Tạp chí Tin học và Điều khiển học, T. 19, S. 2 (2003), 101–109

NGÔN NGỮ NHÓM CÔ LẬP

LÊ QUỐC HÁN, NGUYỄN THỊ BÍCH

Khoa Toán - Tin, Trường Đại học Vinh

Abstract. On isolate languages having a group as syntactic monoid. Languages mentioned in the title are considered. We describe syntactic monoids of such languages and when they are regular we provide different characterizations in terms of automata, grammars and so on.

Tóm tắt. Trong bài báo này, chúng tôi khảo sát các ngôn ngữ cô lập có vị nhóm cú pháp là một nhóm và mô tả ôtômát của lớp ngôn ngữ này. Trong trường hợp chúng là ngôn ngữ chính qui, chúng tôi đã mô tả được ôtômát, văn phạm sinh ra ngôn ngữ đó.

1. MỞ ĐẦU

Khái niệm ngôn ngữ nhóm được đưa ra bởi A.V. Aniximov ([1]) vào năm 1971. Đó là những ngôn ngữ nghịch ảnh của đơn vị qua đồng cấu của vị nhóm các từ hữu hạn vào một nhóm. Trong bài báo này, chúng tôi sẽ thay "đơn vị nhóm" bởi "nhóm con rời rạc của nhóm". Lớp ngôn ngữ này thực sự chứa lớp ngôn ngữ trong [1].

Giả sử S là một nửa nhóm. Quan hệ ρ trên S được gọi là *ổn định phải (trái)* nếu $\forall a, b, c \in S$, từ $a\rho b$ suy ra $ac\rho bc$ (hoặc $ca\rho cb$). Một quan hệ tương đương (phản xạ, đối xứng và bắc cầu), ổn định phải (trái) trên S được gọi là một *tương đẳng phải (trái)*. Quan hệ ρ trên S được gọi là một *tương đẳng* nếu ρ vừa tương đẳng phải, vừa tương đẳng trái.

Giả sử S là một nửa nhóm và H là tập con của S. Ta xét quan hệ $\wp_H \subseteq S \times S$ như sau:

$$\wp_H = \{(x, y) \in S \times S | uxv \in H \Longleftrightarrow uyv \in H, \quad \forall u, v \in S\}.$$

Khi đó $\wp_H$ được gọi là *tương đẳng chính* hay *tương đẳng cú pháp của* H và vị nhóm thương $S/\wp_H$ được gọi là *vị nhóm cú pháp của* H *trong* S. Tập con H được gọi là *rời rạc* trong S nếu tương đẳng $\wp_H$ là tương đẳng đồng nhất, nghĩa là $(x, y) \in \wp_H \Leftrightarrow x = y$.

Ta còn xét *tương đẳng một phía* trên S như sau:

$$\Re_H = \{(x, y) \in S \times S | xu \in H \Longleftrightarrow yu \in H, \ \forall u \in S\}.$$

Khi đó $\Re_H$ là tương đẳng phải trên S và được gọi là *tương đẳng chính phải Đuybrây sinh bởi* H *trong* S.

Giả sử X là một tập hợp tùy ý và X^* là vị nhóm tự do sinh bởi X với đơn vị là từ Λ, khi đó mỗi phần tử khác đơn vị của X^* biểu diễn được một cách duy nhất dưới dạng tích của hữu hạn các phần tử của X.

Theo tiêu chuẩn Suytstxenbejce ([2]), vị nhóm con Y của X^* là vị nhóm con tự do khi và chỉ khi $\forall x \in X^*$, từ các điều kiện $xY \cap Y \neq \varnothing$ và $Yx \cap Y \neq \varnothing$ suy ra $x \in Y$.

Giả sử X là một bảng chữ cái hữu hạn và X^* là vị nhóm con tự do sinh bởi X. Khi đó mỗi tập con bất kỳ L của X* được gọi là *một ngôn ngữ trên* X, còn vị nhóm cú pháp của L trong X^* sẽ được gọi là *vị nhóm cú pháp* của L và được ký hiệu là $\mu(L)$. Ngôn ngữ L được gọi là *ngôn ngữ nhóm* nếu $\mu(L)$ là một nhóm. Theo [4], L là một ngôn ngữ có vị nhóm cú pháp đẳng cấu với nhóm G khi và chỉ khi tồn tại một toàn cấu $\varphi : X^* \to G$ sao cho $L = \varphi^{-1}(H)$, trong đó H là tập con rời rạc của G. Trong bài báo này, ta xét ngôn ngữ L tương ứng với H là nhóm con rời rạc của G.

2. NGÔN NGỮ NHÓM CÔ LẬP

Ngôn ngữ L trên X được gọi là *cô lập bên trái* (hay bên phải) nếu $\forall u, x \in X^*$, từ $u \in L$ và $ux \in L$ (hay tương ứng $xu \in L$) kéo theo $x \in L$. Ngôn ngữ L được gọi là *cô lập* nếu nó cô lập cả bên trái và bên phải.

Tập con H của nửa nhóm S được gọi là *tập con mạnh theo nghĩa Đuybrây*, nếu $\forall a, b, x, y \in S$, từ $ax, ay, bx \in H$ kéo theo $by \in H$. Ngôn ngữ L trên X được gọi là *ngôn ngữ mạnh theo nghĩa Đuybrây*, nếu L là tập con mạnh của vị nhóm X^*.

Bổ đề 2.1. *Giả sử G là nhóm và H là tập con khác rỗng của G. Khi đó các khẳng định sau là tương đương:*

(i) *H là tập con mạnh theo nghĩa Đuybrây của G*

(ii) *Nếu $h_1, h_2, h_3 \in H$ thì $h_1h_2^{-1}h_3 \in H$.*

(iii) *H là lớp ghép phải (trái) theo một nhóm con của G.*

Chứng minh.

(i) $\Rightarrow$ (ii). Vì $h_1, h_2, h_3 \in H$ nên $h_2h_2^{-1}h_2 \in H$, $h_2h_2^{-1}h_3 \in H$, $h_1h_2^{-1}h_2 = h_1 \in H$; mà H là tập con mạnh của G nên $h_1h_2h_3^{-1} \in H$ (ở đây ta sử dụng định nghĩa trên với $a = h_2h_2^{-1}$, $b = h_1h_2^{-1}$, $x = h_2$ và $y = h_3$).

(ii) $\Rightarrow$ (i). Giả sử $ax, ay, bx \in H$. Khi đó $(bx)(ax)^{-1}ay \in H \Rightarrow by \in H \Rightarrow H$ là tập con mạnh của G.

(ii) $\Rightarrow$ (iii). Vì $H \neq \varnothing$ nên $\exists g \in H$. Giả sử $K = \{x \in G | gx \in H\}$. Do $e \in K$ nên $K \neq \varnothing$. Nếu $a, b \in K$ thì $ga, gb, g \in H$ nên $ga^{-1}b = g(ga)^{-1}.gb \in H \Rightarrow ab^{-1} \in K \Rightarrow K$ là nhóm con của G. Vì G là nhóm nên theo cách xác định K, ta suy ra $H = gK$.

(iii) $\Rightarrow$ (i). Giả sử $H = gK$, trong đó K là nhóm con của G và $h_1, h_2, h_3 \in H$. Khi đó $h_1 = gk_1$, $h_2 = gk_2$, $h_3 = gk_3$ với $k_1, k_2, k_3 \in K$. Từ đó

$$h_1h_2^{-1}h_3 = gk_1(gk_2)^{-1}.gk_3 = g.k_1.k_2^{-1}g^{-1}.gk_3 = gk_1k_2^{-1}k_3 \in gK = H.$$

■

Hệ quả 2.1. *Giả sử G là nhóm và H là tập con mạnh chứa đơn vị của G. Khi đó H là nhóm con của G.*

Chứng minh. Trong chứng minh Bổ đề 2.1, (ii) $\Rightarrow$ (iii), ta chỉ cần lấy $g = e$. Khi đó $H = eK = K$ trong đó K là nhóm con của G.

Định lý 2.1. *Giả sử L là ngôn ngữ nhóm trên X. Khi đó các khẳng định sau đây là tương đương:*

(i) *L là ngôn ngữ cô lập.*

(ii) *$L = \varphi^{-1}(H)$, trong đó H là nhóm con của G và $\varphi : X^* \to G$ là toàn cấu từ X^* lên $G \cong \mu(L)$.*

(iii) *L là vị nhóm con tự do của X^*.*

(iv) *L chứa từ rỗng Λ và là ngôn ngữ mạnh theo nghĩa Đuybrây.*

Chứng minh.

(i) $\Rightarrow$ (ii). Giả sử $L = \varphi^{-1}(H)$. Khi đó L là cô lập nên L chứa Λ. Suy ra $e = \varphi(\Lambda) \in \varphi(H)$. Giả sử $a, b \in H$. Khi đó tồn tại $u, v \in L$ sao cho $\varphi(u) = a$, $\varphi(v) = b$. Vì G là nhóm nên tồn tại $w \in X^*$

sao cho $\varphi(w) = a^{-1}$. Khi đó $\varphi(wu) = e \in H$ nên $uw \in L$, mà $u \in L$ nên $w \in L \Rightarrow a^{-1} = \varphi(w) \in H$.

Ta lại có $\varphi(wuv) = \varphi(w).\varphi(u).\varphi(v) = a^{-1}.a.b = b \in H$ nên $wuv \in L \Rightarrow uv \in L \Rightarrow ab = \varphi(u).\varphi(v) = \varphi(uv) \in \varphi(L) = H$. Vậy H là nhóm con của G.

(ii) $\Rightarrow$ (i). Giả sử $L = \varphi^{-1}(H)$, trong đó H là nhóm con của G. Thế thì từ $u \in L$, $uw \in L \Rightarrow \varphi(u) \in H$, $\varphi(uw) = \varphi(u).\varphi(w) \in H \Rightarrow \varphi(w) \in H$ vì H là nhóm con của $G \Rightarrow w \in L$. Vậy L cô lập bên trái. Tương tự, L cô lập bên phải nên từ đó suy ra L là cô lập trên X^*.

(ii) $\Rightarrow$ (iii). Từ giả thiết $L = \varphi^{-1}(H)$ và H là nhóm con của G ta suy ra L là vị nhóm con của X^*. Ta chứng minh L là vị nhóm con tự do của X^*. Thật vậy, giả sử $w \in X^*$ thoả mãn các điều kiện $wL \cap L \neq \emptyset$ và $Lw \cap L \neq \emptyset$. Khi đó tồn tại các từ $x, y \in L$ sao cho $wx = y$ và do đó $\varphi(y) = \varphi(wx) = \varphi(w).\varphi(x) \in H$, mà $x \in L$ nên $\varphi(x) \in H$, do đó $\varphi(w) \in H$, vì H là nhóm con của G, suy ra $w \in L$. Theo tiêu chuẩn Suytxenbécje ([2]), ta có L là vị nhóm tự do của X^*.

(iii) $\Rightarrow$ (ii). Vì L là vị nhóm tự do của X^* nên $\Lambda \in L \Rightarrow e = \varphi(\Lambda) \in H$. Sử dụng tiêu chuẩn vị nhóm tự do nêu trên, ta chứng minh được: $\forall a, b \in H$ thì $a^{-1} \in H$ và $ab \in H$ nên H là nhóm con của G.

(ii) $\Rightarrow$ (iv). Vì $L = \varphi^{-1}(H)$, trong đó H là nhóm con của G nên $e \in H \Rightarrow \Lambda \in L$ Giả sử $ux, uy, vx \in L$. Khi đó $\varphi(u).\varphi(x), \varphi(u).\varphi(y), \varphi(v).\varphi(x) \in H$ và H là nhóm con nên $\varphi(vy) = \varphi(v)\varphi(y) = [\varphi(v).\varphi(x)].[\varphi(v).\varphi(x)]^{-1}.[\varphi(u).\varphi(y)] \in H$. Suy ra $vy \in L$. Vậy L là ngôn ngữ mạnh theo nghĩa Đuybrây.

(iv) $\Rightarrow$ (ii). Vì L chứa từ rỗng Λ nên $e \in H$.

Giả sử $ac, ad, bc \in H$, trong đó $a, b, c, d \in G$. Khi đó tồn tại $u, v, x, y \in X^*$ sao cho $\varphi(u) = a$, $\varphi(v) = b$, $\varphi(x) = c$, $\varphi(y) = d$. Vì $L = \varphi^{-1}(H)$ nên từ $ac, bd, bc \in H$ suy ra $ux, uy, vx \in L$. Do đó $vy \in L$. Vì L là ngôn ngữ mạnh theo nghĩa Đuybrây $\Rightarrow bd \in H$. Vậy H là tập con mạnh theo nghĩa Đuybrây và chứa đơn vị của nhóm G nên theo Bổ đề 2.1 ta có H là nhóm con của G. Định lý 2.1 được chứng minh. ∎

3. ÔTÔMÁT CỦA NGÔN NGỮ NHÓM CÔ LẬP

Giả sử L là ngôn ngữ trên X và $\Re_L$ là tương đẳng chính phải Đuybrây sinh bởi L trong X^*. Ta định nghĩa ôtômát đoán nhận ngôn ngữ L, ký hiệu $\omega(L)$ là:

$$\omega(L) := \{X^*/\Re_L,\ X,\ \overline{\Lambda},\ \delta, \{\overline{w} | w \in L\}\},$$

mà tác dụng của X^* lên $X^*/\Re_L$ như sau: $\overline{u}.f = \overline{uf}$, trong đó $\overline{u}$ là lớp tương đẳng (theo môđun $\Re_L$) chứa từ u; $a_0 = \overline{\Lambda}$ là trạng thái ban đầu và $\{\overline{w} | w \in L\}$ được gọi là tập trạng thái cuối cùng. Ta sẽ ký hiệu $X^*/\Re_L$ là A và tập $\{\overline{w} | w \in L\}$ là A'; còn hàm chuyển trạng thái là δ, cụ thể ta viết $\delta(a, f) = b$ thay cho $\overline{u}.f = \overline{uf}$, trong đó $a = \overline{u}$ và $b = \overline{v}$.

Như vậy, ôtômát đoán nhận L sẽ là:

$$\omega(L) = \{A,\ X,\ a_0,\ \delta,\ A'\},$$

trong đó $L = \{w \in X^* | \delta(a_0, w) \in A'\}$. Rõ ràng mỗi từ $u \in X^*$ xác định một ánh xạ $\delta_u : A \to A$, còn từ rỗng sinh ra ánh xạ đồng nhất. Tập hợp các ánh xạ đó là một vị nhóm con của vị nhóm các phép biến đổi của tập A và được ký hiệu là $T(A)$.

Mệnh đề 3.1. ([6]) *Với mỗi ngôn ngữ L trên X, ta có $\mu(L) \cong T(A)$.*

Một ngôn ngữ L trên X được gọi là ngôn ngữ chính quy nếu nó là ngôn ngữ hữu hạn, hoặc thu được từ các tập con hữu hạn của X^* bằng cách áp dụng một số hữu hạn các phép toán hợp, tích và lặp.

Sử dụng định lý Klecne ([4]) chứng minh được mệnh đề sau:

Mệnh đề 3.2. ([4]) *Giả sử L là ngôn ngữ trên X. Khi đó, các khẳng định sau đây tương đương:*

(i) *L là ngôn ngữ chính quy.*

(ii) *Ôtômát $\omega(L)$ đoán nhận ngôn ngữ L là hữu hạn.*

(iii) *Vị nhóm cú pháp $\mu(L)$ là hữu hạn.*

Chú ý rằng sự tương đương giữa (i) và (ii) có thể suy ra trực tiếp từ định lý Mylhill - Norode ([12])

Giả sử L là ngôn ngữ trên X. Khi đó ôtômát $\omega(L)$ được gọi là *tách được* nếu $\forall a, b \in A$, từ $\delta(a,x) = \delta(b,x)$ kéo theo $a = b \forall x \in X$. Ôtômát $\omega(L)$ được gọi là *đầy đủ*, nếu $\forall x \in A$, $\forall a \in X$, tồn tại $b \in A$ sao cho $\delta(b,x) = a$.

Định lý 3.1. *Giả sử L là ngôn ngữ chính qui trên X. Khi đó các khẳng định sau đây là tương đương:*

(i) *L là ngôn ngữ nhóm cô lập.*

(ii) *Ôtômát $\omega(L) = (A,\ X,\ a_0,\ \delta,\ A')$ là tách được và $A' = \{a_0\}$.*

(iii) *Ôtômát $\omega(L) = (A,\ X,\ a_0,\ \delta,\ A')$ là đầy đủ và $A' = \{a_0\}$.*

Chứng minh. Ta sẽ chứng minh sự tương đương giữa (i) và (ii), còn sự tương đương giữa (i) và (iii) được lập luận tương tự.

(i) $\Rightarrow$ (ii). Vì $\mu(L)$ là một nhóm và $T(A) \cong \mu(L)$ nên $T(A)$ cũng là một nhóm, do đó mọi phần tử của $T(A)$ khả nghịch. Mặt khác, $T(A)$ là nhóm con của vị nhóm các phép biến đổi của tập A, nên mọi phần tử của $T(A)$ đều là đơn ánh. Nói riêng ra, $\forall x \in X$, ta có $\delta_x : A \to A$ là đơn ánh. Do đó từ $\delta_x(a) = \delta_x(b)$ suy ra $a = b$. Do đó $\omega(L)$ là tách được.

Ta lại có L là ngôn ngữ cô lập nên $\Lambda \in L \Rightarrow a_0 \in A'$. Hơn nữa, $\forall u \in L$ thì $ux \in L \Leftrightarrow x \in L$, $\forall x \in X^*$ vì L cô lập, do đó $\overline{u} = \overline{\Lambda}$ nên $A' = \{a_0\}$.

(ii) $\Rightarrow$ (i). Vì L là ngôn ngữ chính qui nên theo Mệnh đề 3.2 ta có: A hữu hạn $\Rightarrow T(A)$ hữu hạn. Ta chứng minh rằng $\forall \delta_u \in T(A)$, ta có δ_u là đơn ánh. Thật vậy, nếu $u = \Lambda$ thì khẳng định đó là hiển nhiên.

Giả sử $u \neq \Lambda$. Khi đó $u = x_1.x_2...x_n$ nên từ

$$\delta(a,u) = \delta(b,u) \Rightarrow \delta(a, x_1x_2...x_n) = \delta(b, x_1x_2...x_n) \Rightarrow \delta((a, x_1x_2...x_{n-1}), x_n) = \delta((b, x_1x_2...x_{n-1}), x_n)$$
$$\Rightarrow \delta(a, x_1x_2...x_{n-1}) = \delta(b, x_1x_2...x_{n-1}) \Rightarrow ... \Rightarrow \delta(a, x_1) = \delta(b, x_1) \Rightarrow a = b,$$

trong đó $x_1, x_2, ..., x_n \in X$. Vì A là hữu hạn nên đơn ánh $\delta u : A \to A$ cũng là toàn ánh và do đó δ_u là song ánh. Suy ra $T(A)$ là vị nhóm con của nhóm hữu hạn (gồm tất cả các phép thế của tập A), nên bản thân $T(A)$ cũng là một nhóm (hữu hạn), mà $\mu(L) \cong T(A)$ nên $\mu(L)$ là nhóm (hữu hạn) $\Rightarrow L$ là ngôn ngữ nhóm (chính qui).

$A' = \{a_0\}$ nên $u \in L \Leftrightarrow \overline{u} = a_0 \Leftrightarrow \overline{u} = \overline{\Lambda} \Leftrightarrow (ux \in L \Leftrightarrow x \in L,\ \forall x \in X^*)$. Vậy L là cô lập.

Chứng minh Định lý 3.1 kết thúc. ∎

Giả sử L là ngôn ngữ trên X. Khi đó ôtômát $\omega(L) = (A,\ X,\ a_0,\ \delta,\ A')$ được gọi là *liên thông mạnh* nếu $\forall a, b \in A$, tồn tại $u, v \in X^*$ sao cho $\delta(a,u) = b$ và $\delta(b,v) = a$. Ôtômát $\omega(L)$ được gọi là *ổn định* nếu từ $\delta(a_0,u) = \delta(a_0,v)$, ta suy ra $\delta(a,u) = \delta(a,v) \, \forall a \in A$.

Ta thu được kết quả sau:

Định lý 3.2. *Giả sử L là ngôn ngữ trên X. Khi đó ba khẳng định sau là tương đương:*

(i) *L là ngôn ngữ cô lập và phản xạ mạnh theo nghĩa L có bốn tính chất:*

1) $\forall u, v \in X^*,\ uv,\ u \in L \Rightarrow v \in L.$

2) $\forall u, v \in X^*,\ uv \in L \Rightarrow vu \in L.$

3) $\forall u, v \in X^*,\ u,\ v \in L \Rightarrow uv \in L.$

4) *Mỗi từ thuộc X^* là một đoạn ban đầu của một từ nào đó thuộc L.*

(ii) *$\mu(L)$ là một nhóm và $\mathcal{L} = \{[u] | u \in L\}$ là đơn vị của $\mu(L)$.*

(iii) *Ôtômát $\omega(L) = (A,\ X,\ a_0,\ \delta,\ A')$ đoán nhận ngôn ngữ L là liên thông mạnh, ổn định và $A' = \{a_0\}$.*

Chứng minh.

(i) $\Rightarrow$ (ii). $\forall u \in X^*$, $\exists v \in X^*$ sao cho $vu \in L$ (tính chất 4). Khi đó $\forall x, y \in X^*$ ta có $xvuy \in L \Rightarrow vuyx \in L$ (tính chất 2) $\Rightarrow yx \in L$ (tính chất 1) $\Rightarrow xy \in L \Rightarrow x.\Lambda.y \in L$.

Đảo lại, nếu $xy \in L \Rightarrow yx \in L \Rightarrow vuyx \in L \Rightarrow xvuy \in L$. Do đó $(vu, \Lambda) \in \wp_L \Rightarrow [vu] = [\Lambda] \Rightarrow [v][u] = [\Lambda] \Rightarrow [v]$ là nghịch đảo của $[u]$ trong vị nhóm $\mu(L) \Rightarrow \mu(L)$ là một nhóm.

Ta lại có $L \neq \varnothing$ theo tính chất 1, do đó nếu $u \in L$ thì từ $u.\Lambda, u \in L \Rightarrow \Lambda \in L \Rightarrow \mathcal{L}$ chứa đơn vị của $\mu(L)$. Giả sử $u \in L$, theo chứng minh trên, ta có $xuy \in L \Leftrightarrow xy \in L,\ \forall x, y \in X^*$ nên $[u] = [\Lambda] \Rightarrow \mathcal{L}$ là đơn vị của $\mu(L)$.

(ii) $\Rightarrow$ (i). Giả sử $\mu(L)$ là một nhóm và $\mathcal{L}$ là đơn vị của $\mu(L)$. Khi đó $uv \in L,\ u \in L \Rightarrow [u].[v] = [uv] = [\Lambda]$ và $[u] = [\Lambda] \Rightarrow [v] = [\Lambda]$ vì $[\Lambda]$ là đơn vị của $\mu(L) \Rightarrow v \in L$ và $\mathcal{L} = [\Lambda]$.

Ta lại có $uv \in L \Rightarrow [u].[v] = [uv] = [\Lambda] \Rightarrow [v].[u] = [\Lambda] \Rightarrow [vu] = [\Lambda] \Rightarrow vu \in L$.

$$u,\ v \in L \Rightarrow [u] = [\Lambda]$$

$$[v] = [\Lambda] \Rightarrow [uv] = [u].[v] = [\Lambda] \Rightarrow uv \in L.$$

Mặt khác, $\forall x \in X^*, \exists y \in X^*$ sao cho $[x].[y] = [\Lambda]$, vì $\mu(L)$ là nhóm $\Rightarrow xy \in L$.

(ii) $\Rightarrow$ (iii). Vì $\mathcal{L}$ là đơn vị của $\mu(L)$ nên $\forall u \in L$, ta có $[u] = [\Lambda] \Rightarrow (ux \in L \Leftrightarrow \Lambda x \in L,\ \forall x \in X^*) \Rightarrow \overline{u} = \overline{\Lambda} \Rightarrow A' = \{a_0\}$. $\forall a, b, \in A,\ a = \overline{u},\ b = \overline{v},\ \exists x, y$ sao cho $[u].[x] = [v]$ và $[v].[y] = [u] \Rightarrow$

$$\begin{cases} \overline{ux} = \overline{v} \\ \overline{vy} = \overline{u} \end{cases} \Rightarrow \begin{cases} \delta(a, x) = b \\ \delta(b, y) = a \end{cases}$$

$\Rightarrow \delta$ là liên thông mạnh.

Ta lại có: $\wp_L \subset \Re_L$, ta cần chứng minh $\Re_L \subset \wp_L$.

Giả sử $(u, v) \in \Re_L$ và $xuy \in L \Rightarrow [x][u].[y] = [\Lambda] \Rightarrow [u][y][x] = [\Lambda] \Rightarrow uyx \in L \Rightarrow vyx \in L$, vì $(u, v) \in \Re_L \Rightarrow [v][y][x] = [\Lambda] \Rightarrow [x][v][y] = [\Lambda] \Rightarrow xvy \in L$. Tương tự $xvy \in L \Rightarrow xuy \in L,\ \forall x,\ y \in X^* \Rightarrow [u] = [v] \Rightarrow (u, v) \in \wp_L$.

Do đó $\Re_L = \wp_L$.

Ta chứng minh tính ổn định của $\omega(L)$. Giả sử $\delta(a_0, u) = \delta(a_0, v) \Rightarrow \overline{u} = \overline{v} \Rightarrow [u] = [v]$, vì $\Re_L = \wp_L \Rightarrow (xuy \in L \Leftrightarrow xvy \in L,\ \forall x, y \in L)$. Đặt $\overline{x} = a$, ta có $\delta(a, u) = \delta(a, v),\ \forall a \in A$ nên $\omega(L)$ là ổn định.

(iii) $\Rightarrow$ (ii). Từ tính ổn định của $\omega(L)$ ta suy ra $\Re_L \subset \wp_L$ mà ta luôn luôn có $\wp_L \subset \Re_L$ nên $\Re_L = \wp_L$. Vì $A' = \{a_0\}$ nên $\mathcal{L}$ là phần tử đơn vị của $\mu(L)$. Ta chứng minh $\mu(L)$ là một nhóm.

Thật vậy, $\forall u \in X^*$, do tính liên thông mạnh của $\omega(L)$, $\exists v \in X^*$ sao cho $\delta(a, v) = a_0$, trong đó $a = \overline{u} \Rightarrow \overline{uv} = \overline{\Lambda}\ \Rightarrow [uv] = [\Lambda]$, vì $\Re_L = \wp_L \Rightarrow [u].[v] = [\Lambda] \Rightarrow [v]$ là nghịch đảo của $[u]$ trong $\mu(L) \Rightarrow \mu(L)$ là một nhóm.

Chứng minh định lý kết thúc.

■

4. VĂN PHẠM CỦA NGÔN NGỮ NHÓM CÔ LẬP

Văn phạm là một danh sách $G = (N, X, P, \sigma)$, trong đó:

(i) N là bảng chữ cái phụ, $N = \{p_1, p_2, ..., p_k\}$.

(ii) X là tập hợp hữu hạn các phần tử, gọi là *bảng chữ cái chính,* thoả mãn điều kiện $X \cap N = \varnothing$, khi đó $V = N \cup X$ được gọi là *bảng chữ cái hỗn hợp.*

(iii) P là tập hữu hạn các cặp từ (u, v), trong đó $u \in N^* - \{\Lambda\}$, $v \in V^*$. Nếu $(u, v) \in P$ thì ta dùng ký hiệu $u \to v$. Khi đó P được gọi là *tập các qui tắc thế.*

(iv) σ là ký hiệu bổ trợ, $\sigma \in N$, gọi là *ký hiệu ban đầu.*

Ta nói y sinh ra (trực tiếp) z, ký hiệu $y \Rightarrow z$ nếu $\exists u_1, u_2, u, v \in V^*$ sao cho $u \to v$ và $y = u_1 u u_2,\ z = u_1 v u_2$. Ta ký hiệu $y \Rightarrow^* z$ nếu $\exists z_1, z_2, ..., z_n$ sao cho

$$y = z_1 \Rightarrow z_2 \Rightarrow ... \Rightarrow z_n = z.$$

Ngôn ngữ L được gọi là ngôn ngữ sinh bởi văn phạm G, nếu:

$$L = \{w \in X^* | \sigma \Rightarrow^* w\}.$$

Khi đó ta ký hiệu $L = L(G)$.

Khái niệm văn phạm trên đưa ra bởi Chomsky lần đầu tiên vào năm 1959, và đã tỏ ra có nhiều ứng dụng trong máy tính, chẳng hạn máy Agôn ([4]). Chúng tôi đưa vào loại văn phạm sau đây để mô tả các ngôn ngữ nhóm chính quy.

Văn phạm G được gọi là *thuần tuý bên phải,* nếu G gồm các quy tắc sau:

(i) $p_i \to x q_i$ sao cho với mỗi $x \in X, p_i$ chạy khắp N và $\{q_i\}$ là một hoán vị của $\{p_i\}$.

(ii) $p \to \Lambda$ với ít nhất một $p \in N$.

Nếu điều kiện (ii) được thay bằng điều kiện (ii')

(ii)' $p \to \Lambda$ khi và chỉ khi $p = \sigma$ thì văn phạm G được gọi là *thuần túy bên phải chặt.*

Tương tự như chứng minh Định lý 3.1, ta có thể chứng minh được mệnh đề sau (xem [5]).

Mệnh đề 4.1. *Giả sử L là ngôn ngữ chính quy trên X. Khi đó các khẳng định sau đây là tương đương:*

(i) *$\mu(L)$ là một nhóm.*

(ii) *$\omega(L) = (A, X, a_0, \delta, A')$ tách được.*

(iii) *$\omega(L) = (A, X, a_0, \delta, A')$ đầy đủ.*

Từ Định lý 3.1, ta mô tả được văn phạm của ngôn ngữ nhóm chính quy.

Định lý 4.1. *Ngôn ngữ chính quy L là ngôn ngữ nhóm khi và chỉ khi L được sinh bởi văn phạm thuần túy bên phải.*

Chứng minh.

Điều kiện cần:

Giả sử $L \subset X^*$ là ngôn ngữ nhóm chính quy được đoán nhận bởi ôtômát $\omega(L) = (A, X, a_0, \delta, A')$ hữu hạn và tách được. Ta xây dựng văn phạm G như sau:

$$G = (N, X, P, \sigma),$$

trong đó $N = A,\ \sigma = a_0$, các quy tắc thuộc P là:

- $a_i \to x a_i'$ nếu $a_i, a_i', \in A,\ x \in X$ sao cho $\delta(a_i, x) = a_i'$.

• $a \to \Lambda$ nếu $a \in A'$.

Thế thì:

+ Rõ ràng a_i chạy khắp N, và do L là ngôn ngữ nhóm nên mọi $x \in X$, δ_x là song ánh từ A lên chính nó. Do đó $\{a'_i\} = \{a_i\}$.

+ Tồn tại $a \in A$ sao cho $\delta(a, \Lambda) \in A'$ (hiển nhiên). Do đó tồn tại ít nhất $a \in N$ sao cho $a \to \Lambda$.

Như vậy, G thuần túy bên phải. Ta hãy chứng minh $L(\omega) = L(G)$, tức là văn phạm xây dựng như trên sinh ra L.

Trước hết ta chứng minh $L(G) \subset L(\omega)$.

Giả sử $u \in L(G)$, khi đó $\sigma \Rightarrow^* u$. Hai trường hợp có thể sảy ra:

• Nếu $u = \Lambda$ và $\sigma \Rightarrow^* u$, thì do tồn tại $z_1, z_2, ..., z_k$ sao cho

$$\begin{cases} z_1 = \sigma = u_1 p_1 v_1, \quad \text{với} \;\; p_1 \to q_1 \\ z_2 = u_1 q_1 v_1, \quad (u_1, q_1, p_1, v_1 \in V^* = (N \cup X)^* \\ \dots\dots\dots\dots\dots \\ z_{k-1} = u_{k-1} p_{k-1} v_{k-1} \\ z_k = u_{k-1} q_{k-1} v_{k-1}, \quad \text{với} \quad p_{k-1} \to q_{k-1}. \end{cases}$$

(Ta ký hiệu p_i, q_i thay cho a_i, a'_i). Thế thì $z_k = u = \Lambda$, nên từ đẳng thức cuối cùng và định nghĩa vị nhóm tự do, ta phải có:

$$u_{k-1} = q_{k-1} = v_{k-1} = \Lambda.$$

Theo cách xây dựng các quy tắc của P, ta thấy $p_{k-1} \in A'$ và $z_{k-1} = p_{k-1}$, với $p_{k-1} \in A'$, $A' \cap X = \varnothing$ mà $z_{k-2} \Rightarrow z_{k-1}$ nên phải có $z_{k-1} = z_{k-2} = ... = \sigma$.

Từ đó $\sigma = \Lambda.p_{k-1}.\Lambda = a_0 \in A'$. Vì $p_{k-1} \in A'$, mà $\delta(a_0, \Lambda) = a_0 \in A'$ nên $\Lambda \in L(\omega)$, hay $u \in L(\omega)$.

• Nếu $u = x_1 x_2 ... x_n$, với $x_i \in X$ thì tồn tại $z_1, z_2, ..., z_k$ sao cho $\sigma = z_1 \Rightarrow z_2 \Rightarrow ... \Rightarrow z_k = u$, nên $\sigma = z_1 = u_1 p_1 v_1 = a_0$, $z_2 = u_1 q_1 v_1$, với $p_1, a_0 \in N$ mà V^* là vị nhóm tự do sinh bởi $N \cup X$, với $N \cap X = \varnothing$, nên từ đẳng thức đầu ta phải có:

$$u_1 = v_1 = \Lambda, \;\; p_1 = a_0.$$

Giả sử $q_1 = \Lambda$, thế thì $a_0 = p_1 \to \Lambda$, nên $a_0 \in A'$ và $z_2 = \Lambda$.

Theo cách xây dựng P, ta phải có $z_2 = z_3 = ... = z_k = u$, nên $u = \Lambda$. Và do $a_0 \in A'$, nên phải có $u = \Lambda \in L(\omega)$.

Nếu $q_1 \neq \Lambda$, thế thì $q_1 = y_1 a_1$, với $y_1 \in X$, $a_1 \in N$. Khi đó từ $z_2 = u_2 p_2 v_2 = y_1 a_1$, $z_3 = u_2 q_2 v_2$, với $p_2, a_1 \in N$; $v_1, v_2 \in V^*$, $y_1 \in X$ và $N \cap X = \varnothing$, nên từ đẳng thức đầu, suy ra $v_2 = \Lambda$, $p_2 = a_1$, $u_2 = y_1$ (theo định nghĩa của vị nhóm tự do trên $V = N \cup X$). Khi đó:

Hoặc $q_2 = \Lambda$, suy ra $z_3 = z_4 = ... = z_k = u$ (theo quy tắc xây dựng P) và từ đó $u = y_1$, $a_1 = p_2 \in A'$, mà $a_0 = p_1 \to y_1 a_1$ nên từ $\delta(a_0, y_1) = a_1 \in A'$, suy ra $y_1 \in L(\omega)$ hay $u \in L(\omega)$.

Hoặc $q_2 = y_2 a_2$, với $y_2 \in X$, $a_2 \in N$, thế thì từ $z_3 = u_3 p_3 v_3 = y_1 y_2 a_2$, $z_4 = u_3 q_3 v_3$ với $p_3 \to q_3$, y_1, $y_2 \in X$; $p_3, a_2 \in N$; $N \cap X = \varnothing$ và $u_3, v_3 \in V^* = (N \cup X)^*$.

Suy ra $v_3 = \Lambda$, $p_3 = a_2$ và $u_3 = y_1 y_2$. Do đó, hoặc $q_3 = \Lambda$ thì $u = z_4 = ... = z_k$, trong đó $z_4 = y_1 y_2 \Lambda.\Lambda = y_1 y_2$, $a_2 = p_1 = a_1 y_1$, nên $\delta(a_0, y_1) = a_1$; $a_1 \to y_2 a_2$ nên $\delta(a_1, y_2) = a_2 = p_3 \in A'$, vì $p_3 \to q_3 = \Lambda$.

Do đó $\delta(a_0, u) = \delta(a_0, y_1 y_2) = \delta(a_1, y_2) = a_2 \in A'$. Suy ra $u \in L(\omega)$.

Nếu $q_3 = y_3 a_3$, với $y_3 \in X$, $a_3 \in N$, thì lý luận tiếp, sau không quá k bước, ta đi đến:

1) Hoặc là $u \in L(\omega)$.

2) Hoặc là $z_k = y_1y_2...z_ka_k = x_1x_2...x_m$, với $x_i \in X,\ a_k \in N$ và theo định nghĩa của vị nhóm tự do trên $(N \cup X)^*$ ta suy ra $k+1 = m$ và $y_i = x_i\ (1 \le i \le k),\ a_k = x_m$ với $a_k \in N$ và $x_m \in X$, trong đó $N \cap X = \varnothing$. Mâu thuẫn.

Như vậy, từ $u \in L(G)$, ta suy ra $u \in L(\omega)$. Hay $L(G) \subset L(\omega)$.

Bây giờ ta chứng minh $L(\omega) \subset L(G)$.

Thật vậy, giả sử $u \in L(\omega)$, suy ra $\delta(a_0, u) = a' \in A'$ thì hoặc $u = \Lambda$, suy ra $\delta(a_0, \Lambda) = a_0 \in A'$, nên $a_0 \to \Lambda$; mà $\sigma = a_0 = \Lambda.a_0.\Lambda,\ u = \Lambda = \Lambda.\Lambda.\Lambda$, nên từ $a_0 \to \Lambda$, ta có $\sigma \Rightarrow^* u$, vậy $u \in L(G)$.

Hoặc $u = x_1x_2...x_k$, với $x_i \in X,\ (i = 1, 2, ..., k)$ và $\delta(a_0, x_1) = a_1,\ \delta(a_1, x_2) = a_2, ..., \delta(a_{k-1}, x_k) = a_k = a' \in A'$, (vì $u \in L(\omega)$) nên

$$a_0 \to x_1a_1,\ a_1 \to x_2a_2, ..., a_{k-1} \to x_ka_k, \quad \text{với } a_k \to \Lambda.$$

Thế thì, vì $\sigma = a_0 = \Lambda.a_0.\Lambda,\ x_1a_1 = \Lambda.x_1a_1.\Lambda$, nên $\sigma \Rightarrow x_1a_1$ vì $a_0 \to x_1a_1$.

Vì $x_1a_1 = x_1a_1.\Lambda,\ x_1x_2a_1 = x_1x_2a_2.\Lambda$, nên $x_1a_1 \Rightarrow x_1x_2a_2$ vì $a_1 \to x_2a_2$.

....

Vì $x_1...x_{k-1}a_{k-1} = x_1x_2...x_{k-1}a_{k-1}.\Lambda,\ ua_k = x_1...x_ka_k.\Lambda$, nên $x_1...x_{k-1}a_{k-1} \Rightarrow u_ka_{k-1}$ vì $a_{k-1} \to x_ka_k$.

Vì $ua_k = ua_k.\Lambda,\ u = u.\Lambda.\Lambda$, nên $ua_k \Rightarrow u$, vì $a_k \to \Lambda$.

Do đó $\sigma \Rightarrow^* u$, hay $u \in L(G)$. Vậy $L(\omega) \subset L(G)$.

Ta đã chứng minh $L(\omega) = L(G)$.

Điều kiện đủ:

Giả sử L sinh bởi văn phạm $G = (N, X, P, \sigma)$ thuần túy bên phải. Ta xây dựng ôtômát $\omega(B, X, P, b_0, B')$ như sau:

$$B = N,\ B' = \{p \in N | p \to \Lambda\}.$$

Theo 2) ta có $B' \neq \varnothing,\ b_0 = \sigma$ và $\rho(p_i, x) = q_i$ nếu $p_i \to xq_i$. Vì p_i chạy khắp N và $\{q_i\}$ là một hoán vị của $\{p_i\}$ nên ρ_x là một hàm chuyển trạng thái từ B lên chính nó.

Lập luận như chứng minh điều kiện cần, ta có $L(B) = L(G)$.

Giả sử $\omega(L) = (A, X, a_0, \delta, A')$ là ôtômát đoán nhận L (trong đó $A = X^*/\Re_L$). Xét tương ứng:

$$\varphi : B \to A,$$
$$b \mapsto \overline{u}$$

với $\overline{\rho}(b_0, u) = b_0$ và $\overline{\rho}(b_0, u) = \overline{\rho}(b_0, v)$ kéo theo

$$\overline{\rho}(b_0, uv) = \overline{\rho}((b_0, u), w) = \overline{\rho}((b_0, v), w) = \overline{\rho}(b_0, w)$$

nên $uw \in L \Leftrightarrow vw \in L,\ \forall w \in X^*$, tức là $\overline{u} = \overline{v}$.

Do đó φ là một ánh xạ, hơn nữa nó là một ánh xạ lên. Vì $\Re_L$ là tương đẳng phải nên $\overline{wu} = \overline{w}u$, suy ra $\varphi(b_0, wu) = \varphi(b_0, w).u$ hay $\varphi(bu) = \varphi(b).u$ với $\overline{\rho}(b_0, w) = b_0w = b$. Vậy φ là một toàn cấu ôtômát.

Giả sử $x \in X$, thế thì $\forall a \in A,\ a = \overline{u},\ \exists b \in B$ sao cho $\varphi(b) = a$ mà G thuần túy phải, nên $\exists b' \in B' :\ \overline{\rho}(b', x) = b$ (tức là $b' \to xb$) hay $b'x = b$. Suy ra $\varphi(b')x = \varphi(b)$.

Giả sử $\varphi(b') = a'$. Thế thì $\delta(a', x) = a$ hay $a'\delta_x = a$, suy ra δ_x là toàn ánh từ A lên A. Mặt khác, φ là toàn ánh từ B lên A nên $cardB \geq cardA$, mà B hữu hạn nên A hữu hạn.

Do đó $\omega(L) = (A, X, a_0, \delta, A')$ là ôtômát hữu hạn và đầy đủ.

Vậy L là ngôn ngữ nhóm chính quy. ∎

Từ Định lý 3.2 và Định lý 4.1, với chú ý: Ngôn ngữ nhóm chính quy L là ngôn ngữ cô lập khi và chỉ khi $A' = \{a_0\}$, trong đó $\omega(L) = (A, X, a_0, \delta, A')$ là ôtômát tối tiểu đoán nhận L, ta có:

Hệ quả 4.1. *Ngôn ngữ chính quy L là ngôn ngữ nhóm cô lập khi và chỉ khi L được sinh bởi văn phạm thuần túy bên phải chặt.*

5. KẾT LUẬN

Bài báo đã đề cập đến các điều kiện để một ngôn ngữ nhóm là ngôn ngữ cô lập và mô tả dáng điệu ôtômát của các ngôn ngữ nhóm cô lập chính qui hay phản xạ mạnh. Việc khảo sát ôtômát của các ngôn ngữ nhóm cô lập tổng quát là một bài toán mở và hứa hẹn nhiều kết quả thú vị. Trên cơ sở đó đã mô tả văn phạm của các ngôn ngữ nhóm chính quy cô lập.

TÀI LIỆU THAM KHẢO

[1] A.V.Aniximov, Về các ngôn ngữ nhóm (tiếng Nga), *Điều khiển học* (4) (1971) 18–24.

[2] A. H. Cliphớt và G. B. Preston, *Lý thuyết nửa nhóm,* 2 tập, NXB Đại học và Trung học chuyên nghiệp, Hà Nội, 1979.

[3] Phan Đình Diệu, *Lý thuyết Ôtômat và thuật toán,* NXB Đại học và Trung học chuyên nghiệp, Hà Nội, 1977.

[4] S. Eilenberg, *Automata, Languages and Machines,* Vol. B., Academic Press, New York, 1976.

[5] Lê Quốc Hán và Trần Văn Hạo, "Về ngôn ngữ nhóm", Tuyển tập *Hội thảo cơ sở tin học và bảo vệ tin,* Viện Toán học Việt Nam, Hà Nội, 1987, 46–49.

[6] Lê Quốc Hán, Ngôn ngữ nhóm Aben, *Tạp chí Tin học và Điều khiển học,* (3) (2001).

[7] D.S Jonhson and M.R. Garey, *Computer and Intractability,* W.H. Freeman and Company, 1989.

[8] B. Le Saec, Saturating right congruences, *Theoretical Informatics and Application,* **24** (6) (1990).

[9] B. Le Saec B., Dare V.R., Seromony R., "Strong recognition of rational ω-languages," International conference on Mathematical Foundation of Informatics, Ha Noi, 1999.

[10] J.B. Pecuchet, On the complementation of Buchi automata, *Theoretical Computer Science,* **47** (1986) 95–98.

[11] A. Prasad Sistla, Y- Moshe, Pierre Wolper, The complementation problem for Buchi automata with applications to temporal logic, *Theoretical Computer Science,* **49** (1987) 217–237.

[12] Đặng Huy Ruận, *Lý thuyết ngôn ngữ hình thức và ôtômát,* NXB Đại học Quốc gia Hà Nội, 2002.

Nhận bài ngày 1 - 5 -2002