Tạp chí Tin học và Điều khiển học, T.23, S.4 (2007), 309–316

MÃ ĐÀN HỒI VÀ MỘT TIẾP CẬN ĐẠI SỐ

VŨ THÀNH NAM, PHAN TRUNG HUY

Khoa Toán - Tin ứng dụng, Trường ĐH Bách khoa Hà Nội

Abstract. A new kind of products to be set up using control components is one of new research directions in theory of codes recently. Type of codes like that zigzag codes or T-codes has been studied by different scientists. In this paper, a new product of words is proposed and named as the spring product. On the basics of the propose, a new type of codes, i.e., spring codes is considered and certain basic properties are established which permits to build an algorithm checking wherther a given regular language is spring code or not.

Tóm tắt. Một trong những hướng nghiên cứu mở rộng trong lý thuyết mã là sử dụng các yếu tố điều khiển xây dựng khái niệm tích của các từ để xây dựng các lớp mã mới. Những hình thức mã mới như mã zigzag, mã điều khiển theo tích trộn đã được nhiều tác giả trên thế giới nghiên cứu. Trong bài này, chúng tôi đề xuất một hình thức tích mới - tích đàn hồi. Từ đó đưa ra lớp mã mới dựa trên tiếp cận đồ thị và đại số mã tích đàn hồi. Một số tính chất của lớp mã này được xây dựng, từ đó cho phép thiết lập một thuật toán kiểm tra một ngôn ngữ chính quy có là mã đàn hồi hay không.

1. GIỚI THIỆU

Giả sử A là tập hữu hạn hoặc vô hạn các ký hiệu mà ta gọi là bảng chữ cái. Trong bài này, các bảng chữ giả thiết là hữu hạn.

Tập tất cả các từ hữu hạn trên A bao gồm cả từ rỗng ε được ký hiệu là A^*, tập $A^* - \{\varepsilon\} = A^+$ là nửa nhóm tự do sinh bởi A. Tích các từ thông thường là phép nối ghép từ (concatenation). Cho từ w, w', ký hiệu $|w|$ là độ dài từ w, và ký hiệu $w' <_P w$ nếu w' là tiền tố (prefix) thực sự của w ($w'| < |w|$).

Ngôn ngữ $X \subseteq A^+$ gọi là mã nếu mỗi từ $w \in A^+$ có không quá một phân tích bởi các từ trong $X (w = x_1 ... x_n,\ n \geq 1,\ x_i \in X)$. Như vậy, trong mã thông thường, tích hai từ là phép đặt 2 từ cạnh nhau.

Một trong các hướng mở rộng nghiên cứu lý thuyết mã là đưa ra các khái niệm tích mở rộng, sử dụng các yếu tố điều khiển, nhập nhằng. Từ đó xây dựng các lớp mã mới.

Những năm 1990 đã có một số phương pháp mở rộng khái niệm tích các từ mã sử dụng các kỹ thuật khác nhau để từ đó đề xuất xây dựng các lớp mã mới. Có thể kể đến:

- Phân tích zigzag do M. Anselmo đề xuất trong [1]. Ý tưởng của phân tích zigzag là trong phân tích có thể chứa các bước lùi khử từ.

- Mã tích trộn có điều khiển dựa trên tích trộn ([8, 9, 12]) vào cuối những năm 1990. Trong đó ý tưởng tích trộn có điều khiển là sử dụng thành phần điều khiển để xác định quá trình mã và giải mã.

Từ đó có thể thấy nghiên cứu lý thuyết mã gần đây có xu hướng đưa vào các yếu tố điều

khiển, đa trị, nhập nhằng để mở rộng khái niệm tích, từ đó xây dựng những lớp mã mới. Về khía cạnh ứng dụng, bảo mật dữ liệu nhờ áp dụng một phương pháp mã hóa đơn trị (một bản rõ cho ta một bản mã) và lâu dài nguy cơ bị thám mã sẽ tăng bởi các tấn công xác suất dựa trên mẫu thu lượm bởi đối phương. Mã hóa đa trị và biến động (một bản rõ có thể đưa ra nhiều bản mã khác nhau ngẫu nhiên và độ dài co dãn cũng khác nhau) là một tiếp cận tăng độ khó thám mã lên rất cao vì số mẫu thu được sẽ là quá nhỏ để có thể sử dụng tấn công xác suất.

Theo xu hướng đó, trong bài này, với cơ sở là tích đàn hồi, trong đó tích của hai từ có thể nén lại hoặc dãn dài, đã được giới thiệu lần đầu tiên trong [10], chúng tôi trình bày một dạng của hình thức mã đàn hồi dựa trên cơ sở đại số và lý thuyết đồ thị, và đặt quan tâm nghiên cứu trên lớp các ngôn ngữ chính quy.

2. TÍCH ĐÀN HỒI VÀ MÃ ĐÀN HỒI TRÊN ĐỒ THỊ

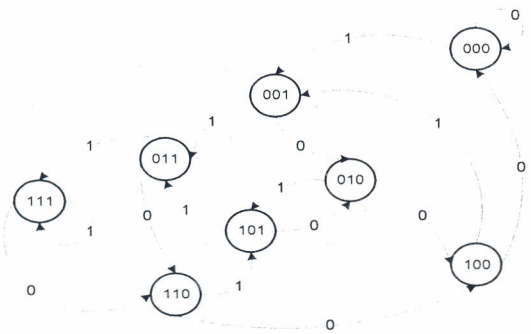
Mở đầu mục này, trước hết xin nhắc lại khái niệm về tích đàn hồi và mã đàn hồi dựa trên phương pháp đồ thị, đã được trình bày lần đầu trong [10].

Ta giới hạn xem xét các ngôn ngữ xây dựng từ bảng chữ nhị phân $B = \{0, 1\}$ có độ dài như nhau, $X \subseteq B^k = \{0, 1\}^k$. Ý tưởng xây dựng tích đàn hồi là trong quá trình mã hóa, tích của các từ không là tích ghép như tích thông thường mà có thể "co lại" hoặc "kéo dãn" - nghĩa là có tính đàn hồi.

Trong mục này, chúng ta sẽ sử dụng đồ thị để đặc trưng khái niệm tích đàn hồi (được gọi là đồ thị xác định mã đàn hồi).

Đồ thị mã đàn hồi: cho tập B^k gồm 2^k đỉnh. Mỗi đỉnh được gán tên bởi xâu k bit có giá trị từ 0 đến $2^k - 1$. Từ mỗi đỉnh $b = b_1b_2...b_k \in B^k$ có 2 cung đi đến 2 đỉnh p, q có $k - 1$ bit đầu trùng với $k - 1$ bit cuối của b. Cụ thể, cung từ đỉnh $p = b_1b_2...b_k$ với nhãn d, $d = 0$ hay 1, sẽ có đỉnh cuối là $p = b_2...b_kd$.

Ví dụ 2.1. Với $k = 3$, ta có đồ thị mô tả cho $B^3 = \{0, 1\}^3$ như sau



Hình 2.1. Đồ thị mã đàn hồi

Tích đàn hồi

Với việc sử dụng biểu diễn bằng đồ thị như trên, ta có thể định nghĩa tích đàn hồi của hai từ $x, y \in B$ như sau.

Định nghĩa 2.1. Cho ngôn ngữ $X \subseteq B^k = \{0, 1\}^k$, hai từ $x, y \in X$ mà hai đỉnh tương ứng trong đồ thị của B^k là x_B, y_B. Một giá trị tích đàn hồi của x và y, ký hiệu $x._p y$ được xác định bởi nhãn w của một đường đi p từ x_B đến y_B, không đi qua các đỉnh trung gian thuộc X, $p : x_B \rightsquigarrow y_B$.

Chú ý rằng qua cách thể hiện bằng đồ thị ở trên, có thể có nhiều đường đi $p : x_B \rightsquigarrow y_B$ hoặc không có p, nghĩa là tích đàn hồi của x và y có thể xác định một cách không đơn trị nếu lựa chọn được nhiều đường đi p.

Ta định nghĩa $w = x_{1.p}x_{2.p}...p_{x_n} = (x_{1.p}x_{2.p...p}x_{n-1})_{.p}x_n$. Khi đó, dãy từ $x_1, x_2, ..., x_n$ được gọi là một sự phân tích đàn hồi của từ w thành các từ thuộc X.

Ví dụ 2.2. Cho $X = \{000, 010, 110, 101\}$ và ánh xạ mã hóa cho ứng các chữ bản rõ a, b, c, d thành dãy các xâu nhị phân, xem như a là 000, b là 010, c là 110, d là101.

Khi đó từ ab được mã bởi xâu 00(0)10 là một tích đàn hồi của 000 và 010 (xem như $a_{.p}b$)với tính chất "co lại" thay vì như tích thông thường 000010. Có thể thấy 00010 phân tích (giải mã) duy nhất thành từ ab xem như dãy các từ 000, 010 trong X.

Tuy nhiên nếu mã từ ad bởi xâu 000101 theo tích thông thường thì giải mã (theo tích đàn hồi) lại là abd vì có một khai triển tích đàn hồi $000101 = (000)_{.p}(010)_{.p}(101)$ (xem như $a_{.p}b_{.p}d$).

Để tránh tình huống này, khi mã hóa ad ta sẽ "kéo dãn" từ mã bởi tích đàn hồi thích hợp $000_{.p}101 = 0001101$ (xem như $a_{.p}d$) , khi đó 0001101 được giải mã (duy nhất) thành ad.

Từ khái niệm tích đàn hồi, ta xây dựng khái niệm mã đàn hồi như sau.

Định nghĩa 2.2. Cho ngôn ngữ $X \subseteq B^k = \{0, 1\}^k$, X là mã tích đàn hồi nếu một từ bất kỳ được phân tích theo tích đàn hồi bởi các từ trong X là duy nhất.

Từ định nghĩa mã đàn hồi, ta nhận được tính chất hiển nhiên sau.

Tính chất 2.1. *Cho ngôn ngữ $X \subseteq B^k = \{0, 1\}^k$, điều kiện cần và đủ để X là mã đàn hồi là*

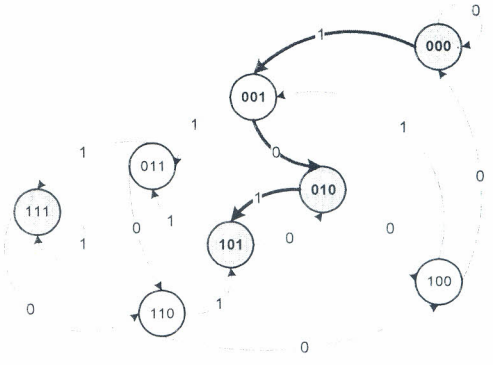
$$\forall x, y \in X : x_A^+ \cap A^+y - A^+XA^+ \neq \phi.$$

Ví dụ 2.3. Cho B^3, ngôn ngữ $X = \{000, 010, 101, 111\}$. Giả sử có ánh xạ mã:

$$a \to 000,\ b \to 010,\ c \to 111,\ d \to 101.$$

Tích ab được mã hóa bởi đường đi từ đỉnh 000 đến đỉnh 010 qua đỉnh 001 : $ab \to 00010$.

Tích abd được mã hóa bởi đường đi từ đỉnh 000 qua 001,010 đến 101: $abd \to 000101$.



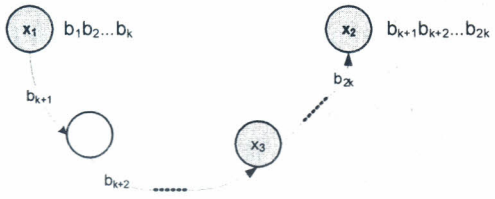
Hình 2.2. Mã hóa sử dụng tích đàn hồi

Việc giải mã được tiến hành bằng việc duyệt theo con đường xác định bởi các nhãn. Chẳng hạn 000101 được giải mã như sau: từ đỉnh $000 = a$ theo nhãn 1 đến đỉnh 001, tiếp tục theo nhãn 0 đến đỉnh $010 = b$, cuối cùng theo nhãn 1 đến đỉnh $101 = d$.

Mệnh đề 2.2. *Cho ngôn ngữ $X \subseteq B^k$. Nếu với mọi cặp đỉnh $x, y \in X$, tồn tại ít nhất một đường đi không qua bất kỳ đỉnh nào khác thuộc X thì X là mã đàn hồi.*

Chứng minh. Giả sử ngược lại, nếu X là mã đàn hồi nhưng có 2 đỉnh x_1, x_2 mà mọi đường đi giữa chúng đều qua ít nhất một đỉnh thuộc X.

$$x_1 = b_1b_2...b_k,\ x_2 = b_{k+1}b_{k+2}...b_{2k}.$$



Xét đường đi từ x_1 đến x_2 qua các cung có nhãn $b_{k+1}b_{k+2}...b_{2k}$. Đường đi này mã hóa cho từ x_1x_2. Từ giả thiết ta có đường đi này đi qua đỉnh x_3 thuộc X và do đó nó cũng là mã hóa cho $x_1x_3x_2$. Như thế tồn tại từ có hai phân tích theo tích đàn hồi, X không là mã đàn hồi. ∎

3. ÁNH XẠ LẬP MÃ

Trong hệ mã, các phép mã hóa, giải mã dựa trên các bộ mã có bản chất là các ánh xạ (từ bảng chữ bản rõ sang bảng chữ bản mã), như thế, để có thể triển khai ứng dụng, ta cần nghiên cứu xây dựng ánh xạ lập mã.

Ánh xạ mã đàn hồi

Cho bảng chữ bản rõ Σ hữu hạn, vị nhóm $M, B \subseteq M$. Đồng cấu $h : \Sigma^* \to M$ tương ứng mỗi chữ cái a với phần tử $m = h(a) \in B$.

Từ mã đàn hồi trên đồ thị ở mục trước, trong mục này, để mở rộng lớp mã, ta sẽ trình bày khái niệm đồ thị trên vị nhóm.

Định nghĩa 3.2.1. Cho vị nhóm hữu hạn M, bảng chữ Σ hữu hạn và một đồng cấu vị nhóm $h : \Sigma^* \to M$. Một đồ thị có hướng $G(M, h, \Sigma)$ trên vị nhóm M được định nghĩa bởi:

(i) Tập đỉnh của G là M.

(ii) Tập các cung được xác định bởi mỗi cung với nhãn t, $t \in \Sigma$, đi từ đỉnh m đến $n, m, n \in M$, là bộ (m, n, t) thỏa $m.h(t) = n$.

Định nghĩa 3.2.2. Cho vị nhóm M, bảng chữ Σ hữu hạn và đồng cấu vị nhóm $h : \Sigma^* \to M$, $B \subseteq M$. Nếu với mọi $m, n \in B$, tồn tại đường đi từ m đến n không qua các đỉnh trung gian b' thuộc B, thì B được gọi là tập mã đàn hồi trên đồ thị $G(M, h, \Sigma)$.

Ta có ngay đặc trưng sơ cấp của tập mã đàn hồi sau.

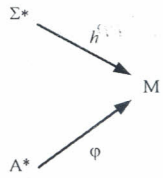
Tính chất 3.2.1. *Cho bảng chữ Σ, nếu $B = \{h(a_i) : a_i \in \Sigma\}$ là mã đàn hồi thì B thuộc một lớp thỏa quan hệ Green R.*

Định nghĩa 3.2.3. Cho bảng chữ bản rõ Σ hữu hạn, vị nhóm hữu hạn M, đồng cấu vị nhóm $h : \Sigma^* \to M, B = h(\Sigma)$. Cho bảng chữ bản mã A, đồng cấu vị nhóm $\varphi : A^* \to M$. Cặp (h, φ) được gọi là cặp ánh xạ lập mã đàn hồi nếu thỏa:

(i) h thu hẹp trên Σ là song ánh;

(ii) $\forall b \in B : \varphi^{-1}(b) \neq \{\varepsilon\},\ \varphi^{-1}(b) \neq \phi$;

(iii) B là mã đàn hồi trên đồ thị $G(M, \varphi, A)$.



Hình 3.2.1. Cặp ánh xạ lập mã đàn hồi

Sơ đồ ứng dụng cặp ánh xạ lập mã đàn hồi

Quá trình mã hóa

a) Cho từ hiện bản rõ $x = a_1a_2...a_k$. Mã hóa từng chữ cái của bảng chữ bản rõ như sau:

$a_1 \to w_1 \in \varphi^{-1}(h(a_1))$, sao cho không có tiền tố w' nào của w_1 có $\varphi(w') \in B$;

$a_2 \to w_2$, tương tự trên;

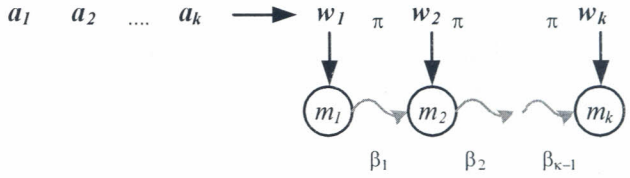
...

$a_k \to w_k$.

b) Quá trình mã hóa các xâu từ hiện được thực thi như sau (theo phương pháp mã đàn hồi):

$a_1a_2 \to w_1\beta_1$, trong đó β_1 là nhãn của đường đi p từ đỉnh đồ thị ứng với $\varphi(w_1)$ đến đỉnh ứng với $\varphi(w_2)$ mà không qua đỉnh trung gian nào của B.

Tiếp tục ta có $x = a_1a_2...a_k \to y = w_1\beta_1\beta_2...\beta_{k-1}$.



Hình 3.2.2. Quá trình mã hóa

Quá trình giải mã

a) Từ chuỗi mã hóa y, tìm xâu tiền tố ngắn nhất w_1 sao cho $\varphi(w_1) = m_1 \in B$.

Vì h là song ánh nên tồn tại duy nhất chữ cái $a_1 \in A : m_1 = h(a_1)$.

b) Đọc tiếp đến khi được xâu $w_1\beta_1$ sao cho $\varphi(w_1\beta_1) = m_2 \in B$. Do h là song ánh nên tồn tại duy nhất $a_2 \in A : m_2 = h(a_2)$.

Quá trình được thực hiện tiếp tục đến khi giải mã xong.

4. MỘT TIẾP CẬN ĐẠI SỐ VÀ MÃ ĐÀN HỒI CHÍNH QUY

Trước hết, chúng tôi giới thiệu một hình thức về mã đàn hồi, sử dụng các công cụ đại số. Độc giả có thể xem thêm [3, 6] về các kiến thức cơ sở có liên quan. Sau đó trình bày một số kết quả, trong đó kết quả chính nhằm chứng minh sự tồn tại của thuật toán kiểm định một ngôn ngữ chính quy có là mã đàn hồi hay không.

Cho bảng chữ cái A hữu hạn, $X \subseteq A^*$, R là một tương đẳng trên A^* với chỉ số hữu hạn (M là vị nhóm thương A^*/R có hữu hạn phần tử).

Ta nói tương đẳng R thỏa X (hay X được thỏa bởi tương đẳng R nếu $\forall x \in X$, $\forall x' \in A^* : xRx' \Rightarrow x' \in X$. Từ đó ta có, nếu tương đẳng R chỉ số hữu hạn thỏa X thì $X = \cup[x]_R$ là hợp của hữu hạn các lớp thương theo tương đẳng R. Ví dụ tầm thường, tương đẳng cú pháp $\sim_X$ của X xác định bởi $\forall u, v \in A^* : u \sim_x v \Leftrightarrow \forall t, s \in A^* : tus \in X \Leftrightarrow tvs \in X$, là một tương đẳng thỏa X.

Tính chất 4.1. [6]

1) *X là ngôn ngữ chính quy khi và chỉ khi X thỏa được bởi một tương đẳng chỉ số hữu hạn;*

2)*X là ngôn ngữ chính quy khi và chỉ khi tương đẳng cú pháp $\sim_X$ của X là một tương đẳng chỉ số hữu hạn.*

Định nghĩa 4.1. Cho ngôn ngữ $X \subseteq A^*$, tương đẳng ρ chỉ số hữu hạn, ta nói X là mã đàn hồi theo tương đẳng ρ nếu:

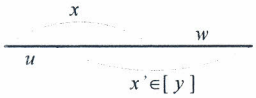
1) A^*X thỏa bởi ρ;

2) $\forall x \in X, \forall y \in A^*X$, tồn tại A^*X thác triển của x, tức là tồn tại từ $w \in A^*$ sao cho

i) $xw \in A^*X$;

ii) $\forall w_1 <_P w : xw_1 \notin A^*X$ và;

iii) $xw\rho y$.



Ta nói X là mã đàn hồi nếu có tương đẳng ρ chỉ số hữu hạn sao cho X là mã đàn hồi theo ρ. Ta có ngay tính chất sau.

Tính chất 4.2. *Nếu X là mã đàn hồi theo tương đẳng $\rho_1, \rho_1 \subseteq \rho_2$ và A^*X thỏa ρ_2 thì X là mã đàn hồi theo tương đẳng ρ_2.*

Chứng minh. Thật vậy, trong định nghĩa mã đàn hồi ta có:

1) Do X là mã đàn hồi theo tương đẳng ρ_1 do đó A^*X thỏa ρ_1, mặt khác theo giả thiết ta có A^*X thỏa ρ_2.

2) $\forall x \in X$, $\forall y \in A^*X$, tồn tại A^*X thác triển xw của x để $xw\rho_1 y$, do $\rho_1 \subseteq \rho_2$ ta có $xw\rho_2 y$.

Từ 1) và 2), X là mã đàn hồi theo tương đẳng ρ_2. ∎

Hệ quả sau chỉ ra tính phổ dụng của tương đẳng cú pháp $\sim_{A^*X}$ theo khái niệm mã đàn hồi.

Hệ quả 4.1. *Nếu X là mã đàn hồi theo tương đẳng ρ nào đó thì X là mã đàn hồi theo tương đẳng cú pháp $\sim_{A^*X}$ của A^*X.*

Chứng minh. Đây là hệ quả trực tiếp từ mệnh đề trên và bao hàm $\rho \subseteq \sim_{A^*X}$ theo tính chất của tương đẳng cú pháp A^*X. ∎

Một trong những câu hỏi cơ bản là cho tập X, có thuật toán để kiểm tra X có là mã hay không? Từ hệ quả về tính phổ dụng trên, ta thấy rằng, để kiểm tra X có là mã đàn hồi theo tương đẳng ρ nào đó hay không có thể quy về kiểm tra X có là mã đàn hồi theo tương đẳng $\sim_{A^*X}$ hay không.

Với điều kiện ngôn ngữ X là chính quy, ta có kết quả sau.

Định lý 4.1. *Cho ngôn ngữ X chính quy, tồn tại thuật toán kiểm tra X có là mã đàn hồi hay không.*

Chứng minh. Gọi $\rho = \sim_{A^*X}$ là tương đẳng cú pháp của A^*X, $M = A^*/\rho$ là vị nhóm cú pháp của A^*X. Do X, A^* là ngôn ngữ chính quy, A^*X chính quy và M hữu hạn. Xây dựng đồng cấu φ cú pháp $\varphi : A^* \to M$, $x \in X : \varphi(x) = [x]\rho$. Đặt $B = \varphi(X)$, $B \subseteq M$.

Đặt $C = \varphi(A^*X)$, $C \subseteq M$. Do A^*X thỏa ρ nên $\varphi^{-1}(C) = A^*X$.

Vì M là hữu hạn, B, $C \subseteq M$, từ đó $|B|$ và $|C|$ hữu hạn.

Lập luận 1. X là mã đàn hồi, với $x \in X$, $y \in A^*X$ tùy ý ta có tồn tại A^*X thác triển, có nghĩa tồn tại w để:

(i) $xw \in A^*X$;

(ii) $\forall w_1 <_P w$ (w_1 là tiền tố của w); $xw_1 \notin A^*X$;

(iii) $xw\rho y$.

Xét đồ thị có hướng hữu hạn có gán nhãn, với tập đỉnh là M, trong đó đường đi từ m đến $n, m, n \in M$ với nhãn $\alpha \in A^*$ được định nghĩa bởi $\delta : m \xrightarrow{\alpha} n = \varphi(\alpha).m$ (khi α là một chữ thuộc A, ta hiểu δ là cung của đồ thị với nhãn α).

Lập luận 2. Các điều kiện (i), (ii), (iii) sẽ đưa về điều kiện tương đương, có đường đi từ $b = \varphi(x) \in B$ đến $c = \varphi(y) \in C; b \rightsquigarrow c$ mà nó không đi qua bất cứ điểm $c' \in C$ trung gian nào, $b = \varphi(x) \in B$ và $c = \varphi(y) \in C$. Thật vậy:

a) Nếu có đường đi $b \rightsquigarrow c$ mà nó không đi qua bất cứ điểm $c' \in C$ trung gian nào. Giả sử nhãn của đường đi là w, khi đó xw là A^*X thác triển của x mà (i), (iii) thỏa mãn (theo định nghĩa về đường đi đã nêu trên và tính chất sơ cấp là A^*X thỏa bởi $\rho = \sim_{A^*X}$). Do đường đi không có đỉnh trung gian thuộc C, suy ra (ii) thỏa mãn với xw.

b) Ngược lại, giả sử x có A^*X thác triển là từ xw thỏa (i), (ii), (iii), khi đó theo (i) và (ii), w là nhãn một đường đi từ b đến c. Do (ii), suy ra đường đi này không đi qua một đỉnh trung gian c' thuộc C nào ngoại trừ đỉnh cuối c.

Từ các lập luận trên, thay vì kiểm tra tính chất trên X, A^*X, ta có thể kiểm tra trên đồ thị và các tập đỉnh B, C, tìm đường đi từ đỉnh b đến đỉnh c thỏa điều kiện trên. Do M có hữu hạn phần tử nên ta có thuật toán mô tả một cách hình thức như sau để kiểm tra X có là mã đàn hồi theo tương đẳng $\sim_{A^*X}$ không, nhờ phương pháp quen thuộc trong lý thuyết đồ thị.

Thuật toán Test (kiểm tra X có là mã đàn hồi theo tương đẳng $\sim_{A^*X}$ không)

Bước 1. Tính $B = \varphi(X)$; $C = \varphi(A^*X)$;

(Do X, A^*X chính quy nên có thuật toán tính B, C)

Bước 2.

```
Test=true;
For b ∈ B do
    For c ∈ C do
        Nếu không tồn tại đường đi từ b đến c mà không qua đỉnh c' ∈ C nào thì
        Test=false;
        Exit;
    EndFor;
EndFor;
```

Bước 3. Return(Test);

Việc chỉ ra thuật toán này kết thúc phép chứng minh định lý. ■

Chú ý. Điều kiện 2.(ii) trong định nghĩa được thỏa mãn với từ xw được gọi là *điều kiện tránh* A^*X.

Ví dụ 4.1. Cho ngôn ngữ chính quy L trên bảng chữ bản mã Γ. Đặt $X = A^*L$. Dễ thấy $A^*X = X$. Giả sử Σ là bảng chữ bản rõ và X đã là mã đàn hồi theo tương đẳng ρ trên Γ, ta sẽ xây dựng một lược đồ mã hóa và giải mã. Trước hết, để ý rằng, nếu A^*L thỏa tương đẳng thì X và A^*X cũng vậy.

Quá trình mã hóa: Do X là mã đàn hồi (trên bảng chữ bản mã), ta có thể xây dựng phương pháp mã hóa xác định bởi ánh xạ đơn ánh. Ứng mỗi chữ cái a của bảng chữ bản rõ Σ với một lớp tương đẳng ρ, ký hiệu $[x_A]$ trong X, tích đàn hồi của hai chữ cái a, b được xác định bởi nhãn w của một đường đi (giá trị u tùy ý thuộc $[x_A]$ ghép với nhãn w) tùy ý tránh $A^*X(= X)$ từ lớp tương đẳng $[x_A]$ đến $[x_B]$.

Quá trình giải mã: Biết từ u khởi đầu, ta xác định được chữ cái a của bản rõ, đọc từ trái sang đến khi nhận được từ uw thuộc A^*X, mà ảnh ngược của nó ứng với chữ cái b tiếp theo của bản rõ,...

5. KẾT LUẬN

Tích đàn hồi là một hướng nghiên cứu mở rộng sử dụng các yếu tố nhập nhằng, đa trị trên các tiếp cận ghép từ mã mà một số nghiên cứu như [1, 7, 11, 12] đã xem xét. Để nghiên cứu các đặc trưng, chúng ta có thể áp dụng nhiều kỹ thuật khác nhau. Còn nhiều vấn đề lý thú cần tiếp tục nghiên cứu về lớp mã này, chẳng hạn:

- Các tính chất đại số, tổ hợp và phân lớp trên các mã đàn hồi.
- Xây dựng thuật toán tìm tập X là mã đàn hồi cực đại.
- Xác định các mã đàn hồi hiệu quả đưa vào ứng dụng thực tế bảo mật dữ liệu...

TÀI LIỆU THAM KHẢO

[1] M. Anselmo, Sur les codes zig-zag et leur decidabilité, *Theor. Comp. Sc.* **74** (1990) 341–354.

[2] A. Arnold, Deterministic and non-ambiguous rational ω-languages, *Lecture Notes in Computer Science* **192** (1985) 138–146.

[3] J. Berstel and D. Perrin, *Theory of Codes*, Academic Press, NewYork, 1985.

[4] Do Long Van, Bertrand Le Saec, Igor Littovsky, On coding morphism for ZigZag code, *Theoretical Informatics and Applications* **26** (6) (1992).

[5] Do Long Van, Bertrand Le Saec, Igor Littovsky, Stability for the Zigzag submonoids, *Theory Computer Science* **108** (2) (1993) 237–249.

[6] S. Eilenberg, *Automata, Languages and Machines* Vol. A, Acad. Pres. New York, 1974.

[7] Phan Trung Huy, Do Long Van, On non-ambiguous Buchi V-automata, *Proceedings of the third Asian Mathematical Conference 2000*, Diliman, Philippines, 23 - 27 October 2000 (224–233).

[8] A. Mateescu, G.D. Mateescu, G. Rozenberg, A. Salomaa, Shuffle-like operations on omega-words, New trends in formal languages, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, Heidelberg **Vol. 1218** 1997 (395–411).

[9] A. Mateescu, G. Rozenberg, and A. Salomaa, Shuffle on trajectories: Syntactic constraints, *Theor. Comp. Sci.* **197** (1) (1998) 1–56.

[10] Vu Thanh Nam, Phan Trung Huy, Nguyen Thi Thanh Huyen, Mã tích đàn hồi và tìm kiếm trên văn bản mã hoá sử dụng thuật toán so mẫu theo tiếp cận mờ, *Báo cáo khoa học tại Hội nghị Ứng dụng toán học toàn quốc lần thứ 2*, Hà Nội, 12-2005.

[11] Do Long Van, Nguyen Huong Lam, Phan Trung Huy, On codes concerning bi-infinite words, *Acta Cybernetica* **11** (1–2) Szeged (1993).

[12] Xavier Augros, "Des Algorithmes Autour des Codes Rationnels", Thèse Docteur en Sciences 2001, Univ. Nice - Sofia Antipolis.

Nhận bài ngày 5 - 7 - 2006
Nhận lại sau sửa ngày 14 - 1 -2007