

Chương 4. Mã Cyclic

Câu 1.6: Chứng minh rằng nếu $g(x)$ là đa thức sinh của một mã cyclic (n, k) bất kỳ thì hệ số tự do $g_0 = 1$

Câu 1.17: Định nghĩa mã cyclic

Câu 2.17: Cho mã cyclic $(7,4)$ với đa thức sinh $g(x) = x^3 + x^2 + 1$.

a. Hỏi mã này có khả năng phát hiện và sửa bao nhiêu sai?

b. Tìm từ mã hệ thống đầu ra với đầu vào $m = 1111$

Câu 2.21: Tìm mã cyclic $(8,5)$ trên vành đa thức $\mathbb{Z}_2[x]/x^8 + 1$. Tìm khoảng cách Hamming của mã đó.

Câu 2.22:

Mã nào dưới đây là mã cyclic? Mã nào dưới đây tương đương với một mã cyclic?

(a) $C1 = 0000; 1110; 1011; 0111; 1101$

(b) $C2 = 111; 100; 010; 001$

(c) $C3$ với ma trận sinh $G1$:

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(d) $C4$ với ma trận sinh $G2$:

$$G_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Câu 2.23:

Cho mã cyclic $(7,4)$ có đa thức sinh $g(x) = 1 + x + x^3$. Hãy xây dựng ma trận sinh G và ma trận kiểm tra H ở dạng hệ thống của mã này.

Câu 2.24:

Cho mã cyclic $(15,8)$ có $g(x) = x^7 + x^6 + x^4 + 1$. Hãy xây dựng ma trận sinh G và ma trận kiểm tra H ở dạng hệ thống?

Câu 2.26:

Hãy phân tích nhị thức $x^7 + 1$ thành tích của các đa thức bất khả quy và mô tả tất cả các mã cyclic có độ dài $n = 7$ trên vành đa thức $\mathbb{Z}_2[x]/x^7 + 1$



Lý thuyết thông tin – Đức Huy

Câu 2.27:

Hãy phân tích nhị thức $x^{15} + 1$ thành tích của các đa thức bất khả quy và tính số lượng các mã cyclic có độ dài $n = 15$ trên vành đa thức $\mathbb{Z}_2[x]/x^{15} + 1$.

Câu 2.28:

Cho mã cyclic $(7, 4, 3)$ có $g(x) = 1 + x + x^3$. Giả sử từ mã nhận được của bộ mã trên có dạng: $v(x) = x^6 + x^5 + x^4 + x^3 \leftrightarrow 0001111$. Hãy sử dụng thuật toán chia dịch vòng (bẩy lỗi) để tìm lại từ mã đã phát?

Câu 2.29:

Cho $g(x) = x^8 + x^6 + x^4 + x^2 + 1$ là đa thức trên trường nhị phân.

- Tìm mã cyclic có tỉ lệ mã $r_1 = k/n$ nhỏ nhất với đa thức sinh là $g(x)$.
- Tìm khoảng cách Hamming của bộ mã ở câu a.

Câu 2.30:

Xét đa thức $g(x) = x + 1$ trên trường nhị phân.

- Chứng minh rằng đa thức này có thể tạo ra một mã cyclic với n bất kỳ. Tìm k tương ứng.
- Chọn một giá trị n bất kỳ. Tìm dạng hệ thống của G và H của mã được tạo nên bởi $g(x)$.

Câu 3.4:

Cho mã cyclic $(7, 3)$ với đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$.

- Xây dựng sơ đồ mã hóa theo phương pháp nhân.
- Tìm từ mã đầu ra với bản tin đầu vào $m = 111$.
- Kiểm tra lại kết quả ở câu b) bằng thuật toán mã hóa theo phương pháp nhân.

Câu 3.6:

Xét một mã cyclic nhị phân tuyến tính hệ thống $(9, 3)$ có đa thức sinh $g(x) = 1 + x^3 + x^6$.

- Xây dựng mạch lập mã hệ thống cho mã theo thuật toán chia.
- Mô tả hoạt động của mạch, tìm từ mã đầu ra tương ứng với khối tin vào $a = 101$.
- Kiểm tra kết quả câu b) bằng thuật toán tương ứng.

Câu 3.8:

Cho mã cyclic $(7, 4)$ có đa thức sinh $g(x) = 1 + x + x^3$. Hãy mô tả sơ đồ chức năng của thiết bị mã hoá hệ thống cho bộ mã này theo phương pháp chia. Giả sử đa thức thông tin $a(x) = 1 + x^2 + x^3$. Hãy tìm từ mã ở đầu ra của thiết bị và kiểm tra lại bằng thuật toán 4 bước tạo từ mã hệ thống.



Lý thuyết thông tin – Đức Huy

Câu 3.9:

Cho mã cyclic $(7,3)$ có đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$. Hãy mô tả sơ đồ chức năng của thiết bị mã hoá hệ thống cho bộ mã này theo phương pháp nhân. Giả sử đa thức thông tin $a(x) = 1 + x^2$. Hãy tìm từ mã ở đầu ra của thiết bị và kiểm tra lại bằng thuật toán tạo từ mã hệ thống theo phương pháp nhân.

Câu 3.10:

- Xây dựng một mã cyclic $(6,2)$ trên trường $Z_2[x]/x^6 + 1$.
- Tìm ma trận G dạng hệ thống của mã này và tìm tất cả các từ mã của bộ mã.
- Mã này có thể sửa bao nhiêu lỗi?

Câu 4.1:

Cho mã cyclic $(7,3)$ có đa thức sinh $g(x) = 1 + x + x^2 + x^4$.

- Vẽ sơ đồ mã hóa cho bộ mã theo phương pháp nhân.
- Hỏi mã này có khả năng sửa được bao nhiêu sai?
- Giả sử phía phát phát đi từ mã 0011101. Do có lỗi nên phía thu nhận được từ mã bị sai ở vị trí x^5 . Hãy sử dụng thuật toán chia dịch vòng để tìm lại từ mã đã phát.

Câu 4.2:

Cho mã cyclic $(7,3)$ với đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$.

- Vẽ sơ đồ mã hóa theo phương pháp chia.
- Khoảng cách Hamming của bộ mã bằng bao nhiêu?
- Vẽ sơ đồ giải mã cho mã này theo phương pháp tổng kiểm tra trực giao.
- Giả sử phía thu nhận được từ mã $c = x^2 + x^4 + x^6 = 0010101$. Thực hiện giải mã để tìm ra từ mã đã phát.

Câu 4.4:

Gọi C là một mã cyclic nhị phân có độ dài từ mã là 15 bit và được tạo ra bởi đa thức sinh $g(x) = x^5 + x^3 + x + 1$

- Hãy chứng tỏ rằng $g(x)$ là một đa thức sinh hợp lệ của một mã cyclic có độ dài từ mã là 15 bit. Tìm đa thức kiểm tra của mã C .
- Tính số bit thông tin của mã C và số từ mã trong mã C .
- Tạo ma trận sinh và ma trận kiểm tra cho mã C .
- Vẽ sơ đồ hệ thống thiết bị thực hiện mã C theo phương pháp chia có dư. Hãy lập bảng phân tích hoạt động của hệ thống thiết bị để tính từ mã ưng với đa thức bản tin $x^9 + x^4 + x^2 + 1$.



Lý thuyết thông tin – Đức Huy

Câu 4.7:

Cho mã cyclic (15,7) và đa thức $g(x) = x^8 + x^7 + x^6 + x^4 + 1$

- Chứng minh rằng $g(x)$ có thể là đa thức sinh của mã cyclic (15,7).
- Vẽ sơ đồ tạo mã theo phương pháp chia và giải thích ngắn gọn nguyên lý hoạt động của mạch.
- Xác định từ mã dạng hệ thống tương ứng với bản tin $m(x) = x^3 + x$ (theo thuật toán)
- Đa thức $d(x) = x^{14} + x^{12} + x^8 + x + 1$ có phải là một từ mã của bộ mã không? Vì sao?

Câu 4.8:

Cho mã cyclic (15,8) và đa thức $g(x) = x^7 + x^6 + x^4 + 1$

- Chứng minh rằng $g(x)$ có thể là đa thức sinh của mã cyclic (15,8)
- Vẽ sơ đồ tạo mã theo phương pháp chia và giải thích ngắn gọn nguyên lý hoạt động của mạch.
- 16
- Xác định từ mã dạng hệ thống tương ứng với bản tin $m(x) = x^2 + x$ (theo thuật toán).
- Đa thức $d(x) = x^{10} + x^9 + x^8 + x + 1$ có phải là một từ mã của bộ mã không? Vì sao?

Câu 4.9:

Cho $x^{15} + 1 = (1 + x)(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$.

- Tìm mã cyclic (15,3) trên vành $\mathbb{Z}_2[x]/x^{15} + 1$.
- Liệt kê 4 từ mã bất kỳ của bộ mã (15,3) trên vành này.
- Vẽ sơ đồ tạo mã cyclic (15,3) bằng phương pháp chia.
- Sử dụng thuật toán tìm từ mã đầu ra biết bản tin đầu vào $m = 1 + x$

