

А.В.Минин

ЛИНЕЙНАЯ СЛОЖНОСТЬ КЛАССА БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ОПТИМАЛЬНОЙ АВТОКОРРЕЛЯЦИЕЙ

Исследована линейная сложность почти сбалансированных двоичных последовательностей с оптимальной автокорреляцией, образованных чередованием конкатенации двоичной последовательности Сидельникова с оптимальной автокорреляцией и почти идеальной последовательности.

Ключевые слова: линейная сложность, автокорреляция, бинарные последовательности

Введение

Сбалансированные и почти сбалансированные двоичные последовательности с оптимальной автокорреляцией широко используются в цифровой связи, радарх и в системах потокового шифрования. В [1] Е.И.Кренгель и П.В.Иванов предложили метод синтеза почти сбалансированных двоичных последовательностей длины $4N$ с оптимальной по автокорреляцией, образованных чередованием конкатенации двоичной последовательности Сидельникова с оптимальной автокорреляцией и почти идеальной последовательности. Авторы предположили, что такие последовательности обладают высокой линейной сложностью и могут быть использованы в системах связи и криптографии. В этой работе докажем предположение о высокой линейной сложности последовательности.

Линейная сложность L является важным параметром оценки двоичной последовательности (s_i) при её применении в качестве ключевого поточного шифра для криптографических приложений. Над полем второго порядка она определяется как наименьшее натуральное число L , для которого существуют константы $c_i = 0, 1; i = 1, K, L$ такие, что выполняется рекуррентное соотношение

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

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

Минимальный полином $m(x)$ и линейную сложность (L) последовательности (s_i) с периодом T можно вычислить по следующим формулам [3]:

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

где $S(x) = s_0 + s_1 x + \dots + s_{T-1} x^{T-1}$ — многочлен последовательности.

1. Определение последовательности

Пусть $GF(p_1^k)$ — конечное поле порядка p_1^k , где p_1 — простое число и a — его примитивный элемент $GF(p_1^k)$. Тогда сбалансированная двоичная последовательность Сидельникова периода $p_1^k - 1$ с оптимальной автокорреляцией задается выражением

$$y_t = \begin{cases} 1, & \text{если } a^t + 1 \text{ не квадрат в } GF(p_1^k), \\ 0, & \text{если } a^t + 1 \text{ является квадратом.} \end{cases} \quad (2)$$

Бинарная последовательность x с периодом M называется почти идеальной, если её периодическая корреляционная функция $R(t) = 0$ для всех $t \not\equiv 0 \pmod{M}$ за исключением одного [4]. Такие последовательности существуют только тогда, когда период $N = 2(p_2^l + 1)$, где p_2 — простое число. Далее, всегда предполагаем, что $N = p_1^k - 1 = p_2^l + 1$, согласно [1], такие p_1, p_2, k, l существуют.

Пусть y — последовательность Сидельникова с периодом N , определенная по (2). Путем конкатенации сформируем последовательность z с периодом $2N$; $z = s \cdot s$, то есть $z = s_0, \dots, s_{N-1}, s_0, \dots, s_{N-1}$.

Пусть h — почти идеальная двоичная последовательность. Рассмотрим последовательность s , сформированную по правилу

$$s_i = \begin{cases} z_k, & \text{если } k = 2i, \\ h_k, & \text{если } k = 2i + 1. \end{cases} \quad (3)$$

то есть $s = I(z, h)$, где I — оператор чередования. Согласно [1], последовательность s обладает оптимальной автокорреляцией и имеет период $4N$.

2. Линейная сложность последовательности

Для $T = 4N$ формула (1) над полем второго порядка примет следующий вид:

$$m(x) = (x^N - 1)^4 / \text{НОД}((x^N - 1)^4, S(x)), L = 4N - \deg \text{НОД}((x^N - 1)^4, S(x)), \quad (4)$$

где $S(x) = s_0 + s_1x + \dots + s_{4N-1}x^{4N-1}$.

Введём вспомогательные многочлены $S_z(x) = \sum_{i=0}^{2N-1} z_i x^i$, $S_h(x) = \sum_{i=0}^{2N-1} h_i x^i$. Тогда, согласно [5], справедливо соотношение

$$S(x) = S_z(x^2) + xS_h(x^2) \quad (5)$$

Теорема. Если последовательность s определена по (3), тогда $L = 4N$.

Доказательство. Согласно определению, получаем, что $S_z(x) = S_y(x) + x^{2N}S_y(x)$, где $S_y(x)$ — многочлен последовательности Сидельникова.

Далее, в [6] было показано, что $S_h(x) = T(x)(1 - x^{2N}) + x^a + \frac{x^{2N}(x^{2N} - 1)}{x - 1}$,

где вспомогательный многочлен $T(x) = \sum_{i=0, h_i \neq 0}^{N-1} h_i x^i$ и $a : h_a = 0$ и $a \leq N - 1$.

Таким образом,

$$S(x) = S_z(x^2) + xS_h(x^2) = S_y(x^2) + x^{2N}S_y(x^2) + xT(x^2)(1 - x^{2N}) + x^{2a} + x^{2N}(x^{2N} - 1)/(x^2 - 1)$$

или

$$S(x) = (x^{2N} - 1)/(x^2 - 1)(S_y(x^2)(x^2 - 1) + xT(x^2)(x^2 - 1) + x^{2a}),$$

так как линейная сложность последовательности исследуется над полем второго порядка.

Далее, из последней формулы получаем, что $S(1) = 1$, то есть $S(x)$ не делится на $x - 1$.

Следовательно, $\text{НОД}((x^N - 1)^4, S(x)) = 1$ и утверждение теоремы следует из (4).

Таким образом, высказанное в [1] предположение о высокой линейной сложности рассматриваемых последовательностей справедливо.

Заключение

В работе представлены результаты исследования линейной сложности почти сбалансированных двоичных последовательностей с оптимальной автокорреляцией. Доказано предположение, что такие последовательности обладают высокой линейной сложностью.

1. Кренгель Е.И., Иванов П.В. Об одной конструкции двоичных последовательностей с оптимальной по модулю автокорреляцией. // 18-я Международная конференция «Цифровая обработка сигналов и ее применение — DSPA-2016». 2016. Т. 1. С. 176-182.
2. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 808 с.
3. Cusick T., Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam: North-Holland Publishing Co., 1998. 430 p.
4. Wolfmann J. Almost perfect autocorrelation sequences // IEEE Transaction on Information Theory. 1992. Vol. IT-38. № 4. P. 1412-1418.
5. Wang Q., Du X. N. The linear complexity of binary sequences with optimal au-tocorrelation // IEEE Trans. Inf. Theory. 2010. Vol. 56. № 12. P. 6388-6397.
6. Edemskiy V., Minin A. About the linear complexity of the almost perfect sequences // International Journal of Communications. 2016. Vol. 1. P. 223-226.

References

1. Krengeľ E.I., Ivanov P.V. Ob odnoy konstruktzii dvoichnykh posledovatel'nostey s optimal'noy po modulyu avtokorrelyatsiyey. // 18-ya Mezhdunarodnaya konferentsiya «Tsifrovaya obrabotka signalov i ee primeneniye — DSPA-2016». 2016. T. 1. S. 176-182.
2. Lidl R., Niderrayer G. Konechnye polya. M.: Mir, 1988. 808 s.

3. Cusick T., Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam: North-Holland Publishing Co., 1998. 430 p.
4. Wolfmann J. Almost perfect autocorrelation sequences // IEEE Transaction on Information Theory. 1992. Vol. IT-38. № 4. P. 1412-1418.
5. Wang Q., Du X. N. The linear complexity of binary sequences with optimal autocorrelation // IEEE Trans. Inf. Theory. 2010. Vol. 56. № 12. P. 6388-6397.
6. Edemskiy V., Minin A. About the linear complexity of the almost perfect sequences // International Journal of Communications. 2016. Vol. 1. P. 223-226.

Minin A.V. Linear complexity of a class of binary sequences with optimal autocorrelation. We study the linear complexity of almost balanced binary sequences with optimal autocorrelation formed by the interleaving of the concatenation a Sidelnikov binary sequence with optimal autocorrelation and an almost perfect sequence.

Keywords: linear complexity, autocorrelation, binary sequences.

Сведения об авторе. А.В.Минин — магистрант каф. ПМИ НовГУ; научный руководитель В.А.Едемский, профессор КПМИ НовГУ; s208076@std.novsu.ru.

Статья публикуется впервые. Поступила в редакцию 16.05.2017.