УДК 519.7

ЗАМЕТКИ О ЛИНЕЙНОЙ СЛОЖНОСТИ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ФОРМИРУЕМЫХ НА БИКВАДРАТИЧНЫХ ВЫЧЕТАХ

В.А.Едемский, А.И.Пальвинский

NOTES ON THE LINEAR COMPLEXITY OF THE SEQUENCES CONSTRUCTED ON BIQUADRATIC RESIDUES

V.A.Edemskiy, A.I.Palvinsky

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

Вычислена линейная сложность семейства бинарных последовательностей, сформированных на основе классов биквадратичных вычетов, с оптимальной периодической автокорреляционной функцией.

Ключевые слова: бинарные последовательности, линейная сложность, конечное поле, классы биквадратичных вычетов

We derived the linear complexity of a family of binary sequences with optimal autocorrelation constructed on the basis of biquadratic residue classes.

Keywords: binary sequences, linear complexity, finite field, biquadratic residue classes

Введение

Периодическая автокорреляционная функция, сбалансированность и линейная сложность являются важными характеристиками бинарных последовательностей [1]. В частности, последовательности с высокой линейной сложностью важны для криптографических приложений [1,2]. Автокорреляционные свойства почти сбалансированных бинарных последовательностей, сформированных на основе классов квадратичных и биквадратичных вычетов по простому модулю p, хорошо известны. Линейная сложность последовательностей Лежандра над конечным полем второго порядка вычислена в [3], порядка p — в [4], отличного от p — в [5]. В то же время линейная сложность последовательности с оптимальной периодической автокорреляционной функцией, сформированных на двух классах биквадратичных вычетов, известна только над полями второго [6] и p-го порядков [5]. В этой статье исследуется линейная сложность и минимальный многочлен вышеупомянутой последовательности над конечными полями других порядков.

Для вычисления линейной сложности обобщается метод, предложенный ранее в [6,7], для последовательностей над полями второго и третьего порядков.

1. Основные определения

Пусть $p=4R+1$ — нечетное простое число и θ — первообразный корень по модулю p [8]. Обозначим через $D_0=\{\theta^{2s} \bmod 2p; s=1,...,(p-1)/2\}$ и $D_1=\theta D_0$, соответственно, классы квадратичных вычетов и невычетов по модулю p. Пусть $H_k=\{\theta^{k+4t} \bmod p, t=0,\dots,R-1\}$, $k=0,\dots,3$ — циклотомические класссы четвертого порядка по модулю p [9]. Здесь H_0 — класс биквадратичных вычетов по модулю p. Тогда для Z_p — кольца классов вычетов по модулю p, справедливы следующие разбиения:

$$Z_p=D_0\cup D_1\cup\{0\} \text{ и } Z_p=H_0\cup H_1\cup H_2\cup H_3\cup\{0\}.$$

Рассмотрим бинарную последовательность S, определяемую на периоде p следующим образом [10]:

$$s_i=\begin{cases}1, \text{если } i\in H_0\cup H_1,\\ -1, \text{в ост. случаях.}\end{cases} \quad (1)$$

Согласно [10], последовательность S обладает оптимальной периодической автокорреляционной функцией, когда $p=x^2+4$, $x\equiv 1(\bmod 4)$. Исследуем её линейную сложность над конечным полем Φ_{q^r}, где q — простое число, отличное от двух и p.

Минимальный полином $m(x)$ и линейную сложность (L) последовательности S можно вычислить по следующим формулам [2]:

$$m(x)=(x^p-1)/\text{НОД}(x^p-1,S(x)),$$
$$L=p-\deg\text{НОД}(x^p-1,S(x)), \quad (2)$$

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

Пусть α — примитивный корень степени N из единицы в расширении поля Φ_{q^r}, тогда $x^p-1=\prod_{j=0}^{p-1}(x-\alpha^j)$. Следовательно, согласно (2), для вычисления минимального многочлена и линейной сложности последовательности S, сформированной по (1), достаточно определить число корней многочлена $S(x)$ в множестве $\{\alpha^v, v=0,1,...,p-1\}$. Метод вычисления значений $S(\alpha^v)$ будет представлен в следующем разделе.

2. Метод вычисления значений многочлена последовательности

Введем вспомогательные многочлены $S_2(x)=\sum_{i\in D_0}x^i$ и $S_4(x)=\sum_{i\in H_0}x^i$.

Лемма 1.

1) Если $v\in D_k$, $k=0,1$, то $S_2(\alpha^v)=S_2(\alpha^{\theta^k})$;

2) Если $v\in H_k$, $k=0,1,2,3$, то $S_4(\alpha^v)=S_4(\alpha^{\theta^k})$.

Таким образом, если $v\in H_k$, то, согласно лемме 1 и определению (1), справедливо следующее соотношение:

$$S(\alpha^v)=S_4(\alpha^{\theta^k})+S_4(\alpha^{\theta^{k+1}}). \quad (3)$$

Следовательно, для вычисления значений $S(\alpha^v)$ достаточно найти $S_4(\alpha^{\theta^k})$. Далее, так как $1+\alpha+\ldots+\alpha^{p-1}=0$, то по лемме 1 получаем, что

$$\begin{gathered}S_2(\alpha)+S_2(\alpha^\theta)=-1 \text{ и}\\ S_4(\alpha)+S_4(\alpha^\theta)+S_4(\alpha^{\theta^2})+S_4(\alpha^{\theta^3})=-1.\end{gathered} \quad (4)$$

Напомним еще одно определение. Циклотомическим числом $(m,n)_d$ порядка d, 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 $i\equiv m \pmod d$ и $j\equiv n \pmod d$ [9]. Другими словами, $(m,n)_2=|(D_m+1)\cap D_n|$ и $(m,n)_4=|(H_m+1)\cap H_n|$.

Следующее утверждение является обобщением теоремы 1 из [6].

Теорема 1. Для $d=2,4$ и $k=0,\ldots,d-1$ справедливы равенства:

$$S_d(\alpha)S_d(\alpha^{\theta^k})=\sum_{f=0}^{d-1}(k,f)_dS_d(\alpha^{\theta^f})+\delta,$$

где $\delta=\begin{cases}(p-1)/d, \text{если } (p-1)/d\equiv 0 \pmod 2 \text{ и } k=0\\ \text{или } (p-1)/d\equiv 1 \pmod 2 \text{ и } k=d/2,\\ 0, \text{в ост. случаях.}\end{cases}$

Воспользовавшись теоремой 1 и формулой (4) вычислим значения $S_2(\alpha)$ и $S_2(\alpha^\theta)$.

Лемма 2. Если $p\equiv 5 \pmod 8$, то $S_2(\alpha)$ и $S_2(\alpha^\theta)$ удовлетворяют уравнению: $y^2+y-(p-1)/4=0$.

Доказательство. По условию $p\equiv 1 \pmod 4$, тогда $\delta=0$, $(1,0)_2=(1,1)_2=(p-1)/4$ [9]. Таким образом, согласно теореме 1, $S_2(\alpha)S_2(\alpha^\theta)=(1,0)_2S_2(\alpha)+(1,1)_2S_2(\alpha^\theta)$ или $S_2(\alpha)S_2(\alpha^\theta)=-(p-1)/4$. Следовательно, $S_2(\alpha), S_2(\alpha^\theta)$ — корни уравнения $y^2+y-(p-1)/4=0$, так как $S_2(\alpha)+S_2(\alpha^\theta)=-1$ по (4). Лемма 2 доказана.

Пусть $x=1+4t, t\in Z$, тогда $p=5+8t+16t^2$.

Лемма 3. Если $p=5+8t+16t^2$, то:

1) $S_4(\alpha)$ и $S_4(\alpha^{\theta^2})$ являются корнями уравнения $z^2-S_2(\alpha)z+S_2(\alpha)t+1+2t+3t^2=0$;

2) $S_4(\alpha^\theta)$ и $S_4(\alpha^{\theta^3})$ являются корнями уравнения $y^2-S_2(\alpha^\theta)y+S_2(\alpha^\theta)t+1+t+3t^2=0$.

Доказательство. По определению вспомогательных многочленов $S_4(\alpha)+S_4(\alpha^{\theta^2})=S_2(\alpha)$ и $S_4(\alpha^\theta)+S_4(\alpha^{\theta^3})=S_2(\alpha^\theta)=-1-S_2(\alpha)$. Далее, $(2,0)_4=(2,2)_4=(p-7+2x)/16$ и $(2,1)_4=(2,3)_4=(p-3-2x)/16$. Тогда, согласно теореме 1, $S_4(\alpha)S_4(\alpha^{\theta^2})=(0,0)_4S_2(\alpha)+(0,1)_4S_2(\alpha^\theta)+(p-1)/4$. Так как $x=1+4t$ и $p=5+8t+16t^2$, то $S_4(\alpha)S_4(\alpha^{\theta^2})=S_2(\alpha)t+1+2t+3t^2$. Из последней формулы и получаем первое утверждение леммы 3.

Аналогично $S_4(\alpha^\theta)S_4(\alpha^{\theta^3})=(2,0)_4S_2(\alpha^\theta)+(2,1)_4S_2(\alpha)+(p-1)/4$ или $S_4(\alpha^\theta)S_4(\alpha^{\theta^3})=S_2(\alpha^\theta)t+1+t+3t^2$. Лемма 3 доказана.

3. Линейная сложность последовательности

Теорема 2. Пусть последовательность S определена по (1). Тогда

$$L=\begin{cases}3(p-1)/4, \text{если } p\equiv 1 \pmod q,\\ p, \text{ если } p\not\equiv 1 \pmod q.\end{cases}$$

Доказательство. В силу формулы (2) вопрос о линейной сложности последовательности S сводится к определению числа корней многочлена $S(x)$ в множестве $\{\alpha^v, v=0,1,\ldots,p-1\}$. Пусть $v\in H_k$ и $S(\alpha^v)=0$, тогда $S_4(\alpha^{\theta^k})=-S_4(\alpha^{\theta^{k+1}})$, согласно (3). По лемме 3 числа $S_4(\alpha^{\theta^k}), S_4(\alpha^{\theta^{k+1}})$ являются корнями двух различных уравнений, т. е. в этом случае существует w такое, что w — корень уравнения $z^2-S_2(\alpha)z+S_2(\alpha)t+1+2t+3t^2=0$, а $(-w)$ — корень уравнения $y^2-S_2(\alpha^\theta)y+S_2(\alpha^\theta)t+1+t+3t^2=0$. Решая одновременно эти два уравнения, находим: $w=-t-2S_2(\alpha)t$ и $(4t^2+2t)S_2(\alpha)^2+(4t^2+2t)S_2(\alpha)+4t^2+2t+1=0$. С другой стороны, по лемме 2 $S_2(\alpha)$ удовлетворяет квадратному уравнению $y^2+y-(p-1)/4=0$. Сравнивая уравнения, получаем, что если $S(\alpha^v)=0$, то $p\equiv 1 \pmod q$.

Далее, если $p\equiv 1 \pmod q$, то в силу леммы 2, $S_2(\alpha)=0$ и $S_2(\alpha^\theta)=-1$ (или наоборот), тогда с точностью до перестановки пар $S_4(\alpha)=t$, $S_4(\alpha^\theta)=t, S_4(\alpha^{\theta^2})=-t, S_4(\alpha^{\theta^3})=-1-t$. Согласно (3), это означает, что $\left|\{v: S(\alpha^v)=0, v=1,\ldots,p-1\}\right|=(p-1)/4$. Так как $S(1)=(p-1)/2$, то применение формулы (2) завершает доказательство теоремы 2.

В условиях теоремы 2 последовательности обладают высокой линейной сложностью.

Расчеты линейной сложности последовательности S, выполненные по алгоритму Берлекэмпа-Месси, подтверждают справедливость полученных результатов.

Заключение

Исследована линейная сложность почти сбалансированных бинарных последовательностей, сформированных на основе классов биквадратичных вычетов, и обладающих оптимальной периодической автокорреляционной функцией. Показано, что рассматриваемые последовательности обладают высокой линейной сложностью.

Работа выполнена при финансовой поддержке проектной части государственного задания в сфере научной активности Министерства образования и науки Российской Федерации, проект №1.949.2014/К.

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. Ding C., Helleseth T., Shan W. On the linear complexity of Legendre sequences // IEEE Trans. Inform. Theory. 1998. V.44. P.1276-1278.
4. Hassan A., Winterhof A. On the k-error linear complexity over *Fp* of Legendre and Sidelnikov sequences // Des. Codes Crypt. 2006. V.40. P.369-374.
5. Wang Q., Lin D., Guang X. On the Linear Complexity of Legendre Sequences Over F_q // IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences. 2014. V.E97-A:7. P.1627-1630
6. Едемский В.А. О линейной сложности троичных последовательностей на основе классов степенных вычетов // Проблемы передачи информации. 2008. Т.44. №4. С.3-11.
7. Едемский В.А. О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискр. мат. 2010. Т.22. №1. С.74-82.
8. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 416 с.
9. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.
10. Ding C., Helleseth T., Lam K.Y. Several Classes of binary sequences with three-level autocorrelation// IEEE Trans. Inform. Theory. 1999. V.45. P.2601-2606.

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, eds. Finite Fields. Cambridge, Cambridge University Press, 1985. (Russ. ed.: Lidl R., Niderraiter G. Konechnye polia. Moscow, “Mir” Publ., 1988. 808 p.).
3. Ding C., Helleseth T., Shan W. On the linear complexity of Legendre sequences. IEEE Trans. Inform. Theory, 1998. , vol. 44, pp. 1276–1278.
4. Hassan A., Winterhof A. On the k-error linear complexity over Fp of Legendre and Sidelnikov sequences. Designs, Codes and Cryptography, 2006, vol. 40, pp. 369-374.
5. Wang Q., Lin D., Guang X. On the Linear Complexity of Legendre Sequences Over Fq. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, vol. E97-A, no.7, pp. 1627-1630.
6. 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.
7. 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. 22, no. 1, pp. 74-82.
8. Ireland K., Rosen M.A. Classical Introduction to Modern Number Theory. Springer, Berlin, 1982. (Russ. ed.: Aierlend K., Rouzen M. Klassicheskoe vvedenie v sovremennuiu teoriiu chisel. Moscow, Mir Publ., 1987. 416 p.).
9. Hall M. Combinatorial Theory. Wiley, New York, 1975. 423 p. (Russ. ed.: Kholl M. Kombinatorika. Moscow, Mir Publ., 1970. 423 p.).
10. Ding C., Helleseth T., Lam K.Y. Several Classes of binary sequences with tree-level autocorrelation. IEEE Transactions on Information Theory, 1999, vol. 45, pp. 2601-2606.