Лекция 09 — Основы булевой алгебры

Содержание

"Мы почитаем всех нулями, а единицами — себя."
— А. С. Пушкин

Аксиоматика

Определение

Булева алгебра — дополненная дистрибутивная решётка.

Иными словами, булева алгебра — это кортеж $\langle B, \vee, \wedge, \neg, 0, 1 \rangle$, где:

- B — множество-носитель булевой алгебры;
- $\vee$, $\wedge$ — бинарные операции (join и meet);
- $\neg$ — унарная операция (*дополнение*);
- 0, 1 — константы (*наименьший* и *наибольший* элементы решётки),

удовлетворяющий 5 группам аксиом.

Аксиомы булевой алгебры

- коммутативность:

$$x \vee y = y \vee x \qquad x \wedge y = y \wedge x$$

- ассоциативность:

$$(x \vee y) \vee z = x \vee (y \vee z) \qquad (x \wedge y) \wedge z = x \wedge (y \wedge z)$$

- дистрибутивность:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \qquad x \vee (y \wedge z) = (x \wedge y) \vee (x \wedge z)$$

- идентичность:

$$x \vee 0 = x \qquad x \wedge 1 = x$$

- дополнение:

$$x \vee \neg x = 1 \qquad x \wedge \neg x = 0$$

Булевы выражения

Определение

Булево выражение определяется рекурсивно:

- переменные и константы являются выражениями;
- если f и g являются выражениями, то также являются выражениями $\neg f$, $\neg g$, $f \wedge g$, $f \vee g$.

Каждое выражение задаёт *булеву функцию* $f : B^n \to B$, где B — носитель булевой алгебры.

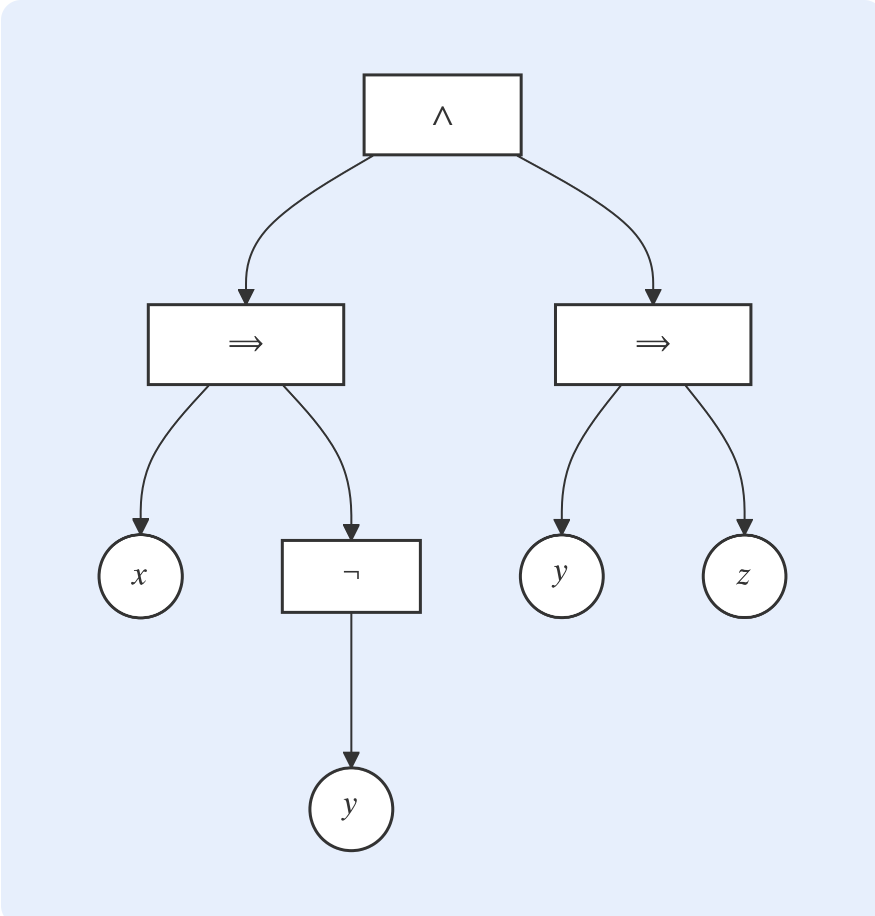
Виды выражений

Тождественно истинное выражение $f \equiv 1$ называется **тавтологией**.
Тождественно ложное выражение $f \equiv 0$ называется **противоречием**.
Выражений, истинность которого зависит от значений переменных, называется **неопределенностью** (*contingency*).

Булевы выражения можно представлять в виде ориентированных деревьев так, что более глубокая операция будет выполняться раньше. Так, например, выражение

$$(x \implies \neg y) \wedge (y \implies z)$$

примет следующий вид:



Таблицы истинности

ⓘ **Определение**

Таблица истинности — способ формального определения булевой функции, явно сопоставляющий каждому возможному набору переменных результат её применения на нём и группирующий получившиеся данные в формате таблицы:

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

ⓘ **Определение**

Два булевых выражения называются **эквивалентными**, если их таблицы истинности совпадают.

Булевы операции

Простые операции

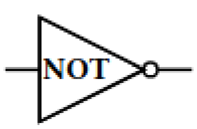
Отрицание

Отрицание — унарная операция, результат которой истинен тогда и только тогда, когда значение операнда ложно.

- Обозначение: $\neg x$
- Неформальное название: «не»/«not»
- Таблица истинности:

x	$\neg x$
0	1
1	0

- Обозначение в логической схеме:



Конъюнкция

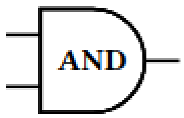
Конъюнкция — бинарная операция, результат которой истинен тогда и только тогда, когда значение обоих операндов истинно.

- Обозначение: $x \wedge y$
- Неформальное название: «и»/«and»

- Таблица истинности:

x	y	$x \land y$
0	0	0
0	1	0
1	0	0
1	1	1

- Обозначение в логической схеме:



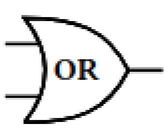
Дизъюнкция

Дизъюнкция — бинарная операция, результат которой истинен тогда и только тогда, когда значение хотя бы одного из операндов истинно.

- Обозначение: $x \lor y$
- Неформальное название: «или»/«or»
- Таблица истинности:

x	y	$x \lor y$
0	0	0
0	1	1
1	0	1
1	1	1

- Обозначение в логической схеме:



Сложные операции

Импликация

Импликация — бинарная операция, результат которой истинен тогда и только тогда, когда ложен первый операнд или истинен второй.

- Обозначение: $x \implies y$
- Упрощённая запись: $\neg x \vee y$
- Неформальное название: «из x следует y»
- Таблица истинности:

x	y	$x \implies y$
0	0	1
0	1	1
1	0	0
1	1	1

- Обозначение в логической схеме отсутствует.

Эквиваленция

Эквиваленция — бинарная операция, результат которой истинен тогда и только, когда значения операндов совпадают.

- Обозначение: $x \iff y$
- Упрощённая запись: $(x \implies y) \wedge (y \implies x)$
- Неформальное название: «равно»/«equal»
- Таблица истинности:

x	y	$x \iff y$
0	0	1
0	1	0
1	0	0
1	1	1

- Обозначение в логической схеме отсутствует.

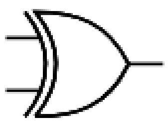
Исключающее «ИЛИ»

Исключающее «ИЛИ» — бинарная операция, результат которой истинен тогда и только тогда, когда значения операндов не совпадают.

- Обозначение: $x \oplus y$
- Упрощённая запись: $(x \land \neg y) \lor (\neg x \land y)$
- Неформальное название: «XOR»
- Таблица истинности:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

- Обозначение в логической схеме:


XOR

Законы булевой алгебры

> **Принцип двойственности**
>
> В любой булевой алгебре верное тождество остаётся верным, если в нём заменить все операторы $\land, \lor$ и константы $0, 1$ на обратные.
>
> *Следствие*. Доказательство любой теоремы даёт два результата.
> Приведенные далее доказательства будут активно пользоваться этим фактом.

Далее будут приведены наиболее важные из свойств логических операций, вытекающие из аксиом булевой алгебры, и их аксиоматические доказательства.

> **Идемпотентность**
>
> $$x \lor x = x \qquad x \land x = x$$
>
> *Доказательство*

$$
\begin{aligned}
x \vee x &= (x \vee x) \wedge 1 && \text{идентичность} \\
&= (x \vee x) \wedge (x \vee \neg x) && \text{дополнение} \\
&= x \vee (x \wedge \neg x) && \text{дистрибутивность} \\
&= x \vee 0 && \text{дополнение} \\
&= x && \text{идентичность}
\end{aligned}
$$

Замечание. Если для произвольных логических переменных x и y выполняется закон идемпотентности, то есть верно, что

$$x \vee y = x \qquad x \wedge y = x,$$

то значения этих переменных совпадают. Это легко продемонстрировать, рассуждая от противного. Предположение $y \neq x$ можно записать в виде $y = \neg x$, тогда из закона дополнения имеем:

$$x \vee \neg x = 1 \qquad x \wedge \neg x = 0,$$

то есть исходные тождества не могут выполняться одновременно.

Поглощение

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

Доказательство

$$
\begin{aligned}
x \vee (x \wedge y) &= (x \wedge 1) \vee (x \wedge y) && \text{идентичность} \\
&= x \wedge (1 \vee y) && \text{дистрибутивность} \\
&= x \wedge 1 && \text{идентичность} \\
&= x && \text{идентичность}
\end{aligned}
$$

Доминирование

$$x \vee 1 = 1 \qquad x \wedge 0 = 0$$

Доказательство

$$
\begin{aligned}
x \vee 1 &= (x \wedge 1) \vee (1 \wedge 1) && \text{идентичность} \\
&= 1 \wedge (x \vee 1) && \text{дистрибутивность} \\
&= 1 \wedge 1 && \text{идентичность} \\
&= 1 && \text{идентичность}
\end{aligned}
$$

Склеивание

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

Доказательство

$$\begin{aligned} xy \vee x\overline{y} &= x(y \vee \overline{y}) && \text{дистрибутивность} \\ &= x \wedge 1 && \text{дополнение} \\ &= x && \text{идентичность} \end{aligned}$$

Инволюция

$$\neg\neg x = x$$

Доказательство

$$\begin{aligned} x \vee \neg\neg x &= (x \vee \neg\neg x) \wedge 1 && \text{идентичность} \\ &= (x \vee \neg\neg x) \wedge (x \vee \neg x) && \text{дополнение} \\ &= x \vee (\neg\neg x \wedge \neg x) && \text{дистрибутивность} \\ &= x \vee 0 && \text{дополнение} \\ &= x && \text{идентичность} \end{aligned}$$

Двойственное утверждение верно автоматически. Тогда имеем:

$$x \vee \neg\neg x = x \qquad x \wedge \neg\neg x = x$$

откуда, согласно закону идемпотентности, $x = \neg\neg x$.

Законы де Моргана

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

Доказательство

$$\begin{aligned} (x \vee y) \vee (\neg x \wedge \neg y) &= ((x \vee y) \vee \neg x) \wedge ((x \vee y) \vee \neg y) && \text{дистрибутивность} \\ &= ((x \vee \neg x) \vee y) \wedge ((y \vee \neg y) \vee x) && \text{коммутативность} + \text{ассоциативность} \\ &= (1 \vee y) \wedge (1 \vee x) && \text{дополнение} \\ &= 1 \wedge 1 && \text{доминирование} \\ &= 1 && \text{идентичность} \end{aligned}$$

$$\begin{aligned} (x \vee y) \wedge (\neg x \wedge \neg y) &= ((\neg x \wedge \neg y) \wedge x) \vee ((\neg x \wedge \neg y) \wedge y) && \text{дистрибутивность} \\ &= ((\neg x \wedge x) \wedge \neg y) \vee ((\neg y \wedge y) \wedge \neg x) && \text{коммутативность} + \text{ассоциативность} \\ &= (0 \wedge \neg y) \vee (0 \wedge \neg x) && \text{дополнение} \\ &= 0 \vee 0 && \text{доминирование} \\ &= 0 && \text{идентичность} \end{aligned}$$

Согласно закону дополнения, $\neg x \wedge \neg y = \neg(x \vee y)$, что и требовалось доказать. Двойственное утверждение верно автоматически.

Единственность дополнения

$$(y = \neg x) \wedge (z = \neg x) \implies x = z$$

Доказательство

$$\begin{aligned}
y &= y \wedge 1 && \text{идентичность} \\
&= y \wedge (x \vee z) && \text{дополнение} \\
&= (y \wedge x) \vee (y \wedge z) && \text{дистрибутивность} \\
&= 0 \vee (y \wedge z) && \text{дополнение} \\
&= (x \wedge z) \vee (y \wedge z) && \text{дополнение} \\
&= z \wedge (x \vee y) && \text{дистрибутивность} \\
&= z \wedge 1 && \text{дополнение} \\
&= z && \text{идентичность}
\end{aligned}$$

Декомпозиция Шеннона

Любая булева функция $f(x_1, x_2, \ldots, x_n)$ представима в виде:

$$\overline{x_i} \wedge f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \vee x \wedge f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$$

или

$$(\overline{x_i} \vee f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)) \wedge (x \vee f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n))$$

Доказательство оставим особо любопытным читателям в качестве упражнения.

Консенсус-теорема

$$xy \vee \overline{x}z \vee yz = xy \vee \overline{x}z$$

Доказательство

$$
\begin{aligned}
xy \vee \overline{x}z \vee yz &= xy \vee \overline{x}z \vee (1 \wedge yz) && \text{идентичность} \\
&= xy \vee \overline{x}z \vee (x \vee \overline{x})yz && \text{дополнение} \\
&= xy \vee \overline{x}z \vee xyz \vee \overline{x}yz && \text{дистрибутивность} \\
&= xy(1 \vee z) \vee \overline{x}z(1 \vee y) && \text{дистрибутивность} \\
&= (xy \wedge 1) \vee (\overline{x}z \wedge 1) && \text{доминирование} \\
&= xy \vee \overline{x}z && \text{идентичность}
\end{aligned}
$$