УДК 004.056.5

О.Я. Різник, І.Ю. Юрчак, В.О. Парубчак
Національний університет "Львівська політехніка",
кафедра систем автоматизованого проектування

ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ БАРКЕРОПОДІБНИХ КОДІВ

Показано можливість побудови баркероподібних кодів за допомогою моделей числових лінійних в'язанок, створення ефективних алгоритмів їх побудови.
Ключові слова – баркероподібний код, модель ЧЛВ, алгоритм

In the paper possibility of Barker codes construction using CLV models is presented. Development of of effective algorithms for their construction are carried out.
Keywords – Barker code, CLV model, algorithm

Вступ

У XXI ст. ми вже не уявляємо свого життя без мобільного зв'язку чи Інтернету. Зі стрімким розвитком цих технологій на передній план вийшли швидкість та надійність. Це досягається різними методами кодування. Під кодуванням розуміють процес перетворення повідомлень у дискретні сигнали.

Системи, що використовують складні шумоподібні сигнали, застосовуються вже більше 50 років. Відомі переваги шумоподібних сигналів, такі, як висока завадостійкість щодо вузькосмугових перешкод великої потужності, можливість розділення абонентів за кодовою ознакою, скритність передачі, висока стійкість до багатопроменевого поширення і навіть висока роздільна здатність при радіолокаційних і навігаційних вимірах, зумовили їх використання в різних системах зв'язку і визначення місця розташування.

Постановка задачі

Вибір псевдовипадкової кодової послідовності в радіотехнічній системі передачі інформації дуже важливий, оскільки від її параметрів залежить посилення оброблення системи, її завадостійкість, чутливість. При одній і тій самій довжині кодової послідовності, параметри системи можуть бути різні.

Нині використовують складні шумоподібні сигнали, які мають деякі переваги. Наприклад, висока захищеність від перешкод, швидкість передачі тощо. Щоб використовувати шумоподібні сигнали, кодові комбінації повинні бути наділені певними математичними характеристиками, основною з яких є автокореляція. Саме коди Баркера відповідають цим вимогам.

Послідовність Баркера – це ряд, що складається з N елементів a_j для $0 \le j \le N$, які мають значення +1 та -1 і чергуються так, що виконується умова:

$$\left| \sum_{j}^{N-v} a_j a_{j-v} \right| \le 1, \tag{1}$$

де $1 \le v \le N$.

Ці коди є трирівневі. Вони є частковим випадком кодів Галуа.

Послідовності Баркера мають мінімальний рівень бокових пелюсток автокореляційної функції, а тому добре підходять для оптимального приймання. Відомі послідовності Баркера мають довжину $2 \le N \le 13$, зокрема, для N=13 код Баркера має вигляд:

$$+1\ +1\ +1\ +1\ +1\ -1\ -1\ +1\ +1\ -1\ +1\ -1\ +1.$$

Коди Баркера мають найкращі серед відомих псевдовипадкових послідовностей властивості шумоподібності (автокореляції), що і зумовило їх широке використання. Ці коди знайшли широке застосування в безпровідних мережах Wi-Fi.

Проілюструємо автокореляцію коду Баркера. У цілях спрощення обчислення автокореляційної функції послідовності Баркера можна розрахувати різницю між числом збігів і незбігів між окремими чіпами послідовності при їх почіповому зсуві один щодо одного. Розглянемо автокореляційну функцію кодової послідовності Баркера завдовжки 11 чіпів, наведену в табл. 1.

Як очевидно з наведеної таблиці, послідовність Баркера має яскраво виражений автокореляційний пік, відповідний накладенню функції самої на себе. Провівши аналогічні розрахунки, неважко переконатися, що інші послідовності не мають аналогічної властивості, тобто мають декілька піків кореляції, що значно знижують завадостійкість переданого сигналу.

У приймачі отриманий сигнал множиться на код Баркера (обчислюється кореляційна функція сигналу), внаслідок чого він стає вузькосмуговим. Тому його фільтрують у вузькій смузі частот, що дорівнює подвоєній швидкості передачі. Будь-яка перешкода, що потрапляє в смугу вихідного широкосмугового сигналу, після множення на код Баркера, навпаки, стає широкосмуговою, тому у вузьку інформаційну смугу потрапляє лише частина перешкоди, приблизно в 11 разів менша за потужністю перешкоди, що діє на вході приймача.

Отже, використання коду Баркера забезпечує можливість передавати сигнал практично на рівні перешкод і до того ж гарантує високу міру достовірності інформації, що приймається. У цьому основний сенс їх вживання.

Таблиця 1

Порівняння автокореляційної функції кодової послідовності Баркера (завдовжки 11 чіпів) з її копією

Значення зсуву	**Послідовність**	**Число збігів А**	**Число неспівпадань Б**	**Значення різниці**
1	01110001001	5	6	-1
2	10111000100	5	6	-1
3	01011100010	5	6	-1
4	00101110001	5	6	-1
5	10010111000	5	6	-1
6	01001011100	5	6	-1
7	00100101110	5	6	-1
8	00010010111	5	6	-1
9	10001001011	5	6	-1
10	11000100101	5	6	-1
0	11100010010	11	0	11

Широке практичне вживання фазоманіпульованих сигналів в системах виявлення обумовлене; порівняно рівномірним розподілом бічних пелюсток кореляційної функції при великому числі дискретів на всій площині, постійністю амплітуди сигналу, а також простотою генерування останнього.

У фазоманіпульованих сигналів мінімально досяжний рівень бічних пелюсток зворотно пропорційний числу дискретів. Тому більшого поширення набули фазоманіпульовані сигнали з підвищеним числом дискретів. Існуючі методи синтезу фазоманіпульованих сигналів розвинені недостатньо, тому на практиці частенько застосовують коди, які не є оптимальними [1, 3].

Для послідовності сигналів, що складається з m імпульсів (дискретів), при способі кодування за допомогою двох значень фази можна синтезувати $M = 2m$ різних сигналів. Число дискретів дорівнює $m = T/\varphi$, де T – тривалість дискрету (кодового знака). Практичне вживання знаходять сигнали з числом дискретів від десятків до тисяч, а кількість різних фазоманіпульованих сигналів велика. Для побудови необхідного сигналу, потрібно з 2m кодових комбінацій вибрати ті, які дають найкраще наближення кореляційної функції до бажаної форми.

Взаємна кореляційна функція (ВКФ) різних сигналів описує як міру схожості форми двох сигналів, так і їх взаємне розташування один відносно одного по координаті (незалежною змінною). Взаємна кореляційна функція двох різних сигналів s(t) і u(t) є таким скалярним добутком сигналів:

$$B_{su}(\tau) = \int_{-\infty}^{\infty} s(t)\, u(t+\tau)\, dt \quad . \tag{2}$$

Взаємна кореляція сигналів характеризує певну кореляцію явищ і фізичних процесів, що відображуються даними сигналами, і може слугувати мірою «стійкості» даного взаємозв'язку при роздільній обробці сигналів в різних пристроях.

Автокореляційна функція (АКФ) сигналу s(t), локалізованого в часі і кінцевого по енергії, є кількісною інтегральною характеристикою форми сигналу, і визначається інтегралом від добутку двох копій сигналу s(t), зрушених відносно один одного на деякий час t:

$$B_s(\tau) = \int_{-\infty}^{\infty} s(t)\, s(t+\tau)\, dt \, . \tag{3}$$

Як очевидно з вираження, АКФ є скалярним добутком сигналу і його копії у функціональній залежності від змінної величини значення зрушення t.

Сигнали, база яких змінюється відповідно до коду Баркера, є унікальними фазоманіпульованими сигналами. Модуль їх автокореляційної функції має мінімально досяжний однаковий рівень бічних пелюсток.

Розв’язання задачі

Відомо, що спроби знайти коди Баркера для m>13 розв’язку не мають [3]. Отже, коди Баркера можна використовувати лише для сигналів з порівняно невеликою базою. Тому актуальним є розроблення алгоритму побудови баркероподібних кодів для m>13 на основі числових лінійок-в'язанок (ЧЛВ) [1].

Методика побудови на основі числових лінійок-в'язанок за критерієм мінімального значення функції автокореляції дискретного сигналу полягає ось у чому [2]:

1) застосовуючи алгоритм вибіркових переміщень (при $2 < N < 12$), алгоритм асиметричних розгалужень (при $12 < N < 18$) чи алгоритм побудови ЧЛВ на базі ідеальних кільцевих в'язанок (при $18 \le N$), вибрати варіант ЧЛВ заданого порядку N необхідної довжини L_N кратності R [1];

2) побудувати L_N-позиційний код μ_i, $i = 1,2,...,L_N$ з однорівневою періодичною функцією автокореляції на базі вибраного варіанта ЧЛВ $(k_1, k_2, ..., k_l, ..., k_N)$, де на N позиціях коду з порядковими номерами x_l, $l = 1,2,...,N$, які визначаються з формули [1, 2]

$$x_l \equiv 1 + \sum_{i=1}^{l} k_i \pmod{L_N}, \tag{2}$$

розмістити символи "1", а на решті $L_N - N$ позиціях – символи "-1" [1].

За допомогою розробленого програмного комплексу був проведений пошук кодів з числом дискретів більше 13 (m>13). Слід зазначити, що в результаті синтезу не удалося отримати фазоманіпульовані сигнали аналогічні кодам Баркера. Проте за допомогою розробленого програмного комплексу були знайдені унікальні коди для фазоманіпульованих сигналів завдовжки більше 13 періодів, що мають, для даного числа дискретів, мінімально досяжний рівень бічних пелюсток функції кореляції (баркероподіні коди).

Таблиця 2

Значення баркероподібних кодів

Число дискретів	**Баркероподібні коди**
14	1111-11-111-1-111-1
15	11-111-11-11-1-1-1111
16	-1-11-11-1-1-1-1-111-1-111
17	1-11-1-111-1-1-111111-1
18	11-1-1111-11-1-11-111111
19	-11-1-11-1-1-11-1-1-1111-1-1-1-1
20	1-1-1-111-11-11-1-111-111111
21	111111-11-1-1-11-111-1-1-111-1
22	111-1-1111111-1-11-1-11-11-11
23	1-1-11-111-11111-1111-11-1-1-111
24	1-1-11-1-1111111-1-1-111-1-1-11-11-1
25	111-1-1111-1-1-1-1-1-11-11-11-1-11-1-11
26	-1-11-1-1-1111-11111-11-1-111111-1-11
27	-1-1-1111-1-1111111-11-1-11-1-111-11-11
28	1-1-1111111-111-1-11-11-1111-1-11-11-1-1
29	-1-1111-11-1-1111-111111-111-1-11-11-1-11
30	1-1-1-111-1111-111111-1-1-11-111-111-11-1-1
31	-1-1-1-111-11111-1-111-1-111-11-1-1-1-11-11-1-1-1
32	1-1-111-111-11-1-1-1111-1-11-11-1111111-11-1
33	-1-1-1-1-111-1-111-111-1-11-11-1-11111-11-11-1111
34	1-11-1-11-1-111-1-1111-11-111-1-11111-1-1-1-1-11-11
35	1-1111-11-111111-11-1-11-11-1-1-1-11-111-1-111-1-1-1
36	11111-1-1-11-1-1111-1-1-11-11-1-11-111-1111-111-111
37	11-11-1-11-1-111111-1-111-1-1-11-1-1-1-1-11-11-1-1-1-111
38	-1-111-11-11-1-1-111-111-11-1-1-1-111-11-1-1-11-1-1-1-1-1-11-1
39	11-1-1111-11-1-11-111-1-1111111-1-1-1-1-1-11-11-11-1-1-11
40	1111-111-11-11-11-11-1-1-1-111111-1-111-1-111-111-11111

Баркероподібні коди з числом дискретів (14-43) наведені в табл. 2. Потрібно зазначити, що для кожного числа дискретів, представлених в цій таблиці, рівень бічних пелюсток нормованої кореляційної функції є мінімальним. Унікальний код для кожного числа дискретів був розрахований за допомогою ЧЛВ.

Висновки

Отже, показана можливість побудови баркероподібних кодів за допомогою ЧЛВ моделей, створення ефективних алгоритмів їх побудови. Дослідження моделей і методів комбінаторної оптимізації розширює сферу практичних застосувань ЧЛВ моделей в задачах інформаційної техніки і проектування систем захисту інформації [2, 3].

1. Різник В.В. Синтез оптимальних комбінаторних систем. – Львів, 1989. 2. Різник О.Я. Завадостійкий спосіб перетворення сигналів // Матер. Четвертої укр. конф. з автоматичного керування ("Автоматика-97"). – Черкаси. – 1997. – С.34. 3. Різник О.Я., Стасевич С.П., Парубчак В.О., Скрибайло-Леськів Д.Ю. Швидкий синтез подібних кодів Баркера // Пр. Міжнар. конф. з математичного моделювання AMSE'2007. – Алушта. – С.23–24.