

А.С.Цурина

# О ЛИНЕЙНОЙ СЛОЖНОСТИ ОБОБЩЕННЫХ ЦИКЛОТОМИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ХОЛЛА С ПЕРИОДОМ $p^{n+1}$

Представлены результаты расчета линейной сложности обобщенных циклотомических последовательностей Холла с периодом  $p^{n+1}$ . Метод расчета линейной сложности основан на использовании значений многочлена классических циклотомических последовательностей с периодом  $p$ .

Ключевые слова: линейная сложность, обобщенные циклотомические последовательности

## 1. Введение

Линейная сложность последовательности  $S = s_0, s_1, \dots$  над полем  $GF(2)$  является важной характеристикой её качества и определяется как наименьшее натуральное число  $L$ , для которого существуют константы  $c_1, \dots, c_L$  из  $GF(2)$  такие, что выполняется рекуррентное соотношение

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

Последовательности, обладающие высокой линейной сложностью ( $L > N/2$ ), важны для криптографических приложений.

Обобщенная циклотомия, включающая в себя классическую как частный случай, была предложена в [1]. Здесь рассмотрим циклотомические последовательности с периодом  $N = p^{n+1}$ .

Пусть  $p = dR + 1$  — нечетное простое число,  $d, R$  — натуральные числа. Обозначим через  $g$  примитивный корень по модулю  $p^{n+1}$ . Мультипликативный порядок  $g$  равен  $p^n(p-1)$  и  $g^{p-1} \equiv 1 \pmod{p}$  [2].

Введем  $D_0 = (g^d)$ , где  $(g^d)$  — подгруппа порядка  $p^n R$ , порожденная  $g^d$  в мультипликативной группе  $Z_N^*$  кольца классов вычетов по модулю  $N$ . Пусть  $D_k = g^k D_0$ ;  $k = 0, 1, \dots, d-1$  и  $p^m D_k = \{p^m a \mid a \in D_k\}$ ,  $m = 0, 1, \dots, n$ , где умножение выполняется в кольце  $Z_N$ , тогда порядок  $|p^m D_k| = p^{n-m} R$ . Как и в [1],  $D_k$  — назовем обобщенными циклотомическими классами. Согласно [1], справедливы разбиения

$$Z_N^* = \bigcup_{k=0}^{d-1} D_k \text{ и } Z_N = \bigcup_{m=0}^n \bigcup_{k=0}^{d-1} p^m D_k \cup \{0\}.$$

Линейная сложность последовательностей, сформированных на основе обобщенных циклотомических классов, исследовалась в целом ряде работ, обзор которых приведен в [3]. В частности, в [4] была изучена линейная сложность ряда обобщенных циклотомических последовательностей с периодом  $N = p^{n+1}$  на основе классов шестеричных вычетов ( $d = 6$ ), в заключение работы [4] отмечено, что также представляет интерес исследование линейной сложности обобщенных циклотомических последовательностей Холла. Решению этой проблемы и посвящена статья.

Пусть  $d = 6$ , то есть  $p \equiv 1 \pmod{6}$ , тогда справедливо разложение  $p = A^2 + 3B^2$ , где  $A, B$  — целые числа и  $A \equiv 1 \pmod{3}$  [2].

Рассмотрим последовательность, сформированную по следующему правилу

$$s_i = \begin{cases} 1, & \text{если } i \equiv q \pmod{N}, q \in C_0 \cup C_1 \cup C_3, \\ 0, & \text{в ост. случаях,} \end{cases} \quad (1)$$

$$\text{где } C_k = D_k \cup pD_k \cup \dots \cup p^n D_k.$$

В [4] был предложен метод вычисления линейной сложности обобщенных циклотомических последовательностей с периодом  $N = p^{n+1}$ . Кратко напомним его основные положения. Пусть  $H_0 = (g)$  — подгруппа, порожденная  $g$  в поле  $GF(p)$ ,  $g$  является и первообразным корнем по модулю  $p$  [5]. Введем

многочлен  $T(x) = \sum_{l \in H_0} x^l$ , то есть  $T(x)$  — многочлен характеристической последовательности с периодом  $p$ , соответствующей  $H_0$ . Обозначим через  $b$  примитивный корень степени  $p$  из единицы в расширении поля  $GF(2)$ .

Согласно [3], если последовательность сформирована по формуле (1), то её линейная сложность

$$L = \begin{cases} p^{n+1} - E \frac{p^{n+1} - 1}{d} - 1, & \text{если } R|I| \equiv 0 \pmod{2}, \\ p^{n+1} - E \frac{p^{n+2} - 1}{d(p+1)} - Fp \frac{p^n - 1}{d(p+1)}, & \text{если } R|I| \equiv 1 \pmod{2}, n \equiv 0 \pmod{2}, \\ p^{n+1} - Ep \frac{p^{n+1} - 1}{d(p+1)} - F \frac{p^{n+1} - 1}{d(p+1)} - 1, & \text{если } R|I| \equiv 1 \pmod{2}, n \equiv 1 \pmod{2}, \end{cases} \quad (2)$$

$$\text{где } E = \left\lfloor h \left| \sum_{k \in \{0,1,3\}} T(b^{g^{h+k}}) = 0, h = 0,1,\dots,5 \right. \right\rfloor, \quad F = \left\lfloor h \left| \sum_{k \in \{0,1,3\}} T(b^{g^{h+k}}) = 1, h = 0,1,\dots,5 \right. \right\rfloor,$$

$$R = (p-1)/6.$$

## 2. Линейная сложность обобщенных циклотомических последовательностей Холла

При исследовании линейной сложности обобщённых циклотомических последовательностей Холла ограничимся случаем, когда  $R$  — четное.

Теорема. Если последовательность формируется по правилу (1) при  $p = A^2 + 3B^2$ , где  $A \equiv 1 \pmod{6}$  и четном значении  $R$ , то при  $n > 0$  её линейная сложность

$$L = \begin{cases} \frac{p^{n+1} - 1}{2}, & \text{если } B \equiv 0 \pmod{12}, \\ \frac{2(p^{n+1} - 1)}{3}, & \text{если } B \equiv 6 \pmod{12}, \\ p^{n+1} - 1, & \text{если } B \equiv \pm 2 \pmod{6}. \end{cases}$$

Доказательство. Воспользуемся формулой (2), так как  $R$  — четное, то линейная сложность последовательности определяется следующей формулой:

$$L = p^{n+1} - E \frac{p^{n+1} - 1}{6} - 1, \quad (3)$$

$$\text{где } E = \left\lfloor h \left| \sum_{k \in \{0,1,3\}} T(b^{g^{h+k}}) = 0, h = 0,1,\dots,5 \right. \right\rfloor. \text{ Значения } T(b^{g^{h+k}}) \text{ были вычислены в [5].}$$

Воспользовавшись ими получаем, что

$$E = \begin{cases} 3, & \text{если } B \equiv 0 \pmod{12}, \\ 2, & \text{если } B \equiv 6 \pmod{12}, \\ 0, & \text{если } B \equiv \pm 2 \pmod{6}. \end{cases}$$

Подставляя значения  $E$  в формулу (3) и получаем утверждение теоремы.

Результаты расчетов для  $p = 433, 457, 601, \dots$  ( $B \equiv 0 \pmod{12}$ ),  $p = 109, 157, 229, \dots$  ( $B \equiv 6 \pmod{12}$ ),  $p = 13, 97, 241, \dots$  ( $B \equiv \pm 2 \pmod{6}$ ) подтверждают справедливость теоремы.

### Заключение

Таким образом, в статье частично решена проблема, поставленная в [4], а именно рассчитана линейная сложность обобщенных циклотомических последовательностей Холла с периодом  $p^{n+1}$  при  $p \equiv 1 \pmod{12}$ . Показано, что последовательности, сформированные по (1) обладают высокой линейной сложностью.

- 
1. Ding C., Helleseht T. New generalized cyclotomy and its applications // Finite Fields. 1998. Appl. 4. P. 140-166.
  2. Ireland K., Rosen M. A Classical introduction to modern number theory. Berlin: Springer-Verlag, 1982. 341 p.
  3. Edemskiy V.A. About computation of the linear complexity of generalized cyclotomic sequences with period  $p^{n+1}$  // Designs, Codes and Cryptography. 2011. Vol. 61. Iss. 3. P. 251-260.
  4. Du X., Chen Z. A generalization of the Hall's sextic residue sequences // Information Sciences. 2013. Vol. 222. P. 784-794.
  5. Цурина А.С. Линейная сложность шестеричных бинарных последовательностей [Электр. ресурс] // Ученые записки НовГУ. 2015. № 4. URL: <http://www.novsu.ru/univer/press/eNotes1/i.1086055/?id=1203418> (дата обращения: 01.10.2017).

### References

1. Ding C., Helleseht T. New generalized cyclotomy and its applications. Finite Fields, 1998, appl. 4, pp. 140-166.
2. Ireland K., Rosen M. A Classical introduction to modern number theory. Berlin, Springer-Verlag, 1982. 341 p.
3. Edemskiy V.A. About computation of the linear complexity of generalized cyclotomic sequences with period  $p^{n+1}$ . Designs, Codes and Cryptography, 2011, vol. 61, iss. 3, pp. 251-260.
4. Du X., Chen Z. A generalization of the Hall's sextic residue sequences. Information Sciences, 2013, vol. 222, pp. 784-794.
5. Tsurina A.S. Lineynaya slozhnost' shesterichnykh binarnykh posledovatel'nostey [Linear complexity of senary binary sequences]. Memors of NovSU, 2015, no. 4. Available at: <http://www.novsu.ru/univer/press/eNotes1/i.1086055/?id=1203418> (accessed: 01.10.2017).

**Tsurina A.S. On the linear complexity of generalized cyclotomic Hall's sequences with period  $p^{n+1}$ .** This article presents the results of the calculation of the linear complexity of generalized cyclotomic Hall's sequences with period  $p^{n+1}$ . The method of calculation of the linear complexity based on values of a polynomial classical cyclotomic sequences with period  $p$ .

**Keywords:** linear complexity, generalized cyclotomic sequence.

Сведения об авторе. А.С.Цурина — магистрант, Институт электронных и информационных систем, направление «Прикладная математика и информатика»; [aleksandra.curina@mail.ru](mailto:aleksandra.curina@mail.ru).

Статья публикуется впервые. Поступила в редакцию 29.11.2017.