Примеры новых идеальных периодических последовательностей

А.Н. Леухин, Н.В. Парсаев

ГОУ ВПО «Марийский государственный технический университет», Йошкар-Ола, пл.Ленина, 3, E-mail: code@martsu.net

Рассмотрены новые фазокодированные последовательности (ФКП) с идеальной периодической автокорреляционной функцией (ПАКФ). В качестве примера для периода $N=100$ показано, что в рамках разработанной алгебраической теории построения ФКП с одноуровневой ПАКФ можно построить более 10700 новых неэквивалентных ФКП с нулевыми боковыми лепестками (БЛ) ПАКФ.

New multiphase sequences with an ideal periodic autocorrelation function are considered. For example it is sown within the boundaries of the developed algebraic theory for synthesis of phase-coded sequences with the one-level periodic autocorrelation function that it is possible to design more than 10700 new non-equivalent multiphase sequences with the zero sidelobes for the period $N=100$.

В системах передачи информации идеи широкополосных сигналов позволяют решать сразу целый ряд задач: это обеспечение теоретически любой достоверности передачи данных (помехоустойчивость), возможность передачи данных со скоростью равной пропускной способности канала (кодовое уплотнение и разделение каналов), скрытность передачи (работа под шумами) и криптографическая защита передаваемых данных (шифрование) [1-5]. Особое внимание в теории сложных сигналов уделяется бинарным последовательностям с почти идеальной ПАКФ (уровень всех БЛ $a=-1$) [3,5] и многофазным последовательностям с идеальной ПАКФ (уровень всех БЛ $a=0$) [1-4].

Получены следующие результаты:

1) Построены ФКП с большой градацией фаз, синтезируемые на основе ступенчатой аппроксимации линейной частотной модуляции (ЛЧМ). Фаза на каждом кодовом интервале может принимать некоторые значения $\pi/N \cdot z$, где $z \in Z_{2N}$ - любое целое неотрицательное число из кольца $Z_{2N}=\{0,1,2,...,2N-1\}$. Известны следующие коды, ассоциируемые с ЛЧМ-сигналом: в начале 60-х годов построены коды Френка периода $N=k^2$ и Задоффа любого периода N и их последующие модификации с аналогичными периодами: коды Чу (1972), коды классов Р (80-е годы), многофазные коды Голомба (1993), а также коды Милевского (1994) периода $N=k^{2m+1}$;

2) Синтезированы бинарные последовательности (фаза на каждом кодовом интервале может принимать только значения 0 и π). Идеи построения бинарных кодовых последовательностей с одноуровневой АКФ (уровень боковых лепестков $a=-1$) сводятся к построению циклических разностных множеств типа Адамара с параметрами $(4t-1, 2t-1, t-1)$. Эта связь была установлена в 1950-х годах сразу в работах нескольких авторов, среди которых следует выделить работы Голомба. Голомб сформулировал задачу построения всех таких разностных множеств. На сегодняшний день получены следующие результаты в области построения разностных множеств (v,k,l) типа Адамара.

В случае размерностей $v \neq 2^n-1$ найдены следующие конструкции разностных множеств: - $v=4t-1=p$ - простое, конструкция квадратичных вычетов; - $v=4t-1=4x^2+27=p$ – простое, конструкция шестиричных вычетов Холла; - $v=4t-1=p_1 \cdot p_2$, $p_2=p_1+2$, p_1, p_2 – простые – конструкция Якоби. Не существует доказательства, что при $v \neq 2^n - 1$ эти конструкции являются единственными. Но для различных значений v методом перебора не удалось найти других конструкций.

В случае размерностей $v = 2^n - 1$ найдены следующие конструкции разностных множеств: - разностные множества Зингера ($p = 2$) для любых $n \geq 2$ (М-последовательности); - конструкции квадратичных вычетов, когда $v = 2^n - 1 = p$ – простое число Мерсенна; - конструкция шестиричных вычетов Холла $v = 2^n - 1 = 4x^2 + 27 = p$; - конструкции Гордона-Милза-Велча (GMW конструкции, каскадные GMW конструкции, обобщенные GMW конструкции, обобщенные каскадные GMW конструкции) для любого составного n, где $n > 4$; - конструкции 3-term и 5-term последовательностей; - конструкции степенных функций Кассами (H и B_k - последовательности); - конструкции Велча-Гонга, основанные на преобразованиях WG (Welch-Gong); - гиперовальные конструкции (конструкции гиперовалов Сегре, конструкции гиперовалов Глинна 1 и 2 типов). Не существует доказательства, что при $v = 2^n - 1$ эти конструкции являются единственными. Но для различных значений $n \leq 10$ методом перебора не удалось найти других конструкций. Начиная с 1950-х годов, примерно каждые 10 лет выполнялся полный перебор для поиска конструкций разностных множеств Адамара для значений n. В 2001 был выполнен полный перебор для показателя степени $n = 10$ [5]. Полный перебор для случая $n = 11$ ожидается примерно в 2010 году, а для случая $n = 12$ в 2020 году.

3) На основании перечисленных бинарных последовательностей путем замены символов кодового алфавита можно построить идеальные бифазные последовательности, впервые рассмотренные в работе [6], и позднее повторно открытые в работе [7].

В авторских работах [8-13] был разработан алгебраический подход, в рамках которого с единых позиций удалось синтезировать все известные на сегодняшний день ФКП с одноуровневой ПАКФ, а также построить значительное большее количество новых ФКП. В данной работе продемонстрируем возможности развитой теории синтеза ФКП с равномерной ПАКФ на примере построения ФКП с идеальной ПАКФ (уровень всех боковых лепестков равен $a = 0$) для периода $N = 100$.

Многофазную последовательность $\mathbf{\Gamma} = \{\gamma_n\}_{0,N-1}$ определим как:

$$\mathbf{\Gamma} = \{\gamma_n\}_{0,N-1} = \{\exp(i\varphi_n)\}_{0,N-1}, \ n = 0,\dots,N-1, \qquad (1)$$

где модуль каждого кодового элемента $|\gamma_n| = 1$, i – мнимая единица, значение фазы φ_n на каждом n-ом кодовом интервале принимает любое вещественное значение из диапазона $[0, 2\pi]$, N – период кодовой последовательности.

Периодическую АКФ $\{\mathrm{r}_\tau\}$ определим на основании выражения:

$$r_\tau = \sum_{n=0}^{N-1} \gamma_{n+\tau \ (\mathrm{mod}\ N)} \cdot \gamma_n^*, \ \tau = 0,1,\dots,N-1, \qquad (2)$$

где γ_n^* – комплексно-сопряженный кодовый элемент, τ – циклический сдвиг.

Нулевой отсчет ПАКФ должен быть равен периоду кодовой последовательности $r_0 = N$, а все остальные (боковые) должны принимать одинаковое значение a: $r_1 = r_2 = \dots = r_{N-1} = a$. Значение уровня боковых лепестков a может быть любым вещественным числом из диапазона $a \in [a_{\min}, a_{\max}]$. Где верхняя граница диапазона может принимать значение $a_{\max} = N$, а нижняя граница $a_{\min} \geq N/(N-1)$.

На основании выражений (1), (2) задача синтеза ФКП с одноуровневой ПАКФ сводится к решению системы трансцендентных уравнений [8-13]. Для исключения из рассмотрения «повернутых» последовательностей положим условие $\varphi = 0^o$.ФКП в фазовом представлении будет иметь вид:

$$\mathbf{\Psi} = \left\lfloor \varphi_0 = 0^o \quad \varphi_1 \quad \varphi_2 \quad \ldots \quad \varphi_{N-1} \right\rfloor, \tag{3}$$

С помощью линейных преобразований можно получить эквивалентные исходной (3) фазокодированные последовательности (последовательности с аналогичными корреляционными свойствами). В общем случае для произвольного периода N может существовать K эквивалентных ФКП, полученных в результате линейных преобразований некоторой исходной последовательности

$$\mathbf{\Phi}^{\mathrm{T}} = \left\lfloor \mathbf{\Psi}^{(0)} \quad \mathbf{\Psi}^{(1)} \quad \ldots \quad \mathbf{\Psi}^{(K-1)} \right\rfloor. \tag{4}$$

Каждая строка матрицы $\mathbf{\Phi}$ представляет собой некоторую ФКП в фазовом представлении. На основании исходной ФКП в общем случае можно сформировать $K = N$ «автоморфных» решений вида:

$$\varphi_n^{(k)} = \varphi_{n+k \mod(N)} - \varphi_k , \tag{5}$$

и $K = N$ «сопряженных» им решений вида

$$\varphi_n^{(k+N)} = \varphi_k - \varphi_{n+k \mod(N)} , \tag{6}$$

$$n = 0,1,..., N-1 ,\ k = 0,1,..., N-1 .$$

Кроме того, на основании исходной ФКП (3) системы уравнений с помощью децимаций можно сформировать еще $K = \varphi(N)$ «изоморфных» ФКП вида:

$$\varphi_n^{(k)} = \varphi_{n \cdot \lambda_k \mod(N)} , \tag{7}$$

λ_k - число взаимно-простое с N , $k = 0,1,...,\varphi(N)-1$, $\varphi(N)$ - функция Эйлера от числа N , $n = 0,1,..., N-1$, а также применить к «изоморфным» ФКП преобразования вида (6).

Таким образом, максимальное число эквивалентных кодовых последовательностей (изоморфных, автоморфных и сопряженных), полученных на основе некоторой кодовой последовательности общего вида, определится как:

$$K = 2 \cdot \varphi(N) \cdot N . \tag{8}$$

Приведем результаты построения новых ФКП с идеальной ПАКФ периода $N = 100$ в рамках разработанной теории синтеза [8-13].

Известными ФКП с идеальной ПАКФ данного периода являются коды Френка и коды Задоффа-Чу. Отметим, что обе указанные многофазные последовательности являются частными случаями бесконечного множества ФКП с идеальной ПАКФ, задаваемых с помощью следующего выражения [13]. Для периода кодовой последовательности, являющегося квадратным числом ($N = z^2$, z − положительное целое) при нулевом уровне $a = 0$ боковых лепестков ПАКФ существует бесконечное множество решений, задаваемых выражением:

$$\varphi_n = \alpha_{n \pmod k} + \frac{2\pi}{z} \cdot \left]\left(\frac{n}{z}\right)\right[\cdot n \pmod z,\ n = 0,1,..., N-1, \tag{9}$$

где $]x[$ − целая часть числа x; $\mathbf{A} = [0 \quad \alpha_1 \quad \alpha_2 \quad \ldots \quad \alpha_{z-1}]$ − вектор фаз, принимающих произвольные значения из диапазона $\alpha_0 = 0$, $\alpha_m \in [0;2\pi]$, $m = 1,\ldots,z-1$.

Для идеальной ФКП существует также преобразование вида:

$$\varphi_n^{(k)} = \varphi_n^{(0)} + 2 \cdot \pi \cdot k \cdot n/N ,\ n = 0,1,..., N-1 ,\ k = 0,1,..., N-1 \tag{10}$$

с помощью которого из исходной ФКП (3) можно сформировать в общем виде $K = N$ кодовых последовательностей, неэквивалентных исходной и друг другу.

В таблице 1 приведем несколько примеров исходных ФКП на основании каждой из которых с помощью преобразований (10) можно сформировать $K = 100$ неэквивалентных ФКП.

Таблица 1. Примеры исходных ФКП с идеальной ПАКФ периода $N = 100$

Фазовое представление ФКП с идеальной ПАКФ (в градусах)
0; 48,922; 306,645; 77,374; 46,293; 273,74; 94,748; 291,41; 333,327; 198,688; 218,633; 346,534; 135,54; 46,736; 92,308; 266,378; 267,189; 154,423; 52,415; 272,418; 284,232; 23,013; 346,467; 210,621; 213,802; 122,148; 109,362; 126,296; 141,986; 358,032; 141,715; 156,992; 206,194; 92,731; 308,763; 294,446; 337,212; 118,177; 301,53; 226,744; 63,413; 147,986; 254,089; 294,776; 287,203; 295,466; 85,205; 252,332; 179,556; 131,594; 304,887; 275,867; 194,617; 306,32; 308,432; 37,824; 321,929; 178,738; 32,739; 249,495; 143,596; 333,04; 265,841; 94,073; 121,84; 226,261; 11,532; 352,857; 351,491; 66,378; 206,149; 256,638; 320,032; 288,602; 146,737; 258,178; 37,242; 68,455; 141,096; 224,582; 338,654; 298,237; 259,3; 87,841; 48,814; 103,404; 23,929; 172,759; 245,5; 60,149; 349,34; 50,243; 240,413; 117,444; 42,835; 17,458; 271,288; 208,582; 190,037; 169,772
0; 249,104; 69,85; 98,944; 141,289; 28,341; 323,904; 346,725; 19,463; 243,32; 155,972; 51,695; 83,945; 337,823; 312,622; 107,226; 77,81; 56,672; 51,963; 72,241; 274,521; 89,743; 265,576; 189,618; 271,521; 281,295; 222,4; 216,503; 207,491; 124,266; 134,543; 229,962; 103,808; 2,479; 209,241; 244,917; 327,933; 147,125; 219,114; 127,948; 98,799; 87,565; 325,918; 313,788; 111,67; 191,362; 283,901; 181,016; 153,443; 259,349; 137,997; 234,165; 39,886; 240,423; 318,744; 54,395; 5,657; 179,749; 81,964; 108,512; 46,349; 21,368; 277,213; 8,215; 343,481; 169,435; 332,361; 316,651; 176,689; 152,009; 207,955; 72,902; 334,763; 198,339; 63,222; 97,061; 252,148; 38,419; 284,869; 273,172; 326,813; 66,102; 329,211; 86,935; 196,163; 69,567; 152,864; 313,206; 7,954; 68,735; 38,533; 169,459; 321,861; 208,207; 303,282; 99,987; 64,199; 79,977; 47,95; 208,045
0; 32,924; 215,484; 14,101; 301,407; 38,265; 69,437; 160,308; 132,186; 342,258; 31,546; 85,622; 107,805; 303,925; 19,84; 232,623; 151,475; 135,529; 288,574; 325,61; 57,412; 85,724; 11,722; 318,929; 182,049; 174,006; 176,28; 327,24; 7,9; 6,156; 149,217; 106,646; 246,606; 265,901; 241,178; 82,18; 213,797; 95,274; 249,174; 48,502; 219,115; 142,56; 187,906; 23,377; 237,353; 205,221; 142,473; 171,395; 150,523; 195,251; 42,708; 110,523; 330,443; 243,823; 332,629; 146,591; 271,899; 293,194; 118,296; 260,809; 153,295; 152,475; 121,298; 196,137; 169,808; 32,706; 31,907; 48,657; 270,126; 299,706; 46,248; 93,155; 243,934; 173,012; 42,261; 253,812; 3,113; 300,94; 155,905; 147,842; 95,079; 181,145; 65,949; 34,492; 33,27; 282,414; 153,875; 221,552; 73,205; 72,196; 218,613; 30,719; 342,715; 187,826; 244,631; 352,359; 179,731; 237,554; 80,364; 337,066
0; 218,593; 279,975; 313,61; 52,458; 194,801; 127,952; 138,856; 245,591; 130,05; 297,544; 181,761; 258,17; 152,459; 298,457; 264,737; 338,721; 169,919; 66,303; 310,595; 356,47; 208,674; 185,7; 68,855; 10,483; 13,809; 45,665; 306,762; 321,814; 111,43; 32,399; 231,535; 46,605; 346,827; 62,308; 312,665; 316,177; 220,772; 178,148; 267,603; 135,217; 212,626; 265,131; 309,862; 258,736; 313,929; 111,204; 130,38; 285,722; 60,415; 273,815; 232,325; 135,92; 19,193; 93,899; 238,127; 296,299; 213,346; 267,198; 59,984; 353,49; 112,425; 50,101; 344,329; 285,878; 170,238; 90,371; 112,138; 233,449; 214,837; 351,616; 10,772; 58,29; 188,256; 237,675; 56,746; 339,694; 225,904; 215,603; 148,498; 83,928; 156,863; 17,217; 288,388; 319,316; 344,677; 327,573; 181,514; 348,221; 280,377; 105,234; 87,02; 76,54; 177,383; 129,511; 281,273; 18,718; 128,436; 339,081; 205,282
0; 48,057; 193,316; 15,772; 133,405; 346,746; 215,375; 284,555; 346,286; 157,19; 40,958; 133,176; 100,468; 156,418; 40,966; 354,904; 133,157; 337,844; 151,604; 235,163; 10,428; 357,626; 330,407; 180,648; 212,058; 342,157; 258,122; 352,387; 326,729; 217,082; 9,83; 253,618; 317,642; 333,256; 356,643; 57,429; 321,702; 109,215; 10,357; 193,335; 234,434; 281,089; 205,313; 177,59; 53,879; 173,444; 279,175; 226,195; 290,617; 52,175; 81,116; 6,272; 1,276; 118,75; 246,906; 218,395; 140,329; 274,988; 34,247; 59,57; 277,839; 18,951; 186,526; 100,97; 86,985; 313,882; 88,487; 74,655; 231,939; 94,811; 225,646; 291,114; 225,033; 158,869; 96,32; 346,489; 90,852; 220,423; 283,332; 241,314; 248,083; 157,684; 253,392; 226,056; 238,517; 7,702; 16,686; 4,096; 52,855; 262,94; 323,737; 279,231; 132,134; 48,17; 250,077; 285,811; 23,244; 167,491; 333,371; 190,985
0; 358,344; 357,683; 118,492; 250,698; 322,83; 179,661; 26,174; 322,317; 34,116; 289,154; 249,515; 172,059; 231,406; 165,696; 189,592; 329,217; 34,205; 349,795; 41,753; 252,724; 246,408; 138,606; 158,634; 39,651; 259,251; 345,028; 125,572; 307,124; 289,094; 289,091; 358,194; 44,471; 317; 323,469; 5,644; 72,113; 324,243; 72,457; 337,968; 269,458; 80,373; 267,221; 260,223; 283,949; 202,354; 108,386; 284,933; 91,24; 44,417; 317,779; 196,574; 273,376; 24,868; 0,506; 134,734; 228,722; 326,894; 89,484; 95,334; 81,983; 207,308; 227,094; 94,848; 255,96; 34,315; 242,052; 349,781; 313,412; 208,641; 344,512; 124,21; 69,595; 196,467; 243,597; 79,333; 350,225; 278,812; 90,81; 150,54; 150,318; 205,085; 136,345; 258,861; 285,511; 317,121; 106,725; 169,403; 186,5; 75,039; 181,308; 96,771; 198,551; 174,688; 193,062; 142,219; 38,978; 9,134; 245,557; 194,409

Затем с помощью преобразований (4-7) для каждой неэквивалентной последовательности можно построить еще $K = 2 \cdot \varphi(100) \cdot 100 = 80000$ эквивалентных последовательностей. Таким образом, каждая исходная ФКП таблицы 1 задает всего $K = 100 \cdot 8000 = 800\,000$ ФКП периода $N = 100$ с идеальной ПАКФ.

Было найдено более 10700 неэквивалентных ФКП с идеальной ПАКФ, каждая из которых приводит к формированию еще 8000 эквивалентных. Отметим, что все такие последовательности отличаются от бесконечного множества ФКП с идеальной ПАКФ, определяемых на основании выражения (9).

Таким образом, в рамках разработанной теории удается синтезировать во много раз большее количество многофазных последовательностей с идеальной ПАКФ по сравнению с известными. Кроме того, были изучены свойства импульсной автокорреляции (ИАКФ) синтезированных последовательностей с идеальной ПАКФ, ввиду того, что один из подходов к построению кодов с хорошими свойствами ИАКФ основан на построении кодов с хорошими свойствами ПАКФ. Экспериментально было показано, что среди всех синтезированных ФКП с идеальной ПАКФ минимальный пиковый уровень БЛ импульсной автокорреляционной функции имеют коды Фрэнка.

Литература

1. Л.Е.Варакин. Системы связи с шумоподобными сигналами. – М.: Сов. радио, 1985, 384с.
2. В.П.Ипатов. Периодические дискретные сигналы с оптимальными корреляционными свойствами. – М.: Радио и связь, 1992, 152 с.
3. P.Fan, M.Darnell. Sequence design for communications Applications. RSP – John Wiley& Sons, Chichester, 1996.
4. N.Levanon, E.Mozeson. Radar signals. – John Wiley& Sons, Chichester, 2005, 411 p.
5. S.W.Golomb, G.Gong. Signal design for good correlation for wireless communication, cryptography, and radar. – Cambridge: University press, 2005, 438 p.
6. И.Н.Амиантов. Избранные вопросы статистической теории связи. –М.:Сов. радио, 1971, 416с.
7.S. W.Golomb. Two-valued sequences with perfect periodic autocorrelation// IEEE Transactions on Aerospace and Electronic Systems, March 1992, V. 28, № 2, pp. 383–386.
8. A.N.Leukhin. Algebraic solution of the synthesis problem for coded sequences// Quantum Electronics, 2005, Vol.35, No.8, pp.688-692.
9. А.Н.Леухин, А.Ю.Тюкаев, С.А.Бахтин, Л.Г.Корнилова. Новые фазокодированные последовательности с хорошими корреляционными характеристиками// Электромагнитные волны и электронные системы, 2007, том 12, №6, с.51-54
10. А.Н.Леухин, Н.В.Парсаев. Синтез шумоподобных фазокодированных последовательностей// Ученые записки Казанского государственного университета. Серия физико-математические науки, 2008, том 150, кн.2, с.38-50.
11. А.Н.Леухин, Н.В.Парсаев, Л.Г.Корнилова. Решение системы нелинейных уравнений для задачи синтеза шумоподобных фазокодированных последовательностей// Нелинейный мир, 2009, том 7, № 10, с.749-756.
12. А.Н.Леухин, Н.В.Парсаев. Общий подход к построению фазокодированных последовательностей с одноуровневой периодической автокорреляционной функцией// Изв. вузов России. Радиоэлектроника, 2009, Вып. 6, с.5-12.
13. А.Н.Леухин, Н.В.Парсаев. Бесконечные множества фазокодированных последовательностей с одноуровневой периодической автокорреляционной функцией// Радиотехника, 2009, №12, с.6-11.