УДК 621.391.1

М.М. Букасов, аспір.
Національний технічний університет України "КПІ"

КІЛЬЦЕВИЙ КОД

(Представлено д.т.н., проф. С.Ф. Телеником)

Розглядається недвійковий надмірний блоковий лінійний код, що може виправляти пакети помилок. Запропоновано алгоритми кодування і декодування, а також розглянуто декілька властивостей коду, використання яких може допомогти виявити помилки більшої кратності.

Вступ

Дуже часто завади в каналі зв'язку та дефекти на носіях інформації мають тенденцію групуватися, що спричиняє появу пакетів з декількох помилок, що йдуть одна за одною. Тому великий практичний інтерес мають коди, що здатні виявляти та виправляти пакети помилок.

Серед **блокових** кодів, що здатні виправляти пакети помилок, найбільш популярні *циклічні коди* (коди Ейбрамсона, Файра [1]), а також коди, що отримують символьним перемеженням кодів, що виправляють помилки меншої кратності (у тому числі й однократні) [1, 2].

Серед **неперервних** кодів, що здатні виправляти помилки, найбільш популярні *згортанні* коди (коди Берлекемпа–Препарата–Мессі, Івадаре [1]). Також, завдяки простоті реалізації, широке застосування в системах передачі даних набув неперервний *ланцюговий* код [2,3], в якому кожен перевірний символ формується за двома інформаційними, що знаходяться на відстані t один від одного (t – найбільша довжина пакета, що може бути виправлений).

В роботі представлений *блоковий* код, для якого операції кодування і декодування здійснюються аналогічно до *неперервного* ланцюгового коду.

Сутність коду

Введемо такі поняття і умовні позначення:

k – кількість інформаційних символів;

r – кількість перевірних символів (для цього $k = r$);

n – загальна кількість символів, $n = k + r$;

пакет помилок довжини l – послідовність з таких l помилкових символів, що перший і останній з них відрізняються від нуля. Далі буде показано, що для даного коду як пакет довжини l можливо розглядати такі вектори помилок, в яких ненульові символи займають усього l позицій з обох кінців кодової комбінації. Так, наприклад, для коду з $n = 8$, помилки з векторами (00**111**000), (00**101**000), (**1**0000**11**), (**1**0000**10**) можна розглядати як пакети помилок довжиною 3 символи;

q – основа (алфавіт) коду;

$\{i\}$ – і-й інформаційний символ (на рисунках позначені великими жирними цифрами);

$\{ij\}$ – перевірний символ, розрахований як

$$\{ij\} = \{i\} \oplus \{j\} \qquad (1)$$

$\oplus$ – операція складання у полі GF (q) [4].

Для наочності подамо кодове слово у формі кільця. Пропонується розставити суміжні інформаційні символи на відстані $2l$ один від одного (при цьому перший і k-й інформаційні символи також розглядаються як суміжні), а посередині – перевірний символ. На рис. 1 наведено приклад побудови кільцевого коду з $k = 7$, $l = 3$. Нижче наведена твірна матриця для цього ж коду. Числа, що стоять над стовпцями матриці, ілюструють алгоритм кодування і позначають розташування інформаційних і перевірних символів.

$$G_{(n,k)} = G_{(14,7)} = \begin{array}{c} \begin{matrix} 1 & \begin{matrix}3\\4\end{matrix} & 6 & \begin{matrix}1\\2\end{matrix} & 4 & \begin{matrix}6\\7\end{matrix} & 2 & \begin{matrix}4\\5\end{matrix} & 7 & \begin{matrix}2\\3\end{matrix} & 5 & \begin{matrix}7\\1\end{matrix} & 3 & \begin{matrix}5\\6\end{matrix} \end{matrix} \\ \left[\begin{array}{cccccccccccccc} 1&0&0&1&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&1&0&0&1&0&0&1&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&1&0&0&1&0 \\ 0&1&0&0&1&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&1&0&0&1 \\ 0&0&1&0&0&1&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&0&0&1&0&0&1&0&0 \end{array}\right] \end{array} \tag{2}$$

Перший рядок матриці містить “1“ лише в 1-му, $(1+l)$-му і $(1-l)$-му стовпцях (під $(1-l)$-м мається на увазі l-й справа). Кожен наступний рядок отримується циклічним зсувом попереднього на $2l$ символи праворуч.

Очевидно, що кодова комбінація такого коду, циклічно зсунута на два розряди, також є дозволеною комбінацією цього коду.

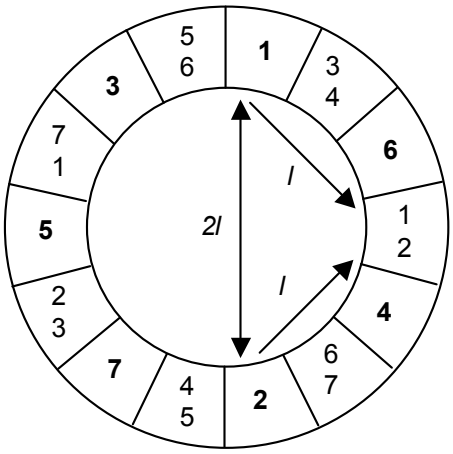

Рис. 1

<u>Порівняльний аналіз</u>

Для кодів, що виправляють пакети помилок, одним з основних параметрів, що визначають їх корегуючу спроможність, є максимальна довжина пакету помилок, що можна виправити.

Ідея виправлення помилок кільцевим кодом полягає у наступному. Будь-які два суміжні інформаційні символи, а також перевірний символ, отриманий як їх сума, розташовані на відстані не менш ніж l один від одного. Це означає, що будь-який пакет помилок довжиною не більш ніж l, не здатний внести помилку більш ніж в одну складову (1), яка може бути відтворена на основі двох інших (якщо відомо положення помилки).

В [1] доведено, що здатність корегування для пакетів помилок довжини l будь-якого лінійного блокового (n,k)- коду визначається умовою:

$$n - k - 2l = z \geq 0\,, \tag{3}$$

де параметр z є *мірою неефективності* блокового коду, що виправляє пакети помилок.

Оскільки $n = 2k$, значення l не може перевищувати $n/4$.

Вибір l розглянемо більш детально для парного и непарного k:

<u>k – парне</u>. Для парного k значення l не може дорівнювати $n/4$, оскільки в цьому випадку два інформаційних символи, віддалені на відстань l один від одного, будуть брати участь у формуванні лише двох перевірних символів. Тобто неможливо буде виявити положення помилок. Таким чином, для парного k:

$$\begin{aligned} &l \leq k/2 - 1, \\ &l_{\max} = k/2 - 1. \end{aligned} \tag{4}$$

Отже, при парному k маємо:

$$z = n - k - 2l = 2k - k - 2(k/2 - 1) = 2\,; \tag{5}$$

<u>k – непарне</u>. З тих же міркувань:

$$l < n/4 = k/2 \tag{6}$$

і оскільки k – непарне, то

$$l_{\max} = (k-1)/2; \quad (7)$$

$$z = n - k - 2l = 2k - k - 2((k-1)/2) = 1. \quad (8)$$

Таким чином, кільцевий код є більш ефективним при непарному k, і далі в роботі будемо розглядати саме цей випадок.

В табл. 1 наведено ряд двійкових циклічних кодів, що виправляють пакети помилок. Коди у цій таблиці зібрані авторами [1] з декількох джерел. Для кожного значення швидкості передачі наведено циклічний або вкорочений циклічний код з найбільшим відомим відношенням l/n. Якщо два або більше кодів мають одне й те ж відношення l/n, то наводиться найкоротший. Для зручності запису твірні поліноми $g(X)$ подані у вісімковій системі числення. Наприклад, $35 = 011101 = X^4 + X^3 + X^2 + 1$. В останньому рядку подані параметри кільцевого коду при непарному k.

Таблиця 1

Деякі циклічні коди, що виправляють пакети помилок

R	(n, k)	$l_{\max}$	z	l/n	Твірний поліном $g(X)$
$\frac{1}{2l+1}$	$(2l+1, 1)$	l	0	$\frac{l}{2l+1}$	$\frac{(X^{2l+1}-1)}{X-1}$
0,42	(7, 3)	2	0	0,286	35
0,60	(15, 9)	3	0	0,200	171
0,63	(27, 17)	5	0	0,185	2671
0,65	(34, 22)	6	0	0,176	15173
0,68	(50, 34)	8	0	0,160	224531
0,81	(67, 54)	6	1	0,090	36365
0,85	(103, 88)	7	1	0,068	114361
0,87	(63, 55)	3	2	0,048	711
0,88	(85, 75)	4	2	0,047	2651
0,91	(131,119)	5	2	0,038	15163
0,92	(169, 155)	6	2	0,035	55725
0,93	(121, 112)	3	3	0,025	1411
0,96	(290, 277)	5	3	0,017	24711
0,98	(511, 499)	4	4	0,008	10451
0,99	(1023, 1010)	4	5	0,004	22365
0,5	$(2l+1, 2l+1)$	l	1	$\frac{l}{4l+2}$	—

Для кільцевого коду при достатньо великому n і непарному k:

$$\lim_{n\to\infty} l/n = \lim_{l\to\infty} l/(4l+2) = 0.25,$$

$$R = k/n = 0{,}5.$$

На рис. 2 зображена залежність відносної швидкості передачі R від відношення l/n до кодів з табл. 1. На рівні $R = 0{,}5$ наведені відношення l/n для кільцевого коду при $l = 3, 5, 11, \infty$. Як видно з графіка, ефективність коду значно підвищується при збільшенні n.

Для порівняння кільцевого коду з неперервним ланцюговим кодом скористаємося поняттям *умовної кодової групи*, довжина якої дорівнює сумі довжини пакета помилок і захисного інтервалу та дорівнює [2]:

$$n' = 4l + 1. \quad (9)$$

При достатньо великому l: $\lim_{l\to\infty} l/n' = \lim_{l\to\infty} l/(4l+1) = 0{,}25$ при $R = 0{,}5$.

Таким чином, ці коди мають приблизно однакову ефективність.

<u>Деякі властивості коду і алгоритм декодування</u>

Алгоритм декодування кільцевого коду, як і багатьох інших кодів, що виправляють помилки, полягає в наступному:

1) на приймальному боці на основі отриманих інформаційних символів розраховуються контрольні символи;
2) розраховані контрольні символи порівнюються з отриманими перевірними символами;
3) робиться висновок про наявність чи відсутність помилки та приймається рішення про її корегування.

Перед тим, як сформулювати алгоритм декодування, розглянемо декілька властивостей кільцевого коду.

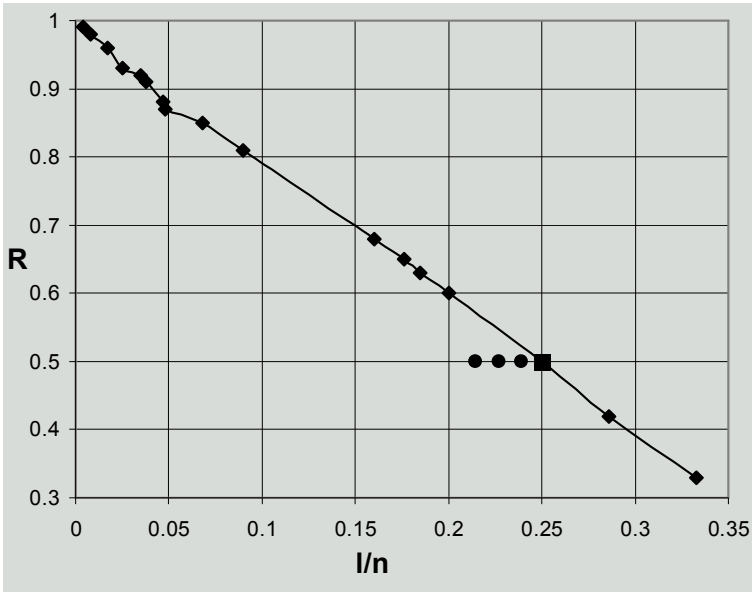

Рис. 2

Теорема 1. Будь-*який пакет помилок довжини* $\le l$, *не спричинить розбіжності усіх контрольних і перевірних символів.*

Доведення. Дійсно, пакет довжини l (l – непарне) здатен спотворити не більш ніж $\frac{l+1}{2}$ інформаційних і $\frac{l-1}{2}$ перевірних символів (чи навпаки). При цьому спотворення одного перевірного символу спричиняє один незбіг контрольних і перевірних символів, а одного інформаційного – два. Таким чином, при наявності пакета помилок довжини l може з'явитися не більш ніж $\frac{l-1}{2}+\frac{l+1}{2}\cdot 2=\frac{3l+1}{2}$ незбігів контрольних і перевірних символів, або, враховуючи, що $k=2l+1$, маємо максимум $\frac{3k-1}{4}$ незбігів і мінімум $k-\frac{3k-1}{4}=\frac{k+1}{4}$ збігів контрольних і перевірних символів. Щ.в.д.

Слід також зазначити, що при непарному l і $k = 2l+1$ у коді відсутні "*замкнені підгрупи перевірок на парність*" (такі, як були розглянуті вище при $l = k/2$). При цьому термін "парність" є дуже умовним, оскільки кільцевий код не є двійковим ($q \ge 2$). Іншими словами, при обході кільця довжиною n з кроком l потрібно n кроків, щоб обійти усе кільце і повернутися у вихідний символ (рис. 2).

Розглянемо процес виправлення пакета помилок кільцевим кодом. На рис. 3 символами "e" позначено положення помилки. Символами "x" позначені перевірні елементи, в яких не збіглися значення контрольних і перевірних символів.

Для перевірного елемента {23} значення контрольних і перевірних символів збігаються, а це означає, що при будь-якому пакеті помилок довжиною не більше за l, символи {2} і {3} – вірогідні. Для перевірного елемента значення контрольних і перевірних символів не збіглися. Оскільки символ {2} вірогідний, робимо висновок, що був спотворений символ {1}, {12} або обидва. Для елемента {71} значення контрольного і перевірного символів також не збіглись.

Оскільки символи {12} і {71} розташовані на відстані $2l$ один від одного і не можуть бути безпосередньо спотворені пакетом помилок довжиною l, робимо висновок, що цей розбіг пов'язаний з помилкою у символі {1}, який бере участь у формуванні обох цих перевірних символів.

Узагальнимо наведені вище міркування, і сформулюємо алгоритм декодування.

Алгоритм. Якщо на черговій ітерації є такі {d}, {de}, {e}, {ef}, {f}, {fg} інформаційні та перевірні елементи, що для {fg} значення контрольних і перевірних елементів збіглись, а для {de} і {ef} – ні, то робиться висновок про те, що у символі {e} була помилка і її потрібно виправити за формулою:

$$\{e\} = \{de\} - \{d\} \qquad (10)$$

або

$$\{e\} = \{ef\} - \{f\}, \qquad (11)$$

де "-" – операція віднімання у полі GF(q), що є зворотною до операції складання $\oplus$.

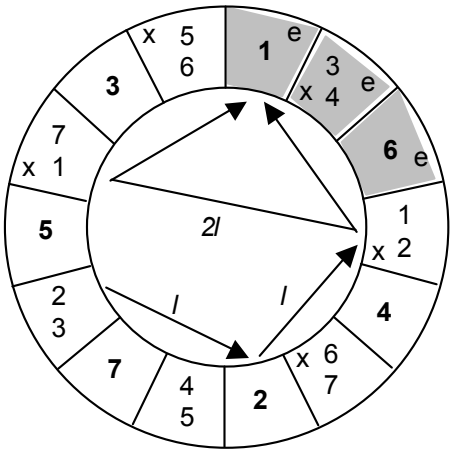

Рис. 3

Після корегування символу {e} робиться повторний розрахунок контрольних символів і перехід на нову ітерацію.

Якщо на черговий ітерації не можна виділити жодної вказаної групи символів, робимо висновок про те, що всі інформаційні символи є вірогідними, а помилки, якщо вони присутні, то лише у перевірних символах.

Наслідок 1. Формули (10) і (11) були записані виходячи з міркувань, що пакет помилок довжини l, що спотворив символ {e}, не здатен спотворити символи {de}, {ef} та {d},{f}, розташовані на відстані l и $2l$ від {e}. Якщо розрахунки за формулами (10) і (11) призвели до різних результатів, робимо висновок, що була помилка більш високої кратності, ніж та, яку може виправити даний код.

Теорема 2. *Якщо* кодова *комбінація кільцевого коду містить у собі інформаційні символи, спотворені пакетом довжиною не більше за l, то присутні не менш ніж дві групи таких інформаційних і перевірних елементів {de}, {e}, {ef}, {f}, {fg}, що для {fg} значення контрольних і перевірних символів збігаються, для {de}* і *{ef} – ні, а символ {e} є крайнім інформаційним символом у пакеті помилок*.

Доведення. У кодовій комбінації інформаційні та перевірні символи чергуються. Очевидно, що при виконанні умови $n = 2k = 2(2l+1) = 4l+2$, незалежно від того, починається пакет з інформаційного символу чи з перевірного (рис. 4), вказана група символів знайдеться. В результаті аналогічних міркувань для інформаційного символу, що є крайнім з другого боку пакета помилок, приходимо до висновку, що вказаних груп символів буде не менше за дві. У випадку, коли пакет помилок спотворив лише один інформаційний елемент, обидві групи будуть вказувати на необхідність його корегування. Щ.в.д.

Наслідок 2. Алгоритм дозволяє виправляти дві помилки за одну ітерацію.

Наслідок 3. Якщо на черговій ітерації алгоритму декодування інформаційні символи, визначені як помилкові, розташовані на відстані більший за l один від одного чи від виправлених на попередніх ітераціях, робимо висновок, що була помилка більш високої кратності, ніж та, яку може виправити даний код.

Наслідок 4. Якщо на останній ітерації алгоритму декодування (коли неможливо виділити жодної описаної в алгоритмі групи символів {de}, {e}, {ef}, {f}, {fg}) є перевірні елементи, в яких не збігаються значення контрольних і перевірних символів, і ці розряди знаходяться на відстані, більшій за l один від одного чи від інформаційних, виправлених на попередніх ітераціях, робимо висновок, що була помилка більш високої кратності, ніж та, яку може виправити даний код.

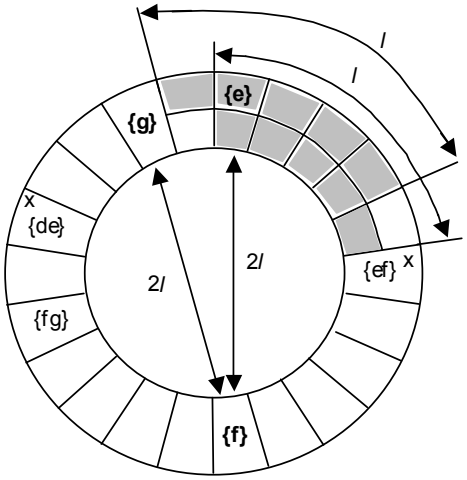

Рис. 4

Висновки

1. Розроблено блоковий лінійний код, що виправляє усі пакети помилок довжиною не більше за l. При цьому, як пакет можна розглядати такі комбінації помилок, у вектори яких ненульові символи займають всього l позицій з обох кінців кодового слова.
2. Код може бути побудований для будь-якого непарного l і q (алфавіт).
3. $k = 2l + 1, n = 2k = 4l + 2$.
4. Основні параметри, що характеризують ефективність коду, такі ж як у неперервного ланцюгового коду: відносна швидкість передачі $R = k / n = 0{,}5$ при $l / n \approx 0{,}25$. При цьому для неперервного коду замість n використовувалось поняття довжини умовної кодової групи.
5. Операція кодування може виконуватись матричним чи алгебраїчним способами. Матричний спосіб полягає в перемноженні вихідної кодової комбінації на твірну матрицю. Алгебраїчний спосіб полягає в розрахунку $r = k$ перевірних елементів за допомогою операції складання у полі GF(q).
6. Приведено алгоритм декодування і доведена його працездатність при будь-якому пакеті помилок довжиною не більше за l.
7. Розглянуті властивості коду, що можуть бути використані для виявлення деяких помилок більш високої кратності. Це може бути ефективно використано у СПД з ОЗ.

ЛІТЕРАТУРА:

1. *Питерсон У., Уэлсон Э.* Коды, исправляющие ошибк: Пер. с англ. / Под ред. Р.Л. Добрушина и С.И. Самойленко. – М.: Мир, 1976. – 596 с.
2. Кодирование информации (двоичные коды) / Н.Т. Березюк, А.Г. Андрущенко, С.С. Мощицкий и др. – Х.: Вища шк., 1978. – 252 с.
3. *Жураковский Ю.П.* Передача информации в ГАП: Учеб. пособие. – К.: Вища шк., 1991. – 216 с.
4. *Муттер В.М.* Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат. Ленингр. отд-ние, 1990. – 288 с.

БУКАСОВ Максим Михайлович – асистент кафедри автоматики і управління в технічних системах Національного технічного університету України “КПІ”.

Наукові інтереси:
– системи передачі даних;
– електроніка і мікропроцесорна техніка;
– програмування.

Подано 11.12.2001