УДК 004.056.55

С.Г. Рассомахін, Д.М. Гажур

Харківський національний університет імені В.Н. Каразіна, Харків

ПОБУДОВА ПСЕВДОВИПАДКОВОГО КОДУ НА ОСНОВІ ЛІНІЙНИХ ГЕНЕРАТОРІВ М-ПОСЛІДОВНОСТЕЙ

Запропоновано метод побудови завадостійкого псевдовипадкового коду із застосуванням лінійного генератору М-послідовностей з метою вирішення задачі виправлення помилок при передачі даних в високошвидкісних системах зв'язку. Розглядаються властивості притаманні М-послідовностям та процес генерації послідовностей максимальної довжини. Приводиться перелік переваг псевдовипадкового кодування на основі обраного генератору ПВП. Досліджується залежність декодування з помилкою від довжини кодового слова. Результати досліджень отримуються за допомогою імітаційної моделі гаусового каналу при різних співвідношеннях сигнал/шум та наводяться у вигляді діаграм.

Ключові слова: *М-послідовність, послідовність максимальної довжини, кодове слово, генератор ПВП на регістрах зсуву зі зворотнім зв'язком, псевдовипадкове кодування, спектр взаємних відстаней.*

Вступ

На сьогодні розвиток цифрових систем зв'язку здобув значних успіхів, будь-то космічна, супутникова чи мобільна галузі. Подібні системи використовують для передачі даних бездротові канали, в яких на переданий сигнал діють перешкоди різної фізичної природи. Таким чином, прийняті дані з досить великою ймовірністю будуть містити помилки і вони втратять свою цінність для одержувача. В результаті виникає проблема забезпечення надійної передачі цифрової інформації по каналах з шумами. Найважливіший внесок у вирішення даної проблеми вносить теорія завадостійкого кодування. На її основі розробляються методи захисту від помилок, що базуються на застосуванні завадостійких кодів. Використання таких кодів дозволяє отримати енергетичний виграш кодування, який характеризує степінь можливого зниження енергетики передачі при кодуванні в порівнянні з відсутністю кодування, якщо достовірність передачі в обох випадках однакова. Цей виграш можна використовувати для покращення параметрів і характеристик властивостей систем передачі даних.

При фіксованому правилу декодування ймовірність помилки залежить лише від обраного коду. Щоб рідше були помилки декодування, обумовлені шумами, кодові слова бажано обирати за можливістю більш «несхожими», такими, щоб вони знаходилися як можна «далі» одне від одного. З огляду на те, що одночас-

© С.Г. Рассомахін, Д.М. Гажур

но збільшувати «відстань» між кодовими точками α_1 ... α_M неможна без зменшення їх кількості M, то бажано розташовувати кодові точки як можна рівномірніше в просторі X^n значень α. Бажана рівномірність досягається по законам масових явищ при великих M (та n), якщо обирати кодові точки незалежно одне від одного випадковим чином [1].

Досить важливим та далеко не тривіальним є факт того, що середня помилка декодування може бути зроблена шляхом вибору коду як завгодно малої при збільшенні числа символів n, без зменшення рівня шумів в каналі та без зменшення кількості інформації що передається, у розрахунку на один символ [2]. Цей результат був отриманий Шенноном в 1948 році. Обсяг корисно використовуваного для розміщення кодових точок евклідового простору коду, а також середні взаємні відстані з збільшенням довжини блоку наближаються до найкращих значень. Такі коди забезпечують одночасно частотну і енергетичну ефективність [3].

Метою статті є розробка нового методу формування псевдовипадкового коду на основі лінійного генератору послідовностей максимальної довжини (М-послідовностей).

Виклад основного матеріалу

1. Генерація псевдовипадкової послідовності

Загальна схема лінійного генератору, формуючого М-послідовність, приведена на рис. 1. Його основу складає регістр зсуву з тригерами, які здійснюють затримку вхідного символу на один такт тривалістю τ_0. Припустимо, що використовуються p різноманітних символів: 0, 1, 2, …, $p-1$. Символи на виходах тригерів при j-му такті позначені через $x_{1,j}$, $x_{2,j}$, ..., $x_{k,j}$, причому $x_{l,j} \in S$.

Символ на вході першого тригеру позначений як $x_{0,j}$, на виході l-го тригеру на $(j+1)$-му такті $x_{l,j} = x_{l-1,j}$, адже з кожним тактом символ з входу «переходить» на вихід. Символи з виходів тригерів надходять на помножувачі, з яких знімають символи $c_1x_{1,j}$, $c_2x_{2,j}$, ..., $c_kx_{k,j}$, $c_l \in S$.

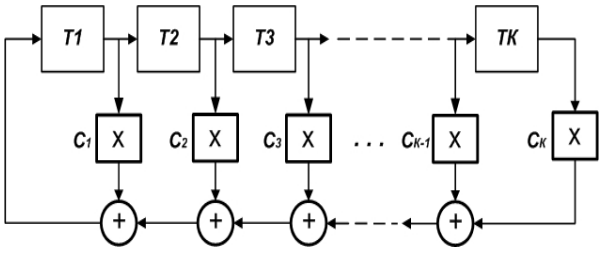


Рис. 1. Лінійний генератор формування М-послідовності

Тому, якщо операція множення в множнику відбувається по модулю $p(\mathrm{mod}\, p)$, то символи $c_l x_{l,j} \in S$.

Суть множення по модулю становиться зрозумілим коли розглядається порівняння двох чисел по третьому числу (модулю). Два цілих числа a та b називаються порівнянними по модулю p, якщо при діленні обох чисел на p їх остатки рівні. Порівняння двох чисел позначається як

$$a \equiv b(\mathrm{mod}\, p). \qquad (1)$$

Залишок від ділення любого числа на p завжди менше p і лежить в межах від 0 до $p-1$. Наприклад, якщо $p=5$, то $12 \equiv 2(\mathrm{mod}\, 5)$, так як залишки від ділення обох чисел дорівнюють нулю. Порівняння (1) говорить про те, що різниця $a-b$ ділиться без залишку. Порівняння двох чисел по модулю p дозволяє записати їх в наступному вигляді: $a = q_1 p + r$, $b = q_2 p + r$, де q_1, q_2 – будь-які цілі числа; r – залишок, $0 \le r \le p-1$. Таким чином, порівняння по модулю p означає переведення довільного цілого числа в кінцеву множину S, що складається з p елементів.

Множення двох чисел по модулю p відбувається наступним чином. Два числа перемножуються, а їх добуток переводиться к кінцеву множину S за допомогою порівняння по модулю p. Множення двох чисел по модулю p записується як $ab = d \equiv$ $\equiv n(\mathrm{mod}\, p)$ при $0 \le r \le p-1$.

Потрібно зазначити, що множення будь-якого числа на нуль означає, що символ на виході множника завжди дорівнює нулеві. Відповідно, множник може бути опущеним. Наприклад, при $p=2$ (символи 0 та 1) множник c_l може приймати значення або 0, або 1, тобто виходи тригерів або підключені до суматорів, або ні. Після множення додавання відбувається також по модулю p. Сума двох цілих чисел переводиться за допомогою порівняння в кінцеву множину S, тобто $a+b=d \equiv r \bmod(p)$ для $0 \le r \le p-1$.

Тепер можна записати, що символ на виході T1 в j-му такті дорівнює

$$x_{0,j} = c_1x_{1,j} + c_2x_{2,j} + \ ... + c_{k-1}x_{k-1,j} + c_kx_{x,j}. \qquad (2)$$

Вираз (2) є лінійним рекурентним рівнянням. Воно дозволяє по відомим k символам на виходах тригерів знайти символ $x_{0,j}$, який в наступному такті перейде на вхід T1.

Аналіз роботи лінійного генератору формування М-послідовності на основі рекурентного рівнян-

ня (2) говорить про те, що його робота повністю визначається характеристичним многочленом

$$f(x) = a_0 x^k + a_1 x^{k-1} + \ \dots\ + a_{k-1} x + a_k,$$

коефіцієнти якого пов'язані з множниками $c_1, \dots, c_k$ співвідношенням:

$$c_n = (-1)^{k+1} a_k. \qquad (3)$$

Від'ємні значення c_n можна звести за допомогою порівняння по модулю p до додатного числа множини S.

Для двійкових М-послідовностей множники c_n та a_n відповідно (3) рівні, тобто $c_n = a_n$, причому $c_0 = a_0 = 1$.

Таким чином, для визначення структури цифрового автомату необхідно знати характеристичний многочлен $f(x)$ степені k, який, по-перше, повинен бути незвідним, тобто його не можна представити у вигляді добутку многочленів менших степенів, а по-друге, він повинен бути первісним (примітивним) відносно двочлена $x^N - 1$ без залишку. Тому характеристичний многочлен є первісним коренем рівняння $x^N - 1$. Якщо характеристичний многочлен є первісним, то він є і незвідним.

Таким чином, для того щоб при заданих N, k та p визначити структуру регістру для формування М-послідовності з періодом $N = p^k - 1$, необхідно в якості характеристичного многочлена взяти первісний многочлен степені k.

Знаючи коефіцієнти a_n, можна однозначно побудувати генератор формування М-послідовностей. Якщо $a_n = c_n = 1$, то вихід n-го тригеру до суматору по модулю 2 не підключений.

2. Побудова псевдовипадкового коду

Зазвичай, методи формування псевдо випадкових кодів зі складною структурою, не є придатними для реального застосування, де кодування та декодування ведеться в реальному часі, адже процес побудови таких кодів буде також складним. В той же час, більшість простих арифметичних генераторів мають свої недоліки, які пов'язані з:

– надто коротким періодом;

– нерівномірним одномірним розподілом;

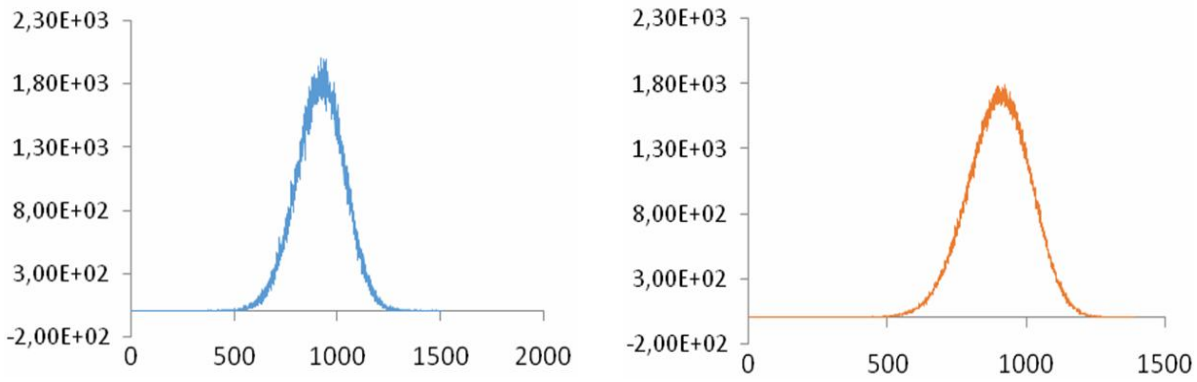
– оберненістю.

В свою чергу метод генерації М-послідовності позбавлений цих недоліків і задовольняє наступним вимогам побудови «хорошого» коду:

– простота та швидкодія;

– рівномірний розподіл чисел в заданому діапазоні;

– відсутні криптографічні властивості, що надають змогу однозначно визначити кодове слово по мінімальній кількості прийнятих символів.



а б

Рис. 2. Спектри взаємних відстаней: а – псевдовипадковий М-код, б – рівномірно випадкового коду

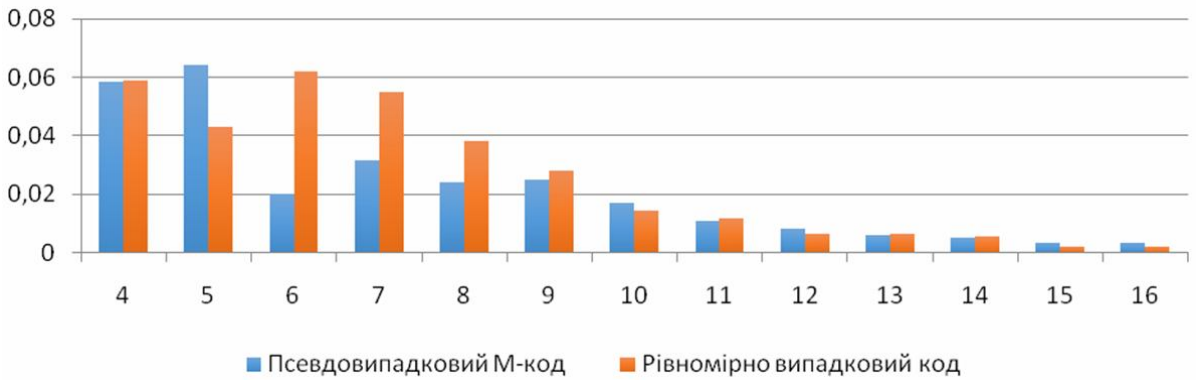


Рис. 3. Діаграма залежносей помилки при декодуванні від довжии кодового слова

Побудова такого коду буде відбуватися в наступний спосіб. Лінійний генератор, розглянутий в попередньому розділі, формує бінарну послідовність з періодом $2^N - 1$ з урахуванням відсутності нульового початкового стану регістрів. Процес формування завадостійкого коду базується на основі такої техніки кодування, як пряма корекція помилок (FEC).

Додавання надлишкової службової інформації відбуватиметься наступним чином. Дані, що подаються на вихід кодуючого пристрою, представляються у вигляді двійкових чисел по k біт. Кожне таке число виконує роль початкового стану для генератору М-послідовностей і є першим символом кодового слова.

Проініціалізований генератор формує бінарну послідовність довжиною $k \cdot (l-1)$, де l – кількість символів (чисел) в кодовому слові. Таким чином відбувається кодування k біт даних.

Для того щоб переконатися в правильності вибору генератору ПВП, на рис. 2 приведено спектри взаємних відстаней кодових точок побудованих запропонованим методом та за допомогою рівномірно випадкового коду.

Наведені результати отримані статистично шляхом обчислення щільності ймовірностей розподілу відстані між парою кодових точок у полі Пуассона за наступних умов:

– незвідний поліном: $x^{16} + x^{15} + x^{14} + x^4$;

– $k = 10$;

– $l = 10$.

Найменше значення спектрів відповідає мінімальним відстаням кодів, а значення спектру в цій точці є середнє число точок коду, що розташовуються на відстані поблизу довільно обраної точки.

Таким чином, коди, отримані за допомогою лінійного генератору М-послідовностей (рис. 2, а), за видом спектру взаємних відстаней нічим не поступаються рівномірно випадковими. Що остаточно переконатися в істині цього твердження, на рис. 3 приведено діаграму залежностей ймовірності декодування з помилкою від довжини кодового слова в умовах гаусового шуму зі спектральною щільністю шуму $N0 = 0,25$.

Висновки

Шляхом порівняння характеристик псевдо випадкового коду отриманих за допомогою генератору М-послідовностей з рівномірно випадковим кодом та аналізу поведінки такого коду за однакових умов в каналі з гаусовим шумом, було доведено цілком можливе використання запропонованого методу побудови завадостійкого коду.

Список літератури

1. Стратонович Р.Л. Теория информации / Р.Л. Стратонович. – М.: Сов радио, 1957. – 424 с.

2. Математическая теорія святи, 1948. – В кн.: К. Шеннон, Работы по теории информации и кибернетике.. – М.: ИЛ, 1963.

3. Рассомахін С.Г. Лінійне цілочисельне декодування псевдовипадкових кодів на основі методу відсікань гоморі / С.Г. Рассомахін // Обробка інформації в складних технічних системах, 2011. – С. 42-47..

4. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков – М.: КУДИЦ-ОБРАЗ, 2003. – 238 с.

Надійшла до редколегії 3.03.2014

Рецензенти: д-р техн. наук, проф. А.В. Бастєєв, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ПОСТРОЕНИЕ ПСЕВДОВИПАДКОВОГО КОДА НА ОСНОВЕ ЛИНЕЙНЫХ ГЕНЕРАТОРОВ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

С.Г. Рассомахин, Д.Н. Гажур

Предложен метод построения помехостойкого псевдослучайного кода с применением линейного генератору М-последовательностей с целью решения задачи исправления ошибок при передаче данных в высокоскоростных системах связи. Рассматриваются свойства, присущие М-последовательностям и процесс генерации последовательностей максимальной длины. Приводится перечень преимуществ псевдослучайной кодировки на основе избранного генератора ПВП. Исследуется зависимость декодирования с ошибкой от длины кодового слова. Результаты исследований получаются с помощью имитационной модели гаусового канала при разных соотношениях сигнал/шум и приводятся в виде диаграмм.

Ключевые слова: *М-последовательность, последовательность максимальной длины, кодовое слово, генератор ПВП на регистрах сдвига с обратной связью, псевдослучайная кодировка, спектр взаимных расстояний.*

CONSTRUCTION OF PSEUDO-RANDOM CODE BASED ON THE LINEAR GENERATOR OF M-SEQUENCES

S.G. Rassomakhin, D.M. Gazhur

The method of construction noise immunity pseudo-random code using a linear generator M-sequences in order to solve the problem of error correction in the transmission of data in high speed communication systems. The properties inherent in the M-sequences and generation of maximal length sequences are considered. Is given a list of benefits pseudo-random coding based on the selected generator pseudo-random sequences. The dependence of decoding error on the length codeword. The research results obtained by the simulation model Gaussian channel with different signal/noise ratio and are in the form of graphs.

Keywords: *M-sequence, the sequence of maximal length code, code word, pseudo-random sequence generator based on the linear feedback shift registers, pseudo-random coding, spectrum of mutual distances.*