Доклады Академии наук СССР
1971. Том 201, № 1

УДК 51:621.391

МАТЕМАТИКА

Г. Н. БЛОХИНА, В. Б. КУДРЯВЦЕВ

О БАЗИСНЫХ ГРУППАХ В k-ЗНАЧНЫХ ЛОГИКАХ

(Представлено академиком А. А. Дородницыным 15 IV 1971)

В заметке изучаются вопросы, связанные с проблемой полноты в k-значных логиках.

1. Одним из возможных путей решения задачи о полноте является, как известно ([1]), отыскание всех предполных классов в данной конечно-значной логике P_k. Однако, как показано в работе ([2]), число предполных классов довольно быстро растет с увеличением k, что автоматически ограничивает практические возможности подобных критериев полноты. В связи с этим особый интерес вызывают исследования на полноту систем, обладающих некоторыми наперед заданными и в то же время достаточно общими свойствами. К числу таковых относятся, например, системы, состоящие из одноместных функций и существенной функции. Различные варианты этой задачи были рассмотрены в работах ([1, 3, 4]). В предлагаемой заметке решается задача А. Саломаа ([3]), в которой требуется описать все группы подстановок, каждая из которых вместе с любой существенной функцией образует полную систему, т. е. так называемые базисные группы. Известно ([3]), что базисные группы существуют лишь при $k \geqslant 5$, поэтому мы ограничиваемся рассмотрением только таких k.

2. Обозначим через E_k множество $\{0, 1, \ldots, k-1\}$, $k \geqslant 5$, и через P_k — множество всех функций, аргументы которых и сами функции принимают значения из E_k. Множество P_k с введенными в нем операциями суперпозиции называется *k-значной логикой*. Множество, состоящее из всех функций, получающихся из функций множества $\mathfrak{M}$ при помощи операции суперпозиции, называется *замыканием множества* $\mathfrak{M}$. Множество $\mathfrak{M}$ называется *замкнутым*, если оно совпадает со своим замыканием, и называется *полным*, если его замыкание совпадает с P_k. Функция из P_k называется *существенной*, если она принимает все значения из E_k и существенно зависит не менее, чем от двух переменных. Одноместная функция, принимающая все значения из E_k, называется *подстановкой*. Множество подстановок с операцией суперпозиции образует *группу*, которую мы обозначим через S_k. Группа $\Pi \subseteq S_k$ называется *базисной*, если она вместе с любой существенной функцией образует полную систему, и *предбазисной*, если она не базисна, но всякая группа, содержащая ее и отличная от нее, уже является базисной. Очевидно, подгруппа базисная тогда и только тогда, когда она не является подгруппой ни одной предбазисной группы. Таким образом, описание базисных групп эквивалентно указанию всех предбазисных групп. Целью этой заметки является указание всех предбазисных групп.

Пусть $R(y_1, y_2, \ldots, y_h)$ — h-местный предикат, аргументы которого принимают значения из E_k. Подстановка $s(x)$ из S_k сохраняет предикат R, если формула $R(y_1, y_2, \ldots, y_h) \to R(s(y_1), s(y_2), \ldots, s(y_h))$ является истинной при всех значениях переменных $y_1, y_2, \ldots, y_h$. Множество всех подстановок, сохраняющих предикат R, которое, очевидно, замкнуто, обозначим через $\Pi(R)$. Два предиката $R_1(y_1, y_2, \ldots, y_h)$ и $R_2(y_1, y_2, \ldots, y_h)$ называются *изоморфными*, если для некоторой подстановки $s(x)$ из S_k

имеет место $R_1(s(y_1), s(y_2), \ldots, s(y_h)) = R_2(y_1, y_2, \ldots, y_h)$. Отношение изоморфизма, очевидно, является отношением эквивалентности. Рассмотрим четыре специальных семейства предикатов.

Семейство Г. Пусть задано натуральное число r, $1 < r < k$, $r \neq k/2$, и выбрано подмножество $\{i_1, i_2, \ldots, i_r\} \subseteq E_k$. Семейство Г для каждого r содержит предикат $R(y)$, область истинности которого состоит из точек $i_1, i_2, \ldots, i_r$, все ему изоморфные предикаты и только их.

Семейство A. Пусть r — делитель k, $r \neq 1$, $r \neq k$. Рассмотрим разбиение $E_k = E^{(1)} \cup E^{(2)} \cup \ldots \cup E^{(k/r)}$, где $E^{(i)} \cap E^{(j)} = \phi$ при $i \neq j$, $i, j = 1, 2, \ldots, k/r$, и мощности компонент равны r. Пусть $R(y_1, y_2)$ предикат, истинный в точках (a, b) таких, что $a \neq b$ и для некоторого i $\{a, b\} \subseteq E^{(i)}$, и ложный в остальных точках. Семейство A для каждого r содержит предикат $R(y_1, y_2)$, все ему изоморфные и только их.

Семейство L. Это семейство не пусто только при $k = p^m$, где простое $p \geqslant 2$. Пусть $k = p^m$ и $G = \langle E_k, + \rangle$ — абелева группа, в которой каждый ненулевой элемент имеет простой порядок p.

При $p = 2$ рассмотрим предикат $R_G(y_1, y_2, y_3, y_4)$, истинный в тех и только тех точках, для которых $y_1 + y_2 = y_3 + y_4$ и $y_i \neq y_j$ при $i \neq j$, $i, j = 1, 2, 3, 4$. При указанном p семейство L содержит для каждой описанной группы G предикат $R_G(y_1, y_2, y_3, y_4)$, все изоморфные ему предикаты и только их.

При $p \neq 2$ рассмотрим предикат $R_G(y_1, y_2, y_3)$, истинный в тех и только тех точках, для которых $y_3 = 2^{-1}(y_1 + y_2)$, где 2^{-1} — такое число из E_p, для которого $2 \cdot 2^{-1} \equiv 1 \pmod p$, $y_i \neq y_j$ при $i \neq j$, $i, j = 1, 2, 3$. При указанном p семейство L содержит для каждой описанной группы G предикат $R_G(y_1, y_2, y_3)$, все изоморфные ему предикаты и только их.

Семейство I. Это семейство не пусто только при $k = h^m$, где $h \geqslant 5$, $m > 1$. Пусть $k = h^m$, обозначим через $[a]_l$ l-й коэффициент в разложении $a = \sum_{l=0}^{m-1} [a]_l h^l$, $a \in E_k$, $[a]_l \in E_h$. Для указанных h и m рассмотрим предикат $R(y_1, y_2)$, истинный в точках (a, b), для которых $[a]_l \neq [b]_l$ при любом $l = 0, 1, \ldots, m-1$, и ложный в остальных точках. Семейство I содержит при каждых указанных h и m предикат $R(y_1, y_2)$, все изоморфные ему предикаты и только их. Обозначим через $V = \Gamma \cup A \cup L \cup I$ и сформулируем наши основные предложения.

Теорема 1. *Группа $\Pi \subseteq S_k$ является базисной тогда и только тогда, когда Π не сохраняет ни одного предиката из V.*

Теорема 2. *Группа $\Pi \subseteq S_k$ является предбазисной тогда и только тогда, когда для некоторого предиката $R \in V$ $\Pi = \Pi(R)$.*

Для предикатов R из семейств Г, A и I введем понятие типа $\tau(R)$, которое является числом r, участвующим в определении R, если $R \in \Gamma \cup A$, и, аналогично,— числом h, если $R \subset I$. Факт сопряженности групп Π_1 и Π_2 из S_k обозначим через $\Pi_1 \sim \Pi_2$.

Теорема 3. *Пусть $R_1, R_2 \in V$; тогда, если:*

а) *R_1 и R_2 из разных семейств Г, A, L, I, то неверно, что $R_1 \sim R_2$;*

б) *$R_1, R_2 \in \Gamma$, то $R_1 \sim R_2$ эквивалентно тому, что $\tau(R_1) = \tau(R_2)$ или $\tau(R_1) + \tau(R_2) = k$;*

в) *$R_1, R_2 \in A$, то $R_1 \sim R_2$ эквивалентно $\tau(R_1) = \tau(R_2)$;*

г) *$R_1, R_2 \in L$, то $R_1 \sim R_2$;*

д) *$R_1, R_2 \in I$, то $R_1 \sim R_2$ эквивалентно $\tau(R_1) = \tau(R_2)$.*

Пусть $\mathfrak{R}$ — множество предикатов; обозначим через $\overline{\mathfrak{R}}$ множество всех групп подстановок Π таких, что для некоторого R из $\mathfrak{R}$ $\Pi = \Pi(R)$. Следуя ([5]), назовем размерностью группы подстановок Π (обозначение: $\dim \Pi$) наименьшее число переменных у предикатов $R(y_1, y_2, \ldots, y_h)$ таких, что $\Pi = \Pi(R)$.

Т е о р е м а 4. *Пусть* $\Pi \subseteq S_k$ — *базисная группа; тогда*

а) $\dim \Pi = 1$, *если* $\Pi \in \overline{\Gamma}$;

б) $\dim \Pi = 2$, *если* $\Pi \in \overline{A} \cup \overline{I}$;

в) $\dim \Pi = 3$, *если* $\Pi \in \overline{L}$ *и* $k = p^m$, $p > 2$;

г) $\dim \Pi = 4$, *если* $\Pi \in \overline{L}$ *и* $k = p^m$, $p = 2$.

Приведем одно простое достаточное условие базисности группы подстановок.

Т е о р е м а 5. *Группа* $\Pi \subseteq S_k$ *является базисной, если она*

а) *4-транзитивна при* $k = 2^m$, $m > 2$;

б) *3-транзитивна при* $k = p^m$, p — *простое*, $p \neq 2$, $m \geqslant 1$;

в) *2-транзитивна при* $k \neq p^m$, p — *простое*, $m \geqslant 1$.

Отметим, что в общем случае степень транзитивности в каждом из пунктов а), б), в) последней теоремы не может быть уменьшена.

Доказательство изложенных результатов опирается на ряд вспомогательных утверждений, а также на теорему И. Розенберга (6) и некоторые предложения работ (1).

Вычислительный центр
Академии наук СССР
Москва

Поступило
15 IV 1971

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] С. В. Яблонский, Тр. Матем. инст. им. В. А. Стеклова АН СССР, 51, 5 (1958). [2] Е. Ю. Захарова, В. Б. Кудрявцев, С. В. Яблонский, ДАН, 186, № 3, 509 (1969). [3] A. Salomaa, Ann. Acad. Sci., Fennical., Ser. AJ, 338, 1 (1964). [4] Р. А. Байрамов, ДАН, 189, № 3, 455 (1969). [5] Г. Н. Блохина, Сборн. Дискретный анализ, в. 16, 1970, стр. 16. [6] J. Rosenberg, C. R., 260, Groupe 1, 5, IV (1965).