РОЗРОБЛЕННЯ ТА МОДЕРНІЗАЦІЯ ОВТ

УДК 621.391

В.І. Грабчак

Академія сухопутних військ , Львів

СИНТЕЗ КАСКАДНИХ КОДІВ З АЛГЕБРОГЕОМЕТРИЧНИМИ КОДАМИ НА ЗОВНІШНІЙ СТУПЕНІ

В статті досліджуються питання побудови каскадних кодів з алгеброгеометричними кодами на зовнішній ступені, застосування яких в апаратурі передачі даних АСУВ дозволить суттєво знизити складність процедур кодування і декодування та підвищити завадостійкість інформації, що оброблюється і передається. Розглядаються теоретичні питання побудови каскадних кодів з алгеброгеометричними кодами на зовнішній ступені, наведений приклад практичної реалізації завадостійкого кодування і декодування каскадних кодів з алгеброгеометричним кодом на зовнішній ступені.

Ключові слова: *каскадні коди, алгеброгеометричні коди, процедури кодування та декодування.*

Вступ

Постановка проблеми в загальному вигляді та аналіз літератури. Важливою вимогою до перспективної автоматизованої системи управління військами (АСУВ) є вірогідність даних, що оброблюються та передаються. Цей показник характеризує здатність системи забезпечувати точне відтворення повідомлень, що передаються, у пунктах прийому [1]. При підвищених вимогах до швидкості і вірогідності інформації, що передається, необхідні показники досягаються застосуванням спеціальних засобів захисту повідомлень від помилок. Одним із найбільш ефективних засобів захисту даних, що передаються, від помилок є методи завадостійкого кодування [2, 3].

Перспективним напрямком у розвитку алгебраїчної теорії завадостійкого кодування є розробка лінійних блокових кодів по алгебраїчних кривих (алгеброгеометричні коди) [4, 5]. В роботі [6] показано, що теорія їх побудови узагальнює більшість відомих алгебраїчних кодів, таких, наприклад, як великий клас циклічних кодів, у тому числі кодів Боуза-Чоудхурі-Хоквінгема, кодів Ріда-Соломона і їх узагальнень, альтернантних кодів, у тому числі кодів Гоппи, Сривестави та інших. Основна перевага методів алгеброгеометричного кодування складається у побудові довгих недвійкових блокових кодів, які мають добрі асимптотичні властивості. У роботі [7] показано, що використання алгеброгеометричних кодів для передачі даних по дискретних каналах зв'язку дозволяє отримати суттєвий енергетичний виграш від кодування.

Основним недоліком застосування алгеброгеометричних кодів є висока складність кодування і декодування кодограм. Для зменшення складності кодування і декодування кодограм пропонується використовувати каскадні коди, які вперше були запропоновані Форні [2, 8] як метод практичної реалізації коду з великою довжиною і високою корегуючою здібністю.

Метою статті є синтез каскадних кодів з алгеброгеометричними кодами на зовнішній ступені, розробка практичних процедур їх кодування і декодування.

Основний матеріал

Каскадні коди. Найбільш розповсюдженою схемою побудови каскадних кодів є схема з двома рівнями кодування. В якості коду зовнішньої ступені, як правило, використовують коди, які спроможні виправити складні комбінації корельованих помилок, мають добрі асимптотичні властивості та відносно просто реалізуються. В якості коду внутрішньої ступені можна вибрати один із багатьох різних кодів [2, 8]. Схема каскадного кодування з двома рівнями наведена на рис. Припустимо, що зовнішнім кодом є недвійковий код, який використовує K – бітові символи. Ці символи надходять до кодера зовнішнього коду від джерела інформації, як показано на рис.1. Крім того, припустимо, що зовнішній код є блоковим і його блок складається з n – символів, причому k з них є інформаційними. Потім K – бітові символи, які виходять з кодера зовнішнього коду, кодуються кодером внутрішнього коду. При цьому добавляються N-K перевірочних двійкових символів,

так що довжина блоку внутрішнього коду дорівнює N. Декодування відбувається у зворотному порядку.

Довжина каскадного коду $N^* = n \cdot N$ двійкових символів, причому $K^* = k \cdot K$ символів кодового слова – інформаційні, і швидкість коду дорівнює $R^* = r \cdot R = \frac{kN}{nN}$, де $R = KN$ і $r = \frac{k}{n}$. За умови, що загальна довжина коду дорівнює $n \cdot N$, каскадне кодування забезпечує таку структуру коду, що декодування може здійснюватися за допомогою двох декодерів для кодів із довжинами N і n відповідно, що дозволяє суттєво знизити складність порівняно з тою, яка вимагалася б при декодуванні коду на одному рівні.

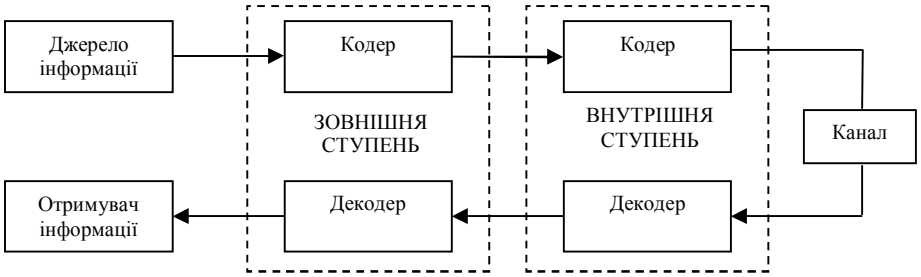

Рис. 1. **Каскадне кодування**

Алгеброгеометричні коди. АГК як лінійні системи на алгебраїчних кривих уперше були запропоновані В.Д. Гоппою [4, 5]. Розглянемо загальну схему побудови АГК [6].

Зафіксуємо скінчене поле GF(q). Нехай X – гладка проективна алгебраїчна крива в проективному просторі P^n над GF(q), g = g(X)– рід кривої, *X(GF(q))* – множина її точок над скінченим полем, N = |X(GF(q))| – їх число. Число N точок кривої X над GF(q) обмежено зверху виразом Хассе-Вейля [4, 5] $N \le 2\sqrt{q} \cdot g + q + 1$.

Нехай C – клас дивізорів на X степеня α. Тоді C визначає відображення $\varphi : X \to P^{k-1}$, де $k \ge \alpha - g + 1$. Набір генераторних функцій $y_i = \varphi(x_i)$ задає АГК довжини $n \le N$.

Кодові характеристики (n, k, d) зв'язані співвідношенням [4, 5]: $k + d \ge n - g + 1$. Якщо $2g - 2 < \alpha \le n$, код зв'язаний характеристиками $(n, \alpha - g + 1, d), d \ge n - \alpha$. Дуальный до нього код також є алгеброгеометричним з характеристиками $(n, n - \alpha + g - 1, d_\perp)$, $d_\perp \ge \alpha - 2g + 2$.

Кодування алгеброгеометричними кодами. Розглянемо варіант побудови АГК, заданого через породжувальну матрицю [6]. АГК над GF(q) побудований через відображення кривої X виду $\varphi : EC \to P^{k-1}$ це лінійний код довжини $n \le N$, кодові слова $C(c_0, c_1, ..., c_{n-1})$ якого задаються рівністю

$$\sum_{j=0}^{k-1} I_j F_j(P_i) = c_i , \qquad (1)$$

де P_i (X_i, Y_i, Z_i) – проективні точки кривої X, тобто (X_i, Y_i, Z_i) – розв'язання однорідного алгебраїчного рівняння, що задають криву X, $i = \overline{1,n}$; $F_j(P_i)$ – значення генераторних функцій у точках кривої.

Це визначення рівносильне матричному поданню АГК:

$$G\,(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}),$$

де G – породжувальна матриця розмірності $k \times n$, $k = \alpha - g + 1$, $\alpha = \deg X \cdot \deg F$.

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}. \qquad (2)$$

Кодове слово, в цьому випадку, може бути сформовано (у матричній формі) як добуток інформаційного вектора-строки на породжувальну матрицю [9]:

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

АГК над GF(q) побудований через відображення кривої X виду $\varphi : EC \to P^{r-1}$ це лінійний код довжини $n \le N$, кодові слова $C(c_0, c_1, ..., c_{n-1})$ якого задаються рівністю

$$\sum_{j=0}^{n-1} c_i F_j(P_i) = 0 , \qquad (3)$$

де $c_i \in GF(q)$, $d \ge \alpha - 2g + 2$, $\alpha = \deg X \cdot \deg F$.

Це визначення рівносильне матричному поданню АГК: $H\,(c_0, c_1, ..., c_{n-1})^T = 0$, де H – перевірочна матриця розмірності r x n, $r = n - k = d + g - 2$.

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}. \qquad (4)$$

Розглянутий алгоритм побудови АГК може бути ефективно використаний при реалізації процедури кодування на зовнішній ступені каскадного коду.

Декодування алгеброгеометричних кодів.

Припустимо, що при передачі по каналу з помилками кодове слово АГК спотворилося, вектор помилок позначимо як $e=(e_0, e_1, ..., e_{n-1})$. Прийняте слово c^* після передачі по каналу з помилками запишеться у вигляді $c^* = c+e = (e_0+c_0, e_1+c_1, ..., e_{n-1}+c_{n-1})$.

Визначимо синдромну послідовність як вектор $S = (S_0, S_2, \ldots, S_{r-1})$, обчислений за наступним правилом

$$S_j = \sum_{i=0}^{n-1} c^* \cdot F_j(P_i), \quad j = \overline{1,r}, \qquad (5)$$

чи в матричній формі $\|S_j\|_r = \|F_j(P_i)\|_{n,r} \|c_i^*\|_n^T$.

Очевидно, що

$$S_j = \sum_{i=0}^{n-1}\left[c_i \cdot F_j(P_i) + e_i \cdot F_j(P_i)\right] = \sum_{i=0}^{n-1} e_i \cdot F_j(P_i),$$

$$j = \overline{1,r},$$

чи в матричній формі

$$\|S_j\|_r = \|F_j(P_i)\|_{n,r} \cdot \|e_i\|_n^T = H\,\|e_i\|_n^T,$$

значення синдрому залежить тільки від вектора помилок і не залежить від кодового слова.

Задача декодування АГК складається у знаходженні вектору помилок $e=(e_0, e_1, ..., e_{n-1})$ за відомою синдромною послідовністю $S = (S_0, S_1, \ldots, S_{r-1})$.

Розглянемо, як генераторні функції однорідні одночлени степеня $\deg F$. Кожен такий одночлен запишемо у вигляді $f_{lmp} = x^l y^m z^p$, $l+m+p = \deg F$.

На множині проективних точок кривої X, які зображені в однорідних координатах у вигляді $P(X, Y, 1)$, значення генераторних функцій набувають вигляду $f_{lm} = X_i^l Y_i^m$, $i = \overline{0, n-1}$, $l+m \le \deg F$. Перевірочна матриця H запишеться у вигляді

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ X_0 & X_1 & \ldots & X_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ Y_0^{\deg F} & Y_1^{\deg F} & \ldots & Y_{n-1}^{\deg F} \end{pmatrix}.$$

Елементи синдромної послідовності як елементи вектора $\|S_{lm}\|_r$, обчислимо за правилом $S_{lm} = \sum_{i=0}^{n-1} c_i^* X_i^l Y_i^m = \sum_{i=0}^{n-1} e_i X_i^l Y_i^m$, $l+m \le \deg F$, чи в матричній формі

$$\|S_{lm}\|_r = H\,\|c_n^*\|_n^T = \|X_i^l Y_i^m\|_{n,r}\,\|e_i\|_n^T. \qquad (6)$$

Таким чином, завдання декодування АГК, побудованого через відображення проективних точок *P (X, Y, 1)* кривої однорідними одночленами степеня deg F еквівалентне завданню вирішення системи з $r = d + g - 1$ нелінійних рівнянь від $3t$ змінних.

Для вирішення цього завдання скористаємося штучним прийомом, що полягає у введенні у розгляд многочлена локаторів помилок (МЛП), рішення якого однозначно локалізують (вказують місце розташування) помилок, що виникають.

Визначимо МЛП АГК як многочлен від двох змінних, степеня ≤ (t – 1):

$$a_{00} + a_{10}x + \ldots + y^{t-1} = 0, \qquad (7)$$

де t – число помилок, що може виправити АГК.

Помноживши обидві частини многочлена (7) на e_i і просумувавши за всіма $i = \overline{0, n-1}$, значеннями в точці $(x = X_i, y = Y_i)$, одержимо рекурентний вираз $a_{ij}S_{ij} + a_{i+1,j}S_{i+1,j} + \ldots + S_{i,j+t-1} = 0$, який задає систему лінійних рівнянь щодо невідомих коефіцієнтів МЛП. У матричному вигляді [9] система лінійних рівнянь запишеться у вигляді

$$\begin{pmatrix} S_{00} & S_{10} & \ldots & S_{1\,t-2} \\ S_{10} & S_{20} & \ldots & S_{2\,t-2} \\ \ldots & \ldots & \ldots & \ldots \\ S_{1\,t-2} & S_{0\,t-2} & \ldots & S_{2\,2t-4} \end{pmatrix} \cdot \begin{pmatrix} a_{00} \\ a_{10} \\ \ldots \\ a_{1\,t-2} \end{pmatrix} = \begin{pmatrix} -S_{0\,t-1} \\ -S_{1\,t-1} \\ \ldots \\ -S_{1\,2t-3} \end{pmatrix} \qquad (8)$$

Після знаходження коефіцієнтів МЛП процедура локалізації помилок полягає у підстановці всіх можливих локаторів і виборі тих, які перетворюють у нуль МЛП. Після знаходження локаторів помилок, що вказують на розташування виниклої помилки, процедура знаходження кратності помилки (значення всіх $e_i \ne 0$) полягає у підстановці локаторів у систему (8), що вироджується в систему $\le r$ лінійних рівнянь відносно $\le t$ невідомих. Алгоритм декодування АГК задамо у вигляді послідовності наступних кроків.

Крок 1. За виразом (5) обчислимо елементи синдромної послідовності.

Крок 2. Вирішимо систему лінійних рівнянь (8). Одержимо значення коефіцієнтів МЛП.

Крок 3. Скористаємось процедурою Ченя [2]. Підставимо усі пари (X, Y), що відповідають проективним точкам кривої, у МЛП. Ті пари, які при підстановці обертають його в нуль – локалізують помилки, тобто вказують на їхнє шукане розташування.

Крок 4. Підставимо отримані локатори помилок у систему рівнянь (8). Розв'язання системи лінійних рівнянь дасть значення (кратність) помилок, що виникли. Локалізація помилок і знайдені їхні значення дозволяють сформувати вектор помилок $e = (e_0, e_1, ..., e_{n-1})$.

Крок 5. Виправимо помилки: $c = c^* - e$.

Вищерозглянутий алгоритм декодування АГК може бути ефективно використаний при реалізації процедури декодування на зовнішній ступені каскадного коду.

Приклад завадостійкого кодування каскадними кодами з АГК на зовнішній ступені.

Зафіксуємо алгебраїчне рівняння

$$x^3 + z^3 + x^2 y + xy^2 + xyz = 0 \qquad (9)$$

над полем GF(2^3).

Після підстановки елементів поля GF(2^3) до рівняння (9) отримаємо їх рішення (табл.1).

Таблиця 1.

Точки кривої $x^3 + z^3 + x^2 y + xy^2 + xyz = 0$ в P^2 над GF(2^3)

	X	Y	Z		X	Y	Z
P_0	α^0	0	α^0	P_7	α^3	α^3	α^0
P_1	α^3	α^0	α^0	P_8	α^2	α^4	α^0
P_2	α^5	α^0	α^0	P_9	α^1	α^5	α^0
P_3	α^6	α^0	α^0	P_{10}	α^5	α^5	α^0
P_4	α^4	α^1	α^0	P_{11}	α^4	α^6	α^0
P_5	α^1	α^2	α^0	P_{12}	α^6	α^6	α^0
P_6	α^2	α^3	α^0				

Примітка: тут і далі α^i – примітивний елемент поля GF(2^3).

На множині точок $\{P_0, P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}\}$ побудуємо АГК зовнішньої ступені каскадного коду.

Зафіксуємо множину генераторних функцій у вигляді многочленів степеня $deg = l : \{x, y, z\}$. Обчислимо значення генераторних функцій у точках кривої і сформуємо перевірочну матрицю АГК:

$$\begin{Vmatrix} \alpha^0 & \alpha^3 & \alpha^5 & \alpha^6 & \alpha^4 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^2 & \alpha^1 & \alpha^5 & \alpha^4 & \alpha^6 \\ 0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^6 \\ \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 & \alpha^0 \end{Vmatrix}, \qquad (10)$$

який задає (13, 10, 3) код, що виправляє одну помилку.

Породжувальна матриця АГК буде мати наступний вигляд

$$\begin{Vmatrix} \alpha^0 & & & & & & & & & \alpha^5 & \alpha^4 & 0 \\ & \alpha^0 & & & & & & & & \alpha^1 & \alpha^5 & \alpha^2 \\ & & \alpha^0 & & & & 0 & & & \alpha^1 & \alpha^1 & \alpha^0 \\ & & & \alpha^0 & & & & & & \alpha^1 & \alpha^6 & \alpha^4 \\ & & & & \alpha^0 & & & & & \alpha^4 & \alpha^6 & \alpha^1 \\ & & & & & \alpha^0 & & & & \alpha^6 & \alpha^1 & \alpha^4 \\ & & & & & & \alpha^0 & & & \alpha^3 & \alpha^2 & \alpha^4 \\ & & 0 & & & & & \alpha^0 & & \alpha^3 & 0 & \alpha^1 \\ & & & & & & & & \alpha^0 & \alpha^2 & \alpha^5 & \alpha^1 \\ & & & & & & & & & \alpha^0 & \alpha^0 & \alpha^3 & \alpha^3 \end{Vmatrix} \qquad (11)$$

В якості коду внутрішньої ступені використаємо породжувальну матрицю коду БЧХ із параметрами (7, 3, 4) над полем GF(2^3)

$$\begin{Vmatrix} 1 & 1 & 1 & 0 & 1 & & 0 \\ 1 & 0 & 1 & 1 & & 1 & \\ 1 & 1 & 0 & 1 & 0 & & 1 \end{Vmatrix} \qquad (12)$$

і перевірочну матрицю коду

$$\begin{Vmatrix} 1 & & & 0 & 1 & 1 & 1 \\ & 1 & & & 1 & 0 & 1 \\ & & 1 & & 1 & 1 & 0 \\ 0 & & & 1 & 0 & 1 & 1 \end{Vmatrix}. \qquad (13)$$

Нехай інформаційний вектор дорівнює $i = \|\alpha^3 \;\; 0 \;\; 0 \;\; \alpha^0 \;\; 0 \;\; \alpha^4 \;\; 0 \;\; \alpha^2 \;\; 0 \;\; \alpha^1\|$, тоді на першому етапі для формування кодового слова зовнішньої ступені каскадного коду $(c_0, c_1, ..., c_{12})$ достатньо помножити інформаційний вектор на породжувальну матрицю АГК (11). В результаті отримаємо кодове слово

$$c = \|\alpha^3 \;\; 0 \;\; 0 \;\; \alpha^0 \;\; 0 \;\; \alpha^4 \;\; 0 \;\; \alpha^2 \;\; 0 \;\; \alpha^1 \;\; \alpha^4 \;\; \alpha^6 \;\; \alpha^0\|, \qquad (14)$$

яке можно представити у вигляді наступної таблиці

1	0	0	1	0	0	0	0	0	0	0	1	1
1	0	0	0	0	1	0	0	0	1	1	0	0
0	0	0	0	0	1	0	1	0	0	1	1	0

На другому етапі для формування перевірочних розрядів скористаємось перевірочною матрицею коду БЧХ (13), для цього помножимо кодове слово зовнішнього коду (14) на перевірочну матрицю коду БЧХ (13) внутрішньої ступені каскадного коду, отримаємо:

1	0	0	1	0	0	0	0	0	0	0	1	1
1	0	0	0	0	1	0	0	0	1	1	0	0
0	0	0	0	0	1	0	1	0	0	1	1	0
0	0	0	1	0	1	0	0	0	1	1	1	1
1	0	0	0	0	0	0	1	0	1	0	1	0
1	0	0	1	0	1	0	1	0	0	1	0	1
0	0	0	1	0	0	0	1	0	1	0	0	1

В такому вигляді кодове слово потрапляє до каналу (рис.1).

Приклад завадостійкого декодування каскадних кодів з АГК на зовнішній ступені. Штучно внесемо помилку в кодове слово. Вектор помилок позначимо як $e = \|e_0,\ e_1,\ ...,\ e_{12}\|$. Прийняте слово c^* запишеться як

$$c^* = c + e = \|c_0 + e_0,\ \ c_1 + e_1,\ \ ...,\ \ c_{12} + e_{12}\|, \quad (15)$$

чи у вигляді таблиці:

1	1	0	1	0	0	0	0	0	0	0	0	1
1	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	1	0	1	0	0	1	1	0
0	0	1	0	0	1	0	0	0	1	1	1	0
0	0	0	0	0	0	0	0	1	1	0	1	0
1	0	0	1	0	1	0	1	0	1	1	0	1
0	0	0	1	0	0	1	1	0	1	0	0	1

Примітка: помилки, що внесені в кодове слово, позначені темним кольором.

На першому етапі помножимо слово c^* на транспоновану перевірочну матрицю БЧХ коду (13). Це дасть можливість виправити всі одиночні помилки в кодовому слові:

1	0	0	1	0	0	0	0	0	0	0	1	1
1	1	0	0	0	1	0	0	0	1	1	0	0
0	1	0	0	0	1	0	1	0	0	1	1	0
0	0	0	1	0	1	0	0	0	1	1	1	1
1	0	0	0	0	0	0	1	0	1	0	1	0
1	0	0	1	0	1	0	1	0	0	1	0	1
0	0	0	1	0	0	0	1	0	1	0	0	1

На другому етапі кодове слово (з помилкою у другому розряді) помножимо на транспоновану перевірочну матрицю АГК зовнішньої ступені каскадного коду (11) та отримаємо синдромний вектор, який дорівнює

$$S = \begin{Vmatrix} S_{10} \\ S_{01} \\ S_{00} \end{Vmatrix} = \begin{Vmatrix} \alpha^2 \\ \alpha^6 \\ \alpha^6 \end{Vmatrix}. \quad (16)$$

Кількість помилок, які може виправити код, $t = 1$, многочлен локаторов помилок АГК (7) набуде вигляду

$$a_{00} + a_{10}x + y = 0 \quad (17)$$

і відповідно рекурентний вираз, який задає систему лінійних рівнянь щодо невідомих коефіцієнтів многочлена локаторів помилок запишеться як

$$S_{10} + S_{01} + aS_{00} = 0. \quad (18)$$

Підставляючи значення синдромного вектору (16) до (18) та розв'язавши його, отримаємо коефіцієнт многочлена локаторов помилок: $a = \alpha^l$.

Шуканий многочлен локаторів помилок набуде вигляд

$$\Lambda(x, y) = x + y + a = 0$$

Скористаємося процедурою Ченя. Підставимо всі пари (X, Y), які відповідають проективним точкам кривої, у многочлен локаторів помилок (17). Ті пари, які при підстановці обертають його в нуль, локалізують помилки, тобто вказують на їхнє шукане розташування.

0. $\Lambda(\alpha^0, 0) = \alpha^0 + 0 + \alpha^1 \neq 0$
1. $\Lambda(\alpha^3, \alpha^0) = \alpha^3 + \alpha^0 + \alpha^1 = 0 - помилка$
2. $\Lambda(\alpha^5, \alpha^0) = \alpha^5 + \alpha^0 + \alpha^1 \neq 0$
3. $\Lambda(\alpha^6, \alpha^0) = \alpha^6 + \alpha^0 + \alpha^1 \neq 0$
4. $\Lambda(\alpha^4, \alpha^1) = \alpha^4 + \alpha^1 + \alpha^1 \neq 0$
5. $\Lambda(\alpha^1, \alpha^2) = \alpha^1 + \alpha^2 + \alpha^1 \neq 0$
6. $\Lambda(\alpha^2, \alpha^3) = \alpha^2 + \alpha^3 + \alpha^1 \neq 0$
7. $\Lambda(\alpha^3, \alpha^3) = \alpha^3 + \alpha^3 + \alpha^1 \neq 0$
8. $\Lambda(\alpha^2, \alpha^4) = \alpha^2 + \alpha^4 + \alpha^1 = 0 - помилка$
9. $\Lambda(\alpha^1, \alpha^5) = \alpha^1 + \alpha^5 + \alpha^1 \neq 0$
10. $\Lambda(\alpha^5, \alpha^5) = \alpha^5 + \alpha^5 + \alpha^1 \neq 0$
11. $\Lambda(\alpha^4, \alpha^6) = \alpha^5 + \alpha^0 + \alpha^1 \neq 0$
12. $\Lambda(\alpha^6, \alpha^6) = \alpha^5 + \alpha^0 + \alpha^1 \neq 0$

Пари (α^3, α^0), (α^2, α^4) обертають його в нуль, тобто локалізують помилки, вказуючи, що помилки розташовані у символах c_1^*, c_8^*, і відповідають проективним точкам $P(\alpha^3, \alpha^0, \alpha^0)$, $P(\alpha^3, \alpha^0, \alpha^0)$.

Підставивши знайдені локатори помилок у систему рівнянь (8), одержимо

$$e_1\alpha^3 + e_8\alpha^2 = \alpha^2;$$
$$e_1\alpha^0 + e_8\alpha^0 = \alpha^6.$$

Розв'язавши останню систему, одержимо: $e_1 = \alpha^6$, $e_9 = 0$. Вектор помилок відповідно дорівнює $e = \| 0 \quad \alpha^6 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \|$.

Виправимо помилку $c = c^* - e$.

Розглянутий алгоритм декодування каскадних кодів з алгеброгеометричним кодом на зовнішній ступені дозволяє ефективно виправляти помилки у спотворених кодових словах.

Висновок

Таким чином, для підвищення вірогідності даних, що оброблюються та передаються в АСУВ, перспективним напрямком є застосування контролюючих помилки алгеброгеометричних кодів. Для зменшення складності кодування і декодування алгеброгеометричних кодів пропонується використовувати алгеброгеометричні коди на зовнішній ступені каскадного коду як метод практичної реалізації коду з великою довжиною і високою корегуючою здатністю. В статті розглянуті теоретичні питання побудови каскадних кодів з алгеброгеометричними кодами на зовнішній ступені та наведено практичний приклад реалізації процедури кодування і декодування алгеброгеометричними кодами, застосування яких в апаратурі передачі даних АСУВ дозволить суттєво знизити складність і підвищити завадостійкість інформації, що оброблюється і передається. Перспективним напрямком подальших досліджень є визначення кількісних показників часової та ємкісної складності запропонованих процедур кодування і декодування алгеброгеометричними кодами на зовнішній ступені каскадного коду.

Список літератури

1. *Зв'язок військовий. Терміни та визначенн: ДСТУ В 3265 – 95. – К.: УкрНДІССІ, 1995. – 23 с.*
2. *Блейхут Р. Теория и практика кодов, контролирующих ошибки / Блейхут Р. – М.: Мир, 1986. – 576 с.*
3. *Злотник Б. М. Помехоустойчивые коды в системах связи / Злотник Б. М. – М.: Радио и связь, 1989. – 232 с.*
4. *Гоппа В.Д. Коды на алгебраических кривых / В.Д. Гоппа // Докл. АН СССР. – 1981. – Т.259, № 6. – С. 1289-1290.*
5. *Гоппа В.Д. Коды и информация / В.Д. Гоппа // Успехи математических наук. – 1984. – Т.30, № 1(235). – С. 77-120.*
6. *Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів: монографія / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов. – Х.: ХУ ПС, 2005. – 267 с.*
7. *Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования / А.А. Кузнецов // Всеукр. меж вед. науч.-техн. сб. – Харьков: ХТУРЭ. – 2003. – № 134. – С. 218-222.*
8. *Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. – М.: Вильямс, 2003. – 1104 с.*
9. *Гантмахер Ф.Р. Теория матриц / Гантмахер Ф.Р. – М.: Наука, 1988. – 552 с.*

Надійшла до редколегії 2.09.2009 р.

Рецензент: доктор технічних наук, доцент Ю.В. Шабатура , Академія сухопутних військ, Львів.

СИНТЕЗ КАСКАДНЫХ КОДОВ С АЛГЕБРОГЕОМЕТРИЧЕСКИМИ КОДАМИ НА ВНЕШНЕЙ СТУПЕНИ

В.И. Грабчак

В статье исследуются вопросы построения каскадных кодов с алгеброгеометрическими кодами на внешней ступени, применение которых в аппаратуре передачи данных АСУВ позволит существенно снизить сложность процедур кодирования и декодирования, а также повысить помехоустойчивость обрабатываемой и передаваемой информации. Рассматриваются теоретические вопросы построения каскадных кодов с алгеброгеометрическими кодами на внешней ступени, приводится пример практической реализации помехоустойчивого кодирования и декодирования каскадных кодов с алгеброгеометрическими кодами на внешней ступени.

Ключевые слова: *каскадные коды, алгеброгеометрические коды, процедуры кодирования и декодирования.*

SYNTHESIS OF CASCADE CODES WITH ALGEBRA-GEOMETRIC CODES ON EXTERNAL STEP

V.I. Hrabchak

In the article, the problems of construction of cascade codes with algebra-geometric ones on external steps are investigated. Their application in a data communication equipment of automatic system of tasking troops will allow to reduce complication of coding and decoding procedures greatly and promote hindrance immunity of processed and transferred information. The theoretical questions of constructions of cascade codes with algebra-geometric codes on external steps are examined, the example of practical realization of hindrance proof coding and decoding of cascade codes with algebra-geometric codes on external steps is given.

Keywords: *cascade codes, algebra-geometric codes, procedures of coding and decoding.*