УДК 621.396.253

Смирнов А.А.

ПРЕДЛОЖЕНИЯ ПО РЕАЛИЗАЦИИ УСТРОЙСТВ ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ С МНОГОУРОВНЕВОЙ ФУНКЦИЕЙ КОРРЕЛЯЦИИ

Исследуется алгебраический подход к формированию больших ансамблей дискретных сигналов с многоуровневой функцией корреляции, который основан на сечении циклических орбит групповых кодов. Число и величина уровней боковых лепестков функции корреляции формируемых последовательностей, а также мощность ансамбля сигналов определяются дистанционными и структурными свойствами колец многочленов над конечными полями. Разрабатываются предложения по аппаратной реализации устройств формирования дискретных сигналов с многоуровневой функцией корреляции.

Ключевые слова: ансамбли дискретных сигналов, многоуровневая функция корреляции, стеганография

1. Постановка проблемы в общем виде и анализ литературы

Большие ансамбли дискретных сигналов используются в стеганографических системах, построенных с использованием технологии прямого расширения спектра [1]. Перспективным направлением в развитии алгебраических методов теории дискретных сигналов является использование развитого математического аппарата теории конечных полей и, в частности, теории колец многочленов, что позволяет связать корреляционные свойства формируемых последовательностей с групповыми и структурными свойствами кодовых последовательностей [2 – 5]. Проведенные в этих работах исследования показали, что развиваемый алгебраический подход к синтезу дискретных сигналов на основе сечения циклических орбит группового кода позволяет формировать большие ансамбли последовательностей, корреляционные свойства которых обладают многоуровневой структурой. Наибольший практический интерес синтезированные сигналы представляют в радиосистемах управления со множественным доступом [6 – 8]. Использование больших ансамблей дискретных сигналов с улучшенными свойствами позволит существенно повысить абонентскую емкость радиосистем управления с кодовым разделением каналов.

В данной работе разрабатываются предложения по аппаратной реализации устройств формирования дискретных сигналов с многоуровневой функцией корреляции. Показано, что разработанные предложения позволяют формировать последовательности с улучшенными корреляционными и ансамблевыми свойствами и практически реализуют разработанный в [2 – 5] метод формирования дискретных сигналов.

2. Алгебраический подход к формированию дискретных последовательностей с многоуровневой функцией корреляции

Предложенный в работах [2 – 5] алгебраический подход к формированию больших ансамблей дискретных сигналов с многоуровневой функцией корреляции основан на сечении циклических орбит групповых кодов. Число и величина уровней боковых лепестков функции корреляции формируемых последовательностей, а также мощность ансамбля сигналов определяются дистанционными и структурными свойствами колец многочленов над конечными полями. Кратко рассмотрим эти положения, составляющие теоретическую основу формирования дискретных сигналов.

Групповой код однозначно задается лидерами (представителями) составляющих его циклических орбит. Под орбитой здесь и далее понимается множество кодовых слов эквивалентных друг другу относительно операции циклического сдвига. Под сечением орбит группового кода будем понимать выбор одного представителя (лидера) каждой орбиты. Дистанционные (корреляционные) свойства образованного таким образом множества лидеров определяются дистанционными свойствами групповых кодов, при этом эквивалентность относительно операции циклического сдвига отсутствует по определению

сечения орбит. Это свойство положим в основу формирования ансамбля дискретных сигналов. Схема сечения ненулевых циклических орбит группового кода представлена на рис. 1.

На рис. 1 показано разложение векторного пространства $GF^n(q)$ на множества непересекающихся орбит V_ξ, $\xi = 0,...,L$, представление группового кода V через объединение конечного числа орбит и схема выбора лидеров орбит – по одному произвольному представителю из каждого циклического подмножества V_ξ, $\xi = 0,...,M$ (для удобства обозначения кодовые слова $C_{\nu,u} = \left(c_0^{\nu,u}, c_1^{\nu,u}, ...c_{n-1}^{\nu,u}\right)$ обозначены двумя индексами: ν – номер орбиты V_ν кода V, $\nu = 1,...,M$; u – номер кодового слова в орбите, $u = 1,...,z_\nu$, где z_ν – число кодовых слов в орбите V_ν, $z_\nu \le n-1$).

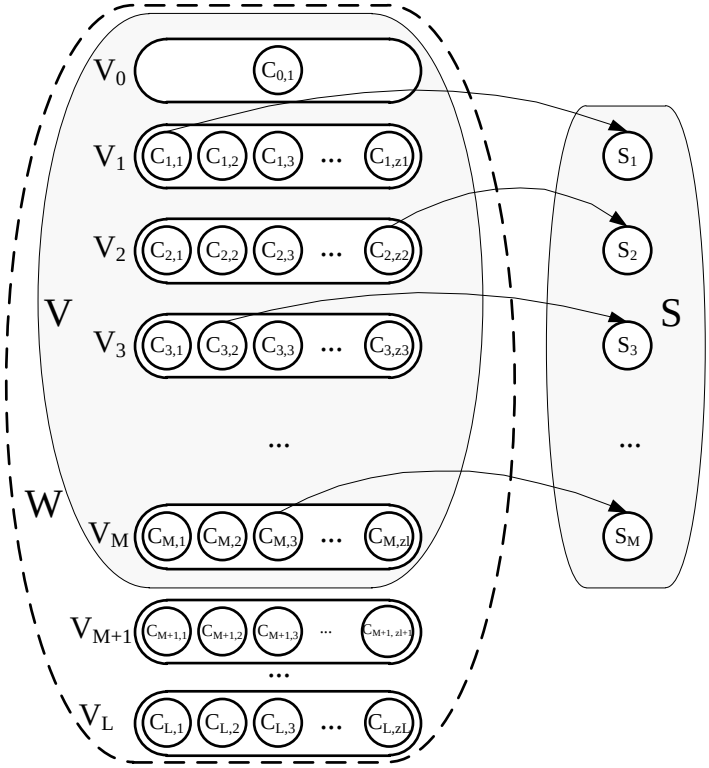

Рис. 1.Схема сечения ненулевых циклических орбит группового кода для формирования ансамбля дискретных сигналов

Из отобранных представителей орбит сформируем множество $S = (S_1, S_2, ..., S_M)$, где $S_\nu = C_{\nu,u}$, $\nu = 1,...,M$, а выбор индекса u при соответствующем $C_{\nu,u}$ определяется правилом сечения ν-й циклической орбиты группового кода.

Рассмотрим двоичный случай, т.е. ограничимся исследованием свойств множества $S = (S_1, S_2, ..., S_M)$, образованного посредством сечения циклических орбит двоичного группового кода. Элементы формируемых дискретных последовательностей (дискретных сигналов) $S_\nu = \left(s_0^\nu, s_1^\nu, ...s_{n-1}^\nu\right)$ зададим по элементам отобранных кодовых слов (лидеров орбит) $C_{\nu,u} = \left(c_0^{\nu,u}, c_1^{\nu,u}, ...c_{n-1}^{\nu,u}\right)$ следующим образом: $s_i^\nu = \begin{cases} 1, c_i^{\nu,u} = 1; \\ -1, c_i^{\nu,u} = 0. \end{cases}$

Предположим, что рассматриваемый (*n*, *k*, *d*) код V имеет весовой спектр вида:

$$\begin{cases} \mathrm{A}(0)=1; \\ \mathrm{A}(1)=0; \\ \mathrm{A}(2)=0; \\ \quad ... \\ \mathrm{A}(\mathrm{d}-1)=0; \\ \mathrm{A}(\mathrm{d}); \\ \mathrm{A}(\mathrm{d}+1); \\ \quad ... \\ \mathrm{A}(\mathrm{n}). \end{cases} \quad (1)$$

$w=0,...,n$, где $A(w)$ – число кодовых слов кода V с весом w.

Тогда образованное сечением циклических орбит кода V множество двоичных дискретных сигналов $S=(S_1,S_2,...,S_M)$, обладает корреляционными и ансамблевыми свойствами, определяемыми следующим утверждением [2 – 5].

Утверждение.

1. Боковые лепестки периодической функции авто- (ПФАК) и взаимной (ПФВК) корреляции ансамбля сигналов $S=(S_1,S_2,...,S_M)$ принимают следующие значения:

$$ПФВК, ПФАК=\frac{n-2w}{n},\ \text{для таких}\ w=d,d+1,...,n,\ \text{что}\ A(w)\neq 0. \quad (2)$$

2. Для всех таких $w=d,d+1,...,n$, что $A(w)=0$ боковые лепестки ПФАК и ПФВК никогда не принимают значений $\frac{n-2w}{n}$.

3. Мощность M ансамбля $S=(S_1,S_2,...,S_M)$ определяется числом ненулевых орбит кода V и ограничена снизу выражением:

$$M\geq\frac{2^k-1}{n}. \quad (3)$$

Равенство выполняется в случае максимального периода последовательностей всех орбит, образующих код, т.е. если код V состоит из набора орбит, образованных последовательностями максимальной длины (m-последовательностями).

Рассмотрим наиболее общий случай, когда двоичный групповой (n,k,d) код над $GF(2)$ задан через проверочный многочлен вида:

$$h(x)=f_{i1}(x)f_{i_2}(x)...f_{i_u}(x)=\prod_{s=1}^{m-1}\left(x-\alpha^{i_1(2^s)}\right)\left(x-\alpha^{i_2(2^s)}\right)...\left(x-\alpha^{i_u(2^s)}\right), \quad (4)$$

где $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x)-u$ произвольных подряд следующих минимальных многочлена элементов $\alpha^{i_1}\in GF(2^m)$, $\alpha^{i_2}\in GF(2^m)$, ..., $\alpha^{i_u}\in GF(2^m)$ соответственно, где порядок элементов α^{i_1}, α^{i_2}, ..., α^{i_u} равен порядку мультипликативной группы конечного поля $GF(2^m)$, $n=2^m-1$, α – примитивный элемент конечного поля $GF(2^m)$, $n=2^m-1$.

Положим без потери общности, что $i_1=1$. Определим проверочный и порождающий многочлен следующим образом:

$$h(x)=\prod_{s=0}^{m-1}\left(x-\alpha^{(2^s)}\right)\left(x-\alpha^{i_2(2^s)}\right)...\left(x-\alpha^{i_u(2^s)}\right),$$

$$g(x)=\frac{x^n-1}{h(x)}=\prod_{j\neq 1,i_2,...i_u}\ \prod_{s=0}^{m_j}\left(x-\alpha^{j(2^s)}\right).$$

Схематично процесс формирования проверочного и порождающего многочлена представлен на рис. 2. Символом v обозначено число классов сопряженных элементов, составляющих мультипликативную группу конечного поля $GF(2^m)$. В первом классе (элементы α^1, α^2, ..., $\alpha^{2^{m_1}} = \alpha^{2^{m-1}}$) содержится m сопряженных элементов (что определяет примитивность элемента α). В следующих классах (элементы α^j, α^{2j}, ..., $\alpha^{j2^{m_2}}$) содержится m_j сопряженных элементов (m_j делит нацело m), $j \in [1..v]$. Для каждого $j \in [1..v]$ соответствующее m_j определяется как наименьшее положительное целое, для которого справедливо равенство:

$$j = \left(j2^{m_j}\right) \bmod \left(2^m - 1\right).$$

Если порядок мультипликативной группы есть простое число, т.е. когда:

$$2^m - 1 = \textit{prime number},$$

тогда:

$$\forall j : m_j = m.$$

Единичный элемент поля $\alpha^0 = 1$ образует дополнительный сопряженный класс из одного элементов.

На рис. 3 представлено соответствующее распределение элементов конечного поля по многочленам $h(x)$ и $g(x)$. Элементы конечного поля из первых u классов сопряженных элементов являются корнями проверочного многочлена $h(x)$. Диапазон элементов конечного поля, в котором лежат корни проверочного многочлена $h(x)$, определяется наибольшим значением z, для которого выполняется условие $\alpha^z = \alpha^{(z) \bmod (2^m - 1)}$, т.е.:

$$z = \max_{s=0,\ldots,m-1} \left\{ \left(2^s\right) \bmod \left(2^m - 1\right), \left(i_2 2^s\right) \bmod \left(2^m - 1\right), \ldots, \left(i_u 2^s\right) \bmod \left(2^m - 1\right) \right\}.$$

В общем случае корни многочленов $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x)$ лежат в диапазоне:

$$\underbrace{\alpha^{i_1}, \ldots, \alpha^{i_1\left(2^{m-1}\right)}, \ldots, \alpha^{i_2}, \ldots, \alpha^{i_2\left(2^{m-1}\right)}, \ldots, \alpha^{i_u}, \ldots, \alpha^{i_u\left(2^{m-1}\right)}}_{z \text{ значений}},$$

откуда имеем:

$$2t = 2^m - z - 1,$$

и, соответственно,

$$d = 2t + 1 = 2^m - z.$$

Соответствующие кодовые параметры группового кода имеют вид:

$$\left(n = 2^m - 1, k = zm, d = 2^m - z\right). \tag{5}$$

Оценим весовой спектр кода. Проверочный многочлен кода с параметрами (5) содержит в качестве сомножителя проверочные многочлены всех кодов, с проверочными многочленами $h(x) = f_{i1}(x) f_{i_2}(x) \ldots f_{i_y}(x), y \le u$.

Отсюда следует, что все кодовые слова групповых кодов с $h(x) = f_{i1}(x) f_{i_2}(x) \ldots f_{i_y}(x), y \le u$ являются кодовыми словами рассматриваемого кода с параметрами (5), т.е. ненулевые компоненты весового спектра образуются поочередным добавлением (в порядке добавления сомножителей в многочлен $h(x) = f_{i1}(x) f_{i_2}(x) \ldots f_{i_y}(x), y \le u$) соответствующей пары элементов (для всех $y = 2,3,\ldots,u$):

$$A(z_y) \ne 0,$$

$$A(2^m - z_y) \ne 0,$$

где:

$$z_y = \max_{s=0,\ldots,m-1} \left\{ \left(2^s\right) \bmod \left(2^m - 1\right), \left(i_2 2^s\right) \bmod \left(2^m - 1\right), \ldots, \left(i_y 2^s\right) \bmod \left(2^m - 1\right) \right\}.$$

При $y=1$ имеем один ненулевой компонент весового спектра $A(2^{m-1})\neq 0$, который соответствует $z_y=2^{m-1}$.

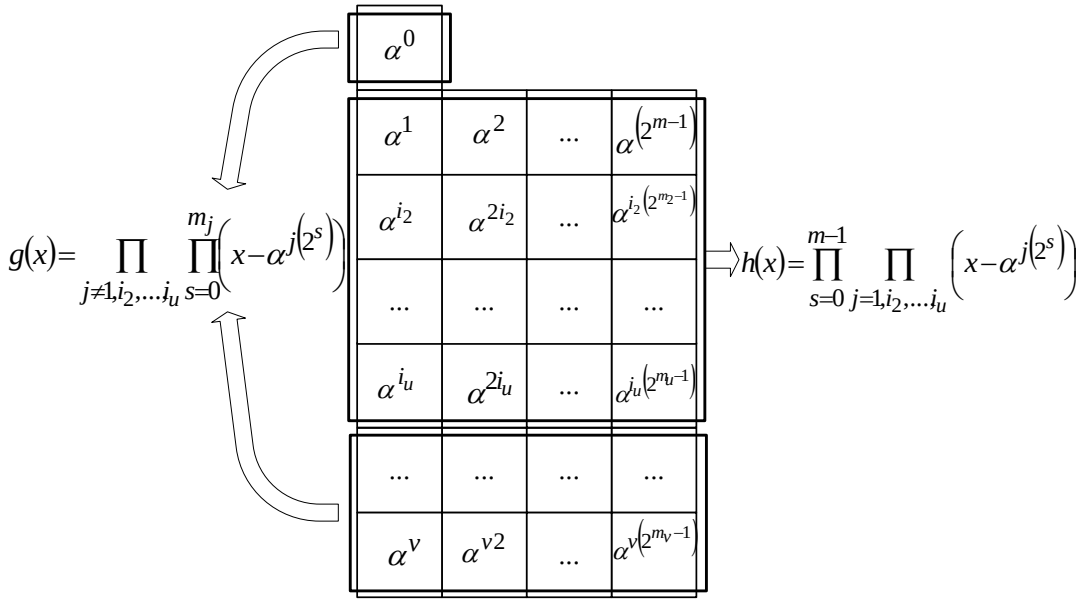

Рис. 2. Схема формирования проверочного и порождающего многочленов группового кода

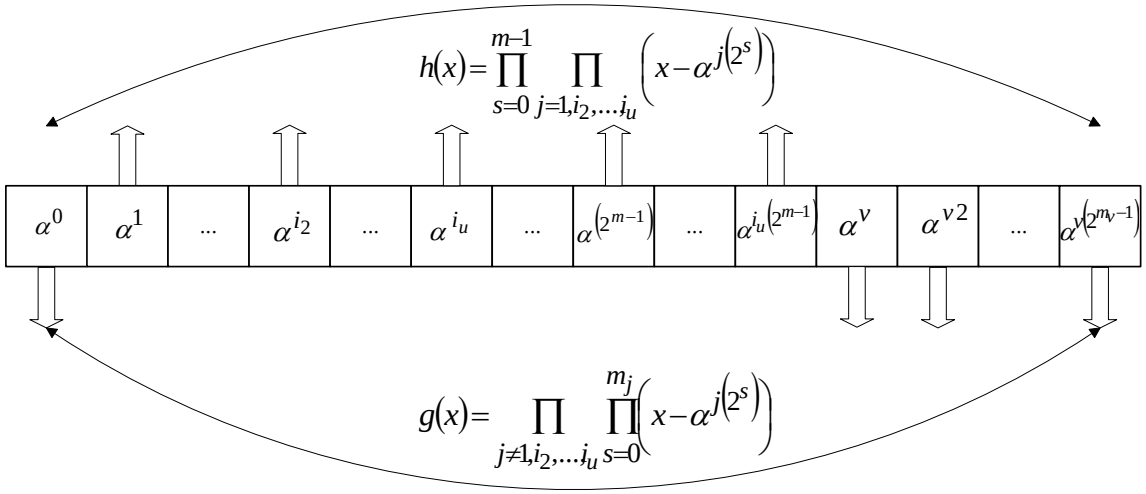

Рис. 3. Распределение элементов конечного поля по проверочному и порождающему многочленам группового кода

Рассмотренные в работах [2 – 5] случаи построения трех и пятиуровневых дискретных сигналов соответствуют:

$$y=2:z_y=2^{m-1}+2^{\frac{m+1}{2}-1},\ A(2^{m-1}+2^{\frac{m+1}{2}-1})\neq 0,\ A(2^{m-1}-2^{\frac{m+1}{2}-1})\neq 0,$$

$$y=3:z_y=2^{m-1}+2^{\frac{m+1}{2}},\ A(2^{m-1}+2^{\frac{m+1}{2}})\neq 0,\ A(2^{m-1}-2^{\frac{m+1}{2}})\neq 0.$$

Таким образом, трех и пятиуровневые дискретные сигналы являются частным случаем построения больших ансамблей дискретных сигналов с многоуровневыми функциями корреляции.

Общее выражение для оценки весового спектра группового кода, заданного проверочным многочленом (4) запишем в виде:

$$A(w)=\begin{cases}1, w=0;\\ \\ 0, w=1,\ldots,z_u-1;\\ \neq 0, w=z_u;\\ \ldots\\ \neq 0, w=z_3=2^{m-1}-2^{\frac{m+1}{2}};\\ 0, w=z_3+1,\ldots,z_2-1;\\ \neq 0, w=z_2=2^{m-1}-2^{\frac{m+1}{2}-1};\\ 0, w=z_2+1,\ldots,z_1-1;\\ \neq 0, w=z_1=2^{m-1};\\ 0, w=z_1+1,\ldots,2^m-z_2-1;\\ \neq 0, w=2^m-z_2=2^{m-1}+2^{\frac{m+1}{2}-1};\\ 0, w=2^m-z_2+1,\ldots,2^m-z_3-1;\\ \neq 0, w=2^m-z_3=2^{m-1}+2^{\frac{m+1}{2}};\\ \ldots\\ \neq 0, w=2^m-z_u;\\ 0, w=w=2^m-z_u+1,\ldots,2^m-1.\end{cases}$$

Таким образом, формируемые предлагаемым методом дискретные сигналы обладают многоуровневыми функциями авто и взаимной корреляции. Величины боковых выбросов принимают конечное число значений, задаваемых весовыми свойствами используемого группового кода.

Оценим мощность ансамбля формируемых дискретных сигналов. Мощность используемого кода $2^k=2^{um}$, всего имеется:

$$2^k-1=2^{um}-1,$$

ненулевых кодовых слов.

Если предположить, что каждое кодовое слово обладает максимальным периодом и в каждой циклической орбите содержится ровно 2^m-1 кодовых слов, тогда выражение для оценки мощности ансамбля формируемых сигналов примет вид:

$$M=\frac{2^{um}-1}{2^m-1}=2^{(u-1)m}+2^{(u-2)m}+\ldots+2^m+1.$$

Анализ последнего выражения показывает, что использование групповых кодов позволяет формировать большие ансамбли дискретных сигналов. Добавление минимального многочлена в качестве очередного сомножителя в проверочном многочлене повышает мощность ансамбля на $2^{(u-i)m}$, где $u-i$ – число добавленных минимальных многочленов.

Соответствующее выражение по оценке уровней боковых лепестков периодической функции корреляции в общем случае примет вид:

$$ПФВК, ПФАК = \begin{cases} \frac{2^m - 2z_u - 1}{2^m - 1}, w = z_u = \\ = \max\limits_{s=0,...,m-1} \left\{ \left(2^s\right) \bmod \left(2^m - 1\right), \left(i_2 2^s\right) \bmod \left(2^m - 1\right), ..., \left(i_u 2^s\right) \bmod \left(2^m - 1\right) \right\}; \\ ... \\ \frac{2^m - 2z_3 - 1}{2^m - 1} = \frac{-1 - 2^{\frac{m+1}{2}+1}}{2^m - 1}, w = z_3 = 2^{m-1} - 2^{\frac{m+1}{2}}; \\ \frac{2^m - 2z_2 - 1}{2^m - 1} = \frac{-1 - 2^{\frac{m+1}{2}}}{2^m - 1}, w = z_2 = 2^{m-1} - 2^{\frac{m+1}{2}-1}; \\ \frac{2^m - 2z_1 - 1}{2^m - 1} = \frac{-1}{2^m - 1}, w = z_1 = 2^{m-1}; \\ \frac{2^m - 2(2^m - z_2) - 1}{2^m - 1} = \frac{-1 + 2^{\frac{m+1}{2}}}{2^m - 1}, w = 2^m - z_2 = 2^{m-1} + 2^{\frac{m+1}{2}-1}; \\ \frac{2^m - 2(2^m - z_3) - 1}{2^m - 1} = \frac{-1 + 2^{\frac{m+1}{2}+1}}{2^m - 1}, w = 2^m - z_3 = 2^{m-1} + 2^{\frac{m+1}{2}}; \\ ... \\ \frac{2^m - 2(2^m - z_u) - 1}{2^m - 1}, w = 2^m - z_u = \\ = 2^m - \max\limits_{s=0,...,m-1} \left\{ \left(2^s\right) \bmod \left(2^m - 1\right), \left(i_2 2^s\right) \bmod \left(2^m - 1\right), ..., \left(i_u 2^s\right) \bmod \left(2^m - 1\right) \right\}. \end{cases} \quad (6)$$

3. Разработка предложений по аппаратной реализации устройств формирования дискретных сигналов предложенным методом

Разработанный метод формирования дискретных сигналов позволяет строить большие ансамбли слабокоррелированных двоичных последовательностей. Рассмотрим возможности практического формирования больших ансамблей слабокоррелированых дискретных сигналов и построения соответствующих аппаратных устройств генерирования двоичных последовательностей. Рассмотрим первый, самый простой случай, который отвечает формированию субортогональных дискретных сигналов через проверочный многочлен группового кода, заданный выражением:

$$h(x) = f_i(x) = \prod_{s=0}^{m-1} \left(x - \alpha^{i\left(2^s\right)} \right).$$

Формирование субортогональных дискретных сигналов отвечает правилу формирования двоичных последовательностей максимальной длины. Структурная схема устройства формирования субортогональных дискретных сигналов показана на рис. 4.

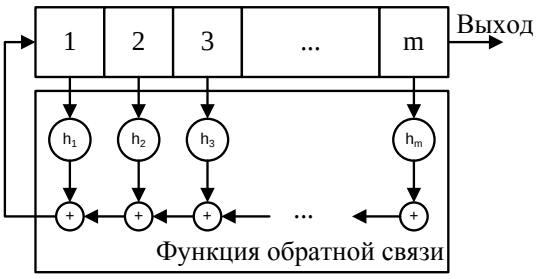

Рис. 4. Структурная схема устройства формирования субортогональных дискретных сигналов

Схема подключения отводов регистра сдвига в кольцо обратной связи задается коэффициентами отобранного примитивного многочлена степени m:

$$h(x) = h_0 + h_1 x + h_2 x^2 + ... + h_m x^m .$$

При этом длина двоичных последовательностей равняется $n = 2^m - 1$ и для их формирования нужно использовать регистр сдвига с m двоичными разрядами. Начальное состояние регистра сдвига задает вид формируемой последовательности.

После введения начального состояния регистра сдвига и определения соответствующих функций обратной связи регистров сдвига устройство функционирует как генератор последовательностей максимальной длины.

Рассмотрим процесс формирования дискретных сигналов с трехуровневой функцией корреляции через проверочный многочлен группового кода, заданный выражением:

$$h(x) = f_{i1}(x) f_{i_2}(x) = \prod_{s=1}^{m-1} \left(x - \alpha^{i_1(2^s)}\right)\left(x - \alpha^{i_2(2^s)}\right).$$

Формирование дискретных сигналов с трехуровневой функцией корреляции (двоичных последовательностей Голда) основывается на том, ее элементы формируются с помощью переключательных схем на основе двух регистров сдвига и сумматора. Структурная схема такого устройства показана на рис. 5.

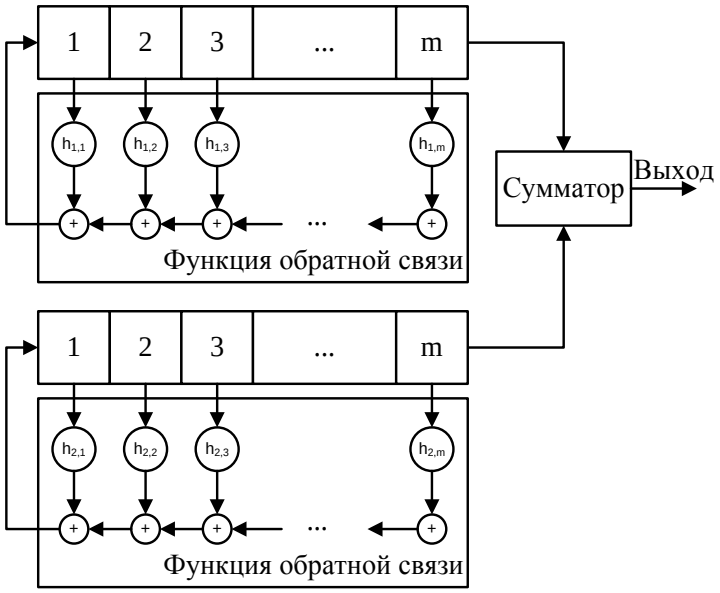

Рис. 5. Структурная схема устройства формирования дискретных сигналов с трехуровневой функцией корреляции

Схема подключения отводов первого и второго регистра сдвига в кольцо обратной связи задается коэффициентами отобранных примитивных многочленов степени m. При этом длина двоичных последовательностей равняется $n = 2^m - 1$ и для их формирования нужно использовать два регистра сдвига с m двоичными разрядами. Начальное состояние регистров сдвига задает вид формируемой последовательности.

Для первого регистра сдвига функция обратной связи задается коэффициентами примитивного многочлена степени m:

$$h_1(x) = h_{1,0} + h_{1,1} x + h_{1,2} x^2 + ... + h_{1,m} x^m = f_{i_1}(x) = \prod_{s=0}^{m-1} \left(x - \alpha^{i_1(2^s)}\right),$$

где $f_{i_1}(x)$ – минимальный многочлен элемента α^{i_1} из конечного поля $GF(2^m)$, который задается через свои корни $\alpha^{i_1(2^s)}$, $s = 0, 1, ..., m-1$.

Соответствующая функция обратной связи второго регистра сдвига задается коэффициентами примитивного многочлена степени m:

$$h_2(x) = h_{2,0} + h_{2,1}x + h_{2,2}x^2 + ... + h_{2,m}x^m = f_{i_2}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_2(2^s)}\right),$$

где $f_{i_2}(x)$ – минимальный многочлен элемента α^{i_2} из конечного поля $GF(2^m)$, который задается через свои корни $\alpha^{i_2(2^s)}$, $s = 0, 1, ..., m-1$.

Порядок элементов α^{i_1} и α^{i_2} равняется порядку мультипликативной группы конечного поля $GF(2^m)$, α – примитивный элемент конечного поля $GF(2^m)$.

Формирование дискретных сигналов с трехуровневой функцией корреляции основано на операции добавления по модулю 2 двух последовательностей максимальной длины, которые формируются соответствующими регистрами сдвига. Операция сложения выполняется сумматором посимвольно. При этом между двумя регистрами поддерживаются одни и те же фазовые соотношения, а формируемая последовательность имеет такую же длину, что и исходные последовательности максимальной длины, к которым применяется операция сложения.

Добавление к одной последовательности максимальной длины другой последовательности максимальной длины, циклический сдвинутой на произвольное количество двоичных разрядов (от 1 до $2^m - 1$) дает последовательность, которая отличается от соответствующих сдвигов исходных последовательностей. Иначе говоря, в случае, когда m простое число, генератор дискретных сигналов с трехуровневой функцией корреляции позволяет формировать:

$$M = \frac{2^{2m} - 1}{2^m - 1} = 2^m + 1$$

последовательностей длины $n = 2^m - 1$.

Рассмотрим случай формирования дискретных сигналов с пятиуровневой функцией корреляции через проверочный многочлен группового кода, заданный выражением

$$h(x) = f_{i1}(x) f_{i_2}(x) f_{i_3}(x) = \prod_{s=1}^{m-1}\left(x - \alpha^{i_1(2^s)}\right)\left(x - \alpha^{i_2(2^s)}\right)\left(x - \alpha^{i_3(2^s)}\right).$$

Формирование дискретных сигналов с пятиуровневой функцией корреляции заключается в том, ее элементы формируются с помощью переключательных схем на основе трех регистров сдвига и сумматора.

На рис. 6. показана структурная схема устройства формирования дискретных сигналов с пятиуровневой функцией корреляции предложенным способом.

Устройство построено через подключение к сумматору выходов трех регистров сдвига.

Схема подключения отводов первого, второго и третьего регистра сдвига в кольцо обратной связи задается коэффициентами отобранных примитивных многочленов $h_1(x)$, $h_2(x)$ и $h_3(x)$ степени m, соответственно.

При этом длина двоичных последовательностей равняется $n = 2^m - 1$ и для их формирования нужно использовать три регистра сдвига с m двоичными разрядами.

Начальное состояние регистров сдвига задает вид формируемой последовательности.

Для первого регистра сдвига функция обратной связи задается коэффициентами примитивного многочлена степени m:

$$h_1(x) = h_{1,0} + h_{1,1}x + h_{1,2}x^2 + ... + h_{1,m}x^m = f_{i_1}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_1(2^s)}\right),$$

где $f_{i_1}(x)$ – минимальный многочлен элемента α^{i_1} из конечного поля $GF(2^m)$, который задается через свои корни $\alpha^{i_1(2^s)}$, $s = 0, 1, ..., m-1$.

Соответствующая функция обратной связи второго регистра сдвига задается коэффициентами примитивного многочлена степени m:

$$h_2(x) = h_{2,0} + h_{2,1}x + h_{2,2}x^2 + ... + h_{2,m}x^m = f_{i_2}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_2(2^s)}\right),$$

где $f_{i_2}(x)$ – минимальный многочлен элемента α^{i_2} из конечного поля $GF(2^m)$, который задается через свои корни $\alpha^{i_2(2^s)}$, $s = 0, 1, ..., m-1$.

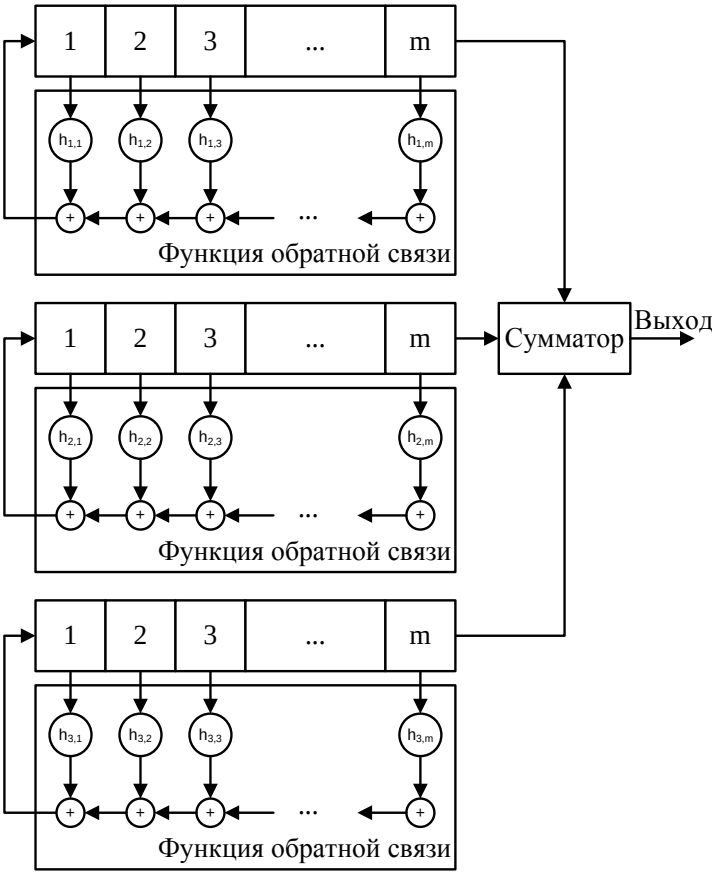

Рис. 6. Структурная схема устройства формирования дискретных сигналов с пятиуровневой функцией корреляции

Функция обратной связи третьего регистра сдвига задается коэффициентами примитивного многочлена степени m:

$$h_3(x) = h_{3,0} + h_{3,1}x + h_{3,2}x^2 + ... + h_{3,m}x^m = f_{i_3}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_3(2^s)}\right),$$

где $f_{i_3}(x)$ – минимальный многочлен элемента α^{i_3} из конечного поля $GF(2^m)$, который задается через свои корни $\alpha^{i_3(2^s)}$, $s = 0, 1, ..., m-1$.

Порядок элементов α^{i_1}, α^{i_2} и α^{i_3} равняется порядку мультипликативной группы конечного поля $GF(2^m)$, α – примитивный элемент конечного поля $GF(2^m)$.

Устройство работает следующим образом. После введения начальных состояний регистров сдвига и определения соответствующих функций обратной связи каждый из трех регистров сдвига формирует последовательности максимальной длины. Три определенных генератора работают синфазно, то есть с помощью тактовых импульсов или другого приема, между тремя регистрами поддерживаются одни и те же фазовые соотношения. На каждом такте работы устройства каждый регистр сдвига формирует на своем выходе один двоичный элемент, который подается на вход сумматора. Операция добавления выполняется сумматором посимвольно. Таким образом, формирование исходной последовательности происходит поэлементно, путем выполнения операции сложения по модулю 2 трех поданных

на сумматор элементов. При этом формируемая последовательность имеет такую же длину, что и исходные последовательности максимальной длины, к которым применяется операция добавления.

Добавление к одной последовательности максимальной длины двух других последовательностей максимальной длины циклически сдвинутых на произвольное количество двоичных разрядов (от 1 до $2^m - 1$) дает последовательность, которая отличается от соответствующих сдвигов исходных последовательностей. Иначе говоря, в случае, когда m простое число, предложенный генератор дискретных последовательностей позволяет формировать:

$$M = \frac{2^{3m} - 1}{2^m - 1} = 2^{2m} + 2^m + 1$$

последовательностей длины $n = 2^m - 1$.

Обобщая рассмотренные устройства формирования дискретных сигналов на случай многоуровневых последовательностей, получим следующую схему. (рис. 7). Устройство построено через подключение к сумматору выходов *u* регистров сдвига. Схема подключения отводов соответствующих регистру сдвига в кольцо обратной связи задается коэффициентами отобранных примитивных многочленов $h_1(x)$, $h_2(x)$, ..., $h_u(x)$ степени m, соответственно. При этом длина двоичных последовательностей равняется $n = 2^m - 1$ и для их формирования нужно использовать *u* регистров сдвига регистры сдвига с m двоичными разрядами. Начальное состояние регистров сдвига задает вид формируемой последовательности.

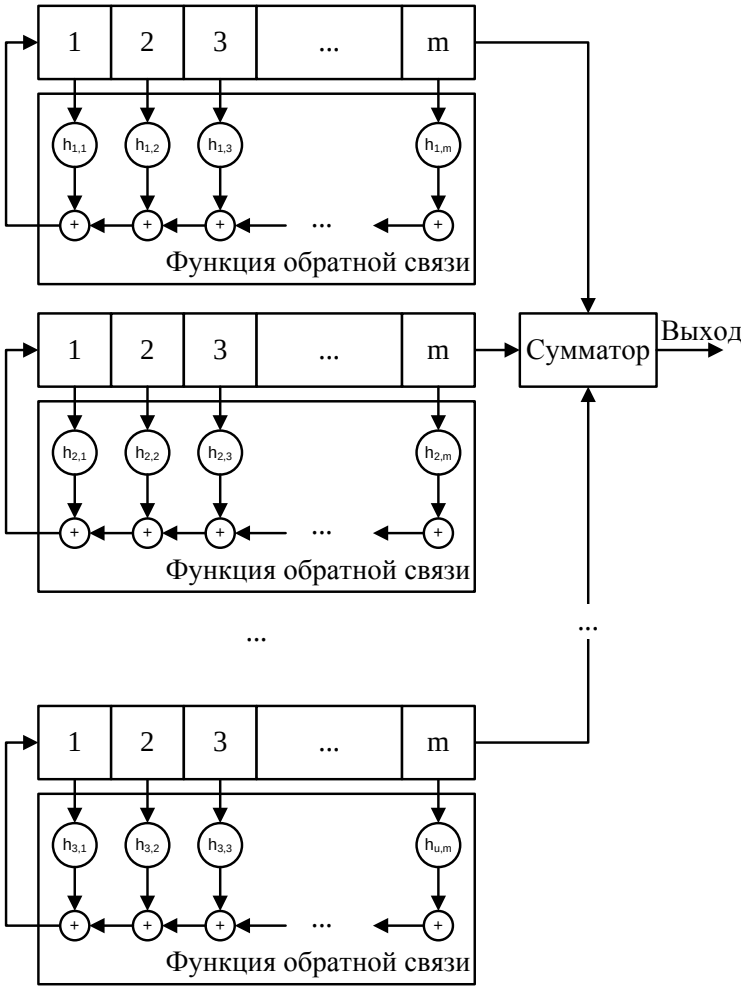

Рис. 7. Структурная схема устройства формирования дискретных сигналов с многоуровневой функцией корреляции

Функции обратной связи регистров сдвига задаются коэффициентами примитивных многочленов степени m:

$$h_1(x) = h_{1,0} + h_{1,1}x + h_{1,2}x^2 + ... + h_{1,m}x^m = f_{i_1}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_1(2^s)}\right)$$

$$h_2(x) = h_{2,0} + h_{2,1}x + h_{2,2}x^2 + ... + h_{2,m}x^m = f_{i_2}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_2(2^s)}\right),$$

...

$$h_u(x) = h_{u,0} + h_{u,1}x + h_{u,2}x^2 + ... + h_{u,m}x^m = f_{i_u}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_u(2^s)}\right)$$

где $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x)$ – минимальные многочлены элементов α^{i_1}, α^{i_2}, ..., α^{i_u}, соответственно, из конечного поля $GF(2^m)$, которые задаются через свои корни $\alpha^{i_1(2^s)}$, $\alpha^{i_2(2^s)}$, ..., $\alpha^{i_u(2^s)}$, $s = 0, 1, ..., m-1$.

Порядок элементов α^{i_1}, α^{i_2}, ..., α^{i_u} равняется порядку мультипликативной группы конечного поля $GF(2^m)$, α – примитивный элемент конечного поля $GF(2^m)$.

Устройство работает рассмотренным выше образом и позволяет формировать:

$$M = \frac{2^{um}-1}{2^m-1} = 2^{(u-1)m} + 2^{(u-2)m} + ... + 2^m + 1$$

последовательностей длины $n = 2^m - 1$.

4. Выводы

Таким образом, в ходе проведенных исследований были разработаны практические предложения, относительно аппаратной реализации устройств формирования дискретных последовательностей.

Разработанные схемы реализуются вычислительно эффективными преобразователями, например, на основе цепей с регистрами сдвига и сумматором (смотри рис. 4 – 7). Они позволяют формировать большие ансамбли дискретных сигналов с улучшенными корреляционными и ансамблевыми свойствами. Таким образом, разработанные предложения позволяют практически реализовать разработанный метод формирования дискретных сигналов.

ЛИТЕРАТУРА

1. Смирнов А.А. Метод стеганографического встраивания информации в неподвижные изображения с использованием сложных дискретных сигналов и прямого расширения спектра / А.А. Смирнов // Науково-технічний журнал «Захист інформації». – Випуск 4 (53). – К.: НАУ. – 2011 – С.64-70.
2. Кузнецов А.А., Смирнов А.А., Сай В.Н. Дискретные сигналы с многоуровневой функцией корреляции // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХНУРЭ.–2011. – Вып. 166. – С. 142-152.
3. Кузнецов А.А., Смирнов А.А., Сай В.Н. Формирование дискретных сигналов с многоуровневой функцией корреляции // Системи обробки інформації. – Харків: ХУ ПС. – 2011 – Вып. 5(95). – С. 50-60.
4. Kuznetsov A.A. Use of Complex Discrete Signals for Steganographic Information Security / A.A. Kuznetsov, A.A. Smirnov // International Journal of Engineering Practical Education. – Volume 1, Issue 1. – USA, Indiana: Science and Engineering Publishing Company. – 2012. – P. 21-25.
5. Смирнов А.А. Сравнительные исследования методов синтеза дискретных сигналов с особыми корреляционными свойствами / А.А. Смирнов, Е.В. Мелешко // Збірник тез V міжнародного науково-технічного симпозіуму «Новітні технології в телекомунікаціях» (ДУІКТ-Карпати-2012) м. Київ. 17-21 січня 2012 р. – Київ: ДУІКТ. – 2012. – С. 80-81.
6. Гряник М.В., Фролов В.И. Технология CDMA – будущее сотовых систем в Украине. – Мир связи, 1998, № 3. – С. 40–43.
7. Науменко Н. І., Стасев Ю. В., Кузнецов О.О., Євсєєв С.П. Теорія сигнально-кодових конструкцій. Х.:ХУ ПС, 2008р. – 489.
8. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

Надійшла: 16.10.2012 р.

Рецензент: д.т.н., професор Конахович Г.Ф.