

ỨNG DỤNG MÃ XYCLIC CỤC BỘ TRONG HỆ THỐNG TRUYỀN TIN

Phan Thanh Minh¹, Nguyễn Thạc Dũng¹

¹Trường Đại học Thông tin Liên lạc

Tóm tắt:

Mã Xyclic cục bộ (XCB) là một bộ mã được xây dựng trên hai cấu trúc đại số nên tạo ra nhiều bộ mã phong phú. Ưu điểm nổi bật của mã XCB ở chỗ do xây dựng mỗi dấu mã là một phần tử của vành đa thức và việc xây dựng mã XCB dựa trên đa thức sinh hoặc trên phân hoạch lớp kề nên có khả năng xây dựng được nhiều bộ mã khác nhau. Vì vậy đánh giá khả năng ứng dụng mã Xyclic cục bộ trong hệ thống truyền tin mà cụ thể trên kênh AWGN là vấn đề cần thiết và quan trọng hiện nay.

Từ khóa: Giải mã ngưỡng, lớp kề, kênh AWGN, vành đa thức, Xyclic cục bộ.

1. MÃ XYCLIC CỤC BỘ VÀ KÊNH AWGN

Mã XCB là một mã tuyến tính có các dấu mã được chọn là một tập con không trống các lớp kề trong phân hoạch của vành đa thức. Các phương pháp xây dựng mã Xyclic cục bộ:

- Cách thứ nhất: Mã xyclic cục bộ được mô tả bằng ma trận sinh $G(n, k)$, có k hàng và n cột [2], [3].

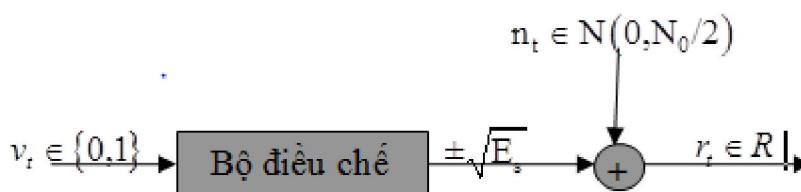
$$G(n, k) = \begin{bmatrix} I_{k,k} \\ P_{k,n-k} \end{bmatrix}$$

Trong đó: $[I_{k,k}]$ là ma trận đơn vị cấp k , $[P_{k,n-k}]$ là ma trận kiểm tra.

- Cách thứ hai: Mã xyclic cục bộ được biểu thị qua trường lớp kề. Nếu gọi giá trị của trường lớp kề là $\alpha 0$ thì các phần tử khác trong lớp kề được tính:

$$\alpha i = (\alpha 0.2i) \bmod P, \quad i = 1 \div k$$

Kênh (AWGN) là kênh có nhiễu tạp âm trắng chuẩn, được biểu diễn như sau:



Hình 1. Mô hình kênh AWGN

Tín hiệu đã được lượng tử truyền trên kênh AWGN bị sai lệch, giá trị thu được là một biến ngẫu nhiên $y_i(x)$ có phân bố như sau:

$$y_i(x) = y_i(x)_{\alpha=0} + y_i(x)_{\alpha=1}$$

$$y_i(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(A-x)^2}{2\sigma^2}} + \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(-A-x)^2}{2\sigma^2}}$$

2. XÂY DỰNG MÃ XYCLIC CỤC BỘ (20, 5) TRÊN KÊNH AWGN

2.1. Phương pháp xây dựng mã Xyclic cục bộ (20, 5)

Để xây dựng thuật toán tìm phân bố trọng số của mã XCB, đầu tiên ta xây dựng các lớp kề cho mã XCB(n, k). Sau đó chọn các lớp kề tạo mã và tìm phân bố trọng số cho mã tương ứng. Kết quả được dự trữ cho quá trình đánh giá và tính toán để tìm P_{ue} tối ưu.

2.1.1. Phổ trọng số của các mã kênh

Ký hiệu C là một mã tuyến tính (n, M, q) có độ dài n , có M từ mã mang tin cần truyền và C xây dựng trên trường hữu hạn $GF(q)$.

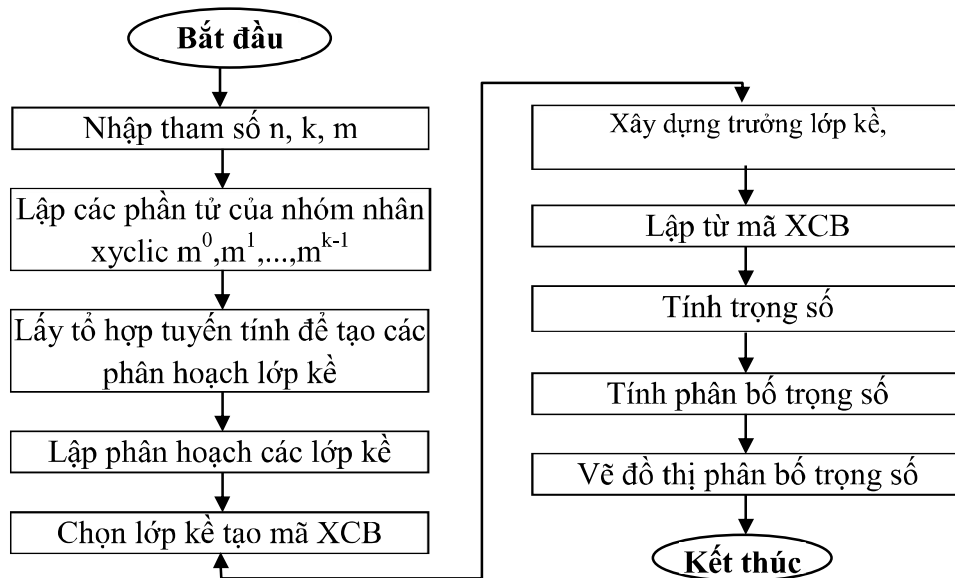
$$A_i^W = A_i^W(C) \left\{ \bar{x} \in C \mid W_H(\bar{x}) = i \right\} \quad \text{Trong đó:}$$

$A_0^W, A_1^W, \dots, A_n^W$ gọi là phổ trọng số của C

$$A_C^W(Z) = \sum_{i=0}^n A_i^W Z^i \quad \text{gọi là hàm phân bố trọng}$$

số của C .

2.1.2. Nhóm nhân xyclic trong vành giao hoán Z_p và các lớp kề của nhóm nhân



Hình 2. Lưu đồ thuật toán tìm phổ trọng số của mã XCB

2.1.3. Phương pháp xây dựng mã xyclic cục bộ (20, 5)

Số bộ mã có thể tạo được từ tất cả các lớp kề là:

$$M = C_6^4 = \frac{6!}{4!(6-4)!} = 15$$

Bảng 1. Phân bố trọng số của bộ mã Xyclic cục bộ (20, 5) xây dựng trên lớp kề

Giả sử α_0 được chọn là trường lớp kề nào đó. Các phần tử còn lại của lớp kề được xác định theo công thức:

$$\alpha_i = (\alpha_0 \cdot m^i) \bmod P$$

Lớp kề thứ nhất gồm các phương trình sau:

$$m^0 + m^1 + m^2 + \dots + m^{i-1} = \alpha_0^1$$

$$m^1 + m^2 + \dots + m^{i-1} + m^i = \alpha_1^1$$

$$\dots \quad (1)$$

....

$$m^{k-1} + m^0 + m^1 + m^2 + \dots + m^{i-2} = \alpha_{k-1}^1$$

Lớp kề thứ 2 gồm các hệ phương trình sau:

$$m^0 + m^1 + m^3 + m^4 + \dots + m^i = \alpha_0^2$$

$$\dots \quad (2)$$

$$m^{i-2} + m^1 + m^2 + \dots + m^{i-1} + m^{k-1} = \alpha_{i-2}^1$$

....

$$m^{k-1} + m^0 + m^1 + m^2 + \dots + m^{i-2} + m^{i-1} = \alpha_{k-1}^2$$

Tìm phổ phân bố trọng số của bộ mã dựa vào lưu đồ thuật toán vết cận khả năng tạo mã XCB như sau:

Dựa vào lưu đồ thuật toán tìm phổ trọng số của mã XCB ta có phân bố trọng số của bộ mã XCB (20,5) xây dựng trên lớp kề được thống kê theo bảng 1.

Lớp kề [1,3,5,7]	A1=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [1,3,5,11]	A2=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [1,3,5,15]	A3=[1 0 0 0 0 1 0 0 0 5 10 10 5 0 0 0 0 0 0 0]
Lớp kề [1,3,7,11]	A4=[1 0 0 0 0 0 0 0 0 10 10 5 5 0 0 1 0 0 0 0]
Lớp kề [1,3,7,15]	A5=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [1,3,11,15]	A6=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [1,5,7,11]	A7=[1 0 0 0 0 0 0 0 0 10 10 5 5 0 0 1 0 0 0 0]
Lớp kề [1,5,7,15]	A8=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [1,5,11,15]	A9=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [1,7,11,15]	A10=[1 0 0 0 0 0 0 0 0 10 10 5 5 0 0 1 0 0 0 0]
Lớp kề [3,5,7,11]	A11=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [3,5,7,15]	A12=[1 0 0 0 0 1 0 0 0 5 10 10 5 0 0 0 0 0 0 0]
Lớp kề [3,5,11,15]	A13=[1 0 0 0 0 1 0 0 0 5 10 10 5 0 0 0 0 0 0 0]
Lớp kề [3,7,11,15]	A14=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]
Lớp kề [5,7,11,15]	A15=[1 0 0 0 0 0 0 0 5 0 16 0 10 0 0 0 0 0 0 0]

2.2. Lựa chọn mã Xyclic cục bộ (20, 5)

2.2.1. Các giới hạn tổng quát

Để lựa chọn được mã XCB (20, 5) tối ưu ta dựa vào các giới hạn sau:

- Giới hạn Griesmer:

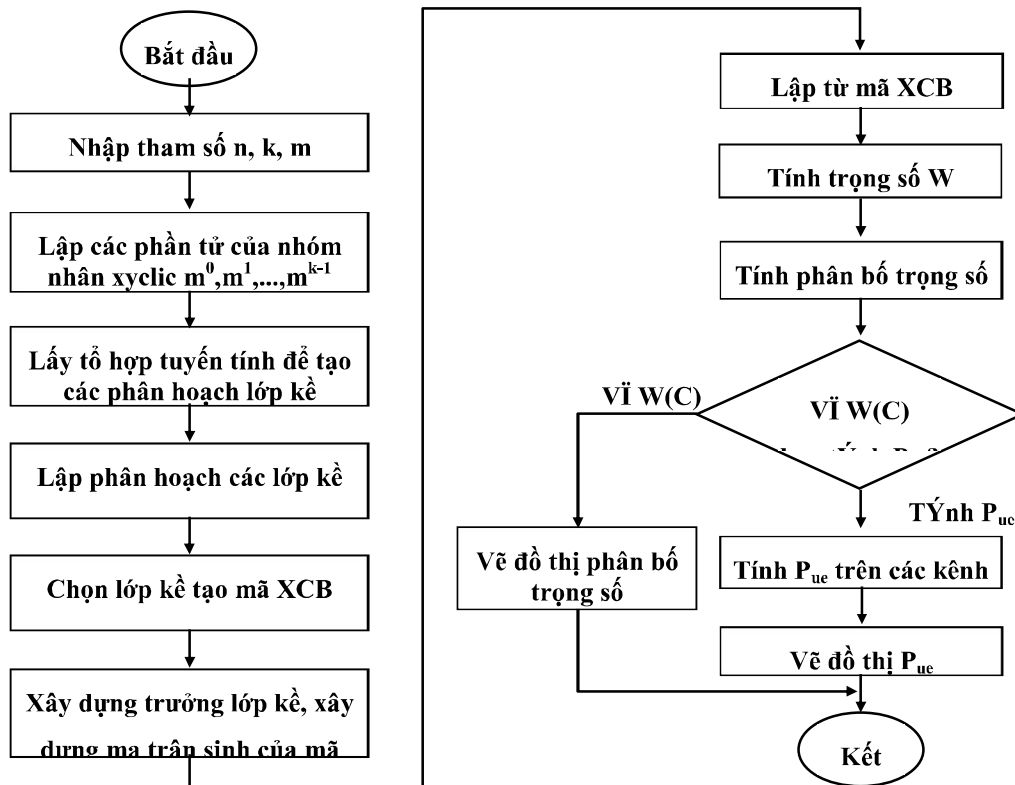
$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_0}{2^i} \right\rceil$$

- Giới hạn Plotkin: $d_0 \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$

- Giới hạn Hamming: $2^{n-k} \geq \sum_{i=0}^t C_n^i$

2.2.2. Thuật toán đánh giá xác suất không phát hiện sai trên kênh truyền

Thuật toán xác định phân bố trọng số và đánh giá xác suất P_{ue} của các bộ mã XCB trên kênh truyền tin như hình 3.



Hình 3. Thuật toán đánh giá xác suất không phát hiện sai trên kênh truyền

2.2.3. Lựa chọn mã Xyclic cục bộ (20, 5)

Xác suất sai sau giải mã xác định theo công thức:

$$P_{ue}(C) = \sum_{\bar{x} \in C} P(\bar{x}) \sum_{\bar{y} \in C/\bar{x}} P(\bar{y}/\bar{x}) \quad (3)$$

Thông thường các từ mã ở đầu phát được phát đi với xác suất như nhau $P(\bar{x}) = \frac{1}{2^k}$ khi đó:

$$P_{ue}(C) = \frac{1}{2^k} \sum_{\bar{x} \in C} \sum_{\bar{y} \in C/\bar{x}} P(\bar{y}/\bar{x}) \quad (4)$$

Trên kênh AWGN, đối với mã tuyến tính có thể giả thiết từ mã toàn không là từ mã phát. $P_{ue}(C)$ có thể bao bằng cận trên theo đường biên tổng (union bound) [1] và phân bố trọng số $W(C)$ với điều chế nhị phân như sau:

$$P_{ue}(C) \leq \sum_{w=d_{\min}}^n A_w Q \left[\sqrt{2wR \frac{E_b}{N_0}} \right] \quad (5)$$

Trong đó $R = k/n$ là tỉ lệ mã hóa, E_b/N_0 là tỷ lệ năng lượng bit trên tạp âm (hoặc SNR trên bit) và hàm $Q(x)$ được định nghĩa:

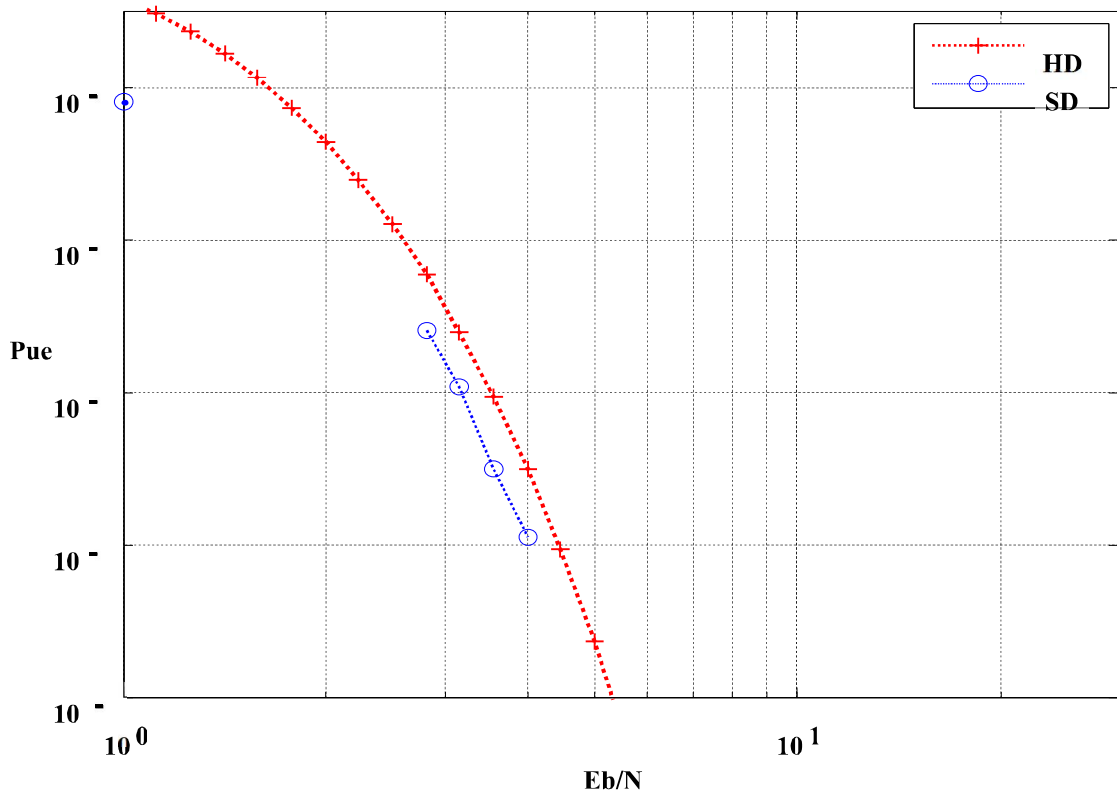
$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-z^2/2} dz, \quad x \geq 0, .$$

Qua mô phỏng, đồ thị xác suất sai sau giải mã trên kênh AWGN của mã XCB(20,5) như hình 4.

Trên đồ thị ta thấy trên kênh AWGN các lớp kề $([1], [3], [7], [11])$; $([1], [5], [7], [11])$; $([1], [7], [11], [15])$ cho P_{ue} nhỏ nhất (xác suất sai sau giải mã), do đó sẽ tạo ra mã XCB (20,5) tốt từ các lớp kề. Mặt khác, khoảng cách Hamming nhỏ nhất của mã XCB (20, 5) xây dựng trên các lớp kề trên đều là: $d_{\min} = 9$. Do đó, mã XCB (20,5) trên các lớp kề sửa được $t=4$ và là mã tối ưu thỏa mãn giới hạn Griesmer:

$$n = 20 \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil = 9 + \frac{9}{2} + \frac{9}{4} + \frac{9}{8} + \frac{9}{16} = 9 + 5 + 3 + 2 + 1 = 20$$

Như vậy, bộ mã XCB (20,5) xây dựng trên lớp kề $\{(1,3,7,11)\}$, $\{(1,5,7,11)\}$, $\{(1,7,11,15)\}$ đạt được xác suất sai sau giải mã từ 10^{-4} đến 10^{-8} khi tỷ số tín trên tạp E_b/N_0 từ 1 đến 10 và thỏa mãn tiêu chuẩn tối ưu Griesmer. Do đó bộ mã XCB (20, 5) xây dựng được lựa chọn là bộ mã tối ưu tạo ra từ các lớp kề.



Hình 4: Đồ thị xác suất sai sau giải mã trên kênh AWGN của mã XCB (20, 5) tạo ra từ lớp kề

3. ĐÁNH GIÁ ỨNG DỤNG MÃ XYCLIC CỤC BỘ (20, 5) TRÊN KÊNH AWGN

3.1. Phương pháp xây dựng giải mã ngưỡng cho mã Xyclic cục bộ (20, 5)

3.1.1. Phân hoạch vành đa thức

Xét vành đa thức $Z_2[x]/x_n + 1$ với n lẻ ta có:

Định nghĩa 1: Cấp số nhân xyclic trên vành đa thức là một tập hợp con có dạng sau:

$$A(a, q) = \{a(x), a(x).q(x), a(x).q^2(x), \dots, a(x).q^{m-1}(x)\} \quad (6)$$

Trong đó: m là số các số hạng của cấp số nhân.

$q(x)$ là công bội; $a(x)$ là số hạng đầu của cấp số nhân

$$a(x).q^m(x) \equiv a(x) \pmod{x^n + 1}$$

Định nghĩa 2: Công bội $q(x)$ của phân hoạch được gọi là hạt nhân của phân hoạch.

Định nghĩa 3: Phân hoạch vành đa thức được gọi là không suy biến nếu phân hoạch bao gồm tất cả các phần tử khác 0 trong vành đa thức. Ngược lại, phân hoạch là phân hoạch suy biến.

Số lớp kề trong phân hoạch không suy biến tùy ý được xác định:

$$N_{(a(x), n)} \geq \left\lceil \frac{2^n - 2}{\text{ord}(a(x))} \right\rceil + 1 \quad (7)$$

3.1.2. Phân hoạch hỗn hợp trên một vành đa thức

Phân hoạch hỗn hợp vành $Z_2[x]/x^n + 1$ được khái quát như sau:

Bước 1: Xác định $\max \text{ord } a(x)$ của phần tử trong vành, tính số ước của $\max \text{ord } a(x)$, số ước số này chính là số kiểu phân hoạch không suy biến của vành.

Bước 2: Phân hoạch vành theo hai hạt nhân trong đó phải có ít nhất một hạt nhân có trọng số lẻ. Chọn một hạt nhân phân hoạch $q_1(x)$ sao cho $\text{ord } q_1(x) = n$, một hạt nhân phân hoạch thứ hai $q_2(x)$ với $\text{ord } q_2(x)$ là bội của n . Một hạt nhân có trọng số lẻ được dùng để phân hoạch các phần tử có trọng số lẻ của vành, hạt nhân còn lại được dùng để phân hoạch các phần tử có trọng số chẵn của vành.

Bước 3: Kết hợp các cấp số nhân xyclic (CGP) của hai phân hoạch với nhau để được một phân hoạch mới.

3.1.3. Xây dựng mã XCB (20, 5) trên phân hoạch hỗn hợp của một vành đa thức

Định lý: Nếu $a(x)$ là phần tử của nhóm nhân nào đó thì cấp cực đại của $a(x)$ được xác định như sau:

- Nếu n lẻ và $x^{n+1} + 1 = \prod f_i(x)$; trong đó $f_i(x)$ là các đa thức bất khả quy.

Khi đó $\max \text{ord}(a(x)) = 2^m - 1$; trong đó $m = \max \deg f_i(x)$

- Nếu n chẵn $n = 2^s(2k + 1)$ và $x^{2k+1} + 1 = \prod f_i(x)$

Khi đó $\max \text{ord}(a(x)) = 2^s(2^m - 1)$ trong đó $m = \max \deg f_i(x)$

Ta có thể xây dựng được mã XCB (20, 5) theo các bước sau:

Bước 1: Dựa vào định lý trên, xác định cấp cực đại của các phần tử trong vành $x^5 + 1$:

$$\max \text{ord}(a(x)) = 2^4 - 1 = 15, \text{ trong đó } m_s = \deg f_2(x) = 4.$$

Số ước của $\max \text{ord}(a(x))$ là 3, bao gồm 3, 5 và 15 và sẽ có tương ứng 3 kiểu phân hoạch không suy biến của vành này là kiểu phân hoạch theo các nhóm nhân xyclic cấp 3, 5 và 15.

Bước 2: Phân hoạch vành thành các CGP theo 2 hạt nhân khác nhau:

- CGP thứ nhất A: chọn công bội $q_1(x) = 1 + x^2 + x^4$ với $W(q_1(x)) = 3$ và $\text{ord}(q_1(x)) = 15$ là bội số của $n = 5$; số hạng đầu $a(x) = 1$, CGP này sẽ bao gồm tất cả các phần tử lẻ của vành.

- CGP thứ hai B: chọn công bội $q_2(x) = x$ với $\text{ord}(q_2(x)) = 5$; số hạng đầu $b(x) = 1 + x$, CGP này sẽ bao gồm các phần tử có trọng số chẵn.

Cấu trúc của 2 CGP như sau:

$$\text{CGP}_1 = A = \{a(x), a(x)q_1(x), a(x)q_1^2(x), \dots, a(x)q_1^{14}(x)\} = \{a_i, i = \overline{1, 15}\}$$

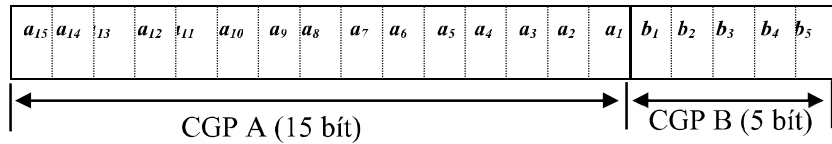
$$A = \{(024), (034), (1), (013), (014), (2), (124),$$

$$(012), (3), (023), (123), (4), (134), (234), (0)\}$$

$$\text{CGP}_2 = B = \{b(x), b(x)q_2(x), b(x)q_2^2(x), \dots, b(x)q_2^4(x)\} = \{b_i, i = \overline{1, 5}\}$$

$$B = \{(01), (12), (23), (34), (04)\} = \{b_i, i = 1, 2, \dots, 5\}$$

Bước 3: Kết hợp hai CGP A và B ta có thể tạo được mã XCB (20, 5):



Hình 5. Cấu trúc từ mã của mã XCB (20,5)

Ma trận sinh của mã này như sau:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Trong ma trận G thì 15 cột đầu tiên tương ứng với CGP A và 5 cột cuối cùng tương ứng với CGP B.

3.1.4. Xây dựng sơ đồ giải mã ngưỡng mã XCB (20, 5)

Xét mã tuyến tính (n, k) trên trường GF(2), gọi H là ma trận kiểm tra của nó, khi đó với mọi từ mã $a = (a_0, a_1, \dots, a_{n-1})$, ta có:

$a.H^T = 0$; trong đó: H^T là ma trận chuyển vị của H

Khi đó mỗi hàng h_j của H là:

$$h_j = (h_{j0}, h_{j1}, \dots, h_{jn-1}) \text{ với } j = \overline{1, r}; r = n - k$$

Sẽ cho một tổng kiểm tra (TKT) của các dấu mã:

$$h_{j0}\alpha_0 + h_{j1}\alpha_1 + \dots + h_{jn-1}\alpha_{n-1} = 0; j = \overline{1, r}$$

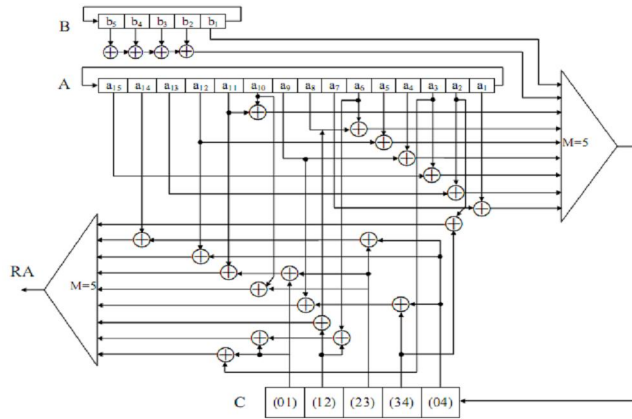
Dựa vào hệ tổng kiểm tra trực giao thiết lập được hệ TKT của mã XCB (20, 5, 9) xây dựng trên một vành đa thức và sơ đồ đánh giá ứng dụng mã XCB(20, 5) như hình 6.

Bảng 2. Hệ tổng kiểm tra của mã Xyclic cục bộ (20, 5, 9) xây dựng trên một vành đa thức

TT	Hệ TKT cho cặp dấu (1 + x) ↔ (01)	TT	Hệ TKT cho dấu (1) ↔ (0)
1)	$a_1 + a_7 = (01)$	1)	$a_2 + (34) = (0)$
2)	$a_2 + a_{13} = (01)$	2)	$a_3 + (01) = (0)$
3)	$a_3 + a_{15} = (01)$	3)	$a_6 + (01) + (12) = (0)$
4)	$a_4 + a_9 = (01)$	4)	$a_8 + (12) = (0)$
5)	$a_5 + a_{12} = (01)$	5)	$a_9 + (04) + (34) = (0)$
6)	$a_6 + a_8 = (01)$	6)	$a_{10} + (23) = (0)$
7)	$a_{10} + a_{11} = (01)$	7)	$a_{11} + (01) + (23) = (0)$
8)	$b_1 = (01)$	8)	$a_{12} + (04) = (0)$
9)	$b_2 + b_3 + b_4 + b_5 = (01)$	9)	$a_{14} + (04) + (23) = (0)$

Thanh ghi B tương ứng với CGP₂, thanh ghi A tương ứng CGP₁. Do hai CGP có công bội (nhịp) khác nhau nên khi giải mã nhịp giải mã cho mỗi thanh ghi là khác nhau. Cụ thể tốc độ nhịp của thanh ghi A sẽ nhanh gấp 3 lần tốc độ nhịp của thanh ghi B.

Sau cấp ngưỡng thứ nhất giải mã thành công các cặp dấu thông tin (01), (12), (23), (34), (04) và được chứa vào thanh ghi C. Nhịp giải mã ở cấp ngưỡng thứ 2 cũng tương tự, tốc độ nhịp thanh ghi A nhanh gấp 3 lần tốc độ thanh ghi C. Sau cấp ngưỡng thứ 2 ta được các dấu thông tin cần giải mã: (0), (1), (2), (3) và (4).

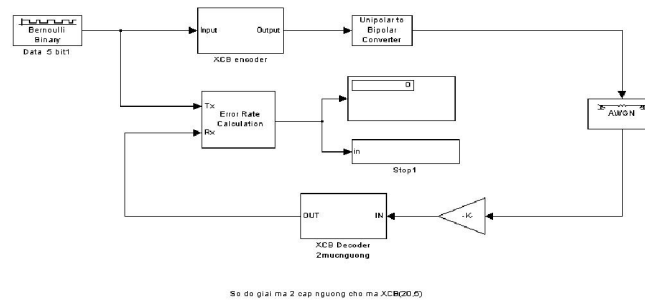


Hình 6. Sơ đồ giải mã ngưỡng cho mã XCB (20, 5) trên vành đa thức x^5+1

3.2. Đánh giá ứng dụng mã xyclic cục bộ (20, 5) trên kênh AWGN

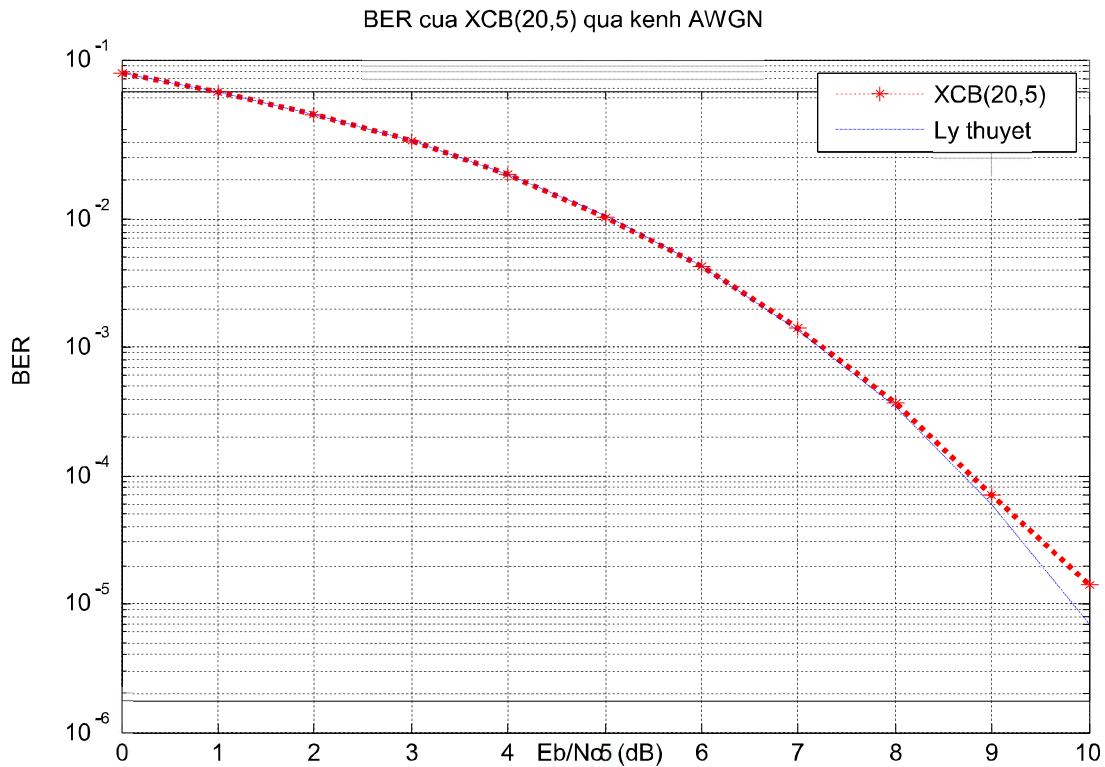
thuyết và mô phỏng giải mã đa số ngưỡng cho mã XCB (20,5) trên kênh AWGN như sau:

Xây dựng sơ đồ mô phỏng so sánh giữa lý



Hình 7: Sơ đồ mô phỏng giải mã ngưỡng cho mã XCB (20, 5, 9) trên kênh AWGN

Kết quả mô phỏng bằng phần mềm Matlab như sau:



Hình 8. Tỷ lệ lỗi bit của mã XCB (20, 5, 9) trên kênh AWGN

Tóm lại, các giá trị BER được tính tại các giá trị khác nhau của SNR, từ 0, 1, 2,..., 10dB, biểu thị trên hình 8 bằng những điểm nút. Trên đồ thị còn biểu diễn hàm xác suất lỗi bit theo lý thuyết P_b [4] và ta thấy chất lượng mã XCB(20,5) truyền qua kênh AWGN khi tỷ số tín trên tạp E_b/N_0 từ 10^{-1} đến 10^{-8} sử dụng giải mã ngưỡng trên vành đa thức cho chất lượng

giải mã tốt và thỏa mãn tiêu chuẩn tối ưu Griesmer. Từ kết quả mô phỏng ta thấy lựa chọn mã XCB (20,5) truyền tốt trên kênh AWGN và có thể ứng dụng mã XCB (20,5) trong hệ thống truyền tin; đồng thời là cơ sở để tiếp tục nghiên cứu tìm ra các tiêu chí mới khác để đánh giá và tạo ra các bộ mã Xyclic cục bộ mới có khả năng sửa sai tốt hơn.

TÀI LIỆU THAM KHẢO

- [1]. Phạm Văn Hoan (2010), “Nghiên cứu đánh giá chất lượng giải mã Xyclic cục bộ trên các kênh truyền tin”, Luận án tiến sĩ kỹ thuật, Học viện Kỹ thuật Quân sự, Hà Nội.
- [2]. Bùi Minh Tiêu (1974), *Cơ sở lý thuyết truyền tin*, NXB ĐH -THCN.
- [3]. Phạm Việt Trung (2005), Nghiên cứu ứng dụng mã sửa sai trong bảo mật thông tin, Luận án tiến sĩ kỹ thuật, Học viện Kỹ thuật Quân sự, Hà Nội.
- [4]. H. Harada and R. Prasad (2002), *Simulation and Software Radio for Mobile Communications*, Artech House.

APPLYING LOCAL CYCLICAL CODES IN COMMUNICATION SYSTEMS

Phan Thanh Minh¹, Nguyen Thac Dung¹

¹*Telecommunication University*

Abstract:

Local cyclic code (LCC) is the block code based on two algebraic structures, so it can create many sets of codes. The major advantage of this code is that the code can build different codes due to each codeword is a base polynomial ring of the circular shifts and the construction of polynomial code based on adjacent layers. Therefore, evaluating the applicability of the local cyclic code in communication systems is very necessary and important in the current.

Key words: Local cyclic codes; AWGN channel; polynomial ring; threshold decoding; adjacent layers.