УДК 621.396.253

ПРОГРАММНАЯ МОДЕЛЬ УСТРОЙСТВА ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ С ОСОБЫМИ КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

А.А. СМИРНОВ

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 программной реализации устройств формирования дискретных сигналов с многоуровневой функцией корреляции.

Ключевые слова: программная модель, дискретные сигналы, особые корреляционные свойства, многоуровневая функция корреляции.

ВВЕДЕНИЕ

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 [1 – 4]. 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 [5–7]. 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 программной 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 [1–4] метод формирования дискретных сигналов.

1. АЛГЕБРАИЧЕСКИЙ ПОДХОД К ФОРМИРОВАНИЮ ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С МНОГОУРОВНЕВОЙ ФУНКЦИЕЙ КОРРЕЛЯЦИИ

Предложенный в работах [1 – 4] 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.

Векторное пространство $GF^n(q)$ расклады-вается на множество непересекающихся орбит V_ξ, $\xi = 0,...,L$. При этом групповой код V представляется через объединение конечного числа орбит. Предлагается следующая схема выбора лидеров орбит – по одному произвольному представителю из каждого циклического подмножества V_ξ, $\xi = 0,...,M$ (для удобства обозначения кодовые слова $C_{v,u} = \left(c_0^{v,u}, c_1^{v,u}, ...c_{n-1}^{v,u}\right)$ обозначены двумя индексами: v – номер орбиты V_v кода V, $v = 1,...,M$; u – номер кодового слова в орбите, $u = 1,...,z_v$, где z_v – число кодовых слов в орбите V_v, $z_v \le n-1$).

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

Рассмотрим двоичный случай, т.е. ограничимся исследованием свойств множества $S = \left(S_1, S_2, ..., S_M\right)$, образованного посредством

сечения циклических орбит двоичного группового кода. Элементы формируемых дискретных последовательностей (дискретных сигналов) $S_v = \left(s_0^v, s_1^v, ...s_{n-1}^v\right)$ зададим по элементам отобранных кодовых слов (лидеров орбит) $C_{v,u} = \left(c_0^{v,u}, c_1^{v,u}, ...c_{n-1}^{v,u}\right)$ следующим образом: $s_i^v = \begin{cases} 1, c_i^{v,u} = 1; \\ -1, c_i^{v,u} = 0. \end{cases}$

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

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

$w = 0,...,n$, 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 [1 – 4].

Утверждение.

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

$$\text{ПФВК, ПФАК} = \frac{n-2w}{n}, \qquad (2)$$

для таких $w = d, d+1, ..., n$, что $A(w) \neq 0$.

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:

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

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:

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

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

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. 1. Символом v обозначено число классов сопряженных элементов, составляющих мультипликативную группу конечного поля $GF\left(2^m\right)$. 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. 2 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.:

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

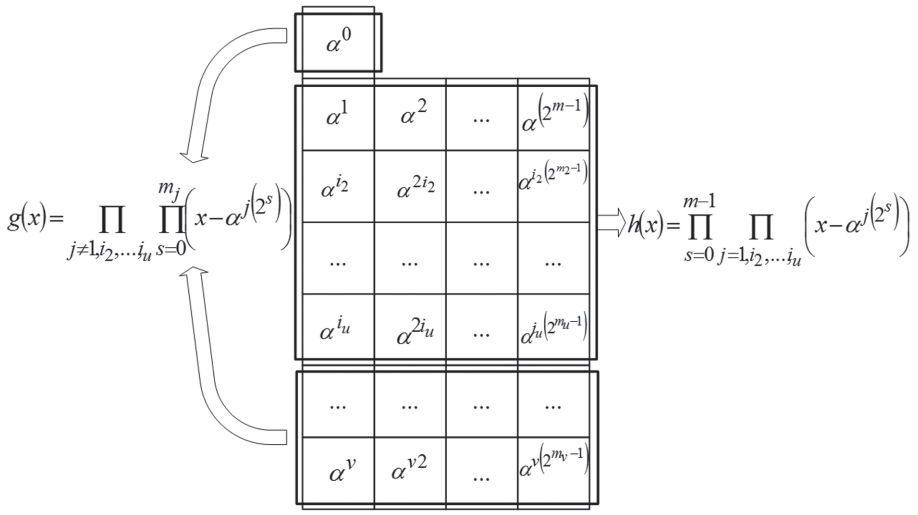

Рис. 1. Схема формирования проверочного и порождающего многочленов группового кода

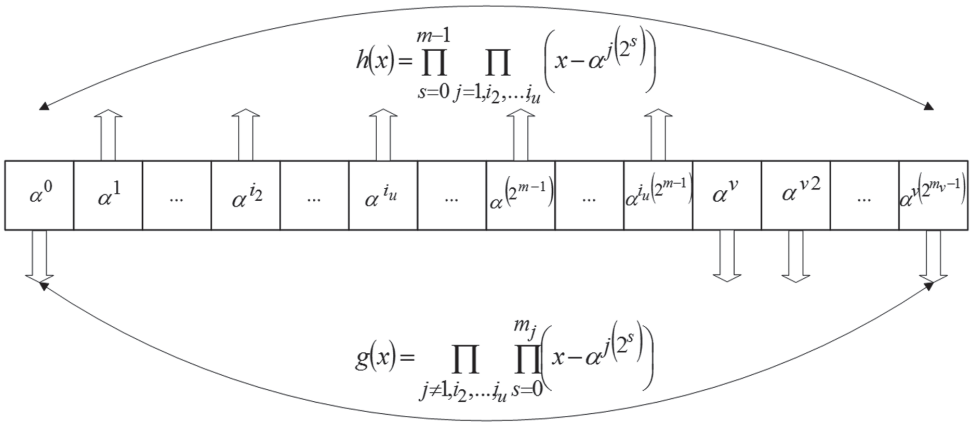

Рис. 2. Распределение элементов конечного поля по проверочному и порождающему многочленам группового кода

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

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

откуда имеем:

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

и, соответственно:

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

Соответствующие кодовые параметры группового кода имеют вид:

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

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

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

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

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

где:

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

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

Рассмотренные в работах [1 – 4] 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:

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

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

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

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.

3. АППАРАТНАЯ РЕАЛИЗАЦИЯ 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.

Формирование дискретных сигналов на случай многоуровневых последовательностей, реализуется с использованием следующей схемы. (рис. 3). 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.

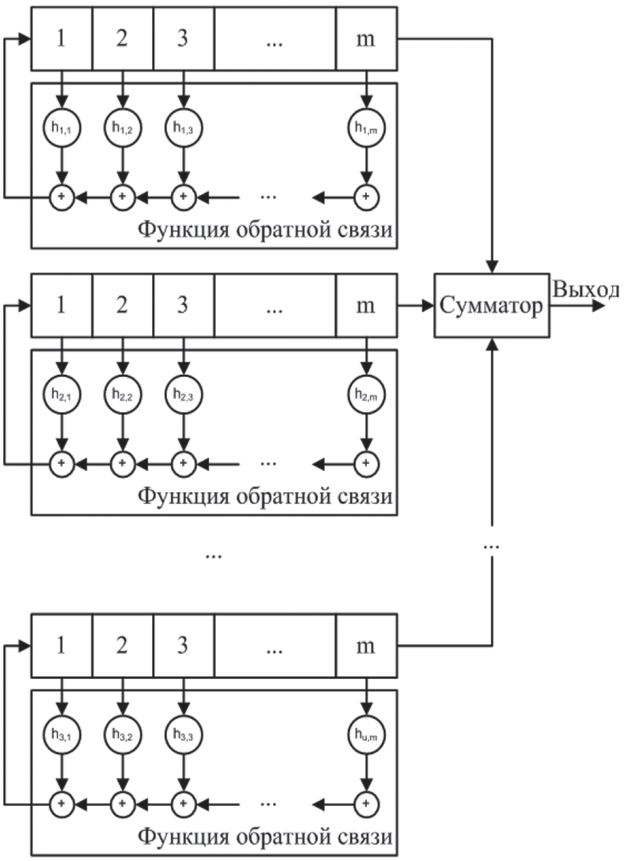

Рис. 3. Структурная схема устройства формирования дискретных сигналов с многоуровневой функцией корреляции

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

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

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

...,

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

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 $\alpha^{i_1(2^s)}$, $\alpha^{i_2(2^s)}$, ..., $\alpha^{i_u(2^s)}$, $s = 0, 1, \ldots, m-1$.

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:

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

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

4. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ УСТРОЙСТВ ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ ПРЕДЛОЖЕННЫМ МЕТОДОМ

Программа создана для практической проверки алгоритмов формирования дискретных сигналов с многоуровневой функцией корреляции предложенным методом, а также для эмпирического доказательства соответствия значений боковых выбросов функции авто- и взаимной корреляции теоретически предсказанным значениям, путём полного перебора при малых значениях *m* (5, 7, 11).

Алгоритм работы программы состоит в следующем.

Сперва выбирается значение *m*, для которого необходимо сформировать ансамбли дискретных сигналов с одно-, трех- и пятиуровневой функцией корреляции.

Затем задается порождающий полином конечного поля $GF(2^m)$ и рассчитываются значения примитивных 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 $GF(2^m)$, $n = 2^m - 1$.

После этого для заданного *m* элементы конечного поля распределяются в циклотомические классы (рис. 1).

Следующим шагом является формирование функций обратной связи регистров сдвига

(линейных рекуррентных регистров), которые задаются коэффициентами примитивных многочленов степени m, соответствующих элементов циклотомических классов.

Для формирования m-последовательностей используется один линейный рекуррентный регистр, функция работы которого задается проверочным полиномом $h(x)$. При этом корни минимальных многочленов $f_{i_1}(x)$, являющихся сомножителями, из которых образуется данный полином, принадлежат элементам одного циклотомического класса.

Для формирования сигналов Голда (дискретные сигналы с трехуровневой функцией авто- и взаимной корреляции) используются два линейных рекуррентных регистра, работа которых задается функциями $f_{i_1}(x)$ и $f_{i_2}(x)$ (рис. 3). Где $f_{i_1}(x)$ и $f_{i_2}(x)$ – два произвольных подряд следующих минимальных многочлена элементов $\alpha^{i_1} \in GF(2^m)$ и $\alpha^{i_2} \in GF(2^m)$ соответственно, где порядок элементов α^{i_1} и α^{i_2} равен порядку мультипликативной группы конечного поля $GF(2^m)$, $n = 2^m - 1$, α – примитивный элемент конечного поля $GF(2^m)$, $n = 2^m - 1$.

Для формирования дискретных сигналов с пятиуровневой функцией авто- и взаимной корреляции используются три линейных рекуррентных регистра, работа которых задается функциями $f_{i_1}(x)$, $f_{i_2}(x)$ и $f_{i_3}(x)$ (рис. 3). Где $f_{i_1}(x)$, $f_{i_2}(x)$ и $f_{i_3}(x)$ – три произвольных подряд следующих минимальных многочлена элементов $\alpha^{i_1} \in GF(2^m)$ и $\alpha^{i_2} \in GF(2^m)$ соответственно, где порядок элементов α^{i_1} и α^{i_2} равен порядку мультипликативной группы конечного поля $GF(2^m)$, $n = 2^m - 1$, α – примитивный элемент конечного поля $GF(2^m)$, $n = 2^m - 1$.

Добавление в дальнейшем еще одного линейного рекуррентного регистра в схему формирования дискретных сигналов, дает добавление еще двух дополнительных боковых выбросов функции авто- и взаимной корреляции (рис. 3).

Следующим этапом работы программы является выбор файла, в который будут записываться ансамбли дискретных сигналов с одно- (m-последовательности), трех- (сигналы Голда) и пятиуровневой функцией авто- и взаимной корреляции (новые классы дискретных сигналов). Кроме того, в данный файл записываются значения боковых выбросов для функции автокорреляции, для каждой сформированной последовательности (рис. 4).

Общий вид окна программы для формирования дискретных сигналов с многоуровневой функцией корреляции показан на рис. 5.

На рис. 5 выделены и пронумерованы области, значение которых следующее:

1 – Поле для выбора степени образующего полинома в $GF(2^m)$.

2 – Вид образующего полинома $GF(2^m)$.

3 – Калькулятор в полученном $GF(2^m)$.

4 – Сформировать дискретные сигналы и рассчитать значения боковых выбросов ПФАК и ПФВК.

5 – Сформировать отчёт в выбранный текстовый файл (m-последовательность, сигналы Голда, дискретные сигналы с пятиуровневой функцией корреляции).

6 – Рассчитанные, для образующего полинома, значения элементов конечного поля $\alpha^{i_1} \in GF(2^m)$, $\alpha^{i_2} \in GF(2^m)$, ..., $\alpha^{i_u} \in GF(2^m)$ 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 $GF(2^m)$, $n = 2^m - 1$.

7 – Распределение элементов конечного поля в циклотомические классы для заданного m.

8 – Перечень рассчитанных $h_j(x)$.

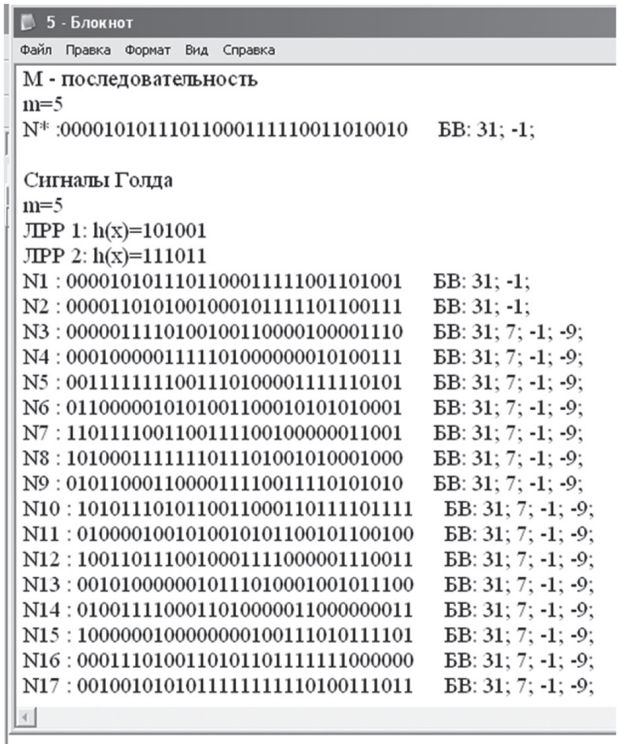

Рис. 4. Пример файла с ансамблями сформированных дискретных сигналов и значений боковых выбросов ПФАК и ПФВК

На рис. 6, 7 отображены, соответственно, вкладка просмотра сгенерированных m-последовательностей, образующих сигналы Голда и дискретные сигналы с многоуровневой функцией корреляции, вкладка просмотра значений функции автокорреляции для m-последовательностей.

Рассмотрим алгоритмическую реализацию формирования элементов конечного поля $GF(2^m)$. На основе выбранного образующего полинома степени m строится циклическое множество полиномов. На алгоритмическом уровне

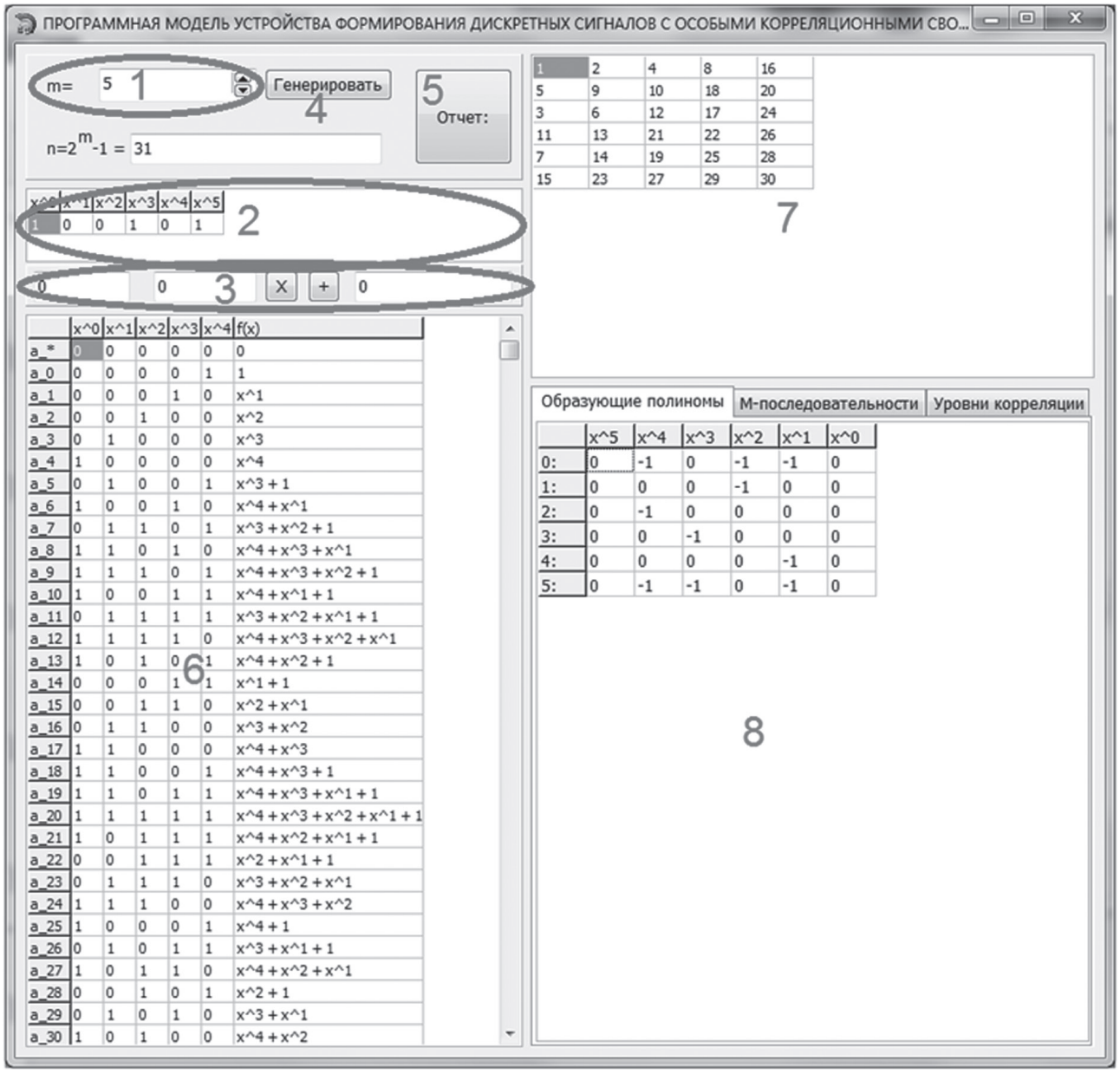

Рис. 5. Общий вид программы формирования дискретных сигналов с многоуровневой функцией корреляции

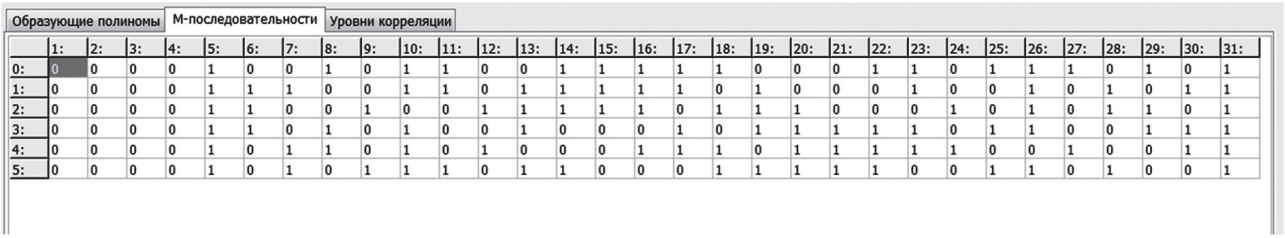

Рис. 6. Вкладка просмотра сгенерированных *m*-последовательностей, образующих сигналы Голда и дискретные сигналы с многоуровневой функцией корреляции

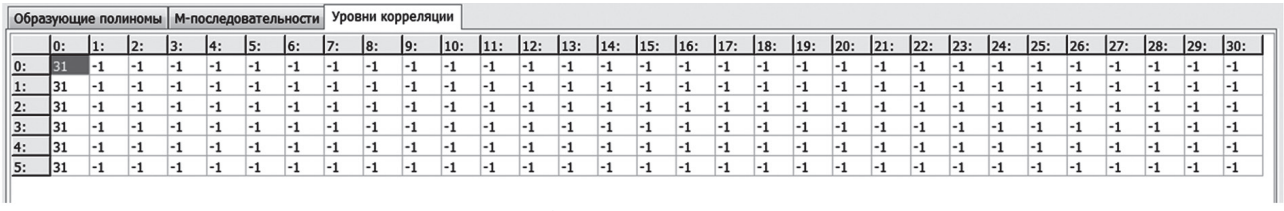

Рис. 7. Вкладка просмотра значений функции автокорреляции для *m*-последовательностей

необходимо, начиная с единичного полинома, перемножать текущий полином на x, после чего дополнить список остатком деления результата умножения на образующий полином. Полином записывается в виде бинарного числа. Описанные действия можно реализовать операцией сдвига влево, и при выталкивании единицы производить сложение по модулю два с образующим полиномом. Реализация процесса показана на следующей схеме (рис. 8).

5. ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ПРОГРАММНОЙ РЕАЛИЗАЦИИ ФОРМИРОВАНИЯ ДИСКРЕТНЫХ СИГНАЛОВ С МНОГОУРОВНЕВОЙ ФУНКЦИЕЙ КОРРЕЛЯЦИИ

Оценим сложность алгоритма при формировании m-последовательности (субортогональных сигналов) и реализации функции автокорреляции. Для определения значения автокорреляции необходимо перемножить попарно элементы последовательности со всеми циклическими сдвигами этой последовательности, при этом нулевые значения принимаются как -1. Количество элементов последовательности задаёт количество операций умножения и количество вычислений значений корреляции исходной функции со сдвинутой. Общее количество операций при вычислении автокорреляции одной последовательности будет пропорциональна квадрату длины этой m-последовательности: $O(n^2)$.

Оценим сложность алгоритма при формировании сигналов Голда и реализации функции автокорреляции этих сигналов. Количество сигналов Голда, которые заданы двумя порождающими m-последовательностями, будет равно n. Каждая последовательность Голда получена поэлементным сложением по модулю два, двух m-последовательностей со смещениями от 0 до $n-1$. Для оценки сложности формирования последовательностей Голда необходимо повторить алгоритм формирования функции автокорелляции m-последовательности n раз, что означает возрастание сложности алгоритма до $n \cdot O(n^2)$, или $O(n^3)$.

Оценим сложность алгоритма при формировании нового класса сигналов (с пятиуровневой функцией корреляции) и реализации функции автокорреляции этих сигналов. Формирование нового класса сигналов (с пятиуровневой функцией корреляции) реализуется комбинацией циклических сдвигов поэлементного сложения трёх m-последовательностей, общее количество которых составляет n^2. В этом случае сложность перебора всех вариантов расширенных сигналов будет $O(n^4)$.

Сложность полного перебора последовательностей расширенных сигналов $O((2^m-1)^4)$, где m – степень образующего полинома.

ВЫВОДЫ

Таким образом, в ходе проведенных исследований были разработаны практические предложения, относительно программной реализации формирования дискретных последовательностей с многоуровневой функцией корреляции.

Разработанные схемы реализуются вычислительно эффективными преобразователями,

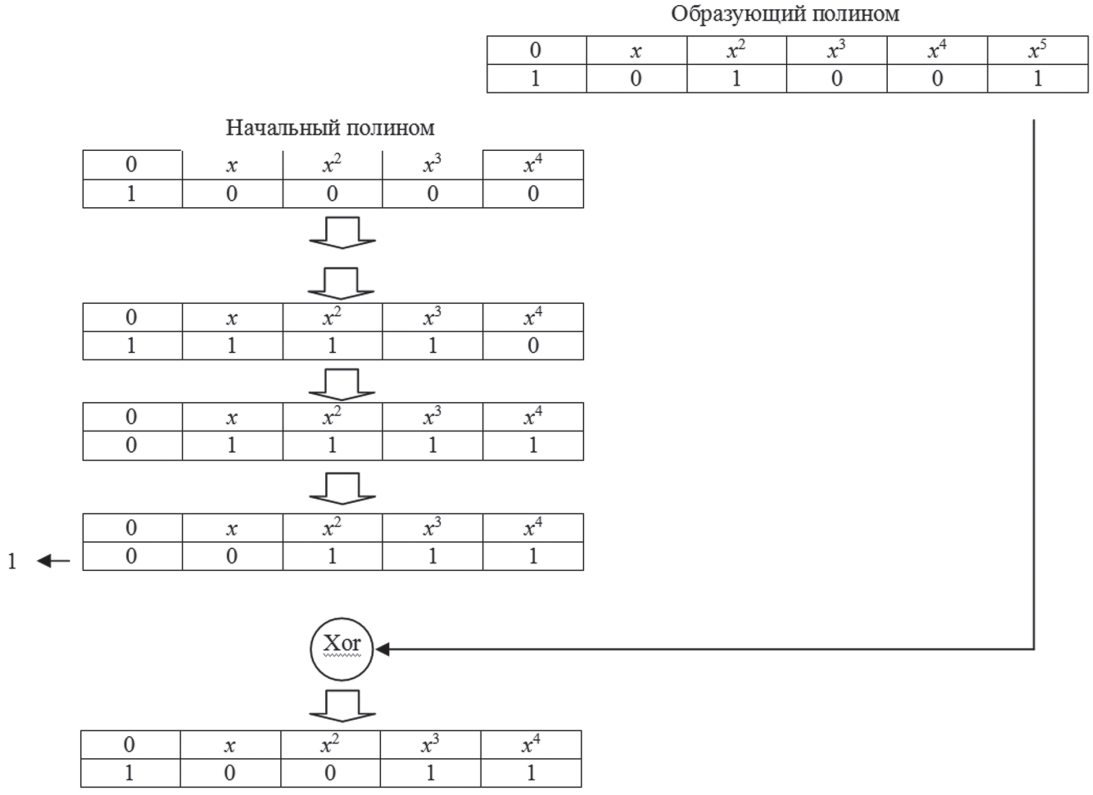

Рис. 8. Схема формирования элементов конечного поля $GF(2^m)$

например, на основе цепей с регистрами сдвига и сумматором (рис. 3). 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.

Разработанное программное обеспечение возможно усовершенствовать в направлении оптимизации скорости формирования дискретных сигналов с многоуровневой функцией корреляции.

Кроме того, разработанное программное обеспечение возможно использовать при проведении лабораторных работ по учебным дисциплинам, в которых рассматриваются вопросы кодового разделения каналов радиоуправления и связи, а также вопросы практической реализации алгоритмов стеганографии с использованием сложных дискретных сигналов.

Литература

[1] Кузнецов А.А., Смирнов А.А., Сай В.Н. Дискретные сигналы с многоуровневой функцией корреляции // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЭ. – 2011. – Вып. 166. – С. 142–152.

[2] 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.

[3] 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.

[4] 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.

[5] Гряник М.В., Фролов В.И. Технология CDMA – будущее сотовых систем в Украине. – Мир связи, 1998, № 3. – С. 40–43.

[6] Науменко Н. І., Стасев Ю. В., Кузнецов О.О., Євсєєв С.П. Теорія сигнально-кодових конструкцій. Х.:ХУ ПС, 2008р. – 489.

[7] Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

Поступила в редколлегию 8.04.2013

Смирнов Алексей Анатольевич, кандидат технических наук, доцент, профессор кафедры программного обеспечения Кировоградского национального технического университета. Научные интересы: защита информации, телекоммуникации, компьютерные сети и системы.

УДК 621.396.253

Програмна модель пристрою формування дискретних сигналів з особливими кореляційними властивостями / О.А. Смірнов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. — № 2. – С. 333–341.

Досліджується алгебраїчний підхід до формування великих ансамблів дискретних сигналів з багаторівневою функцією кореляції, що заснований на перетині циклічних орбіт групових кодів. Число й величина рівнів бічних пелюстків функції кореляції формованих послідовностей, а також потужність ансамблю сигналів визначаються дистанційними й структурними властивостями кілець багаточленів над кінцевими полями. Розробляються пропозиції з програмної реалізації пристроїв формування дискретних сигналів з багаторівневою функцією кореляції.

Ключові слова: програмна модель, дискретні сигнали, особливі кореляційні властивості, багаторівнева функція кореляції.

Іл.: 8. Бібліогр.: 7 найм.

UDC 621.396.253

Software model of a device of forming discrete signals with special correlation properties / A.A. Smirnov // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 333–341.

The paper researches an algebraic approach to forming large ensembles of discrete signals with multi-level correlation function, which is based on the section of circular orbits of group codes. The number and value of sidelobe levels of the correlation function of generated sequences as well as power of a signal ensemble are determined by remote and structural properties of polynomial rings over finite fields. Proposals for a software implementation of devices of forming discrete signals with multi-function correlation are being developed.

Keywords: programming model, discrete signals, special correlation properties, multi-level correlation function.

Fig.: 8. Ref.: 7 items.