Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
17 (2001), 137–139
www.emis.de/journals

ON THE PRODUCT OF ALL ELEMENTS IN A FINITE GROUP

PÁL DÖMÖSI

In honour of Professor Árpád Varecza on his 60^{th} birthday

Abstract. A new elementary and direct proof is given to show a consequence of the Dénes–Hermann Theorem.

1. Motivations

An automaton (without outputs) can be considered as a generating system of a transformation semigroup. Especially, we can also consider an automaton as a generating system of a permutation group if all input letters induce a bijective mapping of the set of states onto itself. By these simple facts, in general, transformation semigroups and permutation groups are useful tools in the algebraic theory of automata [6, 7, 10]. Moreover, finite groups have an important role in the composition of finite automata [8, 11, 12]. One can consider compositions of automata as automata networks [2, 5, 9]. Furthermore, permutation factorization by networks of automata is an important subject in theoretical computer science [14, 15].

The well-known Dénes–Hermann Theorem [1] shows an interesting property of the product factorization of all elements in a finite group. A direct consequence of this result has important applications in compositions of automata [3, 4]. The only known proof of the Dénes–Hermann Theorem uses the Feit–Thomson Theorem. Thus Z. Ésik gave a direct proof of this consequence in [4]. Using an idea of P. P. Pálfy [13], we give another direct and elementary proof of this consequence of the Dénes–Hermann Theorem.

2. Results

Now we show the following

Theorem. *Let $G = \{g_1, \ldots, g_n\}$ be a (finite) order n group. Put*

$$P_G = \{g_{P(1)} \cdots g_{P(n)} : P \text{ is a permutation over } \{1, \ldots, n\}\}.$$

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 a 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 $r \in P_G$, $rr^{-1} = e$.

2000 *Mathematics Subject Classification.* 68Q45.
Key words and phrases. Finite groups, automata.
This work was supported by grants of the "Automata & Formal Languages" project of the Hungarian Academy of Sciences and Japanese Society for Promotion of Science (No 15), and the Hungarian National Foundation for Scientific Research (OTKA T030140).

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 $P_G^{2m} \supseteq eP_G^m = P_G^m$. 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 $g', g'' \in G$, $\varphi'_g : g \to g'g, g \in G$ and $\varphi'_{g''} : g \to gg'', g \in G$ are one-to-one mappings, for every $i = 1, \ldots, m$, $\{rg_{P_i(1)}r^{-1}, \ldots, rg_{P_i(n)}r^{-1}\} = G$. In other words, for every $i = 1, \ldots, m$, $rg_{P_i(1)}r^{-1} \ldots rg_{P_i(n)}r^{-1} \in P_G$ 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 non-commutative, there are $g_i, g_j \in G$ with $g_i g_j \neq g_j g_i$. But then we get $g_i g_j g'_1 \ldots g'_{nm-2} \neq g_j g_i g'_1 \ldots g'_{nm-2}$, $g'_1, \ldots, g'_{nm-2} \in G$. 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.

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*

$$P_G = \{g_{P(1)} \cdots g_{P(n)} : P \text{ is a permutation over } \{1, \ldots, n\}\}.$$

There exists a $g \in G$ with $P_G = G'g$. Thus $P_G = G$, whenever $G = G'$.

Problem. Find an elementary proof of the Dénes–Hermann Theorem.

References

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

[2] P. Dömösi, C. L. Nehaniv, On complete systems of automata, Theoret. Comput. Sci., **245** (2000), 27–54.

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

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

[5] Z. Ésik, A note on isomorphic simulation of automata by networks of two-state automata, *Dicrete Appl.Math.,* **30** (1991) 77–82.

[6] Z. Fülöp, S. Vágvölgyi, A complete classification of deterministic root-to-frontier tree transformation classes, *Theoret. Comput. Science* **81** (1991) 1-15.

[7] Z. Fülöp, H. Vogler, Syntax-Directed Semantics – Formal Models Based on Tree Transducers, *Monographs in Theoretical Computer Science, an EATCS Series,* Springer-Verlag, 1998.

[8] F. Gécseg, Products of Automata, *EATCS Monographs on Theoretical Computer Science, Vol.* **7***,* Springer-Verlag, 1986.

[9] F. Gécseg, B. Imreh, A. Pluhár, On existence of finite isomorphically complete systems, *Journal of Automata, Languages, and Combinatorics* **3** (1998), 77-84.

[10] F. Gécseg, I. Peák, Algebraic Theory of Automata. *Disquisitiones Mathematicae Hungaricae* **2**, *Akadémiai Kiadó, Budapest,* 1972.

[11] K. B. Krohn, J. L. Rhodes, Algebraic theory of machines, I. Prime decomposition theorem for finite semi-groups and machines, *Trans. Amer. Math. Soc.* **116** (1965), 450–464.

[12] 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.

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

[14] M. Tchuente, Permutation factorization on star-connected networks of finite automata, *SIAM Journ. of Alg. Disc. Meth.,* **6** (1985), 537–540.

[15] M. Tchuente, Parallel realization of permutations over tree, *Discrete Math.,* **39** (1982), 211–214.

Received November 20, 2000.

Institute of Mathematics and Informatics,
University of Debrecen,
H-4010 Debrecen, Pf. 12, Hungary
E-mail address: `domosi@math.klte.hu`