УДК 621.391.26

ЛИНЕЙНАЯ СЛОЖНОСТЬ АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДОВЫХ СТРУКТУР ПЕРЕМЕННОЙ СКОРОСТИ

В.В. ПАНЬКОВА, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
vr.pankova@gmail.com

Системы связи используют алгебро-геометрические кодовые структуры переменной скорости передачи информации. Оценка свойства линейной сложности кодовых последовательностей позволяет сделать вывод о возможности их формирования на основе заданного кодового сегмента и проанализировать эффективность процесса кодирования. Алгебро-геометрические кодовые структуры переменной скорости формируются на кривой Эрмита и предназначены для использования в современных сетях инфокоммуникаций.

Ключевые слова: алгебро-геометрический код (АГ-код), кривая Эрмита, линейная сложность, алгоритм Берлекэмпа-Месси (БМ).

Одна из главных задач современных систем передачи информации заключается в повышении эффективности использования пропускной способности каналов, что делает актуальными вопросы совершенствования методов кодирования. Системы связи широко используют коды с переменной скоростью передачи информации, позволяющие применять коллективный доступ с кодовым разделением и распределять полосу пропускания канала между различными источниками информации наиболее оптимально. Методы алгебро-геометрического кодирования являются перспективными и позволяют формировать множество кодовых структур для переменной скорости передачи. Алгоритм БМ позволяет исследовать линейную сложность алгебро-геометрических кодовых векторов переменной скорости, построенных на кривой Эрмита в поле GF(16), и на основе профилей линейной сложности кодовых структур оценить сложность воспроизведения каждой кодированной последовательности.

АГ-коды с переменной скоростью. Исследуемые кодовые конструкции построены на кривой Эрмита, заданной уравнением $f = y^4 + y - x^5$ в поле $GF(16)$, образованном примитивным многочленом $p(x) = x^4 + x + 1$. Кривая содержит 64 рациональные точки. Использование различного набора генераторных функций из базиса $\Phi = \{1, x, y, xy, x^2, x^2y, y^2 \ldots\}$, позволяет внести структурные изменения и сформировать коды $C^*(j)$ разных скоростей [1]: $C^*(10)$, $(64,19,40)$, $a+b \le 6$; $C^*(10)$, $(64,19,40)$, $a+b \le 10$; $C^*(7)$, $(64,30,25)$, $a+b \le 10$; $C^*(5)$, $(64,44,15)$, $a+b \le 10$; $C^*(5)$, $(64,44,15)$, $a+b \le 14$.

Множество кодовых слов $C(c_1, c_2, \ldots, c_{n-1})$ каждой кодовой конструкции $C^*(j)$ получено как произведение информационного вектора-строки на порождающую матрицу:

$$\left\| c_j \right\|_n = G \left\| I_i \right\|_k^T = \left\| \varphi_i(P_j) \right\|_{k,n} \left\| I_i \right\|_k^T, \qquad (1)$$

где $c = (c_0, c_1, \ldots, c_{n-1})$ – кодовое слово;

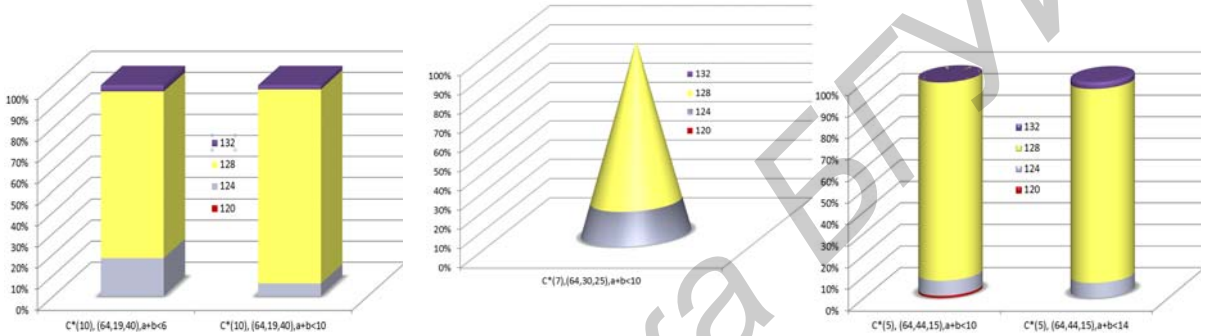
G – порождающая матрица размерности $k \times n$;

$I = (I_0, I_1, \ldots, I_{k-1})$ – информационный вектор.

Линейная сложность кодовых структур. Под линейной сложностью понимают длину самого короткого регистра сдвига с линейной обратной связью (РСЛОС), способного воспроизвести эту последовательность [2].

Анализ линейной сложности выбранных кодовых структур проводится на основе выборки из i=100 сформированных кодовых слов $C(c_1, c_2, ..., c_{n-1})$ каждой конструкции $C^*(j)$. Сформированные вектора алгебро-геометрического кода длиной $n = 64$ символа преобразованы в бинарные последовательности размерности $n = 256$, к которым применён алгоритм БМ. По результатам вычислений построены графики профилей линейной сложности.

Профили исследуемых кодовых структур имеют линейную зависимость, а все кодированные вектора характеризует высокий уровень линейной сложности, граничные значения которого меняются в пределах от 120 до 132. На рис.1 приведенырезультаты моделирования уровней линейной сложности для каждого кода $C^*(j)$.



а *б* *в*

Рис. 1. Значения уровней линейной сложности конструкций АГ-кодов переменной скорости:
а – коды $C^*(10)$; *б* – код $C^*(7)$; *в* – коды $C^*(5)$

На диаграммах представлены коды трёх скоростей передачи информации: для $C^*(10)$ скорость составляет 0,3, для $C^*(7)$ – 0,47, для $C^*(5)$ – 0,69, к тому же конструктивное различие в паре $C^*(10)$, как и в $C^*(5)$, – это разница в степенях генераторных функций. Подавляющее большинство в объёме исследуемых кодовых векторов, около 79-92%, в зависимости от конструкции $C^*(j)$, имеет уровень линейной сложности 128, что означает приемлемый профиль линейной сложности для каждой начальной точки кодированных последовательностей. Более высоким уровнем обладают коды, образованные при помощи генераторных функций более высоких степеней ($C^*(10)$, $a+b \le 10$; $C^*(5)$, $a+b \le 14$), зависимость же линейной сложности от скорости кода не значительна.

Таким образом, АГ-коды характеризуются устойчивой сложностью воспроизведения (РСЛОС с полиномом обратной связи степени не ниже 120), сравнимой со сложностью квадратично-вычетных кодов. Одной такой качественной характеристики, как высокая линейная сложность, недостаточно для гарантии стойкости, но низкая линейная сложность означала бы очевидную недостаточную надёжность при использовании таких кодовых структур в алгоритмах кодирования с переменной скоростью передачи.

Список литературы

1.*PatrickJ.Morandi.*Lecture Notes for Mathematics 601. Error Correcting Codes and Algebraic Curves.Fall, 2001.

2. *Саломатин С.Б*. Поточные криптосистемы: учеб.пособие. Минск, 2006.