УДК 519.15:621.372

О. Різник, Б. Балич , Ю. Нога, Д. Скрибайло-Леськів
Національний університет “Львівська політехніка”,
кафедра автоматизованих систем управління

ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ НА ОСНОВІ ШУМОПОДІБНИХ КОДІВ

Розглянуто перетворення інформації на основі шумоподібних кодів для кодування інформації. Розроблено методику побудови кодових комбінацій чисел на основі теорії числових в’язанок, що дає можливість представлення кодових комбінацій чисел у вигляді шумоподібного коду.

Ключові слова: в’язанка, кодування, лінійка Голомба, шумоподібний код.

In the article transformations of information are examined on the basis of noise codes for realization of code of information. The worked out methods of construction of code combinations of numbers are on the basis of theory of numerical bundles, which enables presentation of code combinations of numbers as a noise code.

Keywords: bundle, code, Golomb ruler, noise code.

Вступ

Головною проблемою сучасної теорії і техніки зв'язку і радіоуправління є підвищення завадозахищеності систем телекомунікацій і, особливо, командних радіоліній управління, в умовах впливу як природних завад, так і створюваних супротивником штучних завад. Одна з основних концепцій підвищення завадозахищеності, що розробляється в цій роботі, полягає в тому, щоб оперативно змінювати робочі ансамблі кодів, збільшуючи тим самим завадостійкість, енергетичну і параметричну прихованість роботи системи зв'язку, а також захист інформації від несанкціонованого доступу. У цій роботі з метою підвищення завадозахищеності сучасних інформаційних систем розроблено регулярний і конструктивний метод синтезу повних класів лінійних і нелінійних систем шумоподібних кодів, що дало змогу істотно підвищити параметричну прихованість і захист інформації від несанкціонованого доступу.

Науково-технічною основою появи сучасних телекомунікаційних мереж є забезпечення максимальної пропускної спроможності систем передачі C за наявної смуги пропускання лінії зв’язку ΔF відповідно до формули Найквіста, одержаної з використанням теореми В.О. Котельнікова:

$$C = 2\Delta F \log M \text{ , [біт/с]}, \qquad (1)$$

де M – кількість дискретних значень сигналу.

Ця формула справедлива за умов відсутності шумів в лінії зв’язку. Практично в лінії зв’язку існують завади (шуми), що призводять до помилок при передачі інформації. Тоді максимальна пропускна спроможність системи передачі визначатиметься формулою Шеннона:

$$C = \Delta F \log\left(1+\frac{P_c}{P_ш}\right) \text{ , [біт/с]}, \qquad (2)$$

де P_c, $P_ш$ – середня потужність коду та завад (шумів).

Важливою вимогою для цифрових систем передачі є забезпечення максимальної завадостійкості систем, яка залежить також від виду використаної модуляції (найкращу завадостійкість забезпечує багатопозиційна частотна маніпуляція). Для підвищення завадостійкості систем передачі використовують завадостійке кодування, за якого до інформаційного повідомлення додають зайві перевіркові біти для виправлення помилок, що однак призводить до розширення спектра сигналу.

Найпоширеніші блокові коди БЧХ (Боуза–Чоудхурі–Хоквенгема), коди Ріда–Соломона, а також безперервні згорткові коди з декодуванням їх за алгоритмом Вітербі.

Постановка проблеми

Особливо цікавим є об'єднання методів кодування і шифрування. Можна стверджувати, що, по суті, кодування – це елементарне шифрування, а шифрування – це елементарне завадостійке кодування. Розроблення і реалізація таких універсальних методів – перспектива сучасних інформаційних систем.

Особливість шумоподібних кодів полягає в тому, що створюється шумоподібний спектр кодової послідовності (найбільш наближена до псевдовипадкової послідовності), а їх взаємна кореляція мінімальна. Найкращим кодом для створення шумоподібної послідовності є код Баркера, але він має велику надлишковість. Для її зменшення побудуємо шумоподібні коди на основі лінійок Голомба.

Корисною особливістю систем з шумоподібним сигналом є їх високі конфіденційність і завадостійкість, особливо до вузькосмугових завад. В основу техніки шумоподібних кодів покладено використання в каналі зв'язку для перенесення інформації декількох реалізацій цих кодів, які на прийомі розділяють за допомогою селекції їх послідовності.

При цьому безпомилково виявити такі коди можна, вводячи надмірності, тобто використовуючи для передавання повідомлень послідовності істотно надлишкової, ніж займає передаване повідомлення.

Перевагою шумоподібного коду є можливість застосовувати новий вигляд селекції – за допомогою послідовності. Цікавою особливістю систем з шумоподібними кодами є її адаптивні властивості – із зменшенням числа завад завадостійкість зростає.

Недоліком є перехід до складнішого носія інформації, що приводить, природно, до відомого ускладнення систем передачі повідомлень.

Розв’язання поставленої задачі

Слабке місце багатьох систем кодування – це статистична слабкість коду, тобто, аналізуючи статистику за деякий період, можна дійти висновку, що це за система і тоді діяти більш цілеспрямовано. Тобто різко скорочується час пошуку ключа. Ця система оперує шумоподібними кодами, які за своїми властивостями, зокрема і статистичний, практично ідентичні білому шуму Гаусса.

Властивості цих послідовностей:

- у кожному періоді послідовності число 1 і 0 відрізняється не більш, ніж на одиницю;
- серед груп з послідовних 1 і 0 в кожному періоді половина має тривалість в один символ, четверта частина має тривалість в два символи, восьма частина має тривалість в чотири символи і так далі.
- кореляційна функція послідовності має єдиний значний пік амплітуди 1 і при всіх зрушеннях дорівнює $1/m$ (m – довжина послідовності).
- кореляцію між векторами обчислюють за формулою:

$$\rho(\chi, y) = \frac{A - B}{A + B} \quad , \tag{3}$$

де A – число позицій, в яких символи послідовностей x і y збігаються; B – число позицій, в яких символи послідовностей x і y різні.

У математиці оптимальною лінійкою або лінійкою Голомба називають набір невід’ємних цілих чисел, розташованих у вигляді поділок на уявній лінійці так, що відстань між будь-якими двома поділками є унікальною. Іншими словами, за всією довжиною лінійки не можна знайти два числа, різниця між якими повторювалася б двічі [1, 2].

Число поділок на лінійці Голомба називають її порядком, а найбільшу відстань між двома її поділками – довжиною. Інколи лінійки Голомба описуються відстанями між сусідніми поділками, а не абсолютними координатами поділок. Максимальне число пар, які можна скласти з поділок лінійки порядку n, дорівнює:

$$\binom{n}{2} = \frac{n(n-1)}{2} . \tag{4}$$

Тому в канонічному представленні лінійки Голомба найменша поділка відповідає нульовій координаті, а наступна за ним поділка розташовується на найменшій з двох можливих відстаней. Зовсім не обов'язково, що лінійка Голомба здатна виміряти всі відстані в межах її довжини, проте якщо це так, то таку лінійку називають досконалою. Проте, досконалі лінійки існують лише для порядків, менших п'яти.

Лінійку Голомба називають оптимальною, якщо не існує коротших лінійок того ж порядку. Іншими словами, лінійка називається оптимальною, якщо значення її останньої поділки мінімально можливе [1].

При проведенні досліджень на послідовності елементів кожній j -й упорядкованій парі чисел (p_j,q_j); $p_j,q_j \in \{1,2,...,N\}$ ставиться у відповідність сума $L_j = L(p_j,q_j)$ на послідовності цілих додатних чисел $K_N = (k_1,k_2,...,k_i,...,k_N)$ (табл. 1):

$$L_j = L(p_j,q_j) = \sum_{i=p_j}^{q_j} k_j \ , \ p_j \le q_j \tag{5}$$

Таблиця 1

Значення можливих сум для N елементів лінійки Голомба

				q_j				
p_j	1	2	...	$l-1$	l	...	$N-1$	N
1	k_1	k_2	...	k_{l-1}	k_l	...	k_{N-1}	k_N
2		$\sum_{i=1}^{2} k_i$	...	$\sum_{i=1}^{l-1} k_i$	$\sum_{i=1}^{l} k_i$	...	$\sum_{i=1}^{N-1} k_i$	$\sum_{i=1}^{N} k_i$
...				...	...	...	...	...
$l-1$				$\sum_{i=l-1}^{l} k_i$	$\sum_{i=l-1}^{l} k_i$	...	$\sum_{i=l-1}^{N-1} k_i$	$\sum_{i=l-1}^{N-1} k_i$
l					$\sum_{i=l-1}^{l} k_i$	...	$\sum_{i=l}^{N-1} k_i$	$\sum_{i=l}^{N} k_i$
...								...
N								$\sum_{i=N-1}^{N} k_i$

Максимально можлива кількість L_N сум на послідовності чисел, значення яких відрізняються між собою, визначається тривіальною залежністю:

$$L_N = \frac{N(N+1)}{2}. \tag{6}$$

У загальному випадку простою лінійкою Голомба порядку N на послідовності N чисел називається така послідовність $K_N = (k_1, k_2, ..., k_i, ..., k_N)$, на якій суми набувають значень всіх L_N чисел, починаючи зі заданого числа. У простішому варіанті ці суми вичерпують значення чисел натурального ряду $1, 2, ..., L_N$.

Одним з практичних використань лінійки Голомба є використання її у фазованих антенних решітках радіоантен, наприклад, у радіотелескопах. Антени з конфігурацією [0 1 4 6] можна зустріти в базових станціях стільникового зв'язку стандарту CDMA.

Ми ж використаємо лінійки Голомба для генерації шумоподібних кодів, оскільки лінійка Голомба за визначенням повинна мати всі різні відліки, а при великих величинах її довжини вона стає подібною на послідовність шумоподібних кодів за їх визначенням [3].

Запропонований метод побудови шумоподібних кодів заснований на перетворенні лінійок Голомба.

Для побудови шумоподібних кодів за допомогою лінійок Голомба порядка N кратності R виділимо рядок із L_N пронумерованих у зростаючому порядку клітинок одновимірного масиву і заповнимо інформаційними "одиницями" клітинки, номери яких збігаються з числами, визначеними з лінійки Голомба. У клітинки, що залишилися незаповненими, занесемо "нулі". Утворена послідовність одиниць і нулів є L_N-розрядним шумоподібним кодом, циклічним зсувом якого можна одержати й решту дозволених комбінацій.

Прикладом такого коду є таблиця кодових комбінацій, складена за допомогою лінійки Голомба порядка $N=7$ кратності $R=1$ (табл. 2):

0 1 4 10 18 23 25.

Таблиця 2

Шумоподібні коди на основі лінійки Голомба з $N=7$ та $R=1$

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

Будь-яка з L_N різних кодових комбінацій шумоподібного коду містить точно N одиничних символів в однойменних розрядах, що випливає з властивостей лінійки Голомба. Решта $L_N - N$ кодових комбінацій шумоподібного коду містять нулі [2].

Мінімальну кодову відстань для цього шумоподібного коду визначають як:

$$d_{\min} = 2(N\text{-}2) \tag{7}$$

Число помилок, які можна виявити t_1, і число помилок, що можна виправити t_2 за допомогою шумоподібного коду, визначають за мінімальною кодовою відстанню:

$$t_1 \le d_{\min} - 1 \tag{8}$$

$$t_2 \le (t_1 - 1)/2 \tag{9}$$

Формули для визначення кількості помилок, які можуть бути виправлені t_2 або виявлені t_1 за допомогою описаного шумоподібного коду:

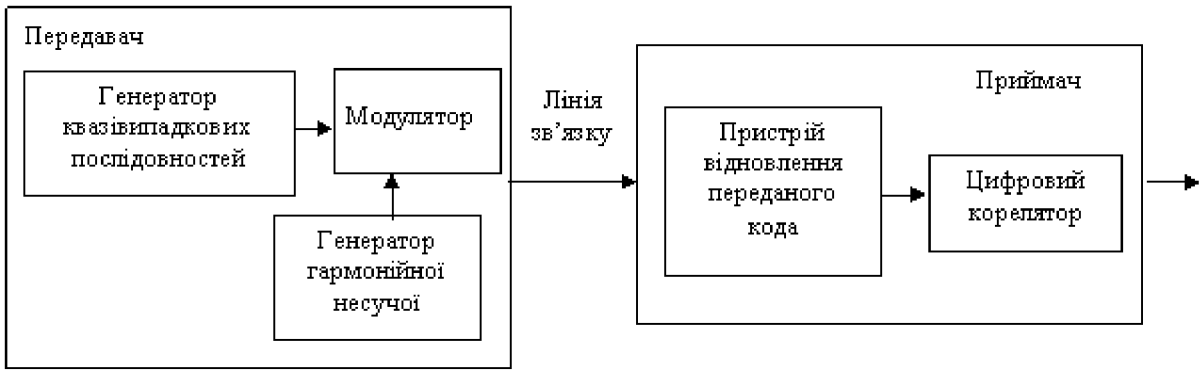
$$t_1 \le 2N - 5, \tag{10}$$

$$t_2 \le N - 2 \tag{11}$$

У розглянутих випадках значення параметрів L_N і N не пов'язані між собою будь-якою аналітичною залежністю і можуть вибиратися довільно. При цьому виникає питання про встановлення оптимального співвідношення між L_N і N, за дотримання якого розглянутий шумоподібний код набуває додаткових переваг. Завадостійкість шумоподібного коду зростає зі збільшенням N за умови мінімізації довжини лінійки Голомба L_N.

Побудовані за допомогою лінійок Голомба шумоподібні коди дають змогу виявляти до $2N-5$ або виправляти до $N-2$ помилок.

Структурну схему системи приймання-передавання інформації з використанням шумоподібних кодів наведено на рисунку.



Структурна схема системи приймання-передавання інформації з використанням шумоподібних кодів

Основними апаратурними частинами приймально-передавальної системи, які дають змогу відтворити переваги шумоподібних кодів, є генератор квазівипадкових послідовностей (КВП) (у нашому випадку лінійок Голомба) і цифровий корелятор. Генератор квазівипадкових послідовностей визначає структуру шумоподібного коду, а цифровий корелятор здійснює узгоджений за структурою сигналу прийом.

Генератори КВП прості в апаратурному виконанні. Можна сказати, що генератори шумоподібного коду не утруднюють апаратну реалізацію, а самі шумоподібні коди мають добрі потенційні можливості для удосконалення трактів приймання-передавання.

Розроблено програмний продукт для кодування та декодування з виправленням помилок за допомогою шумоподібних послідовностей, де необхідно задати:

- вхідні дані (елементи шумоподібної послідовності);
- кількість помилок, які знаходяться та виправляються;
- шлях до файла, який необхідно закодувати та декодувати на основі шумоподібної послідовності.

Висновки

Шумоподобні коди належать до безлічі з украй нерегулярною розгалуженою структурою. Основні поняття теорії поки що знаходяться в процесі становлення та розвитку, але поле їх застосування безперервно розширюється. Великий інтерес до цих кодів пов'язаний з тим, що їх аналоги, такі як квазікоди Баркера, лінійки Голомба, числові в'язанки використовують у реальних завданнях, причому в типових, а не в екзотичних ситуаціях.

Дослідження різних типів шумоподібних кодових послідовностей свідчить про переваги тих із них, які синтезовані на основі лінійок Голомба, що дає змогу досягти більшої криптостійкості та завадостійкості при перетворенні інформації порівняно з класичними шумоподібними кодовими послідовностями.

Розроблено алгоритм та програму спрощеного синтезу завадостійкої шумоподібної кодової послідовності на основі лінійок Голомба та створення ефективного алгоритму кодування і декодування інформації. Дослідження показують, що використання шумоподібних кодових послідовностей на основі лінійок Голомба в задачах перетворення інформації забезпечує простоту апаратурного застосування.

1. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів, 1989. 2. Різник В.В., Різник О.Я., Кісь Я.П., Дурняк Б.В., Парубчак В.О.. Використання монолітних кодів в інформаційних технологіях. МНТК ISDMIT'2006. – Євпаторія. – Т. 2. – С. 39–42. 3. Різник О.Я., Балич Б.І. Використання числових лінійок-в'язанок для кодування інформації // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні науки та інформаційні технології", 2006. – С. 62–64.

УДК 681.3:519.15

В. Різник
Національний університет "Львівська політехніка"»,
кафедра автоматизованих систем управління,
Технологічно-природничий університет м. Бидґощ (Польща)

ПРОБЛЕМА ПОДОЛАННЯ НАДМІРНОСТІ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

Розглянуто новий підхід до розроблення інформаційних технологій та систем управління з поліпшеними якісними показниками, що ґрунтується на використанні ідеї оптимальних структурних пропорцій, що випливає з властивостей гармонізованого простору-часу.

The new approach for developing information technologies and control systems with improved quality factors based on the idea of optimum structural proportions, which follows from properties of harmonized space and time, is prospected in the paper.

Вступ

Під надмірністю системи взагалі розуміють перевищення обсягу сигналів або міри складності структур системи порівняно з їхніми мінімальними значеннями, необхідними для того, щоб виконати поставлене завдання. Коли систему розглядають на рівні технічної реалізації, тоді основними видами надмірності системи є сигнальна й структурна надмірності. На абстрактному рівні говорять про інформаційну надмірність системи, тобто про надмірність у кількості інформації, яку переробляють, і про алгоритмічну надмірність системи, тобто надмірність у складності алгоритму функціонування системи. Розрізняють штучну й природну надмірності. Проблема надмірності системи пов'язана з трьома основними завданнями: 1) введенням штучної надмірності з метою поліпшення основної характеристики системи, наприклад, завадостійкості або точності, надійності тощо; 2) зменшенням природної інформаційної надмірності, щоб спростити систему; 3) раціональним використанням надмірності універсальних багатофункціональних систем у періоди