Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Криптографически слабые функции усложнения для трехчленных линейных рекуррентных последовательностей, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 1, 69–80

DOI: <https://doi.org/10.4213/mvk215>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.207.199.55

26 апреля 2023 г., 15:07:52

**Криптографически слабые функции усложнения
для трехчленных линейных рекуррентных
последовательностей**

Ф. М. Малышев

Математический институт им. В. А. Стеклова Российской академии наук, Москва

Получено 30.IV.2014

Аннотация. Рассматриваются фильтрующие генераторы псевдослучайных последовательностей с входной двоичной трехчленной линейной рекуррентной последовательностью. Указано несколько классов булевых функций усложнения, допускающих построение линейных соотношений между начальными знаками рекуррентной последовательности при наличии специальных фрагментов в выходной последовательности. Допустимость использования таких функций в фильтрующих генераторах требует дополнительных обоснований.

Ключевые слова: рекуррентная последовательность, фильтрующий генератор, псевдослучайная последовательность

Cryptographically weak filter function for trinomial linear recurrent sequences

F. M. Malyshev

Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow

Abstract. We consider filter generators of pseudorandom sequences with binary input linear recurrent sequence having trinomial connection polynomial. Several classes of Boolean filter functions are described allowing to construct linear relations between the elements of input recurrent sequence by special subsets of output sequence. The admissibility of using such functions in the filter generators requires special justification.

Key words: recurrent sequence, filter generator, pseudo-random sequence

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 69–80 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

1. Введение

В работе рассматриваются генераторы псевдослучайных последовательностей $\{y_i \in GF(2), i \in \mathbb{Z}\}$, относящиеся к фильтрующим генераторам [1]. Очередной знак y_i вычисляется по формуле

$$y_i = F(x_{i+l_1}, \dots, x_{i+l_r}), \quad (1)$$

где $\{x_i \in GF(2), i \in \mathbb{Z}\}$ — рекуррентная последовательность порядка m , удовлетворяющая рекуррентному соотношению

$$x_{i+m} = x_i + x_{i+k}, \quad i \in \mathbb{Z}, \quad (2)$$

а $F : GF(2)^r \rightarrow GF(2)$ — булева функция, называемая функцией усложнения в фильтрующем генераторе. Предполагается, что

$$0 \leq l_1 < l_2 < \dots < l_r \leq m, \quad 0 < k < m, \quad \text{НОД}(k, m) = 1.$$

Общий неизбежный недостаток рассматриваемых (как и многих других) генераторов псевдослучайных последовательностей состоит в том, что все знаки последовательности $\{y_i, i \in \mathbb{Z}\}$ выражаются через конечное число знаков $x_0, x_1, \dots, x_{m-1}$. Как правило, значение m существенно меньше числа реально используемых знаков $\{y_i, i \in I \subset \mathbb{Z}\} : m \ll |I|$. Поэтому знаки $y_i, i \in I$, зависимы.

При конструировании конкретных генераторов (в том числе при выборе функций усложнения F) одна из задач состоит в том, чтобы сделать эту зависимость по возможности менее явной, в частности затруднить ее использование для определения начальных знаков $x_0, x_1, \dots, x_{m-1}$. Необходимость тщательного выбора параметров рассматриваемых генераторов подтверждается также доказанными в [2] теоремами о том, что асимптотически при $m \rightarrow \infty$ и ограниченном r для фильтрующих генераторов общего вида можно восстанавливать знаки $x_0, x_1, \dots, x_{m-1}$ с трудоемкостью порядка $O(m)$ по $O(m)$ известным знакам $y_i, i \in I$, где константы в $O(m)$ растут по r быстрее, чем экспоненциально.

Наряду с последовательностью $\{y_i, i \in \mathbb{Z}\}$ будем рассматривать последовательность $\{\delta_i, i \in \mathbb{Z}\}$, $\delta_i = y_i + y_{i+k} + y_{i+m}$, знаки которой предполагаются известными.

В качестве усложняющих далее будут рассматриваться функции следующего вида:

$$F(z_1, \dots, z_r) = \varphi(L(z_1, \dots, z_r)) + L_0(z_1, \dots, z_r), \quad (3)$$

где $L : V_r \rightarrow V_n$ — линейный эпиморфизм, $V_n = GF(2)^n$, $L_0 : V_r \rightarrow GF(2)$ — аффинная функция, $\varphi : V_n \rightarrow GF(2)$ — некоторая булева функция.

Определение 1. Функцию $\varphi : V_n \rightarrow GF(2)$ будем называть *3-линейно сводимой*, если генератор псевдослучайных последовательностей (1), (2) с функцией усложнения (3) при всех значениях параметров $m, k, r, l_1, l_2, \dots, l_r, L, L_0$ обладает следующим дефектом: при некоторой зависящей только от φ константе $c = c(\varphi)$ существуют такие подмножество

$$J \subset \mathbb{Z}, \quad \max J - \min J \leq cm,$$

и вектор

$$\varpi \in GF(2)^{[J]},$$

что из равенства $(\delta_j, j \in J) = \varpi$ следует заранее известное ненулевое линейное соотношение между переменными $x_0, x_1, \dots, x_{m-1}$, коэффициенты которого однозначно задаются указанными параметрами.

В условиях определения 1 функцию усложнения (3) называем *криптографически слабой*. Для приведенных далее классов криптографически слабых функций F значения констант c не превосходят 6, а подмножество J (выбираемое с точностью до сдвига), вектор ϖ и линейное соотношение из определения 1 будут указаны явным образом. Они могут использоваться, в частности, в алгоритмах определения $x_0, x_1, \dots, x_{m-1}$.

Справедливы следующие четыре теоремы.

Теорема 1. При любом $n \leq 1$ булева функция

$$\varphi(v_1, \dots, v_n) = v_1 \cdots v_n$$

является 3-линейно сводимой.

Случай $n = 2$ в теореме 1 подробно исследовался в [4] в связи с алгоритмами восстановления $x_0, x_1, \dots, x_{m-1}$. В частности, в [4] обнаружена 3-линейная сводимость функции $\varphi(v_1, v_2) = v_1 v_2$.

Теорема 2. При любом $n \leq 2$ любая булева функция $\varphi : V_n \rightarrow GF(2)$, для которой $\varphi(0) = 0$, а множество $\{v \in V_n \mid \varphi(v) = 1\} \cup \{0\}$ является собственным линейным подпространством в V_n , является 3-линейно сводимой.

Теорема 3. Все булевы функции φ от 2 и 3 переменных, отличные от константы, являются 3-линейно сводимыми.

Теорема 4. Булева функция

$$\varphi(v_1, v_2, v_3, v_4) = v_1 v_2 + v_3 v_4$$

является 3-линейно сводимой.

Следующее несложное утверждение показывает, что каждая из приведенных в этих теоремах 3-линейно сводимая функция определяет целую серию 3-линейно сводимых функций.

Утверждение 1. Пусть $\varphi : V_n \rightarrow GF(2)$ — 3-линейно сводимая функция, $\Lambda : V_{n'} \rightarrow V_n$ — произвольный линейный эпиморфизм, $G : V_{n'} \rightarrow GF(2)$ — произвольная аффинная функция. Тогда функция $\varphi' : V_{n'} \rightarrow GF(2)$, определяемая соотношением

$$\varphi'(v') = \varphi(\Lambda(v')) + G(v'), \quad v' \in V_{n'},$$

тоже является 3-линейно сводимой.

В случае $n' = n$ в этом утверждении имеем дело с орбитой функции φ под действием полупрямого произведения группы $GL(n, 2)$, действующей на аргументах, и аддитивной группы аффинных функций от n переменных, действующей сдвигами на множестве всех булевых функций от n переменных. Теоремы 1–4 будем доказывать в предположении линейности функции L_0 , чего можно добиваться (при необходимости) инвертированием знаков δ_j , $j \in J$.

Доказательство утверждения 1. Пусть $m, k, r, l_1, l_2, \dots, l_r$ — произвольные числа, удовлетворяющие условиям из введения, $L' : V_r \rightarrow V_{n'}$ — произвольный линейный эпиморфизм, а $L'_0 : V_r \rightarrow GF(2)$ — произвольная аффинная булева функция. Тогда функция усложнения

$$\begin{aligned} F'(z_1, \dots, z_r) &= \varphi'(L'(z_1, \dots, z_r)) + L'_0(z_1, \dots, z_r) = \\ &= \varphi(\Lambda(L'(z_1, \dots, z_r))) + G(L'(z_1, \dots, z_r)) + L'_0(z_1, \dots, z_r) = \\ &= \varphi(L(z_1, \dots, z_r)) + L_0(z_1, \dots, z_r) \end{aligned}$$

будет обладать указанным в определении 1 дефектом, так как φ — 3-линейно сводимая функция,

$$L(z_1, \dots, z_r) = \Lambda(L'(z_1, \dots, z_r))$$

— линейный эпиморфизм, $L : V_r \rightarrow V_n$, а

$$L_0(z_1, \dots, z_r) = G(L'(z_1, \dots, z_r)) + L'_0(z_1, \dots, z_r)$$

— аффинная функция, $L_0 : V_r \rightarrow GF(2)$.

Утверждение 1 доказано. □

Замечание 1. При доказательстве теорем 1–4 в следующих параграфах будем пользоваться конструкцией из [3], предполагающей расположение номеров $i \in \mathbb{Z}$ на плоскости в узлах решетки $\Gamma = \langle e_1, e_2 \rangle_{\mathbb{Z}}$. Векторы e_1, e_2 удобно брать одинаковой длины с углом 60° между ними. Вектор e_1 считаем горизонтальным, направленным вправо, а вектор e_2 — направленным вверх направо. Номер $i = i_1k + i_2m$ приписывается к узлу $i_1e_1 + i_2e_2$. Знаки y_i, x_i , как и различные векторы, связанные с рекуррентной последовательностью (2) и относящиеся к номеру $i \in \mathbb{Z}$, тоже будем приписывать к узлу решетки Γ с номером i . Исключение составляют знаки $\delta_i = y_i + y_{i+k} + y_{i+m}$: знак δ_i будем помещать в центр треугольника с вершинами $i, i+k, i+m$ (см., например, рис. 1 в разделе 2). Вообще говоря, один и тот же номер i приписывается к разным узлам решетки. Это обстоятельство не будет приводить к недоразумениям.

2. Доказательство теоремы 1

Пусть

$$L(z_1, \dots, z_r) = (L_1(z_1, \dots, z_r), \dots, L_n(z_1, \dots, z_r)),$$

где $L_i: V_r \rightarrow GF(2)$, $i = 1, \dots, n$, — ненулевые линейные функции. У нас $\varphi(v_1, \dots, v_n) = v_1 \cdots v_n$, поэтому

$$\begin{aligned} y_i &= F(x_{i+l_1}, \dots, x_{i+l_r}) = \\ &= \varphi(L(x_{i+l_1}, \dots, x_{i+l_r})) + L_0(x_{i+l_1}, \dots, x_{i+l_r}) = \\ &= L_1(x_{i+l_1}, \dots, x_{i+l_r}) \cdots L_n(x_{i+l_1}, \dots, x_{i+l_r}) + L_0(x_{i+l_1}, \dots, x_{i+l_r}), \end{aligned}$$

а

$$\delta_i = y_i + y_{i+k} + y_{i+m} = \varphi(w_i) + \varphi(w_{i+k}) + \varphi(w_{i+m}),$$

где $w_j = (w_{j1}, \dots, w_{jn}) = L(x_{j+l_1}, \dots, x_{j+l_r})$, и

$$\varphi(w_j) = w_{j1} \cdots w_{jn}, \quad j \in \mathbb{Z}.$$

Пользуясь конструкцией, описанной в замечании 1, покажем, что множество $J = \{i, i+k, i+m\}$ и вектор $\varpi = (1, 1, 1)$ удовлетворяют требованиям определения 1 с параметром $c = 1$. Пусть далее $\delta_i = \delta_{i+k} = \delta_{i+m} = 1$.

Обозначим через $\mathbf{m} \in V_n$ вектор, у которого все координаты равны 1. Для остальных ненулевых векторов V_n используем обозначение w . Ясно, что $\varphi(w) = 0$, $\varphi(\mathbf{m}) = 1$.

Коль скоро

$$\delta_i = 1 = \varphi(w_i) + \varphi(w_{i+k}) + \varphi(w_{i+m}),$$

среди трех векторов w_i, w_{i+k}, w_{i+m} есть $\mathfrak{m}$, причем в единственном числе, так как $w_i + w_{i+k} + w_{i+m} = 0$. По этой же причине $\{w_i, w_{i+k}, w_{i+m}\} = \{\mathfrak{m}, w, \bar{w}\}$, где $\bar{w} = w + \mathfrak{m}$, $w \in V_n \setminus \{0, \mathfrak{m}\}$.

Предыдущие рассуждения (возможно, при других $w \in V_n \setminus \{0, \mathfrak{m}\}$) остаются в силе после замены i и на $i+k$, и на $i+m$. Поскольку тройки $\{i, i+k, i+m\}$, $\{i+k, i+2k, i+k+m\}$, $\{i+m, i+m+k, i+2m\}$ попарно пересекаются (см. рис. 1), то существует такой вектор $w \in V_n \setminus \{0, \mathfrak{m}\}$, что

$$\begin{aligned} \{w_i, w_{i+k}, w_{i+m}\} &= \{w_{i+k}, w_{i+2k}, w_{i+k+m}\} = \{w_{i+m}, w_{i+m+k}, w_{i+2m}\} = \\ &= \{\mathfrak{m}, w, \bar{w}\}, \end{aligned}$$

при этом и $\{w_{i+k}, w_{i+m}, w_{i+k+m}\} = \{\mathfrak{m}, w, \bar{w}\}$.

Рис. 1

Рис. 2

На рис. 2 представлена одна из трех возможностей для реализации рис. 1. Две другие возможности получаются из указанной поворотами на 120° по часовой стрелке или против часовой стрелки. Непосредственно по рис. 2 находим искомые линейные соотношения: $w_i = w_{i+k+m}$, $w_{i+m} = w_{i+2k}$, $w_{i+2m} = w_{i+k}$. Они выполняются и для двух других не представленных на рис. 2 реализаций. Теорема 1 доказана. $\square$

3. Доказательство теоремы 2

Для удобства элемент $w \in V_n$ будем обозначать как Б (буква), если $\varphi(w) = 1$, и как Ц (цифра) в противном случае. По условию теоремы 2 совокупность элементов, обозначаемых буквами, образует вместе с нулем собственное линейное подпространство в V_n . Как и в предыдущем доказательстве, полагаем $w_j = L(x_{j+l_1}, \dots, x_{j+l_r})$, $j \in \mathbb{Z}$.

Далее снова пользуемся конструкцией из замечания 1. Покажем, что представленные на рис. 3 множество

$$J = \{i - k, i, i + k, i + 2k, i + 3k - m, i + m, i + m + k\}, \quad |J| = 7,$$

и отвечающий ему вектор $\varpi = (1, 0, 1, 0, 1, 1, 1) \in GF(2)^7$ удовлетворяют требованиям определения 1 с параметром $c = 3$, поскольку $J \subset [i - m, i + 2m]$.

Рис. 3

Пусть далее $(\delta_{i-k}, \delta_i, \delta_{i+k}, \delta_{i+2k}, \delta_{i+3k-m}, \delta_{i+m}, \delta_{i+m+k}) = (1, 0, 1, 0, 1, 1, 1) = \varpi$. Покажем, что представленные на рис. 3 семь векторов $w_j \in V_n$, отличных от шести векторов, помеченных буквой X, имеют указанные там обозначения Б и Ц соответственно. Буква X здесь используется в качестве признака неопределенности.

Каждый узел s на рис. 3 является вершиной треугольника с единицей внутри, поэтому $w_s \neq 0$ для всех 13 узлов s , представленных на этом рисунке. Действительно, если при $\delta_j = 1$ среди w_j, w_{j+k}, w_{j+m} имеется нулевой вектор, то (поскольку $w_j + w_{j+k} + w_{j+m} = 0$) два других вектора должны быть одинаковыми, что приводит к противоречию:

$$\delta_j = \varphi(w_j) + \varphi(w_{j+k}) + \varphi(w_{j+m}) = 0.$$

Если $\delta_j = 0$, то все три вектора w_j, w_{j+k}, w_{j+m} являются цифрами. Логически возможная ситуация с одной цифрой и двумя буквами среди w_j, w_{j+k}, w_{j+m} не может реализоваться, так как $w_j + w_{j+k} + w_{j+m} = 0$, а сумма двух различных букв обязательно, по условию теоремы, является буквой, а не цифрой. У треугольника с единицей внутри хотя бы одна вершина должна быть буквой, поэтому таковой является w_{j+k+m} . Поэтому w_{j+k+m} удовлетворяет линейным соотношениям, которым удовлетворяют векторы собственного линейного подпространства $\{v \in V_n \mid \varphi(v) = 1\} \cup \{0\}$ в V_n . Теорема 2 доказана. $\square$

4. Доказательство теоремы 3

При $n = 2$ теорема 3 следует из теоремы 1 и утверждения 1, приведенного в конце введения. При $n = 3$ и $\deg \varphi = 2$ теорема 3 также следует из теоремы 1 и того же утверждения, поскольку

$$x_1x_2 + x_2x_3 + x_1x_3 = (x_1 + x_2)(x_2 + x_3) + x_2.$$

Далее считаем $n = 3$ и $\deg \varphi = 3$. В соответствии с утверждением 1 можно также считать, что $\varphi(0) = 0$.

Поскольку $\deg \varphi = 3$, вес

$$\|\varphi\| = |\{v \in V_3 \mid \varphi(v) = 1\}|$$

нечетен, а именно $\|\varphi\| \in \{1, 3, 5, 7\}$.

В случае $\|\varphi\| = 1$ утверждение теоремы 3 следует из утверждения теоремы 1. Случай $\|\varphi\| = 5$ по утверждению 1 сводится к случаю $\|\varphi\| = 1$. Действительно, если

$$\{v \in V_3 \mid \varphi(v) = 0\} = \{0, v_1, v_2\},$$

а l — линейная функция, равная нулю на v_1 и v_2 , то для функции $\varphi' = \varphi + l$ имеем $\|\varphi'\| = 1$. Аналогичным образом случай с $\|\varphi\| = 7$ сводится к случаю $\|\varphi\| = 3$, к которому можно применять теорему 2.

Для доказательства теоремы 3 осталось рассмотреть случай, когда множество

$$\{v \in V_3 \mid \varphi(v) = 1\} = \{a, b, c\}$$

является линейно независимой системой векторов — базисом. Обозначим $a + b$ через 6, $a + c$ через 5, $b + c$ через 3 и $a + b + c$ через 7. Далее в доказательстве векторы пространства V_3 из базиса называем буквами, а остальные векторы V_3 называем цифрами. Как и при доказательстве теоремы 2, на буквах функция φ равна единице, а на цифрах 0, 6, 5, 3, 7 функция φ обращается в нуль.

Выделим тройки различных векторов v_1, v_2, v_3 в V_n , для которых

$$v_1 + v_2 + v_3 = 0 \quad \text{и} \quad \delta = \varphi(v_1) + \varphi(v_2) + \varphi(v_3) = 1.$$

Трех букв в тройке не может быть, так как $a + b + c = 7$. Значит, в требуемой тройке одна буква и две цифры. Но $3 + 5 + 6 = 0$, поэтому в выделяемой тройке присутствует вектор 7 в паре с одной из оставшихся трех цифр. В результате остаются следующие варианты:

$$7, 3, a; \quad 7, 5, b; \quad 7, 6, c. \quad (4)$$

Снова воспользовавшись конструкцией из замечания 1, покажем, как и при доказательстве теоремы 1, что множество $J = \{i, j+k, i+m\}$ и вектор $\varpi = (1, 1, 1)$ удовлетворяют требованиям определения 1 с параметром $c = 1$.

Пусть далее $\delta_i = \delta_{i+k} = \delta_{i+m} = 1$. Если, как и в предыдущих доказательствах, $w_j = L(x_{j+l_1}, \dots, x_{j+l_r})$, $j \in \mathbb{Z}$, то для треугольника на рис. 1, согласно (4), имеем только 18 возможностей, а с учетом симметрии — только 3 следующие возможности:

Во всех случаях имеют место линейные соотношения

$$w_i = w_{i+k+m}, \quad w_{i+m} = w_{i+2k}, \quad w_{i+k} = w_{i+2m}.$$

Теорема 3 доказана. □

5. Доказательство теоремы 4

Рассмотрим множество Ω мощности 16, элементами которого являются вершины и ребра графа $K_{3,3}$, а также символ 0. Принятая на рис. 4 нумерация ненулевых элементов множества Ω ненулевыми 16-ричными цифрами (нумерующими также ненулевые векторы V_4 стандартным образом) устанавливает биекцию между V_4 и Ω . В соответствии с этой биекцией векторы из $V_4 \setminus \{0\}$ будем называть соответственно вершинами и ребрами.

Рис. 4

Функция $\varphi: V_4 \rightarrow GF(2)$ из формулировки теоремы 4 принимает значение 0 на ребрах и на нулевом векторе, на всех шести вершинах значение φ равно 1. Сформулируем также на этом языке два правила сложения векторов, в справедливости которых можно убедиться непосредственной проверкой.

Каждое ребро является суммой его концевых вершин. Сумма трех вершин одного уровня (на рис. 4) равна 0. В качестве следствий данных двух базовых правил формулируются (на языке вершин и ребер) правила сложения любой пары ненулевых векторов из V_4 .

Сумма вершин одного уровня равна третьей вершине на том же уровне. Сумма вершин разных уровней равна ребру, их соединяющему. Сумма ребра с одной из его концевых вершин равна другой его концевой вершине. Сумма ребра с не инцидентной ему вершиной верхнего (для определенности) уровня будет ребром, соединяющим нижнюю концевую вершину исходного ребра с не инцидентной ему вершиной верхнего уровня, отличной от второго слагаемого. Сумма двух ребер, не имеющих общих вершин, равна ребру, не имеющему общих вершин с каждым слагаемым. Сумма ребер с общей нижней (для определенности) вершиной равна вершине верхнего уровня, отличной от концевых вершин слагаемых.

Группа G автоморфизмов графа $K_{3,3}$ имеет порядок $72 = 3!^2 \cdot 2$. Она транзитивна на множестве вершин и на множестве ребер. Можно считать, что $G \subset S_\Omega$. Элементы группы G сохраняют сложение (принадлежат $GL(V_4)$) и сохраняют значения функции φ (принадлежат группе инерции функции φ). Данные свойства элементов группы G вместе с ее транзитивностью на вершинах и ребрах далее в доказательстве используются для сокращения числа перебираемых вариантов.

Обратимся снова к конструкции замечания 1 введения. Покажем тогда, что множество

$$J = \{(i, i+k, \dots, i+4m+k, i+5m)\} \cup \{i+6m\} = \\ = \{i+j_0k+j_1m \mid j_0 \geq 0, j_1 \geq 0, j_0+j_1 \leq 5\} \cup \{i+6m\},$$

$|J| = 22$, и вектор $\varpi \in GF(2)^{22}$, представленные в треугольнике на рис. 5, удовлетворяют требованиям определения 1 с параметром $c = 6$.

$$\begin{array}{ccccccc} & & & & & & 1 \\ & & & & & & 0 \\ & & & & & 1 & 1 \\ & & & 0 & 1 & 0 \\ & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

Рис. 5

В этом треугольнике нижняя левая единица, равная δ_i , находится внутри треугольника с вершинами $i, i+k, i+m$ (см. рис. 1). В центрах аналогичных треугольников содержатся остальные элементы треугольника на рис. 5. Там, в частности, нижняя правая единица — это δ_{i+5k} , а самая верхняя единица — δ_{i+6m} .

Обозначим

$$J_0 = \{i+m, i+m+2k, i+m+4k, i+3m, i+3m+2k, i+5m\},$$

$J_1 = J \setminus J_0$. Полагая далее $(\delta_j, j \in J) = \varpi$, имеем: $\delta_j = 0$ для $j \in J_0$ и $\delta_j = 1$ для $j \in J_1$. Проверим, что тогда

$$w_i = w_{i+6k}. \quad (5)$$

Это и будет доказательством теоремы 4.

Для доказательства равенства (5) необходимо проанализировать все треугольники

$$(w_j, j \in \bar{J}), \quad \bar{J} = \{i + j_0 k + j_1 m \mid j_0 \geq 0, j_1 \geq 0, j_0 + j_1 \leq 6\},$$

элементы которых удовлетворяют рекуррентному соотношению $w_j + w_{j+k} + w_{j+m} = 0$ и равенству $\varphi(w_j) + \varphi(w_{j+k}) + \varphi(w_{j+m}) = \delta_j, j \in J \setminus \{i+6m\}$. Напомним, что на ребрах значение φ нулевое, а на вершинах оно равно 1.

Элементы треугольника $(w_j, j \in \bar{J})$ ненулевые. Это было замечено еще при доказательстве теоремы 2. (В треугольнике на рис. 5 дополнительно потребовалась самая верхняя единица, отвечающая δ_{i+6m} , как раз для гарантирования неравенства $w_{i+6m} \neq 0$.)

Ввиду транзитивности группы $\text{Aut}(K_{3,3}) = G \subset S_\Omega$ как на вершинах, так и на ребрах графа $K_{3,3}$ для w_{i+6m} в треугольнике $(w_j, j \in \bar{J})$ достаточно рассмотреть две возможности: $w_{i+6m} = 7$ и $w_{i+6m} = 1$. Далее элементы треугольника $(w_j, j \in \bar{J})$ будем определять (в нескольких, вообще говоря, вариантах) строчка за строчкой, идя сверху вниз, начиная с его вершины, а именно с вектора w_{j+6m} .

Пусть $w_{i+6m} = 7$. Тогда для следующей строчки треугольника $(w_j, j \in \bar{J})$ будем иметь шесть возможностей: $da, ad, e9, 9e, 34, 43$. С учетом действия группы G и зеркальной симметрии можно ограничиться строкой da . Для следующей строки из четырех возможностей по аналогичным соображениям оставляем только две: $e39$ и 493 . Эти два случая рассмотрим отдельно.

В случае $e39$ для четвертой строки из двух возможностей также можно ограничиться одной: $b56f$. После этого пятая, шестая и седьмая строки определяются однозначно: $9271e, 6fdab5, 71e3927$. Как видим, $w_i = w_{i+6k} = 7$.

Продолжение строки 493 осуществляется совершенно аналогично. Из двух симметричных (относительно G) возможностей для четвертой строки берем 62b8. Следующие строки определяются однозначно: 357c4, b8da62, 7c49357. В седьмой строке снова $w_i = w_{i+6k} = 7$.

Все возможности для случая $w_{i+6m} = 1$ представлены на рис. 6, где часть первых вариантов тоже не рассматривается с учетом действия группы G .

Рис. 6

Как видно из этого рисунка, во всех нижних строках крайние элементы одинаковы, что и указывает на требуемое равенство (5).

Теорема 4 доказана. $\square$

В заключение автор выражает благодарность А. М. Зубкову за полезные критические замечания.

Список литературы

- [1] Шнайер Б., *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*, М.: ТРИУМФ, 2003, 816 с.
- [2] Малышев Ф. М., “Сложность восстановления начальных знаков фильтрующих генераторов одного класса”, *Математические вопросы криптографии*, **6:1** (2015), 109–116.
- [3] Малышев Ф. М., “Порождающие наборы элементов рекуррентных последовательностей”, *Труды по дискретной математике*, **11:2** (2008), 86–111.
- [4] Балакин Г. В., “О возможности частичного восстановления некоторых последовательностей по наблюдениям”, *Математические вопросы криптографии*, **4:4** (2013), 7–25.