

В. Б. КУДРЯВЦЕВ

ОТНОСИТЕЛЬНО S -СИСТЕМ ФУНКЦИЙ k -ЗНАЧНОЙ ЛОГИКИ

(Представлено академиком А. А. Дородницыным 5 I 1971)

В заметке рассматриваются вопросы, связанные с проблемой полноты и со свойствами структуры замкнутых классов в k -значной логике.

1°. Одним из возможных путей решения задачи о полноте является, как известно ⁽¹⁾, отыскание всех предполных классов в данной конечнозначной логике P_k . Первые исследования такого рода были проведены Е. Постом, С. В. Яблонским и А. В. Кузнецовым ^(1, 2). В работе ⁽¹⁾, в частности, была установлена конечность числа предполных классов в P_k и доказано, что множество функций является полным в P_k тогда и только тогда, когда оно не содержится ни в одном предполном классе; наряду с этим в ней были эффективно описаны некоторые семейства предполных классов. Позже различными авторами были найдены новые семейства ⁽³⁻⁶⁾. Окончательный список предполных классов удалось установить И. Розенбергу ⁽⁷⁾. Исследования, проведенные в ⁽⁸⁾, показали, что число предполных классов уже при $k = 5$ столь велико, что использование критерия полноты в терминах предполных классов становится практически невозможным. 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 содержащих существенную функцию. Различные варианты этой задачи были рассмотрены в работах ⁽⁹⁻¹¹⁾. В предполагаемой заметке рассматривается задача о полноте S -систем, обобщающая постановки задач упомянутых работ.

2°. Обозначим через E_k множество $\{0, 1, \dots, k-1\}$, $k \geq 2$, и через P_k — множество всех функций $f(x_1, x_2, \dots, x_n)$, аргументы которых и сами функции принимают значения из E_k . Множество P_k с введенными в нем операциями суперпозиции называется k -значной логикой. Функция f из P_k называется S -функцией, если она принимает все k значений; S -функция называется существенной, если она существенно зависит не менее, чем от двух аргументов. Множество, элементами которого являются только S -функции, называется S -множеством. S -замыканием S -множества M называется множество $[M]_S$ всех S -функций, которые получаются из функций множества M при помощи операций суперпозиции. Нетрудно видеть, что для любых S -множеств имеет место $[M]_S \supseteq M$, $[[M]_S]_S = [M]_S$ и если $M_1 \supseteq M_2$, то $[M_1]_S \supseteq [M_2]_S$. S -множество M называется S -замкнутым, если $M = [M]_S$. S -полным, если $[M]_S$ содержит все S -функции из P_k , и S -предполным, если оно не является S -полным, но для любой S -функции $f \notin M$ множество $M \cup \{f\}$ является S -полным. Нетрудно видеть, что, для того чтобы S -множество было S -полным, необходимо и достаточно, чтобы оно не содержалось ни в одном S -предполном S -множестве. Пусть $R(y_1, y_2, \dots, y_n)$ — n -местный предикат, аргументы которого принимают значения из E_k . Функция $f(x_1, x_2, \dots, x_n) \in P_k$ сохраняет предикат R , если формула

$$R(z_{11}, z_{12}, \dots, z_{1n}) \& R(z_{21}, z_{22}, \dots, z_{2n}) \& \dots \& R(z_{n1}, z_{n2}, \dots, z_{nn}) \rightarrow \\ \rightarrow R(f(z_{11}, z_{21}, \dots, z_{n1}), f(z_{12}, z_{22}, \dots, z_{n2}), \dots, f(z_{1n}, z_{2n}, \dots, z_{nn}))$$

является истинной при всех значениях переменных z_{ij} , $i = 1, 2, \dots, n$; $j =$

$= 1, 2, \dots, h$. Множество $\mathfrak{M}$ сохраняет предикат R , если каждая функция из $\mathfrak{M}$ сохраняет R . Множество всех S -функций, сохраняющих R , обозначим через $S(R)$. Рассмотрим шесть специальных семейств предикатов.

Семейство Γ . Пусть $\{i_1, i_2, \dots, i_r\} \subseteq E_k$, $1 \leq r < k$; рассмотрим предикат $R(y)$, истинный в точках $i_1, i_2, \dots, i_r$ и ложный в остальных точках. Семейство Γ состоит из всех предикатов $R(y)$, соответствующих указанным подмножествам E_k , и только из них.

Семейство A . Пусть $E_k = E^1 \cup E^2 \cup \dots \cup E^l$, где $1 < l < k$, $E^i \cap E^j = \emptyset$ при $i \neq j$. Рассмотрим предикат $R(y_1, y_2)$, истинный в точках (a, b) таких, что при некотором $a, b \in E^i$, и ложный в остальных точках. Семейство A состоит из всех предикатов $R(y_1, y_2)$, соответствующих указанным разбиениям множества E_k , и только из них.

Семейство L . Это семейство не пусто только при $k = p^m$, где p простое. 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 точках (a, b, c, d) таких, что $a + b = c + d$, и ложный в остальных точках. При указанном p L содержит для каждой описанной группы G предикат $R_G(y_1, y_2, y_3, y_4)$ и только такие предикаты. Пусть $p \neq 2$. Рассмотрим предикат $R_G(y_1, y_2, y_3)$, истинный в точках (a, b, c) , для которых $c = 2^{-1}(a + b)$, где 2^{-1} — такое число из E_p , для которого $2 \cdot 2^{-1} \equiv 1 \pmod{p}$, и ложный в остальных точках. При указанном p L содержит для каждой описанной группы G предикат $R_G(y_1, y_2, y_3)$ и только такие предикаты.

h -Местные предикаты R_1 и R_2 называются изоморфными, если существует такая подстановка $\sigma(x) \in P_h$, что для любого набора $(a_1, a_2, \dots, a_h)$ истинность $R_1(a_1, a_2, \dots, a_h)$ эквивалентна истинности $R_2(\sigma(a_1), \sigma(a_2), \dots, \sigma(a_h))$.

Семейство I . Это семейство не пусто только при $k = h^m$, где $h \geq 5$, $m > 1$. Пусть $k = h^m$, обозначим через $[a]_l$ l -й коэффициент в разложе-

нии $a = \sum_{l=0}^{m-1} [a]_l h^l$, $a \in E_k$, $[a]_l \in E_h$. 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 $l = 0, 1, \dots, m-1$, и ложный в остальных точках. Семейство I содержит при каждом h и m предикат R , все изоморфные ему предикаты и только их.

Семейство N содержит каждый предикат $R(y_1, y_2)$, область истинности которого является графиком подстановки $\sigma(x) \in P_h$, разлагающейся в произведение циклов одинаковой простой длины, не меньшей двух, и только такие предикаты.

Семейство B не пусто при $k \geq 5$ и состоит из одного двуместного предиката $R^*(y_1, y_2)$, истинного только в точках (a, b) таких, что $a \neq b$.

Обозначим через $W = \Gamma \cup A \cup L \cup I \cup N \cup B$.

Теорема 1. S -множество является S -полным тогда и только тогда, когда оно не сохраняет ни одного предиката из множества W .

Теорема 2. S -множество $\mathfrak{M}$ является S -предполным тогда и только тогда, когда для некоторого предиката $R \in W$ имеет место $S(R) = \mathfrak{M}$.

Интересно отметить, что для любого $R \in N \cup B$ множество $S(R)$ является конечным (с точностью до переименования переменных), для остальных $R \in W \setminus (N \cup B)$ множество $S(R)$ бесконечно. Для предикатов $R_1, R_2 \in I$ будем писать $R_1 \sim R_2$, если подстановка, определяемая одним из этих предикатов, является степенью другой; аналогично для $R_{G_1}, R_{G_2} \in L$ будем писать $R_{G_1} \approx R_{G_2}$, если для групп $G_1 = \langle E_k, + \rangle$ и $G_2 = \langle E_k, \oplus \rangle$ при некотором фиксированном $c \in E_h$ для любых элементов a и b имеет место $a \oplus b = a + b + c$.

Теорема 3. Пусть $R_1, R_2 \in W$, тогда если:

а) R_1 и R_2 из разных семейств Γ, A, L, I, N, B , то $S(R_1) \neq S(R_2)$;

б) $R_1, R_2 \in \Gamma \cup A \cup I$, то при $R_1 \neq R_2$ $S(R_1) \neq S(R_2)$;

в) $R_1, R_2 \in N$, то $S(R_1) = S(R_2)$ эквивалентно $R_1 \sim R_2$;

г) $R_1, R_2 \in L$, то $S(R_1) = S(R_2)$ эквивалентно $R_1 \approx R_2$.

Приведем более компактный по форме критерий S -полноты, который является, конечно, менее сильным, чем теорема 1. Назовем S -множество $\mathfrak{M}$ r -транзитивным (r — степень транзитивности), если для любого r -местного предиката R такого, что $S(R)$ отлично от класса всех S -функций, имеет место $\mathfrak{M} \not\subseteq S(R)$. На основании теоремы 1 может быть установлена

Теорема 4. S -множество является S -полным тогда и только тогда, когда оно

а) 4-транзитивно при $k = 2^n$, $n \geq 1$;

б) 3-транзитивно при $k = p^m$, p простое, $p \neq 2$, $m \geq 1$;

в) 2-транзитивно при $k \neq p^m$, p простое, $m \geq 1$.

Отметим, что в общем случае степень транзитивности в каждом из пунктов а), б) и в) не может быть уменьшена. Обозначим через $s(k)$ число S -предполных множеств.

Теорема 5. $\ln s(k) \sim k \ln k$.

Обозначим через $f^\sigma(x_1, x_2, \dots, x_n) = \sigma(f(\sigma^{-1}(x_1), \sigma^{-1}(x_2), \dots, \sigma^{-1}(x_n)))$ и назовем функцию f^σ двойственной к функции f относительно подстановки $\sigma(x)$, аналогично через $\mathfrak{M}^\sigma$ обозначим множество всех функций, двойственных к функциям из $\mathfrak{M}$ относительно $\sigma(x)$. Множества функций $\mathfrak{M}_1$ и $\mathfrak{M}_2$ называются двойственными, если для некоторой подстановки $\sigma(x)$ имеет место $\mathfrak{M}_1 = \mathfrak{M}_2^\sigma$. Отношение двойственности разбивает множество всех S -предполных S -множеств на классы эквивалентности. Нетрудно описать все эти классы. Пусть $e(k)$ — число указанных классов (или типов соответствующих предикатов).

Теорема 6. $\ln e(k) \sim c\sqrt{k}$, $c = \pi\sqrt{2}/3$.

Система S -замкнутых S -множеств образует структуру по включению, которая наряду с особенностями обладает рядом существенных свойств, сближающих ее со структурой всех замкнутых в обычном смысле классов в P_n .

Теорема 7. Мощность множества S -замкнутых S -множеств счетна при $k = 2$ и равна континууму при $k \geq 3$.

Подмножество $\mathfrak{M}$ S -замкнутого S -множества $\mathfrak{N}$ называется базисом в $\mathfrak{N}$, если $[\mathfrak{M}]_S = \mathfrak{N}$ и для любого $\mathfrak{M}' \subset \mathfrak{M}$ $[\mathfrak{M}']_S \neq \mathfrak{N}$.

Теорема 8. а) При $k = 2$ каждое S -замкнутое S -множество имеет конечный базис и мощность любого базиса не превосходит трех;

б) при любом $k \geq 3$ существуют S -замкнутые S -множества, имеющие базис любой конечной и счетной мощностей, а также не имеющие базиса.

Подсчет, аналогичный проведенному в (8), показывает, что нашим критерием S -полноты, учитывая сравнительно медленный рост числа типов и логическую простоту предикатов, можно пользоваться до $k = 6$, а в терминах типов — до $k = 12$ соответственно. Доказательство изложенных результатов опирается на ряд вспомогательных утверждений, а также на теорему И. Розенберга (7, 12) и некоторые предложения работы (1).

Вычислительный центр
Академии наук СССР
Москва

Поступило
28 XII 1970

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ С. В. Яблонский, Тр. Матем. инст. им. В. А. Стеклова АН СССР, 51, 5 (1958). ² E. Post, Two-valued Iterative Systems, 1941. ³ В. В. Мартынюк, Сборн. Проблемы кибернетики, в. 3, 1960, стр. 49. ⁴ Ло Джун-кай, Acta sci. natur. Univ. Pekinensis, № 3 (1964). ⁵ Ло Чжу-кай, Лю Сюй-хуа, ibid, № 4 (1963). ⁶ Е. Ю. Захарова, Сборн. Проблемы кибернетики, в. 18, 1966, стр. 5. ⁷ J. Rosenberg, C. R. 260. Groupe 1, 5, IV (1965). ⁸ Е. Ю. Захарова, В. Б. Кудрявцев, С. В. Яблонский, ДАН, 186, № 3, 509 (1969). ⁹ A. Salomaa, Ann. Acad. Sci. Fennicae, Ser. A1, № 338, 1 (1964). ¹⁰ G. Rousseau, Proc. Am. Math. Soc., 18, 1009 (1967). ¹¹ Р. А. Байрамов, ДАН, 189, № 3, 455 (1969). ¹² J. Rosenberg, Rev. Roum. Math. Pures et Appl., 14, № 3, 413 (1969).