УДК 681.3.06

УСЛОВИЯ СУЩЕСТВОВАНИЯ НЕЛИНЕЙНЫХ ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ЗАДАННЫМИ СВОЙСТВАМИ

к.т.н. Б.И. Низиенко, А.О. Ивасюк, Я.Ю. Стасева
(представил д.ф.-м.н., проф. С.В. Смеляков)

Сформулированы условия существования нелинейных дискретных последовательностей с заданными свойствами. Определена зависимость между корреляционными и структурными свойствами нелинейных дискретных последовательностей.

Постановка проблемы. Опыт разработки и эксплуатации различных систем, в которых используются нелинейные управляющие последовательности, показывает, что нередки ситуации, когда излишнее усложнение схемы получения нелинейных последовательностей приводит к снижению стойкости системы. Поэтому введение нелинейных функций в схемы генерации управляющих последовательностей сопровождается тщательным анализом их свойств. Процедура анализа достаточно трудоемкая. Одним из путей ее упрощения является разработка условий существования нелинейных последовательностей с заданными свойствами.

Анализ литературы. Вопросу синтеза дискретных последовательностей посвящено большое количество работ, например [1 – 3]. В то же самое время до настоящего момента в этих работах рассматривались либо корреляционные, либо ансамблевые свойства. К настоящему времени остается нерешенной задача существования нелинейных дискретных последовательностей с заданными корреляционными и структурными свойствами.

Целью статьи является разработка условий существования нелинейных дискретных последовательностей с заданными корреляционными и структурными свойствами.

Основной материал. Пусть уровень боковых лепестков периодической функции автокорреляции управляющей последовательности {W} с числом элементов L ограничен значениями $R_{min}(l) \div R_{max}(l)$, где 1 – номер циклического сдвига функции корреляции. Тогда система неравенств, определяющая границы вектора автокорреляции во временной области {W} сигнала, имеет вид

$$\begin{cases} R(0)=\omega_1\omega_1+\omega_2\omega_2+\ldots+\omega_L\omega_L; \\ R_{min}(1)\le\omega_1\omega_2+\omega_2\omega_3+\ldots+\omega_L\omega_1\le R_{max}(1); \\ R_{min}(2)\le\omega_1\omega_3+\omega_2\omega_3+\ldots+\omega_L\omega_2\le R_{max}(2); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ R_{min}(L-1)\le\omega_1\omega_L+\omega_2\omega_1+\ldots+\omega_L\omega_{L-1}\le R_{max}(L-1), \end{cases} \quad (1)$$

где ω_i – элемент дискретного сигнала $\{W\}$, $\omega_i = \{\pm 1\}$.

Требуется определить ω_i, удовлетворяющие условию (1) с учетом взаимокорреляционных и ансамблевых характеристик управляющей последовательности, т.е. определить множество управляющих последовательностей $\{W^j\}$, где $j = \overline{1,M}$; M – размерность ансамбля управляющих последовательностей с заданными авто- и взаимокорреляционными свойствами.

Запишем условие того, что управляющие последовательности W^k и W^j имеют периодическую функцию взаимной корреляции, ограниченную значениями $R^{kj}_{min}(1) \div R^{kj}_{max}(1)$ в виде системы нелинейных неравенств

$$\begin{cases} R^{kj}_{min}(0)\le\omega_1^k\omega_1^j+\omega_2^k\omega_2^j+\ldots+\omega_L^k\omega_L^j\le R_{max}(0); \\ R^{kj}_{min}(1)\le\omega_1^k\omega_2^j+\omega_2^k\omega_3^j+\ldots+\omega_L^k\omega_1^j\le R_{max}(1); \\ R^{kj}_{min}(2)\le\omega_1^k\omega_3^j+\omega_2^k\omega_4^j+\ldots+\omega_L^k\omega_2^j\le R_{max}(2); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ R^{kj}_{min}(L-1)\le\omega_1^k\omega_L^j+\omega_2^k\omega_1^j+\ldots+\omega_L^k\omega_{L-1}^j\le R_{max}(L-1). \end{cases} \quad (2)$$

Система (1) при условии (2) в зависимости от L и R(l) может иметь либо M решений, либо вообще не имеет решений.

Рассмотрим ограничения, накладываемые на L и R(l), т.е. определим необходимые условия существования двоичных дискретных управляющих последовательностей с заданными свойствами. С этой целью выразим R(l) через λ_1 как число произведений вида (+1) • (+1) для заданного 1. Тогда число произведений вида (+1) • (–1) равно $(b - \lambda_1)$, где b – число единиц в управляющей последовательности. Число произведений (–1) • (+1) равно $[L - (b - \lambda_1)]$, а число произведений (–1) • (–1) равно $[L - 2(b - \lambda_1) - \lambda_1]$. Учитывая, что произведения вида (+1) • (+1) = (–1) • (–1), получим

$$\begin{cases} R_1 = L - 4(b - \lambda_1); \\ R_2 = L - 4(b - \lambda_2); \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ R_n = L - 4(b - \lambda_n); \\ \lambda_1 n_1 + \lambda_2 n_2 + \ldots + \lambda_n n_n = b(b-1); \\ n_1 + n_2 + \ldots + n_n = L - 1, \end{cases} \tag{3}$$

где R_i – i-й уровень бокового лепестка периодической функции автокорреляции R_{min} (1) < R_i < R_{max} (1), причем R_i значение имеет место n_i раз.

Анализ выражения (3) показывает, что λ_i также будет принимать n_i различных значений.

Определим величину b, положив

$$\begin{cases} \lambda_n = \lambda_{n-1} + Z_{n-1}; \\ \lambda_{n-1} = \lambda_{n-2} + Z_{n-2}; \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \lambda_2 = \lambda_1 + Z_1, \end{cases} \tag{4}$$

где Z_i – любое целое число.

Выразим из (3) λ_1 и n_i следующим образом:

$$\lambda_1 = \frac{R_1 - L + 4b}{4}; \tag{5}$$

$$n_1 = L - n_2 - n_3 - \ldots - n_n - 1; \tag{6}$$

$$\begin{aligned} n_2 &= n_1 + y_1; \\ n_3 &= n_2 + y_2; \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \\ n_n &= n_{n-1} + y_{n-1}, \end{aligned} \tag{7}$$

где y_i – любое целое число.

Решая систему (3) относительно b получим

$$\frac{R_i - L + 4b}{4}\left[L - (n-2)n_2 - (y_2 + \ldots + y_{n-1}) - 1\right] + \left(\frac{R_1 - L + 4b}{4} + Z_1\right) n_2 +$$

$$+ \left(\frac{R_i - L + 4b}{4} + Z_1 + Z_2\right)(n_2 - y_2) + \ldots + \left(\frac{R_i - L + 4b}{4} + Z_1 + Z_2 + \ldots Z_{n-1}\right) \times \tag{8}$$

$$\times\left[(n-1)n_n + (y_2 + y_3 + \ldots + y_{n-1})\right] - b^2 + b = 0.$$

После преобразований получим

$$L+\{L-(R_i+1)-R_i+4Z_1n_1+4(n_2+y_2)(Z_1+Z_2)+\ldots+$$
$$+4[(n-1)n_2+(y_2+y_3+\ldots+y_{n-1})](Z_1+Z_2+\ldots+Z_{n-1})\}^{1/2}=2b. \quad (9)$$

По условию b – натуральное число, следовательно, выражение в фигурных скобках также натуральное число Q, удовлетворяющее условию $Q \equiv a(\mathrm{mod}\ 2)$.

Тогда, полагая, что $L = 4x + a$, а n_i – принимает целые положительные значения, определим область допустимых значений Q. Имеем

$$4(4x+a)[(n-1)Z_1+\ldots+Z_{n-1}]-4[(n-1)Z_1+$$
$$+\ldots+Z_{n-1}]+4R_ix-R_ia-4x-a<Q. \quad (10)$$

Если теперь определить значения Z_i, то выражение (10) определяет необходимые условия существования управляющих последовательностей с заданными свойствами.

Вывод. Таким образом, необходимые условия достаточно эффектно сужают множество последовательностей, которые могут иметь функцию корреляции с n уровнями и заданным значением R_i.

ЛИТЕРАТУРА

1. *Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.*
2. *Долгов В.И., Горбенко И.Д., Сныткин И.И. Теория дискретных сигналов. Ч. 1. Оптимальные дискретные сигналы с одно- и двухуровневой ПФАК. МО СССР, 1983. – 168 с.*
3. *Горбенко И.Д., Стасев Ю.В., Замула А.А. Теория дискретных сигналов. Ч. 1. Ортогональные дискретные сигналы МО СССР, 1988. – 118 с.*

Поступила 20.02.2004

***НИЗИЕНКО Борис Иванович**, кандидат технических наук, доцент, начальник кафедры ХВУ. В 1980 году окончил ХАИ. Область научных интересов – методы построения автоматизированных систем управления.*

***ИВАСЮК Александр Олегович**, адъюнкт ПВИС. В 2001 году окончил ХВУ. Область научных интересов – методы помехозащиты информационных систем.*

***СТАСЕВА Яна Юрьевна**, научный сотрудник НИЛ ХВУ. В 2002 году окончила ХНУРЭ. Область научных интересов – методы защиты информации в автоматизированных системах управления.*