УДК 621.391

О.О. Кузнецов[1], І.В. Пасько[2]

[1]*Харківський університет Повітряних Сил ім. І. Кожедуба*
[2]*Військовий інститут ракетних військ та артилерії ім. Б. Хмельницького, Суми*

АЛГЕБРАЇЧНИЙ МЕТОД ДЕКОДУВАННЯ ЛІНІЙНИХ БЛОКОВИХ КОДІВ НА АЛГЕБРАЇЧНИХ КРИВИХ У P^3

Розглядаються лінійні блокові коди, побудовані на алгебраїчних кривих (алгеброгеометричні коди) у проективному просторі P^n. Досліджується задача декодування алгеброгеометричних кодів Пропонується алгебраїчний метод декодування кодів на кривих у P^3.

алгеброгеометричний код, декодування, алгебраїчна крива

Постановка проблеми в загальному вигляді,яналізялітератур, я

Перспективним напрямком у розвитку теорії завадостійкого кодування є коди, що виникають на алгебраїчних кривих [1 – 5].

Алгеброгеометричні коди вперше запропоновані в роботах [1, 2]. В [3 – 5] показано, що кодові характеристики цих кодів при великій довжині лежать вище границі Варшамова-Гилберта. У роботах [6, 7] досліджений енергетичний виграш від їх використання в дискретних каналах з незалежними помилками. У той же час методи декодування алгеброгеометричних кодів орієнтовані на вузький клас кодів і, строго говорячи, не дозволяють реалізувати всі їх потенційні властивості. Так, у роботах [8, 9] досліджені неалгебраїчні методи декодування (мажоритарний і переставний методи), у яких показано, що для реалізації мажоритарного методу код повинен допускати повну ортогоналізацію [8], ефективно реалізувати переставний декодер, як показано в [9], для порівняно невеликої довжини коду.

Досліджені в роботах [10 – 12] алгебраїчні методи декодування дозволяють звести задачу локалізації й виправлення помилок до розв‘язання систем лінійних рівнянь. Однак вони дозволяють декодувати тільки коди, які побудовані на алгебраїчних кривих у проективному просторі P^2. У той же час із ростом розмірності P^m істотно зростають потенційні властивості алгеброгеометричних кодів: істотно збільшується їх довжина і виправна здатність.

Таким чином, актуальним є дослідження алгебраїчних методів декодування кодів на кривих у P^m, $m > 2$.

Метою статті є виклад основних результатів, отриманих при розробці алгебраїчного методу декодування лінійних блокових кодів на алгебраїчних кривих у P^3.

Загальнаконструкціякодівяна алгебраїчн, хякр, в, х

Зафіксуємо кінцеве поле GF(q). Нехай Cur – гладка проективна алгебраїчна крива в проективному просторі P^m над GF(q), $g = g(Cur)$ – рід кривої, Cur(GF(q)) – множина її точок над кінцевим полем, $N = |Cur(GF(q))|$ – їх число. Нехай C – клас дивізорів на Cur степеня

$$\alpha > g - 1.$$

Тоді C визначає відображення φ: Cur $\to P^M$, що задає алгеброгеометричний код.

Ця конструкція дозволяє будувати коди з параметрами

$$k + d \ge n - g + 1,$$

довжина n яких менше або дорівнює числу точок на кривій Cur. При $2g < \alpha \le n$ алгеброгеометричний код має параметри:

$$(n, \alpha - g + 1, d);\ d \ge n - \alpha .$$

Подвійний до нього код також є алгеброгеометричним і має параметри:

$$(n, n - \alpha + g - 1, d^{\perp});\ d^{\perp} \ge \alpha - 2g + 2.$$

Розглянемо кодове слово

$$c = (c_0, c_1, \ldots, c_{n-1})$$

алгеброгеометричного (n, k, d) коду над GF(q), побудованого за алгебраїчними кривиим у P^3.

Припустимо, що алгеброгеометричний код заданий через перевірочну матрицю H вигляду (1):

$$H = \begin{pmatrix} F_{0,0,0}(X_0,Y_0,Z_0) & F_{0,0,0}(X_1,Y_1,Z_1) & \ldots & F_{0,0,0}(X_{n-1},Y_{n-1},Z_{n-1}) \\ F_{1,0,0}(X_0,Y_0,Z_0) & F_{1,0,0}(X_1,Y_1,Z_1) & \ldots & F_{1,0,0}(X_{n-1},Y_{n-1},Z_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ F_{0,0,\deg F}(X_0,Y_0,Z_0) & F_{0,0,\deg F}(X_1,Y_1,Z_1) & \ldots & F_{0,0,\deg F}(X_{n-1},Y_{n-1},Z_{n-1}) \end{pmatrix}, \quad (1)$$

де F_{i_x,i_y,i_z} – одночлен степеня $i_x + i_y + i_z \le \deg F$,

тобто $F_{i_x,i_y,i_z} = x^{i_x} \cdot y^{i_y} \cdot z^{i_z}$; $i = 0,\ldots,M-1$;

$$M = C^0_{\deg F} + C^1_{1+\deg F} + C^2_{2+\deg F} + C^3_{3+\deg F};$$

$(X_j, Y_j, Z_j, 1)$ – проективні точки кривій Cur, тобто

такі набори з GF(q), які перетворюють у нуль многочлен кривої.

Тоді справедлива рівність $c \cdot H = 0$, звідки випливає рівність:

$$\sum_{j=0}^{n-1} c_j \cdot F_{i_x,i_y,i_z}(X_j, Y_j, Z_j) = 0,$$

для всіх $i = 0,..., M-1$.

Припустимо, що при передачі по каналу з помилками кодове слово спотворилося, вектор помилок позначимо як

$$e = (e_0, e_1, \ldots, e_{n-1}).$$

Прийняте слово

$$c^* = (c_0^*, c_1^*, ..., c_{n-1}^*),$$

після передачі по каналу з помилками, запишеться у вигляді

$$c^* = c + e = (e_0 + c_0, e_1 + c_1, \ldots, e_{n-1} + c_{n-1}),$$

тобто $c_j^* = c_j + e_j$, $j = 0,\ldots, n-1$.

Визначимо синдромну послідовність як вектор

$$s = \left(s_{0,0,0}, s_{1,0,0}, ..., s_{0,0,\deg F}\right),$$

обчислений за правилом:

$$s_{i_x,i_y,i_z} = \sum_{j=0}^{n-1} e_j \cdot F_{i_x,i_y,i_z}(X_j, Y_j, Z_j),\ i = 0,..., M-1.$$

За визначенням, значення синдромної послідовності s залежить тільки від вектора помилок e і не залежить від кодового слова c. Дійсно, обчислимо добуток $c^* \cdot H = 0$,одержимо

$$(c + e) \cdot H = c \cdot H + e \cdot H = e \cdot H,$$

звідки випливає справедливість $i = 0,..., M-1$ рівностей:

$$\sum_{j=0}^{n-1} (c_j + e_j) \cdot F_{i_x,i_y,i_z}(X_j, Y_j, Z_j) = \sum_{j=0}^{n-1} e_j \cdot F_{i_x,i_y,i_z}(X_j, Y_j, Z_j) = s_{i_x,i_y,i_z}. \quad (2)$$

Задача алгебраїчного декодування кодового слова алгеброгеометричного коду, побудованого за кривою у P^3, полягає в знаходженні вектора

$$e = (e_0, e_1, \ldots, e_{n-1})$$

за відомою синдромною послідовністю

$$s = \left(s_{0,0,0}, s_{1,0,0}, ..., s_{0,0,\deg F}\right).$$

Знаходження вектора e дозволяє у свою чергу відновити кодове слово c за відомою послідовністю c^*:

$$c = c^* - e = (c_0^* - e_0, c_1^* - e_1, ..., c_{n-1}^* - e_{n-1}).$$

Пропонован, йяметодяя алгебраїчногоядекодуванняя

Розв‘язання поставленої задачі алгебраїчного декодування шляхом обчислення вектора

$$e = (e_0, e_1, \ldots, e_{n-1})$$

із сукупності рівностей (2) пов‘язано зі знаходженням n невідомих у системі з M лінійних рівнянь, причому

$$M < n.$$

При розв‘язанні поставленої задачі методами лінійної алгебри в загальному випадку існує множина розв‘язань системи рівнянь (2). У той же час відзначимо, що тільки

$$u \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor$$

значень послідовності

$$(e_0, e_1, \ldots, e_{n-1})$$

не дорівнюють нулю, тобто майже всі $e_j = 0$, за винятком якогось (кінцевого) їх числа (u). З урахуванням цього обмеження існує одне (єдине) розв‘язання сукупності рівнянь (2), яке й необхідно знайти.

Позначимо множину $e_j \neq 0$ символом E. Для однозначного знаходження вектора помилок скористаємося штучним прийомом, що полягає у веденні многочлена локаторів помилок:

$$\Lambda(x, y, z) = x^{u-2} + a_{t-3,1,0} \cdot x^{u-3} \cdot y + ... + a_{1,0,0} \cdot x + a_{0,1,0} \cdot y + a_{0,0,1} \cdot z + a_{0,0,0}, \quad (3)$$

розв‘язаннями якого є локатори – такі набори (X_ξ, Y_ξ, Z_ξ), які перетворюють у нуль многочлен (3), причому всі $e_\xi \in E$.

Многочлен (3) однозначно задає розташування помилок у векторі

$$e = (e_0, e_1, \ldots, e_{n-1}),$$

тому що однозначно вказує на його ненульові компоненти. Інакше кажучи, знаходження коефіцієнтів a_{i_x,i_y,i_z} многочлена локаторів помилок $\Lambda(x, y, z)$ дозволяє однозначно вказати розташування виниклих при передачі кодового слова помилок (але не їх значення – справжні значення ненульових величин e_j), наприклад, шляхом почергової підстановки всіх наборів (X_j, Y_j, Z_j), j = 0,…, n–1 у многочлен $\Lambda(x, y, z)$ і перевірки на його рівність нулю.

Помножимо многочлен (3) на e_j й обчислимо в точці $(X_j, Y_j, Z_j, 1)$, одержимо:

$$e_j \cdot X_j^{u-2} + a_{t-3,1,0} \cdot e_j \cdot X_j^{u-3} \cdot Y_j + ... + a_{1,0,0} \cdot e_j \cdot X_j + a_{0,1,0} \cdot Y_i + a_{0,0,1} \cdot e_j \cdot Z_j + a_{0,0,0} \cdot e_j. \quad (4)$$

Проаналізуємо отриманий вираз. Якщо $e_j \notin E$, тобто $e_j = 0$, тоді всі доданки отриманого многочлена дорівнюють нулю, тобто маємо рівність нулю всього виразу (4). Якщо $e_j \in E$, тобто $e_j \neq 0$, тоді відповідні набори (X_j, Y_j, Z_j) перетворюють у нуль многочлен (3) і, відповідно, многочлен (4). Таким

чином, при будь-якому значенні e_j маємо рівність нулю виразу (4).

Візьмемо суму за всіма j = 0,...,n-1, одержимо:

$$\sum_{j=0}^{n-1} e_j \cdot X_j^{u-2} + \sum_{j=0}^{n-1} a_{t-3,1,0} \cdot e_j \cdot X_j^{u-3} \cdot Y_j + \ldots + \\ + \sum_{j=0}^{n-1} a_{1,0,0} \cdot e_j \cdot X_j + \sum_{j=0}^{n-1} a_{0,1,0} \cdot e_j \cdot Y_j + \\ + \sum_{j=0}^{n-1} a_{0,0,1} \cdot e_j \cdot Z_j + \sum_{j=0}^{n-1} a_{0,0,0} \cdot e_j = 0. \qquad (5)$$

Проаналізуємо отриманий вираз. Значення a_{i_x,i_y,i_z} не залежать від j, винесемо їх за знак підсумовування. З обліком уведених вище позначень, значення одночлена

$$F_{i_x,i_y,i_z} = x^{i_x} \cdot y^{i_y} \cdot z^{i_z}$$

у точці $(X_j, Y_j, Z_j, 1)$ прийме вид

$$F_{i_x,i_y,i_z}(X_j, Y_j, Z_j) = X_j^{i_x} \cdot Y_j^{i_y} \cdot Z_j^{i_z}.$$

З урахуванням останнього виразу (5) перепишеться у вигляді:

$$\sum_{j=0}^{n-1} e_j \cdot F_{u-2,0,0}(X_j, Y_j, Z_j) + \\ + a_{t-3,1,0} \sum_{j=0}^{n-1} e_j \cdot F_{u-3,1,0}(X_j, Y_j, Z_j) + \ldots + \\ + a_{1,0,0} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{1,0,0}(X_j, Y_j, Z_j) + \\ + a_{0,1,0} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{0,1,0}(X_j, Y_j, Z_j) + \\ + a_{0,0,1} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{0,0,1}(X_j, Y_j, Z_j) + \\ + a_{0,0,0} \cdot \sum_{j=0}^{n-1} e_j \cdot F_{0,0,0}(X_j, Y_j, Z_j) = 0.$$

Але за уведеним вище визначенням

$$s_{i_x,i_y,i_z} = \sum_{j=0}^{n-1} e_j \cdot F_{i_x,i_y,i_z}(X_j, Y_j, Z_j).$$

Отже, маємо:

$$s_{u-2,0,0} + a_{t-3,1,0} \cdot s_{u-3,1,0} + \ldots + a_{1,0,0} \cdot s_{1,0,0} + \\ + a_{0,1,0} \cdot s_{0,1,0} + a_{0,0,1} \cdot s_{0,0,1} + a_{0,0,0} \cdot s_{0,0,0} = 0.$$

Повернемося тепер до розгляду многочлена (3). Помножимо його на довільний одночлен $x^{i_x} \cdot y^{i_y} \cdot z^{i_z}$ і проведемо аналогічні міркування. За аналогією з (4) збережеться рівність нулю при будь-якому значенні e_j. Після підсумовування за всіма j = = 0,...,n–1 і виконанні очевидних підстановок одержимо:

$$s_{i_x+u-2,i_y,i_z} + a_{t-3,1,0} \cdot s_{i_x+u-3,i_y+1,i_z} + \ldots + \\ + a_{1,0,0} \cdot s_{i_x+1,i_y,i_z} + a_{0,1,0} \cdot s_{i_x,i_y+1,i_z} + \\ + a_{0,0,1} \cdot s_{i_x,i_y,i_z+1} + a_{0,0,0} \cdot s_{i_x,i_y,i_z} = 0.$$

Виконавши відповідні перетворення для всіх $i = 0,\ldots, M-1$, одержимо систему лінійних рівнянь:

$$\begin{cases} s_{u-2,0,0} + a_{u-3,1,0} \cdot s_{u-3,1,0} + \ldots + a_{1,0,0} \cdot s_{1,0,0} + \\ + a_{0,1,0} \cdot s_{0,1,0} + a_{0,0,1} \cdot s_{0,0,1} + a_{0,0,0} \cdot s_{0,0,0} = 0; \\ s_{u-1,0,0} + a_{u-3,1,0} \cdot s_{u-2,1,0} + \ldots + a_{1,0,0} \cdot s_{2,0,0} + \\ + a_{0,1,0} \cdot s_{1,1,0} + a_{0,0,1} \cdot s_{1,0,1} + a_{0,0,0} \cdot s_{1,0,0} = 0; \\ \ldots \\ s_{2\cdot u-4,0,0} + a_{u-3,1,0} \cdot s_{2\cdot u-5,1,0} + \ldots + a_{1,0,0} \cdot s_{u-1,0,0} + \\ a_{0,1,0} \cdot s_{u-2,1,0} + a_{0,0,1} \cdot s_{u-2,0,1} + a_{0,0,0} \cdot s_{u-2,0,0} = 0. \end{cases} \qquad (6)$$

При числі невідомих v у многочлені локаторів помилок меншому числа елементів синдромної послідовності система лінійних рівнянь (6) розв'язна. Складність її розв‘язання, наприклад, методом Гаусса складе v^2.

Розв‘язання системи (6) дають значення невідомих коефіцієнтів многочлена локаторів помилок $\Lambda(x, y, z)$ (3), що у свою чергу однозначно задає значення локаторів – таких наборів (X_ξ, Y_ξ, Z_ξ), які перетворюють у нуль многочлен (3), причому всі $e_\xi \in E$. Пошук шуканих (X_ξ, Y_ξ, Z_ξ) може бути виконаний, наприклад, почерговою підстановкою всіх (X_j, Y_j, Z_j), j = 0,…, n–1 у многочлен $\Lambda(x, y, z)$ і перевіркою тотожності

$$\Lambda(X_j, Y_j, Z_j) = 0.$$

Знайдені (X_ξ, Y_ξ, Z_ξ) локалізують помилку в кодовому слові, тобто дорівняють нулю n – u невідомих у системі (2). Оскільки решта невідомих u < M, система (2) розв'язна. Складність її розв‘язання, наприклад, методом Гаусса не перевершує u^2. Розв‘язання системи (2) дає шукані (ненульові) значення вектора помилок $e = (e_0, e_1, \ldots, e_{n-1})$, тобто задача декодування вирішена.

Таким чином, у результаті проведених досліджень отримано загальне розв‘язання задачі декодування алгеброгеометричних кодів, побудованих за кривими у P^3.

В, сновк,

Уперше запропонований алгебраїчний метод декодування алгеброгеометричних кодів за кривими у P^3, що дозволяє звести задачу декодування до розв‘язання систем лінійних рівнянь, у яких число невідомих задається конструктивними кодовими характеристиками. Показано, що складність алгебраїчного декодування запропонованим методом росте поліноміально від відправної здатності коду.

Перспективним напрямком подальших досліджень є розробка практичних алгоритмів декоду-

вання з використанням запропонованого методу, дослідження їх часової і ємнісної складності реалізації.

Сп, сокялітератур, я

1. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т. 259, № 6. – С. 1289-1290.

2. Гоппа В.Д. Коды и информация // Успехи математических наук. – 1984. –Т. 30, вып. 1 (235). – С. 77-120.

3. Влэдуц С. Г., Манин Ю. И. Линейные коды и модулярные кривые // Современные проблемы математики. – М.: ВИНИТИ. – 1984. – Т. 25. – С. 209-257.

4. Ruud Pellikaan. Asymptotically good sequences of curves and codes // Proc. 34th Allerton Conf. on Communication, Control, and Computing, Urbana-Champaign, October 2-4, 1996. – 1996. – P. 276-285.

5. Voss, Tom Hoholdt. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps. //IEEE Trans. Info. Theory. – 1997. – vol. IT-43. – P. 128-135.

6. Кузнецов А.А. Энергетический выигрыш алгебро-геометрического кодирования // Радиотехника. – Х.: ХТУРЭ. – 2003. – Вып. 134. – С. 218-222.

7. Кузнецов А.А. Энергетическая эффективность алгеброгеометрических кодов // Электронное моделирование: Международный научно-теоретический журнал. – К: НАНУ, РАН. – 2004. – № 2. – С. 27-38.

8. Кузнецов А.А., Северинов А.В., Лысенко В.Н. Алгоритм мажоритарного декодирования алгеброгеометрических кодов // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ. – 2003. – Вип. 4 (26). – С. 61-66.

9. Северинов А.В., Кузнецов А.А., Куриш В.В. Разработка алгоритма декодирования алгеброгеометрических кодов // Системи обробки інформації. – Х.: НАНУ, ПАНИ, ХВУ. – Вип 1 (17). – 2002. – С. 161-163.

10. Кузнецов А.А., Северинов А.В., Задворный Д.А. Лысенко В.Н. Алгебраическое декодирование кодов по кривым Эрмита // Вісник ХПІ. – Х.: НТУ "ХПІ" – 2003. – № 26. – С 95-102.

11. Feng G.L., Rao T.R.N. Decoding algebraic geometric codes up to the designed minimum distance // IEEE Trans. Inform. Theory. – 1993. – Vol. 39, N 1 – P. 37-46.

12. Sakata S., Justesen J., Madelung Y., Jensen H.E., Hoholdt T. Fast Decoding of Algebraic-Geometric Codes up to the Designed Minimum Distance // IEEE Trans. Inform. Theory. – 1995. – Vol. 41, N 5 – P. 1672-1677.

Надійшла до редколегії 4.08.2006

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.