Sử dụng mã LDPC trong thông tin di động số

Low-Density Parity-Check Code for Mobile Communications

Lê Tiến Thường, Nguyễn Hữu Phương,
Nguyễn Chí Kiên, Hoàng Đình Chiến

Abstract: *In this paper, we firstly describe a relatively new class of channel codes called LDPC codes. Then present an iterative decoding algorithm for LDPC codes based on the message passing algorithm is presented. We construct an LDPC code with small block length using the column permutation method to run simulation on Matlab and on a Motorola's DSP kit. The simulation of a wireless communication system on Matlab shows that this LDPC code has good performance over AWGN and Rayleigh fading channels. The DSP-program used the iterative decoding algorithm for the LDPC code gives appropriate results, as verified by corresponding Matlab programs.*

I. KHÁI NIỆM MÃ LDPC

Mã LDPC (Low-Density Parity-Check code – Mã kiểm tra chẵn lẻ mật độ thấp), hay còn gọi là mã Gallager, được đề xuất bởi Gallager vào năm 1962 [1]. Ngày nay, 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. Theo định nghĩa của Gallager, ma trận kiểm tra chẵn lẻ của mã LDPC còn có đặc điểm là mỗi hàng chứa đúng i phần tử 1 và mỗi cột chứa đúng j phần tử 1. Một mã LDPC như vậy sẽ được gọi là một mã LDPC đều (n, j, i), trong đó n là độ dài khối của mã và cũng chính là số cột của ma trận H. Hình 1 trình bày ma trận kiểm tra chẵn lẻ của một mã LDPC đều (20, 3, 4).

Tại thời điểm ra đời của mã LDPC, năng lực tính toán của máy tính còn khá hạn chế nên các kết quả mô phỏng không phản ảnh được khả năng kiểm soát lỗi cao của mã này. Cho đến tận gần đây, đặc tính vượt trội của mã LDPC mới được chứng minh và Mackay và Neal là hai người được coi là đã phát minh ra mã LDPC một lần nữa nhờ sử dụng giải thuật giải mã dựa trên giải thuật tổng-tích (sum-product algorithm).

1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	1	0
0	0	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0
1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0
0	0	0	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
0	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1
0	0	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1	0	0
0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0
0	1	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	0

Hình 1 Ma trận kiểm tra chẵn lẻ của một mã LDPC đều (20, 3, 4)

Từ định nghĩa ban đầu của Gallager, Luby cùng các tác giả khác đã đánh dấu một bước tiến quan trọng của mã LDPC trong việc đưa ra khái niệm mã LDPC không đều [2]. Đặc điểm của các mã này là trọng lượng hàng cũng như trọng lượng cột không đồng nhất. Các kết quả mô phỏng cho thấy các mã LDPC không đều được xây dựng phù hợp có đặc tính tốt hơn các mã đều. Tiếp theo đó, Davey và Mackay khảo sát các mã không đều trên GF(q) với q>2 (GF: Galois Field – Trường Galois). Theo các tác giả này, khả năng kiểm soát lỗi của loại mã trên GF(q) được cải thiện đáng kể so với các mã trên GF(2) [3].

Việc biểu diễn mã LDPC bằng đồ hình (graph) đóng vai trò quan trọng trong việc xây dựng các giải thuật giải mã. Tanner được coi là người đề xuất các mã dựa trên đồ hình [4]. Nhiều nhà nghiên cứu khác đã phát triển các đồ hình Tanner và các đồ hình thừa số (factor graph) chính là một dạng tổng quát của đồ hình Tanner. Các giải thuật giải mã xác xuất lặp

thường được sử dụng để giải mã cho mã LDPC. McEliece cùng các tác giả khác đã chứng minh rằng các giải thuật giải mã này có thể được xây dựng từ giải thuật truyền belief Pearl, hay còn gọi là giải thuật truyền thông báo (message passing algorithm), một giải thuật được sử dụng khá phổ biến trong ngành trí tuệ nhân tạo [5]. Kschischang cùng các tác giả khác đã tổng quát hoá giải thuật truyền thông báo để xây dựng giải thuật tổng-tích [6]. Đây là một giải thuật có thể được áp dụng trong nhiều ngành khoa học kĩ thuật như trí tuệ nhân tạo, xử lí tín hiệu và thông tin số.

Cấu trúc các mã LDPC cũng là một đề tài nghiên cứu của nhiều nhà lí thuyết thông tin. Các phương pháp được sử dụng có thể là các phương pháp giải tích hoặc ngẫu nhiên. Cấu trúc đầu tiên của mã LDPC được đề xuất bởi Gallager sử dụng phương pháp hoán vị ngẫu nhiên cột ma trận [1]. Với mục đích giảm số lượng vòng kín ngắn (short cycle) trong đồ hình Tanner của mã LDPC, Mackay đã đưa ra một số cấu trúc ngẫu nhiên khác, với các ma trận kiểm tra chẵn lẻ có số bit 1 chồng nhau giữa hai cột bất kì không quá 1 [7]. Trong khi đó, các phương pháp tạo mã giải tích chủ yếu dựa trên hình học hữu hạn (finite geometry) và thiết kế tổ hợp (combinatorial design). Kou cùng các tác giả khác đã đề xuất bốn lớp mã LDPC dựa trên hình học Ơ-clit (Euclidean geometry) và hình học chiếu (projective geometry) [8]. Do đặc điểm là các mã này có thể được đưa về dạng mã vòng (cyclic) hoặc gần-vòng (quasi-cyclic), nên việc mã hoá có thể sử dụng thanh ghi dịch. Các mã LDPC dựa trên thiết kế tổ hợp được xây dựng từ các hệ Steiner và hệ Kirkman, một trường hợp đặc biệt của hệ Steiner. Mackay và Davey đã khảo sát các mã từ hệ Steiner cho các ứng dụng độ dài khối thấp và tỉ lệ mã cao. Các mã này không có các vòng kín độ dài 4, tuy nhiên đặc tính khoảng cách Hamming tối thiểu của chúng khá kém. Hiện nay, các mã xây dựng trên các hệ ba Kirkman (Kirkman triple system) đang được nghiên cứu tại Đại học New Castle (Úc) [9].

II. GIẢI THUẬT GIẢI MÃ LẶP SỬ DỤNG HIỆU LIKELIHOOD

1. Mạng belief

Mạng belief hay còn được gọi là mạng Bayes, mạng nhân quả (causal network), mạng xác suất (probabilistic network), hay bản đồ tri thức (knowledge map), là một khái niệm rất phổ biến trong ngành trí tuệ nhân tạo. Theo Russell và Norvig [10], mạng belief là một cấu trúc dữ liệu mô tả quan hệ giữa các biến ngẫu nhiên và xác định phân bố hiệp xác suất của chúng. Đây là một đồ hình mạng với những đặc điểm sau:

– Mỗi một nút mạng biểu diễn một biến ngẫu nhiên.
– Một mũi tên từ nút X đến nút Y biểu diễn tác động trực tiếp từ X lên Y. Khi đó, X được gọi là nút cha của Y.
– Tại mỗi nút mạng có một bảng xác suất có điều kiện (Conditional Probability Table – CPT) xác định ảnh hưởng của các nút cha lên nút mạng đang xét.
– Sơ đồ mạng là sơ đồ có hướng và không có các vòng kín (Directed, Acyclic Graph – DAG)

Khái niệm căn bản trong mạng belief chính là Belief. Belief(x_i) được định nghĩa là xác suất có điều kiện, hay xác suất hậu nghiệm (a posteriori probability), để một biến X_i nhận giá trị x_i, cho trước dấu hiệu e.

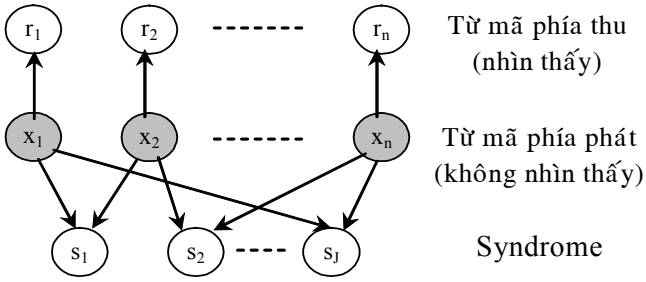
$$Bel(x_i) = p(x_i|e) \quad (1)$$

Người ta đã nhận thấy có thể dùng mạng belief để biểu diễn quan hệ giữa các bit trong từ mã ban đầu, từ mã bị tạp âm và syndrome của một mã LDPC như trong hình 2. Từ đó, bằng cách áp dụng các công thức truyền belief của mạng belief, chúng ta có thể xây dựng giải thuật giải mã lặp dựa trên xác suất cho mã LDPC.

2. Giải thuật truyền belief

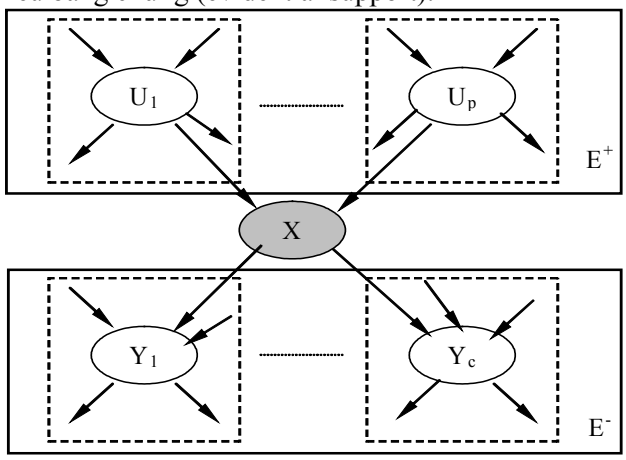
Phần này mô tả tóm tắt giải thuật truyền belief hay còn gọi là giải thuật Pearl [11]. Giải thuật Pearl có thể được sử dụng để tính các xác suất có điều kiện của một tập các biến, cho trước giá trị của các biến dấu hiệu. Trên một đồ thị có hướng, không có vòng kín

(DAG) G, giải thuật truyền belief Pearl là một giải thuật truyền thông báo phân tán trong đó các đỉnh của G trao đổi thông tin về xác suất của chúng. Mỗi nút mạng nhận các thông báo từ các nút cha và nút con của nó, sử dụng các thông báo này để cập nhật belief của bản thân, sau đó gửi các thông báo mới cho các nút cha và nút con.



Hình 2 Mạng belief của mã LDPC

Một ví dụ về mạng belief được cho trong Hình 3. Ở đây, X là biến truy vấn và E là tập các biến dấu hiệu (X không thuộc E). Giả sử ta phải tính P(X|E). Kí hiệu $U = U_1, \ldots, U_p$ là tập các nút cha và $Y = Y_1, \ldots, Y_c$ là tập các nút con của X. Tập dấu hiệu E cho trước có thể được viết lại thành $E = E_i^+ \bigcup E_i^-$, trong đó E_i^+ là dấu hiệu từ các nút mạng ở phía trên (phía các nút cha ông) và E_i^- là dấu hiệu từ các nút mạng ở phía dưới (các nút con cháu). E_i^+ và E_i^- lần lượt được gọi là xác nhận kiểu nhân quả (causal support) và xác nhận kiểu bằng chứng (evidential support).



Hình 3 Một ví dụ về mạng belief

Khi đó, quá trình lặp truyền belief tại một nút X_i có thể được tóm tắt một cách định tính sau:

– Sau khi nhận các bản tin μ từ tất cả các nút cha và các bản tin λ từ tất cả các nút con, X_i cập nhật Belief của bản thân.

– X_i tính toán và gửi đi các bản tin μ cho các nút con Y_j.

– X_i tính toán và gửi đi các bản tin λ đến các nút cha U_j.

– Sau một số vòng lặp, giải thuật dừng lại và giá trị của X_i có thể được quyết định dựa trên Belief của nó.

Như đã nói trong phần A, mạng belief có thể được sử dụng để biểu diễn quan hệ giữa từ mã ban đầu, từ mã nhận được và syndrome của mã LDPC. Vì vậy giải thuật giải mã lặp cho mã LDPC có thể được xây dựng dựa trên giải thuật truyền belief. Như đã biết, khi giải mã, chúng ta phải xác định từ thông tin đã được phát từ từ mã nhận được. Giá trị vector x được lựa chọn phải cực đại hoá xác suất có điều kiện P(x|r), tức là cực đại hoá belief BEL(x), cho trước từ mã nhận được.

3. Giải mã lặp sử dụng hiệu likelihood

Trong giải thuật này, bốn tham số được định nghĩa cho mỗi phần tử khác 0 h_{ij} trong ma trận kiểm tra chẵn lẻ H: $\Psi_{ij}^{a=0}, \Psi_{ij}^{a=1}, \Omega_{ij}^{a=0}$ và $\Omega_{ij}^{a=1}$.

– Ψ_{ij}^{a} là xác suất để bit mã j lấy giá trị a, cho trước thông tin từ tất cả các nút kiểm tra chẵn lẻ trừ nút i.

– Ω_{ij}^{a} là xác suất để nút kiểm tra chẵn lẻ i thoả mãn nếu bit mã x_j=a và các xác suất để các bit mã nhận giá trị của chúng được cho bởi $\left\{\Psi_{ij'}^{a} : j' \in N(i) \setminus j, a = 0,1\right\}$

Sau đây chúng tôi trình bày giải thuật giải mã cho mã LDPC dựa trên hiệu likelihood (hiệu xác suất hậu nghiệm)

– *Giải thuật giải mã:* Giải thuật giải mã lặp của mã LDPC được trình bày trong phần này được xây dựng từ giải thuật truyền belief. Ở đây, các bit mã và nút kiểm tra đều là nhị phân nên chúng ta có thể sử dụng hiệu likelihood thay cho likelihood.

– *Khởi tạo:* Xác suất có điều kiện của tín hiệu thu, cho trước các kí tự phát được cho bởi phương trình:

$$p(r_j \mid -1) = \frac{1}{1+e^{-\frac{2r_j}{\sigma^2}}}$$

và $$p(r_j \mid +1) = \frac{e^{-\frac{2r_j}{\sigma^2}}}{1+e^{-\frac{2r_j}{\sigma^2}}} = 1 - p(r_j \mid -1) \quad (2)$$

Đầu tiên, Ψ_{ij}^0 and Ψ_{ij}^1 lần lượt được khởi tạo bằng $p(r_j|x_j=-1)$ và $p(r_j|x_j=1)$. Trong các ma trận $\{\Psi_{ij}^0\}$ and $\{\Psi_{ij}^1\}$, các bản tin một bit mã gửi đến tất cả các nút kiểm tra chẵn lẻ nối với nó đều giống nhau, lần lượt là $p(r_j|x_j=-1)$ và $p(r_j|x_j=1)$.

– *Giải mã lặp:* Theo chiều ngang: Định nghĩa hiệu $\delta\Psi_{ij} = \Psi_{ij}^0 - \Psi_{ij}^1$. Với tất cả các cặp (i, j), với a = 0 và 1, ta cập nhật các bản tin Ω từ nút kiểm tra s_i đến bit mã x_j:

$$\delta\Omega_{ij} = \prod_{j' \in N(i) \setminus j} \delta\Psi_{ij'}$$
$$\Omega_{ij}^a = \frac{1}{2}\left[1 + (-1)^a \delta\Omega_{ij}\right] \quad (3)$$

Theo chiều dọc: Với tất cả các cặp (i, j), với a = 0 và 1, ta cập nhật các bản tin Ψ từ bit mã x_j đến nút kiểm tra s_i:

$$\Psi_{ij}^a = \alpha_{ij} p(r_j \mid x_j = 2a-1) \prod_{i' \in M(j) \setminus i} \Omega_{i'j}^a \quad (4)$$

trong đó α_{ij} là một hằng số chuẩn hoá được chọn sao cho $\Psi_{ij}^0 + \Psi_{ij}^1 = 1$. Với mỗi j và a=0, 1, cập nhật các xác suất hậu nghiệm Ψ_j^0 và Ψ_j^1 bằng phương trình:

$$\Psi_j^a = \alpha_j p(r_j \mid x_j = 2a-1) \prod_{i \in M(j)} \Omega_{ij}^a \quad (5)$$

trong đó α_j là hằng số chuẩn hoá được chọn sao cho $\Psi_j^0 + \Psi_j^1 = 1$

– *Quyết định:* Giá trị giải mã theo từng bit $\hat{x}_j$ được chọn dựa trên quy tắc: Nếu $\Psi_j^1 > 0.5$, $\hat{x}_j$=1, nếu $\Psi_j^1 \le 0.5$, $\hat{x}_j$=0.

Nếu $\hat{x}H^T = 0$ *thì* $\hat{x}$ *là một từ mã hợp lệ và giải thuật kết thúc thành công.*

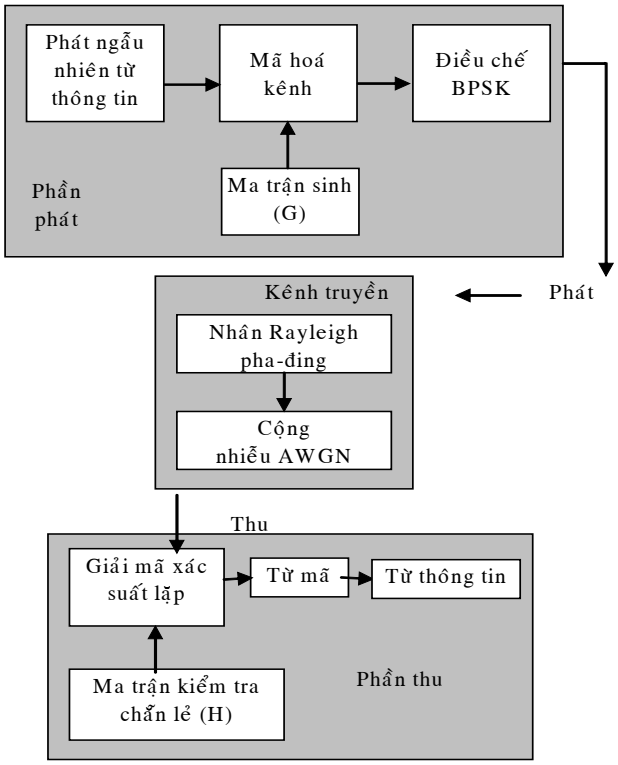
Nếu không,

- Nếu đã đạt đến số lần lặp tối đa, giải thuật được coi là không thành công và dừng.

- Nếu không, bắt đầu một vòng lặp mới.

III. MÔ PHỎNG HỆ THỐNG THÔNG TIN SỬ DỤNG MÃ LDPC TRÊN MATLAB

Sơ đồ khối của hệ thống thông tin vô tuyến mô phỏng được trình bày trong Hình 4.



Hình 4 Sơ đồ khối của hệ thống thông tin

Mã LDPC sử dụng trong mô phỏng là một mã LDPC đều. Ma trận kiểm tra chẵn lẻ của mã (H) có kích thước 16×24. Số phần tử 1 trong mỗi hàng là 3 và trong mỗi cột là 2. Ma trận H được tạo ra bằng phương pháp hoán vị cột ngẫu nhiên. Từ ma trận H, ma trận sinh G được xây dựng bằng phương pháp khử Gauss.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1
9	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
10	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0
11	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0
14	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
15	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
16	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0

Hình 5 Ma trận (H) của mã LDPC (24, 2, 3)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	1	0	0	1	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
2	1	0	1	0	0	0	0	1	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
3	0	1	1	0	0	0	0	1	1	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0
4	1	0	1	1	0	1	0	1	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
5	0	1	1	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0
6	0	1	1	0	0	0	1	1	0	1	1	0	0	1	0	0	0	0	0	0	1	0	0	0
7	0	1	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0
8	1	0	1	1	0	1	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
9	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1

Hình 6: Ma trận (G) của mã LDPC (24, 2, 3)

Khả năng kiểm soát lỗi của mã LDPC nói trên được khảo sát trên các kênh AWGN (Additive White Gaussian Noise) và kênh pha-đing Rayleigh. Trong mỗi mô hình kênh truyền, chương trình mô phỏng hệ thống thông tin số và tính tỉ lệ lỗi bit (BER) với mỗi giá trị E_b/N_0 (năng lượng bit trên mật độ phổ công suất của nhiễu). Số lượng lỗi cho mỗi giá trị E_b/N_0 được tích luỹ đủ lớn (300 lỗi) để bảo đảm độ tin cậy của kết quả.

Kênh AWGN: AWGN hay nhiễu trắng, là nhiễu có phân bố Gauss với trung bình (Mean) bằng 0 và phương sai (Variance), là σ^2. σ^2 cũng chính là công suất của nhiễu AWGN. Phương sai σ^2 và mật độ phổ công suất một phía N_0 của nhiễu liên hệ với nhau bởi công thức sau:

$$\sigma^2 = \frac{N_0}{2} \tag{6}$$

Với sơ đồ điều chế BPSK đơn giản hoá, trong đó bit 0 được điều chế thành –1, bit 1 được điều chế thành 1 (đây chính là tín hiệu đối cực nhị phân), và giả sử độ dài bit là 1, ta sẽ được năng lượng của mỗi bit là E_b=1. Khi đó tỉ số E_b/N_0 sẽ được viết thành:

$$\frac{E_b}{N_0} = \frac{1}{N_0} = \frac{1}{2\sigma^2} \text{ hay } \sigma = \sqrt{\frac{1}{2\frac{E_b}{N_0}}} \tag{7}$$

Đây chính là công thức được sử dụng trong chương trình mô phỏng để tính độ lệch chuẩn của AWGN từ giá trị cho trước của E_b/N_0.

Kênh Rayleigh fading

Theo [12], các nhân tố chính gây nên fading là truyền dẫn đa đường và hiệu ứng dịch tần Doppler. Để biểu diễn ảnh hưởng của các yếu tố này, một mô hình kênh truyền được sử dụng khá phổ biến trong thông tin vô tuyến là mô hình kênh truyền Rayleigh fading. Trong mô hình này, đường bao của đáp ứng xung của kênh truyền, kí hiệu là R, sẽ tuân theo phân phối xác suất Rayleigh. Pha Ψ của đáp ứng xung của kênh truyền sẽ phân phối đều trong khoảng [-π, π].

$$f_R(r) = \begin{cases} \frac{r}{\sigma^2}\exp\left(-\frac{r^2}{2\sigma^2}\right) & r \geq 0 \\ 0 & \text{ở nơi khác} \end{cases}$$

$$f_\psi(\psi) = \begin{cases} \frac{1}{2\pi} & -\pi \leq \psi \leq \pi \\ 0 & \text{ở nơi khác} \end{cases} \tag{8}$$

trong đó σ là tham số của phân bố Rayleigh. Giá trị trung bình và phương sai của biến ngẫu nhiên có phân bố Rayleigh sẽ là:

$$m_x = \sqrt{\frac{\pi}{2}} \times \sigma; \quad \sigma_x^2 = \left(2 - \frac{\pi}{2}\right) \times \sigma^2 \tag{9}$$

Các mô phỏng cho kênh truyền Rayleigh fading sẽ sử dụng công thức: r = *a*x + n

trong đó, r là tín hiệu thu, x là tín hiệu BPSK được phát, a là biến ngẫu nhiên theo phân bố Rayleigh biểu diễn tác động của kênh truyền fading lên tín hiệu. Ở đây, a được chuẩn hoá để $E[a^2]=1$. Có thể chứng minh được hàm mật độ xác suất của a là:

$$f(a) = \begin{cases} 2ae^{-a^2} & a \geq 0 \\ 0 & \text{ở nơi khác} \end{cases} \tag{10}$$

và trung bình và phương sai của a là:

$m_a = 0.8862;\ \sigma_a^2 = 0.2146$; n: nhiễu Gauss

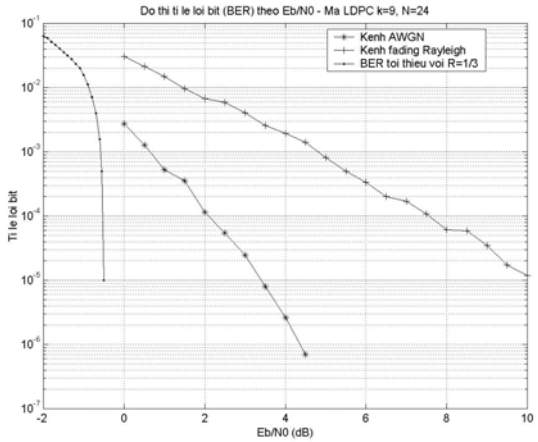
Bảng 1 và 2 trình bày kết quả mô phỏng Matlab trên kênh AWGN và kênh Rayleigh fading. Mỗi giá trị E_b/N_0(dB), số lượng lỗi bit được tích luỹ đến ít nhất là 300. Số lượng vòng lặp tối đa cho mỗi lần giải mã lặp là 20.

Bảng 1 Kết quả mô phỏng trên kênh AGWN

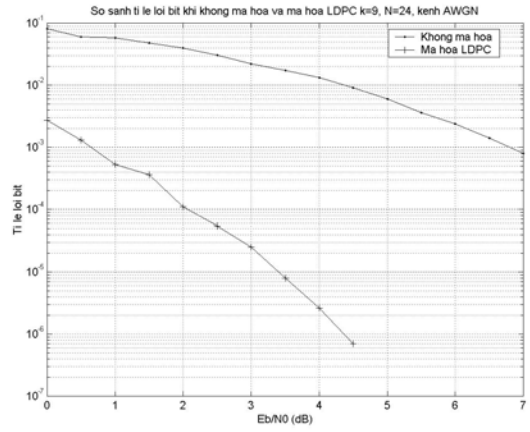
E_b/N_0	0	0.5	1.0	1.5	2.0	2.5
BER	2.7e-3	1.3e-3	5.3e-4	3.6e-4	1.1e-4	5.5e-5
E_b/N_0	3.0	3.5	4.0	4.5		
BER	2.5e-5	8.0e-6	2.6e-6	7.0e-7		

Bảng 2 Kết quả trên kênh Rayleigh fading

E_b/N_0	0	0.5	1.0	1.5	2.0	2.5
BER	3.1e-2	2.1e-2	1.5e-2	9.6e-3	6.7e-3	5.9e-3
E_b/N_0	3.0	3.5	4.0	4.5	5.0	5.5
BER	4.0e-3	2.6e-3	2.0e-3	1.4e-3	8.2e-4	4.9e-4
E_b/N_0	6.0	6.5	7.0	7.5	8.0	8.5
BER	3.4e-4	2.0e-4	1.7e-4	1.1e-4	6.1e-5	5.9e-5
E_b/N_0	9.0	9.5	10.0			
BER	3.5e-5	1.7e-5	1.2e-5			



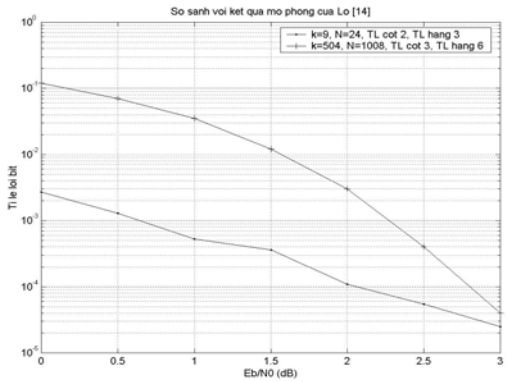
Hình 7: Đồ thị BER theo E_b/N_0 cho các kênh AWGN và Rayleigh, so sánh với đồ thị BER cực tiểu trên kênh AWGN với tỉ lệ mã R=1/3.



Hình 8: So sánh BER khi mã hoá LDPC (24, 2, 3) và khi không mã hoá trên kênh AWGN.

Dựa trên các số liệu thu được, đồ thị BER theo Eb/N0 cho các kênh AWGN và pha-đing Rayleigh được vẽ trên Hình 7, so sánh với đồ thị BER cực tiểu trên kênh AWGN với tỉ lệ mã R=1/3 (Giới hạn Shannon) [13]. Hình 8 so sánh BER khi mã hoá LDPC với trường hợp không mã hoá trên kênh AWGN. Hình 9 so sánh kết quả thu được với kết quả mô phỏng của Lo [14] cho một mã LDPC có k=504, N=1008 (R=1/2).

Hình 9 mô tả việc so sánh kết quả thu được trên kênh AWGN với kết quả mô phỏng của Lo [14] cho mã LDPC có k=504, N=1008 (R=1/2).



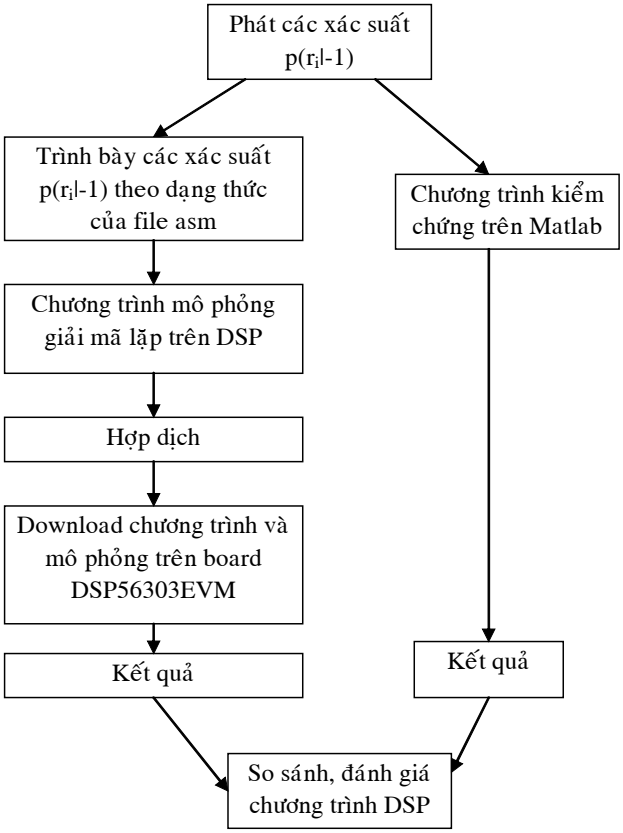
Hình 9: So sánh kết quả

IV. THỰC HIỆN GIẢI THUẬT GIẢI MÃ LẶP TRÊN DSP-MOTOROLA

Mục tiêu của chương trình mô phỏng trên DSP (chip DSP56303 của Motorola) là thực hiện giải mã LDPC trong điều kiện thực tế.

Như đã biết, trong hệ thống thông tin di động GSM, việc mã hoá và giải mã kênh truyền được thực hiện bởi các DSP trong thời gian thực. Ở phần mô phỏng này, với cùng một chuỗi tín hiệu thu, việc giải mã sẽ được tiến hành trên chương trình Matlab và chương trình DSP. Kết quả sẽ được so sánh nhằm kiểm chứng chương trình DSP. Do số lượng từ mã nhỏ (chương trình DSP sử dụng bộ nhớ trong của DSP để lưu các vector đầu vào) nên phần mô phỏng này chỉ để kiểm tra khả năng thực hiện DSP trong quá trình mã hoá - giải mã chứ không phải để khảo sát khả năng kiểm soát lỗi của mã LDPC được tạo ra. Chương trình mô phỏng trên DSP sử dụng kiểu dữ liệu phân số (*fractional*) của họ DSP 56300. Vì các giá trị có thể

của kiểu dữ liệu này là từ –1 đến $1\text{-}1^{-23}$ nên giá trị của vector thu (có thể nằm ngoài dải trên) sẽ không được trực tiếp đưa vào chương trình. Thay vào đó, các giá trị được nạp vào bộ nhớ ban đầu là các xác suất có điều kiện $p(r_i|\text{-}1)$, tức là xác suất để nhận được r_i với điều kiện ở phía phát phát đi giá trị –1.



Hình 10. Quá trình mô phỏng trên DSP và kiểm chứng bằng chương trình Matlab

Kết quả mô phỏng trên DSP

Bảng 3: Kết quả mô phỏng DSP trên kênh AWGN, kiểm chứng bằng Matlab

E_b/N_0 (dB)	Số bit thông tin	Chương trình	Số bit lỗi	Tỉ lệ lỗi bit
0.0	450	Matlab	1	0.00222
		DSP	1	0.00222

Số từ mã đầu vào 50, mỗi từ mã dài 24 bit. Các mẫu được trình bày theo dạng asm để đưa vào chương trình của DSP. Số vòng lặp tối đa của giải thuật giải mã lặp cũng là 20. Bảng 3 và 4 trình bày kết quả mô phỏng trên kênh AWGN và trên kênh fading Rayleigh. Có thể nhận thấy các chương trình Matlab và DSP cho kết quả tương đương.

Bảng 4. Kết quả mô phỏng DSP trên kênh phading Rayleigh, kiểm chứng bằng Matlab

E_b/N_0 (dB)	Số bit thông tin	Chương trình	Số bit lỗi	Tỉ lệ lỗi bit
0.0	450	Matlab	16	0.03556
		DSP	16	0.03556
0.5	450	Matlab	14	0.03111
		DSP	14	0.03111
1.0	450	Matlab	7	0.01556
		DSP	7	0.01556
1.5	450	Matlab	3	0.00667
		DSP	3	0.00667
2.0	450	Matlab	5	0.01111
		DSP	5	0.01111
2.5	450	Matlab	0	0
		DSP	0	0
3.0	450	Matlab	3	0.00667
		DSP	3	0.00667

V. KẾT LUẬN

Các kết quả mô phỏng Matlab trong phần III cho thấy mã LDPC được tạo ra có đặc tính khá tốt trên các kênh truyền AWGN và pha-đing Rayleigh. Tăng ích mã hoá là khoảng 6dB ở BER=10^{-3} (Hình 8). So sánh với mã LDPC có k=504, N=1008 của Lo [14] (Hình 9) cho thấy mã LDPC (24, 2, 3) được tạo có đặc tính tốt hơn trong khoảng $E_b/N_0 = 0 \div 3$ dB (Tuy nhiên đây chỉ là so sánh tương đối vì tỉ lệ mã R của hai mã này khác nhau).

So sánh với đồ thị BER cực tiểu trên kênh AWGN với R=1/3, đồ thị trên kênh AWGN của mã LDPC (24, 2, 3) được tạo có khoảng cách hơn 1dB tại BER=10^{-3} và khoảng 4dB tại BER=10^{-5}. Để lý giải cho sự khác biệt này, chúng tôi có một số nhận xét như sau:

– Đây là mã LDPC có độ dài khối nhỏ, tính chất thưa của ma trận H không rõ ràng. Như đã biết, các mã LDPC chỉ thể hiện đặc tính vượt trội với các độ dài khối lớn.

– Đây là một mã LDPC đều. Người ta đã chứng minh rằng các mã LDPC có đặc tính kém hơn các mã LDPC không đều.

Trong phần IV, việc kiểm chứng bằng các chương

trình Matlab cho thấy quá trình thực hiện giải mã lặp trên DSP cho kết quả phù hợp. Mặc dù các mô phỏng được thực hiện là chưa đầy đủ so với điều kiện thực tế của thông tin di động số, các kết quả mô phỏng cũng đã chỉ ra được khả năng kiểm soát lỗi tốt của mã LDPC trong môi trường này.

Mã LDPC hiện tại vẫn đang là một đề tài đang được nghiên cứu rộng rãi tại các trường đại học và các trung tâm nghiên cứu trên thế giới. Các mã LDPC không đều và các mã LDPC có các phần tử của ma trận kiểm tra chẵn lẻ thuộc GF(q) với q>2 đã được chứng minh là có đặc tính vượt trội và vẫn đang được tiếp tục khảo sát. Các phương pháp tạo mã LDPC cũng là vấn đề nhiều nhà nghiên cứu quan tâm. Sau cùng, đi đôi với các nghiên cứu lí thuyết, việc phát triển mã LDPC cho các ứng dụng thực tế, chẳng hạn như thông tin di động hay lưu trữ số liệu cũng đang được xúc tiến ở nhiều nơi trên thế giới.

TÀI LIỆU THAM KHẢO

[1] R. G. GALLAGER, *"Low density parity check codes,"* IRE Tran.s on Information Theory, IT-8, pp. 21-28, Jan. 1962.

[2] M. G. LUBY, M. MITZENMACHER, M. A. SHOKROLLAHI AND D. A. SPIELMAN, *"Analysis of low density codes and improved designs using irregular graphs,"* Jul. 2002. [Online]. Available: http://www-Math.mit.edu/~spielman/Research/irreg.html

[3] M. C. DAVEY AND D. J. C. MACKAY, *"Low density parity check codes over GF(q),"* IEEE Communication Letters, Volume 2, June 1998.

[4] R. M. TANNER, *"A recursive approach to low complexity codes"*, IEEE Transactions on Information Theory, Vol. IT-27, No. 5, Sep. 1981.

[5] R. J. MCELIECE, D. J. C. MACKAY AND J. F. CHENG, *"Turbo decoding as an instance of Pearl's belief propagation algorithm,"* IEEE Journal on Selected Areas in Communications, Vol.16, No.2, Feb. 1998.

[6] F. R. KSCHISCHANG, B. J. FREY AND H. LOELIGER, *"Factor graphs and the sum product algorithm,"* IEEE Transactions on Information Theory, vol. 47, pp. 498-519, Feb. 2001.

[7] M. C. DAVEY, "*Error-correction using low-density parity-check codes*", PhD Dissertation, University of Cambridge.

[8] Y. KOU, S. LIN AND M. FOSSORIER, *"Low density parity check codes based on finite geometries: A rediscovery and new results"*, IEEE Transactions on Information Theory, Aug. 1999.

[9] S.J JOHNSON AND S.R. WELLER, *"Regular low-density parity check codes from combinatorial designs,"* Proc. IEEE Inf. Theory Workshop, pp.90–92, Cairns, Australia, Sep. 2001.

[10] S. RUSSELL AND P. NORVIG, "*Artificial Intelligence - A Modern Approach*", Prentice-Hall, 1995

[11] J. PEARL, "*Probabilistic Reasoning In Intelligent Systems: Network of Plausible Inference*", Morgan Kaufmann, California, USA 1988.

[12] T. S. RAPPAPORT, "*Wireless Communications – Principle and Practice*", 2nd Edition, Pearson Education Int., 2002

[13] S. HAYKIN, "*Communication Systems*", 4th Edition, John Wiley & Sons, 2001

[14] K. L. LO, "*Layered space time structures with low density parity check and convolutional codes*", Master of Engineering Thesis, School of Electrical & Information Engineering, University of Sydney, Oct. 2001, Australia.

[15] K. C. NGUYEN, "*Sử dụng mã kiểm tra chẵn lẻ mật độ thấp trong thông tin di động số", Luận văn Thạc sĩ*, Trường Đại học Bách khoa Thành phố Hồ Chí Minh, Tháng Sáu, 2003.

Ngày nhận bài: 25/09/2003

SƠ LƯỢC VỀ TÁC GIẢ

LÊ TIẾN THƯỜNG

Sinh năm 1957 tại TP. Hồ Chí Minh.

Đã nhận bằng kỹ sư năm 1981 và tiến sĩ năm 1998 chuyên ngành Điện tử-Viễn thôngtại Đại học Tasmania, Australia. Được phong Phó Giáo sư.

Hiện công tác tại Khoa Điện - Điện tử, Đại học Bách Khoa TP. HCM.

Lĩnh vực nghiên cứu: xử lý tín hiệu, thông tin số, xử lý tín hiệu radar, wavelets và ứng dụng, neural và fuzzy systems.

Email: ltthuong@dee.hcmut.edu.vn

NGUYỄN HỮU PHƯƠNG

Sinh năm 1942

Tốt nghiệp đại học và tiến sĩ tại đại học Auckland, New Zealand năm 1965 và 1969 chuyên ngành điện tử - viễn thông. Được phong Phó Giáo sư.

Hiện là Giám đốc Trung tâm máy tính, Đại học Khoa học Tự nhiên TP.HCM.

Lĩnh vực nghiên cứu: xử lý số tín hiệu, mạch điện tử, wavelets, neural và fuzzy systems.

HOÀNG ĐÌNH CHIẾN

Sinh năm 1955,

Tốt nghiệp đại học thông tin liên lạc Mat-xcơ-va năm 1979, nhận bằng thạc sĩ năm 1997 ngành điện tử viễn thông tại Đại học Bách Khoa TP.HCM.

Hiện là nghiên cứu sinh chuyên ngành viễn thông tại ĐH Bách khoa TP. HCM.

Hướng nghiên cứu: mạch điện tử thông tin, wavelets, neural networks, thông tin vệ tinh.

Email: hdchien@dee.hcmut.edu.vn

NGUYỄN CHÍ KIÊN

Sinh năm 1974 tại Quảng Bình.

Tốt nghiệp Đại học Bách khoa Hà Nội ngành điện tử - viễn thông năm 1997. Nhận bằng Thạc sĩ ngành viễn thông tại Đại học New South Wales, Australia, năm 2002. Nhận bằng Thạc sĩ ngành vô tuyến điện tử tại Đại học Bách khoa TP. HCM năm 2003.

Từ năm 1997-2000: Kỹ sư thiết kế, Phòng nghiên cứu phát triển, Trung tâm VTC1, Công ty Thiết bị Điện thoại, Tổng Công ty Bưu chính Viễn thông Việt nam. Từ 10/2002 đến nay: Kỹ sư hệ thống, Văn phòng Ericsson Vietnam