Л. А. Кирпач, К. П. Сторчак, И. Н. Срибная

ИССЛЕДОВАНИЕ КОМБИНИРОВАННЫХ СИСТЕМ ФАЗОВОЙ СИНХРОНИЗАЦИИ

Рассмотрены комбинированные системы фазовой синхронизации в плане повышения их точности и быстродействия.

Ключевые слова: комбинированные системы фазовой синхронизации; переходная составляющая ошибки; корни характеристического уравнения.

L. A. Kyrpach, K. P. Storchak, I. M. Sribna

STUDY OF COMBINED PHASE CLOCK

We consider the combination of the phase synchronization issues increasing their accuracy and speed.

Keywords: combined phase synchronization system; transient component of error; the roots of the characteristic equation.

УДК 621.391:519.726

Б. Ю. ЖУРАКОВСЬКИЙ, доктор техн. наук, професор,
Державний університет телекомунікацій, Київ

ВИКОРИСТАННЯ КОМПАУНДНИХ КОДІВ ДЛЯ ПЕРЕДАВАННЯ ДАНИХ

Запропоновано оцінювати ефективність завадостійких, зокрема компаундних, кодів для інформаційних каналів за ймовірністю виявлення та ймовірністю виправлення помилок різної кратності, а також за коефіцієнтом збільшення інформаційного масиву.

Ключові слова: завадостійки коди; кодова комбінація; компаундний код; коефіцієнт підвищення достовірності; коефіцієнт збільшення інформаційного каналу.

При передаванні інформації простим ненадлишковим кодом здебільшого вірогідність прийому, залежна від типу каналу та виду завад у ньому, практично недостатня. Її необхідно підвищити, щоб імовірність помилкового прийому повідомлення споживачем була менша, ніж імовірність помилок у повідомленні без вжиття спеціальних заходів.

Як один зі шляхів підвищення вірогідності розглядається застосування надлишкового коду [1].

Усі надлишкові коди можна використовувати з метою:

1) виявлення помилок;

2) виправлення помилок;

3) виявлення та виправлення помилок.

Наприклад, щоб підвищити вірогідність за допомогою кодів, призначених для виявлення помилок, уводять у дію зворотний канал зв'язку. Тоді кодову комбінацію, прийняту по прямому каналу, аналізують, з'ясовуючи, чи дозволена вона. Якщо так, ця комбінація надходить до споживача після відкидання перевірних розрядів. У разі виявлення помилки по зворотному каналу надсилається сигнал запиту, за яким передавальний пристрій повторює передавання інформації. Тому цей пристрій має зберігати інформацію про відправлені сигнали протягом часу, достатнього для аналізу комбінації приймальним пристроєм і отримання можливого запиту про помилки [2].

Системи зі зворотним каналом називають ***системами зі зворотним зв'язком***. Вони мають такі переваги:

• виявляльна здатність коду за однакової надлишковості вища, ніж виправляльна;

• кількість логічних операцій, що їх має виконувати декодер для виявлення помилок, набагато менша за кількість операцій, необхідних для їх виправлення.

Єдиний недолік систем зі зворотним зв'язком — це зниження швидкості передавання інформації. Проте цей недолік стає відчутний тільки в разі незадовільного стану каналу зв'язку.

Виправлення помилок зазвичай здійснюється тоді, коли в каналі зв'язку мають місце незалежні помилки чи короткі пачки помилок. Якщо вага помилок така сама, як довжина кодової комбінації, то виправлення пачок помилок призводить до невиправданої експлуатації кодувальних і декодувальних пристроїв.

Коди, призначені для виправлення помилок, здатні виправляти помилки, вага яких не перевищує 20–25% від довжини кодової комбінації. Найбільш імовірні помилки мають вагу, близьку до половини довжини кодової комбінації. Тому доцільно застосовувати для виправлення ті способи, які дозволяють відокремлювати перевірні імпульси від інформаційних протягом часу, що перевищує ймовірну довжину пачки помилок [3].

Отже, при виборі способу підвищення вірогідності передавання інформації слід брати до уваги такі чинники, як необхідна вірогідність прийому, припустима швидкість передавання, ураховуючи залежність вірогідності від помилок у каналі зв'язку [4].

Сьогодні маємо десятки розроблених кодів, теоретично здатних виявляти й виправляти довільну кількість помилок.

Утім на практиці більшість надлишкових кодів виправляє тільки незалежні помилки. Лише невелика група кодів дозволяє виправляти пакети помилок [5].

Ступінь захисту інформації від помилок, що його забезпечує той чи інший спосіб кодування, залежить передусім від мінімальної кодової відстані $d_{\min}$ даного коду.

Розрізняють три види кодової відстані: ***відстань Хеммінга***, ***Лі*** та ***матричну*** [6]. Найбільшого поширення в теорії кодування набула кодова відстань Хеммінга, тісно пов'язана з поняттям ваги w кодової комбінації — кількістю ненульових її елементів.

Кодова відстань Хеммінга d між двома комбінаціями однакової довжини n визначається як кількість однойменних розрядів (позицій), що містять неоднакові елементи.

Зокрема, для двійкових кодів, оскільки в двійковій арифметиці додавання однакових елементів завжди дає 0, а неоднакових — завжди 1, відстань Хеммінга між двома кодовими комбінаціями можна визначити порозрядним додаванням їх за модулем 2 і подальшим підрахунком кількості ненульових елементів, тобто визначенням ваги w такої суми.

Загальна кількість кодових комбінацій завдовжки n дорівнює 2^n, а кількість тих із цих комбінацій, котрі віддалені від заданої на відстань d, визначається за відомою формулою:

$$C_n^d = n!/[d!(n-d)!]. \qquad (1)$$

Для виявлення всіх помилок кратністю $v_в$ кодова відстань d має задовольняти нерівність $d \geq v_в+1$, а для виправлення помилок кратністю $v_{в.п}$ — нерівність $d \geq 2v_{в.п} + 1$. Щоб можна було виправити та виявити всі помилки, має виконуватись умова

$$d \geq v_{в.п} + v_в + 1. \qquad (2)$$

Через те, що кожний елемент (розряд) комбінації недвійкового (багатопозиційного) коду може, на відміну від двійкового, включати в себе більш як одну позицію ($m \geq 1$) з алфавіту q, то кодова відстань має визначатися виразом

$$d = \sum_{i=1}^{m} d_i, \qquad (3)$$

де m — кількість позицій у кожному розряді (поодинокому новому інтервалі, що відповідає тривалості одного елемента) кодової комбінації.

У ***метриці Хеммінга*** кодова відстань, як і для двійкового коду, визначається кількістю однойменних розрядів із різними позиціями (символами):

$$d_i(x_k, x_l) = \begin{cases} 0, x_k = x_l; \\ 1, x_k \neq x_l. \end{cases} \qquad (4)$$

У ***метриці Лі*** маємо:

$$d_i(x_k, x_l) = \min\{|x_k - x_l|, q - |x_k - x_l|\} = \\ = \min\{d_{j\text{mod}}, q - d_{j\text{mod}}\}, \qquad (5)$$

де $d_{j\text{mod}} = |x_k - x_l|$.

У ***модульній метриці*** $d_i(x_k, x_l) = |x_k - x_l|$, тобто виконується віднімання за модулем q.

Найбільш раціональними слід вважати системи передавання інформації, в яких надлишкові коди використовуються тільки для виявлення помилок. Адже в реальних каналах часто спостерігаються пачки помилок завдовжки в кілька десятків чи сотень символів. Вочевидь, для їх виправлення знадобився б код із довжиною кодової комбінації, яка сягає тисяч чи десятків тисяч розрядів, що технічно здійснити майже неможливо.

Варто наголосити, що на розподіл помилок у каналі впливають не лише зміни швидкості передавання чи потужності сигналу. Насправді характер зазначених помилок істотно залежить від використовуваного модема. Тому вибір модема і коду слід розглядати як єдине завдання, маючи на меті знайти оптимальне його розв'язання.

З'ясувавши характеристики каналу зв'язку, подальший вибір коду здійснюють з огляду на ймовірність помилки. За цим параметром обирають коди, в яких імовірність $P_{н.п.}$ невиявлення помилки менша за $P_{п.доп}$ — допустиму ймовірність помилки [7].

Для досягнення заданої швидкості передавання інформації потрібно вибрати код із мінімально достатньою кількістю перевірних розрядів, які забезпечують $P_{н.п}$. При цьому слід запам'ятати, що виявляльні властивості визначаються не тільки кількістю перевірних розрядів, а й видом перевірних співвідношень. Зокрема, для циклічних кодів — твірним поліномом.

Значного поширення набули ***методи відбору кодів***, які базуються на ***моделюванні реальних потоків*** за допомогою ПК для визначення виду перевірних співвідношень чи виду твірного полінома. Окрім того, при виборі коду доводиться враховувати складність і надійність кодувальних та декодувальних пристроїв.

Як показує практика, найкращий код, здатний не лише виявляти, а й виправляти незалежні (поодинокі) помилки і порівняно простий у реалізації, — це **код Хеммінга**, як двійковий, так і узагальнений. Він має також рекомендації міжнародних організацій. Що ж до пакетів і незалежних помилок, то тут за тими самими параметрами перевагу слід надавати **кодам БЧХ**, **Файра** та **Ріда–Соломона** [8].

Проте завадостійке кодування має істотний недолік: воно призводить до збільшення інформаційного масиву. Коефіцієнт такого збільшення для найважливіших оптимальних кодів наведено в таблиці, де подано також відповідні значення ймовірності спотворення одного елемента в лінії (каналі) зв'язку.

Формати повідомлень (блоків) та знаків при передаванні кодованої інформації визначено ГОСТ 13052-74.

Повідомлення — це текст користувача (починаючи зі знака ПТ і закінчуючи знаком КТ), за яким іде послідовність перевірки ПП (один знак).

Повідомлення при передаванні не розбивається на частини, а передається цілим в одному блоці. Максимальна довжина тексту — 80 знаків.

Формат повідомлення: ПТ — 1 знак; текст — 80 знаків; КТ — 1 знак; ПП — 1 знак.

Формат знака: 1 біт — старт; 7 бітів — інформаційні; 1 біт — парність; 2 біти — стоп.

Для виявлення помилок використовується ***матричний код*** (поздовжньо-поперечна перевірка парності). ПП формується додаванням за модулем 2 інформаційних розрядів, які містяться на однойменних позиціях, та всіх знаків блока, окрім ПТ. Наприкінці йде розряд перевірки на парність (згідно з ГОСТ 28082-89, розділ 1).

Повідомлення при ***кодонезалежному передаванні*** складається з тексту (починаючи зі знака ПТ і закінчуючи знаком КТ), за яким іде ПП — 2 знаки. Після знака ПТ передається показник L довжини тексту — 1 знак.

Вказівка щодо довжини тексту користувача забезпечує можливість прозорого передавання інформації в довільному коді.

Повідомлення не розбивається на частини, а передається одним блоком. Максимальна довжина тексту — 150 знаків.

Формат повідомлення: ПТ — 1 знак; L — 1 знак; текст — 150 знаків; КТ — 1 знак; ПП — 2 знаки.

Формат знака: 1 біт — старт; 8 бітів — інформаційні; 2 біти — стоп.

Для виявлення помилок має використовуватися циклічний код із поліномом $X^{16} + X^{12} + X^5 + 1$.

Формування ПП — згідно з ГОСТ 28082-89.

Коефіцієнт збільшення інформаційного масиву

Імовірність спотворення (передавання з помилкою) одного елемента в лінії (каналі) зв'язку	Кратність помилки	Код, рекомендований для захисту інформації від помилок	Коефіцієнт збільшення інформаційного масиву (при $k = 8$)
$1 \cdot 10^{-4}$	1	Хеммінга ($d = 3$), циклічний ($d = 3$), систематичний ($d = 3$)	1,50 1,50 1,50
	2	Систематичний ($d = 5$), БЧХ ($d = 5$)	2,25 2,58
$0{,}5 \cdot 10^{-3}$	1	Хеммінга ($d = 3$), циклічний ($d = 3$), систематичний ($d = 3$)	1,50 1,50 1,50
	2	Систематичний ($d = 5$), БЧХ ($d = 5$), компаундний ($d = 5$)	2,00 1,84 2,30
$1 \cdot 10^{-3}$	1	Хеммінга ($d = 3$), циклічний ($d = 3$), систематичний ($d = 3$)	1,50 1,50 1,50
	2	Систематичний ($d = 5$), компаундний ($d = 5$), БЧХ ($d = 5$)	2,25 2,35 2,58
$0{,}5 \cdot 10^{-2}$	2	Систематичний ($d = 5$), Файра ($d = 5$), БЧХ ($d = 5$), компаундний ($d = 5$)	2,25 1,39 2,58 3,52
	3	БЧХ ($d = 7$), Файра ($d = 7$), компаундний ($d = 7$), узагальнений код Хеммінга, Ріда – Соломона	3,87 1,59 3,69 1,87 2,37
	4	Ріда – Соломона	2,00
	5	БЧХ ($d = 11$)	3,87
$1 \cdot 10^{-2}$	2	Систематичний ($d = 5$), БЧХ (d=5), Ріда – Соломона	2,25 2,58 1,87
	3	Узагальнений код Хеммінга, БЧХ ($d = 7$)	1,87 3,87
	4	Ріда – Соломона	2,00
	5	БЧХ ($d = 11$)	2,82
	6	Ріда – Соломона	2,625

Розглянемо, наприклад, використання ***компаундних кодів***, обчисливши довжину кодової комбінації (як добуток кількості знаків на кількість інформації в одному знаку) для двох варіантів.

Перший варіант: 83 · 11 біт = 913 (біт).

Поділимо кодову комбінацію на три частини: 913 : 3 ≈ 305 (інформаційних елементів). При цьому можна використати два стандартні варіанти компаундного коду.

1. Беремо компаундний код (n; k) — (381; 325), здатний виправляти поодинокі помилки (a = 9) та пачки помилок завдовжки b = 25.

Обчислюємо коефіцієнт збільшення частини масиву:

$$K_{\text{зб.мас1}} = n/k = 381/325 = 1{,}172,$$

а також коефіцієнт збільшення всього масиву загалом:

$$K_{\text{зб.мас.заг}} = 1{,}172 \cdot 3 = 3{,}52.$$

2. Беремо компаундний код (n; k) — (381; 311), здатний виправляти поодинокі помилки (a = 13) та пачки помилок завдовжки b = 30.

Обчислюємо коефіцієнт збільшення частини масиву:

$$K_{\text{зб.мас1}} = n/k = 381/311 = 1{,}23,$$

а також коефіцієнт збільшення всього масиву загалом:

$$K_{\text{зб.мас.заг}} = 1{,}23 \cdot 3 = 3{,}69.$$

Обираємо варіант 2, що виправляє більшу кількість поодиноких помилок і пачок помилок.

Другий варіант: 155 ·11біт = 1705 (біт).

Поділимо кодову комбінацію на дві частини: 1705 : 2 ≈ 853 (інформаційні елементи). При цьому можна використати два стандартні варіанти компаундного коду.

1. Беремо компаундний код (n; k) — (1023; 872), здатний виправляти поодинокі помилки (a = 21) і пачки помилок завдовжки b = 72.

Обчислюємо коефіцієнт збільшення частини масиву:

$$K_{\text{зб.мас1}} = n/k = 1023/872 = 1{,}173,$$

а також коефіцієнт збільшення всього масиву загалом:

$$K_{\text{зб.мас.заг}} = 1{,}173 \cdot 2 = 2{,}35.$$

2. Беремо компаундний код (n; k) — (1023;888), здатний виправляти поодинокі помилки (a = 19) та пачки помилок завдовжки b = 64.

Обчислюємо коефіцієнт збільшення частини масиву:

$$K_{\text{зб.мас1}} = n/k = 1023/888 = 1{,}152,$$

а також коефіцієнт збільшення всього масиву загалом:

$$K_{\text{зб.мас.заг}} = 1{,}152 \cdot 2 = 2{,}3.$$

Обираємо варіант 1, що виправляє більшу кількість поодиноких помилок і пачок помилок, маючи коефіцієнт збільшення масиву, що всього на 0,05 перевищує відповідний коефіцієнт для варіанта 2.

Література

1. ***Теория*** *кодирования / [Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки]; пер. с япон.— М.: Мир, 1978.— 418 с.*

2. ***Кларк, Дж.-мл.*** *Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк мл., Дж. Кейн; пер. с англ.— М.: Радио и связь, 1987.— 392 с.*

3. ***Элементы*** *теории передачи дискретной информации / [Л. М. Пуртов, А. С. Замрий, А. И. Захаров, В. М. Охорзин]; под. ред. Л. П. Пуртова.— М.: Связь, 1972.— 232 с.*

4. ***Зюко, А. Г.*** *Помехоустойчивость и эффективность систем связи.— М.: Связь, 1986.— 280 с.*

5. ***Блейхут, Р.*** *Теория и практика кодов, контролирующих ошибки / Р. Блейхут.— М.: Мир, 1986.— 576 с.*

6. ***Берликэмп, Э.*** *Алгебраическая теория кодирования / Э. Берликэмп; пер. с англ.— М.: Мир, 1972.— 478 с.*

7. ***Жураковський, Б. Ю.*** *Оцінювання ефективності завадостійких кодів для інформаційних каналів систем управління / Б. Ю. Жураковський // Зв'язок.— 2010.— № 2.— С. 41–43.*

8. ***Жураковський, Б. Ю.*** *Підвищення ефективності захисту інформації від помилок в інформаційних мережах / Б. Ю. Жураковський // Зв'язок.— 2013.— № 1.— С. 19–22.*

Б. Ю. Жураковский

ИСПОЛЬЗОВАНИЕ КОМПАУНДНЫХ КОДОВ ДЛЯ ПЕРЕДАЧИ ДАННЫХ

Предлагается оценка эффективности помехоустойчивых, в частности компаундных, кодов для информационных каналов по вероятности выявления и вероятности исправления ошибок различной кратности, а также по коэффициенту увеличения информационного массива.

Ключевые слова: помехоустойчивые коды; кодовая комбинация; компаундный код; коэффициент повышения достоверности; коэффициент увеличения информационного канала.

B. Yu. Zhurakovsky

THE USAGE OF A COMPOUND OF CODES FOR DATA TRANSMISSION

In the article was proposed an evaluation of the effectiveness of error-correcting codes for the data channels, in particular compound codes, with the probability of detection and probability of correcting errors of different multiplicities, and the magnification information of the array.

Keywords: error-correcting codes; combination; compound code; the rate of increase of reliability; the magnification information of the channel.