом *; такая вершина называется *выходом*.
- Каждой вершине a приписывается булева функция $f_a(x_1, x_2, ...,x_n)$, равная (1) переменной x_i (если a - вход); (2) $f(f_1, f_2, ...,f_k)$, где $f_1, f_2, ...,f_k$ - функции, приписанные началам входящих в a ребер, и f - приписанная a k-арная связка (если a - ФЭ).
- Каждая СФЭ естественным образом реализует вычисление m n-арных булевых функций, где n и m - соотв. количество входов и количество выходов.

- Сложностью L(S) функциональной схемы S называется число функциональных элементов, ее составляющих.

- Вопрос об алгоритме A синтеза СФЭ для произвольной булевой функции n аргументов. Функции Шеннона $L_A(n) = \sup\{L_A(f), f$ - функция n аргументов$\}$.

23. Дешифратор. Асимптотика сложности дешифратора. Верхняя оценка сложности реализации произвольной булевой функции.

- *Дешифратором* D_n называется произвольная СФЭ, имеющая n входов и 2^n-1 выходов и реализующая вычисление 1 на выходе №M и 0 на всех остальных выходах, если на входы подана двоичная запись числа M.

- $L(D_n) \sim 2^n$.

- СДНФ для произвольной булевой функции можно реализовать простейшим способом со сложностью $L_A(n) \sim n2^n$.

24. Мультиплексор. Верхняя оценка сложности мультиплексора.

25. Шифратор. Верхняя оценка сложности шифратора.

- *Дешифратором* S_n называется произвольная СФЭ, имеющая 2^n-1 входов и n выходов и реализующая вычисление двоичной записи числа M, если на входе №M подана 1 и 0 подан на всех остальных входах.

- Одна из возможных реализаций шифратора основана на следующей простой идее. Чтобы бит n числа M оказался равным 1 $\Leftrightarrow$ чтобы была подана 1 на вход, номер которого имеет 1 в n-бите двоичной записи. Поэтому этот выход вычисляется как дизъюнкция всех битов №k входа, в двоичной записи номера которых k этот бит n равен 1. Т.е. достаточно на выход 0 подать дизъюнкцию входов №№1,3,5,...; на выход №1 - дизъюнкцию №№2,3,6,7,... и т.д.; на выход №(n-1) - дизъюнкцию №№2^{n-1},2^{n-1}+1,...2^n-1.

- Сложность этой реализации $L(S) = n2^{n-1}$.

26. Сумматор. Верхняя оценка сложности сумматора.

- *Дешифратором* Σ_n называется произвольная СФЭ, имеющая 2n входов и n выходов и реализующая вычисление двоичная запись числа $(A+B)(\mathrm{mod}\ 2^n)$, если на первую группу из n входов подана двоичная запись числа A и на вторую - двоичная запись числа B.

- Существует схема из 9 элементов, реализующая одновременное вычисление суммы трех битов по mod 2 и бита переноса (*С.В. Яблонский, с. 262, рис. 28*). Поэтому можно указать реализацию сумматора с $L(\Sigma_n) = 9n$.

27. Понятие ограниченно-детерминированной функции.

- Пусть отображение F имеет аргументом некую входную последовательность $\{a(t), t \in \mathbf{N}\}$ букв из алфавита **A** и вычисляет выходную последовательность $\{b(t), t \in \mathbf{N}\}$ букв из алфавита **B**. При этом будем рассматривать только такие отображения, где каждый элемент выхода не зависит от следующих элементов входа, т.е. b(t) есть функция $\{a(1),...,a(t)\}$. Такие F называются *детерминированными автоматами*.

- Детерминированные автоматы (функции) задаются с помощью деревьев. Каждое поддерево с каким-то корнем ε естественным образом определяет соответствующую ему детерминированную функцию F^ε. Два поддерева называются эквивалентными, если соответствующие функции совпадают. Число r (мощность множества) классов эквивалентности поддеревьев называется *весом* детерминированной функции (автомата, дерева).

28. Конечные автоматы и автоматные функции. Представление конечного автомата диаграммой Мура. Автомат единичной задержки.

- Автомат F называется конечным (ограниченно-детерминированным), если он имеет конечный вес r.
- Ограниченно-детерминированная функция с весом r задается с помощью специального графа с r вершинами - диаграммы Мура. Одна из вершин определена в качестве начальной; из каждой вершины исходит N = Card **A** ребер, ребрам приписаны пары $(0,\gamma^0)$, $(1,\gamma^1)$, ... , $(N-1,\gamma^{N-1})$, $\gamma^i \in \mathbf{B}$.
- Канонические уравнения для о.-детерминированного автомата рекуррентным образом определяют функцию:
- $b(t) = b(a(t),q(t-1))$; $q(t) = q(a(t),q(t-1))$; $q(0) = q_o$.
- *Автомат единичной задержки* по входной последовательности вида {a,b,c,...} вычисляет {0,a,b,c,...}, т.е. определяется свойством $b(t) = b(t-1)$, $b(1) = 0$ и может быть реализован следующими каноническими уравнениями: $b(t) = q(t-1)$; $q(t) = a(t)$; $q(0) = 0$.

29. Преобразование периодических последовательностей автоматными функциями.

- Лемма. Пусть на вход F - конечного автомата с λ состояниями подается последовательность a(t) с периодом T (т.е. $a(t+T) = a(t)$ начиная с некоторого момента T_0). Тогда последовательность на выходе имеет период $T'=T\lambda'$, где $\lambda' \le \lambda$.
- Рассмотрим моменты времени T_0, T_0+T, ... , $T_0+\lambda T$. Среди $\lambda+1$ состояния $q(T_0)$, $q(T_0+T)$, ... , $q(T_0+\lambda T)$ найдутся два одинаковых: $q(T_0+iT) = q(T_0+jT)$ при $j > i$. Тогда очевидно, вычисление в момент T_0+jT полностью повторяет вычисление в момент $T_0+iT \Rightarrow$ выходная последовательность имеет период $T' = T(j - i)$.

30. Схемы из функциональных элементов и элементов задержки. Автоматность осуществляемых ими отображений.

- СФЭ, дополненные элементами единичной задержки могут реализовывать любые конечные автоматы. При этом допускаются ориентированные циклы, содержащие хотя бы один элемент единичной задержки.
- Покажем, что любая такая схема S осуществляет некоторое автоматное отображение. Будем считать, что входом и выходом автомата F(S) являются соответственно совокупность входов a(t) и совокупность выходов b(t) схемы S. Совокупность входов элементов единичной задержки из S обозначим q(t), а совокупность выходов этих элементов - q(t-1). Тогда часть S, являющаяся СФЭ (S\{элты ед.з.}), в любой момент времени осуществляет вычисление $b(t)=b(a(t),q(t-1))$ и $q(t)=q(a(t),q(t-1))$. Таким образом, S осуществляет ограниченно-детерминированное отображение $F: a \to b$.

31. Моделирование автоматной функции схемой из функциональных элементов и элементов задержки.

- Любую ограниченно-детерминированную функцию F можно вычислить с помощью СФЭ, пополненной элементами единичной задержки. Пусть F задана каноническими уравнениями $b(t)=b(a(t),q(t-1))$ и $q(t)=q(a(t),q(t-1))$.
- Построим СФЭ, которая в каждый момент времени вычисляет на выходах b(t) и q(t), принимая на входах a(t) и q(t-1). Соединим выходы, помеченные q(t) с входами, помеченными q(t-1) элементами единичной задержки. Очевидно, что построенная S моделирует F.

32. Отсутствие полной конечной системы автоматных функций в случае схем без обратной связи.

37. Алфавитное кодирование. Схемы кодирования, обладающие свойством префикса. Неприводимые коды и их свойства.

- Пусть фиксированы алфавиты A и B. *Алфавитным кодированием* называется замена символов A на слова (конечные последовательности) символов B, т.е. любое инъективное отображение f: $(a_i \in A) \rightarrow (B_i \in B^{\omega})$. Применение f r каждой букве слова (сообщения) A^* кодирует это сообщение в $B^* = f(A^*)$.

- Если B={0,1}, то кодирование называется двоичным. Если длины *кодовых слов* одинаковы: $|B_i| = const$, то код называется равномерным.

- Требование *однозначности декодирования*: по (закодированной) последовательности $B^* = f(A^*)$ однозначно восстанавливается (оригинальная) последовательность A^*.

- Код называется *префиксным*, если ни одно из слов B_i не является началом другого. Очевидно, любой префиксный код однозначен (свойство префикса есть достаточное условие декодируемости).

- Слово в алфавите B называется неприводимым, если (1) оно допускает неоднозначное декодирование; и (2) при удалении из него любого подслова оно допускает однозначное декодирование или не допускает никакого.

- Рассмотрим два разбиения слова B на элементарные слова - T_1(нижнее) и T_2(верхнее) и возьмем произведение этих разбиений - $T = T_1T_2$. Отрезки этого разбиения разделим на два класса. Отрезками первого рода назовем элементарные слова; все остальные назовем отрезками *второго рода*. Ясно, что каждый отрезок первого рода входит только в одно разбиение, а слова второго рода являются одновременно началами и концами элементарных кодов разных разбиений.

- *Лемма*. Любые два отрезка второго рода β и β’ в неприводимом слове B различны. Предположим противное, т.е. B = B’βB’’βB’’’. Утверждается, что слово B’βB’’’ допускает неоднозначное декодирование - т.к. в каждом из четырех случаев расположения β и β’ оказывается возможным выкинуть середину B’’β , сохранив разбиения T_1 и T_2.

- Рассмотрим нетривиальное разложение элементарного кодового слова вида $B_i = \beta < w$ кодовых слов:$D_1...D_w > \beta'$ (предполагается, что β не оканчивается и β’ не начинается на кодовое слово). Введем характеристику кода W = max w , взятый по всем словам B_i и по всем разложениям каждого слова.

38. Теорема Маркова о взаимной однозначности алфавитного кодирования.

- *Теорема* (Марков). Для всякого алфавитного кодирования C существует натуральное $N_0 \le N^* = \left[\frac{(W+1)(L-r+1)}{2}\right]$, такое, что проблема однозначности C сводится к проблеме однозначности кодирования слов в алфавите A длины не более N_o.

- Пусть кодирование C неоднозначно. Для доказательства достаточно установить, что можно найти такое слово B с двумя различными расшифровками A, A’ длины не более N^*. Возьмем произвольное неоднозначно декодируемое слово B^* и выделим из него неприводимое B.

- Все отрезки второго рода в B различны, их число p не превосходит числа возможных начал элементарных кодовых слов : $p \le (l_1-1)+(l_2-1)+...+(l_r-1) = L - r$, где $L = \sum l_i$. Отрезки второго рода β^i разбивают B не более чем на L-r+1 подслов (групп отрезков второго рода), некоторые из которых могут оказаться пустыми.

- Подсчитаем число элементарных слов, входящих в разбиения. С каждым куском связаны $w \le W$ элементарных кодов одного разбиения и один элементарный код другого (чередуясь через один кусок). Отсюда получается оценка для N_o.

40. Неравенство Макмиллана.

- Для однозначного кодирования f с длинами кодовых слов $l_i = |B_i|$ выполняется соотношение $\sum_i q^{-l_i} \le 1$, где q = |B|.

41. Существование кода со свойством префикса в классе кодов с заданными длинами кодовых слов.

- Пусть задан некоторый набор длин кодовых слов l_i, удовлетворяющий неравенству Макмиллана (Крафта). Тогда с помощью простого алгоритма можно построить кодовое дерево с заданным количеством листьев на каждом ярусе.
- Таким образом, имея код с заданным набором длин кодовых слов, можно без ограничения общности считать его префиксным.

42. Коды с минимальной избыточностью (оптимальные коды). Существование приведенного кода.

- Стоимостью кода называется матожидание длины кодового слова. Если известно распределение вероятностей входных букв P: $p_1, p_2, \dots, p_r$, то стоимость кода $C = \langle B_1 B_2 \dots B_r \rangle$ вычисляется как $L(P,C) = \sum_{i=1}^{r} l_i p_i$, где $l_i = |B_i|$.
- В оптимальном коде менее вероятный символ не может кодироваться более коротким словом, т.е. $p_k > p_m \Rightarrow l_k \le l_m$.
- В оптимальном коде всегда найдутся два слова наибольшей длины

43. Теорема редукции.

- Лемма редукции. Пусть для r символов A, появляющихся с вероятностями P: $p_1 \ge p_2 \ge \dots \ge p_r$, причем $p_i = q' + q''$ и $p_i \ge q' \ge q''$. Имеется оптимальный код C с кодовыми словами $B_1 B_2 \dots B_r$. Тогда для алфавита A', полученного 'расщеплением' i буквы на две (с вероятностями q' и q'') оптимальное кодирование имеет вид $C' = \langle B_1 \dots B_i B_{i+1} \dots B_r (B_i 0) (B_i 1) \rangle$.
- Посчитаем стоимость C': $L(C') = L(C) + p_i$. Пусть C не есть оптимальный код и имеется код $C^* = \langle D_1 \dots D_i D_{i+1} \dots D_r D' D'' \rangle$ со стоимостью $L(C^*) < L(C')$. При этом D' и D'' - необходимо самые длинные и отличаются только в последнем разряде, т.е. D' = (D0) D''=(D1). Но тогда с помощью C^* можно построить код C^{**} для первоначального алфавита и распределения вероятностей P со стоимостью $L(\tilde{N}^{**}) < L(C)$ (противоречие с оптимальностью C).

44. Алгоритм построения кода с минимальной избыточностью.

- Строится код Хаффмана и доказывается его оптимальность (по индукции с помощью 43).

45. Самокорректирующиеся коды. Коды Хемминга.

46. Коды с исправлением r ошибок. Оценка функции $M_r(n)$.

47. Машины Тьюринга. Вычислимые функции. Примеры вычислимых функций.

48. Алгоритмическая неразрешимость проблемы самоприменимости машины Тьюринга.