на следующий вопрос: насколько велико может быть различие мощностей полных тупиковых (несокращаемых) множеств S, $S \subseteq A^n$? Например, как ведёт себя (по n при фиксированном m) функция

$$f(m,n) = \max |S_1|/|S_2|,$$

где $m = |A|$, а максимум берётся по всем парам $\{S_1, S_2\}$ полных тупиковых множеств, $S_1, S_2 \subseteq A^n$? Можно доказать, что эта функция не ограничена никакой константой. Более точные оценки её роста значительно прояснили бы структуру полных множеств слов.

ЛИТЕРАТУРА

1. *Евдокимов А. А., Крайнев В. А.* Задачи о полноте систем слов // XXII Обл. науч.-технич. конф. Тезисы. Новосибирск, 1979. С. 105–107.
2. *Евдокимов А. А.* Полные множества слов и их числовые характеристики // Методы дискретного анализа в исследовании экстремальных структур: сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1983. Вып. 39. С. 7–19.
3. *Евдокимов А. А.* Исследование полноты множеств слов и языков с запретами // Вестник Томского государственного университета. Приложение. 2004. № 9(1). С. 8–12.
4. *Evdokimov A. A. and Kitaev S. V.* Crucial words and the complexity of some extremal problems for sets of prohibited words // J. Comb. Theory. Ser. A. 2004. V. 105. P. 273–289.
5. *Berstel J. and Karhumäki J.* Combinatorics on words — a tutorial // Bull. EATCS. 2003. V. 79. P. 178–229.

УДК 512.624.5 DOI 10.17223/2226308X/9/4

О ДОСТАТОЧНОМ УСЛОВИИ ДЛЯ ОТСУТСТИЯ ВОЗМОЖНОСТИ СОКРАЩЕНИЯ ПЕРИОДА В СТАРШИХ ДВОИЧНЫХ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ НАД ПРИМАРНЫМИ КОЛЬЦАМИ

С. А. Кузьмин

Рассматриваются двоичные разрядные последовательности над примарными кольцами нечётной характеристики. Указано достаточное условие для отсутствия сокращения периода в старших разрядных последовательностях в 2 раза при наличии не всех элементов на цикле исходной линейной рекурренты.

Ключевые слова: *линейные рекуррентные последовательности, периоды последовательностей, примарные кольца, разрядные последовательности.*

В настоящее время наблюдается особый интерес к изучению p-ичных разрядных последовательностей над кольцами вычетов по модулю p^n. Это связано с тем, что данные последовательности обладают высокой линейной сложностью и могут быть использованы в датчиках псевдослучайных последовательностей. Со списком работ по данной тематике можно ознакомиться, например, в [1].

Большое внимание уделяется задаче восстановления линейных рекуррентных последовательностей (ЛРП) над примарными кольцами вычетов по их усложнению, особенно в тех случаях, когда ЛРП максимального периода (ЛРП МП) отображается в свою старшую координатную последовательность [2].

Меньше работ посвящено r-ичным разрядным последовательностям, где $r \neq p$, которые также могут быть рассмотрены как усложнения линейных рекуррент над простыми полями и кольцами Галуа. Такие последовательности рассматривались

А. С. Кузьминым в [3]. Им найдены все двоичные разрядные последовательности ЛРП МП над конечным простым полем нечётной характеристики, в которых наблюдается эффект сокращения периода. В [4] эти результаты обобщены и доказано, что сокращение периода в r-ичных разрядных последовательностях над конечным простым полем, где $r > 2$, невозможно.

Любой знак $u(i)$ некоторой ЛРП МП u над примарным кольцом представим в виде

$$u(i) = \sum_{s=0}^{k} u_s(i) 2^s,$$

где $k = [\log_2 p^n]$. Таким образом, последовательность вида $u_s = (u_s(0), u_s(1), \ldots)$, является s-й разрядной последовательностью ЛРП МП u над примарным кольцом. Обозначим $T(u)$, $T(u_l)$ периоды последовательностей u и u_l.

В [5] сформулирован результат о том, что при наличии всех элементов на цикле ЛРП МП u существует только один номер z двоичной разрядной последовательности над кольцом Галуа, зависящий от вида числа p и степени n, для которого $T(u_z) | (T(u)/2)$. Вопрос о возможности сокращения периода в 2 раза в противном случае остался незатронутым.

Лемма 1. Для всех возможных пар элементов a и b кольца $\mathbb{Z}_{p^n}$, таких, что выполняется соотношение $a + b \equiv 0 \pmod{p^n}$, справедлива следующая формула для нахождения числа μ_l пар, у которых совпадают l-е двоичные разряды:

$$\mu_l = 2 \min_l \left\lfloor \frac{(p^n - 1)/2 - 2^l + \min_l}{2^l} \right\rfloor + \min\left(2 \min_l, ((p^n - 1)/2 - 2^l + \min_l) \bmod 2^l\right) + \min_l,$$

где $\min_l = \min(((p^n - 1)/2) \bmod 2^l, 2^l - ((p^n - 1)/2 + 1) \bmod 2^l) + 1$.

Замечание 1. Заметим, что так как $1 \leqslant \min_l \leqslant 2^{l-1} - 1$, то верхняя и нижняя оценки числа μ_l могут быть получены тривиальным образом.

Полученное значение μ_l может быть использовано для доказательства следующих утверждения и теоремы.

Утверждение 1. Пусть u — ЛРП МП над кольцом $\mathbb{Z}_{p^n}$ с характеристическим многочленом $f(x)$, $\deg f = m$, пусть также на цикле последовательности u встречаются $2\mu_l$ различных элементов из $\mathbb{Z}_{p^n}$. Тогда для отсутствия сокращения периода в разрядной последовательности с номером $l > z$ (см. [5]) в 2 раза достаточно выполнения неравенства

$$p^{n-1}(p^m - 1) > (2\mu_l)^m. \tag{1}$$

Замечание 2. Данное утверждение носит скорее теоретический характер, на практике доля номеров двоичных разрядных последовательностей, для которых выполняется неравенство (1) в случае различных p, n, m и l, мала.

Теорема 1. Пусть u — ЛРП над примарным кольцом $\mathbb{Z}_{p^n}$. Если на цикле последовательности u встречается более $2\mu_l$ различных элементов, то $T(u_l) \not| (T(u)/2)$.

ЛИТЕРАТУРА

1. *Сачков В. Н., Горчинский Ю. Н., Зубков А. Н., Яблонский С. В.* Труды по дискретной математике. Т. 1. М.: ТВП, 1997. 280 с.
2. *Кузьмин А. С., Маршалко Г. Б., Нечаев А. А.* Восстановление линейной рекуррентной последовательности над примарным кольцом вычетов по её усложнению // Математические вопросы криптографии. 2010. Т. 1. Вып. 2. С. 31–56.

3. *Кузьмин А. С.* О периодах разрядов в r-ичной системе счисления знаков линейных рекуррентных последовательностей над конечными простыми полями // Безопасность информационных технологий. 1995. Вып. 4. С. 71–75.
4. *Кузьмин С. А.* Периоды разрядных последовательностей линейных рекуррент максимального периода над конечными простыми полями // Прикладная дискретная математика. 2015. № 1(27). С. 62–68.
5. *Кузьмин С. А.* О двоичных разрядных последовательностях над кольцами Галуа, допускающих эффект сокращения периода // Фундамент. и прикл. матем. 2015. Т. 20. № 1. С. 223–230.

УДК 519.7 DOI 10.17223/2226308X/9/5

О ГРУППАХ, ПОРОЖДЁННЫХ ПРЕОБРАЗОВАНИЯМИ СМЕШАННОГО ТИПА И ГРУППАМИ НАЛОЖЕНИЯ КЛЮЧА

Б. А. Погорелов, М. А. Пудовкина

Наиболее распространёнными группами наложения ключа итерационных алгоритмов блочного шифрования являются регулярное подстановочное представление V_n^+ группы векторного наложения ключа, регулярное подстановочное представление $\mathbb{Z}_{2^n}^+$ аддитивной группы кольца вычетов и регулярное подстановочное представление $\mathbb{Z}_{2^n+1}^\odot$ мультипликативной группы простого поля (2^n+1 — простое число). Рассматривается расширение группы $G_n = \langle V_n^+, \mathbb{Z}_{2^n}^+ \rangle$ преобразованиями и группами, естественными для криптографической практики. К числу таких преобразований и групп относятся: группы $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$ и $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$, подстановка псевдообращения над полем $\mathrm{GF}(2^n)$ или кольцом Галуа $\mathrm{GR}(2^{md}, 2^m)$.

Ключевые слова: *группа наложения ключа, аддитивная регулярная группа, сплетение групп подстановок, мультипликативная группа кольца вычетов, кольцо Галуа.*

Группы наложения ключа итерационных алгоритмов блочного шифрования являются, как правило, регулярными абелевыми. Среди них наиболее распространены следующие:

— V_n^+ — регулярное подстановочное представление группы векторного наложения ключа над полем $\mathrm{GF}(2)$. Оно является элементарной абелевой 2-группой и используется в AES, Р34.12-2015 «Кузнечик» и многих других алгоритмах блочного шифрования. Группа V_n^+ имеет $(2^n-1)\dots(2^n-2^{r-1})/(2^r-1)\dots(2^2-1)(2-1)$ изоморфных подгрупп порядка 2^r, $r=1,\dots,n$, и столько же систем импримитивности;

— $\mathbb{Z}_{2^n}^+$ — регулярное подстановочное представление аддитивной группы кольца вычетов. Оно используется, например, в алгоритме блочного шифрования ГОСТ 28147-89. Из цикличности группы следует, что у неё имеется $n-1$ собственных подгрупп и столько же систем импримитивности;

— $\mathbb{Z}_{2^n+1}^\odot$ — регулярное подстановочное представление мультипликативной группы простого поля, в которой элемент 2^n переобозначается как 0 (модульное умножение), а 2^n+1 — простое число. Как мультипликативная группа конечного поля она циклическая порядка 2^n с $n-1$ собственной подгруппой.

В этом смысле последние два способа наложения ключа предпочтительней, так как необходимо, чтобы слой s-боксов и линейный слой рассеивали меньшее число систем импримитивности.