ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТА ОБЧИСЛЮВАЛЬНІ СИСТЕМИ І КОМПЛЕКСИ В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 621.391

В.І. СЛОБОДЗЯН, А.М. СЛІВІНСЬКИЙ
Хмельницький національний університет

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ЗАВАДОСТІЙКОГО КОДУВАННЯ НА ОСНОВІ ЦИКЛІЧНИХ КОДІВ

Проаналізовано проблеми й особливості завадостійкого кодування інформації. Розглянуто методи опису і принципи побудови циклічних кодів. Розроблено систему кодування/декодування інформації з використанням циклічних кодів. Отримано графічну залежність ймовірності невиявленої помилки на вході приймача інформації від ймовірності помилки в каналі зв'язку.

Problems and features of error correcting coding of information are analysed. The methods of description and principles of construction of cyclic kodes are considered. The system of coding/decoding of information is developed with the use of cyclic kodes. Graphic dependence of probability of unfound out an error is got on the entrance of receiver of information from probability of error in the channel of connection.

Ключові слова: циклічний код, породжуючий поліном, синдром

Вступ

Історія кодування, що контролює помилки, почалася в 1948 році публікацією знаменитої статті Клода Шенона «Математична теорія зв'язку». Шенон сформулював теорему для дискретного каналу з шумом: при будь-якій швидкості передачі двійкових символів, меншій, ніж пропускна здатність каналу, існує такий код, при якому ймовірність помилкового декодування буде як завгодно мала. Проте Шенон не вказав, як знайти потрібні коди, а лише довів їх існування. Це стало стимулом до розробки завадостійких кодів.

Під завадостійкими кодами розуміють коди, що дозволяють знаходити і виправляти помилки, що виникають в результаті впливу завад. Завадостійкість кодування забезпечується за рахунок введення надлишковості в кодові комбінації. Теоретичною базою ефективного використання надлишковості, що вводиться, є теорія завадостійкого кодування, яка для кожного конкретного каналу дозволяє вибрати найбільш ефективний метод виявлення і виправлення помилок.

В світовій літературі нараховується більше десятка монографій, присвячених теорії завадостійкого кодування. Першою і методично найбільш досконалою цього напряму є монографія У. Пітерсона «Коды, исправляющие ошибки», видана в 1961 році і перекладена російською мовою в 1964 році.

Питаннями розвитку теорії завадостійкого кодування займались такі зарубіжні спеціалісти як Р. Галлагер, У. Пітерсон, Е. Уелдон, А.Д. Вітербі, Д.К. Омура, Р.К. Боуз, Д.К. Рой-Чоудхурі, Е.Р. Берлекемп, Д. Мессі, І.С. Рід, Г. Соломон, Р. Блейхут, Д. Форні, К. Беруа, Д. Хагенауер, а також російські вчені Е.Л. Блох, В.Д. Колесник, Е.Т. Мірончиков, К.Ш. Зігангіров, Е.М. Габідулін, В.В. Зяблов, А.Г. Зюко, С.Л. Портной та ін.

Теорія завадостійкого кодування заснована на використанні глибокого апарату сучасних абстрактних розділів математики і в першу чергу алгебри. Циклічний код – одна з найбільш яскравих ілюстрацій того, як розумне застосування результатів абстрактної математичної теорії дозволило створити прості й ефективні технічні пристрої – кодери і декодери.

Метою даної статті є дослідження методів опису і принципів побудови циклічних кодів.

Об'єктом дослідження є використання циклічних кодів в теорії завадостійкого кодування.

Методи опису і принципи побудови циклічних кодів

Множина кодових комбінацій (слів) називається циклічним кодом, якщо циклічний зсув будь-якої комбінації цієї множини на будь-яке число розрядів вліво або вправо приводить до комбінації з даної множини [1]. Циклічні коди відносяться до числа групових кодів, в яких кожна комбінація кодується самостійно у вигляді блоку завдовжки n. Блок містить m інформаційних і k контрольних символів. Довжина кодової комбінації $n = m + k$. Якщо в комбінації коду можна точно вказати позиції, займані інформаційними і контрольними символами, то код називається систематичним або роздільним, інакше – несистематичним або нероздільним [1, 4].

Початковим кодом для циклічного кодування є двійковий код і всі його поєднання. Число кодових комбінацій 2^m. При цьому число розрядів m початкового коду визначає число інформаційних символів.

Циклічні коди є різновидністю поліноміальних кодів [2]. При описі циклічного коду найзручнішим є запис його двійкової комбінації у вигляді многочлена деякої фіктивної змінної x

$$F(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x + a_0, \quad (1)$$

де $a_0, a_1, ..., a_{n-2}, a_{n-1}$ – елементи деякого кодового слова.

Використовуючи це позначення, можна визначити поліноміальний код як множину всіх

многочленів степеня не більше, ніж $(n-1)$, які містять як множник деякий фіксований многочлен $G(x)$, який називається породжуючим поліномом. Тоді процес кодування можна подати як результат множення полінома $P(x)$, що являє собою інформаційну послідовність, на породжуючий поліном $G(x)$, а декодування як результат ділення на цей поліном.

У теорії циклічного кодування додавання многочленів виконується як порозрядне додавання по модулю два. При цьому $x^i + x^i = 0$, так як $x^i \oplus x^i \to 1 \oplus 1 = 0$, де $\oplus$ – знак додавання по модулю два. Операція множення (ділення) многочленів включає їх перемножування (ділення) за звичайними правилами з подальшим приведенням подібних членів по модулю два.

Побудова циклічного коду базується на використанні так званого породжуючого (твірного) полінома $G(x)$. В якості породжуючого вибирається простий многочлен, тобто такий, який ділиться тільки сам на себе і на одиницю [1]. Доведено [3], що поліном $G(x)$ породжує циклічний код завдовжки n, якщо він є співмножником в розкладанні двочлена ($x^n + 1$) на прості многочлени. Не виключений вибір в якості породжуючого полінома добутку двох або більше простих многочленів. Проте в останньому випадку циклічний код володітиме дещо гіршими параметрами з погляду потужності безлічі кодових комбінацій. Від виду породжуючого полінома, власне і залежать основні характеристики отриманого коду: надлишковість і корегуюча здатність.

Старший степінь породжуючого полінома визначає кількість контрольних символів. Наприклад, вибираючи для початкового чотирьохрозрядного коду в якості породжуючого полінома простий многочлен $G(x) = x^3 + x + 1$, отримаємо для циклічного коду число контрольних символів $k = 3$ і довжину кодового слова $n = 4 + 3 = 7$.

Поліном

$$H(x) = \frac{(x^n + 1)}{G(x)} \tag{2}$$

називається перевірочним або генераторним поліномом. Вищий степінь перевірочного полінома рівний числу інформаційних розрядів коду m.

Кодові комбінації $F(x)$ циклічного коду, крім загальних для групових кодів обмежень, задовільняють наступним двом умовам:

а) $F(x)/G(x) = 0$, тобто без залишку діляться на породжуючий поліном;

б) $F(x) \cdot H(x) = 0$ по $\mathrm{mod}(x^n + 1)$, тобто при множенні на перевірочний поліном дають тотожний нуль по модулю двочлена $(x^n + 1)$.

На названих вище двох властивостях засновано виявлення і виправлення помилок при передачі циклічних кодів по каналах зв'язку. Ці ж властивості лежать в основі побудови циклічних послідовностей і технічної реалізації кодуючих пристроїв.

Циклічний зсув кодової комбінації F на i кроків вліво (вправо) рівносильний множенню полінома $F(x)$ на одночлен x^i (x^{-i}) по модулю двочлена $(x^n + 1)$.

Будь-яке слово в циклічному коді $F(x)$ ділиться на породжуючий поліном. Звідси витікає, що

$$F(x) = U(x) \cdot G(x), \tag{3}$$

де $U(x)$ – частка від ділення $F(x)$ на $G(x)$.

Співвідношення (3) при $U(x) = P(x)$ описує процес кодування. Початкові комбінації m-розрядного первинного коду представляються як інформаційні поліноми $P(x)$ і множаться на поліном $G(x)$. Наприклад, при множенні початкового чотирьохрозрядного інформаційного полінома $P(x) = x^3 + x^2 + 1$ на породжуючий поліном $G(x) = x^3 + x + 1$ отримаємо кодову комбінацію в циклічному коді

$$F(x) = P(x) \cdot G(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1 \to 1111111.$$

Такий спосіб кодування дає несистематичний циклічний код оскільки в кодовому слові $F(x)$ неможливо вказати місця інформаційних символів. Для їх виділення на приймальній стороні необхідно комбінації циклічного коду ділити на породжуючий поліном, що утрудняє схемну реалізацію декодуючих пристроїв.

Найбільш доцільно циклічний код представляти у вигляді роздільного (n, m) коду. Тоді алгоритм кодування визначається виразом

$$F(x) = x^k P(x) + R(x), \tag{4}$$

де $R(x)$ – залишок від ділення добутку $x^k P(x)$ на породжуючий поліном $G(x)$.

Множення на одночлен x^k відповідає зсуву інформаційної комбінації на k розрядів вліво, що еквівалентно приписуванню k нулів з боку молодших розрядів. Дана операція дозволяє пізніше на місці цих нулів розміщувати контрольні символи.

Кодовим поліномом $F(x)$ є поліном степені менше $(m+k)$, якщо він ділиться без залишку на твірний поліном $G(x)$. Після передачі повідомлення, декодування полягає у виконанні ділення полінома $H(x)$, що відповідає прийнятому коду, на $G(x)$. За відсутності помилок $H(x)=F(x)$ і ділення виконується без залишку. Наявність ненульового залишку вказує на те, що при передачі або зберіганні сталися спотворення інформації.

Циклічний код можна описати повно і компактно за допомогою породжуючої матриці в канонічній формі [1, 2, 4]:

$$F_{m,n} = \left| I_m \quad R_{m,k} \right|, \tag{5}$$

де I_m – одинична квадратна матриця розмірності $m \times k$;

$R_{m,k}$ – матриця контрольних символів розмірності $m \times k$.

Матриця I_m є породжуючою матрицею первинного m-розрядного коду. Її рядки є набором лінійно-незалежних комбінацій первинного коду і визначають вид інформаційних поліномів $P_j(x) = x^j$, де j – j-ий рядок одиничної матриці, $j = m-1,...,1,0$. Рядки матриці контрольних символів $R_{m,k}$ відповідають залишкам $R_j(x)$. В цілому рядки породжуючої матриці $F_{m,n}$ є кодовими поліномами $F_j(x)$, що визначаються по алгоритму (4).

За допомогою породжуючої матриці можуть бути отримані всі 2^m кодових комбінацій циклічного коду шляхом підсумовування рядків матриці по модулю 2 в різних поєднаннях.

Породжуючу матрицю циклічного коду можна також побудувати іншим способом. Процес побудови формалізується наступним чином. Виходячи з числа інформаційних розрядів m, складається одинична матриця I_m. До неї справа приписують матрицю контрольних символів $R_{m,k}$, яка знаходиться за допомогою наступного формального прийому. Одиниця з рядом нулів ділиться на породжуючий поліном і виписуються m проміжних залишків ділення. Ці залишки, записані в зворотному порядку, утворюють матрицю контрольних символів.

Циклічний код можна описати не тільки за допомогою породжуючої матриці, але і за допомогою перевірочної матриці $H_{k,n}$. Частіше всього на практиці застосовується циклічна форма цієї матриці. Перший рядок такої матриці залежить від виду перевірочного полінома $H(x)$, а інші рядки отримують, циклічно зсовуючи вправо перший рядок.

Вид першого рядка перевірочної матриці в циклічній формі зв'язаний з видом перевірочного полінома наступним чином. Поліном $H(x)$ представляють у вигляді кодової комбінації. Запис цієї комбінації в зворотному порядку і приписування до неї справа до $(k-1)$ нульових символів дає перший рядок перевірочної матриці $H_{k,n}$.

Рядки перевірочної матриці дають склад перевірок на парність

$$b_{k-j} = \sum_{i=1}^{n} h_{ij} \cdot a_{n-i}\ ,\ j = 1,...,k\ , \tag{6}$$

де b_{k-j} – результат j-ої перевірки на парність;

$h_{i,j}$ – елемент j-го рядка і i-го стовпця перевірочної матриці;

a_{n-i} – розряди комбінації циклічного коду.

В (6) додавання виконується по модулю 2. Ідея даної перевірки заснована на тому, що за відсутності помилок і при парному числі одиниць в кодовій комбінації сума її розрядів по модулю два завжди рівна нулю.

Із співвідношення (6) при $b_j = 0$ слідує співвідношення для формування контрольних символів

$$a_{k-j} = \sum_{i=1}^{m+j-1} h_{ij} a_{n-i}\ ,\ 1 \le j \le k\ . \tag{7}$$

Співвідношення (7) визначає ще один алгоритм побудови циклічного коду.

Двійкова послідовність $B = b_{k-1}b_{k-2}...b_1b_0$ називається синдромом або виявником помилки. Якщо синдром складається з одних нулів, то комбінація циклічного коду вважається безпомилковою. Ненульова

величина синдрому говорить про наявність помилок. Виправлення помилок проводиться в наступному порядку: прийняту кодову послідовність $H(x)$ ділять на породжуючий поліном $G(x)$ і знаходять залишок (синдром) $B(x)$, по $B(x)$ знаходять вектор помилки, додаванням по модулю 2 синдрома і вектора помилки отримують передану кодову комбінацію $F(x)$. Відповідно, обчислення синдрома є основною операцією, що виконується в процесі кодування і декодування циклічного коду.

Побудова циклічного коду проводиться, виходячи з розрядності m початкового коду і потрібної корегуючої здатності, що задається у вигляді числа виявлених r і числа виправлених s помилок. По суті справи побудова коду зводиться до вибору породжуючого полінома і складанню породжуючої матриці. Корегуюча здатність залежить від кодової відстані d. Під кодовою відстанню між двома комбінаціями F_1 і F_2 розуміють число розрядів, в яких ці комбінації відрізняються одна від одної. Кодова відстань рівна числу одиниць (вазі) W в сумі двох комбінацій по модулю 2, тобто $d = W(F_1 \oplus F_2)$. Якщо код повинен знаходити всі помилки з кратністю r і менше, то $d \geq r+1$. Якщо код повинен виправляти всі помилки з кратністю s і менше, то $d \geq 2s+1$. Якщо код повинен помилки з кратністю s і менше виправляти, а помилки з кратністю від $(s+1)$ до r включно знаходити (причому $r > s$), то $d \geq r+s+1$.

Старший степінь породжуючого полінома рівний числу контрольних символів. Тому першим кроком при виборі породжуючого полінома є визначення числа контрольних розрядів. Це число вибирають на підставі оцінок Хеммінга:

$$k \geq \log_2 \sum_{q=0}^{(d-1)/2} C_n^q \text{ при } d \text{ непарному;} \tag{8}$$

$$k \geq 1 + \log_2 \sum_{q=0}^{(d-1)/2} C_{n-1}^q \text{ при } d \text{ парному.} \tag{9}$$

Породжуючий поліном слід шукати по таблицях розкладання двочлена ($x^n + 1$) на співмножники, що не приводяться.

Поліном $G(x)$ повинен задовільняти двом умовам:

а) степінь полінома рівний k;

б) число ненульових членів більше або рівне d.

Вибраний поліном необхідно перевірити на відповідність потрібній корегуючій здатності. З цією метою одиниця з нулями ділиться на породжуючий поліном. Отримані залишки повинні задовільняти наступним умовам:

а) число різних залишків більше або рівне m;

б) вага або число одиниць кожного залишку більша або рівна ($d-1$);

в) залишки повинні відрізнятися один від одного не менше, ніж в ($d-2$) розрядах.

Якщо в розкладанні двочлена (x^n+1) не можна знайти многочлен зі степенем k і довжиною, не меншою d, то вдаються до побудови вкороченого циклічного коду. Для цього шукаємо найближчий двочлен (x^q+1) із степенем $q > n$, в розкладанні якого є поліном необхідного степеня. При цьому збільшення довжини комбінації $n = m + k$ до величини $q = m' + k$ здійснюється за рахунок інформаційних розрядів ($m' > m$). По вибраному поліному будується породжуюча матриця $F_{m',q}$ коду (q, m'), де $m' = q - k$. В отриманій матриці викреслюємо $(q-n)$ перших рядків і стільки ж стовпців зліва. В результаті отримаємо породжуючу матрицю укороченого циклічного коду.

Для укороченого коду перевірочний поліном визначається як

$$H(x) = \frac{(x^q+1)}{G(x)}. \tag{10}$$

У ряді випадків може вийти, що породжуючий поліном має необхідні степінь k і кількість елементів $n \geq d$, але його використання не забезпечує заданої корегуючої здатності, тобто при діленні 1000... на $G(x)$ не виходять необхідні залишки. В цьому випадку треба підвищувати степінь k (збільшувати число контрольних символів) до тих пір, поки не буде досягнута задана корегуюча здатність.

Розробка системи кодування/декодування інформації з використанням циклічних кодів

Нехай необхідно розробити систему кодування/декодування для дев'ятиелементного первинного коду 101100101, коли код знаходить і виправляє одну помилку. Завдання виконуватимемо в наступній послідовності.

1. Визначення кількості перевірочних елементів k.

Виходячи з того, що $m = 9$ і $s = 1$, вирішуємо систему рівнянь

$$\begin{cases} n = m + k \\ k \geq \log_2\left[1 + \sum_{i=1}^{s} C_n^i\right] = \log_2\left[1 + \sum_{i=1}^{1} C_n^i\right] = \log_2\left[1 + C_n^1\right] = \log_2(1+n). \end{cases} \quad (11)$$

Звідси слідує, що $2^k \geq 1 + n = 1 + m + k \;\Rightarrow\; 2^k - k \geq 1 + m = 1 + 9 = 10$.

Складаємо таблицю для визначення потрібної кількості контрольних символів.

Таблиця 1

Визначення необхідної кількості контрольних символів

k	$2^k - k$
1	1
2	2
3	5
4	12

Таким чином, для забезпечення заданої корегуючої здатності необхідна кількість контрольних символів $k = 4$. Довжина кодової комбінації $n = m + k = 9 + 4 = 13$.

2. Вибір породжуючого полінома.

Після визначення контрольних розрядів k вибираємо породжуючий поліном $G(x)$ (многочлен степеня k). Породжуючий поліном $G(x)$ повинен володіти деякими властивостями:

1) залишки від ділення повинні бути всі різні, тобто його не можна скласти із степенів нижчих порядків, він простий;

2) число залишків полінома має бути рівне кількості помилок в коді, тобто такі поліноми примітивні.

З допомогою таблиці породжуючих поліномів можна знайти необхідний поліном. В таблиці вказані деякі властивості цих многочленів і співвідношення між ними. Приводяться примітивні многочлени з мінімальним числом ненулевих коефіцієнтів. Многочлени представлені у вісімковій системі.

Букви, які приведені після вісімкового представлення многочлена, дають про нього наступну інформацію: A, B, C, D – не примітивний; E, F, G, H – примітивний; A, B, E, F – корені лінійно залежні; C, D, G, H – корені лінійно незалежні; A, C, E, G – корені подвійного многочленна лінійно залежні; B, D, F, H – корені подвійного многочленна лінійно незалежні.

Із таблиці простих поліномів [3, табл. В.2] вибираємо поліном $1 \quad 23F$ і переводимо з вісімкового в двійкове представлення: $23_8 = 010.011_2$. Отримали породжуючий поліном: $G(x) = x^4 + x + 1$.

3. Перевірка породжуючого полінома.

Визначаємо необхідну кодову відстань: $d = 2 \cdot c + 1 = 2 \cdot 1 + 1 = 3$.

Знаходимо добуток $P(x)x^k$.

$P(x)x^k = (x^8 + x^6 + x^5 + x^2 + 1) \cdot x^4 = x^{12} + x^{10} + x^9 + x^6 + x^4 \rightarrow 1011001010000$.

Виконаємо ділення $P(x)x^k$ на $G(x)$.

$$\begin{array}{l|l} x^{12} + x^{10} + x^9 + x^6 + x^4 & x^4 + x + 1 \\ \underline{x^{12} + x^9 + x^8} & \hline x^8 + x^6 + x^4 + x^3 + x + 1 \\ \quad x^{10} + x^8 + x^6 & \\ \quad \underline{x^{10} + x^7 + x^6} & \\ \quad\quad x^8 + x^7 + x^4 & \\ \quad\quad \underline{x^8 + x^5 + x^4} & \\ \quad\quad\quad x^7 + x^5 & \\ \quad\quad\quad \underline{x^7 + x^4 + x^3} & \\ \quad\quad\quad\quad x^5 + x^4 + x^3 & \\ \quad\quad\quad\quad \underline{x^5 + x^2 + x} & \\ \quad\quad\quad\quad\quad x^4 + x^3 + x^2 + x & \\ \quad\quad\quad\quad\quad \underline{x^4 + x + 1} & \\ \quad\quad\quad\quad\quad\quad x^3 + x^2 + 1 \rightarrow 1101. & \end{array}$$

Отриманий залишок від ділення $R(x) = 1101$ є комбінацією контрольних елементів. Таким чином, отримана кодова комбінація має вигляд: $F(x) = P(x)x^k + k(x) = 1011001011101$.

Визначаємо вагу многочлена (кількість одиниць в комбінації): $W = 8$. Порівнюємо W з d. Оскільки виконується умова $W \geq d$, то вибраний поліном підходить як породжуючий.

4. Кодування з допомогою породжуючої матриці.

Породжуюча (твірна) матриця утворюється дописуванням елементів додаткової матриці справа від одиничної транспонованої матриці. Визначення елементів додаткової матриці проводиться по залишках від ділення останнього рядка транспонованої матриці (одиниці з нулями) на породжуючий многочлен.

```
10000000000000 | 10011
10011          | 1001101011
 00110
 00000
  01100
  00000
   11000
   10011
    10110
    10011
     01010
     00000
      10100
      10011
       01110
       00000
        11100
        10011
         11110
         10011
          1101.
```

Кожен отриманий залишок запишемо в рядки перевірочної матриці. Таким чином, породжуюча матриця матиме вигляд

$$F_{13,\ 9} = \begin{Vmatrix} 000000001 & 0011 \\ 000000010 & 0110 \\ 000000100 & 1100 \\ 000001000 & 1011 \\ 000010000 & 0101 \\ 000100000 & 1010 \\ 001000000 & 0111 \\ 010000000 & 1110 \\ 100000000 & 1111 \end{Vmatrix}$$

Просумуємо по модулю 2 ті рядки матриці, номери яких співпадають з номерами розрядів, що містять одиниці в кодовому векторі, який представляє інформаційну частину коду.

$$\begin{array}{r} 1000000001111 \\ 0010000000111 \\ 0001000001010 \\ \oplus \quad 0000001001100 \\ \underline{0000000010011} \\ 1011001011101 \end{array}$$

Таким чином, отримана кодова комбінація має вигляд: $F(x) = 1011001011101$.

5. Побудова матриці синдромів для однократної помилки.

Для визначення елементів матриці синдромів будемо вносити помилку в кодову комбінацію $F(x) = 1011001011101$ почергово починаючи зі старшого розряду, потім ділити на породжуючий поліном, отриманий залишок і буде одним із рядків матриці синдромів.

Нехай помилка виникла в найстаршому розряді, тоді вона має вигляд 0011001011101. Виконаємо ділення полінома, що відповідає кодовій комбінації з помилкою в найстаршому розряді, на породжуючий поліном.

$$\begin{array}{l|l} x^{10}+x^9+x^6+x^4 & x^4+x+1 \\ \underline{x^{10}+x^7+x^6} & \hline x^6+x^5+x^3+x^2+x \\ \quad x^9+x^7+x^4 & \\ \quad \underline{x^9+x^6+x^5} & \\ \quad\quad x^7+x^6+x^5+x^4 & \\ \quad\quad \underline{x^7+x^4+x^3} & \\ \quad\quad\quad x^6+x^5+x^3 & \\ \quad\quad\quad \underline{x^6+x^3+x^2} & \\ \quad\quad\quad\quad x^5+x^2 & \\ \quad\quad\quad\quad \underline{x^5+x^2+x} & \\ \quad\quad\quad\quad\quad x \;\rightarrow\; 0010. & \end{array}$$

Отриманий в результаті ділення залишок (0010) буде синдром для помилки в розряді a_1. Синдроми для інших розрядів визначаються аналогічно.

Таким чином, матриця синдромів матиме вигляд

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \begin{array}{l} всі\ \ правильні \\ помилка\ \ в\ \ розряді\ \ a_1 \\ помилка\ \ в\ \ розряді\ \ a_2 \\ помилка\ \ в\ \ розряді\ \ a_3 \\ помилка\ \ в\ \ розряді\ \ a_4 \\ помилка\ \ в\ \ розряді\ \ a_5 \\ помилка\ \ в\ \ розряді\ \ a_6 \\ помилка\ \ в\ \ розряді\ \ a_7 \\ помилка\ \ в\ \ розряді\ \ a_8 \\ помилка\ \ в\ \ розряді\ \ a_9 \end{array}$$

Отримана матриця синдромів використовується для алгоритму побудови дешифратора помилок декодера. В даний час актуальною є програмна реалізація процесів кодування і декодування.

6. Оцінка ймовірності невиявленої помилки на виході системи передачі інформації.

Визначимо ймовірність помилкового прийому кодової комбінації в умовах біноміального розподілу помилок. При завадостійкому кодуванні розрізняють помилки двох типів: виявлені (або виправлені) кодом і невиявлені помилки. Ймовірність появи невиявлених помилок $P_{нв.}$ (в режимі виправлення)

$$P_{нв.} = 2^{m-n} \sum_{i=s+1}^{n} C_n^i P_{пом.}^i \left(1 - P_{пом.}\right)^{n-i}, \qquad (12)$$

де $P_{пом.}$ – ймовірність помилки в каналі зв'язку.

За допомогою математичного пакету MathCAD проводимо розрахунки і отримуємо графічну залежність ймовірності невиявлених помилок від ймовірності помилки елемента (рис. 1).

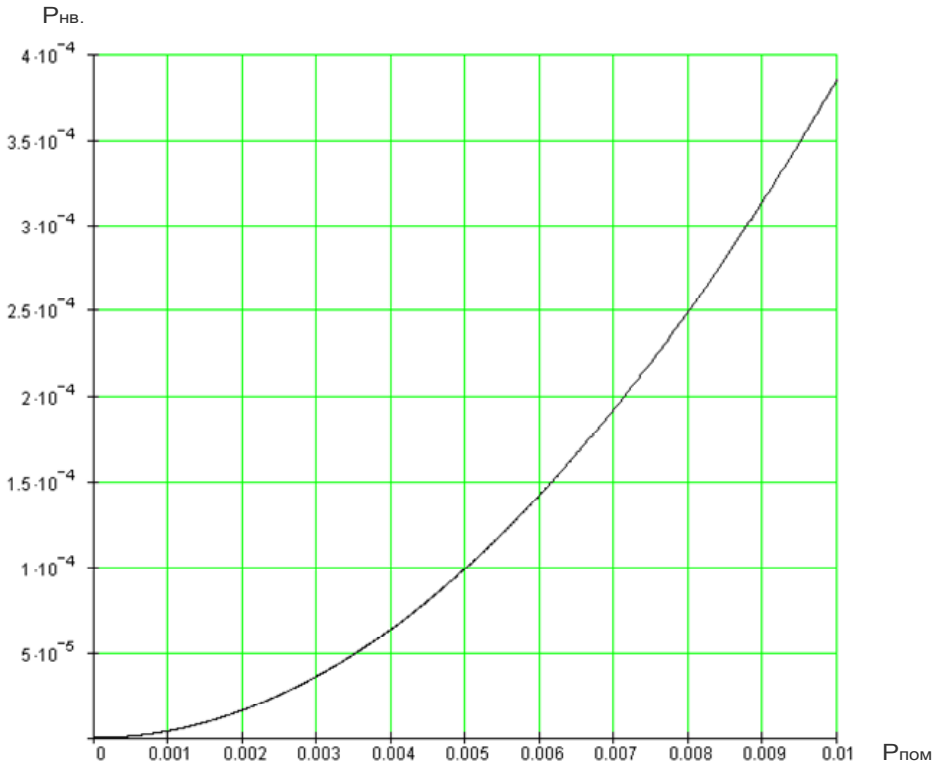

Рис. 1. Графік залежності ймовірності невиявленої помилки на вході приймача від ймовірності помилки в каналі зв'язку

Із графіка видно, що зі збільшенням ймовірності помилки в каналі зв'язку ймовірність виявлення помилки на вході приймача також збільшується.

Висновки

За результатами проведених досліджень можна зробити висновок, що циклічні коди отримали широке застосування завдяки їх ефективності при виявленні і виправленні помилок.

Циклічні коди є різновидністю поліноміальних кодів, тому дії над кодовими комбінаціями зводяться до дій над многочленами. Побудова циклічного коду базується на використанні так званого породжуючого полінома $G(x)$. В якості породжуючого вибирається простий многочлен, тобто такий, який ділиться тільки сам на себе і на одиницю. Тоді процес кодування можна подати як результат множення полінома $P(x)$, що являє собою інформаційну послідовність, на породжуючий поліном $G(x)$, а декодування як результат ділення на цей поліном. Побудова циклічного коду проводиться, виходячи з розрядності m початкового коду і потрібної корегуючої здатності, що задається у вигляді числа виявлених r і числа виправлених s помилок. По суті справи побудова коду зводиться до вибору породжуючого полінома і складання породжуючої матриці.

Зі збільшенням ймовірності помилки в каналі зв'язку ймовірність виявлення помилки на вході приймача також збільшується.

Література

1. Кузьмин И.В. Основы теории информации и кодирования / И.В. Кузьмин, В.А. Кедрус. – 2-е изд., перераб. и доп. – К.: Вища шк. Головное изд-во, 1986. – 238 с.

2. Шварцман В.О. Теория передачи дискретной информации: Учебник для вузов связи / В.О. Шварцман, Г.А. Емельянов. – М.: Связь, 1979. – 424 с.

3. Питерсон У. Коды, исправляющие ошибки / Пер. с англ. / У. Питерсон, Э. Уэлдон. – М.: Мир, 1976. – 593 с.

4. Акулиничев Ю.П. Теория электрической связи: Учеб. Пособие / Ю.П. Акулиничев. – СПб.: Лань, 2010. – 240 с.

Надійшла до редакції
12.10.2010 р.