Дискретная математика

Коченюк Анатолий

6 октября 2020 г.

0.1 Введение

Связаться:

- stankev@gmail.com Собирать культуру общения: указывать Фамилию, Имя
- Телеграм @andrewzta (для немедленного ответа. Если нет, оно утонет).
- +79219034426 (для катастрофических ситуаций, ожидается, что звонить никто не будет) (ни в коем случае не писать смс)

Обращаться можно по методическим вопросам. Если проблема группы – пишет староста.

Не писать по учебно-методическим проблемам (общежитие, медосмотр, армия ..) для этого есть зам. декана Харченко (легко найти контакты в ису)

Про отчётность будет на первой практике.

Лекции есть в ютубе andrewzta

Глава 1

1 курс

1.1 Фундамент

Множество – неопределяемое понятие. Множество состоит из элементов. $a \in A$ а-маленькое принадлежит множеству А-большое

$A = \{2, 3, 9\}$

$A = \{n \mid n \text{ чётно}, n \in \mathbb{N}\}$ – фильтр

A, B :

- $A \cup B = \{a \mid a \in A \text{ или } a \in B\}$
- $A \cap B = \{a \mid a \in A \text{ и } a \in B\}$
- $A \setminus B = \{a | a \in A \text{ и } a \notin B\}$
- $\overline{A} = \{a | a \notin A\}$??? U – универсум

  $\overline{A} = U \setminus A$

  $A \setminus B = A \cap \overline{B}$
- $A \triangle B = A \oplus B = (A \cup B) \setminus (A \cap B)$

Замечание. Если множество – любой набор чего-угодно возникает парадокс Рассела

$A = \{a | a \text{ – множество}, a \notin a\}$

Вопрос лежит ли в себе A?

Определение 1 (Пара)**.** A, B – множества. Мы можем рассмотреть множество пар, где первый элемент из A, а второй из B

$A \times B = \{(a, b) | a \in A, b \in B\}$

$A \times A = A^2$

$(A \times B) \times C = \{(x, y) | x \in A \times B, y \in C\} = \{((a, b), y) | a \in A, b \in B, y \in C\}$

$A \times (B \times C) = \{(a, (y, z)) | a \in A, y \in B, z \in C\}$

$A \times B \times C = \{(a, b, c) | a \in A, b \in B, c \in C\}$

Для простоты, здесь и далее эта операция будет считаться ассоциативной и первые две строчки будут давать то же, что третья – множество троек.

$A \times A \times A = A^3$ $A^n = \begin{cases} A & , n = 1 \\ A \times A^{n-1} & , n > 1 \end{cases}$

$A^0 = \{[]\} = \{\varepsilon\}$ – пустая последовательность.

Пример. $A = 2, 3, 9$ -> $A \times A = \{(2, 2), (2, 3), (2, 9), (3, 2), (3, 3), \ldots\}$

Замечание. У множества есть элемента и для любого элемента из универсума, он либо входит (1 раз) либо не входит.

Определение 2. Функция – отображение, которое каждому элементу из одного множества ставит в соответствие единственный элемент из другого множества

$f : A \to B$

График $\{(x, f(x))\}$.

Формально будем отождествлять функцию и её график.

$f \subset A \times B \quad \forall a \in A \exists! b \in B \quad (a, b) \in f$

Замечание. Не путайте принадлежность и включение

$a \in A$

$A, B, \forall a$ (если $a \in A$, то $a \in B$) $A \subset B$

$D_4 = \{n | n$ кратно $4\}$

$E = \{n | n$ чётно$\}$

$D_4 \subset E$

$\{2, 3, 9\} \subset \{2, 3, 4, \ldots, 9\}$

$A \subset A$

$\emptyset \subset A$

$A \subset U$

Замечание. Необязательно все b попадают в график.

$sqr : \mathbb{N} \to \mathbb{N}$ – только квадраты чисел

Определение 3. $\forall b \in B \exists a \in A : b = f(a)$ – сюръекция

Определение 4. $\forall a \in A \forall b \in B \quad a \neq b \implies f(a) \neq f(b)$

Замечание. Принцип Дирихле – нет инъекции из большего в меньшее множества. Если кроликов больше, чем клеток, то какому-то кролику не хватит клетки

Определение 5. Если f – инъекция и сюръекция, то f – называется биекцией

Если между двумя конечными множествами есть биекция, то у низ равное количество элементов.

Определение 6. Два множества называется равномощными, если между ними есть дикция

B^A – множество функций из A в B

$|A| = a, |B| = b \quad |A \times B| = a \cdot b \quad |B^A| = b^a$

$|A^\emptyset| = 1$ эфемерная функция, которой ничего не передать

$\emptyset^A = \emptyset, A \neq \emptyset$

$\emptyset^\emptyset = 1$

Определение 7. $R \subset A \times B$ – отношение (бинарное)

Пример. $A = B = \mathbb{N} \quad R = \{(a, b) | a < b\} \quad R =<$

$a \vdots b \quad 6 \vdots 2 \quad 6 \not\vdots 5$

$A =$ люди, $B =$ собаки, $R = \{(a, b) | a$ – хозяин$b\}$

Рассмотрим 5 классов отношение на квадрате множества:

1. рефлексивные $\forall a \quad aRa$

$RC(R)$ – рефлексивное замыкание, включаем все пары (a, a)

2. антирефлексивные $\forall a \quad \neg aRa$
3. симметричные $aRb \implies bRa$
4. антисимметричные $aRb, a \neq b \implies \neg bRa$

   или aRb и $bRa \implies a = b$
5. транзитивность $aRb, bRc \implies aRc$

Определение 8. 1+3+5 – рефлексивные, симметричные и тразитивные – называются отношениями эквивалентности.

Теорема 1. R – отношение эквивалентности на X, то элементы X можно разбить на классы эквивалентности так, что:

a и b в одном классе $\implies aRb$ a и b в разных классах $\implies \neg aRb$

множество таких классов обозначается X/R

$N/\equiv_3=$

$$\{\{1, 4, 7, 10, \ldots)$$
$$\{2, 5, 8, 11, \ldots)\}$$
$$\{3, 6, 9, 12, \ldots)\}\}$$
$$.$$

Замечание. Отношение равномощности – отношение эквивалентности.

Классы эквивалентности – порядки. Для конечного случая обозначаются числами

Определение 9. 1+4+5 – рефлексивные, антисимметричные и транзитивные – частичные порядки

Множество, на котором введён частичный порядок, то оно называется частично упорядоченным. (ч.у.м – частично упорядоченное множество, poset – partially organised set)

$R \subset X \times X$

$X, Y, Z \quad R : X \times Y \quad S : Y \times Z$

Определение 10. Композиция отношений:

$T = R \circ S \quad xTy \iff \exists z : xRz$ и zSy

т.е. есть z, через который можно пройти, чтобы попасть в y из x

Замечание. $R \subseteq X \times X \quad S \subseteq X \times X$

$R \circ S \subseteq X \times X$

$R \circ R \subseteq X \times X$ – пройти два раза по стрелкам

$R^3 = R \circ R^2 = R^2 \circ R$ – пути длины ровно 3

$S \circ T \circ U$ – идём по стрлке из S в T, а потом в U

Определение 11. Транзитивное замыкание.

$R^+ = \bigcup\limits_{k=1}^{\infty} R^k$

$R^0 = \{(x, x) | x \in X\}$ – они не включаются по дефолту в R^+

$R^* = \bigcup\limits_{k=0}^{\infty} R^k = R^+ \cup R^0$ – если между двумя вершинами существует какой-либо путь

Замечание. Транзитивное замыкание – транзитивно

Пусть $xR^+y \implies xR^iy$

Пусть $yR^+z \implies yR^jz$

$\implies x(R^i \circ R^j)z \implies xR^kz$

Замечание. $\forall T : T$ – транзитивно. $T \subset R \implies T^+ \subset R$

Доказательство. По индукции:

База: $R^1 \subset T$ – дано

Переход: $R^i \subset T \implies R^{i+1} \subset T$

$xR^{i+1}y \implies x(R \circ R^i)y \implies \exists z : xRz \& zR^iy \implies xTz \& zTy \implies xTy$ (по транзитивности T) ■

1.2 Булевы функции

$\emptyset$ – пустое множество. С функциями из/в него всё достаточно грустно.

$\{unit\}$

void – ничего, константная функция

$\mathbb{B} = \{0, 1\}$

$f : A_1 \times A_2 \times \ldots \times A_n \to B$ – функция от нескольких аргументов. Из одного, но декартового произведения

Булева функция: $f : \mathbb{B}^n \to B$

$n = 0$ – ноль аргументов $\mathbb{B}^0 = \{[]\}$

$\mathbb{0}, \mathbb{1}$

$n = 1$

Таблица 1.1: n=1

x	$\mathbb{0}$	id	$\neg$	$\mathbb{1}$
0	0	0	1	1
1	0	1	0	1

Замечание. Подобные таблицы называются таблицами истинности функций

$n = 2$

Таблица 1.2: n=2

x	y	$\mathbb{0}$	$\wedge$	$\not\to$	P_1	$\not\leftarrow$	P_2	$\oplus$	$\vee$	$\downarrow$	$=$	$\neg P_2$	$\leftarrow$	$\neg P_1$	$\to$	$\uparrow$	$\mathbb{1}$
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

С помощью стрелки Пирса ($\downarrow$) и штриха Шеффера ($\uparrow$) можно выразить любую другую: $\neg x = x \downarrow x$

1.3 Задания булевых функций

Самый простой способ – таблица истинности

$\oplus_n$ – 2^n значений. глупо их все отдельно описывать

1. Задание функции формулой.

   Определим базисные функции, систему связок

   например: $\wedge, \vee, \neg, \oplus$

   $x_1 \oplus x_2 \oplus x_3 \ldots$

$\{f_1, f_2, .., f_n\}$ – базисные.

строка – формула. $f_i(x_1, \ldots, x_k)$ – формула

Определение 12. Дерево разбора формулы. Если у функции арность – k, то у ноды будет ровно k сыновей

$\overline{F}$ – функции, которые записываются формулами, используя F (замыкание F)

Теорема 2 (Теорема о стандартном базисе)**.** $\overline{\{\wedge, \vee, \neg\}} = \mathbb{B}$

Доказательство. Рассмотрим таблицу истинности функции f Она принимает n аргументов и в ней 2^n строк

Пусть $f \neq \mathbb{0}$. Рассмотрим строчки, в которых единицы.

По аргументам запишем с не – аргументы, которые 0, и без не – те, которые 1

$\neg x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4 \wedge x^5$ – 1 на ровно одном наборе элементов. А теперь возьмём "или"по всем строкам, в которых 1

Одна такая строка называется термом.

Такая форма называется совершенной дизъюнктивной нормальная формой ■

Лемма 1. Любая функция, кроме тождественного 0 – есть СДНФ

$x \vee \neg x$ – тождественный ноль

Напоминание о способах задания функций:

$F \quad x_1, x_2, \ldots, x_n f \in F$

$or(and(x, not(y)), or(0, z))$. Такие формы называются формулами. По формуле можно построить дерево разбора.

$\wedge, \vee, \neg$

СДНФ – дизюнкция термов, где каждый терм – коньюнкция литералов. Совершенная – в каждом терме есть все переменные по одному разу

Лемма 2. $\supset F$ – некоторое множество. $\overline{F} = \mathbb{BF}$

$\supset G$ – некоторое множество функций $\forall f \in F \quad f \in \overline{G}$

Тогда с помощью G можно выразить любую функцию $\overline{G} = \mathbb{BF}$

Доказательство. $G \to F \to \forall \implies G \to \forall$ – то, что нужно доказать

фиксируем функцию $h \in \mathbb{BF}$. Она каким-то деревом разбора выражается через функции $f \in F$. Каждая функция f выражается через $g \in \overline{G}$, тогда подставим выражения функций f через g в узлах дерева и получим выражение функции h через $\overline{G}$, значит люая функция выражается через $\overline{G} \implies \overline{G} = \mathbb{BF}$ ■

Пример. $\{\oplus, \wedge, \mathbb{1}\}$

$x \wedge y = x \wedge y \qquad \neg x = x \oplus 1$ – такая запись называется полиномом жегалкина

$x \vee y = (x \wedge y) \oplus x \oplus y$

$x \wedge y = xy \oplus y \oplus x$ – $\wedge$ опускают

$(x \oplus y)(y \oplus z) = xy \oplus y \oplus xz \oplus yz$

$(x \oplus 1)(y \oplus 1) = xy \oplus x \oplus y \oplus 1$

$a \wedge a = a$ – идемпотентность

Теорема 3. Любая булева функция (кроме $\mathbb{0}$) имеет каноничный полином, причём единственный (с точностью до коммутативности и ассоциативности)

Доказательство. булевых функций от n аргументов – 2^{2^n}

Мономов – 2^n. Каждый из них мы можем взять или не взять $\implies$ всего $2^{2^n} - 1$, -1 из случая, где мы рассматриваем пустую сумму.

Есть инъекция из булевых функций в полиному Жегалкина. Это инъеция между равномощными множествами $\implies$ это биекция. ■

1.4 Линейный функции

Полиному Жкгалкина, в которых нету $\wedge$

$x \oplus y \quad x \oplus y \oplus 1$

Определение 13. Функция называется линейной, если её канонический полином Жегалкина не сожержит $\wedge$

Утверждение 1. Если F содержит только линейный функции, то и $\overline{F}$ содержит только линейный функции

Доказательство. $x_1 \oplus x_2 \oplus x_3$

$x_7 \oplus x_8 = (x_1 \oplus x_2 \oplus x_3) \dots$ Заменяем и получаем всё ещё сумму переменных или $\mathbb{1}$

Если формально, строим дерево, заменяем узлы на линейные фукнции, заменяем повторы, раскрываем скобки (пользуемся ассоциативностью $\oplus$) и получаем линейную функцию. ■

Утверждение 2. Если F содержит только функции, сохраняющие 0, то и $\overline{F}$ тоже

аналогично для 1

Определение 14. Функция f называется монотонной $\iff$ для двух наборов $x_1, x_2, \dots, x_n \quad y_1, y_2, \dots, y_n$, что $x_i \leqslant y_i \qquad 0 < 1$

$$f(x_1, x_2, \dots, x_n) \leqslant f(y_1, y_2, \dots, y_n).$$

Утверждение 3. Из монотонных функций не выразить немонотонную

Доказательство. Доказывается индукцией по дереву разбора. Увеличили аргумента, увеличился уровень выше, выше и корень тоже ■

Определение 15. Функция f называется самодвойственная, если

$f(x_1, \dots, x_n) = \neg f(\neg x_1, \dots, \neg x_n)$

Утверждение 4. Из самодвойственных функций тоже не выйти. Тоже деревом разборп

Классы Поста:

1. F_0 – сохраняющие 0
2. F_1 – сохраняющее 1
3. F_l – линейные
4. F_m – монотонные
5. F_s – самодвойственные

Лемма 3. $F \subseteq F_i, i \in \{0,1,l,m,s\} \implies \overline{F} \subseteq F_i$

Следствие 1. $\overline{F}$ – не полно

Теорема 4 (критерий Поста)**.** F – полное $\iff$ $F \not\subseteq F_i$ для всех $i \in \{0,1,l,m,s\}$

Доказательство. $\implies$ Если нет, то все функции лежат внутри этого класса. Не будет включена $\uparrow$ например, не лежащая ни в одном классе Поста

$\impliedby$ $f_0 \notin F_0, f_1 \notin F_1, f_l \notin F_l, f_m \notin F_m, f_s \notin F_s$

$a(x) f_0(x, x, \ldots, x)$

$a(0) = 1$

a $a(1) = 1 \implies a(x) = 1$

b $a(1) = 0 \implies a(x) = \neg x$

$b(x) = f_1(x, x, \ldots, x) \quad b(1) = 0$

1. $b(1) = 0 \implies b(x) = \mathbb{0}$
2. $b(1) = 1 \implies b(x) = \neg x$

1a $\mathbb{1}\ \mathbb{0}$

1b $\mathbb{0}, \neg$

2a $\mathbb{1}, \neg$

2b $\neg, x$

1a $\mathbb{1}, \mathbb{0}$ $f_m(x_1, \ldots, x_n) > f_m(y_1, \ldots, y_n)$ $x_i \leqslant y_i$ Значит первое – 1, а второе – 9

$f_m(x_1, \ldots, x_n)$
$f_m(y_1, \ldots, x_n)$
$f_m(y_1, \ldots, x_n)$
$\vdots$
$f_m(y_1, \ldots, y_n)$

В какой-то момент единица сменилась нулём на соседних строках

$f(y_1, \ldots, y_{i-1}, x_i, \ldots, x_n) = 1$

$f(y_1, \ldots, y_{i-1}, y_i, \ldots, x_n) = 0$

$x_i \leqslant y_i \quad x_i \neq y_i \implies x_i = 0, y_i = 1$

$c(z) = f_m(y_1, \dots y_{i-1}, z, x_{i+1}, \dots, x_n)$ здесь вместо x и y подставлены константы

$c(z) = \neg z$

2b $f_s \quad x_1, x_2, \dots, x_n : f_s(x_1, x_2, \dots, x_n) = \neg f(\neg x_1, \dots, \neg x_n) = t$

$$d(z) = f_s(z^{x_1}, z^{x_2}, \dots, z^{x_n}) \quad x^y = \begin{cases} x & , y = 1 \\ \neg x & , y = 0 \end{cases}$$

$d(0) = t, d(1) = t$

$$\begin{cases} t = 1 \implies d(t) = \mathbb{1} \\ t = 0 \implies d(t) = \mathbb{0} \end{cases}$$

Итак мы получили $\mathbb{1}, \mathbb{0}, \neg$

Воспользуемся нелинейной функцией: f_l среди нелинейных членов в полиноме Жегалкина выберем тот, в котором меньше всего переменных. Не умаляя общности скажем, что он выглядит как $xyu_1 \dots u_k \quad k + 2 \geqslant 2$

$h(x, y) = f_l(x, y, \mathbb{1}, \mathbb{1}, \dots, \mathbb{1}i, \mathbb{0}, \mathbb{0}, \dots \mathbb{0})$ Вместо u_k подставляем $\mathbb{1}$, а вместо остальных $\mathbb{0}$

$h(x, y) = xy[\oplus x][\oplus y][\oplus \mathbb{1}]$ – восемь вариантов.

Если есть $\oplus 1$, напишем $\neg$

$xy[\oplus x][\oplus y]$

$xy = x \wedge y$

$xy \oplus x \oplus y = x \vee y$

$xy \oplus x \quad h(x, \neg y) = x(y \oplus 1) \oplus x = xy$

$xy \oplus y \quad h(\neg x, y) = (x \oplus 1)y \oplus y = xy$ ■

1.5 Преобразование Мёбиуса

$f(x_1, x_2, \dots, x_n) = x \vee y / x / y / 1$

$a_{xy}xy \oplus a_x x \oplus a_y y \oplus a_1$

$$f(x_1, x_2, \dots, x_n) = \bigoplus_{\vec{s} \in \mathbb{B}^n} a_s \prod_{i : s(i) = 1} x_i = \bigoplus_{\vec{s} \leqslant \vec{x}} a_{\vec{s}}$$

$s(i) = 1 \implies x(i) = 1 \iff s \& x = s \iff s \leqslant x$ (покомпонентно)

Определение 16 (Доминирование)**.** $\vec{a} \leqslant \vec{b} \iff \forall i \quad a_i \leqslant b_i$

Таблица истинности:

0	0	0	...	$f_{00\ldots0}$
0	0	...	1	$f_{00\ldots1}$
1	1	...	1	$f_{11\ldots1}$

$f \in \mathbb{B}^{2^n}$

$\vec{a} = M\vec{f} \quad \vec{f} = M\vec{a}$

$M_{xs} = [s \leqslant x]$

Преобразование Мёбиуса – матрица $M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$

Теорема 5. Преобразование матрицы – инволюция ($M = M^{-1}$)

$\vec{a}_t = \bigoplus\limits_{x \leqslant t} f_x$

Доказательство. $\bigoplus\limits_{x \leqslant t} f_x = \bigoplus\limits_{x \leqslant t} \bigoplus\limits_{s \leqslant x} a_s = \bigoplus\limits_{s,x:s \leqslant x \leqslant t} a_s = \bigoplus\limits_{S} [(\#x : s \leqslant x \leqslant t) \% 2] a_s = a_t$

1. $s \not\leqslant t \implies \#x = 0$
2. $s = t \implies \#x = 1, s = x = t$
3. $s \leqslant t_1 \quad s \neq ts$ – нечётное число раз ксориться. z различных разрядов, $z \leqslant 1 \quad 2^z$

■

Пример. $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$ $a_{11} = 1, a_{01} = 0, a_{10} = 0, a_{00} = 1$

$xy \oplus 1$ – штрих Шефера

1.6 Схемы из функциональных элементов (Boolean Circuts)

Определение 17. Топологической сортировкой называется отображение $\varphi : V \to \{1, \ldots, n\} \quad u \neq v \implies \varphi(u) \neq \varphi(v) \quad uv \in E \implies \varphi(u) < \varphi(v)$

Теорема 6. Ациклический ориентированный граф имеет топологическую сортировку.

Лемма 4. Если G ациклический граф, то существует вершина, из которой не выходит рёбер

Доказательство леммы. Возьмём вершину: если

■

Доказательство теоремы. $n = 1$ дадим единственной вершине номер 1

$n > 1$ возьмём вершину из которой нет рёбер , дадим ей номер n и удалим её из графа. Граф от этого не стал иметь циклов, поэтому по индукционному предположению мы можем занумеровать оставшиеся $n-1$ элементов ■

Вершины, в которых нет рёбер называются $x_1, x_2, \ldots, x_n$. Дальше идут внутренние вершины, обозначаемые функциями. Например, если обозначена $\wedge$, то в неё входит два ребра. Если некоммутативная функция, то указывается порядок. Исходящая степень может быть любой. Завершает всё вершина выхода

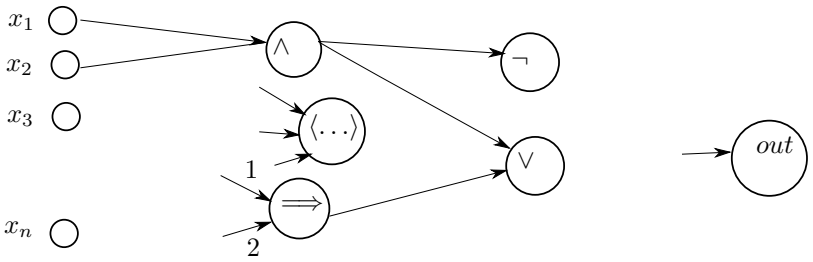

Рис. 1.1: sceme

$x \oplus y = (x \wedge \neg y) \vee (\neg x \wedge y)$

Дерево разбора легко превращается в схему.

Теорема 7. Не существует формулы $len(\phi) = \widetilde{O}(n)$ для $\oplus_n$ в $\{\wedge, \vee, \neg\}$

В схеме мы можем пересипользовать то, что в формуле пришлось бы повторять.

B – базис

Теорема 8. Функцию f можно задать формулой в базе $B \iff f$ можно представить схемой

Определение 18. Сложностью функции f в базисе B $size_B(f) =$ min число функциональных элементов в схеме.

Определение 19. Глубина схемы определяется рекурсивно: глубина входов – 0, глубина вершины – максимум из глубины входящих + 1

$\text{depth}_B(f)$ – минимальная глубина схемы для функции.

Теорема 9. B_1, B_2 – базисы.

$\exists c \quad \forall f \quad size_{B_1}(f) \leqslant c \cdot size_{B_2}(f)$

Доказательство. $B_2 = \{b_1, b_2, \ldots, b_n\}$

b_i выразим через B_1

$C \leqslant \max\limits_{b_i \in B_2} size_{B_1}(b_i)$

(оптимальная схема может быть лучше, поэтому $\leqslant$) ■

Теорема 10. То же самое про глубину

Следствие 2. $size(f)$ без базиса – асимптотическое поведение не зависящее от базиса (по теоремам при переходе к другому базису всё отличается в константу)

Следствие 3. $c_1 size_{B_2}(f) \leqslant size_{B_1}(f) \leqslant c_2 size_{B_2}(f)$

Размер функции с точностью до константы не зависит от базиса

1.7 Конкретные схемы для логических операций

Числа храниться в виде двоичного кода. Занумеруем в двух числах биты: $x_0, \ldots, x_n, y_0, \ldots, y_n$

Побитовое И – n элементов $\wedge$ принимающие соответствующие разряды.

$z_0 = x_0 \wedge y_0 \ldots z_n = x_n \wedge y_n$

Размер схемы: n глубина: 1 $size = n \quad depth = 1$

Побитовое ИЛИ – так же. Любая побитовая операция – так же.

Арифметические операции – не так же. Биты начинают зависеть друг от друга.

Сложение двух битов: заведём два выходных бита: $low = a \oplus b \quad high = a \wedge b$. Такая схема называется неполным сумматором. Неполным, потому что из него не собрать сумматор для целых чисел. Для второго бита понадобиться сложить биты чисел и ещё бит переноса. Но сумма трёх битов, к счастью, все ещё помещается в два бита $1 + 1 + 1 = 3 = 11_2$

$a, b, c \quad low = \oplus_3 (a, b, c) \quad high = med_3 (a, b, c)$ – полный сумматор. Первому биту на перенос подаётся $\mathbb{0}$, а для остальных будут складываться соответствующие биты и перенос с предыдущих битов. Другое название – линейный сумматор.

$size = n \quad depth = n$

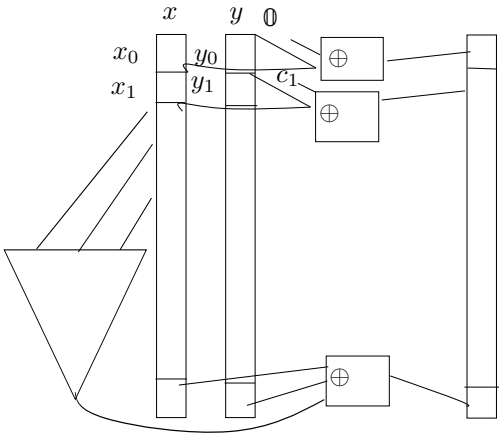

Рис. 1.2: sum

0	0	$\mathbb{0}$	k (kill)
0	1	x	p (propogate)
1	0	x	p
1	1	$\mathbb{1}$	g (generate)

1\ 2	k	g	p
k	k	g	k
g	k	g	g
p	k	g	p

$a(bc) = (ab)c = abc$ – композиция ассоциативна!

Схема композиции: принимает четыре значения, выдаёт два. Имеет константную глубину.

(Дальше жесть, которую я не могу нарисовать, но суть в том, что раз оно ассоциативное, то мы можем запилить двоичное дерево и делать всё за радостный логарифм.)

$size = O(n)$ $depth = O(\log n)$ – Двоичный каскадный сумматор. Лучше сделать нельзя.

$-y = (\sim y) + 1$ отрицательные числа храняться как дополнение $+1$

$x - y = x + (\ y) + 1$. Отрицание y сделать легко, но как добавить ещё 1? Но у нас есть нулевой перенос в нулевой разряд. Давайте сделаем его $c_0 = 1$

			1	0	1	1
			1	1	0	1
			1	0	1	1
		0	0	0	0	
	1	0	1	1		
1	0	1	1			

Умножать двоичные числа в стлбик просто. Схема даже имеет название Матричный умножитель

Дерево Уоллиса: Во-первых превратим сумму трёх чисел в сумму двух. Для трёх чисел поразрядно сделаем сумматор, который будет возвращать сумму и перенос побитого. Здесь мы не передаём перенос никуда. Дальше из переносов сделаем число и из сумм сделаем число. Получим два числа и нам нужно сложить уже их.