МЕТОДИ І АЛГОРИТМИ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 621.391

В. Грабчак, З. Грабчак*
Академія Сухопутних військ,
Харківський університет Повітряних сил

ДЕКОДУВАННЯ КОДОГРАМ В УЗАГАЛЬНЕНИХ КАСКАДНИХ КОДАХ З АЛГЕБРОГЕОМЕТРИЧНИМИ КОДАМИ НА ЗОВНІШНЬОМУ СТУПЕНІ

Розглянуто процедури декодування кодограм в узагальнених каскадних кодах з використанням алгеброгеометричних кодів на зовнішньому ступені. Сформульована і доведена теорема, яка дає змогу оцінити часову й ємкісну складності алгоритмів декодування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішньому ступені та оцінити їхню асимптотичну складність. Виконано порівняльний аналіз складності реалізації алгоритмів декодування кодограм в узагальнених каскадних кодах та еквівалентного двійкового лінійного блокового коду.

Ключові слова: узагальнені каскадні коди, алгеброгеометричні коди, алгоритми декодування, часова та ємкісна складність декодування.

In the article, procedures of decoding of codegrams in the generalized codes of cascades with the use of algebraic-geometrical codes on external stage are considered. The result of the investigation is the theorem which allows to estimate temporal and capacitive complications of algorithms of codegrams decoding in the generalized cascade codes with algebraic-geometrical codes on the external stage and to estimate their asymptotical complication. The article demonstrates the comparative analysis of complication of realization of algorithms of codegrams decoding in the generalized cascade codes on the one hand and, of equivalent dual linear block code on the other hand.

Keywords: generalized cascade codes, algebraic-geometrical codes, algorithms of decoding, temporal and capacitive complications of decoding.

Вступ

Постановка проблеми в загальному вигляді та аналіз літератури. У зв'язку із підвищенням вимог до ефективності процесів управління, постійним зростанням об'єму і швидкості інформації, що передається (дискретних повідомлень), значно зросли вимоги і до вірогідності інформації, що передається (ймовірність помилки не вище ніж $10^{-6} \div 10^{-9}$). Розроблення та реалізація у вітчизняному виробництві методів і технічних засобів підвищення вірогідності інформації, яке передається, є одним з першочергових напрямків Концепції розвитку зв'язку в Україні. Сферою реалізації методів і технічних засобів підвищення вірогідності інформації, що передається, є телекомунікаційні підсистеми Державної інтегрованої інформаційної системи, підсистеми зв'язку воєнного й урядового призначення, телекомунікаційні системи спеціального призначення.

Одним із найефективніших методів підвищення вірогідності інформації, що передається, є завадостійке кодування [1, 2]. За підвищених вимог до вірогідності та низького енергетичного відношення сигнал/завада, наприклад, у системах мобільного і супутникового зв'язку, доцільне застосування каскадних кодів для зменшення складності реалізації декодерів [2, 3]. Відмінною особливістю каскадних схем кодування є кодування (декодування) інформації декількома складовими кодерами (декодерами).

Найпоширенішою схемою побудови каскадних кодів є схема з двома рівнями кодування. Як зовнішній код, як правило, використовують коди Ріда–Соломона. Ці коди найпоширеніші, оскільки є кодами з максимально досяжною відстанню ($d = n - k + 1$) і порівняно просто реалізуються. Внутрішнім кодом можна вибрати один з багатьох різних кодів [2, 3].

Загальним класом каскадних кодів, які мають більше від двох рівнів кодування, є узагальнені каскадні коди. Алгебраїчної теорії побудови узагальнених каскадних кодів, дослідження складності їх реалізації стосується монографія [4]. Узагальнені каскадні коди є однією з найзагальніших схем каскадного кодування і є, в теоретичному плані, узагальненням більшості відомих каскадних кодових конструкцій (ітегровані коди, каскадні коди і коди для локалізації помилок). Найбільший ефект каскадне кодування дає змогу одержати при використанні на зовнішньому ступені алгеброгеометричних кодів [7].

Перспективним напрямом у розвитку завадостійкого кодування є розроблення лінійних блокових кодів за алгебраїчними кривими (алгеброгеометричні коди) [5, 6]. У роботі [8] показано, що теорія їх побудови узагальнює більшість відомих алгебраїчних кодів, таких, наприклад, як великий клас циклічних кодів, зокрема кодів Боуза – Чоудхурі – Хоквінгема, кодів Ріда – Соломона і їхніх узагальнень, альтернантних, кодів, зокрема кодів Гоппи, Сривестави та інших. Основна перевага методів алгеброгеометричного кодування полягає у побудові довгих недвійкових блокових кодів, які мають добрі асимптотичні властивості. У роботі [9] показано, що використання алгеброгеометричних кодів для передавання даних через дискретні канали зв'язку дає змогу отримати істотний 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 узагальнені каскадні коди як метод практичної реалізації коду з великою довжиною і високою корегувальною здатністю.

Мета статті

Метою статті є оцінка часової і ємкісної складності алгоритмів декодування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішньому ступені та оцінка їх асимптотичної складності; порівняльний аналіз складності реалізації алгоритмів декодування кодограм в узагальнених каскадних кодах та еквівалентного двійкового лінійного блокового коду.

Основна частина

Алгеброгеометричні коди. Розглянемо загальну схему побудови алгеброгеометричних кодів [8]. Зафіксуємо скінченне поле $GF(q)$. Нехай X – гладка проективна алгебраїчна крива у проективному просторі P^n над $GF(q)$, $g = g(X)$ – рід кривої, $X(GF(q))$ – множина її точок над скінченним полем, $N = |X(GF(q))|$ – їхня кількість. Кількість N точок кривої X над $GF(q)$ обмежено зверху виразом Хассе - Вейля $N \le 2\sqrt{q} \cdot g + q + 1$ [8, 9].

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 алгеброгеометричний код довжини $n \le N$.

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

Декодування алгеброгеометричними кодами. Уявимо, що під час передавання по каналу з помилками кодове слово алгеброгеометричного коду спотворилося, вектор помилок позначимо як $e = (e_0, e_1, ..., e_{n-1})$. Прийняте слово c^* після передавання 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 $S=(S_0, S_2, ..., S_{r-1})$, обчислений за таким правилом

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

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 алгеброгеометричного коду полягає у знаходженні вектора помилок $e=(e_0, e_1, ..., e_{n-1})$ за відомою синдромною послідовністю $S=(S_0, S_1, ..., S_{r-1})$.

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 $f_{lm} = X_i^l Y_i^m$, $i=\overline{0, n-1}$, $l+m \le \deg F$. Перевірна матриця H запишеться у вигляді

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

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

$$\|S_{lm}\|_r = H\left\|c_n^*\right\|_n^T = \left\|X_i^l Y_i^m\right\|_{n,r} \|e_i\|_n^T. \tag{2}$$

Отже, завдання декодування алгеброгеометричного коду, побудованого через відображення проективних точок $P(X,Y,1)$ кривої однорідними одночленами степеня $\deg F$, еквівалентне завданню розв'язання системи з $r=d+g-1$ нелінійних рівнянь від $3t$ змінних.

Для вирішення цього завдання скористаємося штучним прийомом, що полягає у введенні у розгляд багаточлена локаторів помилок (МЛП), розв'язки якого однозначно локалізують (указують місце розташування) помилок, що виникають.

Визначимо МЛП алгеброгеометричного коду як багатолен від двох змінних, степеня $\le (t-1)$:

$$a_{00} + a_{10} x + ... + y^{t-1} = 0, \tag{3}$$

де t – кількість помилок, які може виправити алгеброгеометричний код.

Помноживши обидві частини багаточлена (3) на e_i і підсумувавши за всіма $i=\overline{0, n-1}$ значеннями в точці $(x=X_i, y=Y_i)$, одержимо рекурентний вираз $a_{ij}S_{ij} + a_{i+1,j}S_{i+1,j} + ... + S_{i,j+t-1} = 0$, який задає систему лінійних рівнянь щодо невідомих коефіцієнтів МЛП. У матричному вигляді система лінійних рівнянь запишеться у вигляді

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

Після знаходження коефіцієнтів МЛП процедура локалізації помилок полягає у підстановці всіх можливих локаторів і виборі тих, які перетворюють на нуль МЛП. Після знаходження локаторів помилок, що вказують на розташування виниклої помилки, процедура знаходження кратності помилки (значення всіх $e_i \neq 0$) полягає у підстановці локаторів у систему (4), що вироджується в систему $\le r$ лінійних рівнянь відносно $\le t$ невідомих. Алгоритм декодування алгеброгеометричного коду задамо у вигляді послідовності таких кроків.

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

Крок 2. Розв'яжемо систему лінійних рівнянь (4). Одержимо значення коефіцієнтів МЛП.

Крок 3. Скористаємось процедурою Ченя [1]. Підставимо всі пари (X, Y), що відповідають проективним точкам кривої, у МЛП. Ті пари, які при підстановці перетворюють його на нуль, локалізують помилки, тобто вказують на їхнє шукане розташування.

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

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

Вищерозглянутий алгоритм декодування алгеброгеометричного коду може бути ефективно використаний при реалізації процедури декодування на зовнішньому ступені узагальненого каскадного коду.

Узагальнені каскадні коди. Для оцінки складності алгоритму декодування кодограм в узагальнених каскадних кодах скористаємося їхнім алгебраїчним описом [4]. За визначенням алгебраїчно заданий узагальнений каскадний код порядку m однозначно визначається n_2 квадратними двійковими матрицями H_0^j, $j = \overline{1, n_2}$ порядку n_1 (які задають (n_1, k_i, d_{1i}) коди внутрішнього ступеня) та $m+1$ груповими над $GF(2^{a_i})$, $i = \overline{1, m+1}$ кодами зовнішнього ступеня з параметрами (n_2, b_i, d_{2i}). Вихідними даними для опису узагальненого каскадного коду є:

- двійкове слово c довжини $n = n_1 n_2$, яке подається у вигляді послідовності двійкових векторів C_j, $j = \overline{1, n_2}$, довжини n_1, тобто
$$c = (c_1, c_2, ..., c_{n_1}, c_{n_1+1}, ..., c_{2n_1}, c_{2n_1+1}, ..., c_{n_2 n_1}) = ((c_1, c_2, ..., c_{n_1}), (c_{n_1+1}, ..., c_{2n_1}), \\ ..., (c_{2n_1+1}, ..., c_{n_2 n_1})) = (C_1, C_2, ..., C_{n_2}), C_j = (c_{(j-1)n_1+1}, ..., c_{jn_1});$$
- n_2 квадратних двійкових матриць H_0^j, $j = \overline{1, n_2}$, порядку n_1;
- $m+1$ групових над $GF(2^{a_i})$, $i = \overline{1, m+1}$, кодів (кодів другого ступеня) з параметрами (n_2, b_i, d_{2i}). При цьому виконується рівність $\sum_{i=1}^{m+1} a_i = n_1$.

В основному варіанті побудови узагальнених каскадних кодів як матриця H_0^j для всіх $j = \overline{1, n_2}$ вибирається одна й та сама трикутна матриця H_0 порядку n_1, яка в клітковій формі має вигляд

$$H_0 = \left\| \begin{matrix} I_{a_1} & & & & & \\ P_{11} & I_{a_2} & & & 0 & \\ P_{21} & P_{22} & I_{a_3} & & & \\ \dots & \dots & \dots & \dots & \dots & \dots \\ P_{m1} & P_{m2} & P_{m3} & \dots & P_{mm} & I_{a_{m+1}} \end{matrix} \right\| = \left\| \begin{matrix} \tilde{H}_0 \\ \tilde{H}_1 \\ \tilde{H}_2 \\ \dots \\ \tilde{H}_m \end{matrix} \right\| \qquad (5)$$

де $\tilde{H}_i = \left\| P_{i_1} \quad P_{i_2} \quad ... \quad P_{i_i} \quad I_{a_1} \quad 0 \quad ... \quad 0 \right\|$, $i = \overline{1,m}$, клітинки P_{i_s} – двійкові матриці розміру $a_{i+1} \times a_s$, I_{a_s} – одинична матриця порядку a_s.

Перевірна матриця H_i, вигляду

$$H_i = \begin{Vmatrix} \tilde{H}_i \\ \tilde{H}_{i+1} \\ ... \\ \tilde{H}_m \end{Vmatrix} = \begin{Vmatrix} P_{i_1} & P_{i_2} & ... & P_{i_i} & I_{a_{i+1}} & & 0 & \\ P_{i+1_1} & P_{i+1_2} & ... & P_{i+1_i} & P_{i+1_{i+1}} & I_{a_{i+2}} & & \\ ... & ... & ... & ... & ... & ... & ... & ... \\ P_{m_1} & P_{m_2} & ... & P_{m_i} & P_{m_{i+1}} & ... & P_{m_m} & I_{a_{m+1}} \end{Vmatrix}, \quad i = \overline{1,m}$$

повністю визначається матрицею H_0 (складається з $m-i+1$ кліткових рядків матриці H_0), задає i-й код внутрішнього ступеня з параметрами (n_1, k_i, d_{1i}). Для кількості інформаційних символів i-го коду виконується співвідношення $k_i = a_1 + a_2 + ... + a_i$.

Зафіксуємо лінійне відображення векторів C_j

$$C_j H_0^T = \left(\gamma_{1j}, \gamma_{2j}, ..., \gamma_{m+1j}\right), \quad j = \overline{1,n_2}, \tag{6}$$

де γ_{ij} – двійковий вектор довжини a_i.

Трактуючи вектори γ_{ij} як елементи поля $GF(2^{a_i})$, складемо з цих елементів, отриманих в результаті відображення (6) (для кожного слова c), вектори $\gamma_i = \left(\gamma_{i1}, \gamma_{i2}, ..., \gamma_{in_2}\right)$, $i = \overline{1,m+1}$. За визначенням [4] двійкове слово c довжини $n = n_1 n_2$ є кодовим словом узагальненого каскадного коду порядку m тоді і тільки тоді, коли всі пов'язані зі словом вектори γ_i, $i = \overline{1,m+1}$ являють собою кодові слова відповідних (i - x) кодів зовнішнього ступеня. У багатьох випадках зручна геометрична трактовка узагальненого каскадного коду показана на рис. 1.

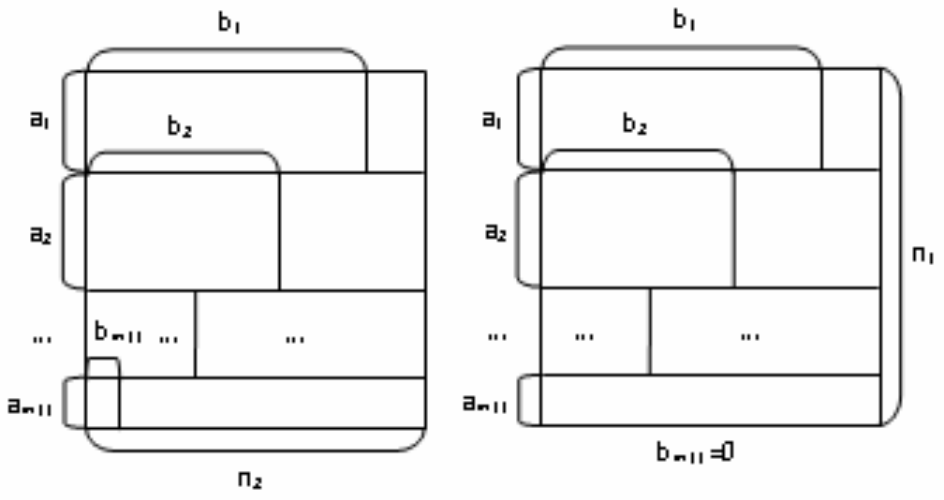

Рис. 1. Геометрична трактовка узагальненого каскадного коду

Величини $a_i > 0$ и $b_i \geq 0$, які визначають внутрішню структуру узагальненого каскадного (n,k,d) коду, вибирають довільно, при цьому (n,k,d) параметри задовольняють такі співвідношення:

$$n = n_1 n_2;\ k = \sum_{i=1}^{m+1} a_i b_i;\ d \geq \begin{cases} \min\left\{ d_{1i} d_{2i} : i = \overline{1,m} \right\} \text{при } b_{m+1} = 0, \\ \min\left\{ d_{2m+1}, d_{1i} d_{2i} : i = \overline{1,m} \right\} \text{при } b_{m+1} \neq 0. \end{cases}$$

Дослідження складності реалізації алгоритмів декодування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішньому ступені. Відповідно до основних положень теорії складності час, який витрачається, як функція розміру задачі, називається часовою

складністю цього алгоритму [3]. Поведінку цієї складності в разі збільшення розміру задачі називають асимптотичною часовою складністю алгоритму. Аналогічно визначається ємкісна та асимптотична ємкісна складність алгоритму.

Виконаємо оцінку часової та ємкісної складності алгоритмів декодування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішньому ступені та виконаємо дослідження їхньої асимптотичної часової та асимптотичної ємкісної складності.

Для оцінки часової та ємкісної складності алгоритмів декодування кодового слова узагальненого каскадного коду сформулюємо і доведемо теорему.

Теорема. Нехай заданий узагальнений каскадний код порядку m з m+1 алгеброгеометричними (n_2, b_j, d_{2j}) кодами на зовнішньому ступені над $GF(2^{a_j})$, $j=\overline{1,m+1}$.

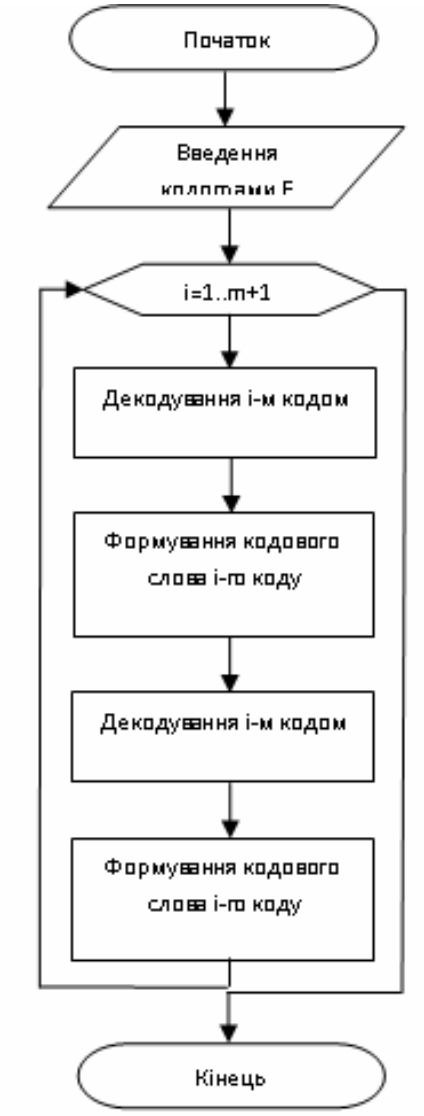

Рис. 2. Схема алгоритму декодування кодового слова узагальненого каскадного коду

Тоді часова складність алгоритмів задається виразом

$$S_Ч = \frac{n\cdot(m+1)}{16} + \frac{n\cdot\sqrt{n}}{16},$$

ємкісна складність алгоритмів

$$S_E = \frac{n\cdot(m+1)}{16} + \frac{n\cdot\sqrt{n}}{16}$$

і, відповідно, асимптотична часова складність

$$S_Ч^* = n\cdot\left(\sqrt{n}+m\right),$$

асимптотична ємкісна складність

$$S_E^* = n\cdot\left(\sqrt{n}+m\right).$$

Доведення. Аналіз схеми алгоритму декодування кодового слова узагальненого каскадного коду (рис. 2) показує, що складність декодування кодового слова узагальненого каскадного коду як функція розміру задачі визначається сумою складностей реалізації алгоритмів декодування кодами зовнішнього і внутрішнього ступенів узагальненого каскадного коду.

Складність декодування циклічних кодів, які виправляють t помилок, визначається складністю розв'язання системи з t лінійних рівнянь і становить близько t^2 операцій додавання і множення елементів у кінцевому полі [1, 3]. З урахуванням складності реалізації операцій над елементами з $GF(2^{a_i})$ часова складність декодування кодового слова узагальненого каскадного коду дорівнює

$$\sum_{i=1}^{m+1}(t_{1i}{}^2 + a_i\cdot t_{2i}^2) \qquad (7)$$

часових інтервалів, де t_{1i} і t_{2i} – виправна здатність кодів внутрішнього і зовнішнього ступенів, відповідно. Ємкісна складність становитиме

$$\sum_{i=1}^{m+1}(t_{1i}{}^2 + a_i\cdot t_{2i}{}^2) \qquad (8)$$

двійкових чарунок пам'яті.

Виконаємо оцінку асимптотичної часової і ємкісної складності декодування кодограм. Для цього спростимо отриманий вираз.

Припустимо, що

$$\forall a_i = \frac{n_1}{m+1},\ \forall t_{1i} = \frac{n_1}{4},\ \forall t_{2i} = \frac{n_2}{4},\ n_2 = n_1 = \sqrt{n}\,. \qquad (9)$$

Тоді після підстановки (9) в (7) і (8) одержимо:

$$S_Ч = \frac{n \cdot (m+1)}{16} + \frac{n \cdot \sqrt{n}}{16},$$

$$S_E = \frac{n \cdot (m+1)}{16} + \frac{n \cdot \sqrt{n}}{16}.$$

На межі в разі збільшення розміру задачі асимптотична складність алгоритму декодування кодограм в узагальнених каскадних кодах дорівнюватиме

$$S_Ч^* = n \cdot \left(\sqrt{n} + m\right), \tag{10}$$

$$S_E^* = n \cdot \left(\sqrt{n} + m\right). \tag{11}$$

Теорема доведена.

Виконаємо порівняльний аналіз часової і ємкісної складності реалізації алгоритмів декодування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішньому ступені та еквівалентного двійкового лінійного блокового коду.

Для реалізації алгоритму декодування кодограм з використанням еквівалентного двійкового лінійного блокового (n, k, d) коду часова складність декодування кодового слова становитиме t^2 операцій додавання і множення двійкових елементів. Ємкісна складність становитиме t^2 двійкових розрядів пам'яті.

За відповідних припущень ($k = \frac{n}{2}$, $t = \frac{n}{4}$) для цього необхідно виконати

$$S_{Ч_E} = \frac{n^2}{16}$$

операцій додавання і добутку, та зберігати

$$S_{E_E} = \frac{n^2}{16}$$

двійкових розрядів пам'яті.

Асимптотична часова та ємкісна складності алгоритму декодування кодограм еквівалентним двійковим лінійним блоковим (n, k, d) кодом запишеться у вигляді

$$S_{Ч_E}^* = n^2, \tag{12}$$

$$S_{E_E}^* = n^2. \tag{13}$$

Аналіз виразів (10)–(13) показує, що часова та ємкісна асимптотична складність алгоритмів декодування кодограми в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішньому ступені визначається загальними сумарними часовими затратами та затратами елементів пам'яті на декодування кодових слів внутрішнього і зовнішнього ступенів узагальненого каскадного коду. Асимптотична часова та ємкісна складності алгоритмів декодування кодограм істотно нижчі (приблизно в $\sqrt{n}$ разів) порівняно із декодуванням кодограм, побудованих на еквівалентному двійковому лінійному блоковому (n, k, d) коді.

На рис. 3 наведено залежності асимптотичної складності реалізації алгоритмів декодування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішньому ступені. Аналіз залежностей показує, що для кодограм довжиною у сотні символів виграш у складності реалізації алгоритмів декодування становить один-два порядки. У разі зміни порядку узагальненого каскадного коду m складність реалізації алгоритмів декодування мало змінюється, що практично істотно не впливає на кінцевий вибір параметрів узагальненого каскадного коду.

Виконані дослідження декодування кодограм з використанням алгеброгеометричних кодів на зовнішньому каскаді узагальненого каскадного коду показали, що складність реалізації алгоритмів зростає поліноміально від параметрів кодів, що використовуються.

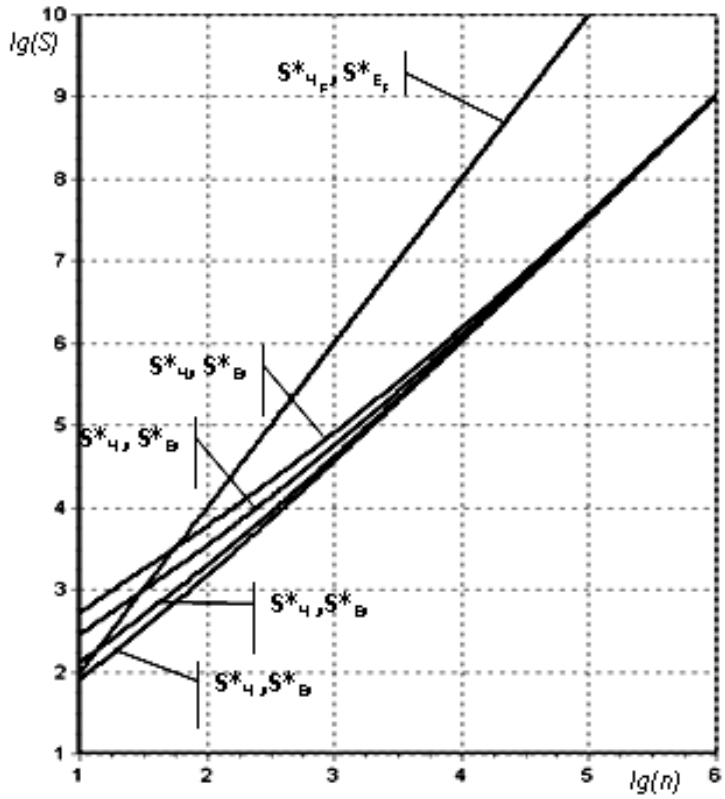

Рис. 3. Залежності асимптотичної складності реалізації алгоритмів декодування кодограм узагальненого каскадного коду

Висновки

Дослідження часової і ємкісної складності алгоритмів показало, що їх реалізація для довжини у сотні символів значно (на один–два порядки) простіша порівняно із традиційними кодовими конструкціями. Показано, що зростання цих складностей у межах збільшення розміру задачі (асимптотична складність) істотно нижча, ніж у випадку використання традиційних кодових схем обробки інформації. В разі зміни порядку узагальненого каскадного коду m складність реалізації алгоритмів декодування мало змінюється, що практично не впливає на кінцевий вибір параметрів узагальненого каскадного коду.

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Пер. с англ.; Р. Блейхут. – М.: Мир, 1986. – 576 с. 2. Злотник Б. М. Помехоустойчивые коды в системах связи / Б. М. Злотник. – М.: Радио и связь, 1989. – 232 с. 3. Бернард Скляр. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с. 4. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. – М.: Связь, 1976. – 240 с. 5. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР / В.Д. Гоппа. – 1981. – Т. 259, № 6. – С. 1289–1290. 6. Гоппа В.Д. Коды и информация. Успехи математических наук / В.Д. Гоппа. – 1984. – Т. 30, вып. 1(235). – С. 77–120. 7. Грабчак В.І. Синтез каскадних кодів з алгеброгеометричними кодами на зовнішній ступені / В.І. Грабчак // Військово-технічний збірник. – Львів: ЛІСВ. – 2009. – Вип. 2. – С. 3–8. 8. Науменко М.І. Теоретичні основи та методи побудови алгебраїчних блокових кодів. Монографія / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов. – Харків: ХУ ПС, 2005. – 267 с. 9. Кузнецов А.А. Энергетический выигрыш алгеброгеометрического кодирования // Всеукр. межвед. науч.-техн. сб. / А.А. Кузнецов. – Харьков: ХТУРЭ. – 2003. – Вып. 134. – С. 218–222.