

О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов

© 2010 г. В. А. Едемский

Предложен метод расчета линейной сложности двоичных периодических последовательностей, сформированных на основе классов биквадратичных и шестеричных вычетов, посредством разложения периода последовательности на сумму квадратов целых чисел. Значения многочлена последовательности вычисляются с использованием циклотомических чисел четвертого и шестого порядков.

1. Введение

Линейная сложность последовательности определяется как длина самого короткого линейного регистра сдвига с обратными связями, с помощью которого можно воссоздать последовательность, и является ее важным показателем [1]. Последовательности, обладающие высокой линейной сложностью, важны для криптографических приложений. Известны алгоритмы определения минимального многочлена последовательности и ее линейной сложности, например, алгоритм Берлекэмп–Месси [1]. В то же время для ряда периодических последовательностей, сформированных на основе классов степенных вычетов, с хорошими автокорреляционными свойствами линейная сложность определяется видом периода последовательности [2–4].

Цель настоящей статьи заключается в определении линейной сложности двоичных периодических последовательностей, сформированных на основе классов биквадратичных и шестеричных вычетов, посредством разложения периода последовательности на сумму квадратов целых чисел. Значения многочлена последовательности вычисляются с использованием циклотомических чисел четвертого и шестого порядков. Данный метод может быть использован для вычисления линейной сложности других последовательностей на основе классов степенных вычетов при известных циклотомических числах.

Пусть $p = dR + 1$ — простое число, где d, R — натуральные числа, $d \neq 1$ и H_k — класс степенных вычетов с номером k :

$$H_k = \{\theta^{k+dt}, t = 0, 1, \dots, R-1\}, \quad k = 0, 1, \dots, d-1,$$

где θ — первообразный корень по простому модулю.

Рассмотрим двоичную последовательность $X = \{x_i\}$ периода p , сформированную на основе классов степенных вычетов:

$$x_i = \begin{cases} 1, & i \in H_k, k \in I, \\ 0 & \text{в остальных случаях.} \end{cases} \quad (1)$$

Здесь I — непустое подмножество множества индексов от 0 до $d - 1$. Обозначим

$$S(t) = x_0 + x_1 t + \dots + x_{p-1} t^{p-1}$$

многочлен последовательности X , принадлежащий $GF(2)[t]$. Согласно [2], линейная сложность последовательности L определяется соотношением

$$L = p - |\{n \mid S(\alpha^n) = 0, n = 0, 1, \dots, p - 1\}|, \quad (2)$$

где α — примитивный корень p степени из единицы в поле разложения K многочлена $t^p - 1$ над $GF(2)$. А так как θ — первообразный корень по модулю p , задача вычисления линейной сложности последовательности X сводится к определению значений $S(\alpha^{\theta^l})$, $l = 1, \dots, p - 1$, и $S(1)$ в поле K .

В следующем разделе рассматривается способ вычисления значений $S(\alpha^{\theta^l})$.

2. Многочлен последовательности и циклотомические числа

Введем дополнительный многочлен

$$S_d(t) = \sum_{n \in H_0} t^n.$$

Следующая лемма является несложным обобщением утверждений, доказанных в [2, 4] для $d = 2$ и $d = 6$.

Лемма 1. Для $f = 0, 1, \dots, d - 1$ справедливы равенства

- (1) $\sum_{n \in H_f} \alpha^n = S_d(\alpha^{\theta^f})$ для $f = 0, 1, \dots, d - 1$;
- (2) $S_d(\alpha^{\theta^f + dg}) = S_d(\alpha^{\theta^f})$ для любого целого числа g ;
- (3) если $\text{ind}_\theta 2 \equiv l \pmod{d}$, то $S_d(\alpha^{\theta^l}) = S_d^2(\alpha)$;
- (4) если $\text{ind}_\theta 2 \equiv 0 \pmod{d}$, то $S_d(\alpha^{\theta^g}) \in \{0, 1\}$ для любого целого числа g ;
- (5) $S_d(\alpha^{\theta^f}) \neq 1$ хотя бы для одного $f = 0, 1, \dots, d - 1$.

Так как

$$0 = \alpha^p - 1 = (\alpha - 1)(1 + \alpha + \dots + \alpha^{p-1}),$$

согласно лемме 1, в поле характеристики два

$$S_d(\alpha) + S_d(\alpha^\theta) + \dots + S_d(\alpha^{\theta^{d-1}}) = 1. \quad (3)$$

Согласно определению,

$$S(\alpha^{\theta^l}) = \sum_{k \in I} S_d(\alpha^{\theta^{k+l}}),$$

таким образом, в силу леммы 1 и определения (2) для нахождения линейной сложности L достаточно найти значения $S_d(\alpha^{\theta^f})$, $f = 0, 1, \dots, d-1$.

Обозначим $(k, f)_d$ циклотомические числа порядка d (см. [5]).

Теорема 1. При $k = 0, 1, \dots, d-1$

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

где

$$\delta = \begin{cases} R, & \text{если } R \equiv 0 \pmod{2}, k = 0 \text{ или } R \equiv 1 \pmod{2}, k = d/2, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Доказательство. Согласно определению $S_d(t)$ и H_0 ,

$$S_d(\alpha)S_d(\alpha^{\theta^k}) = \sum_{u,v=0}^{R-1} \alpha^{\theta^{du+\theta^k+dv}}.$$

Если $\theta^{du} + \theta^{k+dv} \not\equiv 0 \pmod{p}$, то существуют числа f, s , $f \in \{0, 1, \dots, d-1\}$, $s \in \{0, 1, \dots, R-1\}$, такие, что $\theta^{du} + \theta^{dv} \equiv \theta^{f+ds} \pmod{p}$. При каждом значении s число пар (u, v) , являющихся решениями последнего сравнения, совпадает с циклотомическим числом $(k, f)_d$ порядка d (см. [5]). Таким образом,

$$\sum_{u,v=0}^{R-1} \alpha^{\theta^{du+\theta^k+dv}} = \sum_{f=0}^{d-1} \sum_{s=0}^{R-1} (k, f)_d \alpha^{\theta^{f+ds}} + \delta = \sum_{f=0}^{d-1} (k, f)_d S_d(\alpha^{\theta^f}) + \delta,$$

где δ равно числу решений сравнения $\theta^{du} + \theta^{k+dv} \equiv 0 \pmod{p}$. Справедливо сравнение $-1 \equiv \theta^{dR/2} \pmod{p}$, поэтому число δ именно таково, как указано в условиях теоремы, что и требовалось доказать.

Следствие 1. Для любого целого l

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

Теорема 1 и следствие 1 позволяют рассчитать значения $S_d(\alpha^{\theta^f})$, $f = 0, 1, \dots, d-1$, а значит и $S(\alpha^{\theta^f})$, $f = 0, 1, \dots, d-1$, при известных циклотомических числах порядка d , что, согласно (2), делает возможным определение линейной сложности последовательности.

Воспользовавшись известными формулами для вычисления циклотомических чисел [5, 6], в следующих разделах мы определим линейную сложность последовательностей (1) для $d = 4, 6$.

3. Линейная сложность последовательностей на основе классов биквадратичных вычетов с периодом $p = 4R + 1$

Циклотомические числа четвертого порядка определяются разложением (см. [5])

$$p = x^2 + 4y^2, \quad x = 1 + 4z,$$

где x, y, z — целые числа, и зависят от четности R , совпадающей с четностью y .

3.1. Пусть $R \equiv 0 \pmod{2}$, тогда $y = 2w$. Рассчитав по формулам, приведенным в [5], вычеты циклотомических чисел четвертого порядка по модулю два

$$\begin{aligned} 16(2, 0)_4 &= 16(2, 2)_4 = p - 3 + 2x, \\ 16(2, 1)_4 &= 16(2, 3)_4 = p + 1 - 2x, \end{aligned}$$

получаем по теореме 1 и следствию 1 в поле K следующую систему:

$$\begin{aligned} S_4(\alpha)S_4(\alpha^{\theta^2}) &= w(S_4(\alpha) + S_4(\alpha^{\theta^2})) + (z + w)(S_4(\alpha^\theta) + S_4(\alpha^{\theta^3})), \\ S_4(\alpha^\theta)S_4(\alpha^{\theta^3}) &= (z + w)(S_4(\alpha) + S_4(\alpha^{\theta^2})) + w(S_4(\alpha^\theta) + S_4(\alpha^{\theta^3})). \end{aligned} \quad (4)$$

Если $y \equiv 0 \pmod{2}$, то $\text{ind}_\theta 2 \equiv 0 \pmod{2}$ (см. [7]). Согласно лемме 1 и равенству (3), можно считать, не нарушая общности, что $S_2(\alpha) = 1, S_2(\alpha^\theta) = 0$. Тогда

$$S_4(\alpha) + S_4(\alpha^{\theta^2}) = 1, \quad S_4(\alpha^\theta) + S_4(\alpha^{\theta^3}) = 0,$$

и система (4) примет вид

$$\begin{aligned} S_4(\alpha)S_4(\alpha^{\theta^2}) &= z \\ S_4(\alpha^\theta)S_4(\alpha^{\theta^3}) &= z + w. \end{aligned} \quad (5)$$

Пусть $\mathbf{S} = (S_4(\alpha), S_4(\alpha^\theta), S_4(\alpha^{\theta^2}), S_4(\alpha^{\theta^3}))$. Решая систему (5), получаем, что

- (1) $\mathbf{S} = (1, 0, 0, 0)$ или $S = (0, 0, 1, 0)$, если $z \equiv 0 \pmod{2}, w \equiv 0 \pmod{2}$;
- (2) $\mathbf{S} = (1, 1, 0, 1)$ или $S = (0, 1, 1, 1)$, если $z \equiv 1 \pmod{2}, w \equiv 0 \pmod{2}$;
- (3) $\mathbf{S} = (\gamma, 1, 1 - \gamma, 1)$, где γ — корень уравнения $\gamma^2 + \gamma + 1 = 0$, если $z \equiv 0 \pmod{2}, w \equiv 1 \pmod{2}$;
- (4) $\mathbf{S} = (\gamma, 0, 1 - \gamma, 0)$, если $z \equiv 1 \pmod{2}, w \equiv 1 \pmod{2}$.

Найденные значения $S_4(\alpha), S_4(\alpha^\theta), S_4(\alpha^{\theta^2}), S_4(\alpha^{\theta^3})$ позволяют определить по (2) линейную сложность любой последовательности, сформированной по (1) на основе классов биквадратичных вычетов. В частности, имеет место следующее утверждение.

Лемма 2. Если

$$p = (1 + 4z)^2 + 16w^2$$

и двоичная последовательность сформирована по (1) на основе одного класса биквадратичных вычетов, то ее линейная сложность

$$L_1 = \begin{cases} (p-1)/4, & z \equiv 0 \pmod{2}, w \equiv 0 \pmod{2}, \\ 3(p-1)/4, & z \equiv 1 \pmod{2}, w \equiv 0 \pmod{2}, \\ p-1, & z \equiv 0 \pmod{2}, w \equiv 1 \pmod{2}, \\ (p-1)/2, & z \equiv 1 \pmod{2}, w \equiv 1 \pmod{2}, \end{cases}$$

а если на основе трех классов биквадратичных вычетов, то

$$L_3 = \begin{cases} 3(p-1)/4, & z \equiv 0 \pmod{2}, w \equiv 0 \pmod{2}, \\ (p-1)/4, & z \equiv 1 \pmod{2}, w \equiv 0 \pmod{2}, \\ (p-1)/2, & z \equiv 0 \pmod{2}, w \equiv 1 \pmod{2}, \\ p-1, & z \equiv 1 \pmod{2}, w \equiv 1 \pmod{2}. \end{cases}$$

Доказательство. Если последовательность сформирована на основе одного класса биквадратичных вычетов, то число $f = 0, 1, 2, 3$ таких, что $S(\alpha^{\theta^f}) = 0$ совпадает с числом нулей в матрице \mathbf{S} , а если же X сформирована на основе трех классов, то с числом единиц в матрице \mathbf{S} , так как $S(\alpha^{\theta^f}) = 1 - S_4(\alpha^{\theta^f})$ согласно (3). Применение формулы (2) с учетом леммы 1 завершает доказательство.

Если последовательность сформирована на основе двух классов биквадратичных вычетов, то при $I = \{0, 1\}$ ее линейная сложность

$$L_2 = \begin{cases} (p-1)/2, & \text{если } w \equiv 0 \pmod{2}, \\ p-1, & \text{если } w \equiv 1 \pmod{2}, \end{cases}$$

а при $I = \{0, 2\}$ значение $L_2 = (p-1)/2$ для $p = (1+4z)^2 + 16w^2$. Это известный результат [2, 3].

3.2. Пусть $R \equiv 1 \pmod{2}$.

Лемма 3. Если

$$p = x^2 + 4(1+2w)^2$$

и двоичная последовательность сформирована по (1), то при любом числе классов биквадратичных вычетов, отличном от четырех, ее линейная сложность

$$L = \begin{cases} p, & \text{если } R|I| \equiv 1 \pmod{2}, \\ p-1, & \text{если } R|I| \equiv 0 \pmod{2}. \end{cases}$$

Доказательство. Если $y \equiv 1 \pmod{2}$, то $\text{ind}_\theta 2 \not\equiv 0 \pmod{2}$ (см. [7]). Не нарушая общности, будем считать, что $\text{ind}_\theta 2 \equiv 1 \pmod{4}$ (если $\text{ind}_\theta 3 \equiv 3 \pmod{4}$, то заменим θ на θ^{-1}). Тогда, в силу леммы 1, $S_4(\alpha^\theta) = S_4^2(\alpha)$, следовательно, и $S(\alpha^\theta) = S^2(\alpha)$. Таким образом, либо все значения $S(\alpha^{\theta^l}) = 0$, либо $S(\alpha^{\theta^l}) \neq 0$ при $l = 1, \dots, p-1$. Первый вариант невозможен, если число классов биквадратичных вычетов, используемых при построении последовательности, меньше четырех.

Таким образом, линейная сложность последовательности $L = p-1$, если $S(1) = 0$, и $L = p$ в противном случае.

Таблица 1. Вычеты циклотомических чисел шестого порядка по модулю два

$R \equiv 1 \pmod{2}, A = 4 + 6a$				$R \equiv 0 \pmod{2}, A = 1 + 6a$			
B	$3 + 6b$	$5 + 6b$	$1 + 6b$	B	$6b$	$2 + 6b$	$4 + 6b$
$(0, 0)_6$	a	0	0	$(0, 0)_6$	$1 + b$	0	0
$(0, 1)_6$	0	$1 + a$	0	$(0, 1)_6$	0	$1 + b$	0
$(0, 2)_6$	0	0	a	$(0, 2)_6$	0	0	$1 + b$
$(0, 3)_6$	$1 + a$	0	0	$(0, 3)_6$	b	0	0
$(0, 4)_6$	0	a	0	$(0, 4)_6$	0	b	0
$(0, 5)_6$	0	0	$1 + a$	$(0, 5)_6$	0	0	b
$(1, 0)_6$	$a + b$	$1 + b$	$1 + a + b$	$(1, 2)_6$	a	a	a
$(2, 0)_6$	$1 + a + b$	$a + b$	b	$(1, 3)_6$	a	a	$a + b$
$(1, 2)_6$	1	$1 + a$	$1 + a$	$(1, 4)_6$	a	$1 + a + b$	a
$(2, 1)_6$	1	a	a	$(2, 4)_6$	a	$1 + a$	$1 + a$

Наибольший общий делитель

$$\text{GCD}(t^p - 1, S(t)) = \begin{cases} \prod_f \prod_{s=0}^{R-1} (t - \alpha^{\theta^f + 4s}), & S(\alpha^{\theta^f}) = 0, S(1) \neq 0, \\ (t - 1) \prod_f \prod_{s=0}^{R-1} (t - \alpha^{\theta^f + 4s}), & S(\alpha^{\theta^f}) = 0, S(1) = 0, \end{cases}$$

поэтому найденные значения $S_4(\alpha^{\theta^f})$ позволяют также найти характеристический многочлен последовательности $f(t) = (t^p - 1) / \text{GCD}(t^p - 1, S(t))$.

4. Линейная сложность последовательностей на основе классов шестеричных вычетов с периодом $p = 6R + 1$

Циклотомические числа шестого порядка определяются разложением $p = A^2 + 3B^2$, $A \equiv 1 \pmod{3}$ (см. [5, 6]), которое определяет значение A однозначно, B — с точностью до знака. Знак B определим, как в [6], при этом, если $B \equiv 0 \pmod{3}$, то $B/3 \equiv \text{ind}_\theta 3 \pmod{3}$ и всегда $B \equiv -\text{ind}_\theta 2 \pmod{3}$. Если $A \equiv 1 \pmod{3}$, то четность R совпадает с четностью B . Воспользовавшись формулами для циклотомических чисел шестого порядка из [5, 6], приведем табл. 1 для вычетов циклотомических чисел по модулю два (a, b — целые числа).

В следующих двух подраздела, используя теорему 1, вычислим значения $S_6(\alpha^{\theta^f})$.

4.1. Пусть $B \equiv 0 \pmod{3}$, то есть $\text{ind}_\theta 2 \equiv 0 \pmod{3}$.

Согласно (3) и лемме 1 одно из чисел $S_3(\alpha)$, $S_3(\alpha^\theta)$, $S_3(\alpha^{\theta^2})$ равно единице, а остальные — нулю, не нарушая общности, можно считать, что $S_3(\alpha) = 1$. Тогда

$$\begin{aligned} S_6(\alpha) + S_6(\alpha^{\theta^3}) &= 1, \\ S_6(\alpha^\theta) + S_6(\alpha^{\theta^4}) &= 0, \\ S_6(\alpha^{\theta^2}) + S_6(\alpha^{\theta^5}) &= 0. \end{aligned} \tag{6}$$

Воспользовавшись теоремой 1, табл. 1, равенством (6) и свойствами циклотомических чисел, получаем следующие системы уравнений: если $R \equiv 1 \pmod{2}$, то

$$\begin{aligned} S_6(\alpha)S_6(\alpha^{\theta^3}) &= a + 1, \\ S_6(\alpha^\theta)S_6(\alpha^{\theta^4}) &= a + b, \\ S_6(\alpha^{\theta^2})S_6(\alpha^{\theta^5}) &= a + b + 1; \end{aligned} \quad (7)$$

если $R \equiv 0 \pmod{2}$, то

$$\begin{aligned} S_6(\alpha)S_6(\alpha^{\theta^3}) &= b, \\ S_6(\alpha^\theta)S_6(\alpha^{\theta^4}) &= a, \\ S_6(\alpha^{\theta^2})S_6(\alpha^{\theta^5}) &= a. \end{aligned} \quad (8)$$

Дополнительно отметим, что если $p \equiv \pm 1 \pmod{8}$, $a \equiv 1 \pmod{2}$ при нечетном R или $b \equiv 0 \pmod{2}$ при четном R , то $\text{ind}_\theta 2 \equiv 0 \pmod{6}$ (см. [7]) и можно считать, что $S_6(\alpha) = 1$, в силу леммы 1 и (6).

Решая системы (7) и (8), с учетом (6) и сделанного замечания, получим следующие варианты для $\mathbf{S} = (S_6(\alpha), S_6(\alpha^\theta), \dots, S_6(\alpha^{\theta^5}))$: если $R \equiv 1 \pmod{2}$, то

- (1) $\mathbf{S} = (1, 1, 0, 0, 1, 0)$, если $a \equiv 1 \pmod{2}$, $b \equiv 0 \pmod{2}$;
- (2) $\mathbf{S} = (1, 0, 1, 0, 0, 1)$, если $a \equiv 1 \pmod{2}$, $b \equiv 1 \pmod{2}$;
- (3) $\mathbf{S} = (\gamma, 0, 1, 1 - \gamma, 0, 1)$, где γ — корень уравнения $\gamma^2 + \gamma + 1 = 0$, если $a \equiv 0 \pmod{2}$, $b \equiv 0 \pmod{2}$;
- (4) $\mathbf{S} = (\gamma, 1, 0, 1 - \gamma, 1, 0)$, если $a \equiv 0 \pmod{2}$, $b \equiv 1 \pmod{2}$;

если же $R \equiv 0 \pmod{2}$, то

- (1) $\mathbf{S} = (1, 0, 0, 0, 0, 0)$, если $a \equiv 0 \pmod{2}$, $b \equiv 0 \pmod{2}$;
- (2) $\mathbf{S} = (1, 1, 1, 0, 1, 1)$, если $a \equiv 1 \pmod{2}$, $b \equiv 0 \pmod{2}$;
- (3) $\mathbf{S} = (\gamma, 0, 0, 1 - \gamma, 0, 0)$, если $a \equiv 0 \pmod{2}$, $b \equiv 1 \pmod{2}$;
- (4) $\mathbf{S} = (\gamma, 1, 1, 1 - \gamma, 1, 1)$, если $a \equiv 1 \pmod{2}$, $b \equiv 1 \pmod{2}$.

Найденные значения $S_6(\alpha^{\theta^f})$, $f = 0, 1, \dots, 5$ позволяют рассчитать линейную сложность любой двоичной последовательности X , построенной по (1) на основе классов шестеричных вычетов в зависимости от разложения $p = A^2 + 3B^2$, где $B \equiv 0 \pmod{3}$. Здесь ограничимся нахождением линейной сложности почти уравновешенных последовательностей при нечетном R . В связи с тем, что линейная сложность последовательности X , построенной по (1), не меняется при циклическом сдвиге индексов из множества I , достаточно рассмотреть только два варианта: $I = \{0, 1, 2\}$, $I = \{0, 1, 3\}$ (см. [8]).

Согласно (2), линейная сложность последовательности определяется числом значений l таких, что $S(\alpha^{\theta^l}) = 0$. Так как

$$S(\alpha^{\theta^l}) = \sum_{k \in I} S_d(\alpha^{\theta^{k+l}}),$$

значения многочлена последовательности определяются суммированием элементов матрицы \mathbf{S} . Воспользовавшись найденными значениями элементов матрицы \mathbf{S} , получаем следующее утверждение.

Лемма 4. Если

$$p = 4(2 + 3a)^2 + 27(1 + 2b)^2$$

и двоичная последовательность сформирована по (1) для $I = \{0, 1, 2\}$, то ее линейная сложность L задается равенствами

$$L = \begin{cases} (p-1)/2 + 1, & \text{если } a \equiv 1 \pmod{2}, \\ p, & \text{если } a \equiv 0 \pmod{2}, \end{cases}$$

а при $I = \{0, 1, 3\}$

$$L = \begin{cases} (p-1)/6 + 1, & \text{если } a \equiv 1 \pmod{2}, b \equiv 0 \pmod{2}, \\ (p-1)/3 + 1, & \text{если } a \equiv 0 \pmod{2}, b \equiv 1 \pmod{2}, \\ 5(p-1)/6 + 1, & \text{если } a \equiv 1 \pmod{2}, b \equiv 1 \pmod{2}, \\ p, & \text{если } a \equiv 0 \pmod{2}, b \equiv 0 \pmod{2}. \end{cases}$$

В частном случае, когда $b = 0$ ($B = 3$), линейная сложность последовательности Холла определена в [4]. Метод, используемый в [4], не может быть использован для $B \neq 3$.

Линейная сложность других двоичных последовательностей рассчитывается подобным же образом. Характеристический многочлен последовательности определяется, как и при $d = 4$.

4.2. Пусть $B \not\equiv 0 \pmod{3}$.

Пусть $B \equiv 1 \pmod{3}$ для нечетного R и $B \equiv 4 \pmod{3}$ для четного R , тогда $\text{ind}_\theta 2 \equiv 2 \pmod{3}$.

Если $\text{ind}_\theta 2 \equiv 5 \pmod{6}$, то, как и в разделе 3.2, получаем, что

$$L = \begin{cases} p, & \text{если } R|I| \equiv 1 \pmod{2}, \\ p-1, & \text{если } R|I| \equiv 0 \pmod{2}, \end{cases}$$

при любом числе классов степенных вычетов, отличном от шести.

Пусть $\text{ind}_\theta 2 \equiv 2 \pmod{6}$, тогда $p \equiv \pm 1 \pmod{8}$ (см. [7]), и по лемме 1

$$S_6(\alpha^{\theta^2}) = S_6^2(\alpha) \tag{9}$$

и, как и в разделе 3.1, можно считать, не нарушая общности, что $S_2(\alpha) = 1$, $S_2(\alpha^\theta) = 0$, то есть

$$S_6(\alpha) + S_6^2(\alpha) + S_6^4(\alpha) = 1. \tag{10}$$

Если R — нечетное число, то $a \equiv 1 \pmod{2}$ и по теореме 1

$$S_6(\alpha)S_6(\alpha^{\theta^2}) = bS_6(\alpha) + S_6(\alpha^\theta) + bS_6(\alpha^{\theta^2}). \tag{11}$$

Согласно (9), (11) и лемме 1, равенство $S_6(\alpha) = 1$ невозможно, то есть $S_6(\alpha) = \lambda$, где λ — корень уравнения $\lambda^3 + \lambda^2 + 1 = 0$ согласно (10). Из (11) получаем, что

$$(1) \mathbf{S} = (\lambda, \lambda^2 + 1, \lambda^2, \lambda^2 + \lambda, \lambda^2 + \lambda + 1, \lambda + 1), \text{ если } R \equiv 1 \pmod{2}, a \equiv 1 \pmod{2}, \\ b \equiv 0 \pmod{2};$$

- (2) $\mathbf{S} = (\lambda, \lambda + 1, \lambda^2, \lambda^2 + 1, \lambda^2 + \lambda + 1, \lambda^2 + \lambda)$, если $R \equiv 1 \pmod{2}$, $a \equiv 1 \pmod{2}$, $b \equiv 1 \pmod{2}$.

Если же R — четное число, то $b \equiv 0 \pmod{2}$, и по теореме 1

$$S_6(\alpha)S_6(\alpha^\theta) = a(S_6(\alpha^{\theta^2}) + S_6(\alpha^{\theta^3}) + S_6(\alpha^{\theta^4}) + S_6(\alpha^{\theta^5})). \quad (12)$$

Решая систему (12), получаем, что

- (1) $\mathbf{S} = (\lambda, 0, \lambda^2, 0, \lambda^2 + \lambda + 1, 0)$, если $R \equiv 0 \pmod{2}$, $a \equiv 0 \pmod{2}$, $b \equiv 0 \pmod{2}$;
 (2) $\mathbf{S} = (1, \beta, 1, \beta^2, 1, \beta^2 + \beta)$, если $R \equiv 0 \pmod{2}$, $a \equiv 1 \pmod{2}$, $b \equiv 0 \pmod{2}$, где β — корень уравнения $\beta^3 + \beta + 1 = 0$.

Вариант, когда $B \equiv 2 \pmod{3}$, сводится к уже рассмотренному случаю заменой θ на θ^{-1} .

Таким образом, вычисленные значения $S_6(\alpha^{\theta^f})$, $f = 0, 1, \dots, 5$, позволяют рассчитать линейную сложность любых двоичных последовательностей, сформированных по (1) на основе классов шестеричных вычетов, в зависимости от разложения $p = A^2 + 3B^2$ и при $B \not\equiv 0 \pmod{3}$.

Предложенный метод может быть использован для определения линейной сложности и для других последовательностей на основе классов степенных вычетов при известных циклотомических числах.

Список литературы

1. Лидл Р., Нидеррайтер Г., *Конечные поля*. Мир, Москва, 1988.
2. Ding C., Helleseht T., Shan W., On the linear complexity of Legendre sequences. *IEEE Trans. Inf. Theory* (1998) **44**, №3, 1275–1278.
3. Ding C., Helleseht T., Lam K. Y., Several classes of binary sequences with tree-level autocorrelation. *IEEE Trans. Inf. Theory* (1999) **45**, 2601–2606.
4. Kim J. H., Song H. Y., On the linear complexity of Hall's sextic residue sequences. *IEEE Trans. Inf. Theory* (2001) **47**, 2094–2096.
5. Hall M., *Combinatorial theory*. Blaisdell, London, 1967.
6. Whiteman A. L., The cyclotomic numbers of order twelve. *Acta Arithmetica* (1960) **6**, 53–76.
7. Ireland K., Rosen M., *A classical introduction to modern number theory*. Springer, Berlin, 1982.
8. Гантмахер В. Е., Едемский В. А., Результаты синтеза двоичных последовательностей с квазиодноуровневой автокорреляционной функцией, формируемых на основе классов вычетов по простому модулю. *Известия вузов. Радиоэлектроника* (2007) №4, 14–23.

Статья поступила 28.04.2008.