

Исчисление высказываний

Высказывание – утверждение о математических объектах, которому можно однозначно приписать истинностное значение – ИСТИНА или ЛОЖЬ.

Обозначения: ИСТИНА, Т, И, 1
ЛОЖЬ, F, Л, 0.

Рассматриваем следующие операции над этими двумя значениями: \wedge , \vee , \neg , \rightarrow ,

\equiv
Операции можно задать с помощью следующих таблиц (*таблицы истинности*)

a	b	$a \wedge b$	$a \vee b$	$\neg a$	$a \rightarrow b$	$a \equiv b$
л	л	л	л	И	И	И
л	И	л	И		И	л
И	л	л	И	л	л	л
И	И	И	И		И	И

Формулы исчисления высказываний

Рассмотрим понятие переменной – $a, b, c, \dots, x, y, \dots$

Будем строить формулы, последовательно вводя операции над константами И и Л и переменными:

- Атомарная формула $x, И, Л$
- Отрицание $(\neg F)$, где F - формула
- Конъюнкция $(F_1 \wedge F_2)$, где F_1, F_2 - формулы
- Дизъюнкция $(F_1 \vee F_2)$, где F_1, F_2 - формулы
- Следование $(F_1 \rightarrow F_2)$, где F_1, F_2 - формулы
- Эквивалентность $(F_1 \equiv F_2)$, где F_1, F_2 - формулы

Учитывая приоритеты операций и их ассоциативность (слева направо), будем опускать «лишние» скобки.

Примеры формул исчисления высказываний:

- | | |
|--|--|
| 1. $a \vee$ | 3. $a \wedge$ |
| 2. $(a \rightarrow b) \rightarrow (a \vee$
$b)$ | 4. $(a \rightarrow b) \equiv \neg a \vee$
b |

Для заданной формулы F обозначим $\text{Var}(F)$ множество входящих в формулу переменных. Интерпретация формулы – функция на $\text{Var}(F)$ $\mathbf{I} : \text{Var}(F) \rightarrow \{ И, Л \}$

Если задана интерпретация, то можно вычислить значение формулы $\text{Val}(F, \mathbf{I}) \in \{ И, Л \}$

Тавтология – формула, истинная в любой интерпретации: $\text{Val}(F, \mathbf{I}) = И$ для любой \mathbf{I}

Противоречие – формула, ложная в любой интерпретации: $\text{Val}(F, \mathbf{I}) = Л$ для любой \mathbf{I}

(1), (4) – примеры тавтологий; (3) – противоречие; (2) – ни тавтология, ни противоречие

Логическое следствие и эквивалентность формул

Говорят, что формула B является *логическим следствием* формулы A (запись: $A \Rightarrow B$), если в любой интерпретации, в которой истинна формула A , формула B также истинна.

Например:

$$a \Rightarrow a \vee$$

$$a \wedge b \Rightarrow a \rightarrow$$

Говорят, что формулы A и B эквивалентны, если $A \Rightarrow B$ и $B \Rightarrow A$ (запись: $A \Leftrightarrow B$).

Можно еще сказать, что две формулы эквивалентны, если они в любой интерпретации одновременно истинны или одновременно ложны.

Например:

$$a \wedge a \Leftrightarrow a \vee$$

$$a \vee b \Leftrightarrow a \rightarrow$$

b

Три теоремы:

Теорема 1 (связь между логическим следствием и операцией логического следования):

$A \Rightarrow B$ тогда и только тогда, когда формула $A \rightarrow B$ – тавтология.

Теорема 2 (связь между эквивалентностью формул и операцией логической эквивалентности):

$A \Leftrightarrow B$ тогда и только тогда, когда формула $A \equiv B$ – тавтология.

Теорема 3 (о подстановке): если в некоторой формуле подставить вместо некоторой подформулы эквивалентную ей подформулу, то получившаяся формула будет эквивалентна исходной.

Доказательство всех трех теорем очевидно.

Эквивалентное преобразование формул

Несколько важных эквивалентностей исчисления высказываний

□ законы булевой алгебры:

- | | | | |
|----|--|--|-----------------------|
| 1. | $a \wedge a \Leftrightarrow a$ | $a \vee a \Leftrightarrow a$ | идемпотентность |
| 2. | $a \wedge b \Leftrightarrow b \wedge a$ | $a \vee b \Leftrightarrow b \vee a$ | коммутативность |
| 3. | $(a \wedge b) \wedge c \Leftrightarrow a \wedge (b \wedge c)$ | $(a \vee b) \vee c \Leftrightarrow a \vee (b \vee c)$ | ассоциативность |
| 4. | $(a \wedge b) \vee a \Leftrightarrow a$ | $(a \vee b) \wedge a \Leftrightarrow a$ | поглощение |
| 5. | $a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c)$ | $a \vee (b \wedge c) \Leftrightarrow (a \vee b) \wedge (a \vee c)$ | дистрибутивность |
| 6. | $\perp \wedge a \Leftrightarrow \perp$ | $\top \vee a \Leftrightarrow \top$ | ограниченность |
| 7. | $\top \wedge \neg a \Leftrightarrow \neg a$ | $a \vee \neg a \Leftrightarrow \top$ | исключение «третьего» |
| 8. | $\neg \neg a \Leftrightarrow a$ | $\neg \neg \neg a \Leftrightarrow \neg a$ | инволютивность |
| 9. | $\neg(a \vee b) \Leftrightarrow \neg a \wedge \neg b$ | $\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b$ | законы де Моргана |

□ исключение операций, не являющихся операциями решетки:

10. $a \rightarrow b \Leftrightarrow \neg a \vee b$
11. $a \equiv b \Leftrightarrow (a \wedge b) \vee (\neg a \wedge \neg b)$

Исчисление предикатов

Распространяем понятие логической формулы на объекты, отличные от истинностных значений И и Л.

Строим формулы из элементарных объектов *предметной области*.

- константы a, b, c, ...
- переменные x, y, z, ...
- функции разной арности f, g, +, ...

Терм – константа, переменная или применение функции к термам, например:

a + b f (g (x + 1), x)

- предикаты разной арности P, Q, <, ...

Атом – применение предиката к термам, например:

P (x, x + 1) y < x + 1

- формулы, представляющие логические операции над атомами

$(y < x) \rightarrow (y < x + 1)$

- связывание переменных в формуле кванторами всеобщности \forall и существования \exists .

$\forall x(F(x))$ $\exists x(F(x))$

Например:

$\forall x \exists y (x < y)$ $\exists y \forall x (x < y)$

Чтобы вычислить логическое значение формулы, надо задать интерпретацию – сопоставить константам значения из выбранной предметной области, функциям придать смысл, предикатам сопоставить отношения соответствующей арности, а также связать все переменные формулы.

Логическое следствие и эквивалентность

Понятия логического следствия и эквивалентности формул можно перенести в исчисление предикатов:

Формула B является *логическим следствием* формулы A , если в любой интерпретации, в которой истинна A формула B также истинна. $A \Rightarrow B$

Формулы A и B *эквивалентны* ($A \Leftrightarrow B$), если $A \Rightarrow B$ и $B \Rightarrow A$.

Для эквивалентного преобразования формул можно, помимо уже имеющих эквивалентностей, использовать следующие:

- | | | |
|----|---|--|
| 1. | $\forall x(\neg F(x)) \Leftrightarrow$ | $\exists x(\neg F(x)) \Leftrightarrow$ |
| 2. | $\neg \exists x(F(x))$ | $\neg \forall x(F(x))$ |
| | $\forall x \forall y (F(x, y)) \Leftrightarrow \forall y \forall x (F(x,$ | $\exists x \exists y (F(x, y)) \Leftrightarrow \exists y \exists x$ |
| | $y))$ | $(F(x, y))$ |
| 3. | $\forall x(F(x) \wedge G(x)) \Leftrightarrow \forall x(F(x)) \wedge$ | $\exists x(F(x) \vee G(x)) \Leftrightarrow \exists x(F(x)) \vee$ |
| | $\forall x(G(x))$ | $\forall x(G(x))$ |
| 4. | $\forall x(F(x) \wedge G(x)) \Rightarrow \exists x(F(x)) \wedge$ | $\forall x(F(x)) \vee \forall x(G(x)) \Rightarrow \forall x(F(x) \vee$ |
| | $\exists x(G(x))$ | $G(x))$ |

Заметьте, что следующие формулы НЕ эквивалентны, и ни одна из них НЕ является следствием другой:

$$\forall x \exists y (F(x, y)) \quad \text{и} \quad \exists y \forall x (F(x, y))$$

Пример:

$\forall x \exists y (x < y) \Leftrightarrow \forall x \exists y (\neg(x \geq y)) \Leftrightarrow \forall x (\neg \forall y (x \geq y)) \Leftrightarrow \neg \exists x (\forall y (x \geq y))$
 здесь все формулы истинны в стандартной арифметической интерпретации;
 однако формула $\exists y \forall x (x < y)$ - ложна.

Формальные теории

Формализовать понятие доказательства, чтобы можно было формальными методами исследовать, насколько достоверен сам математический метод дедукции.

Будем считать, что утверждения теории описываются *формулами*.

Определение: будем говорить, что задана некоторая формальная теория (ФТ), если

- задан *алфавит* и правила построения *правильных формул* из символов этого алфавита
- выделено некоторое множество формул этого исчисления, называемых *аксиомами* ФТ
- определены некоторые отношения на множестве формул, называемые *правилами вывода*

Если несколько формул связано правилом вывода, то отделяют последнюю формулу, называя ее *заключением*. Остальные формулы при этом называют *посылками*.

Принято отделять посылки от заключения горизонтальной чертой:

$$\frac{A, B, C}{D} \quad - \text{здесь } A, B \text{ и } C \text{ – посылки, а } D \text{ – заключение.}$$

Говорят, что формула D непосредственно выводима из формул A , B и C по одному из правил вывода.

Выводимость из гипотез

Пусть задан набор гипотез $\Gamma = \{ \Gamma_1, \Gamma_2, \dots, \Gamma_n \}$

Вывод – это последовательность формул $\{ F_1, F_2, \dots, F_k = G \}$, такая, что каждая формула F_i

- является аксиомой;
- либо является одной из формул Γ_j ;
- либо получена из предыдущих формул с помощью одного из правил вывода;

Говорят, что формула G выводима из гипотез Γ , если существует ее вывод.

$$\Gamma \vdash G$$

Говорят, что формула G является теоремой данной теории, если существует ее вывод из пустого множества гипотез: $\vdash G$

Формальное исчисление высказываний – это формальная теория, в которой формулами являются логические формулы, аксиомами – некоторые тавтологии, а правила вывода – это правила, по которым можно осуществлять эквивалентное преобразование формул.

Формальная арифметика – это формальная теория предикатов, содержащая в качестве констант целые числа, функций – целочисленные функции, предикатов – отношения на множестве целых чисел. Правила вывода – это опять обычные правила преобразования логических формул.

Формальное исчисление высказываний

Будем строить формулы из (логических) констант a, b, c, \dots с помощью набора логических операций \neg и \rightarrow .

Правильно построенные формулы:

$$(a \rightarrow b) \rightarrow \neg(b \rightarrow a)$$

$$(a \rightarrow a)$$

Аксиомы:

$$(A_1): (a \rightarrow (b \rightarrow a))$$

$$(A_2): ((a \rightarrow (b \rightarrow c)) \rightarrow ((a \rightarrow b) \rightarrow (a \rightarrow c)))$$

$$(A_3): ((\neg b \rightarrow \neg a) \rightarrow ((\neg b \rightarrow a) \rightarrow b))$$

Правила вывода:

(P): правило подстановки

$$\frac{\mathcal{A}}{\mathcal{A}\{B|C\}}$$

Если формула \mathcal{A} содержит в своей записи пропозициональную переменную B , а C — произвольная формула, условимся обозначать через $\mathcal{A}\{B|C\}$ формулу, полученную из \mathcal{A} заменой всех вхождений переменной B формулой C . Если формула \mathcal{A} переменной B не содержит, будем считать, что $\mathcal{A}\{B|C\}$ совпадает с \mathcal{A} .

(MP): modus ponens

$$\frac{\mathcal{A}, \mathcal{A} \rightarrow \mathcal{B}}{\mathcal{B}}$$

Примеры выводов в формальном исчислении высказываний

$\vdash (a \rightarrow a)$

- | | |
|--|--------------|
| 1. $(a \rightarrow (b \rightarrow a))$ | (A_1) |
| 2. $(a \rightarrow ((a \rightarrow a) \rightarrow a))$ | $(1; P)$ |
| 3. $((a \rightarrow (b \rightarrow c)) \rightarrow ((a \rightarrow b) \rightarrow (a \rightarrow c)))$ | (A_2) |
| 4. $((a \rightarrow ((a \rightarrow a) \rightarrow a)) \rightarrow ((a \rightarrow (a \rightarrow a)) \rightarrow (a \rightarrow a)))$ | $(3; P)$ |
| 5. $((a \rightarrow (a \rightarrow a)) \rightarrow (a \rightarrow a))$ | $(2, 4; MP)$ |
| 6. $(a \rightarrow (a \rightarrow a))$ | $(1; P)$ |
| 7. $(a \rightarrow a)$ | $(5, 6; MP)$ |

Теперь теорему $(a \rightarrow a)$ можно использовать в выводах в качестве аксиомы.

$\mathcal{A} \vdash (\mathcal{B} \rightarrow \mathcal{A})$

- | | |
|--|--------------|
| 1. \mathcal{A} | (Γ_1) |
| 2. $(a \rightarrow (b \rightarrow a))$ | (A_1) |
| 3. $(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{A}))$ | $(2; P)$ |
| 4. $(\mathcal{B} \rightarrow \mathcal{A})$ | $(1, 3; MP)$ |

Теперь в выводах можно использовать новое правило вывода
(введение импликации)

$$\frac{\mathcal{A}}{\mathcal{B} \rightarrow \mathcal{A}}$$

Теорема о дедукции

В формальном исчислении высказываний следующие утверждения равносильны:

$$\Gamma, \mathcal{A} \vdash \mathcal{B} \quad \text{и} \quad \Gamma \vdash (\mathcal{A} \rightarrow \mathcal{B})$$

Правило транзитивности

$$\frac{(\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{B} \rightarrow \mathcal{C})}{(\mathcal{A} \rightarrow \mathcal{C})}$$

Вместо вывода $(\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{B} \rightarrow \mathcal{C}) \vdash (\mathcal{A} \rightarrow \mathcal{C})$ построим, опираясь на теорему о дедукции, вывод $(\mathcal{A} \rightarrow \mathcal{B}), (\mathcal{B} \rightarrow \mathcal{C}), \mathcal{A} \vdash \mathcal{C}$.

- | | | |
|----|---|---------------------|
| 1. | $(\mathcal{A} \rightarrow \mathcal{B})$ | (Γ_1) |
| 2. | $(\mathcal{B} \rightarrow \mathcal{C})$ | (Γ_2) |
| 3. | \mathcal{A} | (Γ_3) |
| 4. | \mathcal{B} | $(1, 3; \text{MP})$ |
| 5. | \mathcal{C} | $(2, 4; \text{MP})$ |

Упражнение: выведите правило сечения

$$\frac{(\mathcal{A} \rightarrow (\mathcal{B} \rightarrow \mathcal{C})), \mathcal{B}}{(\mathcal{A} \rightarrow \mathcal{C})}$$

Полнота и непротиворечивость формальной теории

Интерпретация формальной теории – правило, согласно которому некоторым формулам теории сопоставляется истинностное значение.

Интерпретация называется *моделью формальной теории*, если в ней теоремами являются только истинные утверждения (формулы).

Формальная теория называется *полной* в заданной интерпретации, если в ней выводимо любое истинное утверждение.

Формальная теория называется *формально непротиворечивой*, если в ней невозможно одновременно вывести формулы \mathcal{A} и $\neg\mathcal{A}$.

Система аксиом теории называется *независимой*, если ни одну из этих аксиом невозможно вывести из остальных.

Формальная *теория первого порядка* – это формальная теория, формулы которой являются формулами исчисления предикатов. Принято формализацию математических теорий проводить в рамках теорий первого порядка.

Теоремы Геделя о неполноте

Теорема 1. Во всякой *достаточно богатой* формальной теории первого порядка существует такая истинная формула F , что ни F , ни $\neg F$ не выводимы в этой теории.

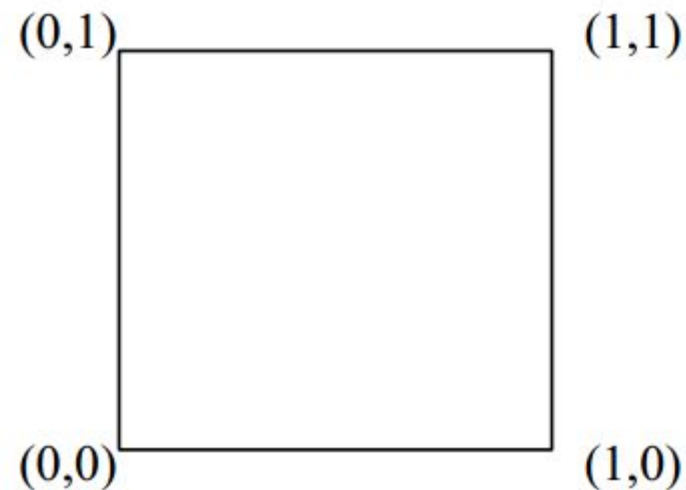
Теорема 2. Во всякой *достаточно богатой* формальной теории первого порядка формула, утверждающая непротиворечивость этой теории, не выводима в ней.

Булевы функции.

Пусть $\alpha=(\alpha_1,\alpha_2,\dots,\alpha_n)$ и $\beta=(\beta_1,\beta_2,\dots,\beta_n)$ – двоичные векторы.
Будем писать $\alpha\leq\beta$ (или $\beta\geq\alpha$), если $\alpha_i\leq\beta_i$ для всех $i=1,2,\dots, n$.

Если $\alpha \leq \beta$, но $\alpha \neq \beta$, будем писать $\alpha < \beta$ (последнее означает, что $\alpha_i \leq \beta_i$ для всех $i=1,2,\dots, n$, и при этом хотя бы одно из этих неравенств строгое). Заметим, что имеются векторы α и β , для которых неверно ни $\alpha \leq \beta$, ни $\beta \leq \alpha$. Такие векторы будем называть несравнимыми.

Двумерные двоичные векторы можно рассматривать как вершины единичного квадрата в двумерном евклидовом пространстве:



Векторы α и β связаны отношением \leq , если из вершины α можно пройти в вершину β по сторонам квадрата в направлении координатных осей (направо и вверх).

Аналогично, трехмерные векторы соответствуют вершинам куба;

векторы α и β связаны отношением \leq , если из вершины α можно пройти в вершину β по ребрам куба в направлении координатных осей.

Пусть

$$U=U(X_1, X_2, \dots, X_n)$$

– произвольная формула алгебры высказываний, содержащая n переменных. Оценка переменных такой формулы – это упорядоченная последовательность из 0 и 1 длины n , то есть n -мерный двоичный вектор.

Каждой оценке переменных

$$(x_1, x_2, \dots, x_n) \in \{0, 1\}^n$$

однозначным образом сопоставляется значение истинности $u \in \{0, 1\}$ высказывания, полученного из формулы U после соответствующей подстановки.

Таким образом, мы получаем соответствие

$$(x_1, x_2, \dots, x_n) \rightarrow u,$$

задающее отображение

$$f_U: \{0,1\}^n \rightarrow \{0,1\},$$

$$u = f_U(x_1, x_2, \dots, x_n).$$

Такие отображения называют булевыми функциями.

Непосредственно из определений вытекает, что формулы алгебры высказываний

$$U=U(X_1, X_2, \dots, X_n)$$

и

$$V=V(X_1, X_2, \dots, X_n)$$

равносильны в том и только том случае, когда функции f_U и f_V совпадают.

Заметим, что Булевы функции представляют интерес не только в связи с их «логическим» происхождением, но и сами по себе.

Введем следующие определения.

Переменные, пробегающие множество $\{0,1\}$, мы будем называть булевыми и обозначать буквами

$$x, y, z, \dots, x_1, x_2, \dots$$

Функция от одной или нескольких булевых переменных, принимающая значение в множестве $\{0,1\}$, называется булевой.

Любую булеву функцию можно задать таблицей, подобной таблице истинности.

Булевы функции от одной переменной– это отображения
Множества $\{0,1\}$ в себя. Булевы функции от одной
переменной можно рассматривать как унарные операции
на множестве $\{0,1\}$.

Булевы функции от двух переменных можно рассматривать как бинарные операции на множестве $\{0,1\}$. В следующей таблице приведены все шестнадцать булевых функций от двух переменных (значения аргументов и функций выписаны в строках, функции перечисляются в столбце).

x_1	0	0	1	1
x_2	0	1	0	1

f_0	0	0	0	0	0 – тождественный ноль
f_1	0	0	0	1	· умножение, конъюнкция
f_2	0	0	1	0	
f_3	0	0	1	1	x_1
f_4	0	1	0	0	
f_5	0	1	0	1	x_2
f_6	0	1	1	0	\oplus – сложение по модулю 2
f_7	0	1	1	1	\vee – дизъюнкция
f_8	1	0	0	0	\downarrow – стрелка Пирса
f_9	1	0	0	1	\leftrightarrow – эквивалентность
f_{10}	1	0	1	0	
f_{11}	1	0	1	1	\leftarrow – обратная импликация
f_{12}	1	1	0	0	
f_{13}	1	1	0	1	\rightarrow – импликация
f_{14}	1	1	1	0	$ $ – штрих Шеффера
f_{15}	1	1	1	1	1 – тождественная единица

Комбинируя перечисленные функции (с помощью суперпозиций), можно строить более сложные булевы функции, в том числе и большего числа переменных, например, $xy \rightarrow zt$ и т.п.

Булевы отрицание, конъюнкция(умножение), дизъюнкция, импликация обладают свойствами, подобными тем, которыми обладают соответствующие логические операции (с естественной заменой равносильности формул на равенство функций).

Приведем некоторые уравнения, в которых одни булевы функции выражены через другие:

$$\neg x = x \rightarrow 0 = x | x = x \downarrow x = 1 \oplus x;$$

$$xy = \neg (\neg x \vee \neg y) = \neg x \downarrow \neg y = (x \downarrow x) \downarrow (y \downarrow y);$$

$$x \vee y = \neg (\neg x \neg y) = \neg x \rightarrow y = (x \rightarrow y) \rightarrow y = \neg x | \neg y \\ = (x | x) | (y | y);$$

$$x \rightarrow y = \neg x \vee y;$$

$$x \leftrightarrow y = (x \rightarrow y) (y \rightarrow x) = xy \vee \neg x \neg y;$$

$$x \oplus y = x \neg y \vee \neg x y.$$

Принцип двойственности

Далее для обозначения отрицания будем использовать знак $x' = \neg x$.

Двойственной к булевой функции

$$f(x, y, \dots, z)$$

называется функция

$$f^*(x, y, \dots, z) = f(x', y', \dots, z').$$

Если

$$f(x,y,\dots,z)$$

представлена формулой, содержащей только конъюнкции, дизъюнкции и отрицания, то двойственная функция получается заменой в этой формуле конъюнкций на дизъюнкции, а дизъюнкций на конъюнкции.

Дизъюнктивная нормальная форма
(ДНФ).

Конъюнктивная нормальная форма
(КНФ).

Пусть функция от трех переменных задана следующей таблицей:

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

тогда

$$f(x,y,z) = x'y'z' \vee xy'z' \vee xyz.$$

Каждый из трех дизъюнктивных членов (слагаемых) записанной формулы соответствует набору значений аргументов, для которого функция принимает значение 1.

Легко видеть, что описанный способ построения формулы по таблице применим к любой функции, не равной тождественно нулю.

Получаемые при этом формулы называются совершенными дизъюнктивными нормальными формами, (СДНФ).

Считается, что СДНФ тождественного нуля– это «пустая» дизъюнкция, не содержащая ни одного дизъюнктивного слагаемого.

Двойственная конструкция приводит к представлению функции в так называемой совершенной конъюнктивной нормальной форме, сокращенно СКНФ.

СКНФ рассмотренной ранее функции имеет следующий вид:

$$f(x,y,z) = (x \vee y \vee z')(x \vee y' \vee z)(x \vee y' \vee z')(x' \vee y \vee z')(x' \vee y' \vee z).$$

Каждый из пяти конъюнктивных членов (множителей) соответствует набору значений аргументов, для которого функция принимает значение 0.

Описанный выше способ построения СДНФ и СКНФ опирается на следующую теорему о разложении функции по переменной.

Теорема. Пусть $f(x_1, x_2, \dots, x_n)$ – произвольная булева функция.

Тогда

$$f(x_1, x_2, \dots, x_n) = x_1 \cdot f(1, x_2, \dots, x_n) \vee x_1' \cdot f(0, x_2, \dots, x_n);$$

$$f(x_1, x_2, \dots, x_n) = (x_1 \vee f(0, x_2, \dots, x_n))(x_1' \vee f(1, x_2, \dots, x_n)).$$

Доказательство. Докажем первую формулу. Чтобы не загромождать выкладки индексами и многоточиями, ограничимся случаем функции от двух переменных.

Доказываемая формула принимает следующий вид:

$$f(x,y) = x \cdot f(1,y) \vee x' \cdot f(0,y).$$

При любом y подстановка в правую часть $x=1$ и $x=0$ дает соответственно

$$1 \cdot f(1,y) \vee 1' \cdot f(0,y) = f(1,y) \vee 0 \cdot f(0,y) = f(1,y) \vee 0 = f(1,y);$$

$$0 \cdot f(1,y) \vee 0' \cdot f(0,y) = 0 \vee 1 \cdot f(0,y) = 1 \cdot f(0,y) = f(0,y).$$

Таким образом, левая и правая части доказываемого равенства совпадают на любом наборе значений аргументов. Следовательно, функции слева и справа от знака равенства равны. На общий случай доказательство распространяется практически без изменений. Достаточно считать, что y обозначает не одну переменную, а набор переменных. Второе равенство из формулировки теоремы доказывается аналогично (кроме того, его справедливость следует из принципа двойственности).

Последовательно применяя несколько раз (по числу переменных) разложение из предыдущей теоремы, можно получить СДНФ булевой функции. Например,

$$\begin{aligned} f(x,y) &= x \cdot f(1,y) \vee x' \cdot f(0,y) = \\ &= x \cdot (y \cdot f(1,1) \vee y' \cdot f(1,0)) \vee x' \cdot (y \cdot f(1,1) \vee y' \cdot f(1,0)) = \\ &= x \cdot y \cdot f(1,1) \vee x \cdot y' \cdot f(1,0) \vee x' \cdot y \cdot f(1,1) \vee x' \cdot y' \cdot f(1,0). \end{aligned}$$

Функция $f(x,y)$ представлена в виде дизъюнкции четырех дизъюнктивных членов. Те из них, для которых коэффициент $f(\alpha,\beta)$ равен нулю, можно отбросить. В результате получится

СДНФ. Например, для функции $f(x,y)=x\oplus y$ имеем

$$f(0,0)=f(1,1)=0 \quad \text{и} \quad f(0,1)=f(1,0)=1 ,$$

поэтому

$$x\oplus y = x \cdot y' \vee x' \cdot y.$$

Элементарной конъюнкцией (конъюнктом) называют конъюнкцию переменных и/или их отрицаний, в которой каждая переменная встречается не более одного раза.

Пустой дизъюнкт считается равным 0.

Конъюнктивной нормальной формой называется конъюнкция конечного числа дизъюнктов.

Полные системы булевых функций

Система булевых функций называется полной, если любая булева функция может быть выражена через функции этой системы с помощью суперпозиций.

Таким образом, в соответствии с определением система функций $\{\wedge, \vee, '\}$ полна.

Поскольку дизъюнкцию можно выразить через конъюнкцию и отрицание, система функций $\{\wedge, '\}$ также полна. Точно так же полной является и система функций $\{\vee, '\}$, поскольку конъюнкцию можно выразить через дизъюнкцию и отрицание. Отрицание можно выразить через ноль и импликацию, дизъюнкцию— через импликацию и отрицание. Следовательно, отрицание и импликация, ноль и импликация также образуют полные системы функций $\{', \rightarrow\}$, $\{0, \rightarrow\}$.

Через \oplus и 1 можно выразить отрицание, так что система функций $\{1, \oplus, \cdot\}$ также является полной. Последнее означает, что любая булева функция может быть представлена в виде многочлена.

При этом ненулевыми коэффициентами при одночленах служат единицы, а одночлены не содержат степеней переменных, поскольку умножение (конъюнкция) идемпотентна. Такие многочлены называют полиномами Жегалкина.

Пример. Вычислим полином Жегалкина для функции

$$f(x,y,z)=(x \rightarrow y) \vee (z \rightarrow y)$$

Имеем

$$\begin{aligned}(x \rightarrow y) \vee (z \rightarrow y) &= (x' \vee y) \vee (z' \vee y) = (xy')' \vee (zy')' = \\ &= (1 \oplus xy') \vee (1 \oplus zy') = (1 \oplus xy') \oplus (1 \oplus zy') \oplus (1 \oplus xy') (1 \oplus zy') = \\ &= 1 \oplus xy' \oplus 1 \oplus zy' \oplus 1 \oplus xy' \oplus zy' \oplus xy' zy' = \\ &= (1 \oplus 1) \oplus (xy' \oplus xy') \oplus (zy' \oplus zy') \oplus 1 \oplus xy' z = \\ &= 0 \oplus 0 \oplus 0 \oplus 1 \oplus xy' z = 1 \oplus xy' z = 1 \oplus x(1 \oplus y)z = 1 \oplus xz \oplus xyz.\end{aligned}$$

При выводе использовались равенства $x' = 1 \oplus x$, $x \oplus x = 0$,

$x \vee y = x \oplus y \oplus xy$ и др.

Существуют полные системы, содержащие всего одну функцию. Отрицание и конъюнкцию можно выразить через стрелку Пирса. Следовательно, стрелка Пирса составляет полную систему функций $\{\downarrow\}$. Точно так же отрицание и дизъюнкция выражаются через штрих Шеффера, так что $\{\bar{\vee}\}$ – тоже полная система функций.

Таким образом, что установить полноту системы функций можно, показав, как через функции этой системы выражаются функции какой-нибудь системы, полнота которой уже известна. Доказательство неполноты может оказаться более изощренным.

Пример. Покажем что система функций $\{\cdot, \vee\}$ неполна.

Действительно, отрицание нельзя выразить через дизъюнкцию

и конъюнкцию. Допустим противное, то есть, что отрицание

удалось представить в виде $x' = f(x, y, \dots, z)$, и при этом функция f

выражена через конъюнкции и дизъюнкции. Тогда

$$1 = 0' = f(0, y, \dots, z) \quad \text{и} \quad 0 = 1' = f(1, y, \dots, z).$$

Но конъюнкция и дизъюнкция монотонны по своим аргументам:

$$\text{если } \alpha_1 \leq \alpha_2 \text{ и } \beta_1 \leq \beta_2 \text{ то } \alpha_1 \wedge \beta_1 \leq \alpha_2 \wedge \beta_2 \text{ и } \alpha_1 \vee \beta_1 \leq \alpha_2 \vee \beta_2.$$

Тем же свойством обладает и любая сложная функция, составленная из конъюнкции и дизъюнкции. Значит,

$$f(0, y, \dots, z) \leq f(1, y, \dots, z),$$

что противоречит предполагаемому равенству.

Важнейшие замкнутые классы булевых функций.

Теорема Поста о полноте

Пусть \mathbf{K} – некоторый класс булевых функций. Замыканием класса \mathbf{K} называется множество всех тех функций, которые могут быть выражены через функции класса \mathbf{K} . Замыкание класса \mathbf{K} будем обозначать через $[\mathbf{K}]$. Класс функций называется замкнутым, если он совпадает со своим замыканием.

Замыкание любой полной системы функций содержит все булевы функции. Для неполной системы функций это уже не так. Например, отрицание не входит в замыкание класса $K = \{\wedge, \vee\}$.

Рассмотрим важнейшие замкнутые классы булевых функций.

Класс P_0 .

Класс P_0 – это класс всех функций, сохраняющих 0, то есть таких функций $f(x_1, x_2, \dots, x_n)$, для которых $f(0, 0, \dots, 0) = 0$.

В этот класс входят:

тождественная функция;

конъюнкция;

дизъюнкция;

сложение по модулю 2;

Не входят: тождественная единица; отрицание; импликация.

Таблица для функции из класса P_0 в первой строке содержит 0, остальные значения могут быть какими угодно.

Класс P_1 . Класс P_1 – это класс всех функций, сохраняющих 1, то есть таких функций $f(x_1, x_2, \dots, x_n)$, для которых $f(1, 1, \dots, 1) = 1$.

В этот класс входят:

тождественная функция;

конъюнкция;

дизъюнкция;

сложение по модулю 2;

импликация.

Не входят в P_1 :

тождественный ноль;

отрицание.

Класс \mathcal{S} .

Класс \mathcal{S} – это класс всех самодвойственных функций, то есть таких функций f , которые совпадают со своей

двойственной функцией, $f^* = f$.

Простейшие примеры самодвойственных функций– x и x' .

Функция

$$xy \vee xz \vee yz$$

также самодвойственная:

$$\begin{aligned}(xy \vee xz \vee yz)^* &= (x \vee y)(x \vee z)(y \vee z) = (x \vee xy \vee xz \vee yz)(y \vee z) = \\ &= xy \vee xz \vee yz \vee xyz = xy \vee xz \vee yz.\end{aligned}$$

Конъюнкция и дизъюнкция не самодвойственны.

В таблице самодвойственной функции значение в последней строке противоположно значению в первой строке, значение в предпоследней– значению во второй, и т.д.

Класс L . Класс L – это класс всех линейных функций, то есть функций, представимых в виде

$$f(x_1, x_2, \dots, x_n) = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \dots \oplus \alpha_n x_n,$$

где $\alpha_1, \alpha_2, \dots, \alpha_n \in \{0, 1\}$ – константы.

Функции $x, x' = 1 \oplus x, x \oplus y$ линейные; конъюнкция, дизъюнкция – нет.

Класс M .

Класс M – это класс монотонных функций.

Функция $f(x_1, x_2, \dots, x_n)$, называется монотонной, если

$$f(\alpha_1, \alpha_2, \dots, \alpha_n) \leq f(\beta_1, \beta_2, \dots, \beta_n)$$

при

$$(\alpha_1, \alpha_2, \dots, \alpha_n) \leq (\beta_1, \beta_2, \dots, \beta_n).$$

Конъюнкция, дизъюнкция монотонны;

отрицание, импликация, сложение по модулю 2 – нет.

Теперь мы можем сформулировать один из важнейших результатов теории булевых функций– теорему Поста о полноте.

Теорема. Класс функций K полон тогда и только тогда, когда он не содержится целиком ни в одном из перечисленных выше пяти классов $P_0, P_1, S, L, M.$

Как было показано, ни один из перечисленных пяти замкнутых классов не является полным (имеются не входящие в него булевы функции). Поэтому не может быть полным ни один класс функций, целиком содержащийся в одном из них. С помощью теоремы Поста можно устано

Имеются булевы функции, не входящие ни в один из классов

$P_0, P_1, S, L, M.$ Любая такая функция в соответствии с теоремой составляет полную систему функций, то есть через эту функцию может быть выражена любая булева функция.

Среди функций от двух переменных такими функциями являются стрелка Пирса и штрих Шеффера.

С помощью теоремы Поста можно установить полноту системы функций, не выписывая непосредственно выражения для булевых функций.