С. С. Марченков

ЗАМКНУТЫЕ КЛАССЫ БУЛЕВЫХ ФУНКЦИЙ

МАИК НАУКА

МОСКВА
ФИЗМАТЛИТ
2000

УДК 519.7
ББК 22.176
М30

Марченков С. С. **Замкнутые классы булевых функций.** — М.: ФИЗМАТЛИТ, 2000. — 128 с. — ISBN 5-9221-0066-1.

В книге рассмотрен круг проблем, связанных с замкнутыми классами булевых функций (классами Поста). Изложено новое компактное доказательство конечной порождаемости всех классов Поста и дано описание решетки классов Поста. Рассмотрено предикатное задание классов Поста и приведено определение классов Поста в терминах некоторых стандартных предикатов. Изложены основы теории Галуа для алгебры булевых функций. Введены булевы вектор-функции, с использованием соответствий Галуа решена проблема полноты для класса всех булевых вектор-функций. Рассмотрены некоторые «сильные» операторы замыкания, которые приводят к конечным решеткам замкнутых классов.

Для научных сотрудников, работающих в области дискретной математики, а также студентов, изучающих булевы функции.

ISBN 5-9221-0066-1

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Теория булевых функций лежит в фундаменте современной дискретной математики. Наряду с булевыми предикатами булевы функции являют собой самые простые объекты дискретной природы. Язык булевых функций хорошо приспособлен для описания подразделения целого на части и взаимосвязи этих частей. Поэтому он широко используется в самых разнообразных областях человеческого знания: будь то собственно математика или кибернетика (теория множеств и математическая логика, алгебра, теория графов и комбинаторика, теория информации, теория формальных языков и языков программирования, синтез управляющих систем и распознавание образов и т. д.), техника (анализ и построение различных устройств коммутации, управления и переработки информации, включая современные ЭВМ, тестирование сложных систем и построение надежных схем из ненадежных элементов), экономика, биология или социология. Список областей, где могут применяться и с успехом применяются результаты и методы теории булевых функций, нетрудно продолжить и далее.

В вопросах приложений булевых функций наиболее часто встречаются две основные задачи: можно ли выразить (изобразить, приблизить) заданную функцию или заданный класс функций булевыми функциями из имеющегося запаса булевых функций, и если это возможно, то каким образом и с какой сложностью?

В качестве выразительных средств в этих задачах могут выступать самые разнообразные средства. Однако наиболее характерной для булевых функций является возможность осуществлять композиции (суперпозиции) функций. Соответственно этому, говоря о выразимости булевой функции f через функции системы булевых функций F, чаще всего имеют в виду, что функцию f можно получить в виде суперпозиции функций системы F.

Если в качестве средств выразимости принять операцию суперпозиции, то задачу выразимости булевых функций в самой общей форме можно представить так: для произвольного (возможно, бесконечного) множества F булевых функций описать множество всех тех булевых функций, которые выразимы в виде суперпозиции функций из F. С привлечением понятия оператора замыкания, определяемого на основе операции суперпозиции, эту же задачу можно сформулировать как задачу описания по произвольному множеству F булевых функций его замыкания $[F]$. Наконец, несколько сужая общность постановки задачи, можно говорить о задаче описания всех замкнутых классов булевых функций (классов Поста).

Эта задача в принципиальном плане была решена Э. Постом в 1921 г. (полное изложение опубликовано в 1941 г.). Однако достаточную известность результаты Поста получили лишь в середине 50-х годов. В 1965–1966 гг. в СССР и во Франции выходят книги [34, 38], где результаты Поста излагаются в более доступной форме. Книга [34] сыграла огромную роль в отечественной литературе, на многие годы определив характер исследований по замкнутым классам булевых функций.

В середине 80-х годов в связи с появлением новых идей ряд специалистов вновь обратились к результатам Поста, чтобы на основе альтернативных подходов еще более упростить их изложение, приблизив его к достигнутому уровню исследований. В результате появилось несколько совершенно различных полных версий доказательства конечной порождаемости замкнутых классов булевых функций.

В то же время круг задач, связанных с классами Поста, постоянно расширялся как за счет распространения понятий на другие функциональные объекты, так и за счет более детального исследования самих классов Поста. Все это поставило вопрос о современном компактном изложении результатов Поста, которое было бы доступно для первоначального знакомства с предметом и, с другой стороны, представляло бы основу для дальнейших исследований в этом направлении. Кроме того, на фоне нового изложения результатов Поста возникла потребность дать введение в круг идей и результатов, которые связаны с замкнутыми классами булевых функций, но пока мало представлены в литературе. Имеется в виду прежде всего предикатное задание классов Поста, теория Галуа для алгебр Поста, замкнутые классы булевых вектор-функций, различные обобщения оператора замыкания.

Изложенные соображения легли в основу создания настоящей книги. Одна из главных целей книги — дать новое, достаточно компактное доказательство конечной порождаемости классов Поста. Этой цели посвящена глава I, где приводится также традиционный материал по решению проблемы полноты в классе P_2. Центральные моменты доказательства конечной порождаемости классов

Поста взяты из работ [30, 19], в главе I они подверглись дальнейшей модификации.

В главе II исследуется предикатное задание классов Поста. Этой теме в литературе уделено сравнительно мало внимания. В главе II вводятся некоторые операции над предикатами, устанавливается связь между этими операциями и замкнутыми классами, определяемыми предикатами, в структурных терминах охарактеризовываются замкнутые классы, которые можно задать конечным числом предикатов, и для каждого из замкнутых классов, допускающих предикатное задание, приводится его предикатное задание через предикаты некоторого стандартного вида. Значительное место в главе II отведено изложению основ теории Галуа для алгебр Поста, которая позволяет, в частности, устанавливать результаты Поста принципиально иным способом, не используя по существу понятия булевой функции и суперпозиции.

В главе III изучаются замкнутые классы булевых вектор-функций — новое перспективное направление в теории булевых функций. Основное содержание главы III концентрируется вокруг проблемы полноты, которая, в отличие от проблемы полноты для булевых функций, решается альтернативным образом на основе теории Галуа для прямых произведений алгебр Поста.

В главе IV рассмотрены примеры некоторых «сильных» операторов замыкания — операторов, позволяющих «сжимать» счетную решетку замкнутых классов булевых функций до конечных размеров.

Книга адресована широкому кругу читателей. Она будет полезна научным работникам, желающим ознакомиться с замкнутыми классами булевых функций и их приложениями, а также студентам вузов, изучающим курс «Дискретная математика», аспирантам математических факультетов, специализирующимся по дискретной математике.

Для понимания основного содержания книги не требуется предварительных знаний. Некоторые элементарные сведения из математической логики, используемые в главах II–IV, можно найти, например, в книге [6].

Глава I

КОНЕЧНАЯ ПОРОЖДАЕМОСТЬ И СТРОЕНИЕ РЕШЕТКИ ЗАМКНУТЫХ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ

§ 1. Основные понятия

Булевы функции. Пусть $E_2 = \{0, 1\}$. Для любого натурального числа n через E_2^n обозначим n-ю декартову степень множества E_2, т. е. множество $E_2 \times \ldots \times E_2$ (n раз). Элементами множества E_2^n являются всевозможные упорядоченные наборы $(a_1, \ldots, a_n)$, где $a_i \in E_2$ при $1 \leqslant i \leqslant n$.

Булевой функцией называется функция, у которой как переменные, так и сама функция, принимают значения из множества E_2. Таким образом, если $f(x_1, \ldots, x_n)$ — булева функция от n переменных, то f отображает множество E_2^n во множество E_2. Булеву функцию от n переменных называют также *n-местной* булевой функцией. Множество всех булевых функций обозначим через P_2.

Существенные и фиктивные переменные. Переменная x_i называется *существенной* для функции $f(x_1, \ldots, x_i, \ldots, x_n)$, если найдутся такие значения $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, что

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Иными словами, переменная x_i является существенной для функции $f(x_1, \ldots, x_n)$, если для некоторых значений $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ одноместная функция $f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$ не равна константе. Переменная, которая не является существенной для функции f, называется *несущественной* или *фиктивной* переменной для f.

Для любого натурального n и любого i, $1 \leqslant i \leqslant n$, пусть $e_i^n(x_1, \ldots, x_i, \ldots, x_n)$ обозначает булеву функцию, значения которой совпадают со значениями переменной x_i. Таким образом, у функции $e_i^n(x_1,\ldots$ $\ldots,x_i,\ldots,x_n)$ единственной существенной переменной является переменная x_i, все остальные переменные фиктивные. Функции e_i^n называются *селекторными функциями*. Функция $e_1^1(x)$ обозначается также через x.

Равенство функций. По сложившейся в отечественной литературе традиции в функциональных построениях булевы функции принято рассматривать с точностью до несущественных переменных. Это означает, что наряду с произвольной булевой функцией f считаются также заданными все функции, которые отличаются от f только несущественными переменными. В связи с этим будем называть функции f,g *равными* и писать $f=g$, если одна из функций f,g получается из другой добавлением и (или) изъятием фиктивных переменных. Подчеркнем, что введенное отношение равенства функций отличается от отношения равенства между функциями, рассматриваемыми как отображения: первое отношение существенно шире второго, поскольку каждая булева функция порождает счетное число равных ей функций. В качестве примера отметим, что равными являются все селекторные функции $e_1^n(x_1,\ldots,x_n)$.

Формулы и реализация функций формулами. Пусть R — непустое множество булевых функций. По индукции определим понятие формулы над R. Одновременно всякой формуле над R будет сопоставлена булева функция, реализуемая этой формулой.

Пусть символом f обозначена n-местная функция из R, а $x_1,\ldots$ $\ldots,x_n$ — символы переменных. Тогда выражение $f(x_1,\ldots,x_n)$ называется *формулой над* R. Формуле $f(x_1,\ldots,x_n)$ сопоставим функцию f, *реализуемую* этой формулой.

Пусть символом g обозначена m-местная функция из R, а $\Phi_1,\ldots$ $\ldots,\Phi_m$ — либо формулы над R, либо символы переменных (не обязательно различные). Тогда выражение $g(\Phi_1,\ldots,\Phi_m)$ называется *формулой над* R. Пусть выражениям Φ_i, отличным от символов переменных (т. е. представляющим формулы над R), уже сопоставлены функции f_i. Выражениям Φ_j, которые представляют собой символы переменных $x_{p(j)}$, сопоставим функции $f_j(x_{p(j)})$, которые совпадают с функциями $e_1^1(x_{p(j)})$. Тогда формуле $g(\Phi_1,\ldots,\Phi_m)$ сопоставляем функцию $g(f_1,\ldots,f_m)$, реализуемую этой формулой. (Мы предполагаем, что читатель представляет, как определяется отображение, которое задает, например, функция

$$g(f_1(x_{11},\ldots,x_{1n_1}),\ldots,f_m(x_{m1},\ldots,x_{mn_m})),$$

где переменные $x_{11},\ldots,x_{mn_m}$ не предполагаются различными.)

Если функция f реализуется формулой, которая составлена только из символов функций $f_1, \ldots, f_s$ (а также символов переменных), то говорят, что функция f является *суперпозицией* функций $f_1, \ldots, f_s$ или что f получена *суперпозицией* функций $f_1, \ldots, f_s$.

Замыкание и замкнутые классы. Пусть R — произвольное множество булевых функций. *Замыканием* (относительно суперпозиции) множества R называется множество всех функций, которые можно реализовать формулами над R. Иными словами, замыкание R состоит из всех функций, которые являются суперпозициями функций из R. Подчеркнем еще раз, что все булевы функции мы рассматриваем с точностью до несущественных переменных.

Замыкание R будем обозначать через $[R]$. Множество R булевых функций называется (*функционально*) *замкнутым множеством*, если $R = [R]$. Замкнутые множества булевых функций принято называть также *замкнутыми классами* булевых функций или *классами Поста*.

Оператор замыкания [ ] обладает следующими легко проверяемыми свойствами (R, R_1, R_2 — произвольные множества булевых функций).

1. $R \subseteq [R]$.
2. $[[R]] = [R]$.
3. Если $R_1 \subseteq R_2$, то $[R_1] \subseteq [R_2]$.
4. $[R_1] \cup [R_2] \subseteq [R_1 \cup R_2]$.
5. $[R_1 \cap R_2] \subseteq [R_1] \cap [R_2]$.
6. $[R_1] \cap [R_2]$ — замкнутый класс.

Итеративные алгебры Поста. Существует чисто алгебраический путь определения понятий суперпозиции, замыкания и замкнутого класса. Введем следующие элементарные алгебраические операции: $\zeta, \tau, \Delta, \nabla, *$.

ζ и τ суть одноместные операции циклической перестановки переменных и транспозиции первых двух переменных. Если f — n-местная функция и $n \geqslant 2$, то n-местные функции ζf и τf определяются соотношениями

$$(\zeta f)(x_1, x_2, x_3, \ldots, x_n) = f(x_2, x_3, \ldots, x_n, x_1),$$

$$(\tau f)(x_1, x_2, x_3, \ldots, x_n) = f(x_2, x_1, x_3, \ldots, x_n).$$

Для одноместной функции f полагаем $\zeta f = \tau f = f$.

Δ есть одноместная операция отождествления первых двух переменных. Результатом выполнения операции Δ над n-местной ($n \geqslant$

$\geqslant 2$) функцией f является $(n-1)$-местная функция Δf, определяемая тождеством

$$(\Delta f)(x_1, x_2, \ldots, x_{n-1}) = f(x_1, x_1, x_2, \ldots, x_{n-1}).$$

Для одноместной функции f полагаем $\Delta f = f$.

∇ есть одноместная операция введения (первой) фиктивной переменной. Если f — n-местная функция, то

$$(\nabla f)(x_1, x_2, \ldots, x_{n+1}) = f(x_2, \ldots, x_{n+1}).$$

Наконец, $*$ есть двуместная операция подстановки. Если f — n-местная, а g — m-местная функции, то $f * g$ является $(m+n-1)$-местной функцией, которая определяется тождеством

$$(f * g)(x_1, \ldots, x_m, x_{m+1}, \ldots, x_{m+n-1}) = \\ = f(g(x_1, \ldots, x_m), x_{m+1}, \ldots, x_{m+n-1}).$$

Из определений следует, что функции $\zeta f, \tau f, \Delta f$ и $f * g$ реализуются формулами над множествами $\{f\}$ и $\{f, g\}$. Поэтому всякий замкнутый (относительно суперпозиции) класс функций R будет также замкнут относительно операций $\zeta, \tau, \Delta, *$: если $\{f, g\} \subseteq R$, то $\{\zeta f, \tau f, \Delta f, f * g\} \subseteq R$. В силу принятого выше соглашения вместе с каждой функцией классу R принадлежат и все равные ей функции. Поэтому класс R будет замкнут относительно операции ∇. Это означает, что всякий замкнутый класс является подалгеброй алгебры $\langle P_2; \zeta, \tau, \Delta, \nabla, * \rangle$, которая носит название *итеративной алгебры Поста над множеством* E_2. Вместе с тем произвольную суперпозицию нетрудно представить в виде последовательного выполнения элементарных операций $\zeta, \tau, \Delta, *$. Поэтому всякая подалгебра итеративной алгебры Поста над множеством E_2 является замкнутым классом булевых функций. Таким образом, замкнутые классы булевых функций — это в точности подалгебры алгебры $\langle P_2; \zeta, \tau, \Delta, \nabla, * \rangle$.

Порождающие множества и базисы. Будем говорить, что множество функций Q *порождает* замкнутый класс R (или класс R *порождается* множеством функций Q), если $[Q] = R$. Если множество Q порождает замкнутый класс R, то говорят также, что множество Q *полно* в классе R. При $[Q] = P_2$ множество Q называется *полным* множеством. Если замкнутый класс R порождается конечным множеством, то R называется *конечно порожденным*.

Отметим следующее очевидное утверждение, которое неоднократно используется в дальнейшем.

Пусть множество Q_1 полно в замкнутом классе R, $Q_2 \subseteq R$ и функции множества Q_1 реализуются формулами над множеством Q_2. Тогда множество Q_2 также полно в классе R.

Множество функций Q называется *базисом* замкнутого класса R, если $[Q] = R$ и $[Q_1] \neq R$ для любого подмножества Q_1 множества Q, отличного от Q.

Порядком функции называется число ее существенных переменных, *порядком* конечной системы функций — максимум из порядков входящих в нее функций. *Порядком* конечно порожденного замкнутого класса R называется максимум из порядков конечных систем функций, порождающих класс R.

Очевидно, что всякий конечно порожденный замкнутый класс имеет конечный базис. Заметим, что, вообще говоря, замкнутый класс может иметь базисы различных порядков. Однако у конечно порожденного замкнутого класса всегда имеется базис минимального порядка, т. е. порядка, совпадающего с порядком этого класса.

§ 2. Двойственность, монотонность, линейность. Критерий полноты

Следующие булевы функции будут играть основную роль на протяжении всего дальнейшего изложения: 0 (константа нуль), 1 (константа единица), $e_1^1(x) = x$ (тождественная функция), $\bar{x}$ (отрицание), xy (конъюнкция, или умножение), $x \vee y$ (дизъюнкция), $x + y$ (сложение по модулю 2). Определение этих функций приведено ниже в таблицах.

x	0	1	x	$\bar{x}$
0	0	1	0	1
1	0	1	1	0

x	y	xy	$x \vee y$	$x + y$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

Функция $\bar{f}(\bar{x}_1, \ldots, \bar{x}_n)$ называется *двойственной* к функции $f(x_1, \ldots$ $\ldots, x_n)$ и обозначается через $f^*(x_1, \ldots, x_n)$. Если $f^* = f$, то функция f называется *самодвойственной*. Множество всех самодвойственных булевых функций обозначим через S.

Поскольку $\bar{\bar{x}} = x$, для любой булевой функции имеет место равенство $f^{**} = f$. Нетрудно видеть, что двойственными друг другу являются константы 0 и 1, функции xy и $x \vee y$. Двойственной к функции $x + y$ будет функция $x + y + 1$. Функции $e_i^n(x_1, \ldots, x_n)$ и $\bar{x}$ самодвойственны.

Если R — множество булевых функций, то через R^* обозначим множество всех функций, двойственных к функциям из R. Отметим следующий очевидный факт: если $R_1 \subseteq R_2$, то $R_1^* \subseteq R_2^*$.

Следующее простое и важное утверждение часто используется в дальнейшем.

Теорема 1.1 (принцип двойственности). *Если*

$$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

то

$$f^*(x_1, \ldots, x_n) = f_0^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n)).$$

Доказательство. Пользуясь соотношением $\bar{\bar{x}} = x$ и определением двойственной функции, получаем последовательно

$$\begin{aligned}
f^*(x_1, \ldots, x_n) = \bar{f}(\bar{x}_1, \ldots, \bar{x}_n) = \\
&= \bar{f}_0(f_1(\bar{x}_1, \ldots, \bar{x}_n), \ldots, f_m(\bar{x}_1, \ldots, \bar{x}_n)) = \\
&= \bar{f}_0(\bar{\bar{f}}_1(\bar{x}_1, \ldots, \bar{x}_n), \ldots, \bar{\bar{f}}_m(\bar{x}_1, \ldots, \bar{x}_n)) = \\
&= \bar{f}_0(\bar{f}_1^*(x_1, \ldots, x_n), \ldots, \bar{f}_m^*(x_1, \ldots, x_n)) = \\
&= f_0^*(f_1^*(x_1, \ldots, x_n), \ldots, f_m^*(x_1, \ldots, x_n)).
\end{aligned}$$

Теорема доказана.

Из теоремы 1.1 легко выводятся следующие утверждения.

Следствие 1.1. *Если R — замкнутый класс, то R^* — также замкнутый класс.*

Следствие 1.2. *Множество S образует замкнутый класс.*

Следствие 1.3. *Если множество Q порождает замкнутый класс R, то множество Q^* порождает замкнутый класс R^*. В частности, если Q — базис класса R, то Q^* — базис класса R^*.*

Теорема 1.2 (о разложении по переменной). *Для произвольной булевой функции $f(x_1, \ldots, x_n)$ и любого i, $1 \leqslant i \leqslant n$, имеет место представление*

$$\begin{aligned}
f(x_1, \ldots, x_i, \ldots, x_n) = x_i \cdot f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \vee \\
\vee \bar{x}_i \cdot f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n). \quad (1.1)
\end{aligned}$$

Доказательство легко получается рассмотрением двух случаев: $x_i = 0$ и $x_i = 1$.

Следствие 1.4. $P_2 = [\{\bar{x}, xy, x \vee y\}] = [\{\bar{x}, xy\}] = [\{\bar{x}, x \vee y\}]$. *Порядок класса P_2 равен двум.*

Доказательство. Поскольку $0 = x \cdot \bar{x}$ и $1 = x \vee \bar{x}$, индукцией по n из теоремы 1.2 получаем, что система функций $\{\bar{x}, xy, x \vee \vee y\}$ полна в классе P_2. Пользуясь далее непосредственно проверяемым соотношением $x \vee y = \overline{\bar{x}\bar{y}}$, заключаем, что полной в P_2 будет система $\{\bar{x}, xy\}$. Согласно следствию 3 из теоремы 1.1 полной в P_2 будет также система $\{\bar{x}, x \vee y\}$. Таким образом, порядок класса P_2 не превосходит двух.

С другой стороны, суперпозиция функций, существенно зависящих не более чем от одной переменной, порождает функцию, которая существенно зависит также не более чем от одной переменной. Поскольку в классе P_2 имеются функции, существенно зависящие не менее чем от двух переменных (например, функции xy и $x \vee y$), заключаем, что порядок класса P_2 не меньше двух. Теорема доказана.

Замечание. В дальнейшем вместо выражений вида $[\{f_1, \ldots \ldots, f_s\}]$ будем писать $[f_1, \ldots, f_s]$.

Пусть $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ — наборы из E_2^n. Будем говорить, что набор a *не превосходит* набора b, и писать $a \leqslant b$, если для любого i, $1 \leqslant i \leqslant n$, выполняется неравенство $a_i \leqslant b_i$. Отношение $\leqslant$ между наборами задает частичный порядок на множестве E_2^n. Функция $f(x_1, \ldots, x_n)$ называется *монотонной*, если она монотонна относительно этого частичного порядка, т.е. если для любых двух наборов a, b из неравенства $a \leqslant b$ следует неравенство $f(a) \leqslant f(b)$.

Обозначим через M множество всех монотонных булевых функций. Нетрудно видеть, что множеству M принадлежат функции $0, 1$, $xy, x \vee y$ и не принадлежат функции $\bar{x}, x + y$. Докажем, что M — замкнутый класс. Пусть $f_0, f_1, \ldots, f_m \in M$,

$$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n) \ldots, f_m(x_1, \ldots, x_n)),$$

a, b — наборы из E_2^n, $a \leqslant b$, $c_i = f_i(a)$, $d_i = f_i(b)$, $1 \leqslant i \leqslant m$ и $c = (c_1, \ldots \ldots, c_m)$, $d = (d_1, \ldots, d_m)$. Тогда в силу монотонности функций $f_1, \ldots \ldots, f_m$ будем иметь $c_1 \leqslant d_1, \ldots, c_m \leqslant d_m$. Следовательно, $c \leqslant d$. Теперь в силу монотонности функции f_0 получаем $f_0(c) \leqslant f_0(d)$. Однако $f(a) = f_0(c)$ и $f(b) = f_0(d)$. Поэтому $f(a) \leqslant f(b)$, и замкнутость класса M установлена.

Из теоремы 1.2 вытекают следующие утверждения.

Следствие 1.5. *Для любой монотонной функции* $f(x_1, \ldots \ldots, x_n)$ *и любого* i, $1 \leqslant i \leqslant n$, *имеет место представление*

$$f(x_1, \ldots, x_i, \ldots, x_n) = x_1 \cdot f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \vee \vee f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n). \quad (1.2)$$

Доказательство. В самом деле, для монотонной функции f при любых значениях $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ выполняется неравенство

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) \leqslant f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n).$$

Поэтому конъюнктивный сомножитель $\bar{x}_i$ в представлении (1.1) для функции f можно опустить.

Следствие 1.6. *Если f — монотонная функция, отличная от константы, то $f \in [xy, x \vee y]$. Далее,*

$$M = [0, 1, xy, x \vee y],$$

порядок класса M равен двум.

Доказательство. Действительно, из очевидных соотношений

$$x \vee 1 = 1, \qquad x \cdot 0 = 0, \qquad 0 \vee 0 = 0$$

следует, что в представлении (1.2) для монотонной функции f, отличной от константы, функция $f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$ не равна константе 1 и хотя бы одна из функций

$$f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n), \qquad f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$$

не равна константе 0. Пользуясь теперь, если необходимо, соотношениями $x \cdot 1 = x$ и $x \vee 0 = x$, исключаем из правой части представления (1.2) функции, равные константам. К оставшимся монотонным функциям

$$f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \quad \text{и (или)} \quad f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n),$$

отличным от констант, вновь применяем разложение (1.2). В итоге приходим к соотношению $f \in [xy, x \vee y]$.

Из доказанного следует, что $M = [0, 1, xy, x \vee y]$ и что порядок класса M не превосходит двух. Вместе с тем порядок класса M не может быть меньше двух, поскольку класс M содержит функции $xy, x \vee y$, существенно зависящие от обеих переменных. Следствие доказано.

Из равенства $\bar{x} = x + 1$ и полноты системы $\{\bar{x}, xy\}$ вытекает, что система $\{1, x + y, xy\}$ полна. Функции $x + y$ и xy представляют собой соответственно сложение и умножение в поле Галуа $GF(2)$. Поэтому, пользуясь коммутативностью сложения и умножения, дистрибутивностью умножения относительно сложения и соотношениями $x + x = 0$, $x \cdot x = x$, всякую формулу над множеством $\{1, x + y, xy\}$ можно привести к эквивалентной полиномиальной форме

$$a + \sum_{(i_1, \ldots, i_s)} a_{i_1 \ldots i_s} \cdot x_{i_1} \cdot \ldots \cdot x_{i_s}, \tag{1.3}$$

где $a, a_{i_1 \ldots i_s} \in E_2$. Полином (1.3) носит название *полинома Жегалкина*. Сравнивая число булевых функций от n переменных с числом полиномов Жегалкина от n переменных, нетрудно убедиться в том, что каждая булева функция представима единственным полиномом Жегалкина.

Булева функция называется *линейной*, если ее полином Жегалкина является линейной функцией. Иными словами, функция $f(x_1, \ldots \ldots, x_n)$ является линейной, если она представима в виде

$$a_0 + a_1 x_1 + \ldots + a_n x_n, \tag{1.4}$$

где $a_0, a_1, \ldots, a_n \in E_2$. Отметим, что в представлении (1.4) выписаны все переменные функции $f(x_1, \ldots, x_n)$. Однако, если, например, $a_i = 0$, $1 \leqslant i \leqslant n$, то переменная x_i для функции $f(x_1, \ldots, x_n)$ является фиктивной и слагаемое $a_i x_i$ в представлении (1.4) можно опустить. Аналогичное замечание справедливо для представления (1.3).

Обозначим через L множество всех линейных функций. Непосредственно из определения следует, что множество L образует замкнутый класс. Легко также убедиться в том, что $L = [1, x+y]$, а порядок класса L равен двум. Классу L принадлежат функции $0, 1, \bar{x}, x+y$ и не принадлежат функции xy и $x \vee y = xy + x + y$.

Обозначим через T_0 множество всех функций f, *сохраняющих константу* 0: $f(0, \ldots, 0) = 0$. Нетрудно проверить, что множество T_0 образует замкнутый класс. Классу T_0 принадлежат функции $0, x, xy$, $x \vee y, x + y$ и не принадлежат функции $1, \bar{x}$.

Рассмотрим полином Жегалкина (1.3) для произвольной функции из класса T_0. Тогда слагаемое a необходимо равно нулю. С другой стороны, суперпозициями функции xy можно получить любую функцию вида $x_{i_1} \cdot \ldots \cdot x_{i_s}$. Следовательно, формулами над множеством $\{x+y, xy\}$ можно реализовать любой полином вида (1.3) при условии, что $a = 0$ (напомним, что $0 = x + x$). Таким образом,

$$T_0 = [x + y, xy],$$

и порядок класса T_0 равен двум.

В дальнейшем нам понадобится соотношение

$$T_0 = [\bar{x}y, x \vee y].$$

Оно вытекает из равенств

$$x + y = x\bar{y} \vee \bar{x}y, \qquad xy = \overline{\bar{x}y}y.$$

Пусть T_1 обозначает множество всех функций f, *сохраняющих константу* 1: $f(1, \ldots, 1) = 1$. Легко заметить, что классы T_0, T_1

двойственны друг другу: $T_1 = T_0^*$ и $T_0 = T_1^*$. Поэтому в силу принципа двойственности имеем

$$T_1 = [x + y + 1, x \vee y] = [\bar{x} \vee y, xy]; \tag{1.5}$$

порядок класса T_1 равен двум.

Отметим, что ни один из замкнутых классов S, M, L, T_0, T_1 целиком не содержится в объединении остальных четырех. Это вытекает из следующих соотношений:

$$\{\bar{x}, xy + xz + yz\} \subset S \setminus (M \cup L \cup T_0 \cup T_1),$$

$$\{0, 1, x \vee y\} \subset M \setminus (S \cup L \cup T_0 \cup T_1),$$

$$\{1, x + y\} \subset L \setminus (S \cup M \cup T_0 \cup T_1),$$

$$\{x + y, xy\} \subset T_0 \setminus (S \cup M \cup L \cup T_1),$$

$$\{x + y + 1, x \vee y\} \subset T_1 \setminus (S \cup M \cup L \cup T_0).$$

Введем обозначения: $x^0 = \bar{x}$, $x^1 = x$.

Лемма 1.1 (о несамодвойственной функции). *Из несамодвойственной функции путем подстановки вместо переменных функций $x, \bar{x}$ можно получить константу.*

Доказательство. Пусть $f(x_1, \ldots, x_n) \notin S$. Тогда найдется такой набор $(a_1, \ldots, a_n)$, что

$$f(a_1, \ldots, a_n) = f(\bar{a}_1, \ldots, \bar{a}_n).$$

Положим $g_i(x) = x^{a_i}$ для $1 \leqslant i \leqslant n$ и

$$g(x) = f(g_1(x), \ldots, g_n(x)).$$

Тогда

$$\begin{aligned} g(0) = f(g_1(0), \ldots, g_n(0)) = f(0^{a_1}, \ldots, 0^{a_n}) = \\ = f(\bar{a}_1, \ldots, \bar{a}_n) = f(a_1, \ldots, a_n) = \\ = f(1^{a_1}, \ldots, 1^{a_n}) = f(g_1(1), \ldots, g_n(1)) = g(1), \end{aligned}$$

и $g(x)$ — константа. Лемма доказана.

Лемма 1.2 (о немонотонной функции). *Из немонотонной функции путем подстановки вместо переменных функций $0, 1, x$ можно получить функцию $\bar{x}$.*

Доказательство. Пусть $f(x_1, \ldots, x_n) \notin M$. Тогда найдутся такие два набора $(a_1, \ldots, a_n)$ и $(b_1, \ldots, b_n)$, что $(a_1, \ldots, a_n) \leqslant (b_1, \ldots \ldots, b_n)$ и

$$f(a_1, \ldots, a_n) > f(b_1, \ldots, b_n).$$

Пусть для $1 \leqslant i \leqslant n$

$$g_i(x) = \begin{cases} 0, & \text{если} \quad a_i = b_i = 0, \\ 1, & \text{если} \quad a_i = b_i = 1, \\ x, & \text{если} \quad a_i = 0,\, b_i = 1 \end{cases}$$

(случай $a_i = 1$, $b_i = 0$ в силу соотношения $(a_1, \ldots, a_n) \leqslant (b_1, \ldots, b_n)$ невозможен). Положим

$$g(x) = f(g_1(x), \ldots, g_n(x)).$$

Тогда

$$g(0) = f(g_1(0), \ldots, g_n(0)) = f(a_1, \ldots, a_n),$$
$$g(1) = f(g_1(1), \ldots, g_n(1)) = f(b_1, \ldots, b_n).$$

Значит, $g(0) > g(1)$ и $g(x) = \bar{x}$. Лемма доказана.

Лемма 1.3 (о нелинейной функции). *Из нелинейной функции путем подстановки функций вида* $0, x$ *можно получить нелинейную функцию от двух переменных.*

Доказательство. Пусть $f(x_1, \ldots, x_n) \notin L$. Тогда в полиноме Жегалкина (1.3) функции f есть нелинейное слагаемое. Выберем нелинейное слагаемое наименьшей степени. Пусть, например, оно имеет вид $x_1 \cdot \ldots \cdot x_k$ $(k \geqslant 2)$. Подставим в функцию $f(x_1, \ldots, x_n)$ вместо переменной x_1 переменную x, вместо переменных $x_2, \ldots, x_k$ — переменную y, а вместо всех остальных переменных — константу 0. Полученную функцию обозначим через $g(x, y)$. В силу минимальности степени слагаемого $x_1 \cdot \ldots \cdot x_k$ полином Жегалкина функции $g(x, y)$ будет иметь вид

$$xy + ax + by + c, \tag{1.6}$$

где $a, b, c \in E_2$. Таким образом, $g \notin L$, и лемма доказана.

Лемма 1.4. *Из нелинейной функции от двух переменных путем подстановки вместо переменных функций вида* $x, \bar{x}$ *можно получить одну из функций* xy *или* $xy + 1$.

Доказательство. Пусть $g(x, y) \notin L$. Тогда полином Жегалкина функции $g(x, y)$ имеет вид (1.6). Положим

$$h(x, y) = g(x + b, y + a)$$

(напомним, что $x + 1 = \bar{x}$). Тогда $h(x, y) = xy + ab + c$, т. е. $h(x, y) \in \{xy, xy + 1\}$. Лемма доказана.

Следующая теорема является критерием полноты в классе P_2.

Т е о р е м а 1.3 (о функциональной полноте). *Для того чтобы система функций Q была полной, необходимо и достаточно, чтобы она целиком не содержалась ни в одном из замкнутых классов S, M, L, T_0, T_1.*

Д о к а з а т е л ь с т в о. Н е о б х о д и м о с т ь. Пусть система Q полна в P_2, т. е. $[Q] = P_2$. Предположим, что система Q целиком входит в один из замкнутых классов S, M, L, T_0, T_1. Обозначим этот класс через R. Тогда в силу замкнутости класса R и свойств замыкания выполняются равенства $P_2 = [Q] = R$, т. е. $P_2 = R$. Однако каждый из классов S, M, L, T_0, T_1 отличен от P_2. Тем самым необходимость установлена.

Д о с т а т о ч н о с т ь. Пусть система Q целиком не содержится ни в одном из замкнутых классов S, M, L, T_0, T_1. Тогда системе Q принадлежат такие функции $f_S, f_M, f_L, f_{T_0}, f_{T_1}$, что

$$f_S \notin S, \qquad f_M \notin M, \qquad f_L \notin L, \qquad f_{T_0} \notin T_0, \qquad f_{T_1} \notin T_1$$

(среди этих функций могут быть и одинаковые). Положим $Q' = \{f_S, f_M, f_L, f_{T_0}, f_{T_1}\}$ и докажем, что $[Q'] = P_2$.

Сначала из функций системы Q' получим константы. Поскольку f_{T_1} не сохраняет единицу, имеет место равенство $f_{T_1}(1, \ldots, 1) = 0$. Следовательно, $f_{T_1}(x, \ldots, x)$ совпадает с одной из функций 0 или $\bar{x}$. В первом случае с помощью функции f_{T_0}, не сохраняющей 0, получаем константу 1: $f_{T_0}(0, \ldots, 0) = 1$. Во втором случае суперпозиция функций $\bar{x}$ и f_S по лемме 1.1 дает одну константу. Вторую константу получаем подстановкой этой константы в функцию f_{T_0} или f_{T_1}.

Имея константы 0, 1 и немонотонную функцию f_M, по лемме 1.2 строим функцию $\bar{x}$. Наконец, используя константы 0, 1, функцию $\bar{x}$ и нелинейную функцию f_L, с помощью лемм 1.3 и 1.4 приходим к одной из функций xy или $xy + 1$.

Таким образом, формулами над множеством Q' реализованы функции $\bar{x}$ и xy (поскольку $xy = \overline{xy + 1}$), которые образуют полную в P_2 систему. Значит, полной в P_2 системой является и система Q. Теорема доказана.

С л е д с т в и е 1.7. *Всякий замкнутый класс булевых функций, отличный от P_2, целиком содержится хотя бы в одном из классов S, M, L, T_0, T_1.*

Назовем класс R булевых функций *предполным* (или *максимальным*), если R не полон, но для любой функции f из $P_2 \setminus R$ множество $R \cup \{f\}$ является полным. Из определения вытекает, что предполный класс замкнут.

Следствие 1.8. *В P_2 существует только пять предполных классов*: S, M, L, T_0, T_1.

§ 3. Некоторые вспомогательные утверждения

В этом параграфе собраны леммы, которые составляют основу доказательства конечной порождаемости всех замкнутых классов.

Обозначим через D множество всех булевых функций, являющихся дизъюнкциями, т. е. множество всех функций $f(x_1, \ldots, x_n)$, представимых в виде

$$a_0 \vee a_1x_1 \vee \ldots \vee a_nx_n, \tag{1.7}$$

где $a_0, a_1, \ldots, a_n \in E_2$. Множеству D принадлежат функции 0, 1 и $x_1 \vee \vee x_2$, но не принадлежит, например, конъюнкция x_1x_2.

Как видно из определения, функции класса D обладают следующим свойством: если функция $f(x_1, \ldots, x_n)$ из класса D существенно зависит от переменной x_i, то в представлении (1.7) функции f имеем $a_0 = 0$, $a_i = 1$. Поэтому $f(0, \ldots, 0) = 0$ и $f(b_1, \ldots, b_{i-1}, 1, b_{i+1}, \ldots \ldots, b_n) = 1$ для любого набора $(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n)$ из E_2^{n-1}.

Исходя из определения, нетрудно показать, что множество D образует замкнутый класс.

Двойственным образом определяем множество K булевых функций, являющихся конъюнкциями, т. е. множество всех булевых функций $f(x_1, \ldots, x_n)$, которые представимы в виде

$$a_0 \cdot (a_1 \vee x_1) \cdot \ldots \cdot (a_n \vee x_n),$$

где $a_0, a_1, \ldots, a_n \in E_2$. Множество K образует замкнутый класс, $K = = D^*$ и $D = K^*$.

Будем говорить, что функция $f(x_1, \ldots, x_n)$ *не превосходит* функцию $g(x_1, \ldots, x_n)$, и писать $f \leqslant g$, если для любого набора $(a_1, \ldots \ldots, a_n)$ из E_2^n выполняется неравенство

$$f(a_1, \ldots, a_n) \leqslant g(a_1, \ldots, a_n).$$

Говорим, что функция $f(x_1, \ldots, x_n)$ *удовлетворяет условию* 0^∞, если существует такое i, $1 \leqslant i \leqslant n$, что

$$f(x_1, \ldots, x_i, \ldots, x_n) \geqslant x_i \tag{1.8}$$

(здесь, разумеется, x_i рассматривается как функция $e_i^n(x_1, \ldots, x_i, \ldots \ldots, x_n)$). Аналогичным образом, функция $f(x_1, \ldots, x_n)$ удовлетворяет условию 1^∞, если существует такое i, $1 \leqslant i \leqslant n$, что

$$f(x_1, \ldots, x_i, \ldots, x_n) \leqslant x_i.$$

Через O^∞ обозначим множество всех функций, удовлетворяющих условию 0^∞, а через I^∞ — множество всех функций, удовлетворяющих условию 1^∞.

Если $f_0, f_1, \ldots, f_m \in O^\infty$ и

$$f_0(y_1, \ldots, y_j, \ldots, y_m) \geqslant y_j, \qquad f_j(x_1, \ldots, x_i, \ldots, x_n) \geqslant x_i,$$

$$f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

то, очевидно,

$$f(x_1, \ldots, x_i, \ldots, x_n) \geqslant x_i.$$

Отсюда вытекает функциональная замкнутость класса O^∞.

Нетрудно видеть, что $I^\infty = (O^\infty)^*$. Поэтому I^∞ — также замкнутый класс. Отметим, что классу O^∞ принадлежат функции $1, x$, $x \vee y, x \vee yz$, но не принадлежит, например, функция xy; классу I^∞ принадлежат соответственно двойственные функции $0, x, xy, x(y \vee z)$, но не принадлежит функция $x \vee y$.

Пусть функция $f(x_1, \ldots, x_n)$ принадлежит классу O^∞, т. е. существует такое i, $1 \leqslant i \leqslant n$, что выполняется соотношение (1.8). Тогда дизъюнктивное добавление x_i к функции $f(x_1, \ldots, x_n)$ не изменит функции f:

$$f(x_1, \ldots, x_n) = x_i \vee f(x_1, \ldots, x_n).$$

Отсюда сразу следует, что

$$f(x_1, \ldots, x_n) = x_i \vee f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n).$$

Таким образом, функция f представима в виде

$$f(x_1, \ldots, x_n) = x_i \vee g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n),$$

где g может быть произвольной булевой функцией. Это представление имеет смысл использовать, разумеется, если $f \neq 1$. Двойственное представление справедливо для функций из класса I^∞.

Будем обозначать через $f_D, f_K, f_L, f_M, f_S, f_{T_0}, f_{T_1}$ такие булевы функции, которые не принадлежат соответственно классам D, K, L, M, S, T_0, T_1.

Лемма 1.5. *Для любых монотонных функций f_D, f_K выполняются соотношения*

$$xy \in [0, f_D], \qquad x \vee y \in [1, f_K].$$

Доказательство. Рассмотрим монотонную функцию $f_D(x_1, \ldots, x_n)$. Можно считать, что функция f_D существенно зависит от всех n переменных. Поскольку все три одноместные монотонные функции $0, 1, x$ принадлежат классу D, имеем $n \geqslant 2$. Из условия $f_D \notin$ $\notin D$ и монотонности функции f следует, что найдется набор с одной единичной компонентой, на котором функция f_D равна нулю. Пусть, например, это набор $(1, 0, \ldots, 0)$. Так как функция f_D монотонна и существенно зависит от переменной x_1, найдется такой набор $(a_2, \ldots$ $\ldots, a_n)$, что $f_D(x_1, a_2, \ldots, a_n) = x_1$. Из равенства $f_D(1, 0, \ldots, 0) = 0$ вытекает, что должно быть $(a_2, \ldots, a_n) \neq (0, \ldots, 0)$. Пусть, например,

$$a_2 = \ldots = a_s = 1, \qquad a_{s+1} = \ldots = a_n = 0, \qquad s \geqslant 2.$$

Заменяя в функции $f_D(x_1, \ldots, x_n)$ переменные $x_3, \ldots, x_s$ переменной x_2, а переменные $x_{s+1}, \ldots, x_n$ — константой 0, будем иметь

$$f_D(x_1, x_2, \ldots, x_2, 0, \ldots, 0) = x_1 x_2.$$

Двойственным образом устанавливается включение $x \vee y \in [1, f_K]$.

Лемма 1.6. *Для любых функций f_L, f_M из T_1 выполняется соотношение*

$$\bar{x} \vee y \in [1, f_L, f_M].$$

Доказательство. Рассмотрим немонотонную функцию $f_M(x_1, \ldots, x_n)$ из класса T_1. Пусть, например, функция f_M немонотонна по переменной x_1. Тогда существует такой набор $(a_2, \ldots, a_n)$, что

$$f_M(x_1, a_2, \ldots, a_n) = \bar{x}_1.$$

В силу условия $f_M \in T_1$ должно быть $(a_2, \ldots, a_n) \neq (1, \ldots, 1)$. Пусть, например,

$$a_2 = \ldots = a_k = 0, \qquad a_{k+1} = \ldots = a_n = 1, \qquad k \geqslant 2.$$

Заменяя в функции $f_M(x_1, \ldots, x_n)$ переменные $x_2, \ldots, x_k$ переменной x_2, а переменные $x_{k+1}, \ldots, x_n$ — константой 1, получим функцию

$$f_M(x_1, x_2, \ldots, x_2, 1, \ldots, 1),$$

совпадающую с одной из функций $\bar{x}_1 \vee x_2, x_1 + x_2 + 1$.

В случае функции $x_1 + x_2 + 1$ возьмем нелинейную функцию f_L из T_1. Очевидно, что $f_L^* \notin L$. Согласно лемме 1.3 из нелинейной функции f_L^* путем подстановки функций вида $0, x$ можно получить нелинейную функцию от двух переменных. Поэтому в силу принципа двойственности из функции f_L путем подстановки функций вида $1, x$ также можно получить некоторую нелинейную функцию $g(x, y)$. Поскольку $g \in T_1$, функция g может совпадать лишь с одной из функций

$$x \vee \bar{y}, \qquad \bar{x} \vee y, \qquad x \vee y, \qquad xy.$$

Доказательство леммы теперь завершают представления

$$\bar{x} \vee y = (x \vee y) + y + 1, \qquad \bar{x} \vee y = xy + x + 1.$$

Лемма 1.7. *Для любой функции f_S, сохраняющей константы 0 и 1, выполняется по крайней мере одно из соотношений*

$$xy \in [f_S], \qquad x \vee y \in [f_S].$$

Доказательство. Рассмотрим несамодвойственную функцию $f_S(x_1, \ldots, x_n)$ из класса $T_0 \cap T_1$. Очевидно, что $n \geqslant 2$. Так как $f_S \notin S$, найдется набор $(a_1, \ldots, a_n)$ такой, что

$$f_S(a_1, \ldots, a_n) = f_S(\bar{a}_1, \ldots, \bar{a}_n).$$

В силу условия $f_S \in T_0 \cap T_1$ имеем

$$(a_1, \ldots, a_n) \notin \{(0, \ldots, 0),\ (1, \ldots, 1)\}.$$

Пусть, например,

$$a_1 = \ldots = a_k = 0, \qquad a_{k+1} = \ldots = a_n = 1, \qquad 1 \leqslant k < n.$$

Заменяя в функции $f_S(x_1, \ldots, x_n)$ переменные $x_1, \ldots, x_k$ переменной x, а переменные $x_{k+1}, \ldots, x_n$ — переменной y, получим функцию $f_S(x, \ldots, x, y, \ldots, y)$, которая совпадает с одной из функций xy или $x \vee y$. Лемма доказана.

Лемма 1.8. *Пусть R — множество булевых функций, $x \vee y \in [R]$, $g \in [R]$, $f \in [R \cup \{0\}]$ и $g \leqslant f$. Тогда $f \in [R]$.*

Доказательство. Пусть Φ — формула над множеством $R \cup \{0\}$, реализующая функцию $f(x_1, \ldots, x_n)$. Заменим всякое вхождение константы 0 в формуле Φ на новую переменную y. Получим формулу над R, реализующую некоторую функцию $h(y, x_1, \ldots, x_n)$ из $[R]$, причем

$$h(0, x_1, \ldots, x_n) = f(x_1, \ldots, x_n).$$

Поскольку $g \leqslant f$, имеет место соотношение

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \vee h(g(x_1, \ldots, x_n), x_1, \ldots, x_n).$$

Таким образом, $f \in [R]$, и лемма доказана.

Положим

$$w(x, y, z) = x \vee yz, \qquad d_n(x_1, \ldots, x_n) = \bigvee_{1 \leqslant i < j \leqslant n} x_i x_j \qquad (n \geqslant 2).$$

Отметим ряд свойств функций w и d_n.

1. $w \in O^\infty$.

2. *Если* $\{f_D, f_K\} \subset M$, *то* $w \in [1, f_D, f_K]$.

В самом деле, в силу леммы 1.5 $\{xy, x \vee y\} \subset [0, 1, f_D, f_K]$. Поэтому также $w \in [0, 1, f_D, f_K]$. Вновь по лемме 1.5 имеем $x \vee y \in [1, f_K]$. Поскольку $x \leqslant w(x, y, z)$, по лемме 1.8 получаем $w \in [1, f_D, f_K]$.

3. $w \in [1, d_3]$; *если* $n > 3$, *то* $w \in [d_n]$.

В самом деле, имеем

$$d_3(x, y, 1) = x \vee y, \qquad x \vee d_3(x, y, z) = x \vee yz$$

и при $n > 3$

$$d_n(x, \ldots, x, y, z) = x \vee yz.$$

4. *Если* $n \geqslant 2$, *то* $d_n \notin O^\infty$.

5. $d_{n+1}(x_1, \ldots, x_n, 0) = d_n(x_1, \ldots, x_n)$, $d_{n+1}(x_1, \ldots, x_n, 1) = x_1 \vee \ldots \ldots \vee x_n$.

6. $d_{n+1} \in [w, d_n]$.

В самом деле, поскольку

$$d_{n+1}(x_1, \ldots, x_{n+1}) = d_n(x_1, \ldots, x_n) \vee (x_1 \vee \ldots \vee x_n)x_{n+1},$$

функцию d_{n+1} можно получить из функций w, d_n за n шагов:

$$d_{n+1}^1(x_1, \ldots, x_{n+1}) = w(d_n(x_1, \ldots, x_n), x_1, x_{n+1}) = \\ = d_n(x_1, \ldots, x_n) \vee x_1 x_{n+1},$$

$$d_{n+1}^2(x_1, \ldots, x_{n+1}) = w(d_{n+1}^1(x_1, \ldots, x_{n+1}), x_2, x_{n+1}) = \\ = d_n(x_1, \ldots, x_n) \vee x_1 x_{n+1} \vee x_2 x_{n+1},$$

. . . .

$$d_{n+1}(x_1, \ldots, x_{n+1}) = d_{n+1}^n(x_1, \ldots, x_{n+1}) = \\ = w(d_{n+1}^{n-1}(x_1, \ldots, x_{n+1}), x_n, x_{n+1}) = \\ = d_n(x_1, \ldots, x_n) \vee x_1 x_{n+1} \vee x_2 x_{n+1} \vee \ldots \vee x_n x_{n+1}.$$

7. $d_3 \in S$; *если* $n \neq 3$, *то* $d_n \notin S$.

Проверяется непосредственно.

Лемма 1.9. *Для любой монотонной функции* $f(x_1, \ldots, x_n)$ *из класса* O^∞, *отличной от константы, выполняется соотношение* $f \in \in [w]$.

Доказательство. Так как $w(x, y, y) = x \vee y$ и $w(0, x, y) = = xy$, то по следствию 1.6 из теоремы 1.2 заключаем, что $f \in [0, w]$.

Кроме того, из соотношения $f \in O^\infty$ следует, что для некоторого i, $1 \leqslant i \leqslant n$, выполняется неравенство

$$x_i \leqslant f(x_1, \ldots, x_i, \ldots, x_n).$$

Очевидно, что $e_i^n(x_1, \ldots, x_n) \in [w]$. Поэтому согласно лемме 1.8 получаем $f \in [w]$. Лемма доказана.

Для любой функции $f(x_1, \ldots, x_n)$ и любого k, $1 \leqslant k \leqslant n$, обозначим через $\mathrm{Id}_k(f)$ множество всех функций, зависящих не более чем от k переменных и полученных из функции f отождествлением переменных (быть может, пустым). Иными словами, множество $\mathrm{Id}_k(f)$ состоит из всех функций вида $f(x_{i_1}, \ldots, x_{i_n})$, где $\{i_1, \ldots, i_n\} \subseteq \{1, \ldots \ldots, n\}$ и множество $\{i_1, \ldots, i_n\}$ содержит не более k различных чисел.

Лемма 1.10. *Для любой монотонной функции* $f(x_1, \ldots, x_n)$, $n \geqslant 2$, *выполняется соотношение*

$$f \in [\{w, d_n\} \cup \mathrm{Id}_{n-1}(f)].$$

Доказательство. Утверждение очевидно, если f константа, а если $f \in O^\infty$ и $f \neq 1$, то оно следует из леммы 1.9.

Пусть $f(x_1, \ldots, x_n) \notin O^\infty$ и $f \neq 0$. Положим

$$A_f = \{w, d_n\} \cup \mathrm{Id}_{n-1}(f).$$

Дальнейшее доказательство будем вести индукцией по n. Если $n = 2$, то $f(x_1, x_2) \in \{x_1x_2, x_1 \vee x_2\}$ и $d_2(x_1, x_2) = x_1x_2$. Следовательно, функция $f(x_1, x_2)$ совпадает с одной из функций $d_2(x_1, x_2), w(x_1, x_2, x_2)$.

Предположим, что $n > 2$ и утверждение леммы справедливо для всех функций, зависящих менее чем от n переменных. Положим

$$g(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n).$$

Если $g = 0$, то по теореме 1.2 о разложении имеем

$$f(x, y, \ldots, y) = x \cdot f(1, y, \ldots, y).$$

Из соотношений $f \notin O^\infty$, $f \neq 0$ и монотонности функции f следует, что $f(1, y \ldots, y) = y$. Значит,

$$f(x, y, \ldots, y) = xy, \qquad xy \in \mathrm{Id}_{n-1}(f),$$

и утверждение леммы справедливо в силу следствия 1.6 из теоремы 1.2.

Пусть $g \neq 0$. Определим функции:

$$f_j^i = f(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n), \qquad 2 \leqslant i \leqslant n, \quad 1 \leqslant j \leqslant n, \quad i \neq j,$$

$$g_j^i = g(x_2, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n), \qquad 2 \leqslant i \leqslant n, \quad 2 \leqslant j \leqslant n, \quad i \neq j,$$

$$p(y_1, \ldots, y_n) = y_1 \cdot (y_2 \vee \ldots \vee y_n) \vee g(y_2, \ldots, y_n),$$

$$q(x_1, \ldots, x_n) = p(x_1, f_1^2, \ldots, f_1^n).$$

По предположению индукции существует формула Φ_g над множеством функций $\{w, d_{n-1}\} \cup \mathrm{Id}_{n-2}(g)$, которая реализует функцию g. Заменим всякое вхождение g_j^i в формулу Φ_g на f_j^i, а всякое вхождение d_{n-1} — на d_n, подставляя всякий раз на место первой переменной в f_j^i и d_n переменную y_1 (всякая функция из $\mathrm{Id}_{n-2}(g)$, зависящая менее чем от $n-2$ переменных, получается из подходящей функции g_j^i дальнейшим отождествлением переменных; поэтому любую функцию из $\mathrm{Id}_{n-2}(g)$ можно обозначить как $g_j^i(x_{i_1}, \ldots, x_{i_{n-2}})$). Получим формулу Φ над множеством A_f, которая реализует некоторую функцию $h(y_1, x_2, \ldots, x_n)$. Из определения функций g, f_j^i, g_j^i, свойства 5 функции d_n и построения формулы Φ следует, что

$$h(0, x_2, \ldots, x_n) = g(x_2, \ldots, x_n).$$

Далее, поскольку

$$f(1, 0, \ldots, 0) = 0, \qquad d_n(1, 0, \ldots, 0) = 0,$$

то будет выполняться также соотношение

$$p(y_1, \ldots, y_n) = y_1 \cdot (y_2 \vee \ldots \vee y_n) \vee h(y_1, \ldots, y_n).$$

Поэтому $p \in [A_f]$ и, следовательно, $q \in [A_f]$. В силу монотонности функции f для всех i, $2 \leqslant i \leqslant n$, имеем

$$x_1 \cdot f_1^i \leqslant f, \qquad f_1^i \leqslant x_i \vee f.$$

Поэтому

$$q(x_1, \ldots, x_n) = x_1 \cdot (f_1^2 \vee \ldots \vee f_1^n) \vee g(f_1^2, \ldots, f_1^n) \leqslant$$
$$\leqslant f \vee g(x_2 \vee f, \ldots, x_n \vee f) \leqslant f$$

(последнее неравенство следует из того, что $g \leqslant f$). Так как в силу следствия 1.6 из теоремы 1.2 функцию f можно реализовать формулой над множеством $\{0, w\}$, применение к функциям f и q леммы 1.8 завершает доказательство леммы 1.10.

Пусть f — монотонная функция, $f \notin O^\infty$ и $f \neq 0$. Обозначим через F_f множество всех таких функций, которые получаются из f

отождествлением переменных (быть может, пустым) и не принадлежат классу O^∞, а при всяком отождествлении любых двух переменных переходят в функции из O^∞. Пусть $p(f)$ обозначает минимальное число переменных у функций из F_f.

Поскольку $f(x,\ldots,x)=x\in O^\infty$, имеем $F_f\neq\varnothing$ и $p(f)\geqslant 2$. Кроме того, любая функция g из F_f, зависящая от $p=p(f)$ переменных, имеет вид d_p. В самом деле, из соотношения $g\notin O^\infty$ и монотонности функции g следует, что

$$g(1,0,\ldots,0)=g(0,1,0,\ldots,0)=\ldots=g(0,\ldots,0,1)=0;$$

а из последних равенств и принадлежности функций

$$g(x_1,x_1,x_3,\ldots,x_p),\qquad g(x_1,x_2,x_1,x_4,\ldots,x_p),\qquad \ldots$$
$$\ldots,\qquad g(x_1,x_2,\ldots,x_{p-1},x_1),\qquad \ldots,\qquad g(x_1,\ldots,x_{p-2},x_{p-1},x_{p-1})$$

классу O^∞ следует, что

$$g(1,1,0,\ldots,0)=g(1,0,1,0,\ldots,0)=\ldots=g(0,\ldots,0,1,1)=1.$$

Таким образом,

$$d_{p(f)}\in[f]. \tag{1.9}$$

Лемма 1.11. *Если $f(x_1,\ldots,x_n)$ — монотонная функция, $f\notin O^\infty$ и $f\neq 0$, то $f\in[w,d_{p(f)}]$.*

Доказательство. В силу леммы 1.10 имеем

$$f\in[\{w,d_n\}\cup\mathrm{Id}_{n-1}(f)].$$

Если $p(f)<n$, то применим лемму 1.10 ко всем функциям из $\mathrm{Id}_{n-1}(f)$, зависящим от $n-1$ переменных. В результате получим

$$f\in[\{w,d_n,d_{n-1}\}\cup\mathrm{Id}_{n-2}(f)].$$

Продолжая подобным образом, в итоге придем к соотношению

$$f\in[\{w,d_n,d_{n-1},\ldots,d_{p(f)}\}\cup\mathrm{Id}_{p(f)-1}(f)].$$

Однако $\mathrm{Id}_{p(f)-1}(f)\subset O^\infty$ и, значит, в силу леммы 1.9 $\mathrm{Id}_{p(f)-1}(f)\subset[w]$. Применяя теперь свойство 6, окончательно получаем $f\in[w,d_{p(f)}]$. Лемма доказана.

Пусть E — множество наборов из E_2^n. Обозначим через χ_E такую булеву функцию от n переменных, которая равна 1 на всех наборах из E и равна 0 на всех остальных наборах. Функцию χ_E назовем *характеристической функцией* множества E.

Лемма 1.12. *Для любой булевой функции f найдется монотонная функция g из $[1, x \vee y, f]$ такая, что $g \leqslant f$.*

Доказательство. Утверждение леммы очевидно, если $f \in M$. Пусть $f(x_1, \ldots, x_n) \notin M$. Если $n = 1$, то $f(x_1) = \bar{x}_1$, и в качестве функции g можно взять константу 0. Пусть $n \geqslant 2$ и функция $f(x_1, \ldots, x_n)$ немонотонна, например, по переменной x_1. Тогда найдется набор $(a_2, \ldots, a_n)$ такой, что

$$f(x_1, a_2, \ldots, a_n) = \bar{x}_1.$$

Обозначим через E множество всех таких наборов. Если $\chi_E(x_2, \ldots, x_n)$ — характеристическая функция множества E, то пусть

$$g_1(x_1, \ldots, x_n) = f(f(x_1, \ldots, x_n) \vee \chi_E(x_2, \ldots, x_n), x_2, \ldots, x_n).$$

Возьмем произвольный набор $(b_1, \ldots, b_n)$ из E_2^n. Если $(b_2, \ldots, b_n) \in E$, то в силу условия

$$f(x_1, b_2, \ldots, b_n) = \bar{x}_1$$

будем иметь

$$g_1(0, b_2, \ldots, b_n) = g_1(1, b_2, \ldots, b_n) = f(1, b_2, \ldots, b_n) = 0.$$

Если же $(b_2, \ldots, b_n) \notin E$, то либо

$$f(0, b_2, \ldots, b_n) = f(1, b_2, \ldots, b_n),$$

либо

$$f(x_1, b_2, \ldots, b_n) = x_1.$$

Поэтому

$$g_1(b_1, \ldots, b_n) = f(b_1, \ldots, b_n).$$

Таким образом, $g_1 \leqslant f$, причем функция $g_1(x_1, \ldots, x_n)$ отлична от функции $f(x_1, \ldots, x_n)$ только на наборах вида $(0, b_2, \ldots, b_n)$, где $(b_2, \ldots, b_n) \in E$ и $f(0, b_2, \ldots, b_n) = 1$.

Имеем, очевидно, $f \leqslant f \vee \chi_E$. Кроме того, согласно теореме 1.3 $[1, x \vee y, f, 0] = P_2$. Поэтому $f \vee \chi_E \in [1, x \vee y, f, 0]$. Значит, в силу леммы 1.8 $f \vee \chi_E \in [1, x \vee y, f]$. Тогда и $g_1 \in [1, x \vee y, f]$.

Если g_1 — немонотонная функция, то применим к ней описанную выше процедуру и получим функцию g_2 такую, что $g_2 \in [1, x \vee y, f]$, $g_2 \leqslant g_1 \leqslant f$ и g_2 отличается от функции g_1 только тем, что принимает значение 0 на некоторых наборах, на которых функция g_1 принимает значение 1. Продолжая подобным образом, в итоге придем к монотонной функции g такой, что $g \in [1, x \vee y, f]$ и $g \leqslant f$. Лемма доказана.

Лемма 1.13. *Пусть* $A \subseteq B \subseteq S$ *и* $[A \cup \{1\}] = [B \cup \{1\}]$. *Тогда*

$$[A] = [B] = [B \cup \{1\}] \cap S.$$

Доказательство. Очевидно, что $[A] \subseteq [B] \subseteq [B \cup \{1\}] \cap \cap S$. Пусть $f(x_1, \dots, x_n)$ — произвольная функция из $[B \cup \{1\}] \cap S$. Поскольку $[A \cup \{1\}] = [B \cup \{1\}]$, найдется формула Φ над множеством $A \cup \{1\}$, которая реализует функцию f. Заменим всякое вхождение константы 1 в формулу Φ на переменную y. Получим формулу над множеством A, которая реализует некоторую функцию $g(y, x_1, \dots \dots, x_n)$. Из соотношений $f, g \in S$ и

$$g(1, x_1, \dots, x_n) = f(x_1, \dots, x_n)$$

следует, что

$$g(0, x_1, \dots, x_n) = \bar{g}(1, \bar{x}_1, \dots, \bar{x}_n) = \bar{f}(\bar{x}_1, \dots, \bar{x}_n) = \\ = f^*(x_1, \dots, x_n) = f(x_1, \dots, x_n).$$

Значит, функция $g(y, x_1, \dots, x_n)$ не зависит существенно от переменной y и, например,

$$f(x_1, \dots, x_n) = g(x_1, x_1, \dots, x_n).$$

Таким образом,

$$[B \cup \{1\}] \cap S \subseteq [A].$$

Лемма доказана.

Лемма 1.14. *Пусть* $A \subseteq T_0$, $x \vee y \in [A]$, $B \subseteq [A]$ *и* $[A \cup \{1\}] = = [B \cup \{1\}]$. *Тогда*

$$[A] = [B \cup \{x \vee y\}] = [A \cup \{1\}] \cap T_0.$$

Доказательство. Очевидно, что

$$[B \cup \{x \vee y\}] \subseteq [A] \subseteq [A \cup \{1\}] \cap T_0.$$

Пусть $f(x_1, \dots, x_n)$ — произвольная функция из класса $[A \cup \{1\}] \cap T_0$. Поскольку $[A \cup \{1\}] = [B \cup \{1\}]$, найдется формула Φ над множеством $B \cup \{1\}$, которая реализует функцию f. Заменим всякое вхождение константы 1 в формулу Φ на $x_1 \vee \dots \vee x_n$. Получим формулу над множеством $B \cup \{x \vee y\}$. Нетрудно убедиться в том, что она реализует функцию f. Поэтому

$$[A \cup \{1\}] \cap T_0 \subseteq [B \cup \{x \vee y\}],$$

и лемма доказана.

§4. Конечная порождаемость замкнутых классов

В предыдущих параграфах были определены следующие замкнутые классы булевых функций: P_2 — множество всех булевых функций; T_0 — множество всех функций, сохраняющих константу 0; T_1 — множество всех функций, сохраняющих константу 1; S — множество всех самодвойственных функций; M — множество всех монотонных функций; L — множество всех линейных функций; D — множество всех дизъюнкций; K — множество всех конъюнкций; O^∞ — множество всех функций, удовлетворяющих условию 0^∞; I^∞ — множество всех функций, удовлетворяющих условию 1^∞.

Пусть $m \geqslant 2$. Говорят, что функция f *удовлетворяет условию* 0^m, если любые m наборов, на которых функция f равна 0, имеют общую нулевую компоненту. Аналогичным образом, функция f удовлетворяет условию 1^m, если любые m наборов, на которых функция f равна 1, имеют общую единичную компоненту.

Определим следующие множества булевых функций: O^m — множество всех функций, удовлетворяющих условию 0^m; I^m — множество всех функций, удовлетворяющих условию 1^m $(m = 2, 3, \ldots)$; U — множество всех функций, существенно зависящих не более чем от одной переменной; C — множество всех функций, которые не имеют существенных переменных (т. е. равных константам).

Отметим, что классы O^∞ и I^∞ можно определить так же, как и классы O^m, I^m. Например, множество O^∞ состоит из всех функций f, которые удовлетворяют следующему условию: все наборы, на которых функция f равна 0, имеют общую нулевую компоненту.

Нетрудно убедиться в том, что все введенные множества булевых функций являются замкнутыми классами и выполняются соотношения

$$1 \in O^\infty \subseteq \ldots \subseteq O^m \subseteq \ldots \subseteq O^2,$$

$$0 \in I^\infty \subseteq \ldots \subseteq I^m \subseteq \ldots \subseteq I^2,$$

$$(O^m)^* = I^m, \qquad (I^m)^* = O^m.$$

Положим

$T_{01} = T_0 \cap T_1$, $\quad K_{01} = K \cap T_{01}$, $\quad C_0 = C \cap T_0$,
$L_0 = L \cap T_0$, $\quad U_{01} = U \cap T_{01}$, $\quad M_0 = M \cap T_0$,
$C_1 = C \cap T_1$, $\quad MI_1^m = M \cap I_1^m$, $\quad D_1 = D \cap T_1$,
$M_1 = M \cap T_1$, $\quad SU = S \cap U$, $\quad I_1^m = I^m \cap T_1$,

$L_{01} = L \cap T_{01}$, $U_1 = U \cap T_1$, $L_1 = L \cap T_1$,
$MO^m = M \cap O^m$, $M_{01} = M \cap T_{01}$, $D_{01} = D \cap T_{01}$,
$MU = M \cap U$, $MI^m = M \cap I^m$, $S_{01} = S \cap T_{01}$,
$D_0 = D \cap T_0$, $SL = S \cap L$, $MO_0^m = M \cap O_0^m$,
$O_0^m = O^m \cap T_0$, $K_0 = K \cap T_0$, $SM = S \cap M$,
$K_1 = K \cap T_1$, $U_0 = U \cap T_0$,

$$m = 2, 3, \ldots, \infty.$$

Л е м м а 1.15. *Произвольный замкнутый класс, целиком лежащий в классе U, совпадает с одним из следующих классов.*

1. *Классы, содержащие константы* 0 *и* 1:

$$U = [0, \bar{x}], \qquad MU = [0, 1, x], \qquad C = [0, 1].$$

2. *Классы, содержащие* 0 *и не содержащие* 1:

$$U_0 = [0, x], \qquad C_0 = [0].$$

3. *Классы, содержащие* 1 *и не содержащие* 0:

$$U_1 = [1, x], \qquad C_1 = [1].$$

4. *Классы, не содержащие* 0 *и* 1:

$$SU = [\bar{x}], \qquad U_{01} = [x].$$

Порядки классов $U, MU, C, U_0, C_0, U_1, C_1, SU, U_{01}$ совпадают с порядками приведенных выше базисов и равны нулю для классов C, C_0, C_1 и единице для всех остальных классов.

Д о к а з а т е л ь с т в о. Класс U содержит ровно четыре функции, зависящие от одной переменной: $0, 1, x, \bar{x}$. Непосредственная проверка показывает, что любой замкнутый класс, целиком лежащий в классе U, совпадает с одним из классов $U, MU, C, U_0, C_0, U_1, C_1, SU$, U_{01} и имеет базис, указанный в списке (пп. 1–4). Утверждение о порядках базисов очевидно.

Л е м м а 1.16. *Произвольный замкнутый класс, целиком лежащий в одном из классов D или K и не содержащийся в классе U, совпадает с одним из следующих классов.*

1. *Классы, содержащие константы* 0 *и* 1:

$$D = [0, 1, x \vee y], \qquad K = [0, 1, xy].$$

2. *Классы, содержащие* 0 *и не содержащие* 1:

$$D_0 = [0, x \vee y], \qquad K_0 = [0, xy].$$

3. *Классы, содержащие* 1 *и не содержащие* 0:

$$D_1 = [1, x \vee y], \qquad K_1 = [1, xy].$$

4. *Классы, не содержащие* 0 *и* 1:

$$D_{01} = [x \vee y], \qquad K_{01} = [xy].$$

Порядки классов $D, K, D_0, K_0, D_1, K_1, D_{01}, K_{01}$ совпадают с порядками приведенных выше базисов и равны двум.

Доказательство. Пусть замкнутый класс F удовлетворяет условиям $F \subseteq D$ и $F \nsubseteq U$. Тогда в F входит дизъюнкция $f(x_1, \ldots \ldots, x_n)$, существенно зависящая не менее чем от двух переменных. Пусть этими переменными будут, например, переменные x_1 и x_2. Тогда (см. представление (1.7))

$$f(x_1, x_2, \ldots, x_2) = x_1 \vee x_2.$$

Суперпозициями функции $x_1 \vee x_2$ можно, очевидно, получить любую дизъюнкцию вида $x_1 \vee \ldots \vee x_m$, где $m \geqslant 1$. Если класс F не содержит дизъюнкций другого вида (т. е. констант 0 или 1), то $F = D_{01}$, и функция $x \vee y$ образует базис класса D_{01}. В противном случае в зависимости от вхождения констант 0 и 1 класс F будет совпадать с одним из классов D, D_0 или D_1, а множества $\{0, 1, x \vee y\}$, $\{0, x \vee y\}$, $\{1, x \vee y\}$ будут соответственно порождать эти классы. Тот факт, что, например, множество $\{0, 1, x \vee y\}$ является базисом класса D, вытекает из следующих соотношений:

$$\{0, 1\} \subset C, \qquad \{0, x \vee y\} \subset T_0, \qquad \{1, x \vee y\} \subset T_1.$$

Очевидно, что порядки классов D, D_0, D_1, D_{01} не могут быть меньше двух.

Двойственным образом рассматриваются классы K, K_0, K_1, K_{01}.

Лемма 1.17. *Произвольный замкнутый класс, целиком лежащий в одном из классов O^∞ или I^∞ и не содержащийся в классах D или K, совпадает с одним из следующих классов.*

1. *Классы, содержащие* 0 *и не содержащие* 1:

$$I^\infty = [\bar{x}y], \qquad MI^\infty = [0, x(y \vee z)].$$

2. *Классы, содержащие* 1 *и не содержащие* 0:

$$O^\infty = [\bar{x} \vee y], \qquad MO^\infty = [1, x \vee yz].$$

3. *Классы, не содержащие* 0 *и* 1:

$$O_0^\infty = [x \vee y\bar{z}], \quad MO_0^\infty = [x \vee yz], \quad I_1^\infty = [x(y \vee \bar{z})], \quad MI_1^\infty = [x(y \vee z)].$$

Порядки классов O^∞, I^∞ равны двум, порядки классов MO^∞, $O_0^\infty, MO_0^\infty, MI^\infty, I_1^\infty, MI_1^\infty$ равны трем.

Доказательство. Пусть F — замкнутый класс, $F \subseteq O^\infty$ и $f_D \in F \setminus D$. Рассмотрим два возможных случая.

1. $1 \in F$.

Пусть $F \subseteq M$. Поскольку $f_D \in O^\infty \setminus D$, из определения классов O^∞ и K легко следует, что в данном случае $f_D \notin K$. Пользуясь свойством 2, заключаем, что $w \in [1, f_D]$. Следовательно, $\{1, w\} \subset F$. С другой стороны, из леммы 1.9 следует, что $F \subseteq [1, w]$. Таким образом, $F = [1, w]$.

Класс MO^∞ по определению состоит из всех монотонных функций класса O^∞. В частности, в качестве класса F можно взять класс MO^∞. Поэтому

$$F = MO^\infty = [1, w] = [1, x \vee yz].$$

Пусть $F \nsubseteq M$, $f_M \in F \setminus M$. Из условия $F \subseteq O^\infty$ следует, что $F \subseteq T_1$. Из определения классов O^∞ и L нетрудно вывести, что $O^\infty \cap L = [1, x]$. Поэтому в данном случае $f_M \notin L$. Применяя лемму 1.6, заключаем, что

$$(\bar{x} \vee y) \in [1, f_M] \subseteq F.$$

Имеем, далее,

$$1 = x \vee \bar{x}, \qquad x \vee yz = \overline{\bar{y} \vee (\bar{z} \vee x))} \vee x.$$

Следовательно, по доказанному

$$[1, x \vee yz] = MO^\infty \subset F.$$

Согласно лемме 1.12 для любой функции f из O^∞ найдется такая монотонная функция g из $[1, x \vee y, f]$ (т. е. из класса MO^∞ и, значит, из класса F), что $g \leqslant f$. По теореме 1.3 $\{\bar{x} \vee y, 0\}$ — полная в P_2 система. Тогда полной будет и система $F \cup \{0\}$. Выбирая теперь в лемме 1.8 в качестве множества R класс F, получаем $f \in F$. Таким образом, $O^\infty \subseteq F$ и

$$F = O^\infty = [\bar{x} \vee y].$$

2. $1 \notin F$.

Из определения класса O^∞ следует, что $F \subseteq T_1$, а из условия $1 \notin F$ следует, что $F \subseteq T_0$. Поскольку $(O^\infty)^* = I^\infty$, $O^\infty \cap I^\infty = [x]$ и $F \nsubseteq D$, класс F содержит несамодвойственную функцию f_S. Применяя лемму 1.7, получаем

$$x \vee y \in [f_S] \qquad \text{или} \qquad xy \in [f_S].$$

Однако $xy \notin O^\infty$. Значит, $x \vee y \in F$.

Согласно рассмотренному случаю 1 имеем

$$[F \cup \{1\}] = MO^\infty \quad \text{или} \quad [F \cup \{1\}] = O^\infty.$$

Если $[F \cup \{1\}] = MO^\infty$, то имеется формула над множеством $F \cup \{1\}$, реализующая функцию $x \vee yz$. Заменим в этой формуле всякое вхождение константы 1 функцией $x \vee y \vee z$. Получим формулу над множеством F, которая в силу соотношений $F \subseteq T_0$, $x \vee yz \in T_0$ также реализует функцию $x \vee yz$. Следовательно, $x \vee yz \in F$. Если теперь выбрать в лемме 1.14 в качестве A класс F, а в качестве B множество $\{x \vee yz\}$, то будем иметь

$$F = [x \vee yz] = [F \cup \{1\}] \cap T_0 = MO^\infty \cap T_0 = MO_0^\infty.$$

Пусть $[F \cup \{1\}] = O^\infty$. Тогда существует формула над множеством $F \cup \{1\}$, которая реализует функцию $x \vee y\bar{z}$. Заменим в этой формуле всякое вхождение константы 1 функцией $x \vee y \vee z$. Получим формулу над множеством F (напомним, что $x \vee y \in F$), которая в силу соотношений $F \subseteq T_0$, $x \vee y\bar{z} \in T_0$ реализует функцию $x \vee y\bar{z}$. Итак, $x \vee y\bar{z} \in F$. Положим далее в лемме 1.14 $A = F$, $B = \{x \vee y\bar{z}\}$. Замечая, что $\bar{x} \vee y \in [1, x \vee y\bar{z}]$, имеем

$$F = [x \vee y\bar{z}] = [F \cup \{1\}] \cap T_0 = O^\infty \cap T_0 = O_0^\infty.$$

Утверждение о порядках классов $MO^\infty, O_0^\infty, MO_0^\infty$ следует из того, что всякая функция из множества $MO^\infty \cup O_0^\infty$, зависящая от двух переменных, является дизъюнкцией.

Классы $I^\infty, MI^\infty, I_1^\infty, MI_1^\infty$ двойственны соответственно классам $O^\infty, MO^\infty, O_0^\infty, MO_0^\infty$. Лемма доказана.

Лемма 1.18. *Произвольный замкнутый класс, целиком лежащий в классе L и не содержащийся в классе U, совпадает с одним из следующих классов.*

1. *Класс, содержащий* 0 *и* 1:

$$L = [1, x + y].$$

2. *Класс, содержащий* 0 *и не содержащий* 1:

$$L_0 = [x + y].$$

3. *Класс, содержащий* 1 *и не содержащий* 0:

$$L_1 = [x + y + 1].$$

4. *Классы, не содержащие* 0 *и* 1:

$$SL = [x + y + z + 1], \qquad L_{01} = [x + y + z].$$

Порядки классов L, L_0, L_1 *равны двум, порядки классов* SL, L_{01} *равны трем.*

Доказательство. Пусть F — замкнутый класс, $F \subseteq L$ и $F \nsubseteq U$. Тогда классу F принадлежит функция, существенно зависящая не менее чем от двух переменных. Пользуясь тождеством $x+x = 0$, с помощью отождествления переменных получаем из нее одну из функций

$$x + y + a, \qquad x + y + z + a,$$

где $a \in E_2$. Суперпозициями любой из этих функций можно получить функцию $x + y + z$:

$$x + (y + z + a) + a = x + y + z,$$

$$(x + y + z + a) + (x + y + z + a) + (x + y + z + a) + a = x + y + z.$$

Тождества

$$x = x + x + x, \qquad x_1 + \ldots + x_{2m+1} = (x_1 + \ldots + x_{2m-1}) + x_{2m} + x_{2m+1}$$

показывают, что классу F принадлежат все функции вида

$$x_1 + \ldots + x_{2m+1},$$

где $m \geqslant 0$. Из определения класса L_{01} следует, что произвольная функция этого класса равна сумме нечетного числа (существенных) переменных. Таким образом, $L_{01} = [x + y + z]$, порядок класса L_{01} равен трем. Кроме того, $L_{01} \subseteq F$.

Пусть $F \neq L_{01}$. Тогда классу F принадлежит функция вида

$$x_1 + \ldots + x_m + a, \tag{1.10}$$

где либо m нечетно и $a = 1$, либо m четно.

Пусть сначала m нечетно и $a = 1$. Отождествляя в функции (1.10) все переменные, получим функцию $x + 1$. Подстановка в функцию $x + 1$ функций класса L_{01} дает все функции вида (1.10), где m нечетно и $a = 1$. Таким образом, в этом случае классу F принадлежат все функции вида (1.10) с нечетным m и произвольным a. Вместе с тем из определения самодвойственности следует, что всякая самодвойственная линейная функция равна сумме нечетного числа (существенных) переменных и, возможно, константы 1. Поэтому $SL = [x + 1, x+y+z]$, порядок класса SL равен трем и $SL \subseteq F$. Из соотношений

$$x + 1 = x + x + x + 1, \qquad (x + y + z + 1) + 1 = x + y + z$$

следует также, что $SL = [x + y + z + 1]$.

Если $F \neq SL$, то в класс F входит функция вида (1.10), где m четно.

Предположим, что классу F принадлежит функция вида (1.10), где m четно и $a = 0$. Отождествляя в функции (1.10) все переменные, получим константу 0. Подстановка константы 0 в функции класса L_{01} дает все функции вида (1.10), где $a = 0$. Очевидно, что множество всех таких функций образует класс L_0. Таким образом, $L_0 = [x + y]$, порядок класса L_0 равен двум и $L_0 \subseteq F$.

Двойственным образом рассматривается случай, когда в класс F входит функция вида (1.10), где m четно и $a = 1$. В этом случае $L_1 = [x + y + 1]$, порядок класса L_1 равен двум и $L_1 \subseteq F$.

Остается рассмотреть случай, когда $L_0 \subseteq F$ и $L_1 \subseteq F$. Тогда $\{0, 1\} \subset F$ и, как нетрудно видеть, класс F совпадает с классом $L = [1, x + y]$.

Л е м м а 1.19. *Произвольный замкнутый класс, целиком лежащий в классе S и не содержащийся в классе L, совпадает с одним из следующих классов*:

$$S = [\bar{x}, xy \vee xz \vee yz], \qquad S_{01} = [\bar{x}y \vee \bar{x}z \vee yz], \qquad SM = [xy \vee xz \vee yz].$$

Порядки классов S, S_{01}, SM равны трем.

Д о к а з а т е л ь с т в о. Пусть F — замкнутый класс, $F \subseteq S$ и классу F принадлежит нелинейная функция f_L.

Если в классе F есть функция f_{T_1}, то в силу самодвойственности $f_{T_1} \notin M$. Поэтому в силу теоремы о полноте

$$[F \cup \{1\}] = [1, f_{T_1}, f_L] = P_2.$$

В силу леммы 1.13, где $A = \{f_{T_1}, f_L\}$ и $B = F$, имеем

$$F = S = [f_{T_1}, f_L].$$

Выбрав в качестве функций f_{T_1} и f_L функции $\bar{x}, xy \vee xz \vee yz$, получим

$$F = S = [\bar{x}, xy \vee xz \vee yz].$$

Пусть $F \subseteq T_1$. Предположим, что в классе F имеется функция $f_M(x_1, \ldots, x_n)$. Можно считать, что функция $f_M(x_1, \ldots, x_n)$ немонотонна по переменной x_1. Тогда найдется такой набор $(a_2, \ldots, a_n)$, что

$$f_M(x_1, a_2, \ldots, a_n) = \bar{x}_1.$$

Заменим в функции $f(x_1, \ldots, x_n)$ переменную x_1 переменной x, все переменные x_i, для которых $a_i = 0$, — переменной y, а все остальные переменные — переменной z. Полученную функцию обозначим через $g(x, y, z)$. Имеем в силу включения $f_M \in T_1 \cap S$ и определения набора $(a_2, \ldots, a_n)$

$$g(0,0,0) = g(1,0,1) = g(1,1,0) = 0, \quad g(1,1,1) = g(0,0,1) = g(0,1,0) = 1.$$

Поэтому при $g(1,0,0) = 0$ получаем $g(x, y, z) = \bar{x}y \vee \bar{x}z \vee yz$, а при $g(1,0,0) = 1$ получаем $g(x, y, z) = x + y + z$.

Согласно лемме 1.6

$$\bar{x} \vee y \in [1, f_L, f_M].$$

Если $g(x, y, z) = \bar{x}y \vee \bar{x}z \vee yz$, то $g(1, y, z) = yz$ и, значит,

$$\{\bar{x} \vee y, xy\} \subset [1, f_L, f_M].$$

Однако множество $\{\bar{x} \vee y, xy\}$ образует базис класса T_1 (см. (1.5)). Поэтому, полагая в лемме 1.13 $A = \{f_L, f_M\}$, $B = F$, получим

$$F = [f_L, f_M] = T_1 \cap S = T_{01} \cap S = S_{01}.$$

Поскольку функция $\bar{x}y \vee \bar{x}z \vee yz$ немонотонна и нелинейна, отсюда, в частности, следует, что

$$F = S_{01} = [\bar{x}y \vee \bar{x}z \vee yz].$$

Пусть $g(x, y, z) = x + y + z$. Поскольку

$$x \vee y \in [\bar{x} \vee y], \qquad x + y + 1 = g(x, y, 1)$$

и множество $\{x \vee y, x + y + 1\}$ образует базис класса T_1 (см. (1.5)), вновь приходим к тому, что система $\{1, f_L, f_M\}$ полна в T_1. Далее продолжаем, как и выше.

Предположим, что $F \subseteq M$. Нетрудно видеть, что любая функция из O^∞, существенно зависящая не менее чем от двух переменных, не является самодвойственной. Таким образом, $S \cap O^\infty = [x]$.

Если f — произвольная функция из F, существенно зависящая не менее чем от двух переменных, то согласно (1.9) имеем

$$d_{p(f)} \in [f].$$

По свойству 7 должно быть $p(f) = 3$. Лемма 1.11 показывает, что $f \in \in [w, d_{p(f)}]$, т.е. $f \in [w, d_3]$. Поскольку $w \in [1, d_3]$, имеем также $f \in \in [1, d_3]$. Следовательно, $F \subseteq [1, d_3]$ и, значит,

$$[F \cup \{1\}] = [1, d_3].$$

Полагая теперь в лемме 1.13 $A = \{d_3\}$, $B = F$, получим $F = [d_3]$. Таким образом, любой замкнутый класс F самодвойственных монотонных функций, отличный от класса $U_{01} = [x]$, совпадает с классом $[d_3]$. Это означает, что

$$F = SM = [d_3].$$

Как нетрудно убедиться, в классе S нет функций, существенно зависящих ровно от двух переменных. Поэтому порядки классов S, S_{01}, SM не могут быть меньше трех. Лемма доказана.

Лемма 1.20. *Произвольный замкнутый класс, целиком лежащий в классе T_1 и не содержащийся в классах $K, L, S, O^\infty, I^\infty$, совпадает с одним из следующих классов.*

1. *Классы, содержащие* 1 *и не содержащие* 0:

$$T_1 = [\bar{x} \vee y, xy], \qquad M_1 = [1, x \vee y, xy],$$

$$O^m = [\bar{x} \vee y, d_{m+1}], \qquad MO^m = [1, d_{m+1}], \qquad m = 2, 3, \ldots$$

2. *Классы, не содержащие* 0 *и* 1:

$$T_{01} = [x \vee y\bar{z}, xy], \qquad M_{01} = [x \vee y, xy],$$

$$O_0^m = [x \vee y\bar{z}, d_{m+1}], \qquad I_1^m = [x(y \vee \bar{z}), d^*_{m+1}], \qquad m = 2, 3, \ldots,$$

$$MO_0^2 = [x \vee y, d_3], \qquad MI_1^2 = [xy, d_3],$$

$$MO_0^m = [d_{m+1}], \qquad MI_1^m = [d^*_{m+1}], \qquad m = 3, 4, \ldots$$

Порядки перечисленных классов совпадают с порядками порождающих их базисов.

Доказательство. Пусть F — замкнутый класс, $F \subseteq T_1$, класс F содержит функции f_K, f_L, f_S и $F \nsubseteq O^\infty$, $F \nsubseteq I^\infty$.

1. Класс F содержит константу 1.

а) Пусть $F \subseteq M$. Из условия $F \nsubseteq O^\infty$ следует, что в классе F имеется функция f_D. По свойству 2 получаем

$$w \in [1, f_D, f_K] \subseteq F.$$

Пусть $m+1 = \min p(f)$, где минимум берется по всем функциям f из $F \setminus O^\infty$. Обозначим через f^{m+1} функцию из $F \setminus O^\infty$, на которой достигается этот минимум. Тогда в силу соотношения (1.9)

$$d_{m+1} \in [f^{m+1}] \subseteq F,$$

а из лемм 1.9, 1.11 и свойства 6 следует, что

$$F \subseteq [1, w, d_{m+1}].$$

Таким образом,

$$F = [1, w, d_{m+1}].$$

Если $m = 1$, то $d_{m+1}(x_1, x_2) = x_1 x_2$ и

$$[1, w, d_2] = [1, x \vee yz, xy] = [1, x \vee y, xy].$$

Следствие 1.6 из теоремы 1.2 показывает, что в этом случае

$$F = M_1 = [1, x \vee y, xy].$$

Очевидно, что порядок класса M_1 равен двум, а множество $\{1, x \vee y, xy\}$ образует базис класса M_1.

Пусть $m \geqslant 2$. Легко проверить, что $d_{m+1} \in O^m$. Поэтому $F \subseteq \subseteq MO^m$. Далее, функция d_p равна нулю на всех наборах из E_2^p, имеющих ровно одну единичную компоненту. Следовательно, $d_p \notin O^m$ при $p < m+1$. Поэтому для любой функции f из $MO^m \setminus O^\infty$ выполняется соотношение $p(f) \geqslant m + 1$. А тогда в силу леммы 1.11 и свойства 6 будем иметь $f \in [1, w, d_{m+1}]$. Таким образом, согласно лемме 1.9 и свойству 3

$$F = MO^m = [1, w, d_{m+1}] = [1, d_{m+1}].$$

Поскольку $p(f) \geqslant m+1$ для любой функции f из $MO^m \setminus O^\infty$, порядок класса MO^m равен $m+1$. Очевидно, что множество $\{1, d_{m+1}\}$ образует базис класса MO^m $(m = 2, 3, \ldots)$. В силу свойств 3 и 5 классы MO^m образуют убывающую цепочку

$$MO^2 \supset MO^3 \supset \ldots \supset MO^m \supset \ldots \supset MO^\infty.$$

б) Пусть $F \nsubseteq M$, т. е. класс F содержит функцию f_M. Согласно лемме 1.6

$$\bar{x} \vee y \in [1, f_L, f_M] \subseteq F.$$

Положим $FM = F \cap M$. Поскольку $x \vee yz \in [\bar{x} \vee y]$, класс FM содержит функции f_D и f_K. Кроме того, согласно лемме 1.12 для любой функции f из F найдется такая монотонная функция g из $[1, x \vee y, f] \subseteq F$, что $g \leqslant f$. Очевидно, если $f \notin O^\infty$, то и $g \notin O^\infty$. Поэтому из условия $F \nsubseteq O^\infty$ следует, что $FM \nsubseteq O^\infty$. Применяя теперь доказанный пункт а), заключаем, что класс FM совпадает с одним из классов M_1, MO^m $(m = 2, 3, \ldots)$.

Если $FM = M_1$, то

$$T_1 = [\bar{x} \vee y, xy] \subseteq [\{\bar{x} \vee y\} \cup M_1] = [\{\bar{x} \vee y\} \cup FM] \subseteq F.$$

Следовательно, в этом случае

$$F = T_1 = [\bar{x} \vee y, xy]. \tag{1.11}$$

Пусть $FM = MO^m$, $2 \leqslant m < \infty$. Если $f \in F$, то согласно лемме 1.12 для некоторой функции g из $FM = [1, d_{m+1}]$ выполняется $g \leqslant f$.

Замечаем, что $\{\bar{x} \vee y, 0\}$ — полная система. Поэтому если в лемме 1.8 в качестве R взять множество $\{1, \bar{x} \vee y, d_{m+1}\}$, то будем иметь

$$f \in [1, \bar{x} \vee y, d_{m+1}] = [\bar{x} \vee y, d_{m+1}].$$

Таким образом,

$$F = [\bar{x} \vee y, d_{m+1}]. \tag{1.12}$$

Каждая из функций $\bar{x} \vee y, d_{m+1}$ принадлежит классу O^m. Поэтому $F \subseteq O^m$. Вместе с тем, как уже доказано, одно из равенств (1.11) или (1.12) выполняется для любого замкнутого класса F такого, что $F \subseteq T_1$, $1 \in F$ и $F \nsubseteq L$, $F \nsubseteq M$, $F \nsubseteq O^\infty$. Соотношения $M \cap \cap O^m = MO^m = FM$ показывают, что

$$F = O^m = [\bar{x} \vee y, d_{m+1}].$$

Так же, как для классов MO^m, устанавливаем, что порядок класса O^m равен $m+1$ и $\{\bar{x} \vee y, d_{m+1}\}$ — базис класса O^m. Очевидно, имеет место цепочка включений

$$O^2 \supset O^3 \supset \ldots \supset O^m \supset \ldots \supset O^\infty.$$

2. Пусть класс F не содержит константу 1.

Очевидно, что $F \subseteq T_0$, т. е. $F \subseteq T_{01}$. Поэтому функция f_S из класса F сохраняет константы 0 и 1. Тогда по лемме 1.7 классу F принадлежит хотя бы одна из функций $x \vee y, xy$.

а) Пусть $x \vee y \in F$.

Предположим, что $F \subseteq M$. По доказанному замкнутый класс $[F \cup \{1\}]$ совпадает с одним из классов M_1 или MO^m $(m = 2, 3, \ldots)$. Если

$$[F \cup \{1\}] = M_1 = [1, x \vee y, xy],$$

то, применяя лемму 1.14 ко множествам F и $\{x \vee y, xy\}$, получим

$$F = [x \vee y, xy] = M_1 \cap T_0 = M_{01}.$$

Очевидно, что $\{x \vee y, xy\}$ — базис класса M_{01}, порядок класса M_{01} равен двум.

Пусть

$$[F \cup \{1\}] = MO^m = [1, d_{m+1}].$$

Функция d_{m+1} принадлежит классу F (см. моделирование константы 1 дизъюнкцией в доказательстве леммы 1.14). Следовательно, применяя лемму 1.14 ко множествам F и $\{d_{m+1}\}$, получим

$$F = [x \vee y, d_{m+1}] = MO^m \cap T_0 = MO_0^m.$$

При $m = 2$ система $\{x \vee y, d_3\}$ образует базис класса MO_0^2, поскольку $[x \vee y] = D_{01}$ и $[d_3] = SM$. При $m > 2$ имеем $x \vee y \in [d_{m+1}]$, и потому $\{d_{m+1}\}$ — базис класса MO_0^m. Очевидно, что порядок класса MO_0^m равен $m+1$ $(m = 2, 3, \ldots)$.

Предположим, что $F \nsubseteq M$. По доказанному класс $[F \cup \{1\}]$ совпадает с одним из классов T_1 или O^m $(m = 2, 3, \ldots)$. В случае

$$[F \cup \{1\}] = T_1 = [\bar{x} \vee y, xy]$$

лемму 1.14 применяем ко множествам F и $\{x \vee y\bar{z}, xy\}$ (принадлежность функций $x \vee y\bar{z}$ и xy классу F доказывается моделированием константы 1 дизъюнкцией, как в лемме 1.14). Получаем

$$F = [x \vee y\bar{z}, xy] = T_1 \cap T_0 = T_{01}.$$

Аналогичным образом поступаем в случае, когда

$$[F \cup \{1\}] = O^m = [\bar{x} \vee y, d_{m+1}].$$

Здесь приходим к соотношениям

$$F = [x \vee y\bar{z}, d_{m+1}] = O^m \cap T_0 = O_0^m.$$

Утверждения о базисах и порядках классов T_{01} и O_0^m устанавливаются стандартным образом.

б) Пусть $xy \in F$. Этот случай двойствен случаю а). Поэтому F совпадает с одним классов

$$MI_1^2 = [xy, d_3], \qquad MI_1^m = [d_{m+1}^*], \quad m = 3, 4, \ldots,$$
$$I_1^m = [x(y \vee \bar{z}), d_{m+1}^*], \quad m = 2, 3, \ldots$$

Двойственной к лемме 1.20 является лемма 1.21.

Лемма 1.21. *Произвольный замкнутый класс, целиком лежащий в классе T_0 и не содержащийся в классах D, L, S, I^∞ и O^∞, совпадает с одним из следующих классов.*

1. *Классы, содержащие* 0 *и не содержащие* 1:

$$T_0 = [\bar{x}y, x \vee y], \qquad M_0 = [0, x \vee y, xy],$$
$$I^m = [\bar{x}y, d_{m+1}^*], \qquad MI^m = [0, d_{m+1}^*], \qquad m = 2, 3, \ldots$$

2. *Классы, не содержащие* 0 *и* 1:

$$T_{01} = [x(y \vee \bar{z}), x \vee y], \qquad M_{01} = [x \vee y, xy],$$
$$I_1^m = [x(y \vee \bar{z}), d_{m+1}^*], \qquad O_0^m = [x \vee y\bar{z}, d_{m+1}], \qquad m = 2, 3, \ldots,$$

$$MI_1^2 = [xy, d_3], \qquad MO_0^2 = [x \vee y, d_3],$$

$$MI_1^m = [d_{m+1}^*], \qquad MO_0^m = [d_{m+1}], \qquad m = 3, 4, \ldots$$

Порядки перечисленных классов совпадают с порядками порождающих их базисов.

Теорема 1.4. *Множество замкнутых классов булевых функций исчерпывается следующим списком классов.*

1. *Классы, содержащие константы* 0 *и* 1:

$$P_2,\ L,\ M,\ D,\ K,\ U,\ MU,\ C.$$

2. *Классы, содержащие* 0 *и не содержащие* 1:

$$L_0,\ M_0,\ T_0,\ D_0,\ K_0,\ U_0,\ C_0,\ I^m,\ MI^m, \qquad m = 2, 3, \ldots, \infty.$$

3. *Классы, содержащие* 1 *и не содержащие* 0:

$$L_1,\ M_1,\ T_1,\ D_1,\ K_1,\ U_1,\ C_1,\ O^m,\ MO^m, \qquad m = 2, 3, \ldots, \infty.$$

4. *Классы, не содержащие* 0 *и* 1:

$$L_{01},\ M_{01},\ S_{01},\ T_{01},\ D_{01},\ K_{01},\ U_{01},\ S,\ SL,\ SM,\ SU,$$
$$O_0^m,\ MO_0^m,\ I_1^m,\ MI_1^m, \qquad m = 2, 3, \ldots, \infty.$$

При этом все перечисленные классы различны, а их порядки и примеры базисов приведены в табл. 1.1.

Доказательство. Пусть F — произвольный замкнутый класс булевых функций. Согласно следствию 1.7 из теоремы 1.3 класс F либо совпадает с классом P_2, либо целиком содержится в одном из замкнутых классов L, M, S, T_0, T_1.

Если $F \subseteq L$, то согласно леммам 1.18 и 1.15 класс F совпадает с одним из классов

$$L,\ L_0,\ L_1,\ SL,\ L_{01},\ U,\ MU,\ C,\ U_0,\ C_0,\ U_1,\ C_1,\ SU,\ U_{01}.$$

Если $F \subseteq S$, то согласно леммам 1.19, 1.18 и 1.15 класс F совпадает с одним из классов

$$S,\ S_{01},\ SM,\ SL,\ L_{01},\ SU,\ U_{01}.$$

Если $F \subseteq T_1$, то согласно леммам 1.15–1.20 класс F совпадает с одним из классов

$$T_1,\ M_1,\ L_1,\ D_1,\ K_1,\ U_1,\ C_1,\ T_{01},\ M_{01},\ S_{01},\ SM,\ L_{01},\ D_{01},\ K_{01},\ U_{01},$$
$$O^m,\ MO^m,\ O_0^m,\ MO_0^m,\ I_1^m,\ MI_1^m, \qquad m = 2, 3, \ldots, \infty.$$

Если $F \subseteq T_0$, то согласно леммам 1.15–1.19, 1.21 класс F совпадает с одним из классов

$$T_0,\ M_0,\ L_0, D_0,\ K_0,\ U_0,\ C_0,\ T_{01},\ M_{01},\ S_{01},\ SM,\ L_{01},\ D_{01},\ K_{01},\ U_{01},$$
$$I^m,\ MO^m,\ I_1^m,\ MI_1^m, O_0^m,\ MO_0^m, \qquad m = 2, 3, \ldots, \infty.$$

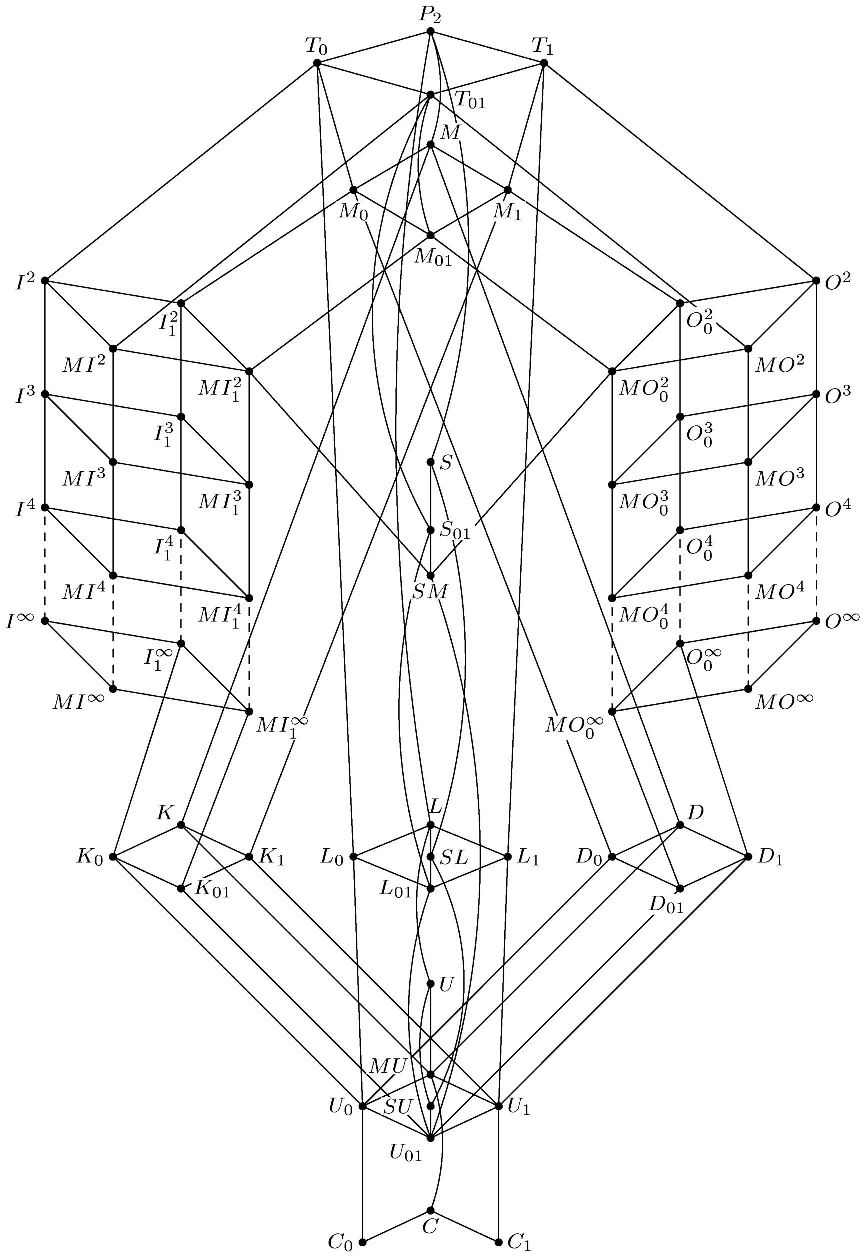
Пусть $F \subseteq M$. В силу предыдущих рассмотрений можно считать, что $F \nsubseteq T_1$, $F \nsubseteq T_0$, $F \nsubseteq D$, $F \nsubseteq K$. Из условия $F \nsubseteq T_1$ следует, что в классе F найдется такая функция f, что $f(1, \ldots, 1) = 0$. В силу монотонности функции f это означает, что $f(x, \ldots, x)$ — константа 0.

Таблица 1.1

Замкнутый класс	Обозначение у Поста	Пример базиса	Порядок
Классы, содержащие константы 0 и 1:			
P_2	C_1	$\bar{x}, x \vee y$	2
M	A_1	$0, 1, x \vee y, xy$	2
L	L_1	$1, x + y$	2
D	S_6	$0, 1, x \vee y$	2
K	P_6	$0, 1, xy$	2
U	O_9	$1, \bar{x}$	1
MU	O_8	$0, 1, x$	1
C	O_7	$0, 1$	0
Классы, содержащие 1 и не содержащие 0:			
T_1	C_2	$\bar{x} \vee y, xy$	2
M_1	A_2	$1, x \vee y, xy$	2
L_1	L_2	$x + y + 1$	2
D_1	S_3	$1, x \vee y$	2
K_1	P_5	$1, xy$	2
U_1	O_5	$1, x$	1
C_1	O_2	1	0
O^m $(m = 2, 3, \ldots)$	F_4^m	$\bar{x} \vee y, d_{m+1}$	$m+1$
MO^m $(m = 2, 3, \ldots)$	F_3^m	$1, d_{m+1}$	$m+1$
O^∞	F_4^∞	$\bar{x} \vee y$	2
MO^∞	F_3^∞	$1, x \vee yz$	3
Классы, содержащие 0 и не содержащие 1:			
T_0	C_3	$\bar{x}y, x \vee y$	2
M_0	A_3	$0, x \vee y, xy$	2

Продолжение таблицы 1.1

Замкнутый класс	Обозначение у Поста	Пример базиса	Порядок
L_0	L_3	$x+y$	2
D_0	S_5	$0, x \vee y$	2
K_0	P_3	$0, xy$	2
U_0	O_6	$0, x$	1
C_0	O_3	0	0
Классы, содержащие 0 и не содержащие 1:			
I^m $(m=2,3,\ldots)$	F_8^m	$\bar{x}y, d_{m+1}^*$	$m+1$
MI^m $(m=2,3,\ldots)$	F_7^m	$0, d_{m+1}^*$	$m+1$
I^∞	F_8^∞	$\bar{x}y$	2
MI^∞	F_7^∞	$0, x(y \vee z)$	3
Классы, не содержащие 0 и 1:			
T_{01}	C_4	$x \vee y\bar{z}$	3
S_{01}	D_1	$d_3(\bar{x}, y, z)$	3
M_{01}	A_4	$x \vee y, xy$	2
L_{01}	L_4	$x+y+z$	3
D_{01}	S_1	$x \vee y$	2
K_{01}	P_1	xy	2
U_{01}	O_1	x	1
S	D_3	$\bar{x}, d_3$	3
SM	D_2	d_3	3
SL	L_5	$x+y+z+1$	3
SU	O_4	$\bar{x}$	1
O_0^m $(m=2,3,\ldots)$	F_1^m	$x \vee y\bar{z}, d_{m+1}$	$m+1$
MO_0^2	F_2^2	$x \vee y, d_3$	3
MO_0^m $(m=3,4,\ldots)$	F_2^m	d_{m+1}	$m+1$
I_1^m $(m=2,3,\ldots)$	F_5^m	$x(y \vee \bar{z}), d_{m+1}^*$	$m+1$
MI_1^2	F_6^2	xy, d_3	3
MI_1^m $(m=3,4,\ldots)$	F_6^m	d_{m+1}^*	$m+1$
O_0^∞	F_1^∞	$x \vee y\bar{z}$	3
MO_0^∞	F_2^∞	$x \vee yz$	3
I_1^∞	F_5^∞	$x(y \vee \bar{z})$	3
MI_1^∞	F_6^∞	$x(y \vee z)$	3


P_2
T_0
T_1
T_{01}
M
M_0
M_1
M_{01}
I^2
O^2
I_1^2
O_0^2
MI^2
MO^2
MI_1^2
MO_0^2
I^3
O^3
I_1^3
O_0^3
MI^3
MO^3
MI_1^3
MO_0^3
S
S_{01}
SM
I^4
O^4
I_1^4
O_0^4
MI^4
MO^4
MI_1^4
MO_0^4
I^∞
O^∞
I_1^∞
O_0^∞
MI^∞
MO^∞
MI_1^∞
MO_0^∞
K
L
D
K_0
K_1
L_0
SL
L_1
D_0
D_1
K_{01}
L_{01}
D_{01}
U
MU
U_0
SU
U_1
U_{01}
C
C_0
C_1

Аналогичным образом, из условия $F \not\subseteq T_0$ выводим, что классу F принадлежит константа 1. Если же $\{0,1\} \subseteq F$ и $F \not\subseteq D$, $F \not\subseteq K$, то согласно лемме 1.5 $\{x \vee y, xy\} \subset F$. По следствию 1.6 из теоремы 1.2 получаем $F = [0, 1, x \vee y, xy] = M$. Теорема доказана.

Полный перечень замкнутых классов булевых функций с указанием базисов приведен в табл. 1.1. Диаграмма включений замкнутых классов представлена на рисунке.

Комментарии. Проблема описания всех замкнутых классов булевых функций поставлена Э. Постом [40]. Ему же принадлежит первое полное решение этой проблемы [40, 41]. В середине 60-х годов почти одновременно в СССР [34] и во Франции [35, 36, 38] появились работы, где с иных позиций и в более доступной форме излагались результаты Поста. В 80-е годы сразу целому ряду исследователей [32, 33, 3, 12, 4, 30, 42, 19] с использованием различных подходов и различной техники удалось получить достаточно компактные доказательства результатов Поста. В § 4, 5 мы в основном следуем изложению А. Б. Угольникова [30, 19].

Алгебраический подход в изучении замкнутых классов булевых функций (подалгебр итеративной алгебры Поста над множеством E_2) принадлежит А. И. Мальцеву [10, 11].

Глава II

ПРЕДИКАТНОЕ ОПИСАНИЕ ЗАМКНУТЫХ КЛАССОВ

§ 1. Булевы предикаты и операции над предикатами

Понятие булева предиката близко к понятию булевой функции. *Булевым предикатом* (или предикатом на множестве E_2) будем называть функцию $\rho(x_1, \ldots, x_k)$ вида $\{0,1\}^k \to \{\text{И}, \text{Л}\}$, где И, Л — истинностные значения «истина» и «ложь». Набор $(a_1, \ldots, a_k)$ удовлетворяет предикату ρ, если $\rho(a_1, \ldots, a_k) = \text{И}$. Совокупность всех булевых предикатов обозначим через $\mathcal{R}_2$. В дальнейшем слово «булев» в сочетании «булев предикат» будем, как правило, опускать.

Если предикаты $\rho(x_1, \ldots, x_k)$ и $\sigma(x_1, \ldots, x_k)$ совпадают как функции, то называем их *эквивалентными предикатами* и записываем это в виде

$$\rho(x_1, \ldots, x_k) \equiv \sigma(x_1, \ldots, x_k),$$

оставляя знак равенства для булевых функций.

Предикат $\rho(x_1, \ldots, x_k)$ нередко отождествляют с его множеством истинности, т. е. со множеством всех наборов $(a_1, \ldots, a_k)$ из E_2^k, которые удовлетворяют предикату ρ. В связи с этим тождественно истинный предикат называем *полным* предикатом, а тождественно ложный — *пустым*. Если множество истинности предиката $\rho(x_1, \ldots, x_k)$ является подмножеством множества истинности предиката $\sigma(x_1, \ldots, x_k)$, то говорят, что предикат ρ *содержится* в предикате σ или что предикат σ есть *расширение* предиката ρ.

Пусть на множестве $\{1, 2, \ldots, k\}$ задано отношение эквивалентности ε, т. е. бинарное рефлексивное, симметричное и транзитивное отношение. *Диагональю*, соответствующей отношению ε, называется такой булев предикат $\delta(x_1, \ldots, x_k)$, что

$$\delta(x_1, \ldots, x_k) \equiv \mathop{\&}_{\varepsilon(i,j)} (x_i = x_j), \tag{2.1}$$

где конъюнкция берется по всем числам i, j из $\{1, 2, \ldots, k\}$, эквивалентным в смысле отношения ε. Иными словами, для произвольного набора $(a_1, \ldots, a_k)$ из E_2^k значение $\delta(a_1, \ldots, a_k)$ истинно в том и только том случае, когда для любых чисел i, j из множества $\{1, 2, \ldots, k\}$ справедлива импликация

$$\varepsilon(i, j) \Rightarrow (a_i = a_j).$$

Если отношение эквивалентности ε единичное (т. е. ему удовлетворяют лишь пары равных чисел), то соответствующая диагональ $\delta(x_1, \ldots, x_k)$ есть

$$(x_1 = x_1) \mathbin{\&} \ldots \mathbin{\&} (x_k = x_k),$$

что представляет собой полный предикат. Если же отношение ε полное, то диагональ $\delta(x_1, \ldots, x_k)$ имеет вид

$$\mathop{\&}_{1 \leqslant i, j \leqslant k} (x_i = x_j).$$

Очевидно, что в этом случае диагонали δ удовлетворяют лишь два набора $(0, \ldots, 0), (1, \ldots, 1)$ и ее можно изобразить короче в виде

$$x_1 = x_2 = \ldots = x_k.$$

При записи диагонали по формуле (2.1) присутствующие в ней предикаты вида $x_i = x_i$ часто опускают. Так же поступают с одним из двух эквивалентных предикатов $x_i = x_j$ и $x_j = x_i$. Например, если отношению эквивалентности ε помимо пар равных чисел удовлетворяют лишь пары $(1, 2)$ и $(2, 1)$, то соответствующую диагональ δ можно записать в виде $x_1 = x_2$.

По причинам, которые будут ясны из дальнейшего, мы причисляем к диагоналям пустой (тождественно ложный) предикат.

Ввиду близости понятий булева предиката и булевой функции для булевых предикатов без специальных определений будут использоваться понятия существенной и фиктивной переменных, перестановки и отождествления переменных.

Введем две важные операции над предикатами.

Пусть $\rho(x_1, \ldots, x_k)$ — булев предикат, $1 \leqslant i \leqslant k$. *Проекцией предиката* $\rho(x_1, \ldots, x_k)$ по переменной x_i называется предикат

$$\rho(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_k) \vee \rho(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_k).$$

Проекция предиката $\rho(x_1, \ldots, x_k)$ по переменной x_i обозначается через $(\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k)$. Из определения легко усматривается, что набор $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k)$ удовлетворяет предикату $(\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k)$ в том и только том случае, когда найдется такой элемент a_i из E_2, что набор $(a_1, \ldots, a_i, \ldots, a_k)$ удовлетворяет предикату $\rho(x_1, \ldots, x_k)$. Это оправдывает название «проекция предиката» и обозначение $(\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k)$. Отметим, что $(\exists x_1)\rho(x_1)$ есть нульместный предикат, который ложен, если тождественно ложен предикат ρ, и истинен в противном случае.

Пусть $\rho(x_1, \ldots, x_k), \sigma(y_1, \ldots, y_l)$ — предикаты из $\mathcal{R}_2$. *Конъюнкцией* предикатов ρ и σ называется $(k+l)$-местный предикат, который задается формулой

$$\rho(x_1, \ldots, x_k) \mathbin{\&} \sigma(y_1, \ldots, y_l).$$

Отметим, что с использованием операций конъюнкции, переименования и отождествления переменных из предикатов $\rho(x_1, \ldots, x_k)$ и $\sigma(x_1, \ldots, x_k)$ можно получить предикат

$$\rho(x_1, \ldots, x_k) \mathbin{\&} \sigma(x_1, \ldots, x_k). \tag{2.2}$$

А именно сначала с помощью введенной операции конъюнкции предикатов образуем $2k$-местный предикат

$$\rho(x_1, \ldots, x_k) \mathbin{\&} \sigma(y_1, \ldots, y_k), \tag{2.3}$$

а затем из предиката (2.3) получаем предикат (2.2) с помощью очевидных отождествлений переменных.

Покажем, что операции проектирования и отождествления переменных перестановочны. Более точно, пусть $\rho(x_1, \ldots, x_k)$ — предикат, $k \geqslant 3$ и, например, предикат $\rho_1(x_2, \ldots, x_k)$ получается из предиката $\rho(x_1, \ldots, x_k)$ проектированием по переменной x_1, а предикат $\rho_2(x_2, \ldots, x_{k-1})$ — из предиката $\rho_1(x_2, \ldots, x_k)$ отождествлением переменных x_{k-1} и x_k:

$$\rho_1(x_2, \ldots, x_k) \equiv (\exists x_1)\rho(x_1, x_2, \ldots, x_k),$$
$$\rho_2(x_2, \ldots, x_{k-1}) \equiv \rho_1(x_2, \ldots, x_{k-1}, x_{k-1}).$$

Пусть, далее, предикат $\rho_3(x_1, \ldots, x_{k-1})$ получается из предиката $\rho(x_1, \ldots, x_k)$ отождествлением переменных x_{k-1}, x_k, а предикат $\rho_4(x_2, \ldots, x_{k-1})$ — из предиката $\rho_3(x_1, \ldots, x_{k-1})$ проектированием по переменной x_1:

$$\rho_3(x_1, \ldots, x_{k-1}) \equiv \rho(x_1, \ldots, x_{k-1}, x_{k-1}),$$
$$\rho_4(x_2, \ldots, x_{k-1}) \equiv (\exists x_1)\rho_3(x_1, x_2, \ldots, x_{k-1}).$$

Тогда

$$\rho_2(x_2, \ldots, x_{k-1}) \equiv \rho_4(x_2, \ldots, x_{k-1}).$$

Для доказательства этой эквивалентности достаточно заметить, что с использованием диагонали $x_{k-1} = x_k$ предикаты ρ_2 и ρ_4 можно выразить так:

$$\rho_2(x_2, \ldots, x_{k-1}) \equiv (\exists x_k)((\exists x_1)\rho(x_1, x_2, \ldots, x_{k-1}, x_k) \,\&\, (x_{k-1} = x_k)),$$
$$\rho_4(x_2, \ldots, x_{k-1}) \equiv (\exists x_1)((\exists x_k)(\rho(x_1, x_2, \ldots, x_{k-1}, x_k) \,\&\, (x_{k-1} = x_k))). \tag{2.4}$$

Легко видеть, что правые части формул (2.4) преобразуются друг в друга с помощью известных логических правил вынесения и перестановки кванторов существования.

В приведенных выше рассуждениях мы фактически применяли некоторые формулы с предикатами. Мы хотим далее продолжить аналогию с формулами над булевыми функциями и ввести понятия формулы над множеством булевых предикатов. Итак, пусть R — непустое множество булевых предикатов. Если ρ есть обозначение k-местного предиката из R, а $x_1, \ldots, x_k$ — различные символы переменных, то $\rho(x_1, \ldots, x_k)$ есть *формула над* R. Все переменные $x_1, \ldots$ $\ldots, x_k$ считаются свободными в формуле $\rho(x_1, \ldots, x_k)$, и эта формула не содержит связанных переменных.

Пусть $A(y_1, \ldots, y_l)$ — формула над R со свободными переменными $y_1, \ldots, y_l$, $1 \leqslant j \leqslant l$, а $x_{i_1}, \ldots, x_{i_l}$ — (не обязательно различные) символы переменных, которые отличаются от связанных переменных формулы $A(y_1, \ldots, y_l)$. Тогда

$$A(x_{i_1}, \ldots, x_{i_l}), \qquad (\exists y_j)A(y_1, \ldots, y_j, \ldots, y_l)$$

суть *формулы над* R.

Свободными переменными формулы $A(x_{i_1}, \ldots, x_{i_l})$ являются переменные $x_{i_1}, \ldots, x_{i_l}$, а связанные переменные совпадают со связанными переменными формулы $A(y_1, \ldots, y_l)$.

Свободные переменные формулы $(\exists y_j)A(y_1, \ldots, y_j, \ldots, y_l)$ суть $y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_l$, а связанные переменные образуются из связанных переменных формулы $A(y_1, \ldots, y_l)$ добавлением переменной y_j.

Если, наконец, $A(x_1, \ldots, x_k), B(y_1, \ldots, y_l)$ — формулы над R соответственно со свободными переменными $x_1, \ldots, x_k$ и $y_1, \ldots, y_l$, причем переменные формулы $A(x_1, \ldots, x_k)$ (свободные и связанные) отличны от (свободных и связанных) переменных формулы $B(y_1, \ldots, y_l)$, то

$$A(x_1, \ldots, x_k) \,\&\, B(y_1, \ldots, y_l)$$

есть *формула над* R со свободными переменными $x_1, \ldots, x_k, y_1, \ldots, y_l$, связанные переменные которой получаются объединением множеств связанных переменных формул $A(x_1, \ldots, x_k)$ и $B(y_1, \ldots, y_l)$.

Так же, как и для формул над множествами булевых функций, вводится понятие *предиката, реализуемого формулой над множеством булевых предикатов.*

Если R — множество булевых предикатов, то через $[R]$ обозначается множество всех предикатов, реализуемых формулами над R. Множество предикатов R, для которого $[R] = R$, называется *замкнутым.* Для оператора замыкания на множестве булевых предикатов справедливы те же самые свойства, которые отмечались в гл. I для оператора замыкания на множестве булевых функций.

Как и булевы функции, булевы предикаты можно рассматривать с точностью до несущественных переменных. Однако для замкнутых классов предикатов более важным свойством является наличие диагоналей. Оно позволяет естественным образом вводить фиктивные переменные. В самом деле, добавить фиктивную переменную x_{k+1} в предикат $\rho(x_1, \ldots, x_k)$ можно с помощью конъюнкции с полной диагональю $x_{k+1} = x_{k+1}$:

$$\rho(x_1, \ldots, x_k) \,\&\, (x_{k+1} = x_{k+1}).$$

Ясно, что из принадлежности одной диагонали $x_1 = x_2$ замкнутому классу предикатов R вытекает принадлежность классу R вообще всех диагоналей. Поэтому иногда в определение формулы над множеством предикатов добавляется еще один пункт, согласно которому формулой над любым множеством предикатов считается выражение $x_1 = x_2$. Это приводит к более широкому понятию замкнутого класса предикатов. Однако далее мы будем пользоваться приведенными выше определениями замыкания и замкнутого класса, оговаривая особо те случаи, когда замкнутый класс содержит все диагонали.

Замкнутые классы булевых предикатов в точности соответствуют подалгебрам алгебры

$$\langle \mathcal{R}_2; \zeta, \tau, \Delta, \exists, \& \rangle, \tag{2.5}$$

где операции ζ, τ, Δ определяются так же, как и в гл. I для булевых функций, $\exists$ — операция проектирования по первой переменной, а $\&$ — операция конъюнкции предикатов, введенная в этом параграфе. Чтобы иметь возможность рассматривать только замкнутые классы, содержащие диагонали, достаточно в сигнатуру алгебры (2.5) добавить нульместную операцию $=$, порождающую диагональ $x_1 = x_2$.

§ 2. Отношение сохранения предиката функцией

Пусть $\rho(x_1, \ldots, x_k)$ — булев предикат, $f(y_1, \ldots, y_n)$ — булева функция. Говорят, что функция $f(y_1, \ldots, y_n)$ *сохраняет предикат* $\rho(x_1, \ldots, x_k)$, если для любых n наборов

$$(a_{11}, \ldots, a_{k1}), \ldots, (a_{1n}, \ldots, a_{kn}),$$

удовлетворяющих предикату ρ, набор

$$(f(a_{11}, \ldots, a_{1n}), \ldots, f(a_{k1}, \ldots, a_{kn}))$$

также удовлетворяет предикату ρ. По определению считаем, что пустой (тождественно ложный) предикат сохраняет любая функция.

Множество истинности непустого предиката $\rho(x_1, \ldots, x_k)$ удобно изображать в виде матрицы X_ρ, состоящей из k строк. Наборы $(a_1, \ldots, a_k)$, удовлетворяющие предикату ρ, записываются в матрице X_ρ (сверху вниз) в виде столбцов, так что элемент a_1 стоит в первой строке, элемент a_2 — во второй и т. д. Порядок столбцов в матрице X_ρ, как правило, несуществен. Число столбцов матрицы X_ρ, т. е. количество наборов, удовлетворяющих предикату ρ, называется *шириной* предиката ρ. Отметим еще, что для диагонали $\delta(x_1, \ldots, x_k)$, соответствующей отношению эквивалентности ε, матрица X_δ состоит из всех столбцов размера k, в которых совпадают i-й и j-й элементы для любой пары (i, j), удовлетворяющей отношению ε.

В качестве примера рассмотрим предикат

$$\rho(x_1, x_2) \equiv (x_1 \leqslant x_2).$$

Его матрица X_ρ имеет вид

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Отношение сохранения предиката $\rho(x_1, \ldots, x_k)$ функцией $f(y_1, \ldots$ $\ldots, y_n)$ можно задать в весьма наглядной форме на «матричном» языке. Пусть матрица X_ρ предиката ρ имеет вид

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \multicolumn{4}{c}{\dotfill} \\ a_{k1} & a_{k2} & \ldots & a_{km} \end{pmatrix}. \tag{2.6}$$

Для произвольных n чисел $i_1, \ldots, i_n$, где $1 \leqslant i_1, \ldots, i_n \leqslant m$, из i_1-го, … …, i_n-го столбцов матрицы X_ρ образуем матрицу

$$\begin{pmatrix} a_{1i_1} & a_{1i_2} & \ldots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \ldots & a_{2i_n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{ki_1} & a_{ki_2} & \ldots & a_{ki_n} \end{pmatrix}. \tag{2.7}$$

Затем к ней по строкам «применим» функцию f:

$$f\begin{pmatrix} a_{1i_1} & a_{1i_2} & \ldots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \ldots & a_{2i_n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{ki_1} & a_{ki_2} & \ldots & a_{ki_n} \end{pmatrix} = \begin{pmatrix} f(a_{1i_1}, a_{1i_2}, \ldots, a_{1i_n}) \\ f(a_{2i_1}, a_{2i_2}, \ldots, a_{2i_n}) \\ \dotfill \\ f(a_{ki_1}, a_{ki_2}, \ldots, a_{ki_n}) \end{pmatrix}. \tag{2.8}$$

Полученный в результате столбец значений также должен быть столбцом матрицы X_ρ.

Для любого предиката ρ из $\mathcal{R}_2$ через $\mathrm{Pol}(\rho)$ обозначим множество всех функций, сохраняющих предикат ρ, а для любой функции f из P_2 через $\mathrm{Inv}(f)$ — множество всех предикатов, каждый из которых сохраняется функцией f.

Отметим ряд свойств множеств $\mathrm{Pol}(\rho)$ и $\mathrm{Inv}(f)$.

1. *Для любого булева предиката ρ множество* $\mathrm{Pol}(\rho)$ *содержит все селекторные функции; для любой булевой функции f множество* $\mathrm{Inv}(f)$ *содержит все диагонали.*

В самом деле, если e_i^n — селекторная функция, то при применении e_i^n к матрице (2.7) в качестве значения получается ее i-й столбец, т. е. один из столбцов матрицы (2.6) предиката ρ. Если же $\rho(x_1, \ldots, x_k)$ — диагональ и, например, в матрице (2.6) предиката ρ совпадают i-я и j-я строки, то эти же строки будут, очевидно, совпадать в матрице (2.7). Следовательно, в столбце из правой части равенства (2.8) будут равны i-й и j-й элементы. Это означает, что функция f сохраняет диагональ ρ.

Из свойства 1 вытекает, что $\mathrm{Pol}(\rho) = P_2$ для диагонали ρ и $\mathrm{Inv}(f) = \mathcal{R}_2$ для селекторной функции f.

2. *Для любого булева предиката ρ множество* $\mathrm{Pol}(\rho)$ *является замкнутым классом булевых функций.*

Поскольку классу $\mathrm{Pol}(\rho)$ принадлежат все селекторные функции, для доказательства свойства 2 достаточно установить, что из $\{f_0, f_1, \ldots, f_l\} \subseteq \mathrm{Pol}(\rho)$ и

$$f(y_1, \ldots, y_n) = f_0(f_1(y_1, \ldots, y_n), \ldots, f_l(y_1, \ldots, y_n))$$

следует $f \in \mathrm{Pol}(\rho)$. Действительно, из принадлежности функций $f_1, \ldots$ $\ldots, f_l$ множеству $\mathrm{Pol}(\rho)$ вытекает, что применение каждой из функций $f_1, \ldots, f_l$ к матрице (2.7) дает некоторый столбец из матрицы (2.6) предиката ρ. Значит, в силу включения $f_0 \in \mathrm{Pol}(\rho)$ применение функции f_0 к матрице размера $k \times l$, составленной из этих столбцов, вновь дает столбец из матрицы (2.6).

3. *Если* π *— перестановка на множестве* $\{1, 2, \ldots, k\}$ *и*

$$\sigma(x_1, \ldots, x_k) \equiv \rho(x_{\pi(1)}, \ldots, x_{\pi(k)}),$$

то $\mathrm{Pol}(\sigma) = \mathrm{Pol}(\rho)$.

В самом деле, матрица X_σ получается из матрицы X_ρ путем перестановки строк в соответствии с π^{-1}. Поэтому, применяя перестановку π^{-1} к строкам матрицы X_ρ, можно получить аналоги матрицы (2.7) и равенства (2.8). Это показывает, что $\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\sigma)$. Обратное включение доказывается аналогичным образом, поскольку матрица X_ρ в свою очередь получается из матрицы X_σ с помощью перестановки строк π.

4. *Пусть предикат* $\sigma(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$ *получается из предиката* $\rho(x_1, \ldots, x_i, \ldots, x_k)$ *проектированием по переменной* x_i:

$$\sigma(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k) \equiv (\exists x_i)\rho(x_1, \ldots, x_i, \ldots, x_k).$$

Тогда $\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\sigma)$.

Если предикат ρ пуст или $k = 1$, то предикат σ пуст или полон. В обоих случаях $\mathrm{Pol}(\sigma) = P_2$, и доказываемое включение выполняется тривиально. В остальных случаях, как нетрудно видеть, матрица X_σ получается из матрицы X_ρ вычеркиванием i-й строки (если при этом образуются одинаковые столбцы, то из каждой группы одинаковых столбцов оставляется один). Поэтому если $f \in \mathrm{Pol}(\rho)$, то для доказательства соотношения $f \in \mathrm{Pol}(\sigma)$ можно пользоваться матрицами (2.6), (2.7) и равенством (2.8), вычеркнув предварительно из них i-ю строку.

5. *Пусть предикат* σ *получается из предиката* ρ *отождествлением переменных. Тогда*

$$\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\sigma).$$

Предположим, например, что

$$\sigma(x_1, \ldots, x_k) \equiv \rho(x_1, \ldots, x_k, x_k).$$

Если предикат σ пуст, то $\mathrm{Pol}(\sigma) = P_2$, и требуемое включение выполняется тривиально. В противном случае рассмотрим произвольную функцию $f(y_1, \ldots, y_n)$ из класса $\mathrm{Pol}(\rho)$. Если каждый столбец матрицы (2.7) является столбцом матрицы X_σ, то по определению предиката σ в матрицу X_ρ будет входить каждый столбец матрицы

$$\begin{pmatrix} a_{1i_1} & a_{1i_2} & \ldots & a_{1i_n} \\ a_{2i_1} & a_{2i_2} & \ldots & a_{2i_n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{ki_1} & a_{ki_2} & \ldots & a_{ki_n} \\ a_{ki_1} & a_{ki_2} & \ldots & a_{ki_n} \end{pmatrix}.$$

Из включения $f \in \mathrm{Pol}(\rho)$ следует, что столбец

$$\begin{pmatrix} f(a_{1i_1}, a_{1i_2}, \ldots, a_{1i_n}) \\ f(a_{2i_1}, a_{2i_2}, \ldots, a_{2i_n}) \\ \dotfill \\ f(a_{ki_1}, a_{ki_2}, \ldots, a_{ki_n}) \\ f(a_{ki_1}, a_{ki_1}, \ldots, a_{ki_n}) \end{pmatrix}$$

также является столбцом матрицы X_ρ. Однако последние две компоненты этого столбца равны. Поэтому в матрицу X_σ входит столбец

$$\begin{pmatrix} f(a_{1i_1}, a_{1i_2}, \ldots, a_{1i_n}) \\ f(a_{2i_1}, a_{2i_2}, \ldots, a_{2i_n}) \\ \dotfill \\ f(a_{ki_1}, a_{ki_2}, \ldots, a_{ki_n}) \end{pmatrix},$$

что доказывает включение $f \in \mathrm{Pol}(\sigma)$.

6. *Пусть предикат $\tau(x_1, \ldots, x_k, y_1, \ldots, y_l)$ получается конъюнкцией непустых предикатов $\rho(x_1, \ldots, x_k)$ и $\sigma(y_1, \ldots, y_l)$:*

$$\tau(x_1, \ldots, x_k, y_1, \ldots, y_l) \equiv \rho(x_1, \ldots, x_k) \,\&\, \sigma(y_1, \ldots, y_l).$$

Тогда

$$\mathrm{Pol}(\tau) = \mathrm{Pol}(\rho) \cap \mathrm{Pol}(\sigma).$$

В самом деле, в силу определения предиката τ имеем

$$\rho(x_1, \ldots, x_k) \equiv (\exists y_1) \ldots (\exists y_l) \tau(x_1, \ldots, x_k, y_1, \ldots, y_l),$$

$$\sigma(y_1, \ldots, y_l) \equiv (\exists x_1) \ldots (\exists x_k) \tau(x_1, \ldots, x_k, y_1, \ldots, y_l).$$

Отсюда по свойству 4 получаем

$$\mathrm{Pol}(\tau) \subseteq \mathrm{Pol}(\rho), \qquad \mathrm{Pol}(\tau) \subseteq \mathrm{Pol}(\sigma)$$

и, следовательно,

$$\mathrm{Pol}(\tau) \subseteq \mathrm{Pol}(\rho) \cap \mathrm{Pol}(\sigma).$$

Пусть теперь $f(z_1, \ldots, z_n) \in \mathrm{Pol}(\rho) \cap \mathrm{Pol}(\sigma)$. Нетрудно видеть, что столбцы матрицы X_τ получаются из столбцов матриц X_ρ и X_σ следующим образом: берется произвольный столбец матрицы X_ρ и к нему снизу приписывается произвольный столбец матрицы X_σ. Возьмем произвольные n столбцов в матрице X_τ:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{k1} & a_{k2} & \ldots & a_{kn} \\ a_{k+1,1} & a_{k+1,2} & \ldots & a_{k+1,n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{k+l,1} & a_{k+l,2} & \ldots & a_{k+l,n} \end{pmatrix}.$$

Как отмечено, столбцы матрицы

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{k1} & a_{k2} & \ldots & a_{kn} \end{pmatrix}$$

входят в матрицу X_ρ, а столбцы матрицы

$$\begin{pmatrix} a_{k+1,1} & a_{k+1,2} & \ldots & a_{k+1,n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{k+l,1} & a_{k+l,2} & \ldots & a_{k+l,n} \end{pmatrix}$$

— в матрицу X_σ. Поэтому в силу соотношения $f \in \mathrm{Pol}(\rho)$ столбец

$$\begin{pmatrix} f(a_{11}, a_{12}, \ldots, a_{1n}) \\ \dotfill \\ f(a_{k1}, a_{k2}, \ldots, a_{kn}) \end{pmatrix}$$

будет входить в матрицу X_ρ, и в силу соотношения $f \in \mathrm{Pol}(\sigma)$ столбец

$$\begin{pmatrix} f(a_{k+1,1}, a_{k+1,2}, \ldots, a_{k+1,n}) \\ \dotfill \\ f(a_{k+l,1}, a_{k+l,2}, \ldots, a_{k+l,n}) \end{pmatrix}$$

будет входить в матрицу X_σ. Значит, столбец

$$\begin{pmatrix} f(a_{11}, a_{12}, \ldots, a_{1n}) \\ \dotfill \\ f(a_{k1}, a_{k2}, \ldots, a_{kn}) \\ f(a_{k+1,1}, a_{k+1,2}, \ldots, a_{k+1,n}) \\ \dotfill \\ f(a_{k+l,1}, a_{k+l,2}, \ldots, a_{k+l,n}) \end{pmatrix}$$

будет входить в матрицу X_τ, т. е. $f \in \mathrm{Pol}(\tau)$.

7. *Если предикаты ρ и σ отличаются только несущественными переменными, то*

$$\mathrm{Pol}(\rho) = \mathrm{Pol}(\sigma). \tag{2.9}$$

Пусть, например, предикат $\sigma(x_1, \ldots, x_k, x_{k+1})$ получается из предиката $\rho(x_1, \ldots, x_k)$ добавлением несущественной переменной x_{k+1}. Тогда

$$\sigma(x_1, \ldots, x_k, x_{k+1}) \equiv \rho(x_1, \ldots, x_k) \,\&\, (x_{k+1} = x_{k+1}).$$

Поэтому свойства 6 и 1 дают равенство (2.9).

8. *Для любой функции f из P_2 множество $\mathit{Inv}(f)$ является замкнутым классом, содержащим все диагонали.*

Это свойство есть следствие свойств 1 и 3–6.

9. *Если* $R = \mathrm{Pol}(\rho(x_1, \ldots, x_k))$, *то* $R^* = \mathrm{Pol}(\rho(\bar{x}_1, \ldots, \bar{x}_k))$.

Достаточно заметить, что матрица $\bar{X}_\rho$ предиката $\rho(\bar{x}_1, \ldots, \bar{x}_k)$ получается из матрицы X_ρ предиката $\rho(x_1, \ldots, x_k)$ заменой нулей единицами и единиц нулями.

§ 3. Соответствие Галуа

Обозначим через $\Phi(f, \rho)$ отношение «булева функция f сохраняет булев предикат ρ» на множестве $P_2 \times \mathcal{R}_2$. Отношение Φ определяет *соответствие Галуа* между подмножествами множеств P_2 и $\mathcal{R}_2$. Более подробно: если F — произвольное подмножество множества P_2, а R — произвольное подмножество множества $\mathcal{R}_2$, то пусть

$$\mathrm{Inv}(F) = \bigcap_{f \in F} \mathrm{Inv}(f), \qquad \mathrm{Pol}(R) = \bigcap_{\rho \in R} \mathrm{Pol}(\rho).$$

Из определений вытекает, что отображения Inv и Pol антимонотонны: если $F_1 \subseteq F_2$ и $R_1 \subseteq R_2$, то

$$\mathrm{Inv}(F_1) \supseteq \mathrm{Inv}(F_2), \qquad \mathrm{Pol}(R_1) \supseteq \mathrm{Pol}(R_2). \tag{2.10}$$

Кроме того, для произвольных подмножеств F из P_2 и R из $\mathcal{R}_2$ очевидным образом выполняются соотношения

$$F \subseteq \mathrm{Pol}(\mathrm{Inv}(F)), \tag{2.11}$$

$$R \subseteq \mathrm{Inv}(\mathrm{Pol}(R)). \tag{2.12}$$

Соотношения (2.10)–(2.12) показывают, что пара отображений Inv и Pol является *соответствием Галуа* между частично упорядоченными по включению множествами всех подмножеств P_2 и $\mathcal{R}_2$. Множество $\mathrm{Pol}(\mathrm{Inv}(F))$ называется *замыканием Галуа* F, а множество

$\mathrm{Inv}(\mathrm{Pol}(R))$ — *замыканием Галуа* R. Нетрудно убедиться в том, что замыкания Галуа обладают всеми свойствами обычного замыкания.

Из свойств $1, 2, 8$ § 2 вытекает, что $\mathrm{Inv}(F)$ является замкнутым классом булевых предикатов, содержащим все диагонали, а $\mathrm{Pol}(R)$ — замкнутым классом булевых функций, содержащим все селекторные функции. В частности, такими же замкнутыми классами будут замыкания Галуа $\mathrm{Pol}(\mathrm{Inv}(F))$ и $\mathrm{Inv}(\mathrm{Pol}(R))$.

Основное содержание теории Галуа для классов Поста состоит в доказательстве обратных утверждений: всякий замкнутый класс F булевых функций, содержащий все селекторные функции, представляет собой замыкание Галуа подходящего множества булевых функций; всякий замкнутый класс R булевых предикатов, содержащий все диагонали, представляет собой замыкание Галуа подходящего множества булевых предикатов. Более того, для упомянутых классов F и R имеют место равенства

$$F = \mathrm{Pol}(\mathrm{Inv}(F)), \qquad R = \mathrm{Inv}(\mathrm{Pol}(R)).$$

Доказательству этих утверждений и будет посвящена оставшаяся часть этого параграфа.

Пусть F — произвольное множество булевых функций, n — натуральное число, $\widetilde{a}_1, \widetilde{a}_2, \ldots, \widetilde{a}_{2^n}$ — все двоичные наборы длины n, расположенные в лексикографическом порядке. Назовем *n-графиком* множества F 2^n-местный предикат $\gamma_n(y_1, \ldots, y_{2^n})$, которому удовлетворяют те и только те наборы длины 2^n, которые имеют вид

$$(f(\widetilde{a}_1), f(\widetilde{a}_2), \ldots, f(\widetilde{a}_{2^n})),$$

где f — n-местная функция из F.

Теорема 2.1. *Пусть F — замкнутый класс булевых функций, содержащий все селекторные функции. Тогда* $F = \mathrm{Pol}(\mathrm{Inv}(F))$.

Доказательство. В силу справедливости включения (2.11) для доказательства теоремы достаточно установить лишь включение

$$\mathrm{Pol}(\mathrm{Inv}(F)) \subseteq F. \tag{2.13}$$

Докажем сначала, что при любом n, $n \geqslant 1$, n-график γ_n класса F принадлежит множеству $\mathrm{Inv}(F)$. Действительно, пусть $g(x_1, \ldots, x_m)$ — произвольная функция из F, а наборы

$$(a_1^1, \ldots, a_{2^n}^1), \ldots, (a_1^m, \ldots, a_{2^n}^m),$$

удовлетворяющие предикату γ_n, отвечают n-местным функциям $f_1, \ldots, f_m$ из F. Тогда набор

$$(g(a_1^1, \ldots, a_1^m), \ldots, g(a_{2^n}^1, \ldots, a_{2^n}^m)) \tag{2.14}$$

имеет вид

$$(h(\widetilde{a}_1), h(\widetilde{a}_2), \ldots, h(\widetilde{a}_{2^n})),$$

где

$$h(x_1, \ldots, x_n) = g(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

В силу замкнутости класса F n-местная функция h принадлежит классу F. Следовательно, набор (2.14) удовлетворяет предикату γ_n и $\gamma_n \in \mathrm{Inv}(F)$.

Теперь нетрудно установить включение (2.13). В самом деле, пусть $f(x_1, \ldots, x_n)$ — произвольная функция из множества

$$\mathrm{Pol}(\mathrm{Inv}(F)).$$

Тогда, в частности, f сохраняет предикат γ_n. Возьмем n наборов

$$(a_1^1, \ldots, a_{2^n}^1), \ldots, (a_1^n, \ldots, a_{2^n}^n),$$

которые удовлетворяют предикату γ_n и отвечают селекторным функциям $e_1^n, \ldots, e_n^n$. Тогда набор

$$(f(a_1^1, \ldots, a_1^n), \ldots, f(a_{2^n}^1, \ldots, a_{2^n}^n)) \tag{2.15}$$

также удовлетворяет предикату γ_n. Однако

$$f(e_1^n(x_1, \ldots, x_n), \ldots, e_n^n(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n).$$

Поэтому набор (2.15) совпадает с набором

$$(f(\widetilde{a}_1), f(\widetilde{a}_2), \ldots, f(\widetilde{a}_{2^n})).$$

А это, согласно определению предиката γ_n, означает, что $f \in F$. Теорема доказана.

Предикат ρ назовем *стандартным*, если соответствующая ему матрица X_ρ не содержит одинаковых строк.

Лемма 2.1. *Пусть F — множество булевых функций, содержащее все селекторные функции, $\rho(x_1, \ldots, x_k)$ — стандартный предикат ширины n и $\rho \in \mathrm{Inv}(F)$. Тогда ρ получается из n-графика γ_n множества F с помощью операций проектирования и перестановки переменных.*

Доказательство. Поскольку F содержит все селекторные функции, то без ограничения общности можно считать, что в матрице X_{γ_n} n-графика γ_n первые n столбцов отвечают селекторным функциям $e_1^n, \ldots, e_n^n$. Тогда любой двоичный набор длины n является началом подходящей строки матрицы X_{γ_n}.

Пусть j-я строка матрицы X_ρ предиката ρ является началом i_j-й строки матрицы X_{γ_n} $(1 \leqslant j \leqslant k)$. Так как $\rho \in \mathrm{Inv}(F)$, то, используя, если необходимо, свойство 3 из § 2, заключаем, что в подматрице матрицы X_{γ_n}, образованной строками с номерами $i_1, \ldots, i_k$, каждый столбец, начиная с $(n+1)$-го, равен одному из первых n столбцов. Следовательно, если спроектировать предикат γ_n по всем переменным, отличным от переменных $x_{i_1}, \ldots, x_{i_k}$, то получится k-местный предикат, который будет отличаться от предиката ρ, быть может, лишь перестановкой переменных. Лемма доказана.

Теорема 2.2. *Пусть R — замкнутый класс предикатов, содержащий все диагонали. Тогда $R = \mathrm{Inv}(\mathrm{Pol}(R))$.*

Доказательство. Так как включение (2.12) справедливо для любых множеств R булевых предикатов, то для доказательства теоремы достаточно установить включение

$$\mathrm{Inv}(\mathrm{Pol}(R)) \subseteq R. \tag{2.16}$$

Далее, в силу леммы 2.1 всякий стандартный предикат $\sigma_1(x_1, \ldots, x_l)$ из $\mathrm{Inv}(\mathrm{Pol}(R))$ ширины n получается из n-графика γ_n множества $\mathrm{Pol}(R)$ с помощью проектирования и перестановки переменных. Кроме того, если предикат σ_2 не является стандартным, то его можно получить из подходящего стандартного предиката с помощью формулы, содержащей диагональ. Например, если матрица X_{σ_2} предиката $\sigma_2(x_1, \ldots, x_l, x_{l+1})$ получается из матрицы X_{σ_1} предиката σ_1 повторением последней строки, то

$$\sigma_2(x_1, \ldots, x_l, x_{l+1}) \equiv \sigma_1(x_1, \ldots, x_l) \mathbin{\&} (x_l = x_{l+1}).$$

Таким образом, включение (2.16) будет доказано, если мы установим, что при любом n, $n \geqslant 1$, n-график γ_n множества $\mathrm{Pol}(R)$ реализуется некоторой формулой над множеством R.

Отметим еще, что это утверждение достаточно доказать для всех значений n, больших некоторого. В самом деле, для всякой n-местной функции f из $\mathrm{Pol}(R)$ в $\mathrm{Pol}(R)$ имеется $(n+1)$-местная функция, которая получается из f добавлением фиктивной переменной. Поэтому n-график множества $\mathrm{Pol}(R)$ можно получить из $(n+1)$-графика множества $\mathrm{Pol}(R)$ проектированием, например, по последним 2^n переменным.

Рассмотрим вначале случай, когда множество $\mathrm{Pol}(R)$ порождается одним предикатом, т. е. существует такой предикат $\rho(x_1, \ldots, x_k)$ из R, что

$$\mathrm{Pol}(R) = \mathrm{Pol}(\rho).$$

Пусть ширина предиката ρ равна s. Зафиксируем натуральное число $n, n \geqslant 2^k$, и будем предполагать, что первые n столбцов матрицы X_{γ_n} соответствуют селекторным функциям $e_1^n(x_1, \ldots, x_n), \ldots$ $\ldots, e_n^n(x_1, \ldots, x_n)$. Посмотрим, каким требованиям удовлетворяют все остальные столбцы матрицы X_{γ_n}. Очевидно, что эти требования вытекают из принадлежности соответствующих функций классу $\mathrm{Pol}(\rho)$. Именно, если в подматрице матрицы X_{γ_n}, образованной произвольными k строками, первые n столбцов принадлежат матрице X_ρ, то и остальные столбцы этой подматрицы также принадлежат матрице X_ρ. Следовательно, «максимальная» (по числу столбцов) матрица с 2^n строками, у которой в первых n столбцах расположены значения селекторных функций $e_1^n, \ldots, e_n^n$ и которая удовлетворяет сформулированному условию, и будет являться матрицей X_{γ_n}. Этими соображениями мы будем руководствоваться при построении предиката γ_n из предиката ρ.

Положим $l = s^n$ (при $s = 1$ полагаем $l = 2^n$), и пусть

$$\rho_1(x_1^1, \ldots, x_k^1, \ldots, x_1^l, \ldots, x_k^l) \equiv \rho(x_1^1, \ldots, x_k^1) \mathbin{\&} \ldots \mathbin{\&} \rho(x_1^l, \ldots, x_k^l).$$

Из определений предиката ρ_1 и операции конъюнкции следует, что в матрице X_{ρ_1} можно так расположить столбцы, что для любых (не обязательно различных) n столбцов матрицы X_ρ в матрице X_{ρ_1} найдутся такие k строк, что подматрица матрицы X_{ρ_1}, образованная этими k строками, в качестве первых n столбцов содержит указанные столбцы матрицы X_ρ. Из определения предиката ρ_1 следует также, что в качестве этих k строк всегда можно выбрать строки с номерами $ik+1, \ldots, (i+1)k$.

Мы хотели бы рассматривать матрицу X_{ρ_1} как «заготовку» для получения матрицы X_{γ_n}. Как и в матрице X_{γ_n}, первые n столбцов матрицы X_{ρ_1} будут соответствовать селекторным функциям $e_1^n, \ldots$ $\ldots, e_n^n$, а остальные столбцы — другим функциям из класса $\mathrm{Pol}(\rho)$.

Отметим все отличия матрицы X_{ρ_1} от матрицы X_{γ_n}. Во-первых, в матрице X_{ρ_1} могут содержаться различные строки, у которых совпадают начала длины n. Во-вторых, начала строк длины n в матрице X_{ρ_1} расположены не обязательно в лексикографическом порядке. В-третьих, в матрице X_{ρ_1} среди начал строк длины n могут не содержаться некоторые двоичные наборы длины n. Наконец, мы должны быть уверены в том, что в столбцах матрицы X_{ρ_1} потенциально «содержатся» все функции из класса $\mathrm{Pol}(\rho)$.

Довольно просто убедиться в выполнении последнего требования. Действительно, для любых l столбцов матрицы X_ρ в матрице X_{ρ_1} содержится столбец, который составлен из этих l столбцов.

Если вспомнить свойство, которым мы наделили первые n столбцов матрицы X_{ρ_1}, то становится понятно, что функции, потенциально «содержащиеся» в столбцах матрицы X_{ρ_1}, удовлетворяют всем требованиям сохранения предиката ρ.

Далее мы последовательно устраним отмеченные выше отличия матрицы X_{ρ_1} от матрицы X_{γ_n}.

Чтобы избавиться от первого нежелательного свойства, определим отношение эквивалентности ε на множестве $\{1, 2, \ldots, kl\}$, полагая $\varepsilon(i, j)$ истинным в том и только том случае, когда в матрице X_{ρ_1} у строк с номерами i, j совпадают начала длины n. Отождествляя в предикате ρ_1 все переменные, которым в отношении ε отвечают эквивалентные номера строк, образуем предикат ρ_2, в матрице X_{ρ_2} которого различны строки с различными началами длины n. В результате мы избавляемся от столбцов матрицы X_{ρ_1}, которые (в силу многозначности) не могут определять функции от n переменных.

Переставим далее в предикате ρ_2 переменные так, чтобы в матрице X_{ρ_3} полученного предиката $\rho_3(y_1, \ldots, y_m)$ наборы длины n, начинающие строки матрицы X_{ρ_3}, следовали в лексикографическом порядке. Если после этого окажется, что $m < 2^n$, то с помощью операции конъюнкции с полными диагоналями добавим к предикату ρ_3 фиктивные переменные $y_{m+1}, \ldots, y_{2^n}$:

$$\rho_4(y_1, \ldots, y_{2^n}) \equiv \rho_3(y_1, \ldots, y_m) \mathbin{\&} (y_{m+1} = y_{m+1}) \mathbin{\&} \ldots \mathbin{\&} (y_{2^n} = y_{2^n}).$$

Нетрудно видеть, что предикат ρ_4 и будет совпадать с предикатом γ_n.

Обратимся теперь к случаю, когда множество $\mathrm{Pol}(R)$ не порождается одним предикатом. Согласно свойству 6 из § 2, это равносильно тому, что множество $\mathrm{Pol}(R)$ не порождается конечным числом предикатов из R. Пусть поэтому $R = \{\rho_1, \rho_2, \ldots\}$. Тогда по определению отображения Pol имеем

$$\mathrm{Pol}(R) = \bigcap_{i=1}^{\infty} \mathrm{Pol}(\{\rho_1, \ldots, \rho_i\}).$$

Используя свойство 6 из § 2, перепишем это равенство в виде

$$\mathrm{Pol}(R) = \bigcap_{i=1}^{\infty} \mathrm{Pol}(\sigma_i), \tag{2.17}$$

где предикат σ_i получен конъюнкцией предикатов $\rho_1, \ldots, \rho_i$. Очевидно также, что

$$\mathrm{Pol}(\sigma_1) \supseteq \mathrm{Pol}(\sigma_2) \supseteq \ldots \tag{2.18}$$

Для любого n, $n \geqslant 1$, множество n-местных функций из $\mathrm{Pol}(R)$ конечно. Поэтому из соотношений (2.17) и (2.18) вытекает, что для любого n найдется такое i_n, что у множеств $\mathrm{Pol}(R)$ и $\mathrm{Pol}(\sigma_{i_n})$ совпадают множества n-местных функций. Следовательно, по доказанному предикат γ_n реализуется формулой, содержащей предикат σ_{i_n} и диагонали. Теорема доказана.

Пусть $\mathcal{M}$ обозначает частично упорядоченное по включению множество всех замкнутых классов булевых функций, содержащих все селекторные функции, $\mathcal{N}$ — частично упорядоченное по включению множество всех замкнутых классов булевых предикатов, содержащих все диагонали. Теоремы 2.1, 2.2 и соотношения (2.10) показывают, что отображения Pol и Inv устанавливают антиизоморфизм частично упорядоченных множеств $\mathcal{M}$ и $\mathcal{N}$. Это позволяет, например, для множества $\mathcal{N}$ строить диаграмму включений, аналогичную диаграмме Поста, если предварительно исключить из последней точки, соответствующие классам C_0, C_1, C (эти и только эти замкнутые классы не содержат селекторных функций). Многие утверждения, касающиеся замкнутых классов булевых функций, имеют свои очевидные аналоги для замкнутых классов булевых предикатов. В следующем параграфе мы рассмотрим лишь аналоги предполных классов и теоремы о полноте. Вместе с тем следует отметить, что некоторые факты из гл. I можно устанавливать принципиально иным образом: сначала на языке булевых предикатов доказать аналоги этих фактов, а затем перенести их на булевы функции, пользуясь антиизоморфизмом частично упорядоченных множеств $\mathcal{M}$ и $\mathcal{N}$.

§ 4. Минимальные классы и минимальные предикаты

В частично упорядоченном множестве $\mathcal{N}$ наименьшим элементом является класс $\mathrm{Inv}(P_2)$ всех диагоналей. Непосредственно следующими за ним будут пять замкнутых классов предикатов:

$$\mathrm{Inv}(T_0), \qquad \mathrm{Inv}(T_1), \qquad \mathrm{Inv}(S), \qquad \mathrm{Inv}(M), \qquad \mathrm{Inv}(L),$$

которые мы называем *минимальными классами*. Из определения следует, что всякий минимальный класс R порождается любым своим предикатом ρ, отличным от диагонали, и диагоналями, т. е.

$$R = [\{\rho\} \cup \mathrm{Inv}(P_2)]. \tag{2.19}$$

Последнее равенство показывает также, что если $R = \mathrm{Inv}(F)$, где F — предполный класс булевых функций, то $\mathrm{Pol}(\rho) = F$ и замыкание

Галуа предиката ρ совпадает с классом R:

$$\mathrm{Inv}(\mathrm{Pol}(\rho)) = R$$

(вопрос об определении предикатов ρ, порождающих минимальные классы, мы отложим до следующего параграфа).

Как видно, отличные от диагоналей предикаты из минимальных классов играют весьма важную роль. Мы называем такие предикаты *минимальными предикатами*. На основании равенства (2.19) можно дать другое определение минимального предиката. Именно, отличный от диагонали предикат ρ является минимальным, если для любого отличного от диагонали предиката σ, реализуемого формулой над множеством $\{\rho\} \cup \mathrm{Inv}(P_2)$, предикат ρ можно в свою очередь реализовать формулой над множеством $\{\sigma\} \cup \mathrm{Inv}(P_2)$.

Напомним, что непустой предикат ρ мы назвали *стандартным*, если его матрица X_ρ не содержит одинаковых строк. В дальнейшем среди отличных от диагоналей предикатов мы хотели бы иметь дело со стандартными предикатами, не содержащими фиктивных переменных. Как вытекает из свойства 7 из § 2, на множество $\mathrm{Pol}(\rho)$ не оказывает влияния введение или удаление фиктивных переменных в предикате ρ. Таким образом, если неполный предикат ρ имеет фиктивные переменные, то из него отождествлением переменных (или с помощью проектирования) можно получить такой предикат ρ', что $\mathrm{Pol}(\rho') = \mathrm{Pol}(\rho)$, и предикат ρ' не имеет фиктивных переменных. Мы хотим проделать подобную редукцию для предикатов, не являющихся стандартными. Пусть, например, в матрице X_ρ предиката $\rho(x_1, \ldots, x_k)$ совпадают i-я и j-я строки, $1 \leqslant i < j \leqslant k$. Полагая

$$\rho'(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k) \equiv \rho(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_k),$$

на основании свойства 5 из § 2 будем иметь $\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\rho')$. Вместе с тем предикат ρ можно получить из предиката ρ' с помощью конъюнкции с диагональю и отождествления переменных:

$$\rho(x_1, \ldots, x_k) \equiv \rho'(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k) \mathbin{\&} (x_i = x_j).$$

Поэтому на основании свойств 5 и 6 из § 2 получаем $\mathrm{Pol}(\rho') \subseteq \mathrm{Pol}(\rho)$. То есть $\mathrm{Pol}(\rho) = \mathrm{Pol}(\rho')$.

Подводя итог проведенным рассуждениям, можно утверждать, что для всякого отличного от диагонали предиката ρ отождествлением переменных (или с помощью проектирования) можно получить стандартный предикат ρ', который не содержит фиктивных переменных и для которого $\mathrm{Pol}(\rho') = \mathrm{Pol}(\rho)$.

Пусть непустой стандартный предикат σ, не имеющий фиктивных переменных, реализуется формулой над множеством $\{\rho\} \cup \cup \operatorname{Inv}(P_2)$. Покажем, что при этих условиях предикат σ можно реализовать формулой над множеством $\{\rho\}$, т. е. формулой, не содержащей диагонали. Для этого заметим, во-первых, что формула над $\{\rho\} \cup \cup \operatorname{Inv}(P_2)$, реализующая предикат σ, не может содержать пустого предиката, поскольку в этом случае пустым оказался бы и предикат σ. Конъюнкция диагоналей также является диагональю. Рассмотрим поэтому действие операции проектирования на конъюнкцию вида $\tau(x_1, \ldots, x_k) \mathbin{\&} D$, где D — непустая диагональ. Пусть проектирование проводится по переменной x_1. Если диагональ D не зависит существенно от переменной x_1, то согласно известным логическим правилам имеем

$$(\exists x_1)(\tau \mathbin{\&} D) \equiv (\exists x_1)\tau \mathbin{\&} D.$$

В противном случае пусть диагональ D имеет вид

$$D \equiv D_1 \mathbin{\&} (x_1 = x_{i_1} = \ldots = x_{i_m}),$$

где диагональ D_1 не зависит существенно от переменных $x_1, x_{i_1}, \ldots \ldots, x_{i_m}$; конъюнкции вида

$$(y_1 = z_1 = \ldots = z_p) \mathbin{\&} (y_1 = w_1 = \ldots = w_q),$$

входящие в диагональ D, мы заменяем на эквивалентные формулы

$$y_1 = z_1 = \ldots = z_p = w_1 = \ldots = w_q.$$

Тогда имеет место эквивалентность

$$(\exists x_1)(\tau(x_1, \ldots, x_k) \mathbin{\&} D) \equiv$$
$$\equiv \begin{cases} \tau(x_{i_1}, x_2, \ldots, x_k) \mathbin{\&} D_1 \mathbin{\&} (x_{i_1} = \ldots = x_{i_m}), & \text{если} \quad i_1 \neq 1, \\ (\exists x_1)\tau(x_1, x_2, \ldots, x_k) \mathbin{\&} D_1 & \text{в противном случае.} \end{cases}$$

Отсюда вытекает, что формулу над множеством $\{\rho\} \cup \operatorname{Inv}(P_2)$, реализующую предикат σ, можно привести к виду

$$\Psi \mathbin{\&} D, \tag{2.20}$$

где Ψ — формула над $\{\rho\}$, а D — диагональ. Поскольку предикат σ стандартен и не содержит фиктивных переменных, диагональ D обязана быть полным предикатом. В этом случае из формулы (2.20) ее можно исключить, не изменив реализуемого формулой (2.20) предиката. Получаем, что предикат σ реализуется формулой Ψ над множеством $\{\rho\}$.

Используя установленные выше редукции, дадим еще одно определение минимального класса.

Замкнутый класс предикатов R, содержащий все диагонали и отличный от класса $\mathrm{Inv}(P_2)$, является *минимальным*, если для любых двух стандартных предикатов ρ, σ, не имеющих фиктивных переменных, из того, что $\rho \in R$ и σ реализуется формулой над $\{\rho\}$, следует, что ρ может быть реализован формулой над $\{\sigma\}$.

Сформулируем на предикатном языке аналог теоремы о полноте из гл. I.

Теорема 2.3. *Пусть R — замкнутый класс предикатов, включающий все диагонали. И пусть в классе R целиком не содержится ни один из минимальных классов*

$$\mathrm{Inv}(T_0),\ \mathrm{Inv}(T_1),\ \mathrm{Inv}(S),\ \mathrm{Inv}(M),\ \mathrm{Inv}(L).$$

Тогда R совпадает с классом $\mathrm{Inv}(P_2)$ всех диагоналей.

Этому утверждению можно придать и несколько иную форму.

Теорема 2.4. *Пусть ρ — отличный от диагонали предикат. Тогда найдется такой минимальный предикат σ, который реализуется формулой над множеством $\{\rho\} \cup \mathrm{Inv}(P_2)$.*

Заметим, что на самом деле в теореме 2.4 предикат σ можно выбрать стандартным и не содержащим фиктивных переменных. Тогда, как мы установили, соответствующая формула, реализующая предикат ρ, не будет содержать диагоналей.

В заключение параграфа установим, например, минимальность предиката

$$\lambda(x_1, x_2, x_3, x_4) \equiv (x_1 + x_2 + x_3 + x_4 = 0)$$

(в следующем параграфе будет показано, что предикат λ определяет предполный класс L).

Легко видеть, что предикат λ стандартен и не содержит фиктивных переменных. Пусть ρ — отличный от диагонали стандартный предикат, который получается из предиката λ с помощью формулы Φ. Покажем, как в формуле Φ можно элиминировать квантор $\exists$.

Чтобы не рассматривать отдельно формулы вида

$$(\exists y)\Bigl(\mathop{\&}_{1 \leqslant i \leqslant m} \lambda(x_1^i, x_2^i, x_3^i, y)\Bigr),$$

перейдем сразу к формулам более общего вида

$$(\exists y)\Bigl(\mathop{\&}_{1 \leqslant i \leqslant m} (x_1^i + \ldots + x_{n_i}^i + y = 0)\Bigr). \tag{2.21}$$

Замечаем, что при $m = 1$ формула (2.21) определяет полный (тождественно истинный) предикат. Если же $m \geqslant 2$, то формулу (2.21) можно представить в следующем эквивалентном виде:

$$(\exists y)\left(\left(\mathop{\&}_{1\leqslant i<j\leqslant m}(x_1^i + \ldots + x_{n_i}^i + x_1^j + \ldots + x_{n_j}^j = 0)\right)\& \right.$$
$$\left. \&(x_1^1 + \ldots + x_{n_1}^1 + y = 0)\right). \quad (2.22)$$

Пользуясь известным правилом внесения квантора $\exists$ в конъюнкцию и полнотой предиката (2.21) при $m = 1$, получаем, что предикат (2.21) при $m \geqslant 2$ эквивалентен предикату

$$\mathop{\&}_{1\leqslant i<j\leqslant m}(x_1^i + \ldots + x_{n_i}^i + x_1^j + \ldots + x_{n_j}^j = 0). \quad (2.23)$$

Таким образом, формулу Φ можно считать бескванторной формулой, представляющей собой конъюнкцию предикатов вида

$$x_1 + \ldots + x_n = 0. \quad (2.24)$$

Поскольку в качестве исходного предиката в формуле Φ фигурирует предикат $x_1 + x_2 + x_3 + x_4 = 0$, то в силу тождества $x + x = 0$ и в силу формулы (2.23) в предикатах (2.24), составляющих формулу Φ, число n должно быть четным. Кроме того, должно выполняться неравенство $n \geqslant 4$, поскольку предикат $x_1 + x_2 = 0$ эквивалентен предикату $x_1 = x_2$, а формула, конъюнктивно содержащая диагональ $x_1 = x_2$, не может определять стандартный предикат.

Предположим, далее, что формула Φ состоит из одного сомножителя (2.24), т. е.

$$\rho(x_1, \ldots, x_n) \equiv (x_1 + \ldots + x_n = 0).$$

При $n = 4$ мы имеем $\rho \equiv \lambda$, а при $n > 4$ —

$$\lambda(x_1, x_2, x_3, x_4) \equiv \rho(x_1, x_2, x_3, x_4, \ldots, x_4)$$

(напомним, что n четно).

Пусть формула Φ состоит из нескольких сомножителей, однако переменные одного из них не входят в другие сомножители. Иными словами, пусть

$$\rho \equiv (x_1 + \ldots + x_n = 0)\ \&\ \sigma(y_1, \ldots, y_k),$$

где

$$\{x_1, \ldots, x_n\} \cap \{y_1, \ldots, y_k\} = \varnothing.$$

Предикат σ не может быть тождественно ложным, иначе тождественно ложным был бы и предикат ρ. Следовательно,

$$(\exists y_1) \ldots (\exists y_k) \sigma(y_1, \ldots, y_k)$$

— полный предикат. Откуда

$$(\exists y_1) \ldots (\exists y_k)\rho \equiv (\exists y_1) \ldots (\exists y_k)((x_1 + \ldots + x_n = 0) \mathbin{\&} \sigma(y_1, \ldots, y_k)) \equiv$$
$$\equiv (x_1 + \ldots + x_n = 0) \mathbin{\&} (\exists y_1) \ldots (\exists y_k)\sigma(y_1, \ldots, y_k) \equiv (x_1 + \ldots + x_n = 0),$$

и мы приходим к рассмотренному выше случаю.

Предположим теперь, что формула Φ содержит подформулу вида

$$\mathop{\&}_{1 \leqslant i \leqslant m} (x_1^i + \ldots + x_{n_i}^i + y = 0), \tag{2.25}$$

где $m \geqslant 2$ и n_i — нечетные числа, отличные от 1. Будем считать, что в формуле (2.25) собраны все сомножители формулы Φ, содержащие переменную y. Конъюнкцию всех остальных сомножителей формулы Φ обозначим через ρ_1. Тогда

$$\rho \equiv \left(\mathop{\&}_{1 \leqslant i \leqslant m} (x_1^i + \ldots + x_{n_i}^i + y = 0) \right) \mathbin{\&} \rho_1 \equiv$$
$$\equiv \left(\mathop{\&}_{1 \leqslant i < j \leqslant m} (x_1^i + \ldots + x_{n_i}^i + x_1^j + \ldots + x_{n_j}^j = 0) \right) \mathbin{\&}$$
$$\mathbin{\&} (x_1^1 + \ldots + x_{n_1}^1 + y = 0) \mathbin{\&} \rho_1. \tag{2.26}$$

Поскольку предикат ρ стандартен, стандартным будет и предикат

$$\left(\mathop{\&}_{1 \leqslant i < j \leqslant m} (x_1^i + \ldots + x_{n_i}^i + x_1^j + \ldots + x_{n_j}^j = 0) \right) \mathbin{\&} \rho_1,$$

который обозначим через ρ_2. Можно также предполагать, что предикат ρ_2 отличен от диагонали, поскольку в противном случае формула Φ либо вырождается в один сомножитель $x_1^1 + \ldots + x_{n_1}^1 + y = 0$, либо реализует предикат, отличный от стандартного. Из (2.26) легко получаем, что $(\exists y)\rho \equiv \rho_2$. Таким образом, мы приходим к отличному от диагонали стандартному предикату ρ_2, который по сравнению с предикатом ρ содержит по крайней мере на одну переменную меньше. Продолжая этот процесс, в конце концов получим предикат λ.

§ 5. Замкнутые классы, определяемые конечным числом предикатов

Согласно результатам § 3, всякий замкнутый класс булевых функций, содержащий все селекторные функции, определяется подходящим, вообще говоря, бесконечным множеством булевых предикатов. Оказывается, что «почти все» замкнутые классы булевых функций можно задать конечным множеством предикатов, т. е. представить в виде $\mathrm{Pol}(R)$, где множество R состоит из конечного числа предикатов. Ниже, в теореме 2.5, полностью охарактеризованы замкнутые классы, обладающие этим свойством. Поскольку в соответствии со свойством 6 из § 2 при определении замкнутого класса булевых функций конечное множество предикатов можно заменить одним предикатом, в доказательстве теоремы 2.5 рассматриваются лишь одноэлементные множества предикатов.

Теорема 2.5. *Для того чтобы замкнутый класс R булевых функций, отличный от P_2, определялся конечным множеством предикатов, необходимо и достаточно, чтобы выполнялись следующие условия: R содержит все селекторные функции и существует конечная последовательность $R_1, \ldots, R_s$ замкнутых классов такая, что класс R строго содержится в каждом из классов $R_1, \ldots, R_s$ и всякий замкнутый класс, строго содержащий R, включает хотя бы один из классов $R_1, \ldots, R_s$.*

Доказательство. Необходимость. Пусть замкнутый класс R определяется предикатом $\rho(x_1, \ldots, x_k)$, т. е. $R = \mathrm{Pol}(\rho)$. Согласно свойству 1 из § 2, класс R содержит все селекторные функции. Предполагая, что $R \neq P_2$, возьмем произвольный замкнутый класс R' такой, что $R \subset R'$ (включение строгое). Тогда в классе R' найдется функция $f(y_1, \ldots, y_n)$, которая не сохраняет предикат ρ. Это значит, что можно выбрать такие n наборов

$$(a_{11}, \ldots, a_{k1}), \ldots, (a_{1n}, \ldots, a_{kn}), \tag{2.27}$$

удовлетворяющие предикату ρ, что набор

$$(f(a_{11}, \ldots, a_{1n}), \ldots, f(a_{k1}, \ldots, a_{kn})) \tag{2.28}$$

не удовлетворяет предикату ρ.

Пусть предикат ρ имеет ширину m. Если $n > m$, то среди наборов (2.27) имеются одинаковые. Отождествляя в функции f соответствующие переменные, получим функцию f' из класса R', зависящую не более чем от m переменных, которая тоже не сохраняет предикат ρ (мы получим тот же самый набор (2.28), если из каждой группы одинаковых столбцов матрицы

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}$$

оставим один и применим к полученной матрице функцию f').

Таким образом, всякий замкнутый класс, строго содержащий класс R, включает функцию, не принадлежащую классу R и зависящую не более чем от m переменных. Если $f_1, \dots, f_s$ — все такие функции, то любой замкнутый класс, содержащий класс R и отличный от него, содержит хотя бы один из замкнутых классов

$$[R \cup \{f_1\}], \dots, [R \cup \{f_s\}].$$

Достаточность. Пусть замкнутый класс R отличен от P_2, содержит все селекторные функции, а замкнутые классы $R_1, \dots, R_s$ выбраны в соответствии с условиями теоремы. Выберем число m так, чтобы множество $R^{(m)}$ всех m-местных функций из R отличалось от любого из множеств $R_1^{(m)}, \dots, R_s^{(m)}$. Докажем, что $R = \mathrm{Pol}(\gamma_m)$, где γ_m — m-график множества R. В самом деле, очевидно, что все функции из R сохраняют предикат γ_m, и потому $R \subseteq \mathrm{Pol}(\gamma_m)$. С другой стороны, если замкнутый класс $\mathrm{Pol}(\gamma_m)$ отличен от R, то он целиком включает некоторый класс R_i и, следовательно, по выбору числа m содержит некоторую функцию $f(y_1, \dots, y_m)$, не входящую в множество $R^{(m)}$. Однако функция f не может сохранять предикат γ_m, поскольку в $R^{(m)}$ содержатся селекторные функции $e_1^m, \dots, e_m^m$ и

$$f(e_1^m(y_1, \dots, y_m), \dots, e_m^m(y_1, \dots, y_m)) = f(y_1, \dots, y_m).$$

Таким образом, класс $\mathrm{Pol}(\gamma_m)$ не может отличаться от класса R, и теорема доказана.

Следствие 2.1. *Любой замкнутый класс булевых функций, отличный от классов*

$$O^\infty,\ O_0^\infty,\ MO^\infty,\ MO_0^\infty,\ I^\infty,\ I_1^\infty,\ MI^\infty,\ MI_1^\infty,\ C,\ C_0,\ C_1, \quad (2.29)$$

определяется конечным числом предикатов. Никакой из классов (2.29) *нельзя определить конечным числом предикатов.*

Доказательство. Как отмечалось выше, класс P_2 определяется любой диагональю. Классы C, C_0, C_1 не содержат селекторных функций и потому вообще не могут определяться никаким множеством булевых предикатов. Для всех остальных замкнутых классов из списка (2.29) вопрос о задании их с помощью конечного числа предикатов решается на основе теоремы 2.5 и анализа диаграммы включений замкнутых классов.

Доказательство теоремы 2.5 указывает на некоторый предикат, определяющий заданный замкнутый класс R. Именно, этим предикатом является m-график γ_m класса R, где число m выбрано так, что множество $R^{(m)}$ отличается от множеств $Q^{(m)}$ для любых классов Q, непосредственно содержащих класс R. Однако, как правило, такой предикат γ_m является избыточным. Более простые предикаты, задающие класс R, можно получить из предиката γ_m с помощью проектирования. Отметим, что все такие предикаты принадлежат классу $\mathrm{Inv}(R)$, поскольку $R = \mathrm{Pol}(\gamma_m)$.

В качестве примера рассмотрим предикатное задание предполных классов T_0, T_1, S, M, L. Легко видеть, что каждое из множеств $T_0^{(1)}, T_1^{(1)}, S^{(1)}, M^{(1)}$ отлично от множества $P_2^{(1)}$. Поэтому каждый из классов T_0, T_1, S, M можно задать одним двуместным предикатом — 1-графиком соответствующего класса. Для классов S и M матрицы 1-графиков имеют вид

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

а для классов T_0 и T_1 — вид

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Нетрудно видеть, что 1-график класса S эквивалентен предикату $x_1 \neq x_2$, а 1-график класса M — предикату $x_1 \leqslant x_2$. Замечаем, далее, что 1-график класса T_0 получается из предиката $x = 0$ добавлением фиктивной переменной. Поэтому согласно свойству 7 из § 2 имеем

$$T_0 = \mathrm{Pol}\{x = 0\}.$$

Аналогичным образом показываем, что класс T_1 определяется предикатом $x = 1$. К такому же выводу мы придем, если воспользуемся равенствами

$$T_0 = \mathrm{Pol}\{x = 0\}, \qquad T_1 = T_0^*$$

и свойством 9 из § 2.

Для класса L множество $L^{(1)}$ совпадает со множеством $P_2^{(1)}$ (1-график класса L является полным предикатом), однако множества $L^{(2)}$ и $P_2^{(2)}$ уже различны. Матрица 2-графика класса L имеет вид

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

а сам 2-график эквивалентен предикату $x_1+x_2+x_3+x_4=0$. Нетрудно проверить, что отождествлением переменных и проектированием из 2-графика класса L можно получить лишь диагонали.

Покажем, что предикаты, определяющие предполные классы T_0, T_1, S, M, L, имеют наименьшее возможное число переменных. Это очевидно для предикатов $x=0$ и $x=1$, задающих классы T_0 и T_1, и почти очевидно для двуместных предикатов, определяющих классы S и M, поскольку всякий непустой и неполный одноместный предикат совпадает с одним из предикатов $x=0$ или $x=1$. Таким образом, остается исследовать на минимальность числа переменных предикат x_1+x_2+ $+x_3+x_4=0$, который задает класс L.

Пусть в класс $\mathrm{Inv}(L)$ входит двуместный или трехместный предикат λ. Поскольку функции $0, 1, \bar{x}$ принадлежат классу L, матрица X_λ предиката λ содержит нулевой и единичный столбцы, и вместе с любым столбцом матрице X_λ принадлежит столбец из противоположных значений (противоположный столбец). Если предикат λ зависит от двух переменных, то мы имеем две возможные матрицы X_λ:

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Первая матрица определяет диагональ $x_1=x_2$, вторая — полный предикат.

Пусть предикат λ зависит от трех переменных. Матрица X_λ не может состоять только из нулевого и единичного столбцов — иначе предикат λ был бы диагональю. Значит, X_λ содержит по крайней мере две пары противоположных столбцов. Если ширина предиката λ равна четырем, то матрица X_λ содержит две одинаковые строки. Как показано в § 4, в этом случае класс $\mathrm{Pol}(\lambda)$ можно определить двуместным предикатом, что, как мы убедились, неверно. Следовательно, ширина предиката λ не меньше шести. Используя теперь включение $x+y \in \mathrm{Pol}(\lambda)$, легко убеждаемся в том, что матрица X_λ наряду с тремя парами противоположных столбцов обязательно содержит и четвертую пару противоположных столбцов. Таким образом, предикат λ оказывается полным.

§ 6. Предикатное задание замкнутых классов

В предыдущем параграфе мы нашли предикаты, которые задают предполные классы T_0, T_1, S, M, L. Здесь мы рассмотрим все остальные замкнутые классы.

Класс U определяется предикатом $x_1 = x_2 \vee x_1 = x_3$. В самом деле, выписав матрицу

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{2.30}$$

предиката $x_1 = x_2 \vee x_1 = x_3$, легко убедиться в том, что функции класса U сохраняют данный предикат. Вместе с тем класс U непосредственно содержится только в классе L, а линейная функция $x_1 + x_2$ не сохраняет предикат $x_1 = x_2 \vee x_1 = x_3$ (достаточно рассмотреть второй и третий столбцы матрицы (2.30)).

Предикат $x_1 = x_2 x_3$ имеет матрицу

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \tag{2.31}$$

Убеждаемся, что функции $0, 1, xy$, образующие базис класса K, сохраняют предикат $x_1 = x_2 x_3$. Значит,

$$K \subseteq \mathrm{Pol}\{x_1 = x_2 x_3\}.$$

Класс K непосредственно содержится только в классе M, а монотонная функция $x \vee y$ не сохраняет предикат $x_1 = x_2 x_3$ (следует рассмотреть второй и третий столбцы матрицы (2.31)). Следовательно, класс K можно задать предикатом $x_1 = x_2 x_3$.

Покажем, что при любом $m, m \geqslant 2$, класс I^m определяется предикатом $x_1 \cdot \ldots \cdot x_m = 0$. Заметим, что матрица предиката $x_1 \cdot \ldots \cdot x_m = 0$ состоит из всех столбцов высоты m, отличных от единичного столбца. Функции $x\bar{y}$ и

$$d^*_{m+1}(x_1, \ldots, x_{m+1}) = \mathop{\&}_{1 \leqslant i < j \leqslant m+1} (x_i \vee x_j),$$

образующие базис класса I^m, сохраняют предикат $x_1 \cdot \ldots \cdot x_m = 0$. Значит,

$$I^m \subseteq \mathrm{Pol}\{x_1 \cdot \ldots \cdot x_m = 0\}.$$

С другой стороны, класс I^2 непосредственно содержится только в классе T_0, а класс I^m при $m \geqslant 3$ — только в классе I^{m-1}. Для доказательства равенства

$$I^m = \mathrm{Pol}\{x_1 \cdot \ldots \cdot x_m = 0\}$$

остается теперь проверить, что функция $x \vee y$ из класса T_0 не сохраняет предикат $x_1 \cdot x_2 = 0$ (достаточно рассмотреть противоположные столбцы в матрице предиката $x_1 \cdot x_2 = 0$), а при $m \geqslant 3$ функция $d_m^*(x_1, \ldots, x_m)$ из класса I^{m-1} не сохраняет предикат $x_1 \cdot \ldots \cdot x_m = 0$:

$$d_m^* \begin{pmatrix} 0 & 1 & \ldots & 1 & 1 \\ 1 & 0 & \ldots & 1 & 1 \\ \multicolumn{5}{c}{\ldots\ldots\ldots\ldots\ldots} \\ 1 & 1 & \ldots & 0 & 1 \\ 1 & 1 & \ldots & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \ldots \\ 1 \\ 1 \end{pmatrix}.$$

Согласно свойству 9 из § 2 класс D, двойственный классу K, определяется предикатом $x_1 = x_2 \vee x_3$, а класс O^m, двойственный классу I^m, — предикатом $x_1 \vee \ldots \vee x_m = 1$.

Все остальные замкнутые классы булевых функций, отличные от классов C, C_0, C_1, можно представить в виде пересечения подходящих классов из числа

$$T_0,\ T_1,\ S,\ M,\ L,\ U,\ K,\ D,\ I^m,\ O^m, \qquad m = 2, 3, \ldots$$

Поэтому согласно свойству 6 из § 2 будут иметь место следующие утверждения:

класс T_{01} как пересечение классов T_0 и T_1 определяется предикатами $x = 0$, $x = 1$;

класс M_0 как пересечение классов T_0 и M определяется предикатами $x = 0$, $x_1 \leqslant x_2$;

класс M_{01} как пересечение классов T_0, T_1 и M определяется предикатами $x = 0$, $x = 1$, $x_1 \leqslant x_2$;

класс S_{01} как пересечение классов T_0 и S определяется предикатами $x = 0$, $x_1 \neq x_2$;

класс SM как пересечение классов S и M определяется предикатами $x_1 \neq x_2$, $x_1 \leqslant x_2$;

классы K_0, K_1 и K_{01} как пересечения класса K соответственно с классами T_0, T_1 и T_{01} определяются предикатами

$$\{x = 0,\ x_1 = x_2x_3\},\ \{x = 1,\ x_1 = x_2x_3\},\ \{x = 0,\ x = 1,\ x_1 = x_2x_3\};$$

класс MU как пересечение классов M и U определяется предикатами $x_1 \leqslant x_2$, $x_1 = x_2 \vee x_1 = x_3$;

класс U_0 как пересечение классов T_0 и U определяется предикатами $x = 0$, $x_1 = x_2 \vee x_1 = x_3$;

класс U_{01} как пересечение классов T_{01} и U определяется предикатами $x = 0$, $x = 1$, $x_1 = x_2 \vee x_1 = x_3$.

Из $L_0 = T_0 \cap L$ следует, что

$$L_0 = \mathrm{Pol}\,\{x = 0,\ x_1 + x_2 + x_3 + x_4 = 0\}.$$

Однако

$$(x_1 + x_2 + x_3 = 0) \equiv (\exists y)((y = 0)\ \&\ (x_1 + x_2 + x_3 + y = 0)),$$

$$(x = 0) \equiv (x + x + x = 0),$$

$$(x_1 + x_2 + x_3 + x_4 = 0) \equiv (\exists y)((x_1 + x_2 + y = 0)\ \&\ (x_3 + x_4 + y = 0)).$$

Поэтому

$$L_0 = \mathrm{Pol}\,\{x_1 + x_2 + x_3 = 0\}.$$

Поскольку $L_{01} = T_1 \cap L_0$, имеем

$$L_{01} = \mathrm{Pol}\,\{x = 1,\ x_1 + x_2 + x_3 = 0\}.$$

Из соотношений $SL = S \cap L$ и

$$(x_1 \neq x_2) \equiv (x_1 + x_2 = 1)$$

выводим, что

$$SL = \mathrm{Pol}\,\{x_1 + x_2 = 1,\ x_1 + x_2 + x_3 + x_4 = 0\}.$$

Имеем, далее,

$$(x_1 + x_2 + x_3 + x_4 = 1) \equiv (\exists y)((x_4 + y = 1)\ \&\ (x_1 + x_2 + x_3 + y = 0)),$$

$$(x_1 + x_2 = 1) \equiv (\exists x_3)(x_1 + x_2 + x_3 + x_3 = 1),$$

$$(x_1 + x_2 + x_3 + x_4 = 0) \equiv (\exists y)((x_1 + x_2 + x_3 + y = 1)\ \&\ (x_4 + y = 1)).$$

Значит, класс SL можно задать предикатом $x_1 + x_2 + x_3 + x_4 = 1$.

Из равенства $SU = S \cap U$ вытекает, что

$$SU = \mathrm{Pol}\,\{x_1 \neq x_2,\ x_1 = x_2 \vee x_1 = x_3\}.$$

Эквивалентности

$$(x_1 \neq x_2 \vee x_1 \neq x_3) \equiv (\exists y)((x_1 \neq y)\ \&\ (y = x_2 \vee y = x_3)),$$

$$(x_1 \neq x_2) \equiv (x_1 \neq x_2 \vee x_1 \neq x_2),$$

$$(x_1 = x_2 \vee x_1 = x_3) \equiv (\exists y)((x_1 \neq y) \,\&\, (y \neq x_2 \vee y \neq x_3))$$

показывают, что класс SU можно определить предикатом

$$x_1 \neq x_2 \vee x_1 \neq x_3.$$

Для любого m, $m \geqslant 2$, имеем

$$MI^m = M \cap I^m.$$

Поэтому

$$MI^m = \mathrm{Pol}\{x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0\}.$$

Аналогичным образом,

$$I_1^m = T_1 \cap I^m, \qquad MI_1^m = M \cap I_1^m.$$

Следовательно,

$$I_1^m = \mathrm{Pol}\,\{x = 1,\ x_1 \cdot \ldots \cdot x_m = 0\},$$

$$MI_1^m = \mathrm{Pol}\,\{x = 1,\ x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0\}.$$

Наконец, поскольку

$$I^\infty = \bigcap_{m=2}^{\infty} I^m, \qquad MI^\infty = \bigcap_{m=2}^{\infty} MI^m,$$

$$I_1^\infty = \bigcap_{m=2}^{\infty} I_1^m, \qquad MI_1^\infty = \bigcap_{m=2}^{\infty} MI_1^m,$$

имеем

$$I^\infty = \mathrm{Pol}\,\{x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\},$$

$$MI^\infty = \mathrm{Pol}\,\{x_1 \leqslant x_2,\ x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\},$$

$$I_1^\infty = \mathrm{Pol}\,\{x = 1,\ x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\},$$

$$MI_1^\infty = \mathrm{Pol}\,\{x = 1,\ x_1 \leqslant x_2,\ x_1x_2 = 0,\ x_1x_2x_3 = 0, \ldots\}.$$

Двойственным образом рассматриваются оставшиеся замкнутые классы

$$MO^m, O_0^m, MO_0^m, O^\infty, MO^\infty, O_0^\infty, MO_0^\infty,$$

отличные от классов C, C_0, C_1.

Основные результаты, полученные в этом параграфе, сведены в табл. 2.1.

Таблица 2.1

Класс	Предикаты, задающие класс
P_2	$x = x$
T_0	$x = 0$
T_1	$x = 1$
T_{01}	$x = 0,\ x = 1$
S	$x_1 \neq x_2$
M	$x_1 \leqslant x_2$
M_0	$x = 0,\ x_1 \leqslant x_2$
M_1	$x = 1,\ x_1 \leqslant x_2$
M_{01}	$x = 0,\ x = 1,\ x_1 \leqslant x_2$
S_{01}	$x = 0,\ x_1 \neq x_2$
SM	$x_1 \neq x_2,\ x_1 \leqslant x_2$
L_0	$x_1 + x_2 + x_3 = 0$
L_1	$x_1 + x_2 + x_3 = 1$
L_{01}	$x = 1,\ x_1 + x_2 + x_3 = 0$
U	$x_1 = x_2 \vee x_1 = x_3$
SU	$x_1 \neq x_2 \vee x_1 \neq x_3$
MU	$x_1 \leqslant x_2,\ x_1 = x_2 \vee x_1 = x_3$
U_0	$x = 0,\ x_1 = x_2 \vee x_1 = x_3$
U_1	$x = 1,\ x_1 = x_2 \vee x_1 = x_3$
U_{01}	$x = 0,\ x = 1,\ x_1 = x_2 \vee x_1 = x_3$
K	$x_1 = x_2 \cdot x_3$
K_0	$x = 0,\ x_1 = x_2 \cdot x_3$
K_1	$x = 1,\ x_1 = x_2 \cdot x_3$
K_{01}	$x = 0,\ x = 1,\ x_1 = x_2 \cdot x_3$
D	$x_1 = x_2 \vee x_3$
D_0	$x = 0,\ x_1 = x_2 \vee x_3$
D_1	$x = 1,\ x_1 = x_2 \vee x_3$
D_{01}	$x = 0,\ x = 1,\ x_1 = x_2 \vee x_3$
L	$x_1 + x_2 + x_3 + x_4 = 0$
SL	$x_1 + x_2 + x_3 + x_4 = 1$
I^m	$x_1 \cdot \ldots \cdot x_m = 0$
MI^m	$x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0$
I_1^m	$x = 1,\ x_1 \cdot \ldots \cdot x_m = 0$
MI_1^m	$x = 1,\ x_1 \leqslant x_2,\ x_1 \cdot \ldots \cdot x_m = 0$
O^m	$x_1 \vee \ldots \vee x_m = 1$
MO^m	$x_1 \leqslant x_2,\ x_1 \vee \ldots \vee x_m = 1$
O_0^m	$x = 0,\ x_1 \vee \ldots \vee x_m = 1$
MO_0^m	$x = 0,\ x_1 \leqslant x_2,\ x_1 \vee \ldots \vee x_m = 1$

Комментарии. Отношение сохранения предиката функций введено А. В. Кузнецовым [7]. Это отношение можно определить также чисто алгебраическим путем, рассматривая подалгебры декартовой степени алгебры с единственной операцией. Соответствия Галуа между произвольными частично упорядоченными множествами и замыкания Галуа введены О. Оре [39, 22] (см. также [43, 23]). На возможность построения теории Галуа для алгебр Поста указывал А. В. Кузнецов [8]. Само построение выполнено независимо В. Г. Боднарчуком, Л. А. Калужниным, В. Н. Котовым, Б. А. Ромовым [2] и Д. Гейгером [37]. Минимальность предикатов, определяющих предполные классы в P_k, $k \geqslant 2$, доказана в [15]. Все замкнутые классы булевых предикатов внешним образом охарактеризованы в [17]. Теорема 2.5 представляет собой булевский вариант более общего утверждения, доказанного С. В. Яблонским [31]. Предикатное описание замкнутых классов булевых функций было известно А. В. Кузнецову (результат не опубликован). Первой публикацией на эту тему явилась статья Г. Н. Блохиной [1]. Дальнейшие упрощения приведены в [19].

Глава III

ЗАМКНУТЫЕ КЛАССЫ БУЛЕВЫХ ВЕКТОР-ФУНКЦИЙ

Пусть k — натуральное число, $k \geqslant 2$. Через P_2^k обозначим множество всех наборов вида

$$(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)), \tag{3.1}$$

где $f_1, \ldots, f_k$ — булевы функции, $n = 1, 2, \ldots$ Если k фиксировано, то набор (1) будем обозначать через $\bar{f}(x_1, \ldots, x_n)$ и называть *булевой вектор-функцией* (размерности k). На булевы вектор-функции можно распространить те определения, которые были введены в гл. I для булевых функций. Так, селекторной функции $e_i^n(x_1, \ldots, x_n)$ из P_2 соответствует селекторная вектор-функция

$$\bar{e}_i^n(x_1, \ldots, x_n) = (e_i^n(x_1, \ldots, x_n), \ldots, e_i^n(x_1, \ldots, x_n)). \tag{3.2}$$

Если

$$\bar{f}(x_1, \ldots, x_n), \qquad \bar{g}_1(y_1, \ldots, y_m), \qquad \ldots, \qquad \bar{g}_n(y_1, \ldots, y_m)$$

— вектор-функции из P_2^k, функция $\bar{f}$ задается вектором (3.1) и

$$\bar{g}_1(y_1, \ldots, y_m) = (g_{11}(y_1, \ldots, y_m), \ldots, g_{1k}(y_1, \ldots, y_m)),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\bar{g}_n(y_1, \ldots, y_m) = (g_{n1}(y_1, \ldots, y_m), \ldots, g_{nk}(y_1, \ldots, y_m)),$$

то i-й компонентой, $1 \leqslant i \leqslant k$, вектор-функции

$$\bar{f}(\bar{g}_1(y_1, \ldots, y_m), \ldots, \bar{g}_n(y_1, \ldots, y_m))$$

по определению считаем функцию

$$f_i(g_{1i}(y_1, \ldots, y_m), \ldots, g_{ni}(y_1, \ldots, y_m)).$$

Таким образом, на множестве P_2^k задана операция суперпозиции. Так же, как и в случае множества P_2, на множестве P_2^k можно определить алгебраические операции $\zeta, \tau, \Delta, \nabla, *$, что позволяет рассматривать вместо замкнутых классов булевых вектор-функций подалгебры итеративной алгебры $\langle P_2^k;\ \zeta, \tau, \Delta, \nabla, * \rangle$.

В этой главе мы для любого k, $k \geqslant 2$, докажем конечную порождаемость множества P_2^k и найдем все предполные в P_2^k классы. Число их при фиксированном k конечно, но экспоненциально возрастает с ростом k. Для описания предполных классов в P_2^k удобно применять технику многоосновных отношений. Доказательство предполноты замкнутых классов, определяемых многоосновными отношениями, опирается на соответствие Галуа. Элементы теории Галуа для системы P_2^k излагаются в § 4.

В дальнейшем для множества P_2^k мы используем без дополнительных определений понятия замыкания, замкнутого класса, предполного класса и т. п. Определения даются лишь в тех случаях, когда соответствующий аналог в P_2 в достаточной степени отличается от определяемого объекта в P_2^k. Например, переменная x_i называется *существенной* для вектор-функции $\bar{f}(x_1, \ldots, x_i, \ldots, x_n)$, если она является существенной хотя бы для одной из функций

$$f_1(x_1, \ldots, x_i, \ldots, x_n), \qquad \ldots, \qquad f_k(x_1, \ldots, x_i, \ldots, x_n).$$

На протяжении всей главы k — фиксированное натуральное число, $k \geqslant 2$.

§ 1. Конечные порождающие системы

Пусть $\bar{f}(x_1, \ldots, x_n)$ — вектор-функция (1). Для любого i, $1 \leqslant i \leqslant k$, через $\mathrm{pr}_i \bar{f}(x_1, \ldots, x_n)$ обозначим булеву функцию $f_i(x_1, \ldots, x_n)$.

Лемма 3.1. *Пусть $\bar{f}_1, \ldots, \bar{f}_m, \bar{e}$ — такие вектор-функции из P_2^k, что каждая из систем булевых функций*

$$\{\mathrm{pr}_1 \bar{f}_1, \ldots, \mathrm{pr}_1 \bar{f}_m\}, \qquad \ldots, \qquad \{\mathrm{pr}_k \bar{f}_1, \ldots, \mathrm{pr}_k \bar{f}_m\}$$

полна в P_2 и

$$\bar{e}(x_1, \ldots, x_k) = (e_1^k(x_1, \ldots, x_k), \ldots, e_k^k(x_1, \ldots, x_k)).$$

Тогда система функций $\{\bar{f}_1, \ldots, \bar{f}_m, \bar{e}\}$ полна в P_2^k.

Доказательство. Рассмотрим произвольную вектор-функцию $\bar{f}(x_1, \ldots, x_n)$ из P_2^k. Зафиксируем i, $1 \leqslant i \leqslant k$. Пользуясь тем, что система булевых функций $\{\mathrm{pr}_i \bar{f}_1, \ldots, \mathrm{pr}_i \bar{f}_m\}$ полна в P_2, суперпозициями функций системы $\{\bar{f}_1, \ldots, \bar{f}_m\}$ образуем такую вектор-функцию $\bar{g}_i(x_1, \ldots, x_n)$, что

$$\mathrm{pr}_i \bar{g}_i(x_1, \ldots, x_n) = \mathrm{pr}_i \bar{f}(x_1, \ldots, x_n).$$

Нетрудно видеть, что

$$\bar{f}(x_1, \ldots, x_n) = \bar{e}(\bar{g}_1(x_1, \ldots, x_n), \ldots, \bar{g}_k(x_1, \ldots, x_n)).$$

Лемма доказана.

Лемма 3.2. *Пусть вектор-функции* $\bar{f}_1, \ldots, \bar{f}_m$ *такие же, как и в лемме* 3.1, *а вектор-функции* $\bar{e}_i(x_1, x_2)$, $1 \leqslant i \leqslant k$, *удовлетворяют условиям*

$$\mathrm{pr}_i\, \bar{e}_i = e_1^2(x_1, x_2), \qquad \mathrm{pr}_j\, \bar{e}_i = e_2^2(x_1, x_2) \quad \text{для} \quad j \neq i.$$

Тогда система вектор-функций $\{\bar{f}_1, \ldots, \bar{f}_m, \bar{e}_1, \ldots, \bar{e}_k\}$ *полна в* P_2^k.

Доказательство. В силу леммы 3.1 достаточно из функций системы $\{\bar{f}_1, \ldots, \bar{f}_m, \bar{e}_1, \ldots, \bar{e}_k\}$ получить вектор-функцию $\bar{e}$. Положим

$$\bar{g}_1(x_1, \ldots, x_k) = \bar{e}_1(x_1, \bar{e}_1(x_k, \bar{e}_1(x_{k-1}, \ldots, \bar{e}_1(x_3, x_2) \ldots))).$$

Легко видеть, что

$$\mathrm{pr}_1\, \bar{g}_1(x_1, \ldots, x_k) = e_1^k(x_1, \ldots, x_k),$$

$$\mathrm{pr}_2\, \bar{g}_1(x_1, \ldots, x_k) = e_2^k(x_1, \ldots, x_k).$$

Пусть для данного s, $2 \leqslant s < k$, суперпозициями функций из $\{\bar{e}_1, \ldots, \bar{e}_k\}$ уже определена такая вектор-функция $\bar{g}_{s-1}(x_1, \ldots, x_k)$, что

$$\mathrm{pr}_1\, \bar{g}_{s-1}(x_1, \ldots, x_k) = e_1^k(x_1, \ldots, x_k), \quad \ldots$$

$$\ldots, \quad \mathrm{pr}_s\, \bar{g}_{s-1}(x_1, \ldots, x_k) = e_s^k(x_1, \ldots, x_k).$$

Полагая

$$\bar{g}_s(x_1, \ldots, x_k) = \bar{e}_{s+1}(x_{s+1}, \bar{g}_{s-1}(x_1, \ldots, x_k)),$$

будем иметь для любого i, $1 \leqslant i \leqslant s+1$,

$$\mathrm{pr}_i\, \bar{g}_s(x_1, \ldots, x_k) = e_i^k(x_1, \ldots, x_k).$$

Следовательно,

$$\bar{e}(x_1, \ldots, x_k) = \bar{g}_{k-1}(x_1, \ldots, x_k),$$

и лемма доказана.

Теорема 3.1. *Класс* P_2^k *является конечно порожденным. Порядок класса* P_2^k *равен двум.*

Доказательство. В лемме 3.2 положим $m = 1$ и

$$\bar{f}_1(x_1, x_2) = (\bar{x}_1 \vee \bar{x}_2, \ldots, \bar{x}_1 \vee \bar{x}_2).$$

Таким образом, класс P_2^k порождается системой из $k+1$ вектор-функций от двух переменных. Очевидно, что класс P_2^k нельзя породить вектор-функциями, зависящими лишь от одной переменной.

Из конечной порождаемости класса P_2^k вытекают важные следствия.

Теорема 3.2. *Всякий замкнутый класс вектор-функций из P_2^k, отличный от P_2^k, содержится в некотором предполном в P_2^k классе. Число предполных в P_2^k классов конечно.*

Доказательство. Пусть F — произвольный замкнутый класс вектор-функций из P_2^k, отличный от класса P_2^k. Обозначим через F' множество, полученное из F добавлением всех селекторных вектор-функций из P_2^k. Нетрудно видеть, что F' — также замкнутый класс, отличный от P_2^k. Пусть $(F')_{x_1x_2}$ обозначает множество всех вектор-функций из F', зависящих от переменных x_1, x_2. Поскольку $F' \neq P_2^k$ и порядок класса P_2^k равен двум, имеем $(F')_{x_1x_2} \neq$ $\neq (P_2^k)_{x_1x_2}$. Очевидно, что число множеств вида $(F')_{x_1x_2}$ конечно. Обозначим через $P(F')$ множество всех вектор-функций из P_2^k, которые сохраняют множество $(F')_{x_1x_2}$. Иными словами, пусть $P(F')$ состоит из всех вектор-функций $\bar{f}(y_1, \ldots, y_n)$ таких, что для любых вектор-функций $\bar{g}_1(x_1, x_2), \ldots, \bar{g}_n(x_1, x_2)$ из $(F')_{x_1x_2}$ вектор-функция

$$\bar{f}(\bar{g}_1(x_1, x_2), \ldots, \bar{g}_n(x_1, x_2))$$

также принадлежит множеству $(F')_{x_1x_2}$. В силу замкнутости класса F' имеем $F' \subseteq P(F')$. В частности, множеству $P(F')$ принадлежат все селекторные вектор-функции. Нетрудно далее проверить, что $P(F')$ — замкнутый класс. Поскольку множеству $(F')_{x_1x_2}$ принадлежат селекторные вектор-функции $\bar{e}_1^2(x_1, x_2), \bar{e}_2^2(x_1, x_2)$, множество $(P(F'))_{x_1x_2}$ совпадает со множеством $(F')_{x_1x_2}$ и, следовательно, замкнутый класс $P(F')$ отличен от P_2^k.

Итак, всякий замкнутый класс F, отличный от P_2^k, содержится в одном из конечного числа замкнутых классов вида $P(F')$. Выберем теперь среди этих классов максимальные по включению (это можно сделать, поскольку число классов вида $P(F')$ конечно). Мы утверждаем, что если $P(F')$ — один из таких максимальных классов, то $P(F')$ является предполным в P_2^k классом. Действительно, класс $P(F')$ замкнут, отличен от P_2^k и согласно своему определению не содержится ни в каком другом замкнутом классе, отличном от $P(F')$ и P_2^k. Теорема доказана.

Следствие 3.1 (критерий полноты в P_2^k). *Система булевых вектор-функций полна в P_2^k тогда и только тогда, когда она целиком не содержится ни в одном из предполных в P_2^k классов.*

§ 2. Классы Слупецкого

Обозначим через Ω_k множество всех вектор-функций $\bar{f}(x_1,\ldots$ $\ldots,x_n)$ из P_2^k таких, что для некоторого i, $1 \leqslant i \leqslant n$, каждая из функций

$$\mathrm{pr}_1\,\bar{f}(x_1,\ldots,x_n), \qquad \ldots, \qquad \mathrm{pr}_k\,\bar{f}(x_1,\ldots,x_n)$$

либо существенно зависит только от переменной x_i, либо является константой. Множество Ω_k, очевидно, образует замкнутый класс. Предполный в P_2^k класс F назовем *классом Слупецкого*, если $\Omega_k \subseteq F$.

Дадим обозначения некоторым замкнутым классам из P_2^k, содержащим множество Ω_k. Для любого i, $1 \leqslant i \leqslant k$, пусть V_i есть множество всех таких вектор-функций $\bar{f}(x_1,\ldots,x_n)$ из P_2^k, что $\mathrm{pr}_i\,\bar{f} \in$ $\in L$ (напомним, что через L в гл. I был обозначен замкнутый класс всех линейных булевых функций). Нетрудно видеть, что множество V_i замкнуто относительно суперпозиции, $V_i \neq P_2^k$ и $\Omega_k \subseteq V_i$.

Пусть $i_1,\ldots,i_s$ — различные числа из множества $\{1,2,\ldots,k\}$, $s \geqslant 2$. Обозначим через $V_{i_1\ldots i_s}$ множество всех таких вектор-функций $\bar{f}(x_1,\ldots,x_n)$ из P_2^k, что хотя бы одна из функций $\mathrm{pr}_{i_1}\,\bar{f},\ldots,\mathrm{pr}_{i_s}\,\bar{f}$ является константой либо найдется такое j, $1 \leqslant j \leqslant n$, что все функции

$$\mathrm{pr}_{i_1}\,\bar{f}(x_1,\ldots,x_n), \qquad \ldots, \qquad \mathrm{pr}_{i_s}\,\bar{f}(x_1,\ldots,x_n)$$

существенно зависят лишь от переменной x_j. Несложно проверить, что множество $V_{i_1\ldots i_s}$ замкнуто относительно суперпозиции, $V_{i_1\ldots i_s} \neq P_2^k$ и $\Omega_k \subseteq V_{i_1\ldots i_s}$.

Если подмножества $\{i_1,\ldots,i_s\}$, $\{j_1,\ldots,j_r\}$ множества $\{1,2,\ldots,k\}$ различны, то классы $V_{i_1\ldots i_s}, V_{j_1\ldots j_r}$ также различны. Более того, они не содержатся друг в друге. В самом деле, если, например, $i_1 \notin \{j_1,\ldots$ $\ldots,j_r\}$, то классу $V_{i_1\ldots i_s}$ принадлежит вектор-функция $\bar{g}(x_1,x_2)$, у которой

$$\mathrm{pr}_{i_1}\,\bar{g}(x_1,x_2) = 0, \qquad \mathrm{pr}_l\,\bar{g}(x_1,x_2) = x_1x_2 \quad \text{при} \quad l \neq i_1.$$

Однако эта вектор-функция не содержится в классе $V_{j_1\ldots j_r}$. Если же

$$\{i_1,\ldots,i_s\} \subset \{j_1,\ldots,j_r\},$$

то классу $V_{i_1\ldots i_s}$ принадлежит вектор-функция $\bar{h}(x_1, x_2)$ такая, что

$$\mathrm{pr}_{i_1}\, \bar{h}(x_1, x_2) = \ldots = \mathrm{pr}_{i_s}\, \bar{h}(x_1, x_2) = x_1$$

и $\mathrm{pr}_l\, \bar{h}(x_1, x_2) = x_2$ при $l \notin \{i_1, \ldots, i_s\}$. Вместе с тем функция $\bar{h}(x_1, x_2)$ не входит в класс $V_{j_1\ldots j_r}$.

Теорема 3.3. *Класс P_2^k содержит ровно $2^k - 1$ классов Слупецкого. Все они имеют вид $V_{i_1\ldots i_s}$, где $\{i_1, \ldots, i_s\} \subseteq \{1, 2, \ldots, k\}$, $s \geqslant 1$.*

Доказательство. Поскольку классы $V_{i_1\ldots i_s}$ попарно не сравнимы по включению и содержат множество Ω_k, для доказательства теоремы достаточно установить следующее утверждение: если система F вектор-функций из P_2^k целиком не содержится ни в одном из классов вида $V_{i_1\ldots i_s}$, то множество $F \cup \Omega_k$ порождает класс P_2^k.

Пусть вектор-функция $\bar{f}$ из F не принадлежит классу V_i, $1 \leqslant i \leqslant k$. Тогда булева функция $\mathrm{pr}_i\, \bar{f}$ нелинейна. Во множество Ω_k входят вектор-функции $\bar{f}_1(x), \bar{f}_2(x)$, удовлетворяющие соотношениям

$$\mathrm{pr}_i\, \bar{f}_1(x) = 0, \qquad \mathrm{pr}_i\, \bar{f}_2(x) = \bar{x}.$$

Поэтому согласно теореме о полноте для класса P_2 тройка булевых функций $\mathrm{pr}_i\, \bar{f}, \mathrm{pr}_i\, \bar{f}_1, \mathrm{pr}_i\, \bar{f}_2$ полна в P_2. Значит, согласно лемме 3.2 для доказательства теоремы достаточно суперпозициями вектор-функций системы $F \cup \Omega_k$ получить вектор-функции $\bar{e}_1(x_1, x_2), \ldots, \bar{e}_k(x_1, x_2)$. Оставшаяся часть доказательства будет посвящена решению этой задачи.

Пусть $\{i_1, \ldots, i_s\} \subseteq \{1, 2, \ldots, k\}$, $s \geqslant 2$ и вектор-функция $\bar{f}(x_1, \ldots, x_n)$ из F не принадлежит классу $V_{i_1\ldots i_s}$. Покажем, во-первых, как суперпозициями функций из $\Omega_k \cup \{\bar{f}\}$ получить такую функцию $\bar{g}(x_1, x_2)$, что

$$\{\mathrm{pr}_{i_1}\, \bar{g}(x_1, x_2), \ldots, \mathrm{pr}_{i_s}\, \bar{g}(x_1, x_2)\} = \{e_1^2(x_1, x_2), e_2^2(x_1, x_2)\}.$$

Из $\bar{f} \notin V_{i_1\ldots i_s}$ следует, что функции $\mathrm{pr}_{i_1}\, \bar{f}, \ldots, \mathrm{pr}_{i_s}\, \bar{f}$ отличны от констант и не существует такого j, $1 \leqslant j \leqslant n$, что все функции

$$\mathrm{pr}_{i_1}\, \bar{f}(x_1, \ldots, x_n), \qquad \ldots, \qquad \mathrm{pr}_{i_s}\, \bar{f}(x_1, \ldots, x_n) \tag{3.3}$$

существенно зависят лишь от переменной x_j. Пусть $x_{j_1}, \ldots x_{j_s}$ — существенные переменные функций (3.3) и не все числа $j_1, \ldots, j_s$ равны между собой.

По определению существенной зависимости для любого t, $1 \leqslant t \leqslant s$, найдутся такие величины $a_1^t, \ldots a_{j_t-1}^t, a_{j_t+1}^t, \ldots, a_n^t$, что

$$\mathrm{pr}_{i_t}\, \bar{f}(a_1^t, \ldots, a_{j_t-1}^t, x_{j_t}, a_{j_t+1}^t, \ldots, a_n^t) \in \{x_{j_t}, \bar{x}_{j_t}\}.$$

Определим вектор-функции $\bar{g}_1(x_1), \ldots, \bar{g}_n(x_n)$:

$$\mathrm{pr}_i\, \bar{g}_l(x_l) = \begin{cases} a_l^t, & \text{если для некоторого } t,\ 1 \leqslant t \leqslant s, \text{ имеем } i = i_t \text{ и } l \neq j_t, \\ x_l & \text{в остальных случаях} \end{cases}$$

$(1 \leqslant i \leqslant k,\ 1 \leqslant l \leqslant n)$. Полагая

$$\bar{f}_1(x_1, \ldots, x_n) = \bar{f}(\bar{g}_1(x_1), \ldots, \bar{g}_n(x_n)),$$

будем иметь для любого t, $1 \leqslant t \leqslant s$,

$$\mathrm{pr}_{i_t}\, \bar{f}_1(x_1, \ldots, x_n) \in \{x_{j_t}, \bar{x}_{j_t}\}.$$

Поскольку последовательность $j_1, \ldots, j_s$ содержит не менее двух различных чисел, переменные $x_1, \ldots, x_n$ вектор-функции $\bar{f}_1(x_1, \ldots, x_n)$ можно так заменить переменными x_1, x_2, что полученная в результате этой замены вектор-функция $\bar{g}_{n+1}(x_1, x_2)$ будет удовлетворять условию

$$\{\mathrm{pr}_{i_1}\, \bar{g}_{n+1}(x_1, x_2), \ldots, \mathrm{pr}_{i_s}\, \bar{g}_{n+1}(x_1, x_2)\} \subseteq \{x_1, \bar{x}_1, x_2, \bar{x}_2\},$$

причем каждая переменная x_1, x_2 является существенной для некоторой функции из множества

$$\{\mathrm{pr}_{i_1}\, \bar{g}_{n+1}(x_1, x_2), \ldots, \mathrm{pr}_{i_s}\, \bar{g}_{n+1}(x_1, x_2)\}.$$

Теперь остается положить

$$\bar{g}(x_1, x_2) = \bar{g}_{n+1}(\bar{g}_{n+1}(x_1, x_2), \bar{g}_{n+1}(x_1, x_2)).$$

Продолжая доказательство теоремы, покажем, как получить вектор-функции $\bar{e}_1, \ldots, \bar{e}_k$. Рассмотрим, например, процесс построения функции $\bar{e}_1(x_1, x_2)$. По доказанному из вектор-функции $\bar{f}$, не принадлежащей классу $V_{1\ldots k}$, и функций множества Ω_k суперпозициями можно получить такую функцию $\bar{g}(x_1, x_2)$, что

$$\{\mathrm{pr}_1\, \bar{g}(x_1, x_2), \ldots, \mathrm{pr}_k\, \bar{g}(x_1, x_2)\} = \{e_1^2(x_1, x_2),\ e_2^2(x_1, x_2)\}.$$

Можно предполагать, что $\mathrm{pr}_1\, \bar{g}(x_1, x_2) = e_1^2(x_1, x_2)$, поскольку в противном случае в вектор-функции $\bar{g}(x_1, x_2)$ можно переставить переменные x_1, x_2. Если

$$\mathrm{pr}_2\, \bar{g}(x_1, x_2) = \ldots = \mathrm{pr}_k\, \bar{g}(x_1, x_2) = e_2^2(x_1, x_2),$$

то вектор-функция $\bar{g}$ совпадает с вектор-функцией $\bar{e}_1$. Пусть $\bar{g} \neq \bar{e}_1$, т. е. среди функций $\mathrm{pr}_2\, \bar{g}(x_1, x_2), \ldots, \mathrm{pr}_k\, \bar{g}(x_1, x_2)$ имеется хотя бы одна функция $e_1^2(x_1, x_2)$. Для определенности будем считать, что

$$\mathrm{pr}_2\, \bar{g}(x_1, x_2) = \ldots = \mathrm{pr}_m\, \bar{g}(x_1, x_2) = e_1^2(x_1, x_2),$$

$$\mathrm{pr}_{m+1}\,\bar g(x_1,x_2) = \ldots = \mathrm{pr}_k\,\bar g(x_1,x_2) = e_2^2(x_1,x_2).$$

Как установлено выше, в замыкании $[F\cup\Omega_k]$ содержится такая функция $\bar h_1(x_1,x_2)$, что

$$\{\mathrm{pr}_1\,\bar h_1(x_1,x_2),\ldots,\mathrm{pr}_m\,\bar h_1(x_1,x_2)\} = \{e_1^2(x_1,x_2),\ e_2^2(x_1,x_2)\}.$$

Так же, как и для функции $\bar g$, можно предполагать, что

$$\mathrm{pr}_1\,\bar h_1(x_1,x_2) = e_1^2(x_1,x_2).$$

Положим

$$\bar h_2(x_1,x_2) = \bar g(\bar h_1(x_1,x_2),x_2).$$

Из определения вектор-функций $\bar g, \bar h_1$ следует, что

$$\{\mathrm{pr}_1\,\bar h_2(x_1,x_2),\ldots,\mathrm{pr}_k\,\bar h_2(x_1,x_2)\} = \{e_1^2(x_1,x_2),\ e_2^2(x_1,x_2)\},$$

$$\mathrm{pr}_1\,\bar h_2(x_1,x_2) = e_1^2(x_1,x_2),$$

$$\mathrm{pr}_{m+1}\,\bar h_2(x_1,x_2) = \ldots = \mathrm{pr}_k\,\bar h_2(x_1,x_2) = e_2^2(x_1,x_2)$$

и среди функций

$$\mathrm{pr}_2\,\bar h_2(x_1,x_2),\qquad \ldots,\qquad \mathrm{pr}_m\,\bar h_2(x_1,x_2)$$

есть хотя бы одна функция $e_2^2(x_1,x_2)$. Таким образом, последовательность

$$\mathrm{pr}_1\,\bar h_2(x_1,x_2),\qquad \ldots,\qquad \mathrm{pr}_k\,\bar h_2(x_1,x_2)$$

содержит по крайней мере на одну функцию $e_2^2(x_1,x_2)$ больше, чем последовательность

$$\mathrm{pr}_1\,\bar g(x_1,x_2),\qquad \ldots,\qquad \mathrm{pr}_k\,\bar g(x_1,x_2).$$

Если

$$\mathrm{pr}_2\,\bar h_2(x_1,x_2) = \ldots = \mathrm{pr}_k\,\bar h_2(x_1,x_2) = e_2^2(x_1,x_2),$$

то мы имеем равенство $\bar h_2(x_1,x_2) = \bar e_1(x_1,x_2)$. В противном случае к функции $\bar h_2(x_1,x_2)$ применяем прием, описанный выше для функции $\bar g(x_1,x_2)$. Не более чем через $k-1$ шагов этого процесса будет получена искомая функция $\bar e_1(x_1,x_2)$. Теорема доказана.

§ 3. Многоосновные предикаты

Предположим, что имеется k «различных» экземпляров множества $E_2=\{0,1\}$, которые обозначим через $E^1,\ldots,E^k$. Под *k-основным предикатом* будем понимать предикат $\rho(x_1,\ldots,x_m)$, у которого переменная x_j принимает значения из множества E^{i_j}, $1\leqslant j\leqslant m$,

$1 \leqslant i_j \leqslant k$. Таким образом, предикат $\rho(x_1, \ldots, x_m)$ отображает множество $E^{i_1} \times \ldots \times E^{i_m}$ во множество истинностных значений $\{И, Л\}$. Переменную x_j предиката $\rho(x_1, \ldots, x_m)$ будем называть *переменной типа* i_j. В чисто технических целях переменные одного типа в предикате ρ удобно записывать рядом. Так, мы будем писать

$$\rho(x_1^1, \ldots, x_{r_1}^1, \ldots, x_1^k, \ldots, x_{r_k}^k), \tag{3.4}$$

указывая верхним индексом тип переменной.

Большинство понятий, приведенных в гл. II для булевых предикатов, с очевидными изменениями переносятся на многоосновные предикаты. Например, пусть на множествах $\{1, \ldots, r_1\}, \ldots, \{1, \ldots, r_k\}$ заданы отношения эквивалентности $\varepsilon_1, \ldots, \varepsilon_k$. Тогда *k-основная диагональ*, соответствующая отношениям $\varepsilon_1, \ldots, \varepsilon_k$, задается формулой

$$\mathop{\&}_{\varepsilon_1(i,j)} \cdots \mathop{\&}_{\varepsilon_k(p,q)} (x_i^1 = x_j^1) \,\&\, \ldots \,\&\, (x_p^k = x_q^k),$$

где конъюнкции берутся по всем парам чисел $(i, j), \ldots, (p, q)$, эквивалентным в смысле отношений $\varepsilon_1, \ldots, \varepsilon_k$.

Над многоосновными предикатами определяются те же операции, что и над булевыми предикатами. Следует лишь подчеркнуть, что в многоосновных предикатах можно отождествлять переменные только одного и того же типа.

Может случиться, что при применении операции проектирования к k-основному предикату образуется l-основный предикат, $l < k$, не содержащий свободных переменных некоторых типов. Этот предикат, тем не менее, иногда будет удобно считать k-основным. Для этого достаточно добавить к предикату фиктивные переменные отсутствующих типов. Как мы увидим далее, подобная операция не влияет на получаемые результаты.

Если R — множество k-основных предикатов, то через $[R]$ обозначим множество всех k-основных предикатов, реализуемых формулами над R. Как и в случае булевых предикатов, k-основный предикат (3.4) ширины m будем задавать в виде матрицы X_ρ с $r_1 + \ldots + r_k$ строками и m столбцами. Будем считать, что наборы $(a_1^1, \ldots, a_{r_1}^1, \ldots \ldots, a_1^k, \ldots, a_{r_k}^k)$, удовлетворяющие предикату ρ, располагаются в матрице X_ρ сверху вниз по столбцам: в первой строке элементы a_1^1, во второй строке элементы a_2^1 и т. д.

Пусть $\bar{f}(x_1, \ldots, x_n)$ — вектор-функция (3.1). Говорим, что вектор-функция $\bar{f}$ *сохраняет k-основный предикат* (3.4), если для любых n наборов

$$(a_1^1, \ldots, a_{r_1}^1, \ldots, a_1^k, \ldots, a_{r_k}^k), \qquad \ldots, \qquad (c_1^1, \ldots, c_{r_1}^1, \ldots, c_1^k, \ldots, c_{r_k}^k),$$

удовлетворяющих предикату ρ, набор

$$(f_1(a_1^1,\ldots,c_1^1),\ldots,f_1(a_{r_1}^1,\ldots,c_{r_1}^1),\ \ \ldots,\ \ f_1(a_1^k,\ldots,c_1^k),\ldots,f_1(a_{r_1}^k,\ldots,c_{r_1}^k))$$

также удовлетворяет предикату ρ.

Множество всех вектор-функций из P_2^k, сохраняющих k-основный предикат ρ, обозначим через $\mathrm{Pol}(\rho)$, а множество всех k-основных предикатов, каждый из которых сохраняется вектор-функцией $\bar f$ из P_2^k, обозначим через $\mathrm{Inv}(\bar f)$. Легко проверяется, что для любого k-основного предиката ρ множество $\mathrm{Pol}(\rho)$ является замкнутым классом вектор-функций из P_2^k, содержащим все селекторные вектор-функции $\bar e_i^n$ $(1 \leqslant i \leqslant n,\ n = 1, 2, \ldots)$, и для любой вектор-функции $\bar f$ из P_2^k множество $\mathrm{Inv}(\bar f)$ является замкнутым классом k-основных предикатов, содержащим все k-основные диагонали. Если R — множество k-основных предикатов, F — множество вектор-функций из P_2^k, то так же, как и в случае булевых функций и булевых предикатов, полагаем

$$\mathrm{Pol}(R) = \bigcap_{\rho\in R} \mathrm{Pol}(\rho), \qquad \mathrm{Inv}(F) = \bigcap_{\bar f\in F} \mathrm{Inv}(\bar f).$$

Еще раз подчеркнем, что для любого множества R k-основных предикатов множество $\mathrm{Pol}(R)$ представляет собой замкнутый класс вектор-функций из P_2^k, содержащий все селекторные вектор-функции, и для любого множества F вектор-функций из P_2^k множество $\mathrm{Inv}(F)$ представляет собой замкнутый класс k-основных предикатов, содержащий все k-основные диагонали.

Заметим, что если предикат ρ не зависит существенно от переменных типа i, то у вектор-функции $\bar f$, сохраняющей предикат ρ, булева компонента $\mathrm{pr}_i\,\bar f$ может быть произвольной булевой функцией (от того же числа переменных, что и функция $\bar f$). Это замечание позволяет нам рассматривать вместо k-основных предикатов l-основные, $l < k$, и говорить о вектор-функциях из P_2^k, сохраняющих l-основные предикаты.

§ 4. Соответствие Галуа

Как и в § 3 из гл. II, пусть $\Phi(\bar f, \rho)$ обозначает отношение «вектор-функция $\bar f$ из P_2^k сохраняет k-основный предикат ρ». Отношение Φ определяет соответствие Галуа между подмножествами множества k-основных предикатов и подмножествами множества P_2^k

вектор-функций размерности k. Действительно, имеют место легко проверяемые соотношения

$$R \subseteq \mathrm{Inv}(\mathrm{Pol}(R)), \tag{3.5}$$

$$F \subseteq \mathrm{Pol}(\mathrm{Inv}(F)). \tag{3.6}$$

Кроме того, если R_1, R_2 — множества k-основных предикатов, F_1, F_2 — множества вектор-функций из P_2^k, то из $R_1 \subseteq R_2$ и $F_1 \subseteq F_2$ следует, что

$$\mathrm{Pol}(R_1) \supseteq \mathrm{Pol}(R_2), \qquad \mathrm{Inv}(F_1) \supseteq \mathrm{Inv}(F_2).$$

Таким образом, отображения Pol и Inv антимонотонны. Множества $\mathrm{Inv}(\mathrm{Pol}(R))$ и $\mathrm{Pol}(\mathrm{Inv}(F))$ суть соответственно замыкания Галуа множества R k-основных предикатов и множества F вектор-функций из P_2^k.

Замыкание Галуа $\mathrm{Inv}(\mathrm{Pol}(R))$ является замкнутым классом k-основных предикатов и содержит все k-основные диагонали. Замыкание Галуа $\mathrm{Pol}(\mathrm{Inv}(F))$ является замкнутым классом вектор-функций из P_2^k и содержит все селекторные вектор-функции.

В этом параграфе мы докажем, что для замкнутого множества R k-основных предикатов, содержащего все k-основные диагонали, имеет место равенство $R = \mathrm{Inv}(\mathrm{Pol}(R))$, а для замкнутого множества F вектор-функций из P_2^k, содержащего все селекторные вектор-функции, — равенство $F = \mathrm{Pol}(\mathrm{Inv}(F))$. Доказательства в значительной степени повторяют соответствующие доказательства для случая булевых функций и предикатов из § 3 из гл. II. Поэтому ниже мы приводим лишь основные моменты доказательств.

Пусть F — множество вектор-функций из P_2^k. Так же, как и в гл. II, для любого n, $n \geqslant 1$, определим k-основный $k2^n$-местный предикат $\gamma_n(y_1^1, \ldots, y_{2^n}^1, \ldots, y_1^k, \ldots, y_{2^n}^k)$, который назовем *$n$-графиком* множества F. Если $\widetilde{a}_1, \ldots, \widetilde{a}_{2^n}$ — все двоичные наборы длины n, расположенные в лексикографическом порядке, то предикату γ_n удовлетворяют те и только те наборы длины $k2^n$, которые имеют вид

$$(f_1(\widetilde{a}_1), \ldots, f_1(\widetilde{a}_{2^n}), \ldots, f_k(\widetilde{a}_1), \ldots, f_k(\widetilde{a}_{2^n})),$$

где $(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$ — n-местная вектор-функция из F.

Теорема 3.4. *Пусть F — замкнутый класс вектор-функций из P_2^k, содержащий все селекторные вектор-функции. Тогда*

$$F = \mathrm{Pol}(\mathrm{Inv}(F)).$$

Доказательство. В силу соотношения (3.6) достаточно установить лишь включение

$$\mathrm{Pol}(\mathrm{Inv}(F)) \subseteq F. \tag{3.7}$$

Ввиду замкнутости класса F n-график γ_n класса F принадлежит множеству $\mathrm{Inv}(F)$. Если $\bar{f}(x_1, \ldots, x_n)$ — вектор-функция из $\mathrm{Pol}(\mathrm{Inv}(F))$, то она, в частности, сохраняет предикат γ_n. Поэтому, взяв n наборов длины $k2^n$, которые удовлетворяют предикату γ_n и соответствуют селекторным вектор-функциям

$$\bar{e}_1^n(x_1, \ldots, x_n), \qquad \ldots, \qquad \bar{e}_n^n(x_1, \ldots, x_n),$$

в силу очевидного равенства

$$\bar{f}(\bar{e}_1^n(x_1, \ldots, x_n), \ldots, \bar{e}_n^n(x_1, \ldots, x_n)) = \bar{f}(x_1, \ldots, x_n)$$

получим, что $\bar{f} \in F$. Таким образом, включение (3.7) справедливо, и теорема доказана.

Как и в случае булевых предикатов, k-основный предикат ρ назовем *стандартным*, если соответствующая ему матрица X_ρ не содержит одинаковых строк.

Лемма 3.3. *Пусть F — множество вектор-функций из P_2^k, содержащее все селекторные вектор-функции, ρ — стандартный k-основный предикат ширины n и $\rho \in \mathrm{Inv}(F)$. Тогда ρ получается из n-графика γ_n множества F с помощью операций проектирования и перестановки переменных.*

Доказательство леммы 3.3 почти дословно повторяет доказательство леммы 2.1. Стоит лишь отметить, что любой двоичный набор длины n будет являться началом ровно k строк матрицы X_{γ_n}, номера этих строк отличаются на величины, кратные 2^n.

Теорема 3.5. *Пусть R — замкнутый класс k-основных предикатов, содержащий все k-основные диагонали. Тогда*

$$R = \mathrm{Inv}(\mathrm{Pol}(R)).$$

Доказательство. В силу соотношения (3.5) установим лишь включение

$$\mathrm{Inv}(\mathrm{Pol}(R)) \subseteq R. \tag{3.8}$$

Из леммы 3.3 в силу вхождения в класс R всех k-основных диагоналей для доказательства соотношения (3.8) достаточно показать, что при любом n, $n \geqslant 1$, n-график γ_n множества $\mathrm{Pol}(R)$ реализуется формулой над множеством R. Так же, как в доказательстве теоремы 2.2, число n можно считать достаточно большим.

Пусть сначала множество $\mathrm{Pol}(R)$ порождается одним k-основным предикатом (3.4), т. е.

$$\mathrm{Pol}(R) = \mathrm{Pol}(\rho).$$

Зафиксируем натуральное n, $n \geqslant 2^{r_1+\ldots+r_k}$, и предположим, что первые n столбцов матрицы X_{γ_n} отвечают селекторным вектор-функциям $\bar{e}_1^n, \ldots, \bar{e}_n^n$. Так же, как в случае одноосновного предиката ρ, сформулируем определяющее свойство матрицы X_{γ_n}.

Именно, выберем в матрице X_{γ_n} $r_1 + \ldots + r_k$ строк следующим образом: r_1 строк из первых 2^n строк, r_2 строк из следующих 2^n строк и т. д. Если в полученной подматрице матрицы X_{γ_n} первые n столбцов будут принадлежать матрице X_ρ, то и остальные столбцы этой подматрицы должны принадлежать матрице X_ρ.

Это свойство матрицы X_{γ_n} положено в основу построения предиката γ_n из предиката ρ.

Пусть s — ширина предиката ρ и для любого i, $1 \leqslant i \leqslant k$, пусть

$$(x_1^i, \ldots, x_{r_i}^i), \qquad \ldots, \qquad (z_1^i, \ldots, z_{r_i}^i)$$

— s^n наборов переменных типа i, не содержащих одинаковых переменных. Положим

$$\rho_1(x_1^1, \ldots, x_{r_1}^1, \ldots, z_1^1, \ldots, z_{r_1}^1, \ldots, x_1^k, \ldots, x_{r_1}^k, \ldots, z_1^k, \ldots, z_{r_1}^k) \equiv$$
$$\equiv \rho(x_1^1, \ldots, x_{r_1}^1, \ldots, x_1^k, \ldots, x_{r_k}^k) \mathbin{\&} \ldots \mathbin{\&} \rho(z_1^1, \ldots, z_{r_1}^1, \ldots, z_1^k, \ldots, z_{r_k}^k).$$

Будем считать, что столбцы матрицы X_{ρ_1} упорядочены таким образом, что для любых (не обязательно различных) n столбцов матрицы X_ρ найдутся такие $r_1 + \ldots + r_k$ строк, что в подматрице матрицы X_{ρ_1}, образованной этими строками, в качестве первых n столбцов стоят выбранные n столбцов матрицы X_ρ. Способ построения предиката ρ_1 из предиката ρ подсказывает, какие именно $r_1 + \ldots + r_k$ строк в матрице X_{ρ_1} следует выбрать. Так же, как и в теореме 2.2, из предиката ρ_1 в три этапа получаем предикат γ_n.

Сначала определяем k отношений эквивалентности $\varepsilon_1, \ldots, \varepsilon_k$ на множествах

$$\{1, 2, \ldots, r_1 s^n\}, \qquad \ldots, \qquad \{(r_1 + \ldots + r_{k-1})s^n + 1, \ldots, (r_1 + \ldots + r_k)s^n\},$$

полагая $\varepsilon_i(t, v)$ истинным в том и только том случае, когда в матрице X_{ρ_1} у строк с номерами t и v совпадают начала длины n. Далее проводим в предикате ρ_1 отождествления переменных, которым в матрице X_{ρ_1} отвечают номера строк, эквивалентные в смысле отношений $\varepsilon_1, \ldots, \varepsilon_k$. Полученный в результате этих отождествлений предикат обозначаем через ρ_2. Осуществляем в предикате ρ_2 перестановку переменных таким образом, чтобы в матрице X_{ρ_3} полученного после этого предиката $\rho_3(y_1^1, \ldots, y_{m_1}^1, \ldots, y_1^k, \ldots, y_{m_k}^k)$ среди строк, отвечающих фиксированному типу переменных, начальные двоичные наборы длины n следовали в лексикографическом порядке. Наконец, если для некоторого i, $1 \leqslant i \leqslant k$, окажется, что $m_i < 2^n$, то путем конъюнкции с диагональю

$$(y_{m_i+1}^i = y_{m_i+1}^i) \,\&\, \ldots \,\&\, (y_{2^n}^i = y_{2^n}^i)$$

добавляем к предикату ρ_3 фиктивные переменные $y_{m_1+1}^i, \ldots, y_{2^n}^i$. В результате получаем n-график γ_n множества $\mathrm{Pol}(\rho)$.

Случай, когда множество R не порождается одним предикатом, рассматривается так же, как в теореме 2.2.

§ 5. Минимальные предикаты

Согласно соответствию Галуа класс $\mathrm{Inv}(P_2^k)$ всех k-основных диагоналей является наименьшим по включению среди замкнутых в смысле Галуа классов k-основных предикатов. Следующими в частично упорядоченном по включению множестве замкнутых в смысле Галуа классов k-основных предикатов являются классы, которые мы называем *минимальными*. Иными словами, замкнутый в смысле Галуа класс k-основных предикатов R называется минимальным, если он отличен от класса $\mathrm{Inv}(P_2^k)$ и между классами R и $\mathrm{Inv}(P_2^k)$ нет других замкнутых в смысле Галуа классов.

Если R — минимальный класс k-основных предикатов, а ρ — предикат из R, отличный от k-основной диагонали, то $R = \mathrm{Inv}(\mathrm{Pol}(\rho))$. Иначе говоря, минимальный класс R порождается любым своим предикатом, отличным от диагонали, и k основными диагоналями. Предикаты минимальных классов, отличные от k-основных диагоналей, мы называем *минимальными k-основными предикатами*.

Так же, как для булевых предикатов, определение минимального k-основного предиката можно дать, не опираясь на понятие минимального класса. Именно, отличный от диагонали k-основный предикат ρ является минимальным, если для любого отличного от диагонали k-основного предиката σ, который реализуется формулой над множеством $\{\rho\} \cup \mathrm{Inv}(P_2^k)$, предикат ρ в свою очередь может быть реализован формулой над множеством $\{\sigma\} \cup \mathrm{Inv}(P_2^k)$.

В дальнейшем нас будут интересовать преимущественно минимальные предикаты, которые являются стандартными и не содержат фиктивных переменных. В этом случае такими же рассуждениями, как в § 5 из гл. II, можно убедиться в том, что в приведенном выше определении минимального предиката множество $\mathrm{Inv}(P_2^k)$ всех k-основных диагоналей можно опустить. В связи с этим доказательство минимальности предиката ρ часто будет проводиться по следующей схеме. Предполагая, что предикат ρ стандартен и не содержит фиктивных переменных, а предикат σ реализуется формулой над предикатом ρ, приводим эту формулу к предваренному виду. Получаем

$$\sigma \equiv (\exists X^1)\ldots(\exists X^k)(\rho_1 \,\&\, \ldots \,\&\, \rho_p), \tag{3.9}$$

где $X^1, \ldots, X^k$ — списки переменных типов $1, \ldots, k$, а предикаты $\rho_1, \ldots$ $\ldots, \rho_p$ получаются из предиката ρ некоторыми подстановками переменных (возможно, с отождествлениями). В дальнейшем проводим анализ формулы (3.9) на предмет ее возможного упрощения и получения формулы, определяющей предикат ρ через предикат σ.

Л е м м а 3.4. *Пусть $\rho(\widetilde{x}^1, \ldots, \widetilde{x}^l)$ — минимальный l-основный предикат, а предикат $\sigma(\widetilde{x}^1, \ldots, \widetilde{x}^l, x^{l+1})$ получается из предиката ρ добавлением фиктивной переменной x^{l+1}:*

$$\sigma(\widetilde{x}^1, \ldots, \widetilde{x}^l, x^{l+1}) \equiv \rho(\widetilde{x}^1, \ldots, \widetilde{x}^l) \,\&\, (x^{l+1} = x^{l+1}). \tag{3.10}$$

Тогда σ — минимальный $(l+1)$-основный предикат.

Д о к а з а т е л ь с т в о. Пусть отличный от диагонали $(l+1)$-основный предикат τ реализуется формулой над множеством $(l+$ $+1)$-основных предикатов $\{\sigma\} \cup \mathrm{Inv}(P_2^{l+1})$. Поскольку согласно формуле (3.10) предикат σ есть конъюнкция предиката ρ и (полной) диагонали $x^{l+1} = x^{l+1}$, после приведения этой формулы к предваренному виду получим

$$\tau \equiv (\exists X^1)\ldots(\exists X^{l+1})(\rho'_1 \,\&\, \ldots \,\&\, \rho'_p \,\&\, D), \tag{3.11}$$

где $X^1, \ldots, X^{l+1}$ — списки переменных типов $1, \ldots, l+1$, предикаты $\rho'_1, \ldots, \rho'_p$ получаются из предиката ρ некоторыми подстановками переменных, а D — $(l+1)$-основная диагональ, которая фиктивно зависит от переменных типа $l+1$. Так же, как в § 5 из гл. II, убеждаемся, что формулу (3.11) можно привести к виду

$$\tau \equiv (\exists Y^1)\ldots(\exists Y^l)(\rho_1 \,\&\, \ldots \,\&\, \rho_q) \,\&\, D_1, \tag{3.12}$$

где $Y^1, \ldots, Y^l$ — списки переменных типов $1, \ldots, l$, предикаты $\rho_1, \ldots$ $\ldots, \rho_q$ получаются из предиката ρ подстановками переменных и D_1 —

$(l+1)$-основная диагональ, которая фиктивно зависит от переменных типа $l+1$. Если Y^{l+1} — все переменные типа $l+1$ предиката τ, то из (3.12) следует, далее, что отличный от диагонали l-основный предикат $\tau^0 \equiv (\exists Y^{l+1})\tau$ можно представить в виде

$$\tau^0 \equiv (\exists Y^1)\ldots(\exists Y^l)(\rho_1 \mathbin{\&} \ldots \mathbin{\&} \rho_q) \mathbin{\&} D_2, \tag{3.13}$$

где D_2 — l-основная диагональ. Значит, в силу минимальности предиката ρ его можно реализовать формулой над множеством $\{\tau^0\} \cup \cup \operatorname{Inv}(P_2^l)$:

$$\rho \equiv (\exists Z^1)\ldots(\exists Z^l)(\tau_1^0 \mathbin{\&} \ldots \mathbin{\&} \tau_r^0 \mathbin{\&} D_3), \tag{3.14}$$

где предикаты $\tau_1^0, \ldots, \tau_r^0$ получаются из предиката τ^0 некоторыми подстановками переменных, а D_3 — l-основная диагональ. Объединяя теперь формулы (3.14), (3.13), (3.10) с очевидной эквивалентностью $\rho \equiv (\exists x^{l+1})\sigma$, убеждаемся, что предикат σ можно реализовать формулой над множеством $\{\tau\} \cup \operatorname{Inv}(P_2^{l+1})$. Лемма доказана.

Лемму 3.4 можно доказать другим способом. Пусть минимальный предикат ρ определяет в P_2^l предполный класс R, т. е. $R = \operatorname{Pol}(\rho)$. Из определения предиката σ сразу следует, что множество $\operatorname{Pol}(\sigma)$ представимо в виде

$$\{(f_1(x_1,\ldots,x_n),\ldots,f_l(x_1,\ldots,x_n),f_{l+1}(x_1,\ldots,x_n))\},$$

где

$$(f_1(x_1,\ldots,x_n),\ldots,f_l(x_1,\ldots,x_n)) \in R, \qquad f_{l+1}(x_1,\ldots,x_n) \in P_2,$$

т. е. у вектор-функции $\bar f(x_1,\ldots,x_n)$ из $\operatorname{Pol}(\sigma)$ первые l компонент образуют вектор-функцию из $\operatorname{Pol}(\rho)$, а $(l+1)$-я компонента может быть произвольной n-местной булевой функцией. Это позволяет доказывать предполноту класса $\operatorname{Pol}(\sigma)$, используя идеи и технику доказательства утверждений из § 1.

Напомним, что через $E^1,\ldots,E^k$ мы обозначили k «различных» экземпляров множества E_2. Очевидно, что изложенная выше теория инвариантна по отношению к переименованию множеств $E^1,\ldots,E^k$. В частности, справедлива следующая

Лемма 3.5. *Пусть $\rho(\widetilde{y}^1,\ldots,\widetilde{y}^k)$ — минимальный k-основный предикат, π — подстановка на множестве $\{1,2,\ldots,k\}$ и*

$$\sigma(\widetilde{x}^1,\ldots,\widetilde{x}^k) \equiv \rho(\widetilde{x}^{\pi(1)},\ldots,\widetilde{x}^{\pi(k)}).$$

Тогда σ — минимальный k-основный предикат.

Лемма 3.6. *Пусть k-основный предикат $\rho(x^1, \widetilde{x}^2, \ldots, \widetilde{x}^k)$ представим в виде*

$$\rho(x^1, \widetilde{x}^2, \ldots, \widetilde{x}^k) \equiv (x^1 = a) \vee \sigma(\widetilde{x}^2, \ldots, \widetilde{x}^k),$$

где $a \in E_2$ и $\sigma(\widetilde{x}^2, \ldots, \widetilde{x}^k)$ — $(k-1)$-основный предикат. И пусть k-основный предикат τ реализуется некоторой формулой над предикатом ρ. Тогда предикат τ можно реализовать такой формулой над предикатом ρ, которая не содержит кванторов по переменным типа 1.

Доказательство. Формулу, реализующую предикат τ, приведем к предваренному виду:

$$\tau \equiv (\exists X^k) \ldots (\exists X^1)(\rho_1 \mathbin{\&} \ldots \mathbin{\&} \rho_p), \tag{3.15}$$

где предикаты $\rho_1, \ldots, \rho_p$ получаются из предиката ρ некоторыми подстановками переменных. Если x_j^1 — переменная из группы X^1 и $\rho_{i_1}, \ldots, \rho_{i_s}$ — все предикаты из числа $\rho_1, \ldots, \rho_p$, содержащие переменную x_j^1, то предикат $\rho_{i_1} \mathbin{\&} \ldots \mathbin{\&} \rho_{i_s}$, очевидно, представим в виде

$$(x_j^1 = a) \vee \sigma_1(\widetilde{y}^2, \ldots, \widetilde{y}^k).$$

Поскольку

$$(\exists x_j^1)((x_j^1 = a) \vee \sigma_1(\widetilde{y}^2, \ldots, \widetilde{y}^k)) \equiv (\exists x_j^1)(x_j^1 = a) \vee \sigma_1(\widetilde{y}^2, \ldots, \widetilde{y}^k)$$

и $(\exists x_j^1)(x_j^1 = a)$ — полный предикат, то

$$(\exists x_j^1)(\rho_{i_1} \mathbin{\&} \ldots \mathbin{\&} \rho_{i_s})$$

— также полный предикат. Это соображение позволяет в формуле (3.15) исключить кванторы по переменным группы X^1, опустив в конъюнкции $\rho_1 \mathbin{\&} \ldots \mathbin{\&} \rho_p$ все сомножители, содержащие переменные группы X^1. Лемма доказана.

Теорема 3.6. *Пусть $n \geqslant 2$ и n-основный предикат*

$$\rho(x^1, \ldots, x^m, x_1^{m+1}, x_2^{m+1}, \ldots, x_1^n, x_2^n)$$

представим в виде

$$(x^1 = a_1) \vee \ldots \vee (x^m = a_m) \vee (x_1^{m+1} = x_2^{m+1}) \vee \ldots \vee (x_1^n = x_2^n),$$

где $a_1, \ldots, a_m \in E_2$, $0 \leqslant m \leqslant n$. Тогда ρ — минимальный предикат.

Доказательство. Из представления предиката ρ видно, что он стандартен и не содержит фиктивных переменных. Поэтому при доказательстве минимальности предиката ρ будем рассматривать лишь формулы, не содержащие диагоналей.

Пусть σ — отличный от диагонали предикат, который является стандартным, не содержит фиктивных переменных и реализуется формулой над предикатом ρ. Учитывая лемму 3.6 и приводя эту формулу к предваренному виду, будем иметь

$$\sigma \equiv (\exists X^{m+1}) \ldots (\exists X^n)(\rho_1 \,\&\, \ldots \,\&\, \rho_p), \tag{3.16}$$

где предикаты $\rho_1, \ldots, \rho_p$ получаются из предиката ρ некоторыми подстановками переменных. Будем считать, что все предикаты $\rho_1, \ldots$ $\ldots, \rho_p$ неполные.

По предположению предикат σ неполон. Это означает, в частности, что существуют такие наборы $\widetilde{a}^1, \ldots, \widetilde{a}^m$, что будет неполным предикат $\sigma(\widetilde{a}^1, \ldots, \widetilde{a}^m, \widetilde{y}^{m+1}, \ldots, \widetilde{y}^n)$. Из представления предиката ρ, неполноты предикатов $\rho_1, \ldots, \rho_p$ и формулы (3.16) следует, что набор $\widetilde{a}^i$, $1 \leqslant i \leqslant m$, состоит только из элементов $\bar{a}_i$. Значит, если в предикате σ для любого i, $1 \leqslant i \leqslant m$, отождествить все переменные типа i, то получится неполный предикат σ_1. Пусть его переменными типов $1, \ldots, m$ будут переменные $x^1, \ldots, x^m$. Поскольку при указанном отождествлении переменных каждый из предикатов $\rho_1, \ldots, \rho_p$ будет содержать дизъюнктивное слагаемое

$$(x^1 = a_1) \vee \ldots \vee (x^m = a_m),$$

предикат σ_1 в силу (3.16) примет вид

$$\sigma_1 \equiv (x^1 = a_1) \vee \ldots \vee (x^m = a_m) \vee (\exists X^{m+1}) \ldots (\exists X^n)(\tau_1 \,\&\, \ldots \,\&\, \tau_p), \tag{3.17}$$

где $\tau_1, \ldots, \tau_p$ — дизъюнктивные части предикатов $\rho_1, \ldots, \rho_p$, не содержащие переменных типов $1, \ldots, m$.

Пусть предикат τ_i, $1 \leqslant i \leqslant p$, имеет вид

$$\tau_1 \equiv \omega_i \vee (x^n_{a_i} = x^n_{b_i}), \tag{3.18}$$

где $(n-m-1)$-основный предикат ω_i не содержит переменных типа n и $a_i \neq b_i$ (поскольку предикат ρ_i и вместе с ним предикат τ_i неполны). Пользуясь эквивалентностью (3.18), представим конъюнкцию $\tau_1 \,\&\, \ldots \,\&\, \tau_p$ в виде дизъюнкции 2^p слагаемых, одно из которых есть диагональ

$$(x^n_{a_1} = x^n_{b_1}) \,\&\, \ldots \,\&\, (x^n_{a_p} = x^n_{b_p}).$$

Очевидно, что

$$(\exists X^n)((x^n_{a_1} = x^n_{b_1}) \,\&\, \ldots \,\&\, (x^n_{a_p} = x^n_{b_p}))$$

— также неполная диагональ (иначе был бы полным предикат σ_1). Значит, ее переменные можно так заменить переменными x^n_1, x^n_2, что в результате получится диагональ $x_1^n = x_2^n$. Если ω — какое-либо из остальных $2^p - 1$ дизъюнктивных слагаемых, составляющих предикат $\tau_1 \mathbin{\&} \ldots \mathbin{\&} \tau_p$, то после указанной замены переменных предикат $(\exists X^n)\omega$ превратится в предикат вида $\omega' \mathbin{\&} (x_1^n = x_2^n)$, где предикат ω' не содержит переменных типа n, либо в предикат ω'. Однако предикат $\omega' \mathbin{\&} (x_1^n = x_2^n)$ поглощается диагональю $x_1^n = x_2^n$. Поэтому формулу

$$(\exists X^n)(\tau_1 \mathbin{\&} \ldots \mathbin{\&} \tau_p)$$

после указанных преобразований можно привести к виду

$$\omega_1' \vee \ldots \vee \omega_q' \vee (x_1^n = x_2^n),$$

где $q \leqslant 2^p - 1$ и предикаты $\omega_1', \ldots, \omega_q'$ представляют собой конъюнкцию некоторых предикатов из числа $\omega_1, \ldots, \omega_p$. Следовательно, обозначая через σ_2 предикат, полученный из предиката σ_1 после указанной подстановки переменных, с учетом эквивалентности (3.17) получим

$$\begin{aligned}\sigma_2 \equiv (x^1 = a_1) \vee \ldots \vee (x^m = a_m) \vee &\\ \vee (\exists X^{m+1}) \ldots (\exists X^{n-1})(\omega_1' \vee \ldots \vee \omega_q') \vee (x_1^n = x_2^n) &\equiv\\ \equiv (x^1 = a_1) \vee \ldots \vee (x^m = a_m) \vee (\exists X^{m+1}) \ldots (\exists X^{n-1})\omega_1' \vee \ldots &\\ \ldots \vee (\exists X^{m+1}) \ldots (\exists X^{n-1})\omega_q' \vee (x_1^n = x_2^n)&.\end{aligned}$$

Далее поступаем с формулами

$$(\exists X^{m+1}) \ldots (\exists X^{n-1})\omega_1', \qquad \ldots, \qquad (\exists X^{m+1}) \ldots (\exists X^{n-1})\omega_q' \tag{3.19}$$

и переменными группы X^{n-1} точно так же, как поступили выше с формулой

$$(\exists X^{m+1}) \ldots (\exists X^n)(\tau_1 \mathbin{\&} \ldots \mathbin{\&} \tau_p)$$

и переменными группы X^n. Отметим лишь одну особенность, которая отсутствовала выше. После выделения в каждом из предикатов (3.19) неполной диагонали от переменных типа $n-1$ мы будем вынуждены одновременно заменять переменные этих диагоналей переменными x_1^{n-1}, x_2^{n-1}. Возможность такой одновременной замены, при которой не возникают полные диагонали, вытекает из неполноты предиката σ_2, а именно из того, что существует такой набор $\widetilde{a}^{n-1}$ значений переменных $\widetilde{x}^{n-1}$ предиката σ_2, при подстановке которых вместо переменных $\widetilde{x}^{n-1}$ получается неполный $(n-1)$-основный предикат. Набор $\widetilde{a}^{n-1}$ состоит из элементов 0, 1. Они и определяют места для переменных x_1^{n-1}, x_2^{n-1}. В итоге мы придем к предикату ρ. Теорема доказана.

Пусть $a, b \in E_2$ и $\rho_{ab}(x^1, x^2)$ — двухосновный предикат, определяемый формулой

$$(x^1 = a) \,\&\, (x^2 = b) \vee (x^1 = \bar{a}) \,\&\, (x^2 = \bar{b}). \tag{3.20}$$

Очевидно, что существуют ровно два различных предиката ρ_{ab}: ρ_{00} и ρ_{01}. Несложно далее убедиться в том, что классу $\mathrm{Pol}(\rho_{00})$ принадлежат все такие вектор-функции $\bar{f}(x_1, \ldots, x_n)$ из P_2^2, что $\mathrm{pr}_1 \bar{f} = \mathrm{pr}_2 \bar{f}$, а классу $\mathrm{Pol}(\rho_{01})$ — все такие вектор-функции $\bar{g}(x_1, \ldots, x_n)$, что $\mathrm{pr}_1 \bar{g} = (\mathrm{pr}_2 \bar{g})^*$, где $(\mathrm{pr}_2 \bar{g})^*$ есть функция, двойственная к функции $\mathrm{pr}_2 \bar{g}$.

Л е м м а 3.7. *Двухосновный предикат ρ_{ab}, задаваемый формулой* (3.20), *является минимальным.*

Д о к а з а т е л ь с т в о. Из определения предиката ρ_{ab} следует, что он стандартен и не содержит фиктивных переменных. Поэтому при доказательстве минимальности предиката ρ_{ab} можно обойтись формулами, не содержащими диагоналей.

Пусть стандартный, отличный от диагонали и не содержащий фиктивных переменных предикат σ реализуется формулой над предикатом ρ_{ab}. Приводя эту формулу к предваренному виду, получим

$$\sigma \equiv (\exists X^1)(\exists X^2)(\rho_{ab}^1 \,\&\, \ldots \,\&\, \rho_{ab}^p), \tag{3.21}$$

где предикаты $\rho_{ab}^1, \ldots, \rho_{ab}^p$ получаются из предиката ρ_{ab} некоторыми подстановками переменных. Замечаем, что имеют место эквивалентности

$$(\exists x^2)(\rho_{ab}(x_{i_1}^1, x^2) \,\&\, \ldots \,\&\, \rho_{ab}(x_{i_s}^1, x^2)) \equiv (x_{i_1}^1 = \ldots = x_{i_s}^1),$$

$$(\exists x^1)(\rho_{ab}(x^1, x_{j_1}^2) \,\&\, \ldots \,\&\, \rho_{ab}(x^1, x_{j_t}^2)) \equiv (x_{j_1}^2 = \ldots = x_{j_t}^2).$$

Пользуясь этими эквивалентностями и алгоритмом элиминирования диагоналей, описанным в § 4 из гл. II, исключаем из формулы (3.21) все кванторы. Поскольку предикат σ стандартен, в полученной формуле будут отсутствовать диагонали. Без ограничения общности можно считать, что эта формула имеет вид $\rho_{ab}^1 \,\&\, \ldots \,\&\, \rho_{ab}^p$. Отождествляя в ней все переменные типа 1 и все переменные типа 2, получим, очевидно, предикат ρ_{ab}. Лемма доказана.

На основании доказанных утверждений опишем теперь все минимальные k-основные предикаты, а точнее, все минимальные классы k-основных предикатов.

Пусть $\rho(\widetilde{x})$ — минимальный булев предикат. С помощью лемм 3.4, 3.5 получаем из него k минимальных k-основных предикатов вида

$$\rho_i(x^1, \ldots, x^{i-1}, \widetilde{x}^i, x^{i+1}, \ldots, x^k) \equiv \rho(\widetilde{x}^i).$$

Тем самым определяются $5k$ минимальных классов. Отметим, что в случае, когда предикат ρ задает предполный класс L, соответствующий ему предикат ρ_i определяет класс $\mathrm{Pol}(\rho_i)$, совпадающий с введенным в § 2 классом Слупецкого V_i. Все $5k$ минимальных классов k-основных предикатов различны. Это вытекает, например, из того, что класс $\mathrm{Pol}(\rho_i)$ состоит в точности из всех вектор-функций $\bar{f}(x_1, \ldots$ $\ldots, x_n)$, для которых $\mathrm{pr}_i\, \bar{f} \in \mathrm{Pol}(\rho)$. Поэтому классы вида $\mathrm{Pol}(\rho_i)$ обозначают иногда как

$$P_2^{i-1} \times M \times P_2^{k-i}, \qquad P_2^{i-1} \times S \times P_2^{k-i}$$

и т. д.

Из каждого двухосновного предиката ρ_{ab} с помощью лемм 3.4, 3.5 и 3.7 получаем $k(k-1)/2$ минимальных k-основных предикатов вида

$$\rho_{ij}(x^1, \ldots, x^i, \ldots, x^j, \ldots, x^k) \equiv \rho_{ab}(x^i, x^j),$$

где $1 \leqslant i < j \leqslant k$. Следовательно, всего с помощью ρ_{ab} можно задать $k(k-1)$ минимальных классов k-основных предикатов. Нетрудно видеть, что все эти $k(k-1)$ минимальных классов различны и не совпадают с ранее определенными минимальными классами. Действительно, это вытекает, например, из того, что класс $\mathrm{Pol}(\rho_{ij})$ состоит в точности из всех функций $\bar{f}(x_1, \ldots, x_n)$ из P_2^k, у которых $\mathrm{pr}_i\, \bar{f} = \mathrm{pr}_j\, \bar{f}$ при $a = b$ и $\mathrm{pr}_i\, \bar{f} = (\mathrm{pr}_j\, \bar{f})^*$ при $a \neq b$.

Теорема 3.6 и леммы 3.4 и 3.5 дают еще

$$\sum_{n=2}^{k} \binom{k}{n} \cdot \sum_{m=0}^{n} \binom{n}{m} \cdot 2^m = \sum_{n=2}^{k} \binom{k}{n} \cdot 3^n = 4^k - 3k - 1$$

минимальных k-основных предикатов. Заметим, что если $s \geqslant 2$ и минимальный k-основный предикат $\rho_{i_1 \ldots i_s}$ имеет вид (выписаны лишь существенные переменные предиката $\rho_{i_1 \ldots i_s}$)

$$(x_1^{i_1} = x_2^{i_1}) \vee \ldots \vee (x_1^{i_s} = x_2^{i_s}),$$

то $\mathrm{Pol}(\rho_{i_1 \ldots i_s}) = V_{i_1 \ldots i_s}$, где $V_{i_1 \ldots i_s}$ — класс Слупецкого, введенный в § 2. Предикаты теоремы 3.6 задают $4^k - 3k - 1$ минимальных классов k-основных предикатов. Чтобы убедиться в этом, можно воспользоваться описанием классов $V_{i_1 \ldots i_s}$, данным в § 2. Кроме того, если k-основный предикат ρ имеет вид (с точностью до несущественных переменных)

$$(x^{i_1} = a_1) \vee \ldots \vee (x^{i_m} = a_m) \vee (x_1^{i_{m+1}} = x_2^{i_{m+1}}) \vee \ldots \vee (x_1^{i_r} = x_2^{i_r}), \quad (3.22)$$

где $a_1, \ldots, a_m \in E_2$, $m \geqslant 1$ и $r \geqslant 2$, то класс $\mathrm{Pol}(\rho)$, как можно проверить, состоит из вектор-функций $\bar{f}(x_1, \ldots, x_n)$ из P_2^k таких, что: либо для некоторого j, $1 \leqslant j \leqslant m$, функция $\mathrm{pr}_{i_j} \bar{f}$ совпадает с константой a_j; либо для некоторого j, $m+1 \leqslant j \leqslant r$, функция $\mathrm{pr}_{i_j} \bar{f}$ является константой или существует такое t, $1 \leqslant t \leqslant n$, что каждая из функций

$$\mathrm{pr}_{i_{m+1}} \bar{f}, \qquad \ldots, \qquad \mathrm{pr}_{i_r} \bar{f}$$

существенно зависит только от переменной x_t.

Теорема 3.7. *Для любого k, $k \geqslant 2$, имеется ровно $4^k + k^2 + k - 1$ минимальных классов k-основных предикатов. Они получаются с помощью лемм* 3.4, 3.5 *из одноосновных минимальных предикатов, двухосновных минимальных предикатов вида ρ_{ab} и многоосновных предикатов вида* (3.22).

Тот факт, что существует не менее $4^k + k^2 + k - 1$ минимальных классов k-основных предикатов, мы установили выше. Оставшаяся часть этой главы будет посвящена доказательству того, что других минимальных классов k-основных предикатов не существует.

§ 6. Редукция предикатов

Согласно теореме 3.2 всякий замкнутый класс вектор-функций из P_2^k, отличный от P_2^k, содержится в некотором предполном в P_2^k классе. Очевидно, что предполные классы включают все селекторные вектор-функции. Поэтому с использованием результатов § 4 получаем двойственное утверждение для предикатов: всякий замкнутый класс k-основных предикатов, включающий все диагонали и отличный от множества $\mathrm{Inv}(P_2^k)$, содержит хотя бы один минимальный класс k-основных предикатов.

Как отмечалось выше, минимальный класс предикатов порождается диагоналями и любым своим предикатом, отличным от диагонали. Таким образом, если ρ — произвольный k-основный предикат, отличный от диагонали, то найдется такой минимальный предикат σ, что σ можно реализовать подходящей формулой над множеством $\{\rho\} \cup \mathrm{Inv}(P_2^k)$. Если же предикат σ стандартен и не содержит фиктивных переменных, то в соответствующей формуле можно обойтись без диагоналей.

Из этих соображений вытекает план дальнейшего доказательства теоремы 3.7. Именно, мы покажем, как из произвольного k-основного предиката ρ, отличного от диагонали, с помощью подходящей формулы определить один из минимальных предикатов, введенных в § 5. Однако нам пока не известно, все ли минимальные классы указаны в теореме 3.7. Поэтому чтобы уменьшить перебор возможных вариантов, мы поступим следующим образом.

Пусть минимальный k-основный предикат $\rho(\widetilde{x}^1, \ldots, \widetilde{x}^k)$ определяет в P_2^k предполный класс $\mathrm{Pol}(\rho)$, отличный от класса Слупецкого. Это значит (см. § 2), что $\Omega \nsubseteq \mathrm{Pol}(\rho)$. Обозначим через γ_1 1-график множества $\mathrm{Pol}(\rho)$. Из соотношения $\Omega \nsubseteq \mathrm{Pol}(\rho)$ следует, что γ_1 отличен от 1-графика множества P_2^k, т. е. γ_1 является неполным предикатом. Поскольку γ_1 — одноместный предикат, он будет отличен также и от диагонали. Следовательно, $\mathrm{Pol}(\gamma_1)$ представляет собой замкнутый класс вектор-функций из P_2^k, отличный от P_2^k. По определению вектор-функции из $\mathrm{Pol}(\rho)$ сохраняют предикат γ_1. Значит, $\mathrm{Pol}(\rho) \subseteq \mathrm{Pol}(\gamma_1)$, и в силу предполноты класса $\mathrm{Pol}(\rho)$ получаем

$$\mathrm{Pol}(\rho) = \mathrm{Pol}(\gamma_1).$$

Таким образом, мы приходим к следующему выводу: всякий предполный в P_2^k класс, отличный от класса Слупецкого, есть класс сохранения своего 1-графика. В частности, можно считать, что отличные от классов Слупецкого предполные классы $\mathrm{Pol}(\rho)$ определяются такими k-основными минимальными предикатами $\rho(\widetilde{x}^1, \ldots, \widetilde{x}^k)$, у которых каждая из групп переменных $\widetilde{x}^1, \ldots, \widetilde{x}^k$ состоит не более чем из двух переменных. А это в свою очередь означает, что для завершения доказательства теоремы 3.7 достаточно исследовать на минимальность лишь предикаты $\rho(\widetilde{x}^1, \ldots, \widetilde{x}^k)$ с указанными ограничениями на количество переменных в группах $\widetilde{x}^1, \ldots, \widetilde{x}^k$.

Мы покажем, что каждый из таких предикатов ρ либо приводится некоторой формулой к одному из минимальных предикатов, описанных в § 5, либо к отличному от диагонали l-основному предикату σ, где $l < k$. Во втором случае можно также считать, что l-основный предикат σ задает k-основный предикат, у которого существенными являются лишь переменные l типов. К l-основному предикату σ применимы те же соображения, что и к k-основному предикату ρ: либо из предиката σ с помощью некоторой формулы можно получить один из минимальных предикатов, описанных в § 5, либо предикат σ имеет не более двух переменных любого типа. Тогда к предикату σ мы применим излагаемую ниже процедуру, которая позволит получить из него либо минимальный предикат из § 5, либо отличный от диагонали l'-основный предикат σ', где $l' < l$. В итоге будет получен один из минимальных предикатов из § 5. Затем применим лемму 3.4.

На первом этапе реализации этого плана мы хотим еще более сузить область изменения предикатов ρ, оставляя для дальнейшего исследования вполне рефлексивные предикаты, из которых операцией проектирования по любой переменной можно получить лишь полные предикаты.

Предикат $\rho(\widetilde{x}^1, \ldots, \widetilde{x}^k)$ назовем *вполне рефлексивным*, если при любом непустом отождествлении переменных (одного и того же типа) он обращается в полный предикат.

Итак, пусть $\rho(x^1, \ldots, x^m, x_1^{m+1}, x_2^{m+1}, \ldots, x_1^k, x_2^k)$ — отличный от диагонали k-основный предикат, $0 \leqslant m \leqslant k$. Рассмотрим предикаты вида

$$(\exists x^i)\rho(x^1, \ldots, x^m, x_1^{m+1}, x_2^{m+1}, \ldots, x_1^k, x_2^k), \quad 1 \leqslant i \leqslant m, \tag{3.23}$$

$$(\exists x_j^i)\rho(x^1, \ldots, x^m, x_1^{m+1}, x_2^{m+1}, \ldots, x_1^k, x_2^k), \quad m+1 \leqslant i \leqslant k, \quad 1 \leqslant j \leqslant 2. \tag{3.24}$$

Если предикат (3.23) отличен от диагонали, то, следовательно, формула (3.23) сводит k-основный предикат ρ к отличному от диагонали $(k-1)$-основному предикату. Если же отличен от диагонали предикат (3.24), то мы получаем отличный от диагонали k-основный предикат, который по сравнению с предикатом ρ имеет на одну переменную меньше. В силу этих соображений далее будем предполагать, что предикаты вида (3.23) и (3.24) суть диагонали.

Допустим, что предикат (3.23) является неполной диагональю D,

$$D \equiv (x_1^{i_1} = x_2^{i_1}) \,\&\, \ldots \,\&\, (x_1^{i_s} = x_2^{i_s}) \tag{3.25}$$

(в диагонали D указаны лишь существенные переменные). И пусть предикат $\Delta\rho$ получается из предиката ρ отождествлением пар переменных $x_1^{i_1}, x_2^{i_1}, \ldots, x_1^{i_s}, x_2^{i_s}$. Очевидно, что предикат $\Delta\rho$ либо полный, либо отличен от диагонали. Если он полон, то, с одной стороны, предикат ρ есть расширение диагонали D (рассматриваемой от всех переменных предиката ρ), а с другой стороны, проекция предиката ρ по переменной x^i совпадает с диагональю D. Значит, предикат ρ совпадает (с точностью до несущественных переменных) с диагональю D, что невозможно по условию.

Если же предикат $\Delta\rho$ отличен от диагонали, то, следовательно, отождествлением переменных предикат ρ редуцируется к отличному от диагонали предикату, имеющему меньшее число переменных, чем предикат ρ.

К аналогичным выводам мы придем, если предположим, что неполной диагональю является предикат (3.24). Таким образом, далее можно считать, что все предикаты вида (3.23), (3.24) являются полными.

Выберем какое-либо i, $m+1 \leqslant i \leqslant k$, и рассмотрим предикат

$$\rho(x^1, \ldots, x^m, x_1^{m+1}, \ldots, x_2^{i-1}, x_1^i, x_1^i, x_1^{i+1}, \ldots, x_2^k),$$

который обозначим через $\Delta\rho$. Как и выше, можно предполагать, что предикат $\Delta\rho$ является диагональю. Предположим далее, что $\Delta\rho$ есть неполная диагональ (3.25). Как отмечалось в § 1 из гл. II, операции отождествления переменных и проектирования перестановочны. Если переменная x предиката ρ не является существенной для диагонали D (т. е. если $x \notin \{x_1^{i_1}, x_2^{i_1}, \ldots, x_1^{i_s}, x_2^{i_s}\}$) и отлична от переменной x_1^i, то, с одной стороны,

$$(\exists x)\Delta\rho \equiv (\exists x)D \equiv D,$$

а с другой стороны, отождествление переменных x_1^i, x_2^i в полном предикате $(\exists x)\rho$ дает, разумеется, полный предикат. Приходим к противоречию: неполная диагональ D совпадает с полным предикатом.

Выбор переменной x с указанными свойствами невозможен только в одном случае: когда $s = k-1$ (и, следовательно, $m = 0$). Если $k \geqslant 3$, то описанный выше прием вновь дает противоречие:

$$(\exists x_1^{i_1})\Delta\rho \equiv (\exists x_1^{i_1})D \equiv (x_1^{i_2} = x_2^{i_2}) \,\&\, \ldots \,\&\, (x_1^{i_s} = x_2^{i_s}),$$

и вместе с тем отождествление переменных x_1^i, x_2^i в полном предикате $(\exists x_1^{i_1})\rho$ дает полный предикат (напомним, что $s = k-1 \geqslant 2$).

Остается рассмотреть случай, когда $k=2$ и $s=1$. Пусть для определенности $i=2$. Согласно предположению предикат $(\exists x_2^2)\rho(x_1^1, x_2^1, x_1^2, x_2^2)$ полон. Это означает, что для любых элементов a_1, a_2, b_1 из E_2 найдется такой элемент b_2 из E_2, что значение $\rho(a_1, a_2, b_1, b_2)$ истинно. Из эквивалентности

$$\rho(x_1^1, x_2^1, x_1^2, x_1^2) \equiv (x_1^1 = x_2^1) \tag{3.26}$$

следует, что при $a_1 \neq a_2$ должно быть также $b_1 \neq b_2$. Значит, предикату ρ удовлетворяют все наборы вида $(a, \bar a, b, \bar b)$, где $a, b \in E_2$. В силу (3.26) ему также удовлетворяют все наборы вида (a, a, b, b). Далее рассмотрим две возможности.

Пусть предикату ρ не удовлетворяет хотя бы один набор вида $(a, a, b, \bar b)$. Полагая тогда

$$\rho_1(x_1^1, x_2^1, x_1^2, x_2^2) \equiv \rho(x_1^1, x_2^1, x_1^2, x_2^2) \,\&\, \rho(x_1^1, x_2^1, x_2^2, x_1^2),$$

убеждаемся в том, что предикату ρ_1 удовлетворяют лишь наборы вида $(a, \bar a, b, \bar b)$ и (a, a, b, b), т. е.

$$\rho_1(x_1^1, x_2^1, x_1^2, x_2^2) \equiv (x_1^1 = x_2^1) \,\&\, (x_1^2 = x_2^2) \vee (x_1^1 \neq x_2^1) \,\&\, (x_1^2 \neq x_2^2).$$

Имеем теперь

$$(\exists x_1^2)(\exists x_2^2)(\rho_1(x_1^1, x_2^1, x_1^2, x_2^2) \mathbin{\&} \rho_1(x_3^1, x_4^1, x_1^2, x_2^2)) \equiv$$
$$\equiv (x_1^1 = x_2^1) \mathbin{\&} (x_3^1 = x_4^1) \vee (x_1^1 \neq x_2^1) \mathbin{\&} (x_3^1 \neq x_4^1) \equiv$$
$$\equiv (x_1^1 + x_2^1 = x_3^1 + x_4^1).$$

Следовательно, в этом случае предикат ρ редуцирован к одноосновному предикату, отличному от диагонали (на самом деле этот одноосновный предикат определяет в P_2 класс L).

Пусть предикату ρ удовлетворяют все наборы вида $(a, a, b, \bar{b})$. Тогда

$$\rho(x_1^1, x_2^1, x_1^2, x_2^2) \equiv (x_1^1 = x_2^1) \vee (x_1^2 \neq x_2^2).$$

Полагая

$$\rho_1(x_1^1, x_2^1, x_1^2, x_2^2) \equiv (\exists x_3^2)(\rho(x_1^1, x_2^1, x_1^2, x_3^2) \mathbin{\&} \rho(x_1^1, x_2^1, x_2^2, x_3^2)),$$

будем иметь

$$\rho_1(x_1^1, x_2^1, x_1^2, x_2^2) \equiv (x_1^1 = x_2^1) \vee (x_1^2 = x_2^2).$$

Следовательно, в этом случае предикат ρ редуцирован к минимальному двухосновному предикату теоремы 3.6.

Итак, далее можно предполагать, что все предикаты $\Delta\rho$, полученные из предиката ρ непустым отождествлением переменных, являются полными. Отсюда вытекает, что ρ — вполне рефлексивный предикат. В частности, ρ есть расширение предиката

$$(x_1^{m+1} = x_2^{m+1}) \vee \ldots \vee (x_1^k = x_2^k)$$

(указаны лишь существенные переменные).

Пусть $m = 0$. Положим

$$\rho_2(x_1^1, x_2^1, \ldots, x_1^k, x_2^k) \equiv \mathop{\&}_{(\pi_1, \ldots, \pi_k)} \rho(x_{\pi_1(1)}^1, x_{\pi_1(2)}^1, \ldots, x_{\pi_k(1)}^k, x_{\pi_k(2)}^k),$$

где конъюнкция берется по всем наборам $(\pi_1, \ldots, \pi_k)$ перестановок на множестве $\{1, 2\}$. Очевидно, что предикат ρ_2 неполон, является расширением предиката

$$(x_1^1 = x_2^1) \vee \ldots \vee (x_1^k = x_2^k) \tag{3.27}$$

и симметричен по каждой паре переменных $x_1^1, x_2^1, \ldots, x_1^k, x_2^k$. Следовательно, предикат ρ_2 совпадает с предикатом (3.27), который определяет в P_2^k класс Слупецкого $V_{1\ldots k}$.

Далее считаем, что $m > 0$. Предположим, что для любого a из E_2 $(k-1)$-основный предикат

$$\rho(a, x^2, \ldots, x^m, x_1^{m+1}, x_2^{m+1}, \ldots, x_1^k, x_2^k)$$

неполон. Тогда для любого a из E_2 в последовательности из 2^{2k-m-1} различных наборов

$$(a, a^2, \ldots, a^m, a_1^{m+1}, a_2^{m+1}, \ldots, a_1^k, a_2^k), \quad \ldots \\ \ldots, \quad (a, c^2, \ldots, c^m, c_1^{m+1}, c_2^{m+1}, \ldots, c_1^k, c_2^k)$$

найдется хотя бы один, который не удовлетворяет предикату ρ. Значит, если

$$(y^2, \ldots, y^m, y_1^{m+1}, y_2^{m+1}, \ldots, y_1^k, y_2^k), \quad \ldots \\ \ldots, \quad (v^2, \ldots, v^m, v_1^{m+1}, v_2^{m+1}, \ldots, v_1^k, v_2^k) \qquad (3.28)$$

— последовательность из 2^{2k-m-1} различных наборов переменных, то $(k-1)$-основный предикат

$$(\exists x^1)(\rho(x^1, y^2, \ldots, y^m, y_1^{m+1}, \ldots, y_2^k) \,\&\ldots\&\, \rho(x^1, v^2, \ldots, v^m, v_1^{m+1}, \ldots, v_2^k)) \qquad (3.29)$$

неполон. Вместе с тем по предположению предикат

$$(\exists x^1)\rho(x^1, x^2, \ldots, x^m, x_1^{m+1}, \ldots, x_2^k)$$

полон. Следовательно, существует такое наименьшее число s, $s \geqslant 2$, что будет неполным предикат (3.29), построенный для последовательности (3.28), состоящей из s наборов. Обозначим этот предикат через ρ^s и покажем, что либо ρ^s отличен от диагонали, либо предикат ρ совпадает с минимальным предикатом ρ_{ab} из § 5.

В самом деле, предикат ρ вполне рефлексивен. Поэтому отождествление переменных y_1^i, y_2^i, $m+1 \leqslant i \leqslant k$, в предикате ρ^s равносильно с точностью до несущественных переменных вычеркиванию в формуле (3.29) сомножителя $\rho(x^1, y^2, \ldots, y^m, y_1^{m+1}, \ldots, y_2^k)$. А это в свою очередь означает, что указанное отождествление переменных приводит к предикату ρ^{s-1}, построенному по формуле (3.29) для последовательности (3.28), состоящей из $s-1$ наборов. По выбору числа s предикат ρ^{s-1} полон. Следовательно, предикат ρ^s есть расширение диагонали $y_1^i = y_2^i$. Аналогичное утверждение справедливо для других пар переменных типа i, входящих в наборы (3.28). Таким образом, предикат ρ^s является расширением предиката

$$(y_1^{m+1} = y_2^{m+1}) \vee \ldots \vee (y_1^k = y_2^k) \vee \ldots \vee (v_1^{m+1} = v_2^{m+1}) \vee \ldots \vee (v_1^k = v_2^k).$$

Поскольку $s \geqslant 2$, отсюда следует, что при $m < k$ предикат ρ^s отличен от диагонали.

Пусть $m = k$. Предположим, что предикат ρ^s является диагональю, в которую, например, конъюнктивно входит сомножитель $y^i = v^i$, $2 \leqslant i \leqslant k$. Если $k \geqslant 3$, то пусть $2 \leqslant j \leqslant k$, $j \neq i$ и ρ_1 обозначает предикат, полученный из предиката ρ^s проектированием по всем s переменным типа j. Из того, что ρ^s — диагональ с конъюнктивным сомножителем $y^i = v^i$, $i \neq j$, следует, что ρ_1 также будет диагональю с конъюнктивным сомножителем $y^i = v^i$. С другой стороны, предикат ρ_1 можно представить в виде

$$
\begin{aligned}
&(\exists x^1)(\exists y^j)\ldots(\exists v^j)(\rho(x^1, y^2, \ldots, y^j, \ldots, y^k)\,\&\ldots \\
&\qquad\qquad\ldots\&\,\rho(x^1, v^2, \ldots, v^j, \ldots, v^k)) \equiv \\
&\equiv (\exists x^1)((\exists y^j)\rho(x^1, y^2, \ldots, y^j, \ldots, y^k)\,\&\ldots\&\,(\exists v^j)\rho(x^1, v^2, \ldots, v^j, \ldots, v^k)).
\end{aligned}
$$

Пользуясь тем, что все предикаты вида (3.23) являются полными, приходим к выводу, что полным будет и предикат ρ_1. Следовательно, этот случай невозможен.

Пусть $k = 2$. Тогда $i = 2$. Если $s \geqslant 3$, то вновь приходим к противоречию. В самом деле, если переменная z^2 из последовательности (3.28) отлична от y^2 и v^2, то отождествление переменных z^2 и v^2 равносильно вычеркиванию из последовательности (3.28) одного набора. Поэтому предикат ρ^s в соответствии с выбором числа s после отождествления переменных должен обратиться в полный предикат. С другой стороны, это отождествление переменных в диагональном предикате ρ^s не касается конъюнктивного сомножителя $y^2 = v^2$ и, значит, дает после отождествления переменных в предикате ρ^s неполную диагональ.

Остается рассмотреть возможность, когда $k = s = 2$. Как показывает непосредственная проверка, из того, что $(\exists x^1)\rho(x^1, x^2)$, $(\exists x^2)\rho(x^1, x^2)$ — полные предикаты и

$$(\exists x^1)(\rho(x^1, y^2)\,\&\,\rho(x^1, v^2)) \equiv (y^2 = v^2),$$

следует, что $\rho(x^1, x^2)$ совпадает с минимальным предикатом вида ρ_{ab}, определенным в § 5.

По доказанному можно считать, что для любого i, $1 \leqslant i \leqslant m$, найдется такое a_i из E_2, что $(k-1)$-основный предикат

$$\rho(x^1, \ldots, x^{i-1}, a_i, x^{i+1}, \ldots, x^m, x_1^{m+1}, x_2^{m+1}, \ldots, x_1^k, x_2^k)$$

полон. Другими словами, это означает, что предикат ρ есть расширение предиката
$$(x^1 = a_1) \vee \ldots \vee (x^m = a_m).$$

Вместе с тем в силу полной рефлексивности предикат ρ является также расширением предиката
$$(x_1^{m+1} = x_2^{m+1}) \vee \ldots \vee (x_1^k = x_2^k).$$

Сопоставляя эти два факта, приходим к выводу, что предикат ρ есть расширение предиката
$$(x^1 = a_1) \vee \ldots \vee (x^m = a_m) \vee (x_1^{m+1} = x_2^{m+1}) \vee \ldots \vee (x_1^k = x_2^k). \quad (3.30)$$

Положим
$$\rho_3(x^1, \ldots, x^m, x_1^{m+1}, x_2^{m+1}, \ldots, x_1^k, x_2^k) \equiv$$
$$\equiv \mathop{\&}_{\pi_{m+1}, \ldots, \pi_k} \rho(x^1, \ldots, x^m, x^{m+1}_{\pi_{m+1}(1)}, x^{m+1}_{\pi_{m+1}(2)}, \ldots, x^k_{\pi_k(1)}, x^k_{\pi_k(2)}),$$

где конъюнкция берется по всем наборам перестановок $(\pi_{m+1}, \ldots, \pi_k)$ на множестве $\{1, 2\}$. Из неполноты предиката ρ легко следует, что предикат ρ_3 совпадает с предикатом (3.30). Это завершает доказательство теоремы 3.7.

Комментарии. Проблема полноты для замкнутых классов вектор-функций рассматривалась Б. А. Ромовым [24, 25]. Описание всех замкнутых классов вектор-функций из P_2^k, $k \geqslant 2$, получено В. А. Таймановым [29]. Им, в частности, найдены все классы Слупецкого в P_2^k. Альтернативное описание получено Б. А. Ромовым [26, 27] (см. также [13]). Перенесение теории Галуа с алгебр Поста на прямые произведения алгебр Поста выполнено Б. А. Ромовым [25], которому принадлежит описание всех минимальных k-основных предикатов [26, 27] (см. также [14]).

Глава IV

СИЛЬНЫЕ ОПЕРАТОРЫ ЗАМЫКАНИЯ

В этой главе будут рассмотрены операторы замыкания, включающие операцию суперпозиции в качестве одной из порождающих или производных операций. Особенностью этих операторов замыкания является то, что соответствующие им решетки замкнутых классов оказываются конечными.

§ 1. Параметрическое замыкание

Мы начнем с определения языка Par параметрической выразимости. Исходными символами языка Par являются символы переменных $x_1, x_2, \ldots$, символы $f_i^{(n)}$ для обозначения всех n-местных булевых функций ($1 \leqslant i \leqslant 2^{2^n}$, $n = 1, 2, \ldots$), знак равенства $=$, логическая связка конъюнкция &, квантор существования $\exists$, левая и правая скобки и запятая. Обычным образом определяется понятие *терма* в языке Par: любой символ переменной языка Par есть терм; если $t_1, \ldots, t_n$ — термы языка Par, а $f_i^{(n)}$ — символ n-местной функции, то $f_i^{(n)}(t_1, \ldots, t_n)$ есть терм. Никаких других термов в языке Par нет.

Если t_1, t_2 — термы языка Par, то выражение $(t_1 = t_2)$ называется *элементарной формулой языка* Par. Из элементарных формул по известным логическим правилам определяются остальные формулы языка Par. Именно, если Φ_1, Φ_2 — формулы языка Par, а x_i — символ переменной, то $(\Phi_1 \,\&\, \Phi_2)$ и $(\exists x_i)\Phi_1$ суть формулы языка Par. Понятия свободной и связанной переменных мы предполагаем известными.

Для удобства изложения наряду с исходными обозначениями будут использоваться также обозначения вида $x, y, z, f^{(n)}, g^{(n)}$, возможно, с нижними индексами. Если число переменных у функции определяется из контекста, то верхний индекс, указывающий на число переменных, будем опускать. Будем также опускать скобки в формулах, когда это не приводит к недоразумению.

Всякая формула языка Par с m свободными переменными очевидным образом определяет m-местное отношение (предикат) на множестве E_2. Пусть $Q \subseteq P_2$, $\Phi(x_1,\ldots,x_m)$ — формула языка Par со свободными переменными $x_1,\ldots,x_m$, все функциональные символы которой суть обозначения функций из Q, и формула $\Phi(x_1,\ldots,x_m)$ определяет отношение $\rho(x_1,\ldots,x_m)$ на множестве E_2. В этом случае говорим, что формула $\Phi(x_1,\ldots,x_m)$ *параметрически выражает отношение* $\rho(x_1,\ldots,x_m)$ через функции множества Q. Отношение ρ называем *параметрически выразимым* через функции множества Q, если существует формула языка Par, которая параметрически выражает отношение ρ через функции множества Q.

Понятие параметрической выразимости перенесем с отношений на функции. Именно, если $f(x_1,\ldots,x_m)$ — булева функция, а формула $\Phi(x_1,\ldots,x_m,y)$ языка Par параметрически выражает отношение $y = f(x_1,\ldots,x_m)$ через функции множества Q, то говорим, что формула Φ *параметрически выражает функцию* f через функции множества Q. Совокупность всех функций, параметрически выразимых через функции множества Q, назовем *параметрическим замыканием* множества Q и обозначим через $\mathrm{Par}[Q]$. Множество Q называется *параметрически замкнутым*, если $\mathrm{Par}[Q] = Q$. Параметрически замкнутые множества называем также параметрически замкнутыми классами.

Отметим несколько свойств параметрического замыкания и параметрически замкнутых классов.

1. *Для любого множества Q булевых функций имеют место соотношения*

$$Q \subseteq \mathrm{Par}[Q], \qquad \mathrm{Par}[\mathrm{Par}[Q]] = \mathrm{Par}[Q].$$

В самом деле, если f — символ n-местной функции из Q, то формула

$$y = f(x_1,\ldots,x_n) \tag{4.1}$$

параметрически выражает функцию f через функции множества Q. Следовательно, $f \in \mathrm{Par}[Q]$.

Для доказательства второго соотношения достаточно заметить, что формулу Φ языка Par, выражающую некоторую функцию через функции множества $\mathrm{Par}[Q]$, можно превратить в формулу языка Par, выражающую ту же функцию через функции множества Q, если в формуле Φ каждое отношение вида (4.1), где $f \in \mathrm{Par}[Q]$, заменить соответствующей формулой языка Par, которая выражает это отношение через функции множества Q.

2. *Пересечение двух параметрически замкнутых класса есть параметрически замкнутый класс*; *если $Q_1 \subseteq Q_2$, то* $\mathrm{Par}[Q_1] \subseteq \mathrm{Par}[Q_2]$.

Это свойство есть очевидное следствие определения параметрического замыкания и обычных свойств операции пересечения и отношения включения.

3. *Любой параметрически замкнутый класс булевых функций содержит класс* U_{01}.

В самом деле, если $e_i^n(x_1,\ldots,x_n)$ — селекторная функция, то отношение $y = e_i^n(x_1,\ldots,x_n)$ параметрически выразимо формулой

$$(y = x_i)\mathbin{\&}\Bigl(\mathop{\&}_{1\leqslant j\leqslant n}(x_j = x_j)\Bigr). \tag{4.2}$$

(Сомножители $x_j = x_j$ добавлены в формулу (4.2) только для того, чтобы обозначить зависимость функции $e_i^n(x_1,\ldots,x_n)$ от всех переменных $x_1,\ldots,x_n$.) Заметим еще, что в формуле (4.2) отсутствуют символы булевых функций. Поэтому, например, $U_{01} \subseteq \mathrm{Par}[\varnothing]$.

4. *Любой параметрически замкнутый класс булевых функций замкнут относительно операции суперпозиции.*

Пусть функции $g_0, g_1, \ldots, g_m$ принадлежат параметрически замкнутому классу Q и

$$f(x_1,\ldots,x_n) = g_0(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n)).$$

Обозначим через

$$\Phi_0(x_1,\ldots,x_m,y),\qquad \Phi_1(x_1,\ldots,x_n,y),\qquad \ldots,\qquad \Phi_m(x_1,\ldots,x_n,y)$$

формулы языка Par, которые параметрически выражают отношения

$$y = g_0(x_1,\ldots,x_m),\qquad y = g_1(x_1,\ldots,x_n),\qquad \ldots,\qquad y = g_m(x_1,\ldots,x_n)$$

через функции множества Q. Тогда формула

$$(\exists y_1)\ldots(\exists y_m)(\Phi_1(x_1,\ldots,x_n,y_1)\mathbin{\&}\ldots$$
$$\ldots\mathbin{\&}\Phi_m(x_1,\ldots,x_n,y_m)\mathbin{\&}\Phi_0(y_1,\ldots,y_m,z))$$

языка Par параметрически выражает отношение

$$z = f(x_1,\ldots,x_n)$$

через функции множества Q. Таким образом, $f \in Q$.

5. *Если формула Φ языка Par параметрически выражает функцию $f(x_1,\ldots,x_n)$ через функции $\{g_1,\ldots,g_k\}$, то формула Φ^*, полученная из формулы Φ заменой всех символов функций $g_1,\ldots,g_k$ соответственно символами двойственных функций $g_1^*,\ldots,g_k^*$, параметрически выражает функцию f^* через функции $\{g_1^*,\ldots,g_k^*\}$* (принцип двойственности для параметрической выразимости).

В самом деле, замечаем, что отношение

$$y = g_i^*(x_1, \ldots, x_m)$$

получается из отношения

$$y = g_i(x_1, \ldots, x_m)$$

постановкой отрицания над всеми переменными:

$$(y = g_i^*(x_1, \ldots, x_m)) \equiv (\bar{y} = g_i(\bar{x}_1, \ldots, \bar{x}_m)).$$

Далее индукцией по построению формулы Φ доказываем, что если подформула Φ_1 формулы Φ определяет отношение $\rho(z_1, \ldots, z_p)$, то соответствующая подформула Φ_1^* формулы Φ^* будет определять отношение $\rho(\bar{z}_1, \ldots, \bar{z}_p)$. Базис индукции установлен выше. Переход от подформул Φ_1, Φ_2 к подформуле $\Phi_1 \mathbin{\&} \Phi_2$ не вызывает затруднений. При рассмотрении подформул вида $(\exists z_1)\Phi_1$ пользуемся очевидной эквивалентностью

$$(\exists z_1)\rho(z_1, \bar{z}_2, \ldots, \bar{z}_p) \equiv (\exists z_1)\rho(\bar{z}_1, \bar{z}_2, \ldots, \bar{z}_p).$$

Таким образом, формула Φ^* определяет отношение

$$\bar{y} = f(\bar{x}_1, \ldots, \bar{x}_n),$$

т. е. отношение

$$y = f^*(x_1, \ldots, x_n).$$

Из свойств 3 и 4 следует, что множество всех параметрически замкнутых классов булевых функций образует подмножество множества всех замкнутых (только относительно операции суперпозиции) классов булевых функций, содержащих класс U_{01}. Ниже мы устанавливаем, какие именно замкнутые классы булевых функций являются параметрически замкнутыми.

Л е м м а 4.1. $T_{01} \subseteq \mathrm{Par}[MO_0^\infty]$.

Д о к а з а т е л ь с т в о. Согласно лемме 1.20 функции $xy, x \vee y\bar{z}$ образуют базис класса T_{01}. Отношения $w = xy$ и $w = x \vee y\bar{z}$ параметрически выразимы через функции $x \vee y, x \vee yz$ класса MO_0^∞:

$$(w = xy) \equiv (w \vee x = x) \mathbin{\&} (w \vee y = y) \mathbin{\&} (w \vee xy = w),$$

$$(w = x \vee y\bar{z}) \equiv$$
$$\equiv (wx = x) \mathbin{\&} (w \vee y = x \vee y) \mathbin{\&} (w \vee z = x \vee y \vee z) \mathbin{\&} (wz = xz).$$

Таким образом,

$$\{xy, x \vee y\bar{z}\} \subset \mathrm{Par}[x \vee yz],$$

и, следовательно, $T_{01} \subseteq \mathrm{Par}[MO_0^\infty]$. Лемма доказана.

Лемма 4.2. $S_{01} \subseteq \mathrm{Par}[SM]$.

Доказательство. Согласно лемме 1.19, функция

$$d_3(\bar{x}, y, z) = \bar{x}y \vee \bar{x}z \vee yz$$

образует базис класса S_{01}. Положим

$$g(x, y, z, w) = x(y \vee z \vee w) \vee yzw.$$

Тогда $g \in SM$ и отношение $w = d_3(\bar{x}, y, z)$ параметрически выразимо через функции $d_3(x, y, z)$ и $g(x, y, z, w)$ из класса SM:

$$(w = d_3(\bar{x}, y, z)) \equiv (y = d_3(x, y, w))\,\&\,(z = d_3(x, z, w))\,\&\,(w = g(w, x, y, z)).$$

Лемма доказана.

Лемма 4.3. *Класс T_0 параметрически замкнут.*

Доказательство. Пусть функция f параметрически выразима через функции $f_1, \ldots, f_k$ из класса T_0 с помощью формулы Φ. Если всем свободным переменным формулы Φ придать значение 0, то, учитывая включение $\{f_1, \ldots, f_k\} \subset T_0$, придем к выводу, что значение формулы Φ будет истинным, поскольку в качестве общего значения всех связанных переменных формулы Φ также можно взять 0. Отсюда следует, что $f \in T_0$. Лемма доказана.

Лемма 4.4. *Класс S параметрически замкнут.*

Доказательство следует из принципа двойственности для параметрической выразимости (свойство 5).

Лемма 4.5. *Класс D параметрически замкнут.*

Доказательство. Предположим, напротив, что класс D не является параметрически замкнутым. Поскольку класс D непосредственно содержится только в классе M (см. диаграмму включений замкнутых классов в гл. I) и параметрически замкнутые классы замкнуты также относительно операции суперпозиции, будет иметь место включение $M \subseteq \mathrm{Par}[D]$. Формула

$$(yx = 0)\ \&\ (y \vee x = 1)$$

параметрически выражает отношение $y = \bar{x}$ через функции класса M. Следовательно, в этом случае существует формула $\Phi(x, y)$, которая параметрически выражает функцию $\bar{x}$ через функции класса D.

Пользуясь тождествами $0 \vee z = z$ и $1 \vee z = 1$, исключим из формулы Φ вхождения констант 0 и 1, стоящих под знаком дизъюнкции. Далее, формула

$$z_1 \vee \ldots \vee z_p = 0 \tag{4.3}$$

эквивалентна формуле

$$(z_1 = 0) \,\&\, \ldots \,\&\, (z_p = 0). \tag{4.4}$$

Заменим в формуле Φ всякую элементарную подформулу вида (4.3) соответствующей формулой (4.4). Полученную после этих преобразований формулу обозначим через $\Phi_1(x, y)$. Очевидно, что формула $\Phi_1(x, y)$ также параметрически выражает функцию $\bar{x}$ через функции класса D.

Пусть $v_1, \ldots, v_r$ — все связанные переменные формулы $\Phi_1(x, y)$. Из формулы $\Phi_1(x, y)$ можно исключить все формулы вида $v_i = 0$ или $v_i = 1$ (а также соответствующие кванторы $\exists v_i$), заменив все остальные вхождения переменной v_i константой 0 или 1 (понятно, что в формулу $\Phi_1(x, y)$ не могут входить одновременно подформулы $v_i = 0$ и $v_i = 1$). Кроме того, в формулу $\Phi_1(x, y)$ не могут входить элементарные подформулы $x = 0$, $x = 1$, $y = 0$ и $y = 1$, поскольку в противном случае формула $\Phi_1(x, y)$ не может быть истинной соответственно при $x = 1$, $x = 0$, $y = 1$ или $y = 0$. Таким образом, исключая из формулы $\Phi_1(x, y)$ все подформулы вида $v_i = 0$ и $v_i = 1$ с последующим исключением, если необходимо, констант 0 и 1 из-под знаков дизъюнкции, мы придем к формуле $\Phi_2(x, y)$, которая параметрически выражает функцию $\bar{x}$ через функции класса D и которая содержит в качестве элементарных подформул лишь формулы вида

$$1 = 1, \qquad z_1 \vee \ldots \vee z_p = 1, \qquad z_1 \vee \ldots \vee z_p = w_1 \vee \ldots \vee w_q, \tag{4.5}$$

где $\{z_1, \ldots, z_p, w_1, \ldots, w_q\} \subseteq \{x, y, v_1, \ldots, v_r\}$. Очевидно, что формулам (4.5) удовлетворяют значения $z_1 = \ldots = z_p = w_1 = \ldots = w_q = 1$. Но тогда $\Phi_2(1, 1)$ истинно, что противоречит эквивалентности

$$\Phi_2(x, y) \equiv (y = \bar{x}).$$

Лемма доказана.

Лемма 4.6. *Класс L параметрически замкнут.*

Доказательство. Пусть формула $\Phi(x_1, \ldots, x_n, y)$ параметрически выражает функцию $f(x_1, \ldots, x_n)$ через функции класса L.

Предположим сначала, что формула Φ не содержит кванторов, т. е. представляет собой конъюнкцию формул вида

$$g_1(z_1, \ldots, z_p) = g_2(w_1, \ldots, w_q), \tag{4.6}$$

где $\{z_1, \ldots, z_p, w_1, \ldots, w_q\} \subseteq \{x_1, \ldots, x_n, y\}$ и $g_1, g_2 \in L$. Перенося в формуле (4.6) слагаемые из правой части в левую часть и проводя, если необходимо, сокращения, получим эквивалентную формулу вида

$$g(z_1, \ldots, z_r) = 0, \tag{4.7}$$

где $\{z_1, \ldots, z_r\} \subseteq \{x_1, \ldots, x_n, y\}$ и g — линейная функция. Можно считать, что функция g не равна тождественно нулю. Если функция $g(z_1, \ldots, z_r)$ не зависит существенно от переменной y, то мы имеем в формуле Φ нетождественное линейное соотношение между независимыми переменными $x_1, \ldots, x_n$, что невозможно. Таким образом, далее можно предполагать, что в формуле (4.7) функция $g(z_1, \ldots, z_r)$ существенно зависит от переменной y. В силу этого формулу (4.7) можно переписать в эквивалентном виде

$$y = h(x_1, \ldots, x_n), \tag{4.8}$$

где h — линейная функция. Если из формулы Φ указанным выше способом можно получить формулу вида (4.8) с другой функцией h, то мы вновь приходим к нетождественному линейному соотношению между переменными $x_1, \ldots, x_n$. Значит, остается одна возможность, когда все подформулы вида (4.8) имеют одну и ту же функцию h. В этом случае, очевидно, функция $f(x_1, \ldots, x_n)$, параметрически выразимая формулой $\Phi(x_1, \ldots, x_n, y)$, совпадает с функцией $h(x_1, \ldots, x_n)$.

Допустим теперь, что формула Φ содержит кванторы $\exists$. Тогда элиминируем кванторы $\exists$ из формулы Φ тем же способом, как и в § 4 из гл. II. Именно, элементарные подформулы вида (4.6), содержащие связанную переменную z, преобразуем к эквивалентному виду

$$z = g_i(z_1^i, \ldots, z_{n_i}^i),$$

где g_i — линейная функция. А далее устраняем квантор $\exists z$ в соответствии со следующими эквивалентностями: при $m \geqslant 2$ формула

$$(\exists z)\left(\mathop{\&}_{1 \leqslant i \leqslant m} (z = g_i(z_1^i, \ldots, z_{n_i}^i))\right)$$

эквивалентна формуле

$$\mathop{\&}_{1 \leqslant i < j \leqslant m} (g_i(z_1^i, \ldots, z_{n_i}^i) + g_j(z_1^j, \ldots, z_{n_j}^j) = 0),$$

а при $m = 1$ тождественно истинна. Лемма доказана.

Лемма 4.7. *Класс U параметрически замкнут.*

Доказательство. Пусть формула $\Phi(x_1, \ldots, x_n, y)$ параметрически выражает функцию $f(x_1, \ldots, x_n)$ через функции класса U.

Предположим сначала, что формула Φ не содержит кванторов. Поскольку каждая функция класса U существенно зависит не более чем от одной переменной, формулу Φ можно представить в виде конъюнкции равенств, обе части которых суть элементы множества

$$\{0, 1, x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n, y, \bar{y}\}.$$

Очевидно, что формула Φ не может содержать противоречивых равенств. Она не может также содержать равенств вида

$$x_i = a, \qquad x_i^\sigma = x_j^\tau,$$

где $a, \sigma, \tau \in E_2$ и $i \neq j$, поскольку каждое из таких равенств налагает нетождественное условие на (независимые) переменные $x_1, \ldots, x_n$. Исключая далее из формулы Φ тождественно истинные равенства, приходим к выводу, что в формулу Φ обязана входить хотя бы одна из формул вида

$$y = a, \qquad y = x_i^\sigma,$$

где $a, \sigma \in E_2$. Понятно, что одновременное вхождение двух различных формул этого вида ведет к противоречию. Оставшаяся возможность показывает, что функция $f(x_1, \ldots, x_n)$ существенно зависит не более чем от одной переменной.

Пусть теперь формула Φ содержит кванторы. Поскольку все функции класса U являются линейными, можно применить процедуру элиминирования кванторов, описанную в лемме 4.6. При этом следует иметь в виду, что формулы вида

$$g_i(z_1^i, \ldots, z_{n_i}^i) + g_j(z_1^j, \ldots, z_{n_j}^j) = 0$$

редуцируются к формулам вида

$$z_p^i + z_q^j = a, \qquad z_p^i = a, \qquad z_q^j = a, \qquad 0 = 0,$$

где $a \in E_2$, $1 \leqslant p \leqslant n_i$, $1 \leqslant q \leqslant n_j$. Лемма доказана.

Теорема 4.1. *Существует ровно* 25 *параметрически замкнутых классов булевых функций:*

$$\begin{gathered} P_2,\ T_0,\ T_1,\ T_{01},\ S,\ S_{01},\ L,\ L_0,\ L_1,\ SL,\ L_{01},\ D,\ D_0, \\ D_1,\ D_{01},\ K,\ K_0,\ K_1,\ K_{01},\ U,\ SU,\ MU,\ U_0,\ U_1,\ U_{01}. \end{gathered} \tag{4.9}$$

Доказательство. Согласно свойству 3 любой параметрически замкнутый класс булевых функций целиком содержит класс U_{01}. Далее, по лемме 4.1 и принципу двойственности для параметрической выразимости (свойство 5) любой замкнутый (относительно операции суперпозиции) класс булевых функций, который содержит хотя бы один из классов MO_0^∞ или MI_1^∞ и отличен от класса T_{01}, не является параметрически замкнутым. Лемма 4.2 показывает, что параметрически замкнутым не является также класс SM. Таким образом, параметрически замкнутыми могут быть лишь классы из списка (4.9).

Согласно леммам 4.3–4.7 и принципу двойственности для параметрической выразимости параметрически замкнутыми являются классы

$$T_0,\ T_1,\ S,\ L,\ D,\ K,\ U. \tag{4.10}$$

Все остальные классы из списка (4.9), отличные от класса P_2, представляют собой пересечения двух или трех классов из (4.10) (класс MU есть пересечение классов D и K). Поэтому в силу свойства 2 все классы из (4.9) параметрически замкнуты. То, что все классы из (4.9) различны, установлено в гл. I. Теорема доказана.

Так же, как и в гл. I, для параметрического замыкания можно ввести понятия параметрического базиса, параметрической полноты и параметрического замыкания. Леммы 4.1 и 4.2 показывают, что понятия базиса из гл. I и параметрического базиса могут существенно различаться. Так, из лемм 4.1 и 4.3 следует, что функция $x \vee yz$, которая является базисом класса MO_0^∞, в то же время образует параметрический базис класса T_{01}. Далее, из теоремы 4.1 следует, что параметрически предполными являются шесть параметрически замкнутых классов T_0, T_1, S, L, D, K. Таким образом, имеет место следующий к р и т е р и й   п а р а м е т р и ч е с к о й   п о л н о т ы.

Система булевых функций параметрически полна в P_2 тогда и только тогда, когда она целиком не содержится ни в одном из параметрически замкнутых классов T_0, T_1, S, L, D, K.

§ 2. Позитивное и другие замыкания

Язык Pos позитивной выразимости получается из языка Par добавлением логической связки дизъюнкция $\vee$. Понятие терма в языке Pos совпадает с понятием терма в языке Par, а понятие формулы является очевидным обобщением понятия формулы в языке Par. Аналогично соответствующим понятиям языка Par вводятся понятия позитивной выразимости отношения и функции через функции множества Q, позитивного замыкания и позитивно замкнутого класса. Через $\mathrm{Pos}[Q]$ обозначается позитивное замыкание множества функций Q.

Свойства 1–5, установленные для параметрического замыкания, без изменения переносятся на позитивное замыкание. Однако свойство 3 допускает существенное усиление.

3. *Любой позитивно замкнутый класс булевых функций содержит класс S_{01}.*

В самом деле, формула

$$(x_1 = x_2) \,\&\, (y = x_3) \vee (x_1 = x_3) \,\&\, (y = x_2) \vee (x_2 = x_3) \,\&\, (y = x_2)$$

языка Pos позитивно выражает отношение

$$y = \bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_2 x_3$$

(через пустое множество функций). Согласно лемме 1.19, функция $\bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_2 x_3$ образует базис класса S_{01}. Значит, любой позитивно замкнутый класс булевых функций, который по свойству 4 замкнут относительно операции суперпозиции, будет содержать класс S_{01}.

Отметим еще следующий факт: всякий позитивно замкнутый класс булевых функций параметрически замкнут. Этот факт есть следствие того, что язык Pos представляет собой расширение языка Par.

Теорема 4.2. *Существует ровно шесть позитивно замкнутых классов булевых функций*:

$$P_2,\ T_0,\ T_1,\ T_{01},\ S,\ S_{01}. \tag{4.11}$$

Доказательство. Согласно результатам гл. I, имеется ровно шесть замкнутых классов булевых функций, целиком содержащих класс S_{01}. Это в точности классы (4.11). Поэтому для доказательства теоремы достаточно установить, что каждый из классов (4.11) является позитивно замкнутым. Это очевидно для класса P_2, а классы T_{01} и S_{01} суть пересечения соответственно классов T_0, T_1 и T_0, S. Таким образом, учитывая свойства 2 и 5 для позитивного замыкания, доказательство позитивной замкнутости достаточно провести лишь для классов T_0 и S. Для класса T_0 проходит доказательство леммы 4.3, поскольку язык Pos содержит лишь «позитивные» логические связки & и $\vee$. А позитивная замкнутость класса S следует, как и в случае параметрического замыкания, из принципа двойственности для позитивного замыкания (свойство 5). Теорема доказана.

Из теоремы 4.2 вытекает, в частности, что позитивно предполными являются классы T_0, T_1 и S.

Наряду с языками Par и Pos естественно рассмотреть еще один язык 1L, который получается из языка Pos добавлением логической связки отрицание $\neg$ и квантора общности $\forall$. Так же, как и для языков Par и Pos, вводятся понятия 1L-выразимости, 1L-замыкания и 1L-замкнутого класса. Для 1L-замыкания справедливы аналоги свойств 1–5. Поскольку язык 1L является расширением языка Pos, всякий 1L-замкнутый класс будет также позитивно замкнутым.

Теорема 4.3. *Существуют только два* 1L-*замкнутых класса булевых функций*: P_2 *и* S.

Доказательство. Как установлено выше, функция $\bar{x}_1 x_2 \vee \vee \bar{x}_1 x_3 \vee x_2 x_3$, образующая базис класса S_{01}, выразима формулой языка Pos (через пустое множество функций). Ясно, что эта формула является формулой и языка 1L. Кроме того, формула

$$\urcorner(y = x)$$

языка 1L выражает функцию $\bar{x}$ (через пустое множество функций). Согласно результатам гл. I функции

$$\bar{x}_1 x_2 \vee \bar{x}_1 x_3 \vee x_2 x_3, \qquad \bar{x}$$

образуют полную в S систему. Следовательно, учитывая свойство 4 для 1L-замыкания, приходим к выводу, что всякий 1L-замкнутый класс булевых функций целиком содержит класс S. Однако класс S является предполным в классе P_2. Поэтому для завершения доказательства теоремы достаточно установить 1L-замкнутость класса S. Это следует из принципа двойственности для 1L-замыкания. Теорема доказана.

Из теоремы 4.3 следует, что проблема 1L-полноты в классе P_2 решается довольно просто: существует только один 1L-предполный класс — класс S.

В операторах замыкания, базирующихся на выразимости в языках Par, Pos и 1L, в качестве основных технических средств замыкания выступают чисто логические средства. В заключение параграфа рассмотрим еще один сильный оператор замыкания — S-замыкание, в котором главную роль играют функционально-алгебраические средства.

Пусть Q — множество булевых функций. S-*замыканием* множества Q назовем такое наименьшее множество функций, которое содержит множество Q, замкнуто относительно операции суперпозиции (в смысле определений гл. I) и относительно операции перехода к двойственным функциям. Иными словами, S-замыкание множества Q — это такой наименьший замкнутый класс R, что $Q \subseteq R$ и наряду с любой булевой функцией классу R принадлежит также двойственная ей функция. S-замыкание множества функций Q обозначим через $[Q]_S$.

Из определения следует, что S-замкнутыми заведомо являются все замкнутые классы, которые состоят только из самодвойственных функций:

$$S,\ S_{01},\ SM,\ SL,\ L_{01},\ SU,\ U_{01}. \tag{4.12}$$

Понятно, что вообще все S-замкнутые классы можно получить, если применить следующее соображение. Возьмем произвольный замкнутый класс R, образуем двойственный ему класс R^*, объединим классы R и R^* и произведем замыкание полученного объединения относительно операции суперпозиции. Это соображение вместе с диаграммой включений замкнутых классов, приведенной в гл. I, дает еще восемь классов, не входящих в список (4.12):

$$P_2,\ M,\ L,\ T_{01}, M_{01},\ U,\ MU,\ C. \tag{4.13}$$

Впрочем, к такому же результату можно прийти, если непосредственно проверить для каждого из замкнутых классов его замкнутость относительно операции перехода к двойственным функциям. Таким образом, имеет место следующее утверждение.

Теорема 4.4. *Существует ровно* 15 *S-замкнутых классов булевых функций. Все они представлены в списках* (4.12) *и* (4.13).

Отметим S-предполные классы в P_2: это M, L, S и T_{01}.

Комментарии. Понятия параметрической выразимости и параметрического замыкания введены А. В. Кузнецовым [9]. Ему же принадлежит теорема 4.1. Языки Pos и 1L рассматривались в работе [18]. Идея S-классификации функций многозначной логики высказывалась несколькими авторами. Первое систематическое исследование в этом направлении проведено Нгуен Ван Хоа [21] (см. также [16]). Другие понятия замыкания для множеств функций многозначной логики предлагались в [5, 29, 28, 20].

СПИСОК ЛИТЕРАТУРЫ

1. *Блохина Г. Н.* О предикатном описании классов Поста // Дискретный анализ. — 1970. — Вып. 16. — С. 16–29.
2. *Боднарчук В. Г.*, *Калужнин Л. А.*, *Котов В. Н.*, *Ромов Б. А.* Теория Галуа для алгебр Поста // Кибернетика. — 1969. — № 3. — С. 1–10; № 5. — С. 1–9.
3. *Гаврилов Г. П.* Индуктивное представление булевых функций и конечная порождаемость классов Поста // Алгебра и логика. — 1984. — Т. 23, № 1. — С. 3–26.
4. *Гаврилов Г. П.* Функциональные системы дискретной математики. — М.: Из-во МГУ, 1985.
5. *Голунков Ю. В.* Полнота систем функций в операторных алгоритмах, реализующих функции k-значной логики // Вероятностные методы и кибернетика. — 1980. — Вып. 17. — С. 23–34.
6. *Ершов Ю. Л.*, *Палютин Е. А.* Математическая логика. — М.: Наука, 1979.
7. *Кузнецов А. В.* Алгебра логики и ее обобщения // Яновская С. А. Математическая логика и основания математики. Математика в СССР за сорок лет. Т. 1. — М.: Физматгиз, 1959. — С. 13–120.
8. *Кузнецов А. В.* Структуры с замыканием и критерии функциональной полноты // Успехи матем. наук. — 1961. — Т. XVI, № 2(98). — С. 201–202.
9. *Кузнецов А. В.* О средствах для обнаружения невыводимости и невыразимости. Логический вывод. — М.: Наука, 1979. — С. 5–33.
10. *Мальцев А. И.* Итеративные алгебры и многообразия Поста // Алгебра и логика. — 1966. — Т. 5, № 2. — С. 5–24.
11. *Мальцев А. И.* Итеративные алгебры Поста. — Новосибирск: Из-во НГУ, 1976.
12. *Марченков С. С.* К существованию конечных базисов в замкнутых классах булевых функций // Алгебра и логика. — 1984. — Т. 23, № 1. — С. 88–99.
13. *Марченков С. С.* О классах Слупецкого в системах $P_k \times \ldots \times P_l$ // Дискретная математика. — 1992. — Т. 4, № 3. — С. 135–148.

14. *Марченков С. С.* О предполных классах в декартовых произведения P_2 и P_3 // Дискретная математика. — 1994. — Т. 6, № 2. — С. 21–42.

15. *Марченков С. С.* Предполнота замкнутых классов в P_k: предикатный подход // Математические вопросы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 117–132.

16. *Марченков С. С.* S-классификация функций многозначной логики // Дискретная математика. — 1997. — Т. 9, № 3. — С. 125–152.

17. *Марченков С. С.* Инварианты классов Поста // Фундаментальная и прикладная математика. — 1998. — Т. 4, № 4. — С. 1385–1404.

18. *Марченков С. С.* О выразимости функций многозначной логики в некоторых логико-функциональных языках // Дискретная математика. — 1999. — Т. 11, № 4. — С. 110–126.

19. *Марченков С. С., Угольников А. Б.* Замкнутые классы булевых функций. — М.: Из-во ИПМ АН СССР, 1990.

20. *Нгуен Ван Хоа.* Об L-эквивалентности систем функций в многозначной логике // Алгебра и логика. — 1988. — Т. 27, № 1. — С. 37–47.

21. *Нгуен Ван Хоа.* О семействах замкнутых классов k-значной логики, сохраняемых всеми автоморфизмами // Дискретная математика. — 1993. — Т. 5, № 4. — С. 87–108.

22. *Оре О.* Теория графов. — М.: Наука, 1968.

23. *Риге Ж.* Бинарные отношения, замыкания, соответствия Галуа // Кибернетический сборник. Вып. 7. — М.: Мир, 1963. — С. 129–185.

24. *Ромов Б. А.* Алгоритм решения проблемы полноты в классе векторных функциональных систем // Математические модели сложных систем. — Киев: ИК АН УССР, 1973. — С. 151–155.

25. *Ромов Б. А.* О решетке подалгебр прямых произведений алгебр Поста конечной степени // Математические модели сложных систем. — Киев: ИК АН УССР, 1973. — С. 156–168.

26. *Ромов Б. А.* О полноте на квадрате функций алгебры логики и в системе $P_k \times P_l$ // Кибернетика. — 1987. — № 4. — С. 9–14.

27. *Ромов Б. А.* Об одной серии максимальных подалгебр прямых произведений алгебр конечнозначных логик // Кибернетика. — 1989. — № 3. — С. 11–16.

28. *Соловьев В. Д.* Замкнутые классы в k-значной логике с операцией разветвления по предикату // Дискретная математика. — 1990. — Т. 2, № 4. — С. 19–25.

29. *Тайманов В. А.* О функциональных системах k-значной логики с операциями программного типа // Доклады АН СССР. — 1983. — Т. 268, № 6. — С. 1307–1310.

30. *Угольников А. Б.* О замкнутых классах Поста // Известия вузов. Математика. — 1988. — № 7. — С. 79–88.

31. *Яблонский С. В.* О строении верхней окрестности для предикатноописуемых классов в P_k // Доклады АН СССР. — 1974. — Т. 218, № 2. — С. 304–307.

32. *Яблонский С. В.* О некоторых результатах в теории функциональных систем // Труды Международного конгресса математиков. — Хельсинки, 1978. — С. 963–971.

33. *Яблонский С. В.* О замкнутых классах в P_2 // Проблемы кибернетики. Вып. 39. — М.: Наука, 1982. — С. 262.

34. *Яблонский С. В.*, *Гаврилов Г. П.*, *Кудрявцев В. Б.* Функции алгебры логики и классы Поста. — М.: Наука, 1966.

35. *Benzaken C.* Definitions et proprietes de certains familles de fonctions booleénnes croissantes // C. R. Acad. Sci. Paris. — 1964. — T. 259, group I. — P. 1369–1371.

36. *Benzaken C.* Les familles de fonctions booleénnes deduites de certains familles de fonctions booleénnes croissates. Criteres de determination de l'indice d'une fonction croissante // C. R. Acad. Sci. Paris. — 1965. — T. 260, group I. — P. 1528–1531.

37. *Geiger D.* Closed systems of functions and predicates // Pacific J. Math. — 1968. — V. 27. — P. 95–100.

38. *Kuntzman J.* Algébre de Boole. — Paris: Dunod, 1965.

39. *Ore O.* Galois connections // Trans. Amer. Math. Soc. — 1944. — V. 55. — P. 493–513.

40. *Post E. L.* Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43, № 4. — P. 163–185.

41. *Post E. L.* Two-valued iterative systems of mathematical logic // Annals of Math. Studies. Princeton Univ. Press. — 1941. — V. 5.

42. *Reschke M.*, *Denecke K.* Ein neuer Beweis für die Ergebnisse von E.L.Post über abgeschlossene Klassen Boolescher Funktionen // J. Process. Cybern. EIK. — 1989. — Bd. 7. — S. 361–380.

43. *Riguet J.* Relations binaire, fermetures, correspondences de Galois // Bull. Soc. Math. France. — 1948. — V. 76. — P. 114–155.

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Сведения об авторе. Марченков Сергей Серафимович родился в 1945 г. Окончил механико–математический факультет Московского государственного университета им. М. В. Ломоносова. Доктор физико–математических наук, ведущий научный сотрудник Института прикладной математики им. М. В. Келдыша РАН, по совместительству профессор Московского государственного технического университета им. Н. Э. Баумана. Опубликовал более 70 научных работ по теории функциональных систем, теории алгоритмов, теории автоматов, математической логике и универсальной алгебре.

S. S. MARCHENKOV

CLOSED CLASSES OF BOOLEAN FUNCTIONS

PHYSICS AND MATHEMATICS PUBLISHERS
International Academic Publishing Company "Nauka"
Rassian Academy of Science

Moscow, 2000, 128 pages

Abstract. The main purpose of the book is to propose the complete description of all closed classes of Boolean functions (Post classes). The new compact proof of finite generation of all Post classes is given in Chapter I. In Chapter II, the base of Galois theory for Post algebras is clarified, and all Post classes obtain the predicate decriptions. The Chapter III is devoted to a perspective direction in the theory of Boolean functions, namely to closed classes of Boolean vector-functions. In this Chapter, the completeness problem is solved by means of Galois theory for direct products of Post algebras. Some "strong"closure operators leading to the finite lattices of closed classes are considered in Chapter IV.

Author. Sergei S. Marchenkov, born 1945. Education: Moscow State University, D. Sc. (Phys. & Math.). Leading scientific resercher in Keldysh Institute of Applied Mathematics, professor at Moscow State Technical University. Over 70 papers in the theory of functional systems, theory of algorithms, theory of automata, mathematical logic, and universal algebra.

Научное издание

МАРЧЕНКОВ Сергей Серафимович

ЗАМКНУТЫЕ КЛАССЫ БУЛЕВЫХ ФУНКЦИЙ

Редактор *Е. Ю. Ходан*
Оригинал-макет *А. А. Черепанова*

ЛР № 071930 от 06.07.99. Подписано в печать 25.07.2000.
Формат 60 × 90/16. Бумага офсетная № 1. Печать офсетная.
Усл. печ. л. 8. Уч.-изд. л. 8,8. Тираж 1000 экз. Заказ №

Издательская фирма «Физико-математическая литература» (ФИЗМАТЛИТ)
МАИК «Наука/Интерпериодика»
117864 Москва, ул. Профсоюзная, 90

Отпечатано с готовых диапозитивов в ППП «Типография «Наука»
121099 Москва, Шубинский пер., 6

ISBN 5-9221-0066-1

9 785922 100663