Содержание

1 План на 3 модуль (или 2 сем...)

1. Множества
2. ЧУМ
3. Исчисление высказываний
4. Исчисление предикатов
5. Теория кодирования

Почитать можно А. Х. Шеня

2 Множества

1. $x \in A$; $y \notin A$
2. Арифметика множеств: $\bigcup, \bigcap, \setminus, \triangle$
3. $\varnothing$
4. $A = \{a, b, c\}$; $B = \{d\} \bigcup A$
5. $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$

Remark 2.1.

Чисто синтаксически вот такой бред: $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ имеет смысл

X – множество: $X \neq \varnothing$. Рассмотрим $x \in X$

$Term(x)$ – проблема, потому что мы не знаем, к каким характеристикам обращаемся и вообще не понятно, что мы выбрали

Спасают аксиомы ZFC

Definition 2.1. Равномощность

A, B – равномощны $\Leftrightarrow \exists f : A \to B$ – биекция
А что с бесконечностями? Давайте возьмем функцию $f : N \to 2N$
Хотя множество четных чисел – подмножество всех, но они равномощны, т.к. f – биекция

Definition 2.2. Характеристическая функция

X – множество. Есть $\chi : X \to \{0, 1\}$, т.е. $\chi(x) = \begin{cases} 1, & x \in X \\ 0, & x \notin X \end{cases}$ – характеристическая функция

А пусть $X \subset Y$

- произведение характеристических функций X и Y – это характеристическая функция $X \bigcap Y$
- $1 - \chi(x)$ – характеристическая функция дополнения X
- $max(\chi_X(x), \chi_Y(x))$ – характеристическая функция $X \bigcup Y$

- $|X| = \sum\limits_{x \in Y} \chi_X(x)$

Example 2.1.

Возьмем 2^N; $B = \{0, 1\}$ и B^∞

Равномощны ли они? Берем $x \in 2^N$, теперь $b_i = \begin{cases} 1, & i \in x \\ 0, & i \notin x \end{cases}$

Definition 2.3. Счетное множество

X – счетное, если X равномощно N

Example 2.2.

Например, множество целых чисел счетно, т.к. $x \in Z \Rightarrow \begin{cases} 2x, & x \geq 0 \\ -2x + 1, & x < 0 \end{cases}$

Proposition 2.1.

1. X – счетно и $Y \subset X \Rightarrow Y$ или счетно, или конечно
2. X – бесконечно. Тогда $\exists Y$ – счетное: $Y \subset X$
3. $X_1, \ldots X_n \ldots$ – конечные или счетные. Тогда $\bigcup X_i$ – конечное или счетное

Доказательство:

1. X – счетно, т.е. соответствует последовательности $\{x_1, \ldots x_n \ldots\} = \xi$
   Возьмем $\xi \cdot \chi(Y)$. Т.е. что-то типа $\{0, 0 \ldots x_{i_1}, 0 \ldots x_{i_2}, 0 \ldots\}$ который равносилен $y_1, y_2, \ldots y_n \ldots = Y$
   В свою очередь эта штука либо конечна, либо счетна, т.к. счетен X
2. Просто выбираем по 1 элементу из X. Если они кончатся на каком-то шаге – X не бесконечно
3. Рисуем табличку. Берем элемент (1, 1), потом (1, 2), потом (2, 1), потом (1, 3) и так далее. То есть по диагоналям. Так переберем вообще все элементы (если не понятно, погуглите метод Кантора)

Exercise 2.1.

В качестве следствия попробуйте построить явную биекцию между множеством рациональных чисел и натуральных

Theorem 2.1.

A – бесконечно, B – нбчс, т.е. B – конечно или счетно
$A \bigcup B$ равномощно A

Доказательство:

$\exists Y \subset A$ – счетное

Y и $Y \bigcup B$ – равномощны

$A \bigcup B = (A \backslash Y) \bigcup (Y \bigcup B)$

$A = Y \bigcup (A \backslash Y)$

Биекция между Y и $Y \bigcup B$ сущесвтует, значит A и $A \bigcup B$ равномощны

Example 2.3.

$[0;1]$ и B^{∞}. Равномощны ли? Да. Последовательность единиц и нулей – это бинпоиск числа
Проблема: $0,(9) = 1,(0)$
$b_1 \dots b_k, 1, 1, 1, 1, (1)$
$(b_1 \dots b_k) + 1$
$R \bigcup [0,1] \sim B^{\infty}$ и $R \bigcup [0,1] \sim [0,1] \Rightarrow [0,1] \sim B^{\infty}$

Example 2.4.

$[0,1] \sim [0,1] \times [0,1]$
$0, a_1 a_2 \dots a_k \dots$
$0, a_1 a_3 a_5 \dots$ и $0, a_2 a_4 a_6 \dots$

Exercise 2.2.

Проблема та же, что и в прошлом примере, но число уязвимых моментов кратно больше. Почините

Theorem 2.2. Кантор-Бернштейн

$A, B;\ A_1 \subset A;\ B_1 \subset B$
$A_1 \sim B, B_1 \sim A \Rightarrow A \sim B$

Доказательство:

A имеет мощность не больше B. Существует какое-то отображение. Нужна его биективность. А где-то по пути может докажем еще и полный порядок

$f : A \to B_1$ – биекция

$g : B \to A_1$ – еще одна биекция

Заметим, что $g(f(A)) = A_2$ – биекция, более того этот процесс можно продолжить до бесконечности

То есть имеем $A \supset A_1 \supset A_2 \dots$ и $A \sim A_2 \sim A_4 \dots$ и $A_1 \sim A_3 \sim A_5 \sim \dots$

Возьмем просто много вложенных C-шек таких, что $C \to C_2 \to C_4 \dots$ и $C_1 \to C_3 \dots$ при какой-то биекции h

Как построить биекцию из C_6 в C_7? Положим $D_i = C_i \setminus C_{i+1}$. Тогда $C_0 = D_0 \bigcup D_1 \bigcup D_2 \dots$

При этом $C_1 = D_1 \bigcup D_2 \bigcup D_3 \dots$

$D_2 = C_2 \setminus C_3;\ D_0 = C_0 \setminus C_1$. Ну тогда $C_2 = D_2 \bigcup C_3$ и $C_0 = D_0 \bigcup C_1$

При этом биекция h все еще существует. Можем сопоставить $D_{2k} \to D_{2(k+1)}$, а $D_{2k+1} \to D_{2k+1}$, т.е. построить биекцию между C_0 и C_1. Победа

Явная биекция: $q(x) = \begin{cases} x, x \in D_{2i+1} \\ h(x), x \in D_{2i} \end{cases}$

Theorem 2.3. Теорема Кантора

B^{inf} – не счетно

Доказательство:

Построили последовательность типа

1. $a_1, a_2 \dots$
2. $b_1, b_2 \dots$
3. $c_1, c_2 \dots$

Ну возьмем еще одну последовательность $a_1, b_2, c_3 \dots$ – она будет отличаться от всех предыдущих как минимум в одном элементе. Значит B^{inf} не счетно

Theorem 2.4. Обобщенная теорема Кантора

$\forall X,\ X \not\sim 2^X$

Доказательство:

Пусть $\exists \varphi : X \to 2^X$ – биекция

$Z = \{x | x \notin \varphi(x)\}$

$Z \subset X$

$\nexists z : \varphi(z) = Z \Rightarrow z \notin Z \Rightarrow z \in Z$

Theorem 2.5. Следствие

$|2^X| > |X|$
$\mathbb{N}, 2^{\mathbb{N}}, 2^{2^{\mathbb{N}}}, \dots$
$\aleph_0, \aleph_1, \dots$

Remark 2.2.

Почему не существует множества всех множеств?
Пусть существует и называется U
Посмотрим на U и 2^U
По Кантору-Бернштейну $U \sim 2^U$, но по теореме Кантора $|U| < |2^U|$????

Theorem 2.6.

A и B – множества
$|A \cup B| = |A| + |B| - |A \cap B|$ при $|A|, |B| < +\infty$
Если же $|A| = +\infty$, а $|B| < +\infty$, то $|A \cup B| = |A|$
Что если $|A| = +\infty$ и $|B| = +\infty$? Скажем, НУО $|A| \leq |B|$, тогда $|A \cup B| = |B|$

Remark 2.3.

Вообще мы умеем еще и $|A \times B|$, но там разница будет только в конечных множествах

Есть так же и возведение в степень. С нбчс работа очевидна, а вот с не нбчс уже не так просто
Что такое $|A|^{|B|}$? Такое описать нормально не получится

Definition 2.4.

Нечто абстрактное и «умозрительное» – $\aleph$
Так, например, $\aleph + n = \aleph$ и $\aleph \cdot n = \aleph$

Definition 2.5. $\geq$

X – множество
«$\geq$» $\subset X \times X$

1. $\forall x \in X \Rightarrow x \geq x$
2. $\forall x, y, z : x \geq y,\ y \geq z \Rightarrow x \geq z$
3. $\forall x, y : x \neq y,\ x \geq y \Rightarrow \overline{y \geq x}$

$\tilde{3}$ $\forall x, y \in X : x \geq y,\ y \geq x \Rightarrow x = y$

Theorem 2.7. Порядок

Заведем отношение $\geq$. Если оно существует для всех пар множества, то это порядок, иначе – частичный порядок
Заметим, что он нестрогий. Для строгого нужно добавить проверку на равенство

Definition 2.6. Частично упорядоченное множество

$(X, \geq_X)$ – ЧУМ

Example 2.5.

Взяли $\mathbb{N}$ и степенной порядок, т.е.

$$a, b \in \mathbb{N};\ \exists x \in N\ (x > 1)\ : \begin{cases} a = x^k \\ b = x^m \end{cases}$$

$a \geq b \Leftrightarrow k \geq m$

Definition 2.7. Индуцированный порядок

Рассмотрим $Y \subset X$. Если пользоваться тем же отношением порядка на $Y \times Y$, то можно смотреть на $\geq_Y = (\geq_X) \cap (Y \times Y)$ – индуцированный порядок

Remark 2.4.

Можно и на $X \times Y$ ввести $\geq_{X \times Y}$: $(x, y) \geq (a, b) \Leftrightarrow \left[\begin{array}{l} x \geq a \\ \begin{cases} x < a \\ y \geq b \end{cases} \end{array}\right.$

Такой порядок называется лексикографическим (покоординатным), что в целом то же, что и $(X, \geq_X) + (Y, \geq_Y)$

Definition 2.8. Наибольший и максимальный элемент

$x \in X$ – наибольший элемент $\Leftrightarrow \forall y \in X : y < x$
$x \in X$. Если $\nexists y \in X : y > x$, то x – максимальный элемент

Remark 2.5.

Наибольший элемент – всегда максимальный, но не наоборот

Definition 2.9. Изоморфизм

$(X, \geq_X) \sim (Y, \geq_Y)$ – изоморфизм, если $\exists f : X \to Y$ – биекция, сохраняющая порядок

Что можно сказать про $(\mathbb{R}, \geq_{\mathbb{R}})$? Можно построить биекцию $x \mapsto x + 1$ – это автоморфизм

А что с $\mathbb{R}_+, \geq_{\mathbb{R}_+}$? Тут уже не получится построить автоморфизм (т.к. из луча $(0, +\infty)$ уйдем в луч $(1, +\infty)$)

Remark 2.6.

Из существования биекции не следует существование автоморфизма
Берем X, Y; $h : X \to Y$ – биекция
И $\forall x, y \in X : x \geq y \Rightarrow h(x) \geq h(y)$
Смотрим на $\mathbb{Z}, \mathbb{Q}$. Пусть $\exists h : \mathbb{Z} \to \mathbb{Q}$
Рассмотрим двойку и тройку
$\nexists x \in \mathbb{Z} : 2 < x < 3$
$h(2) = y_2$; $h(3) = y_3$
$h^{-1}(\frac{y_2+y_3}{2}) = x$
Целого числа между 2 и 3 нет, но по биекции оно есть

Definition 2.10. Плотность

x – плотная точка, если
$\begin{cases} \forall y < x \ \exists z : y < z < x \\ \forall y > x \ \exists z : x < z < y \end{cases}$

Example 2.6.

Возьмем множество $\{0, \frac{1}{2}, \frac{1}{3}, \dots \frac{1}{n} \dots\}$. В нем плотная точка – только 0

Theorem 2.8.

X – всюду плотное (нет соседних элементов), счетное, без наибольшего и наименьшего элемента
Это значит, что $X \cong \mathbb{Q}$

Доказательство:

Возьмем n точек из X и n точек из $\mathbb{Q}$. Построим между ними изоморфизм

Теперь нам нужен изоморфизм из $n+1$ отрезков из X в $n+1$ отрезок множества $\mathbb{Q}$. Далее идем рекурсивно

Получим для точки что-то типа системы стягивающихся отрезков

Exercise 2.3.

Попробуйте придумать явный изоморфизм между $\mathbb{Q}$ и $\mathbb{Q} \cap (0, 1)$

Remark 2.7.

$x \to x + 1$ – автоморфизм $\mathbb{Z}$
$h(\mathbb{N}) \neq \mathbb{N}$
Пусть есть изоморфизм $g(\mathbb{Z}) \to \mathbb{N}$
Применим прошлую функцию и получим $h(g(\mathbb{Z})) \to h(\mathbb{N})$
Но $g(h(\mathbb{Z})) = g(\mathbb{Z}) = \mathbb{N}$, а $h(\mathbb{N}) \neq \mathbb{N}$

Notation 2.1.

$\forall m < n;\ A(m)$ – истина $\Rightarrow A(n)$ (если $A(0)$)

Theorem 2.9.

X – ЧУМ

1. $\forall Y \subset X;\ \exists \min Y$
2. $\nexists x_1, x_2 \dots x_n \dots : x_1 > x_2 > x_3 > \dots > x_n \dots$
3. Для X работает принцип индукции

Remark 2.8.

Переформулируем 3 пункт: A – какое-то произвольное свойство, тогда
$(\forall x (\forall y (y < x) \Rightarrow A(y)) \Rightarrow A(x)) \Rightarrow \forall x\ A(x)$

Доказательство:

$2 \Rightarrow 1$ Пусть $\exists Y$: в Y нет минимального элемента
Рассмотрим $X_1 \in Y \Rightarrow \exists x_2 < x_1 \Rightarrow \exists x_3 < x_2 \dots$

$1 \Rightarrow 2$ очев

$1 \Rightarrow 3$ Пусть $Y \neq \varnothing;\ \forall y \in Y\ \overline{A}(y)$
$X \setminus Y = A(x)$

$\exists y_0 = \min Y \Rightarrow \forall x < y_0\ A(x)$
Тут что-то было

$3 \Rightarrow 1$ Пусть $\exists Y : \nexists \min Y$
$A(x) \sim x \notin Y$
Смотрим на какой-то $x \in Y$. $\forall y < x\ A(y)$
Дословно: если для какого-то x выполнялось бы условие выше, то x был минимальным, а минимального нет, значит x нет

Notation 2.2. Необоснованная индукция

Это примеры, когда индукцию мы использовали, но что-то не так

1. Графы
2. Китайская теорема об остатках

Что не так? На самом деле, например, в КТО мы опирались не на $\mathbb{N}$, а на $\mathbb{N} \times \mathbb{N}$. Надо доказать, что оно фундированное, тогда использование индукции обосновано

Доказательство:

$$\langle a_1, b_1\rangle < \langle a_2, b_2\rangle \Leftrightarrow \left[\begin{array}{l} a_1 < a_2 \\ \begin{cases} a_1 = a_2 \\ b_1 < b_2 \end{cases} \end{array}\right.$$

Рассмотрим $A \subset X$

$A_1 := \{a | \langle a, b\rangle \in A\}$

$A_1 \subset \mathbb{N} \Rightarrow \exists a_1$ – наименьший элемент A_1

$B_1 := \{b | \langle a_1, b\rangle \in A\}$

$B_1 \subset \mathbb{N} \Rightarrow \exists b_1$ – наименьший элемент B_1

Иными словами, в A есть элемент $\langle a_1, b_1\rangle$. Про него мы знаем, что все остальные элементы из A либо больше его по первой координате, либо равны с ним по первой и больше по второй

Значит $\langle a_1, b_1\rangle$ – наименьший, а тогда A – фундированное

Remark 2.9.

Это работает для $\mathbb{N}^k\ \forall k \in \mathbb{N}$

Theorem 2.10.

А что с $\mathbb{N} + \mathbb{N}$?
Возьмем их как $x_1 \dots x_n \dots$ и $y_1 \dots y_n \dots$. Далее $\forall x_i\ \forall y_i\ x_i < y_i$
Давайте докажем, что это множество тоже фундированное

Доказательство:

Пусть $\exists a_1 \dots a_n \dots \in \mathbb{N} + \mathbb{N} : a_1 > a_2 > \dots > a_n > \dots$

Возьмем $b_1 \dots b_n \dots \in \mathbb{N}_1$

$\langle a_1 \dots a_n \dots\rangle \setminus \langle b_1 \dots b_n \dots\rangle$ – бесконечное количество

Example 2.7. Где используется?

Например, если хотим две разных индукции про одно и то же множество

Definition 2.11. Упорядоченное множество

X – фундированное, ρ – линейный порядок
(X, ρ) – (вполне) упорядоченное множество, а ρ в таком случае – полный порядок

Theorem 2.11. Свойства

1. $\forall x \in X\ \exists y \in X : y > x$ и $\nexists z : y > z > x$
2. Если $A \subset X$ и A ограниченное, то у него есть наибольший элемент (супремум достижим)
   А правда ли это? Смотрите попытку доказать

Доказательство:

1. На уровне очев
2. $\forall A \subset X : A$ – ограничено
   $\exists u = \sup A$
   $\exists a = \min\{x | x > A\}$
   А потом оказалось, что вообще нет. Возьмем $\mathbb{N} + \mathbb{N}$. Ноль второго подмножество будет больше любого элемента первого, но недостижим в нем

Exercise 2.4.

Построить вполне упорядоченное множество для рациональных чисел (нужен порядок, гарантирующий фундированность)

Начнем обозначать элементы какого-то множества как $0, 1, 2\dots$. Получили отображение на натуральный ряд. Если множество конечно, то процесс оборвется, иначе получим в точности натуральный ряд

Более того, можем вполне делать $\omega_1, \omega_1 + 1, \omega_1 + 2\dots$. А можем еще и $\omega_2, \omega_2 + 1, \omega_2 + 2\dots$

Definition 2.12. Начальный отрезок

A – вполне упорядоченное множество
Пусть $A = B \sqcup C$. При этом $\forall b \in B\ \forall c \in C\ b < c$
Тогда B – начальный отрезок A

Notation 2.3. Свойства:

1. Начальный отрезок – вполне упорядоченное множество
2. Начальный отрезок начального отрезка – начальный отрезок
3. Если рассмотрим $\{B | B$ – начальный отрезок $A\}$, то это множество упорядочено по включению

Definition 2.13. Трансфинитная индукция

У нас есть индукция с шагом $n \to n+1$, что в целом равносильно рекурсивному доказательству вида $A_{n+1} \leftarrow A_n$ + замкнуть какой-то базой
А что если попытаться сделать $A_x \leftarrow A_{[0,x_1]};\ x_1 < x$?
Индукция, которую получим из такой рекурсии будет трансфинитной

Theorem 2.12. Теорема Цермело

На любом множестве можно ввести такое отношение порядка, что множество станет вполне упорядоченным

Remark 2.10.

Доказывается она как эквивалентная аксиоме выбора

3 Логика и исчисление высказываний

Definition 3.1. Высказывание

Любому высказыванию можем сопоставить ровно один элемент из множества $\{T, F\} =: B$ – истина или ложь

A	B	$A \vee B$	$A \wedge B$
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

Definition 3.2. Пропозициональная формула

A – пропозициональная формула

1. x_i – пропозициональная переменная $\Rightarrow A$ – пропозициональная формула
2. A – пропозициональная формула $\Rightarrow \overline{A}$ – пропозициональная формула
3. A, B – пропозициональные формулы $\Rightarrow (A \vee B), (A \wedge B), (A \to B), (A \Leftrightarrow B)$ – пропозициональные формулы

Definition 3.3. Тавтология

Формула, которая истинна при любых значениях переменных

Example 3.1.

$A \vee \overline{A}$

Remark 3.1.

Все хорошо только если A – пропозициональная переменная. Если это формула, то нужно аккуратно доказывать тавтологичность
Попробуем доказать

Доказательство:

$A = \overline{B}$

Получили $\overline{B} \vee \overline{\overline{B}}$. Попали в рекурсию

$x_1 \dots x_n$ – переменные на B

$f : B^n \to B$

$f(x_1 \dots x_n)$

Definition 3.4. Полный набор связок

Набор связок называется полным, если с его помощью можно выразить любую функцию

Example 3.2.

Система связок $\{\wedge, \vee\}$ – неполная, т.к. нет способа получить $f(0 \dots 0) \mapsto 1$

Lemma 3.1. Лемма об однообразности разбора

$\forall A$ – пропозициональная формула : A – не пропозициональная переменная

$$\exists! \text{ представление в виде } \left[\begin{array}{c} B \vee C \\ B \wedge C \\ B \to C \\ \overline{B} \end{array}\right.$$

Definition 3.5. Скобочный итог

$c_1 \dots c_k$

Скобочный итог$(i) = N_{\text{откр}}(i) - N_{\text{закр}}(i)$

Definition 3.6. Полная система связок

Система связок в пропозициональных формулах называется полной, если с ее помощью можно выразить любую пропозициональную формулу

$x_1 \dots x_n$ – переменные

$f(0 \dots 0) = f_1$

$f(0 \dots 01) = f_2$

$f(1 \dots 1) = f_{2^n}$

$(\overline{x_1} \wedge \overline{x_2} \wedge \dots \wedge \overline{x_n})$ – истинно только если подставили все нули

$(\overline{x_1} \wedge \overline{x_2} \wedge \dots \wedge x_n)$ – истинно только если подставили все нули, кроме последнего

Делаем так вплоть до $(x_1 \dots x_n)$

Теперь скажем, что берем n-ую скобку только если f_n – истина. Объединяем все через $\vee$

Definition 3.7. КНФ

Можем $\begin{pmatrix} x_1 & \dots & x_k & f \\ 0 & \dots & 0 & f_1 \\ 0 & \dots & 1 & f_2 \\ \dots & \dots & \dots & \dots \\ 1 & \dots & 1 & f_{2^n} \end{pmatrix}$

Если $f_i = 1$, то берем $x_1 \wedge x_2 \wedge \overline{x_3} \dots \wedge x_k$ (если $x_i = 0$, то берем $\overline{x_i}$)

Делаем $\bigvee$ по всем i таким, что $f_i = 1$

Это конъюнктивная нормальная форма

Definition 3.8. Моном

$\bigwedge x_i$ – моном

Definition 3.9. Полином Жегалкина

Если сделаем моном на $\oplus$, то получим полином Жегалкина

Theorem 3.1.

Любую булеву функцию можно представить в виде полинома Жегалкина

Доказательство:

$\overline{A} = A \oplus 1$

$A \vee B = A \oplus B \oplus (A \wedge B)$

$A \wedge B = AB$ – это можно честно перемножить

Theorem 3.2. Критерий Поста

Система связок полна $\Leftrightarrow$ она не входит ни в один из 5 классов:

1. Монотонные функции
   Есть функция f, она монотонная, если
   $a_1 \dots a_k \geq b_1 \dots b_k \Leftrightarrow f(a_1 \dots a_k) \geq f(b_1 \dots b_k)$
2. Функции, сохраняющие 0
3. Функции, сохраняющие 1
4. Линейные функции
5. Самодвойственные функции
   $f(\overline{x_1} \dots \overline{x_k}) = \overline{f(x_1 \dots x_k)}$

Доказательство:

f – не сохраняет 0

$f(0 \dots 0) = 1$

$f(1 \dots 1) = \left[\begin{array}{l} 0 \\ 1 \end{array}\right.$

g – не сохраняет 1

$g(0 \dots 0) = \left[\begin{array}{l} 0 \\ 1 \end{array}\right.$

$g(1\dots1) = 1$
$h(1, 0\dots0) = 0$
$h(0, 0\dots0) = 1$
То есть даже из двух констант умеем получать отрицание
$P(x_1 \dots x_k)$ – нелинейная
НУО $P(x_1 \dots x_k) = x_1x_2A(x_3 \dots x_k) \oplus x_1B(x_3 \dots x_k) \oplus x_2C(x_3 \dots x_k) \oplus D(x_3 \dots x_k)$
Зафиксируем набор $\alpha = x_3 \dots x_k : A(\alpha) = 1$

$$P(x_1, x_2, \alpha) = \begin{cases} x_1x_2 \\ x_1x_2 \oplus x_1 \\ x_1x_2 \oplus x_2 \\ x_1x_2 \oplus x_1 \oplus x_2 \\ x_1x_2 \oplus 1 \\ x_1x_1 \oplus x_1 \oplus 1 \\ x_1x_2 \oplus x_2 \oplus 1 \\ x_1x_2 \oplus x_1 \oplus x_2 \oplus 1 \end{cases}$$

А тут уже есть и $\wedge$, и $\vee$, значит есть полная система связок, значит доказали

Definition 3.10.

$C_b(f)$ – минимальный размер схемы элементов из B для вычисления f

Remark 3.2.

$\exists\lambda$
$C_{B_1}(f) \leq \lambda C_{B_2}(f)$
$C_{B_2}(f) \leq \lambda C_{B_1}(f)$

Notation 3.1.

$X = x_1 \dots x_k$
$Y = y_1 \dots y_k$ (НУО равны, иначе к меньше в начало докидаем нули)
Хотим функцию Compare. Какого она может быть размера?

Theorem 3.3. Список аксиом

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $(A \wedge B) \to A$
4. $(A \wedge B) \to B$
5. $A \to (B \to (A \wedge B))$
6. $A \to (A \vee B)$
7. $B \to (A \vee B)$
8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
9. $\neg A \to \overline{A}$
10. $(A \to B) \to ((A \to \neg B) \to \neg A)$
11. $A \vee \neg A$

Remark 3.3.

К этому набору аксиом (являющихся тавтологиями) добавим правило вывода – modus ponens. Таким образом получим всю теорию исчисления высказываний

Theorem 3.4. Теорема о корректности исчисления высказываний

Любая теорема является тавтологией

Доказательство:

Для доказательства нужно доказать, что это все действительно тавтологии + доказать правило вывода

Exercise 3.1.

Доказать, что все это тавтологии

Theorem 3.5. Теорема о полноте исчисления высказываний

Любая тавтология является теоремой исчисления высказываний

Lemma 3.2.

D – некоторая формула $\Rightarrow (D \to D)$ – теорема

Definition 3.11. Вывод

Γ – некоторое множество формул
Вывод из Γ – конечная последовательность формул, все они

1. Аксиомы
2. Элементы Γ
3. Получены из предыдущих по правилу вывода

Definition 3.12. Выводимость

$\Gamma \vdash A$ – A выводима из Γ, т.е. является в ней последней формулой
Если $\Gamma = \varnothing$, то пишут просто $\vdash A$

Lemma 3.3. Лемма о дедукции

$\Gamma \vdash A \to B \Leftrightarrow \Gamma \cup \{A\} \vdash B$

Доказательство:

$\Rightarrow$ $\Gamma \cup \{A\} \vdash A \to B$
$\Gamma \cup \{A\} \vdash A$. Тогда по MP $\Gamma \cup \{A\} \vdash B$