Tạp chí Tin học và Điều khiển học, T. 20, S. 1 (2004), 73–79

MÃ HÓA KÊNH, NHÌN TỪ QUAN ĐIỂM CỦA LÝ THUYẾT HỆ THỐNG

NGÔ ĐÔNG HẢI

Học viện Công nghệ Bưu chính Viễn thông

Abstract. From the point of view of system Theory, a channel coder (or decoder) is a multiple input - multiple output (MIMO) invariant linear system. The system states can be fully analysed in the state space by criteria of the system theory. The stability, controllability and observability of the system are guaranteed by the limit of the noise.

Tóm tắt. Theo quan điểm của lý thuyết hệ thống, một bộ mã hóa kênh (hay giải mã) là một hệ thống tuyến tính bất biến MIMO. Trạng thái của hệ hoàn toàn có thể phân tích trong không gian trạng thái bằng các tiêu chuẩn của lý thuyết hệ thống. Tính ổn định, tính điều khiển được và quan sát được của hệ được đảm bảo bằng giới hạn của nhiễu.

1. MỞ ĐẦU

Đa số các hệ thống thông tin đều cố gắng nâng cao hiệu suất sử dụng kênh truyền thông qua việc mã hóa dữ liệu bằng mã kênh (từ đây gọi chung là mã) trước khi thực hiện điều chế. Mục đích của các loại mã là phát triển một phương pháp truyền thông tin sao cho có thể giảm thiểu xác suất gây ra lỗi, đồng thời cung cấp khả năng phát hiện, định vị lỗi và sửa được lỗi ở một mức độ nào đó.

Lý thuyết về mã đã được nghiên cứu và phát triển tương đối hoàn thiện và đã được trình bày trong rất nhiều giáo trình chuyên ngành. Bài viết này trình bày một cách nhìn tổng quát về mã nói chung, thông qua việc khảo sát quá trình mã hóa - giải mã bằng lý thuyết hệ thống. Theo đó, quá trình mã hóa - giải mã là các ánh xạ tuyến tính. Các bộ mã hóa - giải mã được coi là các hệ thống tuyến tính bất biến rời rạc. Bài viết cũng sẽ trình bày giới hạn của nhiễu kênh truyền mà theo đó quá trình giải mã còn có thể thực hiện được.

2. BIỂU DIỄN MÃ TRONG KHÔNG GIAN TUYẾN TÍNH

Định nghĩa 1. Mã hóa nguồn tin M theo một bộ mã nào đó là một phép ánh xạ 1:1 biến đổi một tin $u_i \in M$ thành một tổ hợp các ký hiệu v_i của bộ mã.

Trong bài viết này, chúng tôi thống nhất ký hiệu F là một trường hữu hạn tổng quát. Khi cần chi tiết hơn, ta ký hiệu F_q là trường hữu hạn q phần tử. Điển hình của trường hữu hạn phần tử là trường Galois.

Định nghĩa 2. Cho $C \subseteq W_T$, C là một mã xoắn khi và chỉ khi C là một sub-module $F[z]$ của $F^n[z]$. Nếu $C \subseteq F^n[z]$ là một mã xoắn thì tồn tại một số dương k sao cho:

$$\varphi : F^k[z] \to F^m[z]$$
$$u(z) \to v(z)$$
$$Im(\varphi) = C$$

Định nghĩa trên tương đương với: Tồn tại một ma trận đa thức $G(z)$ kích thước nxk không suy biến thỏa mãn:

$$C = \{v(z)|\exists u(z) \in F^k[z],\ v(z) = G(z)u(z)\} \tag{1}$$

Khi đó, gọi $g_1(z), g_2(z), ..., g_k(z) \in F^n[z]$ là các cơ sở của C, tập các đa thức $g_i(z)$ tạo thành ma trận $G(z)$ và biểu diễn $v(z)$ theo $u(z)$ như (1) là duy nhất. C thỏa mãn các điều kiện trên gọi là mã xoắn k/n. $G(z)$ gọi là ma trận sinh của mã xoắn. $G(z)$ có kích thước kxn.

3. BIỂU DIỄN MÃ TRONG KHÔNG GIAN TRẠNG THÁI

Xét mã xoắn k/n có ma trận sinh:

$$G(z) = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1k} \\ g_{21} & g_{22} & \cdots & g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ g_{n1} & g_{n2} & \cdots & g_{nk} \end{pmatrix}$$

Ta có thể biểu diễn: $V = uG$ hay

$$v(t) = u(t)G \tag{2}$$

Gọi z là khâu trễ, thực hiện biến đổi Z của (1) ta có:

$$V(z) = U(z)G \tag{3}$$

Trong (1), u và v là các véc tơ thành phần của các không gian véc tơ F^n và F^k. $V(z)$ là véc tơ n chiều, $U(z)$ là véc tơ k chiều.

Ký hiệu t là thời điểm xuất hiện các ký hiệu đầu vào ($t \in Z_+$), trạng thái của bộ mã hóa gồm σ thành phần đầu vào được lưu giữ trong các ô nhớ:

$$(u_1(t-1), u_1(t-2), ..., u_1(t-k_1), u_2(t-1), u_2(t-2), ..., u_2(t-k_2), ..., u_k(t-1), u_k(t-2), ..., u_k(t-k_k)) \tag{4}$$

Có tối đa 2^k trạng thái khác nhau của bộ mã hóa.

Khi đó, theo quan điểm của lý thuyết hệ thống:

+ Một bộ mã hóa mã xoắn (n, k) là một thiết bị tuyến tính rời rạc có nhớ gồm k đầu vào và n đầu ra, thực hiệnn ánh xạ một từ mã k bit thành một từ mã n bit, trong đó n ký hiệu đầu ra tại thời điểm t phụ thuộc không chỉ vào k ký hiệu đầu vào tại thời điểm đó mà còn phụ thuộc vào M ký hiệu đầu vào trước thời điểm t và được đặc trưng bằng hệ phương trình sai phân trạng thái:

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) \\ v(t) &= Cx(t) + Du(t) \\ x(0) &= 0 \end{aligned} \tag{5}$$

+ Một bộ mã hóa mã khối là một hệ thống tuyến tính rời rạc không nhớ gồm k đầu vào và n đầu ra, được đặc trưng bằng hệ phương trình sai phân trạng thái:

$$x(t+1) = Ax(t) + Bu(t)$$

$$v(t) = Cx(t) \tag{6}$$

$$x(0) = 0$$

+ Một bộ mã hóa mã vòng là một trường hợp đặc biệt của bộ mã hóa mã khối, gồm k đầu vào và n đầu ra, đặc trưng bằng hệ phương trình sai phân trạng thái:

$$x(t+1) = Ax(t)$$

$$v(t) = Cx(t) \tag{7}$$

$$x(0) = 0$$

Trong (5), (6) và (7), A, B, C, D là các ma trận trên trường F.

A là ma trận trạng thái mxm; B là ma trận điều khiển kxm;

C là ma trận quan sát mxn; D là ma trận chuyển trạng thái kxn.

Khi $m = 0$, các ma trận A, B và C suy biến, (5) trở thành

$$v(t) = Du(t) \tag{8}$$

tức là mã xoắn trở thành mã khối theo biểu diễn (2).

Dạng biểu diễn (5), (6) và (7) được gọi là biểu diễn bằng phương trình trạng thái của mã. Ta có thể dễ dàng thấy được mối liên hệ giữa (A, B, C, D) trong biểu diễn (5) với G trong cách biểu diễn truyền thống, như sau:

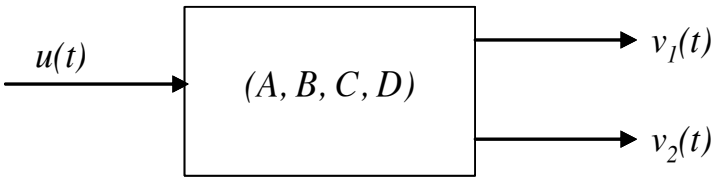
$$G = D + B(z^{-1}I_m - A)^{-1}C \tag{9}$$

(A, B, C, D) gọi là hiện thực hóa G trong không gian trạng thái.

4. TÍNH DUY NHẤT CỦA MÃ

Ví dụ 1. Cho bộ mã hóa mã xoắn $(1, 2, 2)$ trên trường Galois $GF(2)$ (Hình 2) và các ma trận không gian trạng thái như sau:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix};\ B = (1 \quad 0);\ C = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};\ D = (1 \quad 1)$$



Hình 2. Sơ đồ khối hệ thống mã hóa (1,2,2)

Theo (9), ta có $G(z) = (1 + z + z^2)$, tương ứng với sơ đồ mã hóa hình 3.

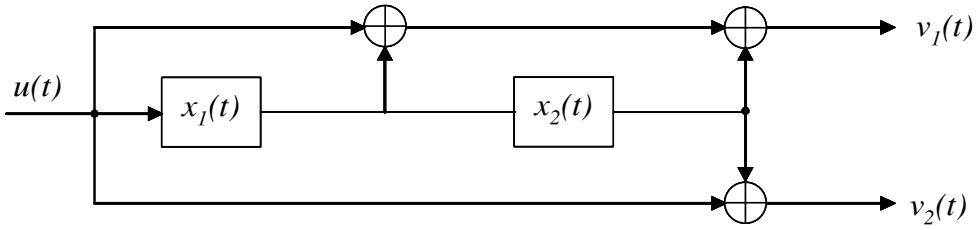
Sơ đồ hình 3 biến một bản tin 1 bit thành bản tin mã hóa 2 bit. Từ sơ đồ ta có thể viết được phương trình trạng thái:

$$x(t+1) = (x_1(t+1), x_2(t+1)) = (u(t), x_1(t)),$$

$$v(t) = (v_1(t), v_2(t)) = (u(t) + x_1(t) + x_2(t), u(t) + x_2(t)).$$

Gải hệ trên ta được bản tin mã hóa:

$$(v_1(t), v_2(t)) = (u(t) + u(t-1) + u(t-2), u(t) + u(t-2)).$$



Hình 3. Sơ đồ bộ mã hóa (1,2,2)

Như vậy, bản tin mã hóa ở đầu ra tại thời điểm t không chỉ phụ thuộc vào đầu vào tại thời điểm đó mà còn phụ thuộc đầu vào ở các thời điểm $t-1$ và $t-2$. Điều này cũng cho thấy bộ mã hóa có hai ô nhớ. Trong trường hợp này, số ô nhớ bằng bậc của bộ mã hóa. Thông thường, số ô nhớ và bậc của một bộ mã hóa là hai giá trị không bằng nhau. Với các bộ mã hóa có bậc hữu hạn, số ô nhớ cần thiết có thể tăng đến vô hạn.

Chúng ta biết rằng, bằng các phép toán hàng sơ cấp, chúng ta có thể biến đổi ma trận G thành một ma trận G' có cùng một không gian hàng, nghĩa là bằng cách hoán vị hay tổ hợp tuyến tính các hàng trong một ma trận sinh, chúng ta sẽ được một ma trận sinh khác của cùng một mã.

Câu hỏi đặt ra là: Tại sao cùng một mã lại có nhiều cách biểu diễn khác nhau? Các cách biểu ở trên được giải thích như thế nào trong không gian trạng thái? Tính duy nhất của mã có bị vi phạm không?

Xét một ma trận vuông T bất kỳ. Đặt $\widetilde{x} = Tx$ hay $x = T^{-1}\widetilde{x}$ và thay vào (5) ta có:

$$T^{-1}\widetilde{x} = AT^{-1}\widetilde{x} + Bu,$$

$$v = CT^{-1}\widetilde{x} + Du \tag{10}$$

Nhân bên trái hai vế biểu thức đầu của (10) với T, ta được:

$$\widetilde{x} = TAT^{-1}\widetilde{x} + TBu,$$

$$v = CT^{-1}\widetilde{x} + Du. \tag{11}$$

Đặt $\widetilde{A} = TAT^{-1}, B = TB, \widetilde{C} = CT^{-1}$ và $\widetilde{D} = D$, ta viết lại:

$$\widetilde{x} = \widetilde{A}\widetilde{x} + \widetilde{B}u,$$

$$v = \widetilde{C}\widetilde{x} + \widetilde{D}u. \tag{12}$$

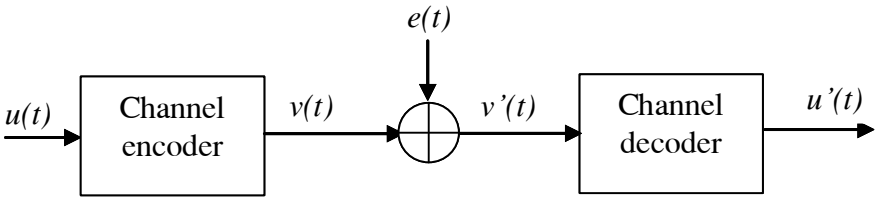
Vì T có thể chọn bất kỳ nên về lý thuyết, ta có thể có vô số trường hợp tương tự. Tuy nhiên, biểu diễn (12) hoàn toàn tương đương với biểu diễn (5) vì hai ma trận trạng thái A và $\widetilde{A}$ là hai ma trận đồng dạng, với mỗi cặp (A, B, C, D) và $(\widetilde{A}, \widetilde{B}, \widetilde{C}, \widetilde{D})$ thì T là duy nhất và với cùng tổ hợp các tín hiệu đầu vào u ta luôn nhận được cùng tổ hợp tín hiệu đầu ra v.

Bổ đề 1. *Các ma trận A, B, C, D biểu diễn mã $\mathcal{C}$ được định nghĩa ở trên là duy nhất theo nghĩa sau: Nếu $(\widetilde{A}, \widetilde{B}, \widetilde{C}, \widetilde{D})$ cũng là bộ các ma trận biểu diễn cùng mã $\mathcal{C}$ thì tồn tại một ma trận khả nghịch T duy nhất thỏa mãn:*

$$(\widetilde{A}, \widetilde{B}, \widetilde{C}, \widetilde{D}) = (TAT^{-1}, TB, CT^{-1}, D).$$

5. TÍNH BỀN VỮNG CỦA MÃ

Để có thể khảo sát quá trình mã hóa và giải mã, ta có thể mô phỏng một hệ thống thông tin như sau:



Hình 4. Sơ đồ hệ thống của quá trình Mã hóa-Giải mã

Trong đó $e(t)$ là nhiễu sinh ra trên đường truyền.

$v'(t)$ là từ mã nhận được tại đầu thu.

$u'(t)$ là thông tin sau giải mã.

Các tổ hợp mã truyền trên kênh truyền luôn phải chịu tác động của các nguồn nhiễu, dẫn đến kết quả là tổ hợp mã nhận được tại đầu vào bộ giải mã là tổng của tổ hợp mã được truyền với véc tơ lỗi:

$$v'(t) = v(t) + e(t).$$

(Để đơn giản, ta giả sử kênh truyền là tuyến tính và không quan tâm đến vấn đề điều chế).

Tác động của nhiễu có thể dẫn đến hai khả năng: Một là, khi lỗi sinh ra trong từ mã còn nằm trong một giới hạn nào đó thì việc giải mã coi như thực hiện được hoàn toàn. Hai là, khi lỗi gây ra trên từ mã vượt quá giới hạn cho phép, hệ thống có thể mất ổn định và do đó không thể điều khiển và quan sát được (và tất nhiên là không thể thực hiện giải mã được).

Như trên đã trình bày, bộ giải mã thực hiện quá trình ngược của quá trình mã hóa, hay nói cách khác, bộ giải mã thực hiện một ánh xạ tuyến tính 1:1 biến các từ mã trở thành các bản tin có nghĩa. Do đó, bộ giải mã hoàn toàn có thể được mô tả bằng hệ phương trình sai phân tuyến tính có dạng của (5). Không mất tính tổng quát, để đơn giản và quen thuộc về ký hiệu, trong trường hợp lý tưởng khi không có tác động của nhiễu đường truyền, ta mô tả bộ giải mã bằng hệ phương trình sau:

$$x(t+1) = Ax(t) + Bu(t),$$

$$y(t) = Cx(t) + Du(t). \tag{13}$$

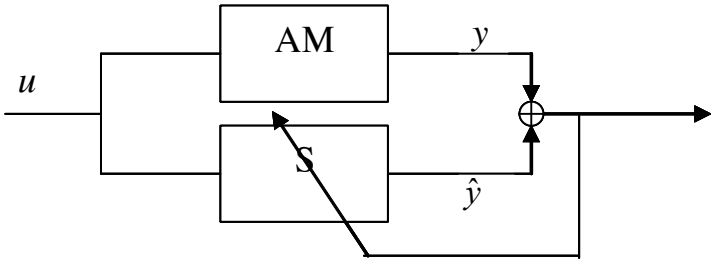
trong đó, (A, B, C, D) là các ma trận tham số đã biết của hệ; u là bản tin đầu vào cần được giải mã (chưa bị tác động của nhiễu); y là bản tin có nghĩa đầu ra.

Coi nhiễu kênh truyền là tác nhân gây nhiễu xạ hệ thống, chuyển hệ thống được khảo sát từ không gian ζ sang không gian ζ':

$$\zeta : \{A, B, C, D\} \to \zeta' : \{A + \Delta A, B + \Delta B, C + \Delta C, D + \Delta 3D\}.$$

Để xem xét giới hạn của tác động nhiễu xạ mà theo đó hệ vẫn đảm bảo tính ổn định, điều khiển được và quan sát được, ta dựa trên cơ sở của lý thuyết ước lượng trạng thái cho hệ thống tuyến tính bất biến được đề xuất và phát triển trong [3].

Theo [3], việc ước lượng trạng thái được thực hiện bằng cách sử dụng một mô hình giả định (AM - Assumed Model) với các tham số biết trước. Tham số và đặc tính của hệ cần khảo sát S được ước lượng theo AM dựa trên việc ước lượng tối ưu sai số bình phương trung bình tối thiểu (MMSE - Minimum Mean Square Error) của tín hiệu đầu ra.



Hình 4. Ước lượng tham số hệ bị nhiễu xạ S bằng mô hình giả định AM

Để đơn giản, ta chọn AM chính là hệ (13) với các ma trận tham số (A, B, C, D) đã biết. Khi đó,$x_a = x_m = x_s = x$(x_a là trạng thái của hệ giả định; x_m là trạng thái của hệ có bậc m được chọn làm hệ giả định; x_s là trạng thái của hệ khảo sát trước khi bị nhiễu xạ).

Dưới tác động nhiễu xạ, hệ được mô tả bởi hệ phương trình:

$$\begin{aligned} x + \Delta x &= (A + \Delta A)(x + \Delta x) + (B + \Delta B)u, \\ y + \Delta y &= (C + \Delta C)(x + \Delta x) + (D + \Delta D)u. \end{aligned} \tag{14}$$

Đặt: $\hat{x} = x + \Delta x$; $\hat{y} = y + \Delta y$; $\hat{A} = A + \Delta A$; $\hat{B} = B + \Delta B$; $\hat{C} = C + \Delta C$; $\hat{D} = D + \Delta D$, ta có:

$$\begin{aligned} \hat{x}(t+1) &= \hat{A}\hat{x}(t) + \hat{B}u(t), \\ \hat{y}(t) &= \hat{C}x(t) + \hat{D}u(t). \end{aligned} \tag{15}$$

Khi đó, tiêu chuẩn tối ưu hóa trạng thái theo [3] được cho bởi:

$$J_{Sopt} = SupE\{\|\hat{x} - \hat{T}^{+}x\|_R^2\},\ \hat{T} \in R^{m\times n},\ \rho(\hat{T}) = m \tag{16}$$

và tiêu chuẩn bình phương trọng số sai số đầu ra tương ứng là:

$$J_{Oopt} = SupE\{\|y - \hat{K}\hat{y}\|_{R_1}^2\},\ \hat{K} \in R^{q\times q},\ \rho(\hat{K}) = q, \tag{17}$$

trong đó, T là một phép biến đổi không đồng dạng; K là một phép biến đổi đồng dạng phù hợp với đầu ra của AM; R và R_1 là các ma trận xác định không âm, có kích thước tương ứng với các chuẩn (norm).

Các tiêu chuẩn trên quyết định giới hạn của các ma trận tham số $\hat{A}, \hat{B}, \hat{C}, \hat{D}$. Để hệ thống (15) điều khiển được và quan sát được. Có hai trường hợp xảy ra:

Thứ nhất, giả sử tác động nhiễu xạ hệ thống có thể đo lường được, nghĩa là có thể định lượng được Δx thì giới hạn của $\hat{A}, \hat{B}, \hat{C}, \hat{D}$ có thể tính toán được nhờ (17), thỏa mãn Định lý 3 trong [3] về ước lượng tham số.

Thứ hai, nếu tác động nhiễu xạ là không thể xác định được, thì giới hạn của $\hat{A}, \hat{B}, \hat{C}, \hat{D}$ để đảm bảo tính điều khiển được và quan sát được của hệ thống được cho như sau:

Vì hệ (13) có các tham số đã biết, đặt $\Delta x = \|x\| = \text{const}$ và gọi λ_1, λ_n tương ứng là giá trị riêng cực đại và cực tiểu khác không của TT^T. Giả sử $A = \text{diag}(-\alpha_1, ..., -\alpha_m)$, $BB^T = \text{diag}(\beta_1, ..., \beta_m)$ và $C^TC = \text{diag}(\gamma_1, ..., \gamma_m)$. Gọi $-\alpha, \beta, \gamma$ tương ứng là các giá trị riêng nhỏ nhất của A, BB^T và C^TC. Khi đó:

Hệ thống bị nhiễu xạ sẽ vẫn ổng định nếu ΔA không làm dịch chuyển các điểm cực sang bên phải mặt phẳng S. Giới hạn của ΔA được cho bởi:

$$\|\Delta A\| \leq 2\sqrt{\alpha_1\lambda_1}/A < \sqrt{\alpha}. \tag{18}$$

Đồng thời, tính điều khiển được và quan sát được của hệ thống vẫn đảm bảo nếu hạng của $\hat{B}$ và $\hat{C}$ không đổi, nghĩa là nếu số các giá trị riêng khác không của $\hat{B}\hat{B}^T$ và $\hat{C}^T\hat{C}$ tương ứng bằng số các giá trị riêng khác không của BB^T và C^TC. Giới hạn của ΔB và ΔC được cho bởi:

$$\|\Delta B\| \leq \sqrt{\beta_1}/B < \sqrt{\beta}, \tag{19}$$

$$\|\Delta C\| \leq \sqrt{\gamma_1\lambda_1\lambda_n}/(\sqrt{\lambda_n} + \Delta) < \sqrt{\gamma}, \tag{20}$$

6. KẾT LUẬN

Theo quan điểm của lý thuyết hệ thống, quá trình mã hóa - giải mã là các ánh xạ 1:1 trong không gian tuyến tính. Các bộ mã hóa - giải mã thực hiện các ánh xạ đó là các hệ thống tuyến tính bất biến rời rạc MIMO ổn định, điều khiển được và quan sát được. Biểu diễn hệ thống mã hóa theo (5) là duy nhất cho mỗi bộ mã. Dưới tác động của nhiễu kênh truyền đóng vai trò là tác nhân nhiễu xạ hệ thống, hệ sẽ đảm bảo được tính ổn định, điều khiển được và quan sát được nếu tác động nhiễu xạ vẫn nằm trong các giới hạn được chỉ ra trong [3].

Phương pháp biểu diễn quá trình mã hóa trong không gian trạng thái mở ra khả năng mô phỏng và khảo sát các thiết bị mã hóa bằng các phương pháp mô phỏng sử dụng máy vi tính.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Thúy Vân, *Lý thuyết mã,* NXB Khoa học kỹ thuật, 1999.

[2] Trần Trọng Huệ, *Đại số và hình học giải tích,* NXB Đại học Quốc gia Hà nội, 2001.

[3] N. N. San, On an Approach to the Estimation of the State-Variable Descriptive Parameters for Linear, Continuous-Time Models, *Optimization* **33** (1995) 235–250.

[4] H. H. Rosenborck, C. Strorey, *Mathematics of Dynamical System,* John Wiley and Sons Inc. Newyork, 1970.

[5] Sandro Zampieri, Sanjoy K. Mitter, Linear system over noethrian ring, *Journal of Mathematical Systems, Estimation and Control,* **6** (2) (1996) 1–26.

[6] Stefan Host, *On Woven Convolutional Codes,* Lund University, 1999.

[7] Robert J. McEliece, *The Algebraic Theory of Convolutional Codes,* California Institute of Technology, 1996.

Nhận bài ngày 12 - 9 - 2003