Tạp chí Tin học và Điều khiển học, T.22, S.1 (2006), 75–83

HÀM TƯƠNG QUAN PHI CHU KỲ VÀ ĐỘ PHỨC TẠP CỦA CÁC DÃY PHI TUYẾN DÙNG TRONG CDMA THẾ HỆ MỚI

NGUYỄN VĂN LÂM, LÊ CHÍ QUỲNH, NGUYỄN VŨ SƠN

Công ty Viteco, 61 Lạc Trung, Hà Nội

Abstract. In this contribution, the method for design and analysis of nonlinear sequences used in the 3.G CDMA, based on the d-Transform is presented. Furthermore, the aperiodical correlation functions and complexity these sequences are investigated. Some simulation example are also given to verify the algorithms used in this paper.

Tóm tắt. Bài viết trình bày phương pháp thiết kế và phân tích của các dãy phi tuyến dựa trên biến đổi d được dùng trong CDMA thế hệ mới. Hơn nữa, các hàm tương quan phi chu kỳ và độ phức tạp của các dãy này đã được nghiên cứu. Một số ví dụ mô phỏng cũng cho xác minh các thuật toán được dùng trong bài báo này.

1. MỞ ĐẦU

Các dãy giả nhiễu PN (pseudo noise sequences) được sử dụng rộng rãi trong công nghệ CDMA (như dãy Gold, Kasami...) vì chúng đáp ứng những yêu cầu về tính tương quan ACF và CCF.

Tuy nhiên, trong các ứng dụng độ bảo mật của chúng không đáp ứng được yêu cầu về độ phức tạp (ELS) lớn. Hơn nữa các hàm tương quan phi chu kỳ cần được nghiên cứu tiếp.

Để đáp ứng yêu cầu ngày càng cao của thông tin di động thế hệ mới, các dãy phi tuyến đang được quan tâm nghiên cứu [1].

Các dãy trên cần đáp ứng được những tiêu chí sau:

- Sử dụng được trong các hệ thống thông tin di động băng rộng dị bộ Asynchronous CDMA.

- Sử dụng trong các hệ thống QS-CDMA (QuasiSynchronous CDMA): chuẩn đồng bộ nhất là các hệ thống nội vùng, in door [2].

- Có hàm tương quan phi chu kỳ (trong trường hợp không đồng bộ lý tưởng), tốt và có độ phức tạp lớn.

Dãy phi tuyến có ACF lý tưởng được biết đến là dãy GMW, có cấu trúc chèn ghép được công bố 1985. Cùng thời gian đó tác giả Lê Chí Quỳnh và S. Prasad, qua biến đổi d đã đề xuất một lớp dãy có cấu trúc tương đương như dãy GMW [3, 4]. Sau đó các nhà khoa học như P. Z. Fan và G. Gong đã chứng minh rằng đại bộ phận các dãy tuyến tính và phi tuyến hữu ích (phân tích được) đều có cấu trúc chèn ghép được mô tả qua thứ tự chèn ghép (theo hàm vết hoặc biến đổi d) [1,5,6]. Lưu ý rằng biến đổi d có những ưu điểm: áp dụng cho mọi dãy bất kỳ và dễ dàng thực hiện phần cứng. Sau đây sẽ phân tích cấu trúc I_p của các dãy trên.

2. PHÂN TÍCH CẤU TRÚC I_P

2.1. Biểu diễn bằng hàm vết

Với m, n là hai số nguyên dương, α là phần tử nguyên tố của trường hữu hạn $GF(2^n)$ và $S = (2^n - 1)/(2^m - 1)$.

Gọi $Tr_p^q(x) = \sum_{k=0}^{q/(p-1)} x^{2^{pk}}$ hàm vết của x là ánh xạ của $GF(2^q)$ xuống $GF(2^p)$ [7].

Thứ tự lồng ghép I_p qua hàm vết Tr là: $Ip = I_p^0, I_p^1, ..., I_p^{S-1}$, với:

$$I_p^j = \begin{cases} i & \text{khi } Tr_m^n(\alpha^j = \alpha^{Si}) \text{ với } i = 0, 1, ..., 2^m - 2 \\ \infty & \text{khi } Tr_m^n(\alpha^j) = 0 \text{ với } j = 0, 1, ..., S - 1 \end{cases} \quad (1)$$

Ví dụ, xét hàm vết của trường $GF(2^8)$ xuống trường con $GF(2^4)$ với đa thức nguyên thuỷ 101110001: $g(x) = x^8 + x^4 + x^3 + x^2 + 1$,

$$S = (2^8 - 1)/(2^4 - 1) = 17,$$

$$Tr_m^n(\alpha) = \sum_{k=0}^{n/(m-1)} \alpha^{2^{4k}} = \alpha + \alpha^{16},$$

với α là nghiệm của $g(x)$ thỏa mãn: $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$.

Bằng các biến đổi toán học ta tính được thứ tự chèn ghép:

$$I_p = \{\infty, 2, 4, 2, 8, 12, 4, 0, 1, 9, 9, 14, 8, 5, 0, 3, 2\}.$$

Hàm vết cho phép khảo sát và mô tả quá trình lấy mẫu dãy PN rất hiệu quả.

2.2. Biến đổi d

Có thể mô tả một cách thuận tiện dãy nhị phân $b_0, b_1, ...b_n$ bằng các đa thức trên trường hữu hạn $GF(2)$ qua phép biến đổi d, được định nghĩa như sau:

$$u(d) = \sum_{i=0}^{n} b_i d^i, \quad (2)$$

và $u(d)$ được biểu diễn:

$$u(d) = \frac{S(d)}{h(d)}, \quad (3)$$

với $S(d)$ là đa thức xác định trạng thái ban đầu của bộ ghi dịch tương ứng với đa thức sinh $h(d)$.

Tương tự biến đổi d của các dãy con do đa thức sinh $h_1(d)$ có bậc m là:

$$F_i(d) = \frac{S_i(d)}{h_1(d)}. \quad (4)$$

Như vậy ta luôn có thể biểu diễn $u(d)$ dưới dạng sau:

$$u(d) = \sum_{i=0}^{S-1} d^i F_i(d^S). \quad (5)$$

Sau nhiều thuật toán biến đổi các đa thức trên trường $GF(2)$ và gán các trạng thái ban đầu $S(d)$ tương ứng với một số nguyên, trong đó pha đặc trưng được gán số 0, cuối cùng cũng tìm ra thứ tự lồng ghép I_p [8].

Để đánh giá khả năng ứng dụng của các các dãy mới (theo tiêu chí nêu ở phần mở đầu) ta đi khảo sát các hàm tương quan sau.

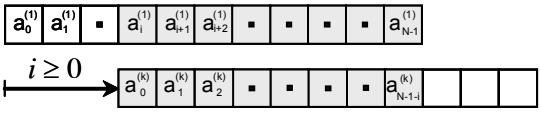
3. CÁC HÀM TƯƠNG QUAN VÀ CÁC TÌNH HUỐNG ĐỒNG BỘ

Xét tín hiệu thu chứa nhiễu giao thoa từ một tín hiệu DS khác:

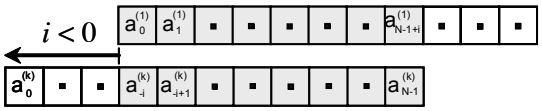
$$\begin{aligned} I_k &= \int_0^T b_k(t-\tau_k)c_k(t-\tau_k)\sqrt{2P}\cos(2\pi f_c t+\phi_k)c_1(t)\cos 2\pi f_c t dt \\ &= \sqrt{P/2}\cos\phi_k\left[b_{-1}^{(k)}\int_0^{\tau_k} c_k(t-\tau_k)c_1(t)dt + b_0^{(k)}\int_{\tau_k}^T c_k(t-\tau_k)c_1(t)dt\right] \end{aligned} \tag{6}$$

I_k phụ thuộc vào hàm tương quan chéo chu kỳ $\int_0^T c_k(t-\tau_k)c_1(t)dt$ nếu $b_{-1}^{(k)} = b_0^{(k)}$ (2 bit cùng dấu), hay hiệu số giữa hai tương quan chéo phi chu kỳ $\int_0^{\tau_k} c_k(t-\tau_k)c_1(t)dt$ và $\int_{\tau_k}^T c_k(t-\tau_k)c_1(t)dt$ nếu $b_{-1}^{(k)} = -b_0^{(k)}$ (2 bit trái dấu). Công thức tương quan chéo giữa hai dạng sang PN liên quan đến tương quan chéo rời rạc phi chu kỳ $C_{k,1}(i)$ của các chuỗi PN tương ứng $\underline{c}^{(k)} = (a_0^{(k)}, a_1^{(k)}, ..., a_{N-1}^{(k)})$ và $\underline{c}^{(1)} = (a_0^{(1)}, a_1^{(1)}, ..., a_{N-1}^{(1)})$ trong đó $C_{k,1}(i)$ được định nghĩa như sau: (Hình 1).

$$C_{k,1}(i) = \begin{cases} \sum_{j=0}^{N-1-i} a_j^{(k)} a_{j+1}^{(1)} & 0 \le i \le N-1 \\ \sum_{j=0}^{N-1-i} a_{j-1}^{(k)} a_j^{(1)} & -(N-1) \le i \le 0 \\ 0 & i \text{ khác trên} \end{cases} \tag{7}$$



Hình 1. a)



Hình 1. b)

Hình 1. Hàm tương chéo phi chu kỳ $C_{k,1}(i)$: a) $0 \le i \le N-1$; b)$-(N-1) \le i < 0$.

$$\int_0^{\tau_k} c_k(t-\tau_k)c_1(t)dt = T_c[C_{k,l}(-(L-i-1))\gamma_k + C_{k,l}(-(L-i))(1-\gamma_k)], \tag{8}$$

$$\int_0^{\tau_k} c_k(t-\tau_k)c_1(t)dt = T_c[C_{k,l}(i)(1-\gamma_k) + C_{k,l}(i+1))\gamma_k]. \tag{9}$$

Tương ứng với Hình 1 có 2 tình huống:

a. Đồng bộ: $\gamma_k = 0$

b. Không đồng bộ: $0 < \gamma_k < 1$

Các giá trị I_k tương ứng cho hai tình huống trên đưa ra tính cho các ví dụ sau.

Ví dụ: Cho hai dãy m được đặc trưng bởi:

$f_1(x) = x^6 + x^5 + 1$

$f_2(x) = x^6 + x^5 + x^4 + x + 1$ đều có độ dài $L = 63$

$a = \{0010011100010111100101000110000100000111111010101100110111011 01\}$

$\{11 - 111 - 1 - 1 - 1111 - 11 - 1 - 1 - 1 - 111 - 11 - 1111 - 1 - 11111 - 111111 - 1 - 1 - 1 - 1 - 1 - 1 - 11 - 11 - 11 - 1 - 111 - 1 - 11 - 1 - 1 - 11 - 1 - 11 - 1\}$

$b = \{1001001111000001101110011000111010111111011010001000010110010 10\}$

$\{-111 - 111 - 1 - 1 - 1 - 111111 - 1 - 11 - 1 - 1 - 111 - 1 - 1111 - 1 - 1 - 11 - 11 - 1 - 1 - 1 - 1 - 1 - 11 - 1 - 11 - 1111 - 11111 - 11 - 1 - 111 - 11 - 11\}$

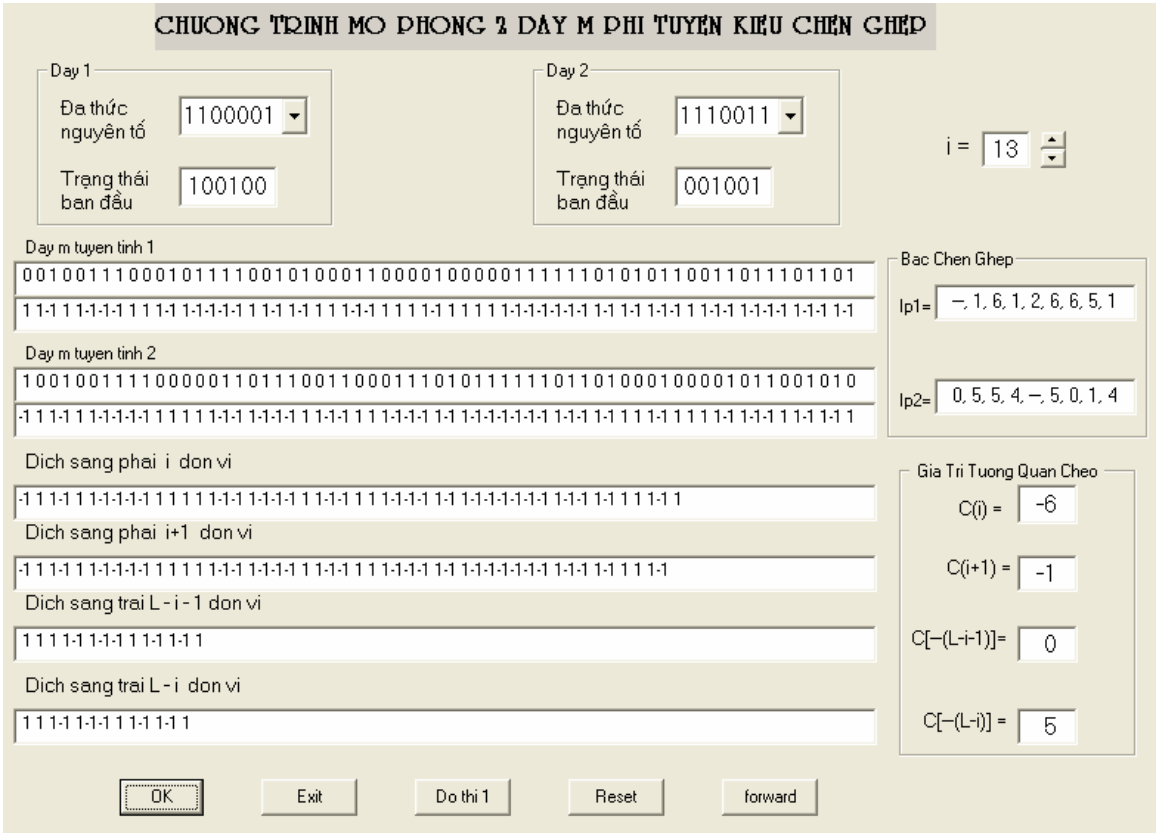
Từ đây ta có:

$I_{p1} = \{\infty, 1, 6, 1, 2, 6, 6, 5, 1\}$

$I_{p2} = \{0, 5, 5, 4, \infty, 5, 0, 1, 4\}$ trong đó ∞ đại diện cho dãy toàn "0".

Với $i = 13$ ta có:

$$C(i) = -6; C(i+1) = -1; C(-(L-i-1)) = 0; C(-(L-i)) = 5$$



Hình 2. Mô phỏng các dãy tuyến tính

Với $P = 2, \phi_k = 0, T_c = 1$ và $b_{-1}^{(k)} = -b_0^{(k)} = 1$

$$I_k = 11 - 10\gamma_k.$$

Trường hợp đồng bộ $\gamma_k = 0 \Rightarrow I_k = 11$ (Hình 3)

Hình 3. Đồ thị nhiễu 2 dãy tuyến tính

Trong các ứng dụng bảo mật tin các m-dãy rất dễ đoán nhận, thực chất chỉ cần biết $2m$ bit liền nhau là có thể xác định trạng thái ban đầu và đa thức sinh. Do đó cần tạo ra dãy phi tuyến có hàm tự tương quan (AFC) tốt như các m-dãy, nhưng chúng rất khó đoán nhận (đối với các dãy tuyến tính cần 12 bit liên tiếp để xác định được dãy, trong khi với các dãy phi tuyến cần 54 bit liên tiếp [3]).

Để có các dãy phi tuyến từ thứ tự lồng ghép I_p, thay thế các dãy con bằng các dãy con khác tương ứng cuối cùng ta có các dãy phi tuyến được tạo ra:

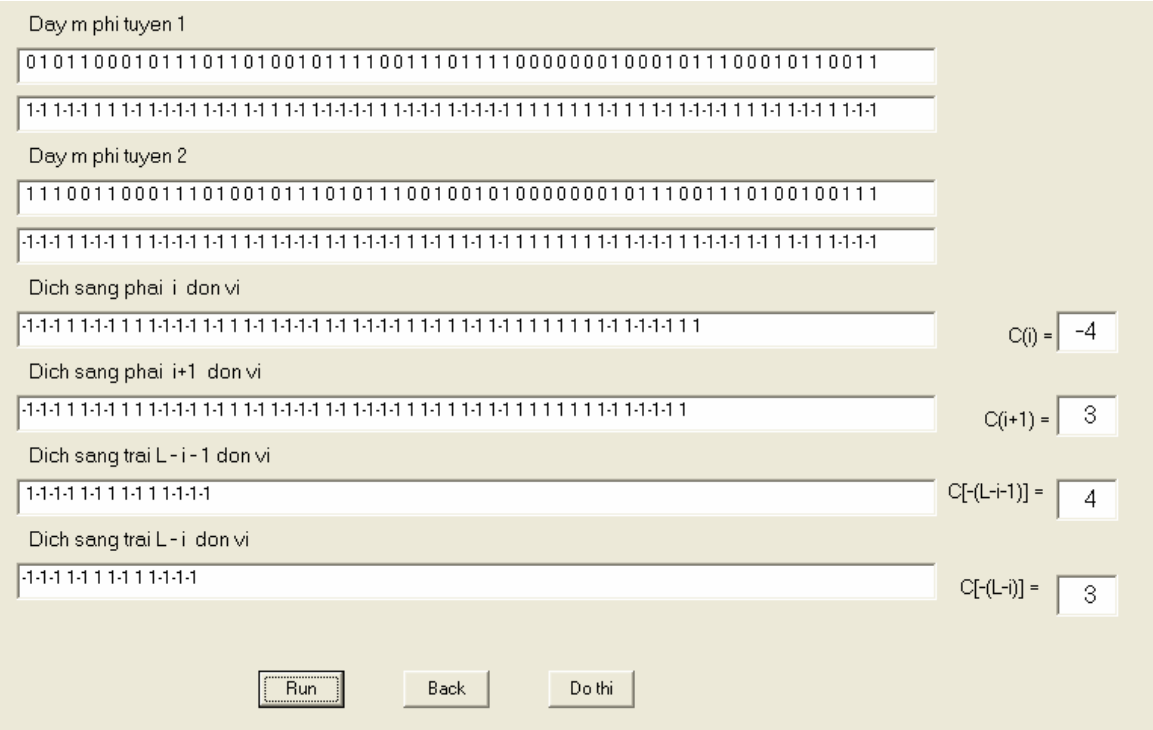
$a = \{01011000101110110100101111001110111100000001000101110001011 0011\}$

$\{1-11-1-1111-11-1-1-11-1-11-111-11-1-1-1-111-1-1-11-1-1-1-11111111-1111-11-1-1-1111-11-1-111-1-1\}$

$b = \{11100110001110100101110101110010010100000001011100111010010 0111\}$

$\{-1-1-111-1-1111-1-1-11-111-11-1-1-11-11-1-1-111-111-11-11111111-11-1-1-111-1-1-11-111-111-1-1-1\}$

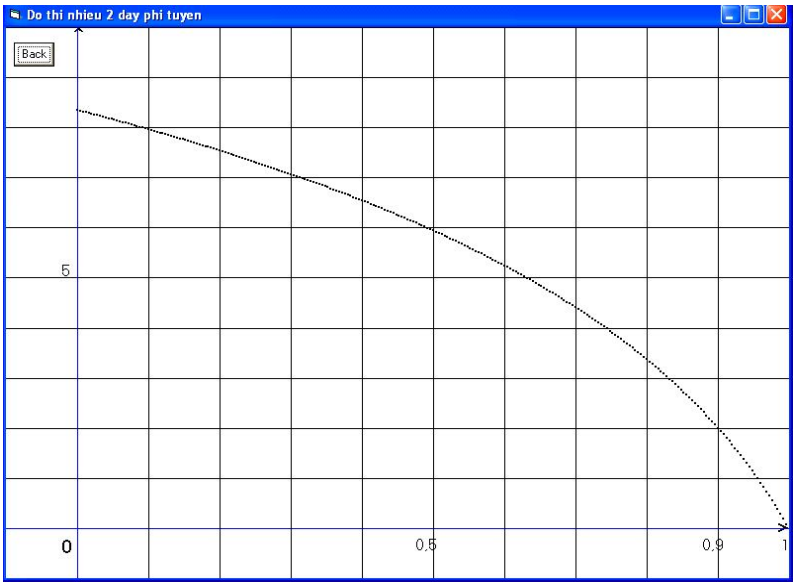
$$C(i) = -4, C(i+1) = 3, C(-(L-i-1)) = 4, C(-(L-i)) = 3.$$



Hình 4. Mô phỏng các dãy phi tuyến

$I_k = 7 - 6\gamma_k$.

Trường hợp đồng bộ $\gamma_k = 0 \Rightarrow I_k = 7$ (Hình 5).



Hình 5. Đồ thị nhiễu 2 dãy phi tuyến

Từ công thức ở trên ta thấy tương quan chéo của dãy phi tuyến nhỏ, gây nhiễu ít. Vì

thế ta phải lựa chọn các giá trị thích hợp sao cho các tương quan chéo đạt giá trị nhỏ nhất. Vì các dãy có độ dài rất lớn, nên công việc tính toán chỉ có thể thực hiện được bằng phần mềm thích hợp.

4. TÍNH ĐỘ PHỨC TẠP ELS

Khoảng tuyến tính tương đương (ELS) là đo sự phức tạp của dãy nhị phân [9]. ELS càng lớn, số bit cần phải quan sát đúng để khôi phục toàn dãy càng lớn. Điều này có nghĩa là quá trình đoán nhận dãy càng phức tạp hơn.

4.1. Giới hạn trên

Đó là khoảng tuyến tính tương đương cực đại đạt được để đánh giá độ phức tạp của dãy. Do đó, để tiện cho việc so sánh chúng ta dùng khái niệm này để đánh giá độ phức tạp của các dãy chèn ghép.

Giới hạn trên đó lấy giá trị m_1S, trong đó m_1 là bậc của đa thức sinh nguyên tố tạo nên dãy con và S là số dãy con được chèn ghép.

Từ công thức ([8])

$$ELS = degh_2(d^S) - degK(d) \tag{10}$$

Ta có thể dễ dàng nhận được giá trị giới hạn trên bằng cách giả thiết rằng:

$degK(d) = 0 \Leftrightarrow K(d) = 1$. Do đó: $ELS = deg\ h_2(d^S) = m_1S$ (11)

Tuy nhiên, giá trị thực của ELS chắc chắn sẽ bé hơn tuỳ thuộc vào biến đổi d của dãy cụ thể đang xét.

4.2. Một số trường hợp

* Ta xét dãy phi tuyến được tạo nên bằng thứ tự chèn ghép:

$I_p = \{2, 12, 9, 3, 8, 8, 1, 2, 13, 5, 9, 0, 13, 0, \infty, 1, 0\}$ với $S = 17$ và $m_1 = 4$ và $h_2(d) = 1 + d^3 + d^4$.

Dùng thuật toán Euclid ta có:

$$\begin{aligned} K(d) =& d^{36} + d^{35} + d^{32} + d^{31} + d^{29} + d^{28} + d^{26} + d^{25} + d^{24} + d^{22} + d^{21} + d^{20} + d^{16} \\ &+ d^{15} + d^{12} + d^{10} + d^7 + d^6 + d^3 + d + 1. \end{aligned}$$

$$ELS = deg\ h_2(d^S) - degK(d) = 68 - 36 = 32.$$

* Ta xét thêm ví dụ với dãy khác cho bởi:

$I_p = \{5, 3, 2, 6, \infty, 2, 6, 4, 1, 4, 0, 5, \infty, 2, 0, 0, 5, 0, \infty, 2, 3, 6, \infty, 6, 5, \infty, 4, \infty, 5, 1, 5, 5, 5, 0, 2,$
$5, 6, 0, 5, 1, 0, 6, 2, 2, 5, 0, 4, 1, 2, \infty, 0, 0, 6, 1, 6, 4, 5, 5, 2, 4, 3, 3, 4, 6, 6, \infty, \infty, 0, 2, 3, 2, 3, 0\}$
với $S = 73$ và $m_1 = 3$ và $h_2(d) = 1 + d^2 + d^3$,

$$ELS = degh_2(d^S) - degK(d) = 219 - 192 = 27.$$

Nhận xét

Ta thấy ELS phụ thuộc vào độ dài của dãy và cấu trúc dãy con, mặc dù ta thấy trường hợp ở trên giới hạn trên lớn hơn nhưng độ phức tạp của dãy là 27 so với ở trên là 32.

Do đó để đánh giá tính chất phi tuyến của dãy, không những ta phải dựa vào độ dài của dãy mà còn phải dựa vào các dãy con của chúng. Khi độ dài dãy tăng lên, có nhiều cách để

phân hoạch dãy và ELS sẽ có thể tăng và khả năng lựa chọn các dãy phi tuyến cũng tăng theo.

Tuy nhiên, như đã nêu ở trên, công việc này đòi hỏi khối lượng tính toán không nhỏ. Thêm nữa, việc tính toán các loại giao thoa, khả năng chống chèn phá... dựa trên các tiêu chí trên còn phức tạp hơn nhiều và vượt quá khuôn khổ bài báo này.

5. KẾT LUẬN

- Trong bài báo, dựa trên biến đổi d, các dãy vừa phi tuyến vừa có tính chất tương quan tốt.

- Các hàm tương quan phi chu kỳ của các dãy phi tuyến đã được nghiên cứu.

- Điều khác biệt ở đây là phương pháp mô tả bằng biến đổi d, trong khi các công trình ở [2, 5, 6] đều dùng công cụ là hàm vết. Biến đổi d có ưu điểm như sau:

1) Dùng trong mọi trường hợp (ví dụ $L \neq 2^n - 1$, không thể dùng hàm vết [6, 15]).

2) Thực hiện phần cứng dễ dàng bằng ghi dịch không cần phần mềm như [10,11, 13].

3) Biến đổi d còn dùng được để mô tả và phân tích tín hiệu cũng như mạch ghi dịch phản hồi tuyến tính (LFSR), điều mà hàm vết không làm được.

- Một số dãy cụ thể có độ dài lớn đã được khảo sát và chúng thỏa mãn những tiêu chí đã nêu.

- Việc khảo sát các dãy (tương quan phi chu kỳ, độ phức tạp) chỉ có thể tiến hành bằng mô phỏng từng dãy cụ thể. Theo chúng tôi biết, chưa có công thức tổng quát tính các giá trị đó, trừ những công trình nghiên cứu về các giới hạn trên và giới hạn dưới.

- Một số nhận thức mới về độ phức tạp cũng được nêu ra dựa trên phần mềm thích hợp.

TÀI LIỆU THAM KHẢO

[1] L. M. Hieu & L. C. Quynh, Design and analysis of sequences with interleaved structure by d-transform, *IETE Journal of Research* vol. **51**, no. 1 (2005) 61–67.

[2] X. D. Lin, K. H. Chang, Optional PN sequences design for quasisynchronous CDMA communication system, *IEEE Trans. Commun.* vol. **45** (1997) 221–226.

[3] L. C. Quynh, S. Prasad, Class of binary sequences with best possible autocorrelation function, *Proc. IEEE* vol. **132**, Part F, no.7 (1985) 577–580.

[4] L. C. Quynh, S. Prasad, A class of binary cipher sequences with good auto and cross correlation function,*Proc. IEEE* vol. **133**, Part F, no. 3 (1986).

[5] X. H. Tang, F. Z. Fan, A class of PN sequences over GF (P) with low correlation zone, *IEEE Trans. Inform. Theory* vol. **41**, no. 4 (2001) 1644–1649.

[6] G. Gong, New design for signal sets with low cross correlation, balance property and large linear span - GF(p) case, *IEEE Trans. Inform. Theory* vol **48**, no. 11 (2002) 2847–2867.

[7] R. J. McEliece, *Finite Field for Computer Scientists and Engineers*, Boston, MA: Kluwer, 1987.

[8] L. C. Quỳnh, N. V. Lâm, Phần mềm tính độ phức tạp của các dãy phi tuyến có độ dài lớn, *Tạp chí BCVT&CNTT*, Kỳ 1, Feb. (2005) 28–29.

[9] J.-S. No and P. V. Kumar, A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, *IEEE Trans. Inform. Theory* vol. **35**, no 2 (1989) 371–379.

[10] R. A. Games, Cross correlation of m-sequences and GMW sequences with the same primitive polynomial,*Discr. Appl. Math.* vol.**12** (1985) 139–146.

[11] A. Klapper, d-form sequences: families of sequences with low correlation values and large linear span, *IEEE Trans. Inform. Theory* vol. **41** (1995) 423–431.

[12] G. Gong and S. W. Golomb, Binary sequences with two-level autocorrelation,*IEEE Trans. Inform. Theory* vol.**45**, no 2 (1999) 692–693.

[13] M. K.Simon, J. Komura, R. A Scholtz, *B. K.Levitt spread spectrum communication*, New York, McGraw-Hill, 2002.

[14] S. Hara and R. Prasad, *Multicarrier Techniques for 4G Mobile Communications*, Artech House, 2003.

[15] R. LIDL & H. Niederreiter, *Introduction to finite field and their application*, Cambridge University press, 2000.

[16] C. Y.Lai, C. K. Lo, Nonlinear orthogonal spreading sequence design for third generation DS - CDMA system, *IEEE Proc. Commun.* vol **140**, no 2 (2002) 105–110.

[17] P. Nicopolitidis, et al. *Wireless network*, John Wiley, 2003.

[18] B. Walke, S. Seidenberg, M. P. Althoft, *UTMS: The fundamental,* John wiley, 2003.

Nhận bài ngày 6 - 12 - 2006
Nhận lại sau sửa ngày 20 - 2 -2006