ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 5 (1), 2025

РАДІОЕЛЕКТРОНІКА

СИНТЕЗ АНСАМБЛІВ КОДІВ ГОЛДА ДЛЯ ЗАСТОСУВАННЯ В МЕРЕЖАХ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ, НАВІГАЦІЇ ТА ІМПУЛЬСНІЙ РАДІОЛОКАЦІЇ

І.Колодчак, І.Чайковський [ORCID: 0000-0003-0653-5121], **Д. Чорний** [ORCID: 0009-0002-1035-071X]

Національний університет «Львівська політехніка», вул. С. Бандери, 12, Львів, 79013, Україна

Відповідальний за рукопис: Іван Колодчак (e-mail: ivankolod5@gmail.com)

(Подано 1 лютого 2025)

Розглянуто алгоритм синтезу ансамблів псевдовипадкових послідовностей бінарних кодів Голда з використанням процедури утворення спареної m-послідовності, яка за допомогою децимації (проріджування) генерується з відповідного примітивного полінома степені n, де $5 \le n \le 10$. В результаті утворюється оптимальна (англ. - preferred) пара m-послідовностей, яка породжує один ансамбль вищезгаданих кодів. Показано, що таких різних (для конкретного значення степеня примітивного полінома n) ансамблів може бути достатньо велика кількість, що дає можливість проектанту відповідної системи по випадковому закону змінювати сигнатуру використовуваних кодів Голда, забезпечуючи при цьому потрібну завадостійкість системи. Запропоновано і наведено приклад використання рекурентного алгоритму, що застосовується в криптографії, для пошуку значень коефіцієнтів відповідного примітивного поліному, який входить в оптимальну пару поліномів, за відомим довільним неперервним фрагментом m-послідовності довжиною не менше 2×n елементів. Передбачається деяке спрощення цієї процедури використовуючи такий спосіб визначення коефіцієнтів примітивного полінома, включаючи його реалізацію шляхом утворення і вирішення (наприклад, класичним методом Гауса з врахуванням особливостей тривіальної двійкової модульної арифметики) системи лінійних рівнянь з коефіцієнтами, вільними членами та невідомими, що є елементами поля Галуа. Крім того, застосування способу утворення лінійної системи рівнянь на базі різницевого рівняння рекурсії разом із вищевказаним, забезпечать меншу обчислювальну складність (для порівняно невеликих вищенаведених значень n), ніж у випадку використання, для таких цілей, відомого алгоритму Берлекемпа-Мессі. Запропоновані критерії впорядкування кодів Голда, зважаючи на їх кореляційні властивості, а також розроблений сервісний алгоритм на мові програмування високого рівня для синтезу та вибору з певного ансамблю потрібної кількості кодів Голда з найкращими, залежно від області їх застосування, кореляційними властивостями.

Ключові слова: *псевдовипадкові коди, m-послідовності, коди Голда, рівняння рекурсії, поле Галуа, примітивний поліном, додавання (множення) за модулем, ансамбль кодів, періодичні, аперіодичні, авто- та взаємо-кореляційні функції дискретних псевдовипадкових послідовностей.*

Вступ і постановка задачі

Аналіз відповідних публікацій [2,4,5,6] показує, що має місце стійка тенденція зростання і постійного удосконалення стільникових мереж з кодовим розділенням (CDMA) і множинним

асинхронним доступом, а також систем супутникової та наземної навігації [4,5]. В названих системах широко використовуються для різних цілей слабокорельовані псевдовипадкові послідовності (ПВП), що є кодами Голда, та їм подібні [1,2] різних періодів і довжин. Передбачається також, що перспективним може бути використання кодів Голда як модулюючих функцій для синтезу бінарних фазоманіпульованих зондувальних радіосигналів в спеціалізованих радіолокаторах, що працюють по малопомітних високодинамічних повітряних цілях при наявності певних апріорних цілевказівок по дальності та кутових координатах. Саме тому актуальною є проблема зручного і швидкого синтезу ансамблів таких кодів та аналізу їх кореляційних властивостей [2,7,6]. Позитивною особливістю ПВП Голда є те, що їх є досить велика кількість і для заданого степеня примітивного полінома n, строго обмеженим зверху та порівняно незначним є рівень паразитних пелюсток їх періодичних авто- та взаємо- кореляційних функцій ($АКФ_П$ та $ВКФ_П$). Зокрема, для n = 10 існує 300 ансамблів кодів Голда зі 1025-ма кодами в кожному та з періодом повторення коду $N = 2^n-1$, а при необмеженому зростанні $N \to \infty$, максимальні значення паразитних пелюсток $АКФ_П$ та $ВКФ_П \to 1/\sqrt{N}$, тобто наближаються до класичної границі Велча [2]. В даній статті зроблена спроба проаналізувати порівняно нескладний алгоритм синтезу ансамблів кодів Голда з використанням процедури децимації, наведеної в [1,2], та вирішенням «зворотної» задачі, яка полягає у визначенні коефіцієнтів примітивного поліному за повністю (або фрагментарно) відомою децимованою m-послідовністю. Сформульовані критерії впорядкування отриманих кодів Голда згідно їх авто- та взаємо- кореляційних властивостей, а також розроблений сервісний алгоритм (до рівня коду на мові програмування PYTHON) для генерації та вибору із заданого ансамблю необхідної кількості з найкращими, відповідно до сфери їх застосування, кореляційними характеристиками.

2. Синтез бінарних ансамблів кодів Голда

Розглянемо алгоритм синтезу ансамблів бінарних кодів Голда з використанням процедури децимації опорних m-послідовностей, що генеруються з табульованих (наведених, наприклад, в [3,6]) примітивних поліномів степенів n = 5,6,7,9,10 з метою утворення децимованих m-послідовностей, які, разом із відповідною вищезгаданою опорною m-послідовністю, утворюють «оптимальні» (англ. − preferred) пари для генерації ПВП Голда. Зауважимо, що для значень n=0(mod)4, кодів Голда не існує, тому значення степеня примітивного поліному n=8 не розглядається. Використаємо процедуру децимації бінарних m-послідовностей, що наведена в [1,2] і яка складається, в залежності від парності чи непарності степеня n примітивного полінома, з декількох порівняно не складних логічно обумовлених правил і висновків, які будуть вказані нижче в процесі опису алгоритму синтезу. Генерація ансамблів кодів Голда здійснюється однойменним алгоритмом із застосовуванням (для отримання опорної m−послідовності) класичного регістра зсуву з лінійними зворотними зв'язками (РЗЛЗЗ) [2,3,6].

Процес генерації кодів відбувається з використанням в даному алгоритмі наступних параметрів, констант та змінних, зокрема:

- n – степінь примітивного поліному, а також кількість двійкових тригерів в регістрі РЗЛЗЗ для генерації опорної m−послідовності, з якої після специфічної процедури «децимації по Голду» утворюються оптимальна (preferred) пара m−послідовностей для подальшого синтезу повного ансамблю;
- МП-$n(j)$, де (n = 5, 6, 7, 9, 10) − різні множини для кожного параметру n всіх примітивних поліномів, що описуються математичним апаратом (алгеброю) кінцевих полів, а їх коефіцієнти належать простому полю Галуа GF(2). Названі множини примітивних поліномів зведені в таблицях, зокрема в [3,6], причому множина МП-5(j=1,…,6) містить 6 поліномів, множина МП-6(j=1,…,6) містить також 6 поліномів, множина МП-7(j=1,…,18) містить 18 поліномів, множина МП-9(j=1,…,48) містить 48 поліномів, множина МП-10(j=1,…,60)

містить 60 поліномів. Всі вони є масивами бінарних констант, а кожна кодова стрічка, що наведена у названих масивах, складається з (n+1) впорядкованих двійкових (0 або 1) символів, які означають наступне:

− перший символ зліва та останній символ справа завжди дорівнюють 1, що означає, по-перше, що вихід кінцевого суматора за (mod)2 (це є модульна сума всіх зворотних лінійних зв'язків регістра РЗЛЗЗ) завжди повинен бути підключений до входу n-розрядного РЗЛЗЗ, а по-друге, це забезпечує генерацію саме m-послідовності, тобто ПВП з максимальним для заданого n періодом;

− всі інші (n-1) двійкових символів відображають використання (при цьому символ коефіцієнта в перемножувачах РЗЛЗЗ = 1) або не використання (при цьому символ коефіцієнта в перемножувачах РЗЛЗЗ = 0) вмістимого з виходу відповідного тригера n-розрядного РЗЛЗЗ для утворення поступових значень модульної суми (тобто елементів генерованої m-послідовності), причому останній (крайній справа) символ, як правило, є виходом, на якому при кожному і-тому часовому зсуві послідовно формуються відповідні значення утворюваної опорної періодичної з періодом ($N = 2^n - 1$) m-послідовності;

Примітка: В загальному випадку n-степеневий двійковий нормований (тобто приведений, для якого $k_n = 1$) примітивний поліном, із використанням для його формалізації «фіктивної» змінної X, причому $k_i \in GF(p)$, де $i = 0, 1, \ldots, n$, має наступний вид:

$$k(X) = k_n \times X^n + k_{n-1} \times X^{n-1} + k_{n-2} \times X^{n-2} + \ldots + k_2 \times X^2 + k_1 \times X^1 + k_0 \times X^0 =$$
$$= (1) \times X^n + (0(1)) \times X^{n-1} + (0(1)) \times X^{n-2} + \ldots + (0(1)) \times X^2 + (0(1)) \times X^1 + (1) \times X^0,$$

- d − допустимий (згідно алгоритму Голда) індекс децимації [проріджування по (mod)N] кожної опорної m−послідовності, що генерується відповідним примітивним поліномом, який належить відомій (наперед заданій) одній із множин МП-$n(j)$ для визначених конкретних значень індексів n та j;
- $N = 2^n - 1$ − довжина (одночасно і період) кодової m-послідовності та коду Голда, причому всі m-послідовності, як і послідовності Голда, повторюються періодично в часі з періодом ($N = 2^n - 1$) необмежено довго, однак у пам'ять фіксуються їх значення протягом лише одного періоду;
- $M = (2^n - 1) + 2$ − кількість (кардинальність) різних кодів Голда, включаючи дві m-послідовності з оптимальної пари, що входять в один ансамбль. Їх генерація повинна здійснюватися для всіх можливих опорних m−послідовностей, примітивні поліноми яких перелічені у вищеназваних масивах МП-$n(j)$, шляхом їх децимації з деякими індексами d_L, які відповідають вимогам алгоритму забезпечуючи утворення оптимальних пар.

Генерація всіх можливих ансамблів кодів Голда здійснюється для кожного примітивного полінома, множина яких задана в п'яти вищеназваних масивах МП-n(j). Алгоритм генерації ансамблів кодів Голда для степенів примітивних поліномів (n = 5,6,7,9,10) складається з ряду нижченаведених кроків.

1. Вибрати перший (або наступний) масив МП- $n(j)$, зафіксувавши при цьому параметр n, де: n = 5, 6, 7, 9, 10 та j, де: j = (1,…,6) або (1,…,6) або (1,…,18) або (1,…,48) або (1,…,60) відповідно.

2. Вибрати перший (або наступний) примітивний поліном з плинного n-го масиву МП-$n(j)$ та згенерувати для отриманого полінома, відповідну йому, опорну m−послідовність U_i , де i = 1, … ,N−1 (структурно-функціональна блок-схема, рис.2).

3. Для отриманої вище «опорної» m−послідовності U_i визначити множину допустимих індексів децимації (d_1, … , d_L), які задовольняють умовам алгоритму Голда, тобто для $d_L = 2^S + 1$, де s є взаємно простим числом (ВПЧ) з n, при умові що n − непарне, або ж s є парним і утворює ВПЧ з

(n/2), при умові, що n − парне та одночасно $n\neq0$(mod)4. Діапазон зміни індексів децимації повинен входити в інтервал $[3 \le (d_1, \dots, d_L) \le N-1]$, а числа $s = 1, 2, \dots$ − натуральні цілі додатні числа.

4. Для кожного індексу децимації ($d_1, \dots, d_L$), отриманого в пункті 3, згенерувати, шляхом прорідження, опорної m−послідовності U_i, L m−послідовностей $V_1, V_2, \dots, V_L$, для яких $V_1 = U_{(i\times d1)modN}$,
$V_2 = U_{(i\times d2)modN}$, …, $V_L = U_{(i\times dL)modN}$, де остаточний індекс, який вказує на вибраний символ U_i, обчислюється як $(i\times d_i)(mod)N$. Таким чином, буде утворено L оптимальних пар m−послідовностей $\{[U_i,V_1], [U_i,V_2], \dots, [U_i,V_{L-1}], [U_i,V_L]\}$, структура яких відповідає умовам алгоритму Голда, причому за допомогою кожної пари можна генерувати один ансамбль кодів, кардинальність якого становить (разом з відповідною їм «оптимальною» парою спарених m−послідовностей) величину $N+2 = (2^n-1)+2$.

5. Для кожної з L отриманих оптимальних пар $\{[U_i,V_{(i\times d1)modN}], [U_i,V_{(i\times d2)modN}], \dots, [U_i,V_{(i\times dL)modN}]\}$ згенерувати, шляхом циклічного зсуву децимованої m−послідовності (V) на N позицій з порозрядним (після кожного зсуву на один розряд) додаванням з (U_i) за (mod)2, L ансамблів по N послідовностей Голда в кожному із них (структурно-функціональна блок-схема, рис.3), запам’ятавши їх значення довжиною в період.

6. Якщо вибраний примітивний поліном не є останнім у плинному масиві МП-$n(j)$, то слід вибрати наступний МП-$n(j+1)$ поліном із цього масиву і перейти до виконання пункту 2.

Якщо вибраний примітивний поліном є останнім у плинному масиві МП-$n(j)$, то слід вибрати наступний масив МП-$(n+1)(j)$ і перейти до виконання пункту 1.

Якщо вибраний примітивний поліном є останнім у плинному масиві МП-$n(j)$, а також останнім є і плинний масив МП-$n(j)$, то це означає, що всі ансамблі кодів Голда згенеровані і збережені в пам’яті комп’ютера.

Оскільки первинною задачею в процесі реалізації вищеописаного алгоритму є отримання опорної m-послідовності, яка задається черговим (вибраним із заданих масивів) примітивним поліномом, стисло наведемо основні варіанти реалізації такої процедури. Згідно [3,6], відомі три теоретично обґрунтовані способи генерації m-послідовностей, а саме:

А) Перший спосіб.

Утворюється система, що складається з i рекурентних різницевих рівнянь, яка випливає з фундаментальної вимоги щодо рівності нулю скалярного добутку $(n+1)$-значного вектора відповідних коефіцієнтів примітивного полінома та $(n+1)$-значного вектора відповідних (неперервно обчислюваних) плинних символів рекурсії, починаючи з символів вектора початкового стану, а саме:

$$k_0 D_{i+0} + k_1 D_{i+1} + \dots + k_{n-2} D_{i+(n-2)} + k_{n-1} D_{i+(n-1)} + k_n D_{i+n} = 0,$$

Враховуючи те, що для примітивного полінома завжди $k_n=1$, отримуємо (для різних i) систему рівнянь,

$$D_{i+n} = -k_0 D_{i+0} - k_1 D_{i+1} - \dots - k_{n-2} D_{i+(n-2)} - k_{n-1} D_{i+(n-1)}, \text{ де } i = 0,1,\dots, N-1,$$

яка вирішується відносно елементів невідомої періодичної рекурсивної послідовності $\left[D_0, D_1, \dots, D_{N-2}, D_{N-1}\right]$ при відомому примітивному поліномі $k(X) = k_0 X^0 + k_1 X^1 + \dots + k_{n-1} X^{n-1} + k_n X^n$ степеня n (причому $k_0\neq0$ а $k_n=1$) та наперед заданому ненульовому векторі початкового стану $\left[D_0 \dots D_{n-1}\right]$. Тобто в даному випадку йдеться про знаходження коефіцієнтів періодичного (з періодом N) нижченаведеного полінома

$$D(X) = D_0 X^{N-1} + D_1 X^{N-2} + \dots + D_{N-2} X^1 + D_{N-1} X^0 = D_0 X^{N-1} + D_1 X^{N-2} + \dots + D_{N-2} X + D_{N-1},$$

як многочлена, обчисленого за модулем полінома-двочлена X^N-1, де $N=p^n-1$ – період шуканої *m*-послідовності в розширеному полі Галуа $GF[p^n]$. Зауважимо, що примітивний поліном k(X) повинен ділити без остачі поліном-двочлен X^N-1, а N, при цьому, є найменшим числом для якого таке ділення є справедливим. Апаратно вищеописана процедура реалізується, як правило, лінійною комутованою схемою на базі регістра зсуву з лінійними зворотними зв'язками та відома як конфігурація Фібоначчі [2,7], причому тактовий інтервал зсуву в регістрі ідентифікується з вищеозначеним додатним цілим числом *i*, різні значення якого утворюють систему рекурентних різницевих рівнянь.

Б) Другий спосіб.

Багатократно обчислюється, починаючи з деякого наперед заданого ненульового вектора початкового стану $[D_0...D_{n-1}]$, нижченаведене співвідношення:

$$D_i(X) = X^1 \times D_{i-1}(X) - D_{i-1(n-1)} \times (k_n)^{-1} \times k(X)$$

де i = 0,1,…,+∞ (додатні цілі числа, включаючи число 0); $D_i, D_{i-1}(X)$ – конкретні (для заданого *i* = 1 або 2, … , або p^n-1) поліноми степенів ≤(*n*-1), що утворюють циклічну мультиплікативну групу розширеного поля Галуа $GF(p^n)$; $(k_n)^{-1}$ – обернене значення коефіцієнта при найстаршому степені *n* примітивного полінома $k(X)$, причому $(k_n)^{-1}=1$, оскільки поліном $k(X)$ завжди повинен бути нормованим, тобто $k_n=1$.

Наведена залежність означає, що після чергового множення на одночлен X^1 плинного полінома $D_{i-1}(X)$ його найстарший (*n*-1)-ий коефіцієнт стає *n*-им і множиться на $(k_n)^{-1}$ та на примітивний поліном $k(X)$. В подальшому отриманий поліном-добуток віднімається від щойно зсунутого полінома $D_i(X)$, що означає виконання операції ділення над поліномом $D_i(X)$, тобто його обчислення за модулем примітивного полінома $k(X)$. Зважаючи на циклічність мультиплікативної групи, послідовні значення *n*-го коефіцієнта полінома $D_i(X)$ утворюють *m*-послідовність з періодом $N=p^n-1$. Апаратно така процедура, як правило, реалізується лінійною комутованою схемою на базі регістра зсуву з лінійними зворотними зв'язками та відома як конфігурація Галуа [2,7], причому тактовий інтервал зсуву задається вищеозначеним додатним цілим числом *i*, яке використовується як індекс у вищенаведеному співвідношенні, а зворотні зв'язки визначаються рішенням рівняння $k(X)=0$ відносно найстаршого (*n*-го степеня) одночлена.

В) Третій спосіб.

Обчислюються всі послідовні значення елементів *m*-послідовності (як послідовні частки) в процесі ділення одного із (p^n-1) довільних ненульових поліномів степеня ≤(*n*-1) на заданий дільник, яким повинен бути двоїстий примітивний поліном $k^*(X)$ степеня *n* відносно первинного (вибраного) примітивного полінома $k(X)$, причому, як відомо, $k^*(X)=X^n\times k(1/X)$. Отже, згенерована *m*-послідовність − це фактично послідовний неперервний ряд коефіцієнтів m_i = [(0,…,p−1) є GF(p)], які розміщуються біля постійно зростаючих (в процесі обчислення) степенів полінома-частки m(x), а саме:

$$m(X) = m_1 \times X^0 + m_2 \times X^1 + ... + m_i \times X^{i-2} + m_k \times X^{i-1},$$

де: i = 0,1,…,+∞ − кількість обчислень, причому, якщо *i*-1 = p^n−1, то генерується один період *m*-послідовності. Така процедура випливає із відомої [3,6] теореми Цирлєра і також може бути реалізована лінійною комутованою схемою на базі регістра зсуву з лінійними зворотними зв'язками. Наприклад, для розширеного поля Галуа GF(2^n), пам'яті регістра (*n*=3) та примітивного полінома $k(X) = X^3 + X^2 + 1$ (його двоїстий еквівалент $k^*(X) = X^3 \times \left({}^{1}\!/_{X^3} + {}^{1}\!/_{X^2} + {}^{1}\!/_{1} \right) = 1 + X^1 + X^3$), список поліномів, які в даному випадку можуть бути початковими діленими з вагами $(X^0 + X^1 + X^2)$, складає множину із семи породжуючих елементів $\{1, X^1, X^2, 1+X^1, 1+X^2, 1+X^1+X^2, X^1+X^2\}$, які [3,6], є членами циклічної мультиплікативної групи розширеного поля GF(2^3). Підстановка (і як первинних ділених і як початкових значень) членів цієї групи задає допустимі наступні можливі процеси ділення поліномів $\{1/k^*(X)$ або $X^1/k^*(X)$ або $X^2/k^*(X)$ або $(1+X^1)/k^*(X)$ або $(1+X^2)/k^*(X)$, $(1+X^1+X^2)/k^*(X)$ або $(X^1+X^2)/k^*(X)\}$, кожен з яких приводить до обчислення (з певним відомим циклічним зсувом) відповідної *m*-послідовності.

Зазначимо також, що для всіх трьох вищенаведених способів генерації *m*-послідовностей справедливі також наступні застереження:

АА) Допустимим є множення (а фактично це ділення) плинного поліному на одночлен X^{-1}=1/X у використаних математичних виразах або, відповідно, зсув у сторону молодших розрядів у лінійних регістрах зсуву при апаратній реалізації. При цьому слід зважати на зміну зворотних зв'язків, які при цьому будуть визначатися двоїстим примітивним поліномом та оберненими утворюючими примітивними елементами мультиплікативної циклічної групи поля Галуа.

ББ) Всі операції (додавання, віднімання, множення і ділення) повинні виконуватися фактично за двійним модулем, який задається характеристикою (розмірністю) *p* простого поля Галуа GF(p) та вибраним примітивним поліномом k(X) степеня *n*. Такі операції часто називають обчисленням по двійному модулю і позначають відповідно як [(modd)k(X),p], причому за (mod)p обчислюються (після зведення подібних членів) коефіцієнти отриманого (плинного) поліному, а за (mod)k(X) − сам плинний поліном, якщо його степінь ≥ *n*.

На рис.1 та рис.2 наведені структурно-функціональні блок-схеми генерації опорних *m*-послідовностей з допомогою регістра зсуву пам'яті *n* з лінійними зворотними зв'язками для *p*-значного та двійкового алфавітів з розширеними полями Галуа GF(p^n) та GF(2^n) відповідно. Наведені схеми відображають більш зручну та широковживану конфігурацію Фібоначчі [7], яка передбачає утворення кожного наступного значення *m*-послідовності з допомогою зовнішнього вузла, що складається з одного багатовходового модульного суматора та сукупності з *n*, з'єднаних (або не з'єднаних) з відповідними входами суматора та відповідними виходами тригерів власне регістра зсуву, модульних перемножувачів. Випадки відсутності зв'язку (тобто нез'єднання) мають місце тоді і тільки тоді, коли відповідний коефіцієнт примітивного полінома дорівнює нулю.

Всі тригери (власне регістра зсуву, який на схемах обведений пунктиром) мають внутрішню специфічну структуру інформаційних зв'язків і зв'язків керування, а саме:

- інформаційний вихід кожного тригера з'єднаний з першим входом відповідного перемножувача, а також з інформаційним входом наступного тригера, причому інформаційний вихід найстаршого тригера [Тг(0)] (його розрядна вага задається степенем $X^{(n-1)+i}$) є одночасно і виходом загального РЗЛЗЗ, з якого, як правило, зчитується генерована *m*-послідовність, а інформаційний вхід наймолодшого тригера [Тг(n-1)] (його розрядна вага задається степенем

X^{0+i}) з'єднаний із виходом суматора вузла зворотного зв'язку через перемножувач на старший коефіцієнт k_n примітивного полінома k(X);

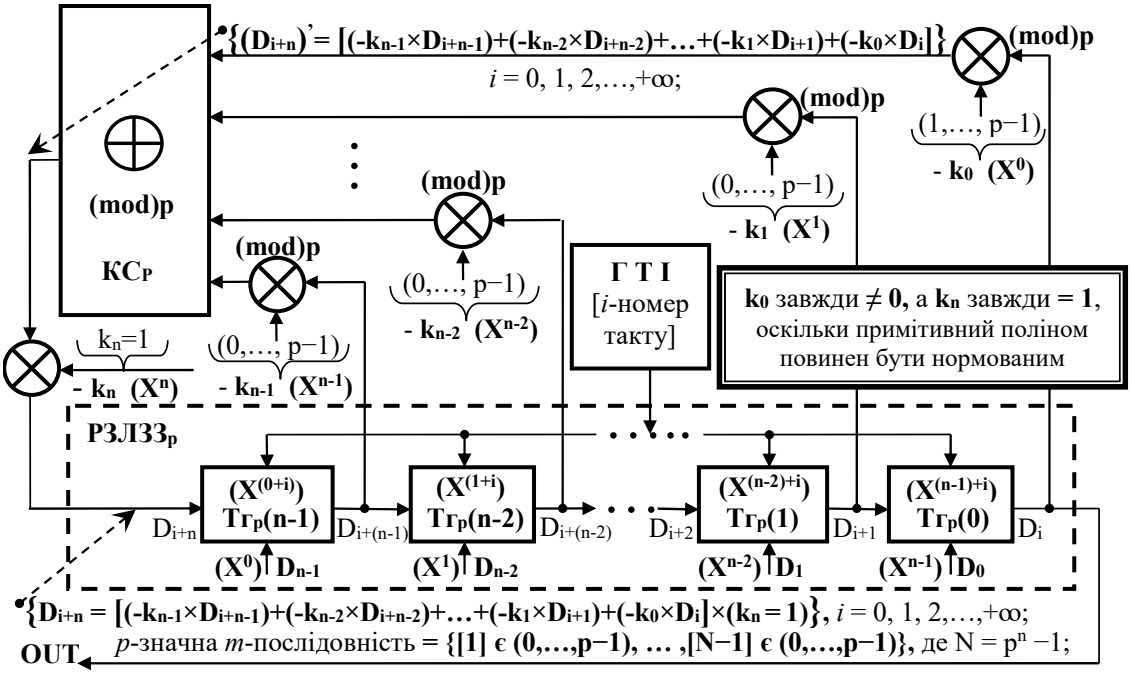

Рис.1 Структурно-функціональна блок-схема генерації p-значної m-послідовності за допомогою регістра РЗЛЗЗ$_P$, побудованого по схемі Фібоначчі

- на другі входи перемножувачів подаються відповідні протилежні відповідному по модулю значення коефіцієнтів примітивного поліному, який породжує дану *m*-послідовность;
- інформаційні входи ($D_{n-1},D_{n-2},\ldots,D_1,D_0$) з відповідними порозрядними вагами ($X^0, X^1,\ldots, X^{n-2}, X^{n-1}$) для початкового встановлення тригерів під'єднані до стартової схеми (на рисунках не показана), причому початкова комбінація зі всіх нулів строго заборонена;
- на входи керування кожного тригера від генератора тактових сигналів (ГТІ) поступають імпульси, робочий фронт яких ініціює одночасний *i*-ий зсув плинного інформаційного коду регістра в сторону старших розрядів та відповідну зміну його стану з урахуванням перехідного процесу в колі зворотного зв'язку, яке реалізується як класична комбінаційна схема, тобто як багатовходова з одним виходом логічна функція Буля.

Кожен зсув на один розряд, якщо він відбувається в напрямку до старших розрядів, здійснює множення плинного полінома зі степенями ($X^{0+i},\ldots, X^{(n-1)+i}$) на поліном-одночлен ($X^1$), що автоматично збільшує всі степені плинного полінома на одиницю.

Конфігурація Фібоначчі забезпечує також те, що символи генерерованої *m*-послідовності можуть неперервно зчитуватися як з виходу кожного тригера регістра зсуву, так і з виходу суматора вузла зворотного зв'язку, причому отримані таким способом *m*-послідовності матимуть відповідне «фазове» випередження, що іноді може давати додатковий позитивний ефект.

Як показано в [9], на базі вищенаведених трьох математично обгрунтованих способів синтезу *m*-послідовностей, може бути утворено декілька (більш або менш ефективних) матричних методів обчислення зазначених псевдовипадкових послідовностей з використанням фундаментального співвідношення між плинними [S(*i*)] та наступними [S(*i*+1)] станами у виді функції переходів (як для кінцевих абстрактних цифрових автоматів) з наперед заданим ненульовим початковим станом [S(0)], а саме:

$$S(i+1) = G^T \times S(i)$$

де: $i = 0,1,2, \ldots, +\infty$ (цілі додатні числа, включаючи число 0), G^T – транспонована супутня матриця примітивного полінома k(X) (фактично це матриця функції переходів розмірністю $n \times n$ елементів), яка складається з певним чином розташованих трьох компонент, а саме: із одиничної матриці E [розмірністю $(n\text{-}1)\times(n\text{-}1)$ елементів], що утворюється (починаючи зверху) шляхом послідовного зсуву вправо примітивного найменшого утворюючого елемента циклічної мультиплікативної групи поля $GF(p^n)$, із нижньої стрічки, яка, в свою чергу, складається з n молодших коефіцієнтів примітивного полінома в результаті вирішення рівняння $k(X)=0$ відносно найстаршого одночлена n-го степеня та з крайнього лівого нульового 0-вектора-стовпця розмірністю $(n\text{-}1)$ елементів.

Здійснюючи деякі допустимі трансформації супутньої матриці G, а саме: транспонування відносно головної або допоміжної діагоналей, а також заміну утворюючого примітивного елемента циклічної мультиплікативної групи та примітивного полінома відповідно на обернені та двоїсті еквіваленти, можна отримувати обчислювальні схеми різної ефективності. При цьому, залежно від потреби в програмній або апаратній реалізації, необхідно також використовувати більш зручні інструментальні особливості вибраної мови програмування та її компілятора або функціональні можливості елементної бази вибраних електронних компонент відповідно.

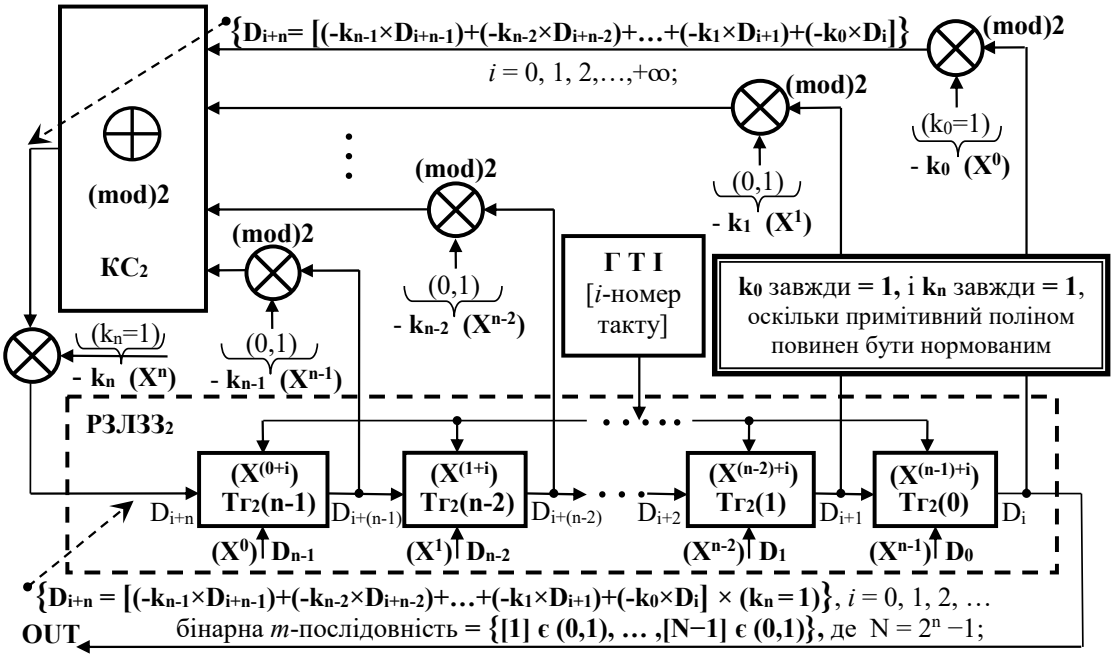

Рис.2 Структурно-функціональна блок-схема генерації бінарної m-послідовності за допомогою регістра РЗЛЗ32, побудованого по схемі Фібоначчі

Зауважимо, що «короткі» знаки мінус «-» при співмножниках $[-k_n, -k_{n-1}, \ldots, -k_2, -k_1]$ в модульній сумі блок-схеми (рис.1) означають обчислення за (mod)p відповідних протилежних до коефіцієнтів примітивного полінома $[k_n, k_{n-1}, \ldots, k_2, k_1]$ елементів в простому полі GF(p). В той же час, на блок-схемі (рис.2) співмножники в модульній сумі та коефіцієнти примітивного полінома співпадають, оскільки в полі Галуа GF(2) обчислення протилежних елементів задається тривіально просто, а саме: [0+0 = 0 та 1+1 = 0] (mod)2, тобто кожен елемент простого поля є протилежним собі.

На рис.3 зображена структурно-функціональна блок-схема остаточної (заключної) стадії генерації одного ансамблю бінарних кодів Голда, який утворюється (пункт 2.3.5 вищенаведеного алгоритму) з однієї оптимальної пари m-послідовностей.

На структурно-функціональних блок-схемах (рис.1, рис.2 та рис.3) використані наступні умовні позначення та скорочення:

$КС_2$, $КС_P$ − комбінаційні схеми з менше ніж *n* входами та одним виходом, що реалізують сумування за (mod)2 або за (mod)p відповідних символів із виходів тригерів регістра зсуву, помножених [за (mod)p або за (mod)2] на протилежні [$-k_n$, $-k_{n-1}$, … , $-k_2$, $-k_1$] або первинні [k_n , k_{n-1} , … , k_2 , k_1] коефіцієнти примітивного полінома;

$Тг_p(0)$, … , $Тг_p(n)$ та $Тг_2(0)$, … , $Тг_2(n)$ − тригери (*p*-значні та двійкові елементи пам'яті), що сукупно утворюють саме регістри зсуву в $РЗЛЗЗ_p$ та $РЗЛЗЗ_2$ відповідно;

Г Т І − генератор *i*-тих тактових імпульсів, фронти та частота яких ініціюють процес генерації, включаючи зсув, сумування та множення відповідних символів, а також визначають швидкість зміни вихідного ПВК;

[(1),(2),…,(N-2),(N-1)] є (0,…,p −1) − ці символи означають, що значення кожного елемента вихідного псевдовипадкового коду належить (є) множині допустимих значень (0,…,p−1) для *p*−значної *m*-послідовності;

[(1),(2),…,(N-2),(N-1)] є (0,1) − ці символи означають, що значення кожного елемента вихідного псевдовипадкового коду належить (є) множині допустимих значень (0, 1) для двохзначної (бінарної) *m*-послідовності;

(1),(2),(3),…,(N-3),(N-2),(N-1) − розряди регістрів, що зберігають символи сформованої вище наведеним алгоритмом пари оптимальних *m*-послідовностей;

OUT − вихід послідовного коду згенерованої *m*-послідовності;

→ (± 1) − оператор перетворення символів, заданих у логічному (0,1) двійковому базисі, в знакозмінний сигнальний базис (± 1), що дозволяє подальше використання необхідних операцій звичайного множення для утворення потрібних модульованих сигнально-кодових конструкцій.

Решта використаних на рисунках умовних позначень та скорочень, що не вказані в цьому списку, розшифровані вище в пункті 2 (в процесі словесного опису алгоритму синтезу кодів Голда) або нижче в пункті 4 (в процесі опису системи рівнянь для вирішення зворотної задачі).

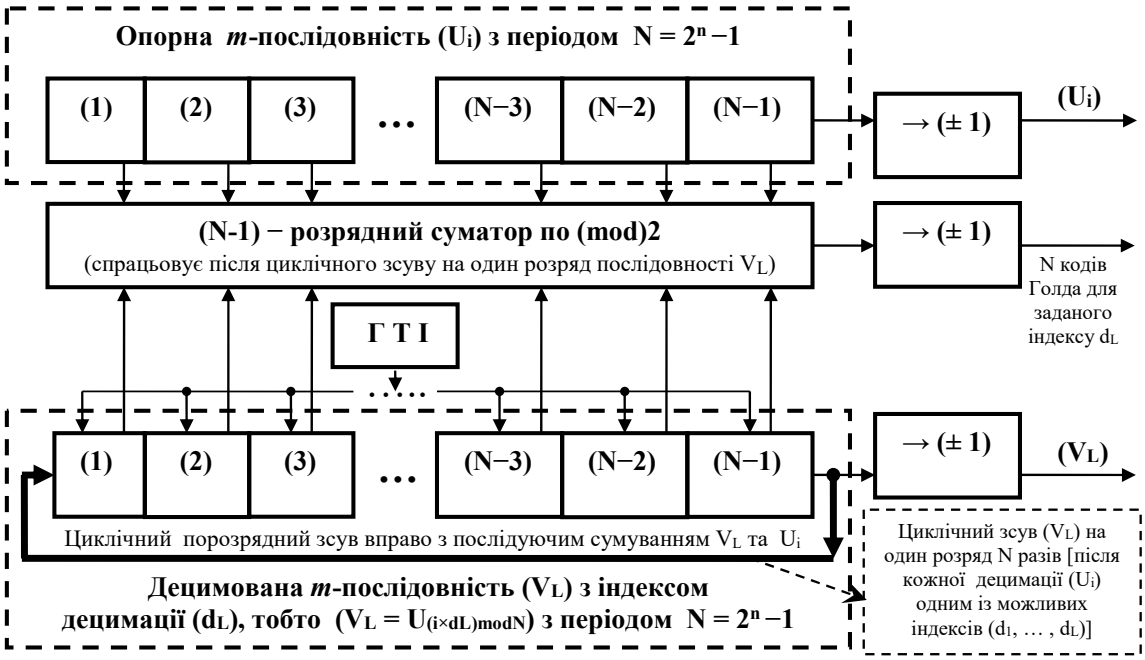

Рис.3 Структурно-функціональна блок-схема генерації одного ансамблю бінарних кодів Голда з пари оптимальних m-послідовностей

3. Критерії впорядкування кодових послідовностей Голда згідно їх кореляційних властивостей та характеристик

Головною перевагою кодів Голда є практичне застосування в мережах CDMA з асинхронним множинним доступом, навігаційних супутникових і наземних системах (з метою надійної

синхронізації та ідентифікації в обох варіантах застосування), а також в імпульсних радіолокаторах (з метою мінімізації взаємних завад, особливо, при роботі в режимах залпової атаки по одній цілі), є їх порівняно незначна та строго обмежена зверху [1,2] величина взаємної «паразитної» кореляції. Саме тому, при виборі з деякого ансамблю для практичного застосування конкретної підмножини кодів Голда, необхідною є доступність інформації стосовно небажаних «паразитних» взаємокореляційних впливів між різними такими псевдовипадковими кодовими послідовностями. Після обчислення різних авто- та взаємо- кореляційних функцій кодів Голда, актуальною стає задача їх відповідного впорядкування, яка потребує певних специфічних критеріїв, зокрема:

а) за зростанням модуля максимального значення всіх пелюсток (для ВКФ) та максимальних бічних пелюсток (для АКФ);

б) за зростанням модуля середнього значення всіх пелюсток (для ВКФ) та середнього значення бічних пелюсток (для АКФ);

в) за зростанням середньоквадратичного відхилення всіх пелюсток (для ВКФ) та середньоквадратичного відхилення бічних пелюсток (для АКФ);

г) за зростанням певної комбінації всіх вищеназваних критеріїв для ВКФ і АКФ.

Незалежно від того яку функцію виконує ПВП Голда в системі: синхронізація інформаційних потоків в мережі CDMA; ідентифікація даних місцезнаходження від різних давачів (супутників, маяків) в супутникових та наземних навігаційних комплексах; вимірювання параметрів (часу затримки, частоти Допплера, кутових координат) в імпульсних і/або неперервних радіолокаторах, первинною базовою операцією завжди є виявлення (з необхідною достовірністю) прийнятих з ефіру корисних сигналів. Прийнятий радіосигнал є здебільшого адитивною сумішшю штучних і природних ефірних завад і внутрішнього теплового шуму приймача системи, тому процедура виявлення сигналу (як випадкового процесу) є, в загальному випадку, ймовірнісною і досить складною. Оскільки, в нашому випадку для вищезазначених застосувань, тип і форма модулюючої функції (тобто комплексної обвідної сигналу) наперед відомі, рішення про наявність (або відсутність) корисного сигналу приймається після демодулятора з використанням методу максимальної правдоподібності при допустимих рівнях вихідних помилок.

Розглянемо завадостійкість процесу виявлення, враховуючи тільки негативний вплив ненульової «паразитної» авто- та взаємо- кореляції, оскільки вплив власного гаусівського шуму приймального тракту добре вивчений, а вплив зовнішних завад суттєво залежить від їх ймовірнісних характеристик і в кожному конкретному випадку застосування повинен аналізуватися окремо. Для цілей виявлення сигналів, які є випадковими процесами з нормальним (або близьким до нього) законом розподілу ймовірностей, доцільно впорядковувати коди Голда (тобто модулюючі функції) за критерієм зростання (або спадання) суми математичного сподівання та середньоквадратичного відхилення паразитних пелюсток їх періодичних і аперіодичних автокореляційних ($АКФ_П$, $АКФ_А$) та взаємно кореляційних ($ВКФ_П$, $ВКФ_А$) функцій. Якщо на вхід приймального пристрою від різних джерел поступає адитивна суміш рівновеликих сигналів, модульованих різними кодовими послідовностями Голда, а виявляти слід тільки той радіосигнал, який модульований одним конкретним кодом («ключем», що присвоєний даному пристрою), то для застосування оптимального алгоритму виявлення необхідно знати статистичні характеристики (наприклад закон розподілу ймовірностей) суміші «паразитних» авто- та взаємо- кореляцій між різними кодами. Завади такого характеру в [2] класифікуються як завади множинного доступу (ЗМД).

Нижче, на рис.4, подані результати математичного моделювання статистичних характеристик прийнятих сигналів в умовах наявності тільки ЗМД за допомогою моделі, створеної засобами пакету «System View» [8] для системного моделювання радіоелектронних пристроїв, зокрема, графіки законів розподілу (не нормованих до одиниці) випадкових процесів сумарної «паразитної» взаємокореляції та нормального (гаусівського) шуму приймального тракту, де: крива 1 − сумарний закон розподілу ймовірностей «паразитної» взаємокореляції деякої множини різних кодів Голда;

крива 2 − сумарний закон розподілу ймовірностей «паразитної» взаємокореляції та нормального шуму приймального тракту; крива 3 − закон розподілу ймовірностей нормального шуму приймального тракту.

Аналізуючи наведені на рис.4 графіки, можна зробити висновок, що закон розподілу ймовірностей сумарної «паразитної» взаємокореляції при зростанні кількості кодових сигнатур (крива 1 − побудована для 24-ох кодів, що поступають на вхід приймача з різними часовими затримками) наближається до нормального. Це означає, що й сумарний (разом з тепловим шумом приймального тракту, крива 3) розподіл є практично нормальним (крива 2). Отже застосування алгоритму максимальної правдоподібності в процесі виявлення сигналу є коректним і практично допустимим.

На рис.5 подана аперіодична взаємокореляційна функція ($ВКФ_А$ графік С-1, С-2) сумарної демодульованої суміші сигналів (в моделі використано 24 різних кодів Голда) з двома опорними кодами Голда, що відповідають двом виявленим сигналам (С-1 та С-2). Обидва сигнали, маючи однаковий вхідний рівень, після корелятора суттєво відрізняються за рівнем та часом затримки від отриманого без завад (С-3) сигналу, оскільки перший (С-1) співпадає за часом з максимальною (додатною), а другий (С-2) – з максимальною (від'ємною) «паразитною» взаємокореляцією. Графік С-3 – це $АКФ_А$ сигналу, який фіксує нульовий (опорний) зсув за часом затримки та рівень автокореляції сигналу при відсутності зовнішніх завад і власного шуму приймача.

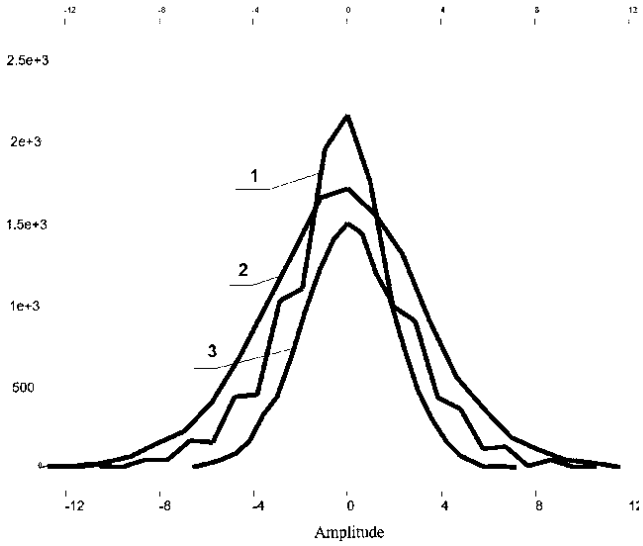

Рис.4 Графіки густини ймовірностей випадкових процесів паразитної взаємокореляції, власного шуму приймального тракту та їх суми

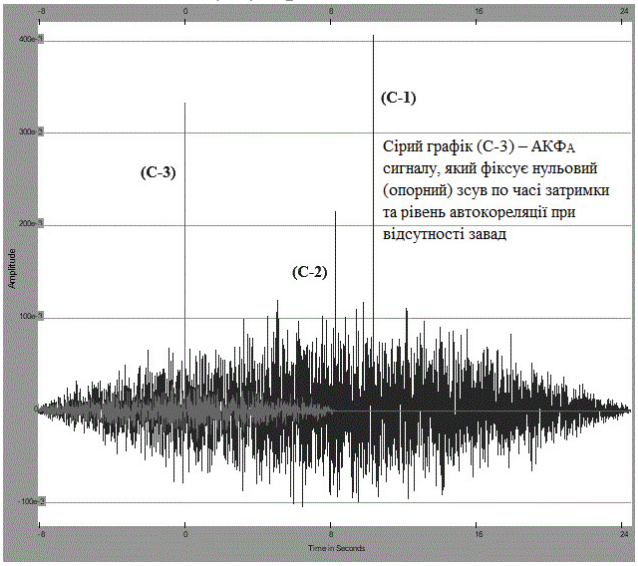

Рис.5 Ілюстрація виявлення одного й того ж сигналу за присутності тільки паразитної взаємокореляції для найбільшого додатнього (С-1) та найбільшого від'ємного (С-2) значень її величин

Зважаючи на результати моделювання, можна зробити висновок, що оптимальним критерієм впорядкування кодів Голда для достатньо ефективного ймовірнісного виявлення є критерій мінімуму суми математичного сподівання і середньоквадратичного відхилення їх «паразитної» взаємокореляції.

4. Визначення параметрів примітивного полінома за відомим неперервним фрагментом m-послідовності яку він породжує

Знаходження коефіцієнтів примітивного полінома або ж (що еквівалентно) структури зворотних зв'язків регістра РЗЛЗЗ за наперед відомою степінню полінома n та конкретних значень неперервного фрагменту (довжиною не менше $2\times n$ символів) згенерованої ним m-послідовності, може бути вирішена з використанням рівняння рекурсії. За допомогою рівняння складається і

розв'язується система із n лінійних рівнянь відносно невідомих коефіцієнтів примітивного полінома. Рівняння рекурсії (як було зазначено вище) – є різницевим рівнянням [2,3,6], яке дозволяє визначати чергове (наступне) значення m-послідовності у виді лінійної комбінації n попередніх її значень. Такі рекурентні співвідношення, зокрема, широко застосовується в криптографії та в теорії кодування. Отже, в загальному випадку, для кінцевого простого GF(p) і розширеного $GF(p^n)$ полів Галуа, де p − просте число, а n – натуральне ціле, маємо наступне рівняння рекурсії (1), з невідомими коефіцієнтами примітивного полінома:

$$D_{i+n} = \left(-k_{n-1}\right)\times D_{i+n-1} + \left(-k_{n-2}\right)\times D_{i+n-2} + \ldots + \left(-k_1\right)\times D_{i+1} + \left(-k_0\right)\times D_i, \qquad (1)$$

де: $i = 0, 1, \ldots, n\text{-}1$ – індекс i, який вказує на неперервний ряд цілих натуральних (включаючи число 0) додатних чисел; $D_i \in GF(p)$ – символи даних, що відповідають плинному стану тригерів та утворюють елементи генерованої m-послідовності; $[k_{n-1}, k_{n-2}, \ldots, k_1, k_0] \in GF(p)$ – елементи вектора постійних коефіцієнтів при відповідних фіктивних змінних X^i примітивного полінома; $[-k_{n-1}, -k_{n-2}, \ldots, -k_1, -k_0] \in GF(p)$ – співмножники у відповідних колах зворотного зв'язку регістра РЗЛЗЗ$_p$, які є протилежними за (mod)p до відповідних коефіцієнтів полінома $[k_{n-1}, k_{n-2}, \ldots, k_1, k_0]$.

В подальшому розглядатимемо тільки бінарні ПВП, для яких існують тільки два елементи поля Галуа (0,1) є GF(2), причому первинні і протилежні їм елементи в цьому полі співпадають, тобто
$0=(-0)=0(\text{mod}2)$ та $1=(-1)=1(\text{mod}2)$. Як наслідок, у всіх нижченаведених рівняннях елементи вектора $[k_{n-1}, k_{n-2}, \ldots, k_1, k_0]$ записані без знаку, оскільки завжди $k_i = (-k_i)$.

Записавши рівняння рекурсії (1) послідовно для значень $i = 0, 1, \ldots, n\text{-}1$, отримаємо наступну систему із n лінійних рівнянь (2) відносно невідомих $[k_{n-1}, k_{n-2}, \ldots, k_1, k_0]$, а саме:

$$\begin{array}{r}
i=0\rightarrow \\
i=1\rightarrow \\
i=2\rightarrow \\
\ldots \\
i=n-3\rightarrow \\
i=n-2\rightarrow \\
i=n-1\rightarrow
\end{array}
\left[\begin{array}{c}
k_{n-1}\times D_{n-1} + k_{n-2}\times D_{n-2} + k_{n-3}\times D_{n-3} + \ldots + k_2\times D_2 + k_1\times D_1 + k_0\times D_0 \\
k_{n-1}\times D_n + k_{n-2}\times D_{n-1} + k_{n-3}\times D_{n-2} + \ldots + k_2\times D_3 + k_1\times D_2 + k_0\times D_1 \\
k_{n-1}\times D_{n+1} + k_{n-2}\times D_n + k_{n-3}\times D_{n-1} + \ldots + k_2\times D_4 + k_1\times D_3 + k_0\times D_2 \\
\ldots \\
k_{n-1}\times D_{2n-4} + k_{n-2}\times D_{2n-5} + k_{n-3}\times D_{2n-6} + \ldots + k_2\times D_{n-1} + k_1\times D_{n-2} + k_0\times D_{n-3} \\
k_{n-1}\times D_{2n-3} + k_{n-2}\times D_{2n-4} + k_{n-3}\times D_{2n-5} + \ldots + k_2\times D_n + k_1\times D_{n-1} + k_0\times D_{n-2} \\
k_{n-1}\times D_{2n-2} + k_{n-2}\times D_{2n-3} + k_{n-3}\times D_{2n-4} + \ldots + k_2\times D_{n+1} + k_1\times D_n + k_0\times D_{n-1}
\end{array}\right]
\begin{array}{l}
= D_n \\
= D_{n+1} \\
= D_{n+2} \\
\ldots \\
= D_{2n-3} \\
= D_{2n-2} \\
= D_{2n-1}
\end{array} \qquad (2)$$

Враховуючи те, що ліва частина утвореної системи лінійних рівнянь складається з n скалярних добутків вектора постійних коефіцієнтів $[k_{n-1}\ k_{n-2}\ \ldots\ k_1\ k_0]$ з кожним із n−значних векторів рекурентно і послідовно зсунутих на i−тактів даних (D_i), система (2) в матричній формі матиме наступний вид (3):

$$\left[\begin{array}{ccccccc}
D_{n-1} & D_{n-2} & D_{n-3} & \ldots & D_2 & D_1 & D_0 \\
D_n & D_{n-1} & D_{n-2} & \ldots & D_3 & D_2 & D_1 \\
D_{n+1} & D_n & D_{n-1} & \ldots & D_4 & D_3 & D_2 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
D_{2n-4} & D_{2n-5} & D_{2n-6} & \ldots & D_{n-1} & D_{n-2} & D_{n-3} \\
D_{2n-3} & D_{2n-4} & D_{2n-5} & \ldots & D_n & D_{n-1} & D_{n-2} \\
D_{2n-2} & D_{2n-3} & D_{2n-4} & \ldots & D_{n+1} & D_n & D_{n-1}
\end{array}\right]
\times
\left[\begin{array}{c}
k_{n-1} \\ k_{n-2} \\ k_{n-3} \\ \ldots \\ k_2 \\ k_1 \\ k_n
\end{array}\right]
=
\left[\begin{array}{c}
D_n \\ D_{n+1} \\ D_{n+2} \\ \ldots \\ D_{2n-3} \\ D_{2n-2} \\ D_{2n-1}
\end{array}\right] (\text{mod})2 \qquad (3)$$

Відомо [2,6], системи (2,3) є сумісними та мають єдиний розв'язок, який й визначає коефіцієнти примітивного полінома та одночасно і множники в колах зворотних зв'язків лінійного регістра зсуву, який генерує відповідну m-послідовність.

Наведемо приклад, який наочно демонструє практичний аспект використання вищенаведених теоретичних залежностей для вирішення «зворотної» задачі. Нехай у нашому випадку є деяка бінарна *m*-послідовність з періодом $N=2^n-1$, де $n = 5$, яка утворена шляхом децимації, згідно алгоритму Голда, з відповідної опорної *m*-послідовності. Для визначення примітивного полінома, який породжує таким способом децимовану спарену *m*-послідовність, візьмемо два різних (хоч достатньо і одного) довільних її неперервних фрагменти (Фр1, Фр2) довжиною 2×5 символів кожен, наприклад:

$$Фр1 = \{1 = D_0, 1 = D_1, 1 = D_2, 1 = D_3, 1 = D_4, 0 = D_5, 0 = D_6, 0 = D_7, 1 = D_8, 1 = D_9\}$$

$$Фр2 = \{1 = D_0, 0 = D_1, 1 = D_2, 1 = D_3, 1 = D_4, 0 = D_5, 1 = D_6, 0 = D_7, 1 = D_8, 0 = D_9\}$$

Рівняння рекурсії (1) для заданих $n = 5$, $i = 0,1,2,3,4$ та $k_0 = k_5 = 1$ матиме вид:

$$D_{i+5} = k_4 \times D_{i+4} + k_3 \times D_{i+3} + k_2 \times D_{i+2} + k_1 \times D_{i+1} + k_0 \times D_i$$

Довільно (без негативного впливу на результат) прийнявши, що послідовність $[D_0 \quad D_1 \quad D_2 \quad D_3 \quad D_4 = 1 \quad 1 \quad 1 \quad 1 \quad 1]$ для Фр1 та послідовність $[D_0 \quad D_1 \quad D_2 \quad D_3 \quad D_4 = 1 \quad 0 \quad 1 \quad 1 \quad 1]$ відповідно для Фр2, будуть векторами початкових станів лінійного регістра зсуву та використовуючи матричне рівняння рекурсії (3), отримаємо для n=5 рівняння (4) яке, враховуючи тривіальність та обчислювальну простоту порозрядних операцій додавання та множення за (mod)2 в полі Галуа GF(2), вирішимо аналітично методом Гауса (тобто методом виключення змінних і приведення матриці до трикутного, або близького до нього, виду), а саме:

$$\begin{bmatrix} D_4 & D_3 & D_2 & D_1 & D_0 \\ D_5 & D_4 & D_3 & D_2 & D_1 \\ D_6 & D_5 & D_4 & D_3 & D_2 \\ D_7 & D_6 & D_5 & D_4 & D_3 \\ D_8 & D_7 & D_6 & D_5 & D_4 \end{bmatrix} \times \begin{bmatrix} k_4 \\ k_3 \\ k_2 \\ k_1 \\ k_0 \end{bmatrix} = \begin{bmatrix} D_5 \\ D_6 \\ D_7 \\ D_8 \\ D_9 \end{bmatrix} (\mathrm{mod})2 \qquad (4)$$

Після почергової підстановки в отриману систему рівнянь (4) значень двійкових символів обох відомих неперервних фрагментів однієї і тієї ж *m*-послідовності, знайдемо вектор постійних коефіцієнтів відповідного примітивного полінома $[k_0\ k_1\ k_2\ k_3\ k_4]$ із остаточних рівнянь рекурсії, що утворюються після перетворень розширених матриць обох систем рівнянь методом Гауса, причому модифіковані матриці та деякі їх відповідні модифіковані елементи позначені нижче символом «*». В першому випадку (для Фр1) достатньо у вихідній розширеній матриці $B_{Фр1}$ до першої її стрічки додати (що еквівалентно відніманню) п’яту і результат записати на місце п’ятої стрічки, а потім скласти другу стрічку з п’ятою (вже модифікованою) і результат зафіксувати на місце п’ятої стрічки, в результаті чого утворюється класична трикутна матриця і розв’язок стає очевидним.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} k_4 \\ k_3 \\ k_2 \\ k_1 \\ k_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix};$$

$$B_{Фр1}=\left[\begin{array}{ccccc|c}1&1&1&1&1&0\\0&1&1&1&1&0\\0&0&1&1&1&0\\0&0&0&1&1&1\\1&0&0&0&1&1\end{array}\right]\Rightarrow;\left[\begin{array}{ccccc|c}1&1&1&1&1&0\\0&1&1&1&1&0\\0&0&1&1&1&0\\0&0&0&1&1&1\\0^*&1^*&1^*&1^*&0^*&1\end{array}\right]^*\Rightarrow;\left[\begin{array}{ccccc|c}1&1&1&1&1&0\\0&1&1&1&1&0\\0&0&1&1&1&0\\0&0&0&1&1&1\\0&0^*&0^*&0^*&1^*&1\end{array}\right]^*\Rightarrow$$

$$\Rightarrow\left[\begin{array}{ccccccccccc}k_4\times D_4&+&k_3\times D_3&+&k_2\times D_2&+&k_1\times D_1&+&k_0\times D_0&=&0\\0&+&k_3\times D_4&+&k_2\times D_3&+&k_1\times D_2&+&k_0\times D_1&=&0\\0&+&0&+&k_2\times D_4&+&k_1\times D_3&+&k_0\times D_2&=&0\\0&+&0&+&0&+&k_1\times D_4&+&k_0\times D_3&=&1\\0&+&0&+&0&+&0&+&k_0\times D^*&=&1\end{array}\right]^*\Rightarrow\left[\begin{array}{l}k_4=0\\k_3=0\\k_2=1\\k_1=0\\k_0=1\end{array}\right];$$

В другому випадку (для Фр2) достатньо у вихідній розширеній матриці $B_{Фр2}$ до першої її стрічки додати (що еквівалентно відніманню) третю і результат записати на місце третьої стрічки, а потім скласти першу стрічку з п'ятою і результат зафіксувати на місце п'ятої стрічки.

$$\left[\begin{array}{ccccc}1&1&1&0&1\\0&1&1&1&0\\1&0&1&1&1\\0&1&0&1&1\\1&0&1&0&1\end{array}\right]\times\left[\begin{array}{c}k_4\\k_3\\k_2\\k_1\\k_0\end{array}\right]=\left[\begin{array}{c}0\\1\\0\\1\\0\end{array}\right];$$

$$B_{Фр2}=\left[\begin{array}{ccccc|c}1&1&1&0&1&0\\0&1&1&1&0&1\\1&0&1&1&1&0\\0&1&0&1&1&1\\1&0&1&0&1&0\end{array}\right]\Rightarrow;\left[\begin{array}{ccccc|c}1&1&1&0&1&0\\0&1&1&1&0&1\\0^*&1^*&0^*&1^*&0^*&0\\0&1&0&1&1&1\\0^*&1^*&0^*&0^*&0^*&1\end{array}\right]^*\Rightarrow$$

$$\Rightarrow\left[\begin{array}{ccccccccccc}k_4\times D_4&+&k_3\times D_3&+&k_2\times D_2&+&0&+&k_0\times D_0&=&0\\0&+&k_3\times D_4&+&k_2\times D_3&+&k_1\times D_2&+&0&=&1\\0&+&k_3\times D^*&+&0&+&k_1\times D_3&+&0&=&0\\0&+&k_3\times D_6&+&0&+&k_1\times D_4&+&k_0\times D_3&=&1\\0&+&k_3\times D^*&+&0&+&0&+&0&=&0\end{array}\right]^*\Rightarrow\left[\begin{array}{l}k_4=0\\k_3=0\\k_2=1\\k_1=0\\k_0=1\end{array}\right];$$

Отже, для *m*-послідовності з її відомими (Фр1, Фр2) фрагментами закон рекурсії і примітивний поліном матимуть один і той же вигляд, зокрема:

$$D_{i+5}=0\times D_{i+4}+0\times D_{i+3}+1\times D_{i+2}+0\times D_{i+1}+1\times D_i=D_{i+2}+D_i$$

Це означає, що чергове значення *m*-послідовності утворюється шляхом додавання за (mod)2 вмістимого нульового і другого тригерів лінійного регістра зсуву побудованого по конфігурації Фібоначчі (рис.2), а породжуючий примітивний нормований поліном k(X) буде наступним:

$$k(X)=k_nX^n+k_{n-1}X^{n-1}+\ldots+k_1X^1+k_0X^0=k_5X^5+k_4X^4+k_3X^3+k_2X^2+k_1X^1+k_0X^0=$$
$$=1\times X^5+0\times X^4+0\times X^3+1\times X^2+0\times X^1+1\times X^0=X^5+X^2+1$$

Після багатократного використання вищеописаного методу для вирішення «зворотної» задачі, знайдемо всі примітивні поліноми, які породжують всі, отримані шляхом децимації згідно алгоритму Голда, спарені *m*-послідовності. Множина оптимальних (отриманих вищенаведеним способом) пар примітивних поліномів для найчастіше вживаних степенів (n = 5, 6, 7, 9, 10)

співпадає з аналогічною множиною оптимальних пар примітивних поліномів, які можуть бути обчислені з використанням дещо складнішого (для низьких степенів поліномів) загальновідомого методу Берлекемпа-Мессі.

5. Загальні параметри створеної програми

Створена і протестована спеціальна комп'ютерна програма, яка видає множини впорядкованих (згідно заданого критерію) кодів Голда та (при необхідності) їх кореляційні характеристики в електронному виді (на екран), або у виді друкованого лістингу (паперовий формат). За необхідності можливе отримання деяких інших необхідних для проектування параметрів кодових послідовностей залежно від специфіки створюваної прикладної системи.

Мова програмування − об'єктно- (і/або процедурно-) орієнтована мова типу PYTHON, текст програми містить необхідні коментарі та пояснення, передбачена процедура інсталяції програми на будь-якому персональному комп'ютері в середовищі операційних систем WINDOWS або LINUX.

Передбачений також зручний і «дружній» діалог програми з користувачем, який повинен бути заздалегідь ознайомлений з особливостями її структури, побудови та функціонування. Користувач повинен також освоїти команди для оперативного діалогу з програмою згідно з відповідною інструкцією.

Висновки і рекомендації

Проаналізовані окремі теоретичні та практичні аспекти синтезу ансамблів псевдовипадкових послідовностей кодів Голда з використанням відомої процедури децимації для утворення «оптимальних» пар m-послідовностей і відповідних примітивних поліномів, що їх породжують. Наведений словесний відповідний алгоритм та варіант адекватних структурно-функціональних блок-схем процедури синтезу.

Приведений аналітичний метод на базі рекурентного алгоритму, що зокрема застосовується в криптографії, з прикладом визначення коефіцієнтів примітивного полінома за наперед відомим неперервним фрагментом (довжиною не менше 2×n символів) відповідної йому децимованої m-послідовності. Передбачається, що цей метод може бути ефективнішим (за обчислювальною складністю) для порівняно невеликих значень ($5 \le n \le 10$) степенів примітивних поліномів, ніж використання для цієї мети методу Берлекемпа-Мессі.

Сформульовані і досліджені деякі критерії, які характеризують авто- та взаємо- кореляційні властивості кодів Голда, що дозволяє впорядковувати їх та вибирати для практичних потреб необхідну кількість кодів із найкращими, залежно від області застосування, кореляційними характеристиками.

Розроблена сервісна програма на мові PYTHON, яка забезпечує зручний інструментарій для генерації кодів Голда, обчислення їх кореляційних характеристик, впорядкування згідно заданого критерію та видавання потрібної кількості потенційно найкращих, залежно від специфіки сфери застосування, псевдовипадкових кодових послідовностей Голда.

Автори бачать доцільність продовження теоретичних і практичних досліджень за даною тематикою, зокрема, в таких напрямках:

а) дослідження можливості (або неможливості) збільшення кількості кодів із параметрами, які відповідають обмеженням на ВКФ згідно алгоритму Голда, шляхом множинного їх об'єднання з різних ансамблів для визначеного однакового періоду;

б) дослідження особливостей синтезу і, відповідно, кардинальність множин та кореляційні характеристики не бінарних кодів Голда, тобто кодів які утворюються на базі p-значних m-послідовностей з елементів простого GF(p) і розширеного GF(pn) полів Галуа.

Список використаних літературних джерел

[1]. Gold R. Optimal Binary Sequences for Spread Spectrum Multiplexing. IEEE Trans. on Information Theory. 1967, vol. IT-13, no. 4, pp. 619–621. doi: 10.1109/TIT.1967.1054048.

[2]. Ipatov V. P. Spread Spectrum and CDMA: Principles and Applications. Lesly, USA, 2005.
[3]. Peterson W. Error-Correcting Codes. University of Florida, Published by the M.I.T Press, Massachusetts Institute of Technology, New York, London. 1972 – 560p.
[4]. Khaled Rouabah, Salim Attia, Rachid Harba, Philippe Ravier, and Sabrina Boukerma. Optimized Method for Generating and Acquiring GPS Gold Codes. International Journal of Antennas and Propagation. Volume 2015. Article ID 956735, 9 pages http://dx.doi.org/10.1155/2015/956735
[5]. Гурський Т.Г., Жук О.Г., Клімович С.О. Напрямки застосування псевдовипадкових послідовностей в радіомережах спеціального призначення. Вісник Хмельницького національного університету. №6. 2012. с.160-167
[6]. Error-Correcting Codes / W. Wesley Peterson, E.J. Weldon, Jr. / CAMBRIDGE, MASSACHUSETTS, and LONDON, ENGLAND, 1972.
[7]. Шрамченко Б. Л. Аналіз послідовностей на виході зсувного регістру з лінійним зворотним зв'язком /Б. Л. Шрамченко // Збірник статей учасників тридцять третьої Міжнародної науково-практичної конференції Інноваційний потенціал світової науки - XXI сторіччя, 20-27 травня 2015р., Запоріжжя. — 2015. — С. 69-72
[8]. SystemView by Elanix: The User Guide to Advanced Dynamic System Analysis Software for Microsoft Windows, CA, 2007, for Microsoft Windows.
[9]. Beletsky A. Generalized Pseudorandom Generators of the Galoisand FibonacciSequences, CEUR Workshop Proceedings, Vol. 2654, 2020, pp.165-181.

SYNTHESIS OF GOLD'S CODE ENSEMBLES FOR USE IN CELLULAR NETWORKS, NAVIGATION AND PULSED RADAR

Ivan Kolodchak, Ihor Tchaikovskyi, Denys Chornyi

Lviv Polytechnic National University, 12, S. Bandery Str., Lviv, 79013, Ukraine

An algorithm for the synthesis of ensembles of pseudorandom sequences of binary Gold codes is considered using the procedure for the formation of the so-called "paired" m-sequence, which is generated by decimation (thinning) from the corresponding primitive polynomial of degree n, where $5 \le n \le 10$. As a result, an optimal (preferred) pair of m-sequences is formed, which gives rise to one ensemble of the above-mentioned codes. It is shown that there can be a sufficiently large number of such different (for a specific value of the degree of the primitive polynomial n) ensembles, which allows the designer of the corresponding system to change the signature of the used Gold codes according to a random law, while ensuring the required noise immunity of the system. An example of the use of a recurrence algorithm used in cryptography to search for the values of the coefficients of the corresponding primitive polynomial, which is included in the optimal pair of polynomials, according to a known arbitrary continuous fragment of the m-sequence with a length of at least 2×n elements, is proposed and given. Some simplification of this procedure is envisaged due to the use of such a method for determining the coefficients of a primitive polynomial, including its implementation by forming and solving (for example, by the classical Gaussian method, taking into account the peculiarities of trivial binary modular arithmetic) a system of linear equations with coefficients, free terms and unknowns that represent the elements of the Galois field. In addition, the application of the method of formation of a linear system of equations on the basis of the difference recursion equation, together with the above, will provide less computational complexity (for relatively small values of n above) than in the case of using, for such purposes, the well-known Berlekamp-Massey algorithm. Criteria for ordering Gold codes have been proposed, taking into account their correlation properties, as well as a service algorithm in a high-level programming language has been developed for synthesis and selection from a certain ensemble of the required number of Gold codes with the best, depending on the field of their application, correlation properties.

Ключові слова: *pseudorandom codes, m-sequences, Gold codes, recursion equations, Galois field, primitive polynomial, addition (multiplication) modulo, ensemble of codes, periodic, aperiodic, auto- and intercorrelation functions of discrete pseudorandom sequences*