Московский физико-технический институт
Физтех-школа прикладной математики и информатики
Математическая логика и теория алгоритмов, осень 2021
Лекции 2–4: пропозициональные формулы и булевы функции

Краткое содержание

Понятие булевой функции. Представление булевой функции в виде таблицы истинности. Количество булевых функций от n переменных. Булевы функции от одного или двух аргументов: константы, отрицание, конъюнкция, дизъюнкция, импликация, эквиваленция, строгая дизъюнкция, штрих Шеффера, стрелка Пирса. Булевы функции от многих аргументов: конъюнкция, дизъюнкция, чётность, условная дизъюнкция, большинство, пороговые функции. Задание булевой функции пропозициональной формулой. Понятия литерала, конъюнкта, дизъюнкта. Представление булевой функции в виде дизъюнктивной или конъюнктивной нормальных форм. Совершенные КНФ и ДНФ и их сокращение. Тавтологии и противоречия. Выполнимые и опровержимые формулы. Примеры тавтологий: закон тождества, закон непротиворечия, закон исключённого третьего, закон двойного отрицания, законы де Моргана, закон контрапозиции, силлогизм. Сложение и умножение булевых переменных. Многочлены Жегалкина. Количество многочленов Жегалкина от n переменных. Многочлен, представляющий константу ноль, является нулевым. Однозначность представления булевой функции в виде многочлена Жегалкина. Композиция булевых функций. Замыкание множества булевых функций. Полные и неполные системы булевых функций. Классы, замкнутые относительно композиции. Решётка Поста. Функции, сохраняющие ноль. Функции, сохраняющие единицу. Монотонные функции, два эквивалентных определения. Двойственные функции и двойственные классы. Самодвойственные функции. Линейные функции. Критерий Поста полноты системы булевых функций. Базисы замкнутых классов. Любой базис всех функций содержит не более 4 функций. Примеры базисов из 1, 2, 3, 4 функций. Базис класса монотонных функций.

Лейтмотивом нашего курса является соответствие между синтаксисом и семантикой, т. е. между правилами построения текстов и их смыслом. В этой лекции мы впервые установим это соответствие для конкретного примера: пропозициональных формул со стороны синтаксиса и булевых функций со стороны семантики.

1 Булевы функции

Определение 1. *Булевой функцией* от n переменных называется любое отображение из $\{0,1\}^n$ в $\{0,1\}$.

Константы 0 и 1 обычно интерпретируются как логические значения: 1 как истина, а 0 как ложь. Поэтому булевы функции также называются логическими.[1] Поскольку область определения любой булевой функции конечна, то её можно определить, задав значения во всех точках. Это часто делают при помощи таблиц истинности: каждая

[1] А булевыми они называются в честь английского математика и логика Джорджа Буля (George Boole).

строчка соответствует набору аргументов, а в столбцах перечислены значения этих аргументов и значение функции. Пример таблицы истинности для функции трёх аргументов показан на рис. 1, художественный взгляд на них — на рис. 2.

Рис. 1: Пример таблицы истинности

p	q	r	$f(p,q,r)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

Посчитаем общее количество всех булевых функций от n переменных. Всего разных наборов из n нулей и единиц будет 2^n штук, т. к. для каждой из n переменных будет 2 варианта. Иными словами, таблица истинности содержит 2^n строк. Поскольку на каждом из 2^n наборов функция может принимать одно из двух значений, то общее количество булевых функций составит 2^{2^n}. При $n \leqslant 2$ это обозримое число, поэтому все функции можно просто перечислить.

Начнём с $n = 0$. Сначала нужно разобраться с тем, что такое «функция нуля переменных». Чтобы было выполнено свойство $\{0,1\}^n = \{0,1\}^n \times \{0,1\}^0$, необходимо чтобы $\{0,1\}^0$ было *синглетоном*, т. е. одноэлементным множеством.[2] В таком случае функция из $\{0,1\}^0$ в $\{0,1\}$ будет задана своим значением на этом единственном элементе. Таким образом, будет всего две булевых функции от 0 переменных: константа 0 (также обозначается $\mathbf{0}$, $\mathbb{0}$, $\bot$) и константа 1 (также обозначается $\mathbf{1}$, $\mathbb{1}$, $\top$). Можно заметить, что количество булевых функций от нуля аргументов — две — соответствует формуле 2^{2^n}. Можно обобщить это рассуждение и получить следующее универсальное соображение: функция нуля аргументов есть константа.

Перейдём к $n = 1$. В этом случае должно быть $2^{2^1} = 4$ различные функции. Две из них уже есть — это логические константы. Оставшиеся две — это тождественная функция $f(p) = p$ и отрицание $f(p) = \neg p$:

p	$\top$
0	1
1	1

p	$\bot$
0	0
1	0

p	p
0	0
1	1

p	$\neg p$
0	1
1	0

Для $n = 2$ будет уже $2^{2^2} = 16$ различных функций. Из них шесть будут существенно зависеть не более, чем от одной переменной: две константы, две проекции (или проектора) и два отрицания аргументов:

[2] Интересно, что это слово дважды вошло в русский технический язык. Сначала в математический как *синглетон*, потом в программистский как *синглтон*.

Рис. 2: Карикатурист Сидней Харрис (Sidney Harris) о таблицах истинности

p	q	$\top$
0	0	1
0	1	1
1	0	1
1	1	1

p	q	$\bot$
0	0	0
0	1	0
1	0	0
1	1	0

p	q	p
0	0	0
0	1	0
1	0	1
1	1	1

p	q	$\neg p$
0	0	1
0	1	1
1	0	0
1	1	0

p	q	q
0	0	0
0	1	1
1	0	0
1	1	1

p	q	$\neg q$
0	0	1
0	1	0
1	0	1
1	1	0

Наиболее важными из оставшихся функций являются конъюнкция $p \wedge q$ (логическое «И», минимум, умножение), дизъюнкция $p \vee q$ (логическое «ИЛИ», максимум) и импликация $p \to q$ (логическое следование, «меньше или равно»).

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Таблицы истинности для конъюнкции и дизъюнкции не вызывают сомнений: конъюнкция истинна, только если оба аргумента истинны, а дизъюнкция истинна, если хотя бы один аргумент истинен. А вот таблицу для импликации стоит обосновать: почему это из лжи следуют и истина, и ложь? Объяснять можно по-разному, один из способов такой: не вызывает сомнений, что при любом x из $x > 8$ следует $x > 4$. Далее, если рассмотреть $x = 10$, то из истинного утверждения будет следовать истинное. При $x = 5$ из

ложного утверждения следует истинное, а при $x = 2$ из лжи следует ложь. Поскольку истинность импликации не должна зависеть от конкретного содержания утверждений, получаем, что из лжи следует что угодно, а истина следует из чего угодно. А вот из истины ложь не следует по самому духу импликации.[3]

Вместе с обратной импликаций ($q \to p$) мы перечислили 10 функций. Осталось 6. Две из них также имеют явный логический смысл: строгая дизъюнкция $p \oplus q$ (исключительное «ИЛИ», XOR, сложение по модулю 2, «не равно») и эквиваленция $p \leftrightarrow q$ (равенство). Оставшиеся четыре являются отрицаниями основных функций: штрих Шеффера $p \mid q$ (отрицание конъюнкции), стрелка Пирса $p \downarrow q$ (отрицание дизъюнкции), а также отрицания импликаций $p \not\to q$ и $q \not\to p$ («больше» и «меньше» соответственно).

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

p	q	$p \mid q$
0	0	1
0	1	1
1	0	1
1	1	0

p	q	$p \downarrow q$
0	0	1
0	1	0
1	0	0
1	1	0

p	q	$p \not\to q$
0	0	0
0	1	0
1	0	1
1	1	0

Уже для трёх аргументов общее количество функций составляет 256, так что перечислять их все долго и не нужно. Но некоторые функции многих переменных мы отметим. Во-первых, конъюнкцию и дизъюнкцию можно рассматривать как функции многих аргументов: конъюнкция будет истинна, если истинны все аргументы, а дизъюнкция — если истинен хотя бы один. Во-вторых, сложение по модулю 2 тоже можно рассмотреть как функцию многих аргументов. В таком случае результат будет единицей, если среди аргументов нечётное число единиц. Поэтому эту функцию называют функцией чётности (parity).[4] В-третьих, часто встречается условная дизъюнкция $p?q : r = (p \to q) \wedge (\neg p \to r)$. В программировании её часто называют тернарным оператором по умолчанию: если p истинно, то значение условной дизъюнкции совпадает с q, а если p ложно, то с r. В-четвёртых, важную роль играют *пороговые функции* (threshold functions): $\mathrm{thr}_{n,k}(x_1, \ldots, x_n)$ истинно, если из n аргументов хотя бы k единиц (т. е. $x_1 + \cdots + x_n \geqslant k$). Частным случаем является функция большинства (majority), принимающая то же значение, что и большинство аргументов. (Если количество аргументов чётно, то нужно каким-то образом договориться о том, чему равна функция, если нулей и единиц поровну). Пороговые функции важны, поскольку они моделируют работу нервных клеток в мозгу: если достаточное число нервных окончаний возбудилось, то сигнал передаётся дальше по аксону. Кроме того, пороговые функции моделируют коллективное принятие решений, поэтому их изучают в теории общественного выбора. В таком случае часто бывает, что аргументы взвешиваются, т. е. входят в левую часть неравенства с некоторыми множителями. Можно приводить и другие примеры важных булевых функций, но мы на этом остановимся.

[3] Всё сказанное верно только для *материальной импликации*, т. е. импликации как булевой функции. В логике рассматривают и другие виды импликации, например, *строгую* и *релевантную*, которые имеют дело и со смыслом высказываний. В некоторых книгах материальную импликацию обозначают символом $\supset$, а символ $\to$ резервируют для другого вида импликации.

[4] Возможно, было бы разумнее называть её функцией *нечётности*, но традиция уже сложилась.

2 Вычисление значений пропозициональной формулы

Напомним, что любая пропозициональная формула либо является пропозициональной переменной, либо построена из более простых формул φ и ψ по одному из правил $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$. Любая пропозициональная формула задаёт значение некоторой булевой функции. Грубо говоря, если подставить в формулу значения всех переменных и потом вычислить все операции, то получится значение этой функции на этом наборе. Более формально, значение формулы на данном наборе определяется индукцией по построению. В данном случае определение почти очевидно, но именно этот факт помогает понять механику таких определений, что поможет в дальнейшем. Будем обозначать значение формулы φ на наборе $(a_1, \ldots, a_n)$ через $[\varphi](a_1, \ldots, a_n)$.

Определение 2. Пусть $(a_1, \ldots, a_n) \in \{0,1\}^n$. Тогда $[\varphi](a_1, \ldots, a_n)$ определяется так:

- Если $\varphi \eqcirc p_i$, то $[\varphi](a_1, \ldots, a_n) = a_i$;
- Если $\varphi \eqcirc \neg\psi$, то $[\varphi](a_1, \ldots, a_n) = \mathrm{neg}([\psi](a_1, \ldots, a_n))$;
- Если $\varphi \eqcirc (\psi_1 \wedge \psi_2)$, то $[\varphi](a_1, \ldots, a_n) = \mathrm{and}([\psi_1](a_1, \ldots, a_n), [\psi_2](a_1, \ldots, a_n))$, аналогично для $(\psi_1 \vee \psi_2)$ и $(\psi_1 \to \psi_2)$.

В этом определении важно отличать знаки $\eqcirc$ и $=$. Первый из них обозначает графическое (посимвольное) равенство, а знаки $\neg$, $\wedge$, $\vee$, $\to$ в выражениях с ним выступают просто в роли символов. Второй означает алгебраическое равенство, а обозначения neg, and и т.д. выступают в роли конкретных логических функций. Например, запись $[\varphi](a_1, \ldots, a_n) = \mathrm{and}([\psi_1](a_1, \ldots, a_n), [\psi_2](a_1, \ldots, a_n))$ нужно понимать так: формулы ψ_1 и ψ_2 более короткие, их значения уже определены, теперь значение φ можно вычислить как конъюнкцию этих значений. Также важно понимать различие обозначений p_i и a_i. Первое из них обозначает переменную, символ формального языка. А второе обозначает некоторое логическое значение, 0 или 1. Все эти сложности связаны с тем, что анализ формального языка также ведётся на некотором метаязыке с использованием некоторых символов, и этот метаязык нужен для объяснения смысла изучаемых выражений на исходном языке.

Теорема 3 (Корректность определения)**.** *Определение 2 однозначно сопоставляет каждой формуле некоторую булеву функцию.*

Эта теорема тоже кажется очевидной, но мы проведём полное доказательство для иллюстрации соответствующих методов.

Доказательство. Во-первых, будем считать, что формула зависит только от тех переменных, которые в неё включены явно. Поэтому не возникает, например, вопроса, от каких переменных зависит формула $(p \wedge q)$: только от p и q, или ещё и от r. (Если бы это было не так, то для однозначности нужно было бы дополнительно указать, от каких переменных будет зависеть функция). Во-вторых, теорема об однозначности разбора позволяет доказать настоящую теорему по индукции. База индукции очевидна: каждая переменная однозначно задаёт соответствующую проекцию. Далее, по каждой формуле можно однозначно установить, из каких подформул она получена, для этих подформул однозначность сопоставления функции можно считать установленной, а значит эта однозначность верна и для всей формулы. □

Можно заметить, что без скобок не было бы не только однозначности разбора, но и однозначности вычисления функции. Например, $p \wedge q \vee r$ при $p = 0$, $q = 0$ и $r = 1$ можно было бы интерпретировать как $(0 \wedge 0) \vee 1 = 0 \vee 1 = 1$ или как $0 \wedge (0 \vee 1) = 0 \wedge 1 = 0$.

3 Задание функций пропозициональными формулами

Как мы выяснили, любой пропозициональной формуле можно однозначно сопоставить булеву функцию. Возникает вопрос, всегда ли булева функция сопоставляется какой-то формуле и, если да, то единственна ли она, и как эту формулу (или одну из этих формул) найти. Ответы на эти вопросы такие: формула есть всегда, она не единственна, находить можно по-разному, но всегда можно найти формулу в конъюнктивной и дизъюнктивной нормальных формах. Проще всего разобраться с вопросом о единственности (при условии существования).

Определение 4. Формулы называются *эквивалентными*, если они задают одну и ту же булеву функцию.

Утверждение 5. *Если некоторую подформулу заменить на эквивалентную, то формула тоже изменится на эквивалентную.*

Доказательство. Это утверждение доказывается индукцией по построению формулы. Действительно, если формулы φ и φ' эквивалентны, то $(\varphi \wedge \psi)$ и $(\varphi' \wedge \psi)$ также эквивалентны: для любого набора $(a_1, \ldots, a_n)$ выполнено $[(\varphi \wedge \psi)](a_1, \ldots, a_n) = [\varphi](a_1, \ldots, a_n) \wedge [\psi](a_1, \ldots, a_n) = [\varphi'](a_1, \ldots, a_n) \wedge [\psi](a_1, \ldots, a_n) = [(\varphi' \wedge \psi)](a_1, \ldots, a_n)$. Аналогичный переход делается для остальных операций. □

Утверждение 6. *У каждой формулы существует бесконечно много эквивалентных ей формул.*

Доказательство. Действительно, формулы p и $(p \wedge p)$ эквивалентны. Значит, любую переменную, входящую в формулу, можно заменить на её конъюнкцию с самой собой и получить более длинную формулу, эквивалентную исходной. С новой формулой можно проделать то же самое, и так бесконечное число раз. □

Разумеется, бесконечность в данном случае будет счётной, поскольку всего существует лишь счётное число формул (в случае счётного числа переменных). Однако, если хотя бы одна формула представляет данную функцию, то ту же функцию представляет счётное число других формул, так что о единственности речи быть не может. Даже если запретить трюки с дублированием переменных, возможно множество других вариантов заменить формулу на эквивалентную. Теперь перейдём к вопросу о существовании и нормальных формах.

Определение 7. *Литералом* называется переменная либо отрицание переменной.

Определение 8. *Конъюнктом* называется конъюнкция литералов. *Дизъюнктом* называется дизъюнкция литералов.

Определение 9. *Конъюнктивной нормальной формой (КНФ)* называется конъюнкция дизъюнктов. *Дизъюнктивной нормальной формой (ДНФ)* называется дизъюнкция конъюнктов.

Для конъюнкции и дизъюнкции легко доказать ассоциативность: формулы $((p \wedge q) \wedge r)$ и $(p \wedge (q \wedge r))$ эквивалентны (и представляют конъюнкцию трёх аргументов), формулы $((p \vee q) \vee r)$ и $(p \vee (q \vee r))$ также эквивалентны (и представляют дизъюнкцию трёх аргументов). Поэтому при записи КНФ и ДНФ лишние скобки опускают. Примером КНФ будет формула $(p \vee \neg q \vee r \vee \neg s) \wedge (\neg p \vee s) \wedge (p \vee q \vee \neg r)$, а примером ДНФ — формула $(\neg p \wedge q \wedge r) \vee (p \wedge \neg q) \vee (p \wedge q \wedge \neg r \wedge s)$. При рассмотрении КНФ и ДНФ мы не будем разрешать конъюнкции или дизъюнкции нуля аргументов (потому что непонятно, как их записать), но будем разрешать конъюнкции и дизъюнкции одного аргумента (это просто сам этот аргумент). Поэтому отдельный конъюнкт будет одновременно и ДНФ как дизъюнкция одного конъюнкта, и КНФ как конъюнкция дизъюнктов, в каждом из которых по одному литералу. То же можно сказать и про отдельный дизъюнкт.

Теорема 10. *Для любой булевой функции существуют выражающие её КНФ и ДНФ.*

Доказательство. Доказательство будет конструктивным: мы укажем способ построения этих формул. Сначала построим ДНФ. Каждому набору значений, на котором функция истинна, мы сопоставим конъюнкт. Если переменная в этом наборе истинна, то в конъюнкт будет включена она сама, а если ложна, то будет включено её отрицание. Итоговая ДНФ будет дизъюнкцией всех таких конъюнктов (см. рис. 3). Формально можно записать так:

$$\varphi = \bigvee_{f(a_1,\ldots,a_n)=1} \bigwedge_{i=1}^{n} p_i^{a_i},$$

где p^a обозначает литерал p, если $a = 1$, и литерал $\neg p$, если $a = 0$. Эта формула действительно выражает функцию f. Конъюнкт $\bigwedge_{i=1}^{n} p_i^{a_i}$ истинен на наборе $(a_1, \ldots, a_n)$ и ложен на всех остальных. (Если a тоже понимать как переменную, то p^a это эквиваленция). Дизъюнкция же таких конъюнктов будет истинна только на тех наборах, которым соответствует один из конъюнктов, т. е. только на тех наборах, на которых функция равна 1. Значит, ДНФ φ представляет функцию f. Осталось заметить, что вся проведённая конструкция работает только в том случае, когда f не является тождественно ложной, иначе получится пустая внешняя дизъюнкция. Однако в этом случае можно представить f как $p \wedge \neg p$.

Теперь построим КНФ. Она будет сделана по похожей схеме. Теперь каждому набору значений, на котором функция ложна, мы сопоставим дизъюнкт. Если переменная в этом наборе истинна, то в дизъюнкт будет включено её отрицание, а если ложна, то она сама. Итоговая КНФ будет конъюнкцией всех таких дизъюнктов. Формально:

$$\psi = \bigwedge_{f(a_1,\ldots,a_n)=0} \bigvee_{i=1}^{n} p_i^{1-a_i}.$$

Можно заметить, что дизъюнкт $\bigvee_{i=1}^{n} p_i^{1-a_i}$ ложен на наборе $(a_1, \ldots, a_n)$ и истинен на всех остальных. Конъюнкция таких дизъюнктов будет ложна только на тех наборах,

Рис. 3: Построение ДНФ и КНФ

p	q	r	$f(p,q,r)$	ДНФ	КНФ
0	0	0	0		$(p \vee q \vee r)\wedge$
0	0	1	0		$(p \vee q \vee \neg r)\wedge$
0	1	0	1	$(\neg p \wedge q \wedge \neg r)\vee$	
0	1	1	0		$(p \vee \neg q \vee \neg r)\wedge$
1	0	0	1	$(p \wedge \neg q \wedge \neg r)\vee$	
1	0	1	0		$(\neg p \vee q \vee \neg r)$
1	1	0	1	$(p \wedge q \wedge \neg r)\vee$	
1	1	1	1	$(p \wedge q \wedge r)$	

которым соответствует один из дизъюнктов, т. е. только на тех наборах, на которых функция равна 0. Значит, КНФ ψ представляет функцию f. Осталось заметить, что вся проведённая конструкция работает только в том случае, когда f не является тождественно истинной, иначе получится пустая внешняя конъюнкция. Однако в этом случае можно представить f как $p \vee \neg p$. □

Рассмотренный способ построения КНФ и ДНФ не самый экономный. Например, формулу $(p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r)$ можно упростить до $p \wedge r$. Однако, по этому способу получаются *совершенные* КНФ и ДНФ, т. е. содержащие ровно одно вхождение каждой переменной в каждый дизъюнкт (конъюнкт). Таким образом, теорема 10 доказывает существование совершенной ДНФ для любой функции, кроме тождественно ложной, и совершенной КНФ для любой функции, кроме тождественно истинной. Нетрудно понять, что для тождественно ложной функции СДНФ нет, а для тождественно истинной функции нет СКНФ. Ведь любой конъюнкт (дизъюнкт), в который каждая переменная входит по одному разу, истинен (ложен) ровно на одном наборе, а значит, на этом наборе истинна (ложна) и вся ДНФ (КНФ), поэтому тождественно ложной (истинной) она быть не может.

Ясно, что для каждой функции существует представляющие её наименьшие КНФ и ДНФ. Однако установить, какие именно КНФ и ДНФ самые короткие, может быть сложно. Дело в том, что нужно выбрать правильный порядок упрощений, а при неправильном можно зайти в тупик. Например, формулу $(p \wedge q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r)$ можно сократить до $(q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r)$, что уже несократимо. Но если действовать в ином порядке и вынести общие множитель из 2-й и 3-й скобок, а также из 1-й и 4-й, то получится $(\neg p \wedge r) \vee (p \wedge q)$, что гораздо короче. Задача о минимизации КНФ или ДНФ — это известная вычислительно сложная задача, для которой неизвестно общего алгоритма, работающего быстрее чем за экспоненциальное время.

4 Тавтологии и противоречия

Важное значение в логике занимают формулы, выражающие логические константы.

Определение 11. *Тавтологией* (tautology) называется формула, истинная на любом наборе значений. *Противоречием* (contradiction, absurdity) называется формула, ложная на любом наборе значений.

Определение 12. *Выполнимой* (satisfiable) называется формула, истинная хотя бы на одном наборе значений (т. е. не являющаяся противоречием). *Опровержимой* (refutable) называется формула, ложная хотя бы на одном наборе значений (т. е. не являющаяся тавтологией).[5]

Некоторые тавтологии настолько давно известны и часто используются в рассуждениях, что получили гордое звание логических законов. Перечислим некоторые из них. При этом в формулировках мы будем использовать большие буквы, подразумевая, что вместо них можно подставить не только переменные, но и произвольные подформулы. Также многие законы мы будем формулировать с использованием символа эквиваленции $\leftrightarrow$.

Закон тождества: $A \to A$. Иными словами, если некоторое утверждение истинно, то оно истинно, например «Масло масляное». Подобные суждения называют тавтологиями не только в логике, но и в обычной жизни.

Закон непротиворечия: $\neg(A \wedge \neg A)$. Ни одно утверждение не может быть одновременно истинным и ложным.

Закон исключённого третьего: $A \vee \neg A$. Третьего не дано, tertium non datur. Любое утверждение либо истинно, либо ложно. Рассуждения, основанные на этом правиле, не устраивали многих математиков первой половины XX века своей неконструктивностью. Например, можно доказать, что иррациональное число в иррациональной степени может быть рациональным. А именно, рассмотрим число $\sqrt{2}^{\sqrt{2}}$. Если оно рационально, то пример получен. Если же оно иррационально, то $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$, т. е. примером таких чисел будут $\sqrt{2}^{\sqrt{2}}$ и $\sqrt{2}$. Такое рассуждение доказывает существование искомых чисел, но не предъявляет конкретный пример.[6] Попытка отказа от закона исключённого третьего привела к построению одной из неклассических логик — интуиционистской. Эта теория оказалась полезной, но попытка перестроить всю математику на этом принципе потерпела крах.

Закон двойного отрицания: $A \leftrightarrow \neg\neg A$. Утверждение истинно тогда и только тогда, когда его отрицание ложно. В одну сторону это не вызывает сомнений: если A истинно, то $\neg A$ должно быть ложным. А вот в другую возникают те же проблемы, что и с законом исключённого третьего: если мы установили ложность $\neg A$, то для вывода об истинности A нужен этот закон. Через несколько лекций мы поймём, что эти два закона в некотором смысле эквивалентны.

[5] В английском языке есть также слово contingency, означающее формулу, которая одновременно выполнима и опровержима.

[6] На самом деле $\sqrt{2}^{\sqrt{2}}$ иррационально.

Закон контрапозиции: $(A \to B) \leftrightarrow (\neg B \to \neg A)$. Пусть B ложно. Тогда A тоже ложно, иначе A было бы истинно, и тогда B тоже было бы истинно, а оно ложно. С этим законом связаны две забавные истории. Впервые узнав об этом законе, я в нём усомнился, подставив в него фразу «Кто не рискует, тот не пьёт шампанского». Путём контрапозиции получается: «Кто пьёт шампанское, тот рискует», а этот вывод мне не понравился. На самом деле во фразе неявно предполагается порядок действий: «Кто сейчас не рискует, тот потом не будет пить шампанского». Тогда по контрапозиции получится: «Кто сейчас пьёт шампанское, тот до этого рискнул». Такой вывод из исходной фразы уже не вызывает сомнений.

Вторая история связана с применением закона контрапозиции в орнитологии. Пусть мы хотим проверить тезис «Все грачи чёрные». Непосредственная его проверка связана с поездками, организацией полевых исследований, поиском достаточного числа грачей и проверкой их цвета. Однако можно поступить проще: взять контрапозицию, т. е. утверждение «Все нечёрные объекты не являются грачами». После этого можно никуда не ездить, а походить по квартире, найти оранжевый апельсин, красный помидор, зелёное яблоко и т.п., и убедиться в том, что все эти нечёрные предметы не являются грачами. Разумеется, такое исследование ни в один орнитологический журнал не примут, но с точки зрения логики не так просто объяснить, почему.

Законы де Моргана: $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$, $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$. Отрицание конъюнкции равносильно дизъюнкции отрицаний, а отрицание дизъюнкции равносильно конъюнкции отрицаний. Например, если экзамен ставится тем, кто знает теорию и умеет решать задачи, то не сдать экзамен — то же самое, что не знать теорию или не уметь решать задачи. А если для выполнения учебного плана нужно ходить на технический курс или на гуманитарный курс по выбору, то не выполнить план — значит не ходить ни на технический, ни на гуманитарный курс.

Силлогизм: $((A \to B) \wedge (B \to C)) \to (A \to C)$. Этот приём рассуждений известен со времён Древней Греции: «Все люди смертны, Сократ — человек, следовательно Сократ смертен». Здесь A означает «быть Сократом», B — «быть человеком», C — «быть смертным». Аристотель различал много видов силлогизмов, в которые также были включены отрицания. Мы же отметим, что то же самое рассуждение можно записать несколько иной формулой: $(A \to B) \to ((B \to C) \to (A \to C))$. Здесь две посылки ($A \to B$ и $B \to C$) перестали быть равноправными, одна из них явно выделена как первая, другая как вторая. На рис. 4 проиллюстрировано *неправильное* применение силлогизма.

В курсе нам встретятся и другие тавтологии, но пока что остановимся на этих.

5 Многочлены Жегалкина

Как мы уже выяснили, среди булевых функций есть умножение (конъюнкция) и сложение (строгая дизъюнкция). Как всегда, если есть сложение и умножение, то мож-

Рис. 4: Неправильное применение силлогизма (Сидней Харрис)

но рассматривать многочлены. Специфика булевых значений даёт дополнительные соотношения: $x^2 = x$ и $x \oplus x = 0$. Это значит, что степени выше первой не нужны, и коэффициенты помимо единицы также не нужны. Это мотивирует следующее определение:

Определение 13. *Одночленом (мономом) Жегалкина* называется произведение (конъюнкция) различных переменных. *Многочленом (полиномом) Жегалкина* называется сумма различных одночленов.

При этом, как обычно, произведением нуля переменных будет считаться тождественная единица, а суммой нуля переменных будет считаться тождественный ноль. Базовые связки легко выражаются как многочлены Жегалкина:

$$\neg x = x \oplus 1;$$
$$x \wedge y = xy;$$
$$x \vee y = x \oplus y \oplus xy;$$
$$x \to y = 1 \oplus x \oplus xy;$$
$$x \leftrightarrow y = x \oplus y \oplus 1.$$

Многочлены Жегалкина можно считать ещё одной нормальной формой, потому что любую функцию можно так выразить. Правда, это не будет формула в нашем исходном понимании, потому что будет использована связка $\oplus$. Впрочем, ясно, что исходный выбор конъюнкции, дизъюнкции и импликации в качестве базовых связок был достаточно произвольным, и по сути ничего не изменится, если рассмотреть вместо этого

конъюнкцию и строгую дизъюнкцию (также нужно добавить тождественную единицу для выражения соответствующего монома).

Прежде чем доказывать теорему, заметим, что многочлены можно складывать и умножать. При этом результат получается обычным символьным сложением и умножением с учётом соотношений $x^2 = x$ и $x \oplus x = 0$ (где x может быть переменной или более сложным выражением). Для сложения можно заметить следующий факт: сумма многочленов P и Q включает в себя те и только те одночлены, которые встречаются ровно в одном из многочленов P и Q, т. е. сложение работает как симметрическая разность. Также можно заметить, что вычитание и сложение суть одно и то же, поскольку все вычисления проходят по модулю 2. Перейдём к основной теоерме.

Теорема 14 (о многочленах Жегалкина)**.** *Любую булеву функцию можно выразить многочленом Жегалкина, причём единственным образом с точностью до порядка слагаемых и множителей.*

Доказательство. Вначале посчитаем количество многочленов Жегалкина от n переменных. Общее количество одночленов будет равно 2^n, т. к. каждая переменная может входить или не входить в одночлен. Общее количество многочленов равно 2^{2^n}, поскольку каждый из 2^n одночленов может входить или не входить в сумму. Таким образом, многочленов столько же, сколько и булевых функций. Поскольку каждому многочлену однозначно соответствует некоторая функция, для доказательства однозначности соответствия в обратную сторону достаточно доказать одно из двух: либо что каждой функции соответствует какой-то многочлен, либо что разным многочленам соответствуют разные функции. Для полноты мы докажем оба утверждения.

Первое утверждение основано на выражении отрицания, конъюнкции и дизъюнкции. Можно взять КНФ (или ДНФ), выразить все входящие связки через многочлены, раскрыть скобки, сократить старшие степени и привести подобные слагаемые.

Второе утверждение доказывается от противного. Пусть P и Q суть разные многочлены, но $P(a) = Q(a)$ на любом наборе $a \in \{0,1\}^n$. Тогда рассмотрим разность (она же сумма) $P - Q = P \oplus Q$. Поскольку $P \neq Q$, верно $P \oplus Q \neq 0$. При этом $(P \oplus Q)(a) = P(a) \oplus Q(a) = 0$ для любого a. Иными словами, мы получили ненулевой (т. е. непустой) многочлен S, значение которого равно нулю во всех точках. Докажем, что такого не может быть.

Действительно, S является суммой каких-то одночленов. Выберем среди них одночлен с минимальным количеством переменных (если таких несколько, то любой из них). Без ограничения общности это будет одночлен $x_1 \dots x_k$. Тогда все остальные одночлены, входящие в S, содержат хотя бы одну переменную x_i для $i > k$. Теперь рассмотрим набор $a = (\underbrace{1, \dots, 1}_{k \text{ штук}}, \underbrace{0, \dots, 0}_{n-k \text{ штук}})$. На этом наборе одночлен $x_1 \dots x_k$ будет равен единице, а все остальные одночлены, входящие в S, равны нулю, т. к. содержат какие-то переменные x_i для $i > k$. Значит, на этом наборе S равен единице, что противоречит тому, что он на всех наборах равен нулю. Полученное противоречие показывает, что разным многочленам соответствуют разные функции, откуда в силу равного количества функций и многочленов каждой функции однозначно соответствует многочлен. □

В процессе доказательства теоремы мы получили конкретный способ построения многочлена: привести формулу к нормальной форме, заменить все связки в ней на

соответствующие многочлены, раскрыть все скобки и привести подобные слагаемые. Однако этот способ не самый удобный, познакомимся с некоторыми другими.

Метод неопределённых коэффициентов. Покажем работу метода на примере функции от 3 переменных. На большем числе переменных он работает аналогично. Пусть $m(p,q,r) = a \oplus bp \oplus cq \oplus dr \oplus epq \oplus fqr \oplus gpr \oplus hpqr$. Тогда, подставив все нули, получаем $m(0,0,0) = a$, что сразу даёт один из коэффициентов. Далее, подставляя наборы с одной единицей, получаем равенства вида $m(1,0,0) = a \oplus b$, откуда с учётом уже найденного a получаем $b = m(1,0,0) \oplus a = m(1,0,0) \oplus m(0,0,0)$, аналогично получаем c и d. Далее получаем $m(1,1,0) = a \oplus b \oplus c \oplus e$, откуда находим e, и т. д. Конкретные формулы показаны на рис. 5.

Рис. 5: Коэффициенты в многочлене Жегалкина.

p	q	r	$m(p,q,r)$	одночлен	коэффициент
0	0	0	m_0	1	m_0
0	0	1	m_1	r	$m_0 \oplus m_1$
0	1	0	m_2	q	$m_0 \oplus m_2$
0	1	1	m_3	qr	$m_0 \oplus m_1 \oplus m_2 \oplus m_3$
1	0	0	m_4	p	$m_0 \oplus m_4$
1	0	1	m_5	pr	$m_0 \oplus m_1 \oplus m_4 \oplus m_5$
1	1	0	m_6	pq	$m_0 \oplus m_2 \oplus m_4 \oplus m_6$
1	1	1	m_7	pqr	$m_0 \oplus m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \oplus m_7$

Легко заметить закономерность: с каждой строкой таблицы истинности связан одночлен, состоящий из переменных, которые в этой строке равны единице. А коэффициент при этом одночлене равен сумме значений функции во всех строках, соответствующих делителям этого одночлена. Например, коэффициент при pr получен как сумма значений в строках, соответствующих 1, p, r и pr. Такое правило можно считать отдельным методом и доказывать индуктивно.

Метод суммирования. Переформулируем полученное нами правило в терминах строк таблицы истинности.

Теорема 15. *Для подсчёта коэффициента при некотором одночлене нужно рассмотреть значения во всех строках таблицы истинности, где переменные, отсутствующие в этом одночлене, равны нулю, а присутствующие могут быть равны как нулю, так и единице. Сумма всех этих коэффициентов и будет равна коэффициенту при одночлене.*

Доказательство. Будем доказывать теорему индукцией по числу переменных. Для многочленов от одной переменной её можно проверить непосредственно (и даже для трёх мы уже проверили). Покажем, как переходить от n переменных к $n+1$. При подстановке $p_1 = 0$ получаем, с одной стороны, многочлен, состоящий из одночленов только

от $p_2, \ldots, p_{n+1}$, входящих в исходный многочлен, с другой стороны, функцию, заданную верхней половиной таблицы истинности. По предположению индукции коэффициенты при этих одночленах задаются указанными суммами, и те же самые формулы подойдут и при добавлении p_1. Например, коэффициент при q задаётся формулой $m_0 \oplus m_2$ для многочлена от q и r, он должен быть тем же самым для многочлена от p, q и r, и формула по правилу получается той же.

Теперь подставим $p_1 = 1$. С одной стороны, получится функция от $p_2, \ldots, p_{n+1}$, заданная нижней половиной таблицы истинности. С другой стороны, в многочлене для этой функции будут только такие одночлены Q, что из Q и p_1Q в исходном многочлене есть ровно один одночлен. Иными словами, коэффициент при Q в многочлене для функции при $p_1 = 1$ будет суммой коэффициентов при Q и p_1Q в исходном многочлене. Перенося в другую часть, получаем, что коэффициент при p_1Q в исходном многочлене будет суммой коэффициентов при Q в исходном многочлене и полученном при фиксации $p_1 = 1$. Или, что то же самое, суммой коэффициентах при Q в многочленах, полученных фиксацией $p_1 = 0$ и $p_1 = 1$. Теперь видно, что в первой части будут значения в строках, где $p_1 = 0$, а во второй — в строках, где $p_1 = 1$, а в остальном эти строки соответствуют правилу. Например, посчитаем коэффициент при pq. Коэффициент при q при $p = 0$ задаётся суммой $m_0 \oplus m_2$, а при $p = 1$ — суммой $m_4 \oplus m_6$. Поэтому общий коэффициент при pq задаётся суммой $m_0 \oplus m_2 \oplus m_4 \oplus m_6$, что соответствует полученному ранее. □

Метод БПФ. Итак, мы получилиформулы для всех коэффициентов многочлена Жегалкина. Но как их быстро вычислить? Есть несколько способов, мы разберём один из них. В некоторых источниках он называется методом Паскаля, но это не очень логично: методом Паскаля следует называть метод, использующий треугольник Паскаля. Так что мы назовём его методом БПФ (быстрого преобразования Фурье), не раскрывая подробно смысл такого названия.

Теорема 16. *Коэффициенты при одночленах в многочлене Жегалкина можно получить следующим образом: сначала взять значения в таблице истинности, упорядоченные стандартным образом. Затем для $k = 0, \ldots, n-1$ произвести следующее: к значениям во всех строках с номерами $a \cdot 2^{k+1} + 2^k + b$, где $a = 0, \ldots, 2^{n-k-1} - 1$, $b = 0, \ldots, 2^k - 1$ прибавить значения строк с номерами $a \cdot 2^{k+1} + b$.*

Например, при $n = 3$ нужно сначала ($k = 0$, $a = 0, 1, 2, 3$, $b = 0$) прибавить к 1-й строке 0-ю, к 3-й 2-ю, к 5-й 4-ю и к 7-й 6-ю. Затем ($k = 1$, $a = 0, 1$, $b = 0, 1$) нужно ко 2-й строке прибавить 0-ю, к 3-й 1-ю, к 6-й 4-ю, к 7-й 5-ю. Наконец ($k = 2$, $a = 0$, $b = 0, 1, 2, 3$) нужно прибавить к 4-й строке 0-ю, к 5-й 1-ю, к 6-й 2-ю, к 7-й 3-ю. См. последовательно получаемые формулы на рис. 6 и графическую схему на рис. 7.

Доказательство. Будем доказывать корректность указанной процедуры по индукции. База у нас уже есть, так что докажем, что если указанная процедура работает для n, то работает и для $n + 1$. Заметим, что

$$m(p_1; p_2, \ldots, p_{n+1}) = p_1 m(1; p_2, \ldots, p_{n+1}) + (1 - p_1) m(0; p_2, \ldots, p_{n+1}) :$$

Рис. 6: Вычисление коэффициентов в многочлене Жегалкина методом БПФ: формулы.

p	q	r	$m(p,q,r)$	одночлен	первый этап	второй этап	итог
0	0	0	m_0	1	m_0	m_0	m_0
0	0	1	m_1	r	$m_0 \oplus m_1$	$m_0 \oplus m_1$	$m_0 \oplus m_1$
0	1	0	m_2	q	m_2	$m_0 \oplus m_2$	$m_0 \oplus m_2$
0	1	1	m_3	qr	$m_2 \oplus m_3$	$m_0 \oplus m_1 \oplus m_2 \oplus m_3$	$m_0 \oplus m_1 \oplus m_2 \oplus m_3$
1	0	0	m_4	p	m_4	m_4	$m_0 \oplus m_4$
1	0	1	m_5	pr	$m_4 \oplus m_5$	$m_4 \oplus m_5$	$m_0 \oplus m_1 \oplus m_4 \oplus m_5$
1	1	0	m_6	pq	m_6	$m_4 \oplus m_6$	$m_0 \oplus m_2 \oplus m_4 \oplus m_6$
1	1	1	m_7	pqr	$m_6 \oplus m_7$	$m_4 \oplus m_5 \oplus m_6 \oplus m_7$	$m_0 \oplus m_1 \oplus m_2 \oplus m_3 \oplus$ $m_4 \oplus m_5 \oplus m_6 \oplus m_7$

это проверяется непосредственной подстановкой $p_1 = 1$ и $p_1 = 0$ в обе части формулы. Учитывая, что вычитание и сумма по модулю 2 это одно и то же, после преобразования получаем

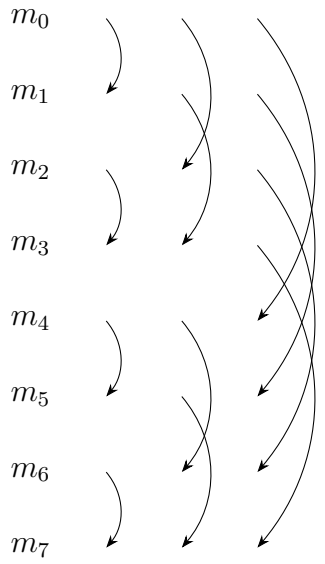
$$m(p_1; p_2, \ldots, p_{n+1}) = m(0; p_2, \ldots, p_{n+1}) \oplus p_1(m(0; p_2, \ldots, p_{n+1}) \oplus m(1; p_2, \ldots, p_{n+1})). \quad (1)$$

Коэффициенты для одночленов в представлении $m(0; p_2, \ldots, p_{n+1})$ по предположению индукции уже получены нашей процедурой для верхней половины таблицы истинности для m. Они же будут коэффициентами для одночленов m, не содержащих p_1, и наша процедура их менять не будет, значит, ответ получится правильным. Аналогично, коэффициенты для одночленов в представлении $m(1; p_2, \ldots, p_{n+1})$ получены нашей процедурой для нижней половины таблицы истинности m. Коэффициент при $p_1 Q$ согласно (1) будет суммой коэффициентов при Q в $m(0; p_2, \ldots, p_{n+1})$ и $m(1; p_2, \ldots, p_{n+1})$ и именно так будет посчитан в последнем шаге нашей процедуры. □

6 Полные и неполные системы булевых функций

Обсудим подробнее, что будет если вместо $\neg$, $\wedge$, $\vee$ и $\to$ выбрать другую систему базовых функций. Прежде всего, можно определить формулы, зависящие от символов $(f_1, \ldots, f_k)$, где символ f_i обозначает некоторую булеву функцию от n_i аргументов. Тогда любая переменная будет формулой, а если $\varphi_1, \ldots, \varphi_{n_i}$ суть формулы, то $f_i(\varphi_1, \ldots, \varphi_{n_i})$ тоже формула. При этом действуют обычные соглашения: если $n_i = 2$, то символ операции пишут между φ_1 и φ_2, а вокруг ставят скобки, если $n_i = 0$, т. е. f_i есть логическая константа, то скобок вообще не ставят, а из функций с $n_i = 1$ фактически остаётся только отрицание, которое ставится перед формулой также без скобок. Иными словами, мы берём всевозможные композиции (суперпозиции) функций из заданного набора. Для построенных этим способом формул можно доказать теорему об однозначности разбора и однозначно определить вычисляемую ими функцию. Основной вопрос заключается в следующем: какие функции можно выразить через заданный набор базовых? В частности, через какие наборы можно выразить любую функцию?

Рис. 7: Вычисление коэффициентов в многочлене Жегалкина методом БПФ: схема.



Нетрудно понять, что для любого заданного набора класс всех функций, через него выражаемых, будет замкнутым относительно композиции. Действительно, композицию уже выраженных функций тоже можно выразить. Оказывается, все такие классы можно полностью описать. Это сделал американский математик Эмиль Пост, создавший классификацию, ныне известную как решётка Поста. Мы изучим наиболее важную её часть и докажем критерий полноты набора булевых функций.

Мы уже знаем, что при помощи КНФ или ДНФ можно выразить любую функцию через $\neg$, $\wedge$ и $\vee$. Законы де Моргана позволяют избавиться либо от дизъюнкции и выразить всё через $\neg$ и $\wedge$, либо от конъюнкции и выразить всё через $\neg$ и $\vee$. Использовав тождество $p \vee q = \neg p \to q$, можно всё выразить и через импликацию и отрицание. А использовав соотношение $\neg p = p \to \mathbf{0}$ — через импликацию и тождественную ложь. Многочлены Жегалкина позволяют выразить все функции через $\wedge$, $\oplus$ и $\mathbf{1}$. (Константа $\mathbf{1}$ — это конъюнкция нуля переменных, но у нас нет синтаксических средств записать её только через $\wedge$. Кроме того, конъюнкция нуля переменных не будет подпадать под определение композиции. А вот константу $\mathbf{0}$ можно выразить как $p \oplus p$). С другой стороны, с использованием только $\wedge$, $\vee$ и $\to$ (без $\neg$) нельзя выразить все функции, поскольку при подстановке в формулу только из этих связок единиц вместо всех переменных будет получаться единица. Это свойство называется сохранением единицы и будет одним из препятствий к полноте системы, которые мы перечислим в критерии Поста. Другим препятствием будет сохранение нуля: поэтому нельзя всё выразить через $\wedge$, $\vee$ и $\oplus$. Всего таких препятствий будет пять. Перейдём к последовательному изложению теории.

Определение 17. Пусть $f\colon \{0,1\}^n \to \{0,1\}$, $g_1\colon \{0,1\}^{k_1} \to \{0,1\}$, $\ldots$, $g_n\colon \{0,1\}^{k_n} \to \{0,1\}$ суть булевы функции. Тогда их *композицией (суперпозицией)* называется функция $h\colon \{0,1\}^m \to \{0,1\}$, определённая равенством

$$h(x_1, \ldots, x_m) = f(g_1(x_{i_{11}}, \ldots, x_{i_{1k_1}}), \ldots, g_n(x_{i_{n1}}, \ldots, x_{i_{nk_n}}))$$

для некоторых наборов индексов $(i_{11}, \ldots, i_{1k_1}), \ldots, (i_{n1}, \ldots, i_{nk_n})$.

Определение 18. Пусть дан класс (множество) булевых функций Q. Тогда *замыканием* класса Q называется класс $[Q]$, составленный из всех композиций любого уровня вложенности функций из класса Q. Под композицией n-го уровня вложенности мы понимаем следующее:

- Для $n = 0$ — все *проекторы*, т. е. функции вида $\mathrm{pr}_i(x_1, \ldots, x_k) = x_i$.
- Для $n > 0$ — любую композицию функции из класса Q и композиций функций из класса Q уровня вложенности не больше $n - 1$.[7]

Нетрудно понять, что композиции первого уровня вложенности — это сами функции из класса Q (применённые к любым переменным), а композиции второго уровня вложенности — их композиции в обычном смысле. Также видно, что определение согласовано с итеративным построением формул: проекторы соответствуют переменным, а более сложные композиции — связкам, применённым к уже построенным формулам.

Прямо из определения можно вывести, что для любых классов Q и R верно $Q \subset [Q]$, $[[Q]] = [Q]$ и если $Q \subset R$, то $[Q] \subset [R]$.

Определение 19. Класс булевых функций Q называется *замкнутым*, если $Q = [Q]$. Класс функций Q называется *полным*, если $[Q]$ есть множество всех булевых функций.

Иначе говоря, класс Q замкнут, если он содержит все проекторы и из того, что функции f, g_1, …, g_n лежат в классе Q, следует, что функция h из определения 17 тоже лежит в Q.

Утверждение 20. *Если классы Q и R замкнуты, то класс $Q \cap R$ тоже замкнут.*

Доказательство. Действительно, если функции f, g_1, …, g_n лежат и в классе Q, и в классе R, то их композиция h тоже лежит и в Q, и в R, поскольку оба класса замкнуты. □

Эмиль Пост полностью перечислил все замкнутые классы и доказал, что они образуют решётку по включению (см. рис. 8). Мы не будем анализировать решётку целиком, перечислим только классы, нужные для критерия полноты системы.

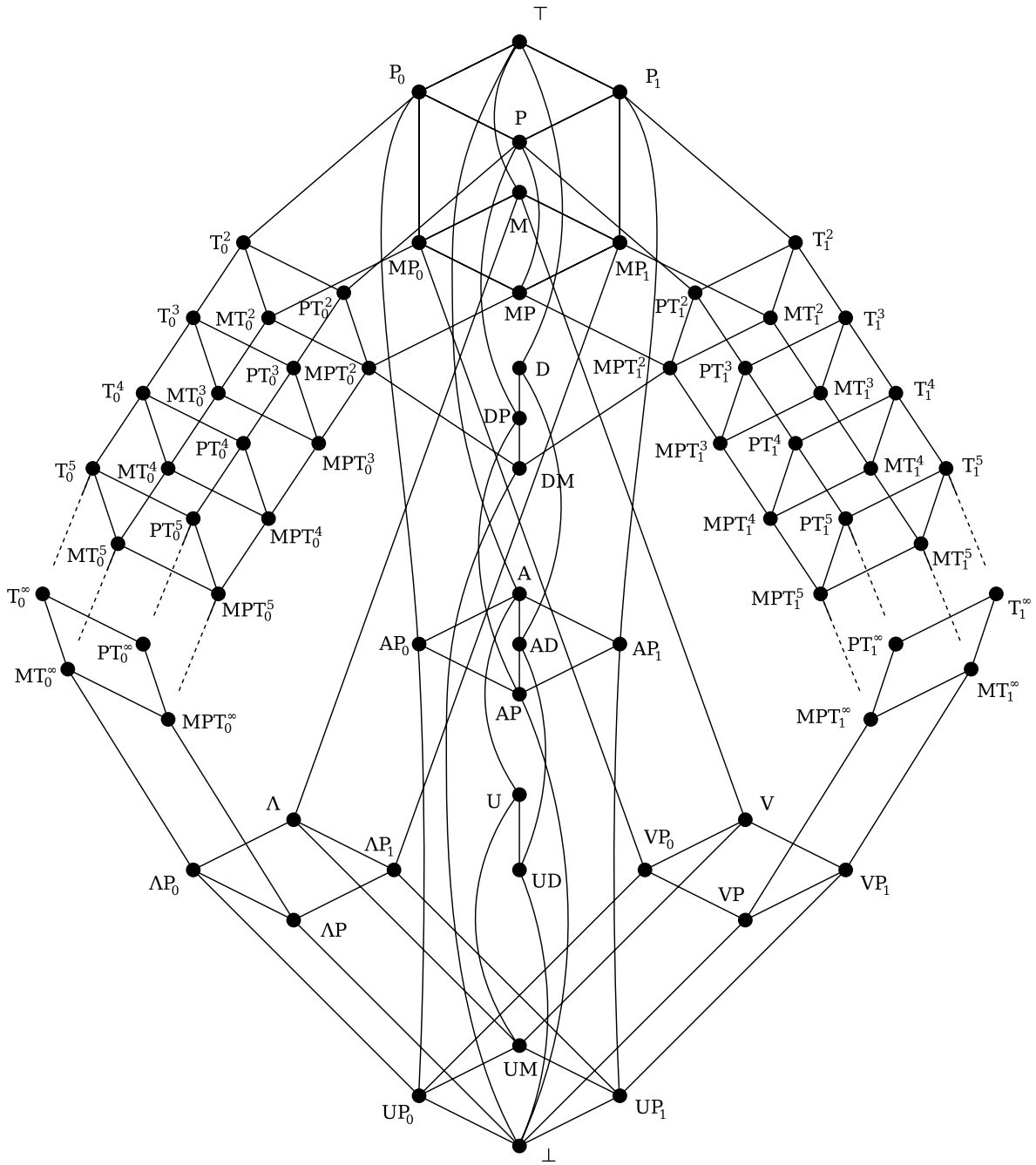
Определение 21. Функция f называется *сохраняющей единицу*, если $f(1, \ldots, 1) = 1$. Класс всех функций, сохраняющих единицу, будем обозначать через P_1.

Например, сохраняют единицу $\mathbf{1}$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$ и т. д. Не сохраняют единицу $\neg$, $\oplus$ и др.

Лемма 22. *Класс P_1 является замкнутым.*

[7] По такому определению композиция уровня n также будет композицией и всех бóльших уровней. Если надо избежать такоего эффекта, нужно требовать, чтобы все задействованные композиции были уровня не больше $n - 1$, а какая-то — уровня ровно $n - 1$.

Рис. 8: Решётка Поста (Автор диаграммы — Эмиль Йержабек, институт математики Чешской Академии наук). Здесь линейные функции обозначены буквой A — аффинные.



Доказательство. Действительно,

$$h(1,\dots,1) = f(g_1(1,\dots,1),\dots,g_n(1,\dots,1)) = f(1,\dots,1) = 1.$$

□

Аналогично определяется класс P_0 функций, сохраняющих 0, и доказывается, что он замкнут. Класс P_0 содержит $\mathbf{0}$, $\wedge$, $\vee$, $\oplus$, но не содержит $\neg$, $\to$, $\leftrightarrow$.

Определение 23. Функция f называется *монотонной*, если при всех $x_1 \leqslant y_1$, …, $x_n \leqslant y_n$ выполнено $f(x_1,\dots,x_n) \leqslant f(y_1,\dots,y_n)$. Класс всех монотонных функций будем обозначать за M.

Например, монотонными будут $\wedge$, $\vee$ и maj, немонотонными — $\neg$, $\to$, $\oplus$.

Лемма 24. *Класс M является замкнутым.*

Доказательство. Действительно, если $x_1 \leqslant y_1,\dots,x_m \leqslant y_m$, то $g_1(x_{i_{11}},\dots,x_{i_{1k_1}}) \leqslant g_1(y_{i_{11}},\dots,y_{i_{1k_1}}),\dots,g_n(x_{i_{n1}},\dots,x_{i_{nk_n}}) \leqslant g_n(y_{i_{n1}},\dots,y_{i_{nk_n}})$, а значит,

$$f(g_1(x_{i_{11}},\dots,x_{i_{1k_1}}),\dots,g_n(x_{i_{n1}},\dots,x_{i_{nk_n}})) \leqslant f(g_1(y_{i_{11}},\dots,y_{i_{1k_1}}),\dots,g_n(y_{i_{n1}},\dots,y_{i_{nk_n}})),$$

т. е. $h(x_1,\dots,x_m) \leqslant h(y_1,\dots,y_m)$, что и требовалось. □

Нам потребуется следующая эквивалентная характеризация класса монотонных функций.

Утверждение 25. *Функция f монотонна тогда и только тогда, когда при всех i, при всех $x_1,\dots,x_{i-1},x_i \leqslant y_i,x_{i+1},\dots,x_n$ выполнено $f(x_1,\dots,x_n) \leqslant f(y_1,\dots,y_n)$.*

Доказательство. Указанное свойство является частным случаем свойства монотонности, поэтому достаточно провести рассуждение в обратную сторону. Предположим, что f не монотонна. Тогда найдутся $x_1 \leqslant y_1$, …, $x_n \leqslant y_n$, такие что $f(x_1,\dots,x_n) > f(y_1,\dots,y_n)$, т. е. $f(x_1,\dots,x_n) = 1$, $f(y_1,\dots,y_n) = 0$. Далее используем т.н. «гибридное» рассуждение: рассмотрим ряд $f(x_1,\dots,x_n)$, $f(y_1,x_2,\dots,x_n)$, …, $f(y_1,\dots,y_{n+1},x_n)$, $f(y_1,\dots,y_n)$. Этот ряд начинается с единицы и заканчивается нулём, значит на каком-то шаге случится переход с единицы на ноль. Это будет означать нарушение свойства. Значит, если свойство выполнено, то функция монотонна, что и требовалось. □

Можно проиллюстрировать это рассуждение такой метафорой: пусть имеется комната с n выключателями и одной люстрой. Монотонность означает, что если включить некоторые выключатели при горящей люстре, то свет останется гореть. А немонотонность — что можно так включить некоторые выключатели, чтобы свет выключился. Если начать их включать по одному, то в какой-то момент свет выключится от включения одного выключателя.

Определение 26. *Двойственной функцией* к функции f называется функция f^*, определённая равенством $f^*(x_1,\dots,x_n) = \neg f(\neg x_1,\dots,\neg x_n)$.

Например, в силу законов де Моргана $\wedge$ и $\vee$ будут двойственны друг другу, а в силу закона контрапозиции будут двойственны импликация $p \to q$ и отрицание импликации $q \not\to p$. Двойственность можно распространить и на классы функций: $K^* = \{f^* \mid f \in K\}$. Например, двойственными будут классы P_0 и P_1. Нетрудно заметить справедливость следующих свойств:

Утверждение 27. *Для любой функции f и любых классов K и L выполнено:*

- $(f^*)^* = f$, $(K^*)^* = K$;
- *Если $K \subset L$, то $K^* \subset L^*$;*
- *Если $K = [L]$, то $K^* = [L^*]$.*

Определение 28. Функция f называется *самодвойственной*, если $f = f^*$. Иными словами, $f(\neg x_1, \ldots, \neg x_n) = \neg f(x_1, \ldots, x_n)$. Класс всех самодвойственных функций будем обозначать через D.

Самодвойственными будут, например, $\neg$ и maj, несамодвойственными — $\wedge$, $\vee$, $\to$. Можно заметить, что свойство самодвойственности похоже на свойство нечётности функций действительного аргумента, только отрицание понимается не арифметически, а логически.

Лемма 29. *Класс D является замкнутым.*

Доказательство. Действительно,

$$\begin{aligned} h(\neg x_1, \ldots, \neg x_m) = \\ &= f(g_1(\neg x_{i_{11}}, \ldots, \neg x_{i_{1k_1}}), \ldots, g_n(\neg x_{i_{n1}}, \ldots, \neg x_{i_{nk_n}})) = \\ &= f(\neg g_1(x_{i_{11}}, \ldots, x_{i_{1k_1}}), \ldots, \neg g_n(x_{i_{n1}}, \ldots, x_{i_{nk_n}})) = \\ &= \neg f(g_1(x_{i_{11}}, \ldots, x_{i_{1k_1}}), \ldots, g_n(x_{i_{n1}}, \ldots, x_{i_{nk_n}})) = \\ &= \neg h(x_1, \ldots, x_m). \end{aligned}$$

□

Определение 30. Функция f называется *линейной*, если она представляется линейным многочленом Жегалкина, т. е. представляется суммой некоторых переменных и, возможно, единицы. Класс линейных функций будем обозначать через L.

Замечание 31. Некоторые источники называют такие функции *аффинными*, а линейными называют только те, где в сумме нет единицы. Соответственно, класс в таком случае обозначается через A, как на рис. 8.

Например, линейными будут $\neg$ и $\leftrightarrow$, т. к. $\neg x = x \oplus 1$ и $x \leftrightarrow y = x \oplus y \oplus 1$, а нелинейными будут $\wedge$ и $\vee$, т. к. $x \wedge y = xy$ и $x \vee y = xy \oplus x \oplus y$.

Лемма 32. *Класс L является замкнутым.*

Доказательство. Действительно, если в сумме переменных и, возможно, единицы, все переменные заменить на подобные суммы, то после сокращений останется подобная сумма. □

Наконец, всё готово к формулировке и доказательству основной теоремы:

Теорема 33 (Критерий Поста)**.** *Класс K является полным тогда и только тогда, когда он не вложен целиком ни в один из классов P_0, P_1, M, D и L. Иными словами, класс полон тогда и только тогда, когда он содержит некоторую функцию, не сохраняющую ноль, некоторую функцию, не сохраняющую единицу, некоторую немонотонную функцию, некоторую несамодвойственную функцию и некоторую нелинейную функцию.*

Заметим, что одна и та же функция может обладать сразу несколькими свойствами, и даже сразу всеми.

Доказательство. Если класс K целиком входит в один из перечисленных замкнутых классов, то и его замыкание входит в этот же замкнутый класс. Поскольку ни один из этих классов не совпадает с множеством всех функций, то K не может быть полным.

Теперь предположим, что класс K содержит функцию f_0, не сохраняющую ноль, f_1, не сохранающую единицу, немонотонную функцию g, несамодвойственную функцию h и нелинейную функцию k (некоторые из этих функций могут совпадать, но мы будем придерживаться различных обозначений). Мы последовательно выразим через эти функции логические константы, отрицание и конъюнкцию, из чего будет следовать полнота, т. к. отрицание и конъюнкция образуют полную систему.

Поскольку f_0 не сохраняет ноль, то $f_0(0,0,\dots,0) = 1$. Если и $f_0(1,1,\dots,1) = 1$, то $f_0(p,p,\dots,p) = \mathbf{1}$, т. е. мы выразили тождественную единицу. Если же $f_0(1,1,\dots,1) = 0$, то $f_0(p,p,\dots,p) = \neg p$, т. е. мы выразили отрицание. Аналогично, $f_1(p,p,\dots,p)$ есть либо тождественный ноль, либо отрицание. Таким образом, через f_0 и f_1 можно выразить либо обе константы, либо отрицание и, возможно, одну из констант. Если выражены и отрицание, и одна из констант, то можно выразить и вторую (например, $\mathbf{1} = \neg\mathbf{0}$). Покажем, что если есть только константы или только отрицание, то оставшиеся функции также можно выразить с помощью g или h.

Пусть имеются $\mathbf{0}$, $\mathbf{1}$ и немонотонная функция g. В силу утверждения 25 для некоторого i и некоторых $x_1,\dots,x_{i-1},x_{i+1},\dots,x_n$ выполнено $g(x_1,\dots,x_{i-1},0,x_{i+1},\dots,x_n) = 1$ и $g(x_1,\dots,x_{i-1},1,x_{i+1},\dots,x_n) = 0$. В таком случае $g(x_1,\dots,x_{i-1},p,x_{i+1},\dots,x_n) = \neg p$, т. е. отрицание можно выразить через константы x_j и g.

Пусть имеются отрицание и несамодвойственная функция h. Тогда для некоторых $x_1,\dots,x_n$ выполнено $h(x_1,\dots,x_n) = h(\neg x_1,\dots,\neg x_n)$. Напомним, что через p^x обозначается литерал p, если $x = 1$, и литерал $\neg p$, если $x = 0$. Заметим, что выражение p^x, рассмотренное как функция двух аргументов, есть эквиваленция, поэтому $p^x = x^p$. Поэтому значение $h(p^{x_1},\dots,p^{x_n})$ совпадает с $h(x_1,\dots,x_n)$ при $p = 1$ и с $h(\neg x_1,\dots,\neg x_n)$ при $p = 0$. Значит, $h(p^{x_1},\dots,p^{x_n})$ является логической константой. Теперь при помощи отрицания можно выразить и другую константу. Например, если $h(1,0,1,1,1,0) = h(0,1,0,0,0,1) = 1$, то $h(p,\neg p,p,p,p,\neg p)$ выражает $\mathbf{1}$.

Наконец, пусть имеются $\mathbf{0}$, $\mathbf{1}$, $\neg$ и нелинейная функция k. Без ограничения общности можно считать, что многочлен Жегалкина для k содержит одночлен, включающий

переменные x_1 и x_2. В таком случае можно представить k в виде $x_1x_2P(x_3,\dots,x_n) \oplus x_1Q(x_3,\dots,x_n) \oplus x_2R(x_3,\dots,x_n) \oplus S(x_3,\dots,x_n)$, при этом $P \neq 0$. В силу теоремы о многочленах Жегалкина для некоторого набора $(a_3,\dots,a_n)$ верно $P(a_3,\dots,a_n) = 1$. Поскольку логические константы уже получены, можно выразить функцию $\bar{k}(x_1,x_2) = k(x_1,x_2,a_3,\dots,a_n) = x_1x_2 \oplus x_1\overline{Q} \oplus x_2\overline{R} \oplus \overline{S}$ для некоторых булевых значений $\overline{Q}$, $\overline{R}$, $\overline{S}$.

Осталось перебрать несколько случаев. Если $\overline{Q} = \overline{R} = 0$, то $\bar{k}$ есть либо конъюнкция, либо штрих Шеффера. В любом случае вместе с отрицанием получится полная система. Если $\overline{Q} = \overline{R} = 1$, то $\bar{k}$ есть либо дизъюнкция, либо стрелка Пирса, т. е. система также будет полной. Если же $\overline{Q} = 1$ и $\overline{R} = 0$, то $\bar{k}$ есть либо импликация, либо отрицание импликации. Система снова получается полной. Случай $\overline{Q} = 1$ и $\overline{R} = 0$ аналогичен.

Итак, в любом случае мы выразили некоторую полную систему, а значит, и изначальная система была полной. □

Помимо полных и неполных систем рассматривают базисные системы для отдельных классов.

Определение 34. Множество S является базисом класса Q, если $Q = [S]$, но $Q \neq [S']$ для $S' \subsetneq S$.

Иными словами, любую функцию из класса Q можно выразить через базис, но ни одну из функций базиса нельзя выразить через остальные. Из критерия Поста вытекает, что любой базис всех функций состоит не более, чем из 5 функций. Из доказательства видно, что достаточно лишь четырёх функций (мы использовали либо немонотонную, либо несамодвойственную), но можно эту теорему доказать и непосредственно.

Теорема 35. *В любом базисе класса всех функций содержится не больше 4 функций.*

Доказательство. Рассмотрим базисную функцию f, которая не сохраняет ноль. Имеем $f(0,0,\dots,0) = 1$. Если в какой-то точке функция равна нулю, то она немонотонна. Если же она всюду равна единице, то она несамодвойственна. Значит, эта функция лежит в дополнении сразу двух классов, и нам достаточно взять ещё три функции, чтобы получить полную систему. □

Для всех чисел от 1 до 4, примеры базисов существуют. Базисом из одной функции будет, например, штрих Шеффера. Базисами из двух функций будут $\{\neg,\wedge\}$, $\{\neg,\vee\}$, $\{\neg,\to\}$ и пр. Базисом из трёх функций будет $\{1,\oplus,\wedge\}$. Примером базиса из 4 функций является $\{0,1,\wedge,\oplus_3\}$, где $\oplus_3(p,q,r) = p \oplus q \oplus r$. Действительно, все функции, кроме 0, сохраняют единицу, все функции, кроме 1, сохраняют ноль, все функции, кроме $\wedge$, линейны и все функции, кроме $\oplus_3$, монотонны, поэтому ни одну функцию исключить нельзя.

Для примера докажем теорему о базисе одного конкретного класса.

Теорема 36. *Любую монотонную функцию можно выразить через* $0,1,\wedge,\vee$.

Доказательство. Поскольку 0 и 1 уже даны, будем выражать неконстантную монотонную функцию f. Раз она монотонна и не константа, то $f(0,0,\dots,0) = 0$ и $f(1,1,\dots,1) = 1$. Будем говорить, что $\mathbf{x} > \mathbf{y}$, если $x_j \geqslant y_j$ при всех j и $x_i > y_i$ при некотором i. Назовём набор минимальным, если $f(\mathbf{x}) = 1$, но $f(\mathbf{y}) = 0$ при всех $\mathbf{y} < \mathbf{x}$. Заметим, что

для любого набора, на котором функция равна единице, существует не больший его минимальный набор: если можно заменить какую-то единицу на ноль, сохранив значение функции, сделаем это, иначе набор минимальный. Рано или поздно минимальный найдётся, т. к. $f(0,0,\ldots,0) = 0$. Также заметим, что в силу монотонности на любом наборе, большем минимального, функция равна 1.

По каждому минимальному набору можно построить конъюнкт, состоящий из всех переменных, которые равны единице в этом наборе. Дизъюнкция таких конъюнктов как раз выражает функцию. Действительно, если функция на некотором наборе равна 1, то найдётся не больший его минимальный, соответствующий конъюнкт будет истинным, а значит, истинна и вся ДНФ. Обратно, если на некотором наборе истинна ДНФ, то истинен хотя бы один конъюнкт, значит на соответствующем минимальном наборе функция равна 1, а значит и на исходном наборе функция равна 1. Таким образом, ДНФ действительно выражает функцию.

Обсудим, зачем мы потребовали, чтобы функция не была равна константе. Если бы она была равна нулю, то не было бы ни одного минимального набора, и ДНФ построить не получилось бы. А если бы она была равна единице, то единственным минимальным набором был бы набор из всех нулей, а по нему нельзя построить конъюнкт.

Заметим напоследок, что можно было бы поступить симметрично, рассмотрев максимальные наборы, на которых функция равна 0, и построив соответствующую КНФ. □

Завершим лекцию сводной таблицей с базисами некоторых классов:

Класс	Примеры базисов
$\top$(все функции)	$\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\mid\}$, $\{\mathbf{1}, \wedge, \oplus\}$
M	$\{\vee, \wedge, \mathbf{0}, \mathbf{1}\}$
L	$\{\mathbf{1}, \oplus\}$, $\{\neg, \leftrightarrow\}$
D	$\{\neg, \mathrm{maj}\}$
P_0	$\{\wedge, \oplus\}$
P_1	$\{\wedge, \rightarrow\}$