

УДК 623.618.2

Ю.В. Стасев, Л.О. Клеванна, О.Ю. Носик

Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків

АЛГОРИТМ ФОРМУВАННЯ СИГНАЛЬНО-КODOVИХ КОНСТРУКЦІЙ З ПОЛІПШЕНИМИ КОРЕЛЯЦІЙНИМИ ВЛАСТИВОСТЯМИ

В статті пропонується алгоритм підвищення перешкодозахищеності систем управління та зв'язку на основі синтезу сигнально-кодovих конструкцій поліпшеними кореляційними властивостями. Показано, що підвищення перешкодозахищеності систем управління та зв'язку можливо при сумісному використанні перешкодозахищених кодів і ортогональних дискретно-частотних сигналів. Формуються умови синтезу сигнально-кодovих конструкцій з заданими кореляційними властивостями. Обґрунтовується вибір перешкодозахищеного коду. Сформульовані та доведені необхідні умови розмірності коду і його мінімальної кодової відстані.

Ключові слова: функція взаємної кореляції, кореляційні властивості, нормована функція кореляції.

Вступ

Постановка проблеми у загальному вигляді.

Якість передачі інформації в телекомунікаційних системах в суттєвій мірі залежить від характеристик використаних сигналів і кодів. В ряді випадків ці характеристики являються неузгодженими, що призводить до зниження основних характеристик, таких як перешкодозахищеність і імотостійкість систем телекомунікації [1–3].

Мета статті – розробка алгоритму формування сигнально-кодovих конструкцій з поліпшеними кореляційними властивостями.

Аналіз останніх досягнень і публікацій. Проведені дослідження показали [1–3], що є декілька методик синтезу сигналів заданими кореляційними властивостями. В теперішній час достатньо обґрунтованими є методики вибору алгоритму кодування інформації, з метою підвищення завадостійкості телекомунікаційних систем. Однак на сьогоднішній час відсутні алгоритми синтезу сигнально-кодovих конструкцій заданими кореляційними властивостями.

Постановка задачі та викладення матеріалів дослідження

Метод формування псевдовипадкових послідовностей оперує ансамблями дискретних сигналів, заданих кодovими словами надлишкового (завадостійкого) коду. Поєднуючи конструктивні особливості алгебраїчних методів синтезу, цей підхід дозволяє теоретично обґрунтувати значення функцій авто- і взаємкореляції сформованих сигналів.

Розглянемо випадок, як утворюючі послідовності дискретних сигналів S використовують кодovі слова циклічного (n, k, d) -коду. Тоді маємо ансамбль дискретних сигналів, авто- і взаємкореляційні властивості.

Формалізуємо завдання синтезу сигналів: необхідно знайти таку множину із M дискретних послідовностей довжини n , за якої

$$\begin{cases} R_1^{ii}(\tau = lT_e) = 1, \text{ якщо } \tau = 0 \pmod{n}; \\ R_1^{ii}(\tau = lT_e) \leq R_{\max}, \text{ якщо } \tau \neq 0 \pmod{n}; \\ R_1^{ij}(\tau = lT_e) \leq R_{\max}, \text{ якщо } C^i \neq C^j_{\rightarrow\tau}. \end{cases} \quad (1)$$

Для синтезу ансамблю сигналів, необхідно вибрати такий циклічний (n, k, d) -код, що дасть необхідні кореляційні (R_1^{ii}) й ансамблеві (M) властивості.

За визначенням циклічний (n, k, d) -код однозначно задається наведеним ненульовим многочленом

$$g(x) = \prod_i (x - \beta^i), \text{ де } \beta^i \in GF(q^m). \quad (2)$$

Найбільше поширення серед циклічних кодів одержали коди Боуза-Чоудхурі-Хоквінгема (БЧХ), в яких як корінь $g(x)$ використовується $2t$ послідовних ступенів довільного елемента $\beta \in GF(q^m)$.

Породжувальний многочлен визначається як

$$g(x) = \text{Н. З. Д. } [f_j(x), f_{j+1}(x), \dots, f_{j+2t-1}(x)], \quad (3)$$

де $f_i(x)$ – мінімальний многочлен елемента $\beta^i \in GF(q^m)$, $i = j, \dots, j + 2t - 1$...

Коренями $f_i(x)$ є всі елементи класу сполучених елементів

$$\{\beta^i, (\beta^i)^q, (\beta^i)^{q^2}, \dots, (\beta^i)^{q^{s-1}}\},$$

де s – найменше ціле число, таке, за якого

$$\beta^{q^s} = \beta, s < m.$$

Довжина коду дорівнює порядку елемента β , тобто найменшому n , для якого $\beta^n = 1$. Отже, код БЧХ можна задати перевірконою матрицею вигляду

$$H = \begin{pmatrix} \beta^0 & \beta^j & \beta^{2j} & \dots & \beta^{(n-1)j} \\ \beta^0 & \beta^{j+1} & \beta^{j+2} & \dots & \beta^{(n-1)(j+1)} \\ \dots & \dots & \dots & \dots & \dots \\ \beta^0 & \beta^{j+2t-1} & \beta^{j+2t} & \dots & \beta^{(n-1)(j+2t-1)} \end{pmatrix}, \quad (4)$$

де кожен елемент повинен бути замінений на відповідний стовпець з m елементів над $GF(q)$. Справедлива така теорема.

Теорема 1 [1–2; 5]. Параметри циклічного блокового (n, k, d)-коду БЧХ над $GF(q)$, заданого породжувальним многочленом виду (3) з коренями $\beta \in GF(q^m)$, задовольняють умові

$$d \geq 2t + 1, k \geq n - m \cdot t.$$

Теорема 1 дає нижню границю розмірності коду БЧХ і його мінімальної кодової відстані. Кодові параметри більшості кодів БЧХ, як правило, лежать вище за цю границю. Так, наприклад, над $GF(2^m)$ виконується рівність

$$f_j(x) = f_{2j}(x),$$

отже, для примітивного двійкового коду БЧХ кодові границі будуть

$$d \geq 2t + 1, k \geq n - m \cdot t. \quad (5)$$

Перевірочна матриця (4) запишеться у вигляді

$$H = \begin{pmatrix} \beta^0 & \beta^1 & \beta^2 & \dots & \beta^{n-1} \\ \beta^0 & \beta^3 & \beta^6 & \dots & \beta^{3(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ \beta^0 & \beta^{2t-1} & \beta^{2t} & \dots & \beta^{(n-1)(2t-1)} \end{pmatrix}, \quad (6)$$

де кожен елемент замінюється відповідним m -розрядним двійковим стовпцем.

Скористаємося виразом (5), який задає співвідношення кодових параметрів двійкового коду БЧХ. Після підстановки у (4–5), з урахуванням (1) одержимо

$$\frac{n - 2 \cdot (2t + 1)}{n} \leq R_{\max},$$

звідки

$$t \geq \frac{n - R_{\max} \cdot n - 2}{4}. \quad (7)$$

У відповідності до кодової границі (границя Синглтона)

$$d \leq n - k + 1$$

і виразу (7) сформулюємо умову формування дискретних сигналів з поліпшеними автокореляційними властивостями, сформованими відповідно до методу формування псевдовипадкових послідовностей.

Теорема 2 При заданих R_{\max} та n , якщо виконується умова

$$R_{\max} > -\left(1 + \frac{2}{n}\right), \quad (8)$$

метод формування псевдовипадкових послідовностей дозволяє формувати дискретні сигнали з поліпшеними властивостями. Якщо умова (8) не виконується, то цей метод не дозволяє формувати дискретні сигнали.

Доказ. Для того, щоб ПФАК задовольняла обмеженням, за яких бічні викиди ПФАК не перевищували б R_{\max} при заданій довжині послідовностей n , необхідно, щоб коригувальна здатність відповідного лінійного блокового коду задовольняла умові (7). Якщо $d=2t+1$, перепишемо границю Синглтона у вигляді

$$t \leq \frac{n - k}{2}.$$

Потужність сформованого ансамблю сигналів задається виразом $M=2^k$, звідки виходить, що для існування сигналів ($M>0$) потрібне виконання рівності $t \leq \frac{n}{2}$, а для сформованих сигналів справедливий вираз (7), звідки

$$\frac{n}{2} \geq t \geq \frac{n - R_{\max} \cdot n - 2}{4}. \quad (9)$$

Після виконання очевидних перетворень одержимо (8), що задає необхідні умови існування сигналів, сформованих з використанням цього методу.

Друга частина теореми доводиться від зворотного. Припустимо, що

$$R_{\max} \leq -\left(1 + \frac{2}{n}\right).$$

Тоді з урахуванням (9) повинна виконуватися умова

$$\frac{n - k}{2} \geq \frac{n - R_{\max} \cdot n - 2}{4},$$

при $k>0$ (тривіальний випадок $k=0$ відповідає одній послідовності з нульових символів), звідки

$$R_{\max} > -\left(1 + \frac{2 - k}{n}\right),$$

що суперечить зробленому вище припущенню. Отже, якщо умова (8) не виконується, тоді метод формування псевдовипадкових послідовностей не дозволяє формувати дискретні сигнали.

Таким чином, для синтезу ансамблів сигналів необхідно для заданого значення R_{\max} розрахувати виправляючу здатність циклічного коду t , вибрати код з необхідними коригувальними можливостями (з необхідним t) і для обраного коду розрахувати потужність сформованих сигналів $M=2^k$.

Циклічний код однозначно задається у поліноміальному вигляді за допомогою породжувального многочлена (3) і/або перевірконої матриці (6). Отже, алгоритм формування дискретних сигналів з використанням циклічних кодів БЧХ подамо у вигляді послідовності кроків.

Крок 1. Увести вихідні дані: довжину послідовності n і максимальне значення бічної пелюстки R_{\max} функції автокореляції.

Крок 2. Відповідно до умови існування дискретних сигналів з поліпшеними автокореляційними властивостями розрахувати необхідну коригувальну здатність за виразом (7). Обчислити потужність ансамблю сигналів $M=2^k$.

Крок 3. Сформувати за виразом (3) породжувальний многочлен $g(x)$ і/або за виразом (6) – перевірку матрицю H .

Схема алгоритму формування дискретних сигналів з використанням циклічних кодів наведена на рис. 1.

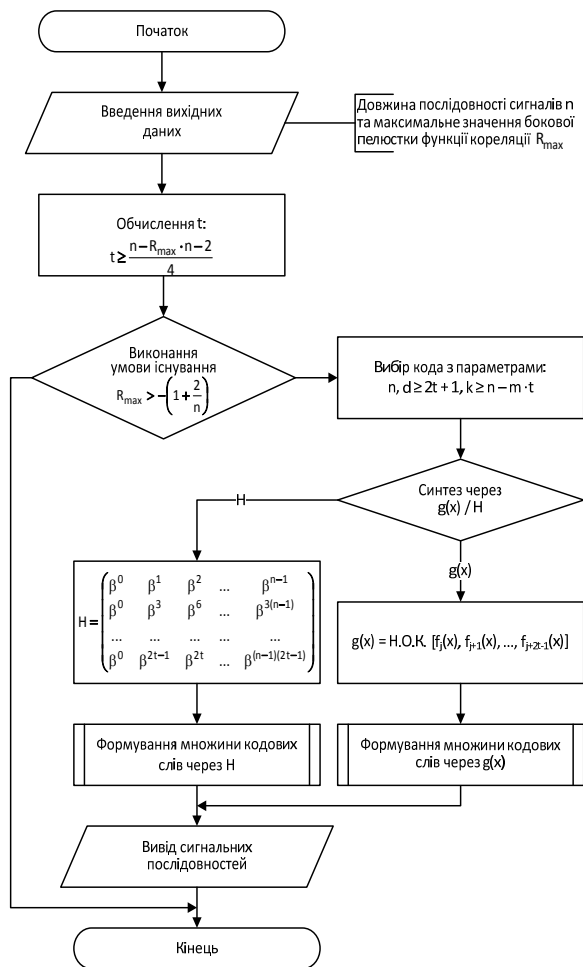


Рис. 1. Схема алгоритму формування дискретних сигналів з використанням циклічних кодів

Крок 4. Сформуванати множину кодових слів – дискретних послідовностей з необхідними кореляційними (R_1^{ii}) і ансамлевими (M) властивостями.

Аналіз алгоритму показує, що після розрахунку параметрів завадостійкого коду виконуються процедури формування кодових слів через перевірючу матрицю й/або через породжувальний многочлен коду. Це стандартні процедури в теорії завадостійкого кодування [1], які легко реалізуються або методами обертання матриць (перший варіант), або методами, заснованими на множенні та приведенні многочленів у кільці (другий варіант).

Розглянемо випадок, коли утворюючі послідовності дискретних сигналів S використовуються кодові слова циклічного (n, k, d) -коду, ваговий спектр якого обмежений зверху значенням d^* .

Тоді завдання синтезу дискретних сигналів можуть бути формалізовані у такий спосіб: потрібно знайти таку множину із M дискретних послідовностей довжини n , щоб

$$\begin{cases} R_1^{ii}(\tau = lT_e) = 1, \text{ якщо } \tau = 0 \bmod(n); \\ R_{\min} \leq R_1^{ii}(\tau = lT_e) \leq R_{\max}, \text{ якщо } \tau \neq 0 \bmod(n); \\ R_{\min} \leq R_1^{ij}(\tau = lT_e) \leq R_{\max}, \text{ якщо } C^i \neq C^j_{\rightarrow\tau}. \end{cases} \quad (10)$$

Таким чином, алгоритм формування дискретних сигналів, полягає у виконанні кроків розглянутого алгоритму.

Висновки і напрямки подальших досліджень

Таким чином, розроблений алгоритм формування псевдовипадкових послідовностей дозволяє отримувати ансамблі сигналів з заданими кореляційними та ансамлевими властивостями.

Список літератури

1. Теорія сигнально-кодових конструкцій: моногр. / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов, С.П. Євсєєв. – Х.: ХУПС, 2008. – 541 с.
2. Науменко М.І. Методи синтеза сигналів з заданими свойствами / М.І. Науменко, О.О. Кузнецов // Международный научно-теоретический журнал. – К.: Институт кибернетики НАН Украины. – 2007. – Вып. 3. – С. 10-17.
3. Метод формування псевдовипадкових послідовностей з поліпшеними автокореляційними властивостями / Ю.В. Стасєв, Д.О. Медведєв, Д.О. Грабенко, Д.В. Жуйков // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХНУ ПС, 2017. – Вип. 4(53). – С. 115-118.
4. Barannik V.V. Structural slotting with uniform redistribution for enhancing trustworthiness of information streams / V.V. Barannik, Yu.N. Ryabukha, S.A. Podlesnyi // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika). – 2017. – № 76 (7). – Pp. 607.
5. Кузнецов А.А. Алгеброгеометрические коды / А.А. Кузнецов // Электроника и системы управления. – К.: НАУ, 2005. – № 2(4). – С. 25-34.
6. Кузнецов А.А. Каскадное кодирование с алгеброгеометрическим кодом внешней ступени / А.А. Кузнецов // Информационно-керуючі системи на залізничному транспорті. – Х.: ХарДАЗТ, 2002. – № 3. – С. 21-25.
7. Alimpiev A.N. The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space / A.N. Alimpiev, V.V. Barannik, S.A. Sidchenko // Telecommunications and Radio Engineering, English translation of Elektrosvyaz and Radiotekhnika. – 2017. – № 76 (6). – Pp. 521-534.

8. Науменко Н.И. Оптимальный и подоптимальный прием сигналов со сверточным кодированием в негауссовских каналах с памятью и фазовой нестационарностью / Н.И. Науменко // Радиоэлектроника. – 1995. – № 1. – С. 52-63. (Изв. высш. учеб. заведений).
9. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. – М.: Связь, 1979. – 744 с.
10. Скляр Б. Цифровая связь. Теоретические основы и практическое применение; пер. с англ. Изд. 2-е, испр./ Б. Скляр. – М.: Издательский дом “Вильямс”, 2003. – 1104 с.
11. Кузнецов А.А. Методика оценки энергетической эффективности двоичных блочных кодов в каналах с группирующимися ошибками / А.А. Кузнецов // Моделювання та інформаційні технології. – К.: НАНУ, 2005. – № 32. – С. 116-124.
12. Кузнецов А.А. Алгеброгеометрические коды / А.А. Кузнецов // Электроника и системы управления. – К.: НАУ, 2005. – № 2(4). – С. 25-34.

References

1. Naumenko, M.I., Stasev, Yu.V., Kuznetsov, O.O. and Cvsev, SP. (2008), “*Teoriya syhnal'no-kodovykh konstruksiy: monohrafiia*” [*Theory of Signal-Code Designs: monohrafiia.*], HUPS, Kharkiv, 541 p.
2. Naumenko, M.I., Kuznetsov, O.O. (2007), “Metody synteza syhnalov s zadannymy svoystvamy” [Methods for synthesizing signals with given properties], *International Scientific and Theoretical Journal*, Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kiev, No. 3, pp. 10-17.
3. Stasev, Yu.V., Medvedev, D.O., Grabenko, D.O. and Zhuikov, D.V. (2016), “The method of formulating psevdovipadkovykh post-lidovnosti in polish with autocorrelated authorities” [The method of formulating psevdovipadkovykh post-lidovnosti in polish with autocorrelated authorities], *Scientific Works of Kharkiv National Air Force University*, KhNU PS, Kharkiv, No. 4 (53), pp. 115-118.
4. Barannik, V.V., Ryabukha, Yu.N. and Podlesnyi, S.A. (2017), “Structural slotting with uniform redistribution for enhancing trustworthiness of information streams”, *Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika)*, No. 76 (7), pp. 607.
5. Kuznetsov, A.A. (2005), “Alhebroheometrycheskye kody” [Algebrogeometric codes], *Electronics and control systems*, NAU, Kiev, No. 2 (4), pp. 25-34.
6. Kuznetsov, A.A. (2002) “Kaskadnoe kodyrovanye s alhebroheometrycheskym kodom vneshney stupeny” [Cascade coding with an algebraic geometric code of an external step], *Information and control systems on the railway transport*, HardAzTt, Kharkiv, No. 3, pp. 21-25.
7. Alimpiev, A.N., Barannik, V.V., Sidchenko, S.A. (2017), “The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space”, *Telecommunications and Radio Engineering, English translation of Elektrosvyaz and Radiotekhnika*, No. 76 (6), pp. 521-534.
8. Науменко, Н.И. (1995), “Оптимальный и подоптимальный прием сигналов со сверточным кодированием в негауссовских каналах с памятью и фазовой нестационарностью” [Optimum and suboptimal reception of signals with convolutional coding in non-Gaussian channels with memory and phase nonstationarity], *Izv. Higher Educational Institutions, Radioelectronics*, No. 1, pp. 52-63.
9. McWilliams, F.J., Sloan, N.J.A. (1979), “*Teoriya kodov, yspravlyayushchykh oshyby*” [*The theory of error correcting codes*], Communications, Moscow, 744 p.
10. Sklyar, B. (2003), “*Tsyfrovaya svyaz'. Teoretycheskiye osnovy y praktycheskoe prymereneye*” [*Digital Communication. Theoretical bases and practical application*], Publishing house "Williams", Moscow, 1104 p.
11. Kuznetsov, A.A. (2005), “A technique for estimating the energy efficiency of binary block codes in channels with grouped errors” [A technique for estimating the energy efficiency of binary block codes in channels with grouped errors], *Modeluvannya te informatsiyini tehnologii*, NASU, Kiev, No. 32, pp. 116-124.
12. Kuznetsov, A.A. (2005), “Alhebroheometrycheskye kody” [Algebrogeometric codes], *Electronics and control systems*, NAU, Kiev, No. 2 (4), pp. 25-34.

Надійшла до редколегії 10.05.2017

Схвалена до друку 17.08.2017

Відомості про авторів:

Стасєв Юрій Володимирович
 доктор технічних наук професор
 професор кафедри
 Харківського національного університету
 Повітряних Сил імені Івана Кожедуба,
 Харків, Україна
<https://orcid.org/0000-0002-3893-0313>
 e-mail: stasev543@gmail.com

Information about the authors:

Stasiev Yuriy
 Doctor of Technical Science Professor,
 professor of the Department
 of Ivan Kozhedub Kharkiv
 National Air Force University,
 Kharkiv, Ukraine
<https://orcid.org/0000-0002-3893-0313>
 e-mail: stasev543@gmail.com

Клеванна Людмила Олексіївна

курсант
Харківського національного університету
Повітряних Сил імені Івана Кожедуба,
Харків, Україна
<https://orcid.org/0000-0002-9757-9455>
e-mail: kleva2014@ukr.net

Klievanna Lyudmila

cadet
of Ivan Kozhedub Kharkiv National
Air Force University
Kharkiv, Ukraine
<https://orcid.org/0000-0002-9757-9455>
e-mail: kleva2014@ukr.net

Носик Олександр Юрійович

курсант
Харківського національного університету
Повітряних Сил імені Івана Кожедуба,
Харків, Україна
<https://orcid.org/0000-0003-4895-7816>
e-mail: nosik.alexander96@gmail.com

Nosik Alexander

cadet
of Ivan Kozhedub Kharkiv National
Air Force University
Kharkiv, Ukraine
<https://orcid.org/0000-0003-4895-7816>
e-mail: nosik.alexander96@gmail.com

**АЛГОРИТМ ФОРМИРОВАНИЯ СИГНАЛЬНО-КODOVЫХ КОНСТРУКЦИЙ
С УЛУЧШЕННЫМИ КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ**

Ю.В. Стасев, Л.А. Клеванная, А.Ю. Носик

В статье предлагается алгоритм повышения помехозащищенности систем управления и связи на основе синтеза сигнально-кодowych конструкций улучшенными корреляционными свойствами. Показано, что повышение помехозащищенности систем управления и связи возможно о совместном использовании препятственно-защищенных кодов и ортогональных дискретно-частотных сигналов. Формируются условия синтеза сигнально-кодowych конструкций с заданными корреляционными свойствами. Обосновывается выбор препятственно-защищенного кода. Сформулированы и доказаны необходимые условия размерности кода и его минимального кодового расстояния.

Ключевые слова: функция взаимной корреляции, корреляционные свойства, нормированная функция корреляции.

**ALGORITHM FOR THE FORMATION OF SIGNAL-CODE STRUCTURES
WITH IMPROVED CORRELATION PROPERTIES**

Yu. Stasiev, L. Klievanna, O. Nosik

In the article, suggests an algorithm for increasing noise immunity of control and communication systems based on the synthesis of signal-code structures by improved correlation properties. It is shown that an increase in noise immunity of control and communication systems is possible about the joint use of non-decode-coding codes and orthogonal discrete-frequency signals. Formation conditions for the synthesis of signal-code structures with specified correlation properties. The choice of the obstacle-dosage code is justified. The necessary conditions for the dimension of the code and its minimum code distance are formulated and proved. It is shown that the periodic correlation functions of the sequences formed by the code words of equidistant codes have a two-level structure, and the generated signal assemblies have improved autocorrelation properties.

Keywords: cross-correlation function, correlation properties, normalized correlation function.