Математическая логика

В. Е. Плиско

1. Предмет математической логики

Название дисциплины, которую мы начинаем изучать, состоит из двух слов: «логика» и «математическая». *Логика* обычно определяется как наука о способах доказательств и опровержений. Слово «математическая» в названии изучаемой нами дисциплины имеет двоякий смысл. Во-первых, оно означает, что математическая логика — это раздел математики, занимающийся применением математических методов в логике. В этом смысле она сродни таким разделам математики, как математическая лингвистика, математическая статистика, математическая физика и др. Но есть и другой важный смысл в слове «математическая»: это слово означает, что математическая логика изучает способы *математических* доказательств и опровержений, т. е. математических рассуждений. Таким образом, математическую логику можно определить как науку о математических рассуждениях, пользующуюся математическими методами.

Потребность в такой науке возникла в математике в конце XIX – начале XX веков. К концу XIX века в работах Коши, Больцано, Вейерштрасса, Кантора, Дедекинда и др. была завершена так называемая *арифметизация* математического анализа. На место туманной геометрической интуиции пришло точное определение действительного числа как объекта, полученного некоторой теоретико-множественной конструкцией из натуральных, целых и рациональных чисел, так что свойства действительных чисел в конечном счете сводились к свойствам натуральных чисел. В то же время Фреге развил теорию натуральных чисел в рамках канторовской теории множеств. Таким образом, математический анализ и все основанные на нем разделы математики были сведены к теории множеств и, казалось, получили единое и прочное обоснование. Неудивительно поэтому, что обнаружение противоречий в теории множеств явилось драматическим событием в истории математики. Рассмотрим два таких противоречия.

Парадокс Кантора (1899). Пусть M — множество всех множеств, через $\mathcal{P}(M)$ обозначается множество всех его подмножеств. По теореме Кантора мощность множества M строго меньше мощности множества $\mathcal{P}(M)$. Но $\mathcal{P}(M) \subseteq M$, так как M содержит в себе все множества. Значит, мощность множества $\mathcal{P}(M)$ не превосходит мощности множества M. Получили противоречие.

Парадокс Рассела (1903). Пусть T — множество всех множеств, которые не являются своими элементами, т. е. $T = \{x | x \notin x\}$. Иными словами, $x \in T$ тогда и только тогда, когда $x \notin x$. Взяв здесь T в качестве x, получаем, что $T \in T$ тогда и только тогда, когда $T \notin T$. Это также противоречие.

В 1908 году немецкий математик Цермело предложил систему аксиом теории множеств, которая впоследствии была расширена Френкелем и носит название системы Цермело – Френкеля ZF. Аксиомы ZF и других известных аксиоматических систем подобраны так, что на их основе можно доказать все обычные математические теоремы, но нельзя воспроизвести известные парадоксы. Например, парадоксы Кантора и Рассела не возникают потому, что в теории ZF не удается доказать, что совокупность всех множеств и «множество» T являются множествами, поскольку в этой теории аксиомы существования множеств позволяют осуществлять обычные математические теоретико-множественные конструкции, но ограничивают применение самого важного канторовского принципа — так называемого принципа свертывания, согласно которому, каково бы ни было данное свойство, можно рассматривать множество, состоящее в точности из всех тех объектов, которые обладают этим свойством.

Однако тот факт, что в аксиоматической теории множеств не удается воспроизвести известные парадоксы, еще не означает, что парадоксы (т. е. противоречия) здесь действительно невозможны. Чтобы строго доказать недоказуемость противоречия, нужно изучать математические доказательства. Этим в основном и занимается математическая логика.

2. Логика высказываний

2.1. Высказывания и логические операции

Высказывание — это повествовательное предложение, для которого имеет смысл говорить о его истинности или ложности. Этим высказывания отличаются, например, от повелительных или вопросительных предложений. Например, «$2 \times 2 = 4$», «Рим — столица Франции» суть высказывания, а предложения «Который час?» или «Решить уравнение $x^2 + 3x - 2 = 0$» высказываниями не являются.

Под *истинностным значением* понимается абстрактный объект («*истина*» или «*ложь*»), сопоставляемый высказыванию в зависимости от того, является это высказывание истинным или ложным. Можно сказать, что «истина» («ложь») — это то общее, что присуще всем истинным (соответственно, ложным) высказываниям. В математической логике для обозначения истинностных значений «истина» и «ложь» чаще всего используются числа 1 и 0 или буквы И и Л, T и F соответственно. Например, высказывание «$2 \times 2 = 4$» имеет истинностное значение 1, а «Рим — столица Франции» — истинностное значение 0. Иногда говорят, что истинностные значения 0 и 1 *двойственны* друг другу.

Из одних высказываний различными способами можно строить новые, более сложные высказывания. *Логическая операция* — это такой способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний. Рассмотрим некоторые примеры логических операций.

Отрицание — логическая операция, в результате которой из данного высказывания A получается новое высказывание «Неверно, что A». Отрицание высказывания A будем обозначать $\neg A$.

Конъюнкция — логическая операция, заключающаяся в соединении двух высказываний A и B в новое высказывание «A и B». Конъюнкцию высказываний A и B будем обозначать $A \,\&\, B$.

Дизъюнкция — логическая операция, заключающаяся в соединении двух высказываний A и B в новое высказывание «A или B». Дизъюнкцию высказываний A и B будем обозначать $A \vee B$.

Импликация — логическая операция, заключающаяся в соединении двух высказываний A и B в новое высказывание «Если A, то B». Импликацию высказываний A и B будем обозначать $A \supset B$.

Эквиваленция — логическая операция, заключающаяся в соединении двух высказываний A и B в новое высказывание «A равносильно B». Эквиваленцию высказываний A и B будем обозначать $A \equiv B$.

Логическая (или *булева*) *функция* — это n-местная функция, определенная на множестве истинностных значений $\{0, 1\}$ и принимающая значения в этом же множестве. С каждой (n-местной) логической операцией φ естественным образом связана (n-местная же) логическая функция f_φ: если $v_1, \ldots, v_n$ — некоторый набор истинностных значений, то $f_\varphi(v_1, \ldots, v_n)$ есть истинностное значение высказывания $\varphi(P_1, \ldots, P_n)$, где $P_1, \ldots, P_n$ — такие высказывания, что истинностное значение высказывания P_i есть v_i $(i = 1, \ldots, n)$. Логические функции, соответствующие рассмотренным выше логическим операциям, могут быть заданы следующими *истинностными таблицами*:

X	$f_\neg(X)$
0	1
1	0

X	Y	$f_\&(X,Y)$	$f_\vee(X,Y)$	$f_\supset(X,Y)$	$f_\equiv(X,Y)$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

В математической логике принято не различать логические операции с одинаковыми истинностными таблицами независимо от того, какое словесное оформление имеют эти логические операции. Например, высказывание $A \supset B$ может передаваться посредством выражений «Если A, то B», «A влечет B», «В случае A имеет место B», «Для A необходимо B», «A, только если B» и т. п. Вот языковые эквиваленты для других логических операций. $\neg A$ может читаться как «Не A», «A не имеет места», «A неверно». Выражение $A \,\&\, B$ может означать «A и B», «Не только A, но и B», «Как A, так и B». Выражение $A \vee B$ может читаться как «A или B или оба», «A или B», «A, если не B». Наконец, $A \equiv B$ может передаваться как «A, если и только если B», «Если A, то B, и обратно», «A эквивалентно B», «A равносильно B», «A тогда и только тогда, когда B».

А вот пример операции над высказываниями, которая не является логической операцией: по высказыванию A строим высказывание «Я знаю, что A». Очевидно, что истинность или ложность такого высказывания зависит не только от истинностного значения высказывания A, но и от осведомленности лица, произносящего это высказывание.

Задачи

1) Путешественник попал в страну, населенную двумя племенами. Члены одного племени всегда лгут, члены другого говорят только правду. Путешественник встречает двух туземцев. «Вы всегда говорите только правду?» — спрашивает он высокого туземца. Тот отвечает: «Тарабара». «Он сказал 'да', — поясняет туземец поменьше ростом, — но он ужасный лжец». К какому племени принадлежит каждый из туземцев?

2) Один житель острова Крит сказал: «Все критяне — лжецы». Истинно или ложно высказывание, произнесенное этим критянином? (Лжец — человек, который всегда говорит неправду.)

3) Один критянин сказал: «То, что я сейчас говорю, — ложь». Является ли высказыванием предложение, произнесенное этим критянином?

4) В какие дни недели истинно высказывание

   а) «Если сегодня вторник, то завтра понедельник»;

   б) «Если сегодня понедельник, то завтра вторник»?

2.2. Алфавит, буква, слово

Как было сказано в разделе 1, математическая логика в основном занимается изучением математических рассуждений. В математике рассуждения обычно оформляются в виде математических текстов. Поэтому будет уместно рассмотреть некоторые общие понятия, относящиеся к письменным математическим языкам.

Элементарные знаки, из которых состоит текст, называются *буквами*. При использовании того или иного значка в качестве буквы нас не интересуют части этого значка, а лишь этот знак в целом. Например, было бы неправильно утверждать, что мягкий знак является частью буквы «ы». При выборе букв необходимо быть уверенным в том, что всякий раз, рассматривая любые две написанные буквы, мы сможем определить, *одинаковы* эти буквы или *различны*.

Алфавит — это конечный список букв. *Слово* в данном алфавите — конечная последовательность букв этого алфавита. Например, последовательность букв «$\pi\alpha\pi\alpha\gamma\iota\gamma\lambda\varepsilon\mu\mu\alpha$» является словом в алфавите, состоящем из букв $\alpha, \beta, \gamma, \delta, \epsilon, \varepsilon, \vartheta, \iota, \kappa, \lambda, \mu, \nu, o, \pi, \rho$. Для удобства рассматривают также *пустое слово* — последовательность, не содержащую ни одной буквы. Пустое слово является словом в любом алфавите. Его обычно обозначают символом Λ. Слово XY, полученное приписыванием справа к слову X слова Y, называется *произведением* слов X и Y. Очевидно, что $\Lambda X = X\Lambda = X$ для любого слова X. Операция произведения слов ассоциативна, но не коммутативна. Слово X называется *началом* слова Y, если существует такое слово Z, что $Y = XZ$. Слово X называется *концом* слова Y, если существует такое слово Z, что $Y = ZX$. Каково бы ни было слово X, каждое из слов Λ и X является началом и концом слова X. *Собственное начало* слова X — это любое начало слова X, отличное от Λ и X. *Собственный конец* слова X — это любой конец слова X, отличный от Λ и X.

Отметим следующие очевидные факты:

- если X и Y — начала слова Z, то X — начало слова Y или Y — начало слова X;
- если X и Y — концы слова Z, то X — конец слова Y или Y — конец слова X.

Говорят, что слово X *входит* в слово Y, если существуют такие слова U и V, что $Y = UXV$. Слово U называется *левым крылом* данного вхождения слова X в слово Y, а V — *правым крылом* этого вхождения. Различные вхождения слова X в слово Y различаются левыми и правыми крыльями этих вхождений.

Пусть слово X входит в слово Y, и пусть Z — произвольное слово. Зафиксируем некоторое вхождение слова X в Y, т. е. представление слова Y в виде UXV. Тогда слово UZV называется результатом *замены* данного вхождения слова X в слово Y на слово Z.

Задачи

1) Сколько вхождений имеет пустое слово в слово «баобаб»?

2) Сколько имеется различных вхождений слова «ба» в слово «баобаб»? Для каждого из них найти результат замены его на пустое слово.

3) Доказать, что всякое начало слова X является началом слова XY, а всякий конец слова Y является концом слова XY.

2.3. Пропозициональные формулы

Алфавит логики высказываний — это множество $\{P, \neg, \&, \vee, \supset, \equiv, (,)\}$. Слова $(P), (PP), (PPP), \ldots$ будем называть *пропозициональными переменными* и обозначать соответственно $P_1, P_2, P_3, \ldots$. Условимся писать P вместо P_1, Q вместо P_2, R вместо P_3, S вместо P_4. Символы $\neg, \&, \vee, \supset, \equiv$ называются *логическими символами* или *логическими связками*.

Понятие *пропозициональной формулы* (или формулы логики высказываний) определяется индуктивно следующим образом:

- Всякая пропозициональная переменная есть формула (такая формула называется *атомной формулой* или *атомом*).
- Если A и B — формулы, то $(\neg A)$, $(A \,\&\, B)$, $(A \vee B)$, $(A \supset B)$, $(A \equiv B)$ — формулы.

Индуктивный характер определения формулы дает возможность использовать в доказательствах так называемый *принцип индукции по построению формулы*. А именно, пусть требуется доказать, что все формулы обладают некоторым свойством $\mathcal{P}$. Для этого достаточно установить, что

1) каждый атом обладает свойством $\mathcal{P}$;

2) если формула A обладает свойством $\mathcal{P}$, то формула $(\neg A)$ обладает свойством $\mathcal{P}$;

3) если формулы A и B обладают свойством $\mathcal{P}$, а λ — одна из связок $\&, \vee, \supset, \equiv$, то формула $(A\lambda B)$ обладает свойством $\mathcal{P}$.

Индуктивный характер определения формулы позволяет также индукцией по построению формулы задавать функции, определенные на множестве всех формул. А именно, пусть

1) каждому атому A поставлен в соответствие некоторый объект $F(A)$;

2) задано правило, определяющее, какой объект $F(\neg A)$ ставится в соответствие формуле $(\neg A)$, если формуле A поставлен в соответствие объект $F(A)$;

3) задано правило, определяющее, какой объект $F(A\lambda B)$ ставится в соответствие формуле $(A\lambda B)$, где λ — одна из связок $\&, \vee, \supset, \equiv$, если формулам A, B уже поставлены в соответствие объекты $F(A)$, $F(B)$.

Тогда для каждой формулы A однозначно определен объект $F(A)$.

Пусть A — слово в алфавите логики высказываний, $l(A)$ — число левых скобок «(» в A, $r(A)$ — число правых скобок «)» в A. Число $s(A) = l(A) - r(A)$ назовем *скобочным итогом* слова A. Для иллюстрации применения индукции по построению формулы докажем следующую теорему.

Теорема 2.1 (теорема о скобочном итоге). *Скобочный итог формулы равен 0. Скобочный итог всякого собственного начала формулы положителен. Скобочный итог всякого собственного конца формулы отрицателен.*

Доказательство. Все три утверждения будем доказывать одновременно индукцией по построению формулы. Если формула A — атом $(P \ldots P)$, то $l(A) = r(A) = 1$. Следовательно, $s(A) = 0$. Любое собственное начало X атома $(P \ldots P)$ имеет вид (или $(P \ldots P$, и в любом случае $l(X) = 1$, $r(X) = 0$, так что $s(X) = 1 - 0 = 1 > 0$. Любой собственный конец Y атома $(P \ldots P)$ имеет вид $P \ldots P)$ или), и в любом случае $l(Y) = 0$, $r(Y) = 1$, так что $s(Y) = 0 - 1 = -1 < 0$.

Пусть формула A имеет вид $(\neg B)$, причем для формулы B выполнено доказываемое утверждение, т. е. $s(B) = 0$, скобочный итог всякого собственного начала формулы B положителен, а скобочный итог всякого собственного конца формулы B отрицателен. Очевидно, $l(A) = l(B) + 1$, $r(A) = r(B) + 1$, следовательно, $s(A) = l(A) - r(A) = l(B) - r(B) = s(B) = 0$. Собственными началами формулы A являются слова (, $(\neg$, а также слова вида $(\neg X$, где X — начало формулы B, так что $s(X) \geq 0$. Очевидно, $s(() = s((\neg) = 1 > 0$; $s((\neg X) = 1 + s(X) \geq 1 > 0$, что и требовалось доказать. Собственными концами формулы A являются слова), $\neg B)$, а также слова вида $X)$, где X — конец формулы B, так что $s(X) \leq 0$. Очевидно, $s()) = s(\neg B)) = -1 < 0$; $s(X)) = s(X) - 1 \leq -1 < 0$, что и требовалось доказать.

Пусть формула A имеет вид $(B\lambda C)$, где λ — одна из связок $\&$, $\vee$, $\supset$, $\equiv$, а B и C — формулы, для которых выполнено доказываемое утверждение, т. е. $s(B) = 0$, $s(C) = 0$, скобочный итог всякого собственного начала формул B и C положителен, а скобочный итог всякого собственного конца формул B и C отрицателен. Очевидно,

$$l(A) = l(B) + l(C) + 1, \quad r(A) = r(B) + r(C) + 1,$$

следовательно,

$$s(A) = l(A) - r(A) = l(B) + l(C) - r(B) - r(C) = s(B) + s(C) = 0.$$

Собственными началами формулы A являются слово (, слова вида $(X$, где X — начало формулы B, так что $s(X) \geq 0$, слово $(B\lambda$, а также слова вида $(B\lambda Y$, где Y — начало формулы C, так что $s(Y) \geq 0$. Очевидно,

$$s(() = 1 > 0;$$

$$s((X) = 1 + s(X) \geq 1 > 0;$$
$$s((B\lambda) = 1 + s(B) + s(\lambda) = 1 > 0;$$
$$s((B\lambda Y) = 1 + s(B) + s(\lambda) + s(Y) \geq 1 > 0,$$

что и требовалось доказать. Собственными концами формулы A являются слово), слова вида $X)$, где X — конец формулы C, так что $s(X) \leq 0$, слово $\lambda C)$, а также слова вида $Y\lambda C)$, где Y — конец формулы B, так что $s(Y) \leq 0$. Тогда

$$s()) = -1 < 0;$$
$$s(X)) = s(X) - 1 \leq -1 < 0;$$
$$s(\lambda C)) = s(\lambda) + s(C) - 1 = -1 < 0;$$
$$s(Y\lambda C)) = s(Y) + s(\lambda) + s(C) - 1 = s(Y) - 1 \leq -1 < 0,$$

что и требовалось доказать. □

Только что доказанная теорема позволяет доказать единственность логического анализа всякой формулы.

Теорема 2.2. *Всякая формула, не являющаяся атомом, может быть единственным образом представлена в одном из видов* $(\neg A)$, $(A \& B)$, $(A \vee B)$, $(A \supset B)$, $(A \equiv B)$ *для некоторых формул* A *и* B.

Доказательство. Возможность представления любой формулы, не являющейся атомом, в одном из видов $(\neg A)$, $(A \& B)$, $(A \vee B)$, $(A \supset B)$, $(A \equiv B)$ вытекает из определения формулы. Остается доказать единственность такого представления.

Очевидно, что представление любой формулы в виде $(\neg A)$, где A — формула, если оно существует, единственно. Действительно, если слова $(\neg A_1)$ и $(\neg A_2)$ совпадают, то, очевидно, слово A_1 совпадает со словом A_2.

Докажем, что никакая формула не может быть представлена одновременно в виде $(\neg A)$ и в виде $(B\lambda C)$, где λ — одна из связок $\&$, $\vee$, $\supset$, $\equiv$, а A, B и C — формулы. Действительно, если $(\neg A) = (B\lambda C)$, то $\neg A = B\lambda C$, и получается, что формула B начинается с символа $\neg$, что, как видно из определения формулы, невозможно.

Докажем теперь, что если формула представлена в виде $(A\lambda B)$ и в виде $(C\mu D)$, где $\lambda, \mu \in \{\&, \vee, \supset, \equiv\}$, а A, B, C, D — формулы, то $\lambda = \mu$, $A = C$, $B = D$. Действительно, если $(A\lambda B) = (C\mu D)$, то $A\lambda B = C\mu D$. Тогда, если A и C не совпадают, то либо A — собственное начало формулы C, либо C — собственное начало формулы A. В любом случае получаем противоречие с теоремой о скобочном итоге (теорема 2.1). Значит, $A = C$, и тогда $\lambda = \mu$, $B = D$, что и требовалось доказать. □

Пусть $Q_1, \ldots, Q_n$ — попарно различные пропозициональные переменные, $A_1, \ldots, A_n$ — произвольные пропозициональные формулы. Индукцией по построению формулы A определим формулу

$$A(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n),$$

которая является результатом одновременной *подстановки* формул $A_1, \ldots, A_n$ вместо $Q_1, \ldots, Q_n$ в A.

Пусть A — атомная формула. Если A совпадает с переменной Q_i $(i = 1, \ldots, n)$, то $A(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n)$ есть A_i. Если A отлична от всех переменных $Q_1, \ldots, Q_n$, то $A(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n)$ есть A.

Пусть A имеет вид $(\neg B)$. Тогда определяем $A(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n)$ как $(\neg B(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n))$.

Наконец, если A имеет вид $(B\lambda C)$, где λ — один из логических символов $\&, \vee, \supset, \equiv$, то определяем $A(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n)$ как $(B(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n)\lambda C(Q_1 \setminus A_1, \ldots, Q_n \setminus A_n))$.

Будем говорить, что формула A является *подформулой* формулы B, если A входит в B. Очевидно, что всякая формула A является подформулой формулы A. Подформула формулы A, отличная от самой формулы A, называется *собственной подформулой* формулы A.

Практически, записывая формулы, мы будем опускать некоторые скобки, рассматривая полученные выражения как сокращенные записи исходных формул. В частности, мы не будем писать внешние скобки у формул, а также вместо подформул вида $(\neg C)$ будем писать $\neg C$. Дальнейшая экономия скобок возможна, если принять соглашение о том, какие логические операции «сильнее» в том смысле, к каком, например, в школьной алгебре операция умножения «сильнее» операции сложения. Для этого расположим логические символы в следующем порядке: $\neg, \&, \vee, \supset, \equiv$, и будем считать, что из всех возможных в первую очередь выполняется та операция, которая в этом списке стоит левее, а из нескольких одинаковых операций выполняется та, которая встречается в выражении раньше. Например, формулу $(((P_1 \supset P_2) \& (P_3 \supset P_4)) \supset (((\neg P_2) \vee P_4))$ можно сокращенно записать так: $(P_1 \supset P_2) \& (P_3 \supset P_4) \supset \neg P_2 \vee P_4$, а выражение $P_1 \supset P_2 \& P_3 \supset P_4 \supset \neg P_2 \vee P_4$ является сокращенным обозначением формулы $(((P_1 \supset (P_2 \& P_3)) \supset P_4) \supset ((\neg P_2) \vee P_4))$.

Задачи

1) Определить, какие из следующих слов являются формулами:

   а) $((P \,\&\, Q)R\neg S)$;

   б) $((P \,\&\, Q) \supset R)$;

   в) $(((S \supset P) \,\&\, \neg P))$;

   г) $(((\neg P) \supset Q) \supset (\neg(R \vee S)))$.

2) Восстановить все скобки в формулах:

   а) $P \supset \neg P \equiv \neg P$;

   б) $\neg P \,\&\, Q \equiv R \,\&\, \neg\neg(P \vee Q) \supset S$.

3) Доказать, что результат одновременной подстановки формул $A_1, \ldots, A_n$ вместо переменных $Q_1, \ldots, Q_n$ в формулу A является формулой.

4) Доказать, что если формула A является собственной подформулой формулы $(\neg B)$, где B — формула, то A является подформулой формулы B.

5) Доказать, что если формула A является собственной подформулой формулы $(B\lambda C)$, где λ — один из логических символов $\&$,$\vee$, $\supset$, $\equiv$, B и C — формулы, то A является подформулой формулы B или подформулой формулы C.

6) Доказать, что если A — подформула формулы B, то результат замены всякого вхождения A в B на формулу C является формулой.

7) Выписать все подформулы следующих формул:

   а) $(((P \supset Q) \,\&\, (R \supset S)) \supset ((\neg Q) \vee S))$;

   б) $((P \supset Q) \supset ((P \supset (\neg Q)) \supset (\neg Q)))$.

2.4. Истинностные таблицы

Пусть $V = \{P_1, P_2, P_3, \ldots\}$ — множество всех пропозициональных переменных. *Оценкой* называется произвольная функция $g : V \to \{0, 1\}$. Индукцией по построению формулы A определим *значение* $g(A)$ формулы A при оценке g. Для любой атомной формулы A значение $g(A)$ задано оценкой g. Положим $g(\neg A) = f_\neg(g(A))$, $g(A\lambda B) = f_\lambda(g(A), g(B))$, где λ — любой из логических символов $\&, \vee, \supset, \equiv$.

Теорема 2.3. *Значение формулы A при оценке g зависит только от значений оценки g на переменных, входящих в A; иными словами, если g_1 и g_2 — две оценки, совпадающие на всех переменных, входящих в A, то $g_1(A) = g_2(A)$.*

Доказательство. Индукция по построению формулы A.

Пусть A есть атом P_i. Тогда, по условию, $g_1(P_i) = g_2(P_i)$, и $g_1(A) = g_1(P_i) = g_2(P_i) = g_2(A)$, что и требовалось доказать.

Пусть A имеет вид $(\neg B)$ для некоторой формулы B, причем, если g_1 и g_2 — две оценки, совпадающие на всех переменных, входящих в B, то $g_1(B) = g_2(B)$. Пусть g_1 и g_2 — две оценки, совпадающие на всех переменных, входящих в A. Тогда, очевидно, они совпадают и на всех переменных, входящих в B; значит, $g_1(B) = g_2(B)$. Теперь имеем: $g_1(A) = f_\neg(g_1(B)) = f_\neg(g_2(B)) = g_2(A)$, что и требовалось доказать.

Пусть A имеет вид $(B\lambda C)$, где λ — один из логических символов $\&$, $\vee$, $\supset$, $\equiv$, а B и C — формулы, для которых выполнено доказываемое утверждение, т. е. если g_1 и g_2 — две оценки, совпадающие на всех переменных, входящих в B, то $g_1(B) = g_2(B)$, и если g_1 и g_2 — две оценки, совпадающие на всех переменных, входящих в C, то $g_1(C) = g_2(C)$. Пусть g_1 и g_2 — две оценки, совпадающие на всех переменных, входящих в A. Тогда, очевидно, они совпадают на всех переменных, входящих в B, и на всех переменных, входящих в C; значит, $g_1(B) = g_2(B)$ и $g_1(C) = g_2(C)$. Теперь имеем: $g_1(A) = f_\lambda(g_1(B), g_1(C)) = f_\lambda(g_2(B), g_2(C)) = g_2(A)$, что и требовалось доказать. □

Теорема 2.3 показывает, что для определения значения формулы A при данной оценке достаточно знать лишь значения этой оценки на переменных, входящих в A. Это позволяет представлять зависимость значения формулы от оценки в виде так называемой истинностной таблицы. Пусть $Q_1, \ldots, Q_n$ — некоторый список переменных, включающий все переменные, входящие в формулу A. *Истинностной таблицей* формулы A над списком $Q_1, \ldots, Q_n$ называется таблица следующего вида:

Q_1	$\dots$	Q_n	A
$\dots$	$\dots$	$\dots$	$\dots$
α_1	$\dots$	α_n	α
$\dots$	$\dots$	$\dots$	$\dots$

Кроме заголовка эта таблица содержит 2^n строк, в которых выписаны все различные наборы нулей и единиц $\alpha_1 \dots \alpha_n$ и значения $\alpha \in \{0, 1\}$ формулы A при оценке, сопоставляющей переменным $Q_1, \dots, Q_n$ соответственно значения $\alpha_1, \dots, \alpha_n$.

В качестве примера рассмотрим построение истинностной таблицы для формулы

$$P \supset (Q \vee R \supset (R \supset \neg P)).$$

Так как формула содержит 3 переменные P, Q, R, ее истинностная таблица состоит из 8 строк. Отметим в формуле порядок выполнения логических операций. Под знаком каждой операции выпишем столбец значений той подформулы, главной операцией в которой является данная.

P	Q	R	$P \supset^5 (Q \vee^1 R \supset^4 (R \supset^3 \neg^2 P))$				
0	0	0	**1**	0	1	1	1
0	0	1	**1**	1	1	1	1
0	1	0	**1**	1	1	1	1
0	1	1	**1**	1	1	1	1
1	0	0	**1**	0	1	1	0
1	0	1	**0**	1	0	0	0
1	1	0	**1**	1	1	1	0
1	1	1	**0**	1	0	0	0

Сначала вычисляются значения подформулы $Q \vee R$ в каждой строке на основе значений переменных Q и R и значения подформулы $\neg P$ на основе значений переменной P. Затем вычисляются значения подформулы $R \supset \neg P$ на основе значений переменной R и подформулы $\neg P$. Далее вычисляются значения подформулы $Q \vee R \supset (R \supset \neg P)$ на основе значений подформул $Q \vee R$ и $R \supset \neg P$. Наконец, вычисляются значения всей рассматриваемой формулы на основе значений переменной P и подформулы $Q \vee R \supset (R \supset \neg P)$. Значения рассматриваемой формулы для наглядности выделены в таблице полужирным шрифтом. Столбец выделенных значений и есть столбец значений данной формулы.

Задачи

Построить истинностные таблицы для следующих формул:

1) $(P \supset Q) \vee (P \supset Q \,\&\, P)$;

2) $P \,\&\, (Q \supset P) \supset \neg P$;

3) $((P \,\&\, \neg Q) \supset Q) \supset (P \supset Q)$;

4) $(P \supset (Q \supset R)) \supset ((P \supset Q) \supset (P \supset R))$;

5) $P \,\&\, (Q \vee \neg P) \,\&\, ((\neg Q \supset P) \vee Q)$.

2.5. Общезначимые пропозициональные формулы

Тавтология (*общезначимая формула, тождественно истинная формула*) — это пропозициональная формула, значение которой при любой оценке равно 1. Истинностная таблица тавтологии обладает тем свойством, что в столбце ее значений во всех строках стоит 1. Каждая тавтология является схемой истинных высказываний и в этом смысле выражает некоторый *логический закон*. Вот некоторые тавтологии (логические законы): $P \supset P$ (закон тождества); $P \vee \neg P$ (закон исключенного третьего); $\neg(P \,\&\, \neg P)$ (закон противоречия); $\neg\neg P \equiv P$ (закон двойного отрицания); $(P \supset Q) \equiv (\neg Q \supset \neg P)$ (закон контрапозиции); $\neg(P \,\&\, Q) \equiv (\neg P \vee \neg Q)$, $\neg(P \vee Q) \equiv (\neg P \,\&\, \neg Q)$ (законы де Моргана).

Противоречие (*противоречивая формула, тождественно ложная формула*) — это пропозициональная формула, значение которой при любой оценке равно 0. Истинностная таблица противоречия обладает тем свойством, что в столбце ее значений во всех строках стоит 0. Очевидно, что формула A является тавтологией тогда и только тогда, когда формула $\neg A$ является противоречием, и что формула A является противоречием тогда и только тогда, когда формула $\neg A$ является тавтологией.

Теорема 2.4 (теорема о подстановке). *Если формула A является тавтологией (противоречием), то формула $A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)$ является тавтологией (соответственно, противоречием), каковы бы ни были попарно различные переменные $Q_1, \ldots, Q_n$ и каковы бы ни были формулы $A_1, \ldots, A_n$.*

Доказательство. Пусть формула A — тавтология, $Q_1, \ldots, Q_n$ — попарно различные пропозициональные переменные, $A_1, \ldots, A_n$ — произвольные формулы, g — произвольная оценка. Пусть g_1 — оценка, которая совпадает с g на всех переменных, отличных от $Q_1, \ldots, Q_n$, а $g_1(Q_i) = g(A_i)$ $(i = 1, \ldots, n)$.

Лемма 2.1. *Пусть $Q_1, \ldots, Q_n$ — попарно различные пропозициональные переменные, $A_1, \ldots, A_n$ — произвольные формулы, g — произвольная оценка. Пусть g_1 — оценка, которая совпадает с g на всех переменных, отличных от $Q_1, \ldots, Q_n$, а $g_1(Q_i) = g(A_i)$ $(i = 1, \ldots, n)$. Пусть A — произвольная формула. Тогда*

$$g(A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = g_1(A). \tag{1}$$

Доказательство. Индукция по построению формулы A.

Если A есть атом, отличный от $Q_1, \ldots, Q_n$, то $A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)$ совпадает с A, $g_1(A)$ совпадает с $g(A)$, и условие (1) выполнено. Если же A есть одна из переменных Q_i $(i = 1, \ldots, n)$, то $A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)$ есть A_i, $g_1(Q_i) = g(A_i)$. Поэтому имеем: $g(A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = g(A_i) = g_1(Q_i) = g_1(A)$.

Пусть A имеет вид $(\neg B)$, причем для формулы B выполнено доказываемое утверждение, т. е.

$$g(B(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = g_1(B). \tag{2}$$

Тогда $A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)$ есть $(\neg B(Q_1\backslash A_1, \ldots, Q_n\backslash A_n))$, и

$g(A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = f_\neg(g(B(Q_1\backslash A_1, \ldots, Q_n\backslash A_n))$ (по определению значения формулы A при оценке g)

$= f_\neg(g_1(B))$ (в силу условия (2)) $= g_1(A)$ (по определению значения формулы A при оценке g_1), что и требовалось доказать.

Пусть, наконец, A имеет вид $(B\lambda C)$, где λ — один из логических символов $\&$, $\vee$, $\supset$, $\equiv$, а B и C — формулы, причем выполнены условия (2) и

$$g(C(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = g_1(C). \tag{3}$$

Тогда $A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)$ есть $(B(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)\lambda C(Q_1\backslash A_1, \ldots, Q_n\backslash A_n))$, и
$g(A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = f_\lambda(g(B(Q_1\backslash A_1, \ldots, Q_n\backslash A_n), g(C(Q_1\backslash A_1, \ldots, Q_n\backslash A_n))$ (по определению значения формулы A при оценке g) $= f_\lambda(g_1(B), g_1(C))$ (в силу условий (2) и (3)) $= g_1(A)$ (по определению значения формулы A при оценке g_1), что и требовалось доказать. Лемма доказана

Продолжим доказательство теоремы. В силу леммы 2.1, $g(A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = g_1(A) = 1$, так как A — тавтология. Таким образом, $g(A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)) = 1$ для любой оценки g, т. е. формула $A(Q_1\backslash A_1, \ldots, Q_n\backslash A_n)$ является тавтологией. Совершенно аналогично рассматривается случай, когда A — противоречие. □

Чтобы проверить, является ли данная формула тавтологией, достаточно построить ее истинностную таблицу. Теорема 2.4 позволяет любую данную тавтологию рассматривать как схему бесконечного числа новых тавтологий, получающихся из данной подстановкой в нее произвольных формул вместо переменных. Так, путем построения истинностной таблицы можно убедиться, что формула

$$(P \supset Q) \supset ((Q \supset R) \supset (P \supset R))$$

является тавтологией. Тогда, в силу теоремы 2.4, тавтологией является любая формула вида

$$(A \supset B) \supset ((B \supset C) \supset (A \supset C)),$$

где A, B, C — произвольные формулы.

Построение истинностной таблицы, которое иногда может оказаться довольно трудоемким (например, в случае большого числа переменных или логических связок в формуле), является не единственным способом проверки того, является ли данная формула тавтологией. На практике можно просто попытаться найти *контрпример* для данной формулы, т. е. такой набор значений переменных, на котором данная формула принимает значение 0. Если поиск такого набора окажется успешным, мы докажем, что формула не является тавтологией. В противном случае мы можем убедиться в бесплодности наших попыток и тем самым доказать, что формула является тавтологией. При этом поиск контрпримера можно вести довольно целенаправленно, учитывая логическую структуру формулы. Попытаемся, например, найти контрпример для

формулы $(P \supset Q) \supset (Q \supset P)$. Рассуждаем следующим образом. Чтобы при некоторой оценке формула вида $A \supset B$ принимала значение 0, необходимо и достаточно, чтобы при этой оценке формула A принимала значение 1, а формула B — значение 0. Таким образом, нам надо найти такую оценку g, при которой а) формула $P \supset Q$ принимает значение 1, б) формула $Q \supset P$ принимает значение 0. Условие б) выполняется лишь в случае, когда $g(Q) = 1$, $g(P) = 0$. Очевидно, что в этом случае условие а) также выполнено. Таким образом, контрпример для данной формулы найден, и тем самым доказано, что она не является тавтологией.

Рассмотрим другой пример. Попробуем найти контрпример для формулы

$$(P \supset R) \& (Q \supset S) \& (\neg R \vee \neg S) \supset \neg P \vee \neg Q.$$

Для этого, очевидно, достаточно найти такую оценку, при которой а) формула $P \supset R$ принимает значение 1, б) формула $Q \supset S$ принимает значение 1, в) формула $\neg R \vee \neg S$ принимает значение 1, г) формула $\neg P \vee \neg Q$ принимает значение 0. В свою очередь, условие г) выполнено только в случае, когда $g(P) = g(Q) = 1$. Но тогда, для выполнения условий а) и б), необходимо $g(R) = g(S) = 1$. Однако в этом случае не выполняется условие в). Таким образом, не существует такой оценки, для которой выполнялись бы условия а) – г). Мы убедились в безнадежности найти контрпример для рассматриваемой формулы и тем самым доказали, что она является тавтологией. Заметим, что истинностная таблица для этой формулы содержит 16 строк, и ее построение заняло бы довольно много времени.

Задачи

1) Доказать, что следующие формулы являются тавтологиями:

   а) $(P \supset Q) \vee (Q \supset P)$;
   б) $P \supset (Q \supset P \& Q)$;
   в) $P \supset (Q \supset P)$;
   г) $P \vee \neg P$;
   д) $P \& Q \supset P$;
   е) $P \& Q \supset Q$;
   ж) $P \supset P \vee Q$;
   з) $Q \supset P \vee Q$;
   и) $\neg\neg P \supset P$;
   к) $P \vee P \supset P$;
   л) $((P \supset Q) \supset P) \supset P$;
   м) $\neg P \supset (P \supset Q)$.

2) Доказать, что каковы бы ни были формулы A, B, C, следующие формулы являются тавтологиями:

   а) $(A \supset B) \vee (B \supset A)$;
   б) $A \supset (B \supset A \& B)$;
   в) $A \supset (B \supset A)$;
   г) $A \& B \supset A$;
   д) $A \supset A \vee B$;
   е) $((A \supset B) \supset A) \supset A$.

3) Доказать, что следующие формулы не являются тавтологиями:

   а) $((P \supset Q \& R) \supset (\neg Q \supset \neg P)) \supset \neg Q$;
   б) $P \vee Q \vee R \supset (P \vee Q) \& (P \vee R)$.

2.6. Равносильные формулы

Формулы A и B называются *равносильными* (или *эквивалентными*), если формула $A \equiv B$ является тавтологией. Если формулы A и B равносильны, этот факт обозначается так: $A \sim B$. Отметим следующий очевидный факт: формулы A и B равносильны тогда и только тогда, когда $g(A) = g(B)$ для любой оценки g. Вот некоторые примеры равносильностей, вытекающие из общезначимости соответствующих эквивалентностей: $\neg\neg P \sim P$; $(P \supset Q) \sim (\neg Q \supset \neg P)$; $\neg(P \,\&\, Q) \sim (\neg P \vee \neg Q)$; $\neg(P \vee Q) \sim (\neg P \,\&\, \neg Q)$; $(P \equiv Q) \sim ((P \supset Q) \,\&\, (Q \supset P))$.

Зафиксируем некоторое вхождение формулы A в формулу C и, имея это в виду, будем обозначать C как C_A. Пусть B — произвольная формула. Через C_B будем обозначать формулу, полученную в результате замены выделенного вхождения формулы A в C на B.

Теорема 2.5 (теорема об эквивалентной замене). *Каковы бы ни были формулы A, B, C, если A входит в C и $A \sim B$, то для любого вхождения формулы A в C имеет место $C_A \sim C_B$.*

Доказательство. Зафиксируем такие формулы A и B, что $A \sim B$, и докажем утверждение теоремы индукцией по построению формулы C.

Если C — атомная формула, а A — ее подформула, то A совпадает с C. Тогда C_A есть A, C_B есть B, и доказываемое утверждение очевидно.

Пусть C имеет вид $(\neg D)$, причем для формулы D выполнено доказываемое утверждение: если A входит в D, то $D_A \sim D_B$. Пусть формула A является подформулой формулы C. Тогда либо A совпадает с C, либо A является собственной подформулой формулы C. Если A совпадает с C, то C_A есть A, C_B есть B, и доказываемое утверждение очевидно. Если же A является собственной подформулой формулы C, то, в силу задачи 4) из раздела 2.3, A входит в D, и C_A имеет вид $(\neg D_A)$. Тогда C_B имеет вид $(\neg D_B)$, и для любой оценки g имеем: $g(C_A) = g(\neg D_A) = f_\neg(g(D_A)) = f_\neg(g(D_B)) = g(\neg D_B) = g(C_B)$, т. е. $C_A \sim C_B$, что и требовалось доказать.

Пусть C имеет вид $(D \lambda E)$, где λ — один из логических символов $\&$, $\vee$, $\supset$, $\equiv$, а C и D — формулы, для которых выполнено доказываемое утверждение: если A входит в D, то $D_A \sim D_B$, и если A входит в E, то $E_A \sim E_B$. Пусть формула A является подформулой формулы C. Тогда либо A совпадает с C, либо A является собственной подформулой формулы C. Если A совпадает с C, то C_A есть A, C_B есть B, и доказываемое утверждение очевидно. Если же A является собственной подформулой формулы C, то, в силу задачи 5) из раздела 2.3, A входит в D или A входит в E, и C_A имеет вид $(D_A \lambda E)$ или вид $(D \lambda E_A)$. В первом случае C_B имеет вид $(D_B \lambda E)$, и для любой оценки g имеем:

$$g(C_A) = g(D_A \lambda E) = f_\lambda(g(D_A), g(E)) = f_\lambda(g(D_B), g(E)) = g(D_B \lambda E) = g(C_B),$$

т. е. $C_A \sim C_B$, что и требовалось доказать. Совершенно аналогично рассматривается второй случай. □

Задачи

1) Доказать следующие равносильности:

   а) $P \,\&\, P \sim P$;

   б) $P \,\&\, Q \sim Q \,\&\, P$;

   в) $P \,\&\, (Q \vee P) \sim P$;

   г) $P \vee P \sim P$;

   д) $P \vee Q \sim Q \vee P$;

   е) $P \vee Q \,\&\, P \sim P$.

2) Доказать следующие равносильности, где A, B, C — произвольные формулы:

   а) $\neg\neg A \sim A$;

   б) $A \supset B \sim \neg A \vee B$;

   в) $\neg(A \supset B) \sim A \,\&\, \neg B$;

   г) $A \,\&\, (B \vee \neg B) \sim A$;

   д) $A \vee B \,\&\, \neg B \sim A$;

   е) $A \supset \neg A \sim \neg A$;

   ж) $(A \vee B) \,\&\, (B \vee C) \,\&\, (C \vee A) \sim A \,\&\, C \vee B \,\&\, C \vee C \,\&\, A$;

з) $(A \vee B) \,\&\, (A \vee \neg B) \sim A$;

и) $A \vee \neg A \,\&\, B \sim A \vee B$;

к) $A \equiv B \sim (A \supset B) \,\&\, (B \supset A)$.

3) Доказать, что формула $A \supset B$ равносильна каждой из следующих формул:

а) $\neg B \supset \neg A$;

б) $A \,\&\, \neg B \supset \neg A$;

в) $A \,\&\, \neg B \supset B$;

г) $\neg(A \,\&\, \neg B)$.

4) Построить формулу, использующую только связку $\supset$, равносильную формуле $P \vee Q$.

5) Построить формулу, использующую только связки $\supset$ и $\equiv$, равносильную формуле $P \,\&\, Q$.

6) Какое максимальное количество попарно неравносильных формул можно построить, используя лишь переменные $P_1, \ldots, P_n$?

7) Путешественник находится в одном из городов А или Б, но в каком именно — ему неизвестно. Он задает собеседнику один вопрос, на который может получить ответ «да» или «нет», причем ответ его собеседника может являться правдой или ложью (чем именно, ему тоже неизвестно). Придумать вопрос, по ответу на который можно безошибочно судить, в каком городе находится путешественник.

8) Доказать, что:

а) $A \equiv A \sim B \equiv B$;

б) $A \equiv (B \equiv C) \sim (A \equiv B) \equiv C$;

в) $A \equiv B \sim B \equiv A$.

9) Доказать, что пропозициональная формула, содержащая только связку $\equiv$, является тавтологией тогда и только тогда, когда каждая переменная входит в нее четное число раз.

10) Доказать, что пропозициональная формула, содержащая только связки $\equiv$ и $\neg$, является тавтологией тогда и только тогда, когда каждая переменная и знак отрицания входят в нее четное число раз.

2.7. Формулы с тесными отрицаниями

Атомные формулы и их отрицания называются *литерами.* Если Q — переменная, то литеры Q и $\neg Q$ называются *контрарными.*

Понятие *формулы с тесными отрицаниями* определяется индуктивно следующим образом:

1) всякая литера считается формулой с тесными отрицаниями;

2) если A и B — формулы с тесными отрицаниями, то $(A \,\&\, B)$, $(A \vee B)$ — формулы с тесными отрицаниями.

Иными словами, формула с тесными отрицаниями — это такая пропозициональная формула, которая содержит лишь связки $\neg$, $\&$, $\vee$, причем связка $\neg$ встречается в ней лишь непосредственно перед переменными.

Теорема 2.6. *Для любой пропозициональной формулы существует равносильная ей формула с тесными отрицаниями.*

Доказательство. Мы докажем следующее, более общее, утверждение: какова бы ни была формула A, существуют формулы с тесными отрицаниями A' и A° такие, что $A' \sim A$, $A^\circ \sim \neg A$. Для доказательства этого утверждения воспользуемся индукцией по построению формулы A.

Если A есть переменная Q, то, очевидно, в качестве A' можно взять литеру Q, а в качестве A° — литеру $\neg Q$.

Пусть формула A имеет вид $(\neg B)$, причем для формулы B построены формулы с тесными отрицаниями B' и B° такие, что $B' \sim B$, $B^\circ \sim \neg B$. Тогда, очевидно, в качестве A' можно взять формулу B°. В качестве A° можно взять формулу B'. Действительно, $\neg A$ есть формула $\neg\neg B$, равносильная формуле B (см. задачу 2а) из раздела 2.6), которая, в свою очередь, равносильна формуле B'.

Рассматривая другие логические связки, мы не будем останавливаться на подробном обосновании выбора формул A' и A°, оставляя эту задачу для читателя.

Пусть формула A имеет вид $(B\lambda C)$, где λ есть $\&$ или $\vee$, причем для формул B и C построены формулы с тесными отрицаниями B', B°, C', C° такие, что

$$B' \sim B, \quad B^\circ \sim \neg B, \quad C' \sim C, \quad C^\circ \sim \neg C. \tag{4}$$

Тогда в качестве A' можно взять формулу $(B'\lambda C')$, а в качестве A° — формулу $(B^\circ \lambda^* C^\circ)$, где

$$\lambda^* = \begin{cases} \&, \text{ если } \lambda = \vee; \\ \vee, \text{ если } \lambda = \&. \end{cases}$$

Пусть формула A имеет вид $(B \supset C)$, причем для формул B и C построены формулы с тесными отрицаниями B', B°, C', C° такие, что выполнены условия (4). Тогда в качестве A' можно взять формулу $(B^\circ \vee C')$, а в качестве A° — формулу $(B' \,\&\, C^\circ)$.

Пусть, наконец, формула A имеет вид $(B \equiv C)$, причем для формул B и C построены формулы с тесными отрицаниями B', B°, C', C° такие, что выполнены условия (4). Тогда в качестве A' можно взять формулу $(B^\circ \vee C') \,\&\, (C^\circ \vee B')$, а в качестве A° — формулу $(B' \,\&\, C^\circ) \vee (C' \,\&\, B^\circ)$. $\square$

Доказательство теоремы 2.6 дает алгоритм приведения произвольной пропозициональной формулы к виду с тесными отрицаниями, т. е. построения формулы с тесными отрицаниями, равносильной данной формуле. Рассмотрим, например, формулу $((P \supset Q) \supset (R \supset \neg P)) \supset (\neg Q \supset \neg R)$. Пользуясь обозначениями и рассуждениями из доказательства теоремы 2.6, получаем следующую цепочку равносильностей:

$$(((P \supset Q) \supset (R \supset \neg P)) \supset (\neg Q \supset \neg R))' \sim ((P \supset Q) \supset (R \supset \neg P))^\circ \vee (\neg Q \supset \neg R)' \sim$$

$$\sim (P \supset Q)' \,\&\, (R \supset \neg P)^\circ \vee (\neg Q)^\circ \vee (\neg R)' \sim (P^\circ \vee Q') \,\&\, R' \,\&\, (\neg P)^\circ \vee Q \vee \neg R \sim (\neg P \vee Q) \,\&\, R \,\&\, P \vee Q \vee \neg R.$$

2.8. Нормальные формы пропозициональных формул

Понятие *дизъюнкта* определяется следующим образом:

1) всякая литера считается дизъюнктом;

2) если D — дизъюнкт, L — литера, то формула $D \vee L$ является дизъюнктом.

Таким образом, пользуясь соглашением об опускании скобок, каждый дизъюнкт можно записать в виде $L_1 \vee \ldots \vee L_n$, где $L_1, \ldots, L_n$ — литеры, $n \geq 1$. Очевидно, что такой дизъюнкт принимает при данной оценке значение 0 тогда и только тогда, когда все литеры $L_1, \ldots, L_n$ принимают значение 0. Отсюда, в частности, следует, что дизъюнкт $L_1 \vee \ldots \vee L_n$ является тавтологией тогда и только тогда, когда среди литер $L_1, \ldots, L_n$ есть контрарные.

Понятие *конъюнкта* определяется следующим образом:

1) всякая литера считается конъюнктом;

2) если K — конъюнкт, L — литера, то формула $K \,\&\, L$ является конъюнктом.

Пользуясь соглашением об опускании скобок, каждый конъюнкт можно записать в виде $L_1 \,\&\, \ldots \,\&\, L_n$, где $L_1, \ldots, L_n$ — литеры, $n \geq 1$. Очевидно, что такой конъюнкт принимает при данной оценке значение 1 тогда и только тогда, когда все литеры $L_1, \ldots, L_n$ принимают значение 1. Отсюда, в частности, следует, что конъюнкт $L_1 \,\&\, \ldots \,\&\, L_n$ является противоречием тогда и только тогда, когда среди литер $L_1, \ldots, L_n$ есть контрарные.

Конъюнктивная нормальная форма (КНФ) определяется так:

1) всякий дизъюнкт есть КНФ;

2) если A есть КНФ, D — дизъюнкт, то формула $A \,\&\, D$ есть КНФ.

Пользуясь соглашением об опускании скобок, каждую конъюнктивную нормальную форму можно записать в виде $D_1 \,\&\, \ldots \,\&\, D_n$, где $D_1, \ldots, D_n$ — дизъюнкты, $n \geq 1$.

Дизъюнктивная нормальная форма (ДНФ) определяется так:

1) всякий конъюнкт есть ДНФ;

2) если A есть ДНФ, K — конъюнкт, то формула $A \vee K$ есть ДНФ.

Пользуясь соглашением об опускании скобок, каждую дизъюнктивную нормальную форму можно записать в виде $K_1 \vee \ldots \vee K_n$, где $K_1, \ldots, K_n$ — конъюнкты, $n \geq 1$.

Пусть Q — переменная, $\alpha \in \{0, 1\}$. Через Q^α будем обозначать литеру Q, если $\alpha = 1$, и литеру $\neg Q$, если $\alpha = 0$. Очевидно, что для любой оценки g выполняются условия:

$$g(Q^\alpha) = 1 \Leftrightarrow g(Q) = \alpha;$$

$$g(Q^\alpha) = 0 \Leftrightarrow g(Q) = \alpha^*,$$

где α^* есть истинностное значение, двойственное значению α, т. е.

$$\alpha^* = \begin{cases} 0, \text{ если } \alpha = 1; \\ 1, \text{ если } \alpha = 0. \end{cases}$$

Пусть $Q_1, \ldots, Q_n$ — некоторый упорядоченный список попарно различных пропозициональных переменных, и пусть g — произвольная оценка. Положим $\alpha_i = g(Q_i)$ $(i = 1, \ldots, n)$. Каждый набор $\alpha = \alpha_1 \ldots \alpha_n$ можно рассматривать как двоичную запись некоторого натурального числа $\overline{\alpha}$. Будем считать, что набор β сдедует за набором α, если $\overline{\alpha} \leq \overline{\beta}$.

Стандартный конъюнкт над списком $Q_1, \ldots, Q_n$, соответствующий набору $\alpha = \alpha_1 \ldots \alpha_n$, — это конъюнкт $Q_1^{\alpha_1} \& \ldots \& Q_n^{\alpha_n}$. Очевидно, что для любой оценки g выполняется следующее условие:

$$g(Q_1^{\alpha_1} \& \ldots \& Q_n^{\alpha_n}) = 1 \Leftrightarrow (\forall i \in \{1, \ldots, n\}) g(Q_i) = \alpha_i.$$

Пусть $K_1, \ldots, K_m$ $(m \geq 1)$ суть некоторые стандартные конъюнкты над списком $Q_1, \ldots, Q_n$, соответствующие наборам $\alpha^1, \ldots, \alpha^m$, выписанным в порядке следования. Формула $K_1 \vee \ldots \vee K_m$ называется *совершенной дизъюнктивной нормальной формой (СДНФ)* над списком $Q_1, \ldots, Q_n$. Очевидно, что для любой оценки g имеет место $g(K_1 \vee \ldots \vee K_m) = 1$ тогда и только тогда, когда набор $g(Q_1), \ldots, g(Q_n)$ совпадает с одним из наборов $\alpha^1, \ldots, \alpha^m$. Заметим, что никакая СДНФ не является противоречием.

Приведенные рассуждения позволяют для любой формулы A, не являющейся противоречием, построить равносильную ей СДНФ над любым списком переменных $Q_1, \ldots, Q_n$, включающем все переменные, входящие в A. А именно, пусть $\alpha^1, \ldots, \alpha^m$ — все наборы значений переменных $Q_1, \ldots, Q_n$, выписанные в порядке следования, на которых формула A принимает значение 1, и пусть $K_1, \ldots, K_m$ — стандартные конъюнкты над списком $Q_1, \ldots, Q_n$, соответствующие наборам $\alpha^1, \ldots, \alpha^m$. Тогда СДНФ $K_1 \vee \ldots \vee K_m$ равносильна формуле A, так как обе эти формулы принимают значение 1 в точности при одних и тех же оценках.

Стандартный дизъюнкт над списком $Q_1, \ldots, Q_n$, соответствующий набору $\alpha = \alpha_1 \ldots \alpha_n$, — это дизъюнкт $Q_1^{\alpha_1} \vee \ldots \vee Q_n^{\alpha_n}$. Очевидно, что для любой оценки g выполняется следующее условие:

$$g(Q_1^{\alpha_1} \vee \ldots \vee Q_n^{\alpha_n}) = 0 \Leftrightarrow (\forall i \in \{1, \ldots, n\}) g(Q_i) = \alpha_i^*.$$

Пусть $D_1, \ldots, D_m$ $(m \geq 1)$ суть некоторые стандартные дизъюнкты над списком $Q_1, \ldots, Q_n$, соответствующие наборам $\alpha^1, \ldots, \alpha^m$, выписанным в порядке следования. Формула $D_1 \& \ldots \& D_m$ называется *совершенной конъюнктивной нормальной формой (СКНФ)* над списком $Q_1, \ldots, Q_n$.

Для набора $\alpha = \alpha_1 \ldots \alpha_n$ через α^* будем обозначать *двойственный* ему набор $\alpha_1^* \ldots \alpha_n^*$. Очевидно, что для любой оценки g имеет место $g(D_1 \& \ldots \& D_m) = 0$ тогда и только тогда, когда набор $g(Q_1), \ldots, g(Q_n)$ совпадает с одним из наборов $(\alpha^1)^*, \ldots, (\alpha^m)^*$. Заметим, что никакая СКНФ не является тавтологией.

Приведенные рассуждения позволяют для любой формулы A, не являющейся тавтологией, построить равносильную ей СКНФ над любым списком переменных $Q_1, \ldots, Q_n$, включающем все переменные, входящие в A. А именно, пусть $\alpha^1, \ldots, \alpha^m$ — все наборы значений переменных $Q_1, \ldots, Q_n$, на которых формула A принимает значение 0. Выпишем в порядке следования наборы $\beta^1 = (\alpha^1)^*, \ldots, \beta^m = (\alpha^m)^*$. Пусть $D_1, \ldots, D_m$ — стандартные дизъюнкты над списком $Q_1, \ldots, Q_n$, соответствующие наборам $\beta^1, \ldots, \beta^m$. Тогда, очевидно, СКНФ $D_1 \& \ldots \& D_m$ равносильна формуле A, так как обе эти формулы принимают значение 0 в точности при одних и тех же оценках.

Задачи

1) Для каждой из следующих формул построить равносильную ей ДНФ и КНФ:

   а) $((P \supset Q) \supset (R \supset \neg P)) \supset (\neg Q \supset \neg R)$;

   б) $((((P \supset Q) \supset \neg P) \supset \neg Q) \supset \neg R) \supset R$;

в) $(P \supset (Q \supset R)) \supset ((P \supset \neg R) \supset (P \supset \neg Q))$.

2) Для каждой из следующих формул построить СДНФ, равносильную ей:

а) $((P \supset Q) \supset \neg P) \supset (P \supset Q \,\&\, P)$;

б) $\neg(P \,\&\, Q \supset \neg P) \,\&\, \neg(P \,\&\, Q \supset \neg Q)$.

3) Для каждой из следующих формул построить СКНФ, равносильную ей:

а) $(R \supset P) \supset (\neg(Q \vee R) \supset P)$;

б) $\neg(P \,\&\, Q \supset P) \vee (P \,\&\, (Q \vee R))$.

2.9. Принцип двойственности

Теорема 2.7. *Пусть A — формула с тесными отрицаниями, а A' — формула с тесными отрицаниями, полученная из A заменой связки $\&$ на $\vee$, связки $\vee$ на $\&$ и каждой литеры на контрарную ей. Тогда $\neg A \sim A'$.*

Доказательство. Индукция по построению формулы с тесными отрицаниями A. Если A есть литера, то A' — контрарная ей литера, и доказываемое утверждение очевидно. Пусть A имеет вид $B \,\&\, C$, где B и C — формулы с тесными отрицаниями, для которых построены формулы с тесными отрицаниями B' и C', так что $\neg B \sim B'$, $\neg C \sim C'$. Тогда A' есть $B' \vee C'$, и $\neg A = \neg(B \,\&\, C) \sim \neg B \vee \neg C \sim B' \vee C' = A'$, что и требовалось доказать. Совершенно аналогично рассматривается случай, когда A имеет вид $B \vee C$, где B и C — формулы с тесными отрицаниями. □

Теорема 2.8 (принцип двойственности). *Пусть A и B — формулы с тесными отрицаниями, а A^* и B^* — формулы с тесными отрицаниями, полученные соответственно из A и B заменой связки $\&$ на $\vee$, а связки $\vee$ на $\&$. Тогда*

1) если A — противоречие, то A^* — тавтология;

2) если A — тавтология, то A^* — противоречие;

3) если $A \sim B$, то $A^* \sim B^*$;

4) если формула $A \supset B$ является тавтологией, то формула $B^* \supset A^*$ также является тавтологией.

Доказательство. Заметим, что замену в формуле с тесными отрицаниями A всех литер на контрарные можно провести в два этапа. Сначала в формулу A подставляем формулы $\neg Q_1, \ldots, \neg Q_n$ вместо всех входящих в нее переменных $Q_1, \ldots, Q_n$. Затем, пользуясь равносильностями $\neg\neg Q_i \sim Q_i$ $(i = 1, \ldots, n)$, опускаем все возникшие двойные отрицания перед переменными, получая равносильную формулу. Таким образом, формула A', рассмотренная в теореме 2.7, равносильна формуле, полученной из A^* указанной подстановкой. Аналогично, формула A^* равносильна формуле, полученной из формулы A' той же подстановкой. Иными словами, если $Q_1, \ldots, Q_n$ — все переменные, входящие в формулу с тесными отрицаниями A, то

$$A' \sim A^*(Q_1 \backslash \neg Q_1, \ldots, Q_n \backslash \neg Q_n), \qquad A^* \sim A'(Q_1 \backslash \neg Q_1, \ldots, Q_n \backslash \neg Q_n). \tag{5}$$

1) Пусть A — противоречие. По теореме 2.7 формула A' равносильна формуле $\neg A$, следовательно, является тавтологией. По теореме о подстановке (теорема 2.4) формула $A'(Q_1 \backslash \neg Q_1, \ldots, Q_n \backslash Q_n)$ также является тавтологией. С другой стороны, в силу (5), эта формула равносильна формуле A^*, которая, таким образом, также является тавтологией.

2) Это утверждение доказывается аналогично предыдущему.

3) Пусть $A \sim B$. Тогда, по теореме об эквивалентной замене, $\neg A \sim \neg B$. По теореме 2.7 отсюда следует $A' \sim B'$, т. е. формула $A' \equiv B'$ является тавтологией. Пусть $Q_1, \ldots, Q_n$ — все переменные, входящие в эту формулу. По теореме о подстановке формула $A'(Q_1 \backslash \neg Q_1, \ldots, Q_n \backslash \neg Q_n) \equiv B'(Q_1 \backslash \neg Q_1, \ldots, Q_n \backslash \neg Q_n)$ является тавтологией. С другой стороны, в силу (5) и теоремы об эквивалентной замене (теорема 2.5), эта формула равносильна формуле $A^* \equiv B^*$, следовательно, $A^* \sim B^*$.

4) Пусть формула $A \supset B$ является тавтологией. Тогда и равносильная ей формула $\neg B \supset \neg A$ также является тавтологией. В силу теоремы 2.7 и теоремы об эквивалентной замене эта формула равносильна формуле $B' \supset A'$, которая, таким образом, также является тавтологией. По теореме о подстановке формула $B'(Q_1 \backslash \neg Q_1, \ldots, Q_n \backslash \neg Q_n) \supset A'(Q_1 \backslash \neg Q_1, \ldots, Q_n \backslash \neg Q_n)$ является тавтологией. С другой стороны, в силу (5) и теоремы об эквивалентной замене, эта формула равносильна формуле $B^* \supset A^*$, которая также является тавтологией. □

Задачи

Пусть дана дизъюнктивная (конъюнктивная) нормальная форма A. Как построить конъюнктивную (соответственно, дизъюнктивную) нормальную форму для $\neg A$?

2.10. Выполнимость и теорема компактности в логике высказываний

Множество пропозициональных формул Γ называется *выполнимым*, если существует такая оценка g, что $(\forall A \in \Gamma) g(A) = 1$. Пропозициональная формула A называется выполнимой, если выполнимо множество $\{A\}$.

Теорема 2.9 (теорема компактности). *Бесконечное множество пропозициональных формул выполнимо тогда и только тогда, когда выполнимо всякое конечное его подмножество.*

Доказательство. Очевидно, что если множество пропозициональных формул Γ выполнимо, то выполнимо любое его подмножество, в частности, любое конечное подмножество. Докажем, что множество Γ выполнимо, если выполнимо любое конечное его подмножество. Поскольку множество всех пропозициональных формул счетно, бесконечное множество Γ также счетно. Пусть $\Gamma = \{A_1, A_2, A_3, \ldots\}$. Положим $\Delta_n = \{A_1, \ldots, A_n\} \quad (n \geq 1)$. Очевидно, каждое из множеств Δ_n — это конечное подмножество множества Γ, следовательно, оно выполнимо по предположению. Пусть g_n — такая оценка, при которой все формулы из Δ_n принимают значение 1. Построим оценку g, индукцией по n определив значение $g(P_n)$ для каждой переменной P_n. Положим $g(P_1) = 1$, если множество $\{n | g_n(P_1) = 1\}$ бесконечно. В противном случае положим $g(P_1) = 0$. Очевидно, в этом случае бесконечно множество $\{n | g_n(P_1) = 0\}$. Таким образом, в любом случае множество $M_1 = \{n | g_n(P_1) = g(P_1)\}$ бесконечно.

Допустим, что уже определены значения $g(P_1), \ldots, g(P_k)$ для некоторого $k \geq 1$, причем множество $M_k = \{n | g_n(P_1) = g(P_1), \ldots, g_n(P_k) = g(P_k)\}$ бесконечно. Положим $g(P_{k+1}) = 1$, если бесконечно множество $\{n | n \in M_k, g_n(P_{k+1}) = 1\}$. В противном случае положим $g(P_{k+1}) = 0$. Очевидно, в этом случае бесконечно множество $\{n | n \in M_k, g_n(P_{k+1}) = 0\}$. Таким образом, в любом случае множество

$$M_{k+1} = \{n | n \in M_k, g_n(P_{k+1}) = g(P_{k+1})\} = \{n | g_n(P_1) = g(P_1), \ldots, g_n(P_k) = g(P_k), g_n(P_{k+1}) = g(P_{k+1})\}$$

бесконечно.

Докажем, что $g(A_n) = 1$ для любого $n \geq 0$. В формуле A_n используется лишь конечное число переменных. Пусть все они содержатся среди переменных $P_1, \ldots, P_k$. По построению множество M_k бесконечно, следовательно, в нем есть элемент $l \geq n$. Так как $l \in M_k$, то $g_l(P_1) = g(P_1), \ldots, g_l(P_k) = g(P_k)$. Заметим, что $A_n \in \Delta_l$, а g_l — такая оценка, при которой все формулы из Δ_l принимают значение 1. Следовательно, $g_l(A_n) = 1$. Но оценка g совпадает с оценкой g_l на всех переменных, входящих в A_n, и по теореме 2.3 $g(A_n) = g_l(A_n) = 1$, что и требовалось доказать. □

Невыполнимое множество высказываний называется также *несовместным* множеством.

Теорема 2.10. *Множество пропозициональных формул несовместно тогда и только тогда, когда несовместно некоторое конечное его подмножество.*

Доказательство. Очевидно, что если некоторое (не обязательно конечное) подмножество множества высказываний Γ несовместно, то и множество Γ несовместно. Обратно, пусть множество Γ несовместно. Допустим, однако, что всякое конечное его подмножество выполнимо. Тогда, по теореме компактности (теорема 2.9) множество Γ также выполнимо. Полученное противоречие показывает, что существует конечное несовместное подмножество множества Γ. □

Задачи

1) Доказать, что следующие формулы выполнимы:

   а) $\neg(P \supset P)$;

   б) $(P \supset Q) \supset (Q \supset P)$;

   в) $(Q \supset P \,\&\, R) \,\&\, (P \vee R \supset Q)$.

2) Определить, выполнимы ли следующие множества формул:

   а) $\{P \vee Q \vee R, P \supset R, \neg Q\}$;

   б) $\{P \vee Q \vee R, P \supset R, \neg R\}$;

   в) $\{P \vee Q \vee R, P \supset Q, \neg Q, \neg R\}$;

г) $\{P \vee Q, Q \supset R, P \supset Q\}$;

д) $\{P \vee Q, Q \supset R, \neg R\}$;

е) $\{P \vee Q, Q \supset R, P \supset Q, \neg R\}$.

2.11. Логическое следование в логике высказываний

Обычным занятием для математиков является установление того факта, что некоторое утверждение вытекает или, как говорят, логически следует из аксиом. Одной из задач математической логики является уточнение понятия логического следования. Интуитивно, тот факт, что утверждение A логически вытекает из утверждений $A_0, \ldots, A_n$, обычно понимается так, что утверждение A истинно всегда, когда истинны утверждения $A_0, \ldots, A_n$. В логике высказываний это понятие уточняется следующим образом: говорят, что пропозициональная формула A *логически следует* из множества пропозициональных формул Γ, и пишут $\Gamma \models A$, если $g(A) = 1$ для любой оценки g, при которой все формулы из Γ принимают значение 1. Если $\Gamma = \{A_0, \ldots, A_n\}$, то вместо $\Gamma \models A$ иногда пишут $A_0, \ldots, A_n \models A$.

Теорема 2.11. *Каковы бы ни были формулы $A_0, \ldots, A_n, A$, имеет место*

$$A_0, \ldots, A_n \models A \tag{6}$$

тогда и только тогда, когда формула

$$A_0 \supset (\ldots (A_{n-1} \supset (A_n \supset A)) \ldots) \tag{7}$$

является тавтологией.

Доказательство. Пусть имеет место (6). Докажем, что формула (7) является тавтологией. Пусть g — произвольная оценка. Очевидно, что если при этой оценке хотя бы одна из формул $A_0, \ldots, A_n$ принимает значение 0, то формула (7) принимает значение 1. Если же при оценке g все формулы $A_0, \ldots, A_n$ принимают значение 1, то в силу (6) $g(A) = 1$, и формула (7) принимает значение 1. Таким образом, при любой оценке g формула (7) принимает значение 1, следовательно, она является тавтологией.

Пусть формула (7) является тавтологией, т. е. при любой оценке принимает значение 1. Докажем (6). Пусть g — такая оценка, при которой все формулы $A_0, \ldots, A_n$ принимают значение 1. Так как и формула (7) принимает при этой оценке значение 1, то необходимо $g(A) = 1$. Таким образом, для любой оценки g, при которой все формулы $A_0, \ldots, A_n$ принимают значение 1, имеет место $g(A) = 1$, что и означает (6). □

Теорема 2.12. *Каковы бы ни были множество пропозициональных формул Γ и формула A, имеет место*

$$\Gamma \models A, \tag{8}$$

если и только если множество $\Gamma \cup \{\neg A\}$ несовместно.

Доказательство. Пусть имеет место (8). Допустим, что множество $\Gamma \cup \{\neg A\}$ выполнимо. Значит, существует такая оценка g, что все формулы из Γ принимают значение 1 и $g(\neg A) = 1$, т. е. $g(A) = 0$, что невозможно в силу (8). Значит, на самом деле множество $\Gamma \cup \{\neg A\}$ несовместно.

Пусть множество $\Gamma \cup \{\neg A\}$ несовместно. Докажем, что имеет место (8). Пусть g — такая оценка, что все формулы из Γ принимают значение 1. Тогда обязательно $g(A) = 1$, ибо в противном случае $g(\neg A) = 1$, и множество $\Gamma \cup \{\neg A\}$ выполнимо. Значит, $g(A) = 1$ для любой оценки g, при которой все формулы из Γ принимают значение 1, т. е. имеет место (8). □

Задачи

1) Среди формул $Q \vee R$, $P \vee \neg Q \supset R$, $P \,\&\, \neg Q$ найти все такие, которые логически следуют из множества формул $\{(P \supset Q) \,\&\, (P \vee R), P \supset R\}$.

2) Доказать, что если формула A логически следует из бесконечного множества формул Γ, то существует такое конечное подмножество Δ множества Γ, что $\Delta \models A$.

3) Доказать, что если формула A логически следует из бесконечного множества формул Γ, то существуют такие формулы $A_0, \ldots, A_n$ из Γ, что формула $A_0 \supset (\ldots (A_{n-1} \supset (A_n \supset A)) \ldots)$ является тавтологией.

3. Алгебра логики

3.1. Пропозициональные формулы в произвольном базисе

Как было отмечено в разделе 2.1, каждой логической операции φ соответствует подходящая булева (или логическая) функция f_φ. Будем отождествлять логические операции, которым соответствует одна и та же булева функция.

Наряду с обычными логическими операциями $\neg$, $\&$, $\vee$, $\supset$, $\equiv$ в математической логике рассматриваются следующие двуместные логические операции: $+$ (сложение), $|$ (штрих Шеффера), $\downarrow$ (стрелка Пирса). Смысл этих логических операций полностью определяется соответствующими им булевыми функциями:

X	Y	$f_+(X,Y)$	$f_\mid(X,Y)$	$f_\downarrow(X,Y)$
0	0	0	1	1
0	1	1	1	0
1	0	1	1	0
1	1	0	0	0

Пусть дан некоторый набор логических операций $F = \{\varphi_1, \ldots, \varphi_n\}$. Этот набор может включать и 0-местные операции, т. е. константы 0 и 1. Обозначения $\varphi_1, \ldots, \varphi_n$ операций из набора F будем называть логическими связками. *Пропозициональные формулы в базисе* F — это слова в алфавите $V \cup \{\varphi_1, \ldots, \varphi_n, (,), ,\}$, определяемые индуктивно следующим образом:

1) все константы из F и все пропозициональные переменные суть формулы в базисе F (такие формулы называются *атомными*);

2) если φ — символ n-местной логической операции из F, а $A_1, \ldots, A_n$ — формулы в базисе F, то слово $\varphi(A_1, \ldots, A_n)$ — формула в базисе F.

Если φ — символ одноместной логической операции из F, то вместо $\varphi(A)$ условимся писать (φA), а если φ — символ двуместной логической операции из F, то вместо $\varphi(A, B)$ будем писать $(A \varphi B)$.

Как и в случае обычных пропозициональных формул, для формул в базисе F доказывается теорема о единственности логического анализа, определяется значение такой формулы при данной оценке, определяется понятие равносильности формул в базисе F, доказывается теорема об эквивалентной замене.

Будем говорить, что n-местная логическая операция φ *выражается через логические операции из множества* F, если существует такая формула A в базисе F, что $\varphi(P_1, \ldots, P_n) \sim A$. Выразить n-местную логическую операцию φ через логические операции из множества F — это значит построить такую формулу A в базисе F, что $\varphi(P_1, \ldots, P_n) \sim A$. Множество логических операций F называется *полным*, если любая логическая операция выражается через логические операции из множества F.

Задачи

1) Сколько существует различных n-местных булевых функций?

2) Выразить

   а) $\&$ и $\supset$ через $\vee$ и $\neg$;

   б) $\vee$ и $\supset$ через $\&$ и $\neg$;

   в) $\vee$ и $\&$ через $\supset$ и $\neg$;

   г) $\neg$ через $\supset$ и 0;

   д) $\neg$ через $+$ и 1;

   е) $\vee$ через $\supset$;

   ж) $\supset$ через $\equiv$ и $\&$.

3) Доказать, что нельзя выразить

   а) $\neg$ через $\&$, $\vee$, $\supset$ и $\equiv$;

   б) $\supset$ через $\&$ и $\vee$;

   в) $\&$ через $\supset$ и $\vee$.

4) Говорят, что логическая операция φ сохраняет 0 (1), если имеет место равносильность $\varphi(0,\ldots,0) \sim 0$ (соответственно, $\varphi(1,\ldots,1) \sim 1$). Сколько существует различных n-местных логических операций, сохраняющих 0 (1)?

5) Доказать, что следующие множества логических операций являются полными:

   а) $\{\&, \vee, \neg\}$;

   б) $\{\vee, \neg\}$;

   в) $\{\&, \neg\}$;

   г) $\{\supset, \neg\}$;

   д) $\{|\}$;

   е) $\{\downarrow\}$;

   ж) $\{\supset, 0\}$;

   з) $\{+, \vee, 1\}$.

6) Доказать, что следующие множества логических операций не являются полными:

   а) $\{\&, \vee, \supset\}$;

   б) $\{\neg\}$.

3.2. Замкнутые классы логических операций

Множество логических операций F называется *замкнутым*, если через операции из F выражаются только операции, принадлежащие множеству F. Например, нетрудно убедиться, что множество логических операций, сохраняющих 0 (см. задачу 4 из раздела 3.1), которое мы будем обозначать C_0, является замкнутым. Замкнуто также множество C_1 всех логических операций, сохраняющих 1. Рассмотрим некоторые другие замкнутые множества логических операций, которые будут играть важную роль в дальнейшем.

3.2.1. Самодвойственные логические операции

Оценка g^* называется *двойственной* к оценке g, если $g^*(P_i) \neq g(P_i)$ для любой переменной P_i; иными словами,

$$g^*(P_i) = \begin{cases} 0, & \text{если } g(P_i) = 1, \\ 1, & \text{если } g(P_i) = 0. \end{cases}$$

Пропозициональная формула A называется *двойственной* к пропозициональной формуле B, если для любой оценки g выполняется условие $g^*(A) \neq g(B)$. Если формула A двойственна к формуле B, то истинностная таблица для A получается из истинностной таблицы для B заменой в ней всюду 0 на 1, а 1 на 0. Пропозициональная формула A называется *самодвойственной*, если она двойственна к самой себе, т. е. $g^*(A) \neq g(A)$ для любой оценки g. Очевидно, что если формула A является самодвойственной, то всякая формула, равносильная формуле A, также является самодвойственной. Говорят, что n-местная логическая операция φ является *двойственной* к n-местной же логической операции ψ, если формула $\varphi(P_1,\ldots,P_n)$ двойственна к формуле $\psi(P_1,\ldots,P_n)$, иными словами, если $\varphi(P_1,\ldots,P_n) \sim \neg\psi(\neg P_1,\ldots,\neg P_n)$. Например, операция $\&$ двойственна к операции $\vee$, а операция $\vee$ двойственна к операции $\&$. Очевидно, что операция φ двойственна к операции ψ, если для любого набора нулей и единиц $\alpha = \alpha_1,\ldots,\alpha_n$ имеет место $f_\varphi(\alpha) \neq f_\psi(\alpha^*)$, где α^* — набор, двойственный набору α (см. раздел 2.8). Логическая операция, двойственная к самой себе, называется самодвойственной. n-местная логическая операция φ является самодвойственной, если формула $\varphi(P_1,\ldots,P_n)$ самодвойственна. В этом случае имеет место равносильность $\neg\varphi(P_1,\ldots,P_n) \sim \varphi(\neg P_1,\ldots,\neg P_n)$. Например, операция $\neg$ является самодвойственной. Очевидно, что операция φ является самодвойственной, если для любого набора нулей и единиц $\alpha = \alpha_1,\ldots,\alpha_n$ имеет место $f_\varphi(\alpha) \neq f_\varphi(\alpha^*)$. Через S обозначим множество всех самодвойственных логических операций.

Теорема 3.1. *Множество логических операций S является замкнутым.*

Доказательство. Для доказательства теоремы достаточно показать, что каждая формула A в базисе S является самодвойственной. Докажем это индукцией по построению формулы A. В случае, когда A есть атом P_i, для любой оценки g имеем: $g(A) = g(P_i) \neq g^*(P_i) = g^*(A)$, т. е. $g(A) \neq g^*(A)$, что и требовалось доказать. Пусть A имеет вид $\varphi(A_1,\ldots,A_n)$, где $\varphi \in S$, а $A_1,\ldots,A_n$ — формулы в базисе S. Предположим, что формулы $A_1,\ldots,A_n$ являются самодвойственными, и докажем, что A — самодвойственная формула.

Пусть g — произвольная оценка, $\alpha_i = g(A_i)$ $(i = 1, \ldots, n)$. Тогда, очевидно, для любого $i = 1, \ldots, n$ имеет место равенство $g^*(A_i) = (\alpha_i)^*$ в силу самодвойственности формул A_i. Положим $\alpha = \alpha_1, \ldots, \alpha_n$. Тогда

$$g(A) = f_\varphi(g(A_1), \ldots, g(A_n)) = f_\varphi(\alpha),$$
$$g^*(A) = f_\varphi(g^*(A_1), \ldots, g^*(A_n)) = f_\varphi(\alpha^*).$$

Но $f_\varphi(\alpha) \neq f_\varphi(\alpha^*)$, так как φ — самодвойственная операция. Таким образом, $g(A) \neq g^*(A)$, что и требовалось доказать. □

3.2.2. Линейные логические операции

Формула A, не содержащая переменных, отличных от $Q_1, \ldots, Q_n$, называется *линейной*, если она равносильна формуле в базисе $\{0, 1, +\}$ вида $\alpha_0 + \alpha_1 \& Q_1 + \ldots + \alpha_n \& Q_n$, где $\alpha_i \in \{0, 1\}$ $(i = 1, \ldots, n)$. В этом случае формулу $\alpha_0 + \alpha_1 \& Q_1 + \ldots + \alpha_n \& Q_n$ будем называть линейным выражением для формулы A. Очевидно, что если формула A является линейной, то всякая формула, равносильная формуле A, также является линейной. n-местная логическая операция φ называется линейной, если формула $\varphi(P_1, \ldots, P_n)$ является линейной. Через L обозначим множество всех линейных логических операций.

Теорема 3.2. *Множество логических операций L является замкнутым.*

Доказательство. Для доказательства теоремы достаточно показать, что каждая формула A в базисе L является линейной. Докажем это индукцией по построению формулы A. В случае, когда формула A есть атом P_i, она имеет линейное выражение $0 + 1 \& P_i$, что и требовалось доказать. Пусть A имеет вид $\varphi(A_1, \ldots, A_n)$, где $\varphi \in L$, а $A_1, \ldots, A_n$ — формулы в базисе L. Предположим, что формулы $A_1, \ldots, A_n$ являются линейными, и докажем, что A — линейная формула. В силу линейности операции φ имеет место равносильность $\varphi(P_1, \ldots, P_n) \sim \alpha_0 + \alpha_1 \& P_1 + \ldots + \alpha_n \& P_n$. Следовательно, по теореме об эквивалентной замене, $\varphi(A_1, \ldots, A_n) \sim \alpha_0 + \alpha_1 \& A_1 + \ldots + \alpha_n \& A_n$. Теперь видно, что если в правую часть этой равносильности вместо формул $A_1, \ldots, A_n$ подставить их линейные выражения, а затем, пользуясь истинностной таблицей для операции $+$, а также свойствами коммутативности и ассоциативности этой операции, привести подобные члены, то получится линейное выражение для формулы $\varphi(A_1, \ldots, A_n)$. □

3.2.3. Монотонные логические операции

Будем говорить, что оценка h *мажорирует* оценку g, и писать $g \leq h$, если $g(P_i) \leq h(P_i)$ для любой переменной P_i. Формула A называется *монотонной*, если $g(A) \leq h(A)$ всякий раз, когда $g \leq h$. Очевидно, что если формула A является монотонной, то всякая формула, равносильная формуле A, также является монотонной. n-местная логическая операция φ называется монотонной, если формула $\varphi(P_1, \ldots, P_n)$ является монотонной. Пусть $\alpha = \alpha_1, \ldots, \alpha_n$ и $\beta = \beta_1, \ldots, \beta_n$ — наборы нулей и единиц. Будем писать $\alpha \leq \beta$, если $\alpha_i \leq \beta_i$ для любого $i = 1, \ldots, n$. Очевидно, что операция φ является монотонной, если $f_\varphi(\alpha) \leq f_\varphi(\beta)$ всякий раз, когда $\alpha \leq \beta$. Через M обозначим множество всех монотонных логических операций.

Теорема 3.3. *Множество логических операций M является замкнутым.*

Доказательство. Для доказательства теоремы достаточно показать, что каждая формула A в базисе M является монотонной. Докажем это индукцией по построению формулы A. В случае, когда формула A есть атом P_i, утверждение очевидно. Пусть A имеет вид $\varphi(A_1, \ldots, A_n)$, где $\varphi \in M$, а $A_1, \ldots, A_n$ — формулы в базисе M. Предположим, что формулы $A_1, \ldots, A_n$ являются монотонными, и докажем, что A — монотонная формула. Пусть g и h — такие оценки, что $g \leq h$. Положим $\alpha_i = g(A_i)$, $\beta_i = h(A_i)$ $(i = 1, \ldots, n)$, $\alpha = \alpha_1, \ldots, \alpha_n$, $\beta = \beta_1, \ldots, \beta_n$. Тогда $\alpha \leq \beta$ в силу монотонности формул $A_1, \ldots, A_n$, и $f_\varphi(\alpha) \leq f_\varphi(\beta)$. Теперь имеем: $g(A) = f_\varphi(g(A_1), \ldots, g(A_n)) = f_\varphi(\alpha) \leq f_\varphi(\beta) = f_\varphi(h(A_1), \ldots, h(A_n)) = h(A)$. Таким образом, $g(A) \leq h(A)$, что и требовалось доказать. □

Задачи

1) Найти логические операции, двойственные константам 0, 1 и операциям $\supset$, $\equiv$, $+$, $|$, $\downarrow$.

2) Найти все самодвойственные двуместные логические операции.

3) Сколько существует различных самодвойственных n-местных логических операций?

4) Сколько существует различных линейных n-местных логических операций?

5) Найти все линейные двуместные логические операции.

6) Найти все монотонные двуместные логические операции.

3.3. Многочлены

Пусть $Q_1, \ldots, Q_n$ — различные переменные. *Одночленом* над списком $Q_1, \ldots, Q_n$ назовем константу 1 и любую формулу вида $Q_{i_1} \& \ldots \& Q_{i_m}$, где $1 \le i_1 < \ldots < i_m \le n$. Очевидно, что имеется ровно 2^n различных одночленов над списком $Q_1, \ldots, Q_n$. *Многочленом* над списком $Q_1, \ldots, Q_n$ будем называть константу 0, а также любую формулу вида $A_1 + \ldots + A_m$, где $A_1, \ldots, A_m$ — различные одночлены над списком $Q_1, \ldots, Q_n$. Многочлены называются также *полиномами Жегалкина*. Будем отождествлять многочлены, составленные из одних и тех же одночленов и различающиеся лишь порядком, в котором они выписаны. Тогда, очевидно, существует ровно 2^{2^n} различных многочленов над списком $Q_1, \ldots, Q_n$.

Теорема 3.4. *Пусть пропозициональная формула A содержит лишь переменные из списка $Q_1, \ldots, Q_n$. Тогда существует ровно один многочлен над списком $Q_1, \ldots, Q_n$, равносильный формуле A.*

Доказательство. Построим для формулы A истинностную таблицу относительно списка $Q_1, \ldots, Q_n$. Если формула A — противоречие, она равносильна многочлену 0. В противном случае пусть $\alpha^1, \ldots, \alpha^m$ — все различные наборы значений переменных $Q_1, \ldots, Q_n$, на которых формула A принимает значение 1, и пусть $K_1, \ldots, K_m$ — стандартные конъюнкты над списком $Q_1, \ldots, Q_n$, соответствующие наборам $\alpha^1, \ldots, \alpha^m$ (см. раздел 2.8). Очевидно, что формула $K_1 + \ldots + K_m$ принимает значение 1 в точности на наборах $\alpha^1, \ldots, \alpha^m$, следовательно, она равносильна формуле A. В каждом из конъюнктов $K_1, \ldots, K_m$ заменим всякую литеру вида $\neg Q_i$ на равносильную ей формулу $(Q_i + 1)$. После этого, пользуясь законом дистрибутивности конъюнкции относительно операции $+$, выражающимся равносильностями $A \& (B + C) \sim A \& B + A \& C$ и $(B + C) \& A \sim B \& A + C \& A$, заменим каждый конъюнкт K_j на равносильный ему многочлен. В полученной формуле, которая представляет собой сумму многочленов, приведем подобные члены, пользуясь равносильностями $A + A \sim 0$ и $A + 0 \sim A$. В результате получим многочлен, равносильный формуле $K_1 + \ldots + K_m$, а значит, и формуле A. Таким образом, доказано существование многочлена, равносильного формуле A. Единственность такого многочлена немедленно вытекает из приведенного выше подсчета числа различных многочленов над списком $Q_1, \ldots, Q_n$. Их оказалось 2^{2^n} — ровно столько же, сколько и различных истинностных таблиц относительно списка $Q_1, \ldots, Q_n$. Значит, различные многочлены над списком $Q_1, \ldots, Q_n$ имеют различные истинностные таблицы относительно этого списка и потому не могут быть равносильны одной и той же формуле. □

В разделе 2.4 мы построили истинностную таблицу для формулы $P \supset (Q \vee R \supset (R \supset \neg P))$. Построим многочлен, равносильный отрицанию этой формулы. Действуем в соответствии с доказательством теоремы 3.4. Формула $\neg(P \supset (Q \vee R \supset (R \supset \neg P)))$ принимает значение 1 только на наборах 101 и 111, поэтому она равносильна формуле $P \& \neg Q \& R + P \& Q \& R$. Заменив здесь подформулу $\neg Q$ на равносильную ей формулу $Q + 1$, получим $P \& (Q + 1) \& R + P \& Q \& R$. Пользуясь дистрибутивностью операции $\&$ относительно $+$ и равносильностью $A \& 1 \& B \sim A \& B$, получаем равносильную формулу $P \& Q \& R + P \& R + P \& Q \& R$. Первое и третье слагаемые в этой формуле «взаимно уничтожаются», так что формула $\neg(P \supset (Q \vee R \supset (R \supset \neg P)))$ равносильна многочлену $P \& R$.

Задачи

1) Найти многочлен над списком переменных P, Q, R, S, принимающий значение 1 только на наборах

   а) 1110, 1101, 1011, 0111; б) 1000, 0100, 0010, 0001; в) 1100, 1001, 1010, 0110, 0101, 0011, 1111.

2) Найти многочлены, равносильные формулам $\neg P$, $P \& Q$, $P \vee Q$, $P \supset Q$, $P \equiv Q$, $P|Q$, $P \downarrow Q$, $P \vee Q \vee R$, $P \& Q \vee Q \& R \vee P \& R$, $P \& Q \& \neg R \vee P \& \neg Q \& R \vee \neg P \& Q \& R$. $(P \supset Q) \supset R$.

3) Какие из формул, перечисленных в предыдущей задаче, являются линейными?

3.4. Критерий полноты множества логических операций

В разделе 3.2 были рассмотрены пять замкнутых классов логических операций: C_0 — класс операций, сохраняющих 0; C_1 — класс операций, сохраняющих 1; S — класс самодвойственных операций; L — класс линейных операций; M — класс монотонных операций. Так как каждый из этих классов замкнут и не совпадает с множеством всех логических операций, то очевидно, что если некоторое множество логических операций F содержится в одном из классов C_0, C_1, S, L, M, то F не является полным. Оказывается, что верно и обратное: если множество логических операций не является полным, то оно включено в один из классов C_0, C_1, S, L, M. Для доказательства этого факта нам потребуются некоторые вспомогательные утверждения.

Теорема 3.5. *Пусть φ — произвольная несамодвойственная логическая операция. Тогда можно выразить 0 и 1 через φ и $\neg$.*

Доказательство. Пусть φ есть n-местная несамодвойственная логическая операция. Тогда существует такой набор нулей и единиц $\alpha = \alpha_1, \ldots, \alpha_n$, что $f_\varphi(\alpha) = f_\varphi(\alpha^*)$. Допустим, что $f_\varphi(\alpha) = f_\varphi(\alpha^*) = 0$. Пусть A_i есть переменная P, если $\alpha_i = 0$, и формула $\neg P$, если $\alpha_i = 1$. Заметим, что для любой оценки g, если $g(P) = 0$, то $g(A_i) = \alpha_i$, а если $g(P) = 1$, то $g(A_i) = \alpha_i^*$. Формула $\varphi(A_1, \ldots, A_n)$ является формулой в базисе $\{\varphi, \neg\}$ и содержит только переменную P. Докажем, что эта формула равносильна формуле 0. Пусть дана произвольная оценка g. Если $g(P) = 0$, то $g(\varphi(A_1, \ldots, A_n)) = f_\varphi(g(A_1), \ldots, g(A_n)) = f_\varphi(\alpha) = 0$. Если же $g(P) = 1$, то $g(\varphi(A_1, \ldots, A_n)) = f_\varphi(g(A_1), \ldots, g(A_n)) = f_\varphi(\alpha^*) = 0$. Итак, мы доказали, что $0 \sim \varphi(A_1, \ldots, A_n)$. Тогда $1 \sim \neg\varphi(A_1, \ldots, A_n)$. Таким образом, 0 и 1 выражаются через φ и $\neg$. Совершенно аналогично доказывается, что если $f_\varphi(\alpha) = f_\varphi(\alpha^*) = 1$, то $1 \sim \varphi(A_1, \ldots, A_n)$, $0 \sim \neg\varphi(A_1, \ldots, A_n)$. □

Теорема 3.6. *Пусть φ — произвольная немонотонная логическая операция. Тогда можно выразить $\neg$ через φ и константы 0 и 1.*

Доказательство. Пусть φ — некоторая n-местная немонотонная логическая операция. Тогда существуют такие наборы нулей и единиц $\alpha = \alpha_1, \ldots, \alpha_n$, $\beta = \beta_1, \ldots, \beta_n$, что $\alpha \leq \beta$, но $f_\varphi(\alpha) > f_\varphi(\beta)$, т. е. $f_\varphi(\alpha) = 1$, $f_\varphi(\beta) = 0$. Пусть A_i есть переменная P, если $\alpha_i < \beta_i$ (т. е. $\alpha_i = 0$, $\beta_i = 1$), и константа α_i, если $\alpha_i = \beta_i$. Заметим, что для любой оценки g, если $g(P) = 0$, то $g(A_i) = \alpha_i$, а если $g(P) = 1$, то $g(A_i) = \beta_i$. Формула $\varphi(A_1, \ldots, A_n)$ является формулой в базисе $\{\varphi, 0, 1\}$ и содержит только переменную P. Докажем, что эта формула равносильна формуле $\neg P$. Пусть дана произвольная оценка g. Если $g(P) = 0$, то

$$g(\varphi(A_1, \ldots, A_n)) = f_\varphi(g(A_1), \ldots, g(A_n)) = f_\varphi(\alpha) = 1.$$

Если же $g(P) = 1$, то

$$g(\varphi(A_1, \ldots, A_n)) = f_\varphi(g(A_1), \ldots, g(A_n)) = f_\varphi(\beta) = 0.$$

Итак, мы доказали, что $\neg P \sim \varphi(A_1, \ldots, A_n)$, т. е. $\neg$ выражается через φ и константы 0 и 1. □

Теорема 3.7. *Пусть φ — произвольная нелинейная логическая операция. Тогда можно выразить $\&$ через φ, 0, 1 и $\neg$.*

Доказательство. Пусть φ — некоторая n-местная нелинейная логическая операция. В силу теоремы 3.4, существует многочлен над списком переменных $P_1, \ldots, P_n$, равносильный формуле $\varphi(P_1, \ldots, P_n)$. Поскольку операция φ не является линейной, то многочлен, равносильный формуле $\varphi(P_1, \ldots, P_n)$, обязательно должен содержать одночлен, не являющийся константой 1 или переменной. Без потери общности можно считать, что в нем есть хотя бы один одночлен, содержащий конъюнкцию $P \,\&\, Q$. Пользуясь законами коммутативности и ассоциативности операции $+$, а также законами дистрибутивности конъюнкции относительно операции $+$, рассматриваемый многочлен можно привести к равносильному виду $P \,\&\, Q \,\&\, A + P \,\&\, B + Q \,\&\, C + D$, где A, B, C, D — многочлены, не содержащие переменных P и Q. Заметим, что формула A не является противоречием, так как в противном случае мы получили бы другое представление формулы $\varphi(P_1, \ldots, P_n)$ в виде многочлена, равносильного формуле $P \,\&\, B + Q \,\&\, C + D$, что противоречило бы единственности представления логической операции в виде многочлена. Значит, $g(A) = 1$ для некоторой оценки g. Для $i = 3, \ldots, n$ пусть $\alpha_i = g(P_i)$. В формулы B, C, D вместо каждой переменной P_i $(i = 3, \ldots, n)$ подставим константу α_i. Очевидно, что существуют такие константы b, c, d, что $b \sim B(P_3 \backslash \alpha_3, \ldots, P_n \backslash \alpha_n)$, $c \sim C(P_3 \backslash \alpha_3, \ldots, P_n \backslash \alpha_n)$, $d \sim D(P_3 \backslash \alpha_3, \ldots, P_n \backslash \alpha_n)$. Тогда формула $\varphi(P, Q, \alpha_3, \ldots, \alpha_n)$ равносильна формуле $P \,\&\, Q + b \,\&\, P + c \,\&\, Q + d$. Простыми преобразованиями нетрудно убедиться, что формула $P \,\&\, Q$ равносильна формуле $\varphi(P + c, Q + b, \alpha_3, \ldots, \alpha_n) + bc + d$, а последняя — формуле в базисе $\{\varphi, 0, 1, \neg\}$ (действительно, например, $P + c \sim P$, если $c = 0$, и $P + c \sim \neg P$, если $c = 1$). Таким образом, формула $P \,\&\, Q$ равносильна формуле в базисе $\{\varphi, 0, 1, \neg\}$, т. е. $\&$ выражается через φ, 0, 1 и $\neg$. □

Теперь можно доказать теорему Поста, дающую критерий полноты множества логических операций.

Теорема 3.8 (теорема Поста). *Множество логических операций является полным тогда и только тогда, когда оно не содержится ни в одном из классов C_0, C_1, S, L, M.*

Доказательство. Как уже отмечалось выше, тот факт, что полное множество логических операций не содержится ни в одном из классов C_0, C_1, S, L, M, следует из замкнутости этих классов и существования логических операций, не входящих в эти классы. Докажем обратное утверждение.

Пусть F — некоторое множество логических операций, не содержащееся ни в одном из классов C_0, C_1, S, L, M. Пусть $\varphi_0 \in F \setminus C_0$, $\varphi_1 \in F \setminus C_1$, $\varphi_s \in F \setminus S$, $\varphi_l \in F \setminus L$, $\varphi_m \in F \setminus M$ (среди операций φ_0, φ_1, φ_s,

φ_l, φ_m могут быть одинаковые). Через A обозначим формулу $\varphi_0(P,\dots,P)$. Пусть g_0 — такая оценка, что $g_0(P)=0$. Тогда $g_0(A)=1$, так как φ_0 не сохраняет 0. Рассмотрим теперь оценку g_1 такую, что $g_1(P)=1$. Если $g_1(A)=1$, то, очевидно, $A\sim 1$. Если же $g_1(A)=0$, то $A\sim\neg P$. Аналогично убеждаемся, что если B — это формула $\varphi_1(P,\dots,P)$, то либо $B\sim 0$, либо $B\sim\neg P$. Таким образом, либо 1) через операции φ_0 и φ_1 выражаются обе константы 0 и 1, либо 2) через операции φ_0 и φ_1 выражается операция $\neg$. В случае 1), в силу теоремы 3.6, используя операцию φ_m, можно выразить операцию $\neg$, а в случае 2), в силу теоремы 3.5, используя операцию φ_s, можно выразить константы 0 и 1. Таким образом, мы доказали, что через операции из множества F можно выразить 0, 1 и $\neg$. Теперь, в силу теоремы 3.7, используя операцию φ_l, можно выразить операцию $\&$. Итак, через операции из множества F можно выразить $\neg$ и $\&$, а так как множество $\{\neg,\&\}$ является полным, то полно и множество F. $\square$

Множество логических операций F называется *независимым*, если никакую операцию $\varphi\in F$ нельзя выразить через операции из $F\setminus\{\varphi\}$. Полное независимое множество логических операций называется *базисом* для множества всех логических операций.

Теорема 3.9. *Всякий базис для множества всех логических операций содержит не более четырех функций.*

Доказательство. В силу теоремы 3.8 любой базис содержит не более пяти логических операций, так как в полном множестве операций F обязательно содержатся операции $\varphi_0\notin C_0$, $\varphi_1\notin C_1$, $\varphi_s\notin S$, $\varphi_l\notin L$, $\varphi_m\notin M$. Как видно из доказательства теоремы 3.8, через операции φ_0 и φ_1 либо выражаются обе константы 0 и 1, не являющиеся самодвойственными, так что можно обойтись без операции φ_s, либо выражается операция $\neg$, не являющаяся монотонной, так что можно обойтись без операции φ_m. $\square$

Задачи

1) Доказать, что трехместная логическая операция ψ, задаваемая многочленом $P\&Q+P\&R+Q\&R$, является самодвойственной.

2) Доказать, что если к множеству C_0 присоединить логическую операцию, не сохраняющую 0, то получится полное множество операций.

3) Доказать, что если к множеству C_1 присоединить логическую операцию, не сохраняющую 1, то получится полное множество операций.

4) Доказать, что если к множеству S присоединить несамодвойственную логическую операцию, то получится полное множество операций.

5) Доказать, что если к множеству L присоединить нелинейную логическую операцию, то получится полное множество операций.

6) Доказать, что если к множеству M присоединить немонотонную логическую операцию, то получится полное множество операций.

7) Найти все такие двуместные логические операции φ, что $\{\varphi\}$ — базис для множества всех логических операций.

8) Доказать, что следующие множества логических операций независимы:

   а) $\{\neg,\equiv\}$; б) $\{\neg,+\}$; в) $\{\equiv,+\}$; г) $\{\equiv,\vee\}$.

9) Доказать, что следующие множества логических операций являются базисами для множества всех логических операций:

   а) $\{\supset,\not\subset\}$, где $P\not\subset Q\sim\neg(Q\supset P)$; б) $\{\equiv,\vee,0\}$.

10) Найти все базисы для множества всех логических операций, составленные из операций 0, 1, $\neg$, $\&$, $\vee$, $\supset$, $\equiv$, $+$, $|$, $\downarrow$.

11) Является ли замкнутым класс всех монотонно убывающих логических операций?

12) С помощью теоремы Поста доказать, что следующие множества логических операций, где $\sigma(P,Q,R)\sim P+Q+R$, не являются полными:

    а) $\{0,\&,\sigma\}$; б) $\{1,\&,\sigma\}$.

4. Исчисление высказываний

4.1. Общее понятие исчисления

Путем построения истинностной таблицы для данной пропозициональной формулы нетрудно проверить, является ли эта формула общезначимой. Однако представляет интерес и другой способ описания общезначимых формул — с помощью исчисления.

Пусть Σ — некоторый алфавит. *Исчисление* в алфавите Σ задается путем указания *аксиом* — некоторых выделенных слов в алфавите Σ — и *правил вывода*, позволяющих из одного или нескольких слов в алфавите Σ получать новые слова в алфавите Σ. *Вывод* в данном исчислении — это конечная последовательность слов $w_1, \ldots, w_n$ в алфавите Σ такая, что для каждого $i = 1, \ldots, n$ слово w_i либо является аксиомой, либо получается из каких-нибудь предшествующих слов этой последовательности по одному из правил вывода. Говорят, что слово w в алфавите Σ *выводимо* в данном исчислении, если существует вывод, оканчивающийся словом w. *Вывод из множества слов* Γ (так называемого множества *гипотез*) в данном исчислении — это конечная последовательность слов $w_1, \ldots, w_n$ в алфавите Σ такая, что для каждого $i = 1, \ldots, n$ слово w_i либо является аксиомой, либо является гипотезой (т. е. принадлежит множеству Γ), либо получается из каких-нибудь предшествующих слов этой последовательности по одному из правил вывода. Говорят, что слово w в алфавите Σ *выводимо из множества* Γ в данном исчислении, если существует вывод из Γ, оканчивающийся словом w.

В дальнейшем мы будем рассматривать так называемые *пропозициональные исчисления*. Это исчисления в алфавите логики высказываний, аксиомы которых суть пропозициональные формулы, а правила вывода позволяют из формул получать только формулы. Таким образом, в пропозициональном исчислении могут выводиться только формулы.

4.2. Классическое исчисление высказываний

Аксиомами *классического исчисления высказываний* называются пропозициональные формулы любого из следующих видов, где A, B, C — произвольные формулы:

1) $A \supset (B \supset A)$;

2) $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;

3) $A \,\&\, B \supset A$;

4) $A \,\&\, B \supset B$;

5) $A \supset (B \supset A \,\&\, B)$;

6) $A \supset A \vee B$;

7) $B \supset A \vee B$;

8) $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;

9) $(A \equiv B) \supset (A \supset B)$;

10) $(A \equiv B) \supset (B \supset A)$;

11) $((A \supset B) \,\&\, (B \supset A)) \supset (A \equiv B)$;

12) $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;

13) $\neg\neg A \supset A$.

Выражения 1) – 13) называются *схемами аксиом* классического исчисления высказываний.

Единственным правилом вывода классического исчисления высказываний является модус поненс (modus ponens; сокращенно: MP) — правило, которое позволяет из формул A и $A \supset B$ получить формулу B. Будем говорить, что формула B является *непосредственным следствием* формул A и $A \supset B$. В соответствии с общим определением, выводом в исчислении высказываний считается такая конечная последовательность формул $A_1, \ldots, A_n$, в которой каждая формула является либо аксиомой, либо непосредственным следствием каких-нибудь двух предшествующих формул. Формула A выводима в исчислении высказываний, если существует вывод, оканчивающийся формулой A; в этом случае будем писать $\vdash A$. Очевидно, что всякая аксиома выводима в исчислении высказываний.

Теорема 4.1. *Какова бы ни была формула A, формула $A \supset A$ выводима в классическом исчислении высказываний.*

Доказательство. Следующая последовательность формул является выводом формулы $A \supset A$:

1) $(A \supset (A \supset A)) \supset ((A \supset ((A \supset A) \supset A)) \supset (A \supset A))$ (аксиома 2);

2) $A \supset (A \supset A)$ (аксиома 1);

3) $(A \supset ((A \supset A) \supset A)) \supset (A \supset A)$ (получена по правилу MP из формул 1 и 2);

4) $(A \supset ((A \supset A) \supset A)$ (аксиома 1);

5) $A \supset A$ (получено по правилу MP из формул 3 и 4). □

Следствие 4.1. *Если некоторое пропозициональное исчисление содержит схемы аксиом 1, 2 и правило вывода modus ponens, то, какова бы ни была формула A, в этом исчислении выводима формула $A \supset A$.*

Доказательство. Очевидно, что построенный при доказательстве теоремы 4.1 вывод формулы $A \supset A$ в классическом исчислении высказываний будет выводом в любом пропозициональном исчислении, которое содержит схемы аксиом 1, 2 и правило вывода modus ponens, следовательно, формула $A \supset A$ выводима в любом таком исчислении. □

Пусть Γ — некоторое множество формул. В соответствии с общим определением, выводом из множества гипотез Γ называется такая конечная последовательность формул $A_1, \ldots, A_n$, в которой каждая формула либо является аксиомой, либо принадлежит множеству Γ, либо является непосредственным следствием каких-нибудь двух предшествующих формул. Формула A выводима из гипотез Γ в исчислении высказываний, если существует вывод из гипотез Γ, оканчивающийся формулой A; в этом случае мы будем писать $\Gamma \vdash A$. Очевидно,что всякая аксиома и всякая формула из Γ выводимы из гипотез Γ. Заметим, что всякий вывод в исчислении высказываний является выводом из пустого множества гипотез, поэтому $\vdash A$ означает то же самое, что и $\emptyset \vdash A$.

Следующая последовательность формул является выводом из множества гипотез $\{A \supset B, B \supset C\}$ формулы $A \supset C$, каковы бы ни были формулы A, B, C:

1) $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$ (аксиома 2);

2) $A \supset B$ (гипотеза);

3) $(A \supset (B \supset C)) \supset (A \supset C)$ (получена по правилу MP из формул 1 и 2);

4) $(B \supset C) \supset (A \supset (B \supset C))$ (аксиома 1);

5) $B \supset C$ (гипотеза);

6) $A \supset (B \supset C)$ (получена по правилу MP из формул 4 и 5);

7) $A \supset C$ (получена по правилу MP из формул 3 и 6).

Таким образом, мы доказали $\{A \supset B, B \supset C\} \vdash A \supset C$.

Отметим некоторые очевидные, но важные свойства выводимости.

Теорема 4.2 (монотонность). *Каковы бы ни были множества формул Γ и Δ и формула A, если $\Gamma \subseteq \Delta$ и $\Gamma \vdash A$, то $\Delta \vdash A$.*

Доказательство. Пусть $A_1, \ldots, A_n$ — вывод формулы A из множества формул Γ. Каждая из формул A_i $(i = 1, \ldots, n)$ либо является аксиомой, либо принадлежит множеству Γ (а значит, и множеству Δ), либо является непосредственным следствием предыдущих формул, т. е. последовательность $A_1, \ldots, A_n$ удовлетворяет определению вывода из множества Δ. Таким образом, существует вывод формулы A из Δ, т. е. $\Delta \vdash A$. □

Теорема 4.3 (транзитивность). *Каковы бы ни были множества формул Γ и Δ и формула A, если $\Gamma \vdash A$, и $\Delta \vdash B$ для любой формулы $B \in \Gamma$, то $\Delta \vdash A$.*

Доказательство. Пусть $A_1, \ldots, A_n$ — вывод формулы A из множества формул Γ. Всюду в этом выводе заменим каждую формулу из Γ на ее вывод из множества Δ. Очевидно, что полученная последовательность является выводом формулы A из Δ. □

Теорема 4.4 (компактность). *Пусть* Γ *— произвольное (возможно, бесконечное) множество формул,* A *— произвольная формула. Если* $\Gamma \vdash A$*, то существует конечное подмножество* $\Delta \subseteq \Gamma$ *такое, что* $\Delta \vdash A$*.*

Доказательство. Пусть $A_1, \ldots, A_n$ — вывод формулы A из множества формул Γ. Пусть Δ — множество всех формул из Γ, встречающихся в этом выводе. Очевидно, что последовательность $A_1, \ldots, A_n$ удовлетворяет определению вывода из Δ. Значит, формула A выводима из конечного множества $\Delta \subseteq \Gamma$. □

Теорема 4.5 (теорема о корректности). *Какова бы ни была формула* A*, если* $\vdash A$*, то* A *общезначима.*

Доказательство. Нетрудно убедиться, что каждая аксиома классического исчисления высказываний общезначима. Очевидно также, что если формулы A и $A \supset B$ общезначимы, то и формула B общезначима. Таким образом, непосредственное следствие двух общезначимых формул является общезначимой формулой. Пусть теперь дан вывод $A_1, \ldots, A_n$ формулы A в классическом исчислении высказываний. Индукцией по i нетрудно доказать, что каждая формула A_i в этом выводе общезначима, в частности, общезначима последняя формула в этом выводе, т. е. A. □

Теорема 4.6 (теорема о дедукции). *Для любых формул* A, B *и множества формул* Γ*, если* $\Gamma \cup \{A\} \vdash B$*, то* $\Gamma \vdash A \supset B$*.*

Доказательство. Пусть $A_1, \ldots, A_n$ — вывод формулы B из множества гипотез $\Gamma \cup \{A\}$. Индукцией по i докажем, что $\Gamma \vdash A \supset A_i$ для каждой из формул A_i $(i = 1, \ldots, n)$. Если $i = 1$, то A_i — либо аксиома, либо гипотеза из Γ, либо формула A. Если A_i — аксиома или гипотеза из Γ, то следующая последовательность формул является выводом формулы $A \supset A_i$ из Γ:

1. $A_i \supset (A \supset A_i)$ (аксиома 1);
2. A_i (аксиома или гипотеза);
3. $A \supset A_i$ (получено по правилу MP из 1. и 2.).

Если же A_i совпадает с A, то построенный в теореме 4.1 вывод формулы $A \supset A$ является выводом из Γ формулы $A \supset A_i$.

Допустим, что для некоторого $k < n$ выполнено, что для каждой из формул $A_1, \ldots, A_k$ формула $A \supset A_i$ $(i = 1, \ldots, k)$ выводима из Γ. Докажем, что формула $A \supset A_{k+1}$ выводима из Γ. Если A_{k+1} — аксиома или гипотеза из $\Gamma \cup \{A\}$, утверждение доказывается точно так же, как в случае $i = 1$. Пусть формула A_{k+1} — непосредственное следствие формулы A_i и формулы A_j (имеющей вид $A_i \supset A_{k+1}$), где $i, j \leq k$. По индуктивному предположению,

$$\Gamma \vdash A \supset A_i, \Gamma \vdash A \supset (A_i \supset A_{k+1}). \tag{9}$$

Следующая последовательность формул является выводом из множества гипотез $\{A \supset A_i, A \supset (A_i \supset A_{k+1})\}$ формулы $A \supset A_{k+1}$:

1. $(A \supset A_i) \supset ((A \supset (A_i \supset A_{k+1})) \supset (A \supset A_{k+1}))$ (аксиома 2);
2. $A \supset A_i$ (гипотеза);
3. $(A \supset (A_i \supset A_{k+1})) \supset (A \supset A_{k+1})$ (получено по правилу MP из формул 1 и 2);
4. $A \supset (A_i \supset A_{k+1})$ (гипотеза):
5. $A \supset A_{k+1}$ (получено по правилу MP из формул 3 и 4).

Таким образом, мы доказали, что $\{A \supset A_i, A \supset (A_i \supset A_{k+1})\} \vdash A \supset A_{k+1}$. Отсюда и из (9) в силу свойства транзитивности выводимости вытекает $\Gamma \vdash A \supset A_{k+1}$, что и требовалось. Так как A_n есть B, то мы доказали, что $\Gamma \vdash A \supset B$. □

Следствие 4.2. *Если пропозициональное исчисление содержит схемы аксиом 1 и 2, и его единственным правилом вывода является modus ponens, то для этого исчисления верна теорема о дедукции: каковы бы ни были множество формул* Γ *и формулы* A, B*, если* $\Gamma \cup \{A\} \vdash B$*, то* $\Gamma \vdash A \supset B$*.*

Доказательство. Если пропозициональное исчисление удовлетворяет условию теоремы, то для этого исчисления остается в силе доказательство теоремы 4.6. □

Теорема 4.7 (обобщенная теорема о корректности). *Для любых множества формул* Γ *и формулы* A*, если* $\Gamma \vdash A$*, то* $\Gamma \models A$*.*

Доказательство. Пусть $\Gamma \vdash A$. По теореме 4.4 существует конечное множество $\Delta = \{A_1, \ldots, A_n\} \subseteq \Gamma$ такое, что $\Delta \vdash A$. Применяя n раз теорему о дедукции, получаем $\vdash A_1 \supset (\ldots \supset (A_n \supset A)\ldots)$. В силу теоремы 4.5, формула $A_1 \supset (\ldots \supset (A_n \supset A)\ldots)$ является тавтологией. Докажем, что $\Gamma \models A$. Пусть g — такая оценка, при которой все формулы из Γ принимают значение 1. В частности, $g(A_i) = 1$ $(i = 1, \ldots, n)$. Так как $A_1 \supset (\ldots \supset (A_n \supset A)\ldots)$ — тавтология, то $g(A_1 \supset (\ldots \supset (A_n \supset A)\ldots)) = 1$. Отсюда и из истинностной таблицы для импликации получаем $g(A) = 1$, что и требовалось доказать. □

Множество формул Γ называется *противоречивым*, если существует такая формула B, что $\Gamma \vdash B$ и $\Gamma \vdash \neg B$. В противном случае множество Γ называется *непротиворечивым*. Очевидно, что если множество Γ противоречиво, то любое более широкое множество $\Delta \supseteq \Gamma$ также противоречиво. С другой стороны, если множество Γ непротиворечиво, то любое подмножество $\Delta \subseteq \Gamma$ также непротиворечиво.

Теорема 4.8 (принцип приведения к абсурду). *Если множество формул* $\Gamma \cup \{A\}$ *противоречиво, то* $\Gamma \vdash \neg A$.

Доказательство. Пусть для формулы B имеет место $\Gamma \cup \{A\} \vdash B$ и $\Gamma \cup \{A\} \vdash \neg B$. Тогда, в силу теоремы о дедукции (теорема 4.6),

$$\Gamma \vdash A \supset B; \Gamma \vdash A \supset \neg B. \tag{10}$$

Построим вывод формулы $\neg A$ из множества гипотез $\{A \supset \neg B, A \supset \neg B\}$:

1. $A \supset B$ (гипотеза);
2. $A \supset \neg B$ (гипотеза);
3. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$ (аксиома 12);
4. $(A \supset \neg B) \supset \neg A$ (получено по правилу MP из 1 и 3);
5. $\neg A$ (получено по правилу MP из 2 и 4).

Таким образом, мы доказали, что $\{A \supset \neg B, A \supset \neg B\} \vdash \neg A$. Отсюда и из (10), в силу транзитивности выводимости, вытекает $\Gamma \vdash \neg A$, что и требовалось. □

Следствие 4.3. *Если пропозициональное исчисление содержит схему аксиом 12, и для этого исчисления верна теорема о дедукции, то для этого исчисления верен принцип приведения к абсурду: если из множества формул* $\Gamma \cup \{A\}$ *выводимо противоречие, то* $\Gamma \vdash \neg A$.

Доказательство. Если пропозициональное исчисление удовлетворяет условию теоремы, то для этого исчисления остается в силе доказательство теоремы 4.8. □

Задачи

1) Построить выводы следующих формул:

   а) $A \vee A \supset A$; б) $A \equiv A$; в) $(A \supset \neg A) \supset \neg A$.

2) Доказать, построив выводы:

   а) $A \equiv B \vdash B \equiv A$; б) $A \,\&\, B \vdash B \,\&\, A$; в) $A \vee B \vdash B \vee A$.

3) Доказать с помощью теоремы о дедукции:

   а) $A \supset (B \supset C) \vdash B \supset (A \supset C)$; б) $\vdash \neg A \supset (A \supset B)$; в) $\neg A \supset \neg B \vdash B \supset A$.

4) Доказать с помощью теоремы о дедукции и принципа приведения к абсурду:

   а) $\vdash A \supset \neg\neg A$; б) $\vdash (A \supset B) \supset (\neg B \supset \neg A)$; в) $\vdash A \supset (\neg B \supset \neg(A \supset B))$.

4.3. Допустимые правила вывода

Теорема о дедукции и принцип приведения к абсурду позволяют доказывать выводимость некоторых формул косвенным образом, без построения вывода. Эти теоремы можно сформулировать в виде так называемых *допустимых правил вывода.* А именно, теорема о дедукции выглядит так: $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$. Это правило называется *«введение импликации»*. Смысл его такой: если верно утверждение в посылке правила («числителе»), то верно и утверждение в его заключении («знаменателе»). Принцип приведения к абсурду формулируется в виде такого допустимого правила: $\dfrac{\Gamma, A \vdash B \quad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$ (*введение отрицания*). Следующая теорема дает примеры других допустимых правил.

Теорема 4.9. *В исчислении высказываний допустимы следующие правила вывода:*

- $\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \,\&\, B}$ *(введение конъюнкции);*
- $\dfrac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash A}$, $\dfrac{\Gamma \vdash A \,\&\, B}{\Gamma \vdash B}$ *(удаление конъюнкции);*
- $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$, $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$ *(введение дизъюнкции);*
- $\dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$ *(удаление дизъюнкции);*
- $\dfrac{\Gamma, \neg A \vdash B \quad \Gamma, \neg A \vdash \neg B}{\Gamma \vdash A}$ *(удаление отрицания);*
- $\dfrac{\Gamma \vdash A \supset B \quad \Gamma \vdash B \supset A}{\Gamma \vdash A \equiv B}$ *(введение эквиваленции);*
- $\dfrac{\Gamma \vdash A \equiv B}{\Gamma \vdash A \supset B}$, $\dfrac{\Gamma \vdash A \equiv B}{\Gamma \vdash B \supset A}$ *(удаление эквиваленции).*

Доказательство. Докажем допустимость правила введения конъюнкции. Пусть

$$\Gamma \vdash A; \qquad \Gamma \vdash B. \tag{11}$$

Следующая последовательность формул является выводом формулы $A \,\&\, B$ из множества гипотез $\{A, B\}$:
1) $A \supset (B \supset A \,\&\, B)$ (аксиома 5);
2) A (гипотеза);
3) $B \supset A \,\&\, B$ (получено по правилу MP из 1 и 2);
4) B (гипотеза);
5) $A \,\&\, B$ (получено по правилу MP из 3 и 4).

Таким образом, $\{A, B\} \vdash A \,\&\, B$. Отсюда и из (11) в силу свойства транзитивности отношения $\vdash$ (теорема 4.3) вытекает $\Gamma \vdash A \,\&\, B$, что и требовалось доказать.

Докажем допустимость правила удаления конъюнкции. Пусть

$$\Gamma \vdash A \,\&\, B. \tag{12}$$

Следующая последовательность формул является выводом формулы A из множества гипотез $\{A \,\&\, B\}$:
1) $A \,\&\, B \supset A$ (аксиома 3);
2) $A \,\&\, B$ (гипотеза);
3) A (получено по правилу MP из 1 и 2).

Таким образом, $\{A \,\&\, B\} \vdash A$. Отсюда и из (12) в силу свойства транзитивности отношения $\vdash$ вытекает $\Gamma \vdash A$, что и требовалось доказать.

Совершенно аналогично доказывается, что при выполнении условия (12) имеет место $\Gamma \vdash B$.

Докажем допустимость правила введения дизъюнкции. Пусть

$$\Gamma \vdash A. \tag{13}$$

Следующая последовательность формул является выводом формулы $A \vee B$ из множества гипотез $\{A\}$:
1) $A \supset A \vee B$ (аксиома 6);
2) A (гипотеза);
3) $A \vee B$ (получено по правилу MP из 1 и 2).

Таким образом, $\{A\} \vdash A \vee B$. Отсюда и из (13) в силу свойства транзитивности отношения $\vdash$ вытекает $\Gamma \vdash A \vee B$, что и требовалось доказать.

Совершенно аналогично доказывается, что если $\Gamma \vdash B$, то $\Gamma \vdash A \vee B$.

Докажем допустимость правила удаления дизъюнкции. Пусть $\Gamma, A \vdash C$ и $\Gamma, B \vdash C$. Из этих условий, в силу теоремы о дедукции, получаем

$$\Gamma \vdash A \supset C; \qquad \Gamma \vdash B \supset C. \tag{14}$$

Следующая последовательность является выводом формулы C из множества $\{A \supset C,\ B \supset C,\ A \vee B\}$:
1) $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$ (аксиома 8);
2) $A \supset C$ (гипотеза);
3) $(B \supset C) \supset (A \vee B \supset C)$ (получено по правилу MP из 1 и 2);
4) $B \supset C$ (гипотеза);
5) $A \vee B \supset C$ (получено по правилу MP из 3 и 4);
6) $A \vee B$ (гипотеза);
7) C (получено по правилу MP из 5 и 6).

Таким образом, $\{A \supset C,\ B \supset C,\ A \vee B\} \vdash C$. Отсюда и из (14), в силу транзитивности отношения $\vdash$, вытекает $\Gamma, A \vee B \vdash C$, что и требовалось доказать.

Докажем допустимость правила удаления отрицания. Пусть $\Gamma, \neg A \vdash B$ и $\Gamma, \neg A \vdash \neg B$. Из этих условий, в силу принципа приведения к абсурду, вытекает

$$\Gamma \vdash \neg\neg A. \tag{15}$$

Следующая последовательность формул является выводом формулы A из множества гипотез $\{\neg\neg A\}$:

1) $\neg\neg A \supset A$ (аксиома 13);

2) $\neg\neg A$ (гипотеза);

3) A (получено по правилу MP из 1 и 2).

Таким образом, $\{\neg\neg A\} \vdash A$. Отсюда и из (15), в силу транзитивности отношения $\vdash$, вытекает $\Gamma \vdash A$, что и требовалось доказать.

Доказательство допустимости правил введения и удаления эквиваленции предлагается в качестве упражнения. □

Теорема 4.10. *Множество пропозициональных формул* Γ *противоречиво тогда и только тогда, когда любая формула выводима из* Γ.

Доказательство. Пусть множество пропозициональных формул Γ противоречиво, и пусть A — произвольная формула. Очевидно, что множество $\Gamma \cup \{\neg A\}$ противоречиво. Тогда, в силу правила удаления отрицания, имеет место $\Gamma \vdash A$. Обратно, пусть любая формула выводима из Γ. В частности, какова бы ни была формула A, имеет место $\Gamma \vdash A$ и $\Gamma \vdash \neg A$, а это как раз и означает, что множество Γ противоречиво. □

Примеры.

1. Докажем, что в исчислении высказываний выводима формула $(\neg A \supset \neg B) \supset (B \supset A)$. В силу теоремы о дедукции, для этого достаточно показать, что

$$\neg A \supset \neg B \vdash B \supset A. \tag{16}$$

В силу той же теоремы, (16) будет доказано, если мы докажем, что

$$\neg A \supset \neg B, B \vdash A. \tag{17}$$

В силу правила удаления отрицания, для доказательства (17) достаточно показать, что множество формул $\Gamma = \{\neg A \supset \neg B,\ B,\ \neg A\}$ противоречиво. Но это действительно так: $\Gamma \vdash B$ (так как $B \in \Gamma$) и $\Gamma \vdash \neg B$ (так как $\neg B$ получается по правилу MP из гипотез $\neg A \supset \neg B$ и $\neg A$).

Приведенное рассуждение можно сделать более «прямым»:

1) $\neg A \supset \neg B,\ B,\ \neg A \vdash B$ (так как $B \in \Gamma$);

2) $\neg A \supset \neg B,\ B,\ \neg A \vdash \neg B$ (так как $\neg B$ получается по правилу MP из гипотез $\neg A \supset \neg B$ и $\neg A$);

3) $\neg A \supset \neg B,\ B \vdash A$ (получается по правилу удаления отрицания из 1 и 2);

4) $\neg A \supset \neg B \vdash B \supset A$ (получается по теореме о дедукции из 3);

5) $\vdash (\neg A \supset \neg B) \supset (B \supset A)$ (получается по теореме о дедукции из 4), что и требовалось доказать.

2. С помощью допустимых правил докажем, что в исчислении высказываний выводима формула

$$A \vee \neg A, \tag{18}$$

выражающая закон исключенного третьего. В силу правила удаления отрицания для этого достаточно показать, что множество формул $\{\neg(A \vee \neg A)\}$ противоречиво. Покажем, что

$$\neg(A \vee \neg A) \vdash A \tag{19}$$

и

$$\neg(A \vee \neg A) \vdash \neg A. \tag{20}$$

Для доказательства (19), в силу правила удаления отрицания, достаточно проверить, что множество формул $\Gamma = \{\neg(A \vee \neg A),\ \neg A\}$ противоречиво. Но это действительно так: $\Gamma \vdash \neg(A \vee \neg A)$ (так как $\neg(A \vee \neg A) \in \Gamma$) и $\Gamma \vdash A \vee \neg A$ (в силу правила введения дизъюнкции, так как, очевидно, $\Gamma \vdash \neg A$). Для доказательства (20), в силу правила введения отрицания, достаточно проверить, что множество формул $\Gamma = \{\neg(A \vee \neg A),\ A\}$ противоречиво. Но это действительно так: $\Gamma \vdash \neg(A \vee \neg A)$ (так как $\neg(A \vee \neg A) \in \Gamma$) и $\Gamma \vdash A \vee \neg A$ (в силу правила введения дизъюнкции, так как, очевидно, $\Gamma \vdash A$). Из (19) и (20) следует, что множество формул $\{\neg(A \vee \neg A)\}$ противоречиво, следовательно, $\vdash A \vee \neg A$, что и требовалось доказать.

Задачи

1) Доказать допустимость правил введения и удаления эквиваленции.

2) Доказать, что множество $\{A \vee B, \neg A, \neg B\}$ противоречиво, каковы бы ни были формулы A и B.

3) С помощью допустимых правил доказать, что следующие формулы выводимы в исчислении высказываний:

а) $\neg\neg\neg A \equiv \neg A$; б) $\neg(A \vee B) \equiv (\neg A \,\&\, \neg B)$; в) $\neg(A \,\&\, B) \equiv (\neg A \vee \neg B)$; г) $A \,\&\, B \equiv \neg(A \supset \neg B)$;

д) $A \supset B \equiv \neg(A \,\&\, \neg B)$; е) $\neg(A \& \neg A)$; ж) $A \& (A \vee B) \equiv A$; з) $A \vee B \,\&\, C \equiv (A \vee B) \,\&\, (A \vee C)$;

и) $(A \supset B) \supset ((C \supset A) \supset (C \supset B))$; к) $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$; л) $(A \supset B) \supset ((C \vee A) \supset (C \vee B))$;

м) $(A \supset B) \supset ((C \,\&\, A) \supset (C \,\&\, B))$; н) $(A \supset B) \vee (B \supset A)$; о) $(A \supset B) \supset \neg A \vee B$; п) $\neg A \vee B \supset (A \supset B)$.

4.4. Полнота классического исчисления высказываний

Множество пропозициональных формул Γ называется *максимальным*, если для любой формулы A имеет место $A \in \Gamma$ или $(\neg A) \in \Gamma$.

Теорема 4.11. *Каково бы ни было непротиворечивое множество пропозициональных формул Γ, существует такое максимальное непротиворечивое множество Δ, что $\Gamma \subseteq \Delta$.*

Доказательство. Пусть Γ — произвольное непротиворечивое множество пропозициональных формул. Множество всех пропозициональных формул счетно. Пусть $A_1, A_2, \ldots, A_n, \ldots$ — какой-либо пересчет всех пропозициональных формул. Для каждого натурального n индуктивно определим множество формул Δ_n следующим образом. Положим $\Delta_0 = \Gamma$. Если множество Δ_i уже определено, пусть

$$\Delta_{i+1} = \begin{cases} \Delta_i \cup \{A_i\}, \text{ если множество } \Delta_i \cup \{A_i\} \text{непротиворечиво;} \\ \Delta_i \cup \{\neg A_i\}, \text{ если множество } \Delta_i \cup \{A_i\} \text{противоречиво.} \end{cases}$$

Индукцией по i докажем, что каждое множество Δ_i непротиворечиво. Множество Δ_0, совпадающее с Γ, непротиворечиво по условию. Допустим, что множество Δ_i непротиворечиво, и докажем непротиворечивость множества Δ_{i+1}. Если множество $\Delta_i \cup \{A_i\}$ непротиворечиво, то $\Delta_{i+1} = \Delta_i \cup \{A_i\}$, следовательно, в этом случае множество Δ_{i+1} непротиворечиво. Если же множество $\Delta_i \cup \{A_i\}$ противоречиво, то $\Delta_{i+1} = \Delta_i \cup \{\neg A_i\}$. Допустим, что множество Δ_{i+1} также противоречиво. Тогда, в силу принципа приведения к абсурду (теорема 4.8), имеет место $\Delta_i \vdash \neg\neg A_i$, а кроме того, очевидно, $\Delta_i \vdash \neg A_i$, что противоречит предположению о непротиворечивости множества Δ_i. Значит, и в этом случае множество Δ_{i+1} непротиворечиво. Пусть Δ — объединение всех множеств Δ_i. Таким образом, $\Gamma = \Delta_0 \subseteq \Delta_1 \subseteq \ldots \subseteq \Delta_i \subseteq \Delta_{i+1} \subseteq \ldots \subseteq \Delta$. Множество Δ является максимальным. Действительно, по построоению, для любой формулы A_i имеет место либо $A_i \in \Delta_{i+1}$, и тогда $A_i \in \Delta$, либо $(\neg A_i) \in \Delta_{i+1}$, и тогда $(\neg A_i) \in \Delta$. Докажем, что множество Δ непротиворечиво. Допустим противное. Тогда существует такая формула A, что $\Delta \vdash A$ и $\Delta \vdash \neg A$. В силу свойства компактности (теорема 4.4), существуют такие конечные множества $\Delta' \subseteq \Delta$ и $\Delta'' \subseteq \Delta$, что $\Delta' \vdash A$ и $\Delta'' \vdash \neg A$. Очевидно, что $\Delta' \cup \Delta'' \subseteq \Delta_i$ для некоторого i. Тогда, в силу свойства монотонности (теорема 4.2), получаем $\Delta_i \vdash A$ и $\Delta_i \vdash \neg A$, что противоречит непротиворечивости множества Δ_i. Значит, множество Δ непротиворечиво. □

Теорема 4.12. *Если Δ — непротиворечивое максимальное множество пропозициональных формул, то, какова бы ни была формула A, если $\Delta \vdash A$, то $A \in \Delta$.*

Доказательство. Пусть Δ — непротиворечивое максимальное множество формул, и пусть $\Delta \vdash A$. Допустим, что $A \notin \Delta$. Тогда $(\neg A) \in \Delta$ в силу максимальности множества Δ. Но тогда $\Delta \vdash \neg A$, что противоречит предположению о непротиворечивости множества Δ. Значит, $A \in \Delta$. □

Теорема 4.13. *Если Δ — непротиворечивое максимальное множество пропозициональных формул, то Δ выполнимо.*

Доказательство. Пусть Δ — непротиворечивое максимальное множество формул. Оценку g определим следующим образом:

$$g(P_i) = \begin{cases} 1, \text{ если } P_i \in \Delta, \\ 0, \text{ если } P_i \notin \Delta. \end{cases}$$

Докажем, что для любой формулы A выполняется условие

$$g(A) = 1 \Leftrightarrow A \in \Delta. \tag{21}$$

Индукция по построению формулы A. Если A есть атомная формула P_i, то для нее условие (21) выполнено по определению оценки g.

Пусть формула A имеет вид $\neg B$, причем для формулы B выполнено доказываемое утверждение, т. е.

$$g(B) = 1 \Leftrightarrow B \in \Delta. \tag{22}$$

Докажем (21). Пусть $g(A) = 1$. Тогда $g(B) = 0$, и, в силу условия (22), $B \notin \Delta$. Тогда $A \in \Delta$ в силу максимальности множества Δ. Обратно, если $A \in \Delta$, то $B \notin \Delta$ в силу непротиворечивости множества Δ. А тогда, в силу (22), $g(B) = 0$ и, значит, $g(A) = 1$, что и требовалось доказать.

Пусть формула A имеет вид $B \,\&\, C$, причем выполнены условия (22) и

$$g(C) = 1 \Leftrightarrow C \in \Delta. \tag{23}$$

Докажем (21). Пусть $g(A) = 1$. Тогда $g(B) = 1$ и $g(C) = 1$ и, в силу условий (22) и (23), $B \in \Delta$ и $C \in \Delta$. По правилу введения конъюнкции имеем $\Delta \vdash A$. Тогда $A \in \Delta$ в силу теоремы 4.12. Обратно, если $A \in \Delta$, то по правилу удаления конъюнкции имеем $\Delta \vdash B$ и $\Delta \vdash C$, а тогда $B \in \Delta$ и $C \in \Delta$ в силу теоремы 4.12. Теперь в силу условий (22) и (23) получаем $g(B) = 1$ и $g(C) = 1$, значит, $g(A) = 1$, что и требовалось доказать.

Пусть формула A имеет вид $B \vee C$, причем выполнены условия (22) и (23). Докажем (21). Пусть $g(A) = 1$. Тогда $g(B) = 1$ или $g(C) = 1$ и, в силу условий (22) и (23), $B \in \Delta$ или $C \in \Delta$. По правилу введения дизъюнкции в обоих случаях имеем $\Delta \vdash A$. Тогда $A \in \Delta$ в силу теоремы 4.12. Обратно, пусть $A \in \Delta$. Тогда $B \in \Delta$ или $C \in \Delta$, ибо в противном случае $(\neg B) \in \Delta$ и $(\neg C) \in \Delta$, а тогда множество Δ противоречиво (см. задачу 2 из раздела 4.3). В силу условий (22) и (23) получаем $g(B) = 1$ или $g(C) = 1$, значит, $g(A) = 1$, что и требовалось доказать.

Пусть формула A имеет вид $B \supset C$, причем выполнены условия (22) и (23). Докажем (21). Пусть $g(A) = 1$. Тогда $g(B) = 0$ или $g(C) = 1$ и, в силу условий (22) и (23), $B \notin \Delta$ и, значит, $(\neg B) \in \Delta$, или $C \in \Delta$. По правилу введения дизъюнкции, в обоих случаях имеем $\Delta \vdash \neg B \vee C$. Тогда $(\neg B \vee C) \in \Delta$ в силу теоремы 4.12. Но, в силу задачи 3п) из раздела 4.3, формула $\neg B \vee C \supset (B \supset C)$ выводима в исчислении высказываний. Значит, $\Delta \vdash A$ и $A \in \Delta$. Обратно, пусть $A \in \Delta$. Докажем, что $g(A) = 1$. Допустим противное, т. е. $g(A) = 0$. Тогда $g(B) = 1$ и $g(C) = 0$. В силу условий (22) и (23) получаем $B \in \Delta$ и $C \notin \Delta$, т. е. $(\neg C) \in \Delta$. Таким образом, $\{B \supset C, B, \neg C\} \subseteq \Delta$, и множество Δ противоречиво. Значит, $g(A) = 1$, что и требовалось доказать.

Рассмотрение случая, когда формула A имеет вид $B \equiv C$, предлагается в качестве упражнения. Таким образом, имеем $g(A) = 1$ для любой формулы A из множества Δ. Это означает, что множество Δ выполнимо. □

Теорема 4.14. *Всякое непротиворечивое множество пропозициональных формул выполнимо.*

Доказательство. Пусть Γ — непротиворечивое множество формул. По теореме 4.11 существует непротиворечивое максимальное множество Δ такое, что $\Gamma \subseteq \Delta$. По теореме 4.13 множество Δ выполнимо, т. е. существует оценка g, при которой все формулы из Δ, в частности, все формулы из Γ, принимают значение 1. Значит, множество Γ также выполнимо. □

Теорема 4.15 (обобщенная теорема о полноте). *Каковы бы ни были множество пропозициональных формул Γ и формула A, если $\Gamma \models A$, то $\Gamma \vdash A$.*

Доказательство. Пусть $\Gamma \models A$. Тогда, в силу теоремы 2.12, множество $\Gamma \cup \{\neg A\}$ несовместно, т. е. невыполнимо. Отсюда и из теоремы 4.14 следует, что оно противоречиво. Но тогда, в силу правила удаления отрицания, $\Gamma \vdash A$. □

Теорема 4.16 (теорема о полноте). *Всякая тавтология выводима в исчислении высказываний.*

Доказательство. Если A — тавтология, то $\emptyset \models A$, и в силу теоремы 4.15 имеем $\emptyset \vdash A$, т. е. $\vdash A$. □

5. Логика предикатов

5.1. Высказывательные формы и кванторы

Не всякое повествовательное предложение может рассматриваться как высказывание. Например, нельзя ставить вопрос об истинности или ложности предложения «Остаток от деления числа n на 7 равен 3». Буква n, входящая в это предложение, играет роль переменной, при подстановке вместо которой обозначения какого-либо натурального числа получается высказывание (истинное или ложное). Вообще, *переменная* — это языковое выражение, служащее для обозначения произвольного объекта из некоторого фиксированного множества, называемого *областью возможных значений* переменной. Если переменная употребляется таким образом, что допускается подстановка вместо нее *имен* (т. е. обозначений) объектов из области возможных ее значений, то эта переменная называется *свободной*. Таковы, например, переменные x, y и z в предложениях $x < y$ и $z = x + 1$. Если же по смыслу выражения, содержащего переменную, подстановка вместо нее имен конкретных объектов недопустима, то эта переменная называется *связанной*. Например, в выражении $\lim\limits_{x \to a} x^2 = y$ переменная x является связанной, а переменные a и y — свободными. В одном выражении одна и та же переменная может употребляться и как свободная, и как связанная. Например, в выражении $\int\limits_0^x x^2 dx$ оба вхождения переменной x в подынтегральное выражение являются связанными, а вхождение ее в качестве верхнего предела интегрирования — свободным. Вообще, следует говорить именно о свободных и связанных *вхождениях* переменной в данное выражение.

Выражение, содержащее свободные вхождения переменных и превращающееся в имя некоторого объекта (или высказывание) всякий раз, когда вместо свободных вхождений каждой переменной подставляется имя какого-либо объекта из области ее возможных значений, называется *именной формой* (соответственно, *высказывательной формой*). Переменные, имеющие свободные вхождения в именную или высказывательную форму, называются ее *параметрами*. Именную или высказывательную форму будем называть n-местной, если она содержит ровно n параметров. В частности, можно говорить и о 0-местных именных и высказывательных формах, понимая под ними соответственно имена и высказывания.

Иногда для k-местной именной или высказывательной формы употребляют обозначение $F(x_1, \ldots, x_k)$, явно указывая все ее параметры. Тогда, если $a_1, \ldots, a_k$ — имена каких-либо объектов из областей возможных значений переменных $x_1, \ldots, x_k$ соответственно, то через $F(a_1, \ldots, a_k)$ обозначается выражение, полученное из $F(x_1, \ldots, x_k)$ подстановкой $a_1, \ldots, a_k$ соответственно вместо свободных вхождений переменных $x_1, \ldots, x_k$.

Примеры.

1) Через $F(x, y)$ обозначим именную форму $\int\limits_x^y yx^2 dx$. Тогда $F(3, 6)$ есть выражение $\int\limits_3^6 6x^2 dx$, которое, очевидно, является именем числа 378.

2) Через $A(i, k, l)$ обозначим высказывательную форму $\sum\limits_{i=k}^{l} \frac{1}{i^2} < \lim\limits_{x \to i} \log_2 x$. Тогда $A(3, 7, 11)$ есть высказывание $\sum\limits_{i=7}^{11} \frac{1}{i^2} < \lim\limits_{x \to 3} \log_2 x$ (очевидно, истинное).

Очевидно, что над высказывательными формами можно совершать логические операции. Так, абсолютно ясен смысл высказывательных форм $\neg A$, $A \,\&\, B$, $A \vee B$, $A \supset B$, если A и B — высказывательные формы. Наряду с такими операциями в математической логике рассматриваются *кванторы*, позволяющие из данной высказывательной формы получать высказывательную форму с меньшим числом параметров, в частности, из одноместной высказывательной формы — высказывание.

Квантор всеобщности по переменной x позволяет из данной высказывательной формы $A(x)$ с единственным параметром x получить высказывание «Для всех x имеет место $A(x)$». Результат применения квантора всеобщности по переменной x к высказывательной форме $A(x)$ будем обозначать $\forall x A(x)$. Высказывание $\forall x A(x)$ считается истинным тогда и только тогда, когда при подстановке в $A(x)$ вместо свободных вхождений переменной x имени любого объекта a из области ее возможных значений всегда получается истинное высказывание $A(a)$. Высказывание $\forall x A(x)$ может читаться также «Для любого x имеет место $A(x)$», «Для всех x верно $A(x)$», «Каждый x обладает свойством $A(x)$»и т. п.

Квантор существования по переменной x позволяет из данной высказывательной формы $A(x)$ с единственным параметром x получить высказывание «Существует такой x, что имеет место $A(x)$». Результат применения квантора существования по переменной x к высказывательной форме $A(x)$ будем обозначать $\exists x A(x)$. Высказывание $\exists x A(x)$ считается истинным тогда и только тогда, когда в области возможных значений переменной x найдется такой объект a, что при подстановке его имени в $A(x)$ вместо свободных

вхождений переменной x получается истинное высказывание $A(a)$. Высказывание $\exists x A(x)$ может читаться также «Для некоторых x имеет место $A(x)$», «Существует x, для которого $A(x)$», «Хотя бы для одного x верно $A(x)$»и т. п.

Отметим еще раз, что в предложениях $\forall x A(x)$ и $\exists x A(x)$ переменная x не является свободной: кванторы «связывают»эту переменную. Очевидно также, что кванторы по переменной x можно применять и к высказывательным формам, содержащим наряду с x и другие параметры. В результате получится высказывательная форма, имеющая те же параметры, что и исходная, кроме x.

Важное значение для логики имеет анализ логической структуры высказываний и высказывательных форм, т. е. выявление того, каким образом данное повествовательное предложение построено из более простых предложений с помощью пропозициональных операций и кванторов. Логический анализ предложений есть своего рода искусство, практические навыки которого можно приобрести путем упражнений. Пусть, например, M и N — два множества, состоящие из действительных чисел. Тогда, используя переменную x, возможными значениями которой являются действительные числа, высказывание «Каждый элемент множества M принадлежит множеству N»можно записать следующим образом: $\forall x(x \in M \supset x \in N)$, а высказывание «Некоторые элементы множества M принадлежат множеству N»можно записать так: $\exists x(x \in M \,\&\, x \in M)$.

Задачи

Найти истинностные значения следующих высказываний, где возможными значениями переменных являются действительные числа:

1) $\forall x \exists y(x + y = 3)$;

2) $\exists y \forall x(x + y = 7)$;

3) $\exists x \exists y(x + y = 11)$;

4) $\forall x \exists y(x + y = 3) \supset 7 = 11$;

5) $\forall x(\exists y(xy = 3) \equiv a \neq 0)$;

6) $\exists a \forall b \exists x(x^2 + ax + b = 0)$.

5.2. Понятие предиката

Логический анализ предложений во многом аналогичен грамматическому анализу сложно-сочиненных и сложно-подчиненных предложений. Однако иногда нас будет интересовать и внутренняя структура простых предложений: *что* и *о чем* говорится в данном предложении. В таком случае в грамматике используются понятия субъекта и предиката. *Субъект* (или подлежащее) — это то, о чем или о ком говорится в предложении, а *предикат* (называемый также сказуемым или группой сказуемого) выражает то, что говорится о субъекте. В математической логике используется более широкая трактовка субъектно-предикатной структуры предложения. Прежде всего, в качестве субъектов данного предложения мы можем выделить одно или несколько имен каких-либо предметов, входящих в это предложение. Заменив затем выделенные имена на переменные, мы получим высказывательную форму, «в чистом виде» выражающую то, что говорится о субъекте или субъектах. Эту высказывательную форму тоже называют предикатом. Рассмотрим, например, высказывание «12 делится на 3», которое, используя общепринятую символику, можно записать так: $3|12$ («число 3 делит число 12»). Выбрав в качестве субъекта число 12, мы получаем одноместный предикат $3|x$ («x делится на 3»). Если же в качестве субъекта взять число 3, то получим другой одноместный предикат $y|12$ («12 делится на y»). Наконец, считая 12 и 3 субъектами этого предложения, получаем двуместный предикат $y|x$ («x делится на y»).

Со всяким предикатом, понимаемым как высказывательная форма, естественным образом связана функция, которая каждому набору значений свободных переменных сопоставляет высказывание, получающееся из данной высказывательной формы подстановкой вместо свободных вхождений переменных имен объектов, выбранных в качестве значений этих переменных. Обобщая это наблюдение, мы приходим к представлению о предикате как о функции, значениями которой являются высказывания. Наконец, если мы не будем различать высказывания, имеющие одно и то же истинностное значение, то придем к следующему определению: k-местным предикатом на множестве M называется функция $P : M^k \to \{0, 1\}$, где M^k — декартова степень множества M, т. е. прямое произведение k одинаковых множеств, равных M. Одноместные предикаты называют также «свойствами».

Пусть P есть k-местный предикат на множестве M. Совокупность всех элементов множества M^k (т. е. кортежей длины k над множеством M), на которых предикат P принимает значение 1, называется *областью истинности* предиката P. Иными словами, область истинности предиката P — это множество $\{\langle a_1, \ldots, a_k\rangle | a_1, \ldots, a_k \in M \,\&\, P(a_1, \ldots, a_k) = 1\}$.

Примеры.

1) На произвольном множестве M может быть определен двуместный предикат $E : M \to \{0, 1\}$ так, что $E(x, y) = 1$ тогда и только тогда, когда x и y совпадают. Этот предикат называют *предикатом равенства* и вместо $E(x, y)$ пишут $x = y$.

2) На произвольной совокупности множеств M можно определить двуместный предикат $P : M \to \{0, 1\}$ так, что $P(x, y) = 1$ тогда и только тогда, когда множество x является элементом множества y. Этот предикат называют *предикатом принадлежности* и вместо $P(x, y)$ пишут $x \in y$.

5.3. Элементарные языки

Чтобы сделать математические утверждения точными математическими объектами, в математической логике используют искусственные языки. Самый распространенный вид таких языков — так называемые *логико-математические языки первого порядка* или *элементарные языки*. Каждый элементарный язык задается своей *сигнатурой* — набором из трех множеств $\Omega = \langle Cn, Fn, Pr\rangle$, где Cn — множество *(предметных) констант*, Fn — множество *функциональных символов*, Pr — множество *предикатных символов*. При этом с каждым функциональным и предикатным символом однозначно связано некоторое натуральное число — количество аргументов (или *валентность*) этого символа. Валентность любого функционального символа положительна, а предикатный символ может иметь и нулевую валентность. Функциональный или предикатный символ, валентность которого равна k, называют k-местным. Во всяком элементарном языке имеется счетный набор *(предметных) переменных*. Элементарный язык с сигнатурой Ω будем называть языком Ω.

Из переменных, констант, функциональных и предикатных символов с помощью скобок (,), запятых и *логических символов* $\neg$, $\&$, $\vee$, $\supset$, $\forall$, $\exists$ строятся выражения, называемые термами и формулами. Определение *терма* носит индуктивный характер и содержит три пункта:

- каждая переменная есть терм;
- каждая константа есть терм;
- если f есть k-местный функциональный символ, а $t_1, \ldots, t_k$ — термы, то выражение $f(t_1, \ldots, t_k)$ есть терм.

Если f — двуместный функциональный символ, то иногда, следуя традиции, вместо $f(t_1, t_2)$ пишут $(t_1 f t_2)$ или просто $t_1 f t_2$. Например, при использовании функционального символа $+$ обычно пишут $x + y$, а не $+(x, y)$. Если f — одноместный функциональный символ, то иногда вместо $f(t)$ пишут ft.

Индуктивный характер определения терма дает возможность использовать в доказательствах *принцип индукции по построению терма*. А именно, пусть требуется доказать, что все термы обладают некоторым свойством P. Для этого достаточно установить, что

- каждая переменная обладает свойством P;
- каждая константа обладает свойством P;
- если f есть k-местный функциональный символ, а термы $t_1, \ldots, t_k$ обладают свойством P, то терм $f(t_1, \ldots, t_k)$ обладает свойством P.

Атомные формулы (или *атомы*) — это выражения вида $P(t_1, \ldots, t_k)$, где P есть k-местный предикатный символ ($k \geq 1$), а $t_1, \ldots, t_k$ — термы. Всякий 0-местный предикатный символ считается атомом. Если P — двуместный предикатный символ, то иногда, следуя традиции, вместо $P(t_1, t_2)$ пишут $(t_1 P t_2)$ или просто $t_1 P t_2$. Например, при использовании предикатного символа равенства $=$ обычно пишут $x = y$, а не $=(x, y)$.

Формулы определяются индуктивно с помощью следующих четырех пунктов.

- Каждый атом есть формула.
- Если Φ — формула, то $\neg\Phi$ — формула.

- Если Φ и Ψ — формулы, то $(\Phi \,\&\, \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \supset \Psi)$ — формулы.
- Если Φ — формула, x — переменная, то $\forall x \Phi$ и $\exists x \Phi$ — формулы.

Символы $\neg, \&, \vee, \supset$ называются *логическими связками*, а $\exists$ и $\forall$ — *кванторами* или *кванторными символами*. В формулах вида $\exists x \Phi$ и $\forall x \Phi$ выражение $\forall x$ или $\exists x$ называется *кванторной приставкой*, а формула Φ — *областью действия* соответствующей кванторной приставки. В дальнейшем выражение $\Phi \equiv \Psi$, где Φ и Ψ — формулы, будем понимать как сокращенное обозначение формулы $(\Phi \supset \Psi) \,\&\, (\Psi \supset \Phi)$.

Вхождение переменной x в формулу Φ называется *связанным*, если оно входит в кванторную приставку $\forall x$ или $\exists x$ или в область действия такой кванторной приставки. Вхождение переменной, не являющееся связанным, называется *свободным*. Формула, не содержащая свободных вхождений переменных, называется *замкнутой формулой* или *высказыванием*.

Индуктивный характер определения формулы дает возможность использовать в доказательствах *принцип индукции по построению формулы*, а также индукцией по построению формулы задавать функции, определенные на множестве всех формул. В качестве примера такой функции рассмотрим следующую функцию.

Пусть даны произвольный список попарно различных переменных $x_1, \ldots, x_k$ и список (не обязательно различных) термов $t_1, \ldots, t_k$. Для каждой формулы Φ индуктивно определим формулу $\Phi[t_1/x_1, \ldots, t_n/x_n]$.

- Если формула Φ есть атом, то $\Phi[t_1/x_1, \ldots, t_n/x_n]$ — формула, полученная в результате одновременной подстановки в Φ термов $t_1, \ldots, t_k$ вместо переменных $x_1, \ldots, x_k$ соответственно.
- Если формула Φ имеет вид $\neg\Psi$, причем формула $\Psi[t_1/x_1, \ldots, t_n/x_n]$ уже определена, то

  $$\Phi[t_1/x_1, \ldots, t_n/x_n] \rightleftharpoons \neg\Psi[t_1/x_1, \ldots, t_n/x_n],$$

  где символ $\rightleftharpoons$ употребляется вместо слов «есть по определению».
- Если Φ имеет вид $(\Psi_1 \lambda \Psi_2)$, где $\lambda \in \{\&, \vee, \supset\}$, и формулы $\Psi_1[t_1/x_1, \ldots, t_n/x_n]$ и $\Psi_2[t_1/x_1, \ldots, t_n/x_n]$ уже определены, то

  $$\Phi[t_1/x_1, \ldots, t_n/x_n] \rightleftharpoons (\Psi_1[t_1/x_1, \ldots, t_n/x_n] \lambda \Psi_2[t_1/x_1, \ldots, t_n/x_n]).$$
- Если формула Φ имеет вид $\kappa x \Psi$, где κ — квантор $\forall$ или $\exists$, причем для любого списка попарно различных переменных $y_1, \ldots, y_m$ и любого списка термов $s_1, \ldots, s_m$ определена формула $\Psi[s_1/y_1, \ldots, s_m/y_m]$, то

  $$\Phi[t_1/x_1, \ldots, t_n/x_n] \rightleftharpoons \kappa x \Psi[t_1/x_1, \ldots, t_n/x_n],$$

  если переменная x отлична от всех переменных $x_1, \ldots, x_k$, и

  $$\Phi[t_1/x_1, \ldots, t_n/x_n] \rightleftharpoons \kappa x \Psi[t_1/x_1, \ldots, t_{i-1}/x_{i-1}, t_{i+1}/x_{i+1}, \ldots, t_n/x_n],$$

  если переменная x совпадает с переменной x_i $(i = 1, \ldots, k)$.

Формулу $\Phi[t_1/x_1, \ldots, t_n/x_n]$ будем называть результатом *подстановки термов* $t_1, \ldots, t_k$ *вместо переменных* $x_1, \ldots, x_k$ в формулу Φ. Практически формула $\Phi[t_1/x_1, \ldots, t_n/x_n]$ получается в результате одновременной подстановки термов $t_1, \ldots, t_k$ вместо свободных вхождений в формулу Φ переменных $x_1, \ldots, x_k$ соответственно. Нетрудно заметить, что если формула Φ не содержит свободных вхождений переменных $x_1, \ldots, x_k$ (в частности, если она замкнута), то $\Phi[t_1/x_1, \ldots, t_n/x_n]$ совпадает с Φ.

Имея в виду дальнейшую подстановку термов $t_1, \ldots, t_k$ вместо переменных $x_1, \ldots, x_k$ в формулу Φ, иногда мы будем употреблять для этой формулы обозначение $\Phi(x_1, \ldots, x_k)$, а для формулы $\Phi[t_1/x_1, \ldots, t_n/x_n]$ — обозначение $\Phi(t_1, \ldots, t_k)$. Например, если $\Phi(x, y, z)$ есть формула $(P(x) \supset \forall x(Q(x, y, z) \,\&\, P(g(x, y))))$, то $\Phi(f(y), g(a, x)), f(a))$ есть формула $(P(f(y)) \supset \forall x(Q(x, g(a, x), f(a)) \,\&\, P(g(x, g(a, x)))))$.

Практически, записывая формулы, принято опускать некоторые скобки. В частности, обычно опускают внешние скобки. Дальнейшая экономия скобок возможна, если принять соглашение о том, какие логические операции «сильнее». Для этого расположим логические символы в следующем порядке: $\forall, \exists, \neg, \&, \vee, \supset, \equiv$ и будем считать, что из всех возможных в первую очередь выполняется та операция, которая в этом списке стоит раньше.

Рассмотрим некоторые примеры элементарных языков.

Сигнатура *языка теории множеств* состоит из одного двуместного предикатного символа $\in$. Следуя установившейся традиции, условимся писать $t_1 \in t_2$ вместо $\in (t_1, t_2)$. Очевидно, что термами языка теории множеств являются только переменные. Вот примеры формул этого языка.

- $\forall z(z \in x \supset z \in y)$. Очевидно, что эта формула является записью предложения $x \subseteq y$.
- $\forall y \neg y \in x$. Эта формула является записью предложения $x = \emptyset$.

Сигнатура *языка формальной арифметики* состоит из константы 0, обозначающей натуральное число 0, одноместного функционального символа s, обозначающего функцию $s(x) = x + 1$, двуместных функциональных символов $+$ и $\cdot$, обозначающих соответственно операции сложения и умножения, и двуместного предикатного символа $=$, обозначающего отношение равенства. Условимся вместо $+(t_1, t_2)$, $\cdot(t_1, t_2)$, $=(t_1, t_2)$ писать соответственно $(t_1 + t_2)$, $(t_1 \cdot t_2)$, $t_1 = t_2$. Иногда будем опускать скобки в термах, имея в виду, что арифметические операции выполняются в следующем порядке: $s, \cdot, +$. Например, терм $((x \cdot y) + s(ss0 \cdot z))$ можно кратко записать так: $x \cdot y + s(ss0 \cdot z)$. Примерами термов этого языка являются выражения $s0, ss0, sss0, \ldots$, обозначающие числа $1, 2, 3, \ldots$. Вот примеры формул языка формальной арифметики.

- $\exists z(z + x = y)$. Очевидно, что эта формула является записью предложения $x \leq y$.
- $\exists z(sz + x = y)$. Эта формула является записью предложения $x < y$.

Сигнатура *языка упорядоченных множеств* состоит из двух двуместных предикатных символов: $=$ (равенство) и $\leq$ (отношение порядка). Условимся писать $t_1 = t_2$ и $t_1 \leq t_2$ вместо $=(t_1, t_2)$ и $\leq(t_1, t_2)$ соответственно. Этот язык предназначен для записи утверждений об упорядоченных множеств. А именно, предполагается фиксированным непустое множество M, на котором задано бинарное отношение $\leq$. На этом языке аксиомы *частично упорядоченного множества* могут быть записаны в виде следующих формул:

- $\forall x(x \leq x)$ (рефлексивность);
- $\forall x \forall y(x \leq y \,\&\, y \leq x \supset x = y)$ (антисимметричность);
- $\forall x \forall y \forall z(x \leq y \,\&\, y \leq z \supset x \leq z)$ (транзитивность).

Задачи

1) Пусть f — одноместный, g — двуместный, h — трехместный функциональные символы, а x, y, z — переменные. Определить, какие из следующих выражений являются термами:

$$f(g(x, y)),\ g(f(z, h(x, y, z))),\ f(g(x), h(x, y, z)).$$

2) Пусть f — одноместный, g — двуместный, h — трехместный функциональные символы, P — одноместный, Q — трехместный предикатные символы, а x, y, z — переменные. Определить, какие из следующих выражений являются атомными формулами:

$$P(f(g(x, y))),\ Q(g(f(z), h(x, y, z))),\ Q(x, P(y), f(z)).$$

3) Указать свободные и связанные вхождения переменных в следующих формулах:

   а) $\exists y(P(z, y) \,\&\, \forall z Q(z, x) \supset R(z))$;
   б) $\forall x(P(x, y) \,\&\, \forall y Q(y, x) \supset R(x))$;
   в) $\forall y \exists z(P(y, z) \,\&\, Q(z, x) \supset R(y))$;
   г) $\forall y \exists z(P(z, y) \,\&\, \forall z Q(z, x) \supset R(y))$.

4) Записать в виде формул языка теории множеств: $x = \{y\}$; $x = \{y, z\}$; $y = \mathcal{P}(x)$ ($\mathcal{P}(x)$ — семейство всех подмножеств множества x); $z = x \cup y$; $z = x \cap y$.

5) Записать в виде формул языка формальной арифметики:

   а) «x — четное число»;
   б) «x — нечетное число»;
   в) «x — простое число»;
   г) «x делится на y»;
   д) «z — наименьшее общее кратное чисел x и y»;
   е) «z — наибольший общий делитель чисел x и y»;

ж) «z — остаток от деления числа x на y».

6) Записать в виде формул языка упорядоченных множеств:

а) аксиомы линейно упорядоченного множества;

б) «x — наименьший элемент»;

в) «x — наибольший элемент»;

г) «x — минимальный элемент»;

д) «x — максимальный элемент».

5.4. Алгебраические системы

Хотя при построении конкретного логико-математического языка обычно подразумевается некоторый смысл составляющих его символов, этот смысл никак не используется при синтаксическом описании языка. После того как выбрана сигнатура языка, мы вправе наделять входящие в нее символы новым смыслом, отличным от того, который вкладывался в них на этапе построения языка. Более того, рассмотрение различных интерпретаций одного и того же языка является одним из важнейших приемов, используемых в математической логике.

Чтобы задать *интерпретацию* языка с сигнатурой $\Omega = \langle Cn, Fn, Pr\rangle$, нужно

1) зафиксировать непустое множество M, называемое *основным множеством* или *носителем интерпретации*;

2) каждой константе $c \in Cn$ сопоставить некоторый элемент $\bar{c} \in M$ — значение константы c в данной интерпретации;

3) каждому (k-местному) функциональному символу $f \in Fn$ сопоставить некоторую (k-местную) функцию $\bar{f} : M^k \to M$ — значение функционального символа f в данной интерпретации;

4) каждому (k-местному) предикатному символу $P \in Pr$ сопоставить некоторый (k-местный) предикат $\bar{P} : M^k \to \{0, 1\}$ — значение предикатного символа P в данной интерпретации. Если P есть 0-местный предикатный символ, то ему сопоставляется значение 0 или 1.

Непустое множество M, рассматриваемое вместе с интерпретацией на нем всех символов сигнатуры Ω, называется *алгебраической системой сигнатуры* Ω и обозначается $\mathfrak{M} = \langle M, \Omega\rangle$. Множество M называют носителем алгебраической системы $\langle M, \Omega\rangle$. *Мощностью* алгебраической системы называется мощность ее носителя.

Пусть фиксирована некоторая алгебраическая система $\mathfrak{M} = \langle M, \Omega\rangle$. Наряду с сигнатурой Ω будем рассматривать сигнатуру Ω', полученную добавлением (имен) всех элементов множества M к множеству констант сигнатуры Ω. Очевидно, что всякий терм в сигнатуре Ω является термом в сигнатуре Ω', и всякая формула в сигнатуре Ω является формулой в сигнатуре Ω'. Пусть t — терм сигнатуры Ω', не содержащий переменных. Индукцией по построению терма t определим элемент $[t] \in M$ — значение терма t в алгебраической системе $\mathfrak{M}$:

- если t есть константа $c \in Cn$, то $[t] \rightleftharpoons \bar{c}$;
- если t есть константа $m \in M$, то $[t] \rightleftharpoons m$;
- если t имеет вид $f(t_1, \ldots, t_n)$, где $f \in Fn$ есть n-местный функциональный символ, а $t_1, \ldots, t_n$ — термы, для которых уже определены значения $[t_i]$ $(i = 1, \ldots, n)$, то $[t] \rightleftharpoons \bar{f}([t_1], \ldots, [t_n])$.

Пусть Φ — замкнутая формула сигнатуры Ω'. *Логической длиной* формулы Φ назовем количество входящих в нее логических символов, т. е. логических связок и кванторов. Индукцией по логической длине формулы Φ определим ее *истинностное значение* $[\Phi] \in \{0, 1\}$ в алгебраической системе $\mathfrak{M}$.

- Пусть логическая длина замкнутой формулы Φ равна 0, т. е. в ней вообще нет логических символов. Тогда Φ — атом $P(t_1, \ldots, t_n)$, где $P \in Pr$ есть n-местный предикатный символ, а $t_1, \ldots, t_n$ — термы, не содержащие переменных, для которых выше определены их значения $[t_1], \ldots, [t_n]$ в алгебраической системе $\mathfrak{M}$. В этом случае положим $[\Phi] \rightleftharpoons \bar{P}([t_1], \ldots, [t_n])$.

  Допустим, что для любой замкнутой формулы Ψ, логическая длина которой не превосходит n, определено ее истинностное значение $[\Psi]$ в алгебраической системе $\mathfrak{M}$, и пусть Φ — замкнутая формула, логическая длина которой равна $n + 1$.

- Если Φ имеет вид $\neg\Psi$, то логическая длина замкнутой формулы Ψ равна n, и, в силу индуктивного предположения, для формулы Ψ уже определено ее истинностное значение $[\Psi]$. В этом случае $[\Phi]$ определяется в соответствии с истинностной таблицей для логической операции $\neg$: $[\Phi]$ есть 0, если $[\Psi] = 1$, и 1 в противном случае.

- Если Φ имеет вид $(\Psi_1 \lambda \Psi_2)$, где λ — любая из логических связок $\&, \vee, \supset$, то логическая длина каждой из замкнутых формул Ψ_1 и Ψ_2 не превосходит n, и, в силу индуктивного предположения, для формул Ψ_1 и Ψ_2 уже определены их истинностные значения $[\Psi_1]$ и $[\Psi_2]$. В этом случае значение $[\Phi]$ определяется в соответствии с истинностной таблицей для логической операции λ.

- Если Φ имеет вид $\exists x \Psi(x)$, то для любого элемента $m \in M$ логическая длина замкнутой формулы $\Psi(m)$ равна n, и, в силу индуктивного предположения, для формулы $\Psi(m)$ уже определено ее истинностное значение $[\Psi(m)]$. В этом случае, по определению, $[\Phi]$ есть 1 тогда и только тогда, когда найдется такой элемент $m \in M$, что $[\Psi(m)] = 1$.

- если Φ имеет вид $\forall x \Psi$, причем для любого элемента $m \in M$ уже определено истинностное значение формулы $\Psi(m)$, то, по определению, значение $[\Phi]$ есть 1 тогда и только тогда, когда $[\Psi(m)] = 1$ для любого элемента $m \in M$.

Поскольку любая замкнутая формула Φ сигнатуры Ω является также замкнутой формулой сигнатуры Ω', то для нее определено ее истинностное значение $[\Phi]$ в алгебраической системе $\mathfrak{M}$. Будем говорить, что формула Φ *истинна* в алгебраической системе $\mathfrak{M}$, если $[\Phi] = 1$, и *ложна* в противном случае. Запись $\mathfrak{M} \models \Phi$ будет означать, что $[\Phi] = 1$, а запись $\mathfrak{M} \not\models \Phi$ будет означать, что $[\Phi] = 0$.

5.5. Выполнимость и общезначимость

Алгебраическая система $\mathfrak{M}$ сигнатуры Ω называется *моделью* замкнутой формулы Φ в сигнатуре Ω, если $\mathfrak{M} \models \Phi$, и *контрмоделью* формулы Φ, если $\mathfrak{M} \not\models \Phi$. Замкнутая формула Φ называется *выполнимой*, если она имеет модель. Множество замкнутых формул Γ называется выполнимым, если существует такая алгебраическая система $\mathfrak{M}$, что $\mathfrak{M} \models \Phi$ для любой формулы $\Phi \in \Gamma$; в этом случае алгебраическая система $\mathfrak{M}$ называется моделью множества формул Γ. Запись $\mathfrak{M} \models \Gamma$ означает, что $\mathfrak{M}$ — модель множества Γ.

Формула $\Phi(x_1, \ldots, x_n)$, содержащая свободно лишь переменные $x_1, \ldots, x_n$, называется выполнимой, если существуют алгебраическая система $\mathfrak{M} = \langle M, \Omega \rangle$ и элементы $m_1, \ldots, m_n \in M$ такие, что $\mathfrak{M} \models \Phi(m_1, \ldots, m_n)$. Нетрудно заметить, что формула $\Phi(x_1, \ldots, x_n)$ выполнима тогда и только тогда, когда выполнима замкнутая формула $\exists x_1 \ldots \exists x_n \Phi(x_1, \ldots, x_n)$.

Замкнутая формула Φ в сигнатуре Ω называется *общезначимой* или *тождественно истинной*, если для любой алгебраической системы $\mathfrak{M}$ сигнатуры Ω имеет место $\mathfrak{M} \models \Phi$. Запись $\models \Phi$ означает, что формула Φ общезначима.

Формула $\Phi(x_1, \ldots, x_n)$, содержащая свободно лишь переменные $x_1, \ldots, x_n$, называется общезначимой или тождественно истинной, если для любой алгебраической системы $\mathfrak{M} = \langle M, \Omega \rangle$ и любых $m_1, \ldots, m_n \in M$ имеет место $\mathfrak{M} \models \Phi(m_1, \ldots, m_n)$. Нетрудно заметить, что формула $\Phi(x_1, \ldots, x_n)$ общезначима тогда и только тогда, когда общезначима замкнутая формула $\forall x_1 \ldots \forall x_n \Phi(x_1, \ldots, x_n)$.

Говорят, что терм t *свободен* для переменной x в формуле Φ, если никакое свободное вхождение x в Φ не находится в области действия квантора по переменной, входящей в t. Например, терм $f(x)$ свободен для переменной y в формуле $\forall z P(y, z)$, а терм $f(z)$ не свободен для переменной y в той же формуле.

Теорема 5.1. *Если терм t свободен для x в формуле $\Phi(x)$, то формулы $\forall x \Phi(x) \supset \Phi(t)$ и $\Phi(t) \supset \exists x \Phi(x)$ общезначимы.*

Мы не будем доказывать эту теорему. Убедимся лишь, что здесь существенно требование, чтобы терм t был свободен для переменной x в формуле $\Phi(x)$. Пусть, например, сигнатура Ω состоит из одного двуместного предикатного символа P, а $\Phi(x)$ есть формула $\exists y P(x, y)$. В качестве терма t возьмем y. (Очевидно, что в этом случае терм t не свободен для переменной x в формуле $\Phi(x)$.) Тогда $\Phi(t)$ есть формула $\exists y P(y, y)$. Покажем, что формула $\forall x \Phi(x) \supset \Phi(t)$, которая есть

$$\forall x \exists y P(x, y) \supset \exists y P(y, y), \tag{24}$$

не общезначима. Рассмотрим алгебраическую систему $\mathfrak{M} = \langle M, \Omega \rangle$, где

$$M = \{a, b\}, \quad \bar{P}(a, b) = \bar{P}(b, a) = 1, \quad \bar{P}(a, a) = \bar{P}(b, b) = 0.$$

Очевидно, что в этой алгебраической системе посылка формулы (24) истинна, а ее заключение ложно, так что формула (24) ложна в алгебраической системе $\mathfrak{M}$ и, следовательно, не общезначима.

Задачи

1) Для каждой из следующих формул найти одну модель и одну контрмодель:
   а) $\exists x \forall y P(x,y)$; б) $\forall x \exists y P(x,y)$; в) $\forall x P(x, f(x))$;
   г) $\forall x \forall y (P(x,y) \supset \exists z (P(x,z) \,\&\, P(z,y)))$; д) $\forall x \forall y \exists z Q(x,y,z)$.

2) Привести пример терма t и формулы Φ таких, что формула $\Phi(t) \supset \exists x \Phi(x)$ не общезначима.

3) Проверить, выполнимы ли следующие формулы:
   а) $\exists x P(x)$:
   б) $\forall x P(x)$;
   в) $\exists x \forall y (Q(x,x) \,\&\, \neg Q(x,y))$;
   г) $\exists x \exists y (P(x) \,\&\, \neg P(y))$;
   д) $\exists x \forall y (Q(x,y) \supset \forall z R(x,y,z))$;
   е) $P(x) \supset \forall y P(y)$.

4) Проверить, общезначимы ли следующие формулы:
   а) $\exists x P(x) \supset \forall x P(x)$;
   б) $\neg(\exists x P(x) \supset \forall x P(x))$;
   в) $\exists x \forall y Q(x,y) \supset \forall y \exists x Q(x,y)$;
   г) $\forall x \exists y Q(x,y) \supset \exists y \forall x Q(x,y)$;
   д) $\neg \exists x P(x) \supset \neg \forall x P(x)$;
   е) $\forall x (P(x) \supset \neg Q(x)) \supset \neg(\exists x P(x) \,\&\, \forall x Q(x))$;
   ж) $\forall x (P(x) \supset \neg Q(x)) \supset \neg(\forall x P(x) \,\&\, \exists x Q(x))$.

5) Доказать, что формула $\forall x \forall y \forall z (P(x,y) \,\&\, P(y,z) \supset P(x,z)) \,\&\, \forall x \neg P(x,x) \,\&\, \forall x \exists y P(x,y)$ выполнима, но не имеет конечной модели.

6) Доказать, что формула $\forall x \exists y (P(x,y) \,\&\, \neg P(y,x) \,\&\, \neg(P(x,x) \equiv P(y,y)))$ не имеет 3-элементной модели.

7) Доказать, что следующие формулы выполнимы, но не имеют конечных моделей:
   а) $\forall x \exists y \forall z ((P(y,z) \supset P(x,z)) \,\&\, P(x,x) \,\&\, \neg P(y,x))$;
   б) $\forall x \forall y \forall z (P(x,x) \,\&\, (P(x,z) \supset P(x,y) \vee P(y,z))) \,\&\, \forall y \exists z \neg P(y,z)$.

5.6. Равносильные формулы

Формулы Φ и Ψ сигнатуры Ω называются *равносильными*, если формула $\Phi \equiv \Psi$ общезначима. Тот факт, что формулы Φ и Ψ равносильны, обозначается так: $\Phi \sim \Psi$. Нетрудно заметить, что замкнутые формулы (высказывания) Φ и Ψ равносильны, если и только если в любой алгебраической системе истинностные значения высказываний Φ и Ψ совпадают, а формулы со свободными переменными $\Phi(x_1, \ldots, x_n)$ и $\Psi(x_1, \ldots, x_n)$ равносильны тогда и только тогда, когда в любой алгебраической системе $\mathfrak{M} = \langle M, \Omega \rangle$ для любых элементов $a_1, \ldots, a_n \in M$ истинностные значения высказываний $\Phi(a_1, \ldots, a_n)$ и $\Psi(a_1, \ldots, a_n)$ совпадают. Очевидно также, что отношение $\sim$ рефлексивно ($\Phi \sim \Phi$), симметрично (если $\Phi \sim \Psi$, то $\Psi \sim \Phi$) и транзитивно (если $\Phi_1 \sim \Phi_2$ и $\Phi_2 \sim \Phi_3$, то $\Phi_1 \sim \Phi_3$). Таким образом, $\sim$ — отношение эквивалентности на множестве всех формул сигнатуры Ω.

Теорема 5.2. *Каковы бы ни были формула $\Phi(x)$, формула Ψ, не содержащая свободно переменную x, и переменная y, не входящая в формулу $\Phi(x)$, имеют место следующие равносильности:*
1) $\neg \forall x \Phi(x) \sim \exists x \neg \Phi(x)$;
2) $\neg \exists x \Phi(x) \sim \forall x \neg \Phi(x)$;
3) $(\forall x \Phi(x) \,\&\, \Psi) \sim \forall x (\Phi(x) \,\&\, \Psi)$;
4) $(\Psi \,\&\, \forall x \Phi(x)) \sim \forall x (\Psi \,\&\, \Phi(x))$;
5) $(\exists x \Phi(x) \,\&\, \Psi) \sim \exists x (\Phi(x) \,\&\, \Psi)$;
6) $(\Psi \,\&\, \exists x \Phi(x)) \sim \exists x (\Psi \,\&\, \Phi(x))$;
7) $(\forall x \Phi(x) \vee \Psi) \sim \forall x (\Phi(x) \vee \Psi)$;

8) $(\Psi \vee \forall x \Phi(x)) \sim \forall x(\Psi \vee \Phi(x))$;
9) $(\exists x \Phi(x) \vee \Psi) \sim \exists x(\Phi(x) \vee \Psi)$;
10) $(\Psi \vee \exists x \Phi(x)) \sim \exists x(\Psi \vee \Phi(x))$;
11) $(\forall x \Phi(x) \supset \Psi) \sim \exists x(\Phi(x) \supset \Psi)$;
12) $(\Psi \supset \forall x \Phi(x)) \sim \forall x(\Psi \supset \Phi(x))$;
13) $(\exists x \Phi(x) \supset \Psi) \sim \forall x(\Phi(x) \supset \Psi)$;
14) $(\Psi \supset \exists x \Phi(x)) \sim \exists x(\Psi \supset \Phi(x))$;
15) $\forall x \Phi(x) \sim \forall y \Phi(y)$;
16) $\exists x \Phi(x) \sim \exists y \Phi(y)$.

Доказательство. Все эти равносильности доказываются несложными рассуждениями, опирающимися на определение истинности формулы в данной алгебраической системе. Для примера рассмотрим доказательство равносильности $(\forall x \Phi(x) \vee \Psi) \sim \forall x(\Phi(x) \vee \Psi)$. Пусть $\mathfrak{M} = \langle M, \Omega \rangle$ — произвольная алгебраическая система. Всем свободным переменным формул $(\forall x \Phi(x) \vee \Psi)$ и $\forall x(\Phi(x) \vee \Psi)$ придадим конкретные значения из множества M. Для полученных высказываний сохраним обозначения $(\forall x \Phi(x) \vee \Psi)$ и $\forall x(\Phi(x) \vee \Psi)$ и докажем, что $\mathfrak{M} \models (\forall x \Phi(x) \vee \Psi) \Leftrightarrow \mathfrak{M} \models \forall x(\Phi(x) \vee \Psi)$.

Пусть $\mathfrak{M} \models (\forall x \Phi(x) \vee \Psi)$. Это означает, что в $\mathfrak{M}$ истинно хотя бы одно из высказываний $\forall x \Phi(x)$ и Ψ. Если $\mathfrak{M} \models \forall x \Phi(x)$, то $\mathfrak{M} \models \Phi(a)$ для любого $a \in M$. Но тогда, очевидно, $\mathfrak{M} \models \Phi(a) \vee \Psi$ для любого $a \in M$, а это означает, что $\mathfrak{M} \models \forall x(\Phi(x) \vee \Psi)$. Если же $\mathfrak{M} \models \Psi$, то, очевидно, $\mathfrak{M} \models \Phi(a) \vee \Psi$ для любого $a \in M$, откуда снова получаем $\mathfrak{M} \models \forall x(\Phi(x) \vee \Psi)$. Таким образом, мы доказали, что если $\mathfrak{M} \models (\forall x \Phi(x) \vee \Psi)$, то $\mathfrak{M} \models \forall x(\Phi(x) \vee \Psi)$.

Пусть теперь $\mathfrak{M} \models \forall x(\Phi(x) \vee \Psi)$. Это означает, что

$$\mathfrak{M} \models \Phi(a) \vee \Psi \text{ для любого } a \in M. \tag{25}$$

Если при этом $\mathfrak{M} \models \Psi$, то, очевидно, $\mathfrak{M} \models (\forall x \Phi(x) \vee \Psi)$. Если же $\mathfrak{M} \not\models \Psi$, то, как следует из (25), $\mathfrak{M} \models \Phi(a)$ для любого $a \in M$. Но тогда $\mathfrak{M} \models \forall x \Phi(x)$, и снова $\mathfrak{M} \models (\forall x \Phi(x) \vee \Psi)$. □

Следующее довольно очевидное утверждение называют *теоремой об эквивалентной замене.*

Теорема 5.3. *Если формула* Φ' *получена заменой в формуле* Φ *некоторой ее подформулы* Ψ *на формулу* Ψ', *причем* $\Psi \sim \Psi'$, *то* $\Phi \sim \Phi'$.

Эта теорема доказывается несложной индукцией по построению формулы Φ с использованием определения истинности формулы в алгебраической системе. Теорема 5.3 дает важный способ *равносильных преобразований* формул: если часть формулы Φ заменяется на равносильную, то в результате получается формула, равносильная формуле Φ.

Задачи

Привести примеры таких формул Φ и Ψ, что
$(\forall x \Phi \,\&\, \Psi) \not\sim \forall x(\Phi \,\&\, \Psi)$;
$(\Psi \,\&\, \forall x \Phi) \not\sim \forall x(\Psi \,\&\, \Phi)$;
$(\exists x \Phi \,\&\, \Psi) \not\sim \exists x(\Phi \,\&\, \Psi)$;
$(\Psi \,\&\, \exists x \Phi) \not\sim \exists x(\Psi \,\&\, \Phi)$;
$(\forall x \Phi \vee \Psi) \not\sim \forall x(\Phi \vee \Psi)$;
$(\Psi \vee \forall x \Phi) \not\sim \forall x(\Psi \vee \Phi)$;
$(\exists x \Phi \vee \Psi) \not\sim \exists x(\Phi \vee \Psi)$;
$(\Psi \vee \exists x \Phi) \not\sim \exists x(\Psi \vee \Phi)$;
$(\forall x \Phi \supset \Psi) \not\sim \exists x(\Phi \supset \Psi)$;
$(\Psi \supset \forall x \Phi) \not\sim \forall x(\Psi \supset \Phi)$;
$(\exists x \Phi \supset \Psi) \not\sim \forall x(\Phi \supset \Psi)$;
$(\Psi \supset \exists x \Phi) \not\sim \exists x(\Psi \supset \Phi)$.

5.7. Предваренные формулы

Формула называется *предваренной*, если она бесквантворная (т. е. не содержит кванторов) или имеет вид $Q_1 x_1 \ldots Q_n x_n \Phi$, где Φ — бесквантворная формула, а Q_i $(i = 1, \ldots, n)$ есть квантор $\forall$ или $\exists$. Например, $\forall x(P(x) \vee Q(y))$ — предваренная формула, а формула $\forall x P(x) \vee Q(y)$ не является предваренной.

Теорема 5.4. *Для любой формулы* Φ *существует предваренная формула* Ψ *такая, что* $\Phi \sim \Psi$.

Доказательство. Теорема доказывается индукцией по построению формулы Φ.

Если Φ — атомная формула, то Φ — бескванторная, следовательно, предваренная формула, и в качестве Ψ можно взять Φ.

Пусть формула Φ имеет вид $\neg\Phi_1$, причем для формулы Φ_1 построена равносильная ей предваренная формула Ψ_1. Тогда, в силу теоремы об эквивалентной замене (теорема 5.3), $\Phi \sim \neg\Psi_1$. Пусть формула Ψ_1 имеет вид $Q_1x_1\ldots Q_nx_n\Psi_1'$, где $Q_1,\ldots,Q_n$ — кванторные символы, а Ψ_1' — бескванторная формула. Тогда $\Phi \sim \neg Q_1x_1\ldots Q_nx_n\Psi_1'$. Применяя равносильности 1) и 2) из теоремы 5.2, получаем, что $\neg Q_1x_1\ldots Q_nx_n\Psi_1' \sim \bar{Q}_1x_1\ldots\bar{Q}_nx_n\neg\Psi_1'$, где $\bar{\forall}$ есть $\exists$, а $\bar{\exists}$ есть $\forall$. Таким образом, в качестве Ψ можно взять формулу $\bar{Q}_1x_1\ldots\bar{Q}_nx_n\neg\Psi_1'$.

Пусть формула Φ имеет вид $\Phi_1\lambda\Phi_2$, где λ есть $\&$, $\vee$ или $\supset$, причем для формул Φ_1 и Φ_2 уже построены равносильные им предваренные формулы Ψ_1 и Ψ_2. Тогда $\Phi \sim \Psi_1\lambda\Psi_2$. Индукцией по суммарному количеству n кванторов в формулах Ψ_1 и Ψ_2 докажем, что для формулы $\Psi_1\lambda\Psi_2$ существует равносильная ей предваренная формула, и попутно покажем, как ее строить. Если $n=0$, то Ψ_1 и Ψ_2 — бескванторные формулы, и формула $\Psi_1\lambda\Psi_2$ сама является предваренной. Пусть доказываемое утверждение верно для $n=k$. Если теперь $n=k+1$, то хотя бы одна из формул Ψ_1 и Ψ_2 содержит квантор. Пусть формула Ψ_1 имеет вид $Qx\Psi_1'(x)$, где $\Psi_1'(x)$ — предваренная формула. Тогда формула $\Psi_1\lambda\Psi_2$ имеет вид $Qx\Psi_1'(x)\lambda\Psi_2$. Пусть для определенности Q есть $\forall$, а λ есть $\&$. Если x не входит свободно в Ψ_2, воспользуемся равносильностью 3) из теоремы 5.2. Получим, что $(Qx\Psi_1'(x)\lambda\Psi_2) \sim Qx(\Psi_1'(x)\lambda\Psi_2)$. Суммарное количество кванторов в формулах $\Psi_1'(x)$ и Ψ_2 равно k, и по индуктивному предположению формула $\Psi_1'(x)\lambda\Psi_2$ равносильна некоторой предваренной формуле Ψ''. Значит, $Qx(\Psi_1'(x)\lambda\Psi_2) \sim Qx\Psi''$, и в качестве Ψ можно взять формулу $Qx\Psi''$. Если же x входит свободно в Ψ_2, воспользуемся равносильностью 15) из теоремы 5.2 и, выбрав переменную y, не входящую свободно в Ψ_2 и вообще не встречающуюся в формуле $\Psi_1'(x)$, заменим формулу $Qx\Psi_1'(x)$ на равносильную ей формулу $Qy\Psi_1'(y)$, и далее рассуждаем, как выше. При рассмотрении других случаев для кванторного символа Q и связки λ нужно пользоваться подходящими из равносильностей 5), 7), 9), 11), 13), 15), 16) теоремы 5.2. Если формула Ψ_1 является бескванторной, а формула Ψ_2 имеет вид $Qx\Psi_2'(x)$, где $\Psi_2'(x)$ — предваренная формула, рассуждаем точно так же, пользуясь равносильностями 4), 6), 8), 10), 12), 14), 15), 16) теоремы 5.2.

Пусть формула Φ имеет вид $Qx\Phi_1$, где Q есть $\forall$ или $\exists$, причем для формулы Φ_1 построена равносильная ей предваренная формула Ψ_1. Тогда формула Φ равносильна предваренной формуле $Qx\Psi_1$, что и требовалось доказать. $\square$

Построение предваренной формулы, равносильной данной формуле Φ, называют приведением формулы Φ к *предваренному виду* или *предваренной форме*.

Задачи

Привести к предваренной форме следующие формулы:

1) $\neg\exists x\forall y\exists z\forall u P(x,y,z,u)$;

2) $\exists x\forall y P(x,y)\,\&\,\exists x\forall y Q(x,y)$;

3) $\exists x\forall y P(x,y)\vee\exists x\forall y Q(x,y)$;

4) $\exists x\forall y P(x,y)\supset\exists x\forall y Q(x,y)$;

5) $\forall x\exists y(P(x)\supset Q(y,z))\supset\exists x\forall z(Q(x,z)\,\&\,P(y))$;

6) $\forall x P(x)\supset\forall y(\forall z Q(x,z)\supset\forall u P(u))$.

5.8. Аксиоматические теории

Аксиоматический метод построения научной теории состоит в том, что некоторые исходные положения, называемые *аксиомами* или *постулатами*, принимаются «без доказательства», а все другие утверждения этой теории выводятся из них путем рассуждения.

Аксиоматический метод в математике впервые был использован Евклидом в III веке до н. э. в его книге «Начала» при изложении основ элементарной геометрии, теории чисел, алгебры и других разделов античной математики. «Начала» Евклида составлены по определенной схеме, сложившейся еще до Евклида в древнегреческой науке: сначала приводятся определения и постулаты, а затем формулировки теорем и их доказательства. Некоторые *определения* в «Началах» — это просто *описания* исходных понятий. Например, «Точка есть то, что не имеет частей». Ясно, что такое «определение» вряд ли может быть использовано в математических доказательствах. Однако в «Началах» имеются и определения, являющиеся таковыми в

современном смысле: они *называют* понятия. Например, «Параллельные суть прямые, которые, находясь в одной плоскости и будучи неограниченно продолжены в обе стороны, ни с той, ни с другой стороны между собой не встречаются». Вслед за определениями в «Началах» идут *постулаты*. среди них — знаменитый V постулат Евклида: «Если прямая, пересекающая две прямые, образует с ними внутренние односторонние углы, сумма которых меньше двух прямых, то эти прямые пересекаются с той стороны, где эта сумма меньше двух прямых». На основе определений и постулатов путем доказательства выводятся новые геометрические утверждения — *теоремы*.

Поскольку предполагалось, что геометрия есть описание реального физического пространства, вполне естественно, что Евклид считал постулаты «самоочевидными истинами». Однако V постулат кажется слишком сложным, чтобы его можно было причислить к «самоочевидным истинам». Поэтому на протяжении веков было потрачено много усилий на попытки доказать V постулат на основе остальных постулатов. Хотя все эти попытки оказались неудачными, они все же привели к некоторым положительным результатам. В частности, было доказано, что V постулат Евклида эквивалентен следующему утверждению: «Через точку, не лежащую на данной прямой, проходит ровно одна прямая, параллельная данной прямой».

К началу XIX века начало возникать подозрение о недоказуемости V постулата Евклида. Это подозрение перешло почти в полную уверенность, когда в 1826 году великий русский математик Н. И. Лобачевский построил геометрическую теорию, основанную на системе постулатов, в которой V постулат Евклида заменен утверждением, несовместимым с ним: «Через точку, не лежащую на данной прямой, проходит более чем одна прямая, параллельная данной прямой». Хотя «истинность» такой аксиомы кажется сомнительной, при выводе следствий из нее какие-либо противоречия не встречаются.

Следующим событием на пути построения неевклидовой геометрии явилось построение различных моделей геометрии Лобачевского средствами геометрии Евклида. Например, в модели, предложенной выдающимся немецким математиком Клейном в 1871 году, плоскость интерпретируется как внутренность какого-нибудь круга, а прямая — как хорда этого круга без своих концов. В такой интерпретации оказываются истинными все аксиомы геометри Лобачевского. Наличие подобных моделей показывает, что геометрия Лобачевского столь же непротиворечива, как и геометрия Евклида.

Построение моделей геометрии Лобачевского имело принципиальное значение для развития аксиоматического метода, поскольку оно привело к осознанию возможности рассматривать аксиоматическую теорию чисто формально, не предполагая заранее какое-либо определенное значение основных понятий. Более того, мы вольны выбирать значения этих понятий каким угодно образом, лишь бы при этом оказывались истинными аксиомы.

Полная свобода от какой-либо интерпретации позволяет расширить и само понятие аксиоматической теории. Представление об аксиомах как «самоочевидных истинах» теряет смысл: утверждение, очевидное в одной интерпретации, может не быть таковым, оставаясь истинным, в другой интерпретации. Нас будут интересовать только такие аксиоматические теории, аксиомы которых записываются в виде формул подходящего элементарного языка.

5.9. Элементарные теории

Элементарной теорией, или *теорией первого порядка* называется произвольное множество высказываний некоторого элементарного языка. Высказывания, составляющие теорию, будем называть *аксиомами* этой теории. Теория называется *совместной*, если она имеет модель. В противном случае теория называется *несовместной*. Рассмотрим некоторые примеры элементарных теорий.

1. Наивная теория множеств. Язык теории множеств рассматривался в разделе 5.3. Его сигнатура состоит из одного двуместного предикатного символа $\in$. На этом языке можно записать многие предложения, относящиеся к теории множеств. Например, $\forall u(u \in z \equiv (z \in x \vee z \in y)$ означает $z = x \cup y$.

В канторовской теории множеств основополагающим является так называемый *принцип свертывания*: если имеется некоторое свойство, которым могут обладать или не обладать произвольные множества, то существует множество, содержащее только те множества, которые обладают этим свойством. Если ограничиться рассмотрением только таких свойств множеств, которые выражаются формулами языка теории множеств, указанный принцип можно выразить посредством схемы аксиом $\exists x \forall y(y \in x \equiv \Phi)$, называемой *аксиомой свертывания*, где Φ — произвольная формула рассматриваемого языка, не содержащая свободно переменную x. Теория, состоящая из универсальных замыканий всех примеров аксиомы свертывания называется *наивной теорией множеств*.

2. Теория групп. *Язык теории групп* состоит из одной константы 0, одного двуместного функционального символа $+$ и предикатного символа равенства $=$. Условимся писать $(t_1 + t_2)$ и $t_1 = t_2$ вместо $+(t_1, t_2)$ и $=(t_1, t_2)$ соответственно. На этом языке аксиомы группы записываются следущим образом:

G1. $\forall x \forall y \forall z((x + y) + z = x + (y + z))$;

G2. $\forall x(x+0=x\,\&\,0+x=x)$;

G3. $\forall x\exists y(x+y=0\,\&\,y+x=0)$.

Теория, состоящая из высказываний G1 – G3, называется *теорией групп*. Интерпретация теории первого порядка в языке, содержащем символ равенства, называется *нормальной*, если в ней символ $=$ интерпретируется именно как равенство. Всякая нормальная модель теории групп является (или называется) *группой*.

3. Теория частично упорядоченных множеств. *Язык упорядоченных множеств* содержит только символ равенства и двуместный предикатный символ $\leq$. Условимся писать $t_1 \leq t_2$ и $t_1 = t_2$ вместо $\leq(t_1,t_2)$ и $=(t_1,t_2)$ соответственно. *Теория частично упорядоченных множеств* состоит из следующих аксиом:

O1. $\forall x\neg(x\leq x)$;

O2. $\forall x\forall y(x\leq y\,\&\,y\leq x\supset x=y)$;

O3. $\forall x\forall y\forall z(x\leq y\,\&\,y\leq z\supset x\leq z)$.

Всякая нормальная модель этой теории является частично упорядоченным множеством.

Задачи

1) Доказать, что наивная теория множеств несовместна. (Указание: рассмотреть пример аксиомы свертывания, когда Φ есть формула $\neg(y\in y)$.)

2) Выписать аксиомы теории линейно упорядоченных множеств.

3) Описать элементарные языки для теории колец и теории полей. Выписать аксиомы кольца и аксиомы поля.

5.10. Логическое следствие

Говорят, что высказывание Φ языка Ω *логически (семантически) следует* из множества высказываний T языка Ω, и пишут $T\models\Phi$, если Φ истинно во всякой модели множества T. В этом случае высказывание Φ называется *логическим следствием* множества высказываний T.

Теоремами теории первого порядка T в языке Ω называются высказывания языка Ω, которые логически следуют из T. Таким образом, теорема данной теории T — это высказывание, истинное во всех моделях теории T.

Теорема 5.5. *Высказывание Φ языка Ω является логическим следствием множества высказываний T языка Ω тогда и только тогда, когда множество высказываний $T\cup\{\neg\Phi\}$ невыполнимо.*

Доказательство. 1) Пусть Φ является логическим следствием множества высказываний T, т. е. $T\models\Phi$. Докажем, что множество $T\cup\{\neg\Phi\}$ невыполнимо. Допустим противное, т. е. что существует модель $\mathfrak{M}$ множества $T\cup\{\neg\Phi\}$. Тогда $\mathfrak{M}\models T$ и $\mathfrak{M}\models\neg\Phi$. Но так как Φ логически следует из T, то Φ истинно в любой модели множества T, в частности, $\mathfrak{M}\models\Phi$, что невозможно. Полученное противоречие показывает, что множество $T\cup\{\neg\Phi\}$ невыполнимо.

2) Пусть множество $T\cup\{\neg\Phi\}$ невыполнимо. Докажем, что $T\models\Phi$. Пусть $\mathfrak{M}$ — модель множества T. Тогда непременно $\mathfrak{M}\models\Phi$, ибо в противном случае $\mathfrak{M}$ была бы моделью множества $T\cup\{\neg\Phi\}$, что невозможно. □

Теорему 5.5 можно переформулировать так: высказывание Φ является теоремой теории T тогда и только тогда, когда при добавлении аксиомы $\neg\Phi$ к теории T получается несовместная теория.

Задачи

1) Доказать, что если T — несовместная теория в языке Ω, то любое высказывание языка Ω является теоремой теории T.

2) Доказать, что если существует такое высказывание Φ, что Φ и $\neg\Phi$ являются теоремами теории T, то T несовместна.

3) Является ли высказывание $\forall x\forall y(x+y=y+x)$ теоремой теории групп?

4) Доказать, что высказывание $\forall x\forall y(x+y=x\,\&\,y+x=x\supset y=0)$ является теоремой теории групп.

5) Пусть Φ есть формула $\exists x\forall y(x\leq y)$. Доказать, что ни Φ, ни $\neg\Phi$ не являются теоремами теории частично упорядоченных множеств.

6. Исчисление предикатов

Нахождение логических следствий из системы аксиом данной аксиоматической математической теории составляет основное содержание деятельности всякого математика. Как практически искать логические следствия из данной системы аксиом? Ясно, что нет смысла действовать в полном соответствии с определением логического следствия, т. е. перебрать все модели данной системы аксиом и убедиться, что в них истинно данное утверждение, ибо у совместной теории бесконечно много моделей. Все же иногда путем некоторого рассуждения удается доказать, что то или иное утверждение логически следует из аксиом. Такое рассуждение мы называем *доказательством*, а полученное с его помощью следствие из аксиом — *теоремой*. Оказывается, что таким образом можно доказать любое утверждение, логически вытекающее из аксиом, записанных в виде формул языка первого порядка, а необходимые для этого методы доказательства можно полностью обозреть и систематизировать. Это делается с помощью так называемого *исчисления предикатов*.

6.1. Классическое исчисление предикатов

Пусть фиксирован некоторый элементарный язык сигнатуры Ω. Исчисление предикатов в сигнатуре Ω задается следующим набором *схем аксиом*:

1) $A \supset (B \supset A)$;

2) $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;

3) $A \,\&\, B \supset A$;

4) $A \,\&\, B \supset B$;

5) $A \supset (B \supset A \,\&\, B)$;

6) $A \supset A \vee B$;

7) $B \supset A \vee B$;

8) $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;

9) $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;

10) $\neg\neg A \supset A$;

11) $\forall v A(v) \supset A(t)$;

12) $A(t) \supset \exists v A(v)$.

В схемах 11 и 12 $A(v)$ — произвольная формула сигнатуры Ω, v — произвольная переменная, t — терм сигнатуры Ω, *свободный для переменной v в формуле $A(v)$* (т. е. никакое свободное вхождение переменной v в формулу $A(v)$ не находится в области действия квантора по переменной, входящей в t), $A(t)$ — результат *подстановки* терма t вместо всех свободных вхождений переменной v в формулу $A(v)$.

Правилами вывода исчисления предикатов являются:

(I) $\dfrac{A,\ A \supset B}{B}$ (*modus ponens*);

(II) $\dfrac{A \supset B}{\exists v A \supset B}$ (*удаление квантора существования*);

(III) $\dfrac{B \supset A}{B \supset \forall v A}$ (*введение квантора всеобщности*).

В правилах (II) и (III) A и B — произвольные формулы сигнатуры Ω, v — произвольная переменная, не имеющая свободных вхождений в формулу B.

Выводом в исчислении предикатов называется конечная последовательность формул $\Phi_1, \ldots, \Phi_n$ такая, что для каждого $i = 1, \ldots, n$ формула Φ_i либо есть аксиома, либо получается из одной или двух предыдущих формул по одному из правил вывода. Говорят, что формула Φ *выводима* в исчислении предикатов и пишут $\vdash \Phi$, если существует вывод в исчислении предикатов, оканчивающийся формулой Φ. Будем говорить, что применение правила (II) или (III) *связывает* переменную v.

Пример. Следующая последовательность формул является выводом формулы $\forall x P(x) \supset \forall y P(y)$:

1. $\forall x P(x) \supset P(y)$ (аксиома 11);

2. $\forall x P(x) \supset \forall y P(y)$ (получено по правилу (III) из формулы 1).

В этом выводе применение правила (III) связывает переменную y.

Пусть Γ — некоторое множество формул, которые мы условно будем называть *гипотезами*. *Квазивыводом из множества гипотез* Γ называется конечная последовательность формул $\Phi_1, \ldots, \Phi_n$ такая, что для каждого $i = 1, \ldots, n$ формула Φ_i либо есть аксиома, либо есть гипотеза (т. е. принадлежит множеству Γ), либо получается из одной или двух предыдущих формул по одному из правил вывода. Для произвольного квазивывода $\Phi_1, \ldots, \Phi_n$ и для каждого $i = 1, \ldots, n$ определим по индукции множество формул $\Delta(\Phi_i) \subseteq \Gamma$:

1) если Φ_i есть аксиома, то $\Delta(\Phi_i) = \emptyset$;

2) если Φ_i есть гипотеза, то $\Delta(\Phi_i) = \{\Phi_i\}$;

3) если формула Φ_i получена по правилу modus ponens из Φ_k и Φ_l $(k, l < i)$, то $\Delta(\Phi_i) = \Delta(\Phi_k) \cup \Delta(\Phi_l)$;

4) если формула Φ_i получена по правилу (II) или (III) из формулы Φ_k $(k < i)$, то $\Delta(\Phi_i) = \Delta(\Phi_k)$.

Если гипотеза $\Phi \in \Gamma$ принадлежит множеству $\Delta(\Phi_i)$, будем говорить, что в данном квазивыводе формула Φ_i *зависит* от гипотезы Φ.

Выводом из Γ называется квазивывод из Γ, удовлетворяющий следующему условию: всякое применение в этом квазивыводе правила (II) или (III) к формуле Φ_i связывает переменную, не входящую свободно ни в одну из формул из множества $\Delta(\Phi_i)$. Говорят, что формула Φ *выводима из множества гипотез* Γ и пишут $\Gamma \vdash \Phi$, если существует вывод из Γ, оканчивающийся формулой Φ. Заметим, что $\vdash \Phi$ означает то же самое, что и $\emptyset \vdash \Phi$.

Пример 1. Следующая последовательность формул является выводом формулы $Q(x)$ из множества гипотез $\{P(x), \forall y(P(y) \supset Q(y))\}$:
1. $\forall y(P(y) \supset Q(y))$ (гипотеза);
2. $\forall y(P(y) \supset Q(y)) \supset (P(x) \supset Q(x))$ (аксиома 11);
3. $P(x) \supset Q(x)$ (получено по правилу modus ponens из формул 1 и 2);
4. $P(x)$ (гипотеза);
5. $Q(x)$ (получено по правилу modus ponens из формул 3 и 4).

Пример 2. Пусть переменная u не входит в формулу $\Phi(v)$. Следующая последовательность является выводом формулы $\exists u\Phi(u)$ из множества гипотез $\{\exists v\Phi(v)\}$:
1. $\exists v\Phi(v)$ (гипотеза);
2. $\Phi(v) \supset \exists u\Phi(u)$ (аксиома 12);
3. $\exists v\Phi(v) \supset \exists u\Phi(u)$ (получено по правилу (II) из формулы 2);
4. $\exists u\Phi(u)$ (получено по правилу modus ponens из формул 1 и 3).

Отметим некоторые очевидные, но важные свойства выводимости.
1) *Монотонность*: если $\Gamma \vdash \Phi$ и $\Gamma \subseteq \Delta$, то $\Delta \vdash \Phi$.
2) *Компактность*: если $\Gamma \vdash \Phi$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash \Phi$.

Нетрудно проверить, что каждая аксиома исчисления предикатов общезначима, т. е. истинна в любой интерпретации при любой оценке свободных переменных. Довольно очевидна также корректность каждого из трех правил вывода: при применении этих правил к общезначимым формулам получается общезначимая формула. Это позволяет утверждать, что верна следующая теорема о корректности исчисления предикатов.

Теорема 6.1. *Всякая формула, выводимая в исчислении предикатов, общезначима.*

Тавтологией в языке Ω назовем формулу, получающуюся подстановкой формул языка Ω вместо пропозициональных переменных в пропозициональную тавтологию. Например, если Φ — произвольная формула языка Ω, то формула $\Phi \supset \Phi$ является тавтологией в языке Ω.

Теорема 6.2. *Всякая тавтология выводима в исчислении предикатов.*

Доказательство. Пусть тавтология получена подстановкой некоторых формул $\Phi_1, \ldots, \Phi_n$ в пропозициональную тавтологию $A(p_1, \ldots, p_n)$ вместо пропозициональных переменных $p_1, \ldots, p_n$, т. е. имеет вид $A(\Phi_1, \ldots, \Phi_n)$. В силу теоремы о полноте исчисления высказываний (теорема 4.16), существует вывод формулы $A(p_1, \ldots, p_n)$ в исчислении высказываний. Поскольку все схемы аксиом исчисления высказываний являются схемами аксиом исчисления предикатов, то, заменив в этом выводе переменные $p_1, \ldots, p_n$ на формулы $\Phi_1, \ldots, \Phi_n$, а остальные пропозициональные переменные — на произвольные формулы языка Ω, получим вывод формулы $A(\Phi_1, \ldots, \Phi_n)$ в исчислении предикатов, что и требовалось. $\square$

Задачи

1) Определить, являются ли выводами в исчислении предикатов следующие последовательности формул:

   а) 1. $\forall x \exists y P(x,y) \supset \exists y P(f(y),y)$;

   б) 1. $\forall x P(x) \supset P(f(y))$,
      2. $\forall x P(x) \supset \forall y P(f(y))$;

   в) 1. $P(x) \supset \exists x P(x)$,
      2. $(P(x) \supset \exists x P(x)) \supset (\forall x P(x) \supset (P(x) \supset \exists x P(x)))$,
      3. $\forall x P(x) \supset (P(x) \supset \exists x P(x))$.

2) Построить выводы в исчислении предикатов следующих формул:

   а) $\forall x \forall y P(x,y) \supset \forall y \forall x P(x,y)$;

   б) $\exists x \exists y P(x,y) \supset \exists y \exists x P(x,y)$;

   в) $\exists x \forall y P(x,y) \supset \forall y \exists x P(x,y)$;

   г) $\forall x \forall y P(x,y) \supset \forall x P(x,x)$;

   д) $\exists x P(x,x) \supset \exists y \exists x P(x,y)$.

3) Пусть переменная y не входит свободно в формулу $\Phi(x)$ и свободна для x в $\Phi(x)$. Доказать, построив выводы:

   а) $\exists y \Phi(y) \vdash \exists x \Phi(x)$;

   б) $\forall y \Phi(y) \vdash \forall x \Phi(x)$.

4) Пусть переменная x не входит свободно в формулу Φ. Построить выводы следующих формул:

   а) $\Phi \supset \forall x \Phi$;

   б) $\exists x \Phi \supset \Phi$.

5) Построить выводы из множества гипотез $\{\forall x(P(x) \supset Q(x))\}$ следующих формул:

   а) $\exists x P(x) \supset \exists x Q(x)$;

   б) $\forall y P(y) \supset \forall z Q(z)$.

6) Доказать, что если $\Gamma \vdash \forall v A(v)$, то $\Gamma \vdash A(t)$ для любого терма t, свободного для v в $A(v)$.

7) Доказать, что если $\Gamma \vdash A(t)$ для некоторого терма t, свободного для v в $A(v)$, то $\Gamma \vdash \exists v A(v)$.

6.2. Теорема о дедукции

Теорема 6.3 (теорема о дедукции). *Каковы бы ни были множество формул* Γ *и формулы* Φ, Ψ, *если* $\Gamma \cup \{\Phi\} \vdash \Psi$, *то* $\Gamma \vdash \Phi \supset \Psi$.

Доказательство. Сначала отметим одно простое, но важное свойство выводимости. Пусть имеется вывод $\Phi_1, \ldots, \Phi_n$ формулы Ψ из множества гипотез Γ, в котором Ψ не зависит от гипотезы $\Phi \in \Gamma$. Вычеркнем из него все формулы Φ_i, для которых $\Phi \in \Delta(\Phi_i)$. Нетрудно проверить, что получившаяся новая последовательность формул является выводом из множества $\Gamma \setminus \{\Phi\}$ и оканчивается формулой Ψ, т. е. является выводом формулы Ψ из $\Gamma \setminus \{\Phi\}$. Более того, в полученном выводе каждая формула зависит от тех же гипотез, от которых она зависела в исходном выводе.

Приступим к доказательству теоремы о дедукции. Пусть $\Phi_1, \ldots, \Phi_n$ — вывод формулы Ψ из множества гипотез $\Gamma \cup \{\Phi\}$. Для $i = 1, \ldots, n$ через $\Delta'(\Phi_i)$ обозначим множество тех гипотез из Γ, от которых в этом выводе зависит формула Φ_i (иными словами, $\Delta'(\Phi_i) = \Delta(\Phi_i) \cap \Gamma$). По индукции докажем, что для любого $i = 1, \ldots, n$ существует вывод из Γ формулы $\Phi \supset \Phi_i$, в котором $\Phi \supset \Phi_i$ не зависит от гипотез, не входящих в $\Delta'(\Phi_i)$.

Сначала рассмотрим случай, когда в выводе $\Phi_1, \ldots, \Phi_n$ формула Φ_i не зависит от Φ. Тогда, как мы заметили выше, существует вывод формулы Φ из Γ, в котором Φ_i зависит от тех же гипотез, что и в исходном выводе. Продолжим этот вывод до вывода формулы $\Phi \supset \Phi_i$ из Γ:

... [вывод формулы Φ из Γ]

а) Φ_i (зависит от $\Delta(\Phi_i)$);

a+1) $\Phi_i \supset (\Phi \supset \Phi_i)$ (аксиома 1, зависит от $\emptyset$);

a+2) $\Phi \supset \Phi_i$ (получено по правилу modus ponens из формул a) и a+1), зависит от $\Delta(\Phi_i)$).

Теперь рассмотрим случай, когда Φ_i есть формула Φ. Тогда следующая последовательность формул является выводом формулы $\Phi \supset \Phi_i$, т. е. формулы $\Phi \supset \Phi$, в исчислении предикатов:

1) $(\Phi \supset (\Phi \supset \Phi)) \supset ((\Phi \supset ((\Phi \supset \Phi) \supset \Phi)) \supset (\Phi \supset \Phi))$ (аксиома 2);

2) $\Phi \supset (\Phi \supset \Phi)$ (аксиома 1);

3) $(\Phi \supset ((\Phi \supset \Phi) \supset \Phi)) \supset (\Phi \supset \Phi)$ (получено по правилу modus ponens из формул 1 и 2);

4) $\Phi \supset ((\Phi \supset \Phi) \supset \Phi)$ (аксиома 1);

5) $\Phi \supset \Phi$ (получено по правилу modus ponens из формул 3 и 4).

Этот вывод является также выводом формулы $\Phi \supset \Phi$ из Γ, причем в этом выводе формула $\Phi \supset \Phi$ не зависит ни от каких гипотез, в частности, не зависит от гипотез, не входящих в $\Delta'(\Phi_i)$.

Перейдем к доказательству по индукции для общего случая. Если $i = 1$, то формула Φ_i либо 1) является аксиомой или принадлежит множеству Γ, либо 2) совпадает с Φ. В случае 1) Φ_i не зависит от Φ, и утверждение доказано выше. В случае 2) утверждение также доказано выше.

Пусть $i = k + 1$, и для каждого $j \leq k$ доказываемое утверждение верно, т. е. существует вывод из Γ формулы $\Phi \supset \Phi_j$, в котором Φ_j не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$. В случаях, когда Φ_i является аксиомой или гипотезой из $\Gamma \cup \{\Phi\}$, утверждение уже доказано. Рассмотрим случай, когда в исходном выводе из $\Gamma \cup \{\Phi\}$ формула Φ_i получена по одному из правил вывода.

Пусть формула Φ_i получена по правилу modus ponens из формул Φ_j и Φ_l $(j, l \leq k)$, причем формула Φ_l имеет вид $\Phi_j \supset \Phi_i$. В этом случае $\Delta'(\Phi_i) = \Delta'(\Phi_j) \cup \Delta'(\Phi_l)$. По индуктивному предположению, существует вывод из Γ формулы $\Phi \supset \Phi_j$, в котором $\Phi \supset \Phi_j$ не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$, а также существует вывод из Γ формулы $\Phi \supset \Phi_l$, в котором $\Phi \supset \Phi_l$ не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$. Выпишем подряд эти выводы и продолжим их до вывода из Γ формулы $\Phi \supset \Phi_i$:

. . . [вывод из Γ формулы $\Phi \supset \Phi_j$]

a) $\Phi \supset \Phi_j$ (зависит только от $\Delta'(\Phi_j)$);

. . . [вывод из Γ формулы $\Phi \supset \Phi_l$]

b) $\Phi \supset (\Phi_j \supset \Phi_i)$ (зависит только от $\Delta'(\Phi_l)$);

b+1) $(\Phi \supset \Phi_j) \supset ((\Phi \supset (\Phi_j \supset \Phi_i)) \supset (\Phi \supset \Phi_i))$ (аксиома 2, зависит от $\emptyset$);

b+2) $(\Phi \supset (\Phi_j \supset \Phi_i)) \supset (\Phi \supset \Phi_i)$ (получено по правилу modus ponens из формул a) и b+1), зависит только от $\Delta'(\Phi_j)$;

b+3) $\Phi \supset \Phi_i$ (получено по правилу modus ponens из формул b) и b+2), зависит только от $\Delta'(\Phi_j) \cup \Delta'(\Phi_l) = \Delta'(\Phi_i)$.

Пусть формула Φ_i получена по правилу (II) из формулы Φ_j $(j \leq k)$. В этом случае формула Φ_j имеет вид $\Phi' \supset \Psi$, а формула Φ_i имеет вид $\exists v \Phi' \supset \Psi$, где Φ' и Ψ — формулы сигнатуры Ω, v — переменная, не имеющая свободных вхождений в Ψ. При этом $\Delta(\Phi_i) = \Delta(\Phi_j)$. Случай, когда Φ_i не зависит от Φ, нами уже рассмотрен. Поэтому будем считать, что Φ_i зависит от Φ. Следовательно, Φ_j также зависит от Φ. Отсюда и из определения вывода из гипотез вытекает, что Φ и все формулы из $\Delta'(\Phi_j)$ не содержат свободных вхождений переменной v. По индуктивному предположению, существует вывод из Γ формулы $\Phi \supset \Phi_j$ (т. е. формулы $\Phi \supset (\Phi' \supset \Psi)$), в котором $\Phi \supset \Phi_j$ не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$. Продолжим его до вывода из Γ формулы $\Phi \supset \Phi_i$ (т. е. формулы $\Phi \supset (\exists v \Phi' \supset \Psi)$), в котором $\Phi \supset \Phi_i$ не зависит от гипотез, не входящих в $\Delta'(\Phi_i)$:

. . . [вывод из Γ формулы $\Phi \supset (\Phi' \supset \Psi)$]

a) $\Phi \supset (\Phi' \supset \Psi)$ (зависит только от $\Delta'(\Phi_j)$);

. . . [вывод формулы $\Phi' \supset (\Phi \supset \Psi)$ из формулы $\Phi \supset (\Phi' \supset \Psi)$ средствами исчисления высказываний];

b) $\Phi' \supset (\Phi \supset \Psi)$ (зависит только от $\Delta'(\Phi_j)$);

b+1) $\exists v \Phi' \supset (\Phi \supset \Psi)$ (получено по правилу (II) из b), зависит только от $\Delta'(\Phi_j)$);

. . . [вывод формулы $\Phi \supset (\exists v \Phi' \supset \Psi)$ из формулы $\exists v \Phi' \supset (\Phi \supset \Psi)$ средствами исчисления высказываний];

c) $\Phi \supset (\exists v \Phi' \supset \Psi)$ (зависит только от $\Delta'(\Phi_j) = \Delta'(\Phi_i)$).

Таким образом, случай, когда формула Φ_i получена по правилу (II), полностью рассмотрен.

Пусть формула Φ_i получена по правилу (III) из формулы Φ_j $(j \leq k)$. В этом случае формула Φ_j имеет вид $\Psi \supset \Phi'$, а формула Φ_i имеет вид $\Psi \supset \forall v \Phi'$, где Φ' и Ψ — формулы сигнатуры Ω, v — переменная, не имеющая свободных вхождений в Ψ. При этом $\Delta(\Phi_i) = \Delta(\Phi_j)$. Случай, когда Φ_i не зависит от Φ, нами уже рассмотрен. Поэтому будем считать, что Φ_i зависит от Φ. Следовательно, Φ_j также зависит от Φ. Отсюда и из определения вывода из гипотез вытекает, что Φ и все формулы из $\Delta'(\Phi_j)$ не содержат свободных

вхождений переменной v. По индуктивному предположению, существует вывод из Γ формулы $\Phi \supset \Phi_j$ (т. е. формулы $\Phi \supset (\Psi \supset \Phi')$), в котором $\Phi \supset \Phi_j$ не зависит от гипотез, не входящих в $\Delta'(\Phi_j)$. Продолжим его до вывода из Γ формулы $\Phi \supset \Phi_i$ (т. е. формулы $\Phi \supset (\Psi \supset \forall v\Phi')$), в котором $\Phi \supset \Phi_i$ не зависит от гипотез, не входящих в $\Delta'(\Phi_i)$:

... [вывод из Γ формулы $\Phi \supset (\Psi \supset \Phi')$]

a) $\Phi \supset (\Psi \supset \Phi')$ (зависит только от $\Delta'(\Phi_j)$);

... [вывод формулы $\Phi \,\&\, \Psi \supset \Phi'$ из формулы $\Phi \supset (\Psi \supset \Phi')$ средствами исчисления высказываний];

b) $\Phi \,\&\, \Psi \supset \Phi'$ (зависит только от $\Delta'(\Phi_j)$);

b+1) $\Phi \,\&\, \Psi \supset \forall v\Phi'$ (получено по правилу (III) из формулы b), зависит только от $\Delta'(\Phi_j)$);

... [вывод формулы $\Phi \supset (\Psi \supset \forall v\Phi')$ из формулы $\Phi \,\&\, \Psi \supset \forall v\Phi'$ средствами исчисления высказываний];

c) $\Phi \supset (\Psi \supset \forall v\Phi')$ (зависит только от $\Delta'(\Phi_j) = \Delta'(\Phi_i)$).

Таким образом, случай, когда формула Φ_i получена по правилу (III), также полностью рассмотрен. Теорема 6.3 доказана.

Рассмотрим одно применение теоремы о дедукции.

Теорема 6.4 (обобщенная теорема от корректности). *Каковы бы ни были множество высказываний* Γ *и высказывание* Φ, *если* $\Gamma \vdash \Phi$, *то* $\Gamma \models \Phi$.

Доказательство. Пусть $\Gamma \vdash \Phi$. Тогда, в силу свойства компактности, существует конечное множество $\Delta = \{\Phi_1, \ldots, \Phi_n\} \subseteq \Gamma$ такое, что $\Delta \vdash \Phi$. Применяя n раз теорему о дедукции, получаем

$$\vdash \Phi_1 \supset (\ldots \supset (\Phi_n \supset \Phi)\ldots).$$

В силу теоремы о корректности исчисления предикатов (теорема 6.1), формула $\Phi_1 \supset (\ldots \supset (\Phi_n \supset \Phi)\ldots)$ общезначима. Докажем, что $\Gamma \models \Phi$. Пусть $\mathfrak{M}$ — модель множества Γ. Тогда все формулы $\Phi_1, \ldots, \Phi_n$ истинны в интерпретации $\mathfrak{M}$. Так как, кроме того, общезначимая формула $\Phi_1 \supset (\ldots \supset (\Phi_n \supset \Phi)\ldots)$ истинна в интерпретации $\mathfrak{M}$, то, очевидно, формула Φ также истинна в интерпретации $\mathfrak{M}$. Теорема 6.4 доказана.

Задачи

1) Доказать, что если $\Gamma \vdash \Phi$, а переменная v не входит свободно в формулы из Γ, то $\Gamma \vdash \forall v\Phi$.

2) Доказать, что если $\Gamma, \Phi \vdash \Psi$, а переменная v не входит свободно в формулы из Γ и в формулу Ψ, то $\Gamma, \exists v\Phi \vdash \Psi$.

3) Доказать, что следующие формулы выводимы в исчислении предикатов:

   а) $\forall x P(x) \,\&\, \forall x Q(x) \supset \forall x(P(x) \,\&\, Q(x))$;
   б) $\forall x(P(x) \,\&\, Q(x)) \supset \forall x P(x) \,\&\, \forall x Q(x)$;
   в) $\exists x P(x) \vee \exists x Q(x) \supset \exists x(P(x) \vee Q(x))$;
   г) $\exists x(P(x) \vee Q(x)) \supset \exists x P(x) \vee \exists x Q(x)$;
   д) $\exists x(P(x) \,\&\, Q(x)) \supset \exists x P(x) \,\&\, \exists x Q(x)$;
   е) $\forall x P(x) \vee \forall x Q(x)) \supset \forall x(P(x) \vee Q(x))$;
   ж) $\exists x(P(x) \supset Q(x)) \supset (\forall x P(x) \supset \exists x Q(x))$;
   з) $(\forall x P(x) \supset \exists x Q(x)) \supset \exists x(P(x) \supset Q(x))$;
   и) $\forall x(P(x) \supset Q(x)) \supset (\forall x P(x) \supset \forall x Q(x))$;
   к) $\forall x(P(x) \supset Q(x)) \supset (\exists x P(x) \supset \exists x Q(x))$.

4) Доказать, что каковы бы ни были формула $\Phi(x)$, формула Ψ, не содержащая свободно переменную x, и переменная y, не входящая в формулу $\Phi(x)$, следующие формулы выводимы в исчислении предикатов:
   $\neg\forall x\Phi(x) \supset \exists x\neg\Phi(x)$; $\exists x\neg\Phi(x) \supset \neg\forall x\Phi(x)$; $\neg\exists x\Phi(x) \supset \forall x\neg\Phi(x)$; $\forall x\neg\Phi(x) \supset \neg\exists x\Phi(x)$;
   $(\forall x\Phi(x) \,\&\, \Psi) \supset \forall x(\Phi(x) \,\&\, \Psi)$; $\forall x(\Phi(x) \,\&\, \Psi) \supset (\forall x\Phi(x) \,\&\, \Psi)$; $(\Psi \,\&\, \forall x\Phi(x)) \supset \forall x(\Psi \,\&\, \Phi(x))$;
   $\forall x(\Psi \,\&\, \Phi(x)) \supset (\Psi \,\&\, \forall x\Phi(x))$; $\exists x(\Phi(x) \,\&\, \Psi) \supset (\exists x\Phi(x) \,\&\, \Psi)$; $(\exists x\Phi(x) \,\&\, \Psi) \supset \exists x(\Phi(x) \,\&\, \Psi)$;
   $(\Psi \,\&\, \exists x\Phi(x)) \supset \exists x(\Psi \,\&\, \Phi(x))$; $\exists x(\Psi \,\&\, \Phi(x)) \supset (\Psi \,\&\, \exists x\Phi(x))$; $(\forall x\Phi(x) \vee \Psi) \supset \forall x(\Phi(x) \vee \Psi)$;
   $\forall x(\Phi(x) \vee \Psi) \supset (\forall x\Phi(x) \vee \Psi)$; $(\Psi \vee \forall x\Phi(x)) \supset \forall x(\Psi \vee \Phi(x))$; $\forall x(\Psi \vee \Phi(x)) \supset (\Psi \vee \forall x\Phi(x))$;
   $(\exists x\Phi(x) \vee \Psi) \supset \exists x(\Phi(x) \vee \Psi)$; $\exists x(\Phi(x) \vee \Psi) \supset (\exists x\Phi(x) \vee \Psi)$; $(\Psi \vee \exists x\Phi(x)) \supset \exists x(\Psi \vee \Phi(x))$;
   $\exists x(\Psi \vee \Phi(x)) \supset (\Psi \vee \exists x\Phi(x))$; $(\forall x\Phi(x) \supset \Psi) \supset \exists x(\Phi(x) \supset \Psi)$; $\exists x(\Phi(x) \supset \Psi) \supset (\forall x\Phi(x) \supset \Psi)$;
   $(\Psi \supset \forall x\Phi(x)) \supset \forall x(\Psi \supset \Phi(x))$; $\forall x(\Psi \supset \Phi(x)) \supset (\Psi \supset \forall x\Phi(x))$; $(\exists x\Phi(x) \supset \Psi) \supset \forall x(\Phi(x) \supset \Psi)$;
   $\forall x(\Phi(x) \supset \Psi) \supset (\exists x\Phi(x) \supset \Psi)$; $(\Psi \supset \exists x\Phi(x)) \supset \exists x(\Psi \supset \Phi(x))$; $\exists x(\Psi \supset \Phi(x)) \supset (\Psi \supset \exists x\Phi(x))$;
   $\forall x\Phi(x) \supset \forall y\Phi(y)$; $\exists x\Phi(x) \supset \exists y\Phi(y)$.

6.3. Расширения непротиворечивых теорий

Множество формул Γ называется *противоречивым*, если существует такая формула Φ, что $\Gamma \vdash \Phi$ и $\Gamma \vdash \neg\Phi$. В противном случае множество Γ называется *непротиворечивым*.

Предложение 6.1. *Множество Γ противоречиво тогда и только тогда, когда $\Gamma \vdash \Psi$, какова бы ни была формула Ψ.*

Доказательство. Докажем, что если множество Γ противоречиво, то $\Gamma \vdash \Psi$, какова бы ни была формула Ψ. В силу монотонности отношения выводимости, очевидно, что если множество Γ противоречиво, то противоречиво и множество $\Gamma \cup \{\neg\Psi\}$, какова бы ни была формула Ψ. Значит, существует такая формула Φ, что $\Gamma \cup \{\neg\Psi\} \vdash \Phi$ и $\Gamma \cup \{\neg\Psi\} \vdash \neg\Phi$. По теореме о дедукции (теорема 6.3) отсюда следует, что $\Gamma \vdash \neg\Psi \supset \Phi$ и $\Gamma \vdash \neg\Psi \supset \neg\Phi$. Построим вывод формулы Ψ из множества гипотез $\{\neg\Psi \supset \Phi, \neg\Psi \supset \neg\Phi\}$:

1. $\neg\Psi \supset \Phi$ (гипотеза);
2. $\neg\Psi \supset \neg\Phi$ (гипотеза);
3. $(\neg\Psi \supset \Phi) \supset ((\neg\Psi \supset \neg\Phi) \supset \neg\neg\Psi)$ (аксиома 9);
4. $(\neg\Psi \supset \neg\Phi) \supset \neg\neg\Psi$ (получено по правилу modus ponens из формул 1 и 3);
5. $\neg\neg\Psi$ (получено по правилу modus ponens из формул 2 и 4);
6. $\neg\neg\Psi \supset \Psi$ (аксиома 10);
7. Ψ (получено по правилу modus ponens из формул 5 и 6).

Таким образом, мы доказали, что $\{\neg\Psi \supset \Phi, \neg\Psi \supset \neg\Phi\} \vdash \Psi$. Отсюда и из транзитивности отношения выводимости следует, что $\Gamma \vdash \Psi$.

Тот факт, что если $\Gamma \vdash \Psi$ для любой формулы Ψ, то множество Γ противоречиво, очевиден. Действительно, в этом случае для произвольной формулы Φ имеет место $\Gamma \vdash \Phi$ и $\Gamma \vdash \neg\Phi$. □

Зафиксируем какую-нибудь замкнутую формулу Φ и через $\bot$ обозначим формулу $\Phi \& \neg\Phi$. Очевидно, что множество Γ противоречиво тогда и только тогда, когда $\Gamma \vdash \bot$. Действительно, если множество Γ противоречиво, то в силу предложения 6.1 имеет место $\Gamma \vdash \bot$. Обратно, если $\Gamma \vdash \bot$, т. е. $\Gamma \vdash \Phi \& \neg\Phi$, то с использованием аксиом 3 и 4 можно вывести из Γ формулы Φ и $\neg\Phi$. Таким образом, в дальнейшем вместо слов «множество Γ противоречиво» можно писать $\Gamma \vdash \bot$. Из свойств монотонности и компактности, которыми обладает отношение выводимости, вытекает, что множество непротиворечиво тогда и только тогда, когда всякое конечное его подмножество непротиворечиво. Наконец, отметим еще некоторые важные факты.

Предложение 6.2. *1) Каковы бы ни были множество формул Γ и формула Ψ, имеет место $\Gamma \cup \{\Psi\} \vdash \bot$ тогда и только тогда, когда $\Gamma \vdash \neg\Psi$.*

2) Каковы бы ни были множество формул Γ и формула Ψ, имеет место $\Gamma \cup \{\neg\Psi\} \vdash \bot$ тогда и только тогда, когда $\Gamma \vdash \Psi$.

Доказательство. 1) Пусть $\Gamma \cup \{\Psi\} \vdash \bot$. Тогда для любой формулы Φ имеет место $\Gamma \cup \{\Psi\} \vdash \Phi$ и $\Gamma \cup \{\Psi\} \vdash \neg\Phi$. По теореме о дедукции отсюда следует, что $\Gamma \vdash \Psi \supset \Phi$ и $\Gamma \vdash \Psi \supset \neg\Phi$. Средствами исчисления высказываний нетрудно построить вывод формулы $\neg\Psi$ из множества гипотез $\{\Psi \supset \Phi, \Psi \supset \neg\Phi\}$. Таким образом, $\{\Psi \supset \Phi, \Psi \supset \neg\Phi\} \vdash \neg\Psi$. Отсюда и из транзитивности отношения выводимости следует, что $\Gamma \vdash \neg\Psi$.

Обратно, если $\Gamma \vdash \neg\Psi$, то в силу монотонности отношения выводимости имеет место $\Gamma \cup \{\Psi\} \vdash \neg\Psi$. Так как, с другой стороны, $\Gamma \cup \{\Psi\} \vdash \Psi$, получаем, что в этом случае множество $\Gamma \cup \{\Psi\}$ противоречиво.

2) Пусть $\Gamma \cup \{\neg\Psi\} \vdash \bot$. Тогда в силу только что доказанного утверждения 1) имеет место $\Gamma \vdash \neg\neg\Psi$. Отсюда с использованием аксиомы 10 легко получается $\Gamma \vdash \Psi$. Обратное утверждение доказывается точно так же, как в случае утверждения 1). □

Наша ближайшая цель — доказать, что всякое непротиворечивое множество высказываний совместно, т. е. имеет модель.

Теорема 6.5. *Пусть $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ — непротиворечивые множества высказываний сигнатуры Ω, причем $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \ldots \subseteq \Gamma_n \subseteq \Gamma_{n+1} \subseteq \ldots$. Тогда множество $\Gamma = \bigcup\limits_{n=1}^{\infty} \Gamma_n$ непротиворечиво.*

Доказательство. Допустим, что множество Γ противоречиво. Тогда противоречиво некоторое конечное его подмножество $\Delta \subseteq \Gamma$. Очевидно, что $\Delta \subseteq \Gamma_n$ для некоторого n. Следовательно, множество Γ_n противоречиво, что невозможно по условию. Значит, на самом деле множество Γ непротиворечиво. □

Множество высказываний Γ сигнатуры Ω будем называть *максимальным*, если для любого высказывания Φ сигнатуры Ω имеет место либо $\Phi \in \Gamma$, либо $\neg\Phi \in \Gamma$.

Предложение 6.3. *Если* Γ *— максимальное непротиворечивое множество высказываний сигнатуры* Ω*, то, каково бы ни было высказывание* Φ *сигнатуры* Ω*, если* $\Gamma \vdash \Phi$*, то* $\Phi \in \Gamma$*.*

Доказательство. Допустим, что $\Gamma \vdash \Phi$, но $\Phi \notin \Gamma$. Тогда $\neg\Phi \in \Gamma$ в силу максимальности множества Γ, и $\Gamma \vdash \neg\Phi$, что невозможно в силу непротиворечивости множества Γ. □

Теорема 6.6. *Если* Γ *— максимальное непротиворечивое множество высказываний, то для любых высказываний* Φ *и* Ψ *имеет место*

1) $\neg\Phi \in \Gamma$ *тогда и только тогда, когда* $\Phi \notin \Gamma$*;*

2) $\Phi \,\&\, \Psi \in \Gamma$ *тогда и только тогда, когда* $\Phi \in \Gamma$ *и* $\Psi \in \Gamma$*;*

3) $\Phi \vee \Psi \in \Gamma$ *тогда и только тогда, когда* $\Phi \in \Gamma$ *или* $\Psi \in \Gamma$*;*

4) $\Phi \supset \Psi \in \Gamma$ *тогда и только тогда, когда* $\Phi \notin \Gamma$ *или* $\Psi \in \Gamma$*.*

Доказательство. 1) Если $\neg\Phi \in \Gamma$, то $\Phi \notin \Gamma$ в силу непротиворечивости множества Γ. Обратно, если $\Phi \notin \Gamma$, то $\neg\Phi \in \Gamma$ в силу максимальности множества Γ.

2) Если $\Phi \,\&\, \Psi \in \Gamma$, то $\Gamma \vdash \Phi$, $\Gamma \vdash \Psi$, и в силу предложения 6.3 имеем $\Phi \in \Gamma$ и $\Psi \in \Gamma$. Обратно, если $\Phi \in \Gamma$ и $\Psi \in \Gamma$, то $\Gamma \vdash \Phi \,\&\, \Psi$, и в силу предложения 6.3 имеем $\Phi \,\&\, \Psi \in \Gamma$.

3) Пусть $\Phi \vee \Psi \in \Gamma$, но $\Phi \notin \Gamma$ и $\Psi \notin \Gamma$. Тогда $\neg\Phi \in \Gamma$ и $\neg\Psi \in \Gamma$ в силу максимальности множества Γ. Формула $\neg\Phi \supset (\neg\Psi \supset \neg(\Phi \vee \Psi))$ является тавтологией. Следовательно, в силу теоремы 6.2, она выводима в исчислении предикатов. Теперь очевидно, что $\Gamma \vdash \neg(\Phi \vee \Psi)$. Но тогда Γ противоречиво. Значит, на самом деле, если $\Phi \vee \Psi \in \Gamma$, то $\Phi \in \Gamma$ или $\Psi \in \Gamma$. Обратно, если $\Phi \in \Gamma$ или $\Psi \in \Gamma$, то $\Gamma \vdash \Phi \vee \Psi$, и $\Phi \vee \Psi \in \Gamma$ в силу предложения 6.3.

4) Пусть $\Phi \supset \Psi \in \Gamma$, но $\Phi \in \Gamma$ и $\Psi \notin \Gamma$. Тогда, очевидно, $\Gamma \vdash \Psi$, а с другой стоороны, $\neg\Psi \in \Gamma$ в силу максимальности множества Γ, что невозможно, так как Γ непротиворечиво. Обратно, допустим, что $\Phi \notin \Gamma$ или $\Psi \in \Gamma$. Если $\Phi \notin \Gamma$, то $\neg\Phi \in \Gamma$, а так как формула $\neg\Phi \supset (\Phi \supset \Psi)$ является тавтологией и выводима в исчислении предикатов, то $\Gamma \vdash \Phi \supset \Psi$ и $\Phi \supset \Psi \in \Gamma$ в силу предложения 6.3. Если же $\Psi \in \Gamma$, то $\Gamma \vdash \Phi \supset \Psi$, так как формула $\Psi \supset (\Phi \supset \Psi)$ является аксиомой. □

Теорема 6.7. *Если множество высказываний* Γ *сигнатуры* Ω *непротиворечиво, то существует максимальное непротиворечивое множество высказываний* Γ' *сигнатуры* Ω *такое, что* $\Gamma \subseteq \Gamma'$*.*

Доказательство. Будем считать, что сигнатура Ω не более чем счетна. Тогда множество всех высказываний сигнатуры Ω счетно. Зафиксируем пересчет $\Phi_0, \Phi_1, \Phi_2, \ldots$ всех высказываний сигнатуры Ω. Определим последовательность непротиворечивых множеств высказываний $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ следующим образом. Положим $\Gamma_0 = \Gamma$. Пусть непротиворечивое множество высказываний Γ_n уже определено. Если $\Gamma_n \vdash \neg\Phi_n$, определяем Γ_{n+1} как $\Gamma_n \cup \{\neg\Phi_n\}$. Очевидно, что в этом случае множество Γ_{n+1} непротиворечиво, так как в противном случае $\Gamma_n \vdash \Phi$ в силу предложения 6.2, что невозможно, так как Γ_n непротиворечиво. Если же $\Gamma_n \nvdash \neg\Phi_n$, определяем Γ_{n+1} как $\Gamma_n \cup \{\Phi_n\}$. В этом случае множество Γ_{n+1} непротиворечиво в силу предложения 6.2. Таким образом, мы получили последовательность непротиворечивых множеств высказываний $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$, причем $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \ldots \subseteq \Gamma_n \subseteq \Gamma_{n+1} \subseteq \ldots$. По теореме 6.5 множество $\Gamma' = \bigcup\limits_{n=1}^{\infty} \Gamma_n$ непротиворечиво. Из построения множеств Γ_n видно, что множество Γ' является максимальным. □

Множество высказываний Γ сигнатуры Ω будем называть *насыщенным*, если всякий раз, когда формула вида $\exists v\Phi(v)$ выводима из Γ, имеет место также $\Gamma \vdash \Phi(c)$ для некоторой константы c из Ω.

Теорема 6.8. *Пусть* Γ *— непротиворечивое множество высказываний сигнатуры* Ω*, и пусть сигнатура* Ω' *получена добавлением к* Ω *счетного множества дополнительных констант. Тогда существует максимальное непротиворечивое насыщенное множество высказываний* Γ' *сигнатуры* Ω' *такое, что* $\Gamma \subseteq \Gamma'$*.*

Доказательство. Пусть сигнатура Ω' получена добавлением к Ω множества дополнительных констант $M = \{c_0, c_1, c_2, \ldots\}$. Множество высказываний вида $\exists v\Phi$ сигнатуры Ω' счетно. Зафиксируем некоторый пересчет таких формул

$$\exists v_0\Phi_0, \exists v_1\Phi_1, \exists v_2\Phi_2, \ldots. \tag{26}$$

Определим последовательность множеств высказываний $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$, причем Γ_n $(n = 0, 1, 2, \ldots)$ будет некоторым максимальным множеством высказываний в синатуре Ω_n, полученной добавлением к Ω лишь конечного числа констант из множества M. При этом в ходе построения последовательности $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ некоторые формулы из последовательности (26) будут вычеркиваться. Положим $\Omega_0 = \Omega$, Γ_0 — максимальное непротиворечивое расширение множества Γ в сигнатуре Ω_0, существующее в силу теоремы 6.7. Пусть максимальное непротиворечивое множество Γ_n в сигнатуре Ω_n построено. Пусть $\exists v\Phi(v)$ — первая еще не

вычеркнутая формула сигнатуры Ω_n из последовательности (26) такая, что $\Gamma_n \vdash \exists v\Phi(v)$. Пусть c — первая константа из множества M, не встречающаяся в формулах из Γ_n и в формуле $\Phi(v)$. Пусть Ω_{n+1} — сигнатура, полученная добавлением к Ω_n константы c. Докажем, что множество высказываний $\Gamma_n \cup \{\Phi(c)\}$ в сигнатуре Ω_{n+1} непротиворечиво. Допустим противное, т. е. что $\Gamma_n \cup \{\Phi(c)\} \vdash \bot$. Тогда, в силу теоремы о дедукции, существует вывод из Γ_n формулы $\Phi(c) \supset \bot$. Заменим всюду в этом выводе каждое вхождение константы c на переменную u, которая не встречается ни в одной из формул этого вывода. При такой замене сохраняется логическая структура формул, следовательно, каждая аксиома превратится в аксиому. Гипотезы, т. е. формулы из Γ_n, вообще не изменятся. Таким образом мы получим вывод из Γ_n формулы $\Phi(u) \supset \bot$. Применив к этой формуле правило (II), получим вывод из Γ_n формулы $\exists u\Phi(u) \supset \bot$. С помощью примера, рассмотренного в разделе 6.1, и теоремы о дедукции нетрудно показать, что формула $\exists u\Phi(u) \supset \bot$ выводима из формулы $\exists v\Phi(v) \supset \bot$. Поэтому $\Gamma_n \vdash \exists v\Phi(v) \supset \bot$, а так как $\Gamma_n \vdash \exists v\Phi(v)$, то $\Gamma_n \vdash \bot$, что невозможно в силу предположения о непротиворечивости множества Γ_n. В качестве Γ_{n+1} возьмем максимальное непротиворечивое расширение множества $\Gamma_n \cup \{\Phi(c)\}$ в сигнатуре Ω_{n+1}, существующее в силу теоремы 6.7. Последовательность $\Gamma_0, \Gamma_1, \Gamma_2, \ldots$ построена. Положим $\Omega' = \bigcup\limits_{n=1}^{\infty} \Omega_n$, $\Gamma' = \bigcup\limits_{n=1}^{\infty} \Gamma_n$. В силу теоремы 6.5, множество Γ' непротиворечиво. Докажем, что множество Γ' является максимальным в сигнатуре Ω'. Пусть Φ — произвольное высказывание сигнатуры Ω'. Формула Φ содержит лишь конечное число констант и потому является высказыванием некоторой сигнатуры Ω_n. Тогда при построении множества Γ_n в него должна была попасть одна из формул Φ и $\neg\Phi$. Следовательно, одна из этих формул попала в Γ'. Наконец, докажем, что множество Γ' является насыщенным. Пусть высказывание вида $\exists v\Phi(v)$ выводимо из Γ. Тогда $\Gamma_n \vdash \exists v\Phi(v)$ для некоторого n. Но это означает, что при построении множеств Γ_i $(i > n)$ рано или поздно была рассмотрена формула $\exists v\Phi(v)$, и для некоторой константы c формула $\Phi(c)$ была включена в Γ'. Следовательно, $\Gamma' \vdash \Phi(c)$. Очевидно также, что $\Gamma \subseteq \Gamma'$. □

6.4. Теорема Гёделя о полноте исчисления предикатов

Теорема 6.9. *Всякое непротиворечивое максимальное насыщенное множество высказываний имеет модель.*

Доказательство. Пусть Γ — непротиворечивое максимальное насыщенное множество высказываний сигнатуры Ω. Интерпретацию $\mathfrak{M}$ определим следующим образом. Ее носителем будет множество M всех термов сигнатуры Ω, не содержащих переменных. Для любой константы c сигнатуры Ω положим $c^* = c$. Для каждого (скажем, n-местного) функционального символа f сигнатуры Ω и для любых элементов (т. е. термов) $t_1, \ldots, t_n \in M$ положим $f^*(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$. Для каждого (скажем, n-местного) предикатного символа P сигнатуры Ω и для любых элементов (т. е. термов) $t_1, \ldots, t_n \in M$ положим $P^*(t_1, \ldots, t_n) = И$, если и только если формула $P(t_1, \ldots, t_n)$ принадлежит множеству Γ.

Докажем, что для любого высказывания Φ сигнатуры Ω имеет место

$$\mathfrak{M} \models \Phi \Leftrightarrow \Phi \in \Gamma. \tag{27}$$

Индукция по количеству логических символов в формуле Φ. Если в Φ нет логических символов, то Φ имеет вид $P(t_1, \ldots, t_n)$, и в этом случае (27) выполнено в силу задания интерпретации $\mathfrak{M}$.

Допустим, что утверждение (27) имеет место для любого высказывания Φ, содержащего не более n логических символов, и докажем это утверждение для любого высказывания Φ, в котором $n+1$ логических символов.

Пусть высказывание Φ имеет вид $\neg\Psi$ для некоторого высказывания Ψ. Тогда Ψ содержит n логических символов, и в силу индуктивного предположения имеет место

$$\mathfrak{M} \models \Psi \Leftrightarrow \Psi \in \Gamma. \tag{28}$$

Докажем (27). Пусть $\mathfrak{M} \models \Phi$. Тогда $\mathfrak{M} \not\models \Psi$, и в силу (28) $\Psi \notin \Gamma$. Тогда $\Phi \in \Gamma$ в силу максимальности множества Γ. Обратно, если $\Phi \in \Gamma$, то $\Psi \notin \Gamma$ в силу непротиворечивости множества Γ. Тогда, в силу (28), имеет место $\mathfrak{M} \not\models \Psi$, а значит, $\mathfrak{M} \models \Phi$.

Пусть высказывание Φ имеет вид $\Psi_1 \,\&\, \Psi_2$ для некоторых высказываний Ψ_1 и Ψ_2. Тогда каждое из высказываний Ψ_1, Ψ_2 содержит не более n логических символов, и в силу индуктивного предположения имеет место

$$\mathfrak{M} \models \Psi_i \Leftrightarrow \Psi_i \in \Gamma \ (i = 1, 2). \tag{29}$$

Докажем (27). Пусть $\mathfrak{M} \models \Phi$. Тогда $\mathfrak{M} \models \Psi_i$ $(i = 1, 2)$, и в силу (29) $\Psi_i \in \Gamma$ $(i = 1, 2)$. Тогда $\Phi \in \Gamma$ в силу утверждения 2) теоремы 6.6. Обратно, если $\Phi \in \Gamma$, то $\Psi_i \in \Gamma$ $(i = 1, 2)$ в силу утверждения 2) теоремы 6.6. Тогда, в силу (29), имеет место $\mathfrak{M} \models \Psi_i$ $(i = 1, 2)$, а значит, $\mathfrak{M} \models \Phi$.

Пусть высказывание Φ имеет вид $\Psi_1 \vee \Psi_2$ для некоторых высказываний Ψ_1 и Ψ_2. Тогда каждое из высказываний Ψ_1, Ψ_2 содержит не более n логических символов, и в силу индуктивного предположения имеет место (29). Докажем (27). Пусть $\mathfrak{M} \models \Phi$. Тогда $\mathfrak{M} \models \Psi_1$ или $\mathfrak{M} \models \Psi_2$, и в силу (29) $\Psi_1 \in \Gamma$ или $\Psi_2 \in \Gamma$. Тогда $\Phi \in \Gamma$ в силу утверждения 3) теоремы 6.6. Обратно, если $\Phi \in \Gamma$, то $\Psi_1 \in \Gamma$ или $\Psi_2 \in \Gamma$ в силу утверждения 3) теоремы 6.6. Тогда, в силу (29), имеет место $\mathfrak{M} \models \Psi_1$ или $\mathfrak{M} \models \Psi_2$, а значит, $\mathfrak{M} \models \Phi$.

Пусть высказывание Φ имеет вид $\Psi_1 \supset \Psi_2$ для некоторых высказываний Ψ_1 и Ψ_2. Тогда каждое из высказываний Ψ_1, Ψ_2 содержит не более n логических символов, и в силу индуктивного предположения имеет место (29). Докажем (27). Пусть $\mathfrak{M} \models \Phi$. Тогда $\mathfrak{M} \not\models \Psi_1$ или $\mathfrak{M} \models \Psi_2$, и в силу (29) $\Psi_1 \notin \Gamma$ или $\Psi_2 \in \Gamma$. Тогда $\Phi \in \Gamma$ в силу утверждения 4) теоремы 6.6. Обратно, если $\Phi \in \Gamma$, то $\Psi_1 \notin \Gamma$ или $\Psi_2 \in \Gamma$ в силу утверждения 4) теоремы 6.6. Тогда в силу (29) имеет место $\mathfrak{M} \not\models \Psi_1$ или $\mathfrak{M} \models \Psi_2$, а значит, $\mathfrak{M} \models \Phi$.

Пусть высказывание Φ имеет вид $\exists v \Psi(v)$ для некоторой формулы $\Psi(v)$, не содержащей свободных переменных, отличных от v. Тогда, каков бы ни был терм $t \in M$, высказывание $\Psi(t)$ содержит n логических символов, и в силу индуктивного предположения имеет место

$$\mathfrak{M} \models \Psi(t) \Leftrightarrow \Psi(t) \in \Gamma. \tag{30}$$

Докажем (27). Пусть $\mathfrak{M} \models \Phi$. Тогда для некоторого терма $t \in M$ имеет место $\mathfrak{M} \models \Psi(t)$, и в силу (30) $\Psi(t) \in \Gamma$. Тогда $\Gamma \vdash \exists v \Psi(v)$, и $\Phi \in \Gamma$ в силу предложения 6.3. Обратно, если $\Phi \in \Gamma$, то $\Psi(c) \in \Gamma$ для некоторой константы c в силу насыщенности множества Γ. Тогда, в силу (30), имеет место $\mathfrak{M} \models \Psi(c)$, а значит, $\mathfrak{M} \models \Phi$.

Пусть высказывание Φ имеет вид $\forall v \Psi(v)$ для некоторой формулы $\Psi(v)$, не содержащей свободных переменных, отличных от v. Тогда, каков бы ни был терм $t \in M$, высказывание $\Psi(t)$ содержит n логических символов, и в силу индуктивного предположения имеет место (30). Докажем (27). Пусть $\mathfrak{M} \models \Phi$. Тогда для любого терма $t \in M$ имеет место $\mathfrak{M} \models \Psi(t)$, и в силу (30)

$$\Psi(t) \in \Gamma \text{ для любого терма } t \in M. \tag{31}$$

Допустим, однако, что $\Phi \notin \Gamma$. Тогда $\neg\Phi \in \Gamma$ в силу максимальности множества Γ. Нетрудно доказать, что из формулы $\neg\forall v \Psi(v)$ выводима формула $\exists v \neg\Psi(v)$. В силу предложения 6.3, формула $\exists v \neg\Psi(v)$ принадлежит множеству Γ. Тогда $\neg\Psi(c) \in \Gamma$ для некоторой константы c в силу насыщенности множества Γ. Но это невозможно в силу (31) и непротиворечивости множества Γ. Значит, $\Phi \in \Gamma$. Обратно, если $\Phi \in \Gamma$, то для любого терма $t \in M$ имеет место $\Gamma \vdash \Psi(t)$ и $\Psi(t) \in \Gamma$. Тогда, в силу (30), имеет место $\mathfrak{M} \models \Psi(t)$ для любого терма $t \in M$, а значит, $\mathfrak{M} \models \Phi$.

Из доказанного следует, что $\mathfrak{M}$ является моделью множества Γ. □

Теорема 6.10. *Всякое непротиворечивое множество высказываний имеет модель.*

Доказательство. Пусть Γ — непротиворечивое множество высказываний сигнатуры Ω. В силу теоремы 6.8, существует такое максимальное непротиворечивое насыщенное множество высказываний Γ' сигнатуры Ω', полученной добавлением к Ω счетного множества дополнительных констант, что $\Gamma \subseteq \Gamma'$. По теореме 6.9, существует модель $\mathfrak{M}'$ множества Γ'. Это интерпретация сигнатуры Ω'. Рассмотрим интерпретацию $\mathfrak{M}$ сигнатуры Ω с тем же носителем, что и $\mathfrak{M}'$, в котором символы из Ω интерпретируются точно так же, как и в $\mathfrak{M}'$. Иными словами, $\mathfrak{M}$ — это по сути та же интерпретация $\mathfrak{M}'$, в которой нас не интересуют значения символов, не входящих в сигнатуру Ω. Довольно очевидно (хотя это можно доказать строго), что всякое высказывание сигнатуры Ω истинно в интерпретации $\mathfrak{M}$ тогда и только тогда, когда оно истинно в интерпретации $\mathfrak{M}'$. Так как все высказывания из множества Γ истинны в $\mathfrak{M}'$, то они истинны и в $\mathfrak{M}$. Значит, $\mathfrak{M}$ — модель множества Γ. □

Теорема 6.11 (теорема Лёвенгейма – Скулема). *Любое непротиворечивое множество высказываний в не более чем счетной сигнатуре имеет счетную модель.*

Доказательство. Пусть Γ — непротиворечивое множество высказываний в не более чем счетной сигнатуре Ω. В силу теоремы 6.8, существует максимальное непротиворечивое насыщенное его расширение Γ' в сигнатуре Ω', полученной добавлением к Ω счетного множества дополнительных констант. При доказательстве теоремы 6.9 была построена модель множества Γ', носителем которой является множество всех термов сигнатуры Ω', не содержащих переменных, которое, очевидно, счетно. Модель множества Γ, построенная при доказательстве теоремы 6.10, имеет тот же носитель, следовательно, эта модель счетна. □

Теорема 6.12 (теорема Гёделя о полноте). *Любая общезначимая формула выводима в исчислении предикатов.*

Доказательство. Пусть Φ — общезначимая формула. Если в ней есть свободные переменные $v_1, \ldots, v_n$, то замкнутая формула $\forall v_1 \ldots \forall v_n \Phi$, которую мы обозначим через Ψ, также общезначима. Докажем $\vdash \Psi$. Допустим противное, т. е. что $\nvdash \Psi$. Тогда, в силу утверждения 2) предложения 6.2, множество $\{\neg\Psi\}$ непротиворечиво. По теореме 6.10, оно имеет модель. В этой модели формула Ψ ложна, что противоречит ее общезначимости. Значит, $\vdash \forall v_1 \ldots \forall v_n \Phi$, а тогда, очевидно, и $\vdash \Phi$. □

Теорема 6.13. *В исчислении предикатов выводимы все общезначимые формулы и только они.*

Доказательство. Это утверждение вытекает из теоремы 6.12 и теоремы о корректности исчисления предикатов (теорема 6.1). □

Теорема 6.14 (обобщенная теорема Гёделя о полноте). *Пусть* Γ *— произвольное множество высказываний сигнатуры* Ω, Φ *— высказывание сигнатуры* Ω, *причем* $\Gamma \models \Phi$. *Тогда* $\Gamma \vdash \Phi$.

Доказательство. Пусть $\Gamma \models \Phi$. Допустим, что $\Gamma \nvdash \Phi$. Тогда, в силу предложения 6.2, множество $\Gamma \cup \{\neg\Phi\}$ непротиворечиво. По теореме 6.10, оно имеет модель $\mathfrak{M}$, так что $\mathfrak{M} \models \Gamma$ и $\mathfrak{M} \models \neg\Phi$. С другой стороны, если $\mathfrak{M} \models \Gamma$, то $\mathfrak{M} \models \Phi$, ибо $\Gamma \models \Phi$. Полученное противоречие показывает, что на самом деле $\Gamma \vdash \Phi$. □

Теорема 6.15. *Высказывание* Φ *логически следует из множества высказываний* Γ *тогда и только тогда, когда* Φ *выводится из* Γ.

Доказательство. Это утверждение вытекает из теоремы 6.14 и обощенной теоремы о корректности исчисления предикатов (теорема 6.4). □

Теорема 6.16 (локальная теорема Мальцева). *Если любое конечное подмножество множества высказываний* Γ *имеет модель, то* Γ *имеет модель.*

Доказательство. Пусть любое конечное подмножество множества высказываний Γ имеет модель. Покажем, что Γ имеет модель. В силу теоремы 6.10, для этого достаточно показать, что множество Γ непротиворечиво. Но это действительно так, ибо если бы Γ было противоречиво, то в силу свойства компактности отношения выводимости было бы противоречиво некоторое конечное его подмножество, которое в таком случае не имело бы модели вопреки условию теоремы. □

Теорема 6.17 (теорема Мальцева о компактности). *Пусть* Γ *— произвольное множество высказываний сигнатуры* Ω, Φ *— произвольное высказывание сигнатуры* Ω, *причем* $\Gamma \models \Phi$. *Тогда существует конечное множество* $\Delta \subseteq \Gamma$ *такое, что* $\Delta \models \Phi$.

Доказательство. Пусть $\Gamma \models \Phi$. Тогда $\Gamma \vdash \Phi$ по теореме 6.14. В силу свойства компактности отношения выводимости существует конечное множество $\Delta \subseteq \Gamma$ такое, что $\Delta \vdash \Phi$. Согласно обобщенной теореме о корректности исчисления предикатов, в этом случае имеет место $\Delta \models \Phi$. □

6.5. Теории первого порядка с равенством

При формализации математических теорий очень часто используется предикат равенства $=$. Однако, если в языке первого порядка имеется предикатный символ $=$, мы вовсе не обязаны интерпретировать его именно как равенство. Алгебраическую систему $\mathfrak{M}$ сигнатуры $\Omega \cup \{=\}$ будем называть *нормальной* алгебраической системой, если в $\mathfrak{M}$ предикатный символ $=$ интерпретируется именно как предикат равенства.

Через $Eq(\Omega)$ обозначим следующее множество высказываний сигнатуры $\Omega \cup \{=\}$:

Eq1. $\forall x(x = x)$;

Eq2. $\forall x \forall y(x = y \supset y = x)$;

Eq3. $\forall x \forall y \forall z(x = y \,\&\, y = z \supset x = z)$;

Eq(f). $\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n (x_1 = y_1 \,\&\, x_n = y_n \supset f(x_1, \ldots, x_n) = f(y_1, \ldots, x_y))$ для каждого (n-местного) функционального символа f сигнатуры Ω;

Eq(P). $\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n (x_1 = y_1 \,\&\, x_n = y_n \supset P(x_1, \ldots, x_n) \supset P(y_1, \ldots, x_y))$ для каждого (n-местного) предикатного символа P сигнатуры Ω.

Теорема 6.18. *Множество высказываний* Γ *сигнатуры* $\Omega \cup \{=\}$ *имеет нормальную модель тогда и только тогда, когда множество* $\Gamma \cup Eq(\Omega)$ *имеет модель.*

Доказательство. Допустим, что множество высказываний Γ в сигнатуре $\Omega \cup \{=\}$ имеет нормальную модель $\mathfrak{M}$. Очевидно, что все высказывания из $Eq(\Omega)$ истинны в любой нормальной интерпретации, в частности, в $\mathfrak{M}$. Следовательно, $\mathfrak{M}$ является моделью множества $\Gamma \cup Eq(\Omega)$.

Обратно, допустим, что $\mathfrak{M}$ — некоторая модель множества высказываний $\Gamma \cup Eq(\Omega)$, и множество M — носитель этой модели. Пусть E есть $=^*$, т. е. двуместный предикат на M, интерпретирующий предикатный символ $=$. Определим на множестве M бинарное отношение $\approx$ следующим условием: если $a, b \in M$, то $a \approx b$ тогда и только тогда, когда $E(a, b) = И$. Так как в $\mathfrak{M}$ истинны высказывания Eq1 – Eq3, то $\approx$ — отношение эквивалентности на M. Более того, так как для каждого функционального символа f в $\mathfrak{M}$ истинно высказывание $\mathrm{Eq}(f)$, то функция f^*, интерпретирующая в $\mathfrak{M}$ функциональный символ f, согласована с этим отношением эквивалентности в том смысле, что если $a_1 \approx b_1, \ldots, a_n \approx b_n$, то $f^*(a_1, \ldots, a_n) \approx f^*(b_1, \ldots, b_n)$. Наконец, так как для каждого предикатного символа P в $\mathfrak{M}$ истинно высказывание $\mathrm{Eq}(P)$, то предикат P^*, интерпретирующий в $\mathfrak{M}$ предикатный символ P, согласован с отношением эквивалентности $\approx$ в том смысле, что если $a_1 \approx b_1, \ldots, a_n \approx b_n$, то $P^*(a_1, \ldots, a_n) = P^*(b_1, \ldots, b_n)$. Пусть $M/\approx$ — множество всех классов эквивалентности по отношению $\approx$. Определим интерпретацию $\mathfrak{M}/\approx$ следующим образом. Носителем ее будет множество $M/\approx$. Значением константы c в интерпретации $\mathfrak{M}/\approx$ будет класс эквивалентности $[c^*]$, которому принадлежит элемент c^*, интерпретирующий константу c в $\mathfrak{M}$. Значением функционального символа f в интерпретации $\mathfrak{M}/\approx$ будет функция, которая каждому набору классов эквивалентности $[a_1], \ldots, [a_n]$ сопоставляет класс эквивалентности элемента $f^*(a_1, \ldots, a_n)$. В силу упомянутой выше согласованности функции f^* с отношением эквивалентности $\approx$, такое задание функции корректно в том смысле, что ее значение на наборе классов эквивалентности не зависит от выбора представителей этих классов. Значением предикатного символа P сигнатуры $\Omega \cup \{=\}$ в интерпретации $\mathfrak{M}/\approx$ будет предикат, который на любом наборе классов эквивалентности $[a_1], \ldots, [a_n]$ принимает такое же значение, как и предикат P^* на наборе $a_1, \ldots, a_n$. В силу упомянутой выше согласованности предиката P^* с отношением эквивалентности $\approx$, такое задание предиката корректно в том смысле, что его значение на наборе классов эквивалентности не зависит от выбора представителей этих классов. Очевидно, что при этом предикатный символ $=$ интерпретируется в системе $\mathfrak{M}/\approx$ именно как равенство, т. е. $\mathfrak{M}/\approx$ — нормальная интерпретация.

Пусть g — произвольная оценка в интерпретации $\mathfrak{M}$, т. е. функция, сопоставляющая каждой переменной некоторый элемент множества M. Через g' обозначим оценку в интерпретации $\mathfrak{M}/\approx$, которая каждой переменной v сопоставляет класс эквивалентности $[g(v)]$. Несложной индукцией по построению терма t сигнатуры Ω можно доказать, что значение $g'(t)$ терма t при оценке g' есть класс эквивалентности $[g(t)]$ значения терма t при оценке g. С помощью этого утверждения, индукцией по построению формулы Φ сигнатуры Ω можно доказать, что истинностное значение формулы Φ при оценке g' в интерпретации $\mathfrak{M}/\approx$ совпадает с истинностным значением формулы Φ при оценке g в интерпретации $\mathfrak{M}$. В частности, для любого высказывания Φ его истиностные значения в интерпретациях $\mathfrak{M}$ и $\mathfrak{M}/\approx$ совпадают. Так как все высказывания из Γ истинны в $\mathfrak{M}$, то все они истинны и в $\mathfrak{M}/\approx$, т. е. $\mathfrak{M}/\approx$ — нормальная модель множества высказываний Γ. □

Исчислением предикатов с равенством в сигнатуре Ω называется исчисление, полученное добавлением к обычному исчислению предикатов в сигнатуре Ω множества аксиом $Eq(\Omega)$.

Теорема 6.19. *Если множество высказываний Γ сигнатуры $\Omega \cup \{=\}$ непротиворечиво в исчислении предикатов с равенством, то Γ имеет нормальную модель.*

Доказательство. Так как в исчислении предикатов с равенством из множества высказываний Γ не выводится противоречие, то множество высказываний $\Gamma \cup Eq(\Omega)$ непротиворечиво в обычном смысле. В силу теоремы 6.10, множество $\Gamma \cup Eq(\Omega)$ имеет модель, а тогда, по теореме 6.18, множество Γ имеет нормальную модель. □

Теорема 6.20. *Всякое непротиворечивое в исчислении предикатов с равенством множество высказываний Γ в не более чем счетной сигнатуре $\Omega \cup \{=\}$ имеет не более чем счетную нормальную модель.*

Доказательство. Так как в исчислении предикатов с равенством из множества высказываний Γ не выводится противоречие, то множество высказываний $\Gamma \cup Eq(\Omega)$ непротиворечиво в обычном смысле. В силу теоремы Лёвенгейма – Сулема (теорема 6.11), множество $\Gamma \cup Eq(\Omega)$ имеет счетную модель $\mathfrak{M}$. Как показано при доказательстве теоремы 6.18, Γ имеет нормальную модель вида $\mathfrak{M}/\approx$, которая, очевидно, не более чем счетна. □

Теорема 6.21. *Всякое высказывание сигнатуры $\Omega \cup \{=\}$, истинное в любой нормальной интерпретации, выводимо в исчислении предикатов с равенством в сигнатуре $\Omega \cup \{=\}$.*

Доказательство. Пусть высказывание Γ сигнатуры $\Omega \cup \{=\}$ истинно в любой нормальной интерпретации. Допустим, что Φ не выводится в исчислении предикатов с равенством. Тогда множество $\{\neg\Phi\}$ непротиворечиво в исчислении предикатов с равенством. В силу теоремы 6.19, множество $\{\neg\Phi\}$ имеет нормальную модель, что невозможно, ибо в любой нормальной интерпретации истинно высказывание Φ. □

Теорема 6.22. *Пусть Γ — произвольное множество высказываний сигнатуры $\Omega \cup \{=\}$, причем любое конечное его подмножество имеет нормальную модель. Тогда Γ имеет нормальную модель.*

Доказательство. Пусть любое конечное подмножество множества высказываний Γ сигнатуры $\Omega \cup \{=\}$ имеет нормальную модель. Тогда, очевидно, любое конечное подмножество множества $\Gamma \cup Eq(\Omega)$ имеет модель. В силу локальной теоремы Мальцева (теорема 6.16), множество $\Gamma \cup Eq(\Omega)$ имеет модель, а в силу теоремы 6.18 в этом случае Γ имеет нормальную модель, что и требовалось доказать. □

Теорема 6.23. *Если множество высказываний Γ сигнатуры $\Omega \cup \{=\}$ для любого натурального n имеет нормальную модель мощности, большей n, то Γ имеет бесконечную модель.*

Доказательство. Для каждого натурального $n \geq 1$ определим формулу E_n следующим образом. В качестве E_1 возьмем формулу $\exists x(x = x)$. При $n \geq 2$ формула E_n выглядит так:

$$\exists x_1 \ldots \exists x_n \left(\mathop{\&}_{1 \leq i < j \leq n} \neg(x_i = x_j) \right).$$

Очевидно, что формула E_n истинна во всякой нормальной интерпретации, содержащей не менее n элементов. Пусть $\Delta = \Gamma \cup \{E_1, E_2, \ldots\}$. Всякое конечное подмножество множества Δ имеет нормальную модель. Действительно, любое конечное подмножество множества Δ содержит лишь конечное число высказываний вида E_n и потому является подмножеством множества $\Gamma \cup \{E_1, \ldots, E_m\}$ для некоторого m. По условию, Γ имеет конечную нормальную модель мощности $> m$. Очевидно, что в этой модели истинны все высказывания $E_1, \ldots, E_m$, так что она является моделью множества $\Gamma \cup \{E_1, \ldots, E_m\}$. В силу теоремы 6.22, множество Δ имеет нормальную модель, которая, очевидно, может быть только бесконечной. Она же будет и бесконечной моделью множества Γ. □

Теорема 6.24. *Не существует высказывания сигнатуры $\Omega \cup \{=\}$, которое было бы истинным во всех конечных нормальных интерпретациях и ложным во всех бесконечных интерпретациях.*

Доказательство. Допустим, что высказывание Φ истинно во всех конечных нормальных интерпретациях. Тогда, очевидно, для любого натурального n множество $\{\Phi\}$ имеет нормальную бесконечную модель мощности, большей n, и в силу теоремы 6.23 имеет бесконечную модель. Значит, Φ не может быть ложным во всех бесконечных интерпретациях. □

6.6. Аксиоматизируемые классы алгебраических систем

Класс K алгебраических систем сигнатуры Ω называется *(конечно) аксиоматизируемым*, если существует (конечное) множество высказываний Γ сигнатуры Ω такое, что K есть в точности класс всех моделей множества Γ (в этом случае Γ называется *аксиоматикой* класса K).

Теорема 6.25. *Пусть K_1 и K_2 — (конечно) аксиоматизируемые классы алгебраических систем сигнатуры Ω. Тогда их пересечение $K_1 \cap K_2$ также является (конечно) аксиоматизируемым классом.*

Доказательство. Пусть K_1 и K_2 — аксиоматизируемые классы алгебраических систем сигнатуры Ω, и пусть Γ_1 — аксиоматика класса K_1, а Γ_2 — аксиоматика класса K_1. Это означает, в частности, что

$$(\forall \Phi \in \Gamma_1)(\forall \mathfrak{M} \in K_1)\mathfrak{M} \models \Phi; \tag{32}$$

$$(\forall \Phi \in \Gamma_2)(\forall \mathfrak{M} \in K_2)\mathfrak{M} \models \Phi. \tag{33}$$

Докажем, что множество высказываний $\Gamma_1 \cup \Gamma_2$ является аксиоматикой класса $K_1 \cap K_2$.

Требуется доказать, что алгебраическая система $\mathfrak{M}$ сигнатуры Ω принадлежит классу $K_1 \cap K_2$ тогда и только тогда, когда $\mathfrak{M}$ является моделью для $\Gamma_1 \cup \Gamma_2$. Итак, пусть $\mathfrak{M}$ принадлежит классу $K_1 \cap K_2$. Это означает, что

$$\mathfrak{M} \in K_1; \tag{34}$$

$$\mathfrak{M} \in K_2. \tag{35}$$

Пусть Φ — произвольное высказывание из множества $\Gamma_1 \cup \Gamma_2$. Тогда $\Phi \in \Gamma_1$ или $\Phi \in \Gamma_2$. Докажем, что $\mathfrak{M} \models \Phi$. Пусть $\Phi \in \Gamma_1$. Тогда из (34) и (32) немедленно вытекает $\mathfrak{M} \models \Phi$. Аналогично, если $\Phi \in \Gamma_2$, то из (35) и (33) также вытекает $\mathfrak{M} \models \Phi$. Таким образом, мы доказали, что всякая алгебраическая система из класса $K_1 \cap K_2$ является моделью множества высказываний $\Gamma_1 \cup \Gamma_2$.

Докажем теперь, что всякая модель множества высказываний $\Gamma_1 \cup \Gamma_2$ принадлежит классу $K_1 \cap K_2$. Итак, пусть $\mathfrak{M}$ является моделью для $\Gamma_1 \cup \Gamma_2$. Это означает, что в $\mathfrak{M}$ истинно любое высказывание из $\Gamma_1 \cup \Gamma_2$. В частности, если Φ — произвольное высказывание из множества Γ_1, то $\mathfrak{M} \models \Phi$, т. е. $\mathfrak{M}$ является моделью множества Γ_1, а тогда имеет место (34), так как Γ_1 — аксиоматика класса K_1. Аналогично, если Φ — произвольное высказывание из множества Γ_2, то $\mathfrak{M} \models \Phi$, т. е. $\mathfrak{M}$ является моделью множества Γ_2, а тогда имеет место (35), так как Γ_2 — аксиоматика класса K_2. Из (34) и (35) получаем $\mathfrak{M} \in K_1 \cap K_2$, что и требовалось.

Таким образом, мы доказали, что любая алгебраическая система сигнатуры Ω является моделью множества высказываний $\Gamma_1 \cup \Gamma_2$ тогда и только тогда, когда она принадлежит классу $K_1 \cap K_2$. Это как раз и означает, что $\Gamma_1 \cup \Gamma_2$ является аксиоматикой класса $K_1 \cap K_2$. Заметим, что если множества Γ_1 и Γ_2 оба конечны, то их объединение $\Gamma_1 \cup \Gamma_2$ также конечно. Тем самым мы доказали, что пересечение любых двух конечно аксиоматизируемых классов является конечно аксиоматизируемым классом. □

Теорема 6.26. *Пусть K_1 и K_2 — (конечно) аксиоматизируемые классы алгебраических систем сигнатуры Ω. Тогда их объединение $K_1 \cup K_2$ также является (конечно) аксиоматизируемым классом.*

Доказательство. Пусть K_1 и K_2 — аксиоматизируемые классы алгебраических систем сигнатуры Ω, и пусть Γ_1 — аксиоматика класса K_1, а Γ_2 — аксиоматика класса K_1. Это означает, в частности, что выполняются условия (32) и (33). Докажем, что множество высказываний $\Gamma = \{\Phi_1 \vee \Phi_2 | \Phi_1 \in \Gamma_1, \Phi_2 \in \Gamma_2\}$ является аксиоматикой класса $K_1 \cup K_2$.

Требуется доказать, что алгебраическая система $\mathfrak{M}$ сигнатуры Ω принадлежит классу $K_1 \cup K_2$ тогда и только тогда, когда $\mathfrak{M}$ является моделью для Γ. Итак, пусть $\mathfrak{M}$ принадлежит классу $K_1 \cup K_2$. Это означает, что выполняется хотя бы одно из условий (34) и (35). Пусть Φ — произвольное высказывание из множества Γ. Тогда Φ имеет вид $\Phi_1 \vee \Phi_2$, где $\Phi_1 \in \Gamma_1$, $\Phi_2 \in \Gamma_2$. Докажем, что $\mathfrak{M} \models \Phi$. Пусть выполнено условие (34). Тогда из (32) немедленно вытекает $\mathfrak{M} \models \Phi_1$, а значит, $\mathfrak{M} \models \Phi$. Аналогично, если выполнено условие (35), то из (33) вытекает $\mathfrak{M} \models \Phi_2$ и $\mathfrak{M} \models \Phi$. Таким образом, мы доказали, что всякая алгебраическая система из класса $K_1 \cup K_2$ является моделью множества высказываний Γ.

Докажем теперь, что всякая модель множества высказываний Γ принадлежит классу $K_1 \cup K_2$. Итак, пусть $\mathfrak{M}$ является моделью для Γ. Это означает, что в $\mathfrak{M}$ истинно любое высказывание из Γ. Допустим, однако, что $\mathfrak{M}$ не принадлежит классу $K_1 \cup K_2$. Тогда $\mathfrak{M} \notin K_1$, $\mathfrak{M} \notin K_2$. Так как Γ_1 и Γ_2 — аксиоматики классов K_1 и K_2 соответственно, найдутся высказывания $\Phi_1 \in \Gamma_1$ и $\Phi_2 \in \Gamma_2$ такие, что $\mathfrak{M} \not\models \Phi_1$ и $\mathfrak{M} \not\models \Phi_2$. Но тогда $\mathfrak{M} \not\models \Phi_1 \vee \Phi_2$, что невозможно, ибо высказывание $\Phi_1 \vee \Phi_2$ принадлежит множеству Γ, а $\mathfrak{M}$ является моделью для Γ.

Таким образом, мы доказали, что любая алгебраическая система сигнатуры Ω является моделью множества высказываний Γ тогда и только тогда, когда она принадлежит классу $K_1 \cup K_2$. Это как раз и означает, что Γ является аксиоматикой класса $K_1 \cup K_2$. Заметим, что если множества Γ_1 и Γ_2 оба конечны, то множество Γ также конечно. Тем самым мы доказали, что объединение любых двух конечно аксиоматизируемых классов является конечно аксиоматизируемым классом. □

Теорема 6.27. *Класс K алгебраических систем сигнатуры Ω является конечно аксиоматизируемым тогда и только тогда, когда и класс K, и его дополнение $\bar{K}$ в классе всех алгебраических систем сигнатуры Ω аксиоматизируемы.*

Доказательство. Пусть класс K алгебраических систем сигнатуры Ω конечно аксиоматизируем, и пусть $\{\Phi_1, \ldots, \Phi_n\}$ — его конечная аксиоматика. Пусть Φ есть формула $\Phi_1 \& \ldots \& \Phi_n$. Тогда, очевидно, какова бы ни была алгебраическая система $\mathfrak{M}$ сигнатуры Ω, выполняется условие $\mathfrak{M} \in K \Leftrightarrow \mathfrak{M} \models \Phi$, откуда вытекает $\mathfrak{M} \notin K \Leftrightarrow \mathfrak{M} \not\models \Phi$, т. е. $\mathfrak{M} \in \bar{K} \Leftrightarrow \mathfrak{M} \models \neg\Phi$. Это означает, что множество, состоящее из одного высказывания $\neg\Phi$, является аксиоматикой класса $\bar{K}$. Таким образом, мы доказали, что если класс K конечно аксиоматизируем, то и он, и его дополнение $\bar{K}$ аксиоматизируемы.

Докажем теперь, что если класс K и его дополнение $\bar{K}$ оба аксиоматизируемы, то K конечно аксиоматизируем. Итак, пусть классы K и $\bar{K}$ аксиоматизируемы, и пусть Γ — аксиоматика для K, а Γ' — аксиоматика для $\bar{K}$. Как видно из доказательства теоремы 6.25, множество высказываний $\Gamma \cup \Gamma'$ является аксиоматикой пустого класса $K \cap \bar{K}$, следовательно, множество $\Gamma \cup \Gamma'$ не имеет моделей. В силу локальной теоремы Мальцева (теорема 6.16), существует конечное подмножество $\Delta^\circ \subseteq \Gamma \cup \Gamma'$, которое не имеет моделей. Оба множества $\Delta = \Delta^\circ \cap \Gamma$ и $\Delta' = \Delta^\circ \cap \Gamma'$ конечны. Докажем, что множество Δ является аксиоматикой класса K.

Пусть $\mathfrak{M}$ — модель множества Δ. Докажем, что $\mathfrak{M} \in K$. Допустим противное. Тогда $\mathfrak{M} \in \bar{K}$, и в $\mathfrak{M}$ истинны все высказывания из Δ'. Значит, в $\mathfrak{M}$ истинны все высказывания из $\Delta^\circ = \Delta \cup \Delta'$, что противоречит предположению о невыполнимости множества Δ°. Таким образом, мы доказали, что всякая модель множества высказываний Δ принадлежит классу K. Обратное утверждение, что всякая алгебраическая система $\mathfrak{M}$ из класса K является моделью множества Δ, очевидно, так как $\Delta \subseteq \Gamma$, а Γ является аксиоматикой класса K, так что в любой алгебраической системе из K, в частности, в $\mathfrak{M}$, истинны все высказывания из Γ, в частности, все высказывания из Δ. □

Класс K нормальных алгебраических систем сигнатуры с равенством $\Omega \cup \{=\}$ называется (конечно) аксиоматизируемым, если существует (конечное) множество высказываний Γ сигнатуры $\Omega \cup \{=\}$ такое, что K есть в точности класс всех нормальных моделей множества Γ (в этом случае Γ называется аксиоматикой класса K). Примерами аксиоматизируемых классов являются класса всех групп, класс всех абелевых групп, класс всех колец, класс всех колец без делителей нуля, класс всех полей, класс всех полей фиксированной характеристики $p > 0$.

Теорема 6.28. *Пусть K — аксиоматизируемый класс алгебраических систем сигнатуры $\Omega \cup \{=\}$, содержащий конечные нормальные алгебраические системы со сколь угодно большим числом элементов. Тогда K содержит бесконечную нормальную алгебраическую систему.*

Доказательство. Пусть K — аксиоматизируемый класс алгебраических систем сигнатуры $\Omega \cup \{=\}$, и Γ — его аксиоматика. Пусть K содержит конечные нормальные алгебраические системы со сколь угодно большим числом элементов. По условию, для любого натурального n в классе K имеется конечная нормальная алгебраическая система, содержащая белее n элементов, которая, таким образом, является нормальной моделью множества высказываний Γ. В силу теоремы 6.23, множество Γ имеет бесконечную нормальную модель, которая принадлежит классу K, так как Γ — аксиоматика класса K.

Задачи

1) Доказать, что множество всех алгебраических систем сигнатуры Ω является конечно аксиоматизируемым.

2) Доказать, что если класс нормальных алгебраических систем K сигнатуры с равенством $\Omega \cup \{=\}$ аксиоматизируем, то класс всех бесконечных нормальных систем из K также аксиоматизируем.

3) Выписать аксиоматики следующих классов алгебраических систем:

   а) класс всех групп;

   б) класс всех абелевых групп;

   в) класс всех колец;

   г) класс всех колец без делителей нуля;

   д) класс всех полей;

   е) класс всех полей фиксированной характеристики $p > 0$;

   ж) класс всех полей характеристики 0.

4) Доказать, что не являются аксиоматизируемыми:

   а) класс всех конечных групп;

   б) класс всех конечных абелевых групп.

5) Доказать, что не являются конечно аксиоматизируемыми:

   а) класс всех бесконечных групп;

   б) класс всех бесконечных абелевых групп;

   в) класс всех полей характеристики 0.

6) Доказать, что класс всех полей ненулевой характеристики не является аксиоматизируемым.

7) Доказать, что объединение и пересечение аксиоматизируемых классов нормальных алгебраических систем сигнатуры с равенством $\Omega \cup \{=\}$ являются аксиоматизируемыми.

8) Доказать, что класс K нормальных алгебраических систем сигнатуры с равенством $\Omega \cup \{=\}$ является конечно аксиоматизируемым тогда и только тогда, когда и класс K, и его дополнение $\bar{K}$ в классе всех нормальных алгебраических систем сигнатуры $\Omega \cup \{=\}$ являются аксиоматизируемыми.

7. Метод резолюций

7.1. Представление высказываний в скулемовской форме

Пусть фиксирован некоторый язык первого порядка сигнатуры Ω. Через V будем обозначать множество переменных, через T — множество всех термов сигнатуры Ω. Формулы вида $P(t_1, \ldots, t_n)$, где P — предикатный символ, $t_1, \ldots, t_n \in T$, называются *атомами*. Если A — атом, то формулы A и $\neg A$ называются *литерами*.

Пусть фиксирована некоторая интерпретация $\mathfrak{M}$ сигнатуры Ω, причем множество M — носитель (предметная область) этой интерпретации. *Оценкой* называется произвольная функция $v : V \to M$. Для каждой интерпретации и каждой оценки определено значение любого терма в этой интерпретации при этой оценке, а также истинностное значение любой формулы в данной интерпретации при данной оценке.

Будем говорить, что формула Φ находится *в стандартной форме*, если каждая ее подформула вида $\Psi_1 \lambda \Psi_2$, где $\lambda \in \{\&, \vee, \supset\}$, обладает таким свойством: если какая-либо переменная x связана в Ψ_1 (Ψ_2), то x не входит в Ψ_2 (соответственно, в Ψ_1). Например, формула $\forall x P(x) \,\&\, Q(y)$ находится в стандартной форме, а формула $\forall x P(x) \,\&\, \forall x Q(x)$ — нет. Очевидно, что путем переименования связанных переменных каждую формулу можно привести к стандартной форме, т. е. построить равносильную ей формулу в стандартной форме. Так, формула $\forall x P(x) \,\&\, \forall x Q(x)$ равносильна формуле $\forall x P(x) \,\&\, \forall y Q(y)$, которая, очевидно, находится в стандартной форме.

Говорят, что формулы Φ и Ψ *равновыполнимы*, и пишут $\Phi \sim_{sat} \Psi$, если Φ выполнима тогда и только тогда, когда Ψ выполнима. Заметим, что если $\Phi \sim \Psi$, то $\Phi \sim_{sat} \Psi$. Очевидно, что существуют только два класса эквивалентности относительно $\sim_{sat}$: класс выполнимых и класс невыполнимых формул. Например, формулы $\forall x P(x, a)$ и $\forall x P(a, x)$ обе выполнимы, следовательно, они равновыполнимы (но не равносильны). Формула $\exists x P(x, a) \,\&\, \neg P(b, a)$ выполнима, а формула $P(b, a) \,\&\, \neg P(b, a)$ невыполнима, следовательно, эти формулы не равновыполнимы.

Нашей целью является представление замкнутых формул первого порядка в некотором специальном виде, удобном для применения автоматических методов доказательства теорем. Первый шаг в преобразовании формулы Φ состоит в замене ее на равносильную формулу $\alpha(\Phi)$, не содержащую символа $\supset$, в которой символ $\neg$ стоит только перед атомами (такая формула строится из литер с помощью логических символов $\&, \vee, \forall, \exists$). Для получения формулы $\alpha(\Phi)$ используются следующие равносильности:

- $\Phi_1 \supset \Phi_2 \sim \neg\Phi_1 \vee \Phi_2$;
- $\neg(\Phi_1 \,\&\, \Phi_2) \sim \neg\Phi_1 \vee \neg\Phi_2$;
- $\neg(\Phi_1 \vee \Phi_2) \sim \neg\Phi_1 \,\&\, \neg\Phi_2$;
- $\neg\neg\Phi \sim \Phi$;
- $\neg\forall x \Phi \sim \exists x \neg\Phi$;
- $\neg\exists x \Phi \sim \forall x \neg\Phi$.

Пример. Если Φ есть формула $\neg\forall x \exists y (P(x, y) \,\&\, Q(y) \supset R(y))$, то формула $\alpha(\Phi)$ строится следующим образом:

$$\neg\forall x \exists y (P(x, y) \,\&\, Q(y) \supset R(y)) \sim \exists x \neg\exists y (P(x, y) \,\&\, Q(y) \supset R(y)) \sim \exists x \forall y \neg (P(x, y) \,\&\, Q(y) \supset R(y)) \sim$$

$$\sim \exists x \forall y \neg(\neg(P(x, y) \,\&\, Q(y)) \vee R(y)) \sim \exists x \forall y (\neg\neg(P(x, y) \,\&\, Q(y)) \,\&\, \neg R(y)) \sim \exists x \forall y (P(x, y) \,\&\, Q(y) \,\&\, \neg R(y)).$$

Формулу будем называть *α-нормальной*, если к ней преобразование α уже неприменимо, т. е. она не содержит символа $\supset$, а символ $\neg$ стоит только перед атомами

Следующий шаг в преобразовании формулы Φ состоит в замене ее на равновыполнимую формулу $\beta(\Phi)$, не содержащую символа $\exists$. Будем считать, что формула Φ уже находится в стандартной форме, и является α-нормальной. Строим формулу Φ^* следующим образом. Если в Φ нет кванторов существования $\exists$, то Φ^* есть Φ. В противном случае находим первое слева вхождение квантора вида $\exists x$. Пусть это вхождение не находится в области действия никакого квантора всеобщности. Через $\Phi_{\exists x}$ обозначим формулу, полученную вычеркиванием из Φ этого вхождения квантора $\exists x$. Тогда Φ^* есть формула $\Phi_{\exists x}[a/x]$, полученная заменой в формуле $\Phi_{\exists x}$ всех свободных вхождений переменной x на новую константу a. Таким образом, в этом случае Φ^* — это формула в более широкой сигнатуре. Если первое слева вхождение квантора существования $\exists$

находится в области действия кванторов всеобщности $\forall y_1, \ldots, \forall y_n$, перечисляемых в порядке их появления в формуле слева направо, то Φ^* есть формула $\Phi_{\exists x}[f(y_1, \ldots, y_n)/x]$, полученная вычеркиванием из Φ квантора $\exists x$ и заменой в полученной формуле всех свободных вхождений переменной x на терм $f(y_1, \ldots, y_n)$, где f — новый функциональный символ. Таким образом, и в этом случае Φ^* — формула в более широкой сигнатуре. Через $\beta(\Phi)$ обозначим результат последовательного применения к формуле Φ операции * до полного устранения кванторов существования.

Пример. Если Φ есть формула

$$(\forall x \exists y P(x, y) \vee \forall u \exists v \neg Q(u, v)) \,\&\, \exists z \neg P(z, z),$$

то Φ^* — это формула

$$(\forall x P(x, f(x)) \vee \forall u \exists v \neg Q(u, v)) \,\&\, \exists z \neg P(z, z);$$

Φ^{**} — это формула

$$(\forall x P(x, f(x)) \vee \forall u \neg Q(u, g(u))) \,\&\, \exists z \neg P(z, z);$$

наконец, Φ^{***} (она же $\beta(\Phi)$) есть формула

$$(\forall x P(x, f(x)) \vee \forall u \neg Q(u, g(u))) \,\&\, \neg P(a, a).$$

Построение формулы $\beta(\Phi)$ обычно называют *скулемизацией* в честь норвежского логика Скулема, соавтора теоремы Лёвенгейма – Скулема, а саму формулу $\beta(\Phi)$ называют *скулемовской формой* формулы Φ.

Докажем, что если формула Φ замкнута, то $\Phi \sim_{sat} \beta(\Phi)$. Для этого достаточно показать, что для любой замкнутой α-нормальной формулы Φ имеет место $\Phi \sim_{sat} \Phi^*$.

Лемма 7.1. *Пусть Φ есть α-нормальная формула, находящаяся в стандартной форме, и пусть Φ содержит вхождение квантора κx, которое не находится в области действия никакого другого квантора. Через $\Phi_{\kappa x}$ обозначим формулу, полученную зачеркиванием в Φ этого вхождения квантора κx. Тогда $\Phi \sim \kappa x \Phi_{\kappa x}$.*

Доказательство. Лемма по существу утверждает, что из α-нормальной формулы, находящейся в стандартной форме, любой квантор, который не находится в области действия никакого другого квантора, можно «выносить наружу», получая при этом равносильную формулу. Доказывается лемма индукцией по количеству связок $\&$ и $\vee$ в формуле Φ. Если таких связок нет, то, поскольку формула Φ является α-нормальной, она имеет вид $\kappa_1 x_1 \ldots \kappa_n x_n \Psi$, где Ψ — литера. Тогда вхождение квантора κx, о котором идет речь в лемме, есть $\kappa_1 x_1$. В этом случае $\kappa x \Phi_{\kappa x}$ совпадает с Φ, и доказываемое утверждение очевидно.

Допустим теперь, что утверждение леммы верно для любой формулы, в которой не более k связок $\&$ и $\vee$, и рассмотрим формулу Φ, в которой $k+1$ связок $\&$ и $\vee$. Если Φ имеет вид $\kappa x \Psi$, то, как и рассмотренном выше случае, $\kappa x \Phi_{\kappa x}$ совпадает с Φ, и доказываемое утверждение очевидно. Рассмотрим случай, когда Φ имеет вид $\Psi_1 \lambda \Psi_2$, где $\lambda \in \{\&, \vee\}$. Допустим, что квантор κx, о котором идет речь в лемме, входит в формулу Ψ_1. Очевидно, что в Ψ_1 не более k связок $\&$ и $\vee$, так что в силу индуктивного предположения имеем $\Psi_1 \sim \kappa x \Psi_{1\kappa x}$. Тогда $\Phi \sim \kappa x \Psi_{1\kappa x} \lambda \Psi_2$. Так как Φ находится в стандартной форме, то переменная x не входит свободно в Ψ_2, и имеет место равносильность $\kappa x \Psi_{1\kappa x} \lambda \Psi_2 \sim \kappa x (\Psi_{1\kappa x} \lambda \Psi_2)$. С другой стороны, очевидно, что $\Psi_{1\kappa x} \lambda \Psi_2$ как раз и есть $\Phi_{\kappa x}$, так что утверждение доказано. Случай, когда квантор κx, о котором идет речь в лемме, входит в формулу Ψ_2, рассматривается совершенно аналогично. $\square$

Лемма 7.2. *Пусть Φ — замкнутая α-нормальная формула, находящаяся в стандартной форме. Тогда $\Phi \sim_{sat} \Phi^*$.*

Доказательство. Если в Φ нет кванторов существования $\exists$, то Φ^* есть Φ, и доказываемое утверждение очевидно. Если первое слева вхождение квантора вида $\exists x$ не находится в области действия никакого квантора всеобщности, то это вхождение не находится в области действия никакого квантора, и по лемме 7.1 имеем $\Phi \sim \exists x \Phi_{\exists x}$. С другой стороны, в этом случае Φ^* есть формула $\Phi_{\exists x}[a/x]$, полученная заменой в формуле $\Phi_{\exists x}$ всех свободных вхождений переменной x на новую константу a. Таким образом, достаточно доказать, что $\exists x \Phi_{\exists x} \sim_{sat} \Phi_{\exists x}[a/x]$. Обозначим формулу $\Phi_{\exists x}$ через Ψ и докажем, что $\exists x \Psi \sim_{sat} \Psi[a/x]$. Пусть формула $\Psi[a/x]$ выполнима, т. е. истинна в некоторой интерпретации. Тогда, очевидно, в той же интерпретации истинна и формула $\exists x \Psi$, т. е. эта формула также выполнима. Обратно, пусть формула $\exists x \Psi$ выполнима. Тогда существует интерпретация, в которой эта формула истинна. Истинность формулы $\exists x \Psi$

означает, что существует такая оценка f, при которой в этой интерпретации истинна формула Ψ. Придадим константе a значение $f(x)$. Тогда в полученной интерпретации будет истинна формула $\Psi[a/x]$, значит, она также выполнима.

Пусть первое слева вхождение квантора существования $\exists x$ находится в области действия кванторов всеобщности $\forall y_1, \ldots, \forall y_n$, перечисляемых в порядке их появления в формуле слева направо. Тогда квантор $\forall y_1$ не находится в области действия никакого другого квантора, и по лемме 7.1 имеет место $\Phi \sim \forall y_1 \Phi_{\forall y_1}$. Применяя теперь лемму 7.1 к формуле $\Phi_{\forall y_1}$, получаем, что $\Phi \sim \forall y_1 \forall y_2 \Phi_{\forall y_1 \forall y_2}$. Продолжая эти рассуждения дальше, получаем, что $\Phi \sim \forall y_1 \forall y_2 \ldots \forall y_n \Phi_{\forall y_1 \forall y_2 \ldots \forall y_n}$. Тогда в формуле $\Phi_{\forall y_1 \forall y_2 \ldots \forall y_n}$ квантор $\exists x$ не находится в области действия никакого другого квантора, и по лемме 7.1 имеет место $\Phi_{\forall y_1 \forall y_2 \ldots \forall y_n} \sim \exists x \Psi$, где Ψ есть формула $\Phi_{\forall y_1 \forall y_2 \ldots \forall y_n \exists x}$. Тогда $\Phi \sim \forall y_1 \forall y_2 \ldots \forall y_n \exists x \Psi$. С другой стороны, в этом случае Φ^* есть формула $\Phi_{\exists x}[f(y_1, \ldots, y_n)/x]$, полученная вычеркиванием из Φ квантора $\exists x$ и заменой в полученной формуле всех свободных вхождений переменной x на терм $f(y_1, \ldots, y_n)$, где f — новый функциональный символ. Очевидно, что в формуле $\Phi_{\exists x}[f(y_1, \ldots, y_n)/x]$ можно «вынести наружу» кванторы $\forall y_1 \forall y_2 \ldots \forall y_n$ подобно тому, как мы это сделали выше с формулой Φ. В результате получится формула $\forall y_1 \forall y_2 \ldots \forall y_n \Psi[f(y_1, \ldots, y_n)/x]$, равносильная формуле $\Phi_{\exists x}[f(y_1, \ldots, y_n)/x]$. Таким образом, теперь достаточно доказать, что

$$\forall y_1 \forall y_2 \ldots \forall y_n \exists x \Psi \sim_{sat} \forall y_1 \forall y_2 \ldots \forall y_n \Psi[f(y_1, \ldots, y_n)/x].$$

Пусть формула $\forall y_1 \forall y_2 \ldots \forall y_n \Psi[f(y_1, \ldots, y_n)/x]$ выполнима, т. е. истинна в некоторой интерпретации. Тогда, очевидно, в той же интерпретации истинна и формула $\forall y_1 \forall y_2 \ldots \forall y_n \exists x \Psi$, т. е. эта формула также выполнима. Обратно, пусть формула $\forall y_1 \forall y_2 \ldots \forall y_n \exists x \Psi$ выполнима. Тогда существует интерпретация, в которой эта формула истинна. Истинность формулы $\forall y_1 \forall y_2 \ldots \forall y_n \exists x \Psi$ означает, что существует такая функция f^*, которая каждому набору $a_1, \ldots, a_n$ сопоставляет такой элемент b, что в этой интерпретации истинна формула Ψ при оценке, которая сопоставляет переменным $y_1, \ldots, y_n$ значения $a_1, \ldots, a_n$, а переменной x — значение b. Придадим функциональному символу f в качестве значения указанную функцию f^*. Тогда в полученной интерпретации будет истинна формула $\forall y_1 \forall y_2 \ldots \forall y_n \Psi[f(y_1, \ldots, y_n)/x]$, значит, она также выполнима. □

Из леммы 7.2 немедленно следует, что замкнутая формула Φ и ее скулемовская форма $\beta(\Phi)$ равновыполнимы.

Задачи

Привести к скулемовской форме следующие формулы:
1) $\neg(\forall x P(x) \supset \exists y \forall z Q(y, z))$;
2) $\forall x(\neg P(x, a) \supset \exists y(P(y, g(x)) \,\&\, \forall z(P(z, g(x)) \supset P(y, z))))$;
3) $\neg(\forall x P(x) \supset \exists y P(y))$.

7.2. Представление высказывания в виде множества дизъюнктов

В скулемовской форме $\beta(\Phi)$ высказывания Φ используются только квантор $\forall$, логические связки $\&$, $\vee$ и связка $\neg$, которая встречается только перед атомами. Так как $\beta(\Phi)$ есть α-нормальная формула, находящаяся в стандартной форме, то в силу леммы 7.1 она равносильна предваренной формуле, полученной чисто механическим «вынесением наружу» всех кванторов, так что $\beta(\Phi)$ равносильна формуле вида $\forall y_1 \ldots \forall y_n \Psi$, где Ψ — бескванторная формула, построенная из литер с помощью связок $\&$ и $\vee$. Будем считать, что скулемовская форма любого высказывания имеет именно такой вид. В логике высказываний формулы, подобные Ψ, называют формулами с тесными отрицаниями. Пользуясь законом дистрибутивности

$$\Phi_0 \vee \Phi_1 \,\&\, \Phi_2 \sim (\Phi_0 \vee \Phi_1) \,\&\, (\Phi_0 \vee \Phi_2),$$

формулу Ψ можно привести к конъюнктивной нормальной форме вида $D_1 \,\&\, \ldots \,\&\, D_m$, где каждая из формул D_i $(i = 1, \ldots, m)$ есть дизъюнкт, т. е. имеет вид $L_1 \vee \ldots L_k$, где $L_1, \ldots, L_k$ — атомы. Эту формулу легко восстановить по ее бескванторной части $(L_1^1 \vee \ldots L_{k_1}^1) \,\&\, \ldots \,\&\, (L_1^m \vee \ldots L_{k_m}^m)$, которую мы обозначим $\gamma(\Phi)$ и, в свою очередь, представляем ее в виде множества дизъюнктов $D(\Phi) = \{L_1^1 \vee \ldots \vee L_{k_1}^1, \ldots, L_1^m \vee \ldots \vee L_{k_m}^m\}$. Таким образом, представление высказывания Φ в виде множества дизъюнктов получается следующим алгоритмом:

1) высказывание Φ приводим к стандартному виду и строим формулу $\alpha(\Phi)$, которая равносильна формуле Φ, не содержит символа $\supset$, а символ $\neg$ стоит в ней только перед атомами;

2) по высказыванию $\alpha(\Phi)$ строим скулемовскую форму формулы Φ — формулу $\beta(\Phi)$, которая равносильна формуле вида $\forall y_1 \ldots \forall y_n \Psi$, где Ψ — бескванторная формула, построенная из литер с помощью связок $\&$ и $\vee$, при этом формулы $\beta(\Phi)$ и Φ равновыполнимы;

3) в формуле $\beta(\Phi)$ отбрасываем кванторы, бесквантерную часть Ψ приводим к конъюнктивной нормальной форме и получаем формулу $\gamma(\Phi)$ вида $D_1 \,\&\, \ldots \,\&\, D_m$, где $D_1, \ldots, D_m$ — дизъюнкты; тогда искомое множество есть $D(\Phi) = \{D_1, \ldots, D_m\}$.

Пример. Пусть Φ есть формула $\neg(\forall x \exists y P(x,y) \,\&\, \forall u \forall v(\neg P(u,v) \supset R(u)) \supset \forall z R(z))$. Тогда $\alpha(\Phi)$ есть формула

$$\forall x \exists y P(x,y) \,\&\, \forall u \forall v(\neg P(u,v) \vee R(u)) \,\&\, \exists z \neg R(z),$$

а $\beta(\Phi)$ есть формула

$$\forall x P(x, f(x)) \,\&\, \forall u \forall v(\neg P(u,v) \vee R(u)) \,\&\, \neg R(a).$$

Наконец, $\gamma(\Phi)$ есть формула

$$P(x, f(x)) \,\&\, (\neg P(u,v) \vee R(u)) \,\&\, \neg R(a),$$

и

$$D(\Phi) = \{P(x, f(x)), \neg P(u,v) \vee R(u), \neg R(a)\}.$$

Введем в язык константу $\bot$, которая будет считаться атомом, обозначающим «ложь». Этот атом можно использовать в дизъюнктах, причем очевидны следующие равносильности: $A \vee \bot \vee B \sim A \vee B$, $\bot \vee \bot \sim \bot$.

Литера вида A, где A — атом, называется *положительной*, а литера вида $\neg A$, где A — атом, называется *отрицательной*. Литеры A и $\neg A$ называются *контрарными*.

7.3. Эрбрановский универсум

Допустим, что нас интересует вопрос о выполнимости высказывания Φ. Очевидно, что в этом случае достаточно решить аналогичный вопрос для скулемовской формы высказывания Φ, ибо высказывания Φ и $\beta(\Phi)$ равновыполнимы. Оказывается, что для высказываний, находящихся в скулемовской форме, возможные модели можно искать среди довольно ограниченного класса возможных интерпретаций — так называемых эрбрановских интерпретаций, к описанию которых мы переходим.

Пусть имеется некоторое множество дизъюнктов $\mathcal{C}$. Через $CS(\mathcal{C})$ обозначим множество всех констант, встречающихся в дизъюнктах из $\mathcal{C}$, через $FS_n(\mathcal{C})$ — множество всех n-местных функциональных символов, встречающихся в дизъюнктах из $\mathcal{C}$. Индукцией по n определим множество термов без переменных H_n следующим образом. Пусть $H_0 = CS(\mathcal{C})$, если это множество не пусто. Если же в дизъюнктах из $\mathcal{C}$ нет ни одной константы, пусть $H_0 = \{a\}$, где a — произвольная константа. Допустим, что для некоторого $i \geq 1$ определено множество термов H_{i-1}. Тогда пусть

$$H_i = H_{i-1} \cup \{f(t_1, \ldots, t_n) | f \in FS_n(\mathcal{C}); t_1, \ldots, t_n \in H_{i-1}; n \in \mathbf{N}\}.$$

Положим $H(\mathcal{C}) = \bigcup\limits_{i=0}^{\infty} H_i$. Множество $H(\mathcal{C})$ называется *эрбрановским универсумом* для множества дизъюнктов $\mathcal{C}$.

Пример. Пусть $\mathcal{C} = \{\neg P(x) \vee P(f(x)),\ P(h(x,x)),\ \neg P(h(u,v)) \vee Q(v)\}$. Тогда

$$H_0 = \{a\},\ H_1 = \{a,\ f(a),\ h(a,a)\},$$

$$H_2 = \{a,\ f(a),\ h(a,a)\, f(f(a)),\ f(h(a,a)), h(f(a), f(a)),\ h(f(a), h(a,a)),\ h(h(a,a), f(a)),\ h(h(a,a), h(a,a))\}.$$

Пусть $\mathcal{C}$ — произвольное множество дизъюнктов, $PS_n(\mathcal{C})$ — множество всех n-местных предикатных символов, встречающихся в дизъюнктах из $\mathcal{C}$. Множество

$$AS(\mathcal{C}) = \{P(t_1, \ldots, t_n) | P \in PS_n(\mathcal{C});\ t_1, \ldots, t_n \in H(\mathcal{C});\ n \in \mathbf{N}\}$$

называется *множеством атомов* для $\mathcal{C}$. Множество

$$LS(\mathcal{C}) = AS(\mathcal{C}) \cup \{\neg A | A \in AS(\mathcal{C})\}$$

называется *множеством литер* для $\mathcal{C}$.

Пусть $\mathcal{C}$ — произвольное множество дизъюнктов, D — дизъюнкт из $\mathcal{C}$. *Основным примером* дизъюнкта D называется любой дизъюнкт, полученный подстановкой в D элементов эрбрановского универсума $H(\mathcal{C})$ вместо переменных.

Пример. Пусть $\mathcal{C} = \{P(x) \vee P(f(x)),\ \neg P(a),\ \neg P(f(a))\}$. Тогда $P(a) \vee P(f(a))$ и $P(f(a)) \vee P(f(f(a)))$ суть основные примеры дизъюнкта $P(x) \vee P(f(x))$ из $\mathcal{C}$.

Эрбрановская интерпретация для множества дизъюнктов $\mathcal{C}$ определяется следующим образом. Ее носителем является множество $H(\mathcal{C})$. Если $a \in CS(\mathcal{C})$, то $a^* = a$. Если $f \in FS_n(\mathcal{C})$, то f^* есть функция, которая каждому набору $h_1, \ldots, h_n$ элементов из $H(\mathcal{C})$ сопоставляет терм $f(h_1, \ldots, h_n)$ из $H(\mathcal{C})$. Таким образом, эрбрановская интерпретация —это не то же самое, что интерпретация, носителем которой является эрбрановский универсум. Важно, что константы и функциональные символы интерпретируются определенным выше стандартным образом. Различные эрбрановские интерпретации отличаются друг от друга интерпретацией предикатных символов.

Пример. Пусть $\mathcal{C} = \{P(x) \vee P(f(x)),\ P(a),\ \neg P(f(z)) \vee Q(u),\ \neg Q(g(y, y))\}$. Тогда

$$H(\mathcal{C}) = \{a,\ f(a),\ g(a, a),\ f(f(a)), \ldots\}.$$

В случае эрбрановской интерпретации значения сигнатурных символов таковы, что $a^* = a$, $f^*(h) = f(h)$ для любого $h \in H(\mathcal{C})$, $g^*(h_1, h_2) = g(h_1, h_2)$ для любых $h_1, h_2 \in H(\mathcal{C})$. Каждый из предикатных символов P и Q может интерпретироваться самыми различными способами. Положим, например, $P^*(h) = 1$ для любого h из $H(\mathcal{C})$, $Q^*(h_1, h_2) = 0$ для любых $h_1, h_2 \in H(\mathcal{C})$. В этой интерпретации первый дизъюнкт (представляющий формулу $\forall x(P(x) \vee P(f(x)))$) имеет значение 1 а, скажем, третий дизъюнкт (представляющий формулу $\forall z \forall u(\neg P(f(z)) \vee Q(u))$) имеет значение 0.

7.4. Существование эрбрановской модели для выполнимого множества дизъюнктов

Эрбрановская интерпетация для множества дизъюнктов $\mathcal{C}$ характеризуется интерпретацией предикатных символов, а именно, множеством атомов для $\mathcal{C}$, истинных в этой интерпретации. Важность рассмотрения эрбрановских интерпретаций обусловлена следующей теоремой.

Теорема 7.1. *Множество дизъюнктов выполнимо тогда и только тогда, когда оно имеет эрбрановскую модель.*

Доказательство. Нам нужно доказать, что множество дизъюнктов $\mathcal{C}$ выполнимо, если и только если существует эрбрановская интерпретация для $\mathcal{C}$, в которой все дизъюнкты из $\mathcal{C}$ истинны, т. е. истинна формула, представленная множеством дизъюнктов $\mathcal{C}$. Очевидно, что если существует эрбрановская модель для $\mathcal{C}$, то $\mathcal{C}$ выполнимо. Докажем обратное утверждение. Допустим, что множество дизъюнктов $\mathcal{C}$ выполнимо, и пусть $\mathfrak{M}$ — его модель с носителем M. Для произвольных $c \in CS(\mathcal{C})$, $f \in FS(\mathcal{C})$, $P \in PS(\mathcal{C})$ посредством c^*, f^*, P^* будем обозначать их интерпретации в $\mathfrak{M}$. Определим отображение $\omega : H(\mathcal{C}) \to M$ следующим образом. Если $c \in CS(\mathcal{C})$, то $\omega(c) = c^*$. Если $CS(\mathcal{C}) = \emptyset$ и $H_0 = \{a\}$, то пусть $\omega(a)$ — произвольный (но фиксированный) элемент из M. Если для термов $t_1, \ldots, t_n \in H(\mathcal{C})$ определены значения $\omega(t_1), \ldots, \omega(t_n)$, и $f \in FS_n(\mathcal{C})$, то $\omega(f(t_1, \ldots, t_n)) = f^*(\omega(t_1), \ldots, \omega(t_n))$. Нетрудно заметить, что если $CS(\mathcal{C}) \neq \emptyset$, то для любого терма $t \in H(\mathcal{C})$ элемент $\omega(t)$ есть t^* — значение терма t в интерпретации $\mathfrak{M}$. Теперь построим эрбрановскую интерпретацию, которую мы обозначим $H(\mathfrak{M})$, в определенном смысле согласованную с моделью $\mathfrak{M}$. Для задания эрбрановской интерпретации достаточно указать значения предикатных символов. Для $P \in PS_n(\mathcal{C})$ предикат $\overline{P}$, интерпретирующий предикатный символ P в $H(\mathfrak{M})$, определим так: $\overline{P}(t_1, \ldots, t_n) = P^*(\omega(t_1), \ldots, \omega(t_n))$ для любых термов $t_1, \ldots, t_n \in H(\mathcal{C})$. Докажем, что так построенная интерпретация $H(\mathfrak{M})$ является моделью множества дизъюнктов $\mathcal{C}$. Пусть $\mathcal{C} = \{D_1, \ldots, D_m\}$. Тогда $\mathcal{C}$ представляет формулу $\forall y_1 \ldots \forall y_p (D_1 \,\&\, \ldots \,\&\, D_m)$, где $y_1, \ldots, y_p$ — все переменные, входящие в дизъюнкты $D_1, \ldots, D_m$. Допустим, что эта формула ложна в интерпретации $H(\mathfrak{M})$. Покажем, что в таком случае она ложна и в интерпретации $\mathfrak{M}$. Отсюда будет следовать доказываемое утверждение, так как $\mathfrak{M}$ — модель для $\mathcal{C}$.

Итак, пусть формула, представленная множеством дизъюнктов $\mathcal{C}$, ложна в интерпретации $H(\mathfrak{M})$. Тогда существует оценка $v : V \to H(\mathcal{C})$, при которой некоторый дизъюнкт D_i принимает значение 0 в интерпрретации $H(\mathfrak{M})$. Пусть этот дизъюнкт имеет вид $L_1 \vee \ldots \vee L_k$, где $L_1, \ldots, L_k$ — литеры. Пусть $L \in \{L_1, \ldots, L_k\}$. Тогда литера L также принимает значение 0 в интерпрретации $H(\mathfrak{M})$ при оценке v. Литера L имеет вид $P(t_1, \ldots, t_n)$ или $\neg P(t_1, \ldots, t_n)$ для некоторого предикатного символа $P \in PS(\mathcal{C})$ и некоторых термов $t_1, \ldots, t_n$. Для доказательства утверждения достаточно показать, что существует такая оценка переменных $v' : V \to M$, что истинностное значение любого атома при оценке v' в интерпретации $\mathfrak{M}$ совпадает с истинностным значением этого атома при оценке v в интерпретации $H(\mathfrak{M})$. Действительно, так как при оценке v литера L принимает значение 0 в интерпретации $H(\mathfrak{M})$, то при оценке v' эта литера примет значение 0 в интерпретации $\mathfrak{M}$. Поскольку это верно для любой литеры $L \in \{L_1, \ldots, L_k\}$, то при оценке v' дизъюнкт D_i примет значение 0 в интерпретации $\mathfrak{M}$. Значит, формула, представленная множеством дизъюнктов $\mathcal{C}$, ложна в интерпрретации $\mathfrak{M}$.

Оценку v' определим так: $v'(x) = \omega(v(x))$ для любой переменной x. Используя определение отображения ω, нетрудно доказать, что имеет место равенство $v'(t) = \omega(v(t))$ для любого терма t. Значениями термов $t_1, \ldots, t_n$ при оценке v будут некоторые термы $h_1, \ldots, h_n \in H(\mathcal{C})$. Тогда значениями этих термов при оценке v' будут элементы $\omega(h_1), \ldots, \omega(h_n) \in M$. Значением атома $P(t_1, \ldots, t_n)$ при оценке v' в интерпретации $\mathfrak{M}$ будет $P^*(\omega(h_1), \ldots, \omega(h_n))$, а значением этого атома при оценке v в интерпретации $H(\mathfrak{M})$ будет $\overline{P}(h_1, \ldots, h_n)$. По определению интерпретации $H(\mathfrak{M})$, эти значения совпадают. Значит, v' — искомая оценка. □

Теорема 7.1 показывает, что для доказательства невыполнимости множества дизъюнктов $\mathcal{C}$ достаточно убедиться, что это множество дизъюнктов не имеет эрбрановской модели. Поскольку в эрбрановских интерпретациях для $\mathcal{C}$ все константы и функциональные символы имеют фиксированный смысл, все внимание должно уделяться интерпретации предикатных символов, которую можно рассматривать как приписывание истинностных значений атомам из $AS(\mathcal{C})$. А именно, выполнимость множества дизъюнктов $\mathcal{C}$ означает, что существует такое приписывание истинностных значений атомам из $AS(\mathcal{C})$, при котором все основные примеры дизъюнктов из $\mathcal{C}$ истинны.

Пример. Пусть $\mathcal{C} = \{P(x, f(a)), \neg P(u, v) \vee Q(f(v)), \neg Q(z)\}$. Среди основных примеров дизъюнктов из $\mathcal{C}$ есть такие: $P(a, f(a)), \neg P(a, f(a)) \vee Q(f(f(a))), \neg Q(f(f(a)))$. Очевидно, что они не могут быть истинны одновременно, значит, множество $\mathcal{C}$ невыполнимо.

Задачи

1) Определить, существует ли эрбрановская модель для множества дизъюнктов

   а) $\{P(x), \neg Q(f(y))\}$;

   б) $\{P(x), \neg P(f(y))\}$.

2) Доказать, что множество дизъюнктов $\{P(x), \neg P(y) \vee Q(y, a), \neg Q(z, a)\}$ невыполнимо.

7.5. Теорема Эрбрана

Теорема 7.2 (теорема Эрбрана). *Множество дизъюнктов $\mathcal{C}$ невыполнимо тогда и только тогда, когда существует конечное невыполнимое множество основных примеров дизъюнктов из $\mathcal{C}$.*

Доказательство. Допустим, что существует конечное невыполнимое множество $\mathcal{C}' = \{D'_1, \ldots, D'_k\}$ основных примеров дизъюнктов из $\mathcal{C}$. Очевидно, что формула $D'_1 \,\&\, \ldots \,\&\, D'_k$ получается подстановкой термов из $H(\mathcal{C})$ в формулу вида $D_1 \,\&\, \ldots \,\&\, D_k$, где $D_1, \ldots, D_k$ — некоторые дизъюнкты из $\mathcal{C}$. Так как формула $D'_1 \,\&\, \ldots \,\&\, D'_k$ невыполнима, то не существует такой эрбрановской интерпретации, в которой все основные примеры всех дизъюнктов из $\mathcal{C}$ были бы истинны. Это означает, что множество $\mathcal{C}$ невыполнимо.

Обратно, пусть множество дизъюнктов $\mathcal{C}$ невыполнимо. Тогда, в силу теоремы 7.1, не существует эрбрановской модели для $\mathcal{C}$, а это означает, что невыполнимо множество всех основных примеров дизъюнктов из $\mathcal{C}$. В силу локальной теоремы (теорема 6.16), существует конечное невыполнимое подмножество этого множества, что и требовалось доказать. □

Задачи

1) Найти невыполнимое множество основных примеров дизъюнктов из $\mathcal{C}$, если

   а) $\mathcal{C} = \{P(x, a, g(x, b)), \neg P(f(y), z, g(f(a), b))\}$;

   б) $\mathcal{C} = \{P(x), Q(y, f(y)) \vee \neg P(y), \neg Q(g(u), v)\}$.

2) Доказать с помощью теоремы Эрбрана, что следующие формулы общезначимы:

   а) $\forall x \exists y P(x, y) \supset \exists y \forall x P(x, y)$;

   б) $\neg \exists x P(x) \supset \neg \forall x P(x)$;

   в) $(\forall x (P(x) \supset \neg Q(x)) \supset \neg (\exists x P(x) \,\&\, \forall x Q(x))$;

   г) $(\forall x (P(x) \supset \neg Q(x)) \supset \neg (\forall x P(x) \,\&\, \exists x Q(x))$.

7.6. Метод резолюций для логики высказываний

Пусть $\mathcal{C}$ — конечное или бесконечное множество дизъюнктов, не содержащих переменных. В этом случае атомы можно рассматривать как пропозициональные переменные, ибо различные атомы принимают значения 0 и 1 независимо друг от друга. Мы рассматриваем дизъюнкты как множества литер. Это значит, что порядок литер в дизъюнкте не играет никакой роли, и в дизъюнкте нет повторяющихся литер. Пустой дизъюнкт обозначается $\bot$ и считается тождественно ложным. Пусть дизъюнкты D_1 и D_2 содержат контрарные литеры, т. е. имеют вид $C_1 \vee P$ и $C_2 \vee \neg P$, где C_1, C_2 — дизъюнкты, P — пропозициональная переменная. *Резольвентой* дизъюнктов D_1 и D_2 называется дизъюнкт $C_1 \vee C_2$. Эту резольвенту будем называть *резольвентой по переменной* P. В том случае, когда дизъюнкты D_1 и D_2 имеют вид A и $\neg A$, где A — атом, их резольвентой считается пустой дизъюнкт.

Пример. Дизъюнкт $Q \vee R$ является резольвентой дизъюнктов $P \vee R$ и $\neg P \vee Q \vee R$ по переменной P.

Правило резолюции позволяет из двух дизъюнктов, содержащих контрарные литеры, получить их резольвенту.

Теорема 7.3. *Если D — резольвента дизъюнктов D_1 и D_2, то $\{D_1, D_2\} \models D$.*

Доказательство. Пусть дизъюнкты D_1 и D_2 имеют вид $C_1 \vee A$ и $C_2 \vee \neg A$, где C_1 и C_2 — дизъюнкты (возможно, пустые), A — атом. Тогда D есть $C_1 \vee C_2$, а $\{D_1, D_2\} \models D$ означает, что для любой оценки пропозициональных переменных v, если $v(C_1 \vee A) = 1$ и $v(C_2 \vee \neg A) = 1$, то $v(C_1 \vee C_2) = 1$. Пусть v — произвольная оценка, для которой $v(C_1 \vee A) = 1$, $v(C_2 \vee \neg A) = 1$. Если $v(A) = 0$, то, очевидно, $v(C_1) = 1$, а если $v(A) = 1$, то $v(C_2) = 1$. Таким образом, в любом случае $v(D) = 1$, что и требовалось доказать. □

Резолюционным выводом дизъюнкта D из множества дизъюнктов $\mathcal{C}$ называется конечная последовательность дизъюнктов, в которой каждый дизъюнкт либо принадлежит множеству $\mathcal{C}$, либо получается из двух предшествующих дизъюнктов по правилу резолюции, а последний дизъюнкт есть D.

Пример. Следущая последовательность дизъюнктов является резолюционным выводом пустого дизъюнкта из множества дизъюнктов $\mathcal{C} = \{\neg P \vee Q, \neg Q, P\}$:

1) $\neg P \vee Q$;

2) $\neg Q$;

3) P;

4) $\neg P$ (получено по правилу резолюции из дизъюнктов 1 и 2);

5) $\bot$ (получено по правилу резолюции из дизъюнктов 3 из и 4).

Если существует резолюционный вывод дизъюнкта D из множества дизъюнктов $\mathcal{C}$, пишут $\mathcal{C} \vdash D$.

Теорема 7.4. *Если $\mathcal{C} \vdash D$, то $\mathcal{C} \models D$.*

Доказательство. Пусть v — такая оценка пропозициональных переменных, что $v(\mathcal{C}) = \{1\}$. Пусть $D_1, \ldots, D_n$ — резолюционный вывод дизъюнкта D из $\mathcal{C}$ (это означает, в частности, что D_n есть D). Индукцией по i докажем, что $v(D_i) = 1$. Если дизъюнкт D_i принадлежит множеству $\mathcal{C}$, то $v(D_i) = 1$ по условию. В частности, $v(D_1) = 1$. Пусть для всех $j < i$ доказываемое утверждение верно, и пусть дизъюнкт D_i получен по правилу резолюции из дизъюнктов D_k и D_l, где $k, l < i$, так что $v(D_k) = v(D_l) = 1$. Тогда, по теореме 7.3, $v(D_i) = 1$, что и требовалось доказать. □

Метод резолюций может быть использован для доказательства невыполнимости множества дизъюнктов.

Теорема 7.5. *Если $\mathcal{C} \vdash \bot$, то множество дизъюнктов $\mathcal{C}$ невыполнимо.*

Доказательство. Невыполнимость множества дизъюнктов $\mathcal{C}$ означает, что не существует оценки v, при которой все дизъюнкты из $\mathcal{C}$ принимают значение 1. Допустим противное, т. е. $v(\mathcal{C}) = \{1\}$ для некоторой оценки. Если при этом $\mathcal{C} \vdash \bot$, то, по теореме 7.4, $v(\bot) = 1$, что невозможно. □

Теорема 7.6 (теорема о полноте метода резолюций). *Если множество дизъюнктов $\mathcal{C}$ невыполнимо, то $\mathcal{C} \vdash \bot$.*

Доказательство. Пусть множество дизъюнктов $\mathcal{C}$ невыполнимо. В силу теоремы компактности для логики высказываний(теорема 2.9), существует конечное невыполнимое подмножество $\mathcal{C}'$ множества $\mathcal{C}$. Если мы докажем, что $\mathcal{C}' \vdash \bot$, то, очевидно, будет доказано $\mathcal{C} \vdash \bot$. Итак, пусть $\mathcal{C}' \vdash \bot$ — конечное невыполнимое множество дизъюнктов. Индукцией по количеству переменных в дизъюнктах из $\mathcal{C}'$ докажем, что $\mathcal{C}' \vdash \bot$. Если в $\mathcal{C}'$ вообще нет переменных, то $\mathcal{C}'$ состоит только из пустого дизъюнкта $\bot$, и тогда $\mathcal{C}' \vdash \bot$. Пусть существует резолюционный вывод пустого дизъюнкта из любого невыполнимого множества дизъюнктов, содержащего $\leq n$ переменных, и пусть $\mathcal{C}'$ — конечное невыполнимое множество дизъюнктов, в котором $n+1$ переменных. Пусть P — переменная, входящая в $\mathcal{C}'$. Можно считать, что в $\mathcal{C}'$ нет дизъюнктов, которые содержали бы одновременно литеры P и $\neg P$, так как при удалении таких дизъюнктов из невыполнимого множества получается невыполнимое множество дизъюнктов. Через $\mathcal{C}'_0$ обозначим множество всех тех дизъюнктов из $\mathcal{C}'$, которые не содержат переменную P, через $\mathcal{C}'_+$ обозначим множество дизъюнктов из $\mathcal{C}'$, которые содержат литеру P, а через $\mathcal{C}'_-$ — множество дизъюнктов из $\mathcal{C}'$, которые содержат литеру $\neg P$. Допустим, что множество $\mathcal{C}'_-$ пусто. Тогда каждый дизъюнкт, содержащий переменную P, имеет вид $D \vee P$, где D — дизъюнкт. В этом случае множество дизъюнктов $\mathcal{C}'_0$ непусто и невыполнимо. Действительно, если бы нашлась оценка v, для которой $v(\mathcal{C}'_0) = \{1\}$, то, положив $v(P) = 1$, мы получили бы, что $v(\mathcal{C}'_+) = \{1\}$, значит и $v(\mathcal{C}') = \{1\}$, что невозможно, так как, по условию, множество $\mathcal{C}'$ невыполнимо. Множество $\mathcal{C}'_0$ содержит $\leq n$ переменных, и, по индуктивному предположению, имеет место $\mathcal{C}'_0 \vdash \bot$, следовательно, $\mathcal{C}' \vdash \bot$. Аналогично доказывается, что $\mathcal{C}' \vdash \bot$, если множество $\mathcal{C}'_+$ пусто. Рассмотрим теперь случай, когда множества $\mathcal{C}'_-$ и $\mathcal{C}'_+$ оба не пусты. Обозначим через $\mathcal{C}'_1$ множество всех резольвент дизъюнктов из $\mathcal{C}'_-$ и $\mathcal{C}'_+$ по переменной P. Докажем, что множество $\mathcal{C}'_0 \cup \mathcal{C}'_1$ невыполнимо. Допустим противное, т. е. что для некоторой оценки v имеет место $v(\mathcal{C}'_0) = \{1\}$ и $v(\mathcal{C}'_1) = \{1\}$. Продолжим эту оценку на переменную P, положив $v(P) = 1$. Так как множество $\mathcal{C}'$ невыполнимо, то в нем найдется дизъюнкт, который при такой оценке принимает значение 0. Очевидно, что он принадлежит множеству $\mathcal{C}'_-$ и имеет вид $D_1 \vee \neg P$, причем $v(D_1) = 0$. Если же оценку v продолжить на переменную P, положив $v(P) = 0$, то найдется дизъюнкт из $\mathcal{C}'_+$ вида $D_2 \vee P$, где $v(D_2) = 0$. Резольвента дизъюнктов $D_1 \vee \neg P$ и $D_2 \vee P$ есть $D_1 \vee D_2$ и принадлежит множеству $\mathcal{C}'_1$, следовательно, $v(D_1 \vee D_2) = 1$. С другой стороны, $v(D_1 \vee D_2) = v(D_1) \vee v(D_2) = 0$. Полученное противоречие показывает, что на самом деле множество $\mathcal{C}'_0 \cup \mathcal{C}'_1$ невыполнимо. В этом множестве n переменных, и, по индуктивному предположению, из него выводим пустой дизъюнкт. Так как каждый дизъюнкт множества $\mathcal{C}'_0 \cup \mathcal{C}'_1$ выводим из $\mathcal{C}'$, в силу транзитивности отношения выводимости получаем $\mathcal{C}' \vdash \bot$, что и требовалось. □

Таким образом, множество дизъюнктов является невыполнимым тогда и только тогда, когда из него выводится пустой дизъюнкт.

Задачи

1) С помощью метода резолюций доказать, что следующие множества дизъюнктов невыполнимы:

   а) $\{P \vee Q \vee R,\ \neg P \vee R,\ \neg Q,\ \neg R\}$;

   б) $\{P \vee Q,\ \neg Q \vee R,\ \neg P \vee Q,\ \neg R\}$.

2) С помощью метода резолюций доказать, что следующие формулы тождественно истинны:

   а) $P \vee \neg P \,\&\, Q \supset P \vee Q$;

   б) $(P \vee Q) \,\&\, (P \vee \neg Q) \supset P$;

   в) $(P \vee Q) \,\&\, (Q \vee R) \,\&\, (R \vee P) \supset P \,\&\, Q \vee Q \,\&\, R \vee R \,\&\, P$.

7.7. Алгоритм унификации

Пусть фиксирован некоторый язык первого порядка сигнатуры Ω. *Подстановкой* называется частичная функция из множества переменных V в множество T всех термов сигнатуры Ω с конечной областью определения. Если θ — подстановка с областью определения $\{x_1, \ldots, x_m\}$, причем $\theta(x_i) = s_i$ $(i = 1, \ldots, m)$, то пишут $\theta = \{x_1 \to s_1, \ldots, x_m \to s_m\}$. Например, область определения подстановки $\{x \to f(z),\ z \to y\}$ состоит из переменных x и z, причем переменной x эта подстановка сопоставляет терм $f(z)$, а переменной z — терм y. Пустая подстановка обозначается ε.

Для каждого терма t индукцией по его построению определяется терм $t\theta$ — результат применения подстановки θ к терму t. Если t есть $x \in V$, причем $x \notin \{x_1, \ldots, x_n\}$, то $t\theta = t$. Если терм t есть $x \in \{x_1, \ldots, x_n\}$, то $t\theta = \theta(x)$. Если терм t имеет вид $f(t_1, \ldots, t_n)$, где f — функциональный символ, $t_1, \ldots, t_n \in T$, то $t\theta = f(t_1\theta, \ldots, t_n\theta)$. На этом определение терма $t\theta$ завершено. По сути, результат применения подстановки $\theta = \{x_1 \to s_1, \ldots, x_m \to s_m\}$ к терму t — это результат подстановки в t термов $s_1, \ldots, s_m$ вместо всех вхождений переменных $x_1, \ldots, x_m$ соответственно.

Пример. Пусть $\theta = \{x \to f(x),\ y \to g(x,z)\}$, терм t есть $g(f(x), g(f(z),y))$. Тогда $t\theta$ есть терм $g(f(f(x)), g(f(z), g(x,z)))$.

Для каждой формулы Φ индукцией по ее построению определяется формула $\Phi\theta$ — результат применения подстановки θ к формуле Φ. Если Φ есть атом $P(t_1,\ldots,t_n)$, где P — предикатный символ, $t_1,\ldots,t_n \in T$, то $\Phi\theta$ есть формула $P(\theta t_1,\ldots,\theta t_n)$. Если Φ имеет вид $\Psi_1 \lambda \Psi_2$, где $\lambda \in \{\&, \vee, \supset\}$, то $\Phi\theta$ есть формула $(\Psi_1\theta)\lambda(\Psi_2\theta)$. Если Φ имеет вид $\neg\Psi$, то $\Phi\theta$ есть формула $\neg(\Psi\theta)$. Наконец, если Φ имеет вид $\kappa x \Psi$, где $\kappa \in \{\forall, \exists\}$, $x \in V$, причем $x \notin \{x_1,\ldots,x_n\}$, то $\Phi\theta$ есть формула $\kappa x(\Psi\theta)$. Если же Φ имеет вид $\kappa x\Psi$, где $\kappa \in \{\forall,\exists\}$, $x \in \{x_1,\ldots,x_n\}$, то $\Phi\theta$ есть формула $\kappa x(\Psi\theta')$, где $\theta' = \theta|_{\{x_1,\ldots,x_n\}\setminus\{x\}}$, т. е. θ' есть сужение подстановки θ путем выбрасывания переменной x из ее области определения. На этом определение формулы $\Phi\theta$ завершено. По сути, результат применения подстановки $\theta = \{x_1 \to s_1,\ldots,x_m \to s_m\}$ к формуле Φ — это результат подстановки в Φ термов $s_1,\ldots,s_m$ вместо свободных вхождений переменных $x_1,\ldots,x_m$ соответственно.

Пусть даны подстановки $\theta = \{x_1 \to t_1,\ldots,x_n \to t_n\}$ и $\lambda = \{y_1 \to u_1,\ldots,y_m \to u_m\}$. *Произведением* (или *композицией*) подстановок θ и λ называется подстановка, обозначаемая $\theta \circ \lambda$, которая получается из множества $\{x_1 \to t_1\lambda,\ldots,x_n \to t_n\lambda, y_1 \to u_1,\ldots,y_m \to u_m\}$ вычеркиванием всех элементов $x_j \to t_j\lambda$, для которых $t_j\lambda = x_j$, и всех элементов $y_i \to u_i$, для которых $y_i \in \{x_1,\ldots,x_n\}$.

Пример. Пусть $\theta = \{x \to f(y),\ y \to z\}$, $\lambda = \{x \to a,\ y \to b,\ z \to y\}$. Тогда $\theta \circ \lambda = \{x \to f(b),\ z \to y\}$.

Произведение $\theta \circ \lambda$ подстановок θ и λ обладает тем свойством, что $E(\theta \circ \lambda) = (E\theta)\lambda$ для любого выражения E. Заметим, что $\varepsilon \circ \theta = \theta \circ \varepsilon = \theta$, какова бы ни была подстановка θ.

Подстановка θ называется *унификатором* для множества выражений $\{E_1,\ldots,E_k\}$, если $E_1\theta = \ldots = E_k\theta$. Множество выражений называется *унифицируемым*, если для него существует унификатор.

Пример. Множество атомов $\{P(a,y),\ P(x,f(b))\}$ унифицируемо. Подстановка $\{x \to a,\ y \to f(b)\}$ является его унификатором.

Унификатор σ для множества выражений W называется *наиболее общим унификатором* для W, если, каков бы ни был унификтор θ для W, существует такая подстановка λ, что $\theta = \sigma \circ \lambda$. Оказывается, для любого унифицируемого множества выражений существует наиболее общий унификатор. Он может быть найден с помощью следующего алгоритма. Пусть дано множество выражений W. *Множество рассогласований* для W получается следующим образом. В выражениях из W выявляем первую слева позицию, на которой не во всех выражениях из W стоит один и тот же символ, и выписываем из каждого выражения из W те его подвыражения, которые начинаются с этой позиции. Полученное множество подвыражений и есть множество рассогласований для W.

Пример. Пусть W есть $\{P(x,f(y,z)),\ P(x,a),\ P(x,g(h(k(x))))\}$. Мы видим, что начала $P(x,$ во всех этих выражениях одинаковые, а различия начинаются с пятой позиции, и множество рассогласований для W — это множество термов $\{f(y,z),\ a,\ g(h(k(x)))\}$.

Алгоритм унификации работает по шагам. На k-м шаге строятся множество выражений W_k и подстановка σ_k. При $k = 0$ полагаем $W_0 = W$, $\sigma_0 = \varepsilon$. Пусть множество выражений W_k и подстановка σ_k построены. Если W_k состоит только из одного выражения, то σ_k — наиболее общий унификатор для W, и выполнение алгоритма на этом заканчивается. Если же в W_k два или более выражений, то находим множество рассогласований для W_k, которое обозначим D_k. Если среди элементов множества D_k есть переменная v_k и терм t_k такие, что v_k не входит в t_k, то полагаем $\sigma_{k+1} = \sigma_k \circ \{v_k \to t_k\}$, $W_{k+1} = W_k\{v_k \to t_k\}$ и переходим к следующему шагу. В противном случае множество W не унифицируемо, и выполнение алгоритма заканчивается.

Пример. Пусть $W = \{P(a,\ x,\ f(g(y))),\ P(z,\ f(z),\ f(u))\}$. Тогда $\sigma_0 = \varepsilon$, $W_0 = W$. Так как в W_0 более одного элемента, найдем множество рассогласований для него: $D_0 = \{a,\ z\}$. Переменная z не входит в терм a, так что полагаем

$$\sigma_1 = \{z \to a\},$$

$$W_1 = W_0\{z \to a\} = \{P(a,\ x,\ f(g(y))),\ P(a,\ f(a),\ f(u))\}.$$

Так как в W_1 более одного элемента, найдем множество рассогласований для него: $D_1 = \{x,\ f(a)\}$. Переменная x не входит в терм $f(a)$, поэтому полагаем

$$\sigma_2 = \sigma_1 \circ \{x \to f(a)\} = \{z \to a,\ x \to f(a)\},$$

$$W_2 = W_1\{x \to f(a)\} = \{P(a,\, f(a),\, f(g(y))),\; P(a,\, f(a),\, f(u))\}.$$

Так как в W_2 более одного элемента, найдем множество рассогласований для него: $D_2 = \{g(y),\, u\}$. Переменная u не входит в терм $g(y)$, поэтому полагаем

$$\sigma_3 = \sigma_2 \circ \{u \to g(y)\} = \{z \to a,\, x \to f(a),\, u \to g(y)\},$$

$$W_3 = W_1\{x \to f(a)\} = \{P(a,\, f(a),\, f(g(y))),\; P(a,\, f(a),\, f(g(y)))\} = \{P(a,\, f(a),\, f(g(y))).$$

Множество W_3 состоит только из одного выражения. Значит, σ_3 — наиболее общий унификатор для W.

Задачи

Применить алгоритм унификации к следующим множествам атомов:

1) $\{Q(a),\, Q(b)\}$;

2) $\{Q(a, x),\, Q(a, a)\}$;

3) $\{Q(a, x, f(x)),\, Q(a, y, y)\}$;

4) $\{Q(x, y, z),\, Q(u, h(v, v), u)\}$;

5) $\{P(x_1, g(x_1), x_2, h(x_1, x_2), x_3, k(x_1, x_2, x_3)),\; P(y_1, y_2, e(y_2), y_3, f(y_2, y_3), y_4)\}$.

7.8. Метод резолюций для логики предикатов

Если две или более литер дизъюнкта D имеют наиболее общий унификатор θ, то дизъюнкт $D\theta$ называется *склейкой* дизъюнкта D. Например, первая и вторая литеры дизъюнкта $P(x) \vee P(f(y)) \vee \neg Q(x)$ имеют наиболее общий унификатор $\{x \to f(y)\}$, и дизъюнкт $P(f(y)) \vee \neg Q(f(y))$ является склейкой этого дизъюнкта.

Пусть D_1 и D_2 — два дизъюнкта, которые не имеют общих переменных, и пусть D_1 содержит литеру A_1, а D_2 содержит литеру $\neg A_2$, где A_1, A_2 — атомы, имеющие наиболее общий унификатор θ. Тогда дизъюнкт $(D_1\theta \setminus \{A_1\theta\}) \cup (D_2\theta \setminus \{\neg A_2\theta\})$ называется *резольвентой* дизъюнктов D_1 и D_2. При этом литеры $A_1, \neg A_2$ называются *отрезаемыми литерами*. Например, резольвентой дизъюнктов $P(x) \vee Q(x)$ и $\neg P(a) \vee R(y)$ является дизъюнкт $Q(a) \vee R(y)$, а резольвентой дизъюнктов $P(f(a))$ и $\neg P(y)$ является пустой дизъюнкт $\bot$.

Правило резолюции состоит в получении из двух дизъюнктов их резольвенты.

Резолюционным выводом из множества дизъюнктов Γ называется конечная последовательность дизъюнктов, в которой каждый дизъюнкт либо принадлежит множеству Γ, либо является склейкой какого-нибудь из предыдущих дизъюнктов, либо получается по правилу резолюции из каких-нибудь двух предыдущих дизъюнктов. Говорят, что дизъюнкт D *выводится* из множества дизъюнктов Γ, и пишут $\Gamma \vdash D$, если существует резолюционный вывод из Γ, последним дизъюнктом которого является D.

Теорема 7.7 (корректность метода резолюций). *Каковы бы ни были множество дизъюнктов Γ и дизъюнкт D, если $\Gamma \vdash D$, то $\Gamma \models D$.*

Доказательство. Индукция по длине k резолюционного вывода дизъюнкта D из Γ. Если $k = 1$, то $D \in \Gamma$, и доказываемое утверждение очевидно. Допустим, что теорема справедлива в случае, когда длина вывода $< k$. Пусть существует резолюционный вывод D из Γ, и длина этого вывода равна k. Если $D \in \Gamma$, то доказываемое утверждение очевидно. Пусть D есть склейка некоторого дизъюнкта C, который встречается в этом выводе раньше, чем D. Тогда, по индуктивному предположению, $\Gamma \models C$. Достаточно доказать, что формула $C \supset D$ общезначима. На самом деле она выводима в исчислении предикатов. Действительно, пусть $x_1, \ldots, x_n$ — все переменные, входящие в дизъюнкт C. Тогда C является сокращенной записью формулы $\forall x_1 \ldots \forall x_n C$, а D получается подстановкой в C некоторых термов $t_1, \ldots, t_n$ вместо $x_1, \ldots, x_n$ и является краткой записью формулы $\forall y_1 \ldots \forall y_m D$, где $y_1, \ldots, y_m$ — все переменные, входящие в дизъюнкт D. Тогда, очевидно, формула $C \supset D$ выводима в исчислении предикатов с помощью аксиом 11, правила силлогизма и правила (III).

Пусть D есть резольвента дизъюнктов D_1 и D_2, которые встречаются в этом выводе раньше, чем D. Тогда, по индуктивному предположению, $\Gamma \models D_1$, $\Gamma \models D_2$. Достаточно доказать, что $\{D_1, D_2\} \models D$. Дизъюнкт D_1 имеет вид $C_1 \vee A_1$, а дизъюнкт D_2 имеет вид $C_2 \vee \neg A_2$, причем атомы A_1 и A_2 имеют наиболее общий унификатор θ. Тогда D имеет вид $C_1\theta \vee C_2\theta$. Пусть $x_1, \ldots, x_n$ — все переменные, входящие хотя бы в один из дизъюнктов D_1, D_2. Тогда, очевидно, $\{D_1, D_2\} \models \forall x_1 \ldots \forall x_n((C_1 \vee A_1)\,\&\,(C_2 \vee \neg A_2))$. С помощью аксиомы 11 и правила силлогизма получаем, что формула

$$\forall x_1 \ldots \forall x_n((C_1 \vee A_1)\,\&\,(C_2 \vee \neg A_2)) \supset (C_1\theta \vee A)\,\&\,(C_2\theta \vee \neg A),$$

где A есть одновременно $A_1\theta$ и $A_2\theta$, выводима в исчислении предикатов. Поскольку любая формула вида $(\Phi_1 \vee \Psi) \,\&\, (\Phi_2 \vee \neg\Psi) \supset (\Phi_1 \vee \Phi_2)$, очевидно, является пропозициональной тавтологией и, следовательно, выводима в исчислении предикатов, то, по правилу силлогизма, получаем выводимость в исчислении предикатов формулы $\forall x_1 \ldots \forall x_n((C_1 \vee A_1) \,\&\, (C_2 \vee \neg A_2)) \supset (C_1\theta \vee C_2\theta)$. Отсюда с помощью правила (III) получаем выводимость в исчислении предикатов формулы $\forall x_1 \ldots \forall x_n((C_1 \vee A_1) \,\&\, (C_2 \vee \neg A_2)) \supset \forall y_1 \ldots \forall y_m(C_1\theta \vee C_2\theta)$, где $y_1, \ldots, y_m$ — все переменные, входящие в $C_1\theta \vee C_2\theta$. Отсюда следует $\{D_1, D_2\} \models D$, что и требовалось доказать. □

Следствие 7.1. *Если существует резолюционный вывод пустого дизъюнкта $\bot$ из множества дизъюнктов Γ, то множество Γ невыполнимо.*

Доказательство. Пусть $\Gamma \vdash \bot$. Тогда $\Gamma \models \bot$ в силу теоремы 7.7, откуда следует, что Γ не имеет модели, поскольку $\bot$ не имеет модели. □

Теорема 7.8 (полнота метода резолюций). *Если множество дизъюнктов Γ невыполнимо, то $\Gamma \vdash \bot$.*

Доказательство. Пусть множество дизъюнктов Γ невыполнимо. Тогда, в силу теоремы Эрбрана (теорема 7.2), существует конечное невыполнимое множество основных примеров дизъюнктов из Γ. Обозначим это множество Δ. В силу теоремы о полноте метода резолюций для логики высказываний (теорема 7.6), существует резолюционный вывод из Δ пустого дизъюнкта $\bot$. Пусть этот вывод имеет вид $D_1, \ldots, D_n$, причем D_n есть $\bot$. Индукцией по i докажем, что для любого дизъюнкта D_i $(i = 1, \ldots, n)$ существует такой дизъюнкт C_i, что $\Gamma \vdash C_i$ и $D_i = C_i\theta$ для некоторой подстановки θ.

Если $D_i \in \Delta$ (в частности, при $i = 1$), то D_i есть основной пример некоторого дизъюнкта из Γ, значит, существует такой дизъюнкт C_i, что $\Gamma \vdash C_i$ и $D_i = C_i\theta$ для некоторой подстановки θ. При этом, возможно, в результате применения подстановки θ к дизъюнкту C_i некоторые литеры в нем отождествились. Это означает, что D_i получается некоторой подстановкой θ' из некоторого дизъюнкта C_i', являющегося склейкой дизъюнкта C_i. Тогда $D_i = C_i'\theta'$, причем $\Gamma \vdash C_i'$.

Пусть дизъюнкт D_i получен по правилу резолюции из дизъюнктов D_k, D_l, где $k, l < i$. Индуктивное предположение состоит в том, что существуют дизъюнкты C_k и C_l такие, что $\Gamma \vdash C_k$, $\Gamma \vdash C_l$ и $D_k = C_k\theta_k$, $D_l = C_l\theta_l$ для некоторых подстановок θ_k и θ_l. Можно считать, что дизъюнкты C_k и C_l не имеют общих переменных, так что $D_k = C_k\theta$, $D_l = C_l\theta$, где $\theta = \theta_1 \cup \theta_2$. Так как к дизъюнктам D_k и D_l применимо правило резолюции, то D_k имеет вид $D_k' \vee A$, а D_l имеет вид $D_l' \vee \neg A$ для некоторого атома A. Тогда, C_k имеет вид $C_k' \vee A_k$, а C_l имеет вид $C_l' \vee \neg A_l$ для некоторых атомов A_k, A_l, причем $D_k' = C_k'\theta$, $D_l' = C_l'\theta$, $A = A_k\theta = A_l\theta$. Это значит, что атомы A_k и A_l унифицируемы и имеют наиболее общий унификатор σ, а так как θ тоже является их унификатором, то $\theta = \sigma \circ \lambda$ для некоторой подстановки λ. Таким образом, к дизъюнктам C_k и C_l применимо правило резолюции, причем резольвентой является дизъюнкт $C_k'\sigma \vee C_l'\sigma$, который и можно взять в качестве C_i. Действительно, $\Gamma \vdash C_i$, причем $D_i = D_k' \vee D_l' = C_k'\theta \vee C_l'\theta = C_k'(\sigma \circ \lambda) \vee C_l'(\sigma \circ \lambda) = C_i\lambda$.

При $i = n$ получаем, что $\Gamma \vdash \bot$, что и требовалось доказать. □

Задачи

1) Найти склейки следующих дизъюнктов (если они существуют):

   а) $P(x) \vee Q(y) \vee P(f(x))$;

   б) $P(x) \vee P(a) \vee Q(f(x)) \vee Q(f(a))$;

   в) $P(x, y) \vee P(a, f(a))$;

   г) $P(x) \vee P(f(y)) \vee Q(x, y)$.

2) Найти все возможные резольвенты следующих пар дизъюнктов (если они существуют):

   а) $\neg P(x) \vee Q(x, b)$ и $P(a) \vee Q(a, b)$;

   б) $\neg P(x) \vee Q(x, x)$ и $\neg Q(a, f(a))$;

   в) $\neg P(x, y, u) \vee \neg P(y, z, v) \vee \neg P(x, v, w) \vee P(u, z, w)$ и $P(g(x_1, y_1), x_1, y_1)$.

3) Доказать с помощью метода резолюций, что следующие множества дизъюнктов невыполнимы:

   а) $\{\neg P(x) \vee Q(f(x), x),\ P(g(b)),\ \neg Q(y, z)\}$;

   б) $\{P(x),\ Q(x, f(x)) \vee \neg P(x),\ \neg Q(g(y), z)\}$.

7.9. Применение метода резолюций для доказательства теорем

Пусть дана аксиоматическая теория первого порядка T. Для простоты будем считать, что множество аксиом теории T конечно, а значит, его можно заменить одной замкнутой формулой A — конъюнкцией всех аксиом. По определению, теоремами теории T являются логические следствия из A. В силу теоремы 5.5, каково бы ни было высказывание Φ, имеет место $A \models \Phi$ тогда и только тогда, когда множество высказываний $\{A, \neg\Phi\}$ невыполнимо. Очевидно, что последнее выполняется тогда и только тогда, когда невыполнима формула $A \,\&\, \neg\Phi$. Обозначим эту формулу Ψ. Приведем формулу Ψ к скулемовской форме. Получим формулу Ψ^*, равновыполнимую с формулой Ψ. Следовательно, для доказательства утверждения $A \models \Phi$ достаточно убедиться, что формула Ψ^* не имеет модели. Для этого представим формулу Ψ^* в виде множества дизъюнктов $\mathcal{C}$ и воспользуемся методом резолюций, а именно, попытаемся построить резолюционный вывод из $\mathcal{C}$ пустого дизъюнкта $\bot$. Если это удастся, то тем самым будет доказано, что множество дизъюнктов $\mathcal{C}$ невыполнимо, следовательно, формула Ψ^* не имеет модели, а значит, формула Ψ также не имеет модели, а тогда $A \models \Phi$, т. е. высказывание Φ является теоремой теории T. Этот метод находит практическое применение в области автоматического доказательства теорем.

Пример. Докажем с помощью метода резолюций, что

$$\{\forall x\forall y\forall z(P(x,y) \supset (P(y,z) \supset P(x,z)),\ \forall x\neg P(x,x)\} \models \neg\exists x\exists y(P(x,y) \,\&\, P(y,x)).$$

Для этого достаточно доказать, что формула

$$\forall x\forall y\forall z(P(x,y) \supset (P(y,z) \supset P(x,z))\,\&\,\forall x\neg P(x,x)\,\&\,\neg\neg\exists x\exists y(P(x,y)\,\&\,P(y,x))$$

не имеет модели. α-нормальная форма этой формулы имеет вид

$$\forall x\forall y\forall z(\neg P(x,y) \vee \neg P(y,z) \vee P(x,z))\,\&\,\forall u\neg P(u,u)\,\&\,\exists v\exists w(P(v,w)\,\&\,P(w,v)).$$

Скулемовская форма этой формулы выглядит так:

$$\{\forall x\forall y\forall z(\neg P(x,y) \vee \neg P(y,z) \vee P(x,z))\,\&\,\forall u\neg P(u,u)\,\&\,P(a,b)\,\&\,P(b,a).$$

Таким образом, рассматриваемая формула представляется следующим множеством дизъюнктов:

1) $\neg P(x,y) \vee \neg P(y,z) \vee P(x,z)$
2) $\neg P(u,u)$
3) $P(a,b)$
4) $P(b,a)$

Продолжим этот список до резолюционного вывода пустого дизъюнкта:

5) $\neg P(b,z) \vee P(a,z)$ (получено по правилу резолюции из дизъюнктов 1 и 4)
6) $P(a,a)$ (получено по правилу резолюции из дизъюнктов 4 и 5)
7) $\bot$ (получено по правилу резолюции из дизъюнктов 3 и 6)

Итак, мы доказали, что рассматриваемое множество дизъюнктов невыполнимо, следовательно, невыполнима и представляемая им формула.

Задачи

Доказать с помощью метода резолюций:

1) $\{\forall xP(x) \supset \exists xQ(x)\} \models \exists x(P(x) \supset Q(x))$;
2) $\{\exists x(P(x) \supset Q(x))\} \models \forall xP(x) \supset \exists xQ(x)$;
3) $\{\exists x\forall yP(x,y)\} \models \forall x\exists yP(y,x)$;
4) $\models \forall x\forall yP(x,y) \supset \forall y\forall xP(x,y)$;
5) $\models \exists x\exists yP(x,y) \supset \exists y\exists xP(x,y)$;
6) $\models (\exists xP(x) \supset \forall xQ(x)) \supset \forall x(P(x) \supset \forall xQ(x))$;
7) $\models (\forall x(P(x) \supset \forall xQ(x)) \supset (\exists xP(x) \supset \forall xQ(x))$.

7.10. Хорновские дизъюнкты

Дизъюнкт называется *хорновским*, если он содержит не более одной положительной литеры. Пустой дизъюнкт $\bot$ является хорновским. Если непустой хорновский дизъюнкт не содержит положительных литер, он называется *запросом* (причины для такого названия выяснятся позднее). Запрос имеет вид

$$\neg A_1 \vee \ldots \vee \neg A_n,$$

где $n \geq 1$, $A_1, \ldots, A_n$ — атомы, и является сокращенной записью формулы $\forall x_1 \ldots \forall x_m(\neg A_1 \vee \ldots \vee \neg A_n)$, где $x_1, \ldots, x_m$ — все переменные, входящие в дизъюнкт. Эта формула равносильна формуле

$$\forall x_1 \ldots \forall x_m \neg(A_1 \,\&\, \ldots \,\&\, A_n).$$

Если хорновский дизъюнкт содержит одну положительную литеру и несколько отрицательных, он называется *правилом* или *процедурой*. Правило имеет вид

$$A \vee \neg A_1 \vee \ldots \neg A_n,$$

где $n \geq 1$, $A, A_1, \ldots, A_n$ — атомы, и является сокращенной записью формулы $\forall x_1 \ldots \forall x_m(A \vee \neg A_1 \vee \ldots \neg A_n)$, где $x_1, \ldots, x_m$ — все переменные, входящие в дизъюнкт. Эта формула равносильна формуле

$$\forall x_1 \ldots \forall x_m(A_1 \,\&\, \ldots \,\&\, A_n \supset A).$$

Если непустой хорновский дизъюнкт не содержит отрицательных литер, он называется *фактом*. Факт имеет вид A, где A — атом, и является сокращенной записью формулы $\forall x_1 \ldots \forall x_m A$, где $x_1, \ldots, x_m$ — все переменные, входящие в этот атом.

Теорема 7.9. *Пусть* Γ *— множество хорновских дизъюнктов,* $\mathcal{H}$ *— некоторое семейство эрбрановских моделей для множества* Γ*. Пусть эрбрановская модель* $\mathfrak{H}_0$ *определяется следующим образом: для любого (*n*-местного) предикатного символа* P *и элементов эрбрановского универсума* $h_1, \ldots, h_n \in H$

$$P^{\mathfrak{H}_0}(h_1, \ldots, h_n) = 1 \rightleftharpoons (\forall \mathfrak{H} \in \mathcal{H}) P^{\mathfrak{H}}(h_1, \ldots, h_n) = 1.$$

Тогда $\mathfrak{H}_0$ *является моделью для* Γ*.*

Доказательство. Докажем, что любой дизъюнкт из Γ истинен в интерпретации $\mathfrak{H}_0$. Рассмотрим случай, когда этот дизъюнкт является запросом. Тогда он является записью формулы вида

$$\forall x_1 \ldots \forall x_m(\neg A_1 \vee \ldots \vee \neg A_n).$$

Поскольку эта формула истинна в каждой интерпретации из $\mathcal{H}$, то для любых значений $h_1, \ldots, h_m \in H$ переменных $x_1, \ldots, x_m$ и любой эрбрановской модели для Γ найдется такой атом A_i $(i = 1, \ldots, n)$, который при этих значениях переменных принимает значение 0. Но тогда, по определению интерпретации $\mathfrak{H}_0$, значение атома A_i при этих значениях переменных в $\mathfrak{H}_0$ также есть 0, а тогда значение литеры $\neg A_i$ и всего дизъюнкта есть 1. Таким образом, при любых значениях переменных $x_1, \ldots, x_m$ рассматриваемый дизъюнкт истинен в интерпретации $\mathfrak{H}_0$, значит, формула $\forall x_1 \ldots \forall x_m(\neg A_1 \vee \ldots \vee \neg A_n)$ истинна в интерпретации $\mathfrak{H}_0$, что и требовалось доказать.

Рассмотрим случай, когда дизъюнкт из Γ является правилом. Тогда он равносилен формуле

$$\forall x_1 \ldots \forall x_m(A_1 \,\&\, \ldots \,\&\, A_n \supset A).$$

Зафиксируем произвольные значения $h_1, \ldots, h_m \in H$ переменных $x_1, \ldots, x_m$. Допустим, что при этих значениях переменных атомы $A_1, \ldots, A_n$ истинны в интерпретации $\mathfrak{H}_0$, и докажем, что тогда и атом A истинен в интерпретации $\mathfrak{H}_0$. Истинность атомов $A_1, \ldots, A_n$ в интерпретации $\mathfrak{H}_0$ означает, что они истинны в любой интерпретации из $\mathcal{H}$. Поскольку рассматриваемая формула также истинна в любой интерпретации из $\mathcal{H}$, то атом A при рассматриваемых значениях переменных принимает значение 1 в любой интерпретации из $\mathcal{H}$, а значит, он принимает значение 1 в интерпретации $\mathfrak{H}_0$, что и требовалось доказать.

Наконец, рассмотрим случай, когда дизъюнкт из Γ является фактом. Тогда он равносилен формуле $\forall x_1 \ldots \forall x_m P(x_1, \ldots, x_m)$. Поскольку эта формула истинна в любой интерпретации из $\mathcal{H}$, то для любых элементов эрбрановского универсума $h_1, \ldots, h_m$ и любой интерпретации $\mathfrak{H} \in \mathcal{H}$ имеет место $P^{\mathfrak{H}}(h_1, \ldots, h_m) = 1$. Тогда, по определению интерпретации $\mathfrak{H}_0$, имеет место $P^{\mathfrak{H}_0}(h_1, \ldots, h_m) = 1$ для любых элементов эрбрановского универсума $h_1, \ldots, h_m$, а это означает, что формула $\forall x_1 \ldots \forall x_m P(x_1, \ldots, x_m)$ истинна в интерпретации $\mathfrak{H}_0$, что и требовалось доказать. $\square$

В случае, когда $\mathcal{H}$ — семейство всех эрбрановских моделей для Γ, эрбрановская модель $\mathfrak{H}_0$, существование которой утверждается в теореме 7.9, называется *минимальной* эрбрановской моделью для множества хорновских дизъюнктов Γ.

Теорема 7.10. *Пусть* Γ *— некоторое множество хорновских дизъюнктов, причем*

$$\Gamma \models \exists x_1 \ldots \exists x_m (A_1 \,\&\, \ldots \,\&\, A_n),$$

где $A_1, \ldots, A_n$ *— атомы,* $x_1, \ldots, x_m$ *— все входящие в них переменные. Тогда существует такая подстановка* $\theta = \{x_1 \to h_1, \ldots, x_m \to h_m\}$*, где* $h_1, \ldots, h_m \in H$*, что* $\Gamma \models A_1\theta \,\&\, \ldots \,\&\, A_n\theta$*.*

Доказательство. Так как $\Gamma \models \exists x_1 \ldots \exists x_m (A_1 \,\&\, \ldots \,\&\, A_n)$, то множество высказываний

$$\Gamma \cup \{\neg \exists x_1 \ldots \exists x_m (A_1 \,\&\, \ldots \,\&\, A_n)\}$$

невыполнимо. После скулемизации получаем, что невыполнимо множество хорновских дизъюнктов

$$\Gamma \cup \{\neg A_1 \vee \ldots \vee \neg A_n\}.$$

Это означает, что в любой эрбрановской модели для Γ формула $\forall x_1 \ldots \forall x_m (\neg A_1 \vee \ldots \vee \neg A_n)$ ложна, следовательно, ее отрицание $\exists x_1 \ldots \exists x_m (A_1 \,\&\, \ldots \,\&\, A_n)$ истинно. В частности, эта формула истинна в минимальной эрбрановской модели для Γ. Это означает, что существуют такие значения $h_1, \ldots, h_m \in H$ переменных $x_1, \ldots, x_m$, при которых атомы $A_1, \ldots, A_n$ истинны в минимальной модели. Но тогда все они истинны в любой модели для Γ, т. е. $\Gamma \models A_1\theta \,\&\, \ldots \,\&\, A_n\theta$, где $\theta = \{x_1 \to h_1, \ldots, x_m \to h_m\}$. □

7.11. Логические программы

Логической программой называется произвольное конечное множество процедур и фактов. Процедуру, равносильную формуле $\forall x_1 \ldots \forall x_m (A_1 \,\&\, \ldots \,\&\, A_n \supset B)$, в логическом программировании принято записывать в виде

$$B \leftarrow A_1, \ldots, A_n, \tag{36}$$

а факт B — в виде $B \leftarrow$. Таким образом, процедуры и факты записываются единообразно в виде (36), где $n \geq 0$ (при $n = 0$ список атомов справа от $\leftarrow$ считается пустым). В дальнейшем мы будем называть процедурами любые выражения вида (36). При этом атом B называется *заголовком* процедуры (36), а список атомов $A_1, \ldots, A_n$ — ее *телом*.

Интуитивный смысл логической программы состоит в том, что она в форме хорновских дизъюнктов на подходящем языке первого порядка описывает некоторую ситуацию. Рассмотрим, например, следующий язык первого порядка для описания родственных связей между членами семьи Симпсонов, состоящей из Гомера Симпсона (обозначим его h), его жены Мардж (обозначим ее m), их сына Барта (b) и дочерей Лиз (l) и Мэгги (n). Пусть P — двуместный предикат на множестве всех людей такой, что $P(x, y)$ означает «человек x — родитель человека y», а Q — такой двуместный предикат на множестве всех людей, что $Q(x, y)$ означает «человек x — отпрыск человека y». Естественная связь между этими предикатами выражается процедурами

1) $Q(x, y) \leftarrow P(x, y)$;
2) $P(x, y) \leftarrow Q(x, y)$.

К ним можно добавить такие факты:

3) $P(h, b) \leftarrow$;
4) $P(h, l) \leftarrow$;
5) $P(h, n) \leftarrow$;
6) $P(m, b) \leftarrow$;
7) $P(m, l) \leftarrow$;
8) $P(m, n) \leftarrow$.

Факт вроде $Q(b, h)$ включать в логическую программу необязательно, поскольку он следует из факта 3) и правила 1).

Работа логической программы начинается, когда указан запрос. Пусть, например, нас интересует вопрос, является ли Мардж родителем Лиз. Этот вопрос мы записываем так: $?P(m, l)$. Пытаясь ответить на этот вопрос с помощью данной логической программы, мы по существу хотим выяснить, является ли высказывание $P(m, l)$ логическим следствием из высказываний, составляющих логическую программу. Для этого надо к программе добавить отрицание интересующего нас высказывания и попытаться установить невыполнимость полученного множества высказываний. Это делается с помощью метода резолюций. Итак, мы заменяем знак вопроса ? на символ отрицания $\neg$ и формируем запрос

9) $\neg P(m, l)$.

Получив запрос, логическая программа начинает выполняться. Отыскивается процедура, которая *отвечает на запрос*, т. е. такая процедура, заголовок которой унифицируем с запросом. В нашем случае на

запрос отвечает процедура 7). Наиболее общим унификатором запроса и заголовка этой процедуры является пустая подстановка, а их резольвентой — пустой дизъюнкт $\perp$, что свидетельствует об успешной обработке запроса и получении положительного ответа на него.

7.12. Вычислительные аспекты логического программирования

Пусть даны логическая программа П и запрос $?A_1, \ldots, A_n$ ($A_1, \ldots, A_n$ — атомы). Обработка запроса состоит в следующем. Среди процедур, составляющих программу П, отыскивается такая, которая отвечает на запрос, т. е. заголовок которой унифицируем с одним из атомов $A_1, \ldots, A_n$. Пусть, например, факт B, входящий в программу П, унифицируем с атомом A_i ($i = 1, \ldots, n$). Тогда строится наиболее общий унификатор θ атомов B и A_i. Резольвентой факта B и рассматриваемого запроса является новый запрос $?A_1\theta, \ldots, A_{i-1}\theta, A_{i+1}\theta, \ldots, A_n\theta$, который и подлежит дальнейшей обработке. Если же на запрос отвечает правило $B \leftarrow C_1, \ldots, C_m$, т. е. атом B унифицируем с одним из атомовA_i ($i = 1, \ldots, n$), то строится наиболее общий унификатор θ атомов B и A_i. Резольвентой факта B и рассматриваемого запроса является новый запрос $?A_1\theta, \ldots, A_{i-1}\theta, A_{i+1}\theta, \ldots, A_n\theta, C_1\theta, \ldots, C_m\theta$, который подвергается дальнейшей обработке.

Таким образом, на каждой стадии работы программы, или *вычисления*, существует текущий запрос. Последовательность запросов, которые обрабатываются в процессе вычисления, называют *протоколом* вычисления. Таким образом, протокол представляет собой резолюционный вывод из программы и запроса, характеризующийся тем, что на каждом шаге строится резольвента запроса и одной из процедур (а не двух процедур). Вычисление считается успешным, если его протокол оканчивается пустым дизъюнктом $\perp$. В этом случае высказывание, представленное исходным запросом, логически следует из высказываний, составляющих программу. Можно доказать и обратное утверждение: если запрос логически следует из логической программы, то существует успешное вычисление, т. е. резолюционный вывод указанного специального вида, оканчивающийся пустым дизъюнктом.

Вычисление с помощью логической программы недетерминировано в том смысле, что на каждом шаге выбор процедуры, отвечающей на текущий запрос, вообще говоря, неоднозначен: может найтись много процедур, отвечающих на запрос, причем унифицируемыми с заголовками процедур могут оказаться различные атомы, входящие в запрос. Поэтому при обработке данного запроса может возникнуть много различных вычислений, которые составляют так называемое *пространство вычислений*. Пространство вычислений можно представлять в виде дерева, корнем которого является исходный запрос, вершины соответствуют запросам, получающимся в процессе вычислений, а ребра соединяют данный запрос с запросами, получающимися на первом шаге при обработке данного запроса. Ветви такого дерева суть различные вычисления (точнее — их протоколы). Успешному вычислению отвечает конечная ветвь. Конечная ветвь может соответствовать и вычислению, не являющемуся успешным, если оно оканчивается непустым запросом, на который не отвечает ни одна процедура. Возможны также неуспешные бесконечные вычисления.

Значением логической программы называется множество основных атомов A таких, что существует успешное вычисление с запросом $?A$.

Теорема 7.11. *Значение логической программы* П *состоит из всех тех основных атомов, которые истинны в минимальной эрбрановской модели для* П.

Доказательство. Пусть основной атом A принадлежит значению логической программы П, т. е. существует резолюционный вывод пустого дизъюнкта $\perp$ из множества $\Pi \cup \{\neg A\}$. Это означает, что из множества П логически следует высказывание A, так что A истинно в любой модели для П, в частности, в минимальной эрбрановской модели для П.

Обратно, пусть высказывание A, являющееся основным атомом, истинно в минимальной эрбрановской модели для П. Тогда, в силу определения минимальной эрбрановской модели, оно истинно в любой эрбрановской модели для П. Допустим, однако, что A не является логическим следствием из П. Тогда множество $\Pi \cup \{\neg A\}$ выполнимо. Значит, существует эрбрановская модель для этого множества, являющаяся, очевидно, и эрбрановской моделью для П, в которой высказывание A ложно, что, как мы видели, невозможно. $\square$

Теорема 7.12. *Для запроса* $?A_1, \ldots, A_n$ *существует успешное вычисление логической программы* П *тогда и только тогда, когда в минимальной эрбрановской модели для* П *истинно высказывание*

$$\exists x_1 \ldots \exists x_k (A_1 \,\&\, \ldots \,\&\, A_n),$$

где $x_1, \ldots, x_k$ *— все переменные, входящие в формулу* $A_1 \,\&\, \ldots \,\&\, A_n$.

Доказательство. Пусть для запроса $?A_1, \ldots, A_n$ существует успешное вычисление логической программы П. Это означает, что высказывание$\exists x_1 \ldots \exists x_k (A_1 \,\&\, \ldots \,\&\, A_n)$ является логическим следствием из П.

Но тогда это высказывание истинно в любой модели для П, в частности, в минимальной эрбрановской модели для П.

Обратно, пусть высказывание $\exists x_1 \ldots \exists x_k (A_1 \,\&\, \ldots \,\&\, A_n)$ истинно в минимальной эрбрановской модели для П. Это означает, что существует такая подстановка $\sigma = \{x_1 \to h_1, \ldots, x_k \to h_k\}$, где $h_1, \ldots, h_k$ — элементы эрбрановского универсума, что в минимальной эрбрановской модели для П истинны основные атомы $A_1\sigma, \ldots, A_n\sigma$. В силу теоремы 7.11, в этом случае все эти атомы логически следуют из П. Но тогда и высказывание $\exists x_1 \ldots \exists x_k (A_1 \,\&\, \ldots \,\&\, A_n)$ логически следует из П, т. е. существует успешное вычисление для запроса $?A_1, \ldots, A_n$. □

Пусть M — некоторое множество основных атомов. Говорят, что данная логическая программа *корректна* относительно M, если значение программы П является подмножеством множества M. Программа П *полна* относительно M, если M является подмножеством значения программы П.

Если запрос имеет вид $?A_1, \ldots, A_n$, где $A_1, \ldots, A_n$ — атомы с переменными $x_1, \ldots, x_m$, то успешное вычисление означает, что высказывание $\exists x_1 \ldots \exists x_k (A_1 \,\&\, \ldots \,\&\, A_n)$ является логическим следствием из множества высказываний, составляющих программу. Однако логическое программирование позволяет получить нечто большее — значения переменных $x_1, \ldots, x_m$, при которых формула $A_1 \,\&\, \ldots \,\&\, A_n$ истинна. Для этого в ходе вычисления нужно вести так называемый *протокол связываний* данного вычисления, включающий те присваивания из наиболее общих унификаторов, строящихся на каждом шаге, которые влияют на значения переменных $x_1, \ldots, x_m$. Чтобы протокол связываний получился не очень громоздким, и из него можно было бы достаточно просто извлечь ответ, следует соблюдать такие правила. 1) Если на каком-то шаге перед применением правила резолюции необходимо переименование переменных в запросе или в процедуре, то делается переименование переменных именно в процедуре, а не в запросе. 2) Если при построении наиболее общего унификатора возможно присвоение значения переменной, входящей в запрос, или же какой-либо иной переменной, то значение присваивается именно той переменной, которая входит в запрос.

Логические программы можно использовать для вычисления числовых функций. Пусть сигнатура Ω содержит единственную константу 0 и единственный одноместный функциональный символ s. Тогда эрбрановский универсум состоит из термов $0, s(0), s(s(0)), \ldots$, которые можно отождествить с натуральными числами $0, 1, 2, \ldots$. Иными словами, в этом случае эрбрановский универсум есть в точности натуральный ряд. Пусть f — некоторая n-местная частичная функция из $\mathbf{N}$ в $\mathbf{N}$. Пусть сигнатура Ω содержит $(n+1)$-местный предикатный символ P_f, а также, возможно, другие предикатные символы. Будем говорить, что логическая программа П в языке сигнатуры Ω *вычисляет* функцию f, если, каковы бы ни были натуральные числа $k_1, \ldots, k_n, k$, основной атом $P_f(k_1, \ldots, k_n, k)$ принадлежит значению программы П тогда и только тогда, когда $f(k_1, \ldots, k_n) = k$.

Логическая программа, вычисляющая функцию f, позволяет решать различные задачи, касающиеся функции f. Во-первых, она позволяет убедиться в истинности равенства вида $f(k_1, \ldots, k_n) = k$ для конкретных натуральных чисел $k_1, \ldots, k_n, k$. Для этого достаточно указать запрос $?P_f(k_1, \ldots, k_n, k)$. В этом случае успешное вычисление означает справедливость проверяемого равенства. Во-вторых, логическая программа позволяет вычислить значение $f(k_1, \ldots, k_n)$ для конкретных натуральных чисел $k_1, \ldots, k_n$. Для этого достаточно указать запрос $?P_f(k_1, \ldots, k_n, x)$. В этом случае успешное вычисление означает, что значение $f(k_1, \ldots, k_n)$ определено, а полученное из протокола связываний значение переменной x есть искомое значение функции f. В-третьих, программа позволяет решать уравнения вида $f(t_1, \ldots, t_n) = t$, где каждый из термов $t_1, \ldots, t_n, t$ есть либо переменная, либо конкретное натуральное число. Для этого достаточно указать запрос $?P_f(t_1, \ldots, t_n, t)$. В этом случае успешное вычисление означает, что уравнение имеет решение, а полученные из протокола связываний значения переменных дают искомое решение. Очевидно, что если функция вычисляется некоторой логической программой, то она вычислима в интуитивном смысле, следовательно, в силу тезиса Чёрча, является частично-рекурсивной.

Теорема 7.13. *Для любой частично-рекурсивной функции существует вычисляющая ее логическая программа.*

Доказательство. Всякая частично-рекурсивная функция может быть получена из базисных функций $s(x) = x + 1$, $o(x) = 0$, $I_m^n(x_1, \ldots, x_n) = x_m$ $(1 \le m \le n)$ с помощью операций подстановки, рекурсии и минимизации. Поэтому для доказательства теоремы достаточно написать логические программы для вычисления базисных функций и показать, как получить логическую программу для вычисления функции, полученной из некоторых данных функций с помощью операции подстановки, рекурсии или минимизации, если имеются логические протраммы для вычисления данных функций.

Функция s вычисляется следующей логической программой Π_s:

$$P_s(x, s(x)) \leftarrow .$$

Нетрудно убедиться, что в минимальной эрбрановской модели для этой программы истинны все основные атомы вида $P_s(n, n+1)$ и только они.

Функция o вычисляется следующей логической программой:

$$P_o(x, 0) \leftarrow .$$

Функция $I_m^n(x_1, \ldots, x_n) = x_m$ $(1 \leq m \leq n)$ вычисляется следующей логической программой:

$$P_{I_m^n}(x_1, \ldots, x_n, x_m) \leftarrow .$$

Пусть n-местная $(n \geq 1)$ частичная функция h получается с помощью операции подстановки из k-местной функции f и n-местных функций $g_1, \ldots, g_k$, т. е. для любых $x_1, \ldots, x_n \in \mathbf{N}$ имеет место условное равенство

$$h(x_1, \ldots, x_n) \simeq f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n)),$$

и пусть имеются логические программы $\Pi_f, \Pi_{g_1}, \ldots, \Pi_{g_k}$, вычисляющие соответственно функции $f, g_1, \ldots, g_k$. Тогда функция h вычисляется следующей программой:

$$\begin{cases} \Pi_f \\ \Pi_{g_1} \\ \ldots \\ \Pi_{g_k} \\ P_h(x_1, \ldots, x_n, y) \leftarrow P_{g_1}(x_1, \ldots, x_n, y_1), \ldots, P_{g_k}(x_1, \ldots, x_n, y_k), P_f(y_1, \ldots, y_k) \end{cases}$$

Пусть $(n+1)$-местная $(n \geq 1)$ частичная функция h получается с помощью операции рекурсии из n-местной функции f и $(n+2)$-местной функции g, т. е. для любых $x_1, \ldots, x_n, y \in \mathbf{N}$ выполняются следующие условные равенства:

$$h(x_1, \ldots, x_n, 0) \simeq f(x_1, \ldots, x_n);$$

$$h(x_1, \ldots, x_n, y+1) \simeq g(x_1, \ldots, x_n, y, h(x_1, \ldots, x_n, y)),$$

и пусть имеются логические программы Π_f и Π_g, вычисляющие соответственно функции f и g. Тогда функция h вычисляется следующей программой:

$$\begin{cases} \Pi_f \\ \Pi_g \\ P_h(x_1, \ldots, x_n, 0, z) \leftarrow P_f(x_1, \ldots, x_n, z) \\ P_h(x_1, \ldots, x_n, s(y), z) \leftarrow P_h(x_1, \ldots, x_n, y, u), P_g(x_1, \ldots, x_n, y, u, z) \end{cases}$$

Вот как, например, выглядит логическая программа Π_+ для вычисления сложения:

$$\begin{cases} P_+(x, 0, x) \leftarrow \\ P_+(x, s(y), s(z)) \leftarrow P_+(x, y, z) \end{cases}$$

А вот логическая программа $\Pi_\times$ для вычисления умножения:

$$\begin{cases} \Pi_+ \\ P_\times(x, 0, 0) \leftarrow \\ P_\times(x, s(y), z) \leftarrow P_\times(x, y, v), P_+(x, v, z) \end{cases}$$

Пусть n-местная $(n \geq 1)$ частичная функция g получается с помощью операции минимизации (или *μ-оператора*) из $(n+1)$-местной частичной функции f, т. е. для любых $x_1, \ldots, x_n, y \in \mathbf{N}$ значение $g(x_1, \ldots, x_n)$ определено и равно y тогда и только тогда, когда для любого $z < y$ значение $f(x_1, \ldots, x_n, z)$ определено и не равно 0, а $f(x_1, \ldots, x_n, y) = 0$, и пусть имеется логическая программа Π_f, вычисляющая функцию f. Тогда функция g вычисляется следующей программой:

$$\begin{cases} \Pi_f \\ \Pi_\times \\ Q(x_1, \ldots, x_n, 0, s(0)) \leftarrow \\ Q(x_1, \ldots, x_n, s(y), z) \leftarrow Q(x_1, \ldots, x_n, y, u), P_f(x_1, \ldots, x_n, y, v), P_\times(u, v, z) \\ P_g(x_1, \ldots, x_n, z) \leftarrow Q(x_1, \ldots, x_n, s(z), 0), Q(x_1, \ldots, x_n, z, s(v)) \end{cases}$$

Задачи

1) С помощью программы Π_+:

   а) проверить справедливость факта 2+2=4;

   б) вычислить сумму 1+3;

   в) решить уравнение $x + x = 4$;

   г) решить уравнение $x + y = 3$.

2) С помощью программы $\Pi_\times$:

   а) проверить справедливость факта $2 \times 2 = 4$;

   б) вычислить произведение 2×2;

   в) решить уравнение $x^2 = 4$;

   г) решить уравнение $x \times y = 3$.

3) Написать логические программы для вычисления следующих функций:

   а) $f(x, y) = x^y$ (здесь $0^0 = 1$);

   б) $f(x) = x!$ (здесь $0! = 1$);

   в) $\mathrm{sg}(x) = \begin{cases} 1, \text{ если } x > 0; \\ 0, \text{ если } x = 0; \end{cases}$

   г) $\overline{\mathrm{sg}}(x) = \begin{cases} 0, \text{ если } x > 0; \\ 1, \text{ если } x = 0; \end{cases}$

   д) $p(x) = \begin{cases} x - 1, \text{ если } x > 0; \\ 0, \text{ если } x = 0; \end{cases}$

   е) $d(x) = \begin{cases} x - y, \text{ если } x \geq y; \\ 0, \text{ если } x < y; \end{cases}$

   ж) $|x - y|$;

   з) $\max(x, y)$;

   и) $\min(x, y)$;

   к) $x - y$;

   л) $\frac{x}{y}$;

   м) $\sqrt[y]{x}$;

   н) $\frac{x}{2}$;

   о) $\left[\frac{x}{2}\right]$.

8. Интуиционистская логика

8.1. Что такое интуиционизм

Из теорем о корректности и полноте исчисления высказываний вытекает, что пропозициональная формула выводима в исчислении высказываний тогда и только тогда, когда она является тавтологией. Таким образом, может показаться излишним использование исчисления высказываний для описания логических законов. Однако это не совсем так. Во-первых, логические законы не исчерпываются законами логики высказываний, и, скажем, описание законов логики предикатов в виде исчисления представляется единственно возможным. Во-вторых, наряду с изучаемой нами классической логикой возможны другие, неклассические логические системы, и здесь обычно логические принципы, приемлемые с рассматриваемой точки зрения, описываются с помощью подходящего исчисления, и лишь затем ставится вопрос о возможности распознавания этих принципов среди логических формул. В качестве иллюстрации познакомимся с интуиционистской логикой.

Обнаружение парадоксов в теории множеств вызвало интерес математиков к поискам причин их возникновения. В 1908 г. появилась работа голландского математика Брауэра «Недостоверность логических принципов». В ней отмечалось, что принципы классической логики, дошедшие до нас от Аристотеля (4-й век до н. э.), абстрагированы от обращения с конечными совокупностями. Забывая об этом, впоследствии эту логику ошибочно приняли за нечто первичное по отношению к математике и в конце концов стали применять ее без какого-либо оправдания к математике бесконечных множеств. Однако не все принципы, истинные при рассмотрении конечных множеств, переносятся на бесконечные. Например, «Целое больше любой собственной части» или «Во всяком множестве натуральных чисел имеется наибольшее число».

Принципом классической логики, который Брауэр не принимает для бесконечных множеств, является закон исключенного третьего: «Для любого высказывания Ф, либо Ф, либо не Ф». Пусть Ф есть высказывание «Существует элемент множества D, обладающий свойством P», причем свойство P таково, что для любого элемента из D мы можем определить, обладает ли он свойством P. Тогда «не Ф» эквивалентно утверждению «Каждый элемент из D не обладает свойством P». Если D — конечное множество, то в принципе можно обследовать по очереди все его элементы и либо найти элемент, обладающий свойством P, либо убедиться, что все элементы не обладают свойством P, так что в этом случае справедлив закон исключенного третьего. Если же D бесконечно, то принципиально невозможно закончить исследование всех его элементов. Для некоторых множеств D и свойств P мы можем найти элемент, обладающий свойством P, или, напротив, доказать посредством математического рассуждения, что каждый элемент множества D не обладает свойством P (как, например, с помощью известного рассуждения доказывается, что не существует таких натуральных чисел m и n, что $m^2 = 2n^2$). Однако нет никакой уверенности в существовании такого решения вопроса об истинности утверждения Ф в общем случае. Правда, можно было бы считать, что всякая проблема разрешима «в принципе», но это означало бы привлечение философских допущений, что в математике делать не принято.

В отличие от традиционной, классической логики, Брауэр и его последователи развивали другую логику, получившую название *интуиционистской*. Это название обусловлено тем, что в качестве единственного критерия истинности в математике Брауэр провозгласил интуицию. При этом брауэровскую интуицию не следует понимать в каком-то «мистическом» смысле. Согласно концепции Брауэра, математические объекты рождены человеческой мыслью, поэтому истинность суждений о них полностью определяется представлениями об этих объектах того математика, в сознании которого возникли эти объекты. Строго говоря, с точки зрения интуиционизма, сколько математиков — столько и математик. Однако в силу некоторых общих свойств человеческого мышления возможно образование в сознании разных людей сходных математических понятий. К ним относится, например, понятие *натурального числа*. Отправляясь от этого понятия, на основе интуиционистских представлений Брауэром и его школой была развита своеобразная математическая теория.

С точки зрения интуиционизма, как конструирование математических объектов, так и рассуждения о них должны подчиняться критерию интуитивной ясности и убедительности. В конкретных математических построениях интуиционизм проявляется прежде всего в отказе от рассмотрения бесконечной совокупности как актуально данной в завершенном виде. В интуиционистской математике бесконечность рассматривается лишь как становящаяся, или *потенциальная*. Как писал Г. Вейль, «Брауэр открыл нам глаза и показал, как далеко классическая математика, вскормленная превосходящей всякую человеческую способность реализации верой в "абсолютное", идет дальше таких утверждений, которые могут претендовать на реальный смысл и истинность, основанную на доказательствах».

В качестве примера реализации интуиционистской программы в математике рассмотрим интуиционистское построение теории действительных чисел. Как уже отмечалось выше, понятие натурального числа считается интуитивно ясным. Натуральный ряд в интуиционисткой математике рассматривается не как

завершенная совокупность, а как процесс последовательного построения натуральных чисел, начиная с 1. На каждом шаге построения мы можем остановиться, чтобы исследовать полученное на этом шаге число на предмет того, обладает ли оно некоторым определенным свойством. Такой взгляд на натуральный ряд делает возможным доказательство утверждений о натуральных числах методом индукции. Действительно, пусть $P(x)$ — такое свойство натуральных чисел, что $P(1)$ истинно, и с помощью некоторого рассуждения мы можем заключить, что для любого n из истинности $P(n)$ следует истинность $P(n')$, где n' — число, построенное на следующем шаге после n. Теперь, если m — произвольное натуральное число, мы знаем, что в процессе построения чисел от 1 до m на каждом шаге сохраняется свойство P, следовательно, $P(m)$ истинно. Процесс построения натуральных чисел можно фиксировать в некоторой материальной форме. Например, с каждым шагом построения мы можем связывать палочку I на бумаге. Тогда слово I будет отождествляться с числом 1, слово II — с числом 2, и т. д. Такое представление натуральных чисел помогает сравнивать числа, построенные разными людьми в разное время, при помощи простого наблюдения.

Не представляет труда построение *целых* и *рациональных чисел*. Отрицательные целые числа можно отождествлять, например, со словами вида $-n$, где n — изображение натурального числа, число 0 можно отождествить с пустым словом. Нетрудно, с помощью подходящих алгоритмов над словами, определить операции сложения и вычитания целых чисел. Рациональные числа можно отождествить с несократимыми дробями вида m/n, где m — целое, а n — натуральное число. Опять же алгоритмически определяются арифметические операции на рациональных числах. Теперь можно, например, подражая классической теории, строить интуиционистскую теорию действительных чисел. Пусть задано некоторое правило последовательного построения рациональных чисел: на первом шаге строится рациональное число r_1, на втором — число r_2, и т. д. В таком случае будем говорить, что дана *последовательность* r_n. Такая последовательность называется *фундаментальной*, если для каждого натурального числа k мы можем найти натуральное число n_0 такое, что для всех $m, n \geq n_0$ выполняется неравенство $|r_n - r_m| \leq \frac{1}{k}$. Например, последовательность $r_n = \frac{1}{2^n}$ является фундаментальной последовательностью. Действительно, для любого данного k в качестве n_0 можно взять наименьшее число n такое, что $2^n \geq k$. Рассмотрим последовательность q_n, определяемую следующим образом: если n-й знак после запятой в десятичном разложении числа π есть 9 первого вхождения последовательности 0123456789 в это разложение, то $q_n = 1$; в противном случае $q_n = \frac{1}{2^n}$. Очевидно, что последовательность q_n отличается от последовательности r_n не более чем одним членом, но пока мы не знаем, встречается ли последовательность 0123456789 в десятичном разложении числа π, мы не можем найти такое n_0, что для всех $m, n \geq n_0$ выполняется неравенство $|q_n - q_m| \leq \frac{1}{2}$. Следовательно, мы не имеем права утверждать, что последовательность q_n является фундаментальной.

Фундаментальная последовательность рациональных чисел называется *действительным числовым генератором*. Будем считать, что два действительных числовых генератора $a = a_n$ и $b = b_n$ совпадают, и писать $a = b$, если для любого натурального k мы можем найти такое n_0, что для всех $n \geq n_0$ выполняется неравенство $|a_n - b_n| \leq \frac{1}{k}$. Нетрудно проверить, что отношение совпадения между действительными числовыми генераторами является рефлексивным, симметричным и транзитивным. Теперь можно определить интуиционистское действительное число как класс эквивалентности по отношению совпадения. В связи с этим уместно коснуться интуиционистских взглядов на понятие множества. Для интуициониста приемлемы следующие два способа определения множества: 1) посредством задания способа порождения его элементов; 2) посредством указания свойства, которое характеризует элементы множества. Во втором случае соответствующее свойство называется *видом*, а всякий объект, обладающий этим свойством, называется *членом* данного вида. Очевидно, можно рассматривать вид, состоящий в совпадении действительного числового генератора с данным действительным числовым генератором. Такой вид называется *действительным числом*, а всякий его член — представителем этого действительного числа.

8.2. Интуиционистский смысл логических понятий

В интуиционистской математике умозаключения не производятся по заранее установленным правилам, т. е. не фиксируется какая-либо априорная логическая система. Убедительность каждого логического шага должна проверяться непосредственно в соответствии с интуицией. При этом несколько иной, чем в традиционной, классической логике, смысл интуиционисты придают исходным логическим понятиям. Так, в традиционной логике высказывание понимается как такое предложение, которое может быть истинным или ложным, так что истинностное значение есть непременный атрибут всякого высказывания. Интуиционистский взгляд на истинность высказывания представляется более трезвым и соответствующим математической практике. С точки зрения интуиционизма, истинность высказывания связана с возможностью его *доказательства*. Таким образом, высказывание считается истинным, если имеется его доказательство. В этом контексте понимаются и традиционные логические операции над высказываниями. Так, высказывание $\Phi \,\&\, \Psi$ считается истинным тогда и только тогда, когда истинны оба высказывания Φ и Ψ, т. е. мы

располагаем доказательством каждого из этих высказываний. Высказывание $\Phi \vee \Psi$ считается истинным тогда и только тогда, когда истинно хотя бы одно из высказываний Φ и Ψ, т. е. мы располагаем доказательством высказывания Φ или доказательством высказывания Ψ. Высказывание $\Phi \supset \Psi$ считается истинным тогда и только тогда, когда имеется некий общий метод, позволяющий любое доказательство высказывания Φ преобразовать в доказательство высказывания Ψ. Отрицание $\neg\Phi$ высказывания Φ считается истинным, если истинно высказывание $\Phi \supset \bot$, где $\bot$ — некоторое заведомо абсурдное высказывание (например, $0 = 1$). Пусть $\Phi(x)$ — некоторое свойство, которым могут обладать или не обладать объекты подходящим образом заданного множества. Тогда высказывание $\exists x \Phi(x)$ считается истинным, если для некоторого конкретного объекта a из рассматриваемого множества мы имеем доказательство высказывания $\Phi(a)$. Наконец, высказывание $\forall x \Phi(x)$ считается истинным, если имеется общий метод, позволяющий для любого конкретного объекта a из рассматриваемого множества получить доказательство высказывания $\Phi(a)$.

Понятие ложного высказывания не является самостоятельным в интуиционисткой логике: высказывание Φ считается ложным, если нам удалось доказать высказывание $\neg\Phi$. Таким образом, в отличие от классической логики, где каждое высказывание либо истинно, либо ложно, в интуиционистской логике высказывания подразделяются на три класса: истинные, ложные и все прочие, или *непроверенные*, при этом только принадлежность высказывания к одному из первых двух классов является окончательной, а всякое непроверенное высказывание с течением времени в результате исследовательской деятельности человека может перейти в разряд истинных (если удастся доказать его) или в разряд ложных (если удастся его опровергнуть, т. е. доказать истинность отрицания этого высказывания).

Мы видим, что интуиционистское понимание некоторых видов высказываний существенно отличается от классического. Пусть, например, высказывание имеет вид $\Phi \vee \neg\Phi$. Если Φ — истинное высказывание, например, 0=0, то высказывание $\Phi \vee \neg\Phi$ также истинно. Аналогично, высказывание $\Phi \vee \neg\Phi$ истинно, если Φ — ложное высказывание, например, 0=1. Если же Φ — непроверенное высказывание (такое высказывание нетрудно найти в современной научной литературе, где формулируются нерешенные математические проблемы), то мы не можем утверждать, что высказывание $\Phi \vee \neg\Phi$ истинно. Но с классической точки зрения это высказывание истинно, правда, единственным аргументом здесь является тезис, что такое высказывание «истинно всегда».

Рассмотрим еще один хрестоматийный пример математического доказательства, которое неприемлемо с интуиционистской точки зрения.

Теорема 8.1. *Существуют иррациональные числа a и b такие, что число a^b рационально.*

Доказательство. Рассмотрим число $\sqrt{2}^{\sqrt{2}}$. Если это число рационально, то можно взять $a = \sqrt{2}$, $b = \sqrt{2}$. Если же число $\sqrt{2}^{\sqrt{2}}$ иррационально, можно взять $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$. Таким образом, в любом случае нужные a и b существуют. □

Это доказательство является ярким образцом доказательства «чистого существования», когда доказывается существование некоторого объекта без явного предъявления его. Такие доказательства часто встречаются в математике и даже считаются особенно изящными. Но для интуициониста, очевидно, такое доказательство неприемлемо. К счастью, для рассматриваемой теоремы имеется и другое, более глубокое доказательство, показывающее, что число $\sqrt{2}^{\sqrt{2}}$ иррационально, так что искомые числа таковы: $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$.

8.3. Интуиционистское исчисление высказываний

Как уже отмечалось выше, интуиционистская математика не пользуется какой-либо априорной логической системой, оправдывающей совершение того или иного шага в рассуждениях. Единственным критерием правильности рассуждения является интуитивная ясность каждого логического шага. Это, однако, не исключает существования некоторых общих логических правил, которые позволяют из данных истинных математических утверждений интуитивно ясным путем получать другие истинные утверждения. Выявление и изучение таких общих правил составляет предмет *интуиционистской логики*, являющейся важным разделом современной математической логики. Следует заметить, что, как и математическая логика в целом, интуиционистская логика занимается изучением только математических рассуждений и не претендует на возможность широкого ее применения вне математики.

Одним из естественных путей построения интуиционистской логики является критический анализ классической логики и выявление тех ее принципов, которые приемлемы итуиционистски.

Первая попытка построения системы аксиом интуиционистской логики была предпринята А. Н. Колмогоровым в 1925 г. Он исходил из предложенной Гильбертом в 1923 г. системы классической логики, состоящей из следующих схем аксиом:

Г1. $A \supset (B \supset A)$;
Г2. $(A \supset (A \supset B)) \supset (A \supset B)$;
Г3. $(A \supset (B \supset C)) \supset (B \supset (A \supset C))$;
Г4. $(B \supset C) \supset ((A \supset B) \supset (A \supset C))$;
Г5. $A \supset (\neg A \supset B)$;
Г6. $(A \supset B) \supset ((\neg A \supset B) \supset B)$.

Другие законы классической логики высказываний могут быть получены из аксиом с помощью правила modus ponens. Исчисление, задаваемое схемами аксиом Г1 – Г6 вместе с правилом вывода modus ponens, будем называть *исчислением Гильберта*. Подвергая эту систему аксиом критическому анализу с интуиционистской точки зрения, А. Н. Колмогоров приходит к системе аксиом интуиционистской логики, состоящей из схем аксиом Г1 – Г4 исчисления Гильберта, а также следующей схемы аксиом:

$$(A \supset B) \supset ((A \supset \neg B) \supset \neg A).$$

Таким образом, пропозициональное *исчисление Колмогорова* имеет следующие схемы аксиом:
К1. $A \supset (B \supset A)$;
К2. $(A \supset (A \supset B)) \supset (A \supset B)$;
К3. $(A \supset (B \supset C)) \supset (B \supset (A \supset C))$;
К4. $(B \supset C) \supset ((A \supset B) \supset (A \supset C))$;
К5. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$.

Единственным правилом вывода является modus ponens.

Исчисление Колмогорова является исторически первой аксиоматизацией интуиционистской логики высказываний. Позднее другие системы аксиом интуиционистской логики (с более широким запасом выводимых формул) были предложены В. И. Гливенко (1929 г.), Гейтингом (1930 г.), Генценом (1935 г.). Все они эквивалентны между собой в том смысле, что из них выводимы одни и те же логические принципы, и эквивалентны следующей системе аксиом:

ИИВ1. $A \supset (B \supset A)$;
ИИВ2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;
ИИВ3. $A \,\&\, B \supset A$;
ИИВ4. $A \,\&\, B \supset B$;
ИИВ5. $A \supset (B \supset A \,\&\, B)$;
ИИВ6. $A \supset A \vee B$;
ИИВ7. $B \supset A \vee B$;
ИИВ8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
ИИВ9. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;
ИИВ10. $A \supset (\neg A \supset B)$.

Эти схемы аксиом вместе с правилом modus ponens задают *интуиционистское исчисление высказываний*.

Юхансон (1937 г.) ввел в рассмотрение исчисление, задаваемое схемами аксиом ИИ1 – ИИ9, и назвал его *минимальным исчислением*. Если из минимального исчисления исключить аксиому ИИ9, то получится так называемое *позитивное исчисление*, расмотренное Гильбертом и Бернайсом (1934 г.).

Так как в интуиционистском, минимальном и позитивном исчислениях среди схем аксиом есть схемы ИИ1 и ИИ2, а единственным правилом вывода является modus ponens, то, в силу следствия 4.2, для каждого из этих исчислений верна теорема о дедукции: каковы бы ни были множество формул Γ и формулы A, B, если $\Gamma \cup \{A\} \vdash B$, то $\Gamma \vdash A \supset B$. Так как среди схем аксиом интуиционистского и минимального исчислений есть схема ИИ9, то, в силу следствия 4.3, для этих исчислений верен принцип приведения к абсурду: если из множества формул $\Gamma \cup \{A\}$ выводимо противоречие, т. е. $\Gamma \cup \{A\} \vdash B$ и $\Gamma \cup \{A\} \vdash \neg B$ для некоторой формулы B, то $\Gamma \vdash \neg A$.

Соотношение между исчислением Колмогорова и минимальным исчислением выражается следующей теоремой.

Теорема 8.2. *1) Всякая формула, выводимая в исчислении Колмогорова, выводима и в минимальном исчислении. 2) Всякая формула, содержащая только логические связки $\supset$ и $\neg$ и выводимая в минимальном исчислении, выводима и в исчислении Колмогорова.*

Таким образом, можно сказать, что исчисление Колмогорова — это импликативно-негативный фрагмент минимального исчисления.

Задачи

Доказать, что следующие формулы выводимы в интуиционистском исчислении высказываний:

1) $A \supset \neg\neg A$;

2) $\neg\neg\neg A \supset \neg A$;

3) $(A \supset B) \supset (\neg B \supset \neg A)$;

4) $\neg(A \vee B) \supset (\neg A \,\&\, \neg B)$;

5) $A \,\&\, B \supset \neg(A \supset \neg B)$;

6) $A \supset B \supset \neg(A \,\&\, \neg B)$;

7) $\neg(A\& \neg A)$;

8) $A \supset (\neg B \supset \neg(A \supset B))$.

9) $A \vee B \,\&\, C \supset (A \vee B) \,\&\, (A \vee C)$;

10) $(A \supset B) \supset ((C \supset A) \supset (C \supset B))$;

11) $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$;

12) $(A \supset B) \supset ((C \vee A) \supset (C \vee B))$;

13) $(A \supset B) \supset ((C \,\&\, A) \supset (C \,\&\, B))$;

14) $\neg A \vee B \supset (A \supset B)$.

8.4. Логические матрицы

Логической матрицей назовем набор $\mathbf{M} = \langle M, 1, \cdot, +, \to, \sim\rangle$, где M — непустое множество (*носитель* матрицы $\mathbf{M}$), $1 \in M$, $\sim$ — одноместная, а $\cdot$, $+$, $\to$ — двуместные операции на M, причем для любых элементов $x, y \in M$ выполняются условия:

- если $1 \to x = 1$, то $x = 1$;
- если $x \to y = y \to x = 1$, то $x = y$.

В дальнейшем элементы множества M мы будем называть *элементами логической матрицы* $\mathbf{M}$ и иногда будем писать $x \in \mathbf{M}$ вместо $x \in M$.

Оценкой в логической матрице $\mathbf{M}$ называется произвольная функция, которая каждой пропозициональной переменной сопоставляет некоторый элемент из множества M. Всякую оценку f можно продолжить на множество всех пропозициональных формул, положив

$$f(A \,\&\, B) = f(A) \cdot f(B);$$

$$f(A \vee B) = f(A) + f(B);$$

$$f(A \supset B) = f(A) \to f(B);$$

$$f(\neg A) - \sim f(A).$$

Будем говорить, что формула A *истинна* в логической матрице $\mathbf{M}$, если $f(A) = 1$, какова бы ни была оценка f в $\mathbf{M}$. В этом случае логическая матрица $\mathbf{M}$ называется *моделью* пропозициональной формулы A. Если же для некоторой оценки f имеет место $f(A) \neq 1$, то говорят, что формула A *опровергается* в матрице $\mathbf{M}$, а матрица $\mathbf{M}$ называется *контрмоделью* для этой формулы.

Логическая матрица $\mathbf{M}$ называется моделью данного пропозиционального исчисления, если все формулы, выводимые в этом исчислении, истинны в матрице $\mathbf{M}$. Логическая матрица называется *точной моделью* данного исчисления, если в этом исчислении выводимы те и только те формулы, которые истинны в этой матрице.

Теорема 8.3. *Пусть пропозициональное исчисление таково, что его единственным правилом вывода является modus ponens. Тогда логическая матрица* $\mathbf{M}$ *является моделью этого исчисления, если и только если все аксиомы этого исчисления истинны в* $\mathbf{M}$.

Доказательство. Пусть логическая матрица $\mathbf{M}$ является моделью данного пропозиционального исчисления. Поскольку все аксиомы этого исчисления выводимы в нем, они истинны в $\mathbf{M}$ по определению модели. Обратно, пусть в логической матрице $\mathbf{M}$ истинны все аксиомы пропозиционального исчисления, в котором единственным правилом вывода является modus ponens, и пусть $A_1, \ldots, A_n$ — некоторый вывод в этом исчислении. Индукцией по i докажем, что для любого $i = 1, \ldots, n$ формула A_i истинна в матрице $\mathbf{M}$. При $i = 1$ формула A_i является аксиомой и истинна в $\mathbf{M}$ по условию. Пусть для некоторого $k \leq n$ каждая из формул A_i при $i < k$ истинна в $\mathbf{M}$. Докажем, что формула A_k также истинна в $\mathbf{M}$. Если формула A_k является аксиомой, то она истинна в $\mathbf{M}$ по условию. Если же A_k получена по правилу modus ponens из формул A_l и A_m, где $l, m < k$, причем A_m имеет вид $A_l \supset A_k$, то, по индуктивному предположению, для любой оценки f имеет место $f(A_l) = 1$ и $f(A_m) = f(A_l) \to f(A_k) = 1 \to f(A_k) = 1$. Отсюда и из определения логической матрицы следует, что $f(A_k) = 1$ для любой оценки f, т. е. формула A_k истинна в матрице $\mathbf{M}$. Таким образом, любая формула, выводимая в данном исчислении, истинна в матрице $\mathbf{M}$. Значит, $\mathbf{M}$ является моделью этого исчисления. □

Моделью интуиционистского исчисления высказываний является, например, логическая матрица

$$\mathbf{M}_1 = \langle \{0, \frac{1}{2}, 1\}, \cdot, +, \to, \sim \rangle,$$

где $x \cdot y = \min(x, y)$; $x + y = \max(x, y)$; $x \to y = \begin{cases} 1, & \text{если } x \leq y, \\ y, & \text{если } x > y; \end{cases}$ $\sim x = x \to 0 = \begin{cases} 1, & \text{если } x = 0, \\ 0, & \text{если } x \neq 0. \end{cases}$

Теорема 8.4. *Формула* $(A \supset B) \supset ((\neg A \supset B) \supset B)$ *невыводима в интуиционистском исчислении высказываний.*

Доказательство. Рассмотрим такую оценку f в $\mathbf{M}_1$, что $f(A) = f(B) = \frac{1}{2}$. Вычисления показывают, что значение рассматриваемой формулы при этой оценке равно $\frac{1}{2}$, следовательно, эта формула не истинна в модели $\mathbf{M}_1$ интуиционистского исчисления высказываний и потому невыводима в этом исчислении. □

Теорема 8.5. *Формула* $(A \supset B) \supset ((\neg A \supset B) \supset B)$ *невыводима в исчислении Колмогорова.*

Доказательство. Утверждение следует из теоремы 8.4 и того факта, что всякая формула, выводимая в исчислении Колмогорова, выводима и в интуиционистском исчислении высказываний. □

Таким образом, аксиома Г6 исчисления Гильберта невыводима в исчислении Колмогорова.

Заметим также, что при такой оценке f в $\mathbf{M}_1$, что $f(A) = \frac{1}{2}$, $f(B) = 1$, формула $(\neg A \supset \neg B) \supset (B \supset A)$ принимает значение $\frac{1}{2}$; при таких оценках формулы $A \vee \neg A$ и $\neg\neg A \supset A$ также принимают значение $\frac{1}{2}$. Значит, все эти формулы также невыводимы в интуиционистском исчислении высказываний, а следовательно, и в исчислении Колмогорова.

Вот еще один пример модели интуиционистского исчисления высказываний:

$$\mathbf{M}_2 = \langle \{0, 1\}^2 \cup \{1\}, 1, \cdot, +, \to, \sim \rangle,$$

где $1 \cdot a = a \cdot 1 = a$; $1 + a = a + 1 = 1$; $1 \to a = a$; $a \to 1 = 1$; $\sim 1 = \langle 0, 0 \rangle$ (здесь a — произвольный элемент матрицы $\mathbf{M}_2$), а операции над элементами вида $\langle a, b \rangle$, где $a, b \in \{0, 1\}$, определяются так:

$$\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle = \langle \min(a_1, a_2), \min(b_1, b_2) \rangle;$$

$$\langle a_1, b_1 \rangle + \langle a_2, b_2 \rangle = \langle \max(a_1, a_2), \max(b_1, b_2) \rangle;$$

$$\sim \langle a, b \rangle = \begin{cases} 1, & \text{если } a = b = 0, \\ \langle 1 - a, 1 - b \rangle, & \text{если } a \neq 0 \text{ или } b \neq 0; \end{cases}$$

$$\langle a_1, b_1 \rangle \to \langle a_2, b_2 \rangle = \gamma(\sim \langle a_1, b_1 \rangle + \langle a_2, b_2 \rangle),$$

где $\gamma(x) = \begin{cases} 1, & \text{если } x = \langle 1, 1 \rangle, \\ x & \text{если } x \neq \langle 1, 1 \rangle. \end{cases}$

Нетрудно проверить, например, что если $f(A) = \langle 0, 1 \rangle$, то при такой оценке f формула $\neg A \vee \neg\neg A$ принимает значение $\langle 1, 1 \rangle$. Значит, она не истинна в модели $\mathbf{M}_2$ интуиционистского исчисления высказываний и невыводима в этом исчислении (а потому и в исчислении Колмогорова).

Задачи

Доказать, что следующие формулы невыводимы в интуиционистском исчислении высказываний:

1) $P \vee (P \supset Q)$;

2) $(P \supset Q) \vee (Q \supset P)$;

3) $(P \supset Q) \supset \neg P \vee Q$;

4) $\neg(P \,\&\, Q) \supset (\neg P \vee \neg Q)$;

5) $\neg(P \supset Q) \supset P \,\&\, \neg Q$.

8.5. Модели Крипке для логики высказываний

Модель Крипке для логики высказываний — это набор $\mathcal{K} = (K, \preceq, \models)$, где $(K, \preceq)$ — частично упорядоченное множество (т. е. отношение $\preceq$ на множестве K рефлексивно, антисимметрично и транзитивно), называемое *шкалой Крипке*, а $\models$ — некоторое соответствие между множеством K и множеством всех пропозициональных переменных, обладающее тем свойством, что если $\alpha, \beta \in K$, P — переменная, $\alpha \models P$ и $\alpha \preceq \beta$, то $\beta \models P$. Соответствие $\models$ называется *оценкой*. Модель Крипке $\mathcal{K} = (K, \preceq, \models)$ называется конечной, если конечно множество K.

Интуитивный смысл моделей Крипке соответствует интуиционистским представлениям о становящемся характере истинности высказывания. А именно, элементы множества K можно трактовать как «моменты времени», причем $\alpha \preceq \beta$ для $\alpha, \beta \in K$ означает, что момент α предшествует моменту β. При этом моменты времени можно понимать не в «физическом» смысле, а, так сказать, в «логическом»: каждый момент времени характеризуется состоянием знаний в этот момент. Поэтому и шкала Крипке («временна́я шкала»), вообще говоря, не является линейно упорядоченным множеством, ибо в будущем развитие знаний может пойти разными путями. $\alpha \models P$ читается «α вынуждает P» или «P истинно в момент α». Интуитивно, $\alpha \models P$ означает, что в момент α утверждение P является доказанным, а то условие, что если $\alpha \models P$ и $\alpha \preceq \beta$, то $\beta \models P$, выражает так называемый *принцип сохранения истинности*: то, что истинно в данный момент, остается истинным всегда в будущем.

На основе соответствия $\models$ определяется соответствие между множеством K и множеством всех пропозициональных формул, обозначаемое тем же символом $\models$. Это соответствие задается индукцией по построению формулы. Для переменных оно уже определено. Далее полагаем:

- $\alpha \models (A \,\&\, B) \rightleftharpoons [\alpha \models A$ и $\alpha \models B]$;
- $\alpha \models (A \vee B) \rightleftharpoons [\alpha \models A$ или $\alpha \models B]$;
- $\alpha \models (A \supset B) \rightleftharpoons (\forall \beta \succeq \alpha)[\beta \not\models A$ или $\beta \models B]$;
- $\alpha \models \neg A \rightleftharpoons (\forall \beta \succeq \alpha)\beta \not\models A$.

Нетрудно доказать, что принцип сохранения истинности остается верным и для формул: если $\alpha \models A$ и $\alpha \preceq \beta$, то $\beta \models B$.

Говорят, что формула A истинна в модели Крипке $\mathcal{K} = (K, \preceq, \models)$ и пишут $\mathcal{K} \models A$, если для любого $\alpha \in K$ имеет место $\alpha \models A$. Если формула A не истинна в модели Крипке $\mathcal{K}$, т. е. $\mathcal{K} \not\models A$, то $\mathcal{K}$ называют контромоделью для A. Имеет место следующая теорема о корректности и полноте интуиционистского исчисления высказываний относительно моделей Крипке:

Теорема 8.6. *Пропозициональная формула выводима в интуиционистском исчислении высказываний тогда и только тогда, когда она истинна в любой конечной модели Крипке.*

Таким образом, для любой пропозициональной формулы A можно либо построить ее вывод в интуиционистском исчислении высказываний, либо найти контрмодель для A.

Пример. Докажем, что формула $P \vee \neg P$ невыводима в интуиционистском исчислении высказываний, построив для нее контрмодель Крипке. Пусть $K = \{\alpha, \beta\}$, причем $\alpha \preceq \alpha$, $\alpha \preceq \beta$, $\beta \preceq \beta$. Таким образом, шкала Крипке состоит из двух «моментов»: α («сегодня») и β («завтра»). Положим $\beta \models P$. Докажем, что $\alpha \not\models P \vee \neg P$. В силу определения отношения $\models$ для дизъюнкции, $\alpha \not\models P \vee \neg P$ означает, что выполняется хотя бы одно из условий: 1) $\alpha \models P$ или 2) $\alpha \models \neg P$. Условие 1), очевидно, не выполнено. Условие 2), в силу определения отношения $\models$ для отрицания, означает, что а) $\alpha \not\models P$ и б) $\beta \not\models P$. Условие а), очевидно, выполнено, а условие б) — нет. Следовательно, условие 2) также не выполнено. Таким образом, $\alpha \not\models P \vee \neg P$.

Задачи

Доказать, что следующие формулы невыводимы в интуиционистском исчислении высказываний, построив для каждой из них контрмодель Крипке:

1) $P \vee (P \supset Q)$;

2) $\neg\neg P \supset P$;

3) $(P \supset Q) \vee (Q \supset P)$;

4) $P \supset P \,\&\, (Q \vee \neg Q)$;

5) $(P \supset Q) \supset \neg P \vee Q$;

6) $(P \supset Q) \vee (P \supset \neg Q)$;

7) $((P \supset Q) \supset P) \supset P$;

8) $\neg(P \supset Q) \supset P \,\&\, \neg Q$;

9) $\neg(P \,\&\, Q) \supset (\neg P \vee \neg Q)$;

10) $(\neg P \supset \neg Q) \supset (Q \supset P)$;

11) $(\neg Q \supset \neg P) \supset ((\neg Q \supset P) \supset Q)$.

8.6. Интуиционистские элементарные языки

Классическая логика предикатов, которая рассматривалась в разделах 5 и 6, изучает рассуждения, проводимые на каком-либо элементарном языке. Представляет интерес разработка интуиционистской логики предикатов. Но для этого прежде нужно осмыслить, что такое элементарный язык с интуиционистской точки зрения.

Как мы видели в разделе 5.3, при построении элементарного языка фиксируется некоторая непустая предметная область M, а затем некоторым объектам из M, операциям и предикатам на M даются имена, и так возникают константы, функциональные и предикатные символы, составляющие сигнатуру создаваемого языка. Посмотрим на этот процесс с интуиционистской точки зрения. Конечно, нет проблем с рассмотрением какой-нибудь непустой предметной области M как множества, заданного правилом порождения его элементов или свойством, выделяющим его элементы среди элементов другого, ранее заданного множества. Не вызывает трудностей и попытка дать имена некоторым элементам предметной области M. А как трактовать понятие предиката, заданного на M?

В разделе 5.2 мы рассматривали несколько возможных вариантов понятия предиката. Во-первых, конкретный предикат можно трактовать как высказывательную форму $P(x_1, \ldots, x_n)$, записанную на неформальном, но понятном языке, и при этом с ним естественным образом связана высказывательная функция, сопоставляющая каждому набору $a_1, \ldots, a_n$ значений переменных $x_1, \ldots, x_n$ высказывание $P(a_1, \ldots, a_n)$. Такое понимание предиката вполне приемлемо с точки зрения интуиционизма. Далее, рассматривая лишь истинностные значения высказываний $P(a_1, \ldots, a_n)$, мы приходили к пониманию предиката как функции, заданной на предметной области M и принимающей значения 1 («истина») и 0 («ложь»). Этот шаг, конечно же, интуиционистски неприемлем, ибо, как мы знаем, истинностное значение не является обязательным атрибутом произвольного высказывания. Итак, мы должны остановиться на трактовке предиката как высказывательной формы, записанной на подходящем (не обязательно формальном) понятном языке.

Еще больше трудностей возникает при рассмотрении понятия произвольной операции, или функции. Мы говорим, что задана n-местная операция f на множестве M, если каждому набору $a_1, \ldots, a_n$ элементов множества M сопоставлен один определенный элемент из M, обозначаемый $f(a_1, \ldots, a_n)$. Интуиционистская трактовка такого понимания функции означает, что имеется общее правило, сопоставляющее каждому набору $a_1, \ldots, a_n$ элемент $f(a_1, \ldots, a_n)$. Иными словами, можно рассматривать только функции, для которых имеется правило для их вычисления. Ясно, что это далеко от представления о понятии произвольной функции. Гораздо более естественным является представление о функции f как о функциональном отношении, т. е. таком предикате $F(x_1, \ldots, x_n, y)$, что для любых $a_1, \ldots, a_n$ истинно высказывание $F(a_1, \ldots, a_n, f(a_1, \ldots, a_n))$. Тем самым для рассмотрения конкретной функции мы не обязаны обладать правилом для ее вычисления, а лишь должны иметь понятно сформулированное условие, связывающее значения функции и значения ее аргументов. Таким образом, понятие функции перестает быть исходным, а сводится к понятию предиката. Поэтому в рамках интуиционистской логики мы будем рассматривать лишь элементарные языки, сигнатура

которых не содержит функциональных символов. А вместо какой-либо конкретной n-местной функции f, в случае необходимости, мы можем рассматривать $(n+1)$-местный предикат $f(x_1, \ldots, x_n) = y$.

Важным моментом при рассмотрении элементарных языков является описание их семантики. Если в случае классической логики это удается сделать с помощью точного понятия алгебраической системы, то в интуиционизме дело обстоит несколько сложнее. Интуиционистская интерпретация данного элементарного языка сигнатуры Ω начинается с выбора некоторой непустой предметной области M, заданной интуиционистски приемлемым образом. Затем константам из Ω сопоставляются в качестве значений некоторые элементы из M, а предикатным символам из Ω — конкретные предикаты, т. е. высказывательные формы некоторого понятного языка с соответствующим числом параметров. После этого каждая замкнутая формула сигнатуры Ω превращается в высказывание, интуиционистсткий смысл которого определяется интуиционистстким пониманием логических связок и кванторов. Если же формула содержит свободные переменные, она превращается в высказывательную форму, интуиционистсткий смысл которой также понятен.

Приведенное описание интуиционистской семантики элементарных языков ни в коем случае нельзя считать математически строгим. Во-первых, понятие предиката не было уточнено достаточно строгим образом. Во-вторых, интуиционистский смысл логических операций и кванторов также не является математически точным. Можно сказать, что у нас есть лишь интуитивное понимание интуиционистской семантики элементарных языков. Тем не менее, таких представлений достаточно, чтобы начать разработку формальных систем интуиционистской логики предикатов.

8.7. Интуиционистское исчисление предикатов

Пусть фиксирована сигнатура Ω, содержащая лишь константы и предикатные символы. *Интуиционистское исчисление предикатов* в сигнатуре Ω задается следующими схемами аксиом:

ИИП1. $A \supset (B \supset A)$;
ИИП2. $(A \supset B) \supset ((A \supset (B \supset C)) \supset (A \supset C))$;
ИИП3. $A \,\&\, B \supset A$;
ИИП4. $A \,\&\, B \supset B$;
ИИП5. $A \supset (B \supset A \,\&\, B)$;
ИИП6. $A \supset A \vee B$;
ИИП7. $B \supset A \vee B$;
ИИП8. $(A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$;
ИИП9. $(A \supset B) \supset ((A \supset \neg B) \supset \neg A)$;
ИИП10. $A \supset (\neg A \supset B)$;
ИИП11. $\forall v A(v) \supset A(t)$;
ИИП12. $A(t) \supset \exists v A(v)$.

В схемах ИИП11 и ИИП12 $A(v)$ — произвольная формула сигнатуры Ω, v — произвольная переменная, t — терм сигнатуры Ω (т. е. переменная или константа), свободный для переменной v в формуле $A(v)$ (т. е., если t есть переменная u, то никакое свободное вхождение переменной v в формулу $A(v)$ не находится в области действия квантора по переменной u), $A(t)$ — результат подстановки терма t вместо всех свободных вхождений переменной v в формулу $A(v)$.

Правилами вывода интуиционистского исчисления предикатов являются:

(I) $\dfrac{A,\ A \supset B}{B}$ (modus ponens);

(II) $\dfrac{A \supset B}{\exists v A \supset B}$ (удаление квантора существования);

(III) $\dfrac{B \supset A}{B \supset \forall v A}$ (введение квантора всеобщности).

При этом в правилах (II) и (III) формула A не содержит свободных вхождений переменной v.

Мы видим, что интуиционистское исчисление предикатов отличается от классического исчисления предикатов, описанного в разделе 6, лишь схемой аксиом ИИП10, заменяющей закон двойного отрицания. Как и в случае классического исчисления предикатов, определяются понятия квазивывода из гипотез и вывода как такого квазивывода, в котором соблюдаются определенные ограничения на применение правил (II) и (III).

Оправданием применения эпитета «интуиционистское» к этому исчислению является следующий факт. Пусть фиксирована некоторая интерпретация данного языка первого порядка сигнатуры Ω, т. е. выбрана некоторая непустая предметная область M, константам из Ω сопоставлены в качестве значений некоторые элементы из M, а предикатным символам из Ω — конкретные предикаты на M (т. е. высказывательные формы некоторого понятного языка с соответствующим числом параметров). Тогда 1) все аксиомы интуиционистского исчисления предикатов сигнатуры Ω становятся интуиционистски истинными высказываниями или высказывательными формами, замыкания которых кванторами всеобщности по всем параметрам интуиционистски истинны в данной интерпретации; 2) правила вывода сохраняют интуиционистскую истинность.

Для схем аксиом ИИП1 – ИИП10 этот факт отмечался при рассмотрении интуиционистского исчисления высказываний, схемами аксиом которого они являются. Рассмотрим схему аксиом ИИП11. Пусть формула $A(v)$ содержит свободно лишь переменную v, а терм t есть константа c. В фиксированной интерпретации формула $A(v)$ задает конкретный одноместный предикат $P(v)$, а значением константы c является некоторый элемент m из предметной области M. В соответствии с интуиционистским пониманием импликации, истинность формулы $\forall v A(v) \supset A(t)$ в данной интерпретации означает, что существует общий метод, позволяющий любое обоснование («доказательство») высказывания $\forall v P(v)$ преобразовать в обоснование высказывания $P(m)$. Итак, пусть дано доказательство высказывания $\forall v P(v)$. В силу интуиционистского понимания квантора всеобщности, это означает, что нам дан общий метод, позволяющий для любого элемента $a \in M$ получить доказательство высказывания $P(a)$. Применим этот метод к элементу m. Тогда мы получим доказательство высказывания $P(m)$, что и требовалось. Теперь рассмотрим случай, когда формула $A(v)$ содержит свободно переменные, отличные от v, а терм t также может быть переменной u, причем никакое свободное вхождение переменной v в формулу $A(v)$ не находится в области действия квантора по переменной u. Пусть $w_1, \ldots, w_k$ — все параметры формулы $\forall v A(v) \supset A(t)$ (в частности, терм t может быть одной из переменных $w_1, \ldots, w_k$). Требуется доказать, что формула $\forall w_1 \ldots \forall w_k \forall v A(v) \supset A(t)$ интуиционистски истинна в любой интерпретации. Пусть фиксирована некоторая интерпретация сигнатуры Ω. Придадим переменным $w_1, \ldots, w_k$ произвольные значения из предметной области. Тогда формула $A(v)$ превратится в одноместный предикат $P(v)$, а значением терма t будет некоторый элемент m из предметной области. Выше был описан общий метод, позволяющий из обоснования высказывания $\forall v P(v)$ получить обоснование высказывания $P(m)$. Этот метод, очевидно, не зависит от того, какие именно значения мы придали переменным $w_1, \ldots, w_k$. Следовательно, высказывание $\forall w_1 \ldots \forall w_k \forall v A(v) \supset A(t)$ интуиционистски истинно.

Нетрудно провести аналогичные неформальные рассуждения, показывающие, что схема аксиом ИИП12 также является схемой интуиционистски истинных высказываний или тождественно истинных высказывательных форм. Правило вывода modus ponens, очевидно, сохраняет интуиционистсткую истинность. Покажем, что правило (II) (правило удаления квантора существования) также сохраняет интуиционистскую истинность. Пусть высказывание $\forall w_1 \ldots \forall w_k \forall v (A(v) \supset B)$, где $w_1, \ldots, w_k$ — все параметры формулы $A(v) \supset B$, отличные от v, интуиционистски истинно в данной интерпретации. Докажем, что высказывание $\forall w_1 \ldots \forall w_k (\exists v A \supset B)$ также истинно в этой интерпретации. Придадим переменным $w_1, \ldots, w_k$ произвольные значения $m_1, \ldots, m_k$ из предметной области. Тогда формула $A(v)$ превратится в некоторый одноместный предикат $P(v)$, а формула B — в некоторое высказывание Q. Докажем, что истинно высказывание $\exists v P(v) \supset Q$. Для этого надо описать общий метод, который позволяет из любого обоснования высказывания $\exists v P(v)$ получить обоснование высказывания Q. Итак, пусть дано обоснование высказывания $\exists v P(v)$. Это означает, что дан некоторый элемент m из предметной области и обоснование высказывания $P(m)$. В силу истинности высказывания $\forall w_1 \ldots \forall w_k \forall v (A(v) \supset B)$, можно найти обоснование высказывания $P(m) \supset Q$. Теперь, имея обоснование высказывания $P(m)$, мы получаем обоснование высказывания Q, что и требовалось. В приведенном рассуждении описанное обоснование высказывания $\exists v P(v) \supset Q$ не зависело от элементов $m_1, \ldots, m_k$, так что истинность высказывания $\forall w_1 \ldots \forall w_k (\exists v A \supset B)$ доказана.

Совершенно аналогично доказывается, что правило (III) (правило введения квантора всеобщности) сохраняет интуиционистскую истинность.

Задачи

1) Доказать, что для интуиционистского исчисления предикатов имеет место теорема о дедукции: каковы бы ни были множество формул Γ и формулы Φ, Ψ, если $\Gamma \cup \{\Phi\} \vdash \Psi$, то $\Gamma \vdash \Phi \supset \Psi$.

2) Доказать, что если в интуиционистском исчислении предикатов имеет место $\Gamma \vdash \Phi$, а переменная v не входит свободно в формулы из Γ, то $\Gamma \vdash \forall v \Phi$.

3) Доказать, что если в интуиционистском исчислении предикатов имеет место $\Gamma \cup \{\Phi\} \vdash \Psi$, а переменная v не входит свободно в формулы из Γ и формулу Ψ, то $\Gamma \cup \{\exists v \Phi\} \vdash \Psi$.

4) Доказать, что каковы бы ни были формула $\Phi(x)$, формула Ψ, не содержащая свободно переменную x, и переменная y, не входящая в формулу $\Phi(x)$, следующие формулы выводимы в исчислении предикатов:

   а) $\exists x \neg \Phi(x) \supset \neg \forall x \Phi(x)$;

   б) $\neg \exists x \Phi(x) \supset \forall x \neg \Phi(x)$;

   в) $\forall x \neg \Phi(x) \supset \neg \exists x \Phi(x)$;

   г) $(\forall x \Phi(x) \,\&\, \Psi) \supset \forall x (\Phi(x) \,\&\, \Psi)$;

   д) $\forall x (\Phi(x) \,\&\, \Psi) \supset (\forall x \Phi(x) \,\&\, \Psi)$;

е) $(\Psi \,\&\, \forall x \Phi(x)) \supset \forall x (\Psi \,\&\, \Phi(x))$;

ж) $\forall x (\Psi \,\&\, \Phi(x)) \supset (\Psi \,\&\, \forall x \Phi(x))$;

з) $\exists x (\Phi(x) \,\&\, \Psi) \supset (\exists x \Phi(x) \,\&\, \Psi)$;

и) $(\exists x \Phi(x) \,\&\, \Psi) \supset \exists x (\Phi(x) \,\&\, \Psi)$;

к) $(\Psi \,\&\, \exists x \Phi(x)) \supset \exists x (\Psi \,\&\, \Phi(x))$;

л) $\exists x (\Psi \,\&\, \Phi(x)) \supset (\Psi \,\&\, \exists x \Phi(x))$;

м) $(\forall x \Phi(x) \vee \Psi) \supset \forall x (\Phi(x) \vee \Psi)$;

н) $(\Psi \vee \forall x \Phi(x)) \supset \forall x (\Psi \vee \Phi(x))$;

о) $(\exists x \Phi(x) \vee \Psi) \supset \exists x (\Phi(x) \vee \Psi)$;

п) $\exists x (\Phi(x) \vee \Psi) \supset (\exists x \Phi(x) \vee \Psi)$;

р) $(\Psi \vee \exists x \Phi(x)) \supset \exists x (\Psi \vee \Phi(x))$;

с) $\exists x (\Psi \vee \Phi(x)) \supset (\Psi \vee \exists x \Phi(x))$;

т) $\exists x (\Phi(x) \supset \Psi) \supset (\forall x \Phi(x) \supset \Psi)$;

у) $(\Psi \supset \forall x \Phi(x)) \supset \forall x (\Psi \supset \Phi(x))$;

ф) $\forall x (\Psi \supset \Phi(x)) \supset (\Psi \supset \forall x \Phi(x))$;

х) $(\exists x \Phi(x) \supset \Psi) \supset \forall x (\Phi(x) \supset \Psi)$;

ц) $\forall x (\Phi(x) \supset \Psi) \supset (\exists x \Phi(x) \supset \Psi)$;

ч) $\exists x (\Psi \supset \Phi(x)) \supset (\Psi \supset \exists x \Phi(x))$;

ш) $\forall x \Phi(x) \supset \forall y \Phi(y)$;

щ) $\exists x \Phi(x) \supset \exists y \Phi(y)$.

8.8. Модели Крипке для логики предикатов

Пусть фиксирован язык первого порядка с сигнатурой Ω, не содержащей функциональных символов. Модель Крипке для языка сигнатуры Ω — это набор $\mathcal{K} = (K, \preceq, D, \models)$, где $(K, \preceq)$ — частично упорядоченное множество (шкала Крипке), D — функция, каждому элементу $\alpha \in K$ сопоставляющая непустое множество D_α, причем $D_\alpha \subseteq D_\beta$, если $\alpha \preceq \beta$. Если сигнатура Ω содержит константу c, то ей сопоставляется некоторый объект $\bar{c}$, который, по определению, принадлежит любому множеству D_α для $\alpha \in K$. В дальнейшем константа c отождествляется с элементом $\bar{c}$. Наконец, $\models$ — некоторое соответствие между множеством K и множеством всех атомов вида $P(a_1, \ldots, a_n)$, где P есть (n-местный) предикатный символ сигнатуры Ω, а $a_1, \ldots, a_n$ — элементы множества $\bigcup\limits_{\alpha \in K} D_\alpha$, обладающее тем свойством, что если $\alpha \in K$, $P(a_1, \ldots, a_n)$ — атом указанного вида и $\alpha \models P(a_1, \ldots, a_n)$, то $\{a_1, \ldots, a_n\} \subseteq D_\alpha$, и если $\alpha \preceq \beta$, то $\beta \models P(a_1, \ldots, a_n)$.

Соответствие $\models$ называется оценкой атомов в данной модели Крипке. Как и в случае моделей Крипке для логики высказываний, $\alpha \models P(a_1, \ldots, a_n)$ читается «α вынуждает $P(a_1, \ldots, a_n)$» или «$P(a_1, \ldots, a_n)$ истинно в момент α».

На основе соответствия $\models$ определяется соответствие между множеством K и множеством всех замкнутых формул сигнатуры Ω, расширенной за счет констант для обозначения всех элементов множества $\bigcup\limits_{\alpha \in K} D_\alpha$, обозначаемое тем же символом $\models$. Это соответствие задается индукцией по логической длине формулы, т. е. количеству логических символов в ней. Для атомов оно уже определено. Далее полагаем:

- $\alpha \models (A \,\&\, B) \rightleftharpoons [\alpha \models A$ и $\alpha \models B]$;
- $\alpha \models (A \vee B) \rightleftharpoons [\alpha \models A$ или $\alpha \models B]$;
- $\alpha \models (A \supset B) \rightleftharpoons (\forall \beta \succeq \alpha)[\beta \not\models A$ или $\beta \models B]$;
- $\alpha \models \neg A \rightleftharpoons (\forall \beta \succeq \alpha) \beta \not\models A$;
- $\alpha \models \exists v A(v) \rightleftharpoons (\exists a \in D_\alpha) \alpha \models A(a)$;
- $\alpha \models \forall v A(v) \rightleftharpoons (\forall \beta \succeq \alpha)(\forall a \in D_\beta) \beta \models A(a)$.

Здесь $\beta \succeq \alpha$ означает $\alpha \preceq \beta$, а $A(a)$ есть результат подстановки константы a вместо переменной v в формулу $A(v)$.

Говорят, что формула A истинна в модели Крипке $\mathcal{K} = (K, \preceq, D, \models)$ и пишут $\mathcal{K} \models A$, если для любого $\alpha \in K$ имеет место $\alpha \models A$. Если формула A не истинна в модели Крипке $\mathcal{K}$, т. е. $\mathcal{K} \not\models A$, то $\mathcal{K}$ называют контромоделью для A. Имеет место следующая теорема о корректности и полноте интуиционистского исчисления предикатов относительно моделей Крипке:

Теорема 8.7. *Замкнутая формула сигнатуры Ω выводима в интуиционистском исчислении предикатов тогда и только тогда, когда она истинна в любой модели Крипке.*

Таким образом, для любой замкнутой формулы A можно либо построить ее вывод в интуиционистском исчислении предикатов, либо найти контрмодель для A.

Пример. Докажем, что формула $\neg\neg\forall x(P(x) \vee \neg P(x))$ не выводится в интуиционистском исчислении предикатов, построив контрмодель для этой формулы. Пусть $K = \mathbf{N}$, причем $m \preceq n \rightleftharpoons m \leq n$ для любых $m, n \in \mathbf{N}$. Пусть $D_n = \{0, \ldots, n\}$. Положим $m \models P(n) \rightleftharpoons m > n$. Допустим, что

$$0 \models \neg\neg\forall x(P(x) \vee \neg P(x)). \tag{37}$$

В силу определения отношения $\models$ для отрицания, (37) означает, что $(\forall m \in \mathbf{N}) m \not\models \neg\forall x(P(x) \vee \neg P(x))$. В частности, $0 \not\models \neg\forall x(P(x) \vee \neg P(x))$. Это означает, что $m \models \forall x(P(x) \vee \neg P(x))$ для некоторого $m \in \mathbf{N}$. Отсюда и из определения отношения $\models$ для квантора всеобщности следует, что $m \models P(m) \vee \neg P(m)$, так как $m \in D_m$. В силу определения отношения $\models$ для дизъюнкции, это означает, что либо 1) $m \models P(m)$, либо 2) $m \models \neg P(m)$. Однако ни то, ни другое не имеет места. Действительно, условие 1) не выполняется в силу определения отношения $\models$ для атомов. Докажем, что условие 2) также не выполняется. Допустим противное, т. е. $m \models \neg P(m)$. В силу определения отношения $\models$ для отрицания, это означает, что $(\forall n \geq m) n \not\models P(m)$. Но это не так, ибо $m + 1 \models P(m)$. Таким образом, предположение (37) приводит к противоречию. Значит, $0 \not\models \neg\neg\forall x(P(x) \vee \neg P(x))$, и построенная модель Крипке является контрмоделью для формулы $\neg\neg\forall x(P(x) \vee \neg P(x))$.

Задачи.

Путем построения подходящей контрмодели доказать, что каждая из следующих формул не выводится в интуиционистском исчислении предикатов:

1) $\neg\forall x P(x) \supset \exists x \neg P(x)$;

2) $\forall x(P(x) \vee Q) \supset \forall x P(x) \vee Q$;

3) $(\forall x P(x) \supset Q) \supset \exists x(P(x) \supset Q)$;

4) $(Q \supset \exists x P(x)) \supset \exists x(Q \supset P(x)$;

5) $\forall x(P(x) \vee \neg P(x)) \,\&\, \neg\neg\exists x P(x) \supset \exists x P(x)$.

Литература

[1] И. А. Лавров, Л. Л. Максимова. Задачи по теории множеств, математической логике и теории алгоритмов. М.: Физматлит, 1995.

[2] Э. Мендельсон. Введение в математическую логику. М.: Наука, 1971.

[3] Л. Стерлинг, Э. Шапиро. Искусство программирования на языке Пролог. М.: Мир, 1990.

[4] В. А. Успенский, Н. К. Верещагин, В. Е. Плиско. Вводный курс математической логики. М.: ФИЗАТЛИТ, 2002.

[5] К. Хоггер. Введение в логическое программирование. М.: Мир, 1988.

[6] Ч. Чень, Р. Ли. Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.