ВВЕДЕНИЕ. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Все математические дисциплины можно условно разделить на *дискретные* и *непрерывные*. Дискретная математика – это та часть математики, главной особенностью которой является изучение отдельных объектов, без привлечения понятия непрерывности, т.е. дискретность – это антипод непрерывности. В дискретной математике отсутствует понятие предельного перехода, присущее классической, «непрерывной» математике. Она занимается изучением дискретных структур, которые возникают как внутри математики, так и в ее приложениях. Однако она зародилась в глубокой древности, раньше, чем непрерывная математика, хотя особую значимость приобрела только в последние десятилетия, в связи с повсеместным внедрением в практику информационных технологий.

Таким образом, в широком смысле дискретная математика включает в себя все разделы математики, в которых не используются топологические методы, в частности понятие непрерывности. Это – все разделы алгебры, математическая логика, почти вся теория чисел (в том числе всевозможные компьютерные арифметики), многие разделы экономико-математических методов, комбинаторика и многие другие дисциплины. В более узком смысле дискретная математика – это те разделы математической логики, алгебры, теории чисел и математической кибернетики, которые непосредственно составляют теоретический фундамент информатики. В этом узком смысле дискретная математика включает в себя теорию булевых функций и их минимизацию, теорию графов и многие разделы теоретической кибернетики, теорию автоматов и формальных грамматик, комбинаторику, теорию алгоритмов (в том числе теорию сложности вычислений), криптографию и теорию кодирования.

Некоторые из вышеперечисленных разделов имеют не только многочисленные «внутренние» (с точки зрения специалиста по информационным системам или вычислительной техники) приложения, используемые, к примеру, при построении различных дискретных устройств, в программировании и т.д., но их результаты и методы применяются также при решении многих нужных для практики задач. Например, при рассмотрении транспортных задач, для нахождения оптимальных решений в управлении, для выделения «узких мест» при планировании и разработке проектов, при составлении оптимальных расписаний, а также при моделировании сложных технологий и процессов различной природы.

Целью изучения дисциплины является ознакомление студентов с системой понятий и некоторыми наиболее важными в приложениях методами теории множеств, математической логики, теории булевых функций и теории графов. Знания и навыки, полученные при ее изучении, используются в дисциплинах: «Информатика», «Программирование», «Структуры и алгоритмы обработки данных в ЭВМ», «Базы данных», «Экспертные и интеллектуальные системы» и т.д. Но в особенности знания по дискретной математике пригодятся

при изучении дисциплин, связанных с функциональным и логическим программированием, кодированием и защитой информации.

Основная задача состоит в том, чтобы будущие специалисты чётко освоили основные понятия и приёмы работы с булевыми функциями и графами: построение таблиц значений; поиск и исключение фиктивных переменных; приведение булевых функций к стандартной форме (д.н.ф., к.н.ф., многочлен Жегалкина); основные методы минимизации булевых функций; построение диаграммы (рисунка) графа по его матрицам смежности и инцидентности и обратная задача; установление изоморфизма (одинаковости) графов; определение основных характеристик и свойств графов (векторы степеней, планарность, эйлеровость, гамильтоновость и т.п.); изучение важного частного случая графов – деревьев и их свойств.

За недостатком места о приложениях говорится относительно мало. Однако такие примеры содержатся в литературе.

Данное пособие предназначено в основном для изучения основ именно дискретной математики в узком понимании слова, хотя при этом затронуты основополагающие разделы математической логики – исчисление высказываний и исчисление предикатов. Однако математическую логику настоятельно рекомендуется изучать по более фундаментальным источникам, например, [1, 11,15,16,19,23,29]. В то же время, многие разделы дискретной математики в узком смысле слова в данном пособии никак не отражены, в частности, теория кодирования и криптография, теория алгоритмов и теория сложности вычислений. Это связано, в первую очередь, с ограниченностью отводимого времени для изучения дисциплины в учебных планах у студентов, обучающихся информационным технологиям и использованию вычислительной техники. Курс лекций будет также полезен будущим специалистам по прикладной математике, в частности по математическому и компьютерному моделированию.

Пособие – это существенно поработанный и дополненный вариант пособий [20,21].

ЧАСТЬ ПЕРВАЯ. ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

ЧАСТЬ ВТОРАЯ. БУЛЕВЫ ФУНКЦИИ И ИХ МИНИМИЗАЦИЯ

Теорию булевых функций и их минимизации можно считать по праву центральным моментом для математического образования любых инженеров, чья деятельность подразумевает активное использование ЭВМ.

6 ОСНОВНЫЕ СВОЙСТВА БУЛЕВЫХ ФУНКЦИЙ. ДВОЙСТВЕННЫЕ И САМОДВОЙСТВЕННЫЕ БУЛЕВЫ ФУНКЦИИ. ПРИНЦИП ДВОЙСТВЕННОСТИ

См. лекции 1-6

7 СОВЕРШЕННЫЕ ДНФ И КНФ. ПОЛИНОМ ЖЕГАЛКИНА. МОНОТОННЫЕ ФУНКЦИИ. ПОЛНОТА. КРИТЕРИЙ ПОЛНОТЫ

7.1 Совершенные дизъюнктивная и конъюнктивная нормальные формы

В этом разделе под *функцией* будем подразумевать *булеву функцию*. *Дизъюнктивной нормальной формой* (сокращенно, *д. н. ф.* или *ДНФ*) для функции f называется *дизъюнкция элементарных конъюнкций*, как функция равная f, а *элементарной конъюнкцией* называется конъюнкция переменных или их отрицаний. При записи д.н.ф. знак конъюнкции принято опускать. Принято также считать, что одна переменная или её отрицание тоже образуют элементарную конъюнкцию, а одна элементарная конъюнкция – это тоже д.н.ф. Элементарные конъюнкции иногда называют *импликантами* – см. п. 8.1.3.

Примеры 7.1 Рассмотрим несколько булевых функций: $A=x\bar{y}\vee z$, $B=\bar{x}\vee y\vee z$, $C=x\bar{y}\,\bar{z}$, $D=\bar{x}\,\&\,(y\vee z)=\bar{x}(y\vee z)=\bar{x}\wedge(y\vee z)$, $E=\bar{x}\,\bar{y}(x\vee z)$. Функции A, B, C находятся в д.н.ф., так как A есть дизъюнкция двух элементарных конъюнкций $x\bar{y}$ и z; B – дизъюнкция трёх элементарных конъюнкций, каждая из которых состоит из одной *буквы* (или *литеры*, т.е. переменной либо её отрицания); C – дизъюнкция одной элементарной конъюнкции. Функции D и E не имеют вид д.н.ф. (почему?)

Двойственным образом к д.н.ф. определяется *конъюнктивная нормальная форма* (сокращенно *к. н. ф.* или *КНФ*). А именно, говорят, что функция f находится в к.н.ф., если она записана в виде конъюнкции *элементарных дизъюнкций*, т.е. дизъюнкций переменных или их отрицаний. Например, функции, заданные формулами B, C и D из примера 7.1 являются к.н.ф., а формула A к.н.ф. не является; формула E – и не д.н.ф., и не к.н.ф.

Заметим, что о повторениях литер ничего не говорится, таким образом, $A_1=x\vee\bar{x}\vee y$, $B_1=xyy$ – тоже д.н.ф. и к.н.ф. Если же д.н.ф. (к.н.ф.) такова, что в любой её элементарной конъюнкции (дизъюнкции) каждая литера встречается ровно один раз, то такая д.н.ф. (к.н.ф.) называется *совершенной*.

Из функций примера 7.1, только B находится в совершенной к.н.ф., а C – в совершенной д.н.ф. (если считать, что все эти функции от трёх переменных).

7.1.1 Отметим, что во всякого рода приложениях булевы функции применяются довольно часто записанными в виде д.н.ф. или к.н.ф. Значимость этих понятий для теории булевых функций подчёркивает следующая

Теорема 7.1 *1) Любая булева функция, отличная от тождественно равной 0, может быть записана в виде совершенной д.н.ф.;*

2) любая булева функция, отличная от тождественно равной 1, может

быть записана в виде совершенной к.н.ф.

Доказательство этой теоремы очень просто усматривается из способа построения совершенных д.н.ф. и к.н.ф., которые описываются в примере 7.2 ниже.

Следствие 7.1 *Любая булева функция может быть записана как в виде д.н.ф., так и в виде к.н.ф.*

Упражнение 7.1 *Докажите это следствие.*

7.1.2 При работе с д.н.ф. и к.н.ф. очень удобно следующее обозначение:

$$x^{\alpha} = \begin{cases} \bar{x}, & \text{если } \alpha = 0 \\ x, & \text{если } \alpha = 1 \end{cases}, \qquad \text{т.е. } x^0 = \bar{x}, \text{ а } x^1 = x.$$

Таблица 7.1.

№	x	y	z	f
0	0	0	0	1
1	0	0	1	1
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	1
6	1	1	0	0
7	1	1	1	1

Упражнение 7.2 *Проверьте, что $x^{\alpha} = 1$ равносильно тому, что $\alpha = x$, а равенство $x^{\alpha}y^{\beta}z^{\gamma} = 1$ равносильно системе*

$$\begin{cases} x = \alpha \\ y = \beta \\ z = \gamma \end{cases}.$$

Пример 7.2 Составим совершенную д.н.ф. для функции $f = (1,1,0,1,0,1,0,1)$. Здесь, как и ранее, подразумевается, что значения переменных даны в лексикографическом (алфавитном) порядке, первым идёт набор (0,0,0), вторым (0,0,1),…, последним – (1,1,1) – см. также таблицу 7.1.

Нам нужно написать д.н.ф. A именно для функции f, т.е. такую д.н.ф., которая при всех значениях переменных принимает те же значения, что и функция f. Вначале добьёмся того, чтобы наша д.н.ф. принимала значения 1 на тех же наборах, что и f. Вспоминаем, что д.н.ф. – это, прежде всего, дизъюнкция (дизъюнкция чего именно – сейчас пока не важно). А дизъюнкция нескольких членов равна единице, если хоть один член – единица. Поэтому выбираем в таблице значений строки (α,β,γ), где $f(\alpha,\beta,\gamma)$ равно 1. По каждой такой строке (α,β,γ) выписываем элементарную конъюнкцию $x^{\alpha}y^{\beta}z^{\gamma}$, т.е. при $\alpha = 1$ пишем просто x, при $\alpha = 0$ – $\bar{x}$. Согласно упражнению 7.2, эта элементарная конъюнкция $x^{\alpha}y^{\beta}z^{\gamma}$ равна единице при $x = \alpha$, $y = \beta$ и $z = \gamma$. Тогда строка №0 таблицы – (0,0,0) – даёт элементарную конъюнкцию $L_1 = \bar{x}\,\bar{y}\,\bar{z}$; строка № 1 – (0,0,1) – конъюнкцию $L_2 = \bar{x}\,\bar{y}z$; строка с номером 3, (0,1,1) – конъюнкцию $L_3 = \bar{x}yz$; пятая строка (1,0,1) – конъюнкцию $L_4 = x\bar{y}z$; седьмая строка (1,1,1) – $L_5 = xyz$. Окончательно, получаем $A = \bar{x}\,\bar{y}\,\bar{z} \vee \bar{x}\,\bar{y}z \vee \bar{x}yz \vee x\bar{y}z \vee xyz$.

Однако мы добились только, что значения этого выражения A совпадают с функцией f лишь на пяти наборах значений переменных. А что будет в оставшихся трёх случаях? Можно, конечно, подставить последовательно

оставшиеся наборы значений переменных (0,1,0), (1,0,0) и (1,1,0) в д.н.ф. A, и убедиться, что A принимает на них нулевое значение, как и f. Так что, каждый раз при написании совершенной д.н.ф. будем делать такую проверку? Оказывается, в этом нет необходимости. Действительно, мы же написали для f *совершенную* д.н.ф., т.е. такую, у которой в каждую элементарную конъюнкцию L_i входят все переменные ровно по одному разу: либо сама переменная, либо её отрицание. Поэтому каждая элементарная конъюнкция L_i истинна только на одном «своём» наборе значений переменных, а именно, на том по которому она писалась (см. упражнение 7.2). На остальных же значениях переменных L_i – ложна. Например, L_1 истинна только на наборе (0,0,0), L_2 – на наборе (0,0,1) и т.д. Таким образом, на оставшихся трёх наборах все пять элементарных конъюнкций L_1, L_2, L_3, L_4 и L_5 ложные, а значит, на них ложна и вся д.н.ф. A, следовательно, $f = A = \bar{x}\,\bar{y}\,\bar{z} \vee \bar{x}\,\bar{y}z \vee \bar{x}yz \vee x\,\bar{y}z \vee xyz$.

Для построения совершенной к.н.ф. для функции f действуем строго наоборот по сравнению с тем как писалась совершенная д.н.ф.: мы выбираем те наборы (α,β,γ) значений переменных, на которых функция равна *нулю*, и пишем по каждому из них элементарную дизъюнкцию вида $(x^{\bar{\alpha}} \vee y^{\bar{\beta}} \vee z^{\bar{\gamma}})$. В итоге получается: $f = (x \vee \bar{y} \vee z) \wedge (\bar{x} \vee y \vee z) \wedge (\bar{x} \vee \bar{y} \vee z)$.

Упражнение 7.3 *Обоснуйте описанный выше способ построения совершенных к.н.ф., опираясь на принцип двойственности.*

7.2 Многочлен Жегалкина

7.2.1 Напомним, некоторые известные Вам со школы определения, относящиеся к любым многочленам (полиномам). Во-первых, само название говорит о том, что многочлен состоит из нескольких членов – слагаемых. При этом одно слагаемое, т.е. одночлен – это тоже многочлен. Во-вторых, каждое слагаемое в многочлене имеет вид произведения числа и нескольких переменных в каких-то степенях. Показатели степеней должны быть обязательно *целыми неотрицательными* числами. Числа, входящее в произведения называются *коэффициентами*, и они могут быть дробными для обычных многочленов. В-третьих, *степень многочлена* (не обязательно многочлена Жегалкина) всегда определяется как *наибольшая из степеней его членов*, т.е. слагаемых. А вот степень слагаемого (отдельного члена) может определяться по-разному. Иногда её определяют как наивысший из показателей степеней переменных, входящих в запись одночлена. Но нам будет удобнее другое определение. Итак, *степень одночлена* – это *сумма показателей степеней всех переменных в его записи*.

Примеры 7.3. Рассмотрим несколько многочленов: $f = a \cdot x^2 \cdot y^{17} \cdot z + b \cdot x^{12} \cdot z^{10} + c \cdot x^3 \cdot y^5 \cdot z^2 \cdot u^4 + d \cdot y + 7 \cdot x \cdot y \cdot u^7 + 5{,}5$; $g = x \cdot v^2 + 3$; $h = a$. Многочлен f имеет 6 членов-слагаемых, многочлен g – два, а h состоит только из одного слагаемого. Считаем степени одночленов.

Но тут появляется некоторый нюанс: что означают буквы a, b, c и d?

Это переменные или это коэффициенты? Если эти буквы считать как переменные, то степень многочлена f равна: $deg(f) = max\{1+2+17+1, 1+12+10, 1+3+5+2+4, 1+1, 1+1+7, 0\} = 23$; степень многочлена g: $deg(g) = max\{1+2, 0\} = 3$; и, наконец, $\deg(h) = \max\{1\} = 1$.

Мы же с вами договоримся, о том, что первые буквы латинского алфавита a, b, c, d и другие с индексами или без индексов будут обозначать коэффициенты. Тогда мы имеем: $deg(f) = max\{0+2+17+1, 0+12+10, 0+3+5+2+4, 0+1, 1+1+7, 0\} = 22$; $deg(g) = max\{1+2, 0\} = 3$; $deg(h) = max\{0\} = 0$.

Обратите внимание, что многочлен h состоит из одного слагаемого степени нуль, т.е. из одного *свободного члена* – константы. Таким образом, любая константа – это многочлен степени нуль.

7.2.2 *Многочлен* (или *полином) Жегалкина* – это с виду обыкновенный многочлен от нескольких переменных, в котором роль умножения выполняет конъюнкция, в роли сложения – сложение по модулю два, а коэффициентами являются только нули или единицы.

Рассмотрим, какой может быть максимальная степень многочлена Жегалкина с n переменными?

Лемма 7.1 *Максимальная степень многочлена Жегалкина с n переменными не превосходит n.*

Доказательство. Степень выше n нельзя получить в виду равенств: $x^2 = x \cdot x = x \wedge x = x$, $x^3 = x$ и т.д. Поэтому при одной переменной степень не может быть выше первой, при двух переменных x и y максимальная степень – два – у слагаемого вида $a \cdot x \cdot y$; при добавлении переменной z максимальная степень – три – у слагаемого – $b \cdot x \cdot y \cdot z$ и т.д.

Теорема 7.2 *Любую булеву функцию можно записать в виде многочлена Жегалкина единственным способом.*

Доказательство существования (первое, а заодно и способ построения). Этот способ основан на том, что $x \oplus 1 = \bar{x}$. Если функция задана в виде д.н.ф., то сначала убираем дизъюнкцию, используя при этом равенство $K_1 \vee K_2 = K_1 \oplus K_2 \oplus K_1 \cdot K_2$ или правила де Моргана, а все отрицания заменяем прибавлением единицы. После этого раскрываем скобки по обычным правилам, применяя дистрибутивность, при этом учитываем, что четное число одинаковых слагаемых равно нулю (так как $x \oplus x = 0$), а нечетное число одинаковых слагаемых равно одному такому слагаемому. Последнее выражение и есть *полином Жегалкина* данной функции.

Пример 7.4 Найдём многочлена Жегалкина для функции $g(x,y,z) = xy \vee \bar{x}\,\bar{y} \vee \bar{y}z$. Применим правило де Моргана в виде: $a \vee b \vee c = \neg(\bar{a} \wedge \bar{b} \wedge \bar{c})$:

$$g(x,y,z) = \neg[\,\overline{xy} \cdot \neg\,(\bar{x}\bar{y}) \cdot \neg\,(\bar{y}z)\,] = \neg[(xy \oplus 1) \cdot (\bar{x}\,\bar{y} \oplus 1) \cdot (\bar{y}z \oplus 1)] =$$

$$= \neg[(xy \oplus 1) \cdot ((x \oplus 1) \cdot (y \oplus 1) \oplus 1) \cdot ((y \oplus 1) \cdot z \oplus 1)] = (xy \oplus 1) \cdot (xy \oplus x \oplus y) \cdot (yz \oplus z \oplus 1) \oplus 1$$

$$= (xy + xy + xy + xy + x + y) \cdot (yz + z + 1) + 1 = (x + y) \cdot (yz + z + 1) + 1 =$$

$$= xyz + xz + x + yz + yz + y + 1 = xyz \oplus xz \oplus x \oplus y \oplus 1.$$

Замечание. Нарушая правила математической эстетики, мы применили в одной формуле два разных обозначения для одной и той же функции: вначале для отрицания – знак «¬» и черту сверху, чтобы избежать «трёхэтажных» чёрт поверху, а затем «плюс в кружочке» для обозначения заменили обычным – для улучшения восприятия. Можно было бы и вообще для обозначения сложения по модулю два использовать только обычный плюс, но, увы, тогда есть опасность спутать эту операцию с дизъюнкцией – как уже отмечалось, в некоторых даже современных книгах для дизъюнкции употребляется знак «+».

7.2.3 Способ получения многочлена Жегалкина, описанный при доказательстве теоремы 7.2, на практике пригоден лишь для функций, которые задаются весьма короткой д.н.ф. или к.н.ф. Лучше применять более универсальный способ нахождения многочлена, основанный на *методе неопределённых коэффициентов*, с которым мы сейчас познакомимся на конкретном примере. Метод неопределённых коэффициентов, хорош также ещё и тем, что позволяет обосновать единственность многочлена Жегалкина.

Пример 7.5 Найдём многочлена Жегалкина для функции $f(x,y,z)$, заданной таблицей 7.2.

Согласно лемме 7.1 степень нужного нам многочлена не превосходит трёх, значит, нам надо представить данную функцию в виде:

Таблица 7.2

№	x	y	z	f
0	0	0	0	1
1	0	0	1	0
2	0	1	0	0
3	0	1	1	1
4	1	0	0	1
5	1	0	1	0
6	1	1	0	1
7	1	1	1	0

$$f(x,y,z)=a_0+ a_1x+ a_2y+ a_3z+ a_4xy+ a_5xz+ a_6yz+ a_7xyz, \quad (7.1)$$

где все коэффициенты $a_0, a_1, a_2, \ldots, a_7$ – неизвестные пока нам величины, принимающие значения 0 либо 1.

Подставим значение первой строчки (№0) таблицы 7.2 в левую часть формулы (7.1), получим, что $f(0;0;0)=1$; подставляя эти же значения $x = y = z = 0$ в правую часть равенства (7.1) имеем:

$$f(0;0;0)= a_0+ a_1\cdot 0 + a_2\cdot 0 + a_3\cdot 0 + a_4\cdot 0\cdot 0 + a_5\cdot 0\cdot 0 + a_6\cdot 0\cdot 0 + \\ +a_7\cdot 0\cdot 0\cdot 0 = a_0.$$

Вспоминая, что $f(0;0;0)=1$, получаем уравнение № 0:

$$0)\ a_0=1.$$

Таким же образом, из строки №1 таблицы 7.2 при $x = y = 0$ и $z = 1$ получаем, что $f(0;0;1)= 0$; а с другой стороны, $f(0;0;1)= a_0+ a_1\cdot 0 + a_2\cdot 0 + a_3\cdot 1 + a_4\cdot 0\cdot 0 + a_5\cdot 0\cdot 1 + a_6\cdot 0\cdot 1 + a_7\cdot 0\cdot 0\cdot 1 =$. Отсюда получается уравнение

$$1)\ 0=a_0+ a_3;$$

подставляя в него известное из уравнения 0) значение a_0, имеем $0=1+ a_3$. Это уравнение можно решать, по меньшей мере, двумя способами. Можно использовать определение сложения по модулю 2 (таблица 6.3): в этой таблице по третьей и четвёртой строке ищем то значение a_3, добавление которого к 1 даёт значение выражения $1+ a_3$ равное 0. Это $a_3 = 1$. А можно решить это

уравнение как обычное, тогда получим $a_3 = -1$. Теперь видим, что получилось нечётное число -1, а представителем всех нечётных чисел по модулю 2 является единица, и значит, окончательно $a_3 = 1$.

Далее подставляем значения строки №2 из таблицы, а также значение найденных ранее коэффициентов и т.д. Получим последовательно уравнения:

2) $f\{0;1;0\}=0=a_0+a_2 \Rightarrow 0=1+a_2 \Rightarrow a_2=1;$

3) $f\{0;1;1\}=1=a_0+a_2+a_3+a_6 \Rightarrow 1=1+1+1+a_6 \Rightarrow a_6=0;$

4) $f\{1;0;0\}= 1=a_0+a_1 \Rightarrow 1=1+a_1 \Rightarrow a_1=0;$

5) $f\{1;0;1\}=0=a_0+a_1+a_3+a_5 \Rightarrow 0=1+0+1+a_5 \Rightarrow a_5=0;$

6) $f\{1;1;0\}=1=a_0+a_1+a_2+a_4 \Rightarrow 1=1+0+1+a_4 \Rightarrow a_4=1;$

7) $f\{1;1;1\}=0=a_0+a_1+a_2+a_3+a_4+a_5+a_6+a_7 \Rightarrow 0=1+0+1+1+1+0+0+a_7 \Rightarrow a_7=0.$

Таким образом, $a_0=1;\ a_1=0;\ a_2=1;\ a_3=1;\ a_4=1;\ a_5=0;\ a_6=0;\ a_7=0$. Подставляя полученные значения коэффициентов в формулу (7.1), получаем:

$$f = 1 + y + z + xy.$$

Вернёмся к доказательству теоремы 7.2. В общем случае, когда количество переменных у функции равно n, строим для данной функции таблицу значений (истинности), а саму функцию записываем в виде полинома Жегалкина с неопределенными коэффициентами, т.е. в виде, аналогичном (7.1). Затем по очереди подставляем всевозможные наборы значений переменных в это выражение, получаем уравнения, и из них находим коэффициенты, как это делается в примере 7.5. Легко видеть, что за каждую подстановку находим только один коэффициент. Так как число наборов 2^n равно числу коэффициентов (почему?), отсюда следует утверждение теоремы.

Упражнение 7.4 *Докажите, что число неизвестных коэффициентов у функции с n переменными в выражении вида (2) равно 2^n.*

7.3 Суперпозиция функций. Замыкание набора функций. Замкнутые классы функций. Полные наборы

7.3.1 Пусть имеется некоторый набор D, состоящий из конечного числа булевых функций. *Суперпозициями* функций из этого набора называются функции, полученные с помощью конечного числа применения двух операций:

- можно переименовать любую переменную, входящую в функцию из D;
- вместо любой переменной в записи функции из набора D можно поставить функцию из набора D или уже образованную ранее суперпозицию.

В частности, сами функции из набора D также будут суперпозициями, так как их можно получить нулевым количеством переименований переменных.

Предупреждение. Когда вы переименовываете какую-либо переменную или подставляете вместо неё какую-то функцию из D, это действие нужно выполнить *для всех вхождений* выбранной переменной в

записи.

Суперпозицию еще иначе называют *с л о ж н о й* функцией.

П р и м е р ы 7.6 Если дана одна функция $x \mid y$ (штрих Шеффера), то ее суперпозициями, в частности, будут следующие функции: 1) она сама; 2) $x \mid x$ – переименовали переменную y; 3) $x \mid (x \mid y)$ – на место y подставили $x \mid y$; 4) $x|(y|z)$ – обоснуйте сами, и т.д.

З а м ы к а н и е м класса функций K называется множество всех суперпозиций, полученных по любым конечным наборам функций из K, а также добавлением всех функций, которые получаются из этих суперпозиций введением фиктивных переменных. Класс функций K называется *з а м к н у т ы м*, если его замыкание совпадает с ним самим. Несложно понять, что замыкание, применённое к замыканию любого класса, даст в итоге тот же класс, что получился в первый раз. Следовательно, замыкание всякого набора функций есть замкнутый класс.

Набор (система) функций называется *п о л н ы м*, если его замыкание совпадает со всеми булевыми (логическими) функциями. Иначе говоря, полный набор – это множество таких функций, через которые можно выразить все остальные булевы функции.

П р и м е р 7.7 Ввиду теоремы 7.1, её следствия и теоремы 7.2 наборы $F_1 = \{\neg,\wedge,\vee\}$; $F_2 = \{\wedge,\oplus,0,1\}$ – полные. В то же время, системы $F_3 = \{\neg\}$ и $F_4 = \{\wedge,\vee\}$ – неполные (почему?).

Т е о р е м а 7.3 *Если набор $F = \{f_1,\ldots,f_k\}$ – полный, а система $D = \{g_1,\ldots,g_l\}$ такова, что каждая функция f_j из F может быть записана как суперпозиция функций системы D, то набор D – тоже полный.*

Д о к а з а т е л ь с т в о. Пусть h – произвольно выбранная булева функция. Так как система F полная, то h может быть записана в виде формулы, куда входят только функции системы F. По условию каждую функцию f_j в этой формуле можно заменить суперпозицией функций системы D, в результате получится формула, в записи которой участвуют только функции g_i из набора D.

7.3.2 Пять важнейших классов булевых функций:

а) T_0 – это *класс всех тех логических функций, которые на нулевом наборе значений переменных принимают значение 0* (т.е. T_0 – это класс функций, *с о х р а н я ю щ и х константу 0*). Например, это константа 0, дизъюнкция, конъюнкция, а вот импликация сюда не попадает;

б) T_1 – это *класс всех логических функций, которые на единичном наборе значений переменных принимают значение 1* (т.е. T_1 – это класс функций, *с о х р а н я ю щ и х константу 1*). Например, это константа 1, дизъюнкция, конъюнкция, а вот сложение по модулю два сюда не попадает;

в) L – класс *л и н е й н ы х* функций т.е. функций, для которых полином Жегалкина имеет степень не выше одного; например, это константы 0 и 1,

сложение по модулю два, а вот дизъюнкция, конъюнкция сюда не попадают;

г) S – класс *самодвойственных* функций, т.е. функций, совпадающих со своей двойственной: $f^* = f$. Например, функции отрицания и тождественная (т.е. $f(x) = x$) – самодвойственные, а константы 0 и 1, сложение по модулю два, дизъюнкция, конъюнкция – нет.

д) M – класс *монотонных* функций. Опишем класс этих функций более подробно. Пусть имеются два набора длины n из нулей и единиц: $s_1 = (x_1,x_2,\ldots, x_n)$ и $s_2 = (y_1,y_2,\ldots,y_n)$. Будем говорить, что набор s_1 *тотально не больше* набора s_2 и писать $s_1 \sqsubseteq s_2$, если все элементы первого набора не больше (уже в обычном смысле) соответствующих компонент второго: $x_i \le y_i$. Очевидно, что не все наборы длины n сравнимы между собой относительно этого порядка. Это показывает следующий

Пример 7.8 При $n=2$ наборы $(0,1)$ и $(1,0)$ не сравнимы между собой. Действительно, утверждение $(0,1)\sqsubseteq(1,0)$ равносильно по определению тому, что $0 \le 1$ и $1 \le 0$. Поскольку второе утверждение ложно, то нельзя сказать что верно $(0,1)\sqsubseteq(1,0)$. Аналогично, неверно, что $(1,0)\sqsubseteq(0,1)$. При $n=4$ набор (0,1,0,1) тотально и лексикографически (см. начало раздела 5) меньше набора (0,1,1,1), однако с набором (0,1,1,0) тотально он не сравним, хотя меньше его лексикографически. В общем случае, понятно, что несравнимые наборы – это те, в которых есть некоторые координаты типа $(\ldots,0,\ldots,1,\ldots)$ в одном наборе и $(\ldots,1,\ldots,0,\ldots)$ в другом на соответствующих местах.

Лемма 7.2 *Отношение «тотально не больше» – частичный порядок, т.е. оно рефлексивно, антисимметрично и транзитивно*.

Упражнение 7.5 *Докажите эту лемму.*

Функция от n переменных называется *монотонной*, если на тотально меньшем наборе она принимает меньшее или равное значение. Разумеется, эти неравенства должны проверяться только на сравнимых наборах.

Пример 7.9 В таблице 6.3 функции f_0, f_1 (константы 0 и 1, соответственно) являются монотонными функциями, а функции $\bar{x}$, $x \to y$ – нет.

Лексикографический (естественный – см. начало раздела 6) порядок значений переменных обеспечивает тот факт, что если какой-то набор тотально меньше другого набора, то он обязательно расположен в таблице истинности *выше* «большего» набора. Обратное – не верно! Поэтому *если в таблице истинности (при естественном порядке набора переменных) вверху стоят нули, а затем единицы (без разрывов), то эта функция точно является монотонной. Однако возможны случаи, когда 1 стоит до каких-то нулей, но функция является все равно монотонной* (в этом случае наборы, соответствующие «верхней» единице и «нижнему» нулю должны быть *несравнимы*) – см. примеры 7.8 и 7.9 и упражнение 7.5.

Упражнение 7.5 *Докажите, что функция, задаваемая вектором (0,0,0,1,0,1,0,1) при естественном порядке набора переменных, является монотонной.*

Теорема 7.4 *Классы функций T_0, T_1, L, M, S замкнуты.*

Это утверждение следует непосредственно из определения самих этих классов, а также из определения замкнутости. Хотя проверка того, что после введения или удаления фиктивной переменной в монотонную функцию снова получится монотонная функция, требует определённого упорства и аккуратности [30,31].

7.3.3 В теории булевых функций очень большое значение имеет следующая теорема о полноте.

Теорема 7.5 (о полноте). *Для того чтобы некоторый набор функций K был полным, необходимо и достаточно, чтобы этот набор не содержался полностью ни в одном из классов T_0, T_1, L, M, S, т.е. чтобы для любого из этих пяти классов в наборе K имелась хотя бы одна функция, не попадающая в этот класс.*

Заметим, что необходимость этого утверждения очевидна, так как если бы все функции из набора K входили в один из перечисленных классов, то и все их суперпозиции, а значит, и замыкание набора входило бы в этот класс на основании теоремы 7.4. И класс K не мог быть полным, так как ни один из классов T_0, T_1, L, M, S не совпадает с классом всех булевых функций.

Достаточность этого утверждения доказывается довольно сложно, поэтому здесь не приводится, но с этим интересным доказательством можно познакомиться, например, по книгам [30,31].