Title	Algebraic structure of the group of p-permutations on tally sets : Extended Abstract
Author(s)	Nishino, Tetsuro
Citation	数理解析研究所講究録 (1989), 695: 155-161
Issue Date	1989-06
URL	http://hdl.handle.net/2433/101394
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
第 695 巻 1989 年 155-161

ｔａｌｌｙ集合上のｐ－置換群の代数的構造について

Algebraic structure of the group of p-permutations on tally sets
(Extended Abstract)

西野哲朗
Tetsuro Nishino

東京電機大学 情報科学科
Department of Information Sciences, Tokyo Denki University

Abstract

Let G_p^t be the group of p-permutations on tally sets. In this paper, we will show that

$$G_p^t \rhd F_p \rhd A_p \rhd \{ id \}$$

is the unique composition series for G_p^t, where F_p is a normal subgroup of G_p^t composed of finite p-permutations, and A_p is a normal subgroup of F_p of index 2, and id is the identity p-permutation.

1 Introduction

If we follow the approach of F. Klein, the recursive function theory is considered to be the study of properties possessed by sets of natural numbers which are invariant under recursive permutations [11]. Thus, the group of recursive permutations of the natural numbers are of interest in the recursive function theory. In [6], C. F. Kent showed that the group of recursive permutations has algebraic properties similar to those of S_∞, which is the group of all permutations of the natural numbers.

The group S_∞ was studied by L. Onofri [8], and by J. Schreier and S. Ulam [9, 10] around 1930. They showed that

$$S_\infty \rhd F \rhd A \rhd \{ id \}$$

is the unique composition series for S_∞. The normal subgroup F of S_∞ consists of permutations moving only finitely many natural numbers. While, the normal subgroup A of F consists of those finite permutations which are even. Hence A is a subgroup of F of index 2. And id is the identity permutation.

In [6], Kent showed that the analogous result holds for a group R_M of permutations recursive in an arbitrary set $M \subseteq N$. That is

$$R_M \rhd F \rhd A \rhd \{ id \}$$

is the unique composition series for any such R_M.

While, in [3], L. Berman and J. Hartmanis introduced the notion of polynomial time isomorphism (p-isomorphism for short) by using the concept of p-permutations. A p-permutation is a member of the following subgroup G_p of the group of recursive permutations :

$$G_p = \{ f : N \to N \mid f \text{ is a one-one onto map computable in p-time, and } f^{-1} \text{ is also computable in p-time } \}.$$

It is well known that Berman and Hartmanis conjectured that all NP-complete sets are p-isomorphic. The isomorphic question for NP-complete sets has gained a great deal of attention in recent years.

In this paper, we will show that the group G_p^t of p-permutations on tally sets has algebraic properties similar to those of S_∞ and R_M. Namely we will show that

$$G_p^t \rhd F_p \rhd A_p \rhd \{ id \}$$

is the unique composition series for G_p^t, where F_p is a normal subgroup of G_p^t composed of finite p-permutations, and A_p is a normal subgroup of F_p of index 2, and id is the identity p-permutation.

2 Preliminaries

First, we briefly describe the basic concepts in computational complexity. For details, see [2, 5].

We use the standard lexicographic ordering $\leq$ or $<$ on strings. The length of the string x is denoted by $|x|$, and the cardinality of the set S is denoted by $|S|$. The empty string is denoted by λ. A set S is *sparse* iff there exists a polynomial $p(x)$ such that $|\{ w \mid w \in S, \ |w| \leq n \}| \leq p(n)$. And a set S is a *tally set* if $S \subseteq \{ 1 \}^*$. A set S is *bi-infinite* iff both S and $\bar{S}$ are infinite. The composite of two functions f and g is denoted by $f \circ g$. We denote the value of the composite $f \circ g$ for x by $f \circ g(x)$.

The set of natural numbers is denoted by N, i.e. $N = \{ 0, 1, 2, ... \}$. In this paper, we use strings in $\{ 1 \}^*$ to represent natural numbers. That is, 0 is represented by λ and $n \in N$ is represented by 1^n. Thus, an arbitrary set of natural numbers is considered to be a tally set, and especially, $N = \{ 1 \}^*$.

> DTIME($t(n)$) = { S | S is accepted by a deterministic Turing machine which runs in time $t(n)$ }.
>
> $\mathcal{P} = \bigcup_{i \geq 0}$ DTIME(n^i).

For a function $f : N \to N$, $dom(f)$ denotes the domain of f. A function f is *computable in p-time* if there exists a polynomial time bounded deterministic Turing transducer M such that (1) for all $x \in dom(f)$, M outputs $f(x)$, and (2) for all $x \notin dom(f)$, M outputs a special symbol $*$.

In this paper, we deal with the following subgroup of the group of recursive permutations :

> G_p^t = { $f : N \to N$ | f is a one-one onto map computable in p-time, and f^{-1} is also computable in p-time. $N = \{ 1 \}^*$ }.

In this paper, we call a member of G_p^t a *polynomial time permutation* (*p-permutation* for short). A p-permutation which moves infinitely (resp. finitely) many natural numbers is called an *infinite* (resp. *finite*) *p-permutation.*

For a set S, a one-one function $e_S : N \to S$, which enumerates S and is computable in p-time, is called *p-enumeration function* of S. A set which has a p-enumeration function is said to be *p-enumerable.* A set S is *strongly p-enumerable* iff (1) S is p-enumerable, and (2) An inverse $e_S^{-1} : S \to N$ is also computable in p-time (We assume that e_S^{-1} outputs a special symbol, $*$, if an input string is not belong to S). Notice that, from (2), strongly p-enumerable sets are in $\mathcal{P}$.

A function f *optimally compresses* a set S if for any $x \in S$ of length n, $|f(x)| \leq \lceil log(\sum_{i=0}^{n} |S^i|) \rceil$, where S^i is the set of strings in S of length i. The *ranking function* for a set S, r_S, maps strings in S to their index in the standard lexicographic ordering, i.e. $r_S(x) = |\{ w \in S \mid w \leq x \}|$. The ranking is a special kind of optimal compression. As was noted in [4], if $r_S : S \rightarrow N$ is computable in p-time, then so is $r_S^{-1} : N \rightarrow S$ using binary search. In [1], E. W. Allender showed the following theorem.

Theorem A [1] The following are equivalent :

(1) A set S is p-isomorphic to a tally set in $\mathcal{P}$.
(2) A set S is sparse and has a ranking function r_S which is computable in p-time.

□

Next, we briefly describe the basic concepts in group theory. For details, see [7].

A *permutation* on a set S is a one-one onto map $S \rightarrow S$. A permutation which amounts to a circular rearrangement of the symbols permuted is called a *cycle*. The number of letters in a cycle is called its *length*. A cycle of length 2 is called a *2-cycle* or a *transposition*. The 2-cycle which interchanges the symbols s_1 and s_2 is denoted by $(s_1,\ s_2)$. And the composite of the two 2-cycles $(s_1,\ s_2)$ and $(s_3,\ s_4)$ is denoted by $(s_1,\ s_2)(s_3,\ s_4)$.

A subgroup H of G is said to be *normal* in G when $h \in H$ and $g \in G$ imply $ghg^{-1} \in H$. We write $H \lhd G$ if H is a nomal subgroup of G. A group $G \neq \{ u \}$ is called *simple* if it has no nontrivial normal subgroups. Here, u is the identity of G. A *composition series* of G is any series

$$G = G_0 \rhd G_1 \rhd \dots \rhd G_m = \{ u \}$$

where the quotients G_{i-1}/G_i for i, $1 \leq i \leq m$ are simple. These quotients are called the *composition factors*. The following theorem is well known.

Theorem (Jordan-Hölder) Any two composition series for a group G have the same length and isomorphic factors.

□

3 Main Theorem

In this section, we will show a proof sketch of the following Main Theorem.

Main Theorem Let G_p^t be the group of p-permutations on tally sets. Then,

$$G_p^t \rhd F_p \rhd A_p \rhd \{\, id \,\}$$

is the unique composition series for G_p^t, where F_p is a normal subgroup of G_p^t composed of finite p-permutations, A_p is a normal subgroup of F_p of index 2, and id is the identity p-permutation.

In order to prove the Main Theorem, we first prove the following theorem.

Theorem 1 Let G be a normal subgroup of G_p^t. If G contains an infinite p-permutation then $G = G_p$.

We will prove Theorem 1 through a sequence of four lemmas. The ideas of the proofs of these lemmas are from [6].

Lemma 1 Let G be a normal subgroup of G_p^t containing an infinite p-permutation f. Then G contains a p-permutation g with infinitely many disjoint 2-cycles.

□

Lemma 2 Let G be a normal subgroup of G_p^t containing a p-permutation g with infinitely many disjoint 2-cycles, which is constructed in the proof of Lemma 1. Then G has the following property Π :

> Let $A \subseteq N$ be a bi-infinite set such that both A and $\bar{A} = N - A$ are strongly p-enumerable. If e_1 and e_2 are two p-enumeration functions for A, then there exists a p-permutation $h \in G$ such that, for all $n \in N$, $h \circ e_1(n) = e_2(n)$.

□

Lemma 3 Let G be a normal subgroup of G_p^t having the property Π of Lemma 2. Let $f \in G_p^t$ be an arbitrary p-permutation with infinitely many disjoint 2-cycles and infinitely many numbers not in 2-cycles, then $f \in G$.

□

Lemma 4 Let $f \in G_p^t$ be an arbitrary p-permutation. It is possible to express f as a composition $f = f_2 \circ f_1$ of two p-permutations such that both f_1 and f_2 have infinitely many disjoint 2-cycles and infinitely many numbers not in 2-cycles.

□

We now return to the proof of Theorem 1.

Proof of Theorem 1 Let G be a normal subgroup of G_p^t containing an infinite p-permutation. Let $f \in G_p^t$ be an arbitrary p-permutation. By lemma 4, f can be expressed as the product $f_2 \circ f_1$ of two other p-permutations of G_p^t, each of which has a bi-infinite closed set of natural numbers. But, by lemmas 1, 2 and 3, G contains every p-permutation of G_p^t having a bi-infinite closed set of natural numbers. Thus, $f_1 \in G$ and $f_2 \in G$. Since G is a group, $f = f_2 \circ f_1 \in G$. Therefore $G_p^t \subseteq G$, and Theorem 1 is proved.

□

Finally, we return to the proof of Main Theorem.

Proof of Main Theorem By Theorem 1, F_p is maximal normal in G_p^t. Since A_p is a subgroup of F_p of index 2, A_p is maximal normal in F_p. The simplicity of A_p can be shown in the same way that, for $n \geq 5$, the simplicity of the alternating group A_n of all even permutations of $\mathbf{n} = \{ 1, 2, \ldots n \}$ is proven (See, for example, [7]).

By the Jordan-Hölder theorem, it is easily seen that

$$G_p^t \rhd F_p \rhd A_p \rhd \{ id \}$$

is the unique composition series for G_p^t.

□

4 Concluding Remarks

In this paper, we have shown that the group G_p^t of p-permutations on tally sets has algebraic properties similar to those of S_∞, the group of all permutations of the natural numbers. It is to be expected that similar algebraic properties of G_p can be found in order to give some insight into the isomorphism question for NP-complete sets.

Acknowledgments

The author would like to express his sincere thanks to Professor Hiroshi Noguchi of Waseda University for his kind advice. He also thanks Professors Takeo Yaku and Akeo Adachi of Tokyo Denki University for their valuable suggestions.

References

[1] Allender, E. W., and Rubinstein, R. S., "P-Printable Sets", *SIAM J. Comput.*, Vol.17 (1988), pp.1193-1202.

[2] Balcázar, J. L., Díaz, J., and Gabarró, J., *Structural Complexity I*, Springer-Verlag (1988).

[3] Berman, L., and Hartmanis, J., "On Isomorphisms and Density of NP and Other Complete Sets", *SIAM J. Comput.*, Vol.6 (1977), pp.305-322.

[4] Goldberg, A. V. and Sipser M., "Compression and Ranking", *Proc. 17th Annual ACM Symposium on Theory of Computing* (1985), pp. 440-448.

[5] Hopcroft, J. E., and Ullman, J. D., *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley, Reading, Massachusetts (1979).

[6] Kent, C. F., "Constructive Analogues of the Group of Permutations of the Natural Numbers", *Transactions of the AMS*, Vol.104 (1962), pp.347-362.

[7] MacLane, S., and Birkhoff, C., *Algebra - Second Edition*, Macmillan, New York (1979).

[8] Onofri, L., "Teoria delle sostituzioni che operano su una infinitá numerabile di elementi", *Ann. Math. Ser.*, Vol.4 (1927), pp.73-106; Vol.5 (1928), pp.147-168; Vol.7 (1930), pp.103-130.

[9] Schreier, J., and Ulam, S., "Über die Permutationsgruppe der natürlichen Zahlenfolge", *Studia Math.*, Vol.4 (1933), pp.134-141.

[10] Schreier, J., and Ulam, S., "Über die Automorphismen der Permutationsgruppe der natürlichen Zahlenfolge", *Fund. Math.*, Vol.28 (1937), pp.258-260.

[11] Rogers, H., *Theory of Recursive Functions and Effective Computability*, MIT Press, Cambridge, MA. (1967).