CÁC MÃ XYCLIC VÀ XYCLIC CỤC BỘ TRÊN VÀNH ĐA THỨC

Nguyễn Bình

Học viện Công nghệ Bưu chính Viễn thông, 122 Hoàng Quốc Việt, Cầu Giấy, Hà Nội

Email: *nguyenbinh@ptit.edu.vn*

Đến Tòa soạn: 14/12/2012; Chấp nhận đăng: 24/12/2012

TÓM TẮT

Các mã xyclic truyền thống được xây dựng trên các Ideal của vành đa thức. Do việc thực hiện đơn giản, các mã xyclic này được sử dụng rộng rãi trong thực tế. Bài báo này trình bày một lớp mã tuyến tính mới được gọi là các mã xyclic cục bộ (XCB). Các mã này được xây dựng trên các phân hoạch của vành đa thức theo các nhóm nhân xyclic. Các mã xyclic truyền thống được xem là một lớp con của các mã xyclic cục bộ.

Từ khóa: mã XCB (xyclic cục bộ), mã xyclic, vành đa thức, lũy đẳng, nhóm nhân xyclic, giải mã ngưỡng.

1. MỞ ĐẦU

Các mã khống chế sai (mã kênh) là hướng kiến thiết cho định lý mã hóa thứ hai của Shannon. Trong đó hướng chủ đạo là xây dựng các mã trên các cấu trúc đại số với quan điểm mã được xem là 1 tập con có cấu trúc trong một cấu trúc đại số nào đó. Thành tựu nổi bật trong hướng này là các mã xyclic truyền thống được xây dựng trên các Ideal trong vành đa thức với Ideal là phần tử không của vành các lớp đồng dư [1]. Do đặc tính bất biến đối với phép dịch vòng, các mã xyclic rất dễ thực hiện về mặt kĩ thuật và được áp dụng rất rộng rãi trong thực tế cho dù chúng thường không là các mã tốt do khả năng hạn chế trong việc lựa chọn các Ideal. Bài báo này đưa ra một quan điểm xây dựng một lớp mã tuyến tính mới là các mã xyclic cục bộ. Các mã này có khả năng lựa chọn lớn hơn nhiều so với các mã xyclic Ideal nhưng vẫn giữ được đặc tính xyclic (bất biến đối với phép dịch vòng) thuận tiện cho việc thực hiện kĩ thuật. Hơn nữa, theo quan điểm xây dựng các mã xyclic cục bộ, các mã xyclic truyền thống được xem là một lớp con đặc biệt của chúng.

2. PHÂN HOẠCH VÀNH ĐA THỨC VÀ CÁC MÃ XYCLIC CỤC BỘ

2.1. Nhóm nhân xyclic trên vành đa thức

Xét vành đa thức $\left(Z_2[x]/x^n+1\right)=Z_n$

Cho $a(x)\in Z_n$

Định nghĩa: Nhóm nhân xyclic A trên Zn là tập các luỹ thừa khác nhau của a(x)

$$A = \{a^i(x), i = 1, 2, ...\}$$

Cấp của phần tử sinh a(x) của nhóm

$$\text{ord a}(\text{x}) = |\text{A}|$$

Định lí [2]: Với n lẻ, cấp cực đại của một đa thức trong vành được xác định như sau:

$$\max \text{ord a}(\text{x}) = 2^{\text{m}} - 1$$

Với phân tích của $X^n + 1$: $X^n + 1 = \prod_i f_i(x)$

$f_i(x)$: đa thức bất khả quy

$$m = \max_i \deg f_i(x)$$

Với n chẵn: $n = 2^l(2t+1)$

$$X^n + 1 = \prod_i f_i(x)$$

$$m = \max_i \deg f_i(x)$$

$$\max \text{ord a(x)} = 2^{\text{l}}(2^{\text{m}} - 1)$$

Định nghĩa: Đa thức đối xứng (đa thức bù)

Đa thức đối xứng $\bar{a}(x)$ của đa thức a(x) được xác định như sau:

$$\bar{a}(x) = e_0(x) + a(x) \text{ với } e_0(x) = \sum_{i=0}^{n-1} x^i$$

Như vậy nếu $a(x) = \sum_{i \in I} a_i x^i$ thì $\bar{a}(x) = \sum_{j \in I} a_j x^j$

trong đó

$$I \cup J = S_n = \{0, 1, 2, ..., n-1\}$$
$$I \cap J = \phi$$

Bổ đề:

$$ord\, a(x) = ord\, \bar{a}(x)$$
$$\bar{a}^i(x) = \overline{a^i}(x)$$

Định nghĩa: Đa thức luỹ đẳng

Đa thức e(x) được gọi là luỹ đẳng nếu: $e^2(x) = e(x)$

Định nghĩa: Luỹ đẳng nuốt

Với n lẻ, đa thức $e_0(x) = \sum_{i=0}^{n-1} x^i$ là luỹ đẳng nuốt $e_0(x)$ có tính chất sau:

- $e_0^2(x) = e_0(x)$
- $a(x).e_0(x) = \begin{cases} 0 & \text{nếu } w(a(x)) - chan \\ e_0(x) & w(a(x)) - le \end{cases}$

2.2. Các lớp kề xyclic và các luỹ đẳng nguyên thuỷ

Định nghĩa: Các lớp kề xyclic theo modulo n là các tập sau:

$$C_i = \{i.2^j; j = 0,1,2....\}$$

Ta có: $S_n = \cup_i C_i$

Ví dụ:

$n = 7$

$C_0 = \{0\}; \quad C_1 = \{1,2,4\}; \quad C_3 = \{3,6,5\}$

$S_7 = C_0 \cup C_1 \cup C_3$

$n = 9$:

$C_0 = \{0\}; \quad C_1 = \{1,2,4,8,7,5\}; \quad C_3 = \{3,6\}$

$S_9 = C_0 \cup C_1 \cup C_3$

$n = 11$:

$C_0 = \{0\}; \quad C_1 = \{1,2,4,8,5,10,9,7,3,6\}$

$S_{11} = C_0 \cup C_{11}$

$n = 15$:

$C_0 = \{0\}; \quad C_1 = \{1,2,4,8\}; \quad C_3 = \{3,6,12,9\}; \quad C_5 = \{5,10\}; \quad C_7 = \{7,14,13,11\}$

$S_{15} = C_0 \cup C_1 \cup C_3 \cup C_5 \cup C_7$

Nhận xét: Với phân tích của $x^n + 1 = \prod_i f_i(x)$

$$\deg f_i(x) = |C_i|$$

Ví dụ: $n = 7$: $x^7 + 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$

Ta có: $|C_0| = 1, \quad |C_1| = 3, \quad |C_3| = 3$

– Các lũy đẳng nguyên thuỷ là các đa thức có chứa các đơn thức với số mũ thuộc C_i

Ví dụ: n = 7, các luỹ đẳng nguyên thuỷ

$$C_0 = \{0\} : e_1(x) = x^0 = 1$$
$$C_0 = \{1,2,4\} : e_2(x) = x + x^2 + x^4$$
$$C_3 = \{3,6,5\} : e_3(x) = x^3 + x^5 + x^6$$

– Tính chất của các luỹ đẳng nguyên thuỷ:

+ Tổng của hai luỹ đẳng nguyên thuỷ là một luỹ đẳng
+ Tích của hai luỹ đẳng nguyên thuỷ là một luỹ đẳng
+ Số các luỹ đẳng trong 1 vành:

$$N_e = 2^u - 1$$

với u – số các luỹ đẳng nguyên thuỷ

Ví dụ: n = 7, u = 3, N_e = 7

Các luỹ đẳng này là các đa thức

$e_1(x) = 1$, $e_2(x) = x + x^2 + x^4$, $e_3(x) = x^3 + x^5 + x^6$

$e_1(x) + e_2(x) = 1 + x + x^2 + x^4$, $e_1(x) + e_3(x) = 1 + x^3 + x^5 + x^6$

$e_2(x) + e_3(x) = x + x^2 + x^3 + x^5 + x^6$

$$e_1(x) + e_2(x) + e_3(x) = \sum_{i=0}^{6} x^i$$

Mỗi luỹ đẳng là một phần tử đơn vị của một nhóm nhân xyclic nào đó.

2.3. Phân hoạch của vành theo các nhóm nhân xyclic [3]

Xét tập các phần tử khác không của vành $Z_n^* = Z_n \setminus \{0\}$. Ta thực hiện phân hoạch vành theo một nhóm nhân xyclic A nào đó thành các lớp kề theo thuật toán sau:

VÀO: - Z_n^*

- $a(x) \in Z_n^*$ (*a(x)* được gọi là hạt nhân của phân hoạch)

RA: Phân hoạch của vành Z_n^*

Bước 1:

– Xây dựng nhóm nhân xyclic sinh bởi a(x): $A = \{a^i(x), i = 1,2,...\}$

– $Z_n^* = Z_n^* \setminus A$

Bước 2:

– Lấy $b(x) \in Z_n^*$

– Xây dựng cấp số nhân xyclic

$B = b(x).A = \{b(x).a^i(x), i = 1,2,...\}$

– $Z_n^* = Z_n^* \setminus B$

Bước 3:

Lặp lại bước 2 cho tới khi $Z_n^* = \phi$. Các kiểu phân hoạch khác nhau phụ thuộc vào cấp của a(x).

Định nghĩa: Một phân hoạch được gọi là không suy biến nếu nó chứa mọi phần tử của Z_n^*

Bổ đề: Phân hoạch vành là không suy biến nếu và chỉ nếu $w(a(x))$ lẻ

Với mọi giá trị n luôn tồn tại 3 kiểu phân hoạch chính sau:

– Phân hoạch cực tiểu: ord a(x) = 1, w(a(x))- lẻ

khi đó Z_n^* bao gồm $2^n - 1$ lớp kề, mỗi lớp kề là một phần tử trong Z_n^*

– Phân hoạch chuẩn: ord a(x) = n, w(a(x))- lẻ

trong kiểu phân hoạch chuẩn, mỗi lớp kề có lực lượng bằng n và ước của n.

– Phân hoạch cực đại: ord a(x) = max, w(a(x))- lẻ

Ví dụ: n = 5

Phân hoạch chuẩn: a(x) = x

1	2	4	8	16
3	6	12	24	17
5	10	20	9	18
7	14	28	25	19
11	22	13	26	21
15	30	29	27	23
31				

Ghi chú:

Biểu diễn nhị phân của các số mô tả đa thức tương ứng

Ví dụ: $21 = 2^0 + 2^2 + 2^4 \leftrightarrow 1 + x^2 + x^4$

Phân hoạch cực đại: $a(x) = 1 + x^2 + x^4 \leftrightarrow (024)$

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

$$\overline{A}=\begin{Bmatrix}(13),(12),(0234),(24),(23),(0134),(03),(34),(3),(0124),\\(14),(04),(0123),(02),(01),(1234)\end{Bmatrix}$$

Phân hoạch cực đại chỉ gồm 3 lớp kề

A
$\overline{A}$
(01234)

2.4. Định nghĩa mã XCB

Định nghĩa: Mã XCB là một mã tuyến tính có các dấu mã là một tập con không trống tuý ý các lớp kề trong phân hoạch của vành đa thức Zk theo một nhóm nhân xyclic nào đó.

Nhận xét:

– Nếu tập con này chứa nhóm nhân xyclic đơn vị $I=\left\{x^i, i=\overline{0,k-1}\right\}$ thì mã XCB là một mã hệ thống,

– Nếu chỉ chọn 1 lớp kề để tạo mã thì ta có mã xyclic,

– Nếu các lớp kề được chọn nằm trong 1 phân hoạch của vành theo một nhóm nhân xyclic thì ta có mã XCB đơn nhịp. Nếu các lớp kề được chọn nằm trong các phân hoạch khác nhau của vành thì ta có mã XCB đa nhịp. Nếu các lớp kề được chọn nằm trong các phân hoạch của các vành khác nhau thì ta có mã XCB trên các phân hoạch hỗn hợp [4].

– Các mã XCB được mô tả qua các trưởng lớp kề (phần tử đầu tiên của lớp kề) tạo mã.

VD: Mã XCB (15,5,7) được xây dựng từ các lớp kề {1,7,11} trong phân hoạch chuẩn.

1	2	4	8	16		7	14	28	25	19		11	22	13	26	21

5 dấu thông tin 10 dấu kiểm tra

Ma trận sinh:

$$G_{5.15}=\begin{pmatrix}1&0&0&0&0&1&0&0&1&1&1&0&1&0&1\\0&1&0&0&0&1&1&0&0&1&1&1&0&1&0\\0&0&1&0&0&1&1&1&0&0&0&1&1&0&1\\0&0&0&1&0&0&1&1&1&0&1&0&1&1&0\\0&0&0&0&1&0&0&1&1&1&0&1&0&1&1\end{pmatrix}$$

Mã xyclic (15, 5, 7) được xây dựng từ nhóm nhân xyclic $A=\left\{(024)^i, i=1,2\right\}$

Đây là một mã xyclic hệ thống có ma trận sinh:

$$G_{5.15} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

2.5. Nhóm nhân xyclic theo modulo [5]

Định lý: Nhóm nhân xyclic đơn vị theo modulo $h(x)$, $h(x)x^n + 1$.

$$A = \left\{ x^i \bmod h(x), i = 0,1,2,... \right\}$$

Là một mã xyclic ideal có đa thức sinh $g(x) = \left[\frac{x^n + 1}{h(x)} \right]^*$

Với $f^*(x)$ là đa thức đối ngẫu của f(x):

$$f^*(x) = x^{\deg f(x)} . f\left(x^{-1}\right)$$

Ví dụ: $n = 7$, $h(x) = 1 + x + x^3$

$$A = \left\{ 1, x, x^2, 1+x, x+x^2, 1+x+x^2, 1+x^2 \right\}$$

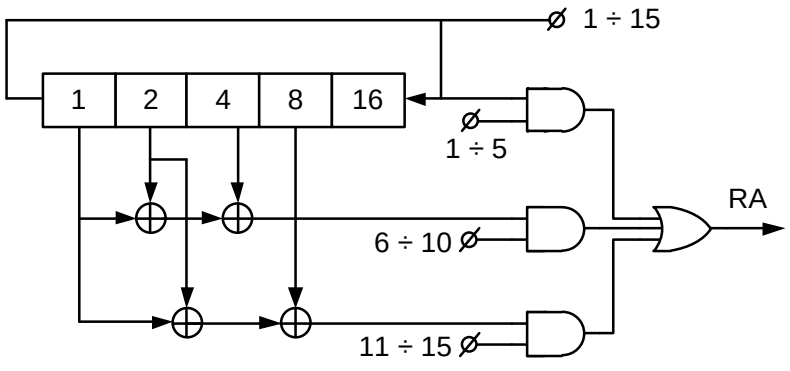
Ta có: $$\frac{x^7 + 1}{x^3 + x + 1} = 1 + x + x^2 + x^4$$

Như vậy A là 1 mã xyclic (7,3,4) có đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$

2.6. Mã hoá cho các mã XCB

Quá trình mã hoá cho các mã XCB là quá trình xây dựng các lớp kề tạo mã.

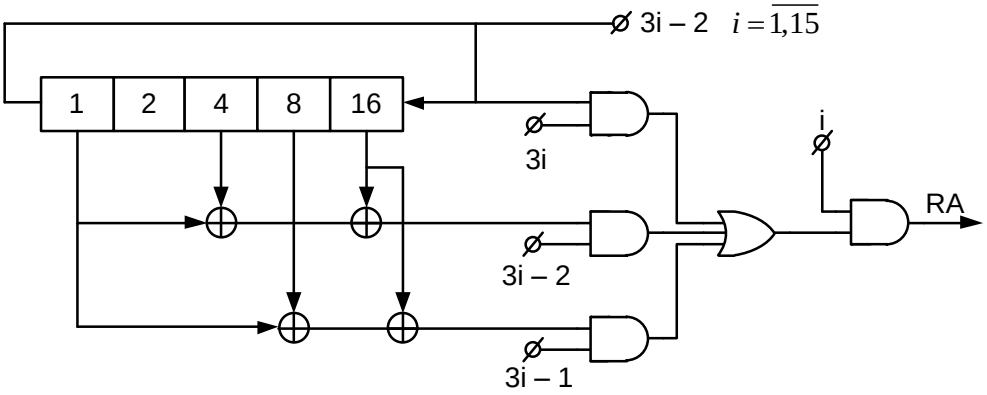
Ví dụ 1: Mã hoá cho các mã (15,5,7) trên phân hoạch chuẩn từ các lớp kề {1,7,11} (hình 2.1).



Hình 2.1. Bộ mã hóa cho mã (15,5,7)

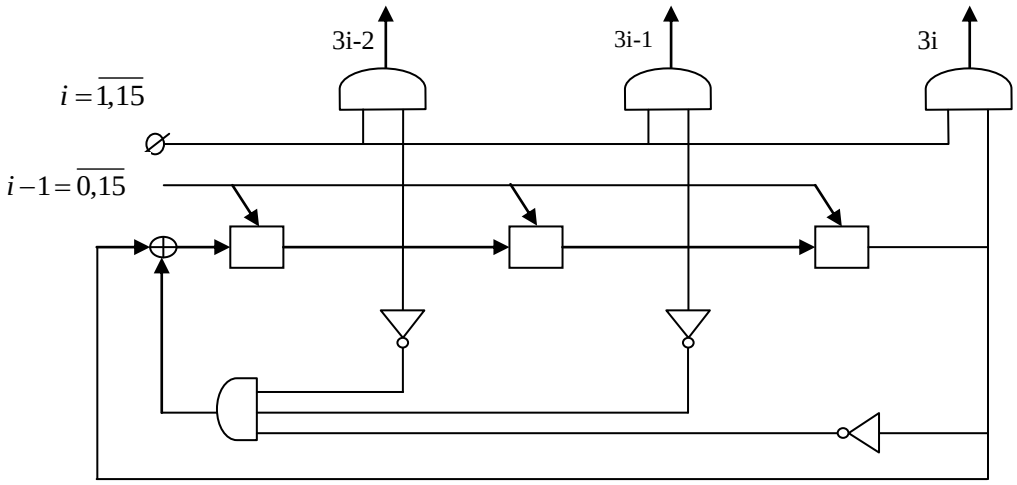
Ví dụ 2: Mã hoá cho mã (15,5,7) trên phân hoạch cực đại từ nhóm nhân xyclic (hình 2.2).

$$A = \left\{ (024)^i, i = 1,2,.... \right\}$$



Hình 2.2. Bộ mã hóa cho mã (15,5,7)

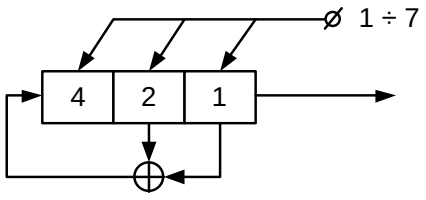
Bộ tạo xung nhịp tương ứng được mô tả trên hình 2.3.



Hình 2.3. Bộ tạo xung nhịp

Ví dụ 3: Mã hoá cho mã xyclic (7,3,4) xây dựng trên nhóm nhân xyclic (hình 2.4).

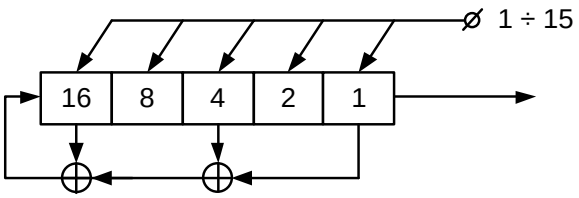
$$A = \left\{ x^i \bmod \left(1 + x + x^3\right), i = \overline{1,7} \right\}$$



Hình 2.4. Bộ mã hóa cho mã (7,3,4)

Ví dụ 4: Mã hoá cho mã xyclic (15,5,7) xây dựng trên nhóm nhân xyclic (hình 2.5).

$$A = \left\{ x^i \bmod x^5 + x^4 + x^2 + 1, i = \overline{0,14} \right\}$$



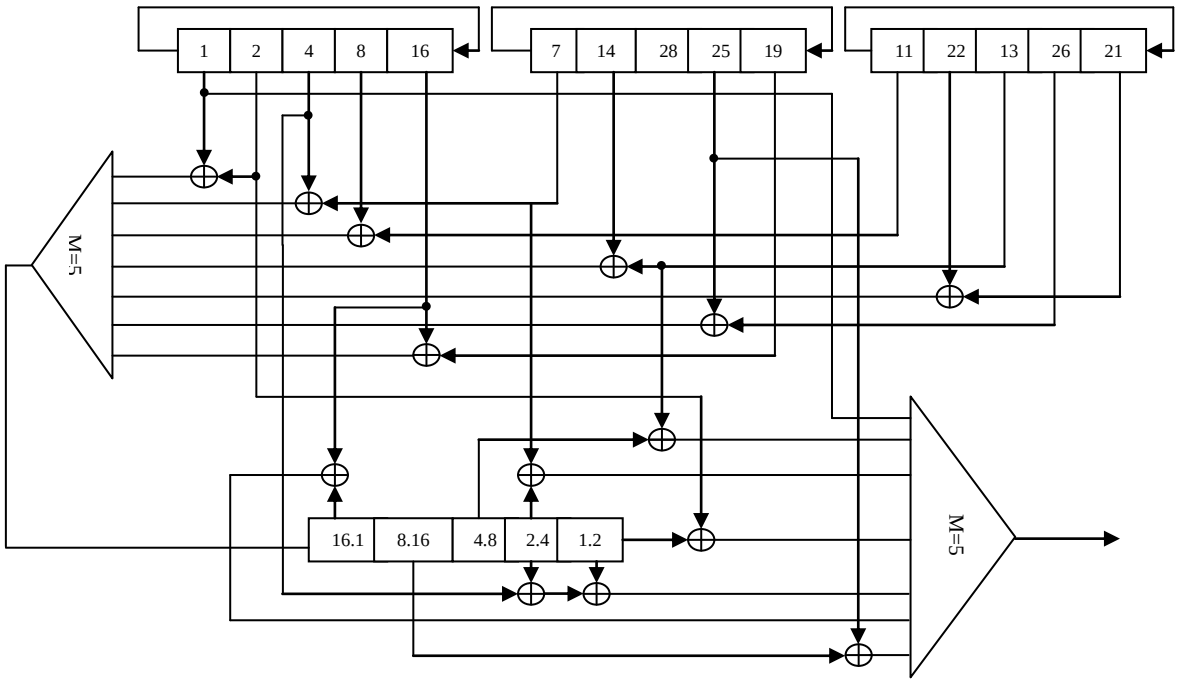
Hình 2.5. Bộ mã hóa cho mã (15,5,7)

$$A = \begin{Bmatrix} 1, x, x^2, x^3, x^4, 1+x^2+x^4, 1+x+x^2+x^3+x^4, 1+x+x^3, x+x^2+x^4, \\ 1+x^3+x^4, 1+x+x^2, x+x^2+x^3, x^2+x^3+x^4, 1+x^2+x^3, x+x^3+x^4 \end{Bmatrix}$$
$$= \left\{ 1, 2, 4, 8, 16, 21, 31, 11, 22, 25, 7, 14, 28, 13, 26 \right\}$$

2.7. Giải mã ngưỡng cho các mã XCB

Các mã XCB ở các ví dụ 1,2 & 4 là các mã có khả năng trực giao. Các mã này có thể giải mã được bằng các sơ đồ ngưỡng với 2 cấp.

Ví du 5: Giải mã ngưỡng cho mã (15,5,7) = {1,7,11} (hình 2.6).



Hình 2.6. Bộ giải mã ngưỡng 2 cấp cho mã (15,5,7)

Hoạt động:

– 15 nhịp đầu: Đưa các dấu mã nhận được vào các ô nhớ tương ứng
– 5 nhịp tiếp: Giải mã cho các cặp dấu mã
– 5 nhịp cuối: Giải mã cho từng dấu thông tin

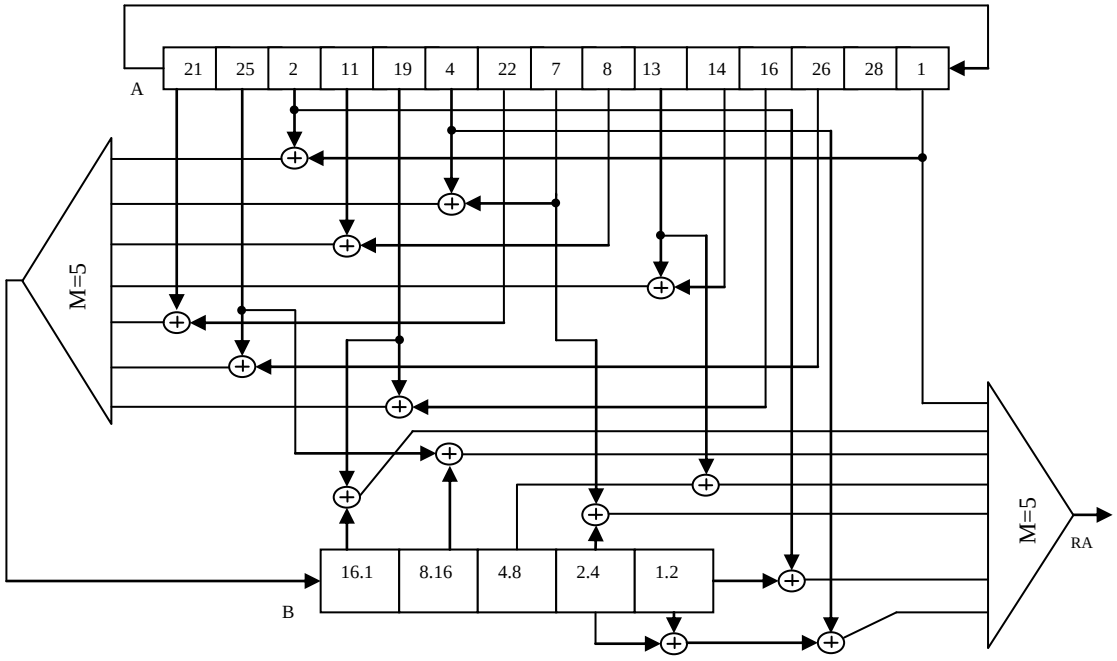
Ví dụ 6: Giải mã ngưỡng cho mã (15,5,7) xây dựng trên nhóm nhân xyclic (hình 2.7).

$$A = \left\{ (024)^i , i = \overline{1,15} \right\}$$

$$A = \{21, 25, 2, 11, 19, 4, 22, 7, 8, 13, 14, 16, 26, 28, 1\}$$

Hoạt động:

– 15 nhịp đầu: Ghi các dấu mã nhận được vào các ô nhớ tương ứng trong thanh ghi A
– Nhịp 16 th: giải mã cho cặp dấu 1.2
– Nhịp 19 th: giải mã cho cặp dấu 2.4
– Nhịp 22 th: giải mã cho cặp dấu 4.8
– Nhịp 25 th: giải mã cho cặp dấu 8.16
– Nhịp 28 th: giải mã cho cặp dấu 16.1
– Nhịp 31 th: giải mã cho dấu thông tin 1
– Nhịp 34 th: giải mã cho dấu thông tin 2
– Nhịp 37 th: giải mã cho dấu thông tin 4
– Nhịp 40 th: giải mã cho dấu thông tin 8
– Nhịp 43 th: giải mã cho dấu thông tin 16



Hình 2.7. Bộ giải mã ngưỡng 2 cấp cho mã (15,5,7)

Ví dụ 7: Giải mã cho mã xyclic (15,5,7) xây dựng trên nhóm nhân modulo (hình 2.8).

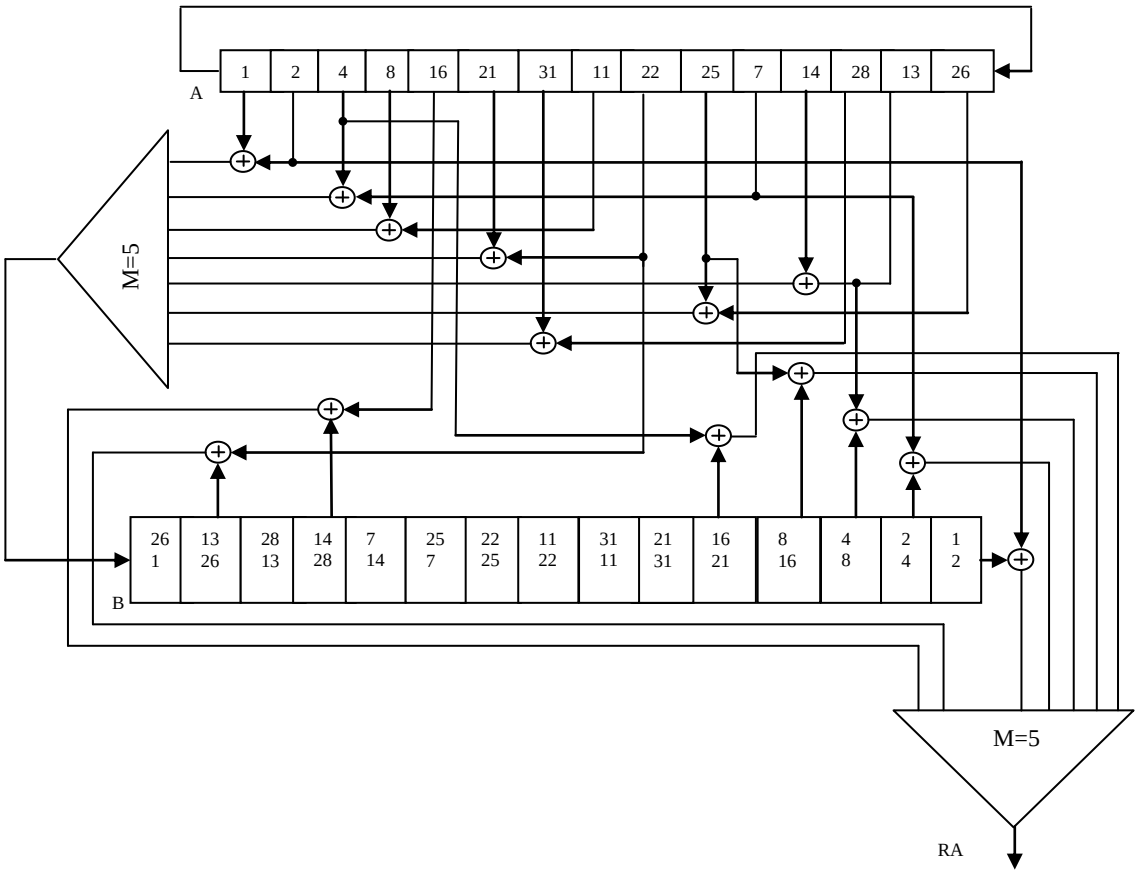
$$h(x) = x^5 + x^4 + x^2 + 1$$

$$A = \left\{ x^i \bmod h(x), i = \overline{0,14} \right\}$$

$$A = \{1, 2, 4, 8, 16, 21, 31, 11, 22, 25, 7, 14, 28, 13, 26\}$$

Hoạt động:

- 15 nhịp đầu: Đưa các dấu mã nhận được vào các ô nhớ;
- 15 nhịp tiếp: Giải mã cho các cặp dấu mã;
- 5 nhịp cuối: Giải mã cho các dấu thông tin.



Hình 2.8. Bộ giải mã ngưỡng 2 cấp cho mã (15,5,7)

3. PHÂN HOẠCH VÀNH ĐA THỨC THEO LỚP CÁC PHẦN TỬ LIÊN HỢP

3.1. Các thặng dư bậc 2 và các phần tử liên hợp [6]

Định nghĩa 3.1: Đa thức $f(x) \in Z_2[x]/x^n + 1$ được gọi là một thặng dư bậc 2 trong vành nếu $f(x) \neq 0$ và tồn tại g(x) sao cho: $g^2(x) \equiv f(x) \bmod x^n + 1$

Gọi Q_n là tập hợp chứa các thặng dư bậc 2.

Bổ đề 3.1: Với n lẻ mọi $f(x) \neq 0$ đều là thặng dư bậc 2. Mỗi f(x) đều có một căn bậc 2 duy nhất. Ta có: $|Q_n| = 2^n - 1$.

Bổ đề 3.2: Với n chẵn, $f(x) \in Q_n$ khi và chỉ khi f(x) là tổng của các đơn thức có mũ chẵn. Ta có: $|Q_n| = 2^{\frac{n}{2}} - 1$.

Bổ đề 3.3: Với n chẵn, các căn bậc 2 của một thặng dư bậc hai được xác định theo công thức sau:

$$g(x) = \left(1 + x^{\frac{n}{2}}\right)\left(\sum_{t \in U} x^t\right) + \sqrt{f(x)}.$$

trong đó U là một tập con tùy ý trong tập $S = \left\{0,1,...,\frac{n}{2} - 1\right\}$. Ta có $U = 2^{\frac{n}{2}}$. Nếu $f(x) = \sum f_i x^{2i}$ thì $\sqrt{f(x)} = \sum f_i x^i$ ($\sqrt{f(x)}$ được gọi là căn bậc 2 chính của $f(x)$).

Các g(x) được gọi là các phần tử liên hợp.

Ví dụ: n = 8.

Các căn bậc hai của các x^{2i} được cho trong bảng sau:

TT \ x^{2i}	x^2	x^4	x^6	x^8
1	(1)	(2)	(3)	(4)
2	(014)	(024)	(034)	(015)
3	(126)	(125)	(135)	(016)
4	(137)	(237)	(236)	(037)
5	(5)	(6)	(7)	(4)
6	(045)	(046)	(047)	(145)
7	(256)	(156)	(157)	(246)
8	(257)	(367)	(267)	(347)
9	(01246)	(01245)	(01345)	(01256)
10	(01347)	(02347)	(02346)	(01357)
11	(12367)	(12357)	(12356)	(02367)
12	(02456)	(01456)	(01457)	(12456)
13	(03457)	(03467)	(02467)	(13457)
14	(23567)	(13567)	(12567)	(23467)
15	(0123467)	(0123457)	(0123456)	(0123567)
16	(0234567)	(0134567)	(0124567)	(1234567)

Chú ý: Trong bảng trên ta kí hiệu các đa thức như sau:

Ví dụ: $(01246) \leftrightarrow 1+x+x^2+x^4+x^6$

$$\left(a_1+a_2+\ldots+a_s\right)^{p_n}=a_1^{p_n}+a_2^{p_n}+\ldots+a_s^{p_n}$$

Lớp chứa các phần tử liên hợp của một thặng dư bậc 2 được xem là một phần tử trong vành chứa các lớp này. Vành này được gọi là vành các phần tử liên hợp. Bằng cách sử dụng các phân hoạch trên các phần tử đơn vị và phần tử không của vành này ta có thể xây dựng được các mã XCB [6, 8, 9]).

Ngoài ra ta cũng có thể xây dựng được các hệ mật trên các cấp số nhân xyclic [7].

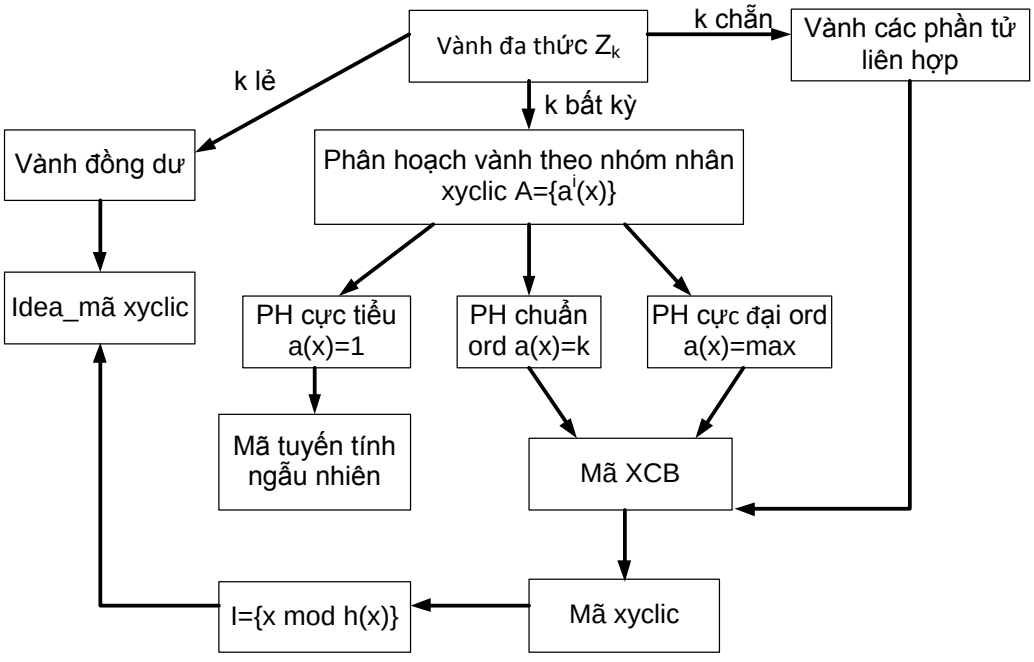
4. KẾT LUẬN

Các mã XCB được xây dựng có khả năng lựa chọn lớn hơn nhiều so với các mã xyclic truyền thống nhưng vẫn giữ được tính đơn giản của việc thể hiện kĩ thuật của các mã xyclic.

Ta có thể thấy rõ trên bảng so sánh sau:

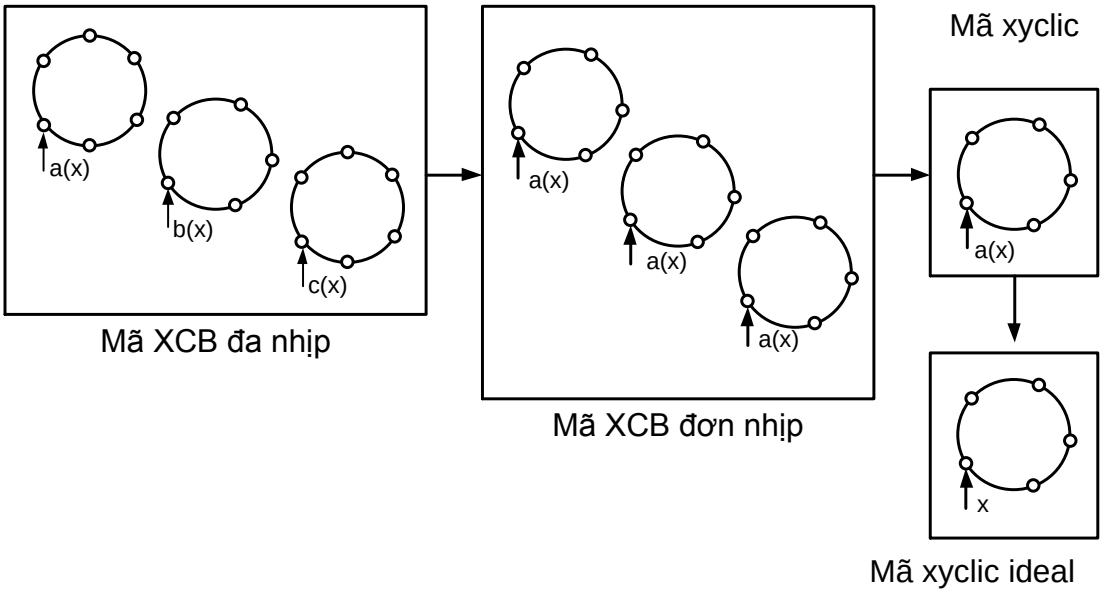
	Khả năng lựa chọn	Khả năng thể hiện kỹ thuật
Mã xyclic	Ít	Đơn giản
Mã xyclic cục bộ	Nhiều	Đơn giản
Mã tuyến tính ngẫu nhiên	Rất nhiều	Phức tạp

Ta có thể phân loại các mã tuyến tính xây dựng trên vành đa thức như trên hình 4.1.



Hình 4.1. Phân loại các mã tuyến tính trên vành đa thức

Các lớp mã XCB được mô tả trên Hình 4.2.



Hình 4.2. Các lớp mã XCB

TÀI LIỆU THAM KHẢO

1. Todd K. Moon – Error Correction Coding: Mathematical Methods and Algorithm. John Wiley & Sons, Inc, 2005.
2. Nguyen Binh, Le Dinh Thich – The Orders of Polynomials and Algorithms for Defining Order of Polynomial over Polynomial Ring, 5th Vietnam Conference on Automation (5th VICA), Hanoi, Vietnam, Oct 2002.
3. Nguyen Binh, Vu Viet, Pham Viet Trung – Decomposition of Polynomial Ring and Coding with Random Clock, CAFEO, 2000.
4. Ngo Duc Thien, Nguyen Binh – Some Local Cyclic Codes Based on Compound Decomposition of Two Polynomial Rings, International Conference on Advanced Technologies for Communications (ATC 2008 - REV'11), Hanoi, Vietnam, October, 2008.
5. Dang Hoai Bac, Nguyen Binh, Nguyen Xuan Quynh – Novel algebraic structure for cyclic codes, Applied Algebra, Algebraic Algorithms, and Error Correcting Codes –Conf. AAECC 17, LNCS 4851, pp 301-310, 2007, Springer-Verlag Berlin Heidelberg.
6. Nguyen Binh, Tran Duc Su, Pham Viet Trung - Decomposition of polynomial ring according to the classes of conjugate elements, AIC-26, Hanoi, Vietnam, 2001.
7. Nguyen Binh – Crypto-System Based on Cyclic Geometric Progressions over Polynomial Ring (Part I&II), REV'02, Vietnam, 2002.
8. Ngô Đức Thiện – Các mã xyclic cục bộ xây dựng trên các phân hoạch hỗn hợp, Luận án Tiến sỹ Kỹ thuật, Học viện Công nghệ Bưu chính Viễn thông, 2010.

9. Đặng Hoài Bắc – Các mã xyclic và xyclic cục bộ trên các vành đa thức có 2 lớp kề xyclic, Luận án Tiến sỹ Kỹ thuật, Học viện Công nghệ Bưu chính Viễn thông, 2010.

ABSTRACT

CYCLIC AND LOCAL CYCLIC CODES OVER POLYNOMIAL RING

Nguyen Binh

Posts and Telecommunications Institue of Technology, 122 Hoang Quoc Viet, Hanoi, Vietnam

Email: *nguyenbinh@ptit.edu.vn*

Traditional cyclic codes are constructed on Ideals of Polynomial ring. Depending on simple technical implementation, these codes are used widely in practice. In this paper, a new class of linear codes is presented. They are called local cyclic codes (LCC). These codes are constructed on decompositions of polynomial ring according to the cyclic multiplicative groups. Traditional cyclic codes are considered as a subclass of Local Cyclic Codes.

Keywords: Local cyclic codes, cyclic codes, polynomial ring, idempotent, cyclic multiplicative group, threshold decoding.