



РАДІОЕЛЕКТРОНІКА

<https://doi.org/10.23939/ictee2025.01.109>

СИНТЕЗ АНСАМБЛІВ КОДІВ ГОЛДА ДЛЯ ЗАСТОСУВАННЯ У 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 (прорідження) генерується з відповідного примітивного полінома степеня n , де $5 \leq n \leq 10$. 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 багато, що дає можливість проєктанту відповідної системи за випадковим законом змінювати сигнатуру використовуваних кодів Голда, забезпечуючи потрібну завадостійкість системи. Запропоновано і наведено приклад використання рекурентного алгоритму, що застосовується в криптографії, для пошуку значень коефіцієнтів відповідного примітивного полінома, який входить в оптимальну пару поліномів, за відомим довільним неперервним фрагментом m -послідовності завдовжки не менше ніж $2 \times n$ елементів. Передбачається деяке спрощення цієї процедури із використанням такого способу визначення коефіцієнтів примітивного полінома, зокрема його реалізацію за допомогою утворення і розв'язання (наприклад, класичним методом Гауса з урахуванням 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 основі різницевого рівняння рекурсії разом із вищевказаним забезпечить меншу обчислювальну складність (для порівняно невеликих вищенаведених значень n), ніж у випадку використання для таких цілей відомого алгоритму Берлекемпа – Мессі. Запропоновано критерії впорядкування кодів Голда, зважаючи на їхні 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 сфери 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 взаємкореляційні функції дискретних псевдовипадкових послідовностей.

Вступ і постановка задачі

Аналіз відповідних публікацій [2, 4–6] показує, що простежується стійка тенденція зростання і постійного удосконалення стільникових мереж із кодовим розділенням (CDMA) і множинним асинхронним доступом, а також систем супутникової та наземної навігації [4, 5]. В названих

системах широко використовують для різних цілей слабкокорельовані 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 модульовальних функцій для синтезу бінарних фазоманіпульованих зондувальних радіосигналів у спеціалізованих радіолокаторах, що працюють по малопомітних високодинамічних повітряних цілях за наявності певних апріорних цілевказівок щодо дальності та кутових координат. Саме тому актуальна проблема зручного і швидкого синтезу ансамблів таких кодів та аналізу їх кореляційних властивостей [2, 7, 6]. Позитивною особливістю ПВП Голда є те, що їх доволі багато і для заданого степеня примітивного полінома n строго обмеженим зверху та порівняно незначним є рівень паразитних пелюсток їхніх періодичних авто- та взаємкореляційних функцій (АКФ_П та ВКФ_П). Зокрема, для $n = 10$ існує 300 ансамблів кодів Голда із 1025 кодами в кожному та з періодом повторення коду $N = 2^n - 1$, а у разі необмеженого зростання $N \rightarrow \infty$, максимальні значення паразитних пелюсток АКФ_П та ВКФ_П $\rightarrow 1/\sqrt{N}$, тобто наближаються до класичної границі Велча [2]. У статті зроблено спробу проаналізувати порівняно нескладний алгоритм синтезу ансамблів кодів Голда із використанням процедури децимації, наведеної в [1, 2], та розв'язанням “зворотної” задачі, яка полягає у визначенні коефіцієнтів примітивного полінома за повністю (або фрагментарно) відомою децимованою m -послідовністю. Сформульовано критерії упорядкування отриманих кодів Голда згідно із їхніми авто- та взаємкореляційними властивостями, а також розроблено 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, у [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 $n \equiv 0 \pmod{4}$ кодів Голда не існує, тому значення степеня примітивного полінома $n=8$ не розглядається. Використаємо процедуру децимації бінарних m -послідовностей, яка наведена в [1, 2] і складається, залежно від парності чи непарності степеня n примітивного полінома, із декількох порівняно нескладних логічно обумовлених правил і висновків, які наведемо нижче, описуючи алгоритм синтезу. Генерація ансамблів кодів Голда здійснюється однойменним алгоритмом із застосуванням (для отримання опорної m -послідовності) класичного регістра зсуву із лінійними зворотними зв'язками (РЗЛЗЗ) [2, 3, 6].

Генерація кодів відбувається із використанням у цьому алгоритмі таких параметрів, констант та змінних, зокрема:

- n – степінь примітивного полінома, а також кількість двійкових тригерів у регістрі РЗЛЗЗ для генерації опорної m -послідовності, з якої після специфічної процедури “децимації за Голдом” 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 параметра n всіх примітивних поліномів, що описуються математичним апаратом (алгеброю) кінцевих полів, а їх коефіцієнти належать простому полю Галуа GF(2). Названі множини примітивних поліномів зведено в таблицях, зокрема в [3, 6], причому множина МП-5 ($j=1, \dots, 6$) містить шість поліномів, множина МП-6 ($j=1, \dots, 6$) – також шість, множина МП-7 ($j=1, \dots, 18$) містить 18 поліномів, множина МП-9 ($j=1, \dots, 48$) – 48 поліномів, множина МП-10 ($j=1, \dots, 60$) містить 60 поліномів. Усі вони є масивами бінарних констант, а кожен кодовий рядок, наведений у названих масивах, складається із $(n+1)$ впорядкованих двійкових (0 або 1) символів, які означають, що:

– перший символ зліва та останній символ справа завжди дорівнюють 1, що означає, по-перше, що вихід кінцевого суматора за $(\text{mod})2$ (це 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 із максимальним для заданого n періодом;

– усі інші $(n-1)$ двійкових символів відображають використання (тоді символ коефіцієнта в перемножувачах РЗЛЗЗ = 1) або не використання (символ коефіцієнта в перемножувачах РЗЛЗЗ = 0) вмісту 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 під час кожного i -го часового зсуву послідовно формуються відповідні значення утворюваної опорної періодичної із 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 $k_i \in \text{GF}(p)$, де $i = 0, 1, \dots, n$, має такий вигляд:

$$\begin{aligned} k(X) &= k_n \times X^n + k_{n-1} \times X^{n-1} + k_{n-2} \times X^{n-2} + \dots + k_2 \times X^2 + k_1 \times X^1 + k_0 \times X^0 = \\ &= (1) \times X^n + (0(1)) \times X^{n-1} + (0(1)) \times X^{n-2} + \dots + (0(1)) \times X^2 + (0(1)) \times X^1 + (1) \times X^0 \end{aligned}$$

- d – допустимий (згідно із алгоритмом Голда) індекс децимації [прорідження за $(\text{mod})N$] 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 фіксують їх значення протягом лише одного періоду;

- $M = (2^n - 1) + 2$ – кількість (кардинальність) різних кодів Голда, ураховуючи дві m -послідовності з оптимальної пари, що входять в один ансамбль. Їх генерація повинна здійснюватися для всіх можливих опорних m -послідовностей, примітивні поліноми яких перераховані у вищеназваних масивах МП- $n(j)$, за допомогою їх децимації з деякими індексами d_L , які відповідають вимогам алгоритму, забезпечуючи утворення оптимальних пар.

Генерація усіх можливих ансамблів кодів Голда здійснюється для кожного примітивного полінома, множину яких задано 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 наведених нижче кроків.

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

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

3. Для отриманої вище “опорної” m -послідовності U_i визначити множину допустимих індексів децимації $(d_1, \dots, d_L)$, які задовольняють умови алгоритму Голда, тобто для $d_L = 2^s + 1$, де s є взаємно простим числом (ВПЧ) з n , за умови, що n – непарне або ж s є парним і утворює ВПЧ з $(n/2)$, якщо n – парне та одночасно $n \neq 0(\text{mod})4$. Діапазон зміни індексів децимації повинен входити в інтервал $[3 \leq (d_1, \dots, d_L) \leq N-1]$, 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 за допомогою прорідження опорну m -послідовність U_i , L m -послідовностей $V_1, V_2, \dots, V_L$, для яких $V_1 = U_{(i \times d_1) \text{ mod } N}$, $V_2 = U_{(i \times d_2) \text{ mod } N}$, $\dots$, $V_L = U_{(i \times d_L) \text{ mod } N}$, де остаточний індекс, що вказує на вибраний символ U_i , обчислюють як $(i \times d_i) \text{ mod } N$. Отже, 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 із відповідною їм “оптимальною” парою спарених m -последовностей) $N+2 = (2^n-1)+2$.

5. Для кожної з L отриманих оптимальних пар $\{[U_i, V_{(i \times d1) \bmod N}], [U_i, V_{(i \times d2) \bmod N}], \dots, [U_i, V_{(i \times dL) \bmod N}]\}$ згенерувати, циклічним зсувом децимованої m -последовності (V) на N позицій з порозрядним (після кожного зсуву на один розряд) додаванням з (U_i) за $(\bmod 2)$, L ансамблів по N последовностей Голда в кожному із них (структурно-функціональна блок-схема, рис. 3), запам'ятавши їх значення завдовжки в період.

6. Якщо вибраний примітивний поліном не є останнім у плинному масиві МП- $n(j)$, необхідно 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- $n(j)$, потрібно 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 й збережені в пам'яті комп'ютера.

Оскільки первинне завдання реалізації вищеописаного алгоритму – отримання опорної m -последовності, яка задається черговим (вибраним із заданих масивів) примітивним поліномом, стисло наведемо основні варіанти реалізації такої процедури. Згідно із [3, 6], відомі три теоретично обгрунтовані способи генерації m -последовностей. Наведемо їх.

А. Перший спосіб.

Утворюється система, що складається з i рекурентних різницевих рівнянь, яка впливає з фундаментальної вимоги, що скалярний добуток $(n+1)$ -значного вектора відповідних коефіцієнтів примітивного полінома та $(n+1)$ -значного вектора відповідних (неперервно обчислюваних) плинних символів рекурсії, починаючи із символів вектора початкового стану, дорівнює нулю, а саме:

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

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

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

яку розв'язуємо відносно елементів невідомої періодичної рекурсивної последовності $[D_0, D_1, \dots, D_{N-2}, D_{N-1}]$ за відомого примітивного полінома $k(X) = k_0 X^0 + k_1 X^1 + \dots + k_{n-1} X^{n-1} + k_n X^n$ степеня n (причому $k_0 \neq 0$ а $k_n=1$) та наперед заданого ненульового вектора початкового стану $[D_0 \dots D_{n-1}]$. Тобто у цьому 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 -последовності в розширеному полі Галуа $\text{GF}[p^n]$. Зауважимо, що примітивний поліном $k(X)$ повинен ділитися без остачі поліном-двочлен X^N-1 , а N у такому разі – найменше число, для якого таке ділення справедливе. Апаратно вищеописана процедура реалізується, як правило, лінійною комутуваною схемою на базі регістра зсуву із 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.

Багаторазовно обчислюють, починаючи з деякого наперед заданого ненульового вектора початкового стану $[D_0 \dots D_{n-1}]$, 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 $i = 0, 1, \dots, +\infty$ (додатні цілі числа, ураховуючи число 0); $D_i, D_{i-1}(X)$ – конкретні (для заданого $i = 1$ або $2, \dots$, або p^n-1) поліноми степенів $\leq(n-1)$, що утворюють циклічну мультиплікативну групу розширеного поля Галуа $\text{GF}(p^n)$; $(k_n)^{-1}$ – 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 плінного полінома $D_{i-1}(X)$ його найстарший $(n-1)$ -й коефіцієнт стає n -м і множиться на $(k_n)^{-1}$ та на примітивний поліном $k(X)$. Потім отриманий поліном-добуток віднімають 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 із 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 вищезначеним додатним цілим числом i , що використовується як індекс у вищенаведеному співвідношенні, а зворотні зв'язки визначають, розв'язавши рівняння $k(X) = 0$ відносно найстаршого $(n$ -го степеня) одночлена.

В. Третій спосіб.

Обчислюють усі послідовні значення елементів m -послідовності (як послідовні частки), виконуючи ділення одного із $(p^n - 1)$ довільних ненульових поліномів степеня $\leq(n-1)$ 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 $m_i = [(0, \dots, p-1) \in \text{GF}(p)]$, які розміщені біля степенів полінома-частки $m(x)$, що постійно зростають під час обчислення, а саме:

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

де $i = 0, 1, \dots, +\infty$ – кількість обчислень, причому, якщо $i-1 = p^n-1$, то генерується один період m -послідовності. Така процедура впливає із відомої [3, 6] теореми Цирлера і також може бути реалізована лінійною комутованою схемою на базі регістра зсуву з лінійними зворотними зв'язками. Наприклад, для розширеного поля Галуа $\text{GF}(2^n)$, пам'яті регістра ($n=3$) та примітивного полінома $k(X) = X^3 + X^2 + 1$ (його двоїстий еквівалент $k^*(X) = X^3 \times \left(\frac{1}{X^3} + \frac{1}{X^2} + \frac{1}{1} \right) = 1 + X^1 + X^3$), список поліномів, які у цьому випадку можуть бути початковими діленими з вагами $(X^0 + X^1 + X^2)$, утворює множину із семи породжувальних 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 $\text{GF}(2^3)$. Підстановка (і як первинних ділених, і як початкових значень) членів цієї групи задає такі допустимі 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, що для всіх трьох вищенаведених способів генерації m -послідовностей справедливі також певні застереження:

АА. Допустимим є множення (а фактично це ділення) плинного полінома на одноклен $X^{-1} = 1/X$ у використаних математичних виразах або, відповідно, зсув у бік молодших розрядів у лінійних регістрах зсуву за апаратної реалізації. Потрібно зважати на зміну зворотних зв'язків, які у такому разі визначатимуться двоїстим примітивним поліномом та оберненими утворювальними 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 за двійним модулем і позначають відповідно як $[(\text{mod})k(X), p]$, причому за $(\text{mod})p$ обчислюють (після зведення подібних членів) коефіцієнти отриманого (плинного) полінома, а за $(\text{mod})k(X)$ – сам плинний поліном, якщо його степінь $\geq n$.

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

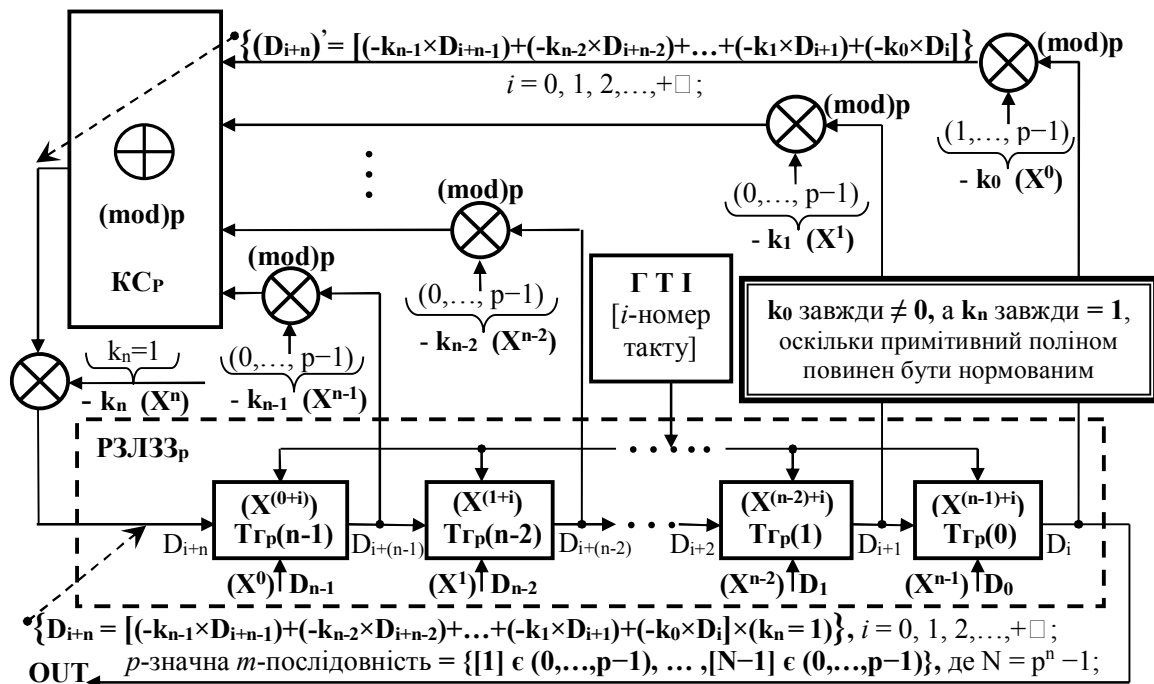


Рис. 1 Структурно-функціональна блок-схема генерації p -значної m -послідовності за допомогою регістра РЗЛЗЗ_p, побудованого за схемою Фібоначчі

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

– інформаційний вихід кожного тригера з'єднаний із першим входом відповідного перемножувача, а також з інформаційним входом наступного тригера, причому інформаційний

вихід найстаршого тригера [Тг(0)] (його розрядна вага задана 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 задана степенем X^{0+i}) з'єднаний із виходом суматора вузла зворотного зв'язку через перемножувач на старший коефіцієнт k_n примітивного полінома $k(X)$;

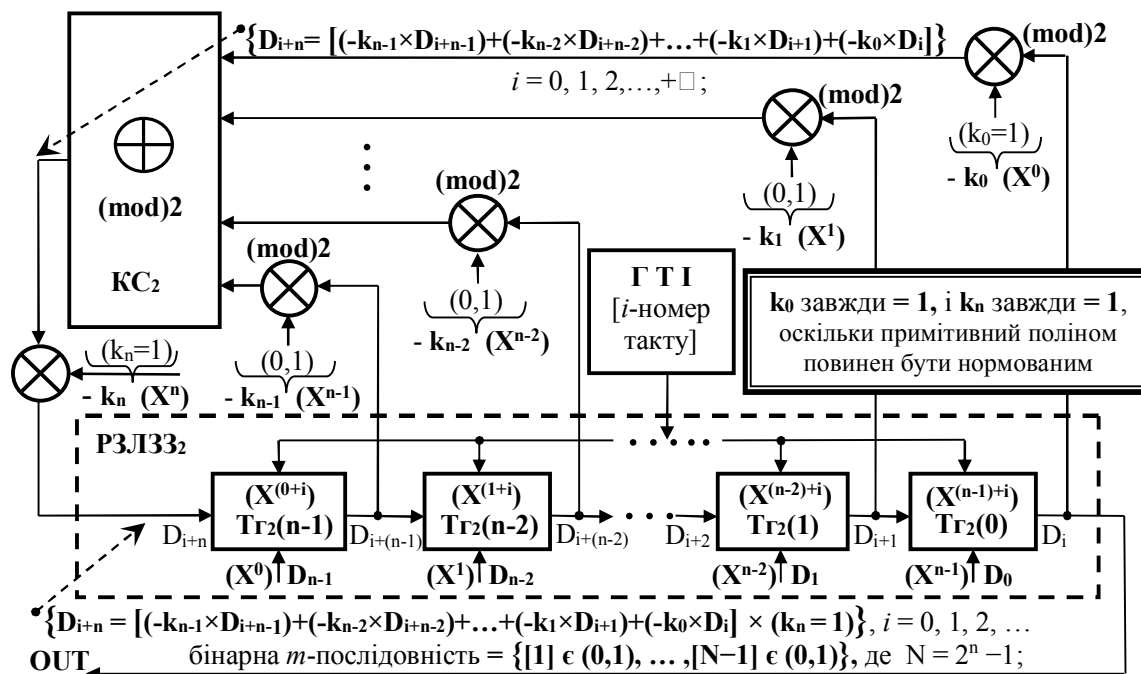


Рис. 2. Структурно-функціональна блок-схема генерації бінарної m -послідовності за допомогою регістра РЗЛЗЗ, побудованого за схемою Фібоначчі

- на другі входи перемножувачів подаються відповідні протилежні відповідному за модулем значення коефіцієнтів примітивного полінома, який породжує цю m -послідовність;
- інформаційні входи ($D_{n-1}, D_{n-2}, \dots, D_1, D_0$) з відповідними порозрядними вагами ($X^0, X^1, \dots, X^{n-2}, X^{n-1}$) для початкового встановлення тригерів під'єднані до стартової схеми (на рисунках не показано), причому початкова комбінація зі всіх нулів строго заборонена;
- на входи керування кожного тригера від генератора тактових сигналів (ГТІ) надходять імпульси, робочий фронт яких ініціює одночасний i -й зсув плинного інформаційного коду регістра у бік старших розрядів та відповідну зміну його стану з урахуванням перехідного процесу в колі зворотного зв'язку, що реалізується як класична комбінаційна схема, тобто як багатовходовою із одним виходом логічна функція Буля.

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

Конфігурація Фібоначчі забезпечує також, що символи генерованої m -послідовності можуть неперервно зчитуватися як із 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 основі вищенаведених трьох математично обґрунтованих способів синтезу m -послідовностей можна утворити декілька (більш або менш ефективних) матричних методів обчислення зазначених псевдовипадкових послідовностей із використанням фундаментального співвідношення між плинними $[S(i)]$ та наступними $[S(i+1)]$ станами у вигляді функції

переходів (як для кінцевих абстрактних цифрових автоматів) із наперед заданим ненульовим початковим станом $[S(0)]$, а саме:

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

де $i = 0, 1, 2, \dots, +\infty$ (цілі додатні числа, ураховуючи число 0), G^T – транспонована супутня матриця примітивного полінома $k(X)$ (фактично це матриця функції переходів розмірністю $n \times n$ елементів), яка складається із розташованих у певний спосіб трьох компонент, а саме: із одиничної матриці E [розмірністю $(n-1) \times (n-1)$ елементів], що утворюється (починаючи зверху) послідовним зсувом вправо примітивного найменшого утворювального елемента циклічної мультиплікативної групи поля $GF(p^n)$, із нижнього рядка, яка, своєю чергою, складається з n молодших коефіцієнтів примітивного полінома в результаті розв’язання рівняння $k(X)=0$ відносно найстаршого одночлена n -го степеня та з крайнього лівого нульового 0-вектора-стовпця розмірністю $(n-1)$ елементів.

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

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

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

На структурно-функціональних блок-схемах (рис. 1–3) використано такі умовні позначення та скорочення:

KC_2, KC_p – комбінаційні схеми з менше ніж n входами та одним виходом, що реалізують підсумування за $(\text{mod})2$ або за $(\text{mod})p$ відповідних символів із виходів тригерів регістра зсуву, помножених [за $(\text{mod})p$ або за $(\text{mod})2$] на протилежні $[-k_n, -k_{n-1}, \dots, -k_2, -k_1]$ або первинні $[k_n, k_{n-1}, \dots, k_2, k_1]$ коефіцієнти примітивного полінома;

$T_{p1}(0), \dots, T_{p1}(n)$ та $T_{p2}(0), \dots, T_{p2}(n)$ – тригери (p -значні та двійкові елементи пам’яті), що сукупно утворюють саме регістри зсуву в РЗЛЗЗ_p та РЗЛЗЗ₂ відповідно;

G_i – генератор i -х тактових імпульсів, фронти та частота яких ініціюють процес генерації, зокрема зсув, підсумування та множення відповідних символів, а також визначають швидкість зміни вихідного ПВК;

$[(1), (2), \dots, (N-2), (N-1)] \in (0, \dots, p-1)$ – ці символи означають, що значення кожного елемента вихідного псевдовипадкового коду належить ($\in$) множині допустимих значень $(0, \dots, p-1)$ для p -значної m -послідовності;

$[(1), (2), \dots, (N-2), (N-1)] \in (0, 1)$ – ці символи означають, що значення кожного елемента вихідного псевдовипадкового коду належить ($\in$) множині допустимих значень $(0, 1)$ для двозначної (бінарної) m -послідовності;

$(1), (2), (3), \dots, (N-3), (N-2), (N-1)$ – розряди регістрів, що зберігають символи сформованої наведеним вище алгоритмом пари оптимальних m -послідовностей;

OUT – вихід послідовного коду згенерованої m -послідовності;

$\rightarrow (\pm 1)$ – оператор перетворення символів, заданих у логічному (0,1) двійковому базисі, в знаковміний сигнальний базис (± 1) , що дозволяє подальше використання необхідних операцій звичайного множення для утворення потрібних модульованих сигнально-кодових конструкцій.

Решту використаних на рисунках умовних позначень та скорочень, не вказаних у цьому списку, розшифровано вище в пункті 2 (у словесному описанні алгоритму синтезу кодів Голда) або нижче в пункті 4 (в описанні системи рівнянь для розв’язання зворотної задачі).

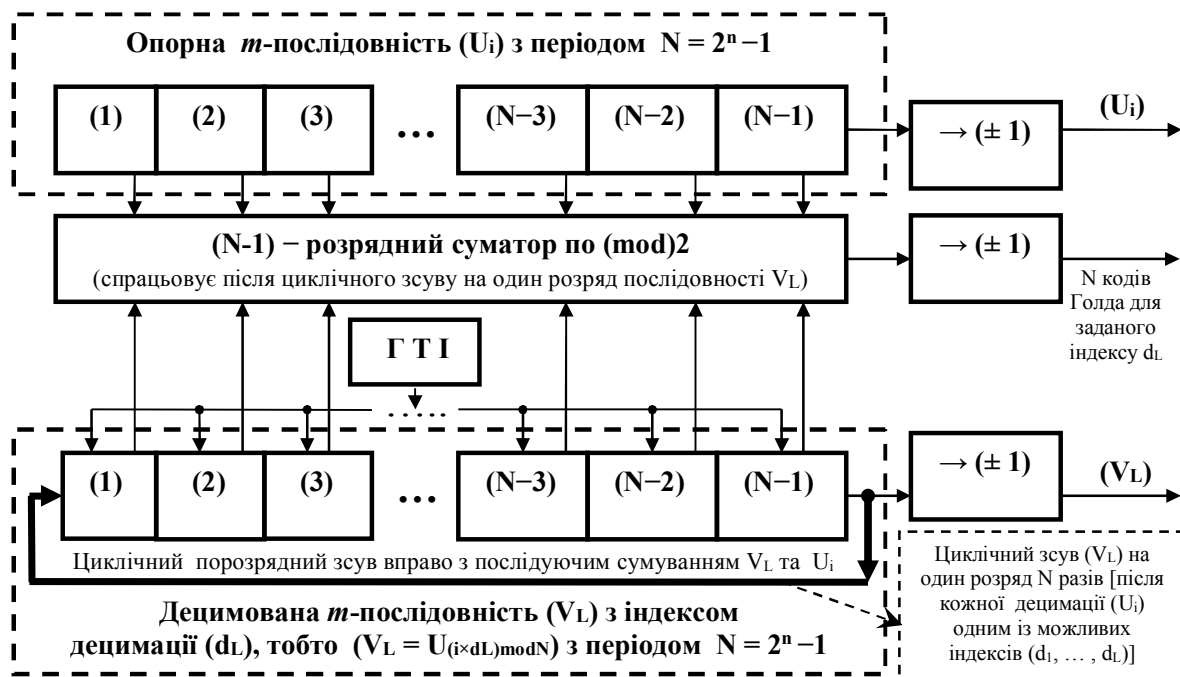


Рис. 3. Структурно-функціональна блок-схема генерації одного ансамблю бінарних кодів Голда із пари оптимальних m -послідовностей

3. Критерії упорядкування кодових послідовностей Голда згідно із їх кореляційними властивостями та характеристиками

Головною перевагою кодів Голда є практичне застосування у 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 (для мінімізації взаємних завад, особливо під час роботи в режимах залпової атаки по одній цілі), є їх порівняно незначна та строго обмежена зверху [1, 2] взаємна “паразитна” кореляція. Саме тому, щоб вибрати із деякого ансамблю для практичного застосування конкретну підмножину кодів Голда, повинна бути доступна інформація стосовно небажаних “паразитних” взаємкореляційних впливів між різними такими псевдовипадковими кодовими послідовностями. Після обчислення різних авто- та взаємкореляційних функцій кодів Голда актуалізується завдання їх відповідного впорядкування, що потребує певних специфічних критеріїв, зокрема:

- а) за зростанням модуля максимального значення усіх пелюсток (для ВКФ) та максимальних бічних пелюсток (для АКФ);
- б) за зростанням модуля середнього значення усіх пелюсток (для ВКФ) та середнього значення бічних пелюсток (для АКФ);
- в) за зростанням середньоквадратичного відхилення усіх пелюсток (для ВКФ) та середньоквадратичного відхилення бічних пелюсток (для АКФ);
- г) за зростанням певної комбінації всіх вищезазначених критеріїв для ВКФ і АКФ.

Незалежно від того, яку функцію виконує ПВП Голда в системі: синхронізація інформаційних потоків у мережі CDMA; ідентифікація даних місцезнаходження від різних давачів (супутників, маяків) у супутникових та наземних навігаційних комплексах; вимірювання параметрів (часу затримки, частоти Доплера, 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 доволі складною. Оскільки в нашому випадку для вищезазначених застосувань тип і форма модулювальної функції (тобто комплексної обвідної сигналу) наперед відомі, рішення про наявність (або відсутність) корисного сигналу приймають після демодулятора із використанням методу максимальної правдоподібності за допустимих рівнів вихідних помилок.

Розглянемо завадостійкість виявлення, враховуючи тільки негативний вплив ненульової “паразитної” авто- та взаємкореляції, оскільки вплив власного гаусівського шуму приймального тракту добре вивчений, а вплив зовнішніх завад істотно залежить від їхніх 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 модулювальні функції) за критерієм зростання (або зменшення) суми математичного сподівання та середньоквадратичного відхилення паразитних пелюсток їх періодичних і аперіодичних автокореляційних (АКФ_П, АКФ_А) та взаємкореляційних (ВКФ_П, ВКФ_А) функцій. Якщо на вхід приймального пристрою від різних джерел надходить адитивна суміш рівновеликих сигналів, модульованих різними кодовими послідовностями Голда, а виявляти потрібно тільки той радіосигнал, який модульований одним конкретним кодом (“ключем”, присвоєним цьому пристрою), то для застосування оптимального алгоритму виявлення необхідно знати статистичні характеристики (наприклад, закон розподілу ймовірностей) суміші “паразитних” авто- та взаємкореляцій між різними кодами. Такі завади в [2] класифікують 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 пакета “System View” [8] для системного моделювання радіоелектронних пристроїв, зокрема, графіки законів розподілу (не нормованих до одиниці) випадкових процесів сумарної “паразитної” взаємкореляції та нормального (гаусівського) шуму приймального тракту, де: крива 1 – сумарний закон розподілу ймовірностей “паразитної” взаємкореляції деякої множини різних кодів Голда; крива 2 – сумарний закон розподілу ймовірностей “паразитної” взаємкореляції 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” взаємкореляції зі зростанням кількості кодових сигнатур (крива 1 – побудована для 24 кодів, що надходять на вхід приймача з різними часовими затримками) наближається до нормального. Це означає, що й сумарний (разом із тепловим шумом приймального тракту, крива 3) розподіл є практично нормальним (крива 2). Отже, застосування алгоритму максимальної правдоподібності для виявлення сигналу є коректним і практично допустимим.

На рис. 5 подано аперіодичну взаємкореляційну функцію (ВКФ_А графік С-1, С-2) сумарної демодульованої суміші сигналів (у 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 істотно відрізняються за рівнем та часом затримки від отриманого без завад (С-3) сигналу, оскільки перший (С-1) збігається за часом з максимальною (додатною), а другий (С-2) – із максимальною (від’ємною) “паразитною” взаємкореляцією. Графік С-3 – це АКФ_А сигналу, який фіксує нульовий (опорний) зсув за часом затримки та рівень автокореляції сигналу за відсутності зовнішніх завад і власного шуму приймача.

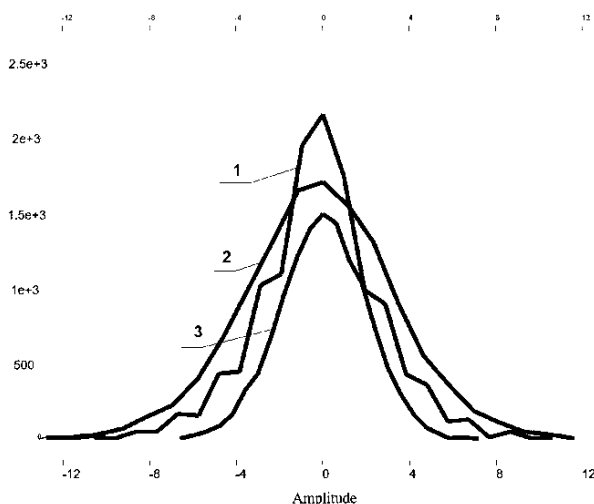


Рис. 4. Графіки густини ймовірностей випадкових процесів паразитної взаємкореляції, власного шуму приймального тракту та їх суми

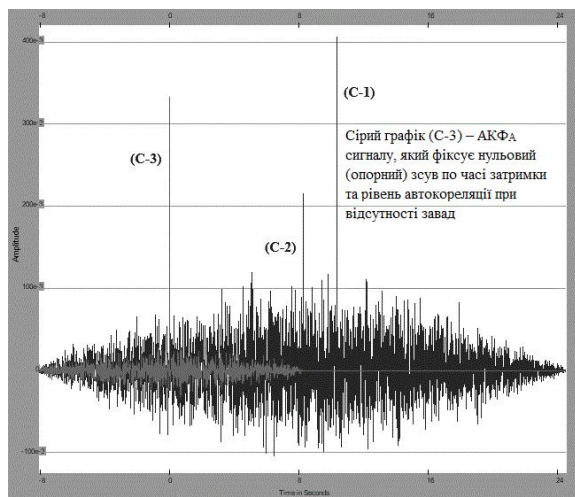


Рис. 5. Виявлення того самого сигналу в присутності тільки паразитної взаємкореляції для найбільшого додатного (C-1) та найбільшого від'ємного (C-2) значень її величин

Зважаючи на результати моделювання, можна зробити висновок, що оптимальним критерієм упорядкування кодів Голда для достатньо ефективного ймовірнісного виявлення є критерій мінімуму суми математичного сподівання і середньоквадратичного відхилення їх “паразитної” взаємкореляції.

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

Коефіцієнти примітивного полінома або ж (що еквівалентно) структури зворотних зв'язків регістра РЗЛЗЗ за наперед відомим степенем полінома n та конкретних значень неперервного фрагмента (довжиною не менше від $2 \times n$ символів) згенерованої ним m -послідовності, можна знайти із використанням рівняння рекурсії. За допомогою рівняння складають і розв'язують систему із n лінійних рівнянь відносно невідомих коефіцієнтів примітивного полінома. Рівняння рекурсії (як зазначено вище) є різницеvim рівнянням [2, 3, 6], яке дає змогу визначати чергове (наступне) значення m -послідовності у вигляді лінійної комбінації n попередніх її значень. Такі рекурентні співвідношення, зокрема, широко застосовують у 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 таке рівняння рекурсії (1), з невідомими коефіцієнтами примітивного полінома:

$$D_{i+n} = (-k_{n-1}) \times D_{i+n-1} + (-k_{n-2}) \times D_{i+n-2} + \dots + (-k_1) \times D_{i+1} + (-k_0) \times D_i, \quad (1)$$

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

Надалі розглядатимемо тільки бінарні ПВП, для яких існують лише два елементи поля Галуа $(0,1) \in GF(2)$, причому первинні й протилежні їм елементи в цьому полі збігаються, тобто $0 = (-0) = 0(\text{mod})2$ та $1 = (-1) = 1(\text{mod})2$. Як наслідок, у всіх нижченаведених рівняннях елементи вектора $[k_{n-1}, k_{n-2}, \dots, k_1, k_0]$ записані без знака, оскільки завжди $k_i = (-k_i)$.

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

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

Оскільки ліва частина утвореної системи лінійних рівнянь складається із n скалярних добутоків вектора постійних коефіцієнтів $[k_{n-1}, k_{n-2}, \dots, k_1, k_0]$ з кожним із n -значних векторів рекурентно і послідовно зсунутих на i тактів даних (D_i) , система (2) в матричній формі матиме такий вигляд (3):

$$\begin{bmatrix} D_{n-1} & D_{n-2} & D_{n-3} & \dots & D_2 & D_1 & D_0 \\ D_n & D_{n-1} & D_{n-2} & \dots & D_3 & D_2 & D_1 \\ D_{n+1} & D_n & D_{n-1} & \dots & D_4 & D_3 & D_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ D_{2n-4} & D_{2n-5} & D_{2n-6} & \dots & D_{n-1} & D_{n-2} & D_{n-3} \\ D_{2n-3} & D_{2n-4} & D_{2n-5} & \dots & D_n & D_{n-1} & D_{n-2} \\ D_{2n-2} & D_{2n-3} & D_{2n-4} & \dots & D_{n+1} & D_n & D_{n-1} \end{bmatrix} \times \begin{bmatrix} k_{n-1} \\ k_{n-2} \\ k_{n-3} \\ \dots \\ k_2 \\ k_1 \\ k_0 \end{bmatrix} = \begin{bmatrix} D_n \\ D_{n+1} \\ D_{n+2} \\ \dots \\ D_{2n-3} \\ D_{2n-2} \\ D_{2n-1} \end{bmatrix} \pmod{2} \quad (3)$$

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

Наведемо приклад, який наочно демонструє практичний аспект використання вищенаведених теоретичних залежностей для розв'язання “зворотної” задачі. Нехай у нашому випадку є деяка бінарна m -послідовність з періодом $N=2^n-1$, де $n=5$, яка утворена за допомогою децимації, згідно із алгоритмом 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) завдовжки 2×5 символів кожен, наприклад:

$$\Phi p1 = \{1 = D_0, 1 = D_1, 1 = D_2, 1 = D_3, 1 = D_4, 0 = D_5, 0 = D_6, 0 = D_7, 1 = D_8, 1 = D_9\}$$

$$\Phi p2 = \{1 = D_0, 0 = D_1, 1 = D_2, 1 = D_3, 1 = D_4, 0 = D_5, 1 = D_6, 0 = D_7, 1 = D_8, 0 = D_9\}$$

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

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

Довільно (без негативного впливу на результат) прийнявши, що послідовність $[D_0 \ D_1 \ D_2 \ D_3 \ D_4 = 1 \ 1 \ 1 \ 1 \ 1]$ для Фр1 та послідовність $[D_0 \ D_1 \ D_2 \ D_3 \ D_4 = 1 \ 0 \ 1 \ 1 \ 1]$ 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 $(\text{mod})2$ у полі Галуа $\text{GF}(2)$, розв'яжемо аналітично методом Гауса (тобто

методом видалення змінних і приведення матриці до трикутного, або близького до нього, вигляду), а саме:

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

Після почергової підстановки в отриману систему рівнянь (4) значень двійкових символів обох відомих неперервних фрагментів тієї самої 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 позначено нижче символом “*”. У першому випадку (для Фр1) достатньо у вихідній розширеній матриці $B_{\text{Фр1}}$ до першого її рядка додати (що еквівалентно відніманню) п’ятий і результат записати на місце п’ятого рядка, а потім скласти другий рядок з п’ятим (вже модифікованим) і результат зафіксувати на місце п’ятого рядка, в результаті чого утворюється класична трикутна матриця і розв’язок стає очевидним.

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

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

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

У другому випадку (для Фр2) достатньо у вихідній розширеній матриці $B_{\text{Фр2}}$ до першого її рядка додати (що еквівалентно відніманню) третій і результат записати на місце третього рядка, а потім скласти перший рядок із п’ятим і результат зафіксувати на місце п’ятого рядка.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} k_4 \\ k_3 \\ k_2 \\ k_1 \\ k_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}; B_{\text{Фр2}} = \left[\begin{array}{ccccc|c} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{array} \right] \Rightarrow \left[\begin{array}{ccccc|c} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0^* & 1^* & 0^* & 1^* & 0^* & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0^* & 1^* & 0^* & 0^* & 0^* & 1 \end{array} \right]^* \Rightarrow$$

$$\Rightarrow \begin{bmatrix} k_4 \times D_4 + k_3 \times D_3 + k_2 \times D_2 + 0 + k_0 \times D_0 = 0 \\ 0 + k_3 \times D_4 + k_2 \times D_3 + k_1 \times D_2 + 0 = 1 \\ 0 + k_3 \times D^* + 0 + k_1 \times D_3 + 0 = 0 \\ 0 + k_3 \times D_6 + 0 + k_1 \times D_4 + k_0 \times D_3 = 1 \\ 0 + k_3 \times D^* + 0 + 0 + 0 = 0 \end{bmatrix}^* \Rightarrow \begin{bmatrix} k_4 = 0 \\ k_3 = 0 \\ k_2 = 1 \\ k_1 = 0 \\ k_0 = 1 \end{bmatrix};$$

Отже, для m -послідовності з її відомими (Фр1, Фр2) фрагментами закон рекурсії та примітивний поліном матимуть такий самий 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 у результаті додавання за (mod)2 вмісту нульового і другого тригерів лінійного регістра зсуву, побудованого за конфігурацією Фібоначчі (рис. 2), а породжувальний примітивний нормований поліном $k(X)$ буде таким:

$$\begin{aligned} k(X) &= k_n X^n + k_{n-1} X^{n-1} + \dots + k_1 X^1 + k_0 X^0 = k_5 X^5 + k_4 X^4 + k_3 X^3 + k_2 X^2 + k_1 X^1 + k_0 X^0 = \\ &= 1 \times X^5 + 0 \times X^4 + 0 \times X^3 + 1 \times X^2 + 0 \times X^1 + 1 \times X^0 = X^5 + X^2 + 1 \end{aligned}$$

Після багаторазового використання вищеприписаного методу для розв'язання “зворотної” задачі знайдемо всі примітивні поліноми, які породжують всі, отримані за допомогою децимації згідно із алгоритмом Голда, спарені m -послідовності. Множина оптимальних (отриманих вищенаведеним способом) пар примітивних поліномів для найчастіше вживаних степенів ($n = 5, 6, 7, 9, 10$) збігається із аналогічною множиною оптимальних пар примітивних поліномів, які можна обчислити із 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 із заданим критерієм) кодів Голда та (за необхідності) їх кореляційні характеристики в електронному вигляді (на екран) або у вигляді друкованого лістингу (паперовий формат). За необхідності можна отримати деякі інші необхідні для проєктування параметри 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 із користувачем, який повинен бути заздалегідь ознайомлений із особливостями її структури, побудови та функціонування. Користувач повинен також засвоїти 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 із використанням відомої процедури децимації для утворення “оптимальних” пар m -послідовностей і відповідних примітивних поліномів, що їх породжують. Наведено словесний відповідний алгоритм та варіант адекватних структурно-функціональних блок-схем процедури синтезу.

Наведено аналітичний метод на основі рекурентного алгоритму, що зокрема застосовується в криптографії, з прикладом визначення коефіцієнтів примітивного полінома за наперед відомим неперервним фрагментом (довжина якого не менше ніж $2 \times n$ символів) відповідної йому децимованої m -послідовності. Передбачається, що цей метод може бути ефективнішим (за обчислю-

вальною складністю) для порівняно невеликих значень ($5 \leq n \leq 10$) степенів примітивних поліномів, ніж використання для цієї мети методу Берлекемпа – Мессі.

Сформульовані й досліджені деякі критерії, які характеризують авто- та взаємкореляційні властивості кодів Голда, що дає змогу впорядковувати їх та вибирати для практичних потреб необхідну кількість кодів із найкращими, залежно від сфери застосування, кореляційними характеристиками.

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

Вважаємо доцільним продовження теоретичних і практичних досліджень за цією тематикою, зокрема, в таких напрямках:

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

б) дослідження особливостей синтезу і, відповідно, кардинальності множин та кореляційні характеристики небінарних кодів Голда, тобто кодів, які утворюються на основі p -значних m -послідовностей із елементів простого $GF(p)$ і розширеного $GF(p^n)$ 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. 560 p.
- [4] Khaled Rouabah, Salim Attia, Rachid Harba, Philippe Ravier, and Sabrina Boukerna. *Optimized Method for Generating and Acquiring GPS Gold Codes*. International Journal of Antennas and Propagation. Vol. 2015. Article ID 956735, 9 p. <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. 2012. № 6. 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. Інноваційний потенціал світової науки – XXI сторіччя: зб. статей учасників тридцять третьої Міжнародної науково-практ. конференції, 20–27 травня 2015 р., 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 Galois and Fibonacci Sequences*, 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 Tchaikovskiy, Denys Chorny

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 $5 \leq n \leq 10$. 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 $2 \times n$ 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.*