数理解析研究所講究録 1222 巻 2001 年 50-52

Irreducibility in equal length for finite semigroups

Pál DÖMÖSI
Institute of Mathematics and Informatics, Debrecen University
Debrecen, Egyetem tér 1, H-4032, Hungary
e-mail: domosi @ math.klte.hu

and

Masami ITO（伊藤 正美）
Faculty of Science, Kyoto Sangyo University
Kyoto 603, Japan
e-mail: ito@ksuvx0.kyoto-su.ac.jp

By the well-known Krohn-Rhodes theorem (see, for example, [4]) the finite irreducible semigroups are exactly the finite simple groups and the subsemigroups of the monoid with two right-zero elements. It is trivial that all finite cyclic simple groups are irreducible in equal length. Moreover, it is easy to see that all subsemigroups of the monoid with two right-zero elements also have this property. Using the Dénes-Hermann theorem [3], we can also show that all finite non-commutative simple groups are irreducible in equal length. Therefore, the finite irreducible semigroups are irreducible in equal length too. Z. Ésik (see [1] and [2]) gave a direct proof of this statement such that he did not use the Dénes-Hermann theorem. Using an idea of P. Pálfy [5], we give another direct, elementary proof. (We note that the only known proof of the Dénes-Hermann theorem uses the Feit-Thompson theorem.)

It is said that a semigroup S *divides* a semigroup T, written $S \preceq T$, iff T has a subsemigroup having a homomorphism onto S. If H is a subset of the semigroup T and the subsemigroup T' generated by H has a homomorphism onto S then we also say that S *divides* T with respect to H and we write $S \preceq_H T$.

Let H be a nonvoid subset of elements of the semigroup T and consider a subsemigroup T' of T generated by H. Consider a homomorphism $\psi : T' \to S$ of T' onto a given semigroup S. Put $S \mid^{n,H} T$ iff $\psi^{-1}(s) \cap H^n \neq \emptyset$ for all $s \in S$. In addition, we put $S \mid^{H} T$ iff $S \mid^{n,H} T$ holds for some n.

Given two transformation semigroups (X, S) and (Y, T), we define the *wreath product* $(Y, T) \int (X, S)$ to be the transformation semigroup with set $Y \times X$ and action semigroup $T^X \times S$ with action $(y, x).(f, s) = (y.f(x), x.s)$.

Given a semigroup S, we define S^λ to be S if S contains an identity element $1 \in S$ with $s1 = 1s = s$ for all $s \in S$, otherwise we take S^λ to be S with new identity element 1 adjoined. Thus S^λ is the minimal monoid containing S as a subsemigroup.

For a semigroup S, we consider the transformation semigroup (S^λ, S) with $s.s' = ss'$ for all $s, s' \in S$ and $1.s = s, s \in S$. If S and T are semigroups then we shall write $T \int S$ for the wreath product of $(T^\lambda, T) \int (S^\lambda, S)$. For every subset H of $T^{S^\lambda} \times S$, we put $H_1 = \{t \mid t \in T : \exists s' \in S^\lambda, (f, s) \in H : t = f(s')\}$ and $H_2 = \{s\ s \in S : \exists (f, s) \in H\}$.

If for arbitrary semigroups S, T, and a subset H of $T^{S^\lambda} \times S$, $S' \preceq_H T^{S^\lambda} \times S$ necessarily implies that either $S' \preceq_{H_1} T$ or $S' \preceq_{H_2} S$ then it is said that S' is *irreducible*.

A direct consequence of the Krohn-Rhodes Theorem [4] is the next statement.

Theorem 1. *The finite irreducible semigroups are exactly the finite simple groups and the subsemigroups of the monoid with two right-zero elements.*

Let H be a subset of $T^{S^\lambda} \times S$ again and consider $H_1 = \{t \mid t \in T : \exists s' \in S^\lambda, (f, s) \in H : t = f(s')\}$ and $H_2 = \{s \mid s \in S : \exists (f, s) \in H\}$ as before.

If for arbitrary semigroups S, T, a subset H of $T^{S^\lambda} \times S$, and a positive integer n, $S' \mid^{n,H} T^{S^\lambda} \times S$ necessarily implies that either $S' \mid^{H_1} T$ or $S' \mid^{H_2} S$ then it is said that S' is *irreducible in equal length*. By this definition, a semigroup is irreducible if it is irreducible in equal length.

The following statement is obvious.

Proposition 2. *The finite simple cyclic groups are irreducible in equal length.*

Next we prove

Proposition 3. *The subsemigroups of the finite monoid with two right-zero elements are irreducible in equal length.*

Proof: Let $S = \{e, z_1, z_2\}$ be the monoid with the identity e and distinct right zeros z_1, z_2. By Theorem 1, all subsemigroups of S are irreducible. Prove that they are irreducible in equal length.

Consider a semigroup T with $S \preceq T$ and let T' be a subsemigroup of T having a homomorphism $\psi : T' \rightarrow S$ onto S. Consider an arbitrary subset H of T' having strings $p_0, p_1, p_2 \in H^+$ with $\psi(p_0) = e, \psi(p_1) = z_1, \psi(p_2) = z_2$. Take words $q_0, q_1, q_2 \in T'^+$ having $q_0 = (p_0)^{|p_1||p_2|}, q_1 = (p_1)^{|p_0||p_2|}, q_2 = (p_2)^{|p_0||p_2|}$. It is clear that $|q_0| = |q_1| = |q_2|$, and simultaneously, $\psi(q_0) = e$, $\psi(q_1) = z_1$, $\psi(q_2) = z_2$. Obviously, $S \mid^{n,H} T$ with $n = |p_0||p_1||p_2|$. This shows that for every subset H of T, $S \preceq_H T$ implies $S \mid^H T$. On the other hand, S is irreducible. Clearly, then S is irreducible in equal length. We omit the easy proof for the appropriate subsemigroups.

Next we prove

Theorem 4. *Let $G = \{g_1, \dots, g_n\}$ be a (finite) order n group. Put $P_G = \{g_{P(1)} \cdots g_{P(n)} : P$ is a permutation over $\{1, \dots, n\}\}$. If G is simple and noncommutative then there exists a positive integer m with $P_G^m = G$.*

Proof: First, for every positive integer t and $r \in P_G$, we have $|P_G^{t+1}| \geq |rP_G^t| = |P_G^t|$, and the group is finite. Therefore, this growing should be finished, i.e., there exists an t_0 such that $t \geq t_0$ implies $|P_G^t| = |P_G^{t_0}|$. Let $m \geq t_0$ be such that $e \in P_G^m$, where e denotes the identity element of the group G. (Of course, for every $r \in P_G$, $rr^{-1} = e$. Thus, for example, m may be an arbitrary positive even number with $m \geq t_0$.) Then $P_G^m P_G^m = P_G^{2m}$ and $P_G^{2m} \subseteq eP_G^m = P_G^m$. But they have the same number of elements, thus $P_G^m P_G^m = P_G^m$, therefore, P_G^m is a subgroup. Prove that for arbitrary $r \in G$, $rP_G^m = P_G^m r$. Indeed, let $g_{P_1(1)} \cdots g_{P_1(n)} \cdots g_{P_m(1)} \cdots g_{P_m(n)} \in {P_G}^m$, $r \in G$. Then, using the fact that for every $g', g'' \in G$, $\varphi'_g : g \rightarrow g'g, g \in G$ and $\varphi'_{g''} : g \rightarrow gg'', g \in G$ are one-to-one mappings, for every $i = 1, \dots, m$, $\{rg_{P_i(1)}r^{-1}, \dots, rg_{P_i(n)}r^{-1}\} = G$. In other words, for every $i = 1, \dots, m$, $rg_{P_i(1)}r^{-1} \dots rg_{P_i(n)}r^{-1} \in P_G$, leading to $rP_G^m r^{-1} = P_G^m$, i.e., $rP_G^m = P_G^m r$. Therefore, every element of G normalizes P_G^m, and thus P_G^m is normal subgroup in G. Since G is noncommutative, there are $g_i, g_j \in G$ with $g_i g_j \neq g_j g_i$. But then we get $g_i g_j g'_1 \cdots g'_{nm-2} \neq g_j g_i g'_1 \cdots g'_{nm-2}$, $g'_1, \dots, g'_{nm-2} \in G$. Thus, of course, $|P_G^m| \geq 2$. Therefore, by the simplicity of G, $P_G^m = G$ necessarily holds.

Let G be a group. An element $g \in G$ is called *commutator* if $g = aba^{-1}b^{-1}$ for some elements $a, b \in G$. The smallest subgroup that contains all commutators of G is called the *commutator subgroup* or derived subgroup of G, and is denoted by G'. It is well-known that $G = G'$ whenever G is simple and non-commutative. Thus we can also get our previous result as a direct consequence of the following well-known theorem.

Theorem 5. **(Dénes-Hermann Theorem)** *Let $G = \{g_1, \ldots, g_n\}$ be a (finite) order n non-commutative group and denote G' its commutator subgroup. Put $P_G = \{g_{P(1)} \cdots g_{P(n)} : P$ is a permutation over $\{1, \ldots, n\}\}$. There exists a $g \in G$ with $P_G = G'g$. Thus $P_G = G$, whenever $G = G'$.*

Now we show the following

Theorem 6. *The non-commutative finite simple groups are irreducible in equal length.*

Suppose that $S = \{g_1, \ldots, g_n\}$ is a non-cyclic simple group. Consider a semigroup T with $S \preceq T$ and let T' be a subsemigroup of T having a homomorphism $\psi : T' \to S$ onto S. Consider an arbitrary subset H of T' having strings $r_1, \ldots, r_n \in H^+$ with $\psi(r_i) = g_i$, $i \in \{1, \ldots, n\}$. Then, using Theorem 4., there exists a positive integer m such that for every $s \in S$ there are permutations $P_{s,1}, \ldots, P_{s,m}$ over $\{1, \ldots, n\}$, with $s = g_{P_{s,1}(1)} \cdots g_{P_{s,1}(n)} \cdots g_{P_{s,m}(1)} \cdots g_{P_{s,m}(n)}$. But then, of course, $\psi(r_{P_{s,1}(1)} \cdots r_{P_{s,1}(n)} \cdots r_{P_{s,m}(1)} \cdots r_{P_{s,m}(n)}) = \psi(r_{P_{s,1}(1)} \cdots r_{P_{s,1}(n)} \cdots r_{P_{s,m}(1)} \cdots r_{P_{s,m}(n)}) = s$. Consequently, there exists a positive integer t $(= m(|r_1| + \ldots + |r_n|))$ such that for every $s \in S$, there is a t-length word $p \in H^+$ with $\psi(p) = s$. Thus we have $S \,|^{t,H}\, T$. Therefore, for every subset H of T, $S \preceq_H T$ implies $S \,|^{H}\, T$. On the other hand, by Theorem 1, S is irreducible. It is easy to show that in this case S is irreducible in equal length too. This ends the proof.

Thus we received a new proof of the following result of Z. Ésik [1], [2].

Theorem 7. *The irreducible semigroups are irreducible in equal length too.*

References

[1] Z. Ésik, An extension of the Krohn-Rhodes decomposition of automata, *in: Proc. IMYC'1988, Smolenice, LNCS, 381,* Springer, 1989, 66-71.

[2] Z. Ésik, Results on homomorphic realization of automata by α_0-products, *TCS, 87,* 1991, 229-249.

[3] J. Dénes and P. Hermann, On the product of all elements in a finite group, *Ann. of Discrete Math., 15,* 1982, 107-111.

[4] K. B. Krohn, J. L. Rhodes and B. R. Tilson, The prime decomposition theorem of the algebraic theory of machines, *in: M. Arbib, ed., Algebraic Theory of Machines, Languages and Semigroups,* Academic Press, New York, 1968.

[5] P. P. Pálfy, On generating systems of non-commutative finite simple groups, personal communication, 1989.