

УДК 511.172, 510.52

РАСПОЗНАВАНИЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОРОЖДАЕМЫХ КОНСЕРВАТИВНЫМИ ФУНКЦИЯМИ

О. Е. Сергеева

Пусть K — класс функций вида $f : R^n \rightarrow R$, где $n = 1, 2, 3, \dots$, и $S(K, N)$ — множество начальных отрезков длины N рекуррентных последовательностей, построенных при помощи функций из K . Рассматривается задача распознавания свойства « $x \in S(K, N)$ » для произвольной последовательности $x \in R^N$. В случае, когда K — класс консервативных функций над кольцом $R = \mathbb{Z}_{p^n}$, предлагается алгоритм решения этой задачи, битовая сложность которого $O(N \log^2 N)$.

Ключевые слова: *схема, функциональные элементы, рекуррентные последовательности, консервативные функции.*

Задача распознавания последовательностей состоит в том, чтобы по заданной последовательности сказать, возможно ли её построить рекуррентно при помощи функции из определённого класса. Так, для распознавания свойства линейности над полем используется алгоритм Берлекэмп — Мессе [1, 2], обобщённый в работах В. Л. Куракина [3] для колец и модулей.

В работах В. С. Анашина [4] предложено для построения рекуррентных последовательностей использовать полиномиальные, дифференцируемые и консервативные функции над кольцом. Такие функции имеют эффективную программную и аппаратную реализацию. В связи с этим в работе рассматриваются функции, сохраняющие систему эквивалентностей, частным случаем которых являются консервативные.

Пусть Ω — конечное множество булевых функций, которое назовём базисом. *Схема из функциональных элементов* [5] — это ориентированный граф без циклов, где каждый вход помечен некоторой переменной, остальные вершины помечены базисными функциями. Если вершина помечена функцией от n аргументов, то её полустепень захода равна n . *Сложностью* схемы назовем число вершин в ней.

Пусть R — конечное k -элементное множество; R^* — множество всех бесконечных последовательностей с элементами из R ; P_R — класс всех функций вида $f : R^n \rightarrow R$ при $n = 1, 2, 3, \dots$.

Определение 1. Последовательность $x_1 x_2 x_3 \dots \in R^*$ называется *рекуррентной над классом* $K \subseteq P_R$, если для некоторого n существует функция f от n аргументов в классе K , такая, что $f(x_i, \dots, x_{n+i-1}) = x_{n+i}$ при всех $i = 1, 2, 3, \dots$.

Для любого целого положительного N обозначим через $S(K, N)$ множество начальных отрезков длины N рекуррентных последовательностей над классом функций K . Далее рассматривается задача распознавания свойства « $x \in S(K, N)$ » для $x \in R^N$. Нас интересует сложность алгоритма, решающего данную задачу, как функция растущего N . Назовём $S(K, N)$ -*схемой* схему из функциональных элементов, которая распознает названное выше свойство. При этом предполагается, что буквы алфавита R кодируются двоичными наборами фиксированной длины s и последовательности подаются на вход схемы в закодированном виде — наборами длины Ns .

Перейдём к описанию класса K .

Определение 2. Пусть $\varepsilon \subset R^l$ — отношение на множестве R , $A \subseteq R^n$. Частичная функция $f : A \rightarrow R$ *сохраняет отношение* ε , если для любых наборов $(x_{11}, \dots, x_{1l})$, $\dots$, $(x_{n1}, \dots, x_{nl})$, удовлетворяющих отношению ε и таких, что функция f определена

на наборах $(x_{11}, \dots, x_{n1}), \dots, (x_{1l}, \dots, x_{nl})$, набор $(f(x_{11}, \dots, x_{n1}), \dots, f(x_{1l}, \dots, x_{nl}))$ также удовлетворяет ε .

Пусть $\varepsilon = \{\varepsilon_1, \dots, \varepsilon_m\}$ — система эквивалентностей на множестве R , такая, что $\varepsilon_1 \supseteq \varepsilon_2 \supseteq \dots \supseteq \varepsilon_m$, и $P_R^{(n)}(\varepsilon)$ — класс функций от n аргументов, сохраняющих все эквивалентности из ε . Если $R = \mathbb{Z}_{p^m}$ и ε — система сравнимостей по модулям $p, p^2, \dots, p^{m-1}$, то $P_R^{(n)}(\varepsilon)$ — это класс консервативных функций. Будем решать поставленную задачу для класса $K = P_R^{(n)}(\varepsilon)$. Важной является следующая

Лемма 1. Пусть $A \subseteq R^n$. Частичная функция $f : A \rightarrow R$, сохраняющая все эквивалентности из ε , может быть продолжена до полностью определенной функции в классе $P_R^{(n)}(\varepsilon)$.

Лемма 1 позволяет построить последовательность $S(K, N)$ -схем сложности $O(N^2)$.

Теорема 1. Для любого n существует последовательность $S(K, N)$ -схем сложности $O(N \log^2 N)$.

ЛИТЕРАТУРА

1. Berlekamp E. R. Algebraic Coding Theory. New York: Mc Craw-Hill, 1968. (Пер.: Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.)
2. Massey J. L. Shift-register synthesis and BCH decoding // IEEE Trans. Inform. Theory. 1969. V. 15. No 1. Part 1. P. 122–127.
3. Куракин В. Л. Алгоритм Берлекэмпа — Мэсси над конечными коммутативными кольцами // Проблемы передачи информ. 1999. № 35. С. 38–50.
4. Анашин В. С. Равномерно распределенные последовательности целых p -адических чисел // Математические заметки. 1994. Т. 55. № 2. С. 3–46.
5. Wegener I. The Complexity of Boolean Functions. John Wiley & Sons Ltd, 1987.