УДК 621.372 .54

ХАРАКТЕРИСТИКИ БАГАТОРІВНЕВИХ ПСЕВДОВИПАДКОВИХ СИГНАЛІВ

Демчук В.В., Трофимюк Р.М.
Тернопільський національний економічний університет, магістри

Останнім часом значного поширення та розвитку набули телекомунікаційні системи на базі шумоподібних сигналів. Вони широко використовуються практично в усіх сучасних засобах радіозв'язку (GSM, CDMA, WiFi), системах супутникової навігації (GPS, ГЛОНАСС, Galileo), а також в безпровідних сенсорних мережах (ZigBee, та інш.). В даних системах використовуються часто використовуються коди Баркера, М-сигнали та інші., проте актуальним є підвищення: завадозахищеності та швидкості передавання інформації, а тому пошук та дослідження нових типів шумоподібних сигналів є актуальною та перспективною науковою задачею.

В статтях [1,2] показано, що перспективним напрямком галузі завадостійкого передавання інформації є використання в якості ШПС М-послідовності з основою p>2. Це дозволяє підвищити імовірність правильного розпізнавання сильно зашумлених сигналів, та збільшити степінь захисту інформації.

Розглянемо багаторівневі М-послідовності на прикладі полів Галуа. Поле - це множина не менше ніж з двох елементів, над якими задана пара бінарних операцій, званих "додаванням" і "множенням" і володіючих тією властивістю, що для них існують зворотні операції: віднімання і ділення (окрім ділення на нуль), причому множення дистрибутивне щодо додавання.

В даному випадку нас цікавлять поля Э. Галуа (E.Galois, 1811-1832) [3], що містять кінцеве число елементів $K = \{ 0, 1, 2, ..., q - 1 \}$. Проте не для будь-якого числа елементів можна підібрати такі операції, що система $\{ K; +, \bullet \}$ є полем. Кінцеві поля позначаються GF(p^r), та існують лише порядку (з числом елементів) p^r, де p - просте число (характеристика поля), r — натуральне число (розмірність поля). При $r = 1$ маємо просте поле GF(p) з розглянутими вище модулярними операціями додавання і множення. Якщо ж p - складове число, то система $\{K;+,\bullet\}$, де додавання і множення — модулярні операції, не є полем: ця система утворює так зване кільце, в якому ділення навіть на ненульовий елемент можливо не завжди.

В будь-якому полі множина К всіх елементів утворює по операції складання циклічну (адитивну) групу; аналогічно множина Ко ненульових елементів утворює по операції множення циклічну (мультиплікативну) групу. Поле GF(p^r) називається розширенням поля GF(p).

Генерація елементів поля GF(p^r). Кінцеві поля GF(p^r) порядку p^r, де характеристика p — просте число, а розмірність r — натуральне число, породжуються за допомогою непривідних поліномів ступені r. Особливо зручно використовувати примітивні поліноми $\pi(x)$; в цьому випадку просте поле GF(p) може бути розширено до поля GF(p^r) за рахунок приєднання кореня α полінома π(x), тобто за допомогою порівнянь по двох модулях p і $\pi(x)$. З різних варіантів перевага була віддана поліномам $\pi(x)$ з мінімальним числом ненульових коефіцієнтів, а при рівності цього числа - поліномам, що мають ненульові коефіцієнти при менших ступенях змінної x. Наприклад, для $p = 2$ з двох примітивних поліномів, що не приводяться, третього ступеня $\pi(x) = x^3 + x^2 + 1$ і $\pi(x) = x^3 + x + 1$ вибирається останній.

Алгоритм послідовного утворення елементів розширеного поля GF(2^r) полягає в наступному:

1) корінь α полінома $\pi(x)$ вибрати як примітивний елемент поля, тобто прийняти $\pi(x) = 0$, звідки слідує $x^r = f(x)$;

2) елементи поля $N \in \{ 0, 1, 2, .., (r - 1), r\}$ зіставити із степенями α^{N-1} і двійковими комбінаціями з r компонент:

3) елементи поля $N \in \{ (r + 1), (r + 2) ... (2^r - 1)\}$ отримати один за одним шляхом зсуву вліво попередній комбінації для N-1.

Заміна бінарних лінійних рекурентних послідовностей максимальної довжини (М-послідовностей) на багаторівневі послідовності з основою p >2, де p – просте число, дозволяє вирішити задачу збільшення ансамблю кодуючих сигналів в багатокористувацьких асинхронних системах та системах криптографічної обробки інформації [7]. Для визначення характеристик систем кодування інформації із багаторівневими кодуючими М-послідовностями необхідний аналіз структурних та кореляційних властивостей М-послідовностей з основою $p > 2$. На рис.1, рис.2 наведено графіки автокореляційної функції з основою 5 та 11 відповідно.

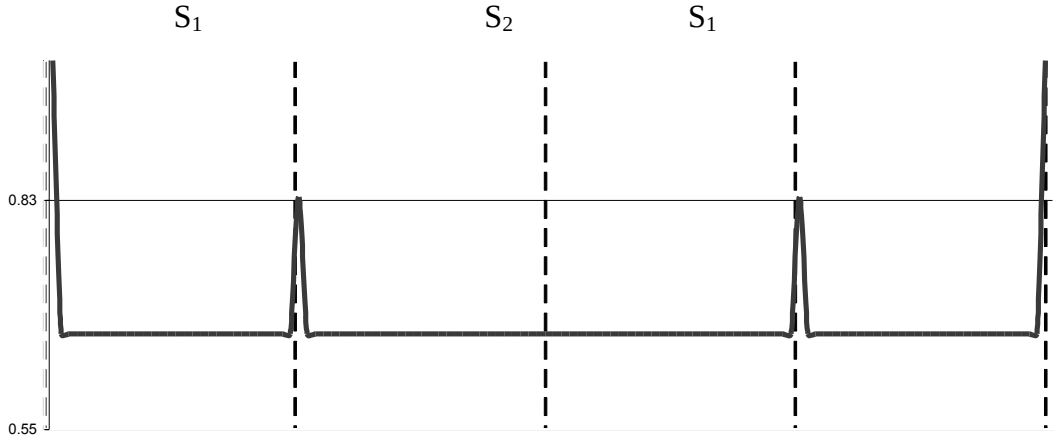

Рисунок 1 - Графік автокореляційної функції для полінома з основою 5

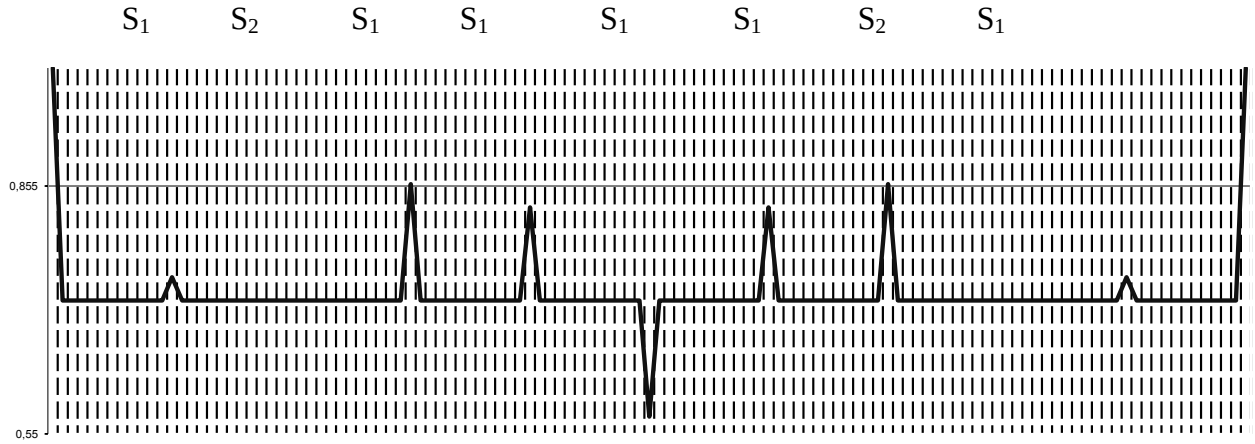

Рисунок 2 - Графік автокореляційної функції для полінома з основою 11

Графіки функцій автокореляції для М-послідовностей з основами $p = 5$ та $p = 11$, відрізняються від автокореляційних функцій бінарних М-послідовностей двома факторами:

1) базовий рівень В функцій автокореляції багаторівневих М-послідовностей перевищує значення 0,5, характерне для автокореляційних функцій бінарних М-послідовностей;

2) в автокореляційних функціях багаторівневих М-послідовностей з'являються бокові додатні та від'ємні пелюстки, амплітуди яких є відповідно більшими та меншими за базовий рівень.

Проте застосування розглянутих М-послідовностей з основою $p>2$ для завадостійкого кодування має недолік – потрібно використовувати канал зв'язку з широкою смугою пропускання, тому в деяких випадках може бути недоцільним застосування такої системи передавання, оскільки, якщо наприклад в якості каналу зв'язку використовується провідна лінія, то широкосмугова лінія вимагає значних економічних затрат.

Список використаних джерел

1. В.М.Галів, С.М. Іщеряков, Т.П.Каюк Властивість серій для багаторівневих М-послідовностей // Вимірювальна та обчислювальна техніка в технологічних процесах: Зб.наукових праць:-Хмельницький : ТУП. – 2002. – Т.1,№ 9.- С154-156.
2. В.М.Галів, С.М. Іщеряков, Т.П.Каюк Структурні властивості багаторівневих М-послідовностей. // Комп'ютерне моделювання та інформаційні технології в науці, економіці та освіті: Зб. наукових праць:- Черкаси: Брама ІСУЕП, 2003.
3. Муттер В.М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат. 1990. – 282с.