A length formula in a semigroup of mappings

Dedicated to Professor S. Furuya on his 60th birthday

By Nobuko IWAHORI

Introduction

Let Ω be a finite set consisting of more than one element. We denote by $T(\Omega)$ the semigroup of all mappings $f: \Omega \rightarrow \Omega$ such that $f(\Omega) \subsetneqq \Omega$. As it is well-known (and also as we shall see in Theorem 1 below), the semigroup $T(\Omega)$ is generated by the elements γ_y^x, where γ_y^x maps x to y and all other elements z of Ω to z. The purpose of this note is to determine the smallest length $l(f)$ of the expressions of $f \in T(\Omega)$ as a product of the γ_y^x. Our main result is Theorem 2 given in § 2 which says that

$$l(f) = |\Omega| + |\mathfrak{C}_f| - |\mathfrak{F}_f|$$

where $|X|$ means the cardinality of a set X, $\mathfrak{F}_f = \{x \in \Omega \mid f(x) = x\}$ and $\mathfrak{C}_f$ is the family of all minimal f-invariant subset Y such that $f(Y) = Y$ (to be defined in § 1).

We would like to acknowledge that the original version of the present note was greatly simplified by suggestions of the referee. We express our gratitude to the referee for these simplifications.

§ 1. The semigroup $T(\Omega)$

Let Ω be a finite set consisting of more than one element. We denote by $T(\Omega)$ the semigroup consisting of all mappings $f: \Omega \rightarrow \Omega$ such that $f(\Omega) \subsetneqq \Omega$. Let $x \in \Omega$, $y \in \Omega$, $x \neq y$. Then we define a mapping $\gamma_y^x: \Omega \rightarrow \Omega$ as follows:

$$\gamma_y^x(z) = \begin{cases} y, & \text{if } z = x, \\ z, & \text{if } z \neq x. \end{cases}$$

Then $\gamma_y^x \in T(\Omega)$, since $|\gamma_y^x(\Omega)| = |\Omega| - 1$. It is well-known that the elements γ_y^x generate the semigroup $T(\Omega)$. (This will be also seen in the proof of Theorem 1 below.)

Now let us introduce several notations. Let $f \in T(\Omega)$. A non-empty subset X of Ω is called to be f-invariant if $f(X) = X$. An f-invariant subset X is called to be minimal if X contains no f-invariant subset other than X. We denote by

$\mathfrak{M}_f$ the family of all minimal f-invariant subsets of Ω.

Let $X \in \mathfrak{M}_f$. We associate subsets $A_i = A_i(X)$ of Ω to X as follows:

$$A_1 = \{y \in (\Omega - X) \mid f(y) \in X\}$$

$$A_i = \{y \in \Omega \mid f(y) \in A_{i-1}\}, \ i = 2, 3, \cdots.$$

Then $f(A_1) \subset X$, $f(A_2) \subset A_1, \cdots$. Let $\Omega(X)$ be the union $X \cup A_1 \cup A_2 \cup \cdots$. It is obvious that $f(\Omega(X)) \subset \Omega(X)$. We note that Ω is partitioned into subsets $\Omega(X)$, $X \in \mathfrak{M}_f$:

$$\Omega = \bigcup_{X \in \mathfrak{M}_f} \Omega(X).$$

In fact, it is easy to see that $\Omega(X) \cap \Omega(Y) = \emptyset$ for $X \in \mathfrak{M}_f$, $Y \in \mathfrak{M}_f$, $X \neq Y$. Now let $x \in \Omega$. Then the sequence x, $f(x)$, $f^2(x), \cdots$ must contain two terms of the form $f^k(x)$, $f^l(x)$ such that $k < l$, $f^k(x) = f^l(x)$. Then $Y = \{f^k(x), f^{k+1}(x), \cdots, f^{l-1}(x)\}$ satisfies $f(Y) = Y$. Thus Y should contain a minimal f-invariant subset X. Then we get $x \in \Omega(X)$. Hence Ω is a union of the subsets $\Omega(X)$, $X \in \mathfrak{M}_f$.

We now define a subfamily $\mathfrak{C}_f$ of $\mathfrak{M}_f$. A minimal f-invariant subset X is called to be pure if $|X| > 2$ and $\Omega(X) = X$ (i.e. $|X| > 2$, $A_i(X) = \emptyset$, $i = 1, 2, \cdots$). We denote by $\mathfrak{C}_f$ the family consisting of all pure minimal f-invariant subsets.

Finally we denote by $\mathfrak{F}_f$ the subset of Ω consisting of all f-fixed points:

$$\mathfrak{F}_f = \{x \in \Omega \mid f(x) = x\}.$$

We are ready to give the following:

THEOREM 1. *Let $f \in T(\Omega)$. Then f can be expressed as a product of the elements γ_y^x of length $|\Omega| - |\mathfrak{F}_f| + |\mathfrak{C}_f|$.*

PROOF. We divide the proof into several cases. We put $\mu(f) = |\Omega| - |\mathfrak{F}_f| + |\mathfrak{C}_f|$ for the sake of convenience.

Case 1. The case $\mathfrak{C}_f \neq \emptyset$.

Note that $\mathfrak{M}_f \neq \mathfrak{C}_f$. (Otherwise f becomes bijective on Ω.) Take $X \in \mathfrak{M}_f - \mathfrak{C}_f$, $Y \in \mathfrak{C}_f$. Then $\Omega(X) - f(\Omega) \neq \emptyset$. Choose $x \in \Omega(X) - f(\Omega)$ and $y \in Y$ arbitrarily. Put $f(y) = z$. Then $z \in Y$, $z \neq y$ since $Y \in \mathfrak{C}_f$. Now construct an element $g \in T(\Omega)$ as follows:

$$g(u) = \begin{cases} f(u), & \text{if } u \neq y, \\ x, & \text{if } u = y. \end{cases}$$

Then $g(\Omega) \not\ni z$. Hence $g \in T(\Omega)$. Furthermore

$$f = \gamma_z^x \cdot g.$$

In fact, if $u \neq y$, $\gamma_z^x \cdot g(u) = \gamma_z^x \cdot f(u) = f(u)$, since $x \notin f(\Omega)$. Also $\gamma_z^x g(y) = \gamma_z^x(x) = z$

$=f(y)$.

It is easily verified that $\mathfrak{F}_f=\mathfrak{F}_g$ and that $\mathfrak{C}_g=\mathfrak{C}_f-\{Y\}$. Thus $|\mathfrak{C}_g|=|\mathfrak{C}_f|-1$ and we have $f=\gamma_z^x\cdot g$ and $\mu(g)=\mu(f)-1$. Therefore the proof will be complete if we can show Theorem 1 for the element $g\in T(\Omega)$. Repeating in this manner, the proof of Theorem 1 is reduced to the case $\mathfrak{C}_f=\varnothing$.

Case 2. The case $\mathfrak{C}_f=\varnothing$.

Let $f\in T(\Omega)$, $C_f=\varnothing$. Then for every $X\in\mathfrak{M}_f$, we have either $A_1(X)\neq\varnothing$ or $|X|=|\Omega(X)|=1$. Let W be the union of $X\in\mathfrak{M}_f$ such that $|X|=|\Omega(X)|=1$. Assume that Theorem 1 is true for the restriction $f|_{\Omega_0}$, where $\Omega_0=\Omega-W$. Then $f|_{\Omega_0}$ can be expressed as a product of the γ_y^x of length $|\Omega_0|-|\mathfrak{F}_0|$ where $\mathfrak{F}_0=\{z\in\Omega_0|f(z)=z\}$. Theorem 1 is then true for f since the expression $f|_{\Omega_0}$ above also can be used as an expression of f and $|\Omega_0|-|\mathfrak{F}_0|=|\Omega|-|W|-|\mathfrak{F}_0|=|\Omega|-|\mathfrak{F}_f|$. Now $g=f|_{\Omega_0}$ satisfies $\mathfrak{C}_g=\varnothing$ and $A_1(Y)\neq\varnothing$ for every $Y\in\mathfrak{M}_g$.

Thus in order to prove Theorem 1, for $f\in T(\Omega)$ we may and shall assume that $\mathfrak{C}_f=\varnothing$ and that $A_1(X)\neq\varnothing$ for every $X\in\mathfrak{M}_f$. Hence $f(\Omega(X))\subsetneqq\Omega(X)$. So the restriction $f|_{\Omega(X)}$ belongs to $T(\Omega(X))$ for every $X\in\mathfrak{M}_f$. Now assume that Theorem 1 is true for each $f|_{\Omega(X)}$. Then $f|_{\Omega(X)}$ can be expressed as a product of the γ_y^x of length $|\Omega(X)|$ or $|\Omega(X)|-1$ respectively, according to $|X|>1$ or $|X|=1$. Putting these expressions together, one obtains an expression of f as a product of the γ_y^x of length $|\Omega|-|\mathfrak{F}_f|$.

Thus the proof of Theorem 1 is reduced to the following.

Case 3. The case $\Omega=\Omega(X)$ for some $X\in\mathfrak{M}_f$.

Let us prove this case by induction on $|\Omega|=|\Omega(X)|$. We first consider the case where $|\Omega(X)|>|X|+1$. Take an element $x\in\Omega(X)-f(\Omega(X))$ and put $f(x)=y$. Define g as follows:

$$g(u)=\begin{cases} f(u), & \text{if } u\neq x, \\ x, & \text{if } u=x. \end{cases}$$

Then $\Omega_0=\Omega-\{x\}$ is stable under g. Furthermore using $|\Omega(X)|>|X|+1$, it is easy to verify that $g|_{\Omega_0}\in T(\Omega_0)$, $f=\gamma_y^x g$. Also one can check that $h=g|_{\Omega_0}$ satisfies $|\mathfrak{F}_h|=|\mathfrak{F}_f|$, $\mathfrak{C}_h=\varnothing$. Since $|\Omega_0|=|\Omega|-1$, Theorem 1 is true for h by our induction-assumption. Then, Theorem 1 is also true for $f=\gamma_y^x\cdot g$.

Thus we have to consider the case where $|\Omega(X)|=|X|+1$. Then we may assume that

$$X=\{1,2,\cdots,n-1\}$$

and that

$$f(i)=i+1, \qquad (i=1,2,\cdots,n-2)$$
$$f(n-1)=1, \qquad f(n)=n-1.$$

If $|X|=1$, then $n=2$ and $f=\gamma_1^2$. So Theorem 1 is true in this case. Now suppose $|X|>1$. Then we have

$$f=\gamma_{n-1}^{n}\gamma_1^{n-1}\gamma_2^1\cdots\gamma_{n-2}^{n-3}\gamma_n^{n-2}.$$

So Theorem 1 is true also in this case. This completes the proof of Theorem 1.

§2. The length formula

Let $f\in T(\Omega)$. We denote by $l(f)$ the smallest length of the expressions of f as a product of the γ_y^x. Then by Theorem 1 we have

$$l(f)<|\Omega|-|\mathfrak{F}_f|+|\mathfrak{C}_f|.$$

We shall prove now the reverse inequality to get Theorem 2 below.

Let $\sigma=(\gamma_{j_k}^{i_k}, \gamma_{j_{k-1}}^{i_{k-1}}, \cdots, \gamma_{j_1}^{i_1})$ be a sequence of length k consisting of the γ_y^x. We call such a sequence a γ-sequence of length k, and write $k=l(\sigma)$. We denote by Γ_σ the set of integers $1, 2, \cdots, l(\sigma)$.

Now for a γ-sequence $\sigma=(\gamma_{j_k}^{i_k}, \cdots, \gamma_{j_1}^{i_1})$ and a point $x\in\Omega$, we associate a sequence $x_0, x_1, \cdots, x_k$ ($k=l(\sigma)$) of length $k+1$ of points $x_i\in\Omega$ as follows:

$$x_0=x, \qquad x_p=\gamma_{j_p}^{i_p}(x_{p-1}), \qquad p=1, 2, \cdots, k.$$

We denote by $(x;\sigma)$ the sequence $x_0, x_1, \cdots, x_k$. Furthermore we define a subset $\Gamma_\sigma(x)$ of Γ_σ as follows:

$$\Gamma_\sigma(x)=\{\nu\in\Gamma_\sigma \mid x_\nu\neq x_{\nu-1}\}.$$

Thus, by definition of the x_ν, ν belongs to $\Gamma_\sigma(x)$ if and only if $\gamma_{j_\nu}^{i_\nu}(x_{\nu-1})\neq x_{\nu-1}$, i.e. if and only if $i_\nu=x_{\nu-1}$, $j_\nu=x_\nu$.

LEMMA 1. *Let $x\in\Omega$, $y\in\Omega$, $x\neq y$, $f\in T(\Omega)$. If there exists a minimal f-invariant subset X such that $x\in X$, $\Omega(X)=X$, then for every γ-sequence $\sigma=(\gamma_{j_k}^{i_k}, \cdots, \gamma_{j_1}^{i_1})$ satisfying $f=\gamma_{j_k}^{i_k}\cdots\gamma_{j_1}^{i_1}$ we have*

$$\Gamma_\sigma(x)\cap\Gamma_\sigma(y)=\emptyset.$$

PROOF. Suppose $\Gamma_\sigma(x)\cap\Gamma_\sigma(y)$ contains an element ν. Put

$$(x;\sigma)=(x_0, x_1, \cdots, x_k)$$
$$(y;\sigma)=(y_0, y_1, \cdots, y_k).$$

Then since $x_{\nu-1}\neq x_\nu$ and $y_{\nu-1}\neq y_\nu$, we have $x_{\nu-1}=i_\nu=y_{\nu-1}$. Then

$$f(x)=\gamma_{j_k}^{i_k}\cdots\gamma_{j_1}^{i_1}(x)=\gamma_{j_k}^{i_k}\cdots\gamma_{j_\nu}^{i_\nu}(x_{\nu-1})$$
$$=\gamma_{j_k}^{i_k}\cdots\gamma_{j_\nu}^{i_\nu}(y_{\nu-1})=\gamma_{j_k}^{i_k}\cdots\gamma_{j_1}^{i_1}(y)=f(y).$$

Hence $f(y) \in X$. However, $\Omega(X)=X$ implies $y \in X$. Then, since f induces a bijection on X, $f(x)=f(y)$ implies $x=y$, which is impossible, q. e. d.

LEMMA 2. *Let $x \in \Omega$, $f \in T(\Omega)$ and let $\sigma=(\gamma_{j_k}^{i_k}, \cdots, \gamma_{j_1}^{i_1})$ be a γ-sequence satisfying $f=\gamma_{j_k}^{i_k} \cdots \gamma_{j_1}^{i_1}$. Then,*

(i) *if $f(x) \neq x$, then $\Gamma_\sigma(x) \neq \emptyset$*

(ii) *for every $X \in \mathfrak{M}_f$, with $\Omega(X)=X$, $|X|>2$ there exists a point $y \in X$ such that $|\Gamma_\sigma(y)|>2$.*

PROOF. (i) If $\Gamma_\sigma(x)=\emptyset$, then $(x;\sigma)=(x_0, x_1, \cdots, x_k)$ satisfies $x_0=x_1=\cdots=x_k$. Hence $x=f(x)$ which is impossible.

(ii) If $y \in X$, $|\Gamma_\sigma(y)| \neq 0$ by (i). Suppose $|\Gamma_\sigma(y)|=1$ for every $y \in X$. Put $X=\{z_1, \cdots, z_p\}$, $f(z_i)=z_{i+1}$ $(i=1, \cdots, p)$, $z_{p+1}=z_1$. Let $\Gamma_\sigma(z_i)=\{\nu_i\}$, $i=1, \cdots, p$. Then the sequence $(z_i;\sigma)=(z_{i,0}, z_{i,1}, \cdots, z_{i,k})$ satisfies $z_i=z_{i,0}=\cdots=z_{i,\nu_{i-1}} \neq z_{i,\nu_i}=\cdots=z_{i,k}=f(z_i)$. Hence $i_{\nu_i}=z_i$, $j_{\nu_i}=f(z_i)=z_{i+1}$. $z_i \notin \{i_1, \cdots, i_k\}-\{i_{\nu_i}\}$. We see that $\nu_1>\nu_2$. In fact, suppose $\nu_1<\nu_2$, then (z_1, σ) should have the form $(z_1, \cdots, z_1, z_2, \cdots, z_2, z_3, \cdots, z_3)$ which contradicts $|\Gamma_\sigma(z_1)|=1$. Similarly one has $\nu_1>\nu_2>\cdots>\nu_p$. Hence $\nu_1>\nu_p$. If $\nu_1=\nu_p$, $f(z_1)=f(z_p)$ $(=j_{\nu_1}=j_{\nu_p})$ which implies $z_1=z_p$, $p=1$ a contradiction. Hence $\nu_1>\nu_p$. Then $(z_p;\sigma)$ should have the form $(z_p, \cdots, z_p, z_1, \cdots, z_1, z_2, \cdots, z_2)$ which contradicts $|\Gamma_\sigma(z_p)|=1$, q. e. d.

LEMMA 3. *Let $f \in T(\Omega)$, $f=\gamma_{j_k}^{i_k} \cdots \gamma_{j_1}^{i_1}$. Then $k>|\Omega|+|\mathfrak{C}_f|-|\mathfrak{F}_f|$.*

PROOF. Let $\sigma=(\gamma_{j_k}^{i_k}, \cdots, \gamma_{j_1}^{i_1})$. Let us consider the set $\Gamma=\bigcup_{x \in \Omega} \Gamma_\sigma(x)$ of $\Gamma_\sigma=\{1, 2, \cdots, k\}$. Let $\mathfrak{C}_f=\{X_1, \cdots, X_d\}$. Then by Lemma 1, Γ is a disjoint union of

$$\Gamma_1=\bigcup_{i=1}^{d} \bigcup_{x \in X_i} \Gamma_\sigma(x) \quad \text{and} \quad \Gamma_2=\bigcup_{z \in \mathfrak{F}_f} \Gamma_\sigma(z) \cup \bigcup_{y \in \Omega'} \Gamma_\sigma(y)$$

where $\Omega'=\Omega-\bigcup_{i=1}^{d} X_i-\mathfrak{F}_f$. Hence $k=|\Gamma_\sigma|>|\Gamma|=|\Gamma_1|+|\Gamma_2|$. Furthermore, $|\Gamma_1|=\sum_{i=1}^{d} |\bigcup_{x \in X_i} \Gamma_\sigma(x)|$ by Lemma 1. Also by Lemma 2.

$$|\bigcup_{x \in X_i} \Gamma_\sigma(x)|>1+|X_i|.$$

Hence $|\Gamma_1|>\sum_{i=1}^{d} |X_i|+d$.

On the other hand,

$$|\Gamma_2|>|\bigcup_{y \in \Omega'} \Gamma_\sigma(y)|.$$

Now there is an injective map $\phi: \Omega' \to \bigcup_{y \in \Omega'} \Gamma_\sigma(y)$. In fact, for $y \in \Omega'$, one has $f(y) \neq y$. Hence $\Gamma_\sigma(y) \neq \emptyset$. Let e be the smallest element in $\Gamma_\sigma(y)$. Then, $i_e=y$. Define $\phi: \Omega' \to \bigcup_{y \in \Omega'} \Gamma_\sigma(y)$ by

$$\psi(y)=e=\min. \quad \text{in} \quad \Gamma_\sigma(y).$$

Then, $i_e=y$ shows that ψ is injective. Thus $|\bigcup_{y\in\Omega'}\Gamma_\sigma(y)|>|\Omega'|$. Hence

$$|\Gamma_2|>|\Omega'|=|\Omega|-|\mathfrak{F}_f|-\sum_{i=1}^{d}|X_i|.$$

Therefore we get $k>|\Gamma_1|+|\Gamma_2|>|\Omega|+d-|\mathfrak{F}_f|$, q. e. d.

We have thus proved the following:

THEOREM 2. *Let $f\in T(\Omega)$. Then $l(f)$ is given by $l(f)=|\Omega|+|\mathfrak{C}_f|-|\mathfrak{F}_f|$ where $\mathfrak{C}_f=\{X\in\mathfrak{M}_f\,|\,|X|>2,\ \Omega(X)=X\}$, $\mathfrak{F}_f=\{x\in\Omega\,|\,f(x)=x\}$.*

(Received October 18, 1976)

Department of Mathematics
College of Science and Engineering
Aoyama Gakuin University
Chitosedai, Setagaya-ku, Tokyo
157 Japan