
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



Trần Thị Miên

NGHIÊN CỨU THUẬT TOÁN GIẢI MÃ LDPC

Chuyên ngành: Kỹ thuật Điện tử

Mã số: 60.52.70

Người hướng dẫn khoa học: GS. TS NGUYỄN BÌNH

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - 2012

MỞ ĐẦU

Trong các hệ thống truyền tin số ngày nay, để chống nhiễu trên kênh truyền, nâng cao chất lượng thông tin đều phải sử dụng mã kênh.

Năm 1962, một họ mã kênh mới đã được Gallager giới thiệu trong luận án tiến sĩ của ông có chất lượng tiệm cận giới hạn Shannon trên kênh tạp âm trắng Gauss cộng cỡ vài phần trăm dB, đó là mã kiểm tra chẵn lẻ mật độ thấp LDPC. Mã LDPC là một lớp của mã khối tuyến tính có khả năng đạt chất lượng gần tới giới hạn dung lượng kênh. Các ứng dụng của mã LDPC đã và đang được thực hiện trong các hệ thống truyền dẫn số với tốc độ truyền dẫn cao, độ chính xác lớn. Tuy nhiên, so với các bộ mã khác thì thuật toán giải mã lặp LDPC khá phức tạp, số lượng vòng lặp nhiều yêu cầu số lượng tính toán quá lớn, làm cho tốc độ giải mã chậm gây độ trễ truyền tin cao. Vì thế, sau gần 35 năm ra đời, loại mã này đã không phát huy được khả năng của nó.

Ngày nay, với sự phát triển vượt bậc của công nghệ tính toán, xử lý và lưu trữ dữ liệu cùng với các thuật toán mới được nghiên cứu, ứng dụng cho nên những vấn đề

khó khăn về mã LDPC đã lần lượt được giải quyết. Hiện nay, trên thế giới đã và đang có nhiều nghiên cứu quá trình giải mã nhằm cải tiến, giảm số lượng tính toán để nâng cao tính khả thi của bộ mã này. Cùng với khoa học của thế giới, em đã chọn luận văn: “Nghiên cứu thuật toán giải mã LDPC”. Luận văn tập trung chủ yếu đến một số nội dung cơ bản sau:

Chương 1: Tổng quan về mã LDPC. Chương này đề cập một cách tổng quan về mô hình chung của hệ thống thông tin số, về lý thuyết mã kênh, tìm hiểu những lý thuyết cơ bản nhất về mã LDPC, từ đó đặt ra vấn đề nghiên cứu của luận văn.

Chương 2: Thuật toán giải mã LDPC. Chương này phân tích quá trình giải mã LDPC sử dụng thuật toán giải mã chuẩn đã được công bố và giải mã cải tiến sử dụng thuật toán dừng nút và dừng sớm.

Chương 3: Đánh giá các thuật toán giải mã LDPC trên AWGN.

Chương 1 - TỔNG QUAN VỀ MÃ LDPC

Giới thiệu chương

Chương này đề cập một cách tổng quan về mô hình chung của hệ thống thông tin số, về lý thuyết mã kênh, tìm hiểu những lý thuyết cơ bản nhất về mã LDPC, từ đó đặt ra vấn đề nghiên cứu của luận văn.

Định nghĩa mã LDPC

Do mã LDPC là một lớp mã khối tuyến tính nên nó có các đặc trưng của mã khối tuyến tính. Chuỗi bit tin chiều dài là k sau khi được mã hoá sẽ thành một từ mã có chiều dài tương ứng là n . Tỷ lệ mã ở đây là $R = k / n$ và có $n - k$ bit kiểm tra. Kích thước ma trận kiểm tra là $H_{(n-k),n}$. Từ mã c được tạo ra phải thoả mãn điều kiện $c.H^T = 0$. Trong đó H^T là ma trận chuyển vị của ma trận H .

Người ta đã chứng minh được các mã LDPC không đều có độ dài khối lớn có thể tiệm cận giới hạn Shannon. Về cơ bản đây là một loại mã khối tuyến tính có đặc điểm là các ma trận kiểm tra chẵn lẻ (H) là các ma trận thưa (sparse matrix), tức là có hầu hết các phần tử là 0, chỉ một số ít là 1 hay mật độ các phần tử 1 là thấp.

Phân loại mã LDPC

Thông thường người ta chia mã LDPC thành hai loại:

+ Nếu trọng lượng các hàng của ma trận H đều bằng nhau và bằng ρ đồng thời trọng lượng các cột của ma trận H cũng bằng nhau và bằng γ thì mã LDPC được tạo ra gọi là mã LDPC đều (n, γ, ρ) , trong đó n là độ dài khối của mã và cũng chính là số cột của ma trận H .

+ Nếu trọng lượng các hàng và trọng lượng các cột của ma trận kiểm tra chẵn lẻ H là không đồng nhất mà chúng thay đổi đối với từng hàng, từng cột thì ta có mã LDPC không đều.

Người ta đã chứng minh được rằng các mã LDPC không đều cho hiệu quả tốt hơn các mã LDPC đều.

Biểu diễn mã LDPC

Có hai cách biểu diễn mã LDPC đó là biểu diễn thông qua ma trận kiểm tra chẵn lẻ H và biểu diễn thông qua đồ hình Tanner.

Mầm (Girth) của một đồ hình Tanner là chiều dài của một chu kỳ nhỏ nhất trong đồ hình. Chu kỳ nhỏ nhất có thể chấp nhận được đối với một đồ hình Tanner là 4. Người ta đã chứng minh được rằng các đồ hình Tanner có

chu vi nhỏ hơn 4 sẽ làm giảm hiệu quả của mã LDPC. Khi xây dựng mã LDPC đạt chất lượng tốt, ta cần tránh để xảy ra các chu kỳ nhỏ xuất hiện, cố gắng tạo ra các chu kỳ lớn.

Mã hóa LDPC

- Mã hóa LDPC dùng ma trận sinh G

Các mã LDPC được định nghĩa trên cơ sở là ma trận kiểm tra chẵn lẻ H , từ ma trận H ta xây dựng ma trận sinh G theo phương pháp khử Gauss - Jordan. Phương pháp này đưa ma trận H về dạng:

$$H = [A, I_{n-k}] \quad (1.10)$$

Ma trận sinh G được xác định theo công thức:

$$G = [I_k, A^T] \quad (1.11)$$

Từ mã thu được là:

$$\begin{aligned} c = uG &= [u_1 \ u_2 \ \dots \ u_k] [I_k, A^T] \\ c &= [c_1 \ c_2 \ \dots \ c_n] \end{aligned} \quad (1.12)$$

Tuy nhiên vấn đề khó khăn ở phương pháp này là ma trận G không bảo đảm được tính thưa như ma trận H . Phương trình mã hóa $c = uG$ được thực hiện ở bộ mã hóa có độ phức tạp gần chính xác bằng n^2 phép tính. Đối với các mã có độ dài từ mã lớn, hàng ngàn đến hàng trăm ngàn bit thì bộ mã hóa sẽ trở nên cực kỳ phức tạp. Để

giảm bớt tính phức tạp trong mã hóa ta có thể sử dụng các ma trận có dạng cấu trúc. Tuy nhiên với những ma trận có tính ngẫu nhiên ta có thể sử dụng phương pháp mã hóa trực tiếp trên ma trận H thông qua biến đổi H về dạng ma trận tam giác dưới. Phương pháp này được trình bày ở phần sau đây.

- Mã hóa LDPC dùng ma trận kiểm tra chẵn lẻ H

Khác với phương pháp trên là tìm ma trận G từ ma trận H cho trước sau đó thực hiện mã hóa với G . Một mã LDPC cũng có thể được mã hóa bằng việc sử dụng trực tiếp ma trận H nhờ biến đổi về dạng gần tam giác dưới. Ý tưởng của phương pháp này là sử dụng chủ yếu các hoán vị hàng và cột sao cho vẫn giữ được đặc điểm thừa của ma trận H .

Trước hết chỉ hoán vị hàng và cột để đưa ma trận về dạng gần như tam giác dưới:

$$H_t = \begin{bmatrix} A & B & T \\ C & D & E \end{bmatrix} \quad (1.13)$$

Với T là ma trận tam giác dưới, g gọi là phần khuyết, nói một cách gần đúng thì g càng nhỏ độ phức tạp của mã hóa càng thấp.

Quá trình định dạng tam giác trên, phép khử Gauss - Jordan được ứng dụng một lần tương đương với việc

nhân ma trận $\begin{bmatrix} I_{m-g} & 0 \\ -ET^{-1} & I_g \end{bmatrix}$ với ma trận H_t

$$\tilde{H} = \begin{bmatrix} I_{m-g} & 0 \\ -ET^{-1} & I_g \end{bmatrix} H_t = \begin{bmatrix} A & B & T \\ \tilde{C} & \tilde{D} & 0 \end{bmatrix} \quad (1.14)$$

Ở đây:

$$\begin{aligned} \tilde{C} &= -ET^{-1}A + C \\ \tilde{D} &= -ET^{-1}B + D \end{aligned} \quad (1.15)$$

Khi thực hiện phép khử Gauss - Jordan để xóa E thì chỉ có \tilde{C} , \tilde{D} bị ảnh hưởng còn các phần khác của ma trận kiểm tra chẵn lẻ vẫn giữ nguyên đặc tính thừa của nó.

Cuối cùng để mã hóa bản tin sử dụng ma trận \tilde{H} , từ mã $c = [c_1 \ c_2 \ \dots \ c_n]$ được chia thành các phần như $c = [u \ p_1 \ p_2]$ với $u = [u_1 \ u_2 \ \dots \ u_k]$ là k bit thông tin, $p_1 = [p_{1_1} \ p_{1_2} \ \dots \ p_{1_g}]$ là g bit kiểm tra đầu và $p_2 = [p_{2_1} \ p_{2_2} \ \dots \ p_{2_{m-g}}]$ là các bit kiểm tra còn lại.

Nếu \tilde{D} là ma trận khả nghịch, ta tính được p_1 theo công thức:

$$p_1 = \tilde{D}^{-1} \tilde{C} u \quad (1.17)$$

Nếu \tilde{D} không khả nghịch thì ta hoán vị các hàng của \tilde{H} đến khi có thể. Khi tìm được p_1 ta tính p_2 theo phương trình:

$$p_2 = -T^{-1}(Au + Bp_1) \quad (1.18)$$

Các ma trận A , B và T rất thưa do đó độ phức tạp của phương trình này rất thấp, khi T là ma trận dạng tam giác trên nên p_2 có thể được tính bằng phép thay thế ngược lại.

Giải mã LDPC

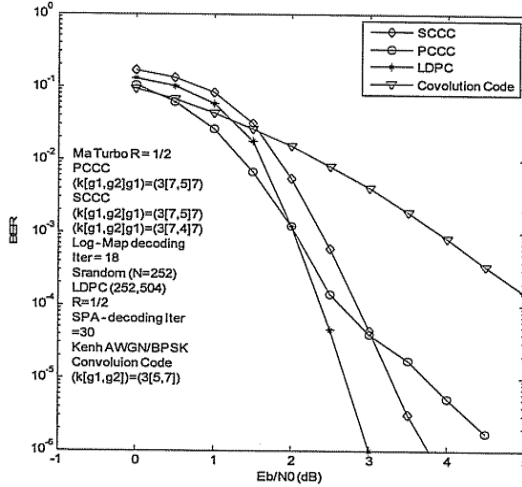
Thuật toán giải mã lặp LDPC sẽ được phân tích kỹ hơn ở chương 2.

Đánh giá chất lượng giải mã LDPC

Đã có nhiều công trình nghiên cứu hiệu quả của mã LDPC so với một số bộ mã kênh có khả năng sửa lỗi mạnh khác như mã chập, mã Turbo. Việc so sánh thực hiện trên cùng một số tham số như cùng độ dài khối của mã, cùng tỉ lệ mã, trên cùng một kênh truyền và sử dụng cùng một kiểu điều chế. Các kết quả đều cho thấy LDPC tốt hơn các mã khác.

Mặc dù các mã khảo sát ở hình vẽ 1.8 có chiều dài từ mã ngắn song kết quả vẫn phản ánh được đúng như

nhận định trên. Hình này còn cho thấy mã LDPC có chất lượng tốt hơn mã chập và mã Turbo trên kênh AWGN, điều chế BPSK lý tưởng với $R = 1/2$ và $n = 504$.



Hình 1.8: So sánh chất lượng LDPC với các mã khác

Với các mã LDPC chất lượng tăng theo chiều dài từ mã, đặc biệt các mã có chiều dài lớn hơn 1000 bit cho chất lượng rất cao. Vì thế họ mã này được phân chia tương đối thành các loại mã dài khi $n > 1000$, mã trung bình là từ 1000 đến 10000, còn lại là mã ngắn. Các hệ thống yêu cầu chất lượng cao thường sử dụng mã dài, tuy nhiên cái giá phải trả là thời gian giải mã lớn, điều đó đồng nghĩa với việc yêu cầu một hệ thống xử lý nhanh và

hiệu quả. Đây cũng là lý do mà loại mã này bị lãng quên trong một thời gian khá dài. Tất nhiên với công nghệ tính toán như hiện nay, vấn đề này không còn là quá khó bởi hàng loạt các cố gắng về công nghệ, tốc độ xử lý và các biện pháp cải tiến thuật toán mã hóa.

Kết luận chương

Chương 1 đã đề cập một cách tổng quát về hệ thống thông tin số, cơ sở về lý thuyết mã kênh của Shannon, phân tích khái niệm, đặc điểm và đánh giá chất lượng của mã LDPC. Từ đây, luận án hướng tới nghiên cứu thuật toán giải mã LDPC để tìm hiểu rõ hơn về loại mã này.

Chương 2 - THUẬT TOÁN GIẢI MÃ LDPC

Giới thiệu chương

Chương này phân tích quá trình giải mã LDPC sử dụng thuật toán giải mã chuẩn đã được công bố và giải mã cải tiến sử dụng thuật toán dùng nút và dùng sớm.

Các thuật toán giải mã LDPC chuẩn đã được công bố

Thuật toán giải mã trên miền xác suất

Ta có thể tóm tắt các bước trong giải mã trên miền xác suất thành những bước sau:

1. Với $i = 0, 1, 2, \dots, n-1$, đặt $P_i = P_r(c_i = 1 | y_i)$ trong đó y_i là tín hiệu thu được thứ i trên kênh truyền.

2. Cập nhật $\{r_{ji}(b)\}$ bằng các biểu thức:

$$r_{ji}(0) = \frac{1}{2} + \frac{1}{2} \prod_{i' \in V_j \setminus i} (1 - 2q_{i'j}(1))$$

$$r_{ji}(1) = 1 - r_{ji}(0)$$

3. Cập nhật $q_{ij}(b)$ sử dụng các biểu thức:

$$q_{ij}(0) = K_{ij}(1 - P_i) \prod_{j' \in C_{i \setminus j}} r_{ji'}(0)$$

$$q_{ij}(1) = K_{ij}P_i \prod_{j' \in C_{i \setminus j}} r_{ji'}(1)$$

4. Với $i = 0, 1, 2, \dots, n-1$, tính:

$$Q_i(0) = K_i(1 - P_i) \prod_{j \in C_i} r_{ji}(0) \quad (2.10)$$

$$Q_i(1) = K_i P_i \prod_{j \in C_i} r_{ji}(1) \quad (2.11)$$

Trong đó K_i được chọn sao cho thỏa mãn

$$Q_i(0) + Q_i(1) = 1$$

5. Với $i = 0, 1, 2, \dots, n-1$, đặt:

$$c_i = \begin{cases} 1 & \text{khi } Q_i(1) > Q_i(0) \\ 0 & \text{khi } Q_i(1) < Q_i(0) \end{cases} \quad (2.12)$$

Nếu $\mathcal{L}H^T = 0$ hoặc số lần lặp cực đại đã đạt được thì dừng tính toán, còn không thì trở lại bước 2.

Thuật toán giải mã SPA trên miền Log

Tương tự thuật toán giải mã Viterbi, thuật toán giải mã SPA theo xác suất khá phức tạp với nhiều phép tính nhân phải thực hiện. Để dễ dàng hơn trong kỹ thuật, người ta thường thực hiện phép tính cộng để thay thế phép tính nhân. Ngoài ra, phép tính theo xác suất còn có thể dẫn đến giới hạn của phép tính số trên máy tính. Do vậy thuật toán giải mã SPA thường được thực hiện trên miền log.

Ta có thể tóm tắt thuật toán giải mã SPA trên miền log như sau:

1. Với $i = 0, 1, 2, \dots, n-1$, khởi tạo $L(q_{ij})$ cho kênh AWGN theo như biểu thức (2.14) đối với tất cả i, j ứng với $h_{ij} = 1$:

$$L(q_{ij}) = L(c_i) = 2y_i / \sigma^2$$

2. Cập nhật $\{L(r_{ji})\}$ theo biểu thức:

$$L(r_{ji}) = \prod_{i' \in V_j \setminus i} \alpha_{i'j} \cdot \phi \left(\sum_{i' \in V_j \setminus i} \phi(\beta_{i'j}) \right)$$

$$\phi(x) = -\log[\tanh(x/2)] = \log \frac{e^x + 1}{e^x - 1}$$

3. Cập nhật $\{L(q_{ij})\}$ theo biểu thức (2.22):

$$L(q_{ij}) = L(c_i) + \sum_{j' \in C_i \setminus j} L(r_{ji'})$$

4. Cập nhật $\{L(Q_i)\}$ theo biểu thức (2.23):

$$L(Q_i) = L(c_i) + \sum_{j' \in C_i} L(r_{ji'})$$

5. Với $i = 0, 1, 2, \dots, n-1$, đặt: $\hat{c}_i = \begin{cases} 1 & \text{khi } L(Q_i) < 0 \\ 0 & \text{khi } L(Q_i) > 0 \end{cases}$

Nếu $\mathcal{L}H^T = 0$ hoặc số lần lặp cực đại đã đạt được thì dừng tính toán, còn không thì trở lại bước 2. Quá trình giải mã được thực hiện một cách lặp đi lặp lại như vậy trên đồ thị Tanner cho đến khi thành công hoặc đạt tới ngưỡng dừng.

Giải mã LDPC cải tiến bằng thuật toán dừng nút và dừng sớm

Giới thiệu vấn đề

Khi phân tích quá trình giải mã ta sẽ nhận thấy sau một số lần lặp từ mã, đầu ra có thể là một từ mã hợp lệ hoặc không hợp lệ nhưng nếu tiếp tục giải mã lặp thì số bit lỗi không giảm hoặc giảm không đáng kể. Nếu phát hiện trường hợp thứ hai, bộ giải mã có thể thoát khỏi vòng lặp sớm hay còn gọi là dừng sớm (Early Stopping - ES) nhằm giảm số lượng tính toán không cần thiết. Một phương pháp ES đã được nghiên cứu ứng dụng cho mã Turbo và LDPC, trong đó chỉ tiêu để đánh giá sự hồi quy của thuật toán giải mã lặp là hệ số tương quan chéo CE:

$$T(\gamma) = \sum_i T_i(\gamma) = \sum_i \frac{|\Lambda e_i^{(\gamma)} - \Lambda e_i^{(\gamma-1)}|^2}{\exp|\Lambda e_i^{(\gamma)}|} \quad (2.25)$$

Với:

$$\Lambda e_i^{(\gamma)} = \sum_{j \in C_i} L^{(\gamma)}(r_{ji}) \quad (2.26)$$

được gọi là thông tin ngoài cho từng nút bit thứ i . Khi giải mã lặp LDPC với thuật toán giải mã là SPA, $T(\gamma)$ được tính cho từng lần lặp và so sánh với ngưỡng T_e , $T_e = (10^{-2} \div 10^{-4})T(1)$. Và khi $T(\gamma') < T_e$ thì có thể dừng tại lần lặp γ' . Nhược điểm của phương pháp sử dụng ES này là phải tính toán (2.25) theo hàm mũ và phải lưu các giá trị cụ thể $\Lambda e_i^{(\gamma-1)}$ dùng để tính toán cho lần lặp thứ γ .

Để giảm số lượng tính toán trong giải mã lặp LDPC, các nhà nghiên cứu còn xây dựng thuật toán dừng nút. Họ đã đưa ra phương pháp loại bỏ nút (Node Elimination) hay dừng nút theo tỷ số LLR với các nút $V^{(s)} = [v_i^{(s)}]$ được gọi là các nút dừng SN (Stopping Node hay Sleeping Node). Tại các nút dừng thì $L^{(\gamma)}(r_{ji})$ và $L^{(\gamma)}(q_{ij})$ ứng với nút tin thứ i đó sẽ không cần phải tính mới mà lấy giá trị tại lần lặp γ' đã quyết định dừng trước đó. Với thuật toán trên, ta có thể giảm được khá lớn phép tính toán. Để xác định các nút dừng, có thể quan sát giá trị tuyệt đối của tỷ số hợp lý LLR $|L_i^{(\gamma)}|$ sau mỗi lần lặp. Nếu

ứng với nút tin v_i có $|L_i^{(\gamma)}|$ lớn thì nút đó được quyết định là nút dừng. Các nhà nghiên cứu đã đưa ra chỉ tiêu nút tin là nút dừng khi:

$$|L_i^{(\gamma)}| > \log \frac{1-a}{a} \quad (2.27)$$

trong đó a là giá trị được xác định phụ thuộc vào E_b/N_0 .

Thuật toán giải mã LDPC sử dụng phương pháp dừng nút này được ký hiệu là SPA-SN(a).

Dưới đây là thuật toán giải mã LDPC cải tiến bằng phương pháp dừng nút và dừng sớm dựa theo sự thay đổi dấu liên tiếp của quyết định cứng cho phép giảm số lượng phép tính, giảm số vòng lặp mà chất lượng suy giảm không đáng kể.

Thuật toán dừng nút và dừng sớm trong giải mã LDPC

Trước tiên, ta định nghĩa các nút dừng là các nút tin có dấu của tỷ số hợp lý LLR tương ứng không thay đổi sau L lần lặp liên tiếp.

Ta ký hiệu tập hợp các nút bit là $V^{(s)} = [v_i^{(s)}]$ và từ mã sau khi quyết định cứng tại lần lặp thứ γ là

$Y^{(\gamma)} = (\hat{y}_1^{(\gamma)}, \hat{y}_2^{(\gamma)}, \dots, \hat{y}_N^{(\gamma)})$ tương ứng với các nút bit (v_1, v_2, \dots, v_n) . Giả thiết thuật toán hồi quy có thể xác định các nút SN bằng cách so sánh giá trị của $c_1^{(\gamma)}$ theo các lần lặp. Nếu $\hat{y}_i^{(\gamma)} = \hat{y}_i^{(\gamma-1)} = \dots = \hat{y}_i^{(\gamma-L)}$ với L là số lượng các bit được quan sát thì nút $v_i^{(s)}$ được gọi là nút SN. Khi đó thì:

$$F_i^{(\gamma)} = \sum_{j=\gamma-L}^{\gamma} \hat{y}_i^{(j)} = L \quad (2.28)$$

với $\hat{y}_i^{(j)} = \pm 1$.

Nếu trong trường hợp chỉ xem xét L lần lặp đầu tiên thì có thể sử dụng phương pháp cộng tích lũy để giảm bộ nhớ trong đó hàm thăm dò cho từng nút v_i là $F_i^{(\gamma)}$ với:

$$F_i^{(\gamma)} = \begin{cases} F_i^{(\gamma-1)} + 1, & \hat{y}_i^{(\gamma)} = \hat{y}_i^{(\gamma-1)} \\ 0, & \hat{y}_i^{(\gamma)} \neq \hat{y}_i^{(\gamma-1)} \end{cases} \quad (2.29)$$

và nút v_i được quyết định là nút dừng khi $F_i^{(\gamma)} = L$.

Thuật toán LDPC sử dụng phương pháp dừng nút bằng cách kiểm tra dấu liên tiếp của bit mã này được ký hiệu là SPA-SN(L).

Khi xác định là các nút dừng thì trong quá trình tính toán lặp tại các nút SN, các biểu thức (2.20), (2.22) và

(2.23) không cần phải thực hiện tính toán mà chỉ nhận giá trị tại lần lặp γ' . Nghĩa là:

$$L^{(\gamma)}(r_{ji}) \Big|_{i \in V^s} = L^{(\gamma')} (r_{ji}) \Big|_{i \in V^s} \quad (2.30)$$

$$L^{(\gamma)}(q_{ij}) \Big|_{i \in V^s} = L^{(\gamma')} (q_{ij}) \Big|_{i \in V^s} \quad (2.31)$$

$$L_i^{(\gamma)}(Q_i) \Big|_{i \in V^s} = L_i^{(\gamma')} (Q_i) \Big|_{i \in V^s} \quad (2.32)$$

Như vậy, các ma trận $L(r_{ji})$ và $L(q_{ij})$ không được đề cập tại các nút SN, do đó có thể giảm được số lượng tính toán của bộ giải mã tại từng lần lặp $\gamma > \gamma'$. Ở đây, ta cũng nhận thấy khi sử dụng phương pháp dừng nút, nếu tất cả các nút bit đều là nút dừng thì có thể thực hiện ES để giảm số lần lặp mặc dù đầu ra của bộ giải mã chưa phải là một từ mã hợp lệ. Vì vậy, ta có một tiêu chí mới để thực hiện ES là:

$$\sum_{j=\gamma-L}^{\gamma} |c_i^{(j)}| = L, \quad \forall i, i = 1, 2, \dots, n \quad (2.33)$$

Phương pháp ES này cũng khá đơn giản với L các bộ nhớ dừng mạch logic và phép cộng (2.33).

Kết luận chương

Như chương 2 đã trình bày, thuật toán giải mã LDPC do Gallager đề xuất ban đầu là MPA, trong đó tính toán được thực hiện trên miền xác suất. Sau đó để đơn giản các phép tính nhân thành các phép tính cộng, thuật toán SPA được đưa ra. Trong thuật toán này, việc tính toán được thực hiện dựa trên tỷ số hợp lý theo hàm log. Chương 2 còn đưa ra định nghĩa về các nút dừng theo dấu liên tiếp của LLR trong giải mã lặp LDPC. Các nút này có thể được xem là đủ độ tin cậy để thực hiện quyết định cứng khi dấu của nó không thay đổi sau một số lần lặp liên tiếp cho trước. Nhờ vậy mà tại các lần lặp tiếp theo, việc tính toán cập nhật thông tin cho các nút này là không cần thiết. Chương 2 đã đưa ra thuật toán giải mã dựa trên các nút dừng, kết hợp dừng sớm mới là SPA-SN(L) cho phép giảm đáng kể độ phức tạp trong tính toán. Chương 3 sẽ thực hiện đánh giá thuật toán SPA và SPA-SN(L) này.

Chương 3 - ĐÁNH GIÁ CÁC THUẬT TOÁN GIẢI MÃ LDPC TRÊN KÊNH AWGN

Giới thiệu chương

Để thuận tiện cho việc so sánh hiệu quả của thuật toán giải mã LDPC đã nêu ở chương 2, chương 3 sẽ thực hiện đánh giá các thuật toán giải mã SPA và SPA-SN(L) trên kênh AWGN.

Đánh giá các thuật toán giải mã LDPC chuẩn trên kênh AWGN

Để đánh giá chất lượng của bộ giải mã LDPC, ta sử dụng một số mã của Mackay và dựa vào chương trình mô phỏng thuật toán giải mã SPA trên miền log với kênh AWGN, thực hiện điều chế BPSK lý tưởng với số lượng từ mã lỗi tương ứng $E_b / N_0 \leq 1dB$, $1dB \leq E_b / N_0 \leq 2dB$, $E_b / N_0 \geq 2dB$ là 300, 200, 100.

Kết quả mô phỏng cho thấy:

- Chất lượng phụ thuộc rất nhiều vào độ dài từ mã. Độ dài từ mã càng lớn hay kích thước ma trận H càng lớn thì chất lượng hệ thống đạt được càng cao, đồ thị tiến gần về giới hạn lý thuyết.

- Số lượng vòng lặp càng lớn, chất lượng giải mã càng cao và vì thế thời gian giải mã cũng tăng, tuy nhiên quan hệ này không phải là tuyến tính vô hạn. Lý do khi thực hiện xây dựng mã dù là ngẫu nhiên hay có cấu trúc cũng không tránh khỏi sự xuất hiện của các chu kỳ hữu hạn. Kết quả là đồ thị chất lượng của mã sẽ hội quy, sàn lồi xuất hiện. Cũng vì vấn đề này mà khi xây dựng mã cần chú ý tránh các trường hợp xảy ra các chu kỳ ngắn nhất là bằng 4.

Vấn đề đặt ra là làm sao giảm thiểu được thời gian giải mã, tận dụng ưu điểm của các mã dài và chất lượng của nó khi số vòng lặp lớn, đáp ứng các dịch vụ truyền thông yêu cầu thời gian thực như hệ thống thoại, thông tin vô tuyến di động hay cố định. Hướng giải quyết bài toán hiện tại cho mã LDPC là cần thiết phải có các bộ giải mã ít độ phức tạp hơn, thời gian xử lý ngắn hơn song độ lợi mã hóa giảm đi không đáng kể.

Đánh giá giải mã LDPC cải tiến bằng thuật toán dùng nút và dùng sớm trên kênh AWGN

Xét bộ giải mã LDPC có tỷ lệ mã hóa là $1/2$, kích thước (504, 252). Giả thiết điều chế BPSK là lý tưởng và

kênh truyền AWGN có trung bình bằng 0 và phương sai $\sigma^2 = N_0 / 2$ (N_0 là mật độ phổ công suất song biên). Giá trị của L có thể chọn theo kết quả mô phỏng là $L = 7, 9$ hoặc 11 và số lần lặp cực đại của thuật toán giải mã LDPC được giả thiết là $\gamma_{\max} = 50$.

Kết quả mô phỏng cho thấy:

- Với L đủ lớn ($L \geq 7$), chất lượng của thuật toán giải mã SPA-SN(L) bị suy giảm khoảng 0.2 dB tại vùng E_b / N_0 nhỏ. Tại vùng E_b / N_0 lớn, chất lượng của thuật toán giải mã mới chỉ suy giảm khoảng 0.1 dB.
- Tại vùng E_b / N_0 nhỏ, khi giải mã LDPC với SPA-SN thì số lần lặp trung bình giảm đi đáng kể. Cụ thể như vùng $0 \leq E_b / N_0 \leq 1.5dB$ số lần lặp trung bình giảm được hơn 50%, tại vùng E_b / N_0 lớn tỷ lệ này giảm dần và hội quy.
- Kết quả so sánh thời gian chạy chương trình mô phỏng trên Laptop Core 2 Duo CPU T7250 2GHz với các thuật toán SPA. SPA-SN ($L = 7$) có số lượng tử mã lỗi tương ứng giá trị của E_b / N_0 giống lần so sánh trước, ta nhận thấy rằng thời gian chạy chương trình của thuật toán SPA-

SN so với thuật toán SPA giảm đi đáng kể tại mọi vùng của E_b/N_0 . Có thể nói rằng thuật toán SPA-SN giảm được 10 lần số lượng các phép tính so với thuật toán SPA thông thường.

- Hệ số phức tạp tính toán của thuật toán dừng nút và dừng sớm giảm thật đáng kể tại vùng E_b/N_0 nhỏ, SPA-SN(L) giảm gần 80% so với SPA thông thường.
- Để giảm thiểu độ phức tạp tính toán, giảm số lần lặp, đơn giản trong thực hiện mà chất lượng vẫn đảm bảo tốt, ta chọn các giá trị $L = 7, 9, 11$ là tối ưu nhất.

Kết luận chương

Chương 3 đã cho ta thấy hệ số phức tạp tính toán của thuật toán dừng nút và dừng sớm giảm gần 80% so với SPA thông thường. Thuật toán giải mã SPA-SN($L = 11$) có chất lượng kém hơn so với SPA tại vùng E_b/N_0 nhỏ khoảng 0.2 dB nhưng lại có chất lượng tốt hơn tại vùng E_b/N_0 lớn khoảng 0.3 dB. Trong khi đó thuật toán dừng nút và dừng sớm chỉ có nhược điểm là chất lượng bị suy giảm khoảng 0.1 đến 0.2 dB tại giá trị E_b/N_0 nhỏ, đây là lượng suy giảm chất lượng có thể chấp nhận được.

KẾT LUẬN VÀ KIẾN NGHỊ

Luận án nghiên cứu một cách chi tiết về mã LDPC, đưa ra các thuật toán giải mã LDPC chuẩn đã được công bố và giải mã LDPC cải tiến bằng thuật toán dừng nút và dừng sớm. Trên cơ sở phân tích các thuật toán giải mã lặp LDPC, tôi đã đưa ra phương án đánh giá các thuật toán giải mã đã nêu trên trên kênh truyền có nhiễu trắng cộng.

Luận án này tập trung nghiên cứu trên đối tượng kênh truyền có nhiễu trắng cộng mà chưa khảo sát trên các mô hình kênh khác. Vì vậy, hướng nghiên cứu tiếp theo sẽ là đánh giá hiệu quả của các thuật toán cải tiến này trên mô hình kênh pha đỉnh.

Để hoàn thành luận văn này, tôi xin được gửi lời cảm ơn chân thành tới **GS.TS Nguyễn Bình**, người trực tiếp hướng dẫn, chỉ bảo, định hướng và giúp đỡ hết mực tận tình trong suốt thời gian qua.

Do có sự hạn chế về thời gian nên bản luận văn không tránh khỏi những thiếu sót. Tôi rất mong được sự góp ý của các thầy để kiến thức về mã LDPC của tôi có thể phong phú hơn.