BỘ GIÁO DỤC VÀ ĐÀO TẠO **TẬP ĐOÀN BCVT VIỆT NAM**

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

****

ĐẶNG HOÀI BẮC

CÁC MÃ CYCLIC VÀ CYCLIC CỤC BỘ TRÊN VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

Chuyên ngành: Kỹ thuật viễn thông
Mã ngành: 62 52 70 05

TÓM TẮT LUẬN ÁN TIẾN SỸ KỸ THUẬT

HÀ NỘI 8/2010

Công trình được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học:

GS.TSKH. Nguyễn Xuân Quỳnh

Phản biện 1: PGS.TS. Bạch Nhật Hồng

Phản biện 2: PGS.TS. Phạm Minh Hà

Phản biện 3: PGS.TS. Hoàng Thọ Tu

Luận án được bảo vệ trước Hội đồng chấm luận án cấp Nhà nước
tại Hội trường 2, Học viện Công nghệ Bưu chính Viễn thông,
122 Hoàng Quốc Việt, Cầu Giấy, Hà nội.
vào hồi: 16 giờ 00 ngày 14 tháng 6 năm 2010

Có thể tìm hiểu luận án tại:

1. Thư viện Quốc gia
2. Thư viện Học viện Công nghệ Bưu chính Viễn thông

DANH MỤC CÔNG TRÌNH CỦA TÁC GIẢ

[1] Nguyen Binh, Dang Hoai Bac, (2004). "Cyclic codes over extended rings of polynomial rings with two cyclotomic cosets". REV-04. November 20-23, 2004, Hanoi, Vietnam

[2] Đặng Hoài Bắc, Nguyễn Bình, (2006) "Tạo dãy m bằng phương pháp phân hoạch trên vành đa thức có hai lớp kề cyclic". Hội nghị khoa học lần thứ 8, Học viện Công nghệ BCVT, 09/2006.

[3] Dang Hoai Bac, Ngo Duc Thien, Nguyen Binh, Young-Hoon Kim, (2007) "PAPR Reduction of Novel Cyclic Codes in OFDM Systems". The 10th ICT Seminar. Organized by PTIT and ETRI. Sept-12th, 2007. Hanoi, Vietnam.

[4] Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh , Young Hoon Kim (2007). "Ploynomial rings with two cyclotomic cosets and their applications in Communication", MMU International Symposium on ICT 2007, Malaysia, ISBN: 983-43160-0-3.

[5] Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh, (2007) "Decomposition in polynomial ring with with two cyclotomic cosets". 36th AIC, November 18-23, 2007, Manila.

[6] Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh, (2007), "Novel Algebraic Structure for Cyclic Codes", Applied Algebra, Algebraic Algorithms, and Error Correcting Codes –Conf. AAECC 17, LNCS 4851, pp 301-310, December, 2007, Springer-Verlag Berlin Heidelberg.

[7] Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh, (2007) "New Algebraic Structure Based on Cyclic Geometric Progressions over Polynomial Ring Applied for Cryptography" IEEE, International Conference on Computational Intelligence and Security (CIS) CIS'07, December 15-19, 2007, Harbin, China.

[8] Dang Hoai Bac, Le Ngoc Hung, (2008), "Using cyclic code in WCDMA cell search algorithm". Journal on Information & Communications and Technologies (Tạp chí chuyên san ICT tiếng Anh) ISSN: 0866-7039, issue 3, pp34-38, June 2008.

[9] Ngo Duc Thien, Dang Hoai Bac, Nguyen Binh, (2008), "Constructing Local Cyclic Code Based on Compound Decompositions of Two Polynomial Rings", The second International Conference on Communication and Electronics – (ICCE-2008), June 04th-06th, 2008, HoiAn, Vietnam.

[10] Ngô Đức Thiện, Đặng Hoài Bắc, Nguyễn Bình, (2008), "Đánh giá hiệu quả của mã cyclic cục bộ so với mã cyclic truyền thống", Tạp chí Khoa học & Công nghệ các trường Đại học kỹ thuật, số 67-2008.

MỞ ĐẦU

Lý do nghiên cứu

Việc nghiên cứu truyền thống về mã cyclic đã khá hoàn chỉnh, tuy nhiên vẫn chưa có công trình nào khảo sát tổng quát về phương diện lý luận và đề xuất phương pháp chung xây dựng mã trên vành đa thức có hai lớp kề cyclic. Đây là vành đa thức đặc biệt vì trong phân tích x^n+1 của vành chỉ gồm hai đa thức bất khả quy, dẫn đến rất ít bộ mã tốt có thể tạo ra trên vành này. Việc khảo sát tường minh về vành đa thức có hai lớp kề cyclic vẫn là một vấn đề mở.

Mục đích nghiên cứu

Mục đích nghiên cứu của luận án là khảo sát đặc điểm của vành đa thức có hai lớp kề cyclic và đề xuất một số cấu trúc đại số xây dựng mã trên vành đa thức này. Dựa trên các kết quả nghiên cứu, luận án cũng đưa ra một số ứng dụng trong các bài toán viễn thông.

Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của luận án là vành đa thức có hai lớp kề cyclic và các cấu trúc đại số để xây dựng mã trên vành đa thức này.

Phạm vi nghiên cứu của luận án này được giới hạn trong việc nghiên cứu các đặc điểm và cấu trúc của vành đa thức có hai lớp kề cyclic, tập trung nghiên cứu các cấu trúc đại số để khắc phục những hạn chế trong việc tạo mã của vành đa thức có hai lớp kề cyclic, tìm

ra các cấu trúc để xây dựng mã trên các vành đa thức chẵn.

Phương pháp và công cụ nghiên cứu

Phương pháp nghiên cứu tổng hợp và phân tích để tìm ra các cấu trúc đại số để xây dựng mã cyclic và các ứng dụng trên vành đa thức có hai lớp kề cyclic, qua đó góp phần hoàn thiện cấu trúc đại số của mã cyclic và đưa ra các điểm ưu việt trong cấu trúc mới.

Luận án sử dụng các công cụ toán học và các công cụ của lý thuyết mã, công nghệ tích hợp số FPGA và một số công cụ mô phỏng để giải quyết, minh chứng cho tính khả thi của nghiên cứu.

Ý nghĩa khoa học và thực tiễn của đề tài

Luận án là một công trình nghiên cứu tương đối hoàn chỉnh về vành đa thức có hai lớp kề cyclic. Những đóng góp mới của luận án là xây dựng thuật toán xác định điều kiện để vành đa thức là vành đa thức có hai lớp kề cylic. Xây dựng mã trên các vành đa thức có hai lớp kề cyclic theo các cấu trúc nhóm nhân, cấp số nhân. Với vành chẵn, vành mở rộng của vành đa thức có hai lớp kề cyclic, tác giả đưa ra phương pháp phân hoạch theo lớp các phần tử liên hợp của lũy đẳng nuốt để tạo mã. Dựa trên các cấu trúc đại số mới, tác giả đề xuất phương án giải quyết một số vấn đề trong viễn thông như giảm PAPR, tìm kiếm cell, tạo dãy m và xây dựng hệ mật luân hoàn.

Cấu trúc của Luận án

Luận án bao gồm phần mở đầu, kết luận và 04 chương nội dung. Chương 1 trình bày tổng quan về mã cyclic và một số xu hướng đã được nghiên cứu liên quan đến luận án, những điểm hạn chế trong của vành đa thức có hai lớp kề cyclic. Chương 2 đề cập đến đặc điểm và cách nhận biết vành đa thức có hai lớp kề cyclic, khảo sát các phân hoạch trên vành đa thức này. Chương 3 đề xuất một số phương pháp xây dựng mã cyclic trên vành đa thức có hai lớp kề cyclic theo cấu trúc đại số mới; xây dựng mã trên vành mở rộng, vành đa thức chẵn. Chương 4, dựa trên các cấu trúc đại số của vành đa thức có hai lớp kề cyclic, đề xuất một số ứng dụng trong bảo mật, giải quyết bài toán giảm tỷ số công suất cực đại trên công suất trung bình PAPR trong hệ thống OFDM, đưa ra thuật toán xây dựng dãy m, tìm kiếm cell ở hướng xuống trong hệ thống WCDMA.

CHƯƠNG 1
TỔNG QUAN

1.1. MỞ ĐẦU

Nhìn chung, các cấu trúc đại số truyền thống trong việc xây dựng mã khối tuyến tính cũng như kỹ thuật mã hóa và giải mã về cơ bản đã được hoàn thiện vào thập kỷ 70 của thế kỷ 20. Tuy nhiên những nghiên cứu trong việc tìm ra các cấu trúc đại số mới vẫn tiếp tục được tiến hành góp phần hoàn thiện thêm lý thuyết

mã và mở ra những ứng dụng hiệu quả hơn trong các bài toán viễn thông.

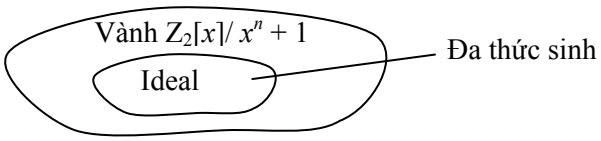
1.2. TÌNH HÌNH NGHIÊN CỨU CÁC VẤN ĐỀ LIÊN QUAN ĐẾN LUẬN ÁN

Mã cyclic được Eugene Prange nghiên cứu đầu tiên năm 1957. Sau đó quá trình nghiên cứu về mã cyclic tập trung theo cả hai hướng sửa lỗi ngẫu nhiên và sửa lỗi cụm. Rất nhiều lớp mã cyclic đã được xây dựng trong những năm này, bao gồm các mã BCH, các mã Reed-Solomon, các mã hình học Euclidean. Một trong các hướng nghiên cứu trên thế giới hiện nay là đánh giá một số giới hạn mã cyclic hoặc đề xuất phương án giải mã tối ưu cho mã cyclic. Một số nghiên cứu đề cập đến mã tuyến tính và đặc tính của đa thức sinh trên cấu trúc trellis.

Tại Việt Nam, mở đầu một hướng nghiên cứu mới về mã sửa sai đó là mã cyclic cục bộ LCC (Local Cyclic Code). Các mã LCC xây dựng theo các nhóm nhân và cấp số nhân trên vành đa thức. Bên cạnh đó là các nghiên cứu tường minh về các phương pháp giải mã ngưỡng theo các hệ tổng kiểm tra trực giao. Các công trình này đều có ý nghĩa về mặt lý thuyết, đề xuất được cấu trúc đại số mới trên vành đa thức như phân hoạch, nhóm nhân, cấp số nhân.

1.3. HẠN CHẾ CỦA VIỆC XÂY DỰNG MÃ CYCLIC TRÊN VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

Như ta đã thấy, theo lý thuyết mã cổ điển, mỗi Ideal tương ứng của một vành đa thức sẽ xây dựng được một bộ mã cyclic. Trong một vành đa thức, Ideal I gồm các đa thức là bội của một đa thức g(x), trong đó g(x) là ước của đa thức $x^n + 1$: $(g(x)) \mid x^n + 1$ hay $x^n + 1 : g(x)$.



Hình 1.1: Phân hoạch vành theo Ideal

Theo phương pháp cổ điển này thì rõ ràng là số bộ mã bị hạn chế (do số đa thức sinh ít). Đặc biệt với vành đa thức có hai lớp kề cyclic sự hạn chế này càng được thể hiện rõ hơn, bởi vì trong phân tích $x^n + 1$ của vành đa thức này chỉ có hai thành phần:

$$x^n + 1 = (x + 1) \sum_{i=0}^{n-1} x^i$$

Số đa thức sinh g(x) có thể thiết lập được từ t đa thức bất khả quy trong phân tích nhị thức $x^n + 1$ được xác định: $I = \sum_{i=1}^{t-1} C_t^i = 2$

Như vậy, số các đa thức sinh g(x) có thể có trên vành đa thức có hai lớp kề cyclic cũng chỉ là 3. Ta chỉ xây dựng được hai bộ mã cyclic tầm thường là mã kiểm tra chẵn (n, n-1) có đa thức sinh g(x) = 1+x với khoảng cách mã d_0=2 và mã lặp (n,1) có đa thức sinh g(x) = $e_o(x)=\sum_{i=0}^{n-1} x^i$ với d_0 = n.

Với những hạn chế trên, trong các công trình nghiên cứu về mã cyclic trên trường GF(2), việc xây dựng mã trên vành đa thức có hai lớp kề cyclic hầu như chưa được đề cập.

1.4. KẾT LUẬN CHƯƠNG

Vì những hạn chế trong việc tạo đa thức sinh, việc xây dựng mã trên vành đa thức có hai lớp kề cyclic chưa xuất hiện trong các tài liệu từ trước đến nay. Đây chính là lý do nghiên cứu của luận án, với mục đích nhằm góp phần phong phú, hoàn thiện hơn về mặt cấu trúc đại số trong lý thuyết mã. Những ứng dụng cụ thể của các mã được xây dựng trên vành đa thức có hai lớp kề cyclic được đề cập trong luận án như một minh chứng cho những ưu điểm của cấu trúc đại số mới được sử dụng trong việc xây dựng mã trên vành đa thức này.

CHƯƠNG 2
XÁC ĐỊNH CÁC ĐẶC ĐIỂM CỦA VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

2.1. MỞ ĐẦU

Trong chương này, chúng ta sẽ đưa ra định nghĩa thế nào là vành đa thức có hai lớp kề cyclic, tìm các điều kiện, xây dựng thuật toán tìm điều kiện để vành đa thức có hai lớp kề cyclic và khảo sát các phân hoạch trên vành đa thức có hai lớp kề cyclic.

2.2. VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

Định nghĩa 2.1: *Vành đa thức theo modulo x^n+1 được gọi là vành đa thức có hai lớp kề cyclic nếu phân tích của x^n+1 thành tích của các đa thức bất khả quy trên trường GF(2) có dạng sau:*

$$x^n + 1 = (x + 1) \sum_{i=0}^{n-1} x^i \tag{2.1}$$

Trong đó (x+1) và $e_o(x) = \sum_{i=0}^{n-1} x^i$ là các đa thức bất khả quy.

Vành đa thức có hai lớp kề cyclic chỉ có 2 chu trình:

$$C_0 = \{0\},\ C_1 = \{1, 2, 2^2, ..., 2^{n-2}\} \text{ trong đó } 2^{n-1} \equiv 1 \bmod n \tag{2.2}$$

Bổ đề 2.1: *Vành đa thức theo modulo x^n+1 là một vành đa thức có hai lớp kề cyclic nếu* ***n*** *thoả mãn:*

- ***n** phải là một số nguyên tố;*
- *phần tử thứ hai phải thoả mãn điều kiện $2^{\varphi(n)/p} \neq 1 \bmod n$ với mỗi ước nguyên tố p của $\varphi(n)$. ($\varphi(n)$ là hàm phi Euler)*

Từ định nghĩa trên, ta thấy rằng $\text{ord}^n 2 = m_1 \leq n-1$. Để phần tử 2 có cấp n-1, phần tử thứ hai phải thoả mãn điều kiện $2^{\varphi(n)/p} \neq 1 \bmod n$, với mỗi p là ước nguyên tố của $\varphi(n)$. Với $\varphi(n) = n-1$ khi n là một số nguyên tố. Căn cứ đặc điểm trên ta xây dựng thuật toán như sau.

Thuật toán xác định giá trị *n* của vành đa thức hai lớp kề cyclic

Vào: số nguyên tố n

Bước 1:tìm phân tích của (n-1); xác định ước nguyên tố p_i.

Bước 2: với mỗi p_i tính $2^{n-1/p_i}$

- Nếu tồn tại p_i sao cho $2^{n-1/p_i} \equiv 1 (\bmod n)$ thì n không thoả mãn.

- n thoả mãn trong các trường hợp còn lại.

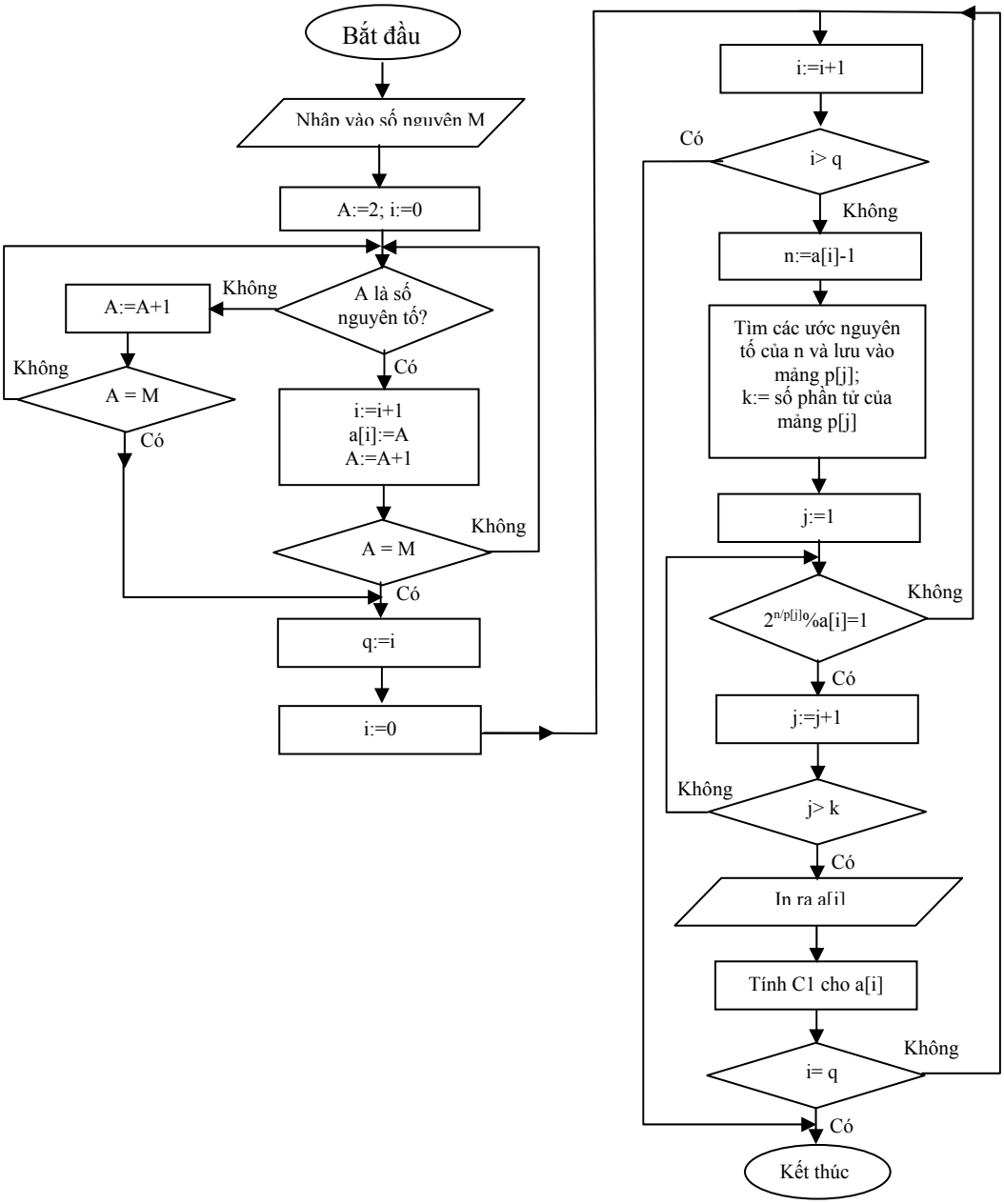
Ra: Giá trị n thoả mãn.

2.3. CÁC KIỂU PHÂN HOẠCH VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

Trên vành đa thức có hai lớp kề cyclic, các dạng phân hoạch cũng tương tự như trên các vành đa thức khác, tuy nhiên do đặc điểm nên sự phân hoạch trên

vành này sẽ phụ thuộc vào cấp cực đại của phần tử trên vành, ta sẽ có các phân hoạch sau:

Lưu đồ thuật toán



- Phân hoạch chuẩn, phân hoạch cực đại, phân hoạch cực tiểu
- Phân hoạch vành thành các cấp số nhân có cùng trọng số
- Phân hoạch vành đa thức thành các cấp số nhân với các phần tử có cùng tính chẵn lẻ của trọng số
- Phân hoạch vành đa thức thành các cấp số nhân với các phần tử có cùng tính chẵn lẻ của trọng số
- Phân hoạch vành đa thức thành cấp số nhân theo modulo h(x)

2.4. KẾT LUẬN CHƯƠNG

Chương này đã xây dựng được thuật toán và lập chương trình tính toán các giá trị n để vành đa thức thỏa mãn điều kiện có hai lớp kề cyclic với n <10.000 và trình bày về các cơ sở phân hoạch theo cấu trúc đại số trên vành đa thức có hai lớp kề cyclic.

CHƯƠNG 3
MỘT SỐ PHƯƠNG PHÁP XÂY DỰNG MÃ CYCLIC VÀ MÃ CYCLIC CỤC BỘ TRÊN VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

3.1. MỞ ĐẦU

Chương ba sẽ đưa ra các phương pháp xây dựng, đánh giá và mô phỏng các mã cyclic trên các vành đa thức có hai lớp kề cyclic và trên vành mở rộng của nó dựa trên các phân hoạch đã đề cập ở chương hai.

3.2. XÂY DỰNG MÃ CYCLIC TRÊN VÀNH ĐA THỨC CÓ HAI LỚI KỀ CYCLIC

3.2.1 Xây dựng mã trên vành đa thức có hai lớp kề cyclic theo cấu trúc nhóm nhân cyclic CMG (CMG: Cyclic Multiplycative Group)

Định nghĩa 3.1: *Nhóm nhân CMG A trên vành đa thức* $\mathbf{Z}_2[x]/(x^n+1)$ *được thiết lập như sau:*

$$A = \left\{ a^i(x) \bmod (x^n+1), i = \overline{1:k} \right\}. \quad \textit{(k: cấp của a(x))} \tag{3.1}$$

Xem xét CMG $A = \{a^i(x)\}$, số lượng các phần tử có thể có của A sẽ là: $|A| = k$. Chúng ta sẽ tạo ra mã cyclic theo định nghĩa sau:

Định nghĩa 3.2: *Mã cyclic dựa trên CMG với chiều dài k chính là mã với các dấu mã là các phần tử của CMG*

Ma trận sinh có dạng như sau: $G = \left[a(x) a^2(x) \ldots a^k(x) \right]$. (3.2)

Nếu $I = \{x^i\} \in A$ thì mã được tạo ra bởi A sẽ là mã đối xứng.

Nếu $a(x) = \sqrt[j]{x}$ thì phần tử thuộc hàng thứ i^{th} của G chính là dịch vòng của hàng thứ $(i-1)^{th}$ về phía bên phải j vị trí.

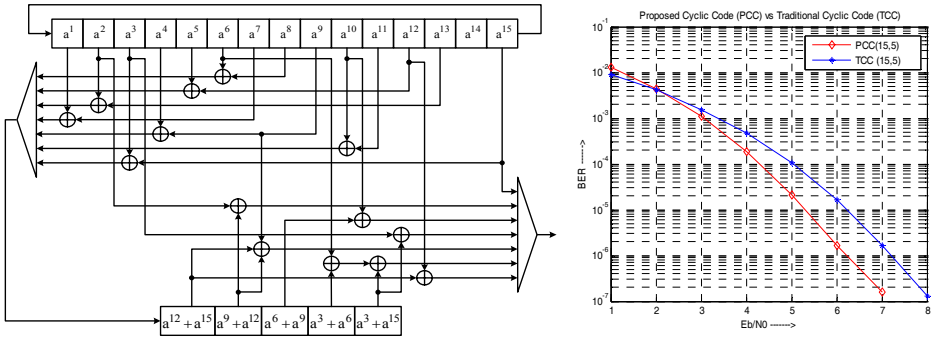
Ta sẽ xem xét việc xây dựng mã trên vành đa thức $\mathbf{Z}_2[x]/(x^5+1)$.

Chọn a(x)= $1+x^2+x^4$, ta có nhóm nhân CMG A: $A=\{a^i(x)\}$

$$=\{(024),(034),(1),(013),(014),(2),(124),(012),(3),(023),(123),(4),(134),(234),(0)\}$$

Ta có mã hệ thống với ma trận sinh như sau:

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



Hình 3.1: Sơ đồ giải mã cyclic (15, 5) và đặc tính BER của TCC và PCC (15,5)

Khả năng xây dựng mã theo CMG phụ thuộc a(x) và cấp a(x). Kết quả mô phỏng so sánh tỉ số lỗi bit BER giữa mã cyclic được đề xuất PCC và mã cyclic truyền thống TCC trên kênh AWGN như hình 3.1.

M

1+x

B

3.2.2. Xây dựng mã vành đa thức có hai lớp kề theo phân hoạch

Việc phân hoạch vành đa thức theo lớp kề, theo nhóm nhân đơn vị hoặc phân hoạch cực đại giúp việc xây dựng mã linh hoạt, tổng quát.

Xét n = 5. Phân hoạch theo nhóm đơn vị I ta có 7 lớp kề như sau:

Bảng 3.1: Phân hoạch của $\mathbf{z}_2[x]/(x^5+1)$ theo nhóm nhân đơn vị I

(0)	(1)	(2)	(3)	(4)
(01)	(12)	(23)	(34)	(04)
(02)	(13)	(24)	(03)	(14)
(012)	(123)	(234)	(034)	(014)
(013)	(124)	(023)	(134)	(024)
(0123)	(1234)	(0234)	(0134)	(0124)
(01234)	*(Ký hiệu: $1+x^2$ =(02))*			

Từ mã (15,5) từ các trưởng lớp kề {(0), (012),

(0)	(1)	(2)	(3)	(4)	(012)	(123)	(234)	(034)	(014)	(013)	(124)	(023)	134)	(024)

(013)} có dạng sau:

Chỉ với bộ mã này ta đã có thể tạo ra $M = 2^3.5^3.3! = 6.000$ bộ mã có cùng tham số.

Số các mã có thể lập trên các phân hoạch của vành $\mathbf{Z}_2[x]/(x^5+1)$:

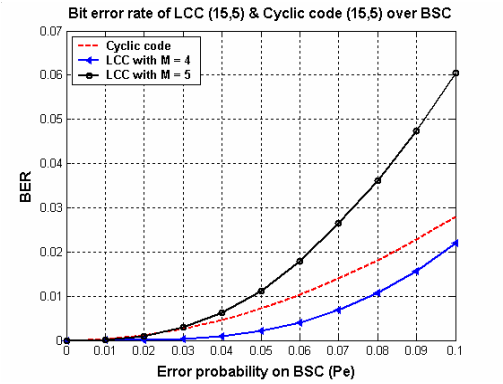
$N = C_6^0 + C_6^1.2.5 + C_6^2.2!.2^2.5^2 + C_6^3.3!.2^3.5^3 + C_6^4.4!.2^4.5^4$
$+ C_6^5.5!.2^5.5^5 + C_6^6.6!.2^6.5^6 \Rightarrow N = 795.723.061$ mã

Trong đó, số mã (15,5) có thể xây dựng trên phân hoạch chuẩn là:

$$N_1 = C_6^3.3!.2^3.5^3 = 6.8.125.\frac{6.5.4}{3.2} = 120.000$$

Số mã hệ thống (15,5): $N_2 = C_6^2.3!.2^3.5^3 = 6.8.125.\frac{6.5}{2} = 90.000$

Như vậy chúng ta thấy số lượng mã được tạo ra với số lượng vượt trội so với số lượng bộ mã được tạo ra theo các cấu trúc truyền thống.



Hình 3.2: Tỷ số lỗi bit của LCC (15,5) và mã cyclic (15,5) truyền thống trên kênh BSC (với pe < 0,1).

3.3. MÃ TRÊN VÀNH MỞ RỘNG CỦA VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

3.3.1. Các thặng dư bậc 2 và các căn bậc 2 của chúng

Định nghĩa 3.3: *Đa thức f(x) được gọi là thặng dư bậc 2 (quadratic residue - QR) trong Z_{2n} nếu tồn tại đa thức g(x) sau:*

$$g^2(x) \equiv f(x) \bmod x^{2n}+1 \quad (3.3)$$

$g(x) \in Z_{2n}$ và được gọi là căn bậc 2 của f(x)

Khi $g(x) = \sqrt{f(x)}$ được gọi là căn bậc 2 chính của f(x). Ta sẽ ký hiệu Q_{2n} là tập các thặng dư bậc 2 trong Z_{2n},.

Bổ đề 3.1: *Đa thức f(x) nằm trong tập các thặng dư bậc 2 Q_{2n} ($f(x) \in Q_{2n}$) khi và chỉ khi f(x) chứa các đơn thức có số mũ chẵn.*

Bổ đề 3.2: *Các căn bậc 2 của một thặng dư bậc 2 được xác định theo công thức sau:*

$$sqr[f(x)] = g(x) = (1+x^n) \sum_{t \in U} x^t + \sqrt{f(x)} \quad (3.4)$$

Trong đó U là một tập gồm các tổ hợp tuỳ ý các giá trị trong tập

s = {0, 1, 2,..., n-1}. Do vậy lực lượng của U sẽ bằng $|U| = 2^n - 1$

Trong vành Z_{2n} có 2^n thặng dư bậc 2, mỗi thặng dư bậc 2 có 2^n căn bậc 2, các căn bậc 2 của các thặng dư bậc 2 tạo nên vành Z_{2n} .

- Ta sẽ gọi các căn bậc 2 của cùng một thặng dư bậc 2 là các phần tử liên hợp (Conjugate Elements) ký hiệu là CEs.

Tính chất chung của các phần tử liên hợp

- Nếu a(x) là căn bậc 2 thì phần tử đối xứng cũng là căn bậc 2.
- Tổng của 2 CEs sẽ cũng chính là một căn bậc 2 của zero.
- Tổng số chẵn các CEs cũng chính là một căn bậc 2 của zero
- Tổng của 3 CEs cũng chính là một CE.

- Tổng số lẻ các CEs cũng chính là một CE.

Tính chất của căn bậc 2 (SRs: Square Roots) của lũy đẳng nuốt

- Các căn bậc 2 của một lũy đẳng trong Z_{2n} sẽ là một nhóm nhân. $e_i(x^2)$ cũng là lũy đẳng nuốt.
- Ngoại trừ $e_i(x^2)$, căn bậc 2 còn lại là các phần tử có bậc 2.

Các đặc tính của phần tử liên hợp của lũy đẳng nuốt

- Dịch vòng cyclic của căn bậc 2 của lũy đẳng nuốt cũng chính là 1 căn bậc 2 của nó.
- Căn bậc 2 của phần tử không, Zero là một nhóm Cộng.
- Tất cả các căn bậc 2 của Zero là thương số của Zero.

3.3.2. Xây dựng mã cylic trên vành mở rộng theo lớp các CEs

Các lớp chứa các phần tử liên hợp tạo nên một vành. Căn bậc 2 của lũy đẳng và căn bậc 2 của Zero tạo nên một vành con của vành $Z_{2n}.Z_{2n}$ được phân hoạch thành 2 lớp, mỗi lớp bao gồm 2^n CEs. Những CEs này là căn bậc 2 của thặng dư bậc 2 trong tập Q_{2n}.

Trên vành đa thức có hai lớp kề cyclic, ta có 2 bộ mã tốt tối ưu như sau (2^{n-1} - 1, n, 2^{n-2} – 1) và (2^{n-1}-1, n-1, 2^{n-2}).

Chúng ta đã biết rằng $\mathbf{z}_2[x]/(x^{2n}+1)$ đẳng cấu với $\mathbf{z}_2[x]/(x^n+1)$. Tât cả các phần tử của vành là các thặng dư bậc 2 của $\mathbf{z}_2[x]/(x^{2n}+1)$ được phân hoạch thành lớp các CEs của thặng dư bậc 2.

Trong phần này chúng ta sẽ thực hiện phân hoạch chuẩn theo các phần tử liên hợp của luỹ đẳng nuốt $e_0(x)$.

Trên vành Z_{2n}, phân hoạch chuẩn 32 phần tử liên hợp của lũy đẳng nuốt thành 4 lớp kề như trong bảng 3.2.

Bảng 3.2: Phân hoạch của các phần tử liên hợp của luỹ đẳng nuốt

N0	**C1**	**C2**	**C3**	**C4**
1	(01234)	(02346)	(03467)	(02468)
2	(12345)	(13457)	(14578)	(13579)
3	(23456)	(24568)	(25689)	
4	(34567)	(35679)	(36790)	
5	(45678)	(46780)	(47801)	
6	(56789)	(57891)	(58912)	
7	(67890)	(68902)	(69023)	
8	(78901)	(79013)	(70134)	
9	(89012)	(80124)	(81245)	
10	(90123)	(91235)	(92356)	

Căn cứ vào phân hoạch như trên ta có thể xây dựng mã cyclic

3.3.3. Xây dựng mã LCC theo các lớp kề của phân hoạch chuẩn trên vành $\mathbf{Z}_2[x]/(x^{2n}+1)$

Để tiện cho việc mã hoá và giải mã ta có một số bổ đề liên quan đến hệ tổng kiểm tra như sau.

Bổ đề 3.3: *Số các tổng kiểm tra trực giao với* $(1+x^n)$ *có thể thiết lập được trong tập* 2^n *phần tử liên hợp với* $e_0(x^2)$ *bằng* 2^{n-1}.

Bổ đề 3.4: *Tập các phần tử liên hợp với luỹ đẳng nuốt* $e_0(x^2)$ *sẽ tạo ra các mã LCC với giá trị sau:* $(n, k, d_0) = (2^n - 1, n, 2^n - 1)$

Để trực giao hóa hệ tổng kiểm tra $a(x)+b(x)=1+x^n$, ta có thể chọn trước giá trị của n dấu thông tin. Ta sẽ xây dựng mã LCC cụ thể từ các lớp kề C_1, C_2. Mã LCC này chính là mã (29, 5) với $d_0 = 14$ đây mã gần tối ưu (29, 5, 14). Khả năng để xây dựng các mã LCC có cùng tham số theo các phần tử liên hợp của luỹ đẳng nuốt trong vành Z_{10} là khá lớn. Với cách xây dựng mã (29,5) như trên ta có 900.3! = 5400 bộ mã có cùng tham số.

3.3.4. Mã LCC trên phân hoạch cực đại của vành $\mathbf{Z}_2[x]/(x^{2n}+1)$.

Trong vành đa thức $\mathbf{Z}_2[x]/(x^{2n}+1)$, chúng ta nhớ rằng cấp của nhóm nhân sinh cyclic $a(x)$ sẽ bằng $2.orda(x)$ trong $\mathbf{Z}_2[x]/(x^{2n}+1)$.

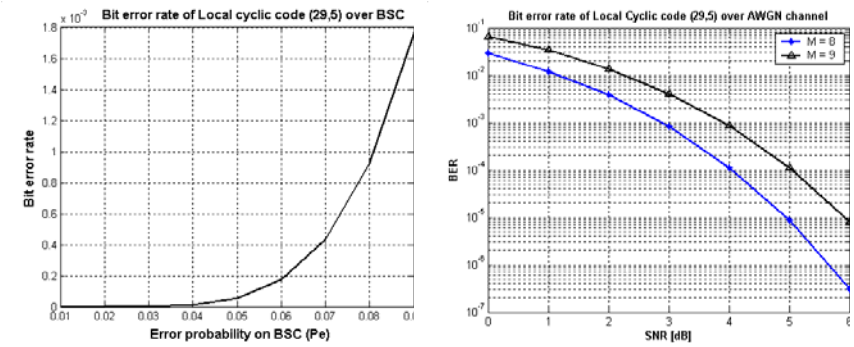
Với n=5, 32 phần tử của lũy đẳng $e_0(x^2)$ phân hoạch như sau:

$$B_1 = \{e_0(x)a^i(x),\ \ i = \overline{0,\ \ 29}\} = \{b^i,\ \ b = \overline{1,\ \ 30}\}$$

$$= \{(01234),\ (02346),\ (01478),\ (34567),\ (35679),(01347),\ (06789),\ (02689),\ (03467),\ (01239),(12359),\ (03679),\ (23456),\ (24568),\ (02369),(56789),(15789),\ (23569),\ (01289),\ (01248),(25689),\ (12345),\ (13457),\ (12589),(45678),(04678),\ (12458),\ (01789),\ (01374),\ (14578)\ \}$$

$$B_2 = \{(02468),\ (13579)\}$$

Ta sẽ sử dụng lớp kề B_1 để tạo mã LCC (29, 5). Ta có mã cyclic $(29,\ \ 5)$ với $d_0 = 14$. Ngưỡng chính của M là 8, bộ mã có khả năng sửa 6 bit thông tin sai.



Hình 3.3: BER mã LCC (29,5) trên kênh BSC và kênh AWGN

Mô phỏng tỉ số lỗi bit BER của mã LCC (29,5) được tạo ra trên kênh nhị phân đối xứng BSC và kênh AWGN với các cấp ngưỡng giải mã theo đa số M=8 và đa số một biểu quyết M=9 như được minh họa trong hình 3.3.

3.3.5. Mã tối ưu trên phần tử liên hợp của lũy đẳng nuốt $e_0(x^2)$

Ta sẽ xem xét đa thức thuộc vành đa thức có hai lớp kề cyclic $a(x) \in \mathbf{Z}_2[x]/(x^{2n}+1)$, bậc của đa thức này $orda(x) = 2^{n-1}-1$. Trong vành đa thức $\mathbf{Z}_2[x]/(x^{2n}+1)$, ta thấy rằng bậc của $a^2(x)$ cũng được xác định tương tự:

$$orda^2(x) = 2^{n-1}-1 \qquad (3.5)$$

Ta sẽ sử dụng đa thức $a^2(x)$ trong vành đa thức $\mathbf{Z}_2[x]/(x^{2n}+1)$ để xây dựng cấp số nhân CGP theo cách như sau:

Phần tử đầu tiên của cấp số nhân sẽ là phần tử liên hợp bất kỳ của lũy đẳng nuốt $e_0(x^2)$. Công bội của nhóm nhân này chính là $a^2(x)$.

Nhóm nhân này là chính là nhóm con (subset) của nhóm nhân CGP với công bội a(x), tương đương với mã: $(2^{n-1} - 1, n, 2^{n-2} - 1)$.

Mã này là mã tối ưu thỏa mãn giới hạn Griesmer. Chúng là các mã trực giao, với phương pháp giải mã ngưỡng với 2 cấp ngưỡng chúng ta sẽ thực hiện được mã này. Tóm lại, với bất kỳ giá trị nào của n, nếu CGP bao gồm phần tử $\sum_{i=n}^{2n-1} x^i$, ta sẽ có mã cyclic ngắn hơn như với tham số $(2^{n-1}-2, n-1, 2^{n-2}-1)$.

Cuối cùng trong chương này, ta sẽ ứng dụng công nghệ CPLD/FPGA để xây dựng phần cứng thực hiện việc giải mã. Kết quả mô phỏng phản ánh đúng hoạt động của FPGA đã được nạp cấu hình dưới dạng giản

đồ thời gian, mạch giả mã sửa được từ mã sai tới 6 bít thông tin.

3.5. KẾT LUẬN CHƯƠNG

Chương 3 đề cập phương thức xây dựng mã trên vành đa thức có hai lớp kề cyclic dựa vào các cấu trúc đại số mới, như nhóm nhân CMG, hay dựa trên các dạng phân hoạch của vành đa thức. Xây dựng mã LCC trên vành chẵn Z_{2n}, vành mở rộng của vành đa thức có hai lớp kề cyclic, mở ra khả năng linh hoạt trong việc tạo mã, góp phần hoàn thiện về cấu trúc đại số trong lý thuyết mã. Trong phần này chúng ta áp dụng công nghệ FPGA nhằm hiện thực hoá các quá trình mã hoá, giải mã một cách tin cậy nhất bằng các mạch phần cứng.

CHƯƠNG 4
MỘT SỐ ỨNG DỤNG CỦA VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

4.1. MỞ ĐẦU

Dựa trên các cấu trúc đại số theo cấp số nhân, nhóm nhân trên vành đa thức có hai lớp kề cyclic, ta đưa ra các ứng dụng cụ thể sau:

+ Tạo hệ mật luân hoàn và khóa giả ngẫu nhiên.

+ Tạo dãy m theo phân hoạch vành đa thức có hai lớp kề cyclic

+ Giảm PAPR trong hệ thống OFDM bằng mã cyclic

+ Ứng dụng mã cyclic trong tìm kiếm cell cho hệ thống WCDMA.

4.2. TẠO HỆ MẬT LUÂN HOÀN VÀ TẠO KHÓA GIẢ NGẪU NHIÊN

Định nghĩa 4.1: *Cấp số nhân luân hoàn (CGP: Circulant Geometric Progression) trên vành đa thức là một cấp số nhân có công bội x và số hạng đầu là a(x).*

$$A = \{a(x)\} = \{a(x).x^i;\ i=0, 1, 2, ..., n-1\} \quad (4.1)$$

Cấp số nhân luân hoàn là một phép biến đổi tuyến tính không suy biến nếu số hạng đầu a(x) thoả mãn điều kiện sau:

$$(a(x), x^n+1) = 1 \quad (4.2)$$

Ma trận tương ứng của phép biến đổi này gọi là ma trận luân hoàn.

$$A = \begin{pmatrix} a(x) \\ x.a(x) \\ x^2.a(x) \\ \dots \\ x^{n-1}.a(x) \end{pmatrix}$$

Phép biến đổi ngược tương ứng: A-1 = $\{a_i^{-1}(x)\}$

Ở đây, $a(x).a^{-1}(x) \equiv 1 \bmod x^n+1$

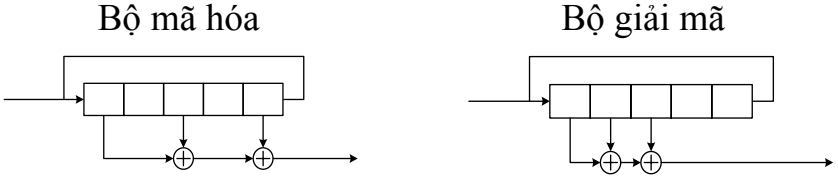
a(x) có thể được dùng làm khoá của 1 hệ mật tuyến tính được xây dựng theo A. Hệ mật này gọi là hệ mật luân hoàn với tính chất sau:

Số các khoá trong hệ mật được xây dựng trên các CGP trong vành đa thức với hai lớp kề cyclic được xác định: $K = 2^{n-1} - 1$

- Trong trường hợp $n = 2^i$: hệ mật dựa trên các CGP tương tự hệ mật này: $x^{2^i} + 1 = (x+1)^{2^i}$

- Với $n = 2^i$ thì $\theta_0(x) = \sum_{i=0}^{n-1} x^i$ là một đa thức có trọng số chẵn. Vì vậy, số của khoá được xác định là: $K = 2^n - 1$.

Từ các cấu trúc đặc điểm trên, chúng ta sẽ xây dựng bộ mã hóa và giải mã trên vành đa thức có hai lớp kề cyclic với n=5 như sau:



Hình 4.1: Cấu trúc bộ mã hóa giải mã của hệ mật luân hoàn.

Số lượng khóa tạo ra trong hệ mật là $K = 2^{n-1} - 1$, tương đương với cấp cực đại của a(x). Để thực hiện việc thay đổi khóa ta làm như sau:

- Hai bên liên lạc chọn trước một phần tử nguyên thủy a(x) (ord $a(x) = 2^{n-1} - 1$)

- Khoá truyền thông b(x) là đa thức tuỳ ý với trọng số lẻ. Khoá này dùng cho khối thông tin đầu tiên (n bit). Khối tin kế tiếp sẽ được mã bởi bộ tạo khoá từ đa thức tạo ra từ phép nhân phần tử nguyên thủy và khoá truyền tin. Việc dùng các khoá là phần tuỳ ý đầu tiên của cấp số nhân luân hoàn với công bội a(x) và phần tử

Input (4) (3) (2) (1) (0)

Output

A={(0)',(1)',(2)',(3)',(4)'

nguyên thủy b(x). Phần không lặp lại của các khoá là $2^{n-1}-1$ phần tử.

Có thể ứng dụng hệ mật này trong mạng thay thế-hoán vị SPN (substitution-permutation network). SPN là mật mã tạo ra bằng cách thay thế và hoán vị các trạng thái, ví dụ như mật mã Feistel.

4.3. TẠO DÃY M BẰNG PHƯƠNG PHÁP PHÂN HOẠCH THEO MODULO h(x) TRÊN VÀNH ĐA THỨC CÓ HAI LỚP KỀ CYCLIC

Một pha của dãy m truyền thống đặc trưng bởi biến đổi d như sau:

$$u(d) = D[u] = \frac{s(d)}{h(d)} \tag{4.3}$$

Trong đó, như đã biết h(d) là đa thức sinh có bậc m và s(d) là biến đổi d của trạng thái ban đầu có bậc < m-1.

Gọi $T^j u$ là dãy dịch pha j nhịp so với u ta có:

$$T^j u = u(d).d^j \pmod{h(d)} = \frac{s(d)}{h(d)}.d^j \pmod{h(d)} \tag{4.4}$$

Từ phân hoạch trên ta sẽ tạo ra được dãy m lồng ghép tuyến tính.

Nhìn chung, bản chất của việc xây dựng dãy m như trên thực chất được xây dựng trên trường GF(2) theo phân hoạch:

$a(x).x^i \bmod g(x)$, i= 1:n với deg(g(x)) = n

+ a(x) là đa thức trên trường thiết lập trạng thái đầu.

+ g(x) là đa thức sinh.

Đối với vành đa thức có hai lớp kề cyclic, ta có phân tích nhị thức:

$$x^n + 1 = (1+x)\sum_{i=0}^{n-1} x^i \tag{4.5}$$

Vành đa thức có hai lớp kề cyclic sẽ có hai đa thức h(x) ở dạng:

+ h(x) = (1+x) và h(x) = $\sum_{i=0}^{n-1} x^i$

Cấp lớn nhất trên vành đa thức có hai lớp kề cyclic sẽ là 2^{n-1} -1. Trên vành này, chúng ta hoàn toàn có thể xây dựng một dãy m có chiều dài L = 2^{n-1} -1 đúng bằng cấp lớn nhất của đa thức trên vành. Cách thức xây dựng dãy m lồng ghép ở đây sẽ dựa trên phân hoạch theo modulo h(x) với phương pháp phân hoạch tạo ra cấp số nhân có chiều dài 2^{n-1} -1 trên vành như sau:

$a^i(x) \bmod h(x)$ (a(x) là công bội của cấp số nhân) (4.6)

Ở đây h(x) đóng vai trò là đa thức sinh để tạo ra dãy m và là đa thức bất khả quy bậc n-1.

Muốn để cho phân hoạch có chiều dài cực đại L = 2^{n-1} -1 thì đa thức a(x) được chọn làm công bội sẽ phải thỏa mãn:

$$\max(\text{ord}\,(a(x)) = 2^{n-1} - 1 \tag{4.7}$$

Việc thay đổi các công bội a(x) khác nhau sẽ cho ta các khả năng tạo dãy mở rộng. Chẳng hạn số khả năng phân hoạch M tạo dãy m tuyến tính trên vành đa thức $x^{13} + 1$ theo modulo h(x) sẽ được tính dựa trên các phần tử nguyên thủy có cấp cực đại 4095 được chọn làm công bội a(x), với cách tính theo hàm φ-Euler:

$$M = \varphi(2^{13}-1 - 1) = \varphi(4095) = \varphi(3.3.5.7.13)$$
$$= 4095(1-1/3).(1-1/5).(1-1/7)(1-1/13) = 1728$$

Như vậy, đối với vành đa thức có hai lớp kề cyclic, việc tạo ra dãy m khá đơn giản nhờ phân hoạch theo modulo $h(x)= \sum_{i=0}^{n-1} x^i$ tương ứng với cấp cực đại của đa thức trên vành

4.4. GIẢM PAPR BẰNG PHƯƠNG PHÁP MÃ HÓA CYCLIC

Một trở ngại chính trong truyền dẫn đa sóng mang OFDM (Orthogonal Frequency Division Multiplexing) chính là tỷ số công suất cực đại trên công suất trung bình PAPR (Peak to Average Power Ratio) tăng cao. Các nghiên cứu gần đây đã đưa ra nhiều giải pháp giải quyết vấn đề này, mục này đề cập đến các phương pháp giảm PAPR bằng phương pháp mã hóa cyclic, với phương thức thực hiện khá đơn giản.

Công suất PAPR của hệ thống truyền dẫn đa sóng mang OFDM sẽ được tính như sau:

$$PAPR = 10\log_{10}[\frac{\max(|s(t)|^2}{P_{avg}}] \text{ (db)} \quad (4.8)$$

Hay được biểu diễn : $PAPR = 10\log_{10}[\frac{P_{peak}}{P_{avg}}]$ (db)

(4.9)

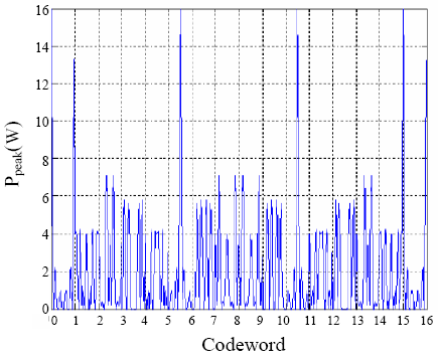
+ P_{avg} là công suất tiêu thụ trung bình bởi mỗi khung (frame).

Nếu công suất trong mỗi sóng mang con tương đương với 1(W), thì Pavg của tín hiệu sẽ bằng N(W) và (4.9) sẽ trở thành:

$$PAPR = 10\log_{10}[\frac{P_{peak}}{N}]$$

(4.10)

Đường bao công suất của 4 sóng mang con với điều chế BPSK trong hệ thống OFDM được vẽ trên hình 4.2.



Hình 4.2: Đường bao công suất của 4 tín hiệu sóng mang

PAPR của các từ dữ liệu của tín hiệu OFDM với 4 sóng mang với cho thấy rằng, các từ mã mà số bit "0" và số bit "1" bằng nhau, hoặc từ mã toàn bit "1" hoặc bit "0" ([0000], [1111], [0101]...) có công suất tương

ứng đạt cực đại. Do vậy muốn giảm PAPR, phải tránh truyền các từ mã này.

Đề xuất phương pháp sử dụng mã cyclic giảm PAPR

Trong đề xuất này, sử dụng các mã cyclic và LCC xây dựng trên nhóm nhân CMG với số lượng bộ mã lớn để giảm PAPR. Phương pháp này về cơ bản là kết hợp sử dụng các đặc tính mã kiểm tra chẵn lẻ và kỹ thuật mã hóa cyclic dựa trên nhóm nhân CMG để giảm PAPR. Ta sẽ xem xét cụ thể với số sóng mang con N=8.

$P_{peak} = N^2 = 64(W)$ $PAPR = 10\log_{10}[\frac{64}{8}] = 9.03(db)$

Quá trình thực hiện theo phương pháp này chia thành 3 bước:

Bước 1: Ánh xạ 8 bit của từ dữ liệu thành từ mã gồm 7 bit dữ liệu và một bit kiểm tra chẵn lẻ. Từ mã sau khi ánh xạ sẽ không dẫn đến công suất PAPR cao. Số lượng các từ mã giảm từ 256 xuống còn 128, việc phân bố công suất đỉnh tương ứng sẽ giảm đi, PAPR lúc này sẽ là 9.03 dB, tương đương với $\log_{10}(8)$ (N=8).

Bước 2: Ứng dụng lý thuyết về mã khống chế sai để tạo ra ma trận sinh G nhằm mục đích mã hóa bản tin u(t) với n dấu mã.

Đa thức sinh G được tạo ra từ cấu trúc nhóm nhân CMG với modulo h(x) có dạng: $G = \left[a^i(x) \bmod h(x), i = \overline{0, t-1} \right]$

Trong đó, a(x) là phần tử bất kỳ trên vành $\mathbf{Z}_2[x]/(x^n+1)$, t là bậc của a(x), h(x) là phần tử trên vành quyết định chiều dài từ mã và khoảng cách Hamming theo bậc của h(x).

Ta xây dựng nhóm nhân CMG đơn vị với modulo h(x) như sau:

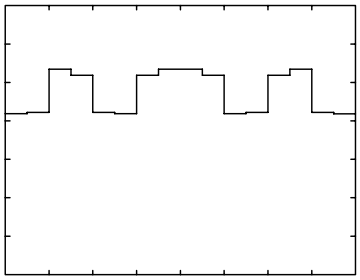
$$\begin{aligned} I &= \left\{x^i \bmod h(x), i = \overline{0,6}\right\} \\ &= \left\{1, x, x^2, x^3, 1+x+x^2, x+x^2+x^3, 1+x+x^3\right\} \end{aligned} \tag{4.10}$$

I tương đương với mã $(7,4,3)$ đa thức sinh $g(x) = 1 + x^4 + x^6$.

Bước 3: Thực hiện mã hóa cyclic (n,k) dựa trên ma trận sinh G(x) ta nhận được: V(t) = u(t)*G(x) Trong đó u(t) là từ dữ liệu k bit.

Sau quá trình mã hóa, 16 từ mã được tạo ra, công suất đỉnh P_{peak} của tín hiệu được mã hóa cho tất cả các khả năng có thể của từ dữ liệu sẽ phân bố từ $0_{10}(0000)_2$ đến $15_{10}(1111)_2$, từ mã hóa được dùng cho sóng mang thông qua biến đổi cyclic như trên từ $0_{10}(0000000)_2$ đến $128_{10}(1111111)_2$. Đa thức sinh G(x) và phân bố công suất đỉnh như hình dưới:

$$G(x) = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{vmatrix}$$



Hình 4.3: Đa thức sinh và PAPR sau khi sử dụng mã cyclic (7,4)

Công suất đỉnh P_{peak} = 25(W) nên: $PAPR = 10\log_{10}[\frac{25}{7}] = 5.5284\,(\text{db})$

So với ban đầu, khi chưa áp dụng mã cyclic PAPR=9.03(db) thì kết quả này đã giảm được 3.5026(db). Phương pháp này khá đơn giản vì việc mã hóa giải mã cyclic thông dụng và dễ dàng.

4.5. SỬ DỤNG MÃ CYCLIC TRONG THUẬT TOÁN TÌM KIẾM CELL WCDMA

Trong hệ thống WCDMA không đồng bộ, quá trình đồng bộ hoá còn gọi là thủ tục tìm kiếm cell theo 3 giai đoạn, giai đoạn 1 thực hiện đồng bộ khe, giai đoạn 2 thực hiện đồng bộ khung và nhận dạng nhóm mã xáo trộn, và giai đoạn 3 yêu cầu mã xáo trộn cho mỗi cell. Với cấu trúc mã cyclic đươc đề xuất với số lượng bộ mã lớn thích hợp với cơ chế tìm kiếm cell khi có nhiều người dùng. Nội dung trong phần này sẽ trình bày

phương thức sử dụng mã cyclic trong thủ tục tìm kiếm cell ở giai đoạn thứ 2 và mô phỏng đánh giá hiệu suất tìm kiếm cell sử dụng các mã cyclic khi tồn tại độ lệch tần số khởi tạo ở thiết bị người dùng UE (User Equipment). Các mã cyclic được đề xuất ở đây là các cấp số nhân cyclic CGP được sử dụng cho quá trình tìm kiếm cell. Tín hiệu nhận được có thể được mô hình hoá bởi phương trình 4.11.

$$r(t) = \sqrt{\frac{E_S}{T_S}}\,\mathrm{Re}\left\{e^{j2\pi f_c t}\alpha(t)\left(\sqrt{\delta}\;\tilde{c}(t)+\sqrt{1-\delta}\,\tilde{s}(t)\right)\right\} + \mathrm{n}(t) \qquad (4.11)$$

E_s : Năng lượng kí hiệu mã hoá kênh đồng bộ (SCH) nhận được

T_s: Độ dài kí hiệu mã SCH (=$256T_c$, T_c là khoảng chu kì chip)

δ (t) : Quá trình Gausssian phức chuẩn hoá

$\tilde{c}(t)$, $\tilde{s}(t)$: Đóng gói phức của tín hiệu PSC, tín hiệu SSC

n(t) : Nhiễu Gaussian cộng với mật độ phổ hai phía $N_0/2$

δ là tỉ số công suất PSC với công suất SCH tổng:

$$\delta = \frac{P_{PSC}}{P_{PSC}+P_{SSC}} \qquad (4.12)$$

Mã cyclic được đề xuất cho việc tìm kiếm cell

Trong phần này, mã cyclic dựa trên cấu trúc cấp số nhân CGP được sử dụng cho SSC trong quá trình tìm kiếm cell. Xem xét vành đa thức $\mathbf{z}_2[x]/(x^n+1)$, dựa trên

CGP, vành đa thức này có thể được phân hoạch thành các lớp kề theo một CGP nào đó. Nhóm nhân này được gọi là nhóm nhân sinh, hay phần tử sinh của phân hoạch.

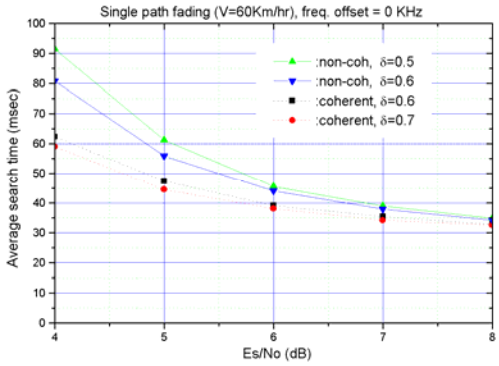
Theo phân tích dựa trên CGP này, các mã cyclic có thể khác nhau có thể được cấu thành. Đối với sơ đồ tìm kiếm cell như trên, ta sẽ sử dụng mã cyclic trên vành đa thức có hai lớp kề cyclic (15,5) được sử dụng như một chuỗi SSC đối với việc tìm kiếm cell.

Trong $\mathbf{z}_2[x]/(x^5+1)$, chúng ta có $x^5+1=(1+x)(1+x+x^2+x^3+x^4)$

Sử dụng phân hoạch với nhóm nhân đơn vị I = {x^i, i = 0, 1,...,n-1}, nghĩa là CGP có một tỉ số chung q(x) = x, 31 thành phần khác không trong $\mathbf{z}_2[x]/(x^5+1)$ có thể được chia thành 7 lớp kề tương ứng với 7 CGP. Chẳng hạn, (15,5) từ mã được tạo ra từ thành phần đầu các tập liên kết {(0), (012), (013)} được mô tả như sau :

(0)	(1)	(2)	(3)	(4)	(012)	(123)	(234)	(034)	(014)	(013)	(124)	(023)	(134)	(	

Dựa trên mã cyclic được đề xuất ở trên, áp dụng chúng cho SSC trong tìm kiếm cell. Mô phỏng này quan tâm cả sơ đồ giải điều chế kết hợp cũng như các sơ đồ giải điều chế không kết hợp ở giai đoạn hai.



Hình 4.5: Hiệu suất tìm kiếm cell trung bình (độ lệch tần "0")

Hình 4.5 mô tả khả năng đồng bộ lỗi của giai đoạn 1 và giai đoạn 2 theo các giá trị Es/No khác nhau và với giá trị δ cố định. Việc sử dụng sơ đồ giải điều chế kết hợp với mã cyclic theo cấu trúc CGP trong tìm kiếm cell giai đoạn 2 với dung lượng các từ mã lớn là rất thích hợp đối với tìm kiếm cell trong hệ thống WCDMA.

4.6. KẾT LUẬN CHƯƠNG

Dựa trên cấu trúc đại số đã đề cập chúng ta có thể tạo ra các hệ mật luân hoàn, các dãy m sử dụng trong các hệ thống WCDMA, hay sử dụng các mã cyclic này để giảm PAPR và ứng dụng trong thuật toán tìm kiếm cell trong WCDMA. Ưu điểm nổi bật của phương pháp xây dựng các mã cyclic dựa trên các cấu trúc nhóm nhân và cấp số nhân là số lượng các bộ mã tốt tạo ra rất lớn, thích hợp với các công nghệ yêu cầu về số lượng lớn các bộ mã.

KẾT LUẬN

Luận án là một công trình nghiên cứu tương đối hoàn chỉnh về vành đa thức có hai lớp kề cyclic. Các kết quả của luận án đạt được là:

1. Xây dựng thuật toán xác định điều kiện để vành đa thức $\mathbf{z}_2[x]/(x^n+1)$ là vành có hai lớp kề cyclic. Thuật toán được xây dựng để tìm ra toàn bộ các vành đa thức có hai lớp kề cyclic với giá trị ***n*** lớn (n < 10.000).

2. Xây dựng các phương pháp tạo mã cyclic và cyclic cục bộ trên vành đa tNhhức có hai lớp kề cyclic nhờ các cấu trúc đại số như cấp số nhân CGP, nhóm nhân CMG hoặc theo các phân hoạch, với số lượng bộ mã tạo ra lớn, qua các mô phỏng đều cho đặc tính tốt. Chẳng hạn, trên vành $\mathbf{z}_2[x]/(x^5+1)$ có thể xây dựng tối đa 795.723.061 bộ mã so sánh với 3 mã tầm thường theo cách xây dựng mã cyclic truyền thống.

3. Dựa trên cấu trúc phân hoạch theo phần tử liên hợp của lũy đẳng nuốt, xây dựng mã cyclic, cyclic cục bộ trên các vành mở rộng, vành chẵn, của vành đa thức có hai lớp kề cyclic, mở ra khả năng tạo các mã có độ dài lớn hơn trên vành nhỏ hơn, mang lại hiệu quả cao khi tính toán, xử lý. Để minh chứng, trong luận án đề cập đến việc xây dựng mã (29,5) trên vành $\mathbf{z}_2[x]/(x^5+1)$. Luận án cũng đưa ra kết quả thực hiện mã hóa, giải mã

nhờ công nghệ tích hợp số FPGA nhằm tăng tính khả thi ứng dụng trong thực tế

4. Ứng dụng cấu trúc đại số mới trên vành đa thức có hai lớp kề cyclic để giải quyết một số vấn đề trong bài toán viễn thông:

a. Sử dụng nhóm nhân luân hoàn xây dựng hệ mật luân hoàn trên vành đa thức có hai lớp kề cyclic. Số khóa được tạo ra khá lớn 2^{n-1}-1, cơ chế mã hóa, giải mã linh hoạt bằng tính chất dịch vòng nhóm nhân.

b. Tạo dãy m tuyến tính với cấu trúc mới là phân hoạch trên vành đa thức có hai lớp kề cyclic theo modulo $h(x)= \sum_{i=0}^{n-1} x^i$.

c. Giải quyết bài toán giảm PAPR trong hệ thống OFDM bằng phương pháp mã hóa cyclic theo cấp số nhân CGP, minh họa cho tín hiệu 8 sóng mang con, kết quả giảm được 3.5dB và tăng tính sửa sai.

d. Sử dụng mã trên vành đa thức có hai lớp kề cyclic để tìm kiếm cell trong hệ thống WCDMA. Mô phỏng cho kết quả tốt với độ lợi từ 0.8 - 1.2 dB. Với ưu điểm số lượng bộ mã tạo ra lớn, các mã này phù hợp với việc tìm kiếm cell khi số lượng thuê bao nhiều.

Các đề xuất ứng dụng trên mới dừng ở mức thiết lập phương pháp, thử nghiệm và đánh giá mô phỏng sơ bộ.

KIẾN NGHỊ HƯỚNG PHÁT TRIỂN TIẾP THEO

+ Hoàn thiện các cấu trúc đại số của vành đa thức có hai lớp kề cyclic, tìm các điều kiện về cấp cực đại của các phần tử trong vành đa thức này.

+ Hệ thống hóa các phương thức xây dựng mã trên vành đa thức có hai lớp kề cyclic, vành mở rộng của vành này. Từ đó, tổng quát để mở rộng sang các trường hữu hạn khác.

+ Đánh giá các kết quả ứng dụng của luận án một cách triệt để mang tính tổng quát, để minh chứng cho tính khả thi khi áp dụng trong thực tế. Những phương thức đề xuất để giải quyết bài toán tìm kiếm cell trong hệ thống WCDMA, giảm PAPR trong hệ thống OFDM cần được thử nghiệm đầy đủ, so sánh với các phương thức hiện có để khẳng định tính ưu việt các phương thức đã được đề xuất.