

Список літератури

1. Головань В.Г., Казакова Н.Ф. Послідовність GMW на основі слідів полів Галуа / Захист інформації. – К.: ДУІКТ. – Спец. випуск (40), 2008. – С.95-100.
2. Сукачев Э.А., Казакова Н.Ф., Чуприна А.А. Синтез сигнальных функций для цифровой радиосвязи // Матер. III Міжнар. наук.-практ. конф. «Наукові дослідження – теорія та експеримент-2007», 14-16 травня 2007 р., Полтава: Інтер-Графіка, 2007. – Т.7. – С.54-57.
3. Кренгель Е.И. О числе псевдослучайных последовательностей Гордона, Милза, Велча. – Техника средств связи, Сер. ТРС, вып. 3, 1979.
4. Golomb S.W. Shift register sequences. – AEGEAN PARK PRESS, Laguna Hills, California, 1982.
5. Кренгель Е.И. Исследование и разработка новых классов псевдослучайных последовательностей и устройств их генерации для систем с кодовым разделением каналов. – Дис. канд. техн. наук: 05.12.13: Москва. – М.: РГБ. – 2000 (Из фондов Российской государственной библиотеки).

УДК 621.396.946; 621.391.001.12

О.О. Скопа, В.І. Гура

Міжнародний гуманітарний університет

СИНТЕЗ ПОХІДНИХ СИСТЕМ СИГНАЛІВ НА ОСНОВІ ПВП GMW, ЩО ВОЛОДІЮТЬ ВЛАСТИВОСТЯМИ ОРТОГОНАЛЬНОСТІ

Сучасний період розвитку широкосмугових систем зв'язку супроводжується бурхливим зростанням числа робіт, присвячених пошуку нових систем ортогональних сигналів, використовуваних в цих системах для розширення спектру і каналостворення [1]. Системи ортогональних сигналів будуються на основі ансамблів ортогональних кодових псевдовипадкових послідовностей, основними вимогами до яких є [2]:

- 1) великий ансамбль послідовностей, що формуються за допомогою єдиного алгоритму;
- 2) хороші кореляційні властивості послідовностей ансамблю;
- 3) збалансованість структури;
- 4) велика лінійна складність або непередбачуваність символів послідовностей.

В даний час в системах зв'язку з CDMA широкого поширення набули ортогональні системи сигналів на основі циркулянтних матриць Адамара і системи функцій Уолша, які є матрицями Адамара порядку 2^N . Відомо [3], що системи ортогональних сигналів на основі матриць Адамара, в цілому характеризуються поганими авто- і взаємкореляційними функціями (АКФ і ВКФ відповідно), що приводить до зростання міжканальних інтерференційних перешкод в приймачі. Тому на практиці з метою зменшення рівня інтерференційних перешкод доцільніше використовувати похідні ортогональні системи сигналів [4, 5], що мають відносно кращі взаємкореляційні характеристики. Нагадаємо, що похідний сигнал синтезується в результаті посимвольного перемножування двох сигналів. Відповідно система, складена з множини похідних сигналів, називається *похідною*. Серед похідних систем сигналів великого поширення набули системи, що будуються таким чином:

Як перший співмножник береться деяка ортогональна система сигналів, послідовності якої не задовольняють вимогам на кореляцію, проте володіють певними перевагами з погляду простоти їх формування і обробки. Це так звана *початкова система сигналів*. Потім як другий співмножник вибирається базисний широкосмуговий сигнал з відносно малими біч-

ними піками АКФ. Як показано в [4], кореляційні властивості такої похідної системи виявляються кращими, ніж у початкової. Зазвичай в якості початкової системи використовують функції Уолша або циркулянтні матриці Адамара, які утворені всіма зрушеннями m -последовностей, а як похідні сигнали – m -последовності. В цьому випадку збалансованість последовностей похідної системи буде тим краще, чим менше пікове значення взаємної кореляції початкових базових последовностей. Аналіз показує, що, в основному, задовольняючи трьом першим критеріям відбору, вищеописані похідні системи сигналів володіють незначною лінійною складністю. Тому актуальним завданням є побудова нових ортогональних похідних систем сигналів великої лінійної складності з прийнятними кореляційними властивостями і збалансованістю.

Для вирішення поставленого завдання були досліджені похідні системи сигналів, в яких початкові системи будуються на основі циклічних зрушень m -последовностей, а як приведені последовності вибрані нелінійні последовності GMW. Оцінка лінійної складності такої похідної системи проводиться за допомогою наступної теореми:

Теорема. Лінійна складність похідної системи сигналів $L_{np,c}$ з початковою m -последовністю довжини 2^N-1 і з последовністю GMW такої ж довжини і лінійною складністю L_{GMW} , знаходиться у межах $L_{GMW}-N \leq L_{np,c} \leq L_{GMW}+N$.

Доказ. Будь-яка последовність $\{b_n\}$ довжини 2^N-1 з елементами над $GF(2)$ може бути представлена у вигляді $b_n = \sum_{\delta \in \Delta} \alpha_{\delta} \alpha^{\delta n}$, де α – примітивний елемент поля $GF(q^N)$, b_n – последов-

ність з елементами над $GF(q)$, Δ – множина індексів при ненульових коефіцієнтах, δ – елемент множини індексів при ненульових коефіцієнтах. Лінійна складність последовності $\{b_n\}$ чисельно рівна кількості елементів в цій сумі. Відомо [6, 7], що m -последовність може бути представлена у вигляді суми вигляду $m_n = tr_1^N(\alpha^n) = \sum_{i=0}^{N-1} \alpha^{2^i n}$ з числом членів рівним N , де tr –

множник різницевої множини, що є зрушенням початкової последовності $\{\alpha_n\}$. А оскільки последовності похідної системи синтезуються в результаті поелементного підсумовування по модулю 2 последовності GMW із зрушеннями m -последовностей, то через попереднє їх лінійна складність виявляється обмеженою знизу величиною $L_{GMW}-N$, а зверху $L_{GMW}+N$ [8]. Теорема доведена.

Як приклад розглянемо випадки $N=10$ і $N=14$. Враховуючи, що для $N=10$ максимальна лінійна складність последовності GMW дорівнює 140 [9], а для $N=14$ – відповідно 1232, маємо:

- для $N=10$: $140-10=130 \leq L_{np,c} \leq 140+10=150$,
- для $N=14$: $1232-14=1218 \leq L_{np,c} \leq 1232+14=1246$.

Звідси видно, що лінійна складність похідних систем на основі нелінійних последовностей GMW і m -последовностей визначається, в основному, лінійною складністю последовностей GMW і може у багато разів перевищувати лінійну складність m -последовностей.

Для розглянутих випадків на основі последовностей GMW був побудований ряд ортогональних похідних систем і проведений розрахунок їх періодичних АКФ і ВКФ. Аналіз показав, що для деяких з них абсолютні пікові значення АКФ і ВКФ, узяті по всіх последовностях системи, не перевищують величини $6\sqrt{N}$. Це всього в 3 рази гірше в порівнянні з ортогональною похідною системою на основі последовностей Голда, яка має якнайкращі кореляційні властивості, але невелику лінійну складність, рівну $2N$.

Що ж до збалансованості последовностей даних систем, то, очевидно, вона повністю визначається значенням піку взаємної кореляції початкових последовностей і, як показують чисельні розрахунки, в кращому разі може бути співставлена з последовностями Голда.

Оцінимо тепер загальне число утворених у такий спосіб ортогональних похідних систем. Відповідно до [10] їх число може бути знайдено по формулі:

$$\left(\varphi \frac{2^N - 1}{N} \right)^2 |GMW| \quad (1)$$

де: φ – функція Ейлера $|GMW|$ – число різних нееквівалентних класів послідовностей GMW довжини $2N-1$.

Відповідно до (1) знаходимо, що для випадків $N=10$ і $N=14$ загальне число таких систем складає відповідно 25200 і 45151344.

Торкаючись питання складності апаратної або програмної реалізації пропонованих систем сигналів, необхідно відзначити, що виникаючі при цьому труднощі пов'язані в основному з генерацією послідовностей GMW. Ці питання достатньо детально досліджені [11]. Найбільш переважним (через свою простоту) є метод [12], що використовує виключно двійкову арифметику, тоді інші або вимагають застосування q -чної арифметики [13...15] або володіють великою апаратною складністю [16...18].

Висновок. Розглянуто синтез похідної системи сигналів, яка базується на псевдовипадковій послідовності GMW та показано, що лінійна складність систем, побудованих на основі нелінійних послідовностей GMW і m -послідовностей, в основному, визначається лінійною складністю послідовностей GMW та може у багато разів перевищувати лінійну складність m -послідовностей.

Список літератури

1. Ojanpera T., Prasad R. Wideband CDMA for third generation mobile communications. – Artech House, Boston-London, 1998.
2. Бессарабова А.П., Журавлев В.И. Псевдослучайные последовательности сигналов и их применение в технике связи. – Итоги науки и техники. Сер. Связь, Москва, ВИНТИ, №7, 1991.
3. Сарватер Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей. – ТИИЭР, №5, 1980.
4. Варакин Л.Е. Теория систем сигналов. – М.: Сов. радио, 1978.
5. Щербина Ю.В., Скопа А.А. Проблемы оценки защищенности автоматизированных систем / Захист інформації. – №4 (41), 2008. – К.: ДУІКТ. – С.23-29.
6. Simon M.K., Omura J.K., Scholtz R.A., Levit B.K. Spread spectrum communications handbook. – McGraw-Hill, Inc., 1994.
7. Скопа А.А., Никифорова К.Б., Согина Н.М. Прикладное применение уравнений Клоппера-Пирсона в системах телекоммуникаций / Наукові записки УНДІЗ. – №2. – К.: УНДІЗ, 2007. – С.83-88.
8. Кренгель Е. И., Мешковский К.А. Ортогональные производные системы сигналов большой линейной сложности // Повышение эффективности цифровых и аналоговых средств радиосвязи / Моск. техн. ун-т связи и информатики. – М.: 2000. – Библ.: 7 назв. – Рус. – Деп. в ЦНТИ «Информсвязь», №21174 Св. 2000 от 20.04.2000.
9. Конопельке В.К., Юрцевич Д.М., Юрцевич М. m -подобные нелинейные последовательности с идеальными автокорреляционными свойствами. // Труды I Междунар. конф. «Цифровая обработка сигналов и ее применение» DSPA'98, сентябрь, 1998 г. – Москва. – 1998.
10. Кренгель Е.И. О числе псевдослучайных последовательностей Гордона, Милза, Велча. – Техника средств связи, Сер. ТРС, вып. 3, 1979.
11. Кренгель Е.И. Исследование и разработка новых классов псевдослучайных последовательностей и устройств их генерации для систем с кодовым разделением каналов. – Дис. канд. техн. наук: 05.12.13: Москва. – М.: РГБ. – 2000 (Из фондов Российской государственной библиотеки).

12. Мешковский К.А., Кренгель Е.И. Генерация псевдослучайных последовательностей Гордона, Милза, Велча. – Радиотехника, №5, 1998.
13. Scholtz R.A., Welch L.R.. GMW sequences. – IEEE Trans. Inform. Theory, vol. IT-30, №9, 1984.
14. Скопа О.О., Фількін К.М. Генератор послідовностей GMW на основі слідів полів Галуа / Наукові записки УНДІЗ. – 2008. – №2(4). – С. 77-82.
15. Скопа О.О., Фількін К.М. Нова послідовність GMW для підвищення безпеки радіосистем з кодовим розділенням каналів / Захист інформації. – Спец. випуск (40), 2008. – К.: ДУІКТ. – С.100-103.
16. А.с. №632067, кл. НОЗ К/84 с приоритетом от 03.05.1977. Генератор псевдослучайных последовательностей двоичных сигналов / К. А. Мешковский, Е. И Кренгель.
17. А.с. №674204, кл. НОЗ К/84 с приоритетом от 05.07.1977. Генератор псевдослучайных последовательностей двоичных сигналов / К. А. Мешковский, Е. И Кренгель.
18. Маракова И.И., Скопа А.А., Сыропятов А.А. Защита информации в беспроводных системах связи // Матер. IV наук.-техн. конф. «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні», 1-3 березня 2006 р

УДК 621.391.001.12/18:621.391:519.72

С.Л. Волков

Міжнародний гуманітарний університет

МЕТОД ШВИДКОГО РОЗРАХУНКУ ВЗАЄМОКОРЕЛЯЦІЙНИХ ВЛАСТИВОСТЕЙ ЧИСЛОВИХ ПОСЛІДОВНОСТЕЙ З ВИКОРИСТАННЯМ ІЗОМОРФНИХ КОЕФІЦІЄНТІВ

Для оцінки взаємокореляційних властивостей послідовностей, які використовуються для кодування та шифрування інформації, часто використовують пікові значення їх періодичних (парних) взаємно-кореляційних функцій (ПВКФ) і меандро-інвертованих (непарних) взаємно-кореляційних функцій (МІВКФ). У роботі [1] в загальному вигляді запропонований метод дослідження кореляційних функцій періодичних двійкових послідовностей, що будуються на основі різницевих множин. Подальший розгляд та аналіз ідей [1] дав можливість встановити, що метод ґрунтується на можливості застосування до всіх класів таких послідовностей понять ізоморфізму і немножників, введених для різницевих множин. Оскільки такі немножники в [2] названі ізоморфними коефіцієнтами, то такий метод дослідження ПВКФ можна назвати *методом ізоморфних коефіцієнтів*. Подальші викладки показують, що він дозволяє істотно прискорити розрахунок на ЕОМ ПВКФ та МІВКФ.

Нехай $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_v)$ і $\beta = (\beta_1, \beta_2, \dots, \beta_v)$ є послідовності довжини $v = 2^N - 1$, які належать одному класу, і нехай t – деяке позитивне ціле, взаємно просте з v . Оскільки за визначенням t є немножник, то послідовності $a' = (a_{i_1}, a_{i_2}, \dots, a_{i_v})$ і $b' = (b_{i_1}, b_{i_2}, \dots, b_{i_v})$, де $i_k = (t(k-1)+1) \bmod v$ для всіх $k = \overline{1, v}$, також належатимуть цьому класу. Очевидно, що ізоморфізм $t: \alpha \rightarrow \alpha'$ є унітарним оператором в евклідовому просторі R^v . Через властивості цього оператора маємо:

$$(\alpha, \beta) = (\alpha', \beta'). \quad (1)$$

Позначимо спектр взаємної кореляції послідовностей α і β через $S(\alpha, \beta)$. Тоді, згідно (1),

$$S(\alpha, \beta) = S(\alpha', \beta') \quad (2)$$