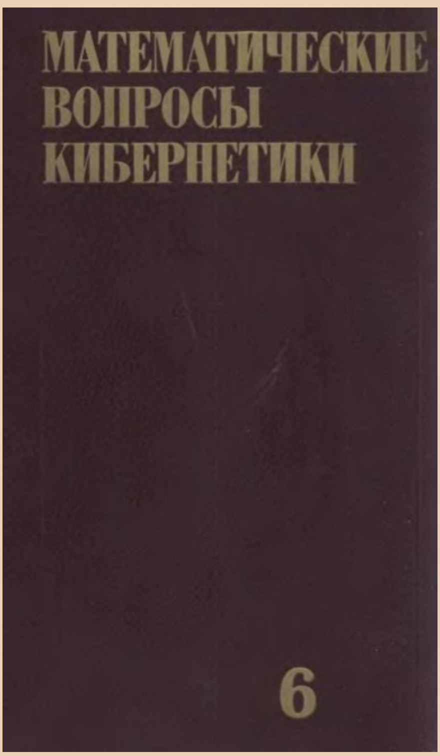

С. С. Марченков

Предполнота замкнутых классов в P_k: предикатный подход

ПРЕДПОЛНОТА ЗАМКНУТЫХ КЛАССОВ В P_k: ПРЕДИКАТНЫЙ ПОДХОД

С. С. МАРЧЕНКОВ

(МОСКВА)

Одной из центральных проблем в теории функций k-значной логики является проблема полноты. Как установил А. В. Кузнецов [4, 15], эта проблема допускает эффективное решение: при любом k, $k \geqslant 2$, в P_k имеется конечное множество предполных классов, и произвольная система функций из P_k полна в P_k в том и только том случае, когда она целиком не содержится ни в одном из классов этого множества. Точное описание множества всех предполных классов, эффективное задание каждого класса из этого множества также является серьезной проблемой. При $k = 2$ она была решена Э. Постом [24, 25], при $k = 3$ — С. В. Яблонским [14, 15]. При произвольном k отдельные серии предполных в P_k классов были определены в работах [4, 5, 6, 20–23]. Завершить описание всех предполных в P_k классов удалось И. Розенбергу [26, 28].

Решение проблемы полноты в P_k условно можно разбить на три этапа: выбор языка описания предполных классов и задание на нем некоторого множества M замкнутых классов, доказательство предполноты всех классов из множества M, доказательство отсутствия других предполных классов, не входящих в множество M. Этапы эти идейно и по трудоемкости не равноценны. В настоящее время общепринятым языком описания предполных классов в P_k является предикатный язык. Предполные классы определяются как классы сохранения подходящим образом выбранных предикатов. Подобный подход в определении предполных классов предложен А. В. Кузнецовым [4], хотя некоторые идеи в этом направлении можно извлечь из более ранних работ М. Краснера [18, 19].

В настоящей работе мы остановимся на втором этапе решения проблемы полноты: речь пойдет о способах доказательства предполноты замкнутых классов в P_k. В известных работах на эту тему используется следующая схема рассуждений. Пусть мы хотим установить предполноту замкнутого класса K. Исходя из определения этого класса подходящим образом охарактеризовываются входящие в него функции. Рассматривается произвольная функция f, не принадлежащая K. С использованием функций класса K из функции f суперпозициями определяются одна или несколько функций $g_1, \ldots, g_m$, также не принадлежащих K, но по некоторым параметрам (характеристикам) более простых, чем функция f. Наконец, из функций $g_1, \ldots, g_m$ и функций класса K образуется одна из стандартных полных систем функций. В общем случае этот путь оказывается довольно трудоемким [6, 15, 28] (так, книга [17] целиком посвящена решению этого вопроса).

Вместе с тем существует принципиально иной путь доказательства предполноты замкнутых классов в P_k, основанный на теории Галуа для алгебр Поста [1] (на возможность ее построения указывал А. В. Кузнецов в [5]). Как оказалось, любой замкнутый класс функций из P_k, содержащий селекторные функции, можно полностью охарактеризовать множеством подходящим образом выбранных инвариантов (предикатов). При этом на множестве инвариантов (предикатов) можно так задать некоторые операции, чтобы совокупность всех множеств предикатов, соответствующих замкнутым классам функций из P_k, в точности совпала с совокупностью всех замкнутых (относительно этих операций) классов предикатов, содержащих диагонали. Соответствие между замкнутыми классами функций и замкнутыми классами предикатов есть соответствие Галуа [8, 9]. Оно определено отношением «функция сохраняет предикат», предложенным А. В. Кузнецовым [4]. При этом предполным классам в P_k соответствуют минимальные классы предикатов, которые порождаются с помощью выбранных операций любыми своими предикатами, отличными от диагоналей. Это позволяет устанавливать предполноту замкнутых классов путем доказательства минимальности соответствующих предикатов. В силу специфики операций, действующих на множестве предикатов, последнее доказательство можно выполнить чисто логическими средствами, не прибегая к понятию функции k-значной логики. В техническом плане такой способ доказательства предполноты замкнутых классов часто оказывается существенно менее трудоемким, чем традиционно применявшийся способ. Стоит также отметить, что этот путь доказательства уже успешно применялся для произведений алгебр Поста [7, 11–13].

В настоящей работе мы устанавливаем предполноту всех предполных в P_k классов, доказывая минимальность определяющих их предикатов.

§ 1. Основные понятия

Если $k \geqslant 2$, то пусть $E_k = \{0, 1, \ldots, k-1\}$ и P_k — множество всех функций $f\colon E_k^n \to E_k$, где $n = 1, 2, \ldots$ Множество P_k называется множеством функций k-значной логики. На множестве P_k определяется операция суперпозиции, что превращает P_k в функциональную систему с операцией суперпозиции [3, 16]. Подмножества множества P_k, замкнутые относительно операции суперпозиции, называются *замкнутыми классами*. Множество всех замкнутых классов частично упорядочено отношением включения. Наибольшим элементом в этом частичном порядке является все множество P_k, максимальные элементы носят название *предполных классов*.

Для любых n и i, $1 \leqslant i \leqslant n$, определяем на E_k *селекторные функции*

$$e_i^n(x_1, \ldots, x_i, \ldots, x_n) = x_i.$$

Предикатом на множестве E_k называют отображение $\rho\colon E_k^m \to \{\text{И}, \text{Л}\}$, где И, Л — истинностные значения «истина» и «ложь». Часто предикат ρ отождествляют с множеством тех наборов из E_k^m, на которых он является истинным. В связи с этим для предикатов ρ, σ, определенных на E_k^m, употребляют выражения «предикат ρ входит в предикат σ» или «предикат σ является расширением предиката ρ», имея в виду, что множество истинности предиката ρ содержится в множестве истинности предиката σ. Тождественно истинный предикат называют также *полным* предикатом, а тождественно ложный — *пустым*. Множество всех предикатов на E_k обозначаем через Π_k.

Пусть δ — отношение эквивалентности на множестве $\{1, 2, \ldots, m\}$, т. е. бинарное рефлексивное, симметричное и транзитивное отношение. *Диагональю*, соответствующей отношению δ, называется такой предикат $\rho(x_1, \ldots, x_m)$ на E_k, что для любого набора $(a_1, \ldots, a_m)$ из E_k^m значение $\rho(a_1, \ldots, a_m)$ истинно в том и только том случае, когда для любых i, j ($1 \leqslant i, j \leqslant m$) справедлива импликация $\delta(i, j) \Rightarrow (a_i = a_j)$. Диагональ, отвечающая единичной эквивалентности δ (в ней эквивалентны только равные элементы), представляет собой *полную диагональ*. Удобно также причислить к диагоналям тождественно ложный предикат.

Пусть $f(x_1,\ldots,x_n)$ — функция из P_k, а $\rho(x_1,\ldots,x_m)$ — предикат из Π_k. Говорят, что функция f *сохраняет предикат* ρ, если для любых n наборов $(a_{11},\ldots,a_{m1}),\ldots,(a_{1n},\ldots,a_{mn})$ из E_k^n, удовлетворяющих предикату ρ, набор

$$(f(a_{11},\ldots,a_{1n}),\ldots,f(a_{m1},\ldots,a_{mn}))$$

также удовлетворяет предикату ρ. Множество функций из P_k, сохраняющих предикат ρ, обозначим $\operatorname{Pol}\rho$. Нетрудно убедиться, что для любого предиката ρ множество $\operatorname{Pol}\rho$ представляет собой замкнутый класс, содержащий все селекторные функции. Кроме того, если ρ — диагональ, то $\operatorname{Pol}\rho = P_k$.

Введем несколько операций над предикатами. Пусть $\rho(x_1,\ldots,x_m)$ — предикат на E_k. *Проекцией* предиката ρ по переменной x_i называется такой $(m-1)$-местный предикат σ на E_k, что

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

Областью действия квантора $\exists x_i$ в формуле (1) является множество E_k, поэтому предикат σ можно также представить в виде

$$\sigma(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_m) \equiv \bigvee_{a\in E_k} \rho(x_1,\ldots,x_{i-1},a,x_{i+1},\ldots,x_m).$$

Если в формуле (1) имеем $m = 1$, то получаем нульместный предикат σ, истинный только в том случае, когда предикат ρ является истинным хотя бы для одного значения из E_k.

Пусть $\rho(x_1,\ldots,x_m)$, $\sigma(x_1,\ldots,x_n)$ — предикаты на E_k. *Конъюнкцией* предикатов ρ и σ называется такой $(m+n)$-местный предикат τ на E_k, что

$$\tau(x_1,\ldots,x_m,x_{m+1},\ldots,x_{m+n}) \equiv \rho(x_1,\ldots,x_m) \,\&\, \sigma(x_{m+1},\ldots,x_{m+n}). \qquad (2)$$

Операции *перестановки* и *отождествления* переменных над предикатами предполагаются известными. Набор операций проектирования, конъюнкции, перестановки и отождествления переменных обозначим через Ω.

Имея все диагонали, с помощью операций из Ω можно выразить другие распространенные операции над предикатами [1]. Например, чтобы добавить к предикату $\rho(x_1,\ldots,x_m)$ фиктивную переменную x_{m+1}, достаточно образовать предикат $\rho(x_1,\ldots,x_m) \,\&\, \sigma(x_{m+1})$, где σ — полная диагональ. Чтобы удалить из предиката ρ фиктивную переменную x_i, можно либо спроектировать предикат ρ по переменной x_i, либо отождествить переменную x_i с любой другой переменной. Для образования конъюнкции вида $\rho(x_1,\ldots,x_m) \,\&\, \sigma(x_1,\ldots,x_m)$ следует сначала с помощью операции конъюнкции получить предикат $\rho(x_1,\ldots,x_m) \,\&\, \sigma(x_{m+1},\ldots,x_{2m})$, а затем произвести в нем необходимые отождествления переменных.

Так же, как с помощью операции суперпозиции на множестве P_k образуются замкнутые классы функций, с помощью операций Ω на множестве Π_k можно образовать замкнутые классы предикатов. Пусть $\Sigma(f,\rho)$ обозначает отношение «функция f сохраняет предикат ρ». Соответствие Галуа [8, 9] между частично упорядоченными по включению множествами всех замкнутых классов функций, содержащих все селекторные функции, и множеством всех замкнутых классов предикатов, содержащих все диагонали, задается двумя функторами, Pol и Inv: если P — произвольное множество функций из P_k, а Π — произвольное множество предикатов из Π_k, то

$$\operatorname{Pol}(\Pi) = \{f\colon\ f \in P_k \text{ и } \Sigma(f,\rho) \text{ для всех предикатов } \rho \text{ из } \Pi\},$$
$$\operatorname{Inv}(P) = \{\rho\colon\ \rho \in \Pi_k \text{ и } \Sigma(f,\rho) \text{ для всех функций } f \text{ из } P\}$$

(см. [1]). Соответствие Галуа в данном случае оказывается антиизоморфизмом. В частности, наибольшему замкнутому классу P_k отвечает наименьший замкнутый класс всех диагоналей, а предполным в P_k классам — *минимальные* классы предикатов. Отличные от диагоналей предикаты из минимальных классов называются *минимальными предикатами.* Согласно определению любые два минимальных предиката из одного и того же минимального класса можно перевести друг в друга с использованием диагоналей и операций набора Ω. Итак, каждый предполный класс определяется подходящим минимальным предикатом.

Определение минимального предиката можно дать в несколько иной форме. Именно, отличный от диагонали предикат ρ будет минимальным, если предикат ρ можно получить с помощью операций Ω из диагоналей и произвольного отличного от диагонали предиката σ, который в свою очередь получен с помощью операций Ω из предиката ρ и диагоналей. Это определение дает возможность доказывать предполноту замкнутых классов в P_k, заданных предикатами, не используя понятие функции из P_k.

Проведем еще несколько упрощений технического характера в определении минимального предиката. Пусть предикат σ получен из ρ введением фиктивной переменной. Нетрудно проверить, что в этом случае $\mathrm{Pol}\,\sigma = \mathrm{Pol}\,\rho$. Поэтому при исследовании предикатов на минимальность можно ограничиться предикатами без фиктивных переменных.

Будем говорить, что предикат $\rho(x_1, \ldots, x_m)$ имеет *повторяющиеся координаты* x_i, x_j, если для любого набора $(a_1, \ldots, a_m)$, удовлетворяющего предикату ρ, имеет место равенство $a_i = a_j$. Предикат, не имеющий повторяющихся координат, называется *стандартным*. Если предикат ρ имеет повторяющиеся координаты x_i, x_j, а предикат σ получен из предиката ρ отождествлением переменных x_i, x_j, то, как легко видеть, $\mathrm{Pol}\,\sigma = \mathrm{Pol}\,\rho$. Следовательно, среди минимальных предикатов можно рассматривать только стандартные предикаты, не содержащие фиктивных переменных. Как замечено в [11, 12], в этом случае в определении минимального предиката можно не использовать диагонали.

Нетрудно видеть, что применение операций из Ω к предикатам носит формульный характер (см., например, формулы (1) и (2)). Соответствующие формулы будем называть $(\exists, \&)$-*формулами*, подчеркивая ведущую роль операций проектирования и конъюнкции. Допуская некоторую вольность речи, будем говорить далее о построении одних предикатов из других с помощью $(\exists, \&)$-формул, имея в виду, конечно, построение предикатов с помощью соответствующих операций. Используя понятие $(\exists, \&)$-формулы, будем в дальнейшем оперировать со следующим понятием минимального предиката.

Стандартный предикат ρ, не имеющий фиктивных переменных, является минимальным, если его можно получить с помощью $(\exists, \&)$-формулы из произвольного отличного от диагонали предиката σ, который в свою очередь получен из предиката ρ некоторой $(\exists, \&)$-формулой.

§ 2. Предикаты классов P, O, L, E, C, B

При определении предикатов, задающих предполные в P_k классы, мы придерживаемся классификации, предложенной И. Розенбергом [28]. Сами определения лишь в незначительных деталях отличаются от определений Розенберга.

Предикаты класса **P**. Пусть π — подстановка на E_k, которая разлагается в циклы одной и той же простой длины. Для любой такой подстановки π класс **P** включает предикат $\pi(x_1) = x_2$, который называется *графиком подстановки* π.

Предикаты класса **O**. Класс **O** содержит всякий двуместный предикат, который определяет на множестве E_k частичный порядок с наименьшим и наибольшим элементами (ограниченный частичный порядок).

Предикаты класса **L**. Класс **L** непуст только в том случае, когда k имеет вид p^l, где p — простое число, $l \geqslant 1$. В этом случае на множестве E_k можно определить бинарную коммутативную операцию $+$ таким образом, что $G = \langle E_k; +\rangle$ будет являться абелевой p-группой периода p (см., например, [2]).

Итак, пусть $k = p^l$ и $G = \langle E_k; +\rangle$ — абелева p-группа периода p. Если $p = 2$, то в класс $\mathbf{L}$ входит четырехместный предикат

$$x_1 + x_2 + x_3 + x_4 = 0, \tag{3}$$

где 0 — нуль группы G. Если же $p > 2$, то в класс $\mathbf{L}$ входит трехместный предикат

$$x_1 + x_2 = x_3 + x_3 = 0 \tag{4}$$

(выражение $x_3 + x_3$ иногда записывают в виде $2x_3$, однако при этом следует помнить, что группа G аддитивна и символ 2, вообще говоря, не обозначает элемент 2 группы G).

Предикаты класса $\mathbf{E}$. Класс $\mathbf{E}$ состоит из всех двуместных предикатов, которые являются отношениями эквивалентности на E_k, отличными от полного и единичного отношений эквивалентности (нетривиальные отношения эквивалентности).

Предикаты класса $\mathbf{C}$. Чтобы определить предикаты класса $\mathbf{C}$, введем несколько новых понятий. Дня любого m, $m \geqslant 2$, положим

$$\tau_m(x_1, \ldots, x_m) \equiv \bigvee_{1 \leqslant i < j \leqslant m} (x_i = x_j).$$

Предикат $\rho(x_1, \ldots, x_m)$ называется *вполне рефлексивным*, если либо $m = 1$, либо $m \geqslant 2$ и ρ является расширением предиката τ_m. Таким образом, если $m \geqslant 2$ и $\rho(x_1, \ldots, x_m)$ — вполне рефлексивный предикат, то ему удовлетворяют все наборы из E_k^m, содержащие каждый не более $m-1$ различных значений.

Предикат ρ называется *вполне симметричным*, если он не меняется при любой перестановке переменных. Неполный предикат $\rho(x_1, \ldots, x_m)$ назовем *центральным*, если он вполне рефлексивен, вполне симметричен и существует такое непустое подмножество C множества E_k (центр предиката ρ), что предикату ρ удовлетворяет всякий набор $(a_1, \ldots, a_m)$ из E_k^m, где $\{a_1, \ldots, a_m\} \cap C \neq \varnothing$. Класс $\mathbf{C}$ состоит из всех центральных предикатов.

Предикаты класса $\mathbf{B}$. Класс $\mathbf{B}$ непуст при $k \geqslant 3$. Чтобы определить предикаты класса $\mathbf{B}$, дадим еще два важных определения.

Пусть $h \geqslant 3$, $l \geqslant 1$ и $k = h^l$. Элемент a множества E_k можно единственным образом представить в виде

$$a = a^{(0)} + a^{(1)}h + \ldots + a^{(l-2)}h^{l-2} + a^{(l-1)}h^{l-1},$$

где $a^{(0)}, \ldots, a^{(l-1)} \in E_h$. Поэтому элемент a представим вектором $(a^{(0)}, \ldots \ldots, a^{(l-1)})$ размерности l, компоненты которого принадлежат множеству E_h. Пусть $\rho(x_1, \ldots, x_m)$ — предикат из Π_h. Определим предикат $\rho^l(x_1, \ldots, x_m)$ из Π_k, который назовем *l-й декартовой степенью* предиката ρ. Если $a_1, \ldots \ldots, a_m$ — произвольные элементы из E_k, которые определяются векторами

$$(a_1^{(0)}, a_1^{(1)}, \ldots, a_1^{(l-1)}), \ldots, (a_m^{(0)}, a_m^{(1)}, \ldots, a_m^{(l-1)}),$$

где $a_j^{(i)} \in E_h$ при $0 \leqslant i \leqslant l-1$, $1 \leqslant j \leqslant m$, то полагаем

$$\rho^l(a_1, \ldots, a_m) \equiv \rho(a_1^{(0)}, \ldots, a_m^{(0)}) \mathbin{\&} \ldots \mathbin{\&} \rho(a_1^{(l-1)}, \ldots, a_m^{(l-1)}).$$

Отметим, что первая степень предиката ρ совпадает с самим предикатом ρ.

Пусть $k \geqslant h$, $\sigma(x_1, \ldots, x_m)$ — предикат из Π_h и q — отображение E_k на E_h (эпиморфизм из E_k в E_h). Предикат $\rho(x_1, \ldots, x_m)$ из Π_k называется *полным эпиморфным прообразом* предиката σ при эпиморфизме q, если для любых элементов $a_1, \ldots, a_m$ из E_k имеет место эквивалентность

$$\rho(a_1, \ldots, a_m) \equiv \sigma(q(a_1), \ldots, q(a_m)).$$

Если $h \geqslant 3$, $l \geqslant 1$, $k \geqslant h^l$ и q — эпиморфизм из E_k в E_{h^l}, то классу **B** принадлежит предикат, являющийся полным эпиморфным прообразом l-й декартовой степени предиката τ_h при эпиморфизме q.

Отметим, что все предикаты из классов **P**, **O**, **L**, **E**, **C**, **B** стандартны и не содержат фиктивных переменных.

Нетрудно проверить, что операция взятия декартовой степени переводит предикат любого из классов **P**, **O**, **L**, **E**, **C**, **B** в предикат того же класса, а операция взятия полного эпиморфного прообраза — предикат любого из классов **E**, **C**, **B** в предикат того же класса. В связи с этим иногда предикаты из множества $\mathbf{P} \cup \mathbf{O} \cup \mathbf{L} \cup \mathbf{E} \cup \mathbf{C} \cup \mathbf{B}$ удается получить из более «простых» предикатов с помощью операций взятия декартовой степени или полного эпиморфного прообраза. Именно так (например, через предикат τ_h) определяются все предикаты класса **B**. На этом же пути можно определить все предикаты класса **E**. В самом деле, пусть $\rho(x_1, x_2)$ — нетривиальное отношение эквивалентности на E_k, имеющее в точности h классов эквивалентности. Выберем из каждого класса эквивалентности по одному представителю и обозначим полученное h-элементное подмножество множества E_k через E. Пусть q есть отображение множества E_k на множество E, ставящее в соответствие любому элементу a из E_k тот единственный элемент b из E, для которого истинно значение $\rho(a, b)$. Нетрудно теперь видеть, что предикат ρ является полным эпиморфным прообразом предиката равенства на E при эпиморфизме q.

Для нас в этом плане наибольший интерес будут представлять предикаты класса L. Пусть p — простое число, $l \geqslant 1$, $k = p^l$ и $G = \langle E_k; + \rangle$ — абелева p-группа периода p. Известно [2], что в группе G можно выбрать базис $e_1, \ldots, e_l$ так, что каждый элемент группы G будет однозначно представим в виде $a_1 e_1 + \ldots + a_l e_l$, где $a_1, \ldots, a_l \in E_p$. В силу этого представления группу G с точностью до группового изоморфизма можно рассматривать как l-мерное векторное пространство V над полем Галуа $GF(p)$ (сложение и умножение в поле $GF(p)$ над элементами из E_p проводится по модулю p). Пусть элементы a_1, a_2, a_3, a_4 из E_k как элементы векторного пространства V задаются наборами коэффициентов $(a_{11}, \ldots, a_{1l}), \ldots, (a_{41}, \ldots, a_{4l})$. В силу независимости элементов базиса $\{e_1, \ldots, e_l\}$ соотношение $a_1 + a_2 + a_3 + a_4 = 0$ (0 — нуль группы G) будет выполняться в том и только том случае, когда будут выполняться (в поле $GF(p)$) все l соотношений

$$a_{11} + a_{21} + a_{31} + a_{41} = 0, \quad \ldots, \quad a_{1l} + a_{2l} + a_{3l} + a_{4l} = 0.$$

Итак, предикат (3) из Π_k изоморфен l-й декартовой степени предиката (3) из класса Π_p. Аналогичное утверждение справедливо для предиката (4).

§ 3. Операции, сохраняющие минимальность

Как мы видели в § 1, минимальность предиката сохраняется при введении и удалении фиктивной переменной или повторяющихся координат. Нетрудно также видеть, что минимальность предиката сохраняется при произвольной перестановке переменных (без отождествлений). Названные операции над предикатами не выводят за пределы класса Π_k. Для нас в дальнейшем более важными будут операции взятия декартовой степени и полного эпиморфного прообраза, которые уже не обладают этим свойством. Прежде чем доказать, что они также сохраняют минимальность предиката, нам потребуется установить перестановочность этих двух операций с операциями из Ω. Иными словами, мы хотим показать, что

$$\Phi(\Psi(\rho)) = \Psi(\Phi(\rho)), \quad \Phi(\rho \,\&\, \sigma) = \Phi(\rho) \,\&\, \Phi(\sigma),$$

где Φ — операция взятия декартовой степени или полного эпиморфного прообраза, а Ψ — одна из одноместных операций набора Ω (частные случаи перестановочности этих операций отмечались в [11]).

Лемма 1. *Операции взятия декартовой степени и полного эпиморфного прообраза перестановочны с операцией проектирования.*

Доказательство. Пусть $\rho(x_1,\ldots,x_m)$ — предикат из Π_h и $\rho^l(x_1,\ldots,x_m)$ — l-я декартова степень предиката ρ. И пусть, например, предикат $\sigma(x_2,\ldots,x_m)$ получается из предиката ρ, а предикат σ_1 — из предиката ρ^l проектированием по переменной x_1. Мы хотим показать, что l-я декартова степень предиката $\sigma(x_2,\ldots,x_m)$ — предикат $\sigma^l(x_2,\ldots,x_m)$ — совпадает с предикатом $\sigma_1(x_2,\ldots,x_m)$. С этой целью переменные x_i, принимающие значения из множества E_{h^l}, будем представлять в векторной форме $x_i = (x_i^0,\ldots,x_i^{l-1})$, где компоненты x_i^j принимают значения из множества E_h. Имеем согласно определению декартовой степени предиката

$$\rho^l(x_1,\ldots,x_m) \equiv \rho(x_1^0,\ldots,x_m^0) \,\&\ldots\&\, \rho(x_1^{l-1},\ldots,x_m^{l-1}). \tag{5}$$

Так как переменные $x_1^0,\ldots,x_1^{l-1}$ могут независимо принимать значения из множества E_h, то из (5) получаем далее навешиванием кванторов существования и применением стандартных логических правил:

$$\begin{aligned}
\sigma_1(x_2,\ldots,x_m) &\equiv (\exists x_1)\rho^l(x_1,\ldots,x_m) \equiv \\
&\equiv (\exists x_1^0)\ldots(\exists x_1^{l-1})(\rho(x_1^0,\ldots,x_m^0) \,\&\ldots\&\, \rho(x_1^{l-1},\ldots,x_m^{l-1})) \equiv \\
&\equiv (\exists x_1^0)\rho(x_1^0,\ldots,x_m^0) \,\&\ldots\&\, (\exists x_1^{l-1})\rho(x_1^{l-1},\ldots,x_m^{l-1}) \equiv \\
&\equiv \sigma(x_2^0,\ldots,x_m^0) \,\&\ldots\&\, \sigma(x_2^{l-1},\ldots,x_m^{l-1}) \equiv \sigma^l(x_2,\ldots,x_m).
\end{aligned}$$

Пусть теперь $\sigma(x_1,\ldots,x_m)$ — предикат из Π_h, $k \geqslant h$, q — эпиморфизм из E_k в E_h и $\rho(x_1,\ldots,x_m)$ — полный эпиморфный прообраз предиката σ при эпиморфизме q. Обозначим далее через $\sigma_1(x_2,\ldots,x_m)$, $\rho_1(x_2,\ldots,x_m)$ предикаты, полученные из предикатов $\sigma(x_1,\ldots,x_m)$, $\rho(x_1,\ldots,x_m)$ проектированием по переменной x_1. Мы хотим показать, что предикат ρ_1 совпадает с полным эпиморфным прообразом предиката σ_1 при эпиморфизме q. Так как $\{q(0),\ldots,q(k-1)\} = E_h$, получаем цепочку эквивалентностей:

$$\begin{aligned}
\rho_1(x_2,\ldots,x_m) &\equiv (\exists x_1)\rho(x_1,x_2,\ldots,x_m) \equiv \\
&\equiv \rho(0,x_2,\ldots,x_m) \vee\ldots\vee \rho(k-1,x_2,\ldots,x_m) \equiv \\
&\equiv \sigma(q(0),q(x_2),\ldots,q(x_m)) \vee\ldots\vee \sigma(q(k-1),q(x_2),\ldots,q(x_m)) \equiv \\
&\equiv (\exists x_1)\sigma(q(x_1),q(x_2),\ldots,q(x_m)) \equiv \sigma_1(x_2,\ldots,x_m).
\end{aligned}$$

Лемма доказана.

Лемма 2. *Операции взятия декартовой степени и полного эпиморфного прообраза перестановочны с операцией конъюнкции.*

Доказательство. Пусть $\rho(x_1,\ldots,x_m)$, $\sigma(x_1,\ldots,x_n)$ — предикаты из Π_h, $\tau(x_1,\ldots,x_{m+n})$ — конъюнкция предикатов ρ и σ. Установим, что предикат τ^l совпадает с конъюнкцией предикатов ρ^l и σ^l. Имеем в силу определений

$$\tau^l(x_1,\ldots,x_{m+n}) \equiv \tau(x_1^0,\ldots,x_{m+n}^0) \mathbin{\&} \ldots \mathbin{\&} \tau(x_1^{l-1},\ldots,x_{m+n}^{l-1}) \equiv$$
$$\equiv \rho(x_1^0,\ldots,x_m^0) \mathbin{\&} \sigma(x_{m+1}^0,\ldots,x_{m+n}^0) \mathbin{\&} \ldots \mathbin{\&} \rho(x_1^{l-1},\ldots,x_m^{l-1}) \mathbin{\&}$$
$$\mathbin{\&} \sigma(x_{m+1}^{l-1},\ldots,x_{m+n}^{l-1}) \equiv \rho^l(x_1,\ldots,x_m) \mathbin{\&} \sigma^l(x_{m+1},\ldots,x_{m+n}).$$

Пусть теперь ρ, σ, τ — такие же, как и выше, $k \geqslant h$, q — эпиморфизм из E_k в E_h и ρ_1, σ_1, τ_1 — полные эпиморфные прообразы предикатов ρ, σ, τ при эпиморфизме q. Покажем, что предикат τ_1 совпадает с конъюнкцией предикатов ρ_1 и σ_1. Исходя из определений, строим цепочку эквивалентностей:

$$\tau_1(x_1,\ldots,x_{m+n}) \equiv \tau(q(x_1),\ldots,q(x_{m+n})) \equiv$$
$$\equiv \rho(q(x_1),\ldots,q(x_m)) \mathbin{\&} \sigma(q(x_{m+1}),\ldots,q(x_{m+n})) \equiv$$
$$\equiv \rho_1(x_1,\ldots,x_m) \mathbin{\&} \sigma_1(x_{m+1},\ldots,x_{m+n}).$$

Лемма доказана.

Аналогично можно получить доказательства перестановочности операций взятия декартовой степени и полного эпиморфного прообраза с операциями перестановки и отождествления переменных.

Лемма 3 по существу получена в [27], лемма 4 отмечалась без доказательства в [10].

Лемма 3. *Операция взятия декартовой степени сохраняет минимальность предикатов.*

Доказательство. Пусть ρ — минимальный предикат, ρ^l — l-я декартова степень предиката ρ и пусть отличный от диагонали предикат σ получен из предиката ρ^l с помощью $(\exists,\&)$-формулы Φ. Обозначим через τ предикат, который получается, если в формуле Φ заменить всюду предикат ρ^l предикатом ρ. В силу перестановочности операции взятия декартовой степени с операциями из Ω предикат σ совпадает с l-й декартовой степенью предиката τ — предикатом τ^l. Отсюда и в силу отличия предиката σ от диагонали вытекает, что предикат τ также должен быть отличен от диагонали. Пользуясь минимальностью предиката ρ, заключаем, что предикат ρ можно получить из предиката τ с помощью подходящей $(\exists,\&)$-формулы Ψ. Еще раз применяем перестановочность операции взятия декартовой степени с операциями из Ω и убеждаемся в том, что предикат ρ^l можно получить из предиката τ^l (т. е. предиката σ) с помощью формулы Ψ. Лемма доказана.

Лемма 4. *Пусть σ — минимальный предикат из Π_h, $k \geqslant h$, q — эпиморфизм из E_k в E_h и ρ — полный эпиморфный прообраз предиката σ при эпиморфизме q. Если из предиката σ с помощью $(\exists,\&)$-формулы невозможно получить неполную диагональ, то ρ — минимальный предикат.*

Доказательство совершенно аналогично доказательству предыдущей леммы. Существенное отличие состоит только в том, что несовпадение с диагональю предиката, полученного из предиката ρ с помощью $(\exists,\&)$-формулы Φ, не гарантирует, вообще говоря, несовпадение с диагональю предиката, полученного из предиката σ с помощью той же формулы Φ. Здесь мы вынуждены использовать соответствующее условие леммы.

В связи с леммой 4 отметим без доказательства (см. также [13]), что неполную диагональ нельзя получить с помощью $(\exists,\&)$-формул из предикатов множества $\mathbf{E}\cup\mathbf{C}\cup\mathbf{B}$. Напротив, из любого предиката, принадлежащего $\mathbf{P}\cup\mathbf{O}\cup\mathbf{L}$, с помощью подходящей $(\exists,\&)$-формулы можно получить предикат равенства.

§ 4. Минимальность предикатов из классов P, O, L, E, C, B

В этом параграфе устанавливаются центральные результаты работы.

Утверждение 1. *Всякий предикат из класса* **P** *минимален.*

Доказательство. Пусть $\rho(x_1, x_2)$ — график подстановки π на E_k, которая разлагается в циклы одной и той же простой длины p. Для любого целого n через π^n обозначим n-ю степень подстановки π и (только в доказательстве этого утверждения) через ρ^n — график подстановки π^n. При $n = 0$ подстановка π^n является тождественной на E_k и потому предикат $\rho^0(x_1, x_2)$ совпадает с диагональю $x_1 = x_2$.

Рассмотрим произвольный отличный от диагонали предикат σ, который получается из предиката ρ с помощью некоторой $(\exists, \&)$-формулы Φ. Покажем прежде всего, как в формуле Φ можно устранить кванторы. Для этого заметим, что $(\pi^m(x_1) = \pi^n(x_2)) \equiv (\pi^{m-n}(x_1) = x_2)$ и, следовательно, справедлива эквивалентность

$$(\exists z)\Bigl(\Bigl(\mathop{\&}_{1\leqslant i\leqslant s} \rho^{m_i}(x_i, z)\Bigr) \,\&\, \Bigl(\mathop{\&}_{1\leqslant j\leqslant t} \rho^{n_j}(z, y_j)\Bigr)\Bigr) \equiv$$

$$\equiv \Bigl(\mathop{\&}_{1\leqslant i<j\leqslant s} \rho^{m_i-m_j}(x_i, x_j)\Bigr) \,\&\, \Bigl(\mathop{\&}_{1\leqslant i<j\leqslant t} \rho^{n_j-n_i}(y_i, y_j)\Bigr) \,\&\, \Bigl(\mathop{\&}_{\substack{1\leqslant i\leqslant s\\ 1\leqslant j\leqslant t}} \rho^{m_i+n_j}(x_i, y_j)\Bigr).$$

Кроме того, если $\tau(x_1, \ldots, x_v, z)$ — произвольный предикат (не обязательно связанный с предикатом ρ), то

$$(\exists z)(\tau(x_1, \ldots, x_v, z) \,\&\, (y_1 = \ldots = y_w = z)) \equiv$$
$$\equiv \tau(x_1, \ldots, x_v, y_1) \,\&\, (y_1 = \ldots = y_w) \qquad (6)$$

(при $w = 1$ тождественно истинный предикат $y_1 = y_1$ можно опустить). С использованием этих эквивалентностей и обычных логических правил из формулы Φ устраняем все кванторы, при этом, правда, могут возникнуть предикаты вида ρ^m и диагонали. Поэтому будем предполагать, что предикат σ реализуется бескванторной формулой Φ, которая составлена из предикатов вида ρ^m и диагоналей. Так как предикат σ отличен от диагонали, то в формулу Φ входит хотя бы один символ ρ^m, где $m \not\equiv 0 \pmod p$. Пусть, например, соответствующей подформулой формулы Φ будет $\rho^m(x_1, x_2)$. Обозначим через $x_3, \ldots, x_s$ остальные переменные предиката σ. Предикат σ отличен от диагонали и, в частности, не является тождественно ложным. Поэтому найдется набор $(a_1, \ldots, a_s)$, который удовлетворяет предикату σ. Поскольку формула $\rho^m(x_1, x_2)$ конъюнктивно входит в формулу Φ, будет истинным также значение $\rho^m(a_1, a_2)$. Положим

$$\sigma_1(x_1, x_2) \equiv (\exists x_3) \ldots (\exists x_s)\sigma_1(x_1, x_2, x_3, \ldots, x_s).$$

Предикат σ_1 отличен от диагонали $x_1 = x_2$, поскольку ему, очевидно, удовлетворяет набор (a_1, a_2) (напомним, что $m \not\equiv 0 \pmod p$), и потому, в частности, из истинности значения $\rho^m(a_1, a_2)$ вытекает неравенство $a_1 \neq a_2$).

Если теперь описанным выше приемом исключить из формулы $(\exists x_3) \ldots$ $\ldots (\exists x_s)\Phi$ кванторы, то мы придем к выводу, что предикат $\sigma_1(x_1, x_2)$ реализуется бескванторной формулой Φ_1, представляющей собой конъюнкцию предикатов вида $\rho^n(x_1, x_2)$, $\rho^n(x_2, x_1)$ и предиката равенства $x_1 = x_2$. Очевидно, однако, что в формулу Φ_1 не может входить предикат $x_1 = x_2$, поскольку предикату σ_1 удовлетворяет набор (a_1, a_2), где $\pi^m(a_1) = a_2$. По этой же причине формула Φ_1 не содержит вхождений предикатов вида $\rho^n(x_1, x_2)$, где $n \not\equiv m \pmod p$, или предикатов вида $\rho^n(x_2, x_1)$, где $n \not\equiv -m \pmod p$.

Значит, формула Φ_1 может содержать лишь предикаты, эквивалентные предикату $\rho^m(x_1, x_2)$, и предикат $\sigma_1(x_1, x_2)$ совпадает с предикатом $\rho^m(x_1, x_2)$.

Если $m \equiv 1 \pmod p$, то $\sigma_1(x_1, x_2) \equiv \rho(x_1, x_2)$, и утверждение доказано. В противном случае в силу простоты числа p найдется такое натуральное число d, что $md \equiv 1 \pmod p$. Имеем тогда

$$\underbrace{\pi^m(\pi^m(\ldots\pi^m}_{d}(x)\ldots)) = \pi^{md}(x) = \pi(x)$$

и, следовательно,

$$\rho(x_1, x_2) \equiv (\exists y_1)\ldots(\exists y_{d-1})\,\&\,(\sigma_1(x_1, y_1)\,\&\,\sigma_1(y_1, y_2)\,\&\ldots\&\,\sigma_1(y_{d-1}, x_2)).$$

Таким образом, предикат ρ получен из предиката σ с помощью $(\exists, \&)$-формулы. Утверждение доказано.

Утверждение 2. *Всякий предикат из класса* **O** *минимален.*

Доказательство. Пусть предикат $\rho(x_1, x_2)$ из Π_k задает на E_k ограниченный частичный порядок. Будем интерпретировать предикат $\rho(x_1, x_2)$ как «x_1 не превосходит x_2». Пусть σ — отличный от диагонали предикат, который получен из предиката ρ с помощью $(\exists, \&)$-формулы Φ. Будем считать, что формула Φ представлена в предваренной форме:

$$\sigma \equiv (\exists X)(\rho_1\,\&\ldots\&\,\rho_s), \tag{7}$$

где X — список переменных, а предикаты $\rho_1, \ldots, \rho_s$ получаются из предиката ρ некоторыми подстановками переменных (возможно, с отождествлениями). Заметим, что имеют место эквивалентности

$$\rho(x_1, x_2)\,\&\,\rho(x_2, x_3)\,\&\ldots\&\,\rho(x_{m-1}, x_m)\,\&\,\rho(x_m, x_1) \equiv$$
$$\equiv (x_1 = x_2 = \ldots = x_m), \qquad \rho(x, x) = \text{И}. \tag{8}$$

Пользуясь этими эквивалентностями и эквивалентностью (6), можно преобразовать формулу (7) в формулу

$$\sigma \equiv (\exists X_1)(\rho_{i_1}\,\&\ldots\&\,\rho_{i_t})\,\&\,D, \tag{9}$$

где D — диагональ, а формула $\rho_{i_1}\,\&\ldots\&\,\rho_{i_t}$ не содержит подформул, представленных левыми частями эквивалентностей (8). Предположим, что расширением диагонали D служит диагональ $x_i = x_j$, т. е.

$$D\,\&\,(x_i = x_j) \equiv D. \tag{10}$$

Из формулы (9) легко следует, что предикат σ содержит в этом случае повторяющиеся координаты x_i, x_j. Как отмечалось в § 1, если предикат σ' получается из предиката σ отождествлением повторяющихся координат, то $\mathrm{Pol}\,\sigma' = \mathrm{Pol}\,\sigma$. В частности, если σ отличен от диагонали, то отличен от диагонали и предикат σ'.

Итак, в формуле (9) можно избавиться от диагонали D, если отождествить все пары переменных x_i, x_j, для которых справедливо (10). К полученной формуле вновь применяем эквивалентности (8), (6) и т. д. В итоге получим отличный от диагонали предикат σ_1, представимый в виде

$$\sigma_1 \equiv (\exists X_2)(\rho_{j_1}\,\&\ldots\&\,\rho_{j_r}), \tag{11}$$

где формула

$$\rho_{j_1}\,\&\ldots\&\,\rho_{j_r} \tag{12}$$

не содержит подформул, эквивалентных левым частям соотношений (8). В связи с этим множество переменных формулы (12) можно считать частично упорядоченным предикатом ρ: переменная y_1 не превосходит переменной y_d, если существуют такие переменные $y_2, \ldots, y_{d-1}$, что среди формул

$\rho_{j_1}, \ldots, \rho_{j_r}$ находятся все формулы $\rho(y_1, y_2)$, $\rho(y_2, y_3), \ldots, \rho(y_{d-1}, y_d)$. Имея в виду это упорядочение, мы будем говорить о минимальных и максимальных переменных формулы (12).

Если x — минимальная переменная, входящая в список X_2, то в формуле (11) можно удалить квантор по переменной x и все подформулы вида $\rho(x, y)$. В самом деле, в силу минимальности переменной x в формулу (12) не входит никакая подформула вида $\rho(z,x)$, а ввиду существования в множестве E_k наименьшего элемента относительно частичного порядка ρ всякая формула

$$(\exists x)(\rho(x, y_1) \mathbin{\&} \ldots \mathbin{\&} \rho(x, y_d))$$

будет тождественно истинной. Аналогичные соображения применимы для максимальных переменных.

Итак, предположим, что в формуле (11) отсутствуют кванторы по минимальным и максимальным переменным. Пусть, например, x_1 — минимальная, x_2 — максимальная переменные, x_1 не превосходит x_2 и $x_3, \ldots, x_n$ — все остальные переменные предиката σ_1. Положим $\sigma_2 \equiv (\exists x_3) \ldots (\exists x_n)\sigma_1$. Утверждается, что предикат σ_2 совпадает с предикатом ρ. В самом деле, если истинно значение $\rho(a, b)$, то в формуле

$$(\exists x_3) \ldots (\exists x_n)(\exists X_2)(\rho_{j_1} \mathbin{\&} \ldots \mathbin{\&} \rho_{j_r}),$$

определяющей предикат σ_2, в качестве значений всех связанных переменных можно выбрать, например, значение a. Если же значение $\rho(a, b)$ ложно, то ложным будет и $\sigma_2(a, b)$, поскольку в формуле (12) переменные x_1, x_2 связаны цепочкой вида

$$\rho(x_1, y_1),\ \rho(y_1, y_2), \ldots, \rho(y_{d-1}, x_2)$$

(напомним, что переменная x_1 не превосходит переменной x_2).

Так как предикат σ_1 получен из предиката σ отождествлением переменных, то предикат ρ, совпадающий с предикатом σ_2, получается из предиката σ с помощью $(\exists, \&)$-формулы. Утверждение доказано.

Утверждение 3. *Всякий предикат из класса* $\mathbf{L}$ *минимален.*

Доказательство. Мы докажем сначала минимальность предикатов из $\mathbf{L}$ в частном случае. Именно, пусть p — простое число, ρ — предикат из Π_p, совпадающий с предикатом (3) при $p = 2$ и с предикатом (4) при $p \geqslant 3$. Последний можно также представить в виде

$$x_1 + x_2 + (p - 2) \cdot x_3 = 0 \tag{13}$$

(здесь и далее сложение и умножение рассматриваются в поле $GF(p)$ вычетов по модулю p). Установим минимальность предиката ρ.

Пусть $a_1, \ldots, a_m$ — ненулевые числа из E_p, $m \geqslant 2$. Замечаем, прежде всего, что уравнение

$$a_1x_1 + \ldots + a_mx_m = 0 \tag{14}$$

разрешимо в поле $GF(p)$ относительно любой переменной x_i. Более точно, если, например, ϑ — единственное решение уравнения $a_mx = p - 1$, то, очевидно,

$$x_m = a_1vx_1 + \ldots + a_{m-1}vx_{m-1}. \tag{15}$$

Отсюда сразу вытекает, что при любом i

$$(\exists x_i)(a_1x_1 + \ldots + a_ix_i + \ldots + a_mx_m = 0) \equiv \text{И}. \tag{16}$$

Далее, при $n \geqslant 2$ предикат

$$(\exists y)\left(\mathop{\&}_{1 \leqslant i \leqslant n} (a_1^ix_1^i + \ldots + a_{m_i}^ix_{m_i}^i + b_iy = 0)\right) \tag{17}$$

можно преобразовать следующим образом. Разрешаем уравнение

$$a_1^1 x_1^1 + \ldots + a_{m_1}^1 x_{m_1}^1 + b_1 y = 0 \tag{18}$$

относительно переменной y,

$$y = a_1^1 v x_1^1 + \ldots + a_{m_1}^1 v x_{m_1}^1, \tag{19}$$

где v — решение уравнения $b_1 x = p - 1$, и подставляем в предикат (17) правую часть равенства (19) вместо всех вхождений переменной y, отличных от первого ее вхождения. Так как предикаты (18) и (19) эквивалентны, то, используя эквивалентности типа (16), получаем, что предикат (17) эквивалентен предикату

$$\begin{aligned}
&(\exists y)\Big((a_1^1 x_1^1 + \ldots + a_{m_1}^1 x_{m_1}^1 + b_1 y = 0)\ \&\\
&\quad \& \mathop{\&}_{2\leqslant i\leqslant n} (a_1^i x_1^i + \ldots + a_{m_i}^i x_{m_i}^i + b_i a_1^1 v x_1^1 + \ldots + b_i a_{m_1}^1 v x_{m_1}^1 = 0)\Big) \equiv\\
&\equiv (\exists y)(a_1^1 x_1^1 + \ldots + a_{m_1}^1 x_{m_1}^1 + b_1 y = 0)\ \&\\
&\quad \& \mathop{\&}_{2\leqslant i\leqslant n} (a_1^i x_1^i + \ldots + a_{m_i}^i x_{m_i}^i + b_i a_1^1 v x_1^1 + \ldots + b_i a_{m_1}^1 v x_{m_1}^1 = 0) \equiv\\
&\quad \equiv \mathop{\&}_{2\leqslant i\leqslant n} (a_1^i x_1^i + \ldots + a_{m_i}^i x_{m_i}^i + b_i a_1^1 v x_1^1 + \ldots + b_i a_{m_1}^1 v x_{m_1}^1 = 0).
\end{aligned} \tag{20}$$

Из приведенных выкладок следует, что если отличный от диагонали предикат σ получен из предиката ρ с помощью $(\exists, \&)$-формулы Φ, то формулу Φ можно считать бескванторной, представляющей собой конъюнкцию предикатов вида (14).

Сделаем еще одно важное для дальнейшего замечание. Как видно из представлений (3) и (13) предиката ρ, сумма коэффициентов в левых частях равенств (3) и (13) равна нулю по модулю p. Очевидно, что это свойство для предикатов вида (14) сохраняется при перестановке и отождествлении переменных. Более того, если этим свойством обладали предикаты вида (14), входящие в формулу (17), то им будут обладать также и предикаты, входящие в последнюю формулу эквивалентностей (20). В самом деле, если сумма коэффициентов уравнения (18) равна нулю по модулю p, то по выбору числа v имеем

$$a_1^1 v + \ldots + a_{m_1}^1 v = 1 \pmod p. \tag{21}$$

Пользуясь теперь соотношениями (21) и

$$a_1^i + \ldots + a_{m_i}^i + b_i = 0 \pmod p,$$

заключаем, что

$$a_1^i + \ldots + a_{m_i}^i + b_i a_1^1 v + \ldots + b_i a_{m_1}^1 v = 0 \pmod p.$$

Итак, формула Φ, реализующая предикат σ, бескванторна и состоит из конъюнктивных сомножителей вида (14), где $a_1 + \ldots + a_m = 0 \pmod p$. При $m = 2$ и $a_1 + a_2 = 0 \pmod p$ предикат (14) совпадает с диагональю $x_1 = x_2$. Так как σ отличен от диагонали, то в формулу Φ должен входить хотя бы один сомножитель вида (14), где $m > 2$. Зафиксируем такой сомножитель (14) и, выразив переменную x_m в виде (15), подставим правую часть равенства (15) в формулу Φ вместо всех остальных вхождений переменной x_m

Полученную формулу обозначим через Ψ. Так как предикаты (14) и (15) эквивалентны, то формула Ψ реализует предикат σ. Представим ее в виде

$$\Psi = (a_1x_1 + \ldots + a_mx_m = 0) \mathbin{\&} \Psi_1, \tag{22}$$

где формула Ψ_1 не содержит переменной x_m. Обозначим через σ_1 предикат, который реализуется формулой Ψ_1. Далее рассмотрим две возможности.

Предикат σ_1 является диагональю. Из вида формулы (22) следует, что предикат σ в этом случае содержит повторяющиеся координаты. Как и в утверждении 2, проведем в предикате σ отождествление всех пар повторяющихся координат. При этом диагональ σ_1 обратится в тождественно истинный предикат, а соотношение (14) — в предикат вида

$$b_1x_1 + \ldots + b_tx_t = 0, \tag{23}$$

где $b_1 + \ldots + b_t = 0 \pmod p$.

В силу отличия предиката (23) от диагонали должно быть $t > 2$. Если $p = 2$, то, очевидно, $b_1 = \ldots = b_t = 1$, $t \geqslant 4$, и потому отождествлением переменных $x_4, \ldots, x_t$ из предиката (23) можно получить предикат (3). Если $p \geqslant 3$, то отождествлением переменных $x_3, \ldots, x_t$ получаем из предиката (23) трехместный предикат того же вида. Поэтому будем считать, что $t = 3$, и обозначим предикат $b_1x_1 + b_2x_2 + b_3x_3 = 0$ через $\sigma_2(x_1, x_2, x_3)$.

Предположим, что какие-либо два числа из множества $\{b_1, b_2, b_3\}$ совпадают. Пусть, например, $b_1 = b_2$. Обозначим через b_1^{-1} такой элемент из E_p, что $b_1 \cdot b_1^{-1} = 1 \pmod p$. Очевидно, что предикат $\sigma_2(x_1, x_2, x_3)$ эквивалентен предикату

$$b_1b_1^{-1}x_1 + b_2b_1^{-1}x_2 + b_3b_1^{-1}x_3 = 0, \tag{24}$$

т. е. предикату

$$x_1x_2 + b_3b_1^{-1}x_3 = 0. \tag{25}$$

Так как $1+1+b_3b_1^{-1} = 0 \pmod p$, то $b_3b_1^{-1} = p-2 \pmod p$. Иными словами, предикат (24) совпадает с предикатом (13).

Пусть все три числа b_1, b_2, b_3 различны. Так как предикат σ_2 эквивалентен предикату (24), то можно считать, $b_1 = 1$. Имеем

$$\begin{aligned}
&(\exists y)(\sigma_2(x_1, x_2, y) \mathbin{\&} \sigma_2(x_2, x_3, y)) \equiv \\
&\qquad \equiv (\exists y)((x_1 + b_2x_2 + b_3y = 0) \mathbin{\&} (x_2 + b_2x_3 + b_3y = 0)) \equiv \\
&\qquad\qquad \equiv (x_1 + b_2x_2 = x_2 + b_2x_3) \equiv (x_1 + (b_2 - 1)x_2 + (p - b_2)x_3 = 0).
\end{aligned}$$

Если числа 1, $b_2 - 1$, $p - b_2$ вновь различны, то применим указанную выше процедуру к предикату $x_1 + (b_2 - 1)x_2 + (p - b_2)x_3 = 0$, получим предикат $x_1 + (b_2 - 2)x_2 + (p - b_2 + 1)x_3 = 0$ и т. д., пока не придем к рассмотренному случаю двух равных коэффициентов. Итак, если σ_1 является диагональю, то с помощью подходящей $(\exists, \&)$-формулы из предиката σ можно получить предикат ρ.

Пусть теперь предикат σ_1 отличен от диагонали. Тогда из предиката σ получаем предикат σ_1:

$$\begin{aligned}
&(\exists x_m)\sigma \equiv (\exists x_m)((a_1x_1 + \ldots + a_mx_m = 0) \mathbin{\&} \sigma_1) \equiv \\
&\qquad\qquad \equiv (\exists x_m)(a_1x_1 + \ldots + a_mx_m = 0) \mathbin{\&} \sigma_1 \equiv \sigma_1,
\end{aligned}$$

который по сравнению с предикатом σ имеет по крайней мере на одну переменную меньше.

В заключение доказательства рассмотрим общий случай, когда $k = p^l$ и ρ — предикат из множества $L \cap \Pi_k$. Как установлено в § 2, тогда предикат ρ

изоморфен l-й декартовой степени предиката (3) при $p = 2$ или предиката (4) при $p \geqslant 3$, определенного на множестве E_p. Остается применить лемму 3.

Утверждение 4. *Всякий предикат из класса* $\mathbf{E}$ *минимален.*

Доказательство. Пусть $\rho(x_1, x_2)$ — нетривиальное отношение эквивалентности на E_k, имеющее h классов эквивалентных элементов, $1 < h < k$. Как показано в § 2, можно выбрать h-элементное множество E и эпиморфизм q из E_k в E такие, что предикат ρ будет являться полным эпиморфным прообразом предиката равенства (на E) при эпиморфизме q.

Пусть отличный от диагонали предикат σ получен из предиката ρ с помощью $(\exists, \&)$-формулы Φ. Через τ обозначим предикат, который получается из предиката равенства применением формулы Φ. Так как справедливы очевидные эквивалентности

$$(x_1 = \ldots = x_m) \;\&\; (x_{m+1} = \ldots = x_{m+n}) \equiv (x_1 = \ldots = x_{m+n}),$$
$$(\exists x_m)(x_1 = \ldots = x_m) \equiv \begin{cases} \text{И}, & \text{если } m = 2, \\ x_1 = \ldots = x_{m-1}, & \text{если } m > 2, \end{cases}$$

то предикат τ можно привести к виду

$$\tau \equiv (x_1 = \ldots = x_m). \tag{26}$$

В силу перестановочности операции взятия полного эпиморфного прообраза с операциями из Ω предикат σ есть полный эпиморфный прообраз предиката τ при эпиморфизме q, а в силу отличия предиката σ от полной диагонали в формуле (24) должно быть $m \geqslant 2$. Тогда отождествлением переменных из τ можно получить предикат $x_1 = x_2$. Пользуясь перестановочностью операции взятия полного эпиморфного прообраза с операцией отождествления переменных, заключаем, что из предиката σ отождествлением переменных можно получить полный эпиморфный прообраз предиката $x_1 = x_2$ при эпиморфизме q, т. е. предикат ρ. Утверждение доказано.

Утверждение 5. *Всякий предикат из класса* $\mathbf{C}$ *минимален.*

Доказательство. Пусть $\rho(x_1, \ldots, x_m)$ — центральный предикат, и пусть отличный от диагонали предикат σ получен из предиката ρ с помощью $(\exists, \&)$-формулы Φ. Замечаем, что

$$(\exists y)(\rho(x_1^1, \ldots, x_{m-1}^1, y) \;\&\; \ldots \;\&\; \rho(x_1^n, \ldots, x_{m-1}^n, y)) \equiv \text{И},$$

поскольку в качестве искомого значения переменной y всегда можно взять элемент центра предиката ρ. Следовательно, формулу Φ можно считать бескванторной. Далее, предикат ρ вполне рефлексивен, а предикат σ отличен от диагонали, поэтому в формулу Φ конъюнктивно входит хотя бы один сомножитель вида $\rho(x_1, \ldots, x_m)$ с попарно различными переменными $x_1, \ldots, x_m$. Заменим в предикате σ все переменные, отличные от переменных $x_1, \ldots, x_m$, переменной x_m. Тогда ввиду полной рефлексивности и полной симметричности предиката ρ в формуле Φ после замены переменных каждый конъюнктивный сомножитель будет эквивалентен либо предикату $\rho(x_1, \ldots, x_m)$, либо полному предикату. Значит, после указанного отождествления переменных из предиката σ получится предикат ρ. Утверждение доказано.

Утверждение 6. *При* $h \geqslant 3$ *предикат* $\tau_h(y_1, \ldots, y_h)$ *на* E_h *минимален.*

Доказательство. Пусть σ — отличный от диагонали предикат, который получен из предиката τ_h некоторой $(\exists, \&)$-формулой. Отождествлениями переменных строим из предиката σ такой отличный от диагонали предикат σ_1, чтобы при дальнейшем отождествлении любых двух переменных в предикате σ_1 получалась диагональ. Пусть предикат σ_1 реализуется

$(\exists,\&)$-формулой Φ. Предикат σ_1 зависит более чем от одной переменной: в противном случае в любой подформуле $\tau_h(y_1,\ldots,y_h)$ формулы Φ не более чем одна из переменных $y_1,\ldots,y_h$ является свободной. Поэтому если x — единственная переменная предиката σ_1, то, выбрав в качестве значений всех связанных переменных значение переменной x, мы в силу полной рефлексивности предиката τ_h придем к тому, что σ_1 — тождественно истинный предикат, что невозможно по предположению.

Предположим, что при некотором отождествлении переменных из предиката σ_1 можно получить неполную диагональ. Тогда, очевидно, подходящим отождествлением переменных из предиката σ_1 можно также получить диагональ вида $x_1 = x_2$. Пусть формула Φ_1, полученная отождествлением переменных из формулы Φ, реализует диагональ $x_1 = x_2$. Тогда любая подформула $\tau_h(y_1,\ldots,y_h)$ формулы Φ_1 в качестве свободных переменных может содержать лишь переменные x_1, x_2. Следовательно, если в формуле Φ_1 взять в качестве значений всех связанных переменных значение переменной x_1, то в силу неравенства $h \geqslant 3$ и полной рефлексивности предиката τ_h мы получим, что формула Φ_1 реализует тождественно истинный предикат, что невозможно по предположению.

Итак, при отождествлении любых двух переменных в предикате σ_1 получается полный предикат. Иными словами, предикат σ_1 вполне рефлексивен. Поэтому число переменных предиката σ_1, определенного на множестве E_h, не превосходит h. Если оно строго меньше h, то так же, как и в предыдущих случаях, взяв в качестве значений всех связанных переменных значение какой-либо одной переменной предиката σ_1, получим, что σ_1 — полный предикат. Следовательно, σ_1 — неполный вполне рефлексивный предикат от h переменных. В частности, σ_1 есть расширение предиката τ_h. Если σ_1 отличен от τ_h, т. е. не вполне симметричен, то предикат τ_h получаем в виде $\mathop{\&}\limits_{\pi} \sigma_1(x_{\pi(1)},\ldots,x_{\pi(h)})$, где конъюнкция распространяется по всем подстановкам π на множестве $\{1,2\ldots,h\}$. Утверждение доказано.

Следствие. *Всякий предикат из класса* $\mathbf{B}$ *минимален.*

Доказательство. Пусть $h \geqslant 3$ и $\rho(x_1,\ldots,x_h)$ — предикат на множестве E_k из класса $\mathbf{B}$. Тогда существуют такие натуральное число l и эпиморфизм из E_k в E_{h^l}, что ρ является полным эпиморфным прообразом l-й декартовой степени предиката τ_h, определенного на множестве E_h. В силу леммы 3 предикат τ_h^l является минимальным предикатом на множестве E_{h^l}. Чтобы далее применить лемму 4 к предикатам ρ и τ_h^l, следует убедиться в том, что из предиката τ_h^l с помощью $(\exists,\&)$-формулы невозможно получить неполную диагональ. В самом деле, если это не так, то посредством $(\exists,\&)$-формулы Φ из предиката τ_h^l можно получить диагональ вида $x_1 = x_2$. Замечаем, что если l-я декартова степень некоторого предиката $\omega(x_1,x_2)$, заданного на E_h, есть диагональ $x_1 = x_2$, то и предикат $\omega(x_1,x_2)$ совпадает с диагональю $x_1 = x_2$. Поэтому, пользуясь перестановочностью операции взятия декартовой степени с операциями из Ω, находим, что с помощью $(\exists,\&)$-формулы Φ из предиката τ_h можно получить диагональ вида $x_1 = x_2$. Как мы убедились при доказательстве утверждения 6, это невозможно. Значит, из предиката τ_h^l с помощью $(\exists,\&)$-формулы нельзя получить неполную диагональ, и лемма 4 применима к предикатам ρ и τ_h^l. Следствие доказано.

Несложно показать, что различным предикатам из множества $\mathbf{P}\cup\mathbf{O}\cup\cup\mathbf{L}\cup\mathbf{E}\cup\mathbf{C}\cup\mathbf{B}$ соответствуют различные предполные классы. Ввиду имеющего место соответствия Галуа для этого достаточно установить, что различные минимальные предикаты невозможно перевести друг в друга с помощью $(\exists,\&)$-формул. Приемы, изложенные при доказательстве утверждений 1–6, позволяют устанавливать это для всех случаев пар минимальных предикатов, отличных от пары минимальных предикатов из класса $\mathbf{B}$ с одним и тем же числом переменных. В этом случае необходимы дополнительные рассуждения, связанные с группами автоморфизмов предикатов.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Каргаполов М. И., Мерзляков Ю. Л. Основы теории групп. — М.: Наука, 1972.
3. Кудрявцев В. Б. Функциональная система. — Математическая энциклопедия. Т. 5. — М.: Советская энциклопедия, 1985. — С. 694–696.
4. 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.
5. Кузнецов А. В. Структуры с замыканием и критерии функциональной полноты // Успехи матем. наук. — 1961. — Т. XVI, № 2 (98). — С. 201–202.
6. Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. Вып. 3. — М.: Физматгиз, 1960. — С. 49–60.
7. Марченков С. С. О полноте в системе $P_3 \times P_3$ // Дискретная математика. — 1992. — Т. 4, вып. 1. — С. 126–145.
8. Оре О. Теория графов. — М.: Наука, 1968.
9. Риге Ж. Бинарные отношения, замыкания, соответствия Галуа // Кибернетич. сб. Вып. 7. — М.: ИЛ, 1963. — С. 129–185.
10. Ромов Б. А. Алгебры частичных функций и их инварианты // Кибернетика. — 1981. — № 2. — С. 1–11.
11. Ромов Б. А. О полноте на квадрате функций алгебры логики и в системе $P_k \times P_l$ // Кибернетика. — 1987. — № 4. — С. 9–14.
12. Ромов Б. А. Об одной серии максимальных подалгебр прямых произведений алгебр конечнозначных логик // Кибернетика. — 1989. — № 3. — С. 11–16.
13. Ромов Б. А. О функциональной полноте в системе $P_2 \times P_k$ // Кибернетика. — 1991. — № 1. — С. 1–8.
14. Яблонский С. В. О функциональной полноте в трехзначном исчислении // Доклады АН СССР. — 1954. — Т. 95, № 6. — С. 1152–1156.
15. Яблонский С. В. Функциональные построения в k-значной логике // Труды матем. ин-та АН СССР. — 1958. — Т. 51. — С. 5–142.
16. Яблонский С. В. О некоторых результатах в теории функциональных систем // Труды международного конгресса математиков, Хельсинки, 1978. — С. 963–971.
17. Яблонский С. В., Гаврилов Г. П., Набебин Л. А. Анализ и синтез схем в многозначных логиках. Ч. 1. — М.: Изд-во МЭИ, 1989.
18. Krasner M. Remarque au sujet de «Une generalisation de la notion de corps» // Journ. de Math. — 1938. — P. 367–385.
19. Krasner M. Generalisation abstraite de la théorie de Galois // Colloques internationaux du Centre National R. S. Algèbre et théorie des nombres. — Paris. — 1949. — V. XXIV. — P. 163–165.
20. Lo Czukai. The precompleteness of the linear function set and the ring // Acta Sci. Natur. Univ. Jiliensis. — 1963. — V. 2. — P. 1–14 (Chinese).
21. Lo Czukai. On the precompleteness of the classes of functions preserving a partition // Acta Sci. Natur. Univ. Jiliensis. — 1963. — V. 2. — P. 105–116 (Chinese).
22. Lo Czukai. Precomplete classes defined by normal k-ary relations in k-valued logics // Acta Sci. Natur. Univ. Jiliensis. — 1964. — V. 3. — P. 39–50 (Chinese).
23. Lo Czukai, Lo Sjui-Kua. Precomplete classes determined by binary relations in many-valued logics // Acta Sci. Natur. Univ. Jiliensis. — 1964. — V. 4. — P. 27–33 (Chinese).
24. Post E. L. Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43. — P. 163–185.
25. Post E. L. Two-valued iterative systems of mathematical logic // Annals of Math. Studies. — 1941. — V. 5.
26. Rosenberg I. G. La structure des fonctions de plusieurs variables sur un ensemble fini // C. R. Acad. Sci. Paris. Ser. A. B. — 1965. — V. 260. — P. 3817–3819.
27. Rosenberg I. G. Maximal clones on algebras A ana A^r // Rendiconti del sircolo mathematico du Palermo, Ser II. — 1969. — V. 18. — P. 329–333.
28. Rosenberg I. G. Über die funktionale Vollständigkeit in den mehrwertigen Logiken // Rozpr. ČSAV Řada Math. Přír. Věd. — Praha. — 1970. — № 80 (4). — S. 3–93.

Поступило в редакцию 3 XI 1992