После того как лемма доказана, разбор формулы проводится так: если она начинается с отрицания, то может быть образована лишь по третьему правилу. Если же она начинается со скобки, то надо скобку удалить, а потом искать непустое начало, имеющее нулевой скобочный итог и не оканчивающееся на знак логической операции. Такое начало единственно (как легко проверить, используя лемму). Это начало и будет первой частью формулы. Тем самым формула разбирается однозначно. ▷

Нет смысла вдаваться в подробности этого (несложного) рассуждения: вообще-то алгоритмы разбора формул — это отдельная большая и практически важная тема (в первую очередь в связи с компиляторами). Приведённый нами алгоритм далеко не оптимален. С другой стороны, мы вообще можем обойти эту проблему, потребовав, чтобы при записи формул левая и правая скобки, окружающие формулу, связывались линией — тогда однозначность разбора формулы не вызывает вопросов, и больше ничего нам не надо.

В дальнейшем мы будем опускать скобки, если они либо не играют роли (например, можно написать конъюнкцию трёх членов, не указывая порядок действий в силу ассоциативности), либо ясны из контекста.

4. Польский логик Лукасевич предлагал обходиться без скобок, записывая в формулах сначала знак операции, а потом операнды (без пробелов и разделителей). Например, $(a + b) \times (c + (d \times e))$ в его обозначениях запишется как $\times{+}ab{+}c{\times}de$. Эту запись ещё называют *польской* записью. *Обратная* польская запись отличается от неё тем, что знак операции идёт после операндов. Покажите, что в обоих случаях порядок действий восстанавливается однозначно.

1.2. Полные системы связок

Рассматриваемая нами система пропозициональных связок (в неё входят $\wedge$, $\vee$, $\to$, $\neg$) *полна* в следующем смысле:

Теорема 3 (Полнота системы связок). Любая булева функция (с любым числом аргументов) может быть записана в виде пропозициональной формулы.

◁ Проще всего пояснить это на примере. Пусть, например, булева функция $\varphi(p, q, r)$ задана таблицей 1.4.

В таблице есть три строки с единицами в правой колонке — три случая, когда булева функция истинна (равна 1). Напишем три конъюнкции, каждая из которых покрывает один случай (а в остальных

p	q	r	$\varphi(p,q,r)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

$$(\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r)$$

Таблица 1.4. Булева функция и задающая её формула.

строках ложна), и соединим их дизъюнкцией. Нужная формула построена.

Ясно, что аналогичная конструкция применима для любой таблицы (с любым числом переменных). ▷

Для формул подобного вида есть специальное название: формулы в *дизъюнктивной нормальной форме*. Более подробно: *литералом* называется переменная или отрицание переменной, *конъюнктом* называется произвольная конъюнкция литералов, а дизъюнктивной нормальной формой называется дизъюнкция конъюнктов. В нашем случае в каждый конъюнкт входит n литералов (где n — число переменных), а число конъюнктов равно числу строк с единицами и может меняться от нуля (тогда, правда, получается не совсем формула, а «пустая дизъюнкция», и её можно заменить какой-нибудь всегда ложной формулой типа $p \wedge \neg p$) до 2^n (если булева функция всегда истинна).

5. Длина построенной в доказательстве теоремы 3 формулы зависит от числа единиц: формула будет короткой, если единиц в таблице мало. А как написать (сравнительно) короткую формулу, если в таблице мало нулей, а в основном единицы?

Иногда полезна двойственная *конъюнктивная нормальная форма*, которая представляет собой конъюнкцию *дизъюнктов*. Каждый дизъюнкт состоит из литералов, соединённых дизъюнкциями. Теорему 3 можно теперь усилить так:

Теорема 4. Всякая булева функция может быть выражена формулой, находящейся в дизъюнктивной нормальной форме, а также формулой, находящейся в конъюнктивной нормальной форме.

◁ Первая часть утверждения уже доказана. Вторая часть ана-

логична первой, надо только для каждой строки с нулём написать подходящий дизъюнкт.

Можно также представить функцию $\neg\varphi$ в дизъюнктивной нормальной форме, а затем воспользоваться законами Де Моргана, чтобы внести отрицание внутрь. $\triangleright$

6. Проведите второй вариант рассуждения подробно.

Вообще говоря, определение нормальной формы не требует, чтобы в каждом конъюнкте (или дизъюнкте) встречались все переменные. (Повторять переменную больше одного раза смысла нет; если, например, переменная и её отрицание входят в одну конъюнкцию, то эта конъюнкция всегда ложна и её можно выбросить.)

7. Приведите пример булевой функции n аргументов, у которой любая дизъюнктивная или конъюнктивная нормальная форма содержит лишь члены длины n. (Указание: рассмотрите функцию, которая меняет своё значение при изменении значения любой переменной.)

Заметим, что при доказательстве теоремы 3 мы обошлись без импликации. Это и не удивительно, так как она выражается через дизъюнкцию и отрицание:

$$(p \to q) \;\leftrightarrow\; (\neg p \vee q)$$

(проверьте!). Мы могли бы обойтись только конъюнкцией и отрицанием, так как

$$(p \vee q) \;\leftrightarrow\; \neg(\neg p \wedge \neg q),$$

или только дизъюнкцией и отрицанием, так как

$$(p \wedge q) \;\leftrightarrow\; \neg(\neg p \vee \neg q)$$

(обе эквивалентности вытекают из законов Де Моргана; их легко проверить и непосредственно). Как говорят, система связок $\wedge, \neg$, а также система связок $\vee, \neg$ являются *полными*. (По определению это означает, что с их помощью можно записать любую булеву функцию.)

8. Докажите, что система связок $\neg, \to$ полна. (Указание: как записать через них дизъюнкцию?)

А вот без отрицания обойтись нельзя. Система связок $\wedge, \vee, \to$ неполна — и по очень простой причине: если все переменные истинны, то любая их комбинация, содержащая только указанные связки, истинна. (Как говорят, все эти связки «сохраняют единицу».)

9. Любая формула, составленная только с помощью связок $\wedge$ и $\vee$, задаёт монотонную булеву функцию (в том смысле, что от увеличения значения любого из аргументов значение функции может только возрасти —

или остаться прежним). Покажите, что верно и обратное: любая монотонная булева функция либо постоянна (всюду истинна или всюду ложна), либо может быть выражена формулой, содержащей только $\wedge$ и $\vee$.

10. Пусть $\varphi \to \psi$ — тавтология. Покажите, что найдётся формула τ, которая включает в себя только общие для φ и ψ переменные, для которой формулы $(\varphi \to \tau)$ и $(\tau \to \psi)$ являются тавтологиями. (Более общий вариант этого утверждения, в котором рассматриваются формулы с кванторами, называется *леммой Крейга*.)

В принципе мы не обязаны ограничиваться четырьмя рассмотренными связками. Любая булева функция может играть роль связки. Например, можно рассмотреть связку $(p\ \texttt{notand}\ q)$, задаваемую эквивалентностью

$$(p\ \texttt{notand}\ q) \ \leftrightarrow\ \neg(p \wedge q)$$

(словами: $(p\ \texttt{notand}\ q)$ ложно, лишь если p и q истинны). Через неё выражается отрицание $(p\ \texttt{notand}\ p)$, после чего можно выразить конъюнкцию, а затем, как мы знаем, и вообще любую функцию. (Знакомые с цифровыми логическими схемами малого уровня интеграции хорошо знакомы с этим утверждением: достаточно большой запас схем И-НЕ позволяет реализовать любую требуемую зависимость выхода от входов.)

Другая интересная полная система связок — сложение по модулю 2, конъюнкция и константа 1 (которую можно считать 0-арной связкой, задающей функцию от нуля аргументов). Представленные в этой системе булевы функции становятся полиномами с коэффициентами в кольце вычетов по модулю 2. Идея рассматривать булевы функции как полиномы (оказавшаяся неожиданно плодотворной в последние годы) была высказана в 1927 г. российским математиком Иваном Ивановичем Жегалкиным.

Назовём *мономом* конъюнкцию любого набора переменных или константу 1 (которую естественно рассматривать как конъюнкцию нуля переменных). Название это естественно, так как при наших соглашениях (1 обозначает истину, 0 — ложь) конъюнкция соответствует умножению.

Назовём *полиномом* сумму таких мономов по модулю 2 (это значит, что $0 \oplus 0 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$ и $1 \oplus 1 = 0$). Ясно, что два повторяющихся монома можно сократить (ведь сложение по модулю 2), так что будем рассматривать только полиномы без повторяющихся мономов. При этом, естественно, порядок членов в мономе (как и порядок мономов в полиноме) роли не играет, их можно переставлять.

Теорема 5 (о полиномах Жегалкина). Всякая булева функция однозначно представляется таким полиномом.

◁ Существование искомого полинома следует из теоремы 4, так как конъюнкция есть умножение, отрицание — прибавление единицы, а дизъюнкцию можно через них выразить (получится $p+q+pq$). Надо только заметить, что степени не нужны: переменные принимают значения 0 и 1, так что x^n можно заменить на x.

Можно также сослаться на известное из алгебры утверждение о том, что всякая функция с аргументами из конечного поля (в данном случае это двухэлементное поле вычетов по модулю 2) задаётся полиномом. (Так получается новое доказательство теоремы 3.)

Далее можно заметить, что полиномов столько же, сколько булевых функций, а именно 2^{2^n}. В самом деле, булева функция может принимать любое из двух значений в каждой из 2^n точек булева куба $\mathbb{B}^n$, а многочлен может включать или не включать любой из 2^n мономов. (Мономов ровно 2^n, потому что каждый моном включает или не включает любую из n переменных.) Поэтому избытка полиномов нет, и если любая функция представима полиномом, то единственным образом.

Можно и не ссылаться на сведения из алгебры и теорему 4, а дать явную конструкцию. Это удобно сделать индукцией по n. Пусть мы уже умеем представлять любую булеву функцию от $n-1$ аргументов с помощью полинома. Тогда $\varphi(p_1,\ldots,p_n)$ можно представить как

$$\varphi(p_1,\ldots,p_n)=\varphi(0,p_2,\ldots,p_n)+[\varphi(0,p_2,\ldots,p_n)+\varphi(1,p_2,\ldots,p_n)]p_1$$

(проверьте). Остаётся заметить, что правую часть можно представить полиномом по предположению индукции.

Для единственности также есть другое доказательство: пусть два многочлена (имеющие степень 1 по каждой переменной) равны при всех значениях переменных. Тогда их сумма (или разность — вычисления происходят по модулю 2) является ненулевым многочленом (содержит какие-то мономы), но тождественно равна нулю. Так не бывает, и это легко доказать по индукции. В самом деле, любой многочлен $A(p_1,\ldots,p_n)$ можно представить в виде

$$A(p_1,\ldots,p_n)=B(p_2,\ldots,p_n)+p_1C(p_2,\ldots,p_n),$$

где B и C — многочлены от меньшего числа переменных. Подставляя сначала $p_1=0$, а затем $p_1=1$, убеждаемся, что многочлены B и

C равны нулю во всех точках, и потому (согласно предположению индукции) равны нулю как многочлены (не содержат мономов). $\triangleright$

11. Пусть F — произвольное поле. Назовём *мультилинейной* функцией полином от n переменных с коэффициентами из F, в котором все показатели степеней равны либо 0, либо 1. (Таким образом, каждый моном в ней есть произведение коэффициента и некоторого набора переменных без повторений.) Будем рассматривать $\mathbb{B} = \{0, 1\}$ как подмножество F. Докажите, что всякая булева функция $\mathbb{B}^n \to \mathbb{B}$ однозначно продолжается до мультилинейной функции $F^n \to F$, и коэффициенты мультилинейной функции можно считать целыми числами.

Если рассматривать произвольные булевы функции в качестве связок, возникает вопрос: в каком случае набор булевых функций образует полный базис? (Это значит, что любая булева функция представляется в виде композиции функций из набора, т. е. записывается в виде формулы, где связками служат функции набора.) Подобные вопросы вызывали в своё время большой интерес и были хорошо изучены. Начальным этапом явилось такое утверждение:

Теорема 6 (критерий Поста). Набор булевых функций является полным тогда и только тогда, когда он не содержится целиком ни в одном из пяти следующих «предполных классов»:

- монотонные функции;
- функции, сохраняющие нуль;
- функции, сохраняющие единицу;
- линейные функции;
- самодвойственные функции.

(Функция f *монотонна*, если она монотонно неубывает по каждому из своих аргументов. Функция f *сохраняет нуль/единицу*, если $f(0, \ldots, 0) = 0$ (соответственно $f(1, \ldots, 1) = 1$). Функция f *линейна*, если она представима многочленом, в котором все мономы содержат не более одной переменной. Наконец, функция f называется *самодвойственной*, если $f(1 - p_1, \ldots, 1 - p_n) = 1 - f(p_1, \ldots, p_n)$.)

$\triangleleft$ Если набор содержится в одном из классов, то и все композиции также не выходят за пределы этого класса (легко проверить для каждого из классов в отдельности) и поэтому набор не является полным. Докажем обратное утверждение. Пусть для каждого класса выбрана какая-то функция, в нём не лежащая. Убедимся, что с

помощью комбинаций выбранных функций можно получить все булевы функции.

У нас есть функция, не сохраняющая нуль. Подставим вместо всех аргументов одну и ту же переменную. Получится функция от одного аргумента, отображающая нуль в единицу, то есть либо константа 1, либо отрицание. Сделав то же самое с функцией, не сохраняющей единицу, получим либо константу нуль, либо отрицание. Таким образом, у нас либо есть отрицание, либо обе константы 0 и 1.

Если есть обе константы, то всё равно можно получить отрицание. Возьмём немонотонную функцию. Легко понять, что она должна менять значение с единицы на нуль при изменении какого-то одного аргумента с нуля на единицу (в самом деле, будем увеличивать аргументы по одному, в какой-то момент значение функции уменьшится.) Зафиксировав значения остальных аргументов (ведь мы считаем, что константы есть), получаем отрицание.

Имея отрицание и несамодвойственную функцию, легко получить константы (если их не было). В самом деле, несамодвойственность означает, что $f(x_1,\dots,x_n) = f(1-x_1,\dots,1-x_n)$ для каких-то значений $x_1,\dots,x_n \in \{0,1\}$. Вместо нулевых значений переменных $x_1,\dots,x_n$ подставим p, вместо единиц подставим $\neg p$, получится одна из констант. Вторая получится отрицанием.

Теперь у нас есть константы, отрицание и нелинейная функция $f(p_1,\dots,p_n)$. Нелинейность означает, что в её представлении в виде многочлена есть моном, состоящий более чем из одной переменной. Пусть, например, этот моном содержит переменные p_1 и p_2. Сгруппируем члены по четырём группам и получим выражение

$$p_1p_2A(p_3,\dots) + p_1B(p_3,\dots) + p_2C(p_3,\dots) + D(p_3,\dots).$$

При этом многочлен $A(p_3,\dots)$ заведомо отличен от нуля, поэтому можно так подставить константы вместо $p_3,\dots,p_n$, чтобы первое слагаемое не обратилось в нуль. Тогда получим либо $p_1p_2 + d$, либо $p_1p_2 + p_1 + d$, либо $p_1p_2 + p_2 + d$, либо $p_1p_2 + p_1 + p_2 + d$. Свободный член d можно менять, если нужно (у нас есть отрицание), так что получается либо p_1p_2 (конъюнкция, и всё доказано), либо $p_1p_2 + p_1 = p_1(p_2+1) = p_1 \wedge \neg p_2$ (убираем отрицание, получаем конъюнкцию, всё доказано), либо $p_1p_2 + p_2$ (аналогично), либо $p_1p_2 + p_1 + p_2 = (1+p_1)(1+p_2) - 1 = \neg(\neg p_1 \wedge \neg p_2) = p_1 \vee p_2$ (дизъюнкция, всё доказано). $\triangleright$