

А.В.Минин

О ЛИНЕЙНОЙ СЛОЖНОСТИ ДВУХ ТРОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Исследована линейная сложность почти идеальных троичных последовательностей и троичных последовательностей с двумя ненулевыми боковыми лепестками автокорреляции.

Ключевые слова: линейная сложность, почти идеальные троичные последовательности

Введение

Псевдослучайные последовательности широко применяются в системах связи и криптографии. Периодическая автокорреляционная функция (ПАКФ) и линейная сложность являются важными параметрами псевдослучайных последовательностей. Последовательность называется почти идеальной, если её ПАКФ $l(t)$ равна нулю при всех $t \not\equiv 0 \pmod{N}$ за исключением одного. Определение почти идеальных последовательностей было введено в [1]. Стоит отметить, бинарные последовательности с такой ПАКФ ещё раньше рассматривались в [2]. Далее, почти идеальные троичные последовательности исследовались в [3—5].

Линейная сложность почти идеальных бинарных последовательностей изучена в [6]. Там же были доказаны предположения о линейной сложности соответствующих бинарных последовательностей, сделанные в [4].

Целью данной работы является оценка линейной сложности над полем третьего порядка почти идеальных троичных последовательностей длины $4(p^n + 1)$ и троичных последовательностей с двумя ненулевыми боковыми лепестками автокорреляции, рассмотренных ранее в [5].

1. Линейная сложность последовательностей Кренгеля

Линейная сложность последовательности над полем третьего порядка определяется как наименьшее натуральное число L , для которого существуют константы $c_i \in GF(3)$; $i = 1, K, L$ такие, что выполняется рекуррентное соотношение

$$s_i = c_1 s_{i-1} + c_2 s_{i-2} + K + c_L s_{i-L} \text{ для всех } i \geq L.$$

Многочлен $m(x) = x^L + c_1 x^{L-1} + c_2 x^{L-2} + K + c_L$ называют минимальным многочленом последовательности [7].

Минимальный многочлен $m(x)$ и линейную сложность L последовательности (s_i) с периодом N можно вычислить по следующим формулам [7]:

$$m(x) = (x^N - 1) / \text{НОД}(x^N - 1, S(x)), \quad L = N - \deg \text{НОД}(x^N - 1, S(x)), \quad (1)$$

$$\text{где } S(x) = s_0 + s_1 x + \dots + s_{N-1} x^{N-1}$$

Пусть p — нечетное простое число, $q = p^n, n = 1, 2, K$. Почти идеальные троичные последовательности периода $N = 4(q + 1)$ с четырьмя нулями на периоде были предложены Кренгелем Е. И. в [3, 4]. Сначала, кратко повторим основные определения из [4]. Далее, будем считать, что $q \equiv 1 \pmod{4}$.

Пусть g — примитивный элемент F_{q^2} — конечного поля порядка q^2 и h примитивный элемент поля F_q . Рассмотрим троичную последовательность, определяемую следующим образом:

$$y_i = y(\text{Tr}(g^i)), \quad i = 0, 1, K, 4(q + 1) - 1, \quad (2)$$

где

$$y(z) = \begin{cases} (-1)^{\lfloor (\text{ind}_h z \bmod 4) / 2 \rfloor}, & \text{если } z \neq 0, \\ 0, & \text{если } z = 0. \end{cases} \quad z \in F_q,$$

$\text{ind}_h z$ представляет собой дискретный логарифм по основанию z , $\lfloor u \rfloor = \max\{k : k < u, k \in \mathbb{N}\}$ и Tr

— функция следа из F_{q^2} в F_q .

Как показано в [4], (y_i) является почти идеальной троичной последовательностью периода $N = 4(q+1)$ и имеет четыре нуля на периоде.

Согласно определению последовательности (y_i) , справедливо следующее утверждение.

Лемма 1.

1. Пусть $b = \min_{y_j=0} j$. Тогда $y_{b+k(q+1)} = 0$ для $k = 0, 1, 2, 3$.

2. Если $j : y_j \neq 0, 0 \leq j \leq 4(q+1)-1$, то $y_{j+2(q+1)} = -y_j$.

Пусть $P_y(x) = \sum_{i=0}^{2q+1} y_i x^i$, $S_y(x) = \sum_{i=0}^{4q+3} y_i x^i$.

Лемма 2. Если последовательность (y_i) определена по (2), то

$$S_y(x) = P_y(x)(1 - x^{2(q+1)}).$$

Лемма 2 следует непосредственно из леммы 1.

Лемма 3. Пусть последовательность (y_i) с периодом $N = 4(q+1)$ определена по (2), тогда $L \leq 2(q+1)$.

Доказательство. По лемме 2 получаем, что $\text{НОД}(x^{4(q+1)} - 1, S_y(x))$ делится на $x^{2(q+1)} - 1$. Следовательно $\deg \text{НОД}(x^{4(q+1)} - 1, S_y(x)) \geq 2(q+1)$. Тогда утверждение леммы 3 следует из (1).

2. Линейная сложность последовательностей длины $8(p^n + 1)$

В [5] были получены новые троичные последовательности длины $8(p^n + 1)$ с 8-ю нулями на периоде и нулевыми боковыми лепестками ПАКФ при всех ненулевых сдвигах за исключением N и $3N$, в которых они равны $-4p^n$. В этом подразделе рассмотрим эти троичные последовательности и оценим их линейную сложность.

Пусть (h_i) троичная последовательность длины $4(p^n + 1)$, полученная объединением двух почти идеальных бинарных последовательностей (u_i) и $(-u_i)$ длин $2(p^n + 1)$. Последовательность (y_i) как в разделе 2.

Рассмотрим последовательность (z_i) с периодом $8(p^n + 1)$, определяемую следующим образом:

$$z_k = \begin{cases} h_i, & \text{если } k = 2i, \\ y_i, & \text{если } k = 2i+1, \end{cases} \quad k = 0, 1, \dots, 8(p^n + 1) - 1, \quad (3)$$

то есть $z = I(h, y)$, где I - оператор чередования [5].

Пусть $S_z(x) = \sum_{i=0}^{8q+7} z_i x^i$, $S_h(x) = \sum_{i=0}^{4q+3} h_i x^i$. Тогда, согласно [8], справедливо соотношение

$$S_z(x) = S_h(x^2) + x S_y(x^2) \quad (4)$$

Лемма 4. Пусть последовательность (z_i) определена по (3). Тогда $L \leq 4(q+1)$.

Доказательство. Из наших определений следует, что $S_h(x) = S_u(x) - x^{2(q+1)} S_u(x)$ или $S_h(x^2) = S_u(x^2)(1 - x^{4(q+1)})$. Далее, по лемме 2 имеем, что

$$S_y(x^2) = P_y(x^2)(1 - x^{4(q+1)}).$$

Следовательно,

$$S_z = S_h(x^2)(1 - x^{4(q+1)}) + x P_y(x^2)(1 - x^{4(q+1)}).$$

Тогда $\text{НОД}(S_z(x), x^{8(q+1)} - 1)$ делится на $x^{4(q+1)} - 1$. Таким образом, по (1) имеем, что $L \leq 4(q+1)$.

Заключение

В работе дана оценка линейной сложности почти идеальных троичных последовательностей и троичных последовательностей с двумя ненулевыми боковыми лепестками автокорреляции. Показано, что такие последовательности имеют низкую линейную сложность.

1. Wolfmann J. Almost perfect autocorrelation sequences // IEEE Transaction on Information Theory. 1992. V. IT-38. № 4. P. 1412-1418.
2. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
3. Krenzel E.I. Almost-perfect and odd-perfect ternary sequences // Proceedings 2004 International Conference on Sequences and Their Applications (SETA '04). LNCS 3486. Berlin: Springer-Verlag, 2005. P. 197-207.
4. Кренгель Е.И. Конструирование почти идеальных и нечетко-идеальных троичных последовательностей // Радиотехника. 2006. № 9. С. 8-12.
5. Кренгель Е.И., Иванов П.В. Новые троичные последовательности с двумя ненулевыми боковыми лепестками периодической автокорреляционной функции и пик-фактором, близким к единице // 18-я Международная конференция «Цифровая обработка сигналов и ее применение — DSPA-2016». 2016. Т. 1. С. 183-187.
6. Edemskiy V., Minin A. About the linear complexity of the almost perfect sequences. International Journal of Communications. 2016. V. 1. P. 223-226
7. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 820 с.
8. Wang Q., Du X. N. The linear complexity of binary sequences with optimal au-tocorrelation // IEEE Trans. Inf. Theory. 2010. V. 56. № 12. P. 6388-6397.

References

1. Wolfmann J. Almost perfect autocorrelation sequences // IEEE Transaction on Information Theory. 1992. V. IT-38. № 4. P. 1412-1418.
2. Ipatov V.P. Periodicheskie diskretnye signaly s optimal'nymi korrelyatsionnymi svoystvami. M.: Radio i svyaz', 1992. 152 s.
3. Krenzel E.I. Almost-perfect and odd-perfect ternary sequences // Proceedings 2004 International Conference on Sequences and Their Applications (SETA '04). LNCS 3486. Berlin: Springer-Verlag, 2005. P. 197-207.
4. Krenzel' E.I. Konstruirovaniye pochtii ideal'nykh i nechetko-ideal'nykh troichnykh posledovatel'nostey // Radiotekhnika. 2006. № 9. S. 8-12.
5. Krenzel' E.I., Ivanov P.V. Novye troichnye posledovatel'nosti s dvumya nenulevymi bokovymi lepestkami periodicheskoy avtokorrelyatsionnoy funktsii i pik-faktorom, blizkim k edinitse // 18-ya Mezhdunarodnaya konferentsiya «Tsifrovaya obrabotka signalov i ee primeneniye — DSPA-2016». 2016. T. 1. S. 183-187.
6. Edemskiy V., Minin A. About the linear complexity of the almost perfect sequences. International Journal of Communications. 2016. V. 1. P. 223-226
7. Lidl R., Niderrayter G. Konechnye polya. M.: Mir, 1988. 820 s.
8. Wang Q., Du X. N. The linear complexity of binary sequences with optimal au-tocorrelation // IEEE Trans. Inf. Theory. 2010. V. 56. № 12. P. 6388-6397.

Minin A.V. About linear complexity of two ternary sequences. We investigate the linear complexity of almost perfect ternary sequences and ternary sequences with two nonzero levels of autocorrelation side lobes.

Keywords: linear complexity, almost perfect ternary sequences

Сведения об авторе. А.В.Минин — магистрант; кафедра ПМИ ИЭУ НовГУ; s208076@std.novsu.ru.

Статья публикуется впервые. Поступила в редакцию 01.12.2016.