УДК 621.391

СТРУКТУРНЫЕ И КОРРЕЛЯЦИОННЫЕ СВОЙСТВА ПОСЛЕДОВАТЕЛЬНОСТЕЙ КОДА ГОППА

С.Б. САЛОМАТИН, В.В. ПАНЬКОВА

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 8 ноября 2021

Аннотация. Рассматриваются свойства апериодической функции автокорреляции и профиля линейной сложности последовательностей, сформированных на основе бинарных кодов Гоппа. Для решения данной задачи разработаны алгоритмы формирования последовательностей кодов Гоппа, вычисления апериодической корреляционной функции, построения профиля линейной сложности на основе процедуры Берлекэмпа-Мэсси. Показано, что апериодическая корреляционная функция последовательностей кодов Гоппа имеет малый уровень максимального бокового лепестка. Графики линейной сложности последовательностей кода Гоппа имеют профиль близкий к профилю линейной сложности эталонного криптографического генератора BBS. Данные свойства позволяют рекомендовать последовательности кода Гоппа для синхронизации блочных помехоустойчивых кодов в системах связи и зондирующих сигналов в системах радиолокации.

Ключевые слова: помехоустойчивый код Гоппа, автокорреляционная функция, линейная сложность булевых функций, алгоритм Берлекэмпа-Мэсси.

Введение

Код Гоппа относится к классу альтернантных кодов [1, 2]. Широко известно применение кодов Гоппа в качестве ядра криптосистемы Мак-Элис [3, 5]. В системах кодирования и защиты данных блочными кодами важными являются задачи поиска последовательностей с «хорошими» корреляционными свойствами и линейной сложностью булевой структуры. Один из путей задач такого рода состоит в исследовании свойств блочных помехоустойчивых кодов.

В настоящей работе рассматриваются свойства бинарных последовательностей кода Гоппа с точки зрения оценки автокорреляционной функции и линейной сложности.

Коды Гоппа

Определим полином Гоппа [1, 2] $g(x)=g_0+g_1x+..,+g_tx^t=\sum_{i=0}^{t}g_ix^i,\ g_i\in GF\left(p^m\right)$. Пусть L образует конечное подмножество расширенного поля $GF\left(p^m\right)$, p – простое число $L=\{\alpha_1,...,\alpha_n\}\subseteq GF\left(p^m\right)$, такое, что $g(\alpha_i)\neq 0$ для всех $\alpha_i\in L$.

Задавая кодовый вектор $\mathbf{c}=(c_1,...,c_n)$ над $GF(q)$ мы получаем функцию

$$R_c(z)=\sum_{i=1}^{n}\frac{c_i}{x-\alpha_i}, \qquad (1)$$

где $(1/(x-\alpha_i))$ единственный полином, степень которого меньше или равна $(t-1)$ и удовлетворяет условию $(x-\alpha_i)/(x-\alpha_i)\equiv 1 \bmod g(x)$.

Код Гоппа $\Gamma(L,g(x))$ содержит все кодовые векторы с такие, что $R_c(z)\equiv 0 \bmod g(x)$.

Параметры кода. Код Гоппа –линейный код, имеющий параметры $(n, k, d_{\min})$. Длина n зависит от подмножества L. Размерность k кода Гоппа $\Gamma(L, g(x))$ над полем $GF(p^m)$, длины n, больше или равна величине $n - mt$ или $k \geq n - mt$. Минимальное кодовое расстояние $d_{\min}$ кода Гоппа $\Gamma(L, g(x))$длины n, больше или равно $(t+1)$ или $d_{\min} \geq t+1$.

Бинарные коды Гоппа. Проверочная матрица кода определяется как матрица $\mathbf{H}$, для которой справедливо соотношение $\mathbf{H}\mathbf{c}^T = 0$, для всех векторов кодовых слов $\mathbf{c}$ в $GF(2^m)$, удовлетворяющих требованиям кода Гоппа.

Предложение. Пусть $g(x)$ – неприводимый полином над полем $GF(2^m)$ и пусть

$$\mathbf{H} = \mathbf{XYZ}, \tag{2}$$

где

$$\mathbf{Y} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_{\mathbf{n}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{\mathbf{t-1}} & \alpha_2^{\mathbf{t-1}} & \dots & \alpha_{\mathbf{n}}^{\mathbf{t-1}} \end{bmatrix}, \quad \mathbf{X} = \begin{bmatrix} g_t & 0 & 0 & \dots & 0 \\ g_{t-1} & g_t & 0 & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ g_1 & g_2 & g_3 & \dots & g_n \end{bmatrix}, \tag{3}$$

$$\mathbf{Z} = \begin{bmatrix} 1/g(\alpha_1) & 0 & \dots & 0 \\ 0 & 1/g(\alpha_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1/g(\alpha_n) \end{bmatrix},$$

тогда матрица $\mathbf{H}$ является проверочной матрицей кода Гоппа $\Gamma(L, g(x))$.

Пример 1. Пусть задано поле $GF(2^m)$, $m = 4$, $f(x) = x^4 + x + 1 = (19)_{dec}$. Построим код Гоппа с параметрами $(n, k) = (16, 4)$, исправляющий $t = 3$ три ошибки. Используя алгоритм Рабина [5], найдем неприводимый полином Гоппа $g(x) = \alpha + \alpha^{14}x + \alpha^{13}x^2 + \alpha^{11}x^3$.

Конечное подмножество расширенного поля $L = \{\alpha_1, \dots, \alpha_n\}$ определим как $L = (\alpha^{14}, \alpha^6, \alpha^{10}, \alpha^{15}, \alpha^2, \alpha^7, \alpha^9, \alpha^3, \alpha^{12}, \alpha^5, \alpha^{11}, \alpha, \alpha^4, \alpha^8, \alpha^0) = (14,6,10,15,2,7,9,3,12,5,11,1,4,8,0)_{\deg}$.

Проверочная матрица кода Гоппа будет иметь вид

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Используя соотношения (2) и (3), генераторная матрица $\mathbf{G}$ может быть построена с использованием проектирования в нулевое подпространство $\mathbf{G} = Nullspace(\mathbf{H}) \bmod p$.

Автокорреляционные свойства последовательностей кода Гоппа

В системах синхронизации блочных кодов используются последовательности с малыми боковыми лепестками апериодических автокорреляционных функций. Покажем, последовательности кода Гоппа имеют низкий уровень боковых лепестков апериодической автокорреляционной функции.

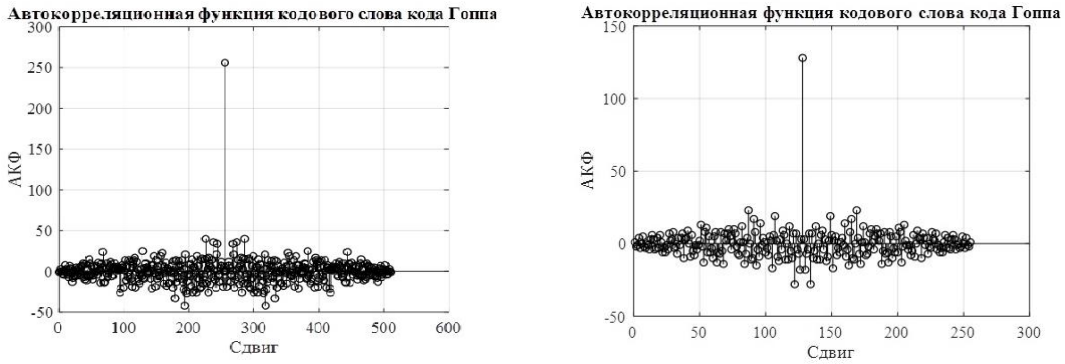
Кодовое слово $\mathbf{c} = (c_0, c_1, ..., c_{n-1}), c_i \in \{0,1\}$ определится как произведение случайного вектора данных $\mathbf{a} = (a_0, a_1, ..., a_{k-1}), a_i \in \{0,1\}$ на генераторную матрицу $\mathbf{G}$: $\mathbf{c} = \mathbf{aG} \bmod p$.

Последовательности $\mathbf{s} = (s_0, s_1, ..., s_{n-1}), s_i \in \{\pm 1\}$ кода Гоппа определим через отображение $s_i = (-1)^{c_i}$. Тогда для последовательности **s** длиной N апериодическая автокорреляционная функция (АКФ) может быть записана следующим образом:

$$r_{xx}(m) = \frac{1}{N} \sum_{i=0}^{N-m-1} s_{i+m} s_i^*.$$

Пример 2. Пусть $n = 256$, $k = 224$, $t = 4$, поле $GF(2^8)$ построено с помощью полинома $f(x) = (285)_{dec}$, полином Гоппа имеет вид $g(x) = \alpha + \alpha^{39}x + \alpha^{132}x^2 + \alpha^{121}x^3 + \alpha^{145}x^4$. Апериодическая АКФ приведена на рис. 1, *а*.

Пусть $n = 128$, $k = 100$, $t = 4$, поле $GF(2^7)$, $f(x) = (137)_{dec}$ полином Гоппа имеет вид $g(x) = \alpha + \alpha^{32}x + \alpha^{88}x^2 + \alpha^{120}x^3 + \alpha^{20}x^4$. Апериодическая АКФ приведена на рис. 1, *б*.



а *б*

Рис. 1. Апериодические АКФ последовательностей кода Гоппа: *а* – код Гоппа длиной $n = 256$; *б* – код Гоппа длиной $n = 128$.

Анализ максимального уровня боковых лепестков апериодической АКФ $\rho_{\max}$ показывает, что для последовательностей кода Гоппа он не превышает величину $\rho_{\max} \le 2{,}6\sqrt{n}$, где n – длина кодовой последовательности.

Оценка линейной сложности кода Гоппа на основе алгоритма Берлекэмпа-Мэсси

Линейной сложностью $LS(c)$ последовательности $\mathbf{c}_i(l) = (c_{0,i}, c_{1,i}, ..., c_{l-1,i})$ называется длина L самого короткого РСЛОС, который может сгенерировать вектор **c**, когда первые L цифр последовательности **c** являются начальным заполнением регистра. Эквивалентное определение: линейная сложность $LS(c)$ определяется как наименьшее неотрицательное целое L, такое, что существует линейная рекуррента с фиксированными константами $(c_0, c_1, ..., c_l)$, удовлетворяющая равенству $c_j + \beta_1 c_{j-1} + ... + \beta_L c_{j-L} = 0, \quad L \le j \le 1$. Коэффициенты $\{\beta_i\}$ определяют полином обратной связи РСЛОС $C(D) = 1 + \beta_1 D + \beta_2 D^2 + ... + \beta_L D^L$ [2].

Алгоритм БМ

Вход: Бинарная последовательность $\mathbf{c}(m) = (c_0, c_1, ..., c_{n-1})$ длиной n.

Выход: Линейная сложность $LS\left(\mathbf{c}(n)\right)$.

1. Инициализация исходных данных $C(D)\leftarrow 1,\ L\leftarrow 0,\ m\leftarrow(-1),\ B(D)\leftarrow 1,\ N\leftarrow 0$.

2. До тех пор пока $N<n$, выполнять следующие операции:

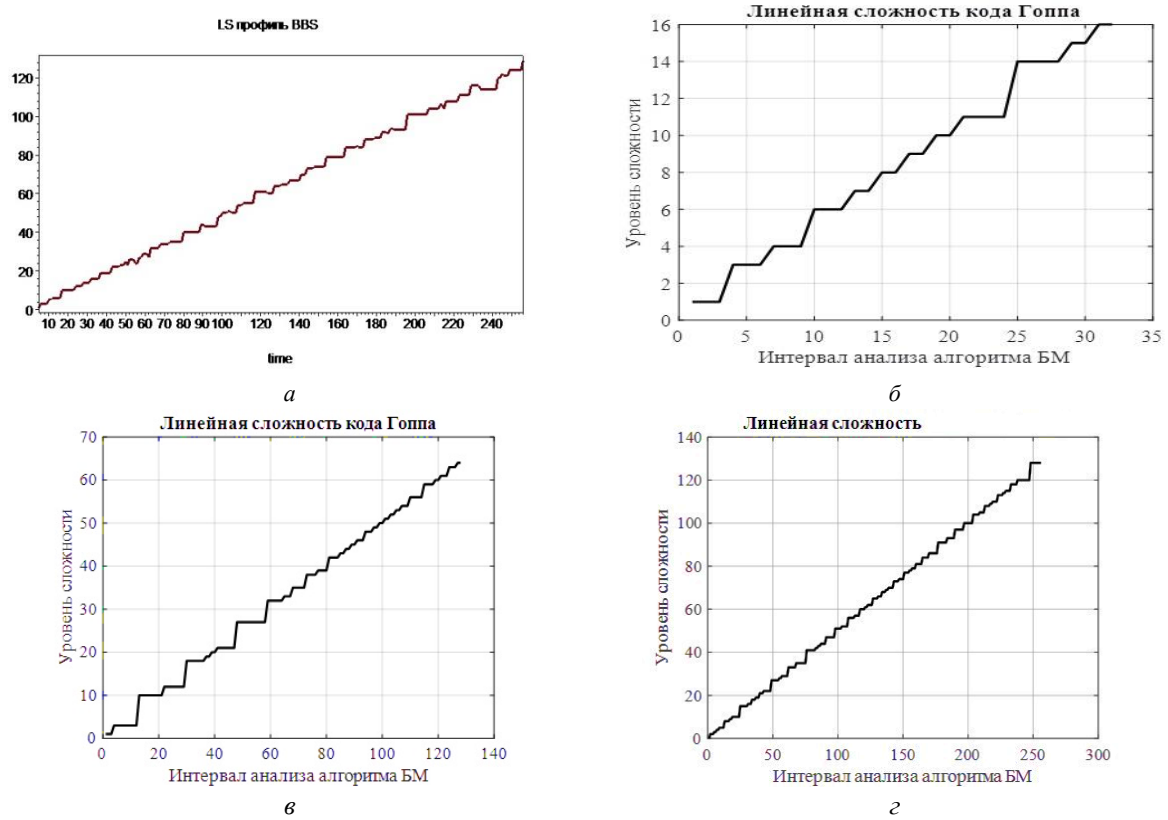
2.1. Вычислять невязку $d\leftarrow c_N+\sum_{i=1}^{L}\beta_i c_{N-i} \bmod 2$.

2.2. Если $d=1$, то выполнять следующие действия: $T(D)\leftarrow C(D)$, $C(D)\leftarrow C(D)+B(D)D^{N-m}$, если $L\le N/2$, тогда $L\leftarrow N+1-L$, $m\leftarrow N$, $B(D)\leftarrow T(D)$.

2.3. $N\leftarrow N+1$.

3. Получение значения L.

Применим алгоритм БМ для оценки линейной сложности кода Гоппа. Для сравнения вычислим профиль линейной сложности последовательности криптографического генератора BBS. На рис. 3, *б*, *в*, *г* приведены графики профилей линейных сложностей последовательностей кода Гоппа и последовательности криптографического генератора BBS [5] (рис. 1, *а*).



а *б* *в* *г*

Рис. 2. Профили линейной сложности последовательностей кода Гоппа: *а* – последовательность BBS, $N=256$; *б* – последовательность кода Гоппа, $N=64$; и *в* – последовательность кода Гоппа, $N=128$; *г* – последовательность кода Гоппа, $N=256$

Анализ результатов вычислений показывают, что последовательности кода Гоппа имеют линейную сложность, близкую к сложности последовательностей криптографических булевых функций.

Заключение

Альтернантные коды Гоппа образуют обширное многообразие кодовых последовательностей. Анализ апериодических автокорреляционных функций показывает, что уровень максимального бокового лепестка не превышает величины $\rho_{\max}\le 2{,}6\sqrt{N}$, что является приемлемым для применения в системах локации и связи, например в устройствах блочной синхронизации. Кроме того, последовательности бинарных кодов Гоппа обладают профилем

линейной сложности, близким к профилю эталонных тестовых криптографических последовательностей BBS. Такое свойство обеспечивает дополнительную криптографическую защиту последовательностей кода Гоппа.

STRUCTURAL AND CORRELATION PROPERTIES OF SEQUENCES OF THE GOPPA CODE

S.B. SALOMATIN, V.V. PANKOVA

Abstract. The properties of the aperiodic autocorrelation function and the linear complexity of sequences formed on the basis of binary Goppa codes are considered. To solve this problem, algorithms have been developed for generating sequences of Goppa codes, calculating the aperiodic correlation function, constructing a linear complexity profile based on the Berlekamp-Massey procedure. It is shown that the aperiodic correlation function of Goppa code sequences has a low level of the maximum side lobe. Linear complexity graphs of Goppa code sequences have a profile close to the linear complexity profile of the BBS reference cryptographic generator. These properties make it possible to recommend Goppa code sequences for the synchronization of block error-correcting codes in communication systems and sounding signals in radar systems.

Keywords: error-correcting Goppa code, autocorrelation function, linear complexity of Boolean functions, Berlekamp-Massey algorithm.

Список литературы

1. Goppa V.D. // Problemy Peredachi Informatsii [Problems of information transmission]. 1970. Vol. 6. P. 207–212.
2. MacWilliams F.J., Sloane N.J.A. The Theory of Error Correcting Codes. New York. North-Holland Publ. 1977. P. 762.
3. Токарева Н.Н. Нелинейные булевы функции: бент-функции и их обобщения. Lap Lambert Academic Publishing (Saarbrucken, Germany). 2011. С. 180.
4. Саломатин С.Б. Поточные криптосистемы. Минск, БГУИР. 2006. С. 76.
5. Bernstein D.J., Buchmann J., Dahmen E. Post Quantum Cryptography. Springer Publishing Company, Incorporated, 1st edition. 2009. P. 249.