ĐỀ XUẤT GIẢI PHÁP GIẢM ẢNH HƯỞNG CỦA CÁC VÒNG KÍN NGẮN CHO CÁC MÃ KIỂM TRA CHẴN LẺ MẬT ĐỘ CAO

PROPOSED SOLUTION TO REDUCE THE INFLUENCE OF SHORT CYCLES FOR HIGH-DENSITY PARITY-CHECK CODES

Nguyễn Thị Hồng Nhung, Phạm Văn Nam, Nguyễn Mai Anh

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

Đến Tòa soạn ngày 02/5/2019, chấp nhận đăng ngày 15/5/2019

Tóm tắt: Giải mã mềm trên cơ sở thuật toán lan truyền niềm tin rất phù hợp với các mã kiểm tra chẵn lẻ mật độ thấp. Tuy nhiên, do khối lượng tính toán lớn nên thuật toán này khó áp dụng trực tiếp cho các mã kiểm tra chẵn lẻ mật độ cao. Dựa trên đặc điểm của giải mã lặp và tính chất của mã đối ngẫu, bài báo này đề xuất thuật toán giải mã mềm cho HDPC dựa vào từ mã đối ngẫu toàn "0". Thuật toán giải mã được đề xuất cho phép nâng cao chất lượng giải mã vì giảm được số vòng kín ngắn trong ma trận kiểm tra. Kết quả mô phỏng với thuật toán giải mã mới cho các mã Hamming, chất lượng giải mã tăng 0,3-0,65 dB tại tỉ lệ lỗi bit 10^{-4}, thời gian giải mã tương đương so với sử dụng BPA.

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

Abstract: The soft-decision decoding based on Belief Propagation Algorithm is suitbale for Low-Density Parity-check Codes. However, due to its computational complexity, it's difficult to directly apply this algorithm to High-Density Parity-check Codes. Based on the characteristics of the iterative decoding and the properties of dual codes, a soft-decision decoding algorithm for HDPC, using zeros codeword of dual code is proposed in this article. The proposed decoding algorithm allows to improve the decoding performance thanks to the number reduction of short cycles in the check matrix. Simulation results of the new decoding algorithm for Hamming codes shows that the decoding performance increases 0,3-0,65 dB at Bit Error Rate 10^{-4} while the decoding time is equivalent to using BPA.

Keywords: Soft-decision decoding, Hamming codes, iterative decoding.

1. ĐẶT VẤN ĐỀ

Một trong những phương pháp giải mã khối tuyến tính hiệu quả hiện nay là giải mã lặp dựa vào đồ hình song biên Tanner [1]. Đồ hình Tanner của một mã khối nhị phân tuyến tính $\mathbf{C}(n,k)$ được xây dựng từ ma trận kiểm tra $\mathbf{H}$. Các mã kiểm tra chẵn lẻ mật độ thấp (LDPC: Low-Density Parity-check Codes) khi áp dụng các thuật toán giải mã lặp (như BPA: Belief Propagation Algorithm) mang lại chất lượng giải mã rất tốt, do đặc điểm có ma trận kiểm tra $\mathbf{H}$ là ma trận thưa với số lượng các phần tử trên mỗi hàng và mỗi cột rất ít nên ít tồn tại các vòng kín ngắn (chu kỳ 4, 6) trong đồ hình Tanner [2]. Ngược lại, các mã cổ điển (đôi khi được gọi là mã kiểm tra chẵn lẻ mật độ cao (HDPC: High-Density Parity-check Codes)) đều có xu hướng chứa nhiều chu kỳ 4, 6 nên chất lượng giải mã không cao [3]. Bài báo này nghiên cứu áp dụng giải mã mềm cho mã khối, đồng thời xuất phát từ tính chất mang tin của từ mã đối ngẫu toàn "0", đưa ra thuật toán giải mã mới, khắc phục được ảnh hưởng của các vòng kín ngắn, áp dụng cho các mã HDPC.

Phần còn lại của bài báo gồm các nội dung chính như sau: mục 2 đánh giá hiệu quả giải mã của BPA khi áp dụng cho mã HDPC, như mã Hamming với số lần lặp khác nhau; mục 3 đề xuất thuật toán giải mã mềm mới dựa trên từ mã đối ngẫu toàn "0" nhằm giảm ảnh hưởng của các vòng kín ngắn; mục 4 đi sâu đánh giá chất lượng thuật toán giải mã mới từ kết quả mô phỏng trên kênh AWGN với các mã Hamming và cuối cùng là phần kết luận.

2. ĐÁNH GIÁ HIỆU QUẢ THUẬT TOÁN BPA CHO CÁC MÃ KIỂM TRA CHẴN LẺ MẬT ĐỘ CAO

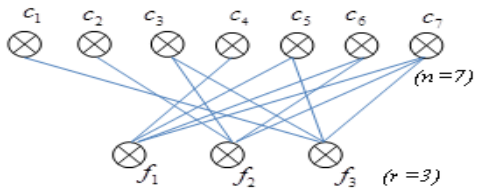
Để truyền qua kênh, giả sử, từ mã **c** được điều chế BPSK (Binary Phase Shift Keying). Trong qua trình truyền, giả sử tín hiệu đã điều chế **x** bị tác động bởi nhiễu Gauss trắng cộng tính (AWGN - Additive White Gaussian Noise) **w** có kỳ vọng bằng không và phương sai $\sigma^2 = N_0/2$ (N_0: là mật độ phổ công suất tạp âm). Kết quả tín hiệu nhận được là:

$$\mathbf{y} = \mathbf{x} + \mathbf{w} \quad (1)$$

Từ (1) cho thấy, tín hiệu nhận được tại đầu thu đều chịu tác động của nhiễu có thể bị sai lệch so với tin truyền đi. Vì vậy, chúng ta cần các phương pháp giải mã để đưa ra tin tại đầu thu là ít sai nhất.

Đồ hình Tanner có quan hệ chặt chẽ với ma trận kiểm tra **H** có kích thước $r \times n$ (n: chiều dài các bít từ mã, r: chiều dài các bít kiểm tra) của bộ mã, thể hiện trên hình 1.

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



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

Đồ hình Tanner gồm hai hàng là các nút mã $c=c_1,c_2,\ldots,c_n$ và các nút kiểm tra $f=f_1,f_2,\ldots,f_n$. Nút kiểm tra f_j nối với nút c_j khi và chỉ khi $H(j,i) = 1$ (với $H(j,i)$ là phần tử ở vị trí hàng j cột i của ma trận kiểm tra **H**). Bộ giải mã sử dụng thuật toán giải mã lặp như BPA, khi đó, thông tin sử dụng để giải mã sẽ được truyền qua lại giữa các nút bit và các nút kiểm tra khi có kết nối trên đồ hình Tanner.

Thuật toán BPA là thuật toán giải mã lặp có hai bước chính [2]:

Bước 1: Cập nhật bản tin cho tất cả các nút kiểm tra $j = 1,2,\ldots,r$ và gửi bản tin từ nút kiểm tra tới các nút bit nối với nó.

Bước 2: Cập nhật bản tin cho tất cả các nút bit $i = 1,2,\ldots,n$ và gửi bản tin từ các nút bit tới nút các kiểm tra nối với nó.

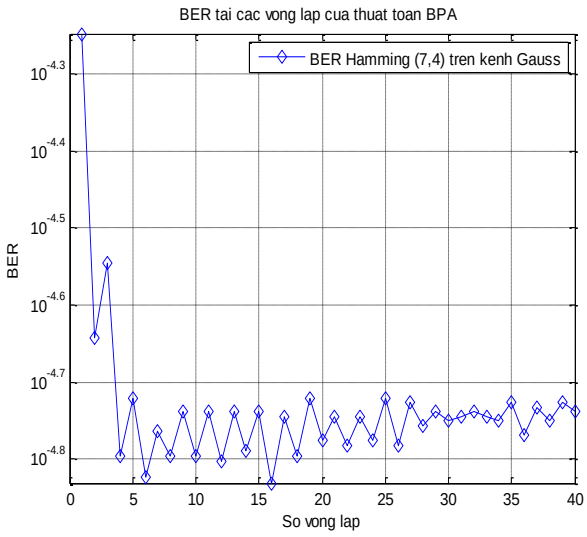
Đầu ra của bộ giải mã là giá trị tỷ lệ hợp lẽ theo hàm log (LLR: Log Likelihood Ratio) của các bit mã được sử dụng để quyết định thành từ mã thăm dò $\overline{c} = \overline{c}_1, \overline{c}_2, ..., \overline{c}_n,$. Nếu syndrome **s** thỏa mãn điều kiện:

$$s = \overline{c} \otimes H^{\mathrm{T}} = [0], \quad (2)$$

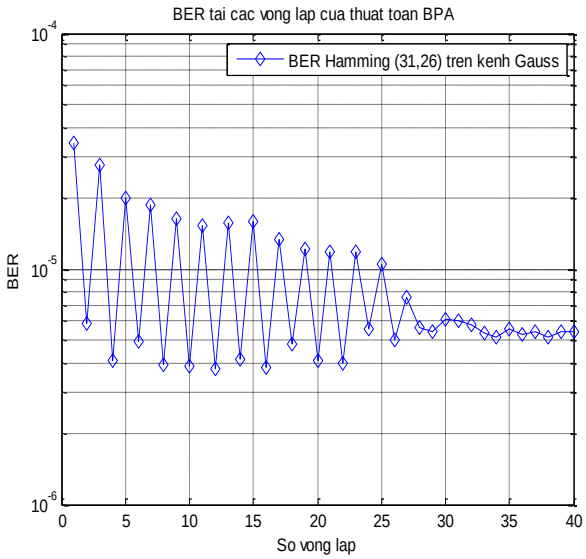
thì dừng lặp và đưa ra từ mã hợp lệ. Nếu điều kiện (2) không thỏa mãn thì quá trình được thực hiện lại từ bước 1cho đến khi đạt số lần lặp cực đại sẽ dừng và đưa ra từ mã tại vòng lặp cuối. Trong đó, $\otimes$ là ký hiệu biểu thị tích Kronecker, $\mathbf{H}^{\mathbf{T}}$ là ma trận chuyển vị của ma trận kiểm tra **H**.

Xét các mã Hamming (7,4) và (31,26). Bằng kỹ thuật mô phỏng Monte–Carlo, khảo sát tỷ lệ lỗi bit (BER: Bit Error Rate) với E_b/N_0 =8 dB (E_b là năng lượng bit trung bình) và số lần lặp K_{max} =40 .

Dựa vào kết quả mô phỏng nhận được trong hình 2, hình 3 ta có nhận xét: Từ lần lặp thứ 5 trở đi chất lượng giải mã cải thiện không đáng kể thậm chí còn kém hơn so với khi thực hiện số vòng lặp nhỏ hơn.



Hình 2. Chất lượng giải mã BPA mã Hamming (7,4)



Hình 3. Chất lượng giải mã BPA mã Hamming (31, 26)

Nhận xét trên có thể giải thích như sau: Ma trận kiểm tra của mã Hamming không đảm bảo tính thưa và tồn tại nhiều vòng kín ngắn trong nó làm giảm chất lượng giải mã, nhất là với các mã có chiều dài lớn. Vì vậy, thuật toán BPA áp dụng cho mã Hamming sẽ cho hiệu quả giải mã không cao và khi số vòng lặp tăng hay chiều dài từ mã tăng thì các vòng kín ngắn xuất hiện càng nhiều nên chất lượng giải mã giảm. Vấn đề đặt ra là làm thế nào để giảm các vòng kín ngắn trong ma trận kiểm tra **H.**

3. ĐỀ XUẤT THUẬT TOÁN GIẢI MÃ MỀM SỬ DỤNG TỪ MÃ ĐỐI NGẪU TOÀN "0" CHO CÁC MÃ MẬT ĐỘ CAO

Theo [1] cho thấy, các hàng trong ma trận kiểm tra **H** là các từ mã đối ngẫu với bộ mã gốc và từ mã đối ngẫu toàn "0" cũng mang thông tin giải mã. Mặt khác, trong quá trình giải mã, các bit kiểm tra (tương ứng với các hàng trong ma trận **H**) có độ tin cậy thấp dễ dẫn đến cho thông tin giải mã kém tin cậy (ví dụ ở bảng 1).

Như vậy, thay vì tích lũy thông tin từ các bit kiểm tra có độ tin cậy thấp ta sẽ chỉ nhận thông tin từ các bit kiểm tra có độ tin cậy cao. Điều này thực hiện bằng cách phải xác định được vị trí hàng chứa từ mã đối ngẫu có độ tin cậy thấp nhất và thay thế hàng đó bằng từ mã đối ngẫu toàn "0". Từ đây hình thành nên ý tưởng xây dựng một thuật toán giải mã mềm mới cho mã Hamming trên cơ sở sử dụng từ mã đối ngẫu toàn "0" (ký hiệu là DCZA: Dual Code' codeword of Zeros Algorithm).

Bảng 1. Khảo sát một số trường hợp giải mã sai khi truyền tin áp dụng thuật toán BPA cho mã Hamming (7, 4) với ma trận kiểm tra H trong hình 1

Từ mã truyền $c_1c_2c_3c_4c_5c_6c_7$	Giải mã $\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4\overline{c}_5\overline{c}_6\overline{c}_7$	Giá trị LLR của các nút kiểm tra
1000110	1010101	1.6135 0.4291 0.2058
0100011	0000000	0.7926 0.1699 1.2368
1110010	0110011	0.5954 1.3045 0.5954
0010111	0000000	1.9698 1.2849 0.9531
0000000	0011001	0.9755 0.1815 0.2757
1000110	1001100	3.1042 0.3243 1.4366

Từ mã truyền $c_1c_2c_3c_4c_5c_6c_7$	Giải mã $\overline{c}_1\overline{c}_2\overline{c}_3\overline{c}_4\overline{c}_5\overline{c}_6\overline{c}_7$	Giá trị LLR của các nút kiểm tra
0100011	1000011	1.4595 0.1384 1.2582
0011010	0000000	0.7883 1.1208 0.4190
0111001	0101010	0.4912 0.4786 0.0539

Từ những phân tích ở trên có thể thấy, việc sử dụng từ mã đối ngẫu toàn "0" thay thế cho một từ mã đối ngẫu có độ tin cậy thấp nhất trong ma trận kiểm tra của **H** mã Hamming sẽ làm tăng chất lượng giải mã khi áp dụng phương pháp giải mã trên cơ sở thuật toán BPA. Đó là do từ mã toàn "0" thuộc mã đối ngẫu nên mang thông tin giải mã cho từ mã gốc, mặt khác số vòng kín ngắn trong ma trận kiểm tra giảm giúp cho việc giải mã lặp dựa vào đồ hình Tanner chính xác hơn.

Vấn đề đặt ra là thay thế từ mã đối ngẫu toàn "0" cho hàng nào của ma trận kiểm tra ban đầu và khi nào trong quá trình giải mã để đạt được độ lợi cả về thời gian và độ tin cậy. Từ nhận xét ở trên, đề xuất chọn cải tiến thuật toán BPA tại vòng lặp thứ tư và tiến hành thay thế hàng chứa từ mã đối ngẫu trong ma trận kiểm tra **H** ứng với vị trí bit kiểm tra có độ tin cậy thấp nhất bằng từ mã đối ngẫu toàn "0". Thuật toán giải mã DCZA được thực hiện như sau:

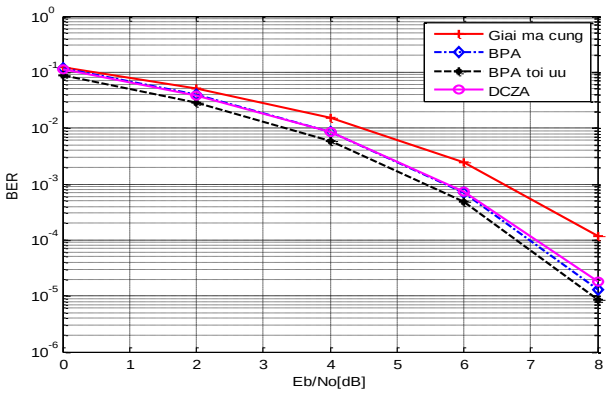
***Bước 1*:** Thực hiện giải mã theo thuật toán BPA dùng ma trận kiểm tra **H** với số lần lặp K_{max}=4. Tại mỗi vòng lặp đều kiểm tra điều kiện (1), nếu thỏa mãn thì đưa ra từ mã tương ứng, nếu không sẽ tiếp tục giải mã đến vòng lặp tối đa và chuyển sang bước 2.

***Bước 2*:** Xác định nút kiểm tra có độ tin cậy nhỏ nhất và thực hiện thay thế hàng trong ma trận **H** ứng với vị trí bit kiểm tra có độ tin cậy thấp nhất đó bằng từ mã đối ngẫu toàn "0".

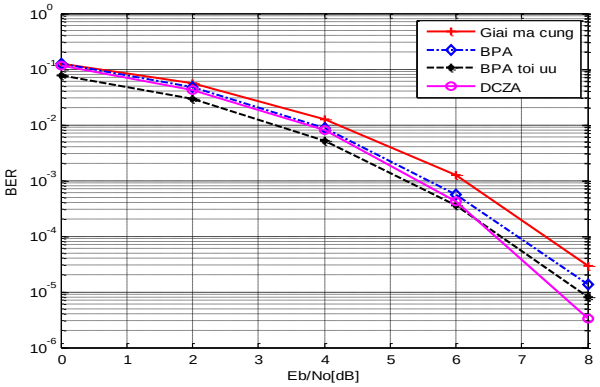
***Bước 3*:** Thực hiện giải mã lại theo thuật toán BPA sử dụng ma trận kiểm tra mới được xây dựng ở bước 2. Tại mỗi vòng lặp vẫn kiểm tra điều kiện (1), nếu thỏa mãn thì đưa ra từ mã tương ứng, nếu không sẽ tiếp tục giải mã và đưa ra từ mã tại vòng lặp tối đa β_{max}.

4. KẾT QUẢ MÔ PHỎNG VÀ THẢO LUẬN

Xét các mã Hamming (7, 4); (15, 11); (31, 26) và (63, 57), giả thiết điều chế BPSK và kênh truyền AWGN. Thực hiện mô phỏng đánh giá chất lượng giải mã của thuật toán giải mã mới DCZA với các thuật toán giải mã cứng, thuật toán BPA, thuật toán BPA tối ưu với cùng thông tin đầu vào, cho kết quả thể hiện trên hình 4, hình 5, hình 6 và hình 7. BPA tối ưu xây dựng trên cơ sở giả thiết bộ giải mã biết trước từ mã truyền để thực hiện quyết định lý tưởng, chọn cực tiểu số lượng lỗi qua tất cả các lần lặp để làm chuẩn so sánh với BPA và thuật toán giải mã mới. Từ kết quả mô phỏng ta thấy, BPA cho chất lượng giải mã tương đương thuật toán giải mã mới khi áp dụng cho mã Hamming (7, 4). Chất lượng giải mã của thuật toán này giảm dần khi chiều dài từ mã tăng dần so với sử dụng thuật toán giải mã cứng, thể hiện trên hình 5, hình 6 và hình 7. Khi áp dụng cho các mã Hamming (15, 11); (31, 26) và (63, 57) thuật toán giải mã mềm sử dụng từ mã đối ngẫu toàn "0" cho độ lợi tương ứng 0,3 dB; 0,45 dB; 0,65 dB tại tỷ lệ lỗi bít $BER = 10^{-4}$ so với thuật toán BPA. Nghĩa là từ mã càng dài, thuật toán mới càng cải thiện chất lượng nhiều hơn so với BPA.



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



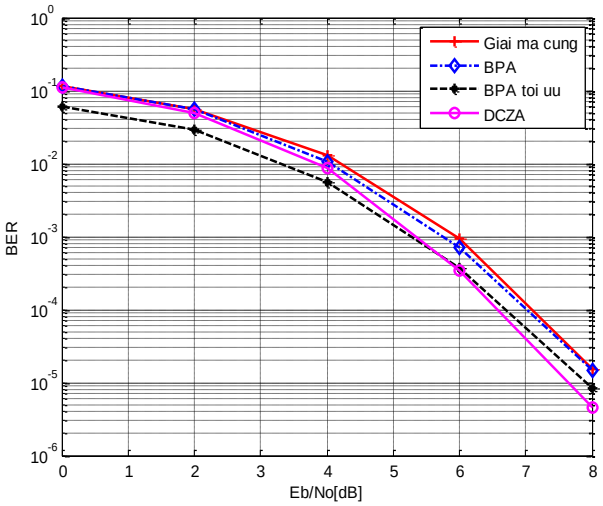
Hình 5. So sánh BER của mã Hamming (15,11) giữa các thuật toán

Điều này cũng hoàn toàn phù hợp với lý thuyết vì với các mã càng dài, việc thay thế một hàng trong ma trận kiểm tra bằng từ mã đối ngẫu toàn "0" sẽ không bị ảnh hưởng đến lượng tin cần có để giải mã, do các hàng còn lại vẫn đủ cung cấp thông tin giải mã. Mặt khác, DCZA sử dụng từ mã đối ngẫu toàn "0" đã giảm được các chu kỳ ngắn nên kết quả giải mã sau các vòng lặp cho chất lượng tăng. DCZA cần thêm bộ so sánh để xác định bít kiểm tra có độ tin cậy nhỏ nhất nên hệ thống phức tạp hơn và thời gian giải mã lâu hơn so với sử dụng BPA. Tuy nhiên, sau khi thay thế hàng trong ma trận **H** bằng từ mã đối ngẫu toàn "0" nên DCZA giảm được số lượng phép tính tối đa so với BPA là $\beta_{max}.O(q^2.w_r)$ [5]. Trong đó, q là bậc của trường Gallois (ta đang xét trong trường nhị phân $GF(2)$ nên q=2), w_r là trọng số hàng.

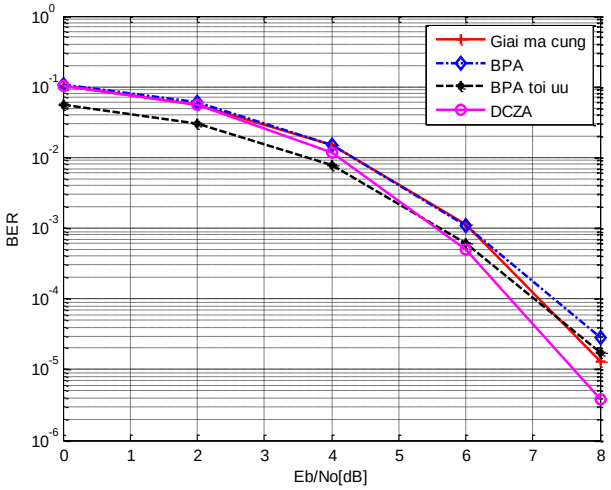
Vì thế, với từ mã dài (chiều dài lớn hơn 15), thời gian giải mã trung bình cho một từ mã giữa BPA và DCZA có thể coi là tương đương, thể hiện trên bảng 2.

Bảng 2. So sánh thời gian trung bình xử lý một từ mã giữa BPA và DCZA với các mã Hamming

Mã	BPA	DCZA
C(7, 4)	0,4743 ms	0.589 ms
C(15, 11)	1,006 ms	1,142 ms
C(31, 26)	3,625 ms	3,664 ms
C(63, 57)	14,229 ms	14,528 ms



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



Hình 7. So sánh BER của mã Hamming (63,57) giữa các thuật toán

5. KẾT LUẬN

Xuất phát từ tính chất đối ngẫu của mã sửa sai, các bít mã trong từ mã đối ngẫu đều mang thông tin của từ mã gốc. Bài báo đã đề xuất thuật toán cải tiến mới sử dụng ma trận kiểm tra có thay thế hàng ứng với vị trí bít kiểm tra có độ tin cậy thấp nhất bằng từ mã đối ngẫu toàn "0". Khả năng kiểm soát lỗi của các HDPC tăng do giảm được số vòng kín ngắn trong ma trận kiểm tra. Thuật toán được đề xuất cải thiện chất lượng giải mã cho các mã Hamming (15, 11); (31, 26) và (63, 57) tương ứng 0,3 dB; 0,45 dB; 0,65 dB tại $BER = 10^{-4}$ so với thuật toán BPA với thời gian giải mã tương đương.

TÀI LIỆU THAM KHẢO

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

[2] R.G. Gallager, *Low Density Parity Check Codes,* Cambridge, MA: MIT, 1963.

[3] J. Knudsen, C. Riera, L. Danielsen, M. Parker, and E. Rosnes, "Random edge-local complementation with applications to iterative decoding of high-density parity-check codes," *Transactions on Information Theory*, vol. 60, Issue: 10, pp. 2796-2808, October 2012.

[4] C.R P. Hartmann and L. D . Rudolph, "An Optimum Symbol-by Symbol decoding rule for linear codes," *IEEE Transactions on Information Theory*, vol. 22, pp. 514-517, 1976.

[5] M. Davey and D. J.C. Mackay, "Low- Density Parity Check Codes over GF(q)", *IEEE Comm. Letters*, 2(6), pp. 165-167, June 1998.

Thông tin liên hệ: **Nguyễn Thị Hồng Nhung**

Điện thoại: 0945 616 629 - Email: nthnhung@uneti.edu.vn
Khoa Điện tử - Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Phạm Văn Nam

Điện thoại: 0946 228 760 - Email: pvnam@uneti.edu.vn
Khoa Điện tử - Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Nguyễn Mai Anh

Điện thoại: 0989 997 649 - Email: nmanh@uneti.edu.vn
Khoa Điện tử - Trường Đại học Kinh tế - Kỹ thuật Công nghiệp.