STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

ZW 1965-009

A combinatorial problem on the semigroup of all transformations of a finite set.

by

P. v. Emde Boas

The Mathematical Centre at Amsterdam, founded the 11th of February, 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

§1. Introduction

Let T_n be the set of all mappings of a finite set consisting of n elements into itself. For convenience we take for the set on which T_n acts the set of the positive integers $\{1, 2, 3, \ldots, n\}$.

If $f \in T_n$ and if $(1)f = k_1$, $(2)f = k_2, \ldots, (n)f = k_n$ then f will be denoted by $(k_1, k_2, \ldots, k_n)$.

The product of two mappings will by definition be their composition: $(k)fg \overset{\mathrm{Def}}{=} ((k)f)g$. Functional composition is an associative operation; hence T_n with this definition of the product is a semigroup.

If $f = (k_1, k_2, \ldots, k_n)$ and $g = (m_1, \ldots, m_n)$ then $fg = (m_{k_1}, m_{k_2}, \ldots, m_{k_n})$.

T_n contains n^n elements, for each of the n objects has n possible images.

T_n contains as a subgroup the set of all 1 - 1 mappings of $\{1, 2, 3, \ldots, n\}$ onto itself. This group will be denoted by S_n; S_n contains n! elements.

An element of T_n will be called an <u>idempotent</u> element iff $f^2 = f$. If $f \in S_n$ and f is idempotent, then f is necessarily the identity mapping $I = (1, 2, 3, \ldots, n)$. We have the following characterisation of idempotent elements:
An element $g \in T_n$ is idempotent iff there exists a set of numbers $\{a_1, a_2, \ldots, a_r\}$ $r \geqq 1$ for which $(a_1)g = a_1$ $(a_2)g = a_2$ $\ldots$ $(a_r)g = a_r$ and $\{1 \ldots n\}g = \{a_1, a_2, \ldots, a_r\}$.

<u>Proof</u>: If g is of this kind, then $g \mid \{1 \ldots n\}g = I \mid \{1 \ldots n\}g$, and hence $g^2 = g \circ g = g \circ I = g$.
Each idempotent has this form: If $(a)g \neq a$ and $a = (b)g$ then $(b)g^2 = (a)g \neq a = (b)g$; hence g is not idempotent.

By way of example we shall write down the complete T_2 and T_3, indicating which elements are idempotent and which are contained in the corresponding S_n.

T_2 : (1,1), (1,2),(2,1), (2,2)
(1,2) is the unity. S_2 consists of (1,2) and (2,1).
(2,1) is the only non-idempotent element of T_2.
(1,1) and (2,2) are clearly idempotent.

T_3 : S_3 consists of: (1,2,3) (identity), (1,3,2), (2,1,3), (2,3,1),
(3,1,2), (3,2,1).
There are 9 non-trivial idempotents: (1,2,2), (1,2,1), (1,1,3),
(1,3,3), (2,2,3), (3,2,3),
(1,1,1), (2,2,2), (3,3,3).
There are 12 non-invertible non-idempotent elements:
(2,1,2), (2,1,1), (1,1,2), (2,2,1),
(3,1,3), (3,1,1), (3,3,1), (1,3,1),
(2,3,2), (3,3,2), (3,2,2), (2,3,3).

The number of idempotent elements of T_n will be denoted by V_n. We have $V_2 = 3$ $V_3 = 10$. The number V_n is given by the formula:

$$V_n = \sum_{k=1}^{n} \binom{n}{k} k^{n-k}.$$

Proof: For each $k \geq 1$ there are $\binom{n}{k}$ ways to choose a set of k numbers that are to be mapped onto themselves and for each of these ways there are k^{n-k} possibilities of mapping the other $n - k$ numbers into the set of the k chosen ones.

§2. Words on finite semigroups

This report deals with a special case of a more general problem that was dealt with in an earlier report by P.C. Baayen, D. Kruyswijk and the author [1]. I shall repeat here some definitions and theorems that will be used in the following.

A word over a semigroup H is a sequence of one or more elements of H: $w = a_1, a_2, a_3, \ldots, a_k$. Its elements are called letters.

The value of a word $w = a_1, a_2, a_3, \ldots, a_k$ is the product of its letters; it is denoted by $|w|$; $|w| = a_1 \circ a_2 \circ a_3 \circ \ldots \circ a_n$ clearly $|w| \in H$.

A subword of a word $w = a_1, a_2, \ldots, a_k$ is a word of the shape $w' = a_r, a_{r+1}, a_{r+2}, \ldots, a_{r+s}$, in which $1 \leqq r \leqq r + s \leqq k$.

A set of subwords of a given word will be called a central word-set if the first letter of each of these subwords has the same index in the original word.

In a central word-set the words can always be ordered by increasing length. The set can then be denoted by $\{w_0, w_0w_1, w_0w_1w_2, \ldots, w_0w_1w_2\ldots w_r\}$ in which the w_j are consecutive subwords of the original word. It is clear that the word-set $\{w_1, w_1w_2, \ldots, w_1w_2\ldots w_r\}$ which is obtained through formally dividing by w_0 is central. We call this set the derived central word-set.

In [I] the following result is obtained:

Theorem: To each finite semigroup H a positive integer λ can be assigned such that any word with length λ over H contains a subword with idempotent value. Denoting the least possible λ for a fixed H with $\lambda(H)$ we have moreover: If H is a group, $\lambda(H)$ is equal to the order of the order of the group.

In this report the following theorem will be proved:

Theorem: For each n, $\lambda(T_n) = n!$.

From this theorem it follows that $\lambda(T_n) = \lambda(S_n)$. This provides us with an example of an extension of a group to a greatly larger semigroup in such a way that the maximal length of words without idempotent subwords does not increase.

§3 Proof of the Theorem

If we take a word w over T_n, then $|w|$ is a mapping. It makes sense therefore to write down an expression like $(a)\ |w| = b$; in this case we say that the word w maps the element a onto b.

We prove first that $\lambda(T_n) \leq n!$

Let w be the word $w = f_1, f_2, \ldots, f_{n!}$

We take the central word-set $C_0 = \{f_1, f_1f_2, f_1f_2f_3, \ldots, f_1f_2\ldots f_{n!}\}$ C_0 consists of n! words. If we look at the images of the element 1 under these words there are two possibilities:

I_1 : There are more than $(n - 1)!$ words in C_0 that map 1 onto 1; they form a central word-set $\{w_{11}, w_{11}w_{12}, w_{11}w_{12}w_{13}, \ldots\}$

II_1 : There are more than $(n - 1)! + 1$ words in C_0 that map 1 onto a fixed other element a_1. They form a central word-set $\{w_{10}, w_{10}w_{11}, w_{10}w_{11}w_{12}, \ldots\}$.

For let I_1 be not true. Then we have at least $n! - (n - 1)! + 1 = (n - 1)(n - 1)! + 1$ words that map 1 into $\{2, \ldots, n\}$. By the pigeonhole principle one of those elements has to serve at least $(n - 1)! + 1$ times as the image of 1.

If II_1 is true we consider the derived word-set $\{w_{11}, w_{11}w_{12}, \ldots\}$. This is a central set containing at least $(n - 1)!$ words each mapping a_1 onto a_1.

In either case the following statement O_1 is true.

O_1 : There exists an element a_1 and a central word-set C_1, containing more than $(n - 1)!$ different subwords of w, each mapping a_1 onto itself.

Suppose the following assertion O_m is true for some m, $1 \leq m \leq n - 1$:

O_m : There exists a set of m different elements $\{a_1 \ldots a_m\}$ and a central word-set C_m, containing at least $(n - m)!$ different subwords of w, under which a_1 is mapped onto a_1, a_2 is mapped onto $a_2, \ldots, a_n$ is mapped onto a_n.

Then from the following three assertions one has to be true:

I_{m+1} : There exists an element a_{m+1}, not contained in $\{a_1 \ldots a_m\}$ and a central word-set C_{m+1} containing at least $(n - m - 1)!$ words from C_m, each mapping a_{m+1} onto itself.

II_{m+1} : There exists an element b_{m+1}, not contained in $\{a_1 \ldots a_m\}$ and a central word-set C'_{m+1} containing at least $(n - m - 1)! + 1$ words from C_m, each mapping b_{m+1} onto a fixed element a_{m+1} not contained in $\{a_1, a_2, \ldots, a_m, b_{m+1}\}$.

III_{m+1} : There exists a word in C_m that maps $\{1\ 2 \ldots n\}$ onto $\{a_1\ a_2 \ldots a_m\}$.

For assume III_{m+1} not to be true. Then there exists an element x which by no word of C_m is mapped into $\{a_1 \ldots a_m\}$. There are $(n - m)!$ mappings and there are $n - m$ possible images of x (x itself being included). Then by the pigeon-hole principle either x is at least $(n - m - 1)!$ times its own image or a fixed element $y \neq x$ is at least $(n - m - 1)! + 1$ times the image of x.

In the first case we take x as the element a_{m+1} and we define C_{m+1} to be the word-set consisting of all those words in C_m mapping x onto itself. Then I_{m+1} follows. Otherwise let $b_{m+1} = x$, $a_{m+1} = y$ and let C'_{m+1} be the word-set consisting of the words in C_m mapping x onto y; now II_{m+1} follows.

If II_{m+1} is found to be true and the set C'_{m+1} contains the words $\{w_{m+1,0}, w_{m+1,0}w_{m+1,1}, w_{m+1,0}w_{m+1,1}w_{m+1,2}, \ldots\}$, we take the derived central word-set $\{w_{m+1,1}, w_{m+1,1}w_{m+1,2}, \ldots\}$, which contains at least $(n - m - 1)!$ words each mapping a_1 onto a_1, a_2 onto $a_2, \ldots, a_m$ onto a_m, and a_{m+1} onto a_{m+1}.

In this way we conclude that O_{m+1} follows if either I_{m+1} or II_{m+1} is true.

If III_{m+1} is true, however, we have arrived at a word in C_m that maps $\{1, 2 \ldots n\}$ onto $\{a_1\ a_2 \ldots a_m\}$. This word maps each element of its image onto itself and hence its value is an idempotent of T_n.

Thus we have proved: $O_m \Rightarrow [O_{m+1}$ or there exists an idempotent subword of w$]$.

Suppose we find O_n to be true. Then there exists at least one subword of w mapping each element of $\{1 \ldots n\}$ onto itself. This word has clearly the identity value and hence is idempotent. This completes the proof of the assertion $\lambda(T_n) \leq n!$

Remark: If we use the symbol A for the assumption:

A: w is a word of length n! over T_n

and if we use the symbol G to denote the assertion

G: There exists an idempotent subword of w

we have the following diagram of implications:

$$\begin{tikzcd}
 & I_1 \arrow[dr] & & I_2 \arrow[dr] & & & & I_n \arrow[dr] & & \\
A \arrow[ur, "or"] \arrow[r] & II_1 \arrow[r] & O_1 \arrow[ur, "or"] \arrow[r] \arrow[dr, "or"'] & II_2 \arrow[r] & O_2 \arrow[rr, dashed, no head] & & O_{n-1} \arrow[ur, "or"] \arrow[r] \arrow[dr, "or"'] & II_n \arrow[r] & O_n \arrow[r] & G \\
 & & & III_2 \arrow[r] & G & & & III_n \arrow[r] & G &
\end{tikzcd}$$

It remains to be shown that $\lambda(T_n) \geq n!$. But this follows trivially from the fact that $S_n \subset T_n$ and that $\lambda(S_n) = n!$, as $\lambda(T_n) \geq \lambda(S_n)$. Thus the proof of our theorem has been completed.

§ 4 Additional remarks

1. In the proof of the inequality $\lambda(T_n) \geq n!$ we made use of the fact that there exists an idempotent-free subword of length $n! - 1$ over T_n with all its letters taken from S_n. It is not true, however, that such maximal idempotent-free words are always words over the group S_n. By way of example, consider T_3.

The word $f_1 f_2 f_3 f_4 f_5$ with $f_1 = (321)$ $f_2 = (131)$ $f_3 = (213)$ $f_4 = (321)$ $f_5 = (131)$ has no idempotent subwords.

Below I list the values of all its subwords.

$|f_1| = (321)$
$|f_2| = (131)$
$|f_3| = (213)$
$|f_4| = (321)$
$|f_5| = (131)$

$|f_1 f_2| = (131)$
$|f_2 f_3| = (232)$
$|f_3 f_4| = (231)$
$|f_4 f_5| = (131)$

$|f_1 f_2 f_3| = (232)$
$|f_2 f_3 f_4| = (212)$
$|f_3 f_4 f_5| = (311)$

$|f_1 f_2 f_3 f_4| = (212)$
$|f_2 f_3 f_4 f_5| = (313)$

$|f_1 f_2 f_3 f_4 f_5| = (313)$

2. In [1] a formula is given for the maximal value of $\lambda(H)$ for all semigroups H with n elements and V idempotents. This maximum value is denoted by $L(n,V)$. In the following tabulation the values of $L(n^n, V_n)$ and $\lambda(T_n)$ are compared for $1 \leq n \leq 5$. We observe that the maximal word length for T_n is rather short.

n	$\lvert T_n\rvert = n^n$	V_n	$L(n^n,V_n)$	$\lambda(T_n) = n!$
1	1	1	1	1
2	4	3	2	2
3	27	10	131072	6
4	256	41	approx. $7.5\ 10^{34}$	24
5	3125	196	approx. $3\ .\ 10^{363}$	120

References

[1] : P.C. Baayen, P. van Emde Boas and D. Kruyswijk: A combinatorial problem on finite semigroups. Mathematical Centre report ZW 1965-006, (1965).