Математическая логика и теория алгоритмов

Посов Илья Александрович

запись конспекта: Блюдин Андрей и Хаматов Вадим

Содержание

1 Математическая логика

1.1 Исчисление высказываний

1.1.1 Основные понятия

Определение. Логическая функция — это множество из 2 элементов. Также, логической функцией называют множество логических значений

$B = \{0, 1\}$, где 0 — это ложь (false), а 1 — это истина (true)

Определение. Логическая функция от n переменных

$$f : B^n \to B$$

Замечание. Часто логические функции вводят как перечисление возможных аргументов и значений функции при этих аргументах

Пример. Введем функцию $f(x, y)$

x	y	f(x,y)
0	0	0
0	1	1
1	0	1
1	1	1

Таблица 1: Таблица истинности для $f(x, y)$

Эту же функцию можно задать функцией $f(x, y) = max(x, y)$

Утверждение. *Функция от n переменных может быть $f(x_1, x_2, x_3, \dots, x_n)$*

При этом количество всех возможных наборов аргументов равняется 2^n, а количество всех возможных функций при всех возможных наборах аргументов равняется 2^{2^n}

Следствие. *Посчитаем количество таких функкий для разных n*

$n = 1$ $\quad 2^2 = 4$ *функций* $f(x)$

$n = 2$ $\quad 2^{2^2} = 16$ *функций* $f(x, y)$

$n = 3$ $\quad 2^{2^3} = 2^8 = 256$ *функций* $f(x, y, z)$

x_1	x_2	...	x_n	f$(x_1, x_2, \ldots, x_n)$
0	0	...	0	0 или 1
...	...	...	...	0 или 1
1	1	...	1	0 или 1

Таблица 2: Таблица истинности для $f(x_1, x_2, \ldots, x_n)$

1.1.2 Функции от 1 переменной (их определения)

Пример. Перечислим все возможные функции от 1 переменной

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1

Данные функции имеют значение:
$f_1(x) = 0$ — функция 0
$f_2(x) = x$ — функция x
$f_3(x) =!x, \bar{x}, \neg x$, not x — функция отрицания (не x)
$f_4(x) = 1$ — функция 1

1.1.3 Функции от 2 переменных (их определения)

Пример. Перечислим все возможные функции от 2 переменных

x	y	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_7(x)$	$f_8(x)$
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

Таблица 3: Таблица истинности для $f(x, y)$

Продолжение:

Перечислим основные значения функций:

$f_2(x, y)$ — это конъюнкция или "лочическое и"или логическое умножение $(xy, x\&y, x \wedge y)$

$f_7(x, y)$ — это исключающее или $(x+y, xXORy, x \oplus y)$, также данную функцию можно ассоциировать как $(x + y)mod2$

$f_8(x, y)$ — это логическое или, но ее можно также записать как $max(x, y)$ $(x|y, x \vee y)$

$f_{10}(x, y)$ — это эквивалентность $(x \Leftrightarrow y, x \equiv y, x == y)$

x	y	$f_9(x)$	$f_{10}(x)$	$f_{11}(x)$	$f_{12}(x)$	$f_{13}(x)$	$f_{14}(x)$	$f_{15}(x)$	$f_{16}(x)$
0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

Таблица 4: Таблица истинности для $f(x, y)$

$f_{14}(x, y)$ — это импликация ($x \Rightarrow y, x \rightarrow y$)
Импликация работает так, что истина следует из чего угодно:
лешия не существует $\Rightarrow$ русалок не существует $= 1$ ($1 \Rightarrow 1 = 1$)
допса скучная $\Rightarrow$ русалок не существует $= 1$ ($0 \Rightarrow 1 = 1$)
русалки существуют $\Rightarrow$ драконы существуют $= 1$ ($0 \Rightarrow 0 = 1$)
x $\Rightarrow$ y = 0 только если x = 1, а y = 0
$f_{12}(x, y)$ — это обратная импликация ($x \Leftarrow y = y \Rightarrow x$)
$f_9(x, y)$ — стрелка Пирса ($x \downarrow y = \overline{x \vee y}$)
$f_{15}(x, y)$ — штрих Шеффера ($x|y = \overline{xy}$)
$f_3(x, y)$ — запрет по y ($x > y = \overline{x \Rightarrow y}$)
$f_1(x, y)$ — 0
$f_4(x, y)$ — x
$f_5(x, y)$ — запрет по x ($x < y = \overline{x \Leftarrow y}$)
$f_6(x, y)$ — y
$f_{11}(x, y)$ — не y ($\neg y$)
$f_{13}(x, y)$ — не x ($\neg x$)
$f_{16}(x, y)$ — 1

Определение. Логические выражения — способ задания логических функций с помощью переменных, цифр 0 или 1 и операций:
$\cdot \quad \vee \quad \Rightarrow \quad \Leftrightarrow \quad + \quad \equiv \quad | \quad \downarrow \quad < \quad >$

Пример. Примеры логических выражений:
$(x \vee y) =$
$(x \Rightarrow yz) \vee (y \equiv z)$
$(0 \Rightarrow x) \vee (1 \Rightarrow y)$

Определение. Значения логического выражения можно записать **Таблицей истинности**

Пример. $f(x, y, z) = (x \vee y)z$

Замечание. Порядок строчек в таблеце истинности может быть любым, но лучше использовать как у двоичных чисел

Утверждение. *Таблицы истинности часто считают постепенно*

x	y	z	f(x,y,z)
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

x	y	z	$x \vee y$	$(x \vee y)z$
...	...	...	...	...
...	...	...	...	...

1.1.4 Приоритеты операций

$$\neg$$

$$\cdot$$

$$\vee$$

$$+ \quad \equiv$$

$$\Rightarrow \quad \Leftarrow$$

$$| \quad \downarrow \quad < \quad >$$

Пример. Примеры приоритетов операций:
$\neg x \vee y = (\neg x) \vee y$
$x \vee yz = x \vee (yz)$
$x \Rightarrow y \vee z = x \Rightarrow (y \vee z)$

1.1.5 Алгебраические преобразования логических выражений

Определение. Алгебраические преобразования логических выражений — изменяем выражения по правилам, обычно в сторону упрощения

Пример. $(0 \Rightarrow x) \vee (1 \Rightarrow y) = 1 \vee (1 \Rightarrow y) = 1$

Утверждение 1.

$$\overline{\overline{x}} = x$$

Доказательство:

x	$\overline{x}$	$\overline{\overline{x}}$
0	1	0
1	0	1

Утверждение 2. *При* $\vee$*:*

$$1 \vee x = 1$$

$$0 \vee x = x$$

$$x \vee y = y \vee x$$

1.1.6 Таблица эквивалентных логических выражений

Утверждение. $x \vee y = y \vee x$ - *симметричность*

$x \vee 0 = x$
$x \vee 1 = 1$
$x \vee x = x$
$x \vee \overline{x} = 1$

Доказательство:

x	$\overline{x}$	$x \vee \overline{x}$
0	1	$0 \vee 1 = 1$
1	0	$1 \vee 0 = 1$

$xy = yx$
$x * 0 = 0$
$x * 1 = x$
$x * x = x$
$x * \overline{x} = 0$
$x + y = y + x$
$x + 0 = x$
$x + 1 = \overline{x}$
$x + x = 0$
$x + \overline{x} = 1$

Утверждение. $x \vee (y \vee z) = (x \vee y) \vee z$ - *ассоциативность*

Ассоциативность означает,что порядок скобок не важен

Пример. $x \Rightarrow y \neq y \Rightarrow x$ - не симметричная функция

Доказательство:

x y	$x \Rightarrow y$	$y \Rightarrow x$
0 0	1	1
0 1	1	0
1 0	0	1
1 1	1	1

Замечание. $x \Rightarrow y \neq y \Rightarrow x$

$x \Rightarrow 0 = \overline{x}$
$0 \Rightarrow x = 1$

Доказательство:

x	$x \Rightarrow 0$
0	$0 \Rightarrow 0 = 1$
1	$1 \Rightarrow 0 = 0$

$x \Rightarrow 1 = 1$
$1 \Rightarrow x = x$
$x \Rightarrow x = 1$
$x \Rightarrow \overline{x} = \overline{x}$
$\overline{x} \Rightarrow x = x$
$\overline{x} \Rightarrow y \Rightarrow z$ *договоримся, что это* $x \Rightarrow y(y \Rightarrow z) \neq (x \Rightarrow y) \Rightarrow z$
$x \Leftrightarrow y = y \Leftrightarrow x$
$x \Leftrightarrow 0 = \overline{x}$
$x \Leftrightarrow 1 = x$
$x \Leftrightarrow x = 1$
$x \Leftrightarrow \overline{x} = 0$
$x \Leftrightarrow (y \Leftrightarrow z) = (x \Leftrightarrow y) \Leftrightarrow z$ - *ассоциативно*

Утверждение. *Дистрибутивность*

$(x \vee y)z = xz \vee yz$
$(x + y)z = xz + yz$ *по таблице истинности*

x y z	$x \Rightarrow y$	$y \Rightarrow z$	$x \Rightarrow (y \Rightarrow z)$	$(x \Rightarrow y) \Rightarrow z$
0 0 0	1	1	1	0
0 0 1	1	1	1	1
0 1 0	1	0	1	0
0 1 1	1	1	1	1
1 0 0	0	1	1	1
1 0 1	0	1	1	1
1 1 0	1	0	0	0
1 1 1	1	1	1	1

$(x\&y) \vee z$ *(*$xy \vee z = (x \vee z)(y \vee z)$
$(x \vee y)\&z = (x\&z) \vee (y\&z)$
$(x\&y) \vee z = (x \vee z)\&(y \vee z)$

Замечание. $(x_1 \vee x_2 \vee x_3)(y_1 \vee y_2) = (x_1 \vee x_2 \vee x_3)y_1 \vee (x_1 \vee x_2 \vee x_3)y_2 = x_1y_1 \vee x_2y_1 \vee x_3y_1 \vee x_1y_2 \vee x_2y_2 \vee x_3y_2$

$xy \vee z = (x \vee z)(y \vee z) = xy \vee xz \vee zy \vee zz = xy \vee xz \vee zy \vee z = xy \vee xz \vee zy \vee z * 1 = xy \vee z(x \vee y \vee 1) = xy \vee z$ сошлось

$x + y = \overline{x \Rightarrow} y$ *- смотри Таблицу истинности*
$(x \Rightarrow y)(y \Rightarrow x) = x \Rightarrow y$

1.1.7 Многочлены Жегалкина

Замечание. Одну и ту же функцию можно записать по разному.

В алгебре: $f(x) = 1 + x = x + 1 = x + 5 - 4 = sin(x - x) + x = ...$
В логике: $f(x, y) = x \vee y = x \vee y \vee 0 = (x \vee y)(\overline{y} \vee y = x\overline{y} \vee y$ *(= - дистрибутивность)*

Многочлены Жегалкина для логической формулы

Определение. $f(x_1......x_n)$ - это многочлен с переменными xi, конспектами 0,1 и со степенями переменных $\leqslant 1$. Это многочлены от xi $\mathbf{Z_2}$

Пример. $f(x, y, z) = 1 + x + yz + xyz$
$1 + x$ $\quad$ $xy + xyz$
$1 + xy$

Не многочлены
$1 + x + (y \vee z)$
$1 + x + z^2$ *нельзя степень 2*

Замечание. В общем случае многочлен от 1 переменной ($a_i = 0$ или 1)
$a_0 + a_1x$

от 2ух: $a_0 + a_1x + a2y + a3xy$

от 3ех: $a_0 + a_1x + a_2y + a_3z + a_4xy + a_5xz + a_6yz + a_7xyz$

В общем случае $f(x1....x_n)$ $a_0 + a_1x_1 + ... + a_nx_n + ax_1x_2 + ax_1x_3$ + ... (все пары переменных) + $ax_1x_2x_3$ + $ax_1x_3x_2$ ←все тройки перменных+$ax_1x_2x_3...x_n$

Определение. $\forall f(x_1...x_n)$ - логические функция $\exists!$ многочлен Жегалкина $g(x_1...x_n) : f = g$

Замечание. Всего 4 функции от 1ой переменной

$f(x) = 0 = \overline{x} = 0 + 0x$

$f(x) = 1 = 1 = 1 + 0x$

$f(x) = x = x = 0 + 1x$

$f(x) = \overline{x} = 1 + x = 1 + 1x$

Доказательство:

Определение. Разные многочлены - это разные логические функции т.е. $f(x_1...x_n = a_0 + ... + a_1x_1...x_n$

$g(x_1...x_n) = b_0 + ... + bx_1...x_n$

$\exists! : a_i \neq b_i$ различающийся

Доказательство:

Возьмем индекс с самым большик количеством переменных

$f(x, y, z) = 1 + x + xy + xyz = ... + 1x + Dy + Dz + 1xy$

$g(x, y, z) = 1 + y + z + xyz... + Dx + 1y + 1z$

для переменных этого слагаемого подставим 1 0xy

для остальных переменных : 0

[В примере $x = 1, y = 0, z = 0 : f(1, 0, 0)$ и $g(1, 0, 0)$]

и в f и в g все другие слагаемые равны 0

Теперь f(...) и g(...)

$f(...) = a_ix1x_2x_3 \neq b_ix_1x_2x_3 \Rightarrow f(x_1...x_n) \neq y$

Доказательство:

Проверим, что многочленов Жегалкина столько, сколько функций:

Посчитаем

$a_0 + a_1x_1 + ... + a_1x_1x_2...x_n$

Сколько слагаемых:

1) 1 слагаемых без переменных

n слагаемых с переменной

$a_1x_1 + ... + a_nx_n$

C_n^2 - слагаемых с 2 - мя переменными

C_n^3 - слагаемых с 3 - мя переменными

C_n^n - слагаемых с n переменными

Всего : $C_n^0 + C_n^1 + C_n^2 + ...C_n^n = 2^n((1 + 1)^2)$

Пример. $a_0 + a_1 x$ - 2 слагаемых

$a_0 + a_1 x + a_2 y + a_3 xy - 2^2 = 4$ слагаемых

2) Все слагаемых имею вид: $x_1, x_2, x_3 ... x_n$ (0 или 1) - 2^n слагаемых

Итого: многочлен Жегалкина от n переменных

Задача. Сколько разных многочленов?

Это столько же, сколько логический функций

Итог:

Следствие: Любая логическая функция может быть представлена в виде многочлена Жегалкина

Пример. $f(x,y) = x \vee y$

$f(x,y) = x * y$ - уже многочлен Жегалкина

Метод неопределенных коэффициентов:

Подберем $x \vee y = a_0 + a_1 x + a_2 y + a_3 xy$

$f(0,0) = 0$

$f(0,0) = a_0 + a_1 * 0 + a_2 * 0 + a_3 ...$

$f(1,0) = 1 \vee 0 = 1$

$f(1,0) = a_0 + a_1 = a_1$ $(a_0 = 0, \Rightarrow a_1 = 1$

$f(0,1) =$ аналогично $\Rightarrow a_1 = 1$

$f(x,y) = x + y + a_3 xy$

$f(1,1) = 1 \vee 1 = 1$

$f(1,1) = 1 + 1 + a_3 = 0 + a_3 = a_3$, $a_3 = 1$

Ответ: $x \vee y = x + y + xy$

Многочлены Жегалкина от 1 переменной:

$f(x)$	Мн Ж
0	0
1	1
x	x
$\bar{x}$	$1 + x$

Многочлены Жегалкина от 2 переменных:

$f(x)$	Мн Ж
0	0
1	1
xy	xy
$x + y$	$x + y$
$x \vee y$	$x + y + xy$

Формулы:

1. $\overline{xy} = \neg(xy) = \overline{x} \vee \overline{y}$

2. $\overline{x \vee y} = \neg(x \vee y) = \overline{x} \cdot \overline{y} = \overline{x}\,\overline{y}$

Замечание. $\overline{xy} \neq \overline{x} \cdot \overline{y} = \overline{x}\,\overline{y}$

Доказательство формул через таблицу истинности:

x	y	$\overline{x \vee y}$	$\overline{x} \cdot \overline{y}$
0	0	1	1
0	1	0	0
1	0	0	0
1	1	0	0

1.1.8 Получение многочлена Жегалкина через алгебраические упрощения

1. **Многочлен Жегалкина для** $\vee$

   $x \vee y = (x = \overline{a}, y = \overline{y}) = \overline{ab} = \overline{\overline{x} \cdot \overline{y}} = \overline{(1+x)(1+y)} = 1 + (1+x)(1+y) = 1 + 1 + x + y + xy = \underline{x + y + xy}$

2. **Многочлен Жегалкина для** $\Leftrightarrow$

   $x \Leftrightarrow y = \overline{x + y} = \underline{1 + x + y}$

3. **Многочлен Жегалкина для** $\Rightarrow$

   $x \Rightarrow y = \overline{x} \vee y = (1+x) \vee y = (1+x) + y + (1+x)y = 1 + x + y + y + xy = \underline{1 + x + xy}$

Замечание. Если есть логическая формула, то ее можно приветси к форме многочлена Жегалкина двумя способами:

1. метод неопределенных коэффициентов:

   $a_0 + a_1x + a_2y + a_3z + \cdots + axyz$

2. метод алгебраических преобразований

Пример. $x \vee y = \overline{\overline{x} \cdot \overline{y}} = \cdots = x + y + xy$

Пример. $x \Rightarrow y = \overline{x} \vee y = \cdots = 1 + x + xy$

Пример. $x \Rightarrow (y \vee \overline{z}) = x \Rightarrow (y + \overline{z} + y \cdot \overline{z}) = x \Rightarrow (y + (1+z) + y \cdot (1+z)) = x \Rightarrow (y + 1 + z + y + yz) = x \Rightarrow (1 + z + yz) = 1 + x + x(1 + z + yz) = 1 + x + x + xz + xyz = 1 + xz + xyz$

Поймем, что: $(x \Leftrightarrow y) \Leftrightarrow z = x \Leftrightarrow (y \Leftrightarrow z)$
$x \Leftrightarrow y \Leftrightarrow z = (1{+}x{+}y) \Leftrightarrow z = 1{+}(1{+}x{+}y){+}z = 1{+}1{+}x{+}y{+}z = x{+}y{+}z$
Вывод:
Заранее не ясно, сложно ли привести логическую формулу к многочлену Жегалкина

1.1.9 Дизъюнктивно-нормальная форма (ДНФ)

Определение. Литерал — это переменная или отрицание переменной

Пример. $x, \overline{x}, y, \overline{y}, z, \overline{z}$

Определение. Конъюнктор — конъюнкция литералов

Пример. $x\overline{y}, xyz, \overline{x}\,\overline{y}\,\overline{z}, \overline{x}z$, ноль (пустой конъюнкт).

Определение. Логическое выражение имеет ДНФ, если она является дизъюнкцией конъюнкторов

Пример. $x\overline{y} \vee \overline{x}\,\overline{z} \vee z \vee \overline{x}\,\overline{y}$ — ДНФ

Пример. $xy \vee \overline{x}\,\overline{y}$ — ДНФ

Пример. $x \vee y$ — ДНФ

Пример. xy — ДНФ

Пример. не ДНФ — $\overline{xy} = \overline{x} \vee \overline{y}$ — ДНФ

Пример. не ДНФ — $x \Rightarrow yz = \overline{x} \vee yz$ — ДНФ

Построение ДНФ по таблице истинности функции:
алгоритм на примере трех переменных

x	y	z	$f(x,y,z)$	
0	0	0	0	
0	0	1	0	
0	1	0	1	$\overline{x}\,y\,\overline{z}$
0	1	1	1	$\overline{x}\,yz$
1	0	0	0	
1	0	1	0	
1	1	0	1	$xy\,\overline{z}$
1	1	1	0	

Берем строки из столбца $f(x,y,z)$, где значения в столбце равны 1

Допустим есть строка: $x = a_1, y = a_2, z = a_3$ (a могут быть как 0, так и 1)

В ответ добавляется конъюнкт xyz ($0 \Rightarrow$ отрицание, $1 \Rightarrow$ не отрицание)

Ответ: $f(x, y, z) = \overline{x}\, y\, \overline{z} \vee \overline{x}\, yz \vee xy\, \overline{z}$

Доказательство корректности алгоритма:

Когда полученный ДНФ $= 1$?

Когда есть конъюнкт равный 1

1. Если первый конъюнкт равняется 1 (в примере $\overline{x}\, y\, \overline{z} = 1$)

   $\Rightarrow$ все литералы конъюнкта равняются 1

   $\Rightarrow$ в примере $\overline{x} = 1 \quad y = 1 \quad \overline{z} = 1$

   $x = 0 \quad y = 1 \quad z = 0$

2. Если второй конъюнкт равняется 1

   $\Rightarrow$ в примере $x = 0 \quad y = 1 \quad z = 1$ — строка из таблицы истинности

3. То же самое с третьим конъюнктом

Посмотрим таблицу с этими конъюнктами:

x	y	z	$\overline{x}\, y\, \overline{z}$	$\overline{x}\, yz$	$xy\, \overline{z}$	$f(x, y, z)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	1	0	0	1
0	1	1	0	1	0	1
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	1	1
1	1	1	0	0	0	0

Замечание. У одной функции могут быть разные ДНФ

Пример. $\underline{\overline{x}\, y\, \overline{z} \vee \overline{x}\, yz \vee xy\, \overline{z}} = \overline{x}\, y(\overline{z} \vee z) \vee xy\, \overline{z} = \underline{\overline{x}\, y \vee xy\, \overline{z}}$ — подчеркнутые выражения являются ДНФ

Пример. $\underline{\overline{x}\, y\, \overline{z} \vee \overline{x}\, yz \vee xy\, \overline{z}} = \overline{z}\ y(\overline{x} \vee x) \vee zy\ \overline{x} = \underline{\overline{z}\, y \vee zy\, \overline{x}} = \underline{y\, \overline{z} \vee \overline{x}\, yz \vee \overline{x}\, x \vee z\, \overline{z}}$ — подчеркнутые выражения являются ДНФ

Получить ДНФ для логической функции/формулы можно:

1. по таблице истинности

2. с помощью алгебраических преобразований

Пример. 1. $\overline{x} = \overline{x}$

2. $x \vee y = x \vee y$

3. $x \cdot y = x \cdot y$

4. $x \Rightarrow y = \overline{x} \vee y$

5. $x \Leftrightarrow y = (x \Rightarrow y)(y \Rightarrow x) = (\overline{x} \vee y)(\overline{y} \vee x) = \overline{x}\overline{y} \vee \overline{x}x \vee y\overline{y} \vee yx = \overline{x}\overline{y} \vee xy$

x	y	$x \Leftrightarrow y$
0	0	1
0	1	0
1	0	0
1	1	1

6. $x + y = \overline{x \Leftrightarrow y} = \overline{\overline{x}\,\overline{y} \vee xy} \ldots$
   $= \overline{\overline{x}\,y} \vee \overline{x \vee \overline{y}} = \overline{\overline{x}} \cdot \overline{y} \vee \overline{x} \cdot \overline{\overline{y}} = x\,\overline{y} \vee \overline{x}\,y$

7. $x \Rightarrow (y + z) = \overline{x} \vee (y + z) = \overline{x} \vee \overline{y}\,z \vee y\,\overline{z}$

1.1.10 Задача (не) выполнимости

Дана логическая формала в ДНФ

Проверить, бывает ли она равна 0?

$\overline{x}\,\overline{y} \vee x \vee y? = 0$

$x = 0, y = 0 \Rightarrow \overline{x}\,\overline{y} = 1$

$\Rightarrow$ данный ДНФ не может быть равным 0

Эта задача обладает особенностью:

1. если знать значения переменных (ответ), то их легко можно быстро проверить

2. подобрать значения переменных для 0 — нет

Нет известного алгоритма, который "принципиально"быстрее полного перебора

У этой задачи класс NP выполнимости (ответ легко проверить, а найти его простым способом невозможно)

Следствие. *То к чему сводится задача (не) выполнимости тоже сложна*

1. *упростить логическое выражение*

2. *поиск минимального ДНФ*

1.1.11 Запись таблиц истинности в виде графика

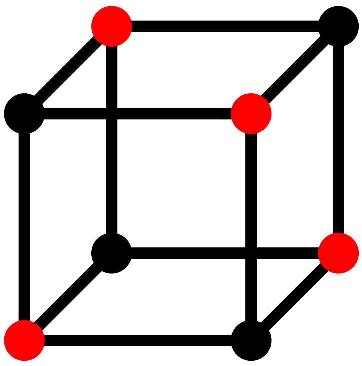
Формула $= f(x, y, z) = x + y$

$$f(0,0) = 0$$

$$f(0,1) = 1$$

$$f(1,0) = 1$$

$$f(1,1) = 0$$



1.1.12 Задача минимизации ДНФ

Данная задача тоже является сложной, также как и задача (не) выполнимости

Дана логическая функция (в виде ДНФ). Необходимо найти самую короткую ДНФ эквивалентную данной.

Минимальной ДНФ считается та, где меньше количество литералов и дизъюнкций

Пример. $\overline{x}\,\overline{y} \vee z$ короче, чем $xy \vee yz$

Замечание. Далее рассматриваться все будет для функции от 3 переменных $f(x, y, z)$

Замечание. Какова таблица истинности $xyz = abc$, где $a = 0$ или $1, b = 0$ и $1, c = 0$ или 1

$0 \Rightarrow$ надо поставить отрицание

$1 \Rightarrow$ нет отрицания

Пример. $f(x, y, z) = \overline{x}\, y\, \overline{z}$

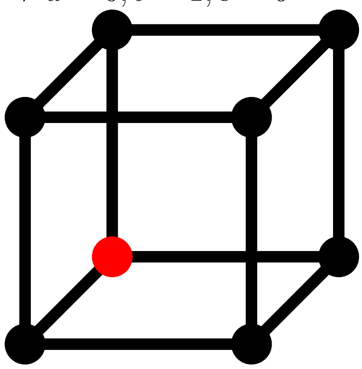
Если $\overline{x}\, y\, \overline{z} = 1$

$\Rightarrow \overline{x} = 1, y = 1, \overline{z} = 1$

$\Rightarrow x = 0, y = 1, z = 0$

$\Rightarrow x = a, y = b, z = c$

$\Rightarrow a = 0, b = 1, c = 0$



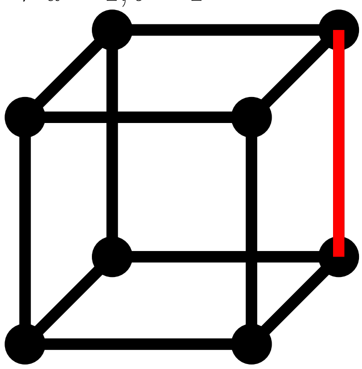
Пример. $f(x, y, z) = xy$

Если $xy = 1$

$\Rightarrow x = 1, y = 1$

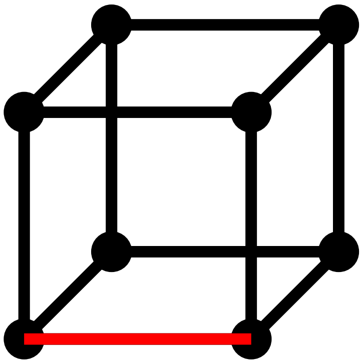
$\Rightarrow x = a, y = b$

$\Rightarrow a = 1, b = 1$



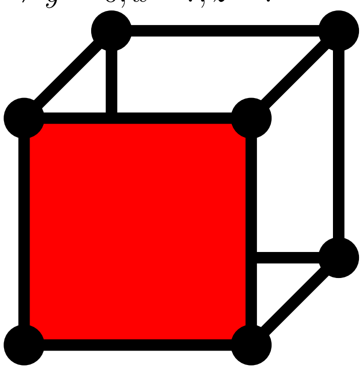
Аналогично, $f(x, y, z) = \overline{y}\, \overline{z}$

ребро: $y = 0, z = 0, x = ?$ — не важно

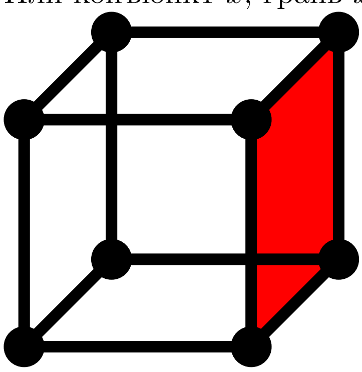


Последнее — конъюнкт из 1 литерала:
$x, \overline{x}, y, \overline{y}, z, \overline{z}$

Пример. $f(x, y, z) = \overline{y}$
Если $\overline{y} = 1$
$\Rightarrow y = 0, x = ?, z = ?$



Или конъюнкт x, грань $x = 1$

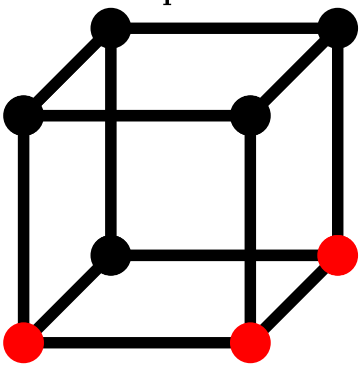


Итого:
xyz — это вершина $x = a, y = b, z = c$
xy — это ребро $x = a, y = b$
x — это грань $x = a$
Попробуем минимизировать ДНФ

Пример. $\overline{x}\,\overline{y}\,\overline{z} \vee x\,\overline{y}\,\overline{z} \vee xy\,\overline{z}$

Найти самый короткий ДНФ для данного выражения

Шаг 1: строим ТИ

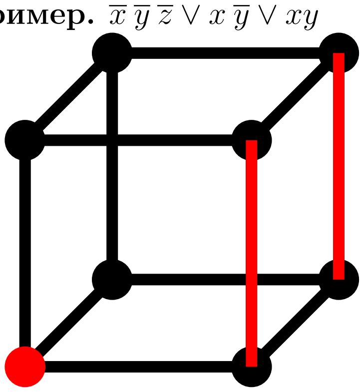


$\overline{x}\,\overline{y}\,\overline{z} = (0,0,0)$
$x\,\overline{y}\,\overline{z} = (1,0,0)$
$xy\,\overline{z} = (1,1,0)$

Шаг 2: упрощаем

Чтобы упростить имеет смысл рассмотреть 2 ребра:
$(0,0,0) - -(1,0,0) = \overline{y}\,\overline{z}$
$(1,0,0) - -(1,1,0) = x\,\overline{z}$
$\Rightarrow$ ДНФ $= \overline{y}\,\overline{z} \vee x\,\overline{z} = \overline{x}\,\overline{y}\,\overline{z} \vee x\,\overline{z} = xy\,\overline{z} \vee \overline{y}\,\overline{z}$
$\Rightarrow$ самое короткое ДНФ $= \overline{y}\,\overline{z} \vee x\,\overline{z}$

Пример. $\overline{x}\,\overline{y}\,\overline{z} \vee x\,\overline{y} \vee xy$



$\Rightarrow$ ДНФ $= x \vee \overline{x}\,\overline{y}\,\overline{z} = x \vee \overline{y}\,\overline{z}$

Замечание. Данный метод позволяет наглядно перебрать все ДНФ и найти минимальный

С помощью алгебраических преобразований мы не сможем понять, что ответ самый оптимальный

Пример. Алгебраические преобразования

$\overline{x}\,\overline{y}\,\overline{z} \vee x\,\overline{y}\,\overline{z} \vee xy\,\overline{z} = \overline{x}\,\overline{y}\,\overline{z} \vee x\,\overline{y}\,\overline{z} \vee x\,\overline{y}\,\overline{z} \vee xy\,\overline{z} = \overline{y}\,\overline{z} \vee x\,\overline{z}$

Но тут непонятно, а вдруг можно сделать еще короче

1.1.13 Двойственная функция

Пусть есть логическая функция: $f = B^n \to B = \{0, 1\}$

Двойственная функция: $f^* = B^n \to B = \{0, 1\}$

$f^*(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}$

Замечание. Мир замены лжи на истину

$$0 \leftrightarrow 1$$

Пример. $f(x, y) = x \vee y$

x	y	f
0	0	0
0	1	1
1	0	1
1	1	1

Новый мир: $1 \to 0, 0 \to 1$

x	y	f^*
1	1	1
1	0	0
0	1	0
0	0	0

Получилось, что $(x \vee y)^* = xy$

Пример. $(x \vee y)^* = \overline{\overline{x} \vee \overline{y}} = \overline{\overline{x}}\,\overline{\overline{y}} = xy$

Пример. $(x + y)^* = \overline{\overline{x} + \overline{y}} = \overline{1 + x + 1 + y} = 1 + x + 1 + y + 1 = 1 + x + y = x \Leftrightarrow y$

Замечание. $f^{**}(x_1, x_2 \ldots x_n) = \overline{f^*(\overline{x_1}, \overline{x_2} \ldots \overline{x_n})} = \overline{\overline{f(x_1, x_2 \ldots x_n)}} = f(x_1, x_2 \ldots x_n)$

Следствие.

$$(xy)^* = x \vee y$$

$$(x \Leftrightarrow y)^* = x + y$$

Теорема о композиции:

$f = f_0(f_1(x_1, \dots x_n), f_2(x_1, \dots x_n), \dots f_m(x_1, \dots x_n))$

f_i — это функции от n переменных $(B^n \to B)(i = 1 \dots n)$

$f_0 = B^m \to B$

Тогда $f^*(x_1, \dots x_n) = f_0^*(f_1^*(x_1, \dots x_n), f_2^*(x_1, \dots x_n), \dots f_m^*(x_1, \dots x_n))$

Доказательство:

$f^* = \overline{f(\overline{x_1}, \dots \overline{x_n})} = \overline{f_0(f_1(\overline{x_1}, \dots \overline{x_n}), f_2(\overline{x_1}, \dots \overline{x_n}) \dots f_m(\overline{x_1}, \dots \overline{x_n}))} = f_0^*(\overline{f_1(\overline{x_1}, \dots \overline{x_n})}, \overline{f_2(\overline{x_1}, \dots \overline{x_n})}, \dots \overline{f_m(\overline{x_1}, \dots \overline{x_n})})$

Следствие. *Если есть $f(x_1, \dots x_n)$ — записано, как логическое выражение с $\cdot$, $\vee$, $\neg$, $+$, $\Leftrightarrow$, то f^* — также выражение, но связки заменяются на двойственные узлы*

$$\vee \leftrightarrow *$$

$$+ \leftrightarrow \Leftrightarrow$$

$$\neg \leftrightarrow \neg$$

так как $(\overline{x})^* = \overline{x}$

Пример.

$$f(x, y, z) = \overline{x \vee \overline{y}\, z} \Leftrightarrow (x + y + z)$$

$$f^*(x, y, z) = (\overline{x \cdot (\overline{y}\, z)}) + (x \Leftrightarrow y \Leftrightarrow z)$$

Пример.

$$f(x_1, \dots x_n) = 1$$

$$\Rightarrow f^*(x_1, \dots x_n) = \overline{1} = 0$$

$$1^* = 0; 0^* = 1$$

1.1.14 Конъюнктивно-нормальная форма КНФ

Определение. Конъюнктивно-нормальная форма — еще одна нормальная форма, похожая на ДНФ

Определение. Литерал — это как и раньше, переменные или отрицательные переменные

$$x, y, \overline{x},\ \overline{y}$$

Определение. Дизъюнкт — дизъюнкция литералов

$$x \vee y;\ x \vee y \vee \overline{z};\ x \vee \overline{z};\ \overline{x}$$

$$\cancel{xy}, \cancel{x \vee yz}$$

Определение. КНФ — это конъюнкция нескольких дизъюнктов

$$(x \vee y)(y \vee \overline{z});$$

$$(x \vee \overline{y} \vee z)(\overline{y} \vee \overline{z})(\overline{x})$$

$$\cancel{xy \vee z}$$

$$x \vee y \vee z$$

— 1 дизъюнкт

$$xyz$$

— 3 дизъюнкта

Определение. У любой логической функции есть КНФ, её можно построить по таблице истинности

Доказательство

Заметим,что если вычислить (КНФ)* (двойственную к КНФ), то получим ДНФ

Пример. $[(x \vee y \vee z)(x \vee \bar{y})(\bar{y} \vee \bar{z})]^* = (xyz) \vee (x\bar{y}) \vee (\bar{y}\bar{z})$

И наоборот (ДНФ)* = КНФ

Итого, чтобы получить КНФ для функции f, надо построить двойственную функцию к ДНФ это функции. Отсюда следует, что КНФ всегда существует

Пример. f(x,y,z) = xy ⇔ z

Выпишем значения xyz из строчек, где $f^* = 1$

$\bar{x}\bar{y}z \quad x\bar{y}\bar{z} \quad \bar{x}y\bar{z} \quad xy\bar{z}$

x	y	z	xy	f	f^*
0	0	0	0	1	0
0	0	1	0	0	1
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	0	1	1
1	0	1	0	0	0
1	1	0	1	0	1
1	1	1	1	1	0

Вспомним определение $f^*(x,y,z) = \overline{f(\bar{x},\bar{y},\bar{z})}$
$f^*(0,0,0) = \overline{f(1,1,1)}$
Итого: $f^* = \bar{x}\bar{y}z \vee \bar{x}y\bar{z} \vee x\bar{y}\bar{z} \vee xy\bar{z}$
$f^*(0,0,1) = \overline{f(1,1,0)}$
$f^*(0,1,0) = \overline{f(1,0,1)}$
По теореме о композиции
$f = (\bar{x} \vee \bar{y} \vee z)(\bar{x} \vee y \vee \bar{z})(x \vee \bar{y} \vee \bar{z})(x \vee y \vee \bar{z})$
Получение КНФ по таблице истинности без двойственной функции
f(x,y,z) = xy $\Leftrightarrow$ z

x	y	z	$f = xy \Leftrightarrow z$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

При x y z = 1 1 0, f= xy $\Leftrightarrow$ z $\leftarrow \bar{x} \vee \bar{y} \vee z$
для 1 - отрицание, для 0 - нет отрицания
Итого: Чтобы построить ДНФ:
- строки с 1, 0 $\leftrightarrow \bar{x}\bar{y}\bar{z}$
1 $\leftrightarrow xyz$
Чтобы получить КНФ:
- строки с 0, 0 $\leftrightarrow xyz$
1 $\leftrightarrow \bar{x}\bar{y}\bar{z}$

Пример. f = x+y

x	y	$x+y$
0	0	0
0	0	1
0	1	1
0	1	0

Нули в: $x \vee y$ $\qquad \bar{x} \vee \bar{y}$

$f = (x \vee y)(\bar{x} \vee \bar{y})$

Замечание. Для функции записанной в форме КНФ, можно поставить задачу "выполнимости".

Вопрос: может ли значение быть $= 1$

- не известно решений, принципиально эффективней полного перебора значений

Пример. $(x \vee y \vee z)(x \vee \bar{y})(y \vee \bar{z})(\bar{x} \vee \bar{z}) = 1$

x = 1

y = 1 подходит

z = 0

Следовательно эта формула выполнима при таком наборе

Многие задачи, головоломки сводятся к задаче выполнимости

Пример. Прицнцип Дирихле

Если есть n клеток и в них n+1 заяц, то $\exists$ клетка, где зайцев $\geqslant 2$.

при n = 2: i = 1 или 2 (клетка) $\qquad x_{ij}$ - в клетке i сидит заяц j

j = 1 или 2 или 3 заяц

Попробуем записать, что в каждой клетке $\leqslant 1$ зайца

а) каждый заяц ровно в одной клетке

$x_{11} \oplus x_{21}$ - заяц 1

$x_{12} \oplus x_{22}$ - заяц 2

$x_{13} \oplus x_{23}$ - заяц 3

б) в каждой клетке не больше 1 зайца

кл/з	1	2	3
1	x_{11}	x_{12}	x_{13}
2	x_{21}	x_{22}	x_{23}

если есть 2 зайца, то один из конъюнктов: $= 1$

$\overline{x_{11}x_{12} \vee x_{11}x_{13} \vee x_{12}x_{13}} \longleftarrow$ в кл $1 \leqslant 1$ зайца

$\overline{x_{21}x_{22} \vee x_{21}x_{23} \vee x_{22}x_{23}} \longleftarrow$ в кл $2 \leqslant 1$ зайца

Соединяем все утверждения:

$(x_{11}+x_{21})(x_{12}+x_{22})(x_{13}+x_{23})(\overline{x_{11}x_{12} \vee x_{11}x_{13} \vee x_{12}x_{13}})(\overline{x_{21}x_{22} \vee x_{21}x_{23} \vee x_{22}x_{23}}) =$ 0 всегда из принципа Дерихле

$(x_{11} \vee x_{21})(\overline{x_{11}} \vee \overline{x_{21}})(x_{12} \vee x_{22})(\overline{x_{12}} \vee \overline{x_{22}})(x_{13} \vee x_{23})(\overline{x_{13}} \vee \overline{x_{23}})(\overline{x_{11}} \vee \overline{x_{12}})(\overline{x_{11}} \vee \overline{x_{13}})(x_{12} \vee x_{13})(\overline{x_{21}} \vee \overline{x_{22}})(\overline{x_{21}} \vee \overline{x_{23}})(\overline{x_{22}} \vee \overline{x_{23}})$

$\longleftarrow$ Берем программу, которая решает КНФ задачу выполнимости. Она скажет - невозможно.

1.1.15 Класс замкнутости

Повторим: Логическая функция: f: $\beta^n \to \beta$

$\beta = \{0, 1\}$

Определение. Класс – это множество логических функций.

Пример. $K_1 =$ класс функций: от двух переменных $K_2 =$ класс функций такой, что $f(x, y) = f(y, x)$

$f(x, y) = x \vee y \in K_1, \in K_2$

$g(x, y) = x \Rightarrow y \in K_1 \notin K_2$

K_3 : класс функций $f(x, ...) = f(\overline{x}, ...)$ функции, которые не зависят от первой переменной

$f(x, y, z) = y \Rightarrow z \in K_3$

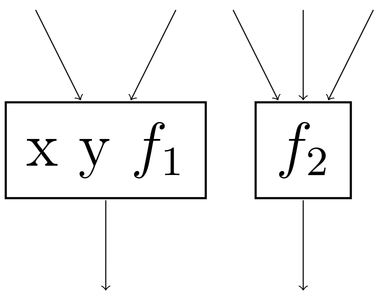
$f(x, y, z) = (x \Rightarrow y) \vee z \notin K_3$

$f(x, y, z) = x\bar{x} \vee y \vee z \in K_3 \quad (x\bar{x})$

$K_4 : \{f(x, y) = x \vee y;\ g(x, y) = x \Rightarrow y\}$

Определение. Замыкание класса

$K = \{f_1, f_2, \dots\}$ — класс функции



K^* — замыкание класса - это класс состоящий из всех композиций функций из К

$\boxed{f_1(f_2)(f_1(x, y), y, z), z)}$ — композиция

если есть функции, подставляем друг в друга, получаем композицию

Пример. : 1)$K = \{0, \bar{x}\} \quad$ (0 - f() $\bar{x} - g(x)$)

$K^* = \{f(), g(f()), g(g(f())), g(g(g(f())))\}$

Пример. $K = \{\bar{x}\}$ возьмем класс только из отрицательных
$K^* = \{\bar{x}, x\}$
$K = \{g(x), g((g(x))), g(g(g(x \dots 1, \dots)))\}$

Пример. $K^* = \{\bar{x}, x \vee y, xy\}$ $\quad K^* = \{, \dots, \forall$, функция $\}$

Определение. Если К - класс:
$K^* = \alpha$, то $\boxed{\text{К - полный}}$, где α — все логические функции
Вывод: $K = \{\bar{x}, x \vee y, xy\}$ — полный

Пример. $K = \{\bar{x}, x \vee y\}$, где $f(x) = \bar{x}$, $g(x, y) = x \vee y$

$xy = \overline{\overline{xy}} = \overline{\overline{x} \vee \overline{y}} = f(g(f(x), f(y)))$
Значит K^* — тоже полный

Определение. Замкнутый класс - К замкнут, если $K^* = K$

Свойства замыкания:
1. $K_1 \subset K_2$, тогда $K_1^* \subset K_2^*$
Доказательство:
Если есть f $\in K_1^* \Rightarrow f =$ композиция $f_1 \in K_1 \Rightarrow$ f - композиция $(f_i \in K_2) \Rightarrow f \in K_2^*$ чтд.
2.Если $K_1 \subset K_2$ и K_1 - полный, то K_2 - полный
Доказательство:
$K_1 \subset K_2 \Rightarrow K_1^* \subset K_2^* \Rightarrow \alpha \subset K_2^* \Rightarrow K_2^* = \alpha$
3. Пусть K_1, K_2 - замкнутое, тогда $K_1 \cap K_2$ - тоже замкнутые
Доказательство:
Пусть есть $f = (K_1 \cap K_2)^*$ - композиция
$f_i \in (K_1 \cap K_2)$
а) $\Rightarrow f_i$ - композиция $f_i = K_1 \Rightarrow f \in K_1^*$
б) $\Rightarrow f_i$ - композиция $f_i = K_2 \Rightarrow f \in K_2^*$
Из а и б следует, что $f \in K_1^* \cap K_2^* = K_1 \cap K_2$
Итог: $f \in (K_1 \cap K_2)^* \Rightarrow f \in K_1 \cap K_2$
$\Rightarrow (K_1 \cap K_2)^* \subset K_1 \cap K_2$, по $K_1 \cap K_2 \subset (K_1 \cap K_2)^*$
$\Rightarrow K_1 \cap K_2 = (K_1 \cap K_2)^*$
$\Rightarrow K_1 \cap K_2$ - замкнут

Замечание. K_1 и K_2 - замкнутые $\Rightarrow K_1 \cup K_2$ - замкнутый

4. $K^* = K^{**}$ для любого класса функций

1.1.16 Примеры замкнутых классов

1. T_0 - класс функций, "сохраняющих ноль"$f \in T_0 \Leftrightarrow$ если $f(0, ...0) = 0$
$x * y \in T_0$
$x + y \in T_0$
$\bar{x} \notin T_0$
$x \Rightarrow y \notin T_0$
$xy + xz + yz \in T_0$
Утверждение: T_0 - замкнут
Доказательство:
$\sqsupset f \in T_0^*$, проверим, что $f \in T_0$
$\Rightarrow T_0^* \subset T_0$
$\Rightarrow T_0^* = T$
f - комп f_i, $f_i \in T_0$
$f_1(f_2(...)f_3(f_4(...)), ...)$ - композиция
подставим все 0
$\Rightarrow f(0, ...0) = 0 \Rightarrow f \in T_0$ чтд

Пример. $f_1(x, y) = x * y \qquad f_1 \in T_0 f_2 \in T_0$
$f_2(x, y) = x + y \qquad f_1(f_2(f_1(x, f_2(y, y)), y) f_1(z, z))$
$x(y + y)$
$f(x, y, z) = (x(y + y) + y) * z * z$
$f(0, 0, 0) = 0$
2. Класс T_1 - сохраняющие 1
$f \in T_1$, если $f(1, ...1) = 1$
$x * y \in T_1$
$x + y \notin T_1$
$x + y + z \in T_1$
$\bar{x} \notin T_1$
$x \Rightarrow y \in T_1$
$xy + xz + yz \in T_1$

Утверждение. T_1 - *замкнут*

Доказательство: смотри T_0
3. Класс $\boxed{\&}$
$f \in \boxed{\&}$, если f можно записать как конъюнкцию нескольких переменных
$f(x, y, z) = yz$
$g(x, y, z) = xyz$
$h(x, y, z) = xz$
$i(x, y, z) = z$

0

1

Все это $\in \boxed{\&}$

Утверждение. *Класс* $\boxed{\&}$ *замкнут*

Композиция $f_i \in \boxed{\&}$

$f_1(..., \boxed{...}, ..., \boxed{...})$ = арг2 * арг4 = подаргумент1* подаргумент2* ... * подаргумент = пер * пер * пер * пер... (произвольная перепеременная)

пер может быть 0 или 1

Утверждение. $\boxed{\&} = \{\&, 0, 1\}^*$

по определению замыкания

$\{f_1(x, y) = x * y$

$f_2() = 0$

$f_3() = 1\}$

4. $\boxed{V}$ - дизъюнкция переменных и 0, 1

$\boxed{V} = \{V, 0, 1\}^*$

Утверждение. $\boxed{V}$ - *замкнут*

Доказательство 1:

смотри доказательство $\boxed{\&}$

Доказательство 2:

$\boxed{V} = \{V, 0, 1\}^* \Rightarrow \boxed{V}^* = \{V, 0, 1\}^{**} = \{V, 0, 1\}^* = \boxed{V}$ свойства замыкания

Доказательство: $\sqsupset f \in K^* \Rightarrow f-$ комп $f_i \Rightarrow f_i \in K^*$

$f = f_1(f_2(...)...) = g_1(g_2(h_1...)) \in k^*$

$\uparrow \quad \uparrow$ комп $g_1 \in K^*$

$g_i \in K \ h_i \in K$

$\Rightarrow f \in K^* \Rightarrow K^* = K^{**}$

Следствие: $\forall K$ - класс K^* - замкнут

если класс замкнут он станет замкнутым

5. Класс u (unit) : 0,1,$f(x, ...x_n) = x_i$ или $\overline{x_i}$

$f(x, y, z) = \bar{z}$

$f(x, y, z, t) = x$

$f(x) = xf(x) = \bar{x}$

Все это $\in u$

6. Класс 1^∞ $f(x_1...x_n) \leqslant x_i$

$0^\infty f(x...x_n) \geqslant x_i$

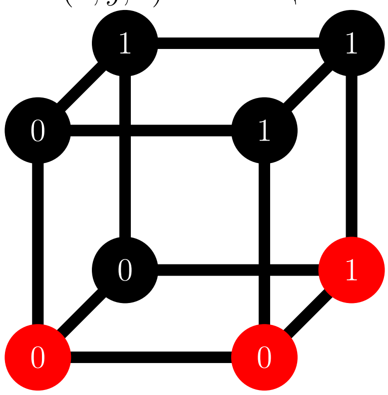
$x * y \leqslant x \qquad xy \in 1^\infty$

$\leqslant y$

$x \vee y \geqslant x \qquad x \vee y \in 0^\infty$
$\geqslant y$
$x \Rightarrow y \geqslant y \qquad x \Rightarrow y \in 0^\infty$
$x \Rightarrow y \leqslant y$
$x = 0$
$y = 0$
$x \Rightarrow y \notin 1^\infty$
7. L - линейная функция L $= \{0, 1, +\}^*$
Все функции из констант и сложения
$x + y \in L$
$x + y + z \in L$
$1 + x \in L$
$\bar{x} \in$
$x * y \in L$
(L - линейные многочлены Жегалкина, степени $\leqslant 1$)
Доказательство: $x * y$ имеет многочлены Жегалкина $x * y$
он единственный $\Rightarrow$ не существует линейного многочлена Жегалкина
8. S - самодвойственные функции
$f \in S$, если f $= f^*$ $\quad$ (f^* - двойственные)
Если функция равна своей двойственной, то она самодвойтсвенная

Пример. $x * y \notin S$
$x \vee y \notin S$
$x \in S$
$\bar{x} \in S$
$x \Rightarrow y \notin S$ т.к. $(x \Rightarrow y)^* = (\bar{x} \vee y)^* = \bar{x} * y \neq \bar{x} \vee y$
$x = 1$

Функция честного голосования $y = 1$ от 3 ёх переменных. $0 \neq 1$
$vote(x, y, z) = 1$, если 1 - иц больше $x + y + z \geq z$
0, если 0 - ей больше $x + y + z \leq 1$
$vote(x, y, z)$: Таблица истинности



$vote(x,y,z) \in S$?

$(xy \vee xz \vee yz)^* = (x \vee y)(x \vee z)(y \vee z) =?xy \vee xz \vee yz$

Раскроем скобки:

$xxy \vee xxz \vee xzy \vee xzz \vee yxy \vee yxz \vee yzy \vee yzz = xy \vee xz \vee xyz \vee xz \vee xy \vee xyz \vee yz \vee yz = xy \vee xz \vee yz \vee xyz = xy \vee xz \vee yz(1 \vee x) = xy \vee xz \vee yz$

т.е. vote $= vote^*$

или проверим таблицой истинности:

читаем снизу вверх, заменяя 0 на 1

xyz	$vote$	$vote^*$
000	0	0
001	0	0
010	0	0
011	1	1
100	0	0
101	1	1
110	1	1
111	1	1

Утверждение. *S - замкнут*

$\sqsupset f \in S^* f =$*композиция* $f_i \in S$

$f = f_i(f_2(...), f_3(...), f_4(...))$

Определение. Высота композиции

$f(x,y,z)$ - высота 1 (1 ф-ия)

$f(g(x,y),y,z)$ - высота 2

$g(x,y) - 1$

$f(g(x,y),y,z) - 2$

Пример. $f(g(h(x),y),h((h(x)),y))$

$g(h(x),y)$ - 2

$h(h(x))$ - 2

$f(g(h(x),y),h((h(x)),y))$ - 3

$f^* = f_1^*(f_2^*(...),, f_n^*(...))$ - теория о композиции

но $f_i \in S \Rightarrow f_i^* = f_i$

$= f_i(f_2(...), ...f_n(...)) = f$

т.е $f^* = f \Rightarrow f \in S$

9. Монотонные функции

$f(x_1,\dots,x_n) \in M$, если $\forall i \quad x_i \geq y_i$

$\Rightarrow f(x_1,\dots,x_n) \geq f(y_1,\dots,y_n)$

Примеры:

1. $f_1(x) = \overline{x} \qquad f_1 \notin M$, так как $f_1(1) = 0, f(0) = 1$. 1 в аргументе функции ≥ 0, но $0 < 1$ в значение функции

2. $f_2(x, y) = x \Rightarrow y \qquad f_2 \notin M$, так как $f_2(1, 0) = 0, f(0, 0) = 1$. $1, 0$ в аргументе функции $\geq 0, 0$, но $0 < 1$ в значение функции

3. $f_3(x, y) = x + y \qquad f_3 \notin M$, так как $f_3(1, 1) = 0, f(1, 0) = 1$. $1, 1$ в аргументе функции $\geq 1, 0$, но $0 < 1$ в значение функции

4. $f_4(x, y) \in M$

5. $f_5(x, y) \in M$

6. $f_6(x, y, z) = xy \vee xz \vee yz \quad \in M$ — функция голосования

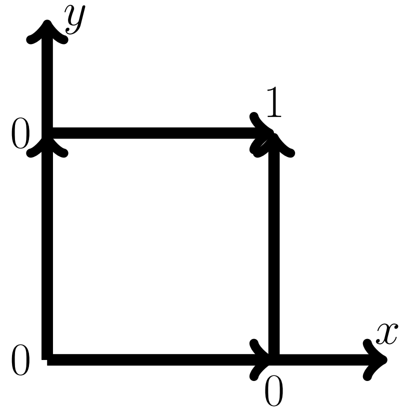
Наглядный способ проверки монотонности
Функция монотонна, когда все стрелки:

1. из 0 в 0

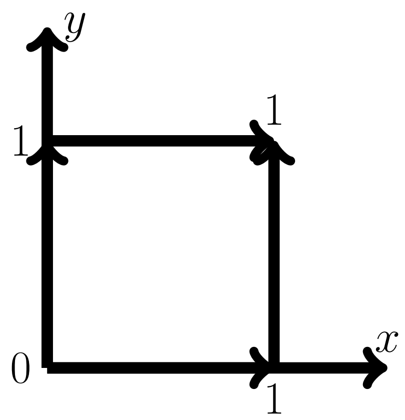
2. из 0 в 1

3. из 1 в 1

Пример. $x * y$
Данная функция монотонна



Пример. $x \vee y$
Данная функция тоже монотонна



Утверждение. M – *замкнут*

То есть если f_i – *мотонна, то* $f(x_1, \dots x_n) = f_1(f_2(\dots) \dots f_m(\dots))$

$f(y_1, \dots y_n) = f_1(f_2(\dots) \dots f_m(\dots))$

$x_1 \dots x_n \geq y_1 \dots y_n$

То где-то в глубине x_i *будут* $\geq$ y_i $\Rightarrow$ *внутри будут получаться значения функции* $f_i(x \dots) \geq f_i(y \dots)$

Замечание. Классы из примеров выше все неполные

Пример. $L = L^* \quad x \cdot y$

Всегда были примеры функций не из классов

$xy \notin L$

$xy \notin S$

$\overline{x} \notin T_0$

$\overline{x} \notin T_1$

$\overline{x} \notin M$

1.1.17 Теорема Поста

Теорема. ***Поста***

(Позволяет понять, полный класс или нет)

K – *полный тогда и только тогда, когда*

$\exists f_1 \in K : \quad f_1 \notin T_0$

$\exists f_2 \in K : \quad f_2 \notin T_1$

$\exists f_3 \in K : \quad f_3 \notin L$

$\exists f_4 \in K : \quad f_4 \notin M$

$\exists f_5 \in K : \quad f_5 \notin S$

Пример. $K = \{\overline{x}; x + y\}$

$\overline{x} \notin T_0, T_1$

но $\overline{x} \in L$ и $x + y \in L \Rightarrow$
K – не полный

Пример. $K = \{\overline{x}; x \vee y\}$
$\overline{x} \notin T_0, T_1, M$
$\overline{x} \in S, L$ но $x \vee y \notin L, S \Rightarrow$
K – полный по теореме Поста

Доказательство в одну сторону:
$\Rightarrow$ если K полный, от противного
Пусть все $f \in K$ отличие, что $f \in T_0$
$\Rightarrow K \subset T_0$
$\Rightarrow K^* \subset T_0^*$
$\Rightarrow K^* \subset T_0 \nleq \alpha$, где α – все функции
$\Rightarrow \leq \alpha$
Доказательство в другую сторону:
Будем выражать через $f_1; f_2; f_3; f_4; f_5$ все другие возможные
Достаточно будет выразить только $\{\overline{x}, x \cdot y\}$ (тогда есть $x \vee y = \overline{\overline{x} \cdot \overline{y}}$)
$\Rightarrow$ есть все ДНФ.
Шаг 1: Давайте выразим 0, 1, $\overline{x}$
Берем $f_1(x_1 \ldots x_n) = \begin{bmatrix} 1, x = 0 (f_1 \notin T_0) \\ 0 \; or \; 1; x = 1 \end{matrix} = 0$ или $\overline{x}$
$f_2(x_1, x_2 \ldots x_n) \notin T_1 = \begin{bmatrix} 0 \; or \; 1, x = 0 \\ 0; x = 1 \end{matrix} = \overline{x}$ или 0
Пояснение:
$f(x, y, z) = x \Rightarrow yz \quad f(x, x, x) = 1$
$f(0, 0, 0) = 1, f \notin T_0$
$f(x, x, x) = 1$
$0 = f_2(x_1 \ldots x_n),\ 1 = f_1(x_1, \ldots x_n)$
$0 = f_2(x_1, \ldots x_n), \overline{x} = f_1(x_1, \ldots x_n), 1 = \overline{0} = f_1(f_2(x_1, \ldots x_n), f_2(x_1, \ldots x_n), \ldots)$
$1 = f_2(x_1, \ldots x_n),\ \overline{x} = f_1(x_1, \ldots x_n),\ f_2(f_1(x_1, \ldots x_n), f_1(x_1, \ldots x_n), \ldots)$
$\overline{x} = f_2(x_1, \ldots x_n),\ \overline{x} = f_1(x_1, \ldots x_n)$
Берем $f_4 \notin M$, где нарушена монотонность, для примера:
$f_4(x_1 = y_1, x_2 = y_2, \ldots, x_n > y_n) = 0_x \neq 1_y$
$f_4(x_1, x_2, \ldots x_n)$ переменная X, где $>$
$f_4(x, y, z, t) = xy + zt \notin M$
$f_4(1, 1, 1, 1) = 0 \quad f_4(1, 0, 1, 1) = 1$
$1, 1, 1, 1 \geq 1, 0, 1, 1$
$\Rightarrow f_4(1, x, 1, 1) = \begin{bmatrix} 1, x = 0 \\ 0; x = 1 \end{matrix} = \overline{x}$

выражены $f_1(x_1, x_2 \dots x_n) = \overline{x} \quad f_2(x_1, x_2, \dots x_n) = \overline{x}$
$f_5 \notin S$
получим с ней 1 и 0
Найдем нарушение S
$\underline{f^*(x_1 \dots x_n)} \neq f(x_1 \dots x_n)$
$f(\overline{x_1}, \dots \overline{x_n}) \neq f(x_1, \dots x_n)$
$f(\overline{x_1}, \overline{x_2}, \dots \overline{x_n}) = f(x_1, \dots x_n)$
Рассмотрим $f_5(x; \overline{x}; x; \dots \overline{x}) =$
(если $x_i = 0 \Rightarrow x \quad x_i = 1 \Rightarrow \overline{x}$)

$$= \left[\begin{array}{l} f(x_1, x_2 \dots x_n)\, when\, x = 0 \\ f(\overline{x_1}, \dots \overline{x_n})\, when\, x = 1 \end{array}\right. = 0 \text{ или } 1$$

Пример. $f(x, y, z) = x \vee yz \notin S$
нужно найти $f(1,0,0) = f(0,1,1)$ (нарушение S)

$$\text{Рассмотрим } f(\overline{x}, x, x) = \left[\begin{array}{ll} f(1,0,0) = 1 & x = 0 \\ f(0,1,1) = 1 & x = 1 \end{array}\right. = 1$$

$f(\overline{x}, x, x) = \overline{x} \vee xx = \overline{x} \vee x = 1$
если получили 0, то $\overline{0} = 1$ и наоборот

Шаг 2:
Имеем $0, 1, \overline{x}$
Надо $x \cdot y$ выразить
Берем $f_3 \in L$
$f_3(x_1, \dots x_n) = \dots + \dots + \dots + x_i y_j + \dots$
Подставим $0; 1; x_i; x_j$
Возьмем самое короткое слагаемое с $x_i \quad x_j$
Для определенности $\exists$ это $x_1 \cdot x_2$
$f_3(x_1 \dots x_n) = 1 + x_1 + x_2 + x_1 x_2 x_3 \dots x_k + \dots$
подставим $x_3 \dots x_k = 1$
остальные $x_{k+1 \dots} = 0$
$f(x_1, x_2, 1, 1, 1, 0, 0, 0, \dots 0) = C_1 + x_1 x_2 + C_2 x_1 + C_3 x_2 + 0 \cdot x_1 x_2 =$

$$g(x_1, x_2) = \left[\begin{array}{l} x_1 x_2 \\ 1 + x_1 x_2 \\ 1 + x_1 + x_1 x_2 \\ 1 + x_2 + x_1 x_2 \\ x_1 + x_1 x_2 \\ x_2 + x_1 x_2 \\ x_1 + x_2 + x_1 x_2 \end{array}\right.$$

если $g(x_1, x_2) = 1 + x_1 x_2$

$\overline{g(x_1, x_2)} = x_1 x_2$ – отрицание уже есть
если $g(x_1, x_2) = 1 + x_1 + x_1 x_2 = 1 + x_2(1 + x_2)$
тогда $\overline{g(x_1, \overline{x_2})} = 1 + (1 + x_1(1 + 1 + x_2)) = x_1 x_2$
все случаи: $g(x_1, x_2) = C_1 + (x_1 + C_2) \cdot (x_2 + C_3)$

Пример. $f_3(x, y, z) = x + yz$
$f_3(0, x, y) = 0 + xy = xy$

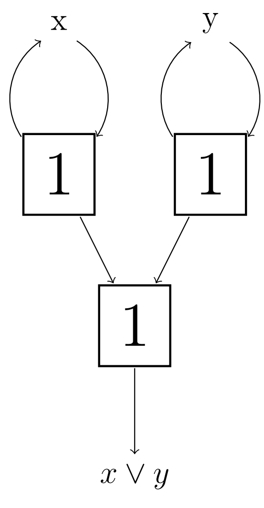
Пример. $f_3(x, y, z) = x \Rightarrow yz = 1 + x + xyz$
$f_3(x, y, 1) = 1 + x + xy = 1 + x(1 + y)$
$\overline{f_3(x, \overline{y}, 1)} = xy$
можно было
$f_3(1, x, y) = 1 + 1 + xy = xy$

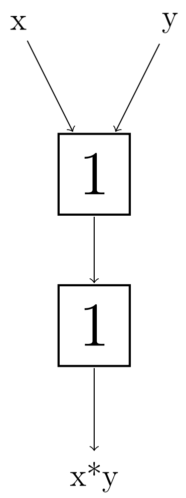
Пример. $f(x, y, z) = x \Rightarrow yz$
$g(x, y) = x + y$
$\notin T_0, T_1, L, M, S$
Выражаем
$f(x, x, x) = x \Rightarrow xx = 1$
$g(x, x) = x + x = 0$
Случай 0, 1, надо $\overline{x}$
Выражаем $\overline{x}$
$g(x, y) \notin M$
$g(1, 0) = 1$
$g(1, 1) = 0$
$\Rightarrow g(1, x) = \overline{x}$
$\Rightarrow \overline{x} = g(f(x, x, x), x)$
Выражаем $x \cdot y$
$f(x, y, z) = xx \Rightarrow yz = 1 + x + xyz$
Догадаемся, что $f(1, x, y) = x \cdot y$
Ответы: $\overline{x} = g(f(x, x, x), x) \quad x \cdot y = f(1, x, y)$

Полные наборы из одной функции (от двух переменных)
$\{f(x, y)\}$ - полный
По теореме Поста: $f(x, y) \notin$ L,M,S,T_0,T_1
Таблица истинности для f:
1 строчка :
xy $f_1 f_2 f_3 f_4$
00 1 1 1 1 $\notin T_0$
4 строчка :
xy $f_1 f_2 f_3 f_4$
11 0 0 0 0 $\notin T_1$

xy	$f1$	$f2$	$f3$	$f4$
00	1	1	1	1
01	0	0	1	1
10	0	1	0	1
11	0	0	0	0

$f_2(x,y) = \bar{y} \in L$
$f_3(x,y) = \bar{x} \in L$
$\Rightarrow f_2, f_3$ не подходят
$f_1 = \overline{x \vee y}$ $f_4 = \overline{x * y}$
$f_1^* = f_4 \quad f_1, f_4 \notin S$
$f_1 = \overline{x + y + xy} = 1 + x + y + xy \notin L$
$f_4 = 1 + xy \notin L$
$f_{1,4}(0,0) = 1 \notin M$
$f_{1,4}(1,1) = 0 \notin M$
Ответ: $\{\overline{x \vee y}\}$ - полный набор
$\{x \downarrow y\}$ - стрелка пирса
$\{x|y\}$ штриф шеффера
x|x $= \bar{x}$
$x|y = \overline{x * y} \Rightarrow \overline{x|y} = x * y \Rightarrow (x|y)|(x|y) = x * y$
$x/y = \overline{xy} = \bar{x} \vee \bar{y} \Rightarrow \bar{x}/\bar{y} = x \vee y$
$\Rightarrow (x/x)/(y/y) = x \vee y$





1.1.18 Автоматическое доказательство теорем

Задача выполнимости: дана функция в КНФ

$(x_1 \vee x_2 \vee \bar{x_3})(\bar{x_1} \vee \bar{x_2} \vee x_3)(x_1 \vee x_4)$

Эффективных алгоритмов для этой задачи нет

...

-всегда 0

-бывает 1

1.1.19 Логическое следствие

Определение. $P_1(x_1...x_k)...P_n(x_1...x_k)$

$n+1$ лог. функций (утверждений)

Q$(x_1...x_k)$

Q - логическое следствие $P_1...P_n$, если для всех наборов значений x_i, когда все $P_j(x_i...x_k) = 1$

$Q(x_1...x_k)$ тоже 1

Пример. $P_1(x, y, z)^{k=3}(x + y) \Leftrightarrow 0$

$P_2(x, y, z) = (y + z) \Leftrightarrow 1$

$Q(x, y, z) = (x + z) \Leftrightarrow 1$

$0 + 1 = x + y + y + z = x + zy + z = 1$

Есть 2 набор (001) и (110), где P_2 - истина

Q должно быть тоже истина.

Замечание. Q - логическое сложение $P_1, P_2...P_n$, по смыслу это теорем

Теорема. *Известно $P_1, P_2...P_n$,тогда Q*

xyz	P_1	P_2	Q
000	1	0	0
001	1	1	1
010	0	1	0
011	0	0	1
100	0	0	1
101	0	1	0
110	1	1	1
111	1	0	0

Определение. Q – логическое следствие $P_1..P_n$ тогда и только тогда, когда $P_1\&P_2\&...\&P_n \Rightarrow Q$ - тождественно 1 эквивалетно $(P_1, P_2...P_n \Rightarrow Q = 1)$

Проверим: $((x+y) \Leftrightarrow 0)((y+z) \Leftrightarrow 1) \Rightarrow ((x+z) \Leftrightarrow 1) = \overline{x+y} * (y+z) \Rightarrow (x+z) = (1+x+y)(y+z) \Rightarrow (x+z) = 1 + (1+x+y)(y+z) + (1+x+y)(y+z)(x+z) = 1+y+z+xy+xz+yy+yz+yx+yz+zx+zz+xyx+xyz+xzx+xzz+yyx+yyz+yzx+yzz = 1$

Доказательство: по ТИ

$x..x_k$	P_1	P_2	..	P_n	Q	$P_1P_2..P_n \Rightarrow Q$
00..0						
.	1	1	1	1	1	$1 \Rightarrow 1 = 1$
.						
.						
.	0	1	1	0	?	$0 \Rightarrow ? = 1$
11..1						$\nearrow$ все 1

$\Rightarrow$ аналогично, по ТИ

$x_1..x_k$	$P_1P_2..P_n \Rightarrow Q$	
1	$1, 0 \Rightarrow 1$	$\leftarrow P_i$ есть 0
1	$1, 1 \Rightarrow 1$	$\leftarrow$ все P_i,$Q = 1$
1	$1, 0 \Rightarrow 0$	
1	.	
1	$1, 0 \Rightarrow 0$	

Следствие: Q - логическое следствие $P_1..P_n$, тогда и только тогда, когда $P_1P_2..P_n\bar{Q}$ тождественно ложь

Замечание. по сути - это доказательство от противного

$P_1P_2..P_n \Rightarrow = 1$

$P_1P_2..P_n \Rightarrow Q = 0$

$P_1...P_n \vee Q = 0 \quad \bar{a} \vee b = \bar{a} * \bar{b}$

$P_1...P_n * \bar{Q} = 0$

$P_1...P_n\bar{Q} = 0$ чтд

Свойства логического следствия:

1. $Q = 1$ логическое следствие $P_1..P_n$

Доказательство: $P_1..P_n\bar{Q} = P_1P_2..P_n\bar{1} = P_1P_2..P_n * 0 = 0$

2. $Q = 0$ логическое следствие $P_1..P_n$ Тогда $P_1 * P_2..P_n = 0$

Доказательство: $0 = P_1..P_n\bar{Q} = P_1..P_n\bar{0} = P_1..P_n * 1 = P_1..P_n$ чтд

$2^{'}$. $Q = 0$ логическое следствие $P_1..P_n$ тогда $\forall$ набора значений $x_1, x_2..x_n$ можно найти $P_i = 0$

Доказательство: $P_1, P_2..P_n = 0 \Rightarrow$ один из $P_i = 0$ чтд

3. Q_1 - логическое следствие $P_1..P_2$

Q_2 - логическое следствие $P_1..P_nQ_1$

Q_i - логическое следствие $P_1..P_nQ_1..Q_{i-1}$ тогда Q_i - логическое следствие $P_1..P_n$

Доказательство: $P_1..P_n\bar{Q}_1 = 0$ (следует из $Q_1(1)$)

$P_1..P_nQ_1\bar{Q}_2 = 0$ (следует из Q_2) $\Rightarrow$

$P_1..P_n\bar{Q}_2 = 0$

$(1) \Rightarrow P_1P_2..P_n = 0$

или

$\bar{Q}_1 = 0 \Leftrightarrow Q = 1$

$P_1..P_n\bar{Q}_2 = 0$

$P_1..P_nQ_1\bar{Q}_2 = 0 \Rightarrow P_1..P_nQ_2 = 0$ чтд

Определение. D_1 - дизъюнкты $D_1 = \mathbf{V} \vee D_1^{'}$

D_2, где $D_2 = \mathbf{V} \vee D_2^{'}$

(дизъюнкты с одним литералом, отличающимся отрицанием)

Тогда, $\mathrm{Res}(D_1, D_2) = D_1^{'} \vee D_2^{'}$ резольвенте

Пример. $\left.\begin{array}{c} x \vee y \vee z \\ \overline{x} \vee z \end{array}\right| Y \vee Z \vee Z = Y \vee Z$

$$\left.\begin{array}{c} x \vee \overline{y} \vee z \\ x \vee y \vee T \end{array}\right| X \vee Z \vee X \vee T = x \vee Z \vee T$$

$$\left.\begin{array}{c} \overline{x} \vee \overline{y} \vee \overline{z} \\ X \vee Y \vee T \end{array}\right| \overline{Y} \vee \overline{Z} \vee \overline{Y} \vee \overline{T} = 1$$

$$\left.\begin{array}{c} \overline{x} \vee \overline{Y} \vee \overline{Z} \\ X \vee Y \vee T \end{array}\right| \overline{X} \vee \overline{Z} \vee X \vee T = 1$$

$$\left.\begin{array}{c} X \vee Y \\ \overline{Y} \end{array}\right| X$$

(особый случай)(часть определения)

$$\left.\begin{array}{c} Y \\ \overline{Y} \end{array}\right| \square = 0$$

$$\left.\begin{array}{c} X \vee Y \vee Z \\ Y \vee T \vee \overline{U} \end{array}\right|$$

Определение. $\mathrm{Res}(D_1, D_2)$ - это логическое следствие D_1 и D_2

Доказательство :

$D_1 = \mathbf{V} \vee D_1^{'}$	$D_2^{'} = \mathbf{V} \vee D_2^{'}$	$D_1^{'} \vee D_2^{'}$
1	1	

если $D_1 = 1, D_2 = 1$,то $D_1^{'} \vee D_2^{'}$
тоже должно быть 1
если $\mathbf{V} = 0$
$1 = D_1 = 0 \vee D_1^{'} = D_1^{'} = 1 \Rightarrow D_1^{'} \vee D_2^{'} = 1$
если $\mathbf{V} = 1$
$1 = D_2 = \bar{1} \vee D_1^{'} = D_2^{'} \Rightarrow D_1^{'} \vee D_2^{'} = 1$

1.1.20 Метод резолюций

Дано: $P_1 P_2 ... P_n, Q$, доказать, что Q -
P:
Шаг 0. запишем $P_i \bar{Q}$ в КНФ
тогда $P_1, P_2 .. P_n, \bar{Q}$ тоже будет иметь КНФ

Пример. $P_1 = x + y \Leftrightarrow 0$
$P_2 = y + z \Leftrightarrow 1 \bar{Q} = \overline{x + z \Leftrightarrow 1} = (x \vee z)(x \vee \bar{z})$
т.е. $P_1 P_2 \bar{Q} =$
$(\bar{x} \vee y)(x \vee \bar{y})(\bar{y} \vee \bar{z})(y \vee z)(\bar{x} \vee z)(x \vee \bar{z})$
$D_1 \quad D_2 \quad D_3 \quad D_4 \quad D_5 \quad D_6$
считаем, что у нас дизъюнктов:
$\bar{x} \vee y \quad \bar{x} \vee \bar{y} \quad \bar{y} \vee \bar{z} \quad y \vee z \quad \bar{x} \vee z \quad x \vee \bar{z}$
$D_1 \quad D_2 \quad D_3 \quad D_4 \quad D_5 \quad D_6$
Шаг 1,2,3...
Считаем резольвенты, пока не получим $\square$

Пример. $\begin{array}{rcl} D_1 & = & \overline{x} \vee y \\ D_2 & = & \overline{y} \vee \overline{z} \end{array} \Bigg| \overline{x} \vee \overline{z} = D_7$

$$\begin{array}{rcl} D_2 & = & x \vee \overline{y} \\ D_4 & = & y \vee z \end{array} \Bigg| x \vee z = D_8$$

$$\begin{array}{rcl} D_7 & = & \overline{x} \vee \overline{z} \\ D_5 & = & \overline{x} \vee z \end{array} \Bigg| x = D_9$$

$$\begin{array}{rcl} D_8 & = & x \vee z \\ D_6 & = & y \vee \overline{z} \end{array} \Bigg| \overline{x} = D_9$$

$$\begin{array}{rcl} D_8 & = & x \vee z \\ D_6 & = & x \vee \overline{z} \end{array} \Bigg| x = D_{10}$$

$$\begin{array}{rcl} D_9 & = & \overline{x} \\ D_{10} & = & x \end{array} \Bigg| \square$$

$\square$ (пустой дизъюнкт получен)

Лекция 9:

Утверждение. *Метод резолюций корректен (Q – логическое следствие $P_1, P_2, \ldots P_n$)*

Если вывести $0 \Rightarrow Q$ *– действительно логическое следствие* $P_1, P_2, \ldots P_n$

Доказательство:

$P_1, P_2, \ldots P_n$ – исходные дьзъюнкты $P_1, P_2, \ldots P_n$ $\overline{Q} = D_1 \ldots D_N$ каждый следующий $D_i (i > N)$ – логическое следствие двух прошлых дизъюнктов

Пусть $x_1, \ldots x_m$ – значения переменных, на которых $P_1, P_2, \ldots P_n$ $\overline{Q} = 1 \Rightarrow D_1 \ldots D_N = 1$

$\Rightarrow D_1 = 1, D_2 = 1 \ldots D_N = 1,\ i > N = 1$

$\Rightarrow 0 = 1$ – невозможно, так как $0 = 0$

Утверждение. *Полнота метода резолюций. Если* $D_1, D_2 \ldots D_N = 0$*, где* D_i *– дизъюнкт, то между резолюций может вывести 0*

Замечание. Метод резолюций не всегда позволяет получить 0 быстро, бывает неудачные D_i шагов примерно 2^N

Доказательство:

Индивидуально по количеству переменных $x_1 \ldots x_m$, $0 \ldots m = 1$

Какие дизъюнкты из первой переменной $x, \overline{x}, x \vee \overline{x} = 1$ среди $D_1, D_2 \ldots D_N$ есть дизъюнкты x и $\overline{x} \Rightarrow [x, \overline{x}] = 0$

Переход $m - 1 \rightarrow m$. То есть для $m - 1$ переход можно всегда вывести 0

D_+ – то есть дизъюнкты, в которых нет $\overline{x_m}$

D_- – то есть дизъюнкт, в которых нет x_m

Пример. $(x_1 \vee \overline{x_2}) \cdot (\overline{x_2} \vee x_3) \cdot (x_1 \vee x_2 \vee \overline{x_3}) \cdot (\overline{x_2} \vee \overline{x_3})$

$D_+ = [(x_1 \vee \overline{x_2}), (x_2 \vee x_3)]$

$D_- = [(x_1 \vee \overline{x_2}), (x_1 \vee x_2 \vee \overline{x_3}), (\overline{x_2} \vee \overline{x_3})]$

Теперь пусть $x_m = 0$ рассмотрим $D_+ \cdots \vee x_m = 0$

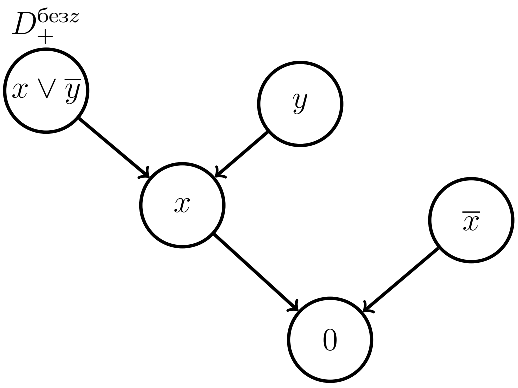
$D_- \cdots \vee \overline{x_m} = 1$

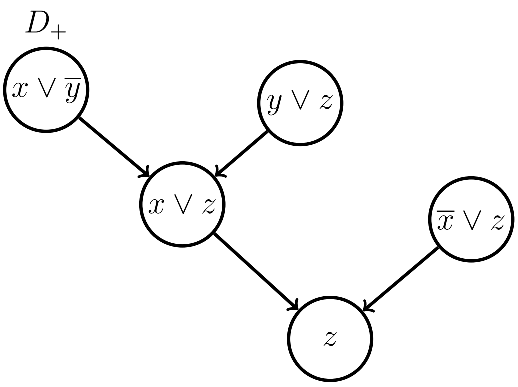
То есть все $D_+ \in 0 \Rightarrow D = 1 \Rightarrow D_1$ несовместимы, то есть $D = 0, D \in D_+$

Выведем из $D_+^{\text{без}x_m} = 0$

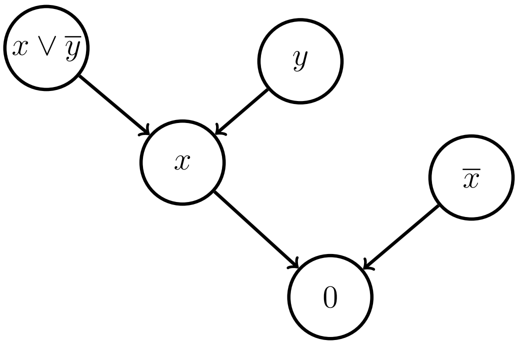
Тогда, если вернуть x_m, D_+ выводит 0 или x_m. Аналогично, если $x_m = 1, D_-$ выводит 0 или $\overline{x_m}$. Если уже получены 0, то все. Если получены x_m и $\overline{x_m} \Rightarrow$

$[x_m, \overline{x_m}] = 0$

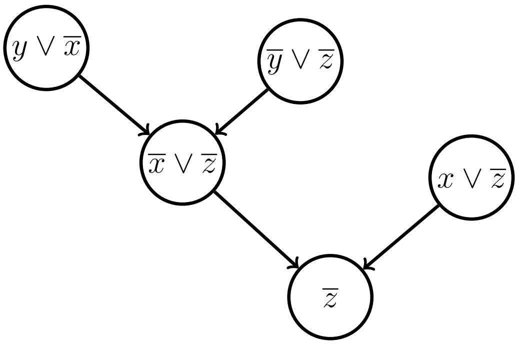




$D_-^{\text{без z}}$



D_-

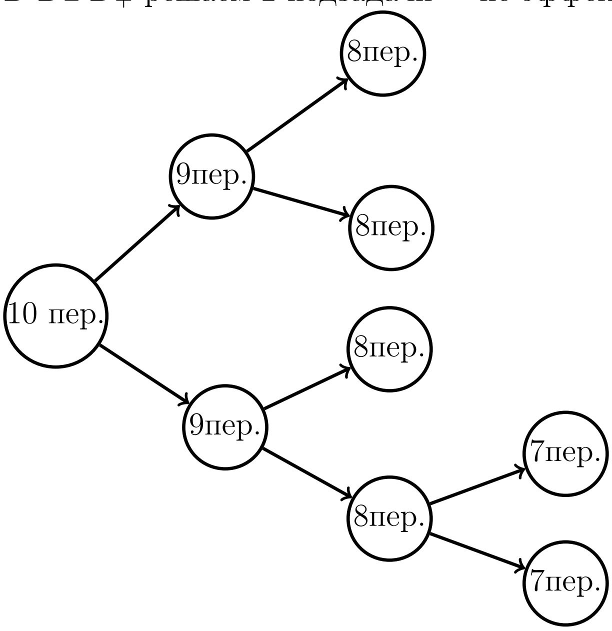


Как доказывать?

Способ 1:

Методом резолюций, как в теореме.

D D_- D_+ решаем 2 подзадачи – не эффективно



и так далее... Всего их будет 512 штук.
Способ 2: насыщение по уровням
Каждый с 0

1. с каждым слагаемым
2. каждый с исходным шагом

1.2 Исчисление предикатов

Определение. Формула исчисления предикатов

1. Вводим множество $\sum_f$ – множество функций символов
2. Вводим множество $\sum_c$ – множество констант (не обязательно функции от 0 переменных)
3. Вводим множество $\sum_p$ – предикатные символы $P(x)$
4. Вводим множество предикатных переменных $\sum_x$

Термины:

1. x – переменная
2. f – символ $(f(t_1, \dots t_n))$ – где $t_1, \dots t_n$ – термины

11 Лекция
Напоминание
Что такое функция исчисления предикатов
$\forall x(\exists y P(f(x), y) \vee Q(g(x, c)))$
f, g, c – функции
$(f(x), y), (g(x, c))$ – атамарные формы
$x, f(x), (f(x), y), x, c, g(x, c)$ – термы
P, Q – предикаты
$\forall \quad \exists$ – кванторы

Определение. Сигнатура – это множество функциональных символов и предикатов

$$f^1, g^2, e^0, P^2, Q^1$$

Определение. Интерпретация – множество + смысл предикатов и функций

В интерпретации функция – это предикат от несвязных переменных
$\forall x(x \geq x)$ – все переменные связаны $= 1$

$\forall(x \geq y)$ – y не связанная переменная $= \begin{cases} 1 & y = 1 \\ 0 & y \neq 1 \end{cases}$

в $M = \mathbb{N}$

Пример. $M = \mathbb{N} = 1, 2, 3, \ldots$ функции $= +$
$x > y = \exists k(x = y + k)$
$x \geq y = x > y \vee x = y = \exists k(x = y + k) \vee x = y$
x – четные $= \exists k(x = k + k)$
$x = 1 \quad = \forall y(y \geq x) = \forall y(\exists k(y = x + k) \vee y = x)$
Добавим в функции $\cdot$

$x \vdots y = \exists k(x = y \cdot k)$

$x \in \mathbb{P}$ – простое число $= \overline{\exists y[(x \vdots y) \cdot (y > 1) \cdot (y < x)]}(x > 1) =$

$= \forall y(x \vdots y \Rightarrow y = x \vee y = 1)(x > 1)$

Определение. Пусть F, G – функции исчисления предикатов
F – тождественно равно $G(F = G)$, если их значения совпадают в $\forall$ интерпретации

Пример. $\forall x(P(x) \Rightarrow Q(x)) = \forall x(\overline{P(x)} \vee Q(x))$
$F = G$
Данные функции тоже равны $a \Rightarrow b = \overline{a} \vee b$

Замечание. Если функции отличаются заменой, верной в логике исчислений высказываний, то они равны

Пример. $\overline{\exists x P(x) \vee \exists x Q(x)} = \overline{\exists x P(x)} \cdot \overline{\exists x Q(x)}$

1.2.1 Операции преобразования

1. Переименование переменной, если P не содержит y

   $\forall x P(x) = \forall y P(y) \qquad \exists x P(x) = \exists y P(y)$

   $\exists k(x = y + k) = \exists l(x = y + l) \neq \exists x(x = y + x) \neq \exists y(x = y + y)$

   $\exists x \forall y P(x, y) = \exists x \forall z P(x, z) \neq \exists x \forall x P(x, x)$ – некорректная функция

2. $\forall x \forall y P(x, y) = \forall y \forall x P(x, y)$

   $\exists x \exists y P(x, y) = \exists y \exists x P(x, y)$

   Доказательство для $\forall$

   Рассмотрим интерпретацию I

левая функция истанна $\Leftrightarrow P(x,y)=1 \quad \forall x,y \in M$

Правая функция истинна $\Leftrightarrow P(x,y)=1 \quad \forall x,y \in M$

Замечание. $\exists x \forall y P(x,y) \neq \forall y \exists x P(x,y)$

$IM = \mathbb{R}, P(x,y) : x > y$

$\forall y \exists x (x > y) = 1$

$\exists x \forall y (x > y) = 0$

3. $\overline{\forall x P(x)} = \exists x \overline{P(x)}$

   $\overline{\exists x P(x)} = \forall x \overline{P(x)}$

   Доказательство для $\forall$

   $IM, PM \to \{0,1\}$

   Если слева 0

   $\overline{\forall x P(x)} = 0 \Leftrightarrow \forall x P(x) = 1$

   $\Leftrightarrow P(x) = 1, x \in M$

   $\Leftrightarrow \overline{P(x)} = 0, x \in M$

   $\Leftrightarrow \exists x \overline{P(x)} = 0$

4. $\exists x P(x) \vee \exists x Q(x) = \exists x (P(x) \vee Q(x))$

   $\forall x P(x) \cdot \forall x Q(x) = \forall x (P(x) \cdot Q(x))$

   Доказательство для $\exists$

   Возьмем $IM, P\mathbb{R}$

   слева $= 0 \Leftrightarrow \begin{cases} \exists x P(x) = 0 \\ \exists x Q(x) = 0 \end{cases} \Leftrightarrow \begin{cases} P(x) = 0, x \in M \\ Q(x) = 0, x \in M \end{cases} \Leftrightarrow P(x) \vee Q(x) = 0, x \in M \Leftrightarrow$

   $\exists x (P(x) \vee Qx()) = 0$

   аналогично для $\forall$

   Замечание. Для другой связки

   $\forall x P(x) \vee \forall x Q(x) \neq \forall x (P(x) \vee Q(x))$

   Рассмотрим $I : M = \mathbb{N}$

   $P(x)$ – x четные

   $Q(x)$ – x нечетные

   $\forall x P(x) = 0$

$\forall x Q(x) = 0$

$\forall x P(x) \lor \forall x Q(x) = 0 \lor 0 = 0$

$\forall x (P(x) \lor Q(x)) = 1$

5. похожа на 4

   $\exists x P(x) \cdot Q = \exists x (P(x) \cdot Q)$

   $\exists x P(x) \lor Q = \exists x (P(x) \lor Q)$

   $\forall P(x) \cdot Q = \forall x (P(x) \cdot Q)$

   $\forall x P(x) \lor Q = \forall x (P(x) \lor Q)$

   Доказательство

   $I : M, P, Q$

   $a \in M$

   слева 1 $\Leftrightarrow \begin{cases} \exists x P(x) = 1 \\ Q = 1 \end{cases} \Rightarrow \begin{cases} P(a) = 1 \\ Q = 1 \end{cases} \Rightarrow P(a) \cdot Q = 1$

   $\Rightarrow \exists x (P(x) \cdot Q) = 1$

   Если слева 0

   если $Q = 0 \Rightarrow P(x) \cdot Q = \exists x (P(x) \cdot Q) = 0$

   если $Q = 1 \Rightarrow$

   $\exists x P(x) = 0$

   $\Rightarrow P(x) = 0, x \in M$

   $\Rightarrow P(x) \cdot Q = Q, x \in M$

   $\Rightarrow \exists x (P(x) \cdot Q) = 0$

6. $\exists x P = P$

   $\forall x P = P$

   Пример. $\forall x P(x, f(x)) \Rightarrow Q$

   $\exists w (\forall x P(x, f(x)) \Rightarrow Q)$

1.2.2 Нормальные формы

Мн Ж, КНФ, ДНФ

Определение. Предваренная нормальная форма

Формула исчисления предикатов имеет ПНФ, если

$$Q_1 x_1 Q_2 x_2 \ldots Q_n x_n (Matrix)$$

$Q_i = \forall$ или $\exists$

Простыми словами, ПНФ – это когда все кванторы стоят впереди

Пример. $\forall x \exists y (P(x,y) \Rightarrow Q(y))$

Пример. $\forall x (P(x,y,z) \vee Q(c))$

Пример. $\cancel{\forall x P(x) \cdot \exists x Q(x)}$

Пример. $\cancel{\forall x (\exists y P(y) \vee Q(x))} = \forall x \exists y (P(y) \vee Q(x))$

Теорема. *Любая формула исчисления предикатов имеет ПНФ*

Алгоритм приведения

1. Все связки кроме $\&, \vee, \neg$ заменяются на $\&, \vee, \neg$

   $a \Rightarrow b = \overline{x} \vee b$

   $a \Leftrightarrow b = (a \vee \overline{b})(\overline{a} \vee b)$

2. Все отрицания внутри кванторов

   $\overline{\forall x P(x)} = \exists x \overline{P(x)}$

   $\overline{\exists x P(x)} = \forall x \overline{P(x)}$

3. По свойству 6 вынести все кванторы в начало, возможно, заменной переменных

Пример. $\forall x P(x) \vee \forall x Q(x)$

$\neq \forall x (P(x) \vee Q(x))$

$= \forall x P(x) \vee \forall y Q(y) =$

$= \forall x (P(x) \vee \forall y Q(y)) =$

$= \forall x \forall y (P(x) \vee Q(y))$ – ПНФ

Лекция 13

Пример. Язык $L_{a=b} = \{$слова, где a и b поровну$\}$

$abc \in L_{a=b}$

$abbbcccc \notin L_{a=b}$

$ababa \notin L_{a=b}$

$\Lambda \in L_{a=b}$

Пример. $L_{a^nb^n} = \{a^nb^n \mid n \in \mathbb{N} \cup \{0\}\} = \{\Lambda, ab, aabb, aaabbb, \dots\}$
x^n – повторение n раз
$L_{a^nb^n} \subset L_{a=b}$

Пример. $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, (,), -\}$
$L_{tel} = \{$язык телефонных номеров$\}$
$+7(921)401 - 00 - 00 \in L_{tel}$

Определение. Грамматика (формальная грамматика) – это формальное описание языка
Если есть грамматика языка L
$\forall$ слова w можно проверить $w \in L$?

Типы грамматик:

0. Грамматику можно описать с помощью машины Тьюринга

   Грамматика = программа проверяет $w \in L$?

   Если для языка создать программу проверки – это тип 0

1. Контекстно-зависимые грамматики

   Контекстно-зависимые языки – описываются через конечно-зависимые грамматики

2. Контекстно-свободные грамматики

   КС языки – те языки, которые можно описать с помощью КС грамматик

3. Регулярные выражения или конечные автоматы

   Регулярные языки задаются регулярными выражениями или конечными автоматами

Замечание. Каждый следующий вид грамматики "проще предыдущего"
Но множества его языков сужаются
Языки типо 0 $\supset$ КЗ-языки $\supset$ КС-языки $\supset$ Регулярные языки

1.2.3 Машина Тьюринга

Определение. Машина Тьюринга = $(A; \square; Q; R; q_0; Q_F)$
A – алфавит, $\neq \emptyset$, множество конечное
$\square \in A$ – специальный символ
Q – состояние, $\neq \emptyset$, множество конечное
R – правила перехода

$q_0 \in Q$ – начальное состояние
$Q_F \subset Q$ – подмножество конечных состояний
$R : A \times Q \to A \times Q \times \{L, R, E - \text{не двигаться}\}$

Пример. $A = \{1, \square\}$
$Q = \{q_0, q_1\}$
$Q_F = \{q_1\}$

R/A	1	$\square$
q_0	$1, q_1, R$	$1, q_1, S$
q_1	не надо	не надо

Конечное количество символов ленты $\neq \square$

0	1	2	3	...	...	...	...	...
1	1	1	1	$\square$	$\square$	$\square$	$\square$	...
$\uparrow$								
q_0								

Сначала головка смотрит на клетку с индексом 0, состояние q_0
Видим символ 1
$R(1, q_0) = 1, q_0, R$ – сдвинуть головку вправо

0	1	2	3	...	...	...	...	...
1	1	1	1	$\square$	$\square$	$\square$	$\square$	...
	$\uparrow$							
	q_0							

Головка на клетке 1
Символ = 1
Состояние = q_0
$R(1, q_0) = 1, q_0, R$

0	1	2	3	...	...	...	...	...
1	1	1	1	$\square$	$\square$	$\square$	$\square$	...
		$\uparrow$						
		q_0						

потом

0	1	2	3	...	...	...	...	...
1	1	1	1	□	□	□	□	...
			↑					

потом

0	1	2	3	...	...	...	...	...
1	1	1	1	□	□	□	□	...
				↑				

Теперь:
Головка: клетка 4
Символ: □
Состояние: q_0
$R(0, q_0) = 1, q_1, E$ – стоим на месте

0	1	2	3	4	...	...	...	...
1	1	1	1	1	□	□	□	...
				↑				

Дано было 1111, результат 11111
Вывод: программа дописывает 1
Работа Машины Тьюринга формально

Определение. Конфигурация: $(w, n \in \mathbb{N} \cup \{0\}, q)$
n – положение головки
$q \in Q$
w – слово на ленте (без хвоста □)
Один шаг исполнения программы:
$(w_1, n_1, q_1) \to (w_2, n_2, q_2)$
$w_1[n_1]$ – символ над головкой
$R(w_1[n_1], q_1) = (a, q_2, L/R/E)$
$w_2 = w_1$ где $w_1[n] = a$
если $L \to n_2 = n_1 - 1$
$R \to n_2 = n_1 + 1$
$E \to n_2 = n_1$
Начало работы: (w, O, q_0)
w – дана
O – головка слова
q_0 – начальное слово
$\to \cdots \to \cdots \to \cdots \to (\overline{\overline{w}}, \overline{q} \in Q_F)$ – конечное состояние
Ответ: $\overline{\overline{w}}$, то есть из слова w получили $\overline{\overline{w}}$

Замечание. (Тезис Чёрге)

Все, что мы интуитивно понимаем как алгоритм, может быть реализовано с помощью машины Тьюринга

Замечание. Модификации машины Тьюринга:

1. ∞ в обе стороны лента

2. несколько лент

3. недетерминированная машина Тьюринга

1, 2, 3 – это все эквивалент обычной машины Тьюринга

Замечание. Про проверку, слово в языке? $w \in ?L$

					$\square$	$\square$	$\square$	$\square$	

Если результат $1 \Rightarrow w \in L$
Если результат $0 \Rightarrow w \notin L$
или
$\{q_1, q_2\} = Q_F$
$q_1 : w \in L$
$q_2 : w \notin L$
Все зависит от конечного состояния

1.2.4 Контекстно-свободные языки

Пример. Email @ server
username $\to$ word
server $\to$ word.word
word $\to \boxed{a}$
word $\to \boxed{b}$
word $\to \boxed{c}$
$E \to u@S \to w@S \to$ (используя правило $s \to w.w$) $w@w.w \to$ (используя правило $w \to ww$) $ww@w.w$
$\to xw@w.w \to xy@w.w$
$\to xy@ww.w \to xy@www.w$
$\to xy@www.ww$

Можно ли получить $xy@@ru$?
нет $\notin L$
то есть слова, которые можно получить, они $\in L$

Пример. Еще

1. $S \rightarrow$

2. $S \rightarrow aSb$

– это грамматика
$S \rightarrow aSb \rightarrow aaSbb \rightarrow aaaSbbb \rightarrow aaabbb$
Какие слова можно вывести?
$\{a^n b^n | n \geq 0\} = \{\Lambda, ab, aabb, aaabbb, \dots\}$

Определение. КС-грамматика – $(A, N, S \in N, R)$
A – алфавит терминальных символов конечен, $\neq \emptyset$
N – алфавит нетерминальных символов, конечен, $\neq \emptyset$
S – начальный нетерминальный
R – множество правил

Лекция 14
КС – грамматика
А – Алфавит
N – нетерминальные символы (алф.)
S $\in$ N – начальное
R – правило вида $N \rightarrow (A \vee N)^*$

Определение. Из слова $w \in (A \in N)^*$ выводится u $\in (A \vee N)^*$ если w $= \dots x \dots \rightarrow u = \dots$ Y ...
где $X \rightarrow Y \in R$

Определение. Вывод – это последовательность $w_i : w_{i-1} \rightarrow w_i$

$w_1 \rightarrow w_2 \rightarrow w_3 \dots \rightarrow w_n = w_1 \rightarrow^* w_n$
вывод w_n из w_1

Определение. Язык, который задает КС - грамматика
$L = \{w / \exists$ вывод $S^* \rightarrow w\}$

Пример. 1) HTML H – начальный нетерминал
$H \rightarrow EH$ T – тэг, L – символы
$H \rightarrow$
$H \rightarrow$
$H \rightarrow EH$
$H \rightarrow EH \rightarrow EEH \rightarrow EE$
$H \rightarrow EE \dots E$
$E \rightarrow T$

$E \to L$
$L \to a$
$L \to b$
$L \to c$
.
.
$L \to A$

Устройство тэгов:
$T \to O$
T – тэг
L – символы
O – открывание тэга
C – закрывание тэга
T – OHC
T – $< \cdots > \cdots < \cdots >$
T – $< \cdots >_{img}$
O $\to < N >$
C $\to < \mathbf{N} >$
N $\to$
N $\to LN$
N $\to$ LLLL
Выведем hello,<b>World<h>!
$H \to EH \to EEG \to^* EEEEEEEEEH \to EEEEEEEEE \to^* LLLLLLLTL \to^* h, T!$
$\to hello, < N > world < \mathbf{N} >!$
$\to^* hello, < b > world < /b >!$
Итого, hello, <b> world $< /t >! \in \alpha$
Что есть в теме?
– алгоритм разбора
Дана грамматика, слово, получить вывод слова или понять, что оно не выводится – специальные виды грамматик с эффектом алг. разбора
$*LL(1)LR(1)LALR(1)\ldots$

1.2.5 Регулярные языки

Задаются регулярными выражениями и конечными автоматами
Регулярные языки и выражения

Определение. Регулярные языки
1) $\{a\}$, где $a \in A$ регулярный

2) если L_1 и L_2 – регулярные, то $L_1L_2 = \{w_1w_2\}, w_1 \in L_1, w_2 \in L_2)$ – регулярный

L_1L_2 – регулярные

$L_1|L_2 = L_1 \vee L_2$ – регулярный

Пример. $\mathrm{A} = \{a, b, c\}$

$\{a\} \qquad \{b\} = \{ad\}$

$\{ab\}|\{b\} = \{abc\}$

$\{a\}|\{b\} = \{a, b\}$

$\{a, b\}|\{b\}|\{c\} = \{ab, bc\}$

$\{ab, b, c\}\{b, bc\} = \{abb, abbc, bb, bbc, cb, cbc\}$

$\{a\}^* = \{\Lambda, a, aa, aaa, \dots\}$

$\{a, b\}^* = \{\Lambda, a, b, aa, ab, ba, bb, aab, abb, \dots\}$ – слова из a и b

$\{a, bc\}^* = \{\Lambda, a, bc, abc, bca, aa, bcbc, \dots, aabc, abcbcaa\}$

Определение. Регулярные выражения – это выражение над языками.

1) Определим – конк, 1, итерация

2)$\{a\}$ – записываются как

Пример. $abc^* = \{ab, abc, abcc, abccc, \dots\} \uparrow$ конк $\downarrow a(bc)^* = \{a, abc, abcbc, abcbcbc, \dots\}$

$(0|1|2)(0|1|2|3|\dots|9) : (0|1|2|3|4|5)$

$(0|1|2|\dots|9)$ – время

$A = \{0, 1, 2, \dots 9, :\}$

23:56 29:40??

Нормальное время

[0123456789]

$((0|1)(0|1\dots|9)(20|21|22|23) : (0|\dots|5)(0)\dots(9))$

Пример. $(a|b)^* = \{\Lambda a, b, ab, aa, bb, ba, \dots, abbaab\dots\}$

$(ab)^* = \{\Lambda, ab, abab, ababab, \dots\}$

$a^*|b^* = \{\Lambda, a, aa, aaa, aaaa, \dots, b, bb, bbb, bbbb, \dots\}$

$\{a^4b^4/n \in \mathbf{N}$ – не регулярный язык

Определение. Конечные автоматы это $\{Q, S \subset Q, F \subset Q, E \subset QxQxA \vee \{\epsilon\})\}$

Q – конечное не пустое множество состояний.

S – начальное состояние

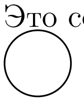
F – конечные состояние

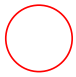
A – алфавит

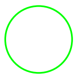
E – переходы между состояниями

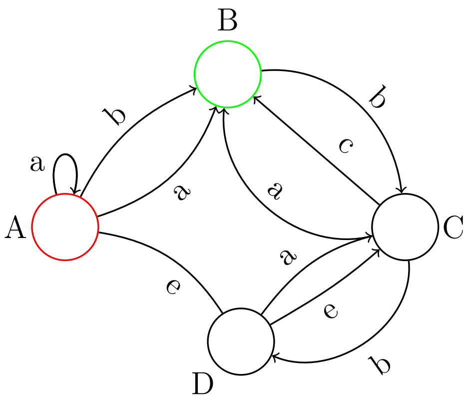
$q_1 \to^{A,\epsilon} q_2$

Это состояние:



Начальное состояние: 

Конечное состояние: 



ϵ – пустой переход
$Q = \{A, B, C, D\}$

Определение. Конфигурация $\in A^*xQ$ – слово и состояние

Пример. (abc,A) (bb,B) (Λ, A)

Определение. Из конфигурации 1 выводится конфигурация 2
$(w_1, q_1) \to (w_2, q_2)$
если $\exists e \in E : q_1 \to^a q_2$ и $W_2 = w_1 a$

Пример. $(\Lambda, A) \to (a, A) \to^{A\to^a A} (aa, A) \to^{A\to^b B}$

$\vdots$

$\to^{B\to^b c} (aabb, c) \to^{c\to^b D} (aabbb, D) \to^{D\to^\epsilon C} (aabbb, c)$

Определение. Какой язык задает конечный автомат?
слово w $\in$ L, если $\exists$ вывод $(\Lambda, s) \to \cdots \to (w, f)$, где $s \in S, f \in F$

S – начальное
f – конечное

если могу прочитать слово w, начав в начальном состоянии, закончив в конечном.

Определение. в прошлом примере

aabbb $\in L$

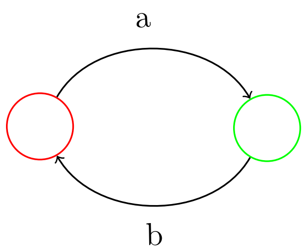
$aabb \in L$

$aab \in L$

$a \in L$

$a \to^{\epsilon} D \to^{a} C$

Пример.



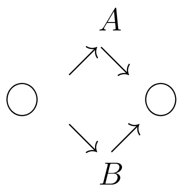
L $= \{a, aba, ababa, \dots\} = a(ba)^*$

Утверждение

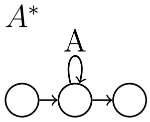
Язык регулярный $\Leftrightarrow \exists$ конечный автомат, который его принимает

AB: $\bigcirc \to^{A} \bigcirc \to^{B}$ B

A/B:



A^*



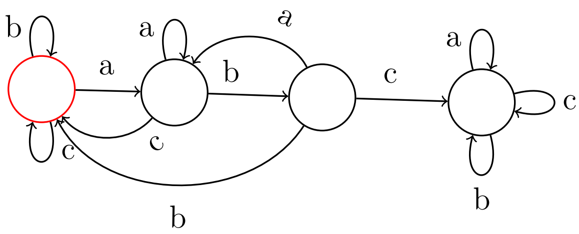
Авт $\to$ Регулярное выражение - убирание вершин

Определение. Детерминированный КА – это КА, у которого

1) |S| $= 1$ ровно 1 нач вершина

2) нет ϵ – переходов

3) $\bigcirc$ $\nearrow\searrow$ нет двух переходов с одинаковыми символами и началом



Дет, язык слов, содержащих abc.
Аналогичный подтерм $(a|b|c)^*abc(a|b|c)^*$