

Copyright © 1972, by the author(s).  
All rights reserved.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission.

THE PRIMITIVE RECURSIVE PERMUTATIONS GENERATE THE  
GROUP OF RECURSIVE PERMUTATIONS

By

Ion Stefan Filotti

Memorandum No. ERL-354

August 1972

ELECTRONICS RESEARCH LABORATORY

College of Engineering  
University of California, Berkeley  
94720

## Acknowledgements

I wish to express my gratitude  
to Professor Manuel Blum for his guidance, his constant interest  
in my work and for uncovering recursive and complexity theory and  
much else to me;  
to Dr. Julia Robinson for her kind advice and encouragement;  
to my friend Richard Epstein for his precious criticism and  
unbounded enthusiasm during this research and also for proof  
reading the manuscript;  
to Professors R. W. Robinson and Philip Spira for their lectures  
and their kind help;  
to Mrs. Doris Simpson for her careful typing;  
to all my friends for their many ways of proving their friendship;  
to Kay for smiling  
and  
to my parents for everything.

This work was supported by the National Science Foundation  
under Grant GJ-708.

THE PRIMITIVE RECURSIVE PERMUTATIONS GENERATE THE  
GROUP OF RECURSIVE PERMUTATIONS

ABSTRACT

Ion Stefan Filotti

The title is proved. More precisely, it is shown that any recursive permutation can be obtained by composing not more than six permutations in  $\mathcal{E}^1$  (Grzegorzczuk's second class) or their inverses. The recursive permutations cannot be obtained by composing less than six permutations in  $\mathcal{E}^1$  or their inverses. Finally, the group generated by the permutations in  $\mathcal{E}^0$  is strictly contained in the group of recursive permutations.

These results completely solve a problem posed by Dr. Julia Robinson and show that, in a sense, primitive recursive permutations have not only very powerful inverses but also very "flexible ones."

The thesis contains a number of additional results concerning the primitive recursive functions and the Grzegorzczuk hierarchy.

The main result has also been obtained simultaneously and independently by V. V. Koz'minikh from Novosibirsk.

## Table of Contents

	Page Nos.
ABSTRACT	iii
1. INTRODUCTION NOTATIONS	1
2. DEFINITION AND MAIN PROPERTIES OF THE PRIMITIVE RECURSIVE FUNCTIONS AND OF THE GRZEGORCZYK HIERARCHY	4
3. GRZEGORCZYK'S CLASS $\mathcal{E}^0$	10
4. RECURSIVE FUNCTIONS AND THEIR GRAPHS. HONEST FUNCTIONS	16
5. SOME RESULTS ON RECURSIVE SETS	24
6. ENUMERATION OF RECURSIVE SETS	29
7. GENERATORS FOR THE GROUP OF RECURSIVE PERMUTATIONS	37
8. THE PERMUTATIONS $\mathcal{E}^0$	50
REFERENCES	55

## 1. INTRODUCTION NOTATIONS

As can be guessed from its title, this thesis is devoted to the solution of the following problem posed by Dr. Julia Robinson: Do the primitive recursive permutations generate the group of recursive permutations?. We answer this question in the affirmative by showing, moreover, that any recursive permutation can be written in the form  $\pi_6^{-1} \pi_5 \pi_4^{-1} \pi_3 \pi_2^{-1} \pi_1$  or  $\pi_6 \pi_5^{-1} \pi_4 \pi_3^{-1} \pi_2 \pi_1^{-1}$  for some primitive recursive permutations  $\pi_i$  ( $i \leq 6$ ). This result is the best possible in the sense that there exist recursive permutations that can not be obtained by composing less than six primitive recursive permutations or their inverses (This result is due to Professor Manuel Blum). Thus the result bears much similarity to certain normal form theorems for recursive functions [11] and shows that, in a sense, primitive recursive permutations have not only very powerful inverses, but also very "flexible" ones.

The solution to Dr. Robinson's problem was obtained by us in May 1971 and was communicated to her and to Professor Blum on June 5, 1971. We showed at that time a slightly weaker form of the present results, namely that any recursive permutation can be obtained by composing not more than thirty two primitive recursive permutations or their inverses. It was immediately pointed out by Richard Epstein, who had closely observed our work during that period, that exactly the same proofs worked for permutations in

Grzegorzczuk's class  $\mathcal{E}^1$  instead of primitive recursive ones.

In December 1971 Dr. Julia Robinson informed us that V. V. Koz'minikh from Novosibirsk had independently solved the same problem, proving moreover that six permutations in the class  $\mathcal{E}^1$  of Grzegorzczuk are enough to generate any recursive permutation. He announced further that the permutations of  $\mathcal{E}^0$  do not generate the group of recursive permutations. We are not familiar with his proofs as his paper is just an abstract. The proofs appearing in this thesis are our own, although we suspect that they can not be essentially different from Koz'minikh's.

The techniques we use are totally elementary. It has been known for a long time that the primitive recursive permutations do not form a group [6] and Dr. Robinson herself had the result of Professor Blum mentioned above. We present here the proofs of Koz'minikh's improved version instead of our original one. Not only is the result a better one, but we also avoid the use of a result due to Kent (Lemma 2.5 of [4]), rendering the proofs more self-contained.

The main results of the thesis appear in Section 7 and Section 8 where we prove that the permutations of  $\mathcal{E}^1$  generate the group of recursive permutations and that the permutations of  $\mathcal{E}^0$  do not. Section 2 and Section 3 review basic facts about the Grzegorzczuk hierarchy. Section 4 contains technical results about the graphs of recursive functions and Section 5 is devoted mainly to the proof of a "representation" theorem (Theorem 5.3) which we find interesting in its own right. Section 6 contains results about sets enumerated by one-one by primitive recursive functions, results

later used in Section 7 and Section 8.

Notation is mostly standard.  $\mathcal{N}$  will denote the set of non-negative integers. Capital letters will usually denote sets of natural numbers and small Roman or Greek letters will denote functions from  $\mathcal{N}$  to  $\mathcal{N}$  (an exception is made in Section 3 where we conform to the use of denoting specific functions by capital letters). A permutation is a function from  $\mathcal{N}$  to  $\mathcal{N}$  which is one-one and onto.

If  $X = \{x_0, x_1, \dots, x_n, \dots\}$  and  $x_i < x_{i+1}$  for  $i \in \mathcal{N}$ , then  $I_X$  will denote the increasing enumeration of  $X$ , i.e. the unique function  $I : \mathcal{N} \rightarrow \mathcal{N}$  such that  $I(n) = x_n$ . If  $X \subseteq \mathcal{N}$  and  $x \in \mathcal{N}$  then  $v_X(x)$  will denote the number of elements  $y \in X$  such that  $y < x$ . In general, if  $Q(z)$  is a one-place predicate,  $vzQ(z)$  will denote the cardinality of the set  $\{z : Q(z)\}$  and  $\mu zQ(z)$  will denote the least  $z$  such that  $Q(z)$ . For any  $X \subseteq \mathcal{N}$ ,  $c_X$  will denote the representing function of  $X$ , i.e. the function  $c$  such that  $c(x) = 0$  if  $x \in X$  and  $c(x) = 1$  if  $x \notin X$ .

Pairs of natural numbers will be encoded by a standard pairing function discussed in Section 3.  $\langle x, y \rangle$  will denote the encoding of the ordered pair  $(x, y)$  and the left and right projections will be denoted by  $r$  and  $l$  respectively. Thus  $\langle l(u), r(u) \rangle = u$ ,  $l(\langle x, y \rangle) = x$  and  $r(\langle x, y \rangle) = y$ .

For any function  $f$ ,  $G_f$  will denote the graph of  $f$ , i.e. the set  $\{\langle x, y \rangle : y = f(x)\}$ .

## 2. DEFINITION AND MAIN PROPERTIES OF THE PRIMITIVE RECURSIVE FUNCTIONS AND OF THE GRZEGORCZYK HIERARCHY

The primitive recursive functions were originally introduced, although not under this name, by Gödel. It was later recognized that not all computable functions were primitive recursive and this led to the definition of the general and of the partial recursive functions. However, all computable functions actually met in practice were primitive recursive. Later Kalmar isolated a class of functions which he called "elementary" and even this much more restricted class of functions seemed to meet most practical needs. On the other hand, to obtain computable functions which are not primitive recursive one has to resort to diagonal arguments. Ackermann constructed a function which is larger than any given primitive recursive function on all but a finite number of its arguments (see [7][12]).

Thus, at this stage, one possesses a formal definition of the intuitive concept of recursion and a way of constructing functions of larger growth than any of the functions defined using the primitive recursive mechanism. Combining these two ideas, Grzegorzczuk [3] was able to exhibit a very natural hierarchy of the primitive recursive functions. Roughly, Grzegorzczuk's idea is the following. Instead of allowing the functions defined by the primitive recursive procedure to grow unboundedly, we will impose the restriction of defining only functions bounded by some

previously defined function. Then, applying Ackermann's procedure, a new function, dominating all the previously defined ones is obtained. Now the process can be repeated using this new function as an initial function as well. A new class of functions, strictly containing the original one is thus produced. Repeating this process denumerably many times produces a denumerable chain of classes of functions, the union of which is the class of all primitive recursive functions. Grzegorzcyk then showed that Kalmar's elementary functions are precisely the functions of  $\mathcal{E}^3$ , the third class of the hierarchy.

The relations of a Grzegorzcyk class have many of the properties of the primitive recursive relations. In particular they are closed under bounded quantification and Boolean operations. Also, Kleene's T-predicate can be shown to be in  $\mathcal{E}^3$  and, after exercising some care, even in  $\mathcal{E}^0$ . As a result of this, in Kleene's normal form for partial recursive functions,  $f(x) = 1\mu_y(\tau(x,y) = 0)$  one can choose  $\tau$  to be in  $\mathcal{E}^i$  for any  $i$ . Also it can be shown that any r.e. set is enumerable by a function in  $\mathcal{E}^0$ .

Let us note "en passant" that these ideas have been more recently extended into the transfinite (see, for example [9]).

We now proceed to briefly review these definitions and the main properties of the Grzegorzcyk hierarchy.

Definition 2.1. Let  $\mathcal{C}$  be a class of functions from  $\mathcal{N}$  to  $\mathcal{N}$ .  $\mathcal{C}$  is closed under substitutions if it is closed under the following three operations:

- (i) Composition of functions. If  $f(x_1, \dots, x_{k-1}, x_k, x_{k+1}, \dots, x_n)$  and  $g(y_1, \dots, y_n)$  are functions in  $\mathcal{C}$  then so is their composition

$$f(x_1, \dots, x_{k-1}, g(y_1, \dots, y_n), x_{k+1}, \dots, x_n)$$

(ii) Identification of variables. If  $f(x_1, \dots, x_j, \dots, x_k, \dots, x_n)$  is a function in  $\mathcal{C}$ , then so is  $f(x_1, \dots, y, \dots, y, \dots, x_n)$ , i.e. the function obtained by substituting  $y$  for both  $x_j$  and  $x_k$  simultaneously. Here  $y$  is a variable different from all the  $x_i$ 's.

(iii) Substitution of a constant. If  $f(x_1, \dots, x_k, \dots, x_n)$  is a function in  $\mathcal{C}$  then so is  $f(x_1, \dots, 0, \dots, x_n)$  obtained by substituting the constant 0 for  $x_k$ .

Definition 2.2. Let  $f(x_1, \dots, x_n, i)$  be a function of  $n + 1$  variables. The functions  $g$  and  $h$  defined by

$$g(x_1, \dots, x_n, y) = \sum_{i \leq y} f(x_1, \dots, x_n, i) \quad (2.1)$$

$$h(x_1, \dots, x_n, y) = \prod_{i \leq y} f(x_1, \dots, x_n, i) \quad (2.2)$$

are said to be defined by bounded summation and bounded multiplication, respectively, from  $f$ . A class  $\mathcal{C}$  is closed under bounded summation (multiplication) if it contains  $g(h)$  defined by (2.1) (2.2) every time it contains  $f$ .

Definition 2.3. Let  $f(\underline{u}, x)$  be a function of  $n + 1$  arguments (here  $\underline{u}$  stands for  $u_1, \dots, u_n$ ). The function

$$g(\underline{u}, y) = \mu x \leq y (f(\underline{u}, x) = 0) \quad (2.3)$$

defined as follows

$$\mu x \leq y (f(\underline{u}, x) = 0) = \begin{cases} \text{the smallest } x \leq y \text{ such that } f(\underline{u}, x) = 0 \\ \text{when such } x \text{ exist} \\ 0 \text{ otherwise} \end{cases}$$

is said to be defined by bounded minimization from  $f$ . A class  $\mathcal{C}$  of functions is closed under bounded minimization if it contains the function  $g$  defined by (2.3) every time it contains  $f$ .

Definition 2.4. Let  $g, h, j$  be given functions and let  $f$  be defined from them by the following equations:

$$f(\underline{u}, 0) = g(\underline{u}) \quad (2.5)$$

$$f(\underline{u}, x + 1) = h(\underline{u}, x, f(\underline{u}, x)) \quad (2.6)$$

$$f(\underline{u}, x) \leq j(x) \quad (2.7)$$

Then  $f$  is said to be defined by bounded primitive recursion from the functions  $g, h$  and  $j$ . If  $f$  is defined from  $g$  and  $h$  by equations (2.5) and (2.6) only, then  $f$  is said to be defined by primitive recursion from  $g$  and  $h$ .

To define Grzegorzczuk's hierarchy we first introduce the following functions:

$$f_0(x, y) = x + 1 \quad (2.8)$$

$$f_1(x, y) = x + y \quad (2.9)$$

$$f_2(x, y) = (x + 1) \cdot (y + 1) \quad (2.10)$$

and for  $n \geq 2$ ,  $f_{n+1}$  defined as follows:

$$f_{n+1}(0, y) = f_n(y + 1, y + 1) \quad (2.11)$$

$$f_{n+1}(x + 1, y) = f_{n+1}(x, f_{n+1}(x, y)) \quad (2.12)$$

Definition 2.5. The class  $\mathcal{C}^n$ , the  $n$ -th class in Grzegorzczuk's

hierarchy, is the smallest class of functions  $\mathcal{C}$  such that

(i) the functions  $\lambda x(x + 1)$ ,  $U_1(x,y) = x$ ,  $U_2(x,y) = y$  and  $f_n(x,y)$  are in  $\mathcal{C}$ .

(ii)  $\mathcal{C}$  is closed under substitutions and bounded primitive recursion.

Definition 2.6. The class  $\mathcal{P}$  of the primitive recursive functions is the smallest class of functions  $\mathcal{C}$  such that

(i) the functions  $\lambda x(x + 1)$ ,  $U_1(x,y) = x$ ,  $U_2(x,y) = y$  are in  $\mathcal{C}$ .

(ii)  $\mathcal{C}$  is closed under substitutions and primitive recursion.

Among the classes  $\mathcal{E}^n$  the class  $\mathcal{E}^3$  is of particular importance as is shown by the following characterization theorem.

Theorem 2.7. (Grzegorzcyk) The following classes of functions are the same:

(i) The class  $\mathcal{E}^3$ .

(ii) The smallest class of functions containing  $\lambda x(x + 1)$ ,  $\lambda xy(x \div y)$ ,  $\lambda xy(x^y)$  and closed under substitutions and bounded minimization.

(iii) The smallest class of functions containing  $\lambda x(x + 1)$ ,  $\lambda xy(x^y)$  and closed under substitutions and bounded primitive recursion.

(iv) The smallest class of functions containing  $\lambda x(x + 1)$ ,  $\lambda xy(x \div y)$ ,  $\lambda xy(x \cdot y)$ ,  $\lambda xy(x^y)$  and closed under substitutions and bounded summation.

(v) The smallest class of functions containing  $\lambda x(x + 1)$ ,  $\lambda xy(x + y)$ ,  $\lambda xy(x \div y)$  and closed under substitutions, bounded summation and bounded multiplication (Kalmar's elementary functions).

Theorem 2.8. (Grzegorzcyk).  $\bigcup_{n \geq 0} \mathcal{E}^n = \mathcal{P}$  and  $\mathcal{E}^{n+1} \supseteq \mathcal{E}^n$ .

To any class of total functions we associate relations.

Definition 2.9. An  $n$ -ary relation  $R(x_1, \dots, x_n)$  is in the class  $\mathcal{C}$  of functions if there exists a function  $f$  in  $\mathcal{C}$  such that

$$R(x_1, \dots, x_n) \Leftrightarrow f(x_1, \dots, x_n) = 0 \quad \text{for all } x_1, \dots, x_n.$$

We will identify sets and relations in the usual manner.

Definition 2.10. Let  $R(\underline{u}, x)$  be an  $n + 1$ -ary relation. The relation  $S$  defined by

$$S(\underline{u}, y) \Leftrightarrow (\exists x \leq y) R(\underline{u}, x) \tag{2.13}$$

is said to be defined from  $R$  by bounded existential quantification.

Similarly, the relation  $t$  defined by

$$T(\underline{u}, y) \Leftrightarrow (\forall x \leq y) R(\underline{u}, x) \tag{2.14}$$

is said to be defined from  $R$  by bounded universal quantification.

Theorem 2.11. (Grzegorzcyk). The relations of  $\mathcal{E}^n (n \geq 0)$  are closed under bounded quantification and under Boolean operations.

As mentioned at the beginning of this section, there exists a function which grows faster than any of the functions of  $\mathcal{E}^n$ .

Theorem 2.12. (Grzegorzcyk). The function  $f_{n+1}(x, x)$  increases faster than any of the functions of  $\mathcal{E}^n (n \geq 0)$ .

### 3. GRZEGORCZYK'S CLASS $\mathcal{E}^0$

We stated in the Introduction the reasons for our interest in  $\mathcal{E}^0$ . This section contains mainly technical results.

Theorem 3.1. Let  $f$  be a function of one variable in  $\mathcal{E}^0$ . There exists a constant  $k$  such that  $f(x) < x + k$  for all  $x$ .

Proof. The proof is by induction on the definition of the functions of  $\mathcal{E}^0$ . The theorem trivially holds for the initial functions and once the function is defined from functions for which the theorem holds it also holds for that function.

Q.E.D.

Proposition 3.2 (Grzegorzcyk). The following functions are in  $\mathcal{E}^0$ .

- (i)  $\lambda xy(y + 1)$ , for any  $y$ .
- (ii)  $0 = \lambda x(0)$ .
- (iii)  $U_1(x, y, z) = x$ , for any  $y$  and  $z$
- (iv)  $U_2(x, y, z) = y$ , for any  $x$  and  $z$ .
- (v)  $U_3(x, y, z) = z$ , for any  $x$  and  $y$ .
- (vi) 
$$P(x) = x \dot{-} 1 = \begin{cases} 0 & \text{if } x = 0 \\ x - 1 & \text{if } x > 0 \end{cases} .$$
- (vii)  $\lambda x(x \dot{-} y)$ , for any  $y$ .
- (viii)  $\sigma(x, y) = x \cdot 0^y = x(1 \dot{-} y)$ .
- (ix)  $\tau(x, y) = x + 0^y$ .
- (x)  $r(x, y) =$  the remainder of the division of  $x$  by  $y$ .

- (xi)  $\left[ \frac{x}{y} \right] =$  the integral part of the quotient of  $x$  and  $y$ .
- (xii)  $\left[ \sqrt{x} \right] =$  the integral part of the square root of  $x$ .
- (xiii)  $Q(x) = \left[ x \div \left[ \sqrt{x} \right]^2 \right]$ .
- (xiv)  $\lambda_{xn} Q^n(x)$ .
- (xv)  $W(x,y) = \nu s < x(Q(s) = y)$ .
- (xvi)  $R(x) = \nu s < x(Q(s) = x)$ .

Proof.

- (i)  $y + 1 = U_2(x, y + 1)$ .
- (ii)  $0(x) = U_2(x, 0)$ .
- (iii)  $U_1(x, y, z) = U_1(x, U_1(y, z))$ .
- (iv)  $U_2(x, y, z) = U_1(U_2(x, y), z)$ .
- (v)  $U_3(x, y, z) = U_2(x, U_2(y, z))$ .
- (vi)  $P(0) = 0(0)$ ,  $P(x + 1) = U_1(x, P(x))$ ,  $P(x) \leq U_1(x, x)$ .
- (vii)  $x \div 0 = U_1(x, x)$ ,  $x \div (y + 1) = U_3(x, y, P(x \div y))$ ,  
 $x \div y \leq U_1(x, y)$ .
- (viii)  $\sigma(x, 0) = U_1(x, x)$ ,  $\sigma(x, y + 1) = 0(U_3(x, y, \sigma(x, y)))$ ,  
 $\sigma(x, y) \leq U_1(x, y)$ .
- (ix)  $\tau(x, 0) = x + 1$ ,  $\tau(x, y + 1) = U_1(x, y, \sigma(x, y))$ ,  
 $\tau(x, y) \leq U_1(x, y) + 1$ .
- (x)  $r(0, y) = 0(y)$ ,  $r(x + 1, y) = U_2(x, \sigma(r(x, y) \div 1, 1 \div (y \div (r(x, y) + 1))))$ ,  $r(x, y) \leq U_2(x, y)$ .
- (xi)  $\left[ \frac{0}{y} \right] = 0(y)$ ,  $\left[ \frac{x+1}{y} \right] = \tau\left(\left[ \frac{x}{y} \right], r(x+1, y)\right)$ ,  $\left[ \frac{x}{y} \right] \leq U_1(x, y)$ .
- (xii)  $\left[ \sqrt{0} \right] = 0$ ,  
 $\left[ \sqrt{x+1} \right] = \tau\left(\left[ \sqrt{x} \right], \left(\left[ \sqrt{x} \right] + 1\right) \div \left[ \frac{x+1}{\left[ \sqrt{x} \right] + 1} \right]\right)$ .  
 $\sqrt{x} \leq U_1(x, x)$ .

(xiii)  $Q(0) = 0,$

$$Q(x + 1) = \sigma(Q(x) + 1, 1 \div r(x + 1, [\sqrt{x + 1} ])),$$

$$Q(x) \leq U_1(x,x).$$

(xiv)  $Q^0(x) = x, Q^{n+1}(x) = Q(Q^n(x)), Q^n(x) \leq U_1(x,x).$

(xv)  $W(0,y) = 0(y),$

$$W(x + 1,y) = \tau(W(x,y), 2 \div \tau(1 \div (y \div Q(x)), Q(x) \div y)),$$

$$W(x,y) \leq U_1(x,y).$$

(xvi)  $R(x) = W(x,Q(x)).$

Q.E.D.

We are now in a position to define a pairing function whose projections are in  $\mathcal{E}^0$ . Let J be defined as follows:  $J(2x,y) = (x + y)^2 + x, J(2x + 1,y) = (x + 1 + y)^2 + x$ . It is easy to see that J maps  $\mathcal{N} \times \mathcal{N}$  one-one onto  $\mathcal{N}$  and that, by the previous Proposition, the two projections  $Q(z) = z \div [\sqrt{z}]^2$  and  $R(z) = \nu u < z(Q(u) = Q(z))$  are both in  $\mathcal{E}^0$ . From now on we will always use Q as our first (or left) projection l and R as our second (or right) projection r. Note that the pairing function J itself is not in  $\mathcal{E}^0$  but in  $\mathcal{E}^2$ . A few values of this pairing function are tabulated below.

R z	36	50	51	67	68	
6						
	25	37	38	52	53	
5						
	16	26	27	39	40	
4						
	9	17	18	28	29	
3						
	4	10	11	19	20	
2						
	1	5	6	12	13	
1						
	0	2	3	7	8	
0		1	2	3	4	5
						Qz

The following property of this pairing function is immediate:

Proposition 3.3. Let  $g$  be a non-decreasing function. The increasing enumeration of the graph of  $g$  will produce the points of the graph in the order of increasing arguments of  $g$ .

This property will be extremely useful later.

To encode  $n$ -tuples of natural numbers we proceed in the usual manner by defining:

$$J(x_0, x_1, \dots, x_n) = J(J(x_0, \dots, x_{n-1}), x_n)$$

for every  $n$ . The projections are given by

$$x_n = RJ(x_0, \dots, x_n),$$

$$x_{n-1} = RQJ(x_0, \dots, x_n),$$

.....

$$x_{n-k} = RQ^k J(x_0, \dots, x_n), \quad (0 < k < n)$$

.....

$$x_0 = Q^n J(x_0, \dots, x_n)$$

By Proposition 3.2 all these projections are functions in  $\mathcal{E}^0$ .

We also need a device for encoding all finite sequences of integers. We do this by associating to the sequence  $(x_0, x_1, \dots, x_n)$  the code number  $J(n+1, J(x_0, x_1, \dots, x_n))$ . In the remaining of this paper we denote  $J(x_0, x_1, \dots, x_n)$  by  $\langle x_0, x_1, \dots, x_n \rangle$  and  $J(n+1, J(x_0, x_1, \dots, x_n))$  by  $\langle\langle x_0, x_1, \dots, x_n \rangle\rangle$ . To this encoding we associate the following decoding functions

which give the length and the  $n$ -th term of the sequence respectively:

$$t(n,m,z) = \begin{cases} RR(z) & \text{if } m = n \\ RRQ^k(z) & \text{if } m = n - k \text{ and } 1 < k < n \\ RQ^n(z) & \text{if } m = 0 \\ 0 & \text{if } m > n \end{cases}$$

$$\text{lgth}(z) = Q(z)$$

$Q(n,z) = Q^n(z)$  can be defined by the following equations:

$$Q(0,z) = Q^0(z) = 0$$

$$Q(1,z) = Q^1(z) = Q(z)$$

$$Q(n+1,z) = Q(Q(n,z))$$

$$Q(n,z) \leq z$$

Hence  $Q(n,z)$  as a function of two arguments is in  $\mathcal{E}^0$  and, consequently,  $t(n,m,z)$  (as a function of three arguments) and  $\text{lgth}(z)$  are in  $\mathcal{E}^0$  as well.

Proposition 3.4. Let  $H$  be a set in  $\mathcal{E}^i$  (respectively  $\mathcal{P}$ ) ( $i \leq 0$ ). The function  $v_H(x) =$  the number of elements  $y < x$  such that  $y \in H$ , is a function in  $\mathcal{E}^i(\mathcal{P})$ .

Proof. Let  $c_H$  be the representing function of  $H$ , i.e. the function taking value 0 and  $H$  and value 1 outside  $H$ .  $v_H$  satisfies the following equations:

$$v_H(0) = 0$$

$$v_H(x+1) = \begin{cases} v_H(x) & \text{if } x \notin H \\ v_H(x) + 1 & \text{if } x \in H \end{cases}$$

Hence  $v_H$  can be defined by:

$$v_H(0) = 0$$

$$v_H(x+1) = \tau(v_H(x), c_H(x))$$

$$v_H(x) \leq U_1(x, x)$$

where  $\tau$  is the function from Proposition 2.14.

Q.E.D.

#### 4. RECURSIVE FUNCTIONS AND THEIR GRAPHS. HONEST FUNCTIONS.

As usual in recursion theory the graph of a function  $f$  is the set  $G_f = \{\langle x, f(x) \rangle : x \in \mathcal{N}\}$ , where  $\langle x, y \rangle$  denotes the encoding of the pair  $(x, y)$  by our standard pairing function  $J$ . A recursive function has always a recursive graph but sometimes the graph of a recursive function may be primitive recursive or even in  $\mathcal{E}^i$ . Such functions have been extensively studied, for example in [8,9], and are sometimes called "honest" functions. Honest functions are functions with easy to compute step-counting functions. The following theorem characterizes honest functions.

Proposition 4.1. Let  $f$  be a partial recursive function.

(i) The predicate  $f(x) = y$  as a predicate of the two variables  $x$  and  $y$  is in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) if and only if there exists a function of two arguments in  $\mathcal{E}^i(\mathcal{P})$  such that for all arguments  $x$ ,  $f(x) = \mu y(\tau(x, y) = 0)$ .

(ii) The graph  $G_f$  of  $f$  is in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 2$ ) if and only if there exists a function  $\tau$  of two arguments in  $\mathcal{E}^i(\mathcal{P})$  such that for all arguments  $x$ ,  $f(x) = \mu y(\tau(x, y) = 0)$ .

Proof. Suppose  $f(x) = \mu y(\tau(x, y) = 0)$  for some function  $\tau \in \mathcal{E}^i(\mathcal{P})$ . Then

$$f(x) = y \Leftrightarrow \tau(x, y) = 0 \wedge (\forall z < y)(\tau(x, z) \neq 0)$$

$$\langle x, y \rangle \in G_f \Leftrightarrow \tau(x, y) = 0 \wedge (\forall z < y)(\tau(x, z) \neq 0)$$

Since  $\mathcal{E}^1$  and  $\mathcal{P}$  are closed under bounded quantification and Boolean operations, and since the projection functions are in  $\mathcal{E}^0$ , the righthand side of these equivalences is a predicate in  $\mathcal{E}^1(\mathcal{P})$ .

Conversely, if  $f(x) = y$  or  $\mathcal{G}_f$  are in  $\mathcal{E}^1(\mathcal{P})$  then  $f(x) = \mu y(f(x) = y)$  and respectively  $f(x) = \mu y(\langle x, y \rangle \in \mathcal{G}_f) = \mu y(c_{\mathcal{G}_f}(\langle x, y \rangle) = 0)$ . Here again  $c_{\mathcal{G}_f}$  is the representing function of  $\mathcal{G}_f$ . This gives the desired representation for  $f$  and proves the proposition.

Q.E.D.

Remark 4.2. If  $\mathcal{G}_f \in \mathcal{E}^1 (i < 2)$  then  $f$  is not necessarily representable in the above form since the pairing function  $\langle x, y \rangle$  is not a function in  $\mathcal{E}^1$ . Therefore only half of (ii) holds in this case.

Proposition 4.1 was first proved by Skolem in the primitive recursive case. We shall say that a function is representable in Skolem normal form if  $f(x) = \mu y(\tau(x, y) = 0)$  for some  $\tau \in \mathcal{E}^i$  or  $\tau \in \mathcal{P}$ . Contrasting with Skolem's is Kleene's normal form (see [7,12])  $f(x) = \text{r}\mu y(\tau(x, y) = 0)$ . Every partial recursive function is representable in Kleene's normal form, but not necessarily in Skolem's normal form.

Proposition 4.3. There exists a function  $g$  which is recursive but not primitive recursive and whose graph  $\mathcal{G}_g$  is in  $\mathcal{E}^0$ .

Proof. Let  $f$  be a recursive but not primitive recursive function. Represent  $f$  in Grzegorzczuk's normal form (see[3]):

$$f(x) = \text{r}\mu y(\tau(x, y) = 0)$$

where  $\tau$  is a function of two variables in  $\mathcal{E}^0$ . Let  $g(x) = \mu y(\tau(x,y) = 0)$ . By Proposition 4.1 and the remark following it  $\mathcal{G}_g \in \mathcal{E}^0$ . However, if  $g$  were primitive recursive so would  $f = rg$  be, contradicting the hypothesis.

Q.E.D.

The previous Proposition can be improved to

Proposition 4.4. There exists a strictly increasing recursive function which is not primitive recursive and whose graph is in  $\mathcal{E}^0$ .

Proof. Let  $g$  be the function of Proposition 4.3. Then  $\mathcal{G}_g$  is in  $\mathcal{E}^0$ . Define  $h$  as follows:

$$h(0) = J(1, g(0))$$

$$h(n) = J(n + 1, J(g(0), g(1), \dots, g(n))) \quad (n > 0)$$

where  $J$  is the standard pairing function. From this,  $g$  can be expressed as a function of  $h$ :

$$g(0) = Rh(0)$$

$$g(n) = RRh(n) \quad (n > 0)$$

Hence  $h$  is not primitive recursive since otherwise  $g$  would be contradicting our initial choice. We can easily convince ourselves, using the properties of the standard pairing function and of the projection functions, that  $h$  is strictly increasing. It remains to check that  $\mathcal{G}_h \in \mathcal{E}^0$ .

First notice that, by the properties of the pairing function, if  $z \in \mathcal{G}_h$  and  $z = \langle x, y \rangle$  then for all  $i \leq x$ ,  $\langle i, g(i) \rangle \leq h(x) \leq z$ .

Hence the following equivalence holds:

$$z \in \mathcal{G}_h \Leftrightarrow [Qz = 0 \wedge QRz = 1 \wedge (\exists t \leq z)(t \in \mathcal{G}_g \wedge Qt = 0 \wedge RRy = Rt)] \vee$$

$$[Qz > 0 \wedge QRz = Qz + 1 \wedge (\forall i \leq Qz)(\exists t \leq z)(t \in \mathcal{G}_g \wedge Qt = i \wedge (i = x \Rightarrow Rt = RQRz) \wedge (i \neq x \Rightarrow Rt = Q^{x-i}QRz))]$$

All the quantifiers on the right-hand side are bounded and all the predicates are in  $\mathcal{E}^0$  by hypothesis or by virtue of Proposition 3.2. Therefore  $\mathcal{G}_h$  is a set in  $\mathcal{E}^0$ .

Q.E.D.

Proposition 4.5. Let  $A \subseteq \mathcal{N}$  be a set.

(i) If  $A \in \mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) then the graph of the increasing enumeration  $I_A$  of  $A$  is in  $\mathcal{E}^i(\mathcal{P})$ .

(ii) For  $i \geq 2$  and  $\mathcal{P}$ , the converse of (i) holds as well, i.e. if  $\mathcal{G}_{I_A} \in \mathcal{E}^i(\mathcal{P})$  then  $A \in \mathcal{E}^i(\mathcal{P})$ .

Proof. (i) Let  $A \in \mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ). Then for all  $n$ ,

$$I_A(n) = \mu y (y \in A \wedge (\forall z < y)(z \in A) = n).$$

All the predicates within brackets are in  $\mathcal{E}^i(\mathcal{P})$  and thus  $I_A$  is representable in Grzegorzczuk normal form. By Proposition 4.1 and Remark 4.2 it follows that  $\mathcal{G}_{I_A} \in \mathcal{E}^i(\mathcal{P})$ .

(ii) If  $i \geq 2$  then the pairing function  $J$  is in  $\mathcal{E}^i$  and hence

$$y \in A \Leftrightarrow (\exists x \leq y) \langle x, y \rangle \in \mathcal{G}_{I_A}$$

since  $I_A$  is an increasing function. Hence  $A \in \mathcal{E}^i(\mathcal{P})$ .

Q.E.D.

It is known that all recursively enumerable sets can be enumerated by primitive recursive functions. More than that, given any recursive function  $f$  there exists a primitive recursive function  $g$  which enumerates the same range and in the same order as  $f$ , although possibly with repetitions. We prove next a similar result for functions in  $\mathcal{E}^0$  instead of primitive recursive functions.

A point  $\langle x + 1, g(x + 1) \rangle$  of  $\mathcal{G}_g$  is called a change of value point if  $g(x) \neq g(x + 1)$ . The function  $g$  which we construct in the next Proposition satisfies the additional requirement that if  $\langle x + 1, g(x + 1) \rangle$  and  $\langle y + 1, g(y + 1) \rangle$  are two points in which  $g$  changes value and if  $x + 1 < y + 1$  then also  $\langle x + 1, g(x + 1) \rangle < \langle y + 1, g(y + 1) \rangle$ . If  $g$  satisfies this requirement, an enumeration in increasing order of the points of  $\mathcal{G}_g$  in which  $g$  changes value will produce these points in the order of increasing arguments of  $g$ .

Proposition 4.6. Let  $f$  be a recursive function. There exists a function  $g \in \mathcal{E}^0$  such that:

(i)  $g$  assumes exactly the values of  $f$  in the same order as  $f$ , but possibly with repetitions.

(ii)  $u < v \wedge g(u + 1) \neq g(u) \wedge g(v + 1) \neq g(v) \Rightarrow \langle u + 1, g(u + 1) \rangle < \langle v + 1, g(v + 1) \rangle$

(iii) The set  $A = \{ \langle u + 1, g(u + 1) \rangle : g(u) \neq g(u + 1) \}$  of points of  $\mathcal{G}_g$  where  $g$  changes value is in  $\mathcal{E}^0$ .

Proof. Assuming the function  $g$  in  $\mathcal{E}^0$  has been constructed, the set  $A$  of (iii) is in  $\mathcal{E}^0$  since

$$\langle u + 1, v \rangle \in A \Leftrightarrow \langle u + 1, v \rangle \in \mathcal{G}_g \wedge v \neq g(u).$$

To prove (i) and (ii) first notice that the graph  $\mathcal{G}_f$  of  $f$  is recursively enumerable. Let  $m$  be a function in  $\mathcal{E}^0$  enumerating  $\mathcal{G}_f$ . Then  $m\ell$  is a function in  $\mathcal{E}^0$  assuming infinitely often each value assumed by  $m$ . Let  $n$  be defined by primitive recursion as follows:  $n(0) = \langle 0, f(0) \rangle$

$$n(u + 1) = \begin{cases} m\ell(u + 1) & \text{if } \ell m\ell(u + 1) = \ell n(u) + 1 \\ & \wedge v = \max\{w < u : rn(w) \neq rn(w + 1)\} \\ & \Rightarrow (\exists t < u + 1)[\ell(t) = v + 1 \\ & \wedge r(t) = rn(v + 1)] \\ n(u) & \text{otherwise} \end{cases}$$

All the predicates in the above definition are in  $\mathcal{E}^0$ . To show that  $n$  is in  $\mathcal{E}^0$  it is therefore enough to place a bound in  $\mathcal{E}^0$  on  $n$ . Since  $m \in \mathcal{E}^0$  there exists, by Proposition 3.1, a constant  $k_1$  such that for all  $x$ ,  $m(x) < x + k_1$ . Let  $k = \max(\langle 0, f(0) \rangle, k_1)$ . Then  $n(0) < 0 + k = k$ . Assuming by induction that  $n(u) < u + k$  we have, by the above definition of  $n(u + 1)$ , either  $n(u + 1) = m\ell(u + 1) < \ell(u + 1) + k < u + 1 + k$  or  $n(u + 1) = n(u) < u + k < u + 1 + k$ . Thus  $\lambda u(u + k)$  is a bound on  $n$  and  $n$  is in  $\mathcal{E}^0$ .

We now claim that  $rn$  is the function  $g$  we need. First,  $g \in \mathcal{E}^0$  since we just showed that  $n \in \mathcal{E}^0$ . Suppose now that for some  $u$ ,  $n(u) = \langle s, f(s) \rangle \in \mathcal{G}_f$ . Let  $v = \max\{w < u : rn(w) \neq rn(w + 1)\}$ . Then  $v$  is the largest point preceding  $u + 1$  at which  $rn$  changes value, i.e.  $rn(v + 1) = rn(u) = f(s)$ . Hence  $n(v + 1) = \langle s, f(s) \rangle$ . If  $n$  is to change value at  $u + 1$  two conditions must be satisfied:

$$(i) \quad \ell n(u) + 1 = s + 1 = \ell m\ell(u + 1), \text{ that is } m\ell(u + 1) = \langle s + 1, f(s + 1) \rangle = n(u + 1).$$

$$(ii) \quad u + 1 > t = \langle v + 1, rn(v + 1) \rangle = \langle v + 1, f(s) \rangle.$$

Hence  $\langle u + 1, rn(u + 1) \rangle = \langle u + 1, f(s + 1) \rangle \geq u + 1 < \langle v + 1, f(s) \rangle$ .

It follows that if  $u + 1$  is a change of value point for  $g = rn$  and, if  $v + 1$  is the largest change of value point preceding it, then  $\langle u + 1, g(u + 1) \rangle < \langle v + 1, g(v + 1) \rangle$ . An immediate induction argument proves (ii). It is also clear from the preceding discussion that whenever  $g$  changes values it assumes a new value of  $f$  and this in the same order in which  $f$  enumerates these values. Furthermore, since  $m\ell$  enumerates each value of  $G_f$  infinitely often a  $u$  satisfying (ii) above is always found and as a consequence  $g$  enumerates each value of  $f$  at least once. This terminates the proof.

Q.E.D.

Sets enumerable by one-one honest functions admit the following useful characterization.

Proposition 4.7. A recursive set  $X$  is enumerable by a one-one primitive recursive function if and only if there exists an infinite primitive recursive set  $G$  such that  $G \subseteq X$ .

Proof. Suppose  $X \supseteq G$ , where  $G$  is a primitive recursive set. Let  $A$  be a primitive recursive set such that  $r(A) = X - G$  and  $r$  is one-one on  $A$  and define  $f$  as follows:

$$f(n) = \begin{cases} r(n) & \text{if } n \in A \\ I_G v_{\bar{A}}(n) & \text{if } n \in \bar{A} \end{cases}$$

$f$  is obviously one-one and enumerates  $X$ .  $I_G$  is honest by Proposition 4.5. Since

$$\langle u, v \rangle \in \mathcal{G}_f \leftrightarrow (u \in A \wedge v = r(u)) \vee (u \notin A \wedge v = h \vee_{\bar{A}}(u))$$

$f$  is honest.

Conversely, let  $f$  be a one-one honest function and let  $X$  be the range of  $f$ . Since  $f$  is one-one there exist infinitely many elements  $x$  such that  $f(x) \geq x$ . Let  $A = \{x : f(x) \geq x\}$  and let  $G = f(A)$ .  $G$  is primitive recursive since

$$y \in G \leftrightarrow \exists x \leq y (f(x) = y).$$

Q.E.D.

## 5. SOME RESULTS ON RECURSIVE SETS

We use this section mainly as a garbage collector.

Theorem 5.3 was an important tool in earlier proofs of the results of Section 8. Although we now possess simpler proofs of those results, Theorem 5.3 is of interest by itself.

Proposition 5.1. Let  $f$  be a function in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) and  $A$  a set in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ). Then  $f^{-1}(A)$  is also a set in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ).

Proof. Evident.

The converse of Proposition 5.1 is false. In fact

Proposition 5.2. Given any recursive set  $X$  there exists a set  $G$  in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) such that  $r(G) = X$  and  $r$  is strictly increasing on  $G$ , ( $r$  is the standard right projection; a similar result holds for the left projection.)

Proof. Since  $X$  is recursive its increasing enumeration  $I_X$  is also recursive. By Proposition 4.6 there exists a function  $g$  in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) such that  $g$  enumerates  $X$  nondecreasingly although with repetitions and that the set  $G = \{ \langle u + 1, g(u + 1) \rangle : g(u) \neq g(u + 1) \}$  of points of  $\mathcal{G}_g$  where  $g$  changes value is in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ). Moreover, Proposition 4.6 ensures that  $r(I_G(n)) = I_X(n)$ . The set  $G$  is our required set.

Q.E.D.

The previous result has an obvious generalization. Instead of asking  $r$  to be increasing on  $G$ , we can ask that  $r(I_G(n)) = f(n)$ ,

where  $f$  is some arbitrary one-one function enumerating the recursive set  $X$ . This could easily be proved by an appropriate use of Proposition 4.6 in the previous proof. In a sense the set  $G$  is a primitive recursive mirror of the recursive set  $X$  and one can pass in a primitive recursive fashion from  $G$  to  $X$  by using the projection  $r$ . Our next goal is to prove a further refinement of this result. Let  $X$  be a given recursive set. We shall show that we can find a primitive recursive set  $H$  and a primitive recursive subset  $G$  and  $H - G$  such that  $r(H) = \mathcal{N}$  and  $r(G) = X$  and that  $r$  increases on both  $G$  and  $H - G$ . If  $H = \{x_0 < x_1 < x_2 \dots\}$  then  $G$  will consist the elements  $x_{I_X(0)}, x_{I_X(1)}, \dots$ . Thus not only is  $G$  a primitive recursive mirror of  $X$ , but its elements are positioned with respect to the elements of  $H$  in exactly the same way in which the elements of  $X$  are positioned with respect to the elements of  $\mathcal{N}$ . This time we state the theorem in its most general form by showing that  $H$  and  $G$  can even be chosen in  $\mathcal{E}^0$  and that instead of  $r$  we can choose a function in  $\mathcal{E}^0$  which maps  $I_G(n)$  onto  $f_X(n)$  and  $I_{H-G}(n)$  onto  $f_{\bar{X}}(n)$  where  $f_X$  and  $f_{\bar{X}}$  are two arbitrary one - one enumerations of  $X$  and  $\bar{X}$  respectively.

Theorem 5.3. Let  $X$  and  $Y$  be two recursive sets such that  $X = \bar{Y}$ . Let  $f_X, f_Y$  be two recursive one - one enumerations of  $X$  and  $Y$  respectively. Then there exist sets  $G$  and  $H$  in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) and a function  $t \in \mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) such that

(i)  $G \subseteq H$ .

(ii)  $H, \bar{H}, G$  and  $H - G$  are infinite.

$$(iii) \quad G = \{x \in H : v_H(x) \in X\}.$$

$$(iv) \quad t \text{ is one - one on } H \text{ and } t(G) = X, \quad t(H) = \mathcal{A}.$$

$$(v) \quad x \in G \Rightarrow t(x) = f_X(v_G(x))$$

$$x \in H - G \Rightarrow t(x) = f_Y(v_{H-G}(x)).$$

Proof. Let  $I'_X, f'_X, I'_Y, f'_Y$  be the functions given by Proposition 4.6 which enumerate the same range as  $I_X, f_X, I_Y, f_Y$  respectively.

Let A,B,C,D be the corresponding sets given by Propositions 4.6 i.e.

$$A = \{ \langle 0, I'_X(0) \rangle \} \cup \{ \langle u+1, I'_X(u+1) \rangle : I'_X(u+1) \neq I'_X(u) \}$$

$$B = \{ \langle 0, f'_X(0) \rangle \} \cup \{ \langle u+1, f'_X(u+1) \rangle : f'_X(u+1) \neq f'_X(u) \}$$

$$C = \{ \langle 0, I'_Y(0) \rangle \} \cup \{ \langle u+1, I'_Y(u+1) \rangle : I'_Y(u+1) \neq I'_Y(u) \}$$

$$D = \{ \langle 0, f'_Y(0) \rangle \} \cup \{ \langle u+1, f'_Y(u+1) \rangle : f'_Y(u+1) \neq f'_Y(u) \}$$

By Proposition 4.5 and 4.6 A,B,C and D are sets in  $\mathcal{E}^i(\mathcal{P})$

( $i \geq 0$ ) and their increasing enumerations  $I_A, I_B, I_C, I_D$  have graphs in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ). Also  $I_A(n) = \langle u, I'_X(n) \rangle$ ,  $I_B(n) = \langle v, f'_X(n) \rangle$ ,  $I_C(n) = \langle w, I'_Y(n) \rangle$ ,  $I_D(n) = \langle y, f'_Y(n) \rangle$  for some  $u, v, w, y$ . Let  $h$  be an increasing function whose graph  $H$  is in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) and dominates  $I_A, I_B, I_C, I_D$ . The following facts are immediate:

$$\begin{aligned} I_H(n) &= \langle n, h(n) \rangle, \quad I\mathcal{G}_{I_A}(n) = \langle n, I_A(n) \rangle, \quad I\mathcal{G}_{I_B}(n) \\ &= \langle n, I_B(n) \rangle, \quad I\mathcal{G}_{I_C}(n) = \langle n, I_C(n) \rangle, \quad I\mathcal{G}_{I_D}(n) = \langle n, I_D(n) \rangle \end{aligned}$$

$$h(n) > I_A(n), \quad h(n) > I_B(n), \quad h(n) > I_C(n), \quad h(n) > I_D(n)$$

$$I_H(n) > I\mathcal{G}_{I_A}(n), \quad I\mathcal{G}_{I_B}(n), \quad I\mathcal{G}_{I_C}(n), \quad I\mathcal{G}_{I_D}(n)$$

$$\begin{aligned} rI_A(n) &= I_X(n), \quad rI_B(n) = f_X(n), \quad rI_C(n) = I_Y(n), \quad rI_D(n) \\ &= f_Y(n) \end{aligned}$$

Let  $G = \{x \in H : (\exists y < x)(y \in \mathcal{G}_{I_A} \wedge v_H(x) = rr(y))\}$ .

Since  $H$  is in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) and  $G$  is defined by bounded quantifiers and propositional connectives from predicates in  $\mathcal{E}^i(\mathcal{P})$  it follows that  $G \in \mathcal{E}^i(\mathcal{P})$ .

Claim:  $G = \{x \in H : v_H(x) \in X\}$ .

Proof of the claim.  $x \in G \Rightarrow x \in H \wedge v_H(x) = rr(y)$  for some  $y \in \mathcal{G}_{I_A}$ ,  $y < x$ . But by the previous facts if  $y \in \mathcal{G}_{I_A}$  then  $y = \langle n, I_A(n) \rangle$  for some  $n$ . Hence  $r(y) = I_A(n)$ . By an earlier remark,  $I_A(n) = \langle u, I_X(n) \rangle$ , for some  $u$  and therefore  $rr(y) = I_X(n)$ . Conversely, let  $x \in H$  such that  $v_H(x) = n \in X$ . Since  $h$  dominates  $I_A$  and since  $h$  is an increasing function, we must have

$$x = I_A(n) = \langle n, h(n) \rangle > \langle n, I_A(n) \rangle = I_{\mathcal{G}_{I_A}}(n)$$

$$rr(I_{\mathcal{G}_{I_A}}(n)) = r(I_A(n)) = I_X(n).$$

Hence if  $x \in H$  and  $v_H(x) \in X$  then  $x \in G$ . It follows that  $H - G = \{x \in H : v_H(x) \in Y\}$ . Since both  $X$  and  $Y = \bar{X}$  are infinite by hypothesis so must  $G$  and  $H - G$  be. We define  $t$  as follows:

$$t(x) = \begin{cases} rr(y) & \text{if } x \in G \text{ and } y = \mu z < x [z \in \mathcal{G}_{I_B} \wedge v_{\mathcal{G}_{I_B}}(z) \\ & = v_G(x)] \\ rr(y) & \text{if } x \in H-G \text{ and } y = \mu z < x [z \in \mathcal{G}_{I_D} \wedge v_{\mathcal{G}_{I_D}}(z) \\ & = v_{H-G}(x)] \\ 0 & \text{if } x \notin H \end{cases}$$

We claim that  $t$  is well defined and in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ).

First notice that  $t$  is defined by bounded quantifiers and logical connectives from predicates in  $\mathcal{E}^i(\mathcal{P})$ . Secondly, assuming  $t$  well defined, we must have  $t(x) \leq x$ , i.e.  $t$  is bounded by the identity.

To show that  $t$  is well defined, suppose that  $x \in G$  and  $v_G(x) = n$ . Since  $I_G(n) \geq I_H(n) > I_{\mathcal{G}_{I_A}}(n), I_{\mathcal{G}_{I_B}}(n)$ , it follows that for each  $x \in G$  there exists a unique  $y \in \mathcal{G}_{I_B}$  such that  $v_{\mathcal{G}_{I_B}}(y) = v_G(x)$  and, moreover, such a  $y$  is smaller than  $x$ . Similarly, if  $x \in H - G$  and  $v_{H-G}(x) = n$  it follows that there exists a unique  $z \in \mathcal{G}_{I_D}$  such that  $v_{\mathcal{G}_{I_D}}(z) = v_{H-G}(x)$ . Thus we have shown that  $t$  is well defined.

Also, if  $x \in G$  and  $v_G(x) = n$  then the unique  $y \in \mathcal{G}_{I_B}$  such that  $v_{\mathcal{G}_{I_B}}(y) = n$  is such that  $rr(y) = f_X(n)$ . Therefore if  $x \in G$  then  $t(x) = f_X(v_G(x))$ . One shows similarly that if  $x \in H - G$  then  $t(x) = f_Y(v_{H-G}(x))$ . This completely proves the theorem.

Q.E.D.

## 6. ENUMERATION OF RECURSIVE SETS

We collect under this heading a number of results concerning recursive sets enumerated by one - to - one primitive recursive functions or by one - to - one functions in one of the Grzegorzczk classes.

Proposition 6.1. Let  $f \in \mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) be such that  $f(x) \geq x$  for all  $x$ . Then  $Rg(f) \in \mathcal{E}^i(\mathcal{P})$ .

Proof.  $y \in Rg(f) \Leftrightarrow \exists x \leq y (y = f(x))$ . The predicate within brackets is in  $\mathcal{E}^i(\mathcal{P})$ .

Q.E.D.

Corollary 6.2. If  $f \in \mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) is increasing then  $Rg(f) \in \mathcal{E}^i(\mathcal{P})$ .

Proof. Any increasing function is such that  $f(x) \geq x$  for all  $x$ .

Q.E.D.

The converse of this Corollary is not true.

Proposition 6.3. There exists a set  $A \in \mathcal{E}^0$  whose increasing enumeration is not in  $\mathcal{E}^0$  and which in fact is not even primitive recursive.

Proof. Let  $g$  be a function as in Proposition 4.4 and let  $A = \mathcal{G}_g$ . By hypothesis  $g$  is not primitive recursive and  $A \in \mathcal{E}^0$ . Since  $g$  is strictly increasing  $I_A(n) = \langle n, g(n) \rangle$ , and by Proposition 3.3  $rI_A(n) = g(n)$ . Hence  $I_A$  cannot be primitive recursive for if it were  $g$  would also be primitive recursive.

Contradiction.

Q.E.D.

Proposition 6.4. A set  $A \in \mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) is enumerated by a one - one function in  $\mathcal{E}^i(\mathcal{P})$  if and only if  $I_A \in \mathcal{E}^i(\mathcal{P})$ .

Proof. The "if" part is trivial.

Suppose on the other hand that  $I_A \notin \mathcal{E}^i(\mathcal{P})$  but that  $f \in \mathcal{E}^i(\mathcal{P})$  is a one - one function such that  $Rg(f) = A$ . Let  $g(x) = \max_{i \leq x} f(i)$ . We claim that  $g \in \mathcal{E}^i(\mathcal{P})$ . For let  $h$  be defined as follows:

$$h(x) = \mu t \leq x (\forall s \leq x) (f(s) \leq f(t)).$$

Then  $h \in \mathcal{E}^i(\mathcal{P})$ , being defined by bounded minimization and bounded quantification from predicates in  $\mathcal{E}^i(\mathcal{P})$  and being bounded by the identity. Hence  $g(x) = f(h(x))$  also belongs to  $\mathcal{E}^i(\mathcal{P})$ .  $g$  takes values in  $A$  and, since  $f$  is one - one by hypothesis, the set  $\{0, 1, \dots, g(x)\}$  contains at least  $x + 1$  elements of  $A$ . Now set

$$k(0) = \mu y \leq g(0) (c_A(y) = 0)$$

$$k(x + 1) = \mu y \leq g(x + 1) (c_A(y) = 0 \wedge y > k(x))$$

$$k(x) \leq g(x)$$

where  $c_A$  is the representing function of  $A$ .  $k$  is defined by bounded primitive recursion from functions and predicates in  $\mathcal{E}^i(\mathcal{P})$  and belongs therefore to  $\mathcal{E}^i(\mathcal{P})$ . By the above remark  $k$  is well defined and increasingly enumerates  $A$  contradicting our assumption.

Q.E.D.

Corollary 6.5. There exist sets in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) which

are not enumerated by any one - one function in  $\mathcal{P}$ .

That there exist recursive sets such as this was already known (see [7], p.140, Problem 9, where it is shown that the range of the Ackermann exponential is such a set).

We now characterize the recursive sets that can be enumerated by a one - one primitive recursive function. In view of Proposition 6.4 the following definition is useful.

Definition 6.6. A set is called strongly primitive recursive if its increasing enumeration  $I_A$  is primitive recursive. Similarly  $A$  is strongly in  $\mathcal{E}^i$  ( $i \geq 0$ ) if  $I_A \in \mathcal{E}^i$ .

Proposition 6.7. A set  $A$  is enumerated by a one - one function in  $\mathcal{E}^i(\mathcal{P})$  ( $i \geq 0$ ) if and only if  $A \supseteq B$  where  $B$  is strongly in  $\mathcal{E}^i$  (strongly primitive recursive).

Proof. Necessity. Let  $f \in \mathcal{E}^i(\mathcal{P})$  be a one - one function and  $Rg(f) = A$ . We construct a strictly increasing function  $h$  such that  $Rg(h) = B \subseteq A$ . Let  $g(x) = \max_{y \leq x} f(y)$ . By the same argument as in Proposition 6.4,  $g \in \mathcal{E}^i(\mathcal{P})$ . Define first a function  $k$  as follows:

$$k(0) = \mu y \leq g(0) (\forall z \leq g(0)) (f(z) \geq f(y))$$

$$k(n+1) = \mu y \leq g(n+1) [f(y) > f(k(n)) \wedge (\forall z \leq g(n+1)) (f(z) > f(k(n)) \Rightarrow f(z) \geq f(y))]$$

$$k(n) \leq g(n)$$

$k$  is defined by primitive recursion and is therefore in  $\mathcal{E}^i(\mathcal{P})$ .

Set now  $h = fk$ . Then  $h \in \mathcal{E}^i(\mathcal{P})$ .  $Rg(h) \subseteq Rg(f) = A$ . It remains

to show that  $h$  is indeed increasing. The argument that follows is typical of a class of counting arguments which will be repeatedly used. We proceed by induction.

$n = 0$ . Since  $f$  is one - one  $\{f(0), f(1), \dots, f(g(0))\}$  contains at least one element  $\geq f(0) = g(0)$ . Two cases may occur:

Case 1.  $\max\{f(0), f(1), \dots, f(g(0))\} = \min\{f(0), f(1), \dots, f(g(0))\}$ .

Then  $f(0), f(1), \dots, f(g(0))$  has just one element, i.e.  $f(0) = f(g(0))$ . This is possible only if  $g(0) = 0$  and hence  $f(0) = 0$ . In this case  $f(1) > f(0)$  and hence among  $f(0), f(1), \dots, f(g(1))$  there must be at least one element  $> f(0)$ . This ensures that  $f(k(1)) > f(k(0))$ .

Case 2.  $\{f(0), f(1), \dots, f(g(0))\}$  has at least two elements.  $f(k(0))$  is the smallest of them and there exists an element  $z > f(k(0))$  among  $f(0), f(1), \dots, f(g(1))$ .

$n \geq 1$ . We assume the induction hypothesis that  $k(0) \leq g(0)$ ,  $k(1) \leq g(1), \dots, k(n) \leq g(n), f(k(0)) < f(k(1)) < \dots < f(k(n))$ .

Again two cases may occur:

Case 1.  $\{f(0), f(1), \dots, f(g(n))\}$  has just  $n + 1$  elements. This can only happen when  $g(n) = n$  and hence, since  $f$  is one - one,  $f(n + 1) > f(n)$ . Since  $n + 1 \leq g(n + 1)$ ,  $f(n + 1) \in \{f(0), \dots, f(g(n + 1))\}$  and thus  $k(n+1)$  can be found which satisfies our claim.

Case 2.  $\{f(0), f(1), \dots, f(g(n))\}$  has  $> n + 1$  elements. Suppose for reductio ad absurdum that there is no  $x \leq g(n + 1)$  such that  $f(x) > f(k(n))$ . But  $k(0), k(1), \dots, k(n) \in \{0, 1, \dots, g(n)\}$ . By definition of  $k(n)$  and  $k(n - 1)$  it follows that  $x \neq k(0) \wedge x \neq k(1) \wedge \dots \wedge x \neq k(n) \wedge x \leq g(n) \Rightarrow f(x) < f(k(n - 1)) \wedge x > g(n - 1)$ .

Therefore  $\{0, 1, \dots, g(n)\} = \{k(0), k(1), \dots, k(n)\} \cup \{x : x \neq k(n) \wedge g(n - 1) < x \leq g(n)\}$ . Also  $k(n) > g(n - 1)$ , for if  $k(n) \leq g(n - 1)$

then  $g(n) \geq x > g(n-1) \Rightarrow f(x) > f(k(n))$  contradicting our hypothesis. Therefore  $\{0,1,\dots,g(n-1)\} = \{k(0),k(1),\dots,k(n-1)\}$  and hence  $g(n-1) = n-1$ . As before we can now distinguish two subcases:

Subcase 2.1.  $g(n) = n$ . Then  $f(n+1) = n > f(n-1)$  and  $k(n+1)$  can be found satisfying our requirements. Contradiction.

Subcase 2.2.  $g(n) > n$ . Then  $k(n)$  is such that  $f(k(n))$  is the smallest  $z$  among  $f(0),f(1),\dots,f(g(n))$  such that  $z > f(k(n-1))$  and there is at least another candidate for  $k(n+1)$  among these elements. Contradiction.

Sufficiency. Let  $A \supseteq B$  and  $I_B \in \mathcal{E}^i(\mathcal{P})$ . By Proposition 5.2 there exists a set  $G \in \mathcal{E}^i(\mathcal{P})$  such that  $r(G) = A - B$  is where  $r$  is our standard first projection. We can assume that  $r$  one - one on  $G$ . Define  $f$  by

$$f(n) = \begin{cases} r(n) & \text{if } n \in G \\ I_B(v_{\bar{G}}(n)) & \text{if } n \notin G \end{cases}$$

$f$  is clearly in  $\mathcal{E}^i(\mathcal{P})$ . It is immediate that  $f$  is one - one and enumerates  $A$ .

Q.E.D.

The intuitive content of the previous Proposition is that sets enumerated by one - one functions in  $\mathcal{E}^i$  cannot be very sparse. More precisely, the increasing enumeration  $I_A$  of such a set  $A$  does not dominate all primitive recursive functions since if  $A \supseteq B$  and  $I_B \in \mathcal{E}^i$  then  $I_A(n) \leq I_B(n)$  for infinitely many  $n$ .

There exist recursive sets  $A$  which are not primitive

recursive and such that both  $A$  and  $\bar{A}$  are enumerated by one - one functions in  $\mathcal{E}_1^i$ . An instance of such a set is  $A = 2X \cup (4\mathcal{N} + 1)$  and  $\bar{A} = 2\bar{X} \cup (4\mathcal{N} + 3)$ , where  $X$  is some recursive and not primitive recursive set. By the criterion offered by Proposition 6.7 both  $A$  and  $\bar{A}$  are enumerated by one - one functions in  $\mathcal{E}^1$ .

Intuitively, a set can be considered very sparse if its increasing enumeration dominates every primitive recursive function. For example the range of the Ackermann exponential is in this sense very sparse. The next Proposition shows that if a set is primitive recursive then either the set or its complement are not very sparse and, even more, one of them can be enumerated by a one - one primitive recursive function.

Proposition 6.8. Let  $G \in \mathcal{E}^i(\mathcal{P})$  ( $i \geq 3$ ) be a set. Suppose that  $I_G$  dominates all functions in  $\mathcal{E}^i(\mathcal{P})$ . Then  $\bar{G}$  has a one - one enumeration in  $\mathcal{E}^i(\mathcal{P})$ .

Proof. We shall prove the theorem for  $i = 3$ . The same proof will work for all  $\mathcal{E}^i$  and for  $\mathcal{P}$ . By Proposition 6.7 it is enough to show that  $\bar{G} \supseteq B$  and  $I_B \in \mathcal{E}^3$ .

Since  $I_G$  dominates all functions of  $\mathcal{E}^3$  it dominates  $\lambda n(2n)$ . Thus there exists an  $m$  such that for  $n > m$  we have  $I_G(n) > 2n$ . Hence for  $n > m$ ,  $G$  possesses not more than  $n$  elements in  $\{0, 1, \dots, 2n\}$ . Suppose now that  $x \in G$ ,  $v_G(x) = k$  and  $k > m$ . Thus in the set  $\{0, 1, \dots, x\}$  there are exactly  $k + 1$  elements of  $G$ .

We now claim that the set  $\{0, 1, \dots, x + (x - 2k + 2)\}$  contains at least one element of  $G$  which is  $> x$ . For, suppose to the contrary that among  $x + 1, x + 2, \dots, 2x - 2k + 2$  there is no element of  $\bar{G}$  which does not already appear in  $\{0, 1, \dots, x\}$ . Then

the set  $\{0, 1, \dots, 2x - 2k + 2\}$  has  $2x - 2k + 3 - (x + 1) + (k + 1) = x - k + 3$  elements in  $G$ . But by our hypothesis there are at most  $x - k + 1$  such elements. This contradiction proves the claim.

Let now  $x_0 \in G$  be such that  $v_G(x_0) > m$  and define  $f$  as follows:

$$f(0) = x_0$$

$$f(n+1) = \begin{cases} f(n) + 1 & \text{if } f(n) + 1 \in \bar{G} \\ \text{any } (f(n) < y \leq 2f(n) - 2k + 2) \text{ where } k = v_G(f(n)+1) \\ & \text{if } f(n) + 1 \in G \end{cases}$$

$$f(n) \leq 2^n x_0$$

$f \in \mathcal{C}^3$  and increasingly enumerates the set  $B \subseteq \bar{G}$  we need.

Q.E.D.

The sets enumerated by one - one functions in  $\mathcal{C}^0$  admit a remarkable characterization.

Proposition 6.9. If  $f \in \mathcal{C}^0$  and  $f$  is one - one, the range of  $f$  is cofinite.

Proof. By Proposition 3.1 there exists a constant  $k$  such that for all  $n$ ,  $f(n) < n + k$ . Suppose that  $Rg(f)$  is co - infinite. Let  $x_0, x_1, \dots, x_k$  be the first  $k$  elements of  $\mathcal{N} - Rg(f)$  and let  $n$  be big enough that  $\{f(0), \dots, f(n)\}$  contains all elements  $\leq x_k$  of  $Rg(f)$ . The  $\{f(0), \dots, f(n)\}$  must contain all element  $p \geq n + k$ . But for  $i \leq n$  we have  $f(i) < i + k \leq n + k$  and hence  $p < n + k$ . Contradiction.

Q.E.D.

Corollary 6.10. There exists no recursive set such that both the set and its complement are infinite and are enumerated by one - one functions in  $\mathcal{E}^0$ .

## 7. GENERATORS FOR THE GROUP OF RECURSIVE PERMUTATIONS

The recursive permutations form a multiplicative group when multiplication is interpreted as the composition of functions and the inverse as the inverse function. We shall denote this group by  $\mathbb{R}$ . Throughout this section we shall restrict our attention to the case of  $\mathcal{E}^1$ . Our results and our proofs remain unchanged in the case of  $\mathcal{E}^i (i > 1)$  or of  $\mathcal{P}$ .

Let us denote by  $\mathbb{P}_n$  the set of permutations of the form  $\pi_n^{-1} \pi_{n-1}^{-1} \pi_{n-2}^{-1} \cdots \pi_2^{-1} \pi_1^{-1}$  when  $n$  is even and of the form  $\pi_n \pi_{n-1}^{-1} \pi_{n-2}^{-1} \cdots \pi_2^{-1} \pi_1^{-1}$  when  $n$  is odd, where  $\pi_i \in \mathcal{E}^1$ . Analogously, let us denote by  $\mathbb{P}'_n$  the set of permutations of the form  $\pi_n \pi_{n-1}^{-1} \pi_{n-2}^{-1} \cdots \pi_2^{-1} \pi_1^{-1}$  when  $n$  is even and of the form  $\pi_n^{-1} \pi_{n-1}^{-1} \pi_{n-2}^{-1} \cdots \pi_2^{-1} \pi_1^{-1}$  when  $n$  is odd. Thus the permutations of  $\mathcal{E}^1$  are precisely the permutations of  $\mathbb{P}_1$  and their inverses are the permutations of  $\mathbb{P}'_1$ . We shall sometimes say that a permutation is of length  $n$  if it belongs to  $\mathbb{P}_n$  or to  $\mathbb{P}'_n$ .

**Proposition 7.1.** The permutations of  $\mathcal{E}^1$  do not form a group.

**Proof.**  $\mathbb{P}_1$  is closed under composition and hence we have to show that it is not closed under inverses.

Let  $G \in \mathcal{E}^1$  be a set whose increasing enumeration  $I_G$  dominates all primitive recursive functions.  $G$  can be chosen infinite and co-infinite (see Proposition 4.5). Now define  $\pi$  as follows:

$$\pi(x) = \begin{cases} 2v_G(x) & \text{if } x \in G \\ 2v_{\bar{G}}(x) + 1 & \text{if } x \in \bar{G} \end{cases}$$

Since  $G \in \mathcal{E}^1$  we have  $\pi \in \mathcal{E}^1$  and since  $G$  is infinite and co-infinite  $\pi$  is a permutation. Now notice that  $\pi^{-1}(2n) = I_G(n)$ . Hence if  $\pi^{-1}$  belonged to  $\mathcal{E}^1$  so would  $I_G$  contradicting our hypothesis.

Q.E.D.

Thus the inverse of a permutation in  $\mathcal{E}^1$  can grow extremely fast on a set whose increasing enumeration is in  $\mathcal{E}^1$ .

The functions of  $\mathcal{E}^1$  are recursively enumerable in the following sense. If  $\{\phi_i\}_{i \in \mathcal{N}}$  is an acceptable Godel numbering of all the partial recursive functions [12, Exercise 2-10], there exists a total recursive function  $\sigma$  such that  $\mathcal{E}^1 = \{\phi_{\sigma(i)} : i \in \mathcal{N}\}$  [7,9]. The next result shows that no matter what recursively enumerable class of total functions we may choose the permutations of length 5 generated by this class do not exhaust the recursive permutations.

Theorem 7.2 (Blum). Let  $\mathcal{C} = \{\phi_{\sigma(i)} : i \in \mathcal{N}\}$  be a recursively enumerable class of total recursive functions. There exists a recursive permutation different from all the permutations of length 5 generated by the class.

Proof. Let  $\tau$  be a total recursive functions enumerating all quintuples  $\langle i_1, i_2, i_3, i_4, i_5 \rangle$  of indices  $i_k$  ( $1 \leq k \leq 5$ ) enumerated by  $\sigma$ . Our goal is to construct a recursive permutation that will differ from all the permutations of the form

$\pi_5^{-1}\pi_4^{-1}\pi_3^{-1}\pi_2^{-1}\pi_1^{-1}$  or  $\pi_5^{-1}\pi_4^{-1}\pi_3^{-1}\pi_2^{-1}\pi_1^{-1}$ , where the  $\pi_i$ 's are permutations in  $\mathcal{C}$ . We describe the computation of  $\pi$  in the following informal procedure for enumerating the graph of  $\pi$ . The computation will keep two lists of quintuples as enumerated by  $\tau$  and will proceed in stages.

Stages n. Using  $\tau$ , append to the bottom of each of the two lists a quintuple that does not already appear in it. Let  $x$  be the smallest element that has not as yet been placed in the domain of  $\pi$  and  $y$  the smallest element that has not as yet been placed in the range of  $\pi$ .

Substage 1(2). Examine in order all the quintuples of the first (second) list. Find the quintuple closest to the top of the list for which there exists  $z \leq x$  ( $z \leq y$ ) such that  $\pi_2(z) = \pi_1(x)$  ( $\pi_4(z) = \pi_5(y)$ ) (For simplicity of notation we denote  $\phi_{i_1, \dots, i_k}$  by  $\pi_k$  if  $\langle i_1, i_2, i_3, i_4, i_5 \rangle$  is the quintuple under consideration). If there is no quintuple satisfying the above conditions go to Substage 2 (the next stage). When and if such a quintuple is found, look for the smallest  $u$  such that  $\pi_4(u) \neq \pi_3(z)$  ( $\pi_2(u) \neq \pi_3(z)$ ) and such that  $\pi_5(u)$  ( $\pi_1(u)$ ) has not as yet been placed in the range (domain) of  $\pi$ . When such a  $u$  is found, place the pair  $\langle x, \pi_5(u) \rangle$  ( $\langle y, \pi_1(u) \rangle$ ) in the graph of  $\pi$  and delete the quintuple from the first (second) list. If during the search for  $u$  it is found that  $\pi_4(\pi_2)$  or  $\pi_5(\pi_1)$  take the same value for different arguments delete the quintuple from the list and proceed again at the beginning of the substage.

To prove the theorem, let  $\pi_1, \pi_2, \pi_3, \pi_4, \pi_5$  be permutations in  $\mathcal{C}$ , and assume that at stage  $n_0$  a quintuple of indices for

these permutations has been placed on the list. Since  $\pi_1$  and  $\pi_2$  are permutations, there exist infinitely many pairs  $(x, z)$  such that  $\pi_2(z) = \pi_1(x)$  and  $z \leq x$ , for otherwise, as can easily be seen by induction,  $\pi_2^{-1} \pi_1$  would not be onto. Thus during Substage 1 the search for  $z$  has infinitely many opportunities to succeed.

After our quintuple has appeared on the list there must be a stage at which it will be the quintuple closest to the top of the list for which such a  $z$  is found. Indeed there are only finitely many quintuples preceding the one under consideration and, once a  $z$  has been found for a quintuple, that quintuple is altogether eliminated from the list. Assuming now that the quintuple is the closest to the top for which  $z$  is found,  $\pi_3(z)$  has a certain value. Since  $\pi_4$  and  $\pi_5$  are permutations and only finitely many elements were so far placed in the range of  $\pi$ ,  $u$  must be found such that  $\pi_4(u) \neq \pi_3(z)$  and such that  $\pi_5(u)$  has not as yet occurred in the range of  $\pi$ . The search for this  $u$  is made by successively computing  $\pi_4(0), \pi_4(1), \dots, \pi_5(0), \pi_5(1), \dots$ . During this search it may be found that  $\pi_4$  or  $\pi_5$  are not one-one which also results in their deletion. This possibility must be taken into consideration as in general  $\mathcal{C}$  does not consist only of permutations. As a matter of fact in the cases which interest us it most certainly will not contain only permutations since it can be shown that the permutations of  $\mathcal{E}^1$  are not recursively enumerable. However if  $\pi_1, \dots, \pi_5$  are permutations then  $\pi_5 \pi_4^{-1} \pi_3 \pi_2^{-1} \pi_1^{-1} \pi_1(x) \neq \pi_5(u)$ . By our construction, though,  $\pi(x) = \pi_5(u)$  and hence we have succeeded in making  $\pi \neq \pi_5 \pi_4^{-1} \pi_3 \pi_2^{-1} \pi_1$ .

It is similarly seen that Substage 2 of our construction will make  $\pi \neq \pi_5^{-1} \pi_4 \pi_3^{-1} \pi_2 \pi_1^{-1}$ . It is immediate from the construction that  $\pi$  is one-one. Finally, since Substage 1 places all integers in the domain while Substage 2 does the same for the range it follows that  $\pi$  is a permutation.

Q.E.D.

Corollary 7.3.  $\mathbb{R} = \mathbb{P}_5$  and  $\mathbb{R} \neq \mathbb{P}_5'$ .

All attempts to generalize Theorem 7.2 to numbers larger than 5 have failed. The reason is that, as shown by our next theorem,  $\mathbb{R} = \mathbb{P}_6'$ . This came as a surprise since even if the permutations of  $\mathcal{E}^1$  generate  $\mathbb{R}$  it is not a priori clear that a bound can be placed on the number of permutations needed to generate an arbitrary recursive one.

Theorem 7.4.  $\mathbb{R} = \mathbb{P}_6'$ .

Proof. The inclusion  $\mathbb{P}_6' \subseteq \mathbb{R}$  is by definition. To show the converse let  $\pi$  be an arbitrary recursive permutation. Let  $\pi(2\mathcal{N}) = X$  and  $\pi(2\mathcal{N}+1) = \bar{X}$ . Let  $A \in \mathcal{E}^1$  be a set such that both  $I_A$  and  $I_{\bar{A}}$  are in  $\mathcal{E}^1$  and  $A \cap X, \bar{A} \cap X, A \cap \bar{X}, \bar{A} \cap \bar{X}$  are infinite. The graph  $\mathcal{G}_\pi$  of  $\pi$  is a recursive set. Let  $G$  be a set in  $\mathcal{E}^1$  such that  $r(G) = \mathcal{G}_\pi$  and that  $r$  is increasing on  $G$ . It follows that  $G$  is infinite and co-infinite. Such a set  $G$  can be found by Proposition 5.2. To every pair  $(x,y)$  of natural numbers such that  $y = \pi(x)$  there corresponds exactly one element  $z \in G$  such that  $x = l(r(z))$  and  $y = r(r(z))$ . Let us set  $a(z) = l(r(z))$  and  $v(z) = r(r(z))$ . The functions  $a$  and  $v$  are obviously in  $\mathcal{E}^1$ . Since  $l$  and  $r$  are one-one on  $\mathcal{G}_\pi$  so are  $a$  and  $v$  on  $G$ .

The set  $G$  is the union of the following four disjoint sets:

$$H_1 = \{z \in G : a(z) \in 2\mathcal{N} \wedge v(z) \in A\}$$

$$H_2 = \{z \in G : a(z) \in 2\mathcal{N} \wedge v(z) \in \bar{A}\}$$

$$K_1 = \{z \in G : a(z) \in 2\mathcal{N} + 1 \wedge v(z) \in A\}$$

$$K_2 = \{z \in G : a(z) \in 2\mathcal{N} + 1 \wedge v(z) \in \bar{A}\}$$

Since both  $G$  and  $A$  are in  $\mathcal{E}^1$  so are  $H_1, H_2, K_1$  and  $K_2$ .

We now define functions  $\pi_i (1 \leq i \leq 6)$  as follows:

$$\pi_1(x) = \begin{cases} a(x) & \text{if } x \in K_1 \cup K_2 \\ 2v_{\overline{K_1 \cup K_2}}(x) & \text{if } x \in \overline{K_1 \cup K_2} \end{cases}$$

$$\pi_2(x) = \begin{cases} 3v_{\overline{K_1 \cup K_2}}(x) & \text{if } x \in \overline{K_1 \cup K_2} \\ 3v_{K_1}(x) + 1 & \text{if } x \in K_1 \\ 3v_{K_2}(x) + 2 & \text{if } x \in K_2 \end{cases}$$

$$\pi_3(x) = \begin{cases} \left\lfloor \frac{3a(x)}{2} \right\rfloor & \text{if } x \in H_1 \cup H_2 \\ 3v_{\overline{H_1 \cup H_2 \cup K_2}}(x) + 1 & \text{if } x \in \overline{H_1 \cup H_2 \cup K_2} \\ 3v_{K_2}(x) + 2 & \text{if } x \in K_2 \end{cases}$$

$$\pi_4(x) = \begin{cases} I_A(2v_{H_1}(x)) & \text{if } x \in H_1 \\ v(x) & \text{if } x \in H_2 \cup K_2 \\ I_A(2v_{\overline{H_1 \cup H_2 \cup K_2}}(x)) & \text{if } x \in \overline{H_1 \cup H_2 \cup K_2} \end{cases}$$

$$\pi_5(x) = \begin{cases} I_A(2v_{H_1}(x)) & \text{if } x \in H_1 \\ I_A(2v_{K_1}(x)) & \text{if } x \in K_1 \\ I_{\bar{A}}(v_{\overline{H_1 \cup K_1}}(x)) & \text{if } x \in \overline{H_1 \cup K_1} \end{cases}$$



$v_{K_1}$  one-one on  $K_1$ ,  $v_{K_2}$  one-one on  $K_2$ , and  $\pi_2(\overline{K_1 \cup K_2})$   
 $= 3\mathcal{N}$ ,  $\pi_2(K_1) = 3\mathcal{N} + 1$ ,  $\pi_2(K_2) = 3\mathcal{N} + 2$ . Thus  $\pi_2$  is a perm-  
utation.  $a(H_1 \cup H_2) = 2\mathcal{N}$ ; hence  $\pi_3(H_1 \cup H_2) = 3\mathcal{N}$  and  $\pi_3$  is  
one-one on  $H_1 \cup H_2$  since  $a$  is. As for  $\pi_2$  we see that  $\pi_3(\overline{H_1 \cup K_2})$   
 $= 3\mathcal{N} + 1$  and  $\pi_3(K_2) = 3\mathcal{N} + 2$  and that  $\pi_3$  is a permutation.

$\pi_4(H_2 \cup K_2) = v(H_2 \cup K_2) = \bar{A}$  and  $\pi_4$  is one-one on  $H_2 \cup K_2$ .  $v_{H_1}$  is one-  
one on  $H_1$  and  $I_A$  is one-one and hence  $\pi_4(H_1) = I_A(2\mathcal{N})$ . Similarly,  
 $\pi_4$  is one-one on  $\overline{H_1 \cup H_2 \cup K_2}$  and  $\pi_4(\overline{H_1 \cup H_2 \cup K_2}) = I_A(2\mathcal{N} + 1)$ .  
Hence  $\pi_4(\overline{H_2 \cup K_2}) = I_A(\mathcal{N}) = A$ ;  $\pi_4$  is also a permutation. For  $\pi_5$   
we see as for  $\pi_4$  that  $\pi_5(H_1 \cup K_1) = I_A(\mathcal{N}) = A$ , that  $\pi_5(\overline{H_1 \cup K_1})$   
 $= \bar{A}$  and that  $\pi_5$  is one-one. Finally,  $\pi_6(H_1 \cup K_1) = A$  and  $\pi_6$  is  
one-one on  $H_1 \cup K_1$  because  $v$  is.  $\pi_6$  maps  $\overline{H_1 \cup K_1}$  one-one onto  $\bar{A}$   
and this proves that  $\pi_6$  is also a permutation.

Let us set  $\pi' = \pi_6 \pi_5^{-1} \pi_4 \pi_3^{-1} \pi_2 \pi_1^{-1}$ . We claim that  $\pi' = \pi$ . By  
our previous remarks,  $\pi_3^{-1} \pi_2 \pi_1^{-1}(2\mathcal{N}) = H_1 \cup H_2$ ,  $\pi_5^{-1} \pi_4(H_1)$   
 $= H_1$ ,  $\pi_6(H_1) = A \cap X$ ,  $\pi_4(H_2) = v(H_2) = \bar{A} \cap X$ ,  $\pi_6 \pi_5^{-1}(\bar{A} \cap X) = \bar{A} \cap X$ .  
By the definition of  $H_1$  and  $H_2$  it follows that for each  $z \in H_1 \cup H_2$   
we have  $\pi'(a(z)) = v(z) = \pi(a(z))$  and hence  $\pi$  and  $\pi'$  agree on  
 $a(H_1 \cup H_2) = 2\mathcal{N}$ .

A similar argument convinces us that  $\pi$  and  $\pi'$  agree on  
 $2\mathcal{N} + 1$ , thereby completely proving the theorem.

Q.E.D.

Our next goal is to show that  $\mathbb{R} = \mathbb{P}_6$ . We need the  
following

Proposition 7.5. Let  $\pi$  be a recursive permutation. There  
exists an infinite and co-infinite set  $A \in \mathcal{C}^1$  and infinite sets  
 $G$  and  $H$  in  $\mathcal{C}^1$  such that  $\pi(A) \supseteq G$  and  $\pi(\bar{A}) \supseteq H$ .

Proof. Let  $g$  be the function in  $\mathcal{E}^1$ , given by Proposition 4.6, which enumerates  $\mathcal{G}_{\pi^{-1}}$  in the same order as the recursive function  $\lambda x \langle x, \pi^{-1}(x) \rangle$ . By Proposition 4.6 the set  $K = \{ \langle u + 1, g(u + 1) \rangle : g(u) \neq g(u + 1) \}$  is in  $\mathcal{E}^1$  and  $rrI_K(n) = n$ ,  $lrI_K(n) = \pi^{-1}(n)$ . Set  $v(x) = rr(x)$  and  $a(x) = lr(x)$ . Then  $vI_K(n) = n$  and  $aI_K(n) = \pi^{-1}(n)$ . To simplify the notation, set  $I_K(n) = k_n$ .

We define now an infinite set  $L$  in  $\mathcal{E}^1$  with the property that  $aI_K(1_{n+1}) > I_K(1_n)$ , where, as in the case of  $K$ , we denote  $I_L(n)$  by  $l_n$ .  $L$  will be the range of the function  $h$  defined below. The functions  $t(n,m,z)$  and  $lgth(z)$  have been defined in Section 3.

$$h(0) = 0$$

$$h(1) = \mu y [y \in K \wedge y > \langle \langle h(0) \rangle \rangle \wedge a(y) > I_K h(0) \\ \wedge \forall u (u \geq y \rightarrow a(u) > I_K h(0))] ]$$

$$h(n + 1) = \mu y [y \in K \wedge y > \langle \langle h(0), h(1), \dots, h(n) \rangle \rangle \\ \wedge a(y) > I_K h(n) \wedge \forall u (u \geq y \rightarrow a(u) > I_K h(n))] ]$$

To show that  $L$  is a set in  $\mathcal{E}^1$  notice first that there are exactly  $u + 1$  elements  $s$  in  $K$  such that  $a(s) \leq u$ . With this observation the following holds:

$$y \in L \leftrightarrow (\exists z < y) (\exists n < y) [lgth(z) = n + 1 \\ \wedge (\forall m \leq n) (\exists u < y) (a(y) > u \wedge u \in K \wedge v_K(u) = t(n,m,z) \\ \wedge \forall s < y (s \in K \wedge a(s) \leq u) = u + 1) ]$$

All the quantifiers are bounded and all the functions are in  $\mathcal{E}^1$ . This proves that  $L \in \mathcal{E}^1$ .

$$\text{Let } G = \{x : x \in L \wedge v_L(x) \text{ is even}\}$$

$$H = \{x : x \in L \wedge v_L(x) \text{ is odd}\}$$

and denote  $I_G(n)$  by  $g_n$  and  $I_H(n)$  by  $h_n$ .  $G$  and  $H$  are obviously sets in  $\mathcal{C}^1$ . By the definition of  $K$  the following inequalities hold:

$$\begin{array}{ll} a(k_{g_0}) > k_{g_0} & a(k_{g_1}) > k_{h_0} \\ a(k_{h_1}) > k_{g_1} & a(k_{g_2}) > k_{h_1} \\ \dots\dots\dots & \dots\dots\dots \\ a(k_{h_n}) > k_{g_n} & a(k_{g_{n+1}}) > k_{h_n} \end{array}$$

Denoting the set  $\{m, m + 1, m + 2, \dots, n\}$  by  $[m, n]$ , let us set

$$A = [0, k_{g_0}] \cup \bigcup_{i \geq 0} [k_{h_i} + 1, k_{g_{i+1}}]$$

Hence  $\bar{A} = \bigcup_{i \geq 0} [k_{g_i} + 1, k_{h_i}]$ . It is immediate that  $A$  is in  $\mathcal{C}^1$ .

We show by induction that the sets  $A$ ,  $G$  and  $H$  we just defined satisfy our Proposition.  $g_0 \in \pi(A)$  since  $\pi^{-1}(g_0) = a(k_{g_0}) \leq k_{g_0}$

and  $[0, k_{g_0}] \subseteq A$ .  $h_0 \in \pi(\bar{A})$  since  $\pi^{-1}(h_0) = a(k_{h_0}) \leq k_{h_0}$  and

$a(k_{h_0}) > k_{g_0}$  and  $[k_{g_0} + 1, k_{h_0}] \subseteq \bar{A}$ .  $g_{n+1} \in \pi(A)$  since  $\pi^{-1}(g_{n+1}) = a(k_{g_{n+1}}) \leq k_{g_{n+1}}$  and  $a(k_{g_{n+1}}) > k_{h_n}$  and  $[k_{h_n} + 1, k_{g_{n+1}}] \subseteq A$ .

$h_{n+1} \in \pi(\bar{A})$  since  $\pi^{-1}(h_{n+1}) = a(k_{h_{n+1}}) \leq k_{h_{n+1}}$  and  $a(k_{h_{n+1}}) > k_{g_{n+1}}$

and  $[k_{g_{n+1}} + 1, k_{h_{n+1}}] \subseteq \bar{A}$ . Hence  $\pi(A) \supseteq G$  and  $\pi(\bar{A}) \supseteq H$ .

Q.E.D.

Let us briefly remark that the previous Proposition is not

trivial in the sense that there exist recursive sets  $X$  which do not contain any infinite primitive recursive set. We shall call such sets internally strange. One can show, by a direct construction which we omit, that there exist recursive sets  $X$  such that both  $X$  and  $\bar{X}$  are internally strange. In fact, if this were not the case one could simplify the proof of Theorem 7.4 and show that  $\mathbb{R} = \mathbb{P}'_5$ . However, as our previous Proposition showed, a recursive permutation cannot map all primitive recursive sets only onto internally strange sets.

Theorem 7.6.  $\mathbb{R} = \mathbb{P}_6$ .

Proof. As in Theorem 7.4, the inclusion  $\mathbb{P}_6 \subseteq \mathbb{R}$  is by definition. We prove now  $\mathbb{R} \subseteq \mathbb{P}_6$ .

Let  $A, G$  and  $H$  be the sets in  $\mathcal{E}^1$  given by Proposition 7.5 for which  $\pi(A) \supseteq G$  and  $\pi(\bar{A}) \supseteq H$ . We can assume without loss of generality that  $\pi(A) - G$  and  $\pi(\bar{A}) - H$  are infinite; for if one of them is finite, say  $\pi(A) - G$ , we only have to replace  $G$  by  $\{x \in G : v_G(x) \in 2\mathcal{N}\}$ .

Let  $K$  be a set in  $\mathcal{E}^1$  such that  $r(K) = \mathcal{G}_\pi$  and let  $a(z) = lr(z)$  and  $v(z) = rr(z)$ . As in Theorem 7.4, if  $\pi(x) = y$ , there is a unique  $z \in K$  such that  $a(z) = x$  and  $v(z) = y$ .  $a$  and  $v$  are in  $\mathcal{E}^1$  and are one-one on  $K$ . The set  $K$  is the union of following four disjoint sets:

$$H_1 = \{z \in K : a(z) \in A \wedge v(z) \in \overline{G \cup H}\}$$

$$K_1 = \{z \in K : a(z) \in A \wedge v(z) \in G\}$$

$$H_2 = \{z \in K : a(z) \in \bar{A} \wedge v(z) \in \overline{G \cup H}\}$$

$$K_2 = \{z \in K : a(z) \in \bar{A} \wedge v(z) \in H\}$$

Again  $H_1, K_1, H_2$  and  $K_2$  are sets in  $\mathcal{G}^1$ . The permutations  $\pi_i (1 \leq i \leq 6)$  are now defined as follows:

$$\pi_1(x) = \begin{cases} 2v_A(x) & \text{if } x \in A \\ 2v_{\bar{A}}(x) + 1 & \text{if } x \in \bar{A} \end{cases}$$

$$\pi_2(x) = \begin{cases} 2v_A a(x) & \text{if } x \in H_1 \cup H_2 \\ 2v_{\overline{H_1 \cup K_1}}(x) + 1 & \text{if } x \in \overline{H_1 \cup K_1} \end{cases}$$

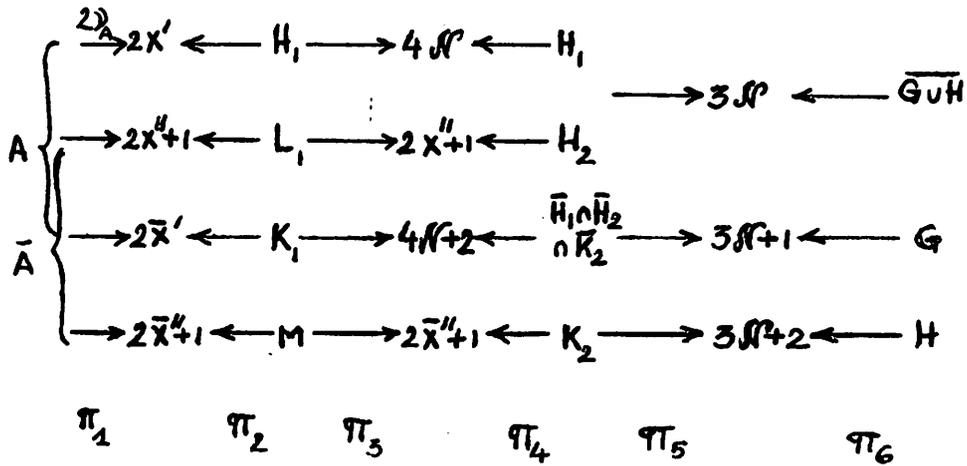
$$\pi_3(x) = \begin{cases} 4v_{H_1}(x) & \text{if } x \in H_1 \\ 4v_G v(x) + 2 & \text{if } x \in K_1 \\ 2v_{\overline{H_1 \cup K_1}}(x) + 1 & \text{if } x \in \overline{H_1 \cup K_1} \end{cases}$$

$$\pi_4(x) = \begin{cases} 4v_{H_1}(x) & \text{if } x \in H_1 \\ 2v_{\bar{A}} a(x) + 1 & \text{if } x \in H_2 \\ 4v_{\overline{H_1 \cup H_2 \cup K_2}}(x) + 2 & \text{if } x \in \overline{H_1 \cup H_2 \cup K_2} \\ 2v_{\bar{A}} a(x) + 1 & \text{if } x \in K_2 \end{cases}$$

$$\pi_5(x) = \begin{cases} 3v_{\overline{G \cup H}} v(x) & \text{if } x \in H_1 \cup H_2 \\ 3v_{\overline{H_1 \cup H_2 \cup K_2}}(x) + 1 & \text{if } x \in \overline{H_1 \cup H_2 \cup K_2} \\ 3v_H v(x) + 2 & \text{if } x \in K_2 \end{cases}$$

$$\pi_6(x) = \begin{cases} 3v_{\overline{G \cup H}}(x) & \text{if } x \in \overline{G \cup H} \\ 3v_G(x) + 1 & \text{if } x \in G \\ 3v_H(x) + 2 & \text{if } x \in H \end{cases}$$

The following diagram represents these definitions:



It is now easily checked, as in the proof of Theorem 7.4,  
 that  $\pi = \pi_6^{-1} \pi_5^{-1} \pi_4^{-1} \pi_3^{-1} \pi_2^{-1} \pi_1$ .

Q.E.D.

Theorem 7.7. For  $1 \leq i \leq 5$ ,  $P_i \subset P_{i+1}$ ,  $P'_i \subset P'_{i+1}$ ,  
 $P_i \neq P'_i$ .

Proof. Immediate from Corollary 7.3 and Theorem 7.4.

Q.E.D.

## 8. THE PERMUTATIONS $\mathcal{E}^0$ .

The permutations of  $\mathcal{E}^0$  do not generate the group of recursive permutations. This is ultimately due to the fact that the functions of  $\mathcal{E}^0$  are bounded by  $\lambda_x(x + k)$  (see §3). Theorem 8.3 of this section shows that, as a consequence of this, permutations generated by permutations in  $\mathcal{E}^0$  always map a set  $X$  such that both  $X$  and  $\bar{X}$  are enumerable by one-one primitive recursive functions onto a set with the same property. Hence the permutations of  $\mathcal{E}^0$  do not generate the recursive ones. Let us remark that the proofs of Section 7 do not hold in the case of  $\mathcal{E}^0$  since one-one functions in  $\mathcal{E}^0$  can not enumerate both a set and its complement. This last property was essential in the proofs we presented there. We start this section by showing that the permutations of  $\mathcal{E}^0$  do not form a group.

Theorem 8.1. There exist permutations in  $\mathcal{E}^0$  whose inverse is not in  $\mathcal{E}^0$ . Hence the permutations of  $\mathcal{E}^0$  do not form a group.

Proof. By Proposition 3.1, for any function  $f$  in  $\mathcal{E}^0$  there exists a constant  $k$  such that for all  $x$ ,  $f(x) < x + k$ . Our goal is to construct a permutation  $f$  in  $\mathcal{E}^0$  such that  $\forall \ell \exists y (f^{-1}(y) \geq y + \ell)$ , ensuring thereby that  $f^{-1}$  is not in  $\mathcal{E}^0$ .

The following permutation  $f$  will satisfy our theorem:

$$f(0) = 0$$

$$f(x) = \begin{cases} x + 1 & \text{if } x + 2 \text{ is not a power of } 2 \\ \mu y < x (y \text{ is a power of } 2) \div 1 & \text{if} \\ & x + 2 \text{ is a power of } 2. \end{cases}$$

A few values of  $f$  are listed below:

$f(0) = 0$	$f(8) = 9$
$f(1) = 2$	$f(9) = 10$
$f(2) = 1$	$f(10) = 11$
$f(3) = 4$	$f(11) = 12$
$f(4) = 5$	$f(12) = 13$
$f(5) = 6$	$f(13) = 14$
$f(6) = 3$	$f(14) = 7$
$f(7) = 8$	

$f$  can be easily defined in  $\mathcal{E}^0$  since, by Corollary 3.7, the predicate "x is a power of 2" is in  $\mathcal{E}^0$ .  $f$  is onto since, if  $x + 1$  is not a power of 2,  $f(x \div 1) = x$  and, if  $x + 1$  is a power of 2,  $f(2x) = x$ .  $f$  is evidently one-one.

To show that  $f^{-1}$  is not in  $\mathcal{E}^0$  notice that the sequence  $l_0 = 0, l_1 = 1, l_2 = 3, \dots, l_n = 2^n - 1, \dots$  has the property that for all  $i, \exists x(x \geq f(x) + l_i)$  since  $2l_n = f(2l_n) + l_n$ .

Q.E.D.

**Proposition 8.2.** Let  $\pi \in \mathcal{E}^0$  be a permutation and  $Y$  an infinite and co-infinite set such that both  $Y$  and  $\bar{Y}$  can be enumerated by one-one primitive recursive functions. Then  $x = \pi^{-1}(Y)$  and  $\bar{x} = \pi^{-1}(\bar{Y})$  can be enumerated by one-one primitive recursive functions.

**Proof.** Since  $\pi \in \mathcal{E}^0$ , there exists a constant  $k$  such that for all  $x, \pi(x) < x + k$  (Proposition 3.1). By Proposition 6.7 there exist sets  $G$  and  $H$  with primitive recursive increasing enumeration such that  $Y \supseteq G$  and  $\bar{Y} \supseteq H$ . It follows that both

$\bar{G}$  and  $\bar{H}$  are also strongly primitive recursive.

Set  $G' = \pi^{-1}(G)$  and  $H' = \pi^{-1}(H)$ . We shall show that  $G'$  is strongly primitive recursive. For every  $n$  and  $x$ , let  $\beta(n,x) = (I_{\bar{G}}I_G)^n(x)$ . It is immediate that  $\beta$  is a primitive recursive function. Hence the function  $\gamma$  defined by the equation

$$\gamma(n) = \beta((n+1)k + n + 1, I_{\bar{G}}(n))$$

is also primitive recursive.

We now claim that for all  $n$ ,  $\gamma(n) \in \bar{G}$  and that there exist  $(n+1)k + n + 1$  elements  $x$  of  $G$  such that  $I_{\bar{G}}(n) < x < \gamma(n)$ . For  $(n+1)k + n + 1 > 0$  and hence, by the definition of  $\gamma$  and  $\beta$ ,  $\gamma(n) \in \bar{G}$ . Now, if  $x \in \bar{G}$  then  $I_G(x) \geq x$  and in fact, since  $I_G(x) \in G$ ,  $I_G(x) > x$ . Further,  $I_{\bar{G}}I_G(x) \geq I_G(x)$  and, since  $I_{\bar{G}}I_G(x) \in \bar{G}$ ,  $I_{\bar{G}}I_G(x) > I_G(x)$ . Hence if  $x \in \bar{G}$ ,  $x$  and  $\beta(1,x)$  are separated by one element in  $G$ . An induction argument shows immediately that  $x$  and  $\beta(m,x)$  are separated by  $m$  elements of  $G$ . This proves the claim.

Let us now define a function  $h$  as follows:

$$h(0) = \mu x \leq \gamma(0) + 1 (\pi(x) \in G)$$

$$h(n+1) = \mu x \leq \gamma(n+1) + n + 1 (x > h(n) \wedge \pi(x) \in G)$$

Clearly,  $h$  is primitive recursive and  $\pi h(n) \in G$ , i.e.

$h$  enumerates a subset of  $G'$ .

Let us show that it actually enumerates  $G'$ . We show by induction on  $n$  that there are at least  $n+1$  elements  $x \leq \gamma(n) + n$  such that  $\pi(x) \in G$ .

$n = 0$ . Suppose to the contrary that for all  $x \leq \gamma(0) + 1$  we have  $\pi(x) \in \bar{G}$ . There exists then  $x \leq \gamma(0) + 1$  such that  $\pi(x) \geq I_{\bar{G}}(\gamma(0) + 1)$ . But, by our previous claim, there exist at least  $k + 1$  elements of  $G$  preceding  $\gamma(0)$  and there are also  $\gamma(0) + 2$  elements  $y$  of  $\bar{G}$  such that  $y \leq I_{\bar{G}}(\gamma(0) + 2)$ . Hence,  $\pi(x) \geq I_{\bar{G}}(\gamma(0) + 1) \geq \gamma(0) + k + 2$ . On the other hand,  $\pi(x) < x + k \leq \gamma(0) + k + 1$ . Contradiction.

$n + 1$ . Let us assume the induction hypothesis that there exist  $n + 1$  elements  $x$  such that  $x \leq \gamma(n) + n$  and that  $\pi(x) \in G$ . Suppose, contradicting our claim, that there are not more than  $n$  elements  $x$  such that  $x \leq \gamma(n + 1) + n + 1$  and  $\pi(x) \in G$ . Hence among the elements  $\leq \gamma(n + 1) + n + 1$  there are  $\gamma(n + 1) + n + 2 - n = \gamma(n + 1) + 2$  elements  $x$  such that  $\pi(x) \in \bar{G}$ . There exists, therefore, an element  $x \leq \gamma(n + 1) + n + 1$  such that  $\pi(x) \geq I_{\bar{G}}(\gamma(n + 1) + 1)$ . Reasoning as for the case  $n = 0$ , we find that  $I_{\bar{G}}(\gamma(n + 1) + 1) \geq \gamma(n + 1) + 1 + (n + 2)k + n + 2 = \gamma(n + 1) + (n + 2)k + n + 3$ . But  $\pi(x) < x + k \leq \gamma(n + 1) + n + 1$  and this is a contradiction.

This concludes the proof that  $h$  enumerates  $G'$  increasingly and hence that  $G'$  is strongly primitive recursive.

A similar argument proves that  $H'$  is strongly primitive recursive. Since  $G' \subseteq X$  and  $H' \subseteq \bar{X}$  it follows that  $X$  and  $\bar{X}$  are indeed enumerable by one-one primitive recursive functions.

Q.E.D.

Theorem 8.3. The group of permutations generated by the permutations in  $\mathcal{E}^0$  contains only permutations which map a set  $X$  such that both  $X$  and  $\bar{X}$  are enumerable by one-one primitive

recursive functions onto sets  $Y$  with the same property. Hence, the permutations of  $\mathcal{E}^0$  do not generate the group of recursive permutations.

Proof. Clearly, if  $\pi \in \mathcal{E}^0$  is a permutation and  $X$  and  $\bar{X}$  are both enumerable by one-one primitive recursive functions, the same holds for  $\pi(X)$  and  $\pi(\bar{X})$ . By the previous Proposition  $\pi^{-1}(X)$  and  $\pi^{-1}(\bar{X})$  are also enumerable by one-one primitive recursive functions. Hence, by induction on the length of a permutation generated by permutations of  $\mathcal{E}^0$ , the same is true for such a permutation. Therefore the permutations of  $\mathcal{E}^0$  do not generate all the recursive permutations, since it is easy to construct a recursive permutation which does not have this property (e.g. any permutation mapping the even integers and the odd integers onto internally strange sets).

Q.E.D.

#### REFERENCES

- [1] F. B. CANNONITO, M. FINKELSTEIN, On primitive recursive permutations and their inverses, Journal of Symbolic Logic, vol. 34(1969), pp. 634-637.
- [2] A. COBHAM, The intrinsic computational difficulty of functions, Proceedings of the 1964 Congress on Logic, Methodology and Philosophy of Sciences (Y. Bar - Hillel, editor), North - Holland Publishing Company, 1965.
- [3] A. GRZEGORCZYK, Some classes of recursive functions, Rozprawy Matematyczne, no. 4, Instytut Matematyczny Polskiej Akademii Nauk, Warsaw, 1953.
- [4] C. F. KENT, Constructive analogues of the group of permutations of natural numbers, Transactions of the American Mathematical Society, vol. 104(1962), pp. 347-362.
- [5] V. V. KOZ'MINIKH, On the representation of partial recursive functions, Proceedings of the Eleventh All - Union Colloquium on Algebra, Academy of Sciences of the Moldavian Socialist Republic, Kishinev, 1971 (in Russian).
- [6] A. V. KUZNECOV, On primitive recursive functions of large oscillation, Doklady Akademii Nauk SSSR, n.s., vol. 71(1950), pp. 233-236 (in Russian).
- [7] A. I. MALCEV, Algorithms and Recursive Functions, Nauka, Moscow 1965.

- [8] A. R. MEYER, D. M. RITCHIE, A classification of the recursive functions (to appear).
- [9] D. M. RITCHIE, Program structure and computational complexity, Ph.D. thesis, Harvard, 1968.
- [10] R. RITCHIE, Classes of predictably computable functions, Transactions of the American Mathematical Society, vol. 106 (1963), pp. 139-173.
- [11] J. ROBINSON, General recursive functions, Proceedings of the American Mathematical Society, vol. 1, no. 6, pp. 703-718.
- [12] H. ROGERS, Jr., Theory of recursive functions and effective computability, McGraw Hill Publishing Company, 1967.
- [13] V. A. USPENSKII, Lecons sur les fonctions calculables, Actualités Scientifiques et Industrielles, no. 1317, Hermann, Paris 1966.