УДК 691.91

О.А. Замула, В.І. Грабчак

Харківський національний університет радіоелектроніки, Харків

АНАЛІЗ АЛГОРИТМІВ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ СИСТЕМ ЗВ'ЯЗКУ З КОДОВИМ РОЗПОДІЛОМ КАНАЛІВ

Проводиться аналіз алгоритмів формування псевдовипадкових послідовностей. На основі проведеного аналізу зроблені висновки щодо можливості їх застосування в системах зв'язку з кодовим розподілом каналів.

песевдовипадкова послідовність, складний сигнал, кореляція, кодовий розподіл каналів

Вступ

Постановка проблеми. Раніше проектування систем багатостанційного доступу з кодовим розподілом каналів (CDMA – Code Division Multiple Access) було скоріше мистецтвом, ніж наукою. Поворотним моментом стало створення теорії формування, обробки й передачі сигналів [1]. Вона дозволяє визначити ефективність використання конкретного ансамблю (множини) сигналів, базуючись лише на знанні їх авто- і взаємокореляційних характеристик. Серед відомих сімейств ПВП довжини $2^m–1$ із близькою до ідеальної автокореляцією [2 – 4] (їх ще називають послідовностями типу Адамара) найбільше поширення в широкосмуговому зв'язку одержали m-послідовності, оскільки генерація цих послідовностей найбільш проста, а їхні властивості в порівнянні з іншими вивчені набагато краще. У цей час у світі налічується не одна сотня робіт з m-послідовностей і інтерес до них не слабшає [5]. Однак, будучи лінійними, m-послідовності характеризуються малим значенням лінійної складності. Даного недоліку позбавлені деякі інші послідовності типу Адамара й послідовності GMW [6]. Таким чином, успішна робота систем з CDMA прямим образом залежить від можливості конструювання великих ансамблів ПВП, що задовольняють всім перерахованим вище вимогам при прийнятній апаратній складності їхньої генерації.

Аналіз публікацій. Існує досить велика кількість робіт, серед яких у першу чергу необхідно назвати фундаментальну статтю М. Персли та Сарватера, опубліковану в 1980р. і присвячену m- і родинним їм сімействам послідовностей: Голда, типу Голда й Касамі [7]. Цікаво, що в цьому переліку відсутнє не менш "родинне" m-послідовностям сімейство послідовностей Гордона, Мілза, Велча, очевидь, невідоме авторам. У цей же час, тобто до 1980-го року, у СРСР був вже опублікований цілий ряд робіт з даних послідовностей, а також отримані патенти на їхнє застосування [2, 4]. З останніх робіт варто виділити оглядові статті [8, 9], у яких перераховані основні характеристики (довжина, потужність, максимальне значення взаємної кореляції й лінійна складність) найбільш відомих і недавно отриманих двійкових псевдовипадкових послідовностей. До них у першу чергу відносяться бент-послідовності, послідовності Ноу, послідовності Кердока, оптимальні перемежовані послідовності, норм-слідові послідовності [6], ряд сімейств послідовностей з ідеальними автокореляційними функціями [8, 9].

Основна частина

Послідовності, що використовуються в сучасних системах CDMA, призначені в основному для розширення спектра й кодового поділу каналів і розділяються на псевдовипадкові послідовності й ортогональні коди [5]. Основна відмінність ПВП від ортогональних кодів полягає в тому, що взаємна кореляція ортогональних кодів строго дорівнює нулю. Тому їх найбільш доцільно застосовувати в синхронних системах. В основному це прямі канали CDMA. В DS-CDMA (Direct Sequence CDMA) системі в передавачі відбувається розширення спектра інформаційного сигналу за рахунок його модуляції кодовою послідовністю. Відповідно на прийомній стороні здійснюється зворотнє звертання прийнятого сигналу при його кореляційній обробці. При цьому дуже важливо забезпечити низьку взаємну кореляцію між сигналами користувачів, що веде до зниження інтерференційних перешкод. З іншої сторони, для надійного та швидкого входження в синхронізм потрібні послідовності з гарними автокореляційними властивостями. У противному випадку великі бічні пелюстки автокореляційної функції можуть привести до прийняття помилкових рішень і, як наслідок, до збільшення часу входження в синхронізм [5]. Крім того, гарні автокореляційні властивості важливі й для надійного поділу багатопроменевих компонентів сигналу. Зазначимо, що автокореляційна (АКФ) і взаємокореляційна функції (ВКФ) ансамблів детермінованих послідовностей зв'язані таким чином, що в них неможливо досягти одночасно гарної авто та взаємної кореляції, тоді як для ансамблів випадкових послідовностей ці функції в достатньому ступені усереднені.

Послідовності, що використовуються в системах зв'язку, умовно можна розділити на лінійні і нелінійні послідовності, а їхні символи на двійкові і недвійкові (відповідно бінарні і не бінарні).

Поряд з ортогональними кодами ключову роль в CDMA системах грають ПВП, які, хоча й генеруються детермінованим образом, мають усі властивості випадкових сигналів. Однак вони вигідно відрізняються від ортогональних послідовностей інваріантністю до тимчасового зрушення. Існує кілька видів ПВП, що володіють різними характеристиками. На теперішній час з'явилися технічні засоби, здатні "вивести" будь-який ансамбль послідовностей із заданими властивостями.

Одним з найбільш простих і надзвичайно ефективних засобів генерації двійкових детермінованих послідовностей – використання регістру зсуву (РС). Послідовність на виході n- розрядного РС зі зворотним зв'язком завжди періодична, причому її період n (число тактів, через яке схема вертається у вихідний стан) не перевищує 2^n.

Теоретично, використовуючи n-розрядний регістр і відповідним чином підібрану логіку зворотнього зв'язку, можна одержати послідовність будь-якої довжини n у межах від 1 до 2^n включно. Послідовність максимальної довжини, або m- послідовність, буде мати період 2^n–1.

Функція автокореляції m-послідовності є періодичною й дворівневою. Рівень бічних максимумів автокореляційної функції не перевищує значення [2, 4]:

$$R_{ij} = \frac{1}{\sqrt{N}}.$$

Псевдовипадкові послідовності з малим значенням аперіодичної кореляційної функції (АКФ) здатні забезпечити синхронізацію переданих і прийнятих сигналів за досить короткий проміжок часу, що звичайно дорівнює довжині самої послідовності. Найбільшу популярність одержали послідовності Баркера.

В CDMA системах найчастіше застосовуються псевдовипадкові послідовності Голда й Касами, що забезпечують малий рівень викидів ВКФ. Коди Голда з періодом 2^n–1 формуються на основі двох m-послідовностей з відбором так званих "кращих пар" (preferred pairs), що мають тризначну функцію автокореляції (–1,–φ(t), φ (t)–2), де

$$\varphi(t) = \begin{cases} 2(N+1)/2 & \text{для парних N;} \\ 2(N+2)/2 & \text{для непарних N.} \end{cases}$$

Коди Голда формуються шляхом посимвольного додавання по модулю 2 двох m- послідовностей (рис. 1). У проекті WCDMA специфіковано три типи кодів Голда: первинний і вторинний ортогональні коди Голда (обоє завдовжки 256 біт) і довгий код.

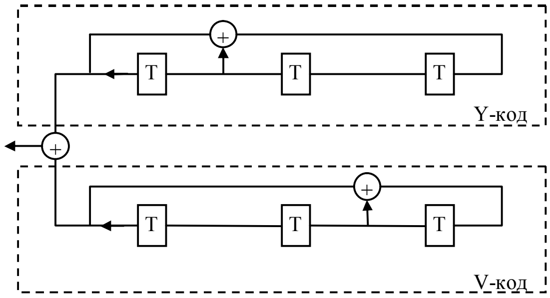

Рис. 1. Генератор кодів Голда (Т – елемент регістру зсуву ; + – суматор по модулю 2

Ортогональні коди Голда створюються на основі m-послідовності завдовжки 255 біт з додаванням одного надлишкового символу. Первинний синхрокод має аперіодичну автокореляційу функцію і використовується для первісного входження в синхронізм. Вторинний синхрокод являє собою немодульований ортогональний код Голда, який передається паралельно з первинним синхрокодом. Кожний вторинний синхрокод вибирається з 17 різних кодів Голда {C1,...,C17}.

Довгий код для прямого каналу являє собою фрагменти коду Голда завдовжки 40 960 чипів. Система зв'язку на базі WCDMA асинхронна, і сусідні базові станції використовують різні коди Голда (усього їх 512), повторювані кожні 10 мс. Асинхронний принцип роботи базових станцій робить їх незалежними від зовнішніх джерел синхронізації. Передбачається застосовувати довгий код і у зворотньому каналі, однак тільки в тій соті, де не задається режим багатокористувацького детектування.

Сімейство кодів Касамі містить послідовності з періодом 2^n–1. Вони вважаються оптимальними в тому розумінні, що для будь-якої "кращої" пари забезпечується максимальне значення автокореляційної функції, рівне (1+2к).

Кодові послідовності Касамі реалізуються за допомогою трьох послідовно включених регістрів зсуву (u, v і w) з різними зворотними зв'язками (рис. 2), кожний з яких формує свою m-послідовність.

Щоб одержати кодові послідовності Касамі з заданими властивостями, послідовності v і w повинні мати різні зсуви.

Коди Касамі завдовжки 256 біт використовуються як короткі послідовності у зворотньому каналі (проект WCDMA) в тій соті, у якій застосовується багатокористувацьке детектування.

Ефективність послідовностей з аперіодичної АКФ прийнято оцінювати показником якості F, який визначається як відношення квадратів синфазних складових сигналу до суми квадратів його расфазованих складових. Таким чином, мірою ефективності аперіодичної кореляції двійкової послідовності є показник якості.

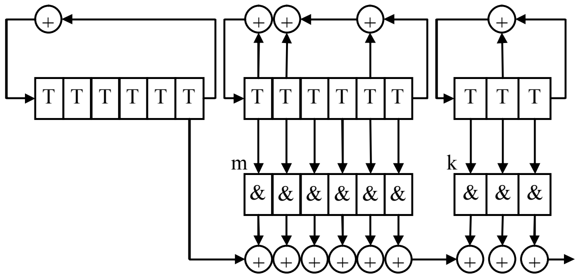

Рис. 2. Генератор кодів Касамі типу kas (6, m, k), де m і k – циклічні зсуви v- і w- кодів відповідно

Розглянемо більш детально ПВП, що формуються генераторами на основі регістрів здвигу з лінійним зворотнім зв'язком – LSFR (Linear Feedback Shift Register). Використовуємий при їх аналізі математичний апарат – теорія лінійних послідовностних машин і теорія кінцевих полів (полів Галуа) [5]. Головними перевагами цих генераторів є:

– простота апаратної та програмної реалізації;

– максимальна швидкість роботи;

– хороші статистичні властивості формуємих послідовностей.

Вихідна інформація для побудови двійкового LSFR – так званий утворюючий поліном. Ступінь цього поліному визначає розрядність регістру здвигу, а ненульові коефіцієнти – характер зворотнього зв’язку.

У загальному випадку двійковому утворюючому поліному ступеню N

$$\Phi(x)=\sum_{i=0}^{N} a_i x^i,\ a_N = a_0 = 1,\ a_j \in \{0,1\},\ j=\overline{1,(N-1)}$$

відповідають пристрої, показані на рис. 3, а (LSFR1-схема Фібоначчі) і рис. 3, б (LSFR2 – схема Галуа) [10].

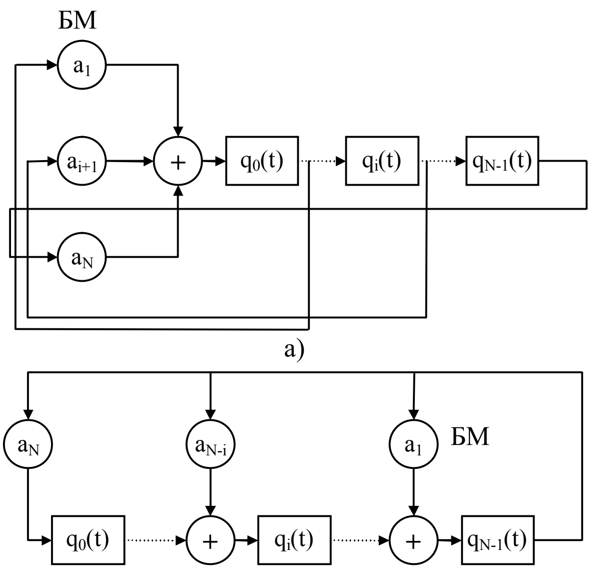

Рис. 3. Загальний вигляд LSFR, що відповідає $\Phi(x)=x^N + a_{N-1}x^{N-1} + ... + a_i x^i + ... + a_2 x^2 + a_1 x + 1$

На рис. 3: а – схема генератора Фібоначчі; б – схема генератора Галуа; БМ – блоки множення на $a \in \{0,1\}; q_j(t) \in \{0,1\}$; при a_j=1 множення на a_j рівноцінно наявності зв’язку; при a_j=0 множення на a_j рівноцінно відсутності зв’язку.

Загальний вигляд генератора двійкових послідовностей, що відповідає рівнянню

$$Q(t+1)=T^k Q(t),$$

де Q(t) і Q(t+1) – стан регістру генератору ПВП відповідно у моменти часу t і t+1 (до та після приходу синхро-імпульсу); T – квадратна матриця порядку N вигляду

$$T_1 = \begin{vmatrix} a_1 & a_2 & ... & a_{N-1} & a_N \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ & & ... & & \\ 0 & 0 & ... & 1 & 0 \end{vmatrix}$$

або

$$T_2 = \begin{vmatrix} 0 & ... & 0 & 0 & a_N \\ 1 & ... & 0 & 0 & a_{N-1} \\ & ... & & & \\ 0 & ... & 1 & 0 & a2 \\ 0 & ... & 0 & 1 & a1 \end{vmatrix};$$

N – ступінь утворюючого поліному

$$\Phi(x)=\sum_{i=0}^{N} a_i x^i,\ a_N = a_0 = 1,$$

$$a_j \in \{0,1\},\ j=\overline{1,(N-1)};$$

k – натуральне, наведене на рис. 4. В частинному випадку при k =1, отримуємо або схему генератора Фібоначі ($T=T_1$), або схему генератора Галуа ($T=T_2$) [10].

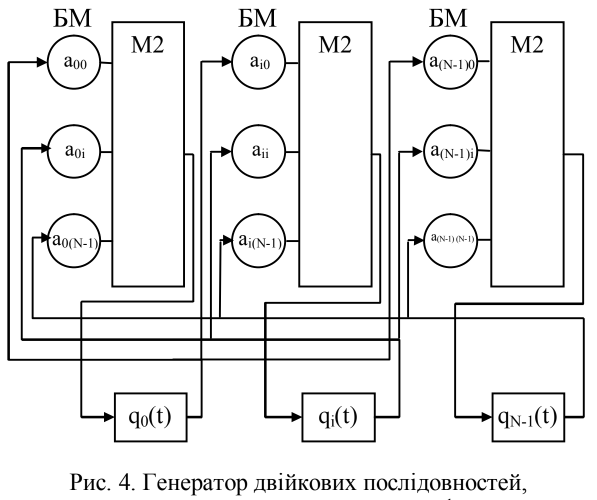

Рис. 4. Генератор двійкових послідовностей, що відповідає рівнянню $Q(t+1)=T^kQ(t)$

Величина, на яку робиться множення в кожному блоці множення (БМ), визначається відповідним коефіцієнтом $a_{ij} \in \{0,1\}$ супроводжуючої матриці

$$V = T^k (i = \overline{0, N-1}, j = \overline{0, N-1}) .$$

Якщо $a_{ij}=0$, це еквівалентно відсутності зв'язку між виходом і-го розряду регістру генератора та входом j-го суматора по модулю два.

Якщо $a_{ij}=1$, це еквівалентно отримання зв'язку між виходом і-го розряду регістру генератора та входом j-го суматора по модулю два.

Так як нульовий стан регістра є забороненим, максимально можливе число станів обладнання, а значить, і максимально можлива довжина формуємої двійкової послідовності, знімаємої з виходу любого з тригеррів, дорівнює $2^N–1$. В цьому випадку діаграма станів генератора складається з одного тривіального циклу та циклу максимальної довжини $2^N–1$.

Висновки

Виходячи з проведеного аналізу алгоритмів синтезу псевдовипадкових послідовностей можливо зробити висновок про те, що серед відомих методів синтезу найбільше практичне застосування знайшли методи, що базуються на рекурентних поліноміальних співвідношеннях, що зумовлено простотою реалізації таких пристроїв, а також одержанням у ряді випадків послідовностей з гарними автокореляційними властивостями. Ці алгоритми дозволяють одержати послідовності із заданими кореляційними властивостями при досить простій апаратній реалізації.

Проте, слід відзначити низку недоліків:

– наведені алгоритми дозволяють отримати невелику кількість псевдовипадкових послідовностей;

– послідовності синтезовані на основі наведених алгоритмів мають низьку структурну складність;

– отримані послідовності, що задовольняють по автокореляційним властивостям не завжди задовольняють по взаємокореляційним властивостям і навпаки.

Подальші дослідження будуть спрямовані на розробку алгоритмів формування псевдовипадкових послідовностей із заданими кореляційними, ансамблевими та структурними властивостями.

Список літератури

1. *Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С. 333-402.*

2. *Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Сов. радио, 1985. – 384 с.*

3. *Лосев В.В. Дискретные сигналы на основе функций Уолша для многоканальной системы передачи информации // Радиотехника и электроника. – 1979. – Т. 24, № 11. – С. 2222-2225.*

4. *Цифровые методы в космической связи / Под ред. Е.В. Кормаровой. – М.: Связь, 1969. – 268 с.*

5. *Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.*

6. *Fazel K., Kaiser S. Multi Carrier and Spread Spectrum Systems. – John Wiley & sons, 2003. – 298 p.*

7. *Сарватер Д.В., Персли М.Б. Взаимнокорреляционные свойства псевдослучайных и родственных последовательностей // ТИИЭР, 1980. – N 5, – С. 59-90.*

8. *Kumar P.V. Recent results on sequences with low autocorrelation. – 1999 IEEE ITW, Kruger National Park, South Africa, June, 1999.*

9. *Hsiao-Hwa C., Hsin-Wei C., Guizani M. Orthogonal complementary codes for Interference-free CDMA technologies // IEEE Wireless Communications. – February, 2006. – Vol 13, № 1. – P. 68-79.*

10. *Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.*

Надійшла до редколегії 13.03.2007

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.