А.В.Минин

О ЛИНЕЙНОЙ СЛОЖНОСТИ РЯДА БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ОПТИМАЛЬНОЙ АВТОКОРРЕЛЯЦИЕЙ

В работе исследована линейная сложность почти сбалансированных двоичных последовательностей с оптимальной автокорреляцией, образованных чередованием двоичной последовательности Динга—Хеллесета—Мартинсена 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, радарах и в системах потокового шифрования. В [1] Е.И.Кренгелем и П.В.Ивановым был предложен метод синтеза почти сбалансированных двоичных последовательностей длины $4N$ с оптимальной автокорреляцией, образованных чередованием конкатенации двоичной последовательности Динга—Хеллесета—Мартинсена с оптимальной трехуровневой автокорреляцией и почти идеальной последовательности. В своей статье авторы предположили, что такие последовательности обладают высокой линейной сложностью и могут быть использованы в системах связи, радиолокационных системах и криптографии. В этой работе докажем предположение о высокой линейной сложности рассматриваемой 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 $c_i = 0, 1; i = 1, \dots, L$, 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 $GF(p)$ — конечное поле, где $p = 4f + 1$ — простое число, f — нечетно. Обозначим через q примитивный элемент конечного поля $GF(p)$. Рассмотрим подгруппу биквадратичных вычетов $D_0 = (q^4)$, порожденную q^4 , положим $D_f = q^f D_0$, для $f = 1, 2, 3$. Тогда D_f — циклотомические классы четвертого порядка [3]. Согласно китайской теореме об остатках, $Z_{2p} \cong Z_2 \times Z_p$ относительно изоморфизма $j : w \rightarrow (w \bmod 2, w \bmod p)$.

Пусть $C_0 = D_i \cup D_j$, $C_1 = D_i \cup D_j$ и $C = \{0\} \times C_0 \cup \{1\} \times C_1$. Рассмотрим почти сбалансированную двоичную последовательность периода $N = 2p$, определяемую как

$$z_i = \begin{cases} 1, & \text{если } i \in C_0, \\ 0, & \text{если } i \in C_1. \end{cases} \quad (2)$$

Согласно [4] последовательность $\{z_i\}$ имеет оптимальную трехуровневую автокорреляционную функцию, если: $p = x^2 + 4$ или $p = 1 + 4y^2$ при соответствующих значениях троек индексов (i, j, l) .

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 [5]. Такие последовательности существуют только тогда, когда период $N = 2(p_1^l + 1)$, где p_1 — простое число. Далее, всегда предполагаем, что $N = 2p = p_1^l + 1$, согласно [1], такие p, p_1, l существуют.

Пусть z — двоичная последовательность Динга—Хеллесета—Мартинсена, сформированная по (1) и h — почти идеальная двоичная последовательность. Рассмотрим последовательность s , определяемую следующим образом

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

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

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 определению, справедливо соотношение

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

Теорема. Если последовательность s определена по (3), тогда $L = 4p$ и $m(x) = (x^p - 1)^4$.

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

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, по (5) получаем, что

$$S(x) = S_z(x^2) + xS_h(x^2) = S_z(x^2) + xT(x^2)(1 - x^{2N}) + x^{2a} + x^{2N}(x^{2N} - 1)/(x^2 - 1) \quad (6)$$

По определению, $S_z(1) = 0$, тогда $S(1) = 1$ по (6). Далее, пусть a — первообразный корень p -ой степени из 1 в расширении поля $GF(2)$. По формуле (6) получаем, что $S(a^k) = S_z(a^{2k}) + a^{2ka}$ для $k = 1, 2, \dots, p - 1$. Согласно [4], имеет место соотношение $(S_z(a^{2k}))^{16} = S_z(a^{2k})$, следовательно, $S(a^k) \neq 0$ для $k = 1, 2, \dots, p - 1$ и $\text{НОД}((x^p - 1), S(x)) = 1$. Применение (4) завершает доказательство теоремы.

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

1. Кренгель Е.И., Иванов П.В. Об одной конструкции двоичных последовательностей с оптимальной по модулю автокорреляцией. // Материалы 18 Международной конференции "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 // North-Holland Mathematical Library. Vol. 55. Amsterdam: North-Holland Publishing Co., 1998. 446 p.
4. Ding C., Helleseht T., Martinsen H. New families of binary sequences with optimal three-level autocorrelation // IEEE Transaction on Information Theory. 2001. Vol. IT-47. P. 428-433.
5. Wolfmann J. Almost perfect autocorrelation sequences // IEEE Transaction on Information Theory. 1992. Vol. IT-38. №. 4. P. 1412-1418.
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 konstruksii dvoichnykh posledovatel'nostey s optimal'noy po modulyu avtokorrelyatsiyey. // Materialy 18 Mezhdunarodnoy konferentsii "Tsifrovaya obrabotka signalov i ee primeneniye — DSPA-2016". 2016. T. 1. S. 176-182
2. Lidl R., Niderrayter G. Konechnye polye. M.: Mir, 1988. 808 s.

3. Cusick T., Ding C., Renvall A. Stream Ciphers and Number Theory // North-Holland Mathematical Library. Vol. 55. Amsterdam: North-Holland Publishing Co., 1998. 446 p.
4. Ding C., Hellesteth T., Martinsen H. New families of binary sequences with optimal three-level autocorrelation // IEEE Transaction on Information Theory. 2001. Vol. IT-47. P. 428-433.
5. Wolfmann J. Almost perfect autocorrelation sequences // IEEE Transaction on Information Theory. 1992. Vol. IT-38. №. 4. P. 1412-1418.
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. About the linear complexity of series of binary sequences with optimal autocorrelation. We study the linear complexity of almost balanced binary sequences with optimal autocorrelation formed by the interleaving of Ding—Hellesteth—Martinsen binary sequence and an almost perfect sequence.

Keywords: linear complexity, autocorrelation, binary sequences.

Сведения об авторе. А.В.Минин — магистрант каф. ПМИ НовГУ им. Ярослава Мудрого, s208076@std.novsu.ru.

Статья публикуется впервые. Поступила в редакцию 29.11.2017.