УДК 621.391.15

О ЛИНЕЙНОЙ СЛОЖНОСТИ ЧЕТВЕРТИЧНЫХ ЦИКЛОТОМИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ 2*p*

В.А.Едемский, А.В.Иванов

ON THE LINEAR COMPLEXITY OF QUATERNARY CYCLOTOMIC SEQUENCES WITH A PERIOD OF 2*p*

V.A.Edemskii, A.V.Ivanov

Институт электронных и информационных систем НовГУ, Vladimir.Edemsky@novsu.ru

Вычислена линейная сложность семейства обобщенных циклотомических четвертичных последовательностей над кольцом классов вычетов четвертого порядка. Последовательности сформированы на основе классов квадратичных вычетов.

Ключевые слова: четвертичные последовательности, линейная сложность, кольцо классов вычетов

We derived the linear complexity of series of generalized cyclotomic quaternary sequences over a residue class ring of order four. The sequences are constructed on the basis of quadratic residue classes.

Keywords: quaternary sequences, linear complexity, residue class ring

Введение

Для криптографических приложений линейная сложность последовательности является важным показателем ее качества [1,2]. В [3,4] был предложен метод вычисления линейной сложности циклотомических последовательностей над полями второго и третьего порядков. Далее, в [5] он был применен к последовательностям, получающимся посредством обратного отображения Грея из четвертичных циклотомических последовательностей. Линейная сложность последовательностей была вычислена над конечным полем четвертого порядка $\mathbb{F}_4$. В этой статье покажем, что упомянутый выше метод может быть применен для исследования линейной сложности четвертичных циклотомических последовательностей с периодом $2p$ над кольцом классов вычетов четвертого порядка. В качестве иллюстрации вычислим линейную сложность последовательностей, автокорреляционная функция которых исследована в [6].

1. Основные определения

Пусть p — нечетное простое число и θ — первообразный корень по модулю p. Известно, что если g — нечетное из чисел θ и $\theta+p$, то g является первообразным корнем по модулю $2p$ [7]. Обозначим через $D_0=\{g^{2s} \bmod 2p; s=1,...,(p-1)/d\}$ класс квадратичных вычетов по модулю $2p$. Далее, если A — подмножество кольца классов вычетов $\mathbb{Z}_{2p}$, то через bA и $A+b$, где $b\in\mathbb{Z}$, будем обозначать следующие множества:

$$bA=\{ba \bmod 2p | a\in A\},\ A+b=\{(a+b) \bmod 2p | a\in A\}.$$

Положим $D_1=gD_0$, тогда справедливо разбиение $\mathbb{Z}_{2p}=D_0\cup D_1\cup 2D_0\cup 2D_1\cup\{0,p\}$.

Рассмотрим последовательность S с периодом $2p$, определяемую на периоде следующим образом [6]:

$$s_i=\begin{cases}0, \text{ если } i=0 \text{ или } i\in D_0,\\ 1, \text{ если } i\in D_1,\\ 2, \text{ если } i=p \text{ или } i\in D_2,\\ 3, \text{ если } i\in D_3.\end{cases} \quad (1)$$

Многочлен $C(x)=1+c_1x+...+c_mx^m$, $C(x)\in\mathbb{Z}_4[x]$ — называется ассоциированным многочленом последовательности S над $\mathbb{Z}_4$, если выполняется соотношение $s_i=-c_1s_{i-1}-c_2s_{i-2}-...-c_ms_{i-m}$ для всех $i: i\ge m$. Линейная сложность (L) последовательности S определяется как наименьшая из степеней ассоциированных многочленов. Известно, что $C(x)$ — ассоциированный многочлен последовательности S тогда и только тогда, когда

$$S(x)C(x)\equiv 0 \left(\bmod(x^{2p}-1)\right), \quad (2)$$

где $S(x)=s_0+s_1x+...+s_{2p-1}x^{2p-1}$.

Пусть $R=GF(2^{2r},2^2)$ — кольцо Галуа характеристики 4, здесь r — порядок 2 по модулю p [8]. Группа обратимых элементов R^* кольца R содержит циклическую подгруппу порядка 2^r-1. Следовательно, в R^* существует элемент γ порядка p, тогда $\alpha=3\gamma$ имеет порядок $2p$ и $\alpha^p=-1$. Далее исследуем значения $S(\alpha^v)$, $v=0,1,...,2p-1$, что и позволит рассчитать линейную сложность последовательности S по формуле (2).

2. Вспомогательные леммы

Метод вычисления значений $S(\alpha^v)$ будет представлен в следующем разделе, а здесь докажем вспомогательные леммы о суммах степеней α. Прежде всего заметим, что в кольце R имеем: $1+\alpha+...+\alpha^{2p-1}=0$ и $1+\alpha^2+...+\alpha^{2p-2}=0$, так как порядок α равен $2p$, тогда

$$\alpha+\alpha^3+...+\alpha^{p-2}+\alpha^{p+2}+...+\alpha^{2p-1}=1. \quad (3)$$

Введем вспомогательные многочлены $S_k(x)=\sum_{i\in D_k}x^k$ и $S_{k+2}(x)=\sum_{i\in 2D_k}x^k$, $k=0,1$, тогда по (1) $S(x)=2x^p+S_1(x)+2S_2(x)+3S_3(x)$. По определению классов вычетов D_k имеем: $S_1(\alpha^v)=S_0(\alpha^{gv})$, $S_2(\alpha^v)=S_0(\alpha^{2v})$ и $S_3(\alpha^v)=S_0(\alpha^{2gv})$.

Таким образом, для вычисления значений $S(\alpha^v)$ достаточно найти $S_0(\alpha^v)$.

Лемма 1. Если $v\in D_k$, $k=0,1$, то $S_0(\alpha^v)=S_0(\alpha^{g^k})$.

Доказательство. Если $v\in D_k$, то $vD_0=g^kD_0$, тогда $S_0(\alpha^v)=\sum_{i\in D_0}\alpha^{vi}=\sum_{j\in g^kD_0}\alpha^j=\sum_{i\in D_0}\alpha^{g^ki}$, что и доказывает лемму 1.

Из леммы 1 и формулы (3) имеем

$$S_0(\alpha)+S_0(\alpha^g)=1. \qquad (4)$$

Согласно (4), не нарушая общности, можно считать, что $S_0(\alpha)\neq 0$ и $2S_0(\alpha)\neq 0$.

Пусть

$$l=\begin{cases}0, \text{ если } p\equiv\pm1 \pmod 8,\\ 1, \text{ если } p\equiv\pm1 \pmod 8,\end{cases}$$

т. е. $l=0$, если 2 является квадратичным вычетом по модулю p и $l=1$ в противоположном случае [7].

Лемма 2. Если $v\in D_k$, то $S_0(\alpha^{2v})=-S_0(\alpha^{g^{k+l}})$, а если же $v\in 2D_k$, то $S_0(\alpha^{2v})=-S_0(\alpha^{g^k})$.

Доказательство. В силу выбора α и определения многочлена $S_0(x)$ имеем $S_0(\alpha^{p+2v})=-S_0(\alpha^{2v})$. Далее, $p+2v$ — нечетное число и $p+2v\equiv\theta^{l+k} \pmod p$ по выбору g и l, поэтому $p+2v \pmod{2p}\in D_{(k+l) \pmod 2}$. Применение леммы 1 завершает доказательство первого равенства, второе утверждение леммы 2 доказывается аналогично.

Леммы 1 и 2 показывают, что для вычисления значений $S_0(\alpha^v)$ достаточно найти $S_0(\alpha)$ и $S_0(\alpha^g)$, что и будет сделано в следующем разделе.

3. Метод вычисления значений ассоциированного многочлена последовательности

Напомним еще одно определение. Циклотомическим числом второго порядка $(m,n)_2$, где m,n — целые числа, называется число решений сравнения $\theta^i+1\equiv\theta^j \pmod p$, $i,j=0,1,\ldots,p-1$ при условии, что $i\equiv m \pmod 2$ и $j\equiv n \pmod 2$ [9]. Другими словами, если $H_m=\{\theta^{m+2t} \bmod p, t=1,\ldots,(p-1)/2\}$, то $(m,n)_2=|(H_m+1)\cap H_n|$.

Лемма 3. Если $m,n=0,1$, то $|(D_m+1)\cap 2D_n|=(m,n+l)_2$, где по-прежнему $l=0$, если 2 — квадратичный вычет по модулю p и $l=1$ в противоположном случае.

Доказательство. Согласно построению классов вычетов и определению l получаем, что $D_m \bmod p=H_m$ и $2D_n \bmod p=H_{(n+l) \pmod 2}$, отсюда и следует справедливость леммы 3.

Следующее утверждение является обобщением теоремы 1 из [3].

Теорема 1. Справедливо равенство

$$S_0^2(\alpha)=-(0,0)_2S_0(\alpha)-(0,1)_2S_0(\alpha^g)+\delta(p-1)/2,$$

где $\delta=\begin{cases}1, \text{ если } (p-1)/2 - \text{ четное число},\\ 0, \text{ иначе.}\end{cases}$

Воспользовавшись теоремой 1 и формулой (4) вычислим значения $S_0(\alpha)$ и $S_0(\alpha^g)$.

Лемма 4.

1. $S_0(\alpha)=1$ и $S_0(\alpha^g)=0$, если $p\equiv\pm1 \pmod{16}$;
2. $S_0(\alpha)=\rho$ и $S_0(\alpha^g)=1-\rho$, если $p\equiv\pm5 \pmod{16}$, где ρ удовлетворяет соотношению $\rho^2+3\rho+3=0$;
3. $S_0(\alpha)=3$ и $S_0(\alpha^g)=2$, если $p\equiv\pm9 \pmod{16}$;
4. $S_0(\alpha)=2+\rho$ и $S_0(\alpha^g)=3-\rho$, если $p\equiv\pm13 \pmod{16}$.

Доказательство. Для удобства обозначим $S_0(\alpha)$ через z, а $S_0(\alpha^g)$ — через y, тогда по теореме 1 и формуле (4) получаем, что

$$z^2=-(0,0)_2z-(0,1)_2(1-z)+\delta(p-1)/2. \qquad (5)$$

Пусть $p\equiv1 \pmod 4$, т. е. $p=1+4u$, $u\in\mathbb{Z}$, тогда $\delta=1$, $(0,0)_2=(p-5)/4=u-1$ и $(0,1)_2=(p-1)/4=u$ [9]. В этом случае соотношение (5) примет вид:

$$z^2=z+u. \qquad (6)$$

Решая в кольце R уравнение (6), при сделанных относительно $S_0(\alpha)$ предположениях, найдем значения z и y:

a) $z=1$ и $y=0$, если $u\equiv0 \pmod 4$;

b) $z=\rho$ и $y=1-\rho$, если $u\equiv1 \pmod 4$;

c) $z=3$ и $y=2$, если $u\equiv2 \pmod 4$;

d) $z=2+\rho$ и $z=3-\rho$, если $u\equiv3 \pmod 4$.

Вариант, когда $p\equiv3 \pmod 4$, исследуется аналогично.

Вычисленные значения $S_0(\alpha)$ и $S_0(\alpha^g)$ позволяют найти $S(\alpha^v)$ и рассчитать линейную сложность последовательности S по формуле (2), что и будет сделано в следующем параграфе.

4. Линейная сложность последовательности

Теорема 2. Пусть последовательность S определена по (1). Тогда $L=2p-1$, если $p\equiv3 \pmod 8$ и $L=2p$, если $p\equiv-3 \pmod 8$.

Доказательство. Покажем сначала, что $S(\alpha^v)\in R^*$ для $v\in D_0\cup D_1\cup 2D_0\cup 2D_1$.

Пусть $v\in D_0$, тогда по лемме 2 имеем $S(\alpha^v)=2+S_0(\alpha^g)-2S_0(\alpha^g)-3S_0(\alpha)$ или $S(\alpha^v)=1-2S_0(\alpha)$

по (4). Аналогично, если $v\in D_1$, то $S(\alpha^v)=1-2S_0(\alpha^g)$. Согласно лемме 4 в обоих случаях $S(\alpha^v)\in R^*$.

Пусть $v\in 2D_0$, тогда по лемме 2 имеем $S(\alpha^v)=2-S_0(\alpha)-2S_0(\alpha)-3S_0(\alpha^g)$, т. е. $S(\alpha^v)=3$ по (4). Последнее равенство имеет место и для $v\in 2D_1$.

Далее, по определению последовательности $S(\alpha^p)=S(-1)=2$, а $S(1)\equiv 2+3(p-1)\,(\mathrm{mod}\,4)$, т. е. $S(1)=0$ для $p\equiv 3\,(\mathrm{mod}\,8)$ и $S(1)\neq 0$ при $p\equiv -3\,(\mathrm{mod}\,8)$.

Пусть $C(x)=(x^{2p}-1)/(x-1)$, если $p\equiv 3\,(\mathrm{mod}\,8)$ и $C(x)=(x^{2p}-1)$, если $p\equiv -3\,(\mathrm{mod}\,8)$. Тогда $S(x)C(x)\equiv 0\left(\mathrm{mod}(x^{2p}-1)\right)$, т. е. $C(x)$ является ассоциированным многочленом последовательности S и $L\le \deg C(x)$.

Предположим, что $L<\deg C(x)$, тогда существует другой ассоциированный многочлен $C_1(x)$, степень которого меньше степени $C(x)$. А так как $S(x)C_1(x)\equiv 0\left(\mathrm{mod}(x^{2p}-1)\right)$, согласно (2), то это означает, что существует u ($u\neq 0$ для $p\equiv 3\,(\mathrm{mod}\,8)$) такое, что $S(\alpha^v)\in 2R$, что противоречит доказанному ранее.

Таким образом, $L=\deg C(x)$ и теорема 2 доказана.

В условиях теоремы 2 последовательности обладают высокой линейной сложностью.

Подобным же образом можно исследовать остальные случаи и показать, что здесь последовательность не обладает высокой линейной сложностью. В частности, имеет место следующее утверждение.

Теорема 3. Для линейной сложности последовательности S, определенной по (1), справедливо:

1. $L=p$ для $p\equiv -1\,(\mathrm{mod}\,16)$;
2. $L=p+1$ для $p\equiv 1\,(\mathrm{mod}\,16)$;
3. $L=(p+3)/2$ для $p\equiv -7\,(\mathrm{mod}\,16)$;
4. $L=(p+1)/2$ для $p\equiv 7\,(\mathrm{mod}\,16)$.

Теорема 3 завершает процесс вычисления линейной сложности последовательности S. Расчеты ее линейной сложности, выполненные по алгоритму Берлекэмпа-Месси, подтверждают справедливость полученных результатов.

Заключение

Рассмотрен метод вычисления линейной сложности циклотомических последовательностей над кольцом классов вычетов четвертого порядка. Вычислена линейная сложность четвертичных циклотомических последовательностей с периодом $2p$, сформированных на классах квадратичных вычетов. Предложенный метод вычисления линейной сложности может быть распространен на последовательности, формируемые на циклотомических классах более высокого порядка.

1. Cusick T.W, Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam: Elsevier, 1998. 474 p.
2. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 820 с.
3. Едемский В.А. О линейной сложности троичных последовательностей на основе классов степенных вычетов // Проблемы передачи информации. 2008. Т.44. №4. С.3-11.
4. Едемский В.А. О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискретная математика. 2010. Т.22. №1. С.74-82.
5. Едемский В.А., Иванов А.В. О линейной сложности последовательностей над конечным полем четвертого порядка // Вестник НовГУ. Сер.: Техн. науки. 2012. №68. С.56-59.
6. Kim Y.-J., Hong Y.-P., Song H.-Y. Autocorrelation of Some Quaternary Cyclotomic Sequences of Length 2p // IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences. 2008. V.E91-A:12. P.3679-3684.
7. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
8. Нечаев А.А. Код Кердока в циклической форме // Дискретная математика. 1989. Т.1. №4. С.123-139.
9. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.

References

1. Cusick T. W, Ding C., Renvall A. Stream Ciphers and Number Theory. Amsterdam, Elsevier Publ., 1998. 474 p.
2. Lidl R., Niederreiter H. Finite Fields (Encyclopedia of Mathematics and Its Applications), vol. 20. Reading, MA: Addison-Wesley, 1983. 820 p. (Russ. ed.: Lidl R., Niderraiter G. Konechnye polia. Moscow, Mir, Publ., 1988. 820 p.).
3. Edemskii V.A. O lineinoi slozhnosti troichnykh posledovatel'nostei na osnove klassov stepennykh vychetov [Linear complexity of ternary sequences formed on the basis of power residue classes]. Problemy peredachi informatsii – Problems of Information Transmission, 2008, vol. 44, no 4, pp. 287–294.
4. Edemskii V.A. O lineinoi slozhnosti dvoichnykh posledovatel'nostei na osnove klassov bikvadratichnykh i shesterichnykh vychetov [On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes]. Diskretnaia matematika – Discrete Mathematics and Applications, 2010, vol. 20, no. 1, pp. 75–84.
5. Edemskii V.A., Ivanov A.V. O linejnoj slozhnosti posledovatel'nostej nad konechnym polem chetvertogo porjadka [On the linear complexity of sequences over a quartic finite field]. Vestnik NovGU. Ser. Tekhnicheskie nauki – Vestnik NovSU. Issue: Engineering Sciences, 2012, vol. 68, pp. 56-59.
6. Kim Y.-J., Hong Y.-P., Song H.-Y. Autocorrelation of Some Quaternary Cyclotomic Sequences of Length 2p. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences. 2008, vol. E91-A:12, pp. 3679-3684.
7. Ireland K., Rosen M. A. Classical Introduction to Modern Number Theory. Springer, Berlin, 1982.416 p. (Russ. ed.: Aierlend K., Rouzen M. Klassicheskoe vvedenie v sovremennuiu teoriiu chisel. Moscow, Mir Publ., 1987. 416 p.).
8. Nechaev A.A. Kod Kerdoka v tsiklicheskoi forme [Kerdock code in a cyclic form]. Diskretnaia matematika – Discrete Mathematics and Applications, 1991, vol. 1, no.4, pp. 365-384.
9. Hall M. Combinatorial Theory. Wiley, New York, 1975. 423 p. (Russ. ed.: Kholl M. Kombinatorika. Moscow, Mir Publ., 1970. 423 p.).