ПДМ. 2013. № 1(19).

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

5–13

Биляк И. Б. Оценки числа появлений элементов на отрезках линейных рекуррентных последовательностей // ПДМ. 2013. № 1(19). С. 5–13.

14–16

Коломеец Н. А. О верхней оценке нелинейности некоторого класса булевых функций с максимальной алгебраической иммунностью // ПДМ. 2013. № 1(19). С. 14–16.

17–33

Шоломов Л. А. Двоичные представления недоопределённых данных и дизъюнктивные коды // ПДМ. 2013. № 1(19). С. 17–33.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

34–49

Семенова Н. А. Представление системы семантически осмысленного ролевого управления доступом в виде цветной сети Петри // ПДМ. 2013. № 1(19). С. 34–49.

50–68

Смольянинов В. Ю. Правила преобразования состояний СУБД ДП-модели // ПДМ. 2013. № 1(19). С. 50–68.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

69–83

Бадеха И. А. Исследование кликовых покрытий рёбер графа // ПДМ. 2013. № 1(19). С. 69–83.

84–92

Ураков А. Р., Тимеряев Т. В. Алгоритм поиска кратчайших путей для разреженных графов большой размерности // ПДМ. 2013. № 1(19). С. 84–92.

93–98

Цициашвили Г. Ш., Осипова М. А., Лосев А. С. Асимптотика вероятности связности графа с низконадёжными рёбрами // ПДМ. 2013. № 1(19). С. 93–98.

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

99–109

Колоколов А. А., Адельшин А. В., Ягофарова Д. И. Исследование задач дискретной оптимизации с логическими ограничениями на основе метода регулярных разбиений // ПДМ. 2013. № 1(19). С. 99–109.

110–116

Кузнецов А. А., Кузнецова А. С. Быстрое умножение элементов в конечных двупорождённых группах периода пять // ПДМ. 2013. № 1(19). С. 110–116.

117–124

Мурин Д. М. О верхней границе плотности инъективных векторов // ПДМ. 2013. № 1(19). С. 117–124.

ŋqdqɐeɎ bɆ dədɆbɎзə d ɕɔɑbɔɐ Ɉqddɏqɐè

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 621.391.1:004.7

ОЦЕНКИ ЧИСЛА ПОЯВЛЕНИЙ ЭЛЕМЕНТОВ НА ОТРЕЗКАХ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

И. Б. Биляк

г. Москва, Россия

E-mail: bil-ib@mail.ru

Рассмотрен некоторый класс тригонометрических сумм от линейных рекуррентных последовательностей. Эти суммы исследуются с использованием метода В. М. Сидельникова. Получены оценки числа появлений элементов на отрезках линейных рекуррент, которые в некоторых случаях уточняют ранее известные результаты.

Ключевые слова: *тригонометрические суммы, линейные рекуррентные последовательности, число появлений элементов.*

Введение

Изучение числа появлений элементов в линейных рекуррентных последовательностях (ЛРП) над кольцами является одной из важных математических задач. Интерес к этой задаче связан прежде всего с построением на основе ЛРП генераторов псевдослучайных чисел, использующих различные способы усложнения аналитического строения линейных рекуррент (см., например, [1]).

Пусть $\mathrm{GF}(q)$ — конечное поле из q элементов, $f(x) = x^m - a_{m-1}x^{m-1} - \ldots - a_1x - a_0$ — реверсивный ($a_0 \neq 0$) неприводимый многочлен степени m над этим полем. Линейной рекуррентной последовательностью над полем $\mathrm{GF}(q)$ с характеристическим многочленом $f(x)$ будем называть последовательность $u = u(0)u(1)u(2)\ldots$ элементов этого поля, удовлетворяющую соотношению

$$u(i+m) = a_0u(i) + a_1u(i+1) + \ldots + a_{m-1}u(i+m-1), \quad i \geqslant 0.$$

Каждая такая ненулевая ЛРП u является чисто периодической последовательностью, при этом её период $T(u)$ равен периоду $T(f)$ многочлена $f(x)$ и делит $q^m - 1$ (см., например, [2]).

Рассмотрим линейные рекуррентные последовательности $u_1, u_2, \ldots, u_r$ с характеристическим многочленом $f(x)$. Назовём эти последовательности линейно независимыми над полем $\mathrm{GF}(q)$, если для всех ненулевых векторов $\bar{c} = (c_1, c_2, \ldots, c_r) \in \mathrm{GF}(q)^r$ последовательность $c_1u_1 + c_2u_2 + \ldots + c_ru_r$ является ненулевой. Обозначим через $N_l(\overline{z}, u_1, \ldots, u_r)$ количество целых чисел $i \in \{0, 1, \ldots, l-1\}$, удовлетворяющих условиям $u_1(i) = z_1$, $u_2(i) = z_2$, …, $u_r(i) = z_r$, где $\overline{z} = (z_1, z_2, \ldots, z_r) \in \mathrm{GF}(q)^r$. Таким образом, величина $N_l(\overline{z}, u_1, \ldots, u_r)$ равна количеству появлений r-граммы $\overline{z}$ на отрезке длины l последовательности векторов, элементы которой имеют вид $(u_1(i), u_2(i), \ldots, u_r(i))$ для всех $i \geqslant 0$.