УДК 621.391

ПОСТРОЕНИЕ ПОМЕХОУСТОЙЧИВЫХ КОДОВ ПО АЛГЕБРАИЧЕСКИМ КРИВЫМ

В.Н. Лысенко
(представил д.т.н., проф. Ю.В. Стасев)

Рассматриваются алгеброгеометрические коды, построенные по точкам алгебраических кривых. Предложен конструктивный подход по сокращению сложности практических схем кодирования и декодирования.

Постановка проблемы в общем виде. Эффективным средством повышения достоверности передаваемой информации являются методы помехоустойчивого кодирования. Одним из перспективных направлений их развития являются методы кодирования, основанные на использовании свойств алгебраических кривых. Нерешенной проблемой в их использовании является высокая сложность реализации процедур кодирования и декодирования. Актуальной научно-технической задачей является разработка методов алгеброгеометрического кодирования, допускающих простую практическую реализацию.

Анализ литературы. Алгеброгеометрические коды как линейные системы на алгебраических кривых впервые были предложены В.Д. Гоппой [1]. Коды, построенные по кривым с большим числом точек по сравнению с родом, лежат выше границы Варшамова-Гилберта [2]. В работах [3 – 4] предложены практические схемы кодирования и декодирования. **Целью статьи** является обоснование конструктивного подхода, по сокращению сложности процедур кодирования и декодирования алгеброгеометрических кодов.

Конструкция кодов по алгебраическим кривым. Пусть C – класс дивизоров на X степени α. Тогда C задает отображение φ: $X \to P^m$, набор генераторных функций $y_i = \varphi(x_i)$ задает алгеброгеометрический код длины $n \le N$. Кодовые характеристики (n, k, d) связаны соотношением $k + d \ge n - g + 1$ [1–2]. Если $2g - 2 < \alpha \le n$, код связан характеристиками $(n, \alpha - g + 1, d \ge n - \alpha)$. Дуальный к нему код также является алгеброгеометрическим с характеристиками $(n, n - \alpha + g - 1, d_\perp \ge \alpha - 2g + 2)$.

Определение [3]. Алгеброгеометрический код по кривой X над GF(q) – это линейный код, состоящий из всех слов $(c_1, c_2, \dots, c_n)$ длины $n \le N$, для которых выполняется равенство $d + g - 1$ уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0, \qquad (1)$$

где $c_i \in GF(q)$, $d \geq \alpha - 2g + 2$, $\alpha = degX \cdot degF$.

Это определение равносильно матричному представлению алгебро-геометрического кода

$$H\,(c_0, c_1, \ldots, c_{n-1})^T = 0,$$

где H – проверочная матрица кода размерности $r \times n$, $r = n - k = d + g - 2$

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \ldots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \ldots & F_1(P_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_{r-1}(P_0) & F_{r-1}(P_1) & \ldots & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}.$$

Известные примеры алгеброгеометрических кодов [1 – 2], практические схемы алгоритмов кодирования и декодирования [3 – 4] рассмотрены для кодов, построенных по точкам кривой Эрмита. Кривая Эрмита (Hermit curve), задается множеством решений однородного алгебраического уравнения

$$x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0 \qquad (2)$$

над полем GF(q), $q = r^2$, r – положительное целое число. Род такой кривой $g = \left(q - \sqrt{q}\right)/2$, число точек $N = q\sqrt{q} + 1$. Точки кривой, как решения уравнения (1), однозначно задаются набором P(X, Y, Z).

Основной затратной процедурой в практических схемах алгеброгеометрического кодирования является вычисление генераторной функции F_j в точке P_i алгебраической кривой X. Для вычисления каждого значения $F_j(P_i)$ необходимо выполнить, в общем виде, три операции возведения в степень и две операции умножения. Для аналогичных вычислений в схемах, использующих известные коды Рида-Соломона, необходимо выполнить одну операцию возведения в степень. Очевидно, что сложность основной базовой операции алгеброгеометрического кодирования выше в несколько раз.

Сокращение сложности практических схем. В статье предлагается конструктивный подход сокращения сложности алгеброгеометрического кодирования, состоящий в использовании алгебраических кривых, заданных множеством решений вида P(X, Y, 1). Применение подобных кривых позволит снизить сложность вычисления генераторных функций в точках кривой, что, в свою очередь, снизит сложность практических схем кодирования и декодирования в целом. В ходе проведенных исследований, путем полного перебора всех неприводимых полиномиальных форм от трех переменных степени 3 – 5 и нахождения их решений, вы-

делен класс кривых (3) – (5), дающих $N = q\sqrt{q} + 1$ решений над полем GF(q), $q = r^2$, r – положительное целое число, при роде $g = \left(q - \sqrt{q}\right)/2$:

$$x^{\sqrt{q}+1} + y^{\sqrt{q}} z + yz^{\sqrt{q}} = 0; \quad (3)$$

$$x^{\sqrt{q}+1} + x^{\sqrt{q}} y + x^{\sqrt{q}} z + xy^{\sqrt{q}} + xz^{\sqrt{q}} + y^{\sqrt{q}+1} = 0; \quad (4)$$

$$x^{\sqrt{q}+1} + x^{\sqrt{q}} y + x^{\sqrt{q}} z + xy^{\sqrt{q}} + xz^{\sqrt{q}} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0. \quad (5)$$

Проведенные исследования свойств точек кривых (2) – (4) показали, что $N = q\sqrt{q}$ решений однозначно задаются набором P(X, Y, 1). Подобная форма точек позволяет упростить процедуру вычисления генераторных функций в точках кривой. При укорочении на один символ кода для вычисления генераторных функций $F_j(P_i)$ необходимо выполнить две операции возведения в степень и одну операцию умножения. Очевидно, что по сравнению с общей схемой алгеброгеометрического кодирования, предлагаемый подход позволяет более чем на треть снизить сложность практической реализации.

Выводы. Использование предлагаемого подхода в известных практических схемах алгеброгеометрического кодирования [3 – 4] позволит на 30 – 40% снизить сложность их реализации.

Перспективы дальнейших исследований. Одним из перспективных направлений дальнейших исследований является изучение групповых свойств точек кривых (2) – (4), выработка практических рекомендаций по их использованию в практических схемах алгеброгеометрического кодирования.

ЛИТЕРАТУРА

1. *Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259. – № 6. – С. 1289 – 1290.*
2. *Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова-Гилберта. // Проблемы передачи информации. – М. – 1982. – № 3. – С. 3 – 6.*
3. *Кузнецов А.А., Северинов А.В., Лысенко В.Н., Науменко И.В. Алгоритм помехоустойчивого кодирования с использованием кодов по кривым Эрмита // Системи обробки інформації.– Х.: НАНУ, ПАНМ, ХВУ. – 2003. – Вип. 6. – С. 181 – 185.*
4. *Кузнецов А.А., Северинов А.В., Лысенко В.Н. Алгоритм мажоритарного декодирования алгеброгеометрических кодов // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ. – 2003. – Вип. 4. – С. 13 – 18.*

Поступила 19.12.2003

***ЛЫСЕНКО Валерий Николаевич**, старший научный сотрудник Научного центра РВиА. В 1985 году окончил ХВВКИУ РВ. Область научных интересов – применение помехоустойчивого кодирования в системах передачи данных.*