BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG
HỌC VIỆN KĨ THUẬT QUÂN SỰ

PHẠM VĂN HOAN

NGHIÊN CỨU ĐÁNH GIÁ CHẤT LƯỢNG GIẢI MÃ XYCLIC CỤC BỘ TRÊN CÁC KÊNH TRUYỀN TIN

Chuyên ngành: Kĩ thuật điện tử
Mã ngành: 62.52.70.01

TÓM TẮT LUẬN ÁN TIẾN SỸ KĨ THUẬT

Hà nội - 2010

Luận án được hoàn thành tại:

Học viện kĩ thuật quân sự - Bộ quốc phòng

Cán bộ hướng dẫn khoa học:

GS-TS Nguyễn Bình
TS Nguyễn Đức Thắng

Phản biện 1: *PGS-TSKH Nguyễn Hồng Vũ*
Cục tác chiến điện tử

Phản biện 2: *PGS-TS Nguyễn Quang Hoan*
Học viện Công nghệ bưu chính viễn thông

Phản biện 3: *PGS Phương Xuân Nhàn*
Đại học Bách khoa Hà nội

Luận án được bảo vệ tại hội đồng chấm luận án cấp nhà nước
họp tại Học viện kĩ thuật quân sự - Bộ quốc phòng
vào hồi 14 giờ ngày 09 tháng 07 năm 2010

Có thể tìm luận án tại:
Thư viện quốc gia
Thư viện Học viện kĩ thuật quân sự - Bộ quốc phòng

Các công trình khoa học của tác giả đã công bố

1. Phạm Văn Hoan, (2006), *Đánh giá mã XCB trên một số kênh truyền*. Tạp chí nghiên cứu khoa học kỹ thuật và công nghệ quân sự, số 14, 3/2006, Trung tâm KHCN QS- BQP. Trang 57- 62.
2. Phạm Văn Hoan, (2006), *Một thuật xác định phân bố trọng số của mã XCB*. Tạp chí nghiên cứu khoa học kỹ thuật và công nghệ quân sự, số 16, 9/2006, Trung tâm KHCN QS- BQP. Trang 81-87.
3. Phạm Văn Hoan, Trần Đình Tấn, (2006), *Chọn mã XCB tốt trên các kênh truyền tin*. Tạp chí nghiên cứu khoa học kỹ thuật và công nghệ quân sự, số 17, 12/2006, Trung tâm KHCN QS- BQP. Trang 57-63.
4. Phạm Văn Hoan, Trần Đình Tấn, (2007), *Một phương pháp chọn mã tối ưu theo độ hiệu quả của kênh*. Tạp chí nghiên cứu khoa học kỹ thuật và công nghệ quân sự, số 21, 12/2007, Trung tâm KHCN QS- BQP.

MỞ ĐẦU

1. TÍNH CẤP THIẾT CỦA ĐỀ TÀI

Mã kênh được sử dụng để nâng cao độ tin cậy chính xác cho các hệ thống truyền tin. Người đặt nền móng cho các nghiên cứu về mã kênh, C.E. Shannon [61], đã đưa ra các cơ sở toán học và các cận lý thuyết cho việc xây dựng các bộ mã kênh. Tuy nhiên, lý thuyết không thể chỉ ra được cách tạo các bộ mã tối ưu có thể đạt được giới hạn đó. Thực tế, các bộ mã hoá, giải mã đơn giản, dễ chế tạo vẫn được ứng dụng rộng rãi trong các hệ thống truyền tin và lưu giữ thông tin. Trong thực tế, tồn tại nhiều loại mã sửa sai khác nhau. Mỗi bộ mã sửa sai có cấu trúc và cơ chế tạo và giải mã khác nhau.

Vào năm 1987 GS -Tiến sĩ Nguyễn Bình và GS-Tiến sĩ Khoa học Nguyễn Xuân Quỳnh đã nghiên cứu ra mã Xyclic cục bộ là một bộ mã được xây dựng trên hai cấu trúc đại số, do đó nó có khả năng sửa lỗi tốt và có tính chất cũng giống như các mã tuyến tính khác. 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 các lớp kề, do đó có khả năng xây dựng được

nhiều bộ mã khác nhau. Hiện nay việc nghiên cứu đưa mã XCB vào ứng dụng là một vấn đề đã và đang được tiếp tục nghiên cứu.

Với đề tài "Nghiên cứu đánh giá chất lượng giải mã XCB trên các kênh truyền tin", luận án đã nghiên cứu cấu trúc và các cơ sở toán học của các mô hình kênh, các mã kênh. Từ đó đề xuất phương pháp đánh giá chất lượng của các bộ mã XCB, xây dựng các thuật toán tìm phân bố trọng số và đánh giá xác suất sai sau giải mã XCB trên một số kênh truyền tin. Dựa vào các cận chất lượng của xác suất sai sau giải mã tìm các bộ mã có chất lượng tốt và so sánh chúng với các bộ mã tốt có cùng cấu trúc đã được công bố. Đồng thời luận án cũng đi xây dựng sơ đồ mô phỏng đánh giá các sơ đồ giải mã ngưỡng cho bộ mã XCB(14,6) trên kênh AWGN.

2. MỤC ĐÍCH NGHIÊN CỨU

Xác định tiêu chí sử dụng để đánh giá mã XCB trên các kênh truyền tin đó là xác suất không phát hiện sai sau giải mã và xây dựng sơ đồ mã hoá và giải mã của bộ mã cụ thể để đánh giá chất lượng giải mã của bộ mã hoá đó trên một số kênh truyền tin .

3. NHIỆM VỤ NGHIÊN CỨU

- Xây dựng thuật toán tìm phân bố trọng số của mã XCB, từ đó làm cơ sở để tính xác suất không phát hiện sai sau giải mã.

- Xác định các định lý giới hạn dùng để tính xác suất không phát hiện sai sau giải mã.

- Xây dựng sơ đồ mã hoá và giải mã của bộ mã XCB(14,6), xây dựng sơ đồ mô phỏng đánh giá chất lượng của bộ mã XCB này trên kênh AWGN thông qua phần mềm Matlab.

4. PHƯƠNG PHÁP NGHIÊN CỨU

Dùng phương pháp toán học kết hợp sử dụng máy tính để khảo sát, phân tích, tổng hợp xử lý các kết quả thực nghiệm từ đó tìm ra các bộ mã XCB tốt dùng trên các kênh truyền tin.

5. CẤU TRÚC CỦA LUẬN ÁN

Luận án gồm 3 chương chính. Cụ thể:

Mở đầu

Chương 1. Tổng quan về kênh và mã kênh

Chương 2. Tính toán phổ trọng số và xác suất lỗi của một số mã XCB

Chương 3. Đánh giá chất lượng mã XCB trên các kênh truyền tin

Kết luận, tài liệu tham khảo, phụ lục.

NỘI DUNG CỦA LUẬN ÁN

Chương 1: TỔNG QUAN VỀ KÊNH VÀ MÃ KÊNH

1.1 Các đặc trưng cơ bản của kênh

1.1.1 Phương trình đường truyền [65]

$$y(t) = x(t) + n(t)$$

(1.1)

1.1.2 Hệ số sử dụng kênh: là tham số quan trọng để đánh giá truyền tin qua kênh.

$$\eta = \frac{v}{C'} = \frac{\text{Tốc độ truyền tin}}{\text{KNTQ}}$$

(1.2)

1.2 Các mô hình kênh điển hình

1.2.1 Mô hình kênh AWGN

Phương trình đường truyền cho kênh AWGN theo như (1.1). Dung lượng kênh AWGN xác định theo công thức Shannon [60]:

$$C'_{(b/s)} = F \log_2\left(1 + \frac{P_{th}}{P_n}\right) \; [bit/giây]$$

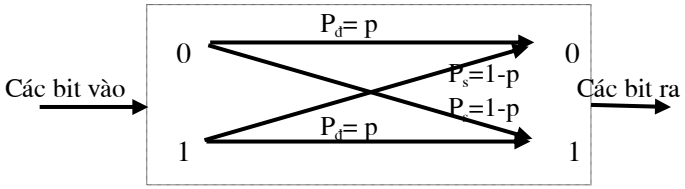
(1.18)

1.2.2 Mô hình kênh nhị phân đối xứng (BSC)

Phương trình đường truyền:

$$Y_i = X_i \oplus N_i$$

(1.19)



Hình 1.2 Mô hình kênh BSC

Xác suất chuyển đổi tin:

$$P(Y_i/X_i) = \begin{cases} P_d = 1 - P_s & \text{Nếu } Y_i = X_i \\ P_s & \text{Nếu } Y_i \neq X_i \end{cases}$$

1.3. Mã kênh

1.3.1 Điều kiện và khả năng sửa lỗi

1. Điều kiện để bộ mã có khả năng sửa lỗi

Điều kiện để bộ mã có khả năng sửa lỗi là khoảng cách mã tối thiểu d_0 của bộ mã phải không nhỏ hơn 3. Nghĩa là: $d_0 \geq 3$.

2. Khả năng sửa lỗi của bộ mã sửa sai: Được đánh giá qua số sai *t* mà mã có khả năng sửa được. Số sai sửa được và khoảng cách mã tối thiểu d_0 quan hệ với nhau:

$$t \leq \left[\frac{d_0 - 1}{2}\right]$$

Kí hiệu [*x*]: lấy phần nguyên của *x*.

1.3.2 Xác suất không phát hiện sai của mã sửa sai

Kí hiệu *C(n,M)* là mã sửa lỗi tuyến tính (*n*: độ dài từ mã, *M*: số từ mã truyền trên kênh).

Phương trình đường truyền*:* $\bar{y} = \bar{x} \oplus \bar{e}$

trong đó $\bar{e}$: vectơ sai ($\bar{e} = (\bar{e}_1, \bar{e}_2, ..., \bar{e}_j, ..., \bar{e}_n)$)

Kí hiệu: $P_{ue} = P_{ue}(C,K)$*:* xác suất không phát hiện được sai. Ta có:

$$P_{ue}(C,K) = \sum_{\bar{x} \in \sigma} P(\bar{x}) \sum_{\bar{y} \in C \setminus \{\bar{x}\}} P(\bar{y}|\bar{x}) \qquad (1.37)$$

Các từ mã gửi đi có xác suất xuất hiện như nhau $P(\bar{x}) = \frac{1}{M}$. Khi này P_{ue} xác định theo công thức:

$$P_{ue}(C,K) = \frac{1}{M}\sum_{\bar{x}\in C}\ \sum_{\bar{y}\in C\setminus\{\bar{x}\}} P(\bar{y}|\bar{x})$$

(1.38)

$$P_{ue}^{(t)}(C,K) = \frac{1}{M}\sum_{\bar{x}\in C}\ \sum_{\bar{x}'\in C\setminus\{\bar{x}\}}\ \sum_{\bar{y}\in M_t(\bar{x}')} P(\bar{y}|\bar{x})$$

(1.41)

Như vậy tiêu chí chính mà ta sẽ tính đến khi sử dụng mã phát hiện sai trên kênh: tính $P_{ue}(C,K)$ hoặc $P_{ue}^{(t)}(C,K)$ như thế nào đối với mã đã cho? với kênh BSC tính: $P_{ue}(C,p)$ hoặc $P_{ue}^{(t)}(C,p)$?

Tìm được phân bố trọng số, $P_{ue}(C,p)$ có thể tính theo định lý 1[62]. Tìm được phân bố trọng số của mã ta có thể tính được xác suất không phát hiện sai và từ đó có thể đánh giá được chất lượng của bộ mã. Phương pháp này ta sẽ áp dụng để đánh giá chất lượng của mã XCB sẽ xét đến trong các chương sau.

1.5. Kết luận chương một

1. Các mã xyclic truyền thống xây dựng trên các Ideal của vành có cấu trúc dễ dàng thực hiện về mặt kỹ thuật và đã được ứng dụng rộng rãi trong các thủ tục truyền tin cơ bản. Tuy nhiên các mã xyclic chỉ được xem xét với các độ dài lẻ và bị hạn chế bởi số lượng các Ideal.

2. Các mã xyclic truyền thống được xem là một lớp con trong các mã xyclic cục bộ, bởi vậy

khả năng lựa chọn của các mã XCB là đa dạng hơn các mã truyền thống. Tuy nhiên chưa có công trình nào đề cập đến khả năng và chất lượng giải mã XCB trên các kênh truyền tin. Do vậy, vấn đề nghiên cứu đánh giá hiệu quả giải mã của mã XCB trên một số kênh truyền và đánh giá khả năng giải mã XCB, xác định bộ mã XCB tốt dùng trên các kênh truyền tin là yêu cầu cấp thiết.

Chương 2: TÍNH TOÁN PHỔ TRỌNG SỐ VÀ XÁC SUẤT LỖI CỦA MỘT SỐ MÃ XCB

2.1. Phổ trọng số của các mã kênh

2.1.2. Phân bố trọng số và phân bố khoảng cách mã của mã tuyến tính [62]

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). Ký hiệu:

$$A_i = A_i(C) = \frac{1}{M}.\left\{\left(\bar{x},\bar{y}\right)\bar{x},\bar{y} \in C \text{ và } d_H\left(\bar{x},\bar{y}\right) = i\right\} \quad (2.1)$$

$$A_C(Z) = \sum_{i=0}^{n} A_i Z^i \quad (2.2)$$

được gọi là hàm phân bố khoảng cách của C

Ký hiệu: $A_i^W = A_i^W(C).\left|\left\{\bar{x} \in C | W_H\left(\bar{x}\right) = i\right\}\right|$

$$A_C^W(Z) = \sum_{i=0}^{n} A_i^W Z^i$$

(2.3)

được gọi là hàm phân bố trọng số của C.

2.1.3. Biến đổi Mac William[62]

Ký hiệu C là mã (n, M, q). Biến đổi William của $A_C(Z)$ được định nghĩa [62]:

$$A_C^{MW}(Z) = \frac{1}{M}(1+(q-1)Z)^n \; A_C\left[\frac{1-Z}{1+(q-1)Z}\right]$$

(2.4)

$$A_C(Z) = \frac{M}{q^n}(1+(q-1)Z)^n \; A_C^{MW}\left(\frac{1-Z}{1-(q-1)Z}\right)$$

(2.6)

2.2. Thuật toán tìm phân bố trọng số của mã xyclic cục bộ

2.2.1 Mở đầu

Để xây dựng thuật toán tìm phân bố trọng số của mã XCB, việc 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..

2.2.3. Lưu đồ thuật toán tìm phân bố trọng số của mã XCB

Lưu đồ thuật toán tìm phổ trọng số và đánh giá P_{ue} của mã XCB hình 2.8.

Ví dụ: Với k=6, n=14 tức là mã *XCB(14, 6)* có phân hoạch các lớp kề:

1	2	4	8	16	32

3	6	12	24	48	33
5	10	20	40	17	34
9	18	36			
7	14	28	56	49	35
13	26	52	41	19	38
25	50	37	11	22	44
21	42				
15	30	60	57	51	39
23	46	29	58	53	43
27	54	45			
31	62	61	59	55	47
0					

Phân bố trọng số của các bộ mã XCB hệ thống(14,6) xây dựng trên các lớp kề được liệt kê theo bảng 2.2.

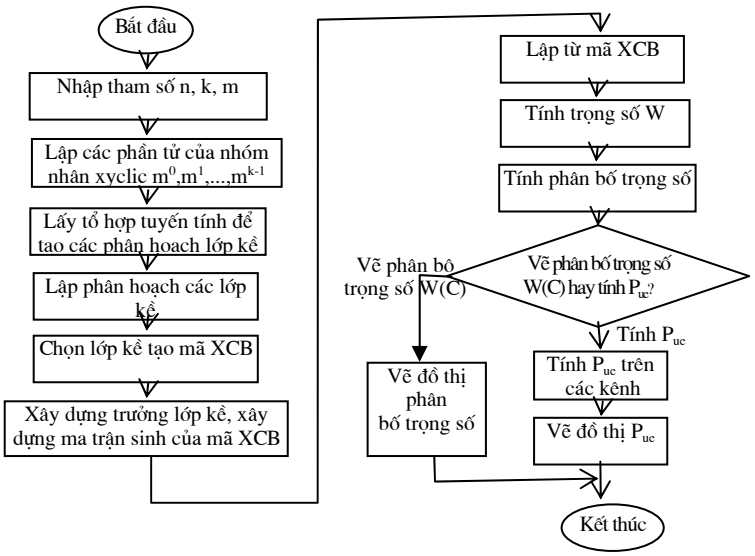
Bảng 2.2 Phân bố trọng số của các mã XCB(14,6)

Lớp kề	Phân bố trọng số	Khoảng cách mã
1,13, 21*	1 0 0 0 0 12 15 8 15 12 0 0 0 0 1	d=5 d=5
1,25, 21*	1 0 0 0 0 12 15 8 15 12 0 0 0 0 1	

Phân bố trọng số của mã *XCB(14,6)* xây dựng trên lớp kề ([1],[7],[21]) hình 2.2. Phân bố trọng số của mã này như sau:

A_i =[1 0 0 0 3 6 12 20 12 6 3 0 0 0 1]

Kết luận: Dựa trên thuật toán tìm phân bố trọng số cho mã XCB, ta có thể tìm được phân bố trọng số của mã XCB, từ đó có thể tính được xác suất không phát hiện sai và đánh giá được chất lượng của mã XCB trên các kênh truyền, do đó có thể tìm được mã XCB tốt cho các ứng dụng trong thực tế. Phần này sẽ cung cấp dữ liệu cho các phần 2.3 và chương 3 để đánh giá và tìm mã XCB tốt trên các kênh truyền.



Hình 2.8: Lưu đồ thuật toán tìm phổ trọng số và đánh giá xác suất P_{ue} của mã XCB

2.3 Xác suất không phát hiện sai của mã sửa lỗi trên các kênh

2.3.1 P_{ue} của kênh BSC

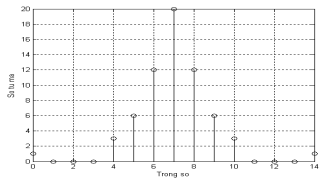
Xác suất sai không phát hiện được của mã *C* trên kênh nhị phân đối xứng kí hiệu là $P_{ue}(C,BSC)$. Ta có:

$$P_{ue}(C, BSC_p) = \frac{M}{2^n} A_C^{M|W}(1-2p) - (1-p)^n \quad (2.44)$$

Ví dụ: Phân bố trọng số của mã XCB (15,5):

$$A_C(Z) = \sum_{i=0}^{n} A_i Z^i = \sum_{i=0}^{15} A_i Z^i = 1 + 15Z^7 + 15Z^8 + Z^{15}$$

Suy ra xác suất sai sau giải mã của mã *XCB(15,5)* trên kênh BSC là: $P_{ue}(p) = 2^{k-n} A_{C^\perp}(1-2p) - (1-p)^n$



Hình 2.2: Phân bố trọng số của mã XCB(14,6) tạo từ lớp kề ([1],[7],[21])

$$P_{ue}(p) = 15p^7(1-p)^8 + 15p^8(1-p)^7 + p^{15}$$

$$P_{ue}(p) \le P_{ue}(1/2) = \frac{2^k - 1}{2^n} = \frac{2^5 - 1}{2^{15}}$$

Các kết quả tính toán cho thấy $P_{ue}(C,p)$ tăng đơn điệu trong khoảng p=[0, 1/2].

Nhận xét:

*) Có thể chọn mã *(n,m)* hoặc (*n,k*) tối ưu theo *p* để sử dụng (với *p* cho trước).

*) Không có phương pháp tổng quát tìm mã tối ưu theo *p* đã biết (ngoại trừ phương pháp vét cạn).

*) Nếu một mã là tốt theo định nghĩa thì nó cũng đủ tốt cho hầu hết các ứng dụng của mã trong thực tế.

*) Một số lớp mã là tốt, nhưng cũng rất nhiều lớp mã không tốt. Chưa có phương pháp nào chỉ ra điều này.

*) Giới hạn $(2^k-1)/2^n$ và 2^{n-k} được sử dụng làm định nghĩa cho mã tốt.

2.3.4. Các giới hạn tổng quát

2.3.4.1 Một vài giới hạn đánh giá chất lượng của mã khối tuyến tính

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

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

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

2.3.4.2 Các giới hạn dưới

Sử dụng kết quả của từ định lý 2.9 đến định lý 2.14 [62].

2.3.4.3 Các giới hạn trên

Sử dụng kết quả từ định lý 2.16 đến định lý 2.21 [62]

<u>*Ví dụ 6:*</u> Xét mã (8,4,3). Theo định lý 2.16 ta có:

$$P_{ue}(C,p) \leq (2^4-1)p^3(1-p)^{8-3} = 15p^3(1-p)^5$$

2.5. Xác suất không phát hiện sai của mã XCB trên một số kênh truyền.

Ký hiệu *C* là bộ mã *XCB(n,k)*. Xác suất sai sau giải mã xác định theo công thức:

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

(2.60)

Xác suất sai sau giải mã của mã *C* được xác định theo phân bố trọng số $A_i(C)$ của mã *C* như sau:

$$P_{ue}(C) = (1-p)^n \sum_{i=0}^{n} Ai(C) \left[\frac{p}{1-p}\right]^i$$

(2.64)

2.5.3 Xác suất không phát hiện sai của mã *XCB(14,6)*

Phân bố trọng số của mã *XCB(14,6)* xây dựng trên lớp kề ([1],[13],[21])

Phân bố trọng số của mã này như sau (Xem mục 2.2):

A_i=[1 0 0 0 0 12 15 8 15 12 0 0 0 0 0 1]

So sánh xác suất P_{ue} của mã *XCB(14,6)* này trên kênh BSC như hình 2.10.

Phân bố trọng số của mã *XCB(14,6)* xây dựng trên lớp kề ([1],[25],[21]) như sau (xem mục 2.2):

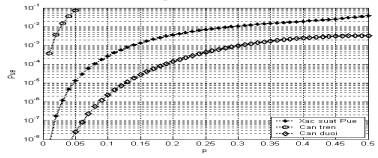
A_i=[1 0 0 0 0 12 15 8 15 12 0 0 0 0 1]

So sánh xác suất P_{ue} của mã *XCB(14,6)* này trên kênh BSC như hình 2.11.

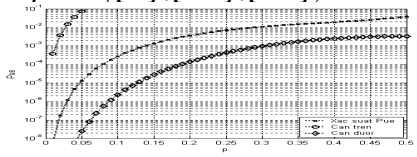
2.5.4 Các cận chất lượng qua mô hình kênh BSC, AWGN, và kênh Pha đinh

2.5.4.1 Mô hình kênh BSC

Theo [60] xác suất giải mã sai, ký hiệu là P_{ue}(C), hay còn gọi là xác suất lỗi giải mã, bằng xác suất của phần bù của sự kiện giải mã đúng, có nghĩa là $P_{ue}(C)$=1- $P_c(C)$. Từ phương trình (1.28) [60], có thể chỉ ra rằng:



Hình 2.11:So sánh xác suất P_{ue} của mã XCB(14,6) tạo từ lớp kề ([1],[13],[21]) trên kênh BSC



Hình 2.12: So sánh xác suất P_{ue} của mã XCB(14,6) tạo từ lớp kề ([1],[25],[21]) trên kênh BSC

$$P_{ue}(C) = 1 - \sum_{i=0}^{\lambda} L_i p^i (1-p)^{n-i}$$

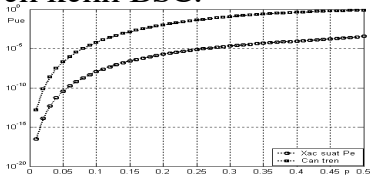
(2.65)

Dựa vào các thảo luận về $P_{ue}(C)$ [60], ta nhận được cận trên biểu diễn dưới dạng:

$$P_{ue}(C) \le \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

(2.66)

dấu bằng xảy ra khi và chỉ khi mã C là một bộ mã hoàn hảo (thỏa mãn cận Hamming với dấu bằng). Hình 2.18 chỉ ra đồ thị theo (2.66) của mã *XCB(20,5)* trên kênh BSC.



Hình 2.18. Đồ thị xác suất $P_{ue}(p)$ cận trên và Pue(p) của mã XCB(20,5) trên kênh BSC.

Từ đồ thị ta thấy rằng mã *XCB(20,5)* luôn cho xác suất không phát hiện sai trên kênh thỏa mãn nhỏ hơn cận trên của P_{ue} (Chất lượng mã trên kênh sẽ tốt hơn). Như vậy mã *XCB(20,5)* đảm bảo chất lượng tốt khi truyền trên kênh BSC.

2.5.4.2 Mô hình 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) [40] và phân bố trọng số *W(C)* với điều chế nhị phân như sau:

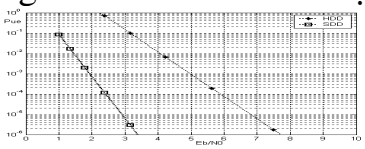
$$P_{ue}(C) \le \sum_{w=d_{\min}}^{n} A_w Q\left[\sqrt{2wR\frac{E_b}{N_0}}\right]$$

(2.67) 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 :

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

Hình 2.19 so sánh các tính toán xác suất giải mã lỗi giải mã quyết định cứng (1.30)[60] và quyết định mềm (2.67) đối với mã *XCB(20,5)*. Giải mã quyết định cứng có thể hiểu như là một



Hình2.19: Kết quả mô phỏng Mã XCB(20,5) đối với giải mã quyết định cứng HDD và giải mã quyết định mềm SDD.

bộ giải mã trên kênh BSC với đầu vào được lấy từ bộ giải điều chế nhị phân. Khi phát qua kênh AWGN ta có kênh BSC tương đương với xác suất lỗi chéo là [22], [34]:

$$p=Q\sqrt{2R\frac{E_b}{N_0}}$$

Hình 2.19 cũng chỉ ra rằng giải mã quyết đinh mềm cho chất lượng tốt hơn giải mã quyết định cứng theo nghĩa là nó cần công suất phát nhỏ hơn tại cùng một giá trị $P_{ue}(C)$. Sai số (tính bằng dB) giữa SNR trên bit tương ứng được gọi là tăng ích mã hóa.

Trong [46], các tác giả đã chỉ ra rằng, đối với mã khối nhị phân hệ thống khi truyền qua kênh

AWGN, xác suất lỗi bit, ký hiệu là $P_b(C)$, có cận cận trên là:

$$P_b(C) = \sum_{w=d_{\min}}^{n} \frac{wA_w}{n} Q\left(\sqrt{2wR\frac{E_b}{N_0}}\right)$$

(2.68) Hình 2.19 chỉ ra kết quả tính cận mã *XCB(20,5)* đối với giải mã quyết định cứng HDD và giải mã quyết định mềm SDD trên kênh AWGN.

2.5.4.3. Mô hình kênh Pha đing Rayleigh phẳng

Một phương pháp tính hàm Q(x) theo hàm mũ (xem [61]) và sau đó tính tích phân hoặc tìm theo cận Chernoff. Kết quả của phương pháp này ta được cận trên không chặt nhưng có thể biểu diễn dưới dạng công thức đơn giản([34], [68]):

$$P_{ue}(C) \le \sum_{w=d_{\min}}^{n} A_w \frac{1}{\left[1+\frac{RE_b}{N_0}\right]^w}$$

(2.69)

Từ các trình bày trong phần này ta thấy rằng mã *XCB(20,5)* thỏa mãn các yêu cầu về cận chất lượng trên các kênh. Do đó mã *XCB(20,5)* cũng là một mã tốt có thể được ứng dụng cho hệ thống truyền tin như các mã xyclic tốt đã biết.

2.6. Kết luận chương hai

1. Phổ trọng số là một tham số quan trọng cần biết khi đánh giá xác suất sai sau giải mã của các mã. Trong chương tác giả đã tìm được phổ trọng số

của các mã *XCB(14, 6), XCB(15, 5), XCB(20, 5)* và *XCB(36, 9)*. Cụ thể tìm được phổ trọng số của các bộ mã với n=12, 14, 15, 20, 36; k= 4, 5, 6, 9. Tìm được xác suất sai sau giải mã và tính được cận trên xác suất sai sau giải mã cho các bộ mã: *XCB(14, 6), XCB(15, 5), XCB(20, 5)* và *XCB(36, 9)*.

2. Trong chương này tác giả đã xây dựng một chương trình xác định phổ trọng số của các mã XCB dựa trên thuật toán vét cạn và chủ yếu xét với các bộ mã có độ dài từ mã chẵn không thể tạo được từ các mã xyclic truyền thống. Trên thực tế chương trình này chỉ khả thi với các giá trị k nhỏ. Với các giá trị k lớn, để giảm nhẹ khối lượng tính toán tác giả đã đưa ra một số nguyên tắc lựa chọn các lớp kề tạo mã trong phân hoạch của vành đa thức theo nhóm nhân xyclic đơn vị.

Có thể thấy rằng đây chỉ là các kết quả ban đầu, để giảm thiểu hơn nữa số các trường hợp cần lựa chọn, cần phải tiếp tục nghiên cứu để xây dựng các tiêu chí chặt chẽ hơn. Chương này cũng xem xét

các cận chất lượng của các mã trên mô hình kênh khác nhau. Các kết quả trong chương này còn được sử dụng trong chương 3.

Chương 3: ĐÁNH GIÁ CHẤT LƯỢNG MÃ XCB TRÊN CÁC KÊNH TRUYỀN TIN

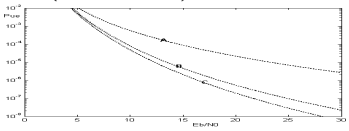
3.1. Phương pháp để chọn mã XCB tốt trên kênh truyền

Từ lý thuyết đã đưa ra trong chương 2 về xác suất không phát hiện sai, ta áp dụng trong phần này để ước lượng (tính) xác suất sai sau giải mã qua một số ví dụ cho các bộ mã sửa sai XCB cụ thể. Từ đó tìm ra các bộ mã XCB tốt trên các kênh truyền tin.

3.1.1. Phương pháp chọn mã XCB tốt

3.1.1.1. Họ mã XCB(20,5)

Đồ thị xác suất sai sau giải mã trên kênh pha đinh phẳng của các mã *XCB(20,5)* xây dựng trên các lớp kề trên (hình 3.1) như sau:



Hình 3.1: Đồ thị xác suất sai sau giải mã trên kênh phađinh phẳng của mã XCB(20,5) xây dựng trên các lớp kề tạo mã.

Như vậy trên đồ thị ta thấy rằng các mã *XCB(20,5)* xây dựng trên các lớp kề tương ứng với đường C sẽ cho chất lượng tin tức tốt trên kênh pha đinh phẳng và các mã xây dựng trên các lớp

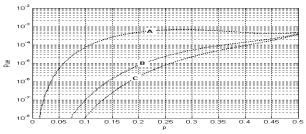
kề này được coi là mã tốt trên kênh pha đinh phẳng.

Đồ thị xác suất sai sau giải mã trên kênh BSC của mã *XCB(20,5)* xây dựng trên các lớp kề trên như sau(hình 3.2).

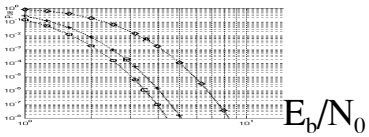
Như vậy các lớp kề tương ứng với đường C sẽ tạo ra mã *XCB(20,5)* tốt trên kênh BSC.

Đồ thị xác suất sai sau giải mã trên kênh AWGN của mã *XCB(20,5)* xây dựng trên các lớp kề trên như hình 3.3.

Như vậy trên kênh AWGN các lớp kề tương ứng với đường C sẽ tạo ra mã *XCB(20,5)* tốt trên kênh AWGN.



Hình 3.2: Đồ thị xác suất sai sau giải mã trên kênh BSC của mã XCB(20,5) tạo từ các lớp kề tạo mã.



Hình 3.3: Đồ thị xác suất sai sau giải mã trên kênh AWGN của mã XCB(20,5 tạo từ các lớp kề tạo mã.

Nhận xét: Qua xét các lớp kề tạo mã *XCB(20,5)* trên các kênh, ta thấy rằng các lớp kề {([1],[3],[7],[11]), ([1],[5],[7],[11]), ([1],[7],[11],[15])}sẽ tạo ra mã *XCB(20,5)* tốt nhất

trên các kênh pha đinh phẳng, kênh BSC và kênh. Các bộ mã này có d_0=9, kiểm tra theo tiêu chuẩn tối ưu Griesmer:

$$n = 20 \geq \sum_{i=0}^{k-1}\left\lceil \frac{d_0}{2^i} \right\rceil = \sum_{i=0}^{4}\left\lceil \frac{9}{2^i} \right\rceil = 9 + \left\lceil \frac{9}{2} \right\rceil + \left\lceil \frac{9}{4} \right\rceil + \left\lceil \frac{9}{8} \right\rceil + \left\lceil \frac{9}{16} \right\rceil = 20$$

Vậy các bộ mã này là các bộ mã tối ưu đạt tiêu chuẩn Griesmer.

Xét tương tự đối với mã *XCB(15, 5),* ta cũng thấy rằng, mã *XCB(15, 5)* tạo từ lớp kề {[1],[7],[11])} trên cả 3 kênh đều cho xác suất sai sau giải mã là nhỏ nhất, bộ mã này có d_0=7. Kiểm tra theo tiêu chuẩn Griesmer:

$$n = 15 \geq \sum_{i=0}^{k-1}\left\lceil \frac{d_0}{2^i} \right\rceil = \sum_{i=0}^{4}\left\lceil \frac{7}{2^i} \right\rceil = 7 + \left\lceil \frac{7}{2} \right\rceil + \left\lceil \frac{7}{4} \right\rceil + \left\lceil \frac{7}{8} \right\rceil + \left\lceil \frac{7}{16} \right\rceil = 15$$

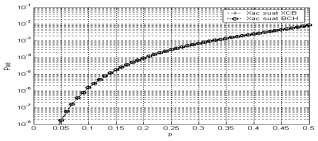
Do đó bộ mã này là bộ mã tối ưu.

Ta xét mã *BCH(15,5)* xây dựng trên trường Galois (2^4) được sinh bởi $p(x)=1+x+x^4$ đa thức sinh của mã này là:

$g(x)=(1+x+x^4)(1+x+x^2+x^3+x^4)(1+x+x^2)=$
$1+x+x^2+x^4+x^5+x^8+x^{10}$

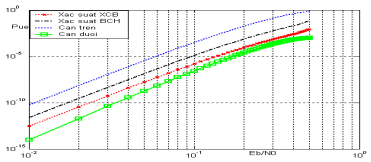
Mã *BCH(15,5)* sửa được 3 lỗi với d_{min}=7. Trọng lượng của đa thức sinh là 7 do vậy khoảng cách nhỏ nhất của mã này là 7.

Các từ mã của mã này được liệt kê trong phần phụ lục. So sánh xác suất sai sau giải mã giữa mã *BCH(15,5,7)* và mã *XCB(15,5,7)* qua Matlab như hình 3.7.



Hình 3.7: So sánh xác suất sai sau giải mã giữa mã BCH(15,5,7) và mã XCB(15,5,7) xét ở trên.

Đồ thị so sánh xác suất không phát hiện sai trên kênh BSC giữa mã *BCH(15,5,7)* và mã *XCB(15,5,7)* với cận trên và cận dưới đánh giá qua Matlab như hình 3.8. Ta thấy rằng hai mã *BCH(15,5,7)* và mã *XCB(15,5,7)* có cùng phân bố trọng số cùng khoảng cách Hamming nhỏ nhất, do đó xác suất không phát hiện sai của hai mã này như nhau. Hay nói một cách khác mã *XCB(15,5,7)* xây dựng trên lớp kề ([1],[7],[11]) có chất lượng tốt tương đương với mã BCH(15,5,7) đã biết. Từ các đồ thị trên các kênh ta thấy rằng mã XCB(15,5) xây dựng trên các lớp kề là mã XCB tốt cho các kênh BSC, AWGN và kênh pha đinh phẳng và cũng tốt so với mã BCH có cùng cấu trúc.



Hình 3.8: Đồ thị so sánh xác suất P_{ue} trên kênh BSC giữa mã BCH(15,5,7) và mã XCB (15,5,7) với cận trên và cận dưới.

3.1.1.4 Họ mã XCB(14, 6)

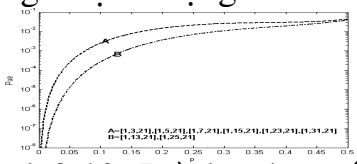
Phân hoạch các lớp kề của mã *XCB(14, 6)* được đưa ra ở phần 2.2.3 mục 2.2. Đồ thị xác suất sai sau giải mã trên kênh BSC của mã *XCB(14, 6)* tạo từ các lớp kề chạy trên Matlab như hình 3.10. Trên đồ thị đường B tương ứng với các lớp kề {([1],[13],[21]), ([1],[25],[21])}. Dựa trên đồ thị ta thấy rằng các lớp kề tạo mã XCB(14, 6) theo đường B cho xác suất sai sau giải mã là nhỏ nhất. Như vậy mã *XCB(14, 6)* tạo từ các lớp kề {([1],[13],[21]), ([1],[25],[21])} là mã tốt trên kênh BSC. Hai bộ mã này có d_0=5, theo tiêu chuẩn Griesmer:

$$n = 14 \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_0}{2^i} \right\rceil = \left\lceil \frac{5}{1} \right\rceil + \left\lceil \frac{5}{2} \right\rceil + \left\lceil \frac{5}{4} \right\rceil + \left\lceil \frac{5}{8} \right\rceil + \left\lceil \frac{5}{16} \right\rceil + \left\lceil \frac{5}{32} \right\rceil = 13$$

Do vậy hai bộ mã này gần đạt tối ưu theo tiêu chuẩn Griesmer.

3.1.2 Nhận xét

Qua xét các ví dụ với các họ mã XCB trên ta thấy rằng khi biết phân bố trọng số của mã ta có thể đánh giá định lượng chất



Hình 3.10: Đồ thị xác suất sai sau giải mã trên kênh BSC của mã XCB(14,6) tạo từ các lớp kề.

lượng của mã bằng tham số xác suất sai sau giải mã. Từ đó có thể đánh giá theo xác suất sai sau giải mã của các lớp kề tạo mã XCB ta có thể chọn

được lớp kề tạo mã XCB tốt như các mã tuyến tính đã biết và tốt trên các kênh truyền tin.

3.2. Đánh giá mã XCB(14,6) theo hai sơ đồ giải mã ngưỡng

3.2.1. Mã xyclic cục bộ (14,6)

Mã *XCB(14,6)* xây dựng trên vành đa thức x^6+1, các lớp kề của vành Z_{63} xây dựng thành các lớp kề của nhóm nhân xyclic cấp 6. Dựa vào các tổng kiểm tra có khả năng trực giao của mã này ta xây dựng được các sơ đồ giải mã đảm bảo khoảng cách mã d_0=5 (sửa được hai sai ngẫu nhiên). Đó là các sơ đồ hai cấp ngưỡng và sơ đồ một cấp ngưỡng.

3.2.2. Hai sơ đồ giải mã cho mã XCB (14,6)

3.2.2.1 Sơ đồ hai cấp ngưỡng: Sơ đồ này cần $(n+k+k/2)$=23 nhịp để giải mã cho 6 dấu thông tin. So với sơ đồ giải mã nhanh, sơ đồ này cần thêm $k/2$ nhịp, nhưng sơ đồ giải mã đơn giản hơn rất nhiều.

3.2.2.2 Sơ đồ một cấp ngưỡng

Dựa trên hệ thống kiểm tra 2 liên hệ ta có thể xây dựng được sơ đồ giải mã ngưỡng dùng một cấp ngưỡng. Ta biết rằng số tổng kiểm tra λ liên hệ lớn nhất có thể thiết lập được bằng:

$$J_{\max} = \left[\frac{(n-1)\lambda}{\Delta}\right]$$

Trong đó: λ : số bậc liên hệ; $[x]$ là phần nguyên của x.

Δ: số dấu mã nằm trong một tổng kiểm tra (không kể dấu cần giải mã).

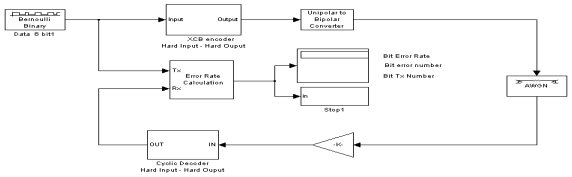
Trong trường hợp mã XCB(14,6) ta có:

$$J_{\max} = \left\lfloor \frac{(14-2)2}{3} \right\rfloor = 8$$

Trong khi đó số tổng kiểm tra phải thiết lập được để đảm bảo d_0=5 là: $J = \lambda(d_0 - 2) + 1 = 2(5-2) + 1 = 7$

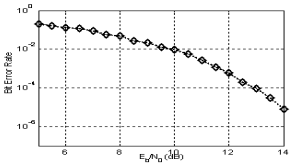
3.2.3 Mô phỏng mã XCB(14,6)

3.2.3.1 Sơ đồ mô phỏng cho mã XCB(14,6) với một cấp ngưỡng



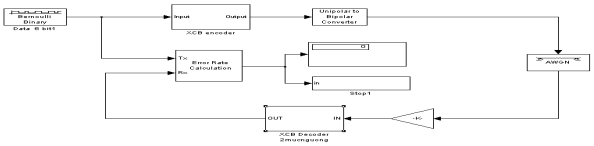
Hình 3.16: Sơ đồ mô phỏng GMĐS một cấp ngưỡng cho mã XCB(14,6) trên kênh AWGN.

Đồ thị mô phỏng giải mã một cấp ngưỡng cho mã XCB(14,6) trên kênh AWGN như sau:



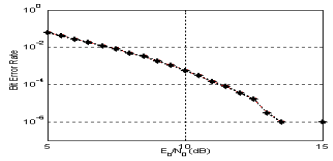
Hình 3.17: Đồ thị chất lượng GMĐS một cấp ngưỡng cho mã XCB(14,6) trên kênh AWGN.

3.2.3.2. Sơ đồ mô phỏng cho mã XCB(14,6) vơi giải mã hai cấp ngưỡng.

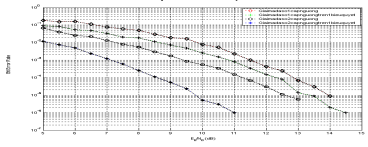


Hình 3.18: Sơ đồ mô phỏng GMĐS hai cấp ngưỡng cho mã XCB(14,6) trên kênh AWGN.

Đồ thị giải mã 2 cấp ngưỡng trên kênh AWGN như sau:



Hình 3.19: Đồ thị chất lượng GMĐS hai cấp ngưỡng cho mã XCB(14,6) trên kênh AWGN.



Hình 3.20: Đồ thị so sánh giữa sơ đồ GMĐS 1 cấp ngưỡng, giải mã trên đa số 1 biểu quyết 1 cấp ngưỡng và sơ đồ GMĐS 2 cấp ngưỡng, giải mã trên đa số 1 biểu quyết 2 cấp ngưỡng.

Từ đồ thị chất lượng của hai bộ giải mã một cấp ngưỡng và hai cấp ngưỡng ta thấy rằng sơ đồ giải mã hai cấp ngưỡng cho chất lượng giải mã tốt hơn so với sơ đồ giải mã một cấp ngưỡng. Nhưng với sơ đồ giải mã một cấp ngưỡng khi giải ra 6 dấu thông tin chỉ cần 14 nhịp để nạp dấu mã và 6 nhịp để giải 6 dấu thông tin, như vậy cần 20 nhịp để giải ra 6 dấu thông tin. Còn với sơ đồ giải mã hai cấp ngưỡng thì cần 14 nhịp để nạp 14 dấu mã, 6 nhịp để giải ra 3 cặp dấu 1.8, 2.16, 4.32 và 6 nhịp để giải ra 6 dấu thông tin. Như vậy cần 24 nhịp để giải ra 6 dấu thông tin. Do đó bộ giải mã hai cấp ngưỡng cho chất lượng giải mã tốt hơn bộ

giải mã một cấp ngưỡng, nhưng tốc độ giải mã sẽ chậm hơn bộ giải mã một cấp ngưỡng. Trên đồ thị chất lượng ta còn thấy rằng giải mã ngưỡng theo đa số trên 1 biểu quyết cho chất lượng giải mã tốt hơn giải mã ngưỡng đa số 1 biểu quyết. Do vậy khi chọn giải mã ngưỡng cho mã XCB(14,6) nói riêng và mã XCB nói chung, ta nên chọn giải mã ngưỡng đa số trên 1 biểu quyết.

3.3. Kết luận chương 3

1. Qua kết quả khảo sát một số bộ mã trên các vành $Z_2(x)/(x^5+1)$ và $Z_2(x)/(x^6+1)$, tìm được các mã XCB có độ dài chẵn (20,5,9) và (14,6,5) là các mã tối ưu và gần tối ưu.

2. Chứng tỏ rằng mã *XCB (15,5,7)* trên vành $Z_2(x)/(x^5+1)$ tương đương với mã xyclic truyền thống trên vành $Z_2(x)/(x^5+1)$ và có chất lượng tốt tương đương như mã *BCH(15,5,7)* đã biết.

3. Chất lượng giải mã còn phụ thuộc vào việc lựa chọn sơ đồ giải mã cụ thể. Vấn đề này được xem xét thông qua ví dụ giải mã ngưỡng cho mã (14,6,5) với 4 sơ đồ giải mã cụ thể là giãi mã với một cấp ngưỡng theo hai mức ngưỡng khác nhau

(giải mã đa số và giải mã trên đa số một biểu quyết) và giải mã với 2 cấp ngưỡng theo 2 mức ngưỡng khác nhau.

KẾT LUẬN VÀ KIẾN NGHỊ

1. Các kết quả của luận án

Luận án đã đạt được những kết quả sau:

1. - Phổ trọng số là một tham số quan trọng cần biết khi đánh giá xác suất sai sau giải mã của các mã. Trong luận án tác giả đã tìm được phổ trọng số của các mã *XCB(14,6), XCB(15,5), XCB(20,5) và XCB(36,9),* tương ứng với các bộ mã có n=12, 14, 15, 20, 36; k=4, 5, 6, 9. Tìm được xác suất sai sau giải mã và tính được cận trên xác suất sai sau giải mã cho các bộ mã: *XCB(14,6), XCB(15,5), XCB(20,5)* và *XCB(36,9)*. Kết quả với bộ mã XCB(14,6) xây dựng trên lớp kề {([1],[13],[21])}, {([1],[25],[21])} có xác suất sai từ 10^{-8} đến 10^{-4} khi xác suất sai trên kênh $0 < p < 0,2$ và gần đạt tiêu chuẩn tối ưu Griesmer; Bộ mã

XCB(15,5) xây dựng trên lớp kề {([1], [7], [11])} đạt được xác suất sai sau giải mã từ 10^{-4} đến 10^{-8} khi tỷ số tín trên tạp trên kênh $10 < \frac{E_b}{N_0} < 35$, thỏa mãn tiêu chuẩn tối ưu Griesmer và đạt chất lượng tương đương với mã *BCH (15,5)* đã biết; 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 giai mã từ 10^{-4} đến 10^{-8} khi tỷ số tín trên tạp $1,2 < \frac{E_b}{N_0} < 10$ và gần đạt tiêu chuẩn tối ưu Griesmer; Bộ mã *XCB(36,9)* xây dựng trên các lớp kề {([1],[19],[21],[508])},{([1],[21],[25],[508])},{([1],[482],[468],[502])},{([1],[466],[460],[508])} đạt xác suất sai nhỏ hơn 10^{-6} khi xác suất sai trên kênh $0,15 < p < 0,5$ và gần thỏa mãn tiêu chuẩn tối ưu Griesmer.

- Để giảm nhẹ khối lượng tính toán khi tham số *k* lớn, trong luận án tác giả cũng đưa ra một số

nguyên tắc lựa chọn các lớp kề tạo mã trong phân hoạch của vành đa thức theo nhóm nhân xyclic đơn vị:

*) Không chọn 2 lớp đối xứng (vì hai lớp đối xứng sẽ tạo ra 1 mã đảo Bauer có d_0=4).

*) Chọn các lớp có $d_0 \le \sum_{i=1}^{s-1} W_i + 1$ đối với mã hệ thống (chọn theo lớp kề đơn vị) trong đó s là số lớp kề, W_i là trọng số của đa thức trưởng lớp kề.

*) Không chọn tất cả các lớp kề có W_i là chẵn (vì nếu chọn W_i chẵn thì khi đó $d_0 \le k$).

2 - Luận án đã tìm được các mã tốt nhất trong các họ mã XCB trên một số vành cụ thể cho các kênh BSC và AWGN, xây dựng được sơ đồ mô phỏng đánh giá hiệu quả của các sơ đồ giải mã ngưỡng một cấp và giải mã ngưỡng hai cấp với các mức ngưỡng khác nhau: giải mã đa số và giải mã trên đa số 1 biểu quyết trên kênh AWGN thông qua ví dụ khảo sát cho mã *XCB(14,6,5)*. Qua kết quả mô phỏng cũng chứng tỏ rằng: chất lượng giải

mã không những phụ thuộc vào cách chọn mã mà còn phụ thuộc vào sơ đồ giải mã.

2. Kiến nghị.

1. Tiếp tục ứng dụng công nghệ mới để đưa các bộ mã có khả năng sửa sai tốt vào trong các mạng thông tin chuyên dụng.

2. Đưa ra các giải pháp kỹ thuật để nâng cao khả năng sửa sai của mã XCB bằng các bộ điều chế nhiều mức. Phát triển kết quả nghiên cứu tìm ra các tiêu chí mới khác để đánh giá và tạo ra các bộ mã XCB mới có khả năng sửa sai tốt.

3. Tiếp tục hoàn thiện các kết quả còn chưa hoàn chỉnh trong luân án bao gồm:

- Xây dựng các thuật toán chọn các lớp kề tạo mã cụ thể và chặt chẽ hơn nhằm giảm bớt khối lượng tính toán khi tìm mã trong các phân hoạch khác nhau.

- Mô phỏng trên các sơ đồ giải mã khác nhau cho các bộ mã khác nhau bao gồm cả các bộ mã có số tổng kiểm tra lẻ nhằm đi tới những kết luận chính xác tổng quát hơn khi áp dụng vào trong thực tế cho hiệu quả cao. Nghiên cứu các sơ đồ giải mã cứng có lặp.

- Nghiên cứu tìm công thức tổng quát tính phân bố trọng số cho mã XCB hoặc cho một vài họ mã XCB đặc biệt.