ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 **МАТЕМАТИКИ** **Выпуск 3**
2012

И. В. Чередник (Москва, ТВП). **Рекурсивно определяющие модули для полилинейных последовательностей.**

Линейной сложностью линейной рекуррентной последовательности (сокращенно ЛРП) над коммутативным кольцом называют степень ее минимального многочлена. При определении линейной сложности для полилинейной рекуррентной последовательности (сокращенно k-ЛРП, или просто ЛРП) возникает ситуация, когда это определение можно дать несколькими способами. Так, в работе [2] было введено 20 определений линейной сложности последовательности. Эти определения можно разбить на группы, характеризующие различные алгебраические и комбинаторные свойства ЛРП. Первая группа определений характеризует ранг модуля сдвигов соответствующей ЛРП. Как и при определении ранга модуля в общей алгебре, под рангом модуля сдвигов понимается либо наименьшее число образующих — группа параметров $\{r_1, r_2, r_3\}$, либо наибольшее число линейно независимых элементов — параметры $\{r_4, r_5, r_6\}$. Вторая группа — $\{r_{11}, \ldots, r_{15}\}$ — характеризует возможность реализации последовательности линейным регистром сдвига. Несколько определений — $\{r_7, r_8, r_9\}$ — можно условно назвать *информационной* линейной сложностью. Последнюю группу — $\{r_{18}, r_{19}, r_{20}\}$ — образуют параметры, которые являются наиболее простыми для вычисления и могут служить для практической оценки остальных определений линейной сложности.

Для последовательностей над полем все эти параметры хороши тем, что позволяют определить, является ли рассматриваемая последовательность u линейной рекуррентой: для этого необходимо и достаточно, чтобы какой-либо из параметров $r_i(u)$ был конечен. Однако для последовательностей над произвольным модулем все обстоит гораздо сложнее. Имеющиеся примеры показывают, что конечность большей части параметров не является достаточным условием для того, чтобы последовательность была линейной рекуррентой. Более того, некоторые параметры не всегда конечны, даже если рассматриваемая последовательность заведомо является линейной рекуррентой.

Модуль ${}_RM$ называется *рекурсивно определяющим модулем* по отношению к группе параметров $\mathcal{R} = \{r_i \mid i \in I\}$ ($\mathcal{R}$*-рекурсивно определяющим*), если для произвольной k-последовательности (многомерной) верно

$$\forall r_i \in \mathcal{R}\colon\ u \text{ — } k\text{-ЛРП над модулем } {}_RM \iff r_i(u) < \infty.$$

Выделим четыре группы параметров

$$\mathcal{R}_1 = \{r_1, r_2, r_3, r_{16}, r_{18}\}, \qquad \mathcal{R}_2 = \{r_1, r_2, r_3, r_7, r_8, r_9, r_{16}, r_{18}\},$$
$$\mathcal{R}_3 = \{r_1, r_2, r_3, r_7, r_8, \ldots, r_{18}\}, \quad \mathcal{R}_4 = \{r_1, r_2, \ldots, r_{20}\}.$$

Теорема. *Пусть M — строгий левый модуль над кольцом R. Тогда*
(а) *если кольцо R — нетерово слева, то модуль M — $\mathcal{R}_1$-рекурсивно определяющий*;

(b) *если вдобавок модуль* M *— нетеров, то* M *—* $\mathcal{R}_2$ *-рекурсивно определяющий*;

(c) *если к тому же кольцо* R *— коммутативно, то* M *—* $\mathcal{R}_3$ *-рекурсивно определяющий*;

(d) *если дополнительно модуль* M *— без кручения, то* M *—* $\mathcal{R}_4$ *-рекурсивно определяющий.*

Данная теорема достаточно полно описывает свойства модулей, при наличии которых они являются рекурсивно определяющими по отношению к тем или иным определениям линейной сложности. Построены различные примеры, показывающие, что при отсутствии одного из свойств, перечисленных в теореме, модуль не может являться рекурсивно определяющим в том или ином смысле.

СПИСОК ЛИТЕРАТУРЫ

1. *Кузьмин А. С.*, *Куракин В. Л.*, *Нечаев А. А.* Псевдослучайные и полилинейные последовательности. — Труды по дискретной математике. Т. 1. М.: ТВП, 1997, с. 139–202.
2. *Куракин В. Л.* Линейная сложность полилинейных последовательностей. — Дискретн. матем., 2001, т. 13, № 1, с. 3–55.