ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

—————— o0o ——————

NGUYỄN THỊ HÀ

PHÂN TÍCH ĐA THỨC THÀNH CÁC ĐA THỨC BẤT KHẢ QUY ĐỂ XÂY DỰNG CÁC MÃ CYCLIC TRÊN TRƯỜNG HỮU HẠN

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN, 8/2020

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

——————— o0o ———————

NGUYỄN THỊ HÀ

PHÂN TÍCH ĐA THỨC THÀNH CÁC ĐA THỨC BẤT KHẢ QUY ĐỂ XÂY DỰNG CÁC MÃ CYCLIC TRÊN TRƯỜNG HỮU HẠN

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 8 46 01 13

NGƯỜI HƯỚNG DẪN KHOA HỌC:
TS. NGUYỄN TRỌNG BẮC

Thái Nguyên, 8/2020

Mục lục

LỜI NÓI ĐẦU

Lý thuyết mã xuất hiện lần đầu tiên vào năm 1948 bởi một công trình của C. E. Shannon về lý thuyết toán học cho lĩnh vực truyền thông. Từ đó đến nay, lý thuyết này đã và đang đóng góp để giải quyết nhiều vấn đề quan trọng trong thông tin liên lạc. Nó được ứng dụng nhiều trong các lĩnh vực như: thông tin điện tử, thu phát thanh, bảo mật...

Lý thuyết mã hóa là một ngành của toán học và khoa học điện toán nhằm giải quyết tình trạng lỗi dễ xảy ra trong quá trình truyền thông số liệu trên các kênh truyền có độ nhiễu cao, dùng những phương pháp tinh xảo khiến phần lớn các lỗi xảy ra có thể được chỉnh sửa. Lý thuyết mã còn xử lý những đặc tính của mã và do vậy phù hợp với những ứng dụng cụ thể.

Lý thuyết mã hóa là một trong những lĩnh vực quan trọng của toán học, có ảnh hưởng đến rất nhiều lĩnh vực khoa học-công nghệ và kinh tế-xã hội. Thực tế cho thấy lý thuyết mã hóa đã vô cùng quan trọng từ xa xưa. Thời nay, với sự phát triển rất nhanh của công nghệ thông tin, và mạng internet thì mã hóa thông tin càng đóng vai trò quan trọng. Mã hóa là một phương pháp bảo vệ thông tin, bằng cách chuyển đổi thông tin từ dạng rõ (thông tin có thể dễ dàng đọc hiểu được) sang dạng mờ (thông tin đã bị che đi, nên không thể đọc hiểu được, để đọc được ta cần phải giải mã nó). Nó giúp ta có thể bảo vệ thông tin, để những kẻ đánh cắp thông tin, dù có được thông tin của chúng ta, cũng không thể hiểu được nội dung của nó. Mã hóa sẽ mang lại tính an toàn cao hơn cho thông tin, đặc biệt là trong thời đại internet ngày nay, khi mà thông tin phải đi qua nhiều trạm trung chuyển trước khi đến được đích. Sau đây, chúng tôi chỉ ra một vài ứng dụng của một số mã cụ thể.

Mã ISBN (International Standard Book Number) là mã số tiêu chuẩn quốc

tế có tính chất thương mại duy nhất để xác định được các thông tin về một quyển sách bất kỳ (ngôn ngữ của cuốn sách, quốc gia xuất bản, lĩnh vực của cuốn sách,...).

Mã BCH (Bose–Chaudhuri–Hocquenghem codes) là một loại mã cyclic và là loại mã sửa lỗi quan trọng, có khả năng sửa được nhiều lỗi và được ứng dụng rộng rãi. Lớp mã BCH có 2 lớp con là mã BCH nhị phân và mã BCH không nhị phân. Trong số những mã BCH không nhị phân này, lớp quan trọng nhất là mã Reed - Solomon. Mã Reed - Solomon được Reed và Solomon giới thiệu lần đầu tiên vào năm 1960, là một mã sửa sai thuộc loại mã tuyến tính. Mã Reed - Solomon được sử dụng để sửa các lỗi trong nhiều hệ thống thông tin số và trong lưu trữ, bao gồm: Các thiết bị lưu trữ (băng từ, đĩa CD, VCD,...), thông tin di động hay không dây (điện thoại di động, các đường truyền Viba), thông tin vệ tinh, truyền hình số DVB, các modem tốc độ cao như: ADSL, VDSL ... Mã Reed - Solomon đặc biệt quan trọng trong việc sửa các bit lỗi xảy ra gần nhau. Mã BCH được dùng cho các cây ATM, trong hệ thống giao dịch của các ngân hàng,...

Mã Hadamard được dùng trong việc truyền thông tin và hình ảnh từ các tàu vũ trụ, các vệ tinh về Trái Đất. Trong môi trường nhiễu loạn không khí lớn thì thông tin và hình ảnh sẽ bị bóp méo, thay đổi khi được truyền trong môi trường nhiễu loạn không khí, vì thế vai trò của mã Hadamard là rất quan trọng trong việc khám phá vũ trụ. Các lớp mã cyclic được dùng trong quân đội của các quốc gia đã đóng góp lớn tới việc bảo mật thông tin và truyền đạt thông tin từ quốc gia tới quân đội.

Mã lượng tử được giới thiệu lần đầu tiên vào năm 1996 bởi Shor [6]. Trong máy tính thông thường, dữ liệu chỉ được lưu dưới dạng 0 và 1, còn máy tính lượng tử sử dụng qubits (quantum bits) cho phép máy tính ghi dữ liệu ở nhiều trạng thái cùng lúc (ví dụ có thể là 0, có thể là 1 hoặc có thể cùng lúc là 0 và 1), điều này cho phép máy tính lượng tử xử lý được những phép tính phức tạp hơn. Người ta tính toán rằng các máy tính lượng tử sẽ giải quyết các vấn đề phức tạp nhanh hơn bất kỳ máy tính cổ điển nào. Máy tính lượng tử cơ

bản khai thác các quy tắc của cơ học lượng tử để tăng tốc độ tính toán. Việc xây dựng một máy tính lượng tử vẫn là một nhiệm vụ khó khăn nhưng bước đầu đã có những thành công từ các tập đoàn lớn trên thế giới như Intel, IBM, Microsoft, và Google. Cho đến nay, máy tính lượng tử không chỉ dừng lại là cuộc cạnh tranh về công nghệ giữa các tập đoàn công nghệ lớn mà nó còn là cuộc cạnh tranh giữa các cường quốc để phục vụ cho hoạt động tình báo nói riêng và quốc phòng nói chung. Sự ra đời của máy tính lượng tử sẽ làm cho các hệ mật nổi tiếng như DES (the Data Encryption Standard), RSA,... sẽ bị phá trong tương lai gần.

Mật mã DES có thể xem là tuyệt đối an toàn vì để giải được nó cần phải kiểm tra một danh sách rất lớn các chìa khoá mã tiềm năng. Ví dụ nếu chúng ta sử dụng một máy tính cổ điển với 64 bits, khi đó sẽ có 2^{64} trạng thái. Với một máy tính cổ điển, cứ cho là mỗi giây kiểm tra được 2 tỷ trạng thái thì cũng cần khoảng 300 năm chạy máy liên tục mới chạy được hết 2^{64} trạng thái-đó là một khoảng thời gian phi thực tiễn. Trong khi đó, một máy tính lượng tử dùng thuật toán lượng tử Grover có thể dễ dàng hoàn tất việc này trong thời gian 4 phút. Thuật toán mã hóa công khai RSA đang được ứng dụng rộng rãi trong ngân hàng, giao dịch trực tuyến và rất nhiều ứng dụng an ninh mạng khác. Sự an toàn của mã RSA nằm ở chỗ máy tính truyền thống không thể phân tích nhanh một số nửa nguyên tố (semiprime) lớn n thành tích của 2 số nguyên tố lớn p và q ($n = pq$). Về mặt toán học đây là một bài toán phức tạp, chẳng hạn để phân tích một số chỉ gồm 129 chữ số thì 600 máy tính cổ điển đã phải hợp lực làm việc liên tục trong vài tháng. Tuy nhiên, một máy tính lượng tử dùng thuật toán lượng tử Shor có thể phân tích một số lớn hơn cả triệu lần trong khoảng thời gian ngắn hơn cũng cả triệu lần.

Trong lĩnh vực sinh học, khái niệm mã DNA được đưa ra lần đầu tiên vào năm 2003, nhằm giúp nhận diện các mẫu vật. Mã DNA sử dụng một trình tự DNA ngắn nằm trong bộ gene của sinh vật như là một chuỗi ký tự duy nhất giúp phân biệt hai loài sinh vật với nhau. Như vậy mã DNA là một phương pháp định danh mà nó sử dụng một đoạn DNA chuẩn ngắn nằm trong bộ gene

của sinh vật đang nghiên cứu nhằm xác định sinh vật đó thuộc về loài nào. Mã vạch DNA rất hữu ích trong việc tìm mối quan hệ giữa các mẫu mặc dù chúng hầu như không giống nhau về hình thái. Mã vạch DNA cũng được ứng dụng tại hải quan nhằm hỗ trợ việc xác định nguồn gốc của sinh vật sống hoặc hàng nhập khẩu, để ngăn cản sự vận chuyển trái phép các loài thực vật và động vật quý hiếm qua biên giới. Mã DNA giúp kiểm soát tác nhân gây hại trong nông nghiệp, giúp định danh nhanh chống các loài gây bệnh ở giai đoạn tiềm ẩn (giai đoạn ấu trùng), hỗ trợ chương trình kiểm soát sâu bệnh bảo vệ cây trồng. Ngoài ra, mã DNA giúp xác định vật chủ trung gian gây bệnh, bảo vệ loài nguy cấp và kiểm tra chất lượng nước.

Qua một số ví dụ về các lớp mã cyclic đã nêu ở trên, giúp chúng ta thấy được phần nào vai trò quan trọng của mã cyclic trong cuộc sống, trong khoa học kĩ thuật.

Đầu tiên, lý thuyết mã được nghiên cứu trên trường hữu hạn và các kết quả cơ bản đã được đúc kết trong hai quyển sách của Huffman và Berlekamp [5]. Sau đó, các nhà toán học đã mở rộng nghiên cứu về mã trên các vành hữu hạn. Hầu hết các nghiên cứu tập trung trong trường hợp độ dài của mã có liên quan đến đặc số của trường. Nếu độ dài của mã chia hết cho đặc số của trường thì mã được gọi là mã nghiệm lặp. Nếu độ dài của mã không chia hết cho đặc số của trường thì mã đó được gọi là mã nghiệm đơn.

Nghiên cứu về mã trên vành giao hoán hữu hạn, đặc biệt là mã nghiệm lặp trên lớp các vành chuỗi hữu hạn cũng được nhiều nhà toán học quan tâm và các nhà toán học cũng đã đưa ra được nhiều kết quả tốt. Trong luận văn này, chúng tôi sử dụng các kết quả của Toán học để xây dựng và nghiên cứu mã cyclic trên trường hữu hạn.

Nội dung chính của luận văn là: trình bày sự phân tích đa thức thành các đa thức bất khả quy trên trường hữu hạn. Sau đó sử dụng kết quả của sự phân tích này để xây dựng các mã cyclic trên trường hữu hạn. Luận văn gồm 2 chương:

Trong chương 1, chúng tôi trình bày định nghĩa trường hữu hạn, cấu trúc của trường hữu hạn. Sau đó chúng tôi trình bày vành đa thức trên trường hữu

hạn. Cuối chương 1 chúng tôi đưa ra một số kiến thức về đa thức bất khả quy.

Trong chương 2, chúng tôi trình bày nội dung chính của luận văn là: phân tích đa thức thành các đa thức bất khả quy trên trường hữu hạn, mã cyclic, xây dựng các mã cyclic trên trường hữu hạn. Để tìm tất cả các mã cyclic trên trường hữu hạn $\mathbb{F}_q$, trong đó $q = p^m$ (p là số nguyên tố bất kì) chúng tôi đi tìm những iđêan của vành $R_n = \mathbb{F}_q[X]/\langle x^n - 1\rangle$.

Nội dung nghiên cứu của luận văn gắn liền với toán sơ cấp, đặc biệt là bài toán phân tích đa thức thành nhân tử rất được quan tâm ở bậc học phổ thông.

Luận văn này được thực hiện tại Trường Đại học Khoa học - Đại học Thái Nguyên và hoàn thành dưới sự hướng dẫn của Tiến sĩ Nguyễn Trọng Bắc. Tôi xin được bày tỏ lòng biết ơn chân thành và sâu sắc tới người hướng dẫn khoa học của mình.

Tôi xin trân trọng cảm ơn Ban giám hiệu Trường Đại học Khoa học - Đại học Thái Nguyên, Ban chủ nhiệm khoa Toán – Tin cùng các giảng viên đã tham gia giảng dạy, đã tạo mọi điều kiện tốt nhất để tôi học tập và nghiên cứu.

Tôi cũng xin chân thành cảm ơn Sở Giáo dục và Đào tạo tỉnh Thái Nguyên, Ban Giám hiệu và các đồng nghiệp trường THPT Hoàng Quốc Việt, huyện Võ Nhai, tỉnh Thái Nguyên đã tạo điều kiện cho tôi hoàn thành tốt nhiệm vụ học tập và công tác của mình.

Cuối cùng tôi xin gửi lời cảm ơn tới gia đình thân yêu, cảm ơn những người bạn thân thiết đã giúp đỡ động viên khích lệ tôi trong suốt quá trình nghiên cứu. Xin chân thành cảm ơn.

Thái Nguyên, tháng 8 năm 2020

Tác giả

Nguyễn Thị Hà

Chương 1

Một số kiến thức chuẩn bị

1.1. Trường hữu hạn

Định nghĩa 1.1. *Trường* là một tập hợp $\mathbb{F}$ cùng với hai phép toán: $+$, được gọi là cộng, và . được gọi là nhân thỏa mãn một số tiên đề. Tập $\mathbb{F}$ là nhóm giao hoán với phép cộng có phần tử đơn vị là *không* và được kí hiệu là 0; Tập $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ cũng là nhóm giao hoán với phép nhân có phần tử đơn vị là *một* và kí hiệu là 1; và phép nhân phân phối với phép cộng. Một trường là *hữu hạn* nếu số phần tử của $\mathbb{F}$ là hữu hạn; Số phần tử của $\mathbb{F}$ được gọi là *cấp* của $\mathbb{F}$.

Ví dụ 1.1. (i) Tập hợp các số nguyên $\mathbb{Z}$ không là một trường vì $3 \in \mathbb{Z}$ không khả nghịch.

(ii) Các tập hợp số hữu tỉ $\mathbb{Q}$, số thực $\mathbb{R}$, số phức $\mathbb{C}$ cùng với phép cộng và nhân, tạo thành một trường.

(iii) Tập hợp $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ đóng kín với phép cộng và nhân thông thường, và cùng với hai phép toán này, $\mathbb{Q}[\sqrt{2}]$ là một trường, phần tử không là $0 + 0\sqrt{2}$, phần tử đơn vị là $1 + 0\sqrt{2}$, phần tử đối của phần tử $a + b\sqrt{2}$ là $-a - b\sqrt{2}$ và nếu $x = a + b\sqrt{2} \neq 0 + 0\sqrt{2}$ thì nghịch đảo của x là $\dfrac{a}{a^2 - 2b^2} - \dfrac{b}{a^2 - 2b^2}\sqrt{2}$.

Ví dụ 1.2. Trường hữu hạn $\mathbb{F}_2$ với hai phần tử $\{0, 1\}$, phép cộng và phép nhân

được thực hiện như sau:

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

Đây cũng là vành của các số nguyên modulo 2.

Ví dụ 1.3. Trường hữu hạn $\mathbb{F}_3$ với ba phần tử $\{0, 1, 2\}$, phép cộng và phép nhân được cho bởi phép cộng và phép nhân modulo 3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Định nghĩa 1.2. (i) Nếu K là một trường con của E thì ta gọi E là một trường mở rộng của K, kí hiệu là E/K.

(ii) Giả sử E/K là một mở rộng trường. Xem E là một không gian véc tơ trên K. Nếu E là K - không gian véc tơ hữu hạn chiều thì ta nói E là *mở rộng bậc hữu hạn* của trường K. Nếu $\dim\ {}_KE = n$ thì n được gọi là *bậc của mở rộng* E/K và được kí hiệu là $[E/K]$.

Định nghĩa 1.3. Giả sử E/K là một mở rộng trường và $f(x) \in K[x]$ là đa thức bậc $n \geq 1$. Ta nói $f(x)$ *phân rã* trên E nếu

$$f(x) = a(x - \alpha_1) \dots (x - \alpha_n)$$