ĐỀ XUẤT NÂNG CAO CHẤT L□ỢNG MÃ HAMMING

PROPOSAL ON QUALITY IMPROVEMENT FOR HAMMING CODES

Nguyễn Thị Hồng Nhung

Khoa Điện tử, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Đến Tòa soạn ngày 06/5/2016, chấp nhận đăng ngày 15/5/2016

Tóm tắt: Trong bài báo này, dựa trên ý tưởng giải mã mềm cho mã khối, tác giả đề xuất áp dụng phương pháp giải mã mềm trên cơ sở giải mã lặp cho mã Hamming và từ đó đưa ra phương án nâng cao chất lượng mã Hamming dựa vào ma trận kiểm tra tương đương mới. Xây dựng ma trận kiểm tra tương đương mới bằng cách thay thế các hàng của ma trận **H** tương đương bằng một số hàng toàn "0" theo tỷ lệ nhất định. Kết quả khảo sát cho thấy chất lượng giải mã tốt hơn các thuật toán mới nhất. Không những thế, khối lượng tính toán giảm nhiều giúp rút ngắn thời gian giải mã nhất là đối với các mã có chiều dài lớn.

Từ khóa: Giải mã mềm, mã Hamming, giải mã lặp.

Abstract: In this article, with the idea of soft decision decoding for linear block codes, soft decision decoding solution based on the iterative decoding for Hamming codes is proposed, and then solution for quality improvement for Hamming codes based on new equivalent parity check matrix is proposed. New equivalent parity check matrix is developed by replacing rows of equivalent **H** matrix with some rows with all "0" with a certain rate. The results show that the decoding performance is better than the latest decoding algorithm. Additionally, the calculation volume reduces drastically leading to the shortening of decoding time, especially for great length codes.

Keywords: Soft decoding, Hamming codes, iterative decoding.

1. ĐẶT VẤN ĐỀ

Mã hóa kênh có vai trò vô cùng quan trọng trong việc truyền dẫn thông tin số. Việc tìm ra các phương án sửa lỗi phía trước (FEC-*Forward Error Correction*) là một nhiệm vụ quan trọng trong việc nâng cao hiệu suất truyền tin. Các họ mã khối trước đây vẫn còn những mặt hạn chế như đánh đổi hiệu suất để giảm lượng tính toán hoặc để đạt hiệu suất mong muốn thì lại tăng độ phức tạp tính toán. Đến nay các nhà thiết kế đã phát triển, cải thiện các kỹ thuật mã hóa sửa sai đưa hiệu suất kênh ngày càng tiến tới giới hạn Shannon. Kỹ thuật giải mã mềm được cải tiến rất nhiều giúp nâng cao hiệu quả giải mã mã khối. Mã LDPC hiện nay là họ mã khối mạnh với khả năng kiểm soát lỗi cao sử dụng thuật toán giải mã mềm BPA [1, 2]. Đã có nhiều cải tiến cho thuật toán BPA nhằm nâng cao hơn nữa chất lượng mã LDPC. Mã LDPC là mã mật độ thấp nên thuật toán BPA và các thuật toán cải tiến cho hiệu quả giải mã cao. Nhưng với các mã khối mật độ cao như mã Hamming [3] thì các giải thuật này lại cho hiệu quả thấp nhất là với các mã có chiều dài lớn.

Trong bài báo này, tôi nghiên cứu phương pháp giải mã mềm trên cơ sở giải mã lặp BPA, đề xuất áp dụng cho mã Hamming từ đó đưa ra ý tưởng cải tiến thuật toán nhằm nâng cao chất lượng mã Hamming [1, 4].

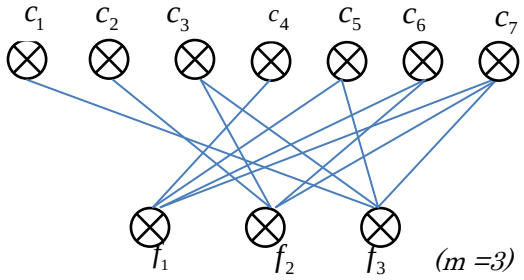
2. ĐỀ XUẤT ỨNG DỤNG THUẬT TOÁN GIẢI MÃ MỀM TRÊN CƠ SỞ GIẢI MÃ LẶP CHO MÃ HAMMING

Mã Hamming do Richard Hamming lần đầu tiên giới thiệu tại [3] là mã kiểm soát lỗi thuộc họ mã khối cho phép sửa được lỗi do một bít sai gây ra và có khả năng phát hiện các lỗi kép. Với sự đơn giản trong sơ đồ mã hóa và giải mã, đồng thời khi số bít mang tin tăng thì số bít kiểm tra cũng tăng nhưng tốc độ tăng của số bít mang tin nhanh hơn nhiều so với độ tăng của số bít kiểm tra nên khi số bít mang tin lớn thì tính kinh tế càng cao. Hiện nay, mã Hamming vẫn còn được ứng dụng nhiều như trong hệ thống truyền thông, hệ thống thông tin, truyền dẫn vệ tinh, hệ thống WiFi và WiMAX,… Với sự phát triển không ngừng của khoa học công nghệ nhất là trong lĩnh vực thông tin, nghiên cứu và tìm ra các thuật toán nhằm nâng cao chất lượng mã Hamming là cần thiết.

Mã Hamming thuộc họ mã khối nên cũng như mã LDPC đều được biểu diễn hiệu quả thông qua đồ hình song biên Tanner như ví dụ trong hình 1. Trên đồ thị này có hai hàng nút gồm các nút bít $c = c_1, c_2, ... c_n$ và các nút kiểm tra $f = f_1, f_2, ... f_m$. Nút kiểm tra f_j nối với nút c_i khi và chỉ khi $\mathbf{H}(j,i) = 1$. Bộ giải mã sử dụng thuật toán giải mã lặp. Khi đó, thông tin sẽ được chuyển qua lại giữa các nút bít và các nút kiểm tra khi có kết nối trên đồ thị Tanner [5].

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Như vậy các thuật toán giải mã lặp cho mã LDPC hoàn toàn có thể đem áp dụng cho mã Hamming.



Hình 1. Ma trận kiểm tra H và đồ thị Tanner tương ứng của mã Hamming (7,4)

2.1. Đề xuất áp dụng thuật toán giải mã mềm BPA cho mã Hamming

Xét mã Hamming (n,k) với n là chiều dài từ mã, k là chiều dài thông tin, tốc độ mã hóa $R= k/n$ và $m= n–k = 2^m –1–k$ là số lượng các bít kiểm tra. Các bít tin $u = u_1, u_2, ... u_k$ được mã hóa Hamming (n,k) thành từ mã $c = c_1, c_2, ... c_n$, sau đó được điều chế và truyền qua kênh. Đầu vào bộ giải mã BPA là tỷ lệ ước lượng theo hàm log (Log Likelihood Ratio – LLR):

$$L(q_{ij}) = L(c'_i) = \log \frac{\Pr(c'_i = 0 | c')}{\Pr(c'_i = 1 | c')} \qquad (1)$$

Ở đây c' là tập các symbol nhận từ kênh và xác suất điều kiện $\Pr(c'_i \mid c')$.

Bộ giải mã Hamming thực hiện giải mã mềm dựa trên $L(c_i' | c')$ và đưa ra từ mã $\overline{c}$

Thuật toán BPA [1] là thuật toán giải mã mềm trên cơ sở giải mã lặp được tóm tắt như sau:

Khởi tạo: Tính LLR $L(c_i')$ cho tất cả các nút bit $i = 1,2,...,n$ và đặt:

$$L^{(k)}(q_{ij}) = L(c'_i) = \log \frac{\Pr(c'_i = 0 | c')}{\Pr(c'_i = 1 | c')} \qquad (2.2)$$

tại vị trí (j,i) thỏa mãn $\mathbf{H}_{ji} = 1$ cho lần lặp thứ nhất, trong đó c_i' là bit mã thứ i và c' là chuỗi ký hiệu thu được.

Bước 1: Cập nhật bản tin cho tất cả các nút kiểm tra $j= 1,2,..., m$ và gửi bản tin $L(p_{ji})$ từ nút kiểm tra tới các nút bit nối với nó. Với $L(p_{ji})$ là tin (LLR) từ các nút kiểm tra f_j gửi tới nút bit c_i như trên hình 1.

Bước 2: Cập nhật bản tin cho tất cả các nút bit $i=1, 2,..., n$ và gửi bản tin $L(q_{ij})$ từ các nút bit tới nút các kiểm tra nối với nó.

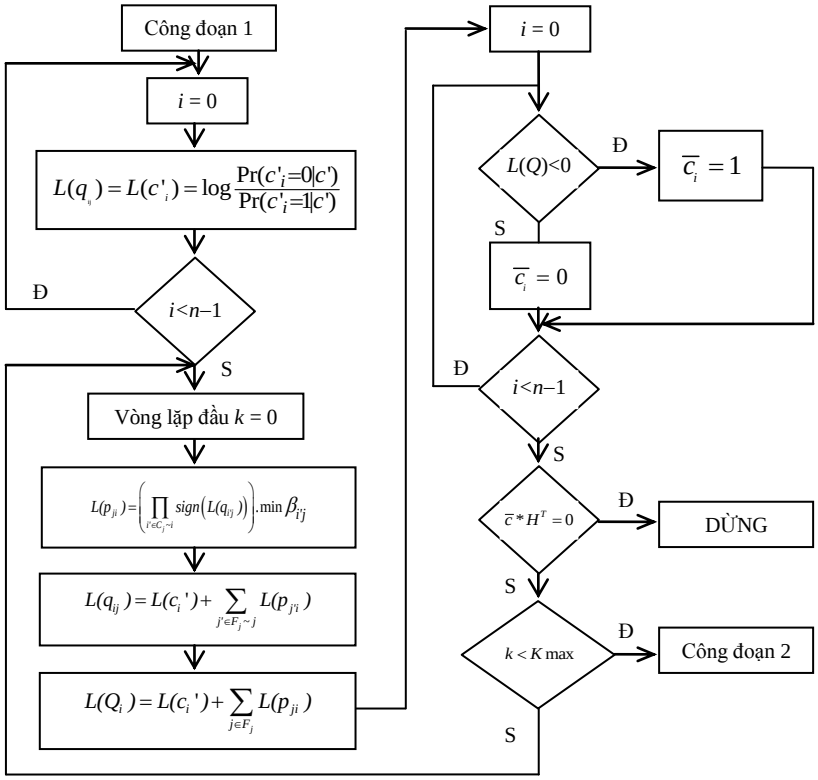
Đầu ra của bộ giải mã là giá trị LLR của các bit mã được sử dụng để quyết định thành từ mã thăm dò $\overline{c} = \overline{c}_1, \overline{c}_2, ... \overline{c}_n$. Nếu hội chứng ***s*** thỏa mãn điều kiện:

$$\mathbf{s} = \overline{c}.\mathbf{H}^T = [0,0,...,0] \quad (3)$$

thì dừng lặp đưa ra từ mã hợp lệ $\overline{C}$. Nếu điều kiện (3) không thỏa mãn thì quá trình được thực hiện lại cho đến khi đạt số lần lặp cực đại K_{max} thì dừng lại và đưa ra từ mã tại lần lặp cuối.

Mã Hamming là mã mật độ cao nên tồn tại nhiều chu kỳ 4 (chu kỳ ngắn) trong đồ hình Tanner [5] nhất là với các mã dài. Vì vậy, thuật toán giải mã mềm trên cơ sở giải mã lặp BPA áp dụng cho mã Hamming dài sẽ làm tăng thời gian giải mã và hiệu quả giải mã không cao.

2.2. Cải tiến thuật toán giải mã mềm BPA cho mã Hamming



Hình 2. Lưu đồ thuật toán BPA - EH - E công đoạn 1

Thực hiện thuật toán cải tiến BPA-EH [1] bằng việc sử dụng các ma trận tương đương cho mã Hamming dẫn đến khối lượng tính toán lớn gấp *m - 1* lần (*m* là số lượng hàng của ma trận kiểm tra). Mã Hamming là mã mật độ cao nên nếu sử dụng thuật toán BPA – EH càng làm tăng rất nhiều các chu kỳ ngắn trên đồ thị Tanner dẫn đến chất lượng cải thiện không đáng kể, thậm chí còn kém hơn so với BPA. Từ đó có phương án xây dựng ma trận kiểm tra mới: Ngoài việc thay thế hàng có độ tin cậy kém của ma trận **H** gốc, chúng ta cũng có thể thay thế một số hàng còn lại bằng hàng toàn "0". Điều này sẽ làm giảm khối lượng tính toán và do đó dẫn đến giảm thời gian giải mã và tăng độ tin cậy.

Nếu kích thước khối mã lớn, số lượng bít bị thay thế trong mỗi lần xóa càng nhiều giúp giảm thời gian giải mã, chất lượng giải mã tăng.

Thuật toán cải tiến BPA – EH – E (BPA base on Equivalent parity check matrix H Eraser)

Định nghĩa các ký hiệu:

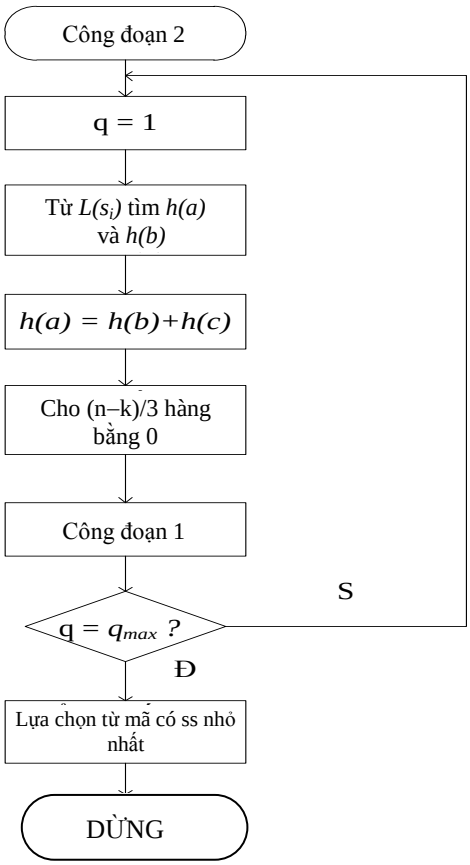
F_j: tập hợp các cột ở đó $\mathbf{H}(j,i)=1$ với j là thứ tự hàng;

C_i: tập hợp các hàng ở đó $\mathbf{H}(j,i)=1$ với i là thứ tự cột;

$F_j \sim i$: tập F_j trừ cột thứ i;

$C_i \sim j$: tập C_i trừ hàng thứ j;

$$\beta_{i'j} = \left|L^{(k)}(q_{i'j})\right|_{i' \in C_i \sim j}$$

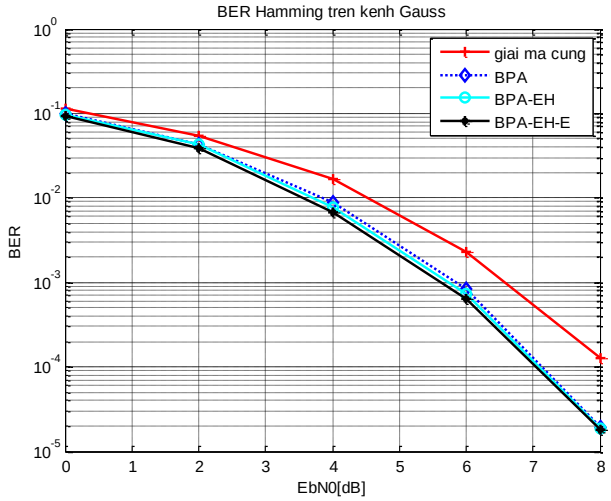


Hình 3. Lưu đồ thuật toán BPA - EH - E công đoạn 2

Công đoạn 1 (hình 2): Được thực hiện giống như thuật toán BPA. Bước cải tiến thực hiện ở công đoạn 2.

Công đoạn 2 (hình 3): Từ công đoạn 1, ta thu được giá trị L(s_i), từ giá trị này thuật toán tìm hàng kém tin cậy *h(a)*, và hàng tin cậy *h(b)* [1]. Sau khi thực hiện thay thế các hàng có độ tin cậy thấp và thay thế luân phiên các hàng của ma trận $\mathbf{H}_e$ bằng các hàng toàn "0" theo tỷ lệ $(n-k)/3$. ($n-k$ *: số hàng của ma trận* $\mathbf{H}$) ta thu được ma trận kiểm tra tương đương mới $\mathbf{H}^*_e$ và thực hiện lại công đoạn 1 với việc sử dụng ma trận kiểm tra mới $\mathbf{H}^*_e$. Kiểm tra điều kiện (3), nếu thỏa mãn thì dừng và đưa ra từ mã. Nếu không, tìm và lưu lại $\bar{c}$ ứng với syndrome trong lần giải mã ứng với $\mathbf{H}^*_e$. Sau đó lại xây dựng lại ma trận $\mathbf{H}^*_e$ và thực hiện công đoạn 1 với ma trận $\mathbf{H}^*_e$ vừa xây dựng được, tương tự kiểm tra theo (3), nếu không thỏa mãn tìm và lưu lại từ mã ứng với q_{max} lần giải mã tiếp theo… Thực hiện đến khi tìm được từ mã hợp lệ hoặc hết $K_{\max}$ lần lặp. Từ mã được chọn $\bar{c}$ sẽ ứng với $s_{\min}$ trong $K_{\max}$ lần giải mã.

3. KẾT QUẢ MÔ PHỎNG VÀ THẢO LUẬN

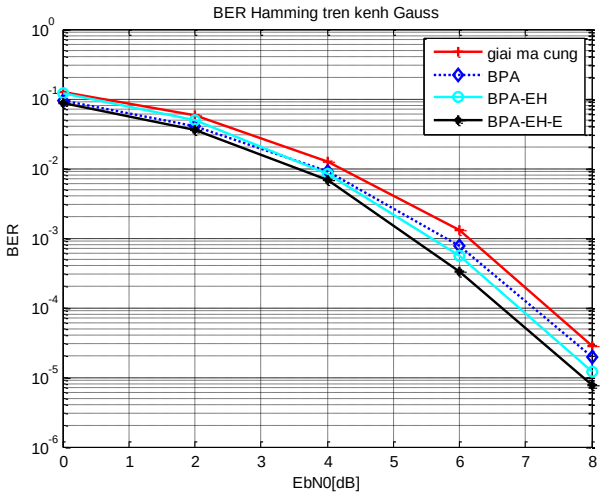


Hình 4. So sánh BER của mã Hamming (7, 4) giữa các thuật toán

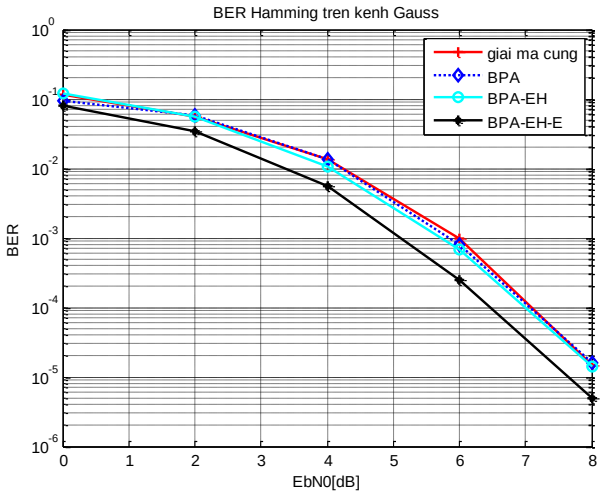
Xét bộ mã Hamming (7, 4), (15,11), (31,26), giả thiết điều chế BPSK lý tưởng và kênh truyền AWGN. Thực hiện mô phỏng đánh giá chất lượng giải mã của các thuật toán giải mã đã nghiên cứu: thuật toán BPA, thuật toán

BPA – EH và thuật toán mới BPA – EH – E thay thế luân phiên các hàng của ma trận tương đương $\mathbf{H}_e$ bằng các hàng toàn "0" theo tỷ lệ $(n-k)/3$ với thuật toán giải mã cứng cho kết quả trên hình 4, 5, 6. Hình 7 so sánh chất lượng thuật toán giải mã mới cho các mã Hamming với độ dài khác nhau.

Từ kết quả mô phỏng ta thấy, nếu áp dụng các thuật toán BPA, BPA-EH, BPA-EH-E cho mã Hamming đều cho chất lượng giải mã tốt hơn so với giải mã cứng. Thuật toán BPA, BPA - EH cho chất lượng cải thiện không đáng kể so với thuật toán giải mã cứng khi chiều dài từ mã tăng.

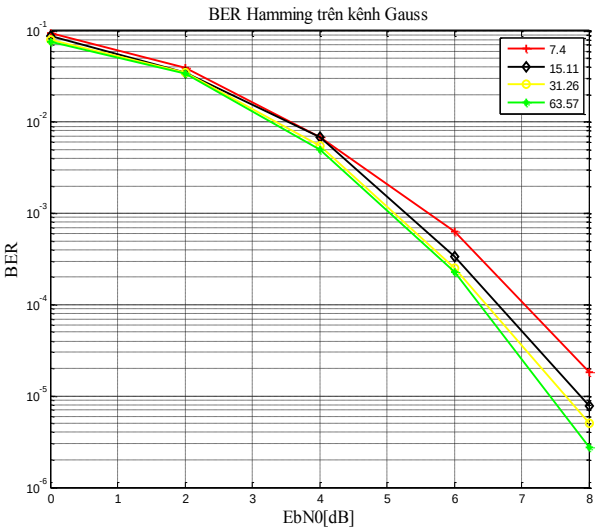


Hình 5. So sánh BER của mã Hamming (15, 11) giữa các thuật toán



Hình 6. So sánh BER của mã Hamming (31, 26) giữa các thuật toán

Thuật toán giải mã Hamming dựa vào ma trận kiểm tra tương đương mới (BPA-EH-E) cho phép nâng cao chất lượng 0,6 dB đến 0,7 dB tại tỷ lệ lỗi bít P_e = 10^{-4} so với giải mã cứng. Chất lượng giải mã tốt hơn so với thuật toán BPA và BPA – EH và thời gian giải mã nhanh hơn do số lượng tính toán trong mỗi lần lặp giảm đáng kể nhờ thay thế một số hàng của ma trận **H** bằng "0". Như vậy với các mã Hamming có độ dài càng lớn thì thuật toán mới mang độ lợi BER cải thiện đáng kể. Điều này có thể giải thích như sau: Do tốc độ tăng của số bít mang tin nhanh hơn nhiều so với độ tăng của số bít kiểm tra nên mật độ bít "1" trong các hàng của các mã càng dài càng lớn làm tăng các vòng chu kỳ ngắn. Khi đó, ma trận kiểm tra tương đương được thực hiện thay thế một số hàng bằng "0" khiến các vòng chu kỳ ngắn giảm. Kiểm tra thuật toán giải mã mới cho các mã Hamming có độ dài khác nhau ở hình 7 cũng cho kết quả phù hợp với phân tích.



Hình 7. So sánh BER của mã Hamming (7,4), (15, 11), (31, 26), (63, 57)

4. KẾT LUẬN

Bài báo đề xuất áp dụng thuật toán giải mã mềm trên cơ sở giải mã lặp BPA cho mã Hamming và đưa ra thuật toán cải tiến mới BPA - EH - E. Thuật toán mới được xây dựng

dựa vào các ma trận kiểm tra tương đương có thay thế một số hàng toàn "0" nhằm hạn chế lượng tính toán, cải thiện chất lượng BER nhất là đối với các mã Hamming có chiều dài lớn. Thuật toán giải mã mềm làm tăng chất lượng giải mã mã Hamming. Chất lượng thuật toán giải mã mới tăng khoảng 0,6 dB đến 0,7 dB tại BER = 10^{-4} so với thuật toán giải mã cứng, độ phức tạp và mức độ tính toán giảm tỉ lệ thuận với chiều dài từ mã.

TÀI LIỆU THAM KHẢO

[1] Nguyen Tung Hung, "*A new decoding algorithm based on equivalent parity check matrix for LDPC codes*," REV Journall on Electronics and Communications, Vol.3, No. 1-2, Jannuary – June 2013, pp.73-76.

[2] R. Muthammal & S. S. R. Madane (2013), "*Design of Wave Pipelined Circuit of LDPC Decoder*", European Journal of Scientific Research,vol. 114, no. 4, pp. 581-585, 11/2013.

[3] Hamming,R.W, "*Error detecting and error correcting codes*", Bell System Tech. J. 29 (1950) 147–160

[4] S. L. Sweatlock (2008), "*Asymptotic Weight Analysis of Low-Density Parity Check (LDPC) Code Ensembles*", PhD thesis, California Institute of Technology, 4/2008.

[5] R. Tanner, "*A recursive approach to low complexity codes*", IEEE Transactions on Information Theory, IT-27(5):533-547, September 1981.

Thông tin liên hệ: **Nguyễn Thị Hồng Nhung**
Điện thoại: 0945616629 - Email: nthnhung@uneti.edu.vn
Khoa Điện tử, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp