СИНТЕЗ И АНАЛИЗ СИГНАЛОВ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

УДК 621.391.1

И. Д. ГОРБЕНКО, д-р техн. наук, А. А. ЗАМУЛА, канд. техн. наук, Р. И. КИЯНЧУК

МЕТОДЫ ПОСТРОЕНИЯ И ИССЛЕДОВАНИЯ СВОЙСТВ ПРОИЗВОДНЫХ НЕЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Системы нелинейных рекуррентных последовательностей (НРП) являются плотноупакованными по периодической функции корреляции (ПФАК), существуют для большого спектра длительностей L, однако размерность ансамбля НРП ограничена, например для НРП характеристического типа – функцией Эйлера. Проведенные исследования показали, что дальнейшее увеличение размерности ансамбля и улучшение структурных свойств может быть достигнуто на основе использования L-позиционных НРП, построение которых осуществляется посредством образования последовательного произведения $Z_i, i=\overline{1,k}$, символов W_i^j НРП с одно- или двухуровневой ПФАК.

Правило построения символов W_i^p производных нелинейных рекуррентных последовательностей (ПНРП) сформулируем в виде

$$W_i^p = \prod_{j=1}^{k} W_{i(\mathrm{mod}\,L_j),j}. \tag{1}$$

ПФАК, построенную по (1) ПНРП, найдем, используя соотношение $r_j(l) = \sum_{i=1}^{L-m} W_i^j \left(W_{i+l}^j\right)^*$:

$$R_w^p(l) = \sum_{i=0}^{L-1} \prod_{j=1}^{K_1} W_{i(\mathrm{mod}\,L_j),j} \prod_{j=1}^{K_2} W_{i+l(\mathrm{mod}\,L_j),j}, \tag{2}$$

где $K_1 \neq K_2$.

Анализ корреляционных свойств с использованием (2) в общем виде затруднен, поэтому рассмотрим ряд частных случаев, важных с теоретической и практической точек зрения.

1. Пусть $K_1 = K_2$, а $L_1 \neq L_2$, тогда (2) имеет вид

$$R_w(l) = \sum_{i=0}^{L-1} W_{i(\mathrm{mod}\,L_1),1} \cdot W_{i+l(\mathrm{mod}\,L_1),1} \cdot W_{i(\mathrm{mod}\,L_2),2} \cdot W_{i+l(\mathrm{mod}\,L_2),2}. \tag{3}$$

Для преобразования (3) представим индекс суммирования i в L_2-ричной системе исчисления

$$i = \upsilon L_2 + \varepsilon, \quad 0 \le \varepsilon \le L_2,\ 0 \le \upsilon \le L_1 \tag{4}$$

$$R_w(l) = \sum_{\upsilon=0}^{L_1-1} \sum_{\varepsilon=0}^{L_2-1} W_{\upsilon L_2-\varepsilon(\mathrm{mod}\,L_1),1} \cdot W_{\upsilon L_2-\varepsilon(\mathrm{mod}\,L_2),2} \cdot W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L_2),2} \cdot W_{\upsilon L_2+\varepsilon l(\mathrm{mod}\,L_2),2} = \sum_{\varepsilon=0}^{L_2-1} W_{\varepsilon(\mathrm{mod}\,L_1),1} \cdot \tag{5}$$

$$\times W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L1),1}.$$

С учетом того, что $r_j(l) = \sum_{i=1}^{L-m} W_i^j \left(W_{i-l}^j\right)^*$

$$\sum_{\varepsilon=0}^{L_2-1} W_{\varepsilon(\mathrm{mod}\,L_2),2} \cdot W_{\varepsilon+l(\mathrm{mod}\,L_2),2} = R_{W_2}(l) \tag{6}$$

Кроме того, если υ принимает значение из множества вычетов по $\bmod L_1$, то $\upsilon L_2 + \varepsilon$ пробегает значения по модулю L_1, поэтому

$$\sum_{\varepsilon=0}^{L_1-1} W_{\upsilon L_2+\varepsilon(\bmod L_1),1} \cdot W_{\upsilon L_2+\varepsilon+l(\bmod L_1),1} = \sum_{q=0}^{L_1-1} W_{q(\bmod L_1),1} \cdot W_{q+\varepsilon(\bmod L_1),1} = R_{W_1}(l) \qquad (7$$

и ПФАК ПНРП может быть вычислена с использованием выражения

$$R_{W''}(l) = R_{W_1}(l) \cdot R_{W_2}(l). \qquad (8$$

Но так как $R_{W_1}(l)$ и $R_{W_2}(l)$ могут принимать соответственно значения L_1 и L_2 при $l = 0$, $R_{W_1}(l)$ и $R_{W_2}(l)$ при $l = \overline{1, L-1}$, то

$$R_{W''}(l) = \begin{cases} L, & при\ l \equiv 0(\bmod L); \\ L_2 R_{W_1}(l), & при\ l \equiv 0(\bmod L_2),\ \mathrm{L} \neq 0\ (\bmod \mathrm{L}_1); \\ L_1 R_{W_2}(l), & при\ l \equiv 0(\bmod L_1),\ l \neq 0(\bmod L_2); \\ R_{W_1}(l) \cdot R_{W_2}(l), & при\ l \neq 0(\bmod L_1, \bmod L_2). \end{cases} \qquad (9$$

Анализ (9) показывает, что минимальные боковые лепестки ПНРП достигаются в случае, если L_2, $R_{w_1}(l)$, L_1, $R_{w_2}(l)$ принимают минимальные значения. Кроме того, как следует из [1], ПНРП имеет максимальный период, если L_1 и L_2 взаимно простые числа.

2. Пусть $K = 3$, а $L_1 \neq L_2 \neq L_3$. В этом случае по аналогии с (9) выражение (2) можно представить в виде

$$R_{W''}(l) = R_{W_1}(l) \cdot R_{W_2}(l) \cdot R_{W_3}(l). \qquad (10$$

Или

$$R_{W''}(l) = \begin{cases} L, & при\ l \equiv 0(\bmod L); \\ R_{W_1}(l) \cdot R_{W_2}(l) \cdot R_{W_3}(l), & при\ l \neq 0(\bmod L_1, L_2, L_3); \\ L_1 \cdot R_{W_2}(l) \cdot R_{W_3}(l), & при\ l \equiv 0(\bmod L_1),\ l \neq 0(\bmod L_2, L_3); \\ L_2 \cdot R_{W_1}(l) \cdot R_{W_3}(l), & при\ l \equiv 0(\bmod L_2),\ l \neq 0(\bmod L_1, L_3); \\ L_3 \cdot R_{W_1}(l) \cdot R_{W_2}(l), & при\ l \equiv 0(\bmod L_3),\ l \neq 0(\bmod L_1, L_2); \\ L_1 \cdot R_{W_2}(l) \cdot L_3, & при\ l \equiv 0(\bmod L_1, L_3),\ l \neq 0(\bmod L_2); \\ L_1 \cdot L_2 \cdot R_{W_3}(l), & при\ l \equiv 0(\bmod L_1, L_2),\ l \neq 0(\bmod L_3); \\ R_{W_1}(l) \cdot L_2 \cdot L_3, & при\ l \equiv 0(\bmod L_2, L_3),\ l \neq 0(\bmod L_1). \end{cases} \qquad (11$$

Рассмотрение (11) показывает, что для минимизации $R_{W''}(l)$ необходимо и достаточно, чтобы $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W3}(l)$ были минимальными, а L_1, L_2 и L_3 – минимальными и взаимопростыми. Минимальное значение R_{W_i}, $i = \overline{1,3}$, равное 0 и достигается только при использовании в качестве W_1 последовательности [2] вида {1 1 1 -1}. В этом случае выражение (11) принимает вид

$$R_{W''}(l) = \begin{cases} L, & при\ l \equiv 0(\bmod L); & а) \\ L_1 \cdot R_{W_2}(l) \cdot R_{W_3}(l), & при\ l \equiv 0(\bmod L_1),\ l \neq 0(\bmod L_2, L_3); & б) \\ L_1 \cdot R_{W_3}(l) \cdot L_2, & при\ l \equiv 0(\bmod L_1, L_2),\ l \neq 0(\bmod L_3); & в) \\ L_1 \cdot R_{W_2}(l) \cdot L_3, & при\ l \equiv 0(\bmod L_1, L_3),\ l \neq 0(\bmod L_2). & г) \end{cases} \qquad (12)$$

Исследование выражений (12, *а*, *б*, *г*) показывает, что для их минимизации необходимо, чтобы как принимаемые значения ПФАК $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W_3}(l)$, так и значения их длительностей были бы минимальными. С учетом того, что $L_1 = 4$, максимальные значения ПФАК $R_W(l)$ дают слагаемые *в*) и *г*). Если L_2 и L_3 – взаимно простые, то минимальные значения $R_{W_2}(l)$ и $R_{W_3}(l)$ могут быть соответственно равны {±1} и {–4,0} или {0,4}, или {2,–2}, поэтому

$$R_{W''}(l) = \begin{cases} L, & при\ l \equiv 0(\mathrm{mod}\, L); & а) \\ \pm 4, & при\ l \equiv 0(\mathrm{mod}\, L_1), l \neq 0(\mathrm{mod}\, L_2, L_3); & б) \\ \pm 4L_1L_2, & при\ l \equiv 0(\mathrm{mod}\, L_1, L_2), l \neq 0(\mathrm{mod}\, L_3); & в) \\ \pm L_1L_3, & при\ l \equiv 0(\mathrm{mod}\, L_1, L_3), l \neq 0(\mathrm{mod}\, L_2). & г) \end{cases} \quad (13)$$

Если L_1 и L_2 – взаимно простые, то выражение $\pm 4L_1L_2$ принимает значение либо $\pm 4L_1R_{W_2}(l)$, либо $\pm 4R_{W_1}(l)L_2$, поэтому максимальный боковой лепесток дает составляющая $\pm L_1L_3$.

Из рассмотренного следует, что для минимизации боковых лепестков необходимо, чтобы L_1, L_2 и L_3 были взаимно простыми. Этого можно достичь, если L_1 и L_2 – простые, а $L_3 \equiv 0(\mathrm{mod}\, 2)$. При этих условиях составляющие (11) принимают значения

$$R_{W''}(l) = \begin{cases} L, & при\ l \equiv 0(\mathrm{mod}\, L); \\ R_{W_1}(l) \cdot R_{W_2}(l) \cdot R_{W_3}(l), & при\ l \neq 0(\mathrm{mod}\, L_1, L_2, L_3); \\ L_1 \cdot R_{W_2}(l) \cdot R_{W_3}(l), & при\ l \equiv 0(\mathrm{mod}\, L_1), l \neq 0(\mathrm{mod}\, L_2, L_3); \\ L_2 \cdot R_{W_1}(l) \cdot R_{W_3}(l), & при\ l \equiv 0(\mathrm{mod}\, L_2), l \neq 0(\mathrm{mod}\, L_1, L_3); \\ L_3 \cdot R_{W_1}(l) \cdot R_{W_2}(l), & при\ l \equiv 0(\mathrm{mod}\, L_3), l \neq 0(\mathrm{mod}\, L_1, L_3). \end{cases} \quad (14)$$

3. Пусть $L_1 = L_2 = L_K = L$, а $K_1 = K_2 = K$. Для этих условий с учетом (2) выражение для ПФАК ПНРП можно представить в виде

$$R_{W_2}(l) = \sum_{i=0}^{L-1} \prod_{j=1}^{K} W_{i,j}^{q} \prod_{j=1}^{K} W_{i-l,j}, \quad (15)$$

причем (15) позволяет вычислить ПФАК, если положить, что $q = r$.

Проведенные исследования показали, что для (15) можно получить оценки, если воспользоваться теорией двухзначных характеров, в частности тем, что для любого нетривиального характера справедливо [3]

$$\sum_{y \in GF(P)} \Psi(ay + b) = \sum_{\substack{y \in GF(P^n) \\ y \neq 0(\mathrm{mod}\, P)}} \Psi(ay + b) + \Psi(b) = 0$$

и фиксированными правилами кодирования. Например, для наиболее мощного класса двухуровневых последовательностей – последовательностей характеристического типа с числом символов $L = 2x = P^n - 1$, $x = 1,2,3,\ldots,z,\ldots$

$$W^q = \left\{ W_i^q, \quad i = \overline{0, P^n - 1} \right\};$$

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \neq 0[\bmod f(x), P]; \\ 1, & \text{если } \Theta_q^i + 1 \equiv 0[\bmod f(x), P]; \end{cases} \quad а)$$

либо (16)

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \neq 0[\bmod f_m(x), P]; \\ -1, & \text{если } \Theta_q^i + 1 \equiv 0[\bmod f_m(x), P]; \end{cases} \quad б)$$

где Θ_q – q-й первообразный элемент поля $GF(P)$, а $f_m(x)$ – m-й первообразный примитивный полином степени n.

Приведем вывод аналитического выражения для ПФАК ПНРП.

Используя (15) и полагая, что $q \neq r$, имеем

$$R_{W_n}(l) = \sum_{i=0}^{L-1} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1). \quad (17)$$

С учетом того, что $\Psi(0) = 0$, [4], при $l \neq 0(\bmod L)$

$$R_{W_n}(l) = \sum_{i=0}^{P^n-2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1) \pm Z \quad (18)$$

где Z – учитывает сумму слагаемых, входящих в (17), для которых

$$(\Theta_q^i + 1) \equiv 0 \vee (\Theta_q^{i+l} + 1) \equiv (\Theta_r^i + 1) \equiv (\Theta_r^{i-l} + 1) \equiv 0[\bmod f_m(x), P] \quad (19)$$

Более точно структуру (19) определяют сформулированные ниже утверждения.

Утверждение 1. Пусть $\Theta_\upsilon^i + 1$ и $\Theta_\upsilon^{i+l} + 1$ есть элементы поля $GF(P^n)$ а Θ_υ^υ – υ-й первообразный элемент, тогда при $l' \neq 0(\bmod L)$ $\Theta_\upsilon^i + 1$ и $\Theta_\upsilon^{i+l} + 1$ никогда не сравнимы с $0[\bmod f_m(x), P]$. Доказательство утверждения следует из цикличности поля $GF(P^n)$ [4].

Утверждение 2. Пусть $\Theta_\upsilon^r + 1$ и $\Theta_k^m + 1$ – элементы поля $GF(P^n)$, а Θ_υ и Θ_k – первообразные. Существуют T^{s1} и T^{s2} автоморфные преобразования, при которых $\Theta_\upsilon^r + 1 \equiv \Theta_k^m + 1 \equiv 0(\bmod L)$.

Доказательство утверждения следует из авто- и изоморфных свойств поля $GF(P^n)$ [4].

С учетом утверждения (17) и (18) выражение (19) распадается на следующие логические высказывания:

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^{i+l} \neq 0(\bmod L); \quad а)$$

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \neq 0(\bmod L); \quad б)$$

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i-l} + 1 \equiv 0(\bmod L); \quad в)$$

$$\Theta_q^i + 1 \neq 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i+l} + 1 \neq 0(\bmod L); \quad г)$$

$$\Theta_q^i + 1 \neq 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \neq 0(\bmod L); \quad д)$$

$$\Theta_q^i + 1 \neq 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i+l} + 1 \equiv 0(\bmod L); \quad е)$$

$$\Theta_q^i + 1 \neq 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \neq 0(\bmod L); \quad ж)$$

$$\Theta_q^i + 1 \neq 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i+l} + 1 \equiv 0(\bmod L). \quad з)$$

(20)

Анализ (20) показывает, что исключающими являются высказывания *а*), *г*), *ж*), *з*), поэтому

$$Z = \Psi\left(-\Theta_q^{i-l}+1\right)\cdot\Psi\left(-\Theta_r^{i}+1\right)\cdot\Psi\left(-\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_q^{-l}+1\right)\cdot\Psi\left(\Theta_r^{i}+1\right),$$

$$\Psi = \left(\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_r^{l}+1\right)\cdot\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)+\Psi\left(-\Theta_r^{-l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_q^{i-l}+1\right). \qquad (21)$$

Если истинно высказываение (20, *а*), то $\Psi\left(\Theta_q^{i}+1\right)=0$, так как $\Theta_q^{i}+1\equiv 0(\mathrm{mod}\,L)$ [4], поэтому $\Psi\left(\Theta_q^{i+l}+1\right)=\Psi\left[\Theta_q^{l}\left(\Theta_q^{i}+\Theta_q^{-l}\right)\right]=\Psi\left[\Theta_q^{l}\left(\Theta_q^{-l}-1\right)\right]=\Psi\left(\Theta_q^{l}\cdot\Theta_q^{-l}-\Theta_q^{l}\right)=\Psi\left(1-\Theta_q^{l}\right)=\Psi\left(-\Theta_q^{l}+1\right)$.

В случае, если $\Theta^{i+l}+1\equiv 0(\mathrm{mod}L)$, то

$$\Psi\left(\Theta_q^{i}+1\right)=-\Psi\left(\Theta_q^{i}\cdot\Theta_q^{l}\cdot\Theta_1^{-l}+1\right)=\Psi\left[\Theta_q^{-l}\left(\Theta_q^{i+l}+\Theta_q^{-l}\right)\right]=\Psi\left[\Theta_q^{-l}\left(\Theta_q^{-l}-1\right)\right]=\Psi\left(-\Theta_q^{-l}+1\right).$$

Преобразуем выражение (18), используя свойство характера Ψ [Альберт], не рассматривая Z сумму, определяемую (П. 7.5), обозначив его переменной X:

$$X=\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^{i}+1\right)\cdot\Psi\left(\Theta_q^{i-l}+1\right)\cdot\Psi\left(\Theta_r^{i}+1\right)\cdot\Psi\left(\Theta_r^{i+l}+1\right)=$$

$$=\Psi\left(\Theta_q^{i}\right)\cdot\Psi\left(\Theta_r^{i}\right)\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^{i}+1\right)\cdot\Psi\left(\Theta_q^{i}+\Theta_q^{-l}\right)\cdot\Psi\left(\Theta_r^{i}+1\right)\cdot\Psi\left(\Theta_r^{i}+\Theta_r^{-l}\right)=\Psi\left(\Theta_q^{l}\right)\cdot\Psi\left(\Theta_r^{l}\right)\cdot Q \qquad (22)$$

Проанализируем выражение

$$Q=\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^{i}+1\right)\cdot\Psi\left(\Theta_q^{i}+\Theta_q^{-l}\right)\cdot\Psi\left(\Theta_r^{i}+1\right)\cdot\Psi\left(\Theta_r^{i}+\Theta_r^{-l}\right),$$

учитывая, что если i принимает значения индексов суммирования, то степени первообразных элементов Θ_q и Θ_r принимают значения всех ненулевых элементов поля $GF(P^n)$. Обозначая ненулевые элементы поля через a_i и b_i соответственно для первообразных Θ_q и Θ_r, при $i=\overline{0,P^n-2}$, перейдем к сумме произведения характеров ненулевых элементов

$$Q=\sum_{a_i,b_i\in GF(P^n)}\Psi\left(a_i+1\right)\cdot\Psi\left(a_i+\Theta_q^{-l}\right)\cdot\Psi\left(b_i+1\right)\cdot\Psi\left(b_i+\Theta_r^{-l}\right). \qquad (23)$$

Полагая в (23) $c_i=a_i+1$ и $d_i=b_i+1$, проанализируем все c_i и d_i, если a_i и b_i пробегают при изменении все ненулевые элементы поля $GF(P^n)$, то c_i и d_i также пробегают все ненулевые поля $GF(P^n)$, исключая 1, поэтому

$$Q=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 1(\mathrm{mod}\,P)}}\Psi\left(c_i\right)\cdot\Psi\left(c_i+\Theta_q^{-l}+1\right)\cdot\Psi\left(d_i\right)\cdot\Psi\left(d_i+\Theta_r^{-l}-1\right) \qquad (24)$$

Если же

$$\begin{aligned} &c_i=1, \quad то\ Q_1=\Psi\left(\Theta_1^{-l}\right)\Psi\left(d_i\right)\Psi\left(d_i+\Theta_r^{-l}-1\right); && а)\\ &d_i=1, \quad то\ Q_2=\Psi\left(c_i\right)\Psi\left(c_i+\Theta_q^{-l}-1\right)\Psi\left(\Theta_r^{-l}\right); && б)\\ &c_i=1, d_i=1, \quad то\ Q_3=\Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right); && в) \end{aligned} \qquad (25)$$

Исключим в (25) условие $c_i,d_i\neq 1(\mathrm{mod}\,P)$, для этого добавим в него и вычтем Q_1, Q_2 и Q_3. В результате получим

$$
\begin{aligned}
Q &= \sum \Psi(c_i)\Psi\left(c_i+\Theta_q^{-l}-1\right)\Psi(d_i)\Psi\left(d_i+\Theta_r^{-l}\right)-\Psi\left(\Theta_q^{-l}\right)\Psi(d_i)\Psi\left(d_i+\Theta_r^{-l}-1\right)- \\
&-\Psi(c_i)\Psi\left(c_i+\Theta_q^{-l}-1\right)\Psi\left(\Theta_r^{-l}\right)-\Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right)= \\
&= \sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}} \Psi\left(c_i^{\,2}\right)\Psi\left(1+\left(\Theta_q^{-l}-1\right)c_i^{-1}\right)\Psi\left(d_i^{\,2}\right)\Psi\left[1+\left(\Theta_r^{-l}-1\right)d_i^{-1}\right]-Q_1-Q_2-Q_3.
\end{aligned}
\tag{26}
$$

Даже принимая во внимание, что $\Theta_q^{-l}-1$ и $\Theta_r^{-l}-1\in GF(P^n)$ являются постоянными, обозначив их как $q_1=\Theta_q^{-p}-1$ и $q_2=\Theta_r^{-l}-1$, $q_1,q_2\neq 0(\mathrm{mod}\,P)$, а также обозначив $x_i=c_i^{-1}$ и $y_i=d_i^{-1}$, которые пробегают так же все элементы поля $GF(P^n)$, получим

$$
Q=\sum_{\substack{x_i,y_i\in GF(P^n)\\ x_i,y_i\neq 0(\mathrm{mod}\,P)}}\Psi(1+q_ix_i)\Psi(1+q_2y_2)-Q_1-Q_2-Q_3.
$$

С учетом (21), (23), (25), выражение (18) есть:

$$
\begin{aligned}
R_{W^n}(l) &= \Psi\left(\Theta_q^{l}\right)\Psi\left(\Theta_r^{l}\right)\{\sum_{\substack{x_i,y_i\in GF(P^n)\\ x_i,y_i\neq 0(\mathrm{mod}\,P)}}\Psi(1+q_ix_i)\Psi(1+q_2y_1)-[\Psi\left(\Theta_q^{-l}\right)\cdot\Psi(d_i)\Psi\left(d_i-\Theta_r^{-l}-1\right)+ \\
&+\Psi(c_i)\Psi\left(c_i+\Theta_q^{-l}-1\right)\Psi\left(\Theta_r^{-l}\right)+\Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right)]\}+\{\Psi\left(-\Theta_q^{l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_r^{i+l}+1\right)+ \\
&+\Psi\left(-\Theta_q^{-l}+1\right)\Psi\left(\Theta_r^{i}+1\right)\Psi\left(\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_r^{l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)+ \\
&+\Psi\left(-\Theta_r^{-l}+1\right)\Psi\left(\Theta_r^{-l}+1\right)\Psi\left(\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_r^{l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)+ \\
&+\Psi\left(-\Theta_r^{-l}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)\},
\end{aligned}
\tag{27}
$$

где запись $\{y\}$ означает, что слагаемые в скобках необходимо брать со знаками $+(-)$ во всевозможных сочетаниях, то есть 2^k – сочетаний, если k-число слагаемых.

Упростим (27) учитывая, что все слагаемые

$$
\begin{aligned}
&\Psi\left(\Theta_q^{l}\right),\Psi\left(\Theta_r^{l}\right)\Psi\left(\Theta_q^{-l}\right),\Psi(d_i),\Psi\left(d_i-\Theta_r^{-l}-1\right),\ldots, \\
&\Psi\left(-\Theta_r^{-l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)\in\{1;-1\}.
\end{aligned}
\tag{28}
$$

Из (28) непосредственно следует, что

$$
\begin{aligned}
Z=\pm\{&\Psi\left(-\Theta_q^{l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_q^{-l}+1\right)\Psi\left(\Theta_r^{i}+1\right)\Psi\left(\Theta_r^{i+l}+1\right)+ \\
&+\Psi\left(-\Theta_r^{l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)+\Psi\left(-\Theta_r^{-l}+1\right)\Psi\left(\Theta_q^{i}+1\right)\Psi\left(\Theta_q^{i+l}+1\right)\}
\end{aligned}
$$

принимает значение на множестве чисел $Z'=\{-4,-3,-2,-1,0,1,2,3,4\}$. Поэтому, используя (28), выражение (27) можно представить

$$
R_{W^n}(l)=\{\pm\sum_{\substack{x_i,y_i\in GF(P^n)\\ x_i,y_i\neq 0(\mathrm{mod}\,P)}}\Psi(1+q_1x_i)\Psi(1+q_2y_i)\pm[3]\}\pm[4],
\tag{29}
$$

где запись [3] и [4] означает, что вместо [3] при анализе необходимо подставлять числа $(-3,-2,-1,0,1,2,3)$, а вместо [4] – числа $(-4,-3,-2,-1,0,1,2,3,4)$.

Рассмотрим вывод аналитического выражения для ПФВК ПНРП. Используя выражение для расчета функции взаимной корреляции

$$R^{\upsilon}_{j,m}(l)=\sum_{i=1}^{L-k}W^{\upsilon}_{i}\left(W^{j}_{i+l}\right)^{*}+\sum_{i=L-k+1}^{L}W^{\upsilon}_{i}\left(W^{m}_{i-L+k}\right)^{*},$$

получим $(j=m)$

$$R^{B}_{W^{n}}(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta^{i}_{r_1}+1\right)\Psi\left(\Theta^{i}_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right). \tag{30}$$

Приведем вывод выражения для оценки выбросов ПФВК

$$R^{B}_{W^{n}}(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta^{i}_{r_1}+1\right)\Psi\left(\Theta^{i}_{r_2}+1\right)\Psi\left(\Theta^{i-l}_{r_3}+1\right)\Psi\left(\Theta^{i-l}_{r_4}+1\right) \tag{30}$$

Далее, аналогично выражению (19)

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta^{i}_{r_1}+1)\cdot\Psi(\Theta^{i}_{r_2}+1)\cdot\Psi(\Theta^{i+l}_{r_3}-1)\cdot\Psi\left(\Theta^{i-l}_{r_4}-1\right)\pm Z, \tag{31}$$

где Z представляет собой сумму слагаемых, входящих в (30), для которых $\Theta^{i}_{r_1}+1\equiv 0\vee\left(\Theta^{i}_{r_2}+1\right)\equiv 0\vee\left(\Theta^{i-l}_{r_3}+1\right)\equiv 0\vee\left(\Theta^{i+l}_{r_4}+1\right)\equiv 0$, что эквивалентно:

$$\Theta^{i}_{r_1}+1\equiv 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad а)$$

$$\Theta^{i}_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\equiv 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i-l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad б)$$

$$\Theta^{i}_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\equiv 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad в)$$

$$\Theta^{i}_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\equiv 0(\mathrm{mod}\,L); \quad г)$$

поэтому:

$$\begin{aligned}Z=\pm\{&\Psi\left(\Theta^{i}_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}+1\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right)+\Psi\left(\Theta^{i}_{r_1}+1\right)\Psi\left(\Theta^{i-l}_{r_3}+1\right)\Psi\left(\Theta^{i-l}_{r4}+1\right)+\\&+\Psi\left(\Theta^{i}_{r_1}+1\right)\Psi\left(\Theta^{i}_{r_2}+1\right)\Psi\left(\Theta_{r_3 i+l}+1\right)+\Psi\left(\Theta^{i}_{r_1}+1\right)\Psi\left(\Theta^{i}_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right)\},\end{aligned} \tag{32}$$

может принимать значения на множестве $Z'=\{-4,-3,-2,-1,0,1,2,3,4\}$, следовательно (29) есть

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta^{i}_{r_1}+1)\cdot\Psi(\Theta^{i}_{r_2}+1)\cdot\Psi(\Theta^{i-l}_{r_3}+1)\cdot\Psi\left(\Theta^{i+l}_{r_4}+1\right)\pm[4]=x\pm[4]. \tag{33}$$

Преобразуем выражение для x следующим образом:

$$\begin{aligned}x&=\Psi\left(\Theta^{l}_{r_3}\right)\Psi\left(\Theta^{l}_{r_4}\right)\sum_{i=0}^{P^n-1}\Psi(\Theta^{i}_{r_1}+1)\Psi(\Theta^{i}_{r_2}+1)\Psi(\Theta^{i}_{r_3}+\Theta^{-l}_{r_3})\Psi(\Theta^{i}_{r_4}+\Theta^{-l}_{r_4})=\\&=\Psi(\Theta^{l}_{r_3})\Psi(\Theta^{l}_{r_4})\cdot Q.\end{aligned} \tag{34}$$

Далее, выражение для Q (обозначив $\Theta^{i}_{r_1}+1=a_i$ и $\Theta^{i}_{r_2}+1=b_i$), представим в виде:

$$Q=\sum_{\substack{a_i,b_i\in GF(P^n)\\ a_i\cdot b_i\neq 1(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi\left(\Theta^{i}_{r_3}+\Theta^{-l}_{r_3}\right)\Psi\left(\Theta^{i}_{r_4}+\Theta^{-l}_{r_4}\right)$$

С учетом (24) – (26), а также того, что $\Theta^{-l}_{r_3}$ и $\Theta^{-l}_{r_3}$ могут принимать все значения из $GF(P^n)$, обозначив $c_i=\Theta^{i}_{r}+\Theta^{-l}_{r}$ и $d_i=\Theta^{i}_{r_4}+\Theta^{-l}_{r_4}$, причем, так как, во-первых,

$\Theta^{i}_{r_3} \neq 0(\mathrm{mod}\,P)$ и $\Theta^{-l}_{r_3} \neq 1(\mathrm{mod}\,P)$, $\Theta^{i}_{r_3} + \Theta^{-l}_{r_3} \neq 1(\mathrm{mod}\,P)$, а во-вторых, при $\Theta^{i}_{r_4} \neq 0(\mathrm{mod}\,P)$ и $\Theta^{-l}_{r_4} \neq 1(\mathrm{mod}\,P)$, $\Theta^{i}_{r_4} + \Theta^{-l}_{r_4} \neq 1(\mathrm{mod}\,P)$, (34), можно представить в виде:

$$R^{B}_{W''}(l) = \sum_{\substack{a_i,b_i,c_i,d_i \in GF(P^n) \\ a_i,b_i,c_i,d_i \neq 0(\mathrm{mod}\,P)}} \Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i) =$$

$$= \sum_{\substack{a_i,b_i,c_i,d_i \in GF(P^n) \\ a_i,b_i,c_i,d_i \neq 0(\mathrm{mod}\,P)}} \Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i) \pm [4] \pm [15] = \sum_{\substack{a_i,b_i,c_i,d_i \in GF(P^n) \\ a_i,b_i,c_i,d_i \neq 0(\mathrm{mod}\,P)}} \Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i) \pm [19]. \quad (35)$$

Анализ (35) показывает, что элементы полей c_i, d_i представляют собой автоморфизмы полей $\Theta^{i}_{r_3}$ и $\Theta^{i}_{r_4}$ при $i = \overline{0, P^{n-2}}$. Сумма в нем берется по всевозможным произведениям характеров над $a_i, b_i, c_i, d_i \in GF(P^n)$ и дает оценку для максимально достигаемого выброса $R^{B}_{W''}(l)_{\max}$. С учетом того, что элементы a_i, b_i, c_i и d_i строятся по различным первообразным и пары условий

$$\Psi(a_i) = \Psi(1) \wedge \Psi(b_i) = \Psi(1);$$
$$\Psi(c_i) = \Psi(1) \wedge \Psi(d_i) = \Psi(1)$$

не истинны, (35) имеет вид

$$R_{W''}(l) = \sum_{\substack{a_i,b_i,c_i,d_i \in GF(P^n) \\ a_i,b_i,c_i,d_i \neq 0(\mathrm{mod}\,P)}} \Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i) \pm [8] \pm [4] =$$

$$= \sum_{\substack{a_i,b_i,c_i,d_i \in GF(P^n) \\ a_i,b_i,c_i,d_i \neq 0(\mathrm{mod}\,P)}} \Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i) \pm [4] \pm [12]. \quad (36)$$

Важной задачей является несбалансированность ПНРП по число символов (+1) и (–1).

Если $\Theta_1, \Theta_2, \ldots, \Theta_k$ – первообразные элементы поля $GF(P^n)$, то несбалансированность в числе символов есть

$$R_{W''}(0) = \sum_{i=0}^{L-1} \prod_{j=1}^{k} \Psi\left(\Theta^{i}_{j} + 1\right).$$

При $k = 2$ аналогично (32)

$$R_{W''}(0) = \sum_{i=0}^{P^n-2} \Psi\left(\Theta^{i}_{r_1} + 1\right)\Psi\left(\Theta^{i}_{r_2} + 1\right) = \sum_{i=0}^{P^n-2} \Psi\left(\Theta^{i}_{r_1} + 1\right)\Psi\left(\Theta^{i}_{r_2} + 1\right) \pm Z,$$

где Z представляет собой сумму слагаемых, для которых

$$\Theta^{i}_{r_1} + 1 = 0 \vee \Theta^{i}_{r_2} + 1 \equiv 0(\mathrm{mod}\,P), \quad (37)$$

то есть

$$Z = \pm\Psi\left(\Theta^{i}_{r_1} + 1\right) + \Psi\left(\Theta^{i}_{r_2} + 1\right) \rightarrow \pm 2 \quad (38)$$

Далее обозначив $a_i = \Theta^{i}_{r_1}$ и $b_i = \Theta^{i}_{r_2}$, а затем $c_i = a_i + 1$ и $d_i = b_i + 1$ аналогично (21) – (25) имеем

$$x = \sum_{\substack{a_i, b_i \in GF(P^n) \\ a_i, b_i \neq 0(\mathrm{mod}\, P)}} \Psi(a_i + 1)\Psi(b_i + 1) = \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 1(\mathrm{mod}\, P)}} \Psi(c_i)\Psi(d_i) =$$

$$\sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0(\mathrm{mod}\, P)}} \Psi(c_i)\Psi(d_i) - \Psi(c_i) - \Psi(d_i) = \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0(\mathrm{mod}\, P)}} \Psi(c_i)\Psi(d_i) \pm [2] \tag{39}$$

С учетом (39)

$$R^B_{W^n}(0) = \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0(\mathrm{mod}\, P)}} \Psi(c_i)\Psi(d_i) \pm [4]. \tag{40}$$

Заметим, что для случая $k = 4$, $R_{W^n}(0)$ можно оценить, используя соотношения (36):

$$R^B_{W^n}(0) = \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0(\mathrm{mod}\, P)}} \Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i) \pm [12]. \tag{41}$$

Анализ (41) показывает, что несбалансированность, а следовательно, и шумы неортогональности с увеличением k увеличиваются и уже при $k = 4$ достигают значительной величины, даже без учета результатов сумм в (40) и (41).

Особенности вычисления выражений (29), (36), (41) и оценки их значений рассмотрим на примере выражения (41).

Воспользовавшись свойством функции характеров, имеем

$$R^B_{W^n}(0) = \sum_{\substack{a_i, b_i, c_i, d_i \in GF(P^n) \\ a_i, b_i, c_i, d_i \neq 0(\mathrm{mod}\, P)}} \Psi(a_i, b_i, c_i, d_i) \pm 12. \tag{42}$$

Для случая двухзначного характера, используя (15) имеем

$$R^B_{W^n}(0) = \sum_{u^* \in GF(P^n)} \exp\left(-\mathrm{j}\pi u_i^*\right) \pm 12. \tag{43}$$

Непосредственный анализ (43) показывает, что оценка максимальных боковых лепестков ПФАК, ПФВК и несбалансированности (тоже максимальной) в числе символов (1) и (−1) может быть сведена к изучению насбалансированности по четности и нечетности индексов производного поля, элементами которого являются числа (полиномы) вида

$$x_i = a_i \cdot b_i \cdot c_i \cdot d_i [\mathrm{mod}\, f(x), P].$$

Сопоставительное рассмотрение (43) показывает, что для анализа НРП (ПНРП) по критерию минимума максимальных выбросов $R^B_W(l)\left(R^B_{W^n}(l)\right)$ с точки зрения вычислительной сложности, предпочтительнее использовать алгоритм (42), а при вычислении основных статистических харктеристик алгоритм (43).

Список литературы: 1 *Виноградов И.М.* Основы теории чисел. – М. : Наука, 1965. 2. Свердлик М.Б.Оптимальные дискретные сигналы. – М. : Сов. радио, 1975. – 200 с. 3. Холл М. Комбинаторика. – М. : Мир. 1970. – 421 с. 4. Альберт А. А. Константные поля // Киберн. сб. ВМП. 3. – М. : Мир, 1966. – 242 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 25.08.2011