STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

ZW 1965-006

A combinatorial problem on finite semigroups

by

P.C. Baayen, P. van Emde Boas and D. Kruyswijk

September 1965

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. Some conventions

Let H be a finite system with an associative binary operation (a finite semigroup). In this report, no special knowledge of semigroups is assumed on the part of the reader.

Our theorems will deal with sequences of elements of H and the proofs involve sequences of such sequences. Hence, to avoid confusion, let us employ the old hand notion of "a word", according to the following conventions.

1. A sequence of one or more terms, in which each term is an element of H, is called a word over H. The comma's in a word will be often left out; if so, the terms will be called letters.
2. The value of a word $w = a_1 a_2 \ldots a_k$ over a semigroup $(H,*)$ is defined by

   $$|w| = a_1 * a_2 * \ldots * a_k.$$

3. A subword of a word W is a word, consisting of one or more consecutive letters of W in their proper order.

§2. Introduction

Some elementary principles in the theory of finite groups admit a neat formulation in the above terminology. We summarize them in the form of a theorem:

Theorem I

a. Any word W of length n, over a group G of order n, contains a subword with unit value.
b. Given a group G of order $n \geq 2$, there is a word W of length n-1 over G, which has no subwords with unit value.

For a proof of this theorem, if needed, see §3.

The object of this note is, to establish some results on finite semigroups, which have a close resemblance to theorem I. The part which is played by the unit element in theorem I, will be taken over by elements e which have the property that $e^2 = e$. Such elements are called: idempotent.

The following theorem II implies the well-known fact, that any finite semigroup has at least one idempotent element. Of course, much easier proofs of the same fact can be given and are available in any text-book on the subject.

Theorem II

To each finite semigroup H a positive integer λ can be assigned, such that any word W of length λ over H contains a subword with idempotent value.

This theorem has an amusing corollary in the theory of numbers (which will be proved, together with the theorem, in §5):

Corollary Given n, there is a constant τ_n such that any positive integer with more than τ_n divisors, has at least one divisor $d \geq 2$ with the property that $d(d-1)$ is divisible by n.

In particular, any positive integer with a sufficient amount of divisors will have a divisor ≥ 2, whose two final digits in the decimal scale are 00, 01, 25 or 76. One might try to find a direct arithmetical proof.

We shall give further attention to this kind of problem in a Mathematical Centre report on arithmetical semigroups, which is soon to appear. In the present note we are concerned with abstract systems only.

When looking for the least possible λ in theorem II, such as to be valid for all H of a fixed order n, we found the following theorem. It gives the critical values of λ, plus an additional item of some interest.

Theorem III

Define a function L(n) as follows:

$$\begin{cases} L(1) = 1,\ L(2) = 2, \\ L(n) = 4^{\frac{n}{3}} \cdot \left(\frac{27}{32}\right)^{\frac{n}{3} - \left[\frac{n}{3}\right]} \quad \text{for } n \geq 3, \end{cases}$$

then L(n) is a positive integer with the following properties:

a. Any word W of length L(n), over a semigroup H of order n, contains a subword with idempotent value.

b. Given $n \geq 2$, there is a semigroup H of order n, over which a word W of length $L(n)-1$ can be constructed, such that W has no subwords with idempotent value.
There is even a commutative H with this property.

Remarks. It is easy to prove that

$$0.89\ (\sqrt[3]{4})^n < L(n) \leq (\sqrt[3]{4})^n \text{ for } n \geq 3.$$

Further we have

$$\left.\begin{aligned} L(n) &= 2^{2k} && \text{if } n = 3k \\ L(n) &= 3.2^{2k-1} && \text{if } n = 3k+1 \\ L(n) &= 9.2^{2k-2} && \text{if } n = 3k+2 \end{aligned}\right\} \quad (k \geq 1).$$

If the latter two formulae are applied with $k = 0$, which is forbidden, they give $1\frac{1}{2}$ and $2\frac{1}{4}$, respectively, whereas the true values of L(1) and L(2) are 1 and 2. The fact that L(n) is an increasing function of n can be easily proved, but is not trivial a priori.

Tabulation for $n \leq 10$:

n	1	2	3	4	5	6	7	8	9	10
L(n)	1	2	4	6	9	16	24	36	64	96

Theorem III will be proved (in §8) as a consequence of the much more intricate theorem IV, to be stated next. It deals with those semigroups of order n, which have a prescribed number of idempotent elements.

Theorem IV

Given a pair of integers n, θ with $n \geq \theta \geq 1$.
Define two integers q and σ by

$$n = (2q-1)\theta + \sigma\ ,\ 0 \leq \sigma \leq 2\theta-1.$$

Then q and σ are uniquely defined and we have $q \geq 1$.
Next, define a function $L(n,\theta)$ by

$$L(n,\theta) = q^{2\theta-\sigma} \cdot (q+1)^{\sigma},$$

then we have:

A. Any word W of length $L(n,\theta)$ over a semigroup of order n which has exactly θ idempotents, contains a subword with idempotent value.

B. Given a pair n, θ with $1 \leq \theta \leq n-1$, there is a semigroup of order n with exactly θ idempotents, over which a word W of length $L(n,\theta)-1$ can be constructed, such that W has no subwords with idempotent value.

There is even a commutative semigroup with this property.

Remark. For readers who have worked their way through the above statement, we mention the following values:

$$L(n,\theta) = 1 \quad \text{if and only if } \theta = n.$$

$$L(n,\theta) = 2^{n-\theta} \quad \text{for } \theta \geq \frac{1}{3} n.$$

$$L(n,1) = \left[\frac{1}{4}(n+1)^2\right] \quad \text{for all } n.$$

$$L(n,2) = \frac{1}{256}(n^4+8n^3) + \mathcal{O}(n^2) \quad \text{for } n \to \infty.$$

Before we give the proofs of I, II, IV and III, one question remains to be settled. Is there a non-commutative semigroup which satisfies the assertion IV B?

Certainly not in all cases. We have, for instance, the fact that a semigroup with $n = 2$, $\theta = 1$ is necessarily commutative. In many cases, however, the answer is affirmative, as may be seen from the following statement, to be proved in §7:

Supplementary theorem

In each of the following cases there is a non-commutative semigroup with the property of theorem IV B.

(i) If q is an even number ≥ 6.

(ii) If q is an odd number ≥ 5, provided that $\sigma \geq 2$.

For instance, any word of 36 letters over any semigroup of order 11 which has only one idempotent, has a subword whose value is equal to that idempotent. But if we replace the number 36 by 35, the assertion becomes false and there are commutative as well as non-commutative semigroups to disprove it.

A special class of non-commutative semigroups (where each member is the semigroup of all mappings of a finite set in itself) will be made the object of further study in a forthcoming Mathematical Centre report, by one of the authors under title.

§3. Proof of theorem I

a. The assertion Ia is trivial in case $n = 1$. For $n \geq 2$, we put $W = a_1 a_2 \ldots a_n$ and consider the sequence

$$e, a_1, a_1 * a_2, \ldots, a_1 * a_2 * \ldots * a_n$$

where e is the unit-element of the group $(G, *)$.
A left-hand division of two equal terms in this sequence (they are provided by the pigeon-hole principle), leads up to the required subword of W.

b. The assertion Ib is trivial in case $n = 2$. For $n \geq 3$, let $(g_1, g_2, \ldots, g_{n-1})$ be an arbitrary permutation of those elements of G which are $\neq e$. Then the sequence

$$g_1, g_1^{-1} * g_2, \ldots, g_{n-2}^{-1} * g_{n-1}$$

fulfils the requirements of Ib, if the terms are considered as letters of a word W. (We remark that by this method $(n-1)!$ different words W can be constructed and that these words are the only ones, which satisfy Ib).

§4. The notion of a central word-set

The following notions and properties will be used frequently in the next sections.

If $a_1 \circ\circ\circ a_p$ and $b_1 \circ\circ\circ b_q$ are words over one and the same semigroup and if we denote them by w_1 and w_2, respectively, then we shall denote the word $a_1 \circ\circ\circ a_p b_1 \circ\circ\circ b_q$ by $w_1 w_2$. Clearly we have

$$|w_1 w_2| = |w_1| * |w_2|,$$

where $*$ is the operation in the semigroup.

A set of one or more words will be called a central set if it can be written as

(1) $$\{w_1, w_1 w_2, w_1 w_2 w_3, \circ\circ\circ\}.$$

It is easily seen that the following assertions hold true:

(i) If all the words of a central set are given, then the components w_i of the presentation (1) and their order of succession are uniquely determined.

(ii) A non-empty subset of a central set is central.

(iii) If (1) contains at least two words, then

(2) $$\{w_2, w_2 w_3, \circ\circ\circ\}$$

is a central set as well.

For instance, if a, b and c are elements of a semigroup, the set

$$\{aba, abacb, abacbb, abacbbaa\}$$

is central and we have, in the presentation (1): $w_1 = aba$, $w_2 = cb$, $w_3 = b$, $w_4 = aa$. Its subset

$$\{abacb, abacbbaa\}$$

is central too, but here we have $w_1 = abacb$, $w_2 = baa$.
Finally

$$\{baa\}$$

is a central set, which has been derived from the previous one like (2) from (1).

§5. Proof of theorem II and its corollary

The following proof may be omitted by the reader, as II is implied by IV A and we shall give an independent proof of IV A. However, the present proof is shorter. The truth of the assertion I is clearly implied by lemma 1 and lemma 2.

Lemma 1. An infinite word over a finite H has a (finite) subword with idempotent value.

Proof. Let $c_1c_2c_3 \ldots$ be an infinite word over $(H,*)$. The c_i may be considered as elements of H or as finite words over H; this will make no difference as to our argument. Consider the infinite, central word-set

$$C = \{c_1, c_1c_2, c_1c_2c_3, \ldots\}.$$

As H is infinite, C will have an infinite subset C_1, such that any word $w \in C_1$ has one and the same value in H. Denoting this subset by

$$C_1 = \{w_1, w_1w_{11}, w_1w_{11}w_{12}, \ldots\},$$

each of its elements has the value $|w_1|$. Next, consider the "derived" set $\{w_{11}, w_{11}w_{12}, w_{11}w_{12}w_{13}, \ldots\}$. This set does not need to be single-valued like C_1, but it has certainly an infinite, single-valued subset:

$$C_2 = \{w_2, w_2w_{21}, w_2w_{21}w_{22}, \ldots\}.$$

Here each of the elements has the value $|w_2|$ and we have moreover $|w_1| * |w_2| = |w_1|$, as the word w_1w_2 is one of the words of C_1. Next, consider the set $\{w_{21}, w_{21}w_{22}, w_{21}w_{22}w_{23}, \ldots\}$ and repeat the previous argument; this can be done as long as one wishes. The procedure yields, finally, an infinite sequence of words

$$w_1, w_2, w_3, \ldots$$

where each w_i is a subword of the given $c_1c_2c_3 \ldots$, and where moreover

(3) $\quad |w_1|*|w_2| = |w_1| \; ; \quad |w_2|*|w_3| = |w_2| \; ; \quad |w_3|*|w_4| = |w_3| \; ;$

and so on.

By the law of associativity, (3) implies

(4) $\quad |w_k| * |w_m| = |w_k|$ for all pairs k, m with k < m.

The values $|w_1|$, $|w_2|$, ... cannot be all different from each other. Hence there is a pair k, m with k < m and $|w_k| = |w_m|$. Then (4) gives $|w_k|^2 = |w_k|$, which proves lemma 1.

Lemma 2. Suppose, there is a finite H to which no boundary length λ can be assigned with the property of theorem I. Then there is an infinite word W over H without subwords of idempotent value.

Proof. The assumption implies the existence of an infinite set of finite words over H:

$$V_1 = \{a_{11}, a_{21}a_{22}, a_{31}a_{32}a_{33}, \ldots\},$$

such that no word in V_1 has a subword with idempotent value. As H is finite, H contains an element b_1, which is the beginning letter of infinitely many words in V_1. These words form a subset $V_2 \subset V_1$. Next, H contains an element b_2, serving as the second letter of infinitely many words of V_2. These words form a $V_3 \subset V_2$ and every word of V_3 has the initial piece b_1b_2. Iterating the argument, an infinite sequence $b_1, b_2, b_3, \ldots$ of elements of H is shown to exist, such that every word in V_{k+1} has the initial piece $b_1b_2 \ldots b_k$. Writing the same infinite sequence as a word

$$W = b_1b_2b_3 \ldots ,$$

we find that each finite subword of W is subword of one of the words in some V_k. Hence it is subword of a word in V_1, so that its value is not idempotent. This proves lemma 2.

Proof of the arithmetical corollary. The multiplicative semigroup of all residue-classes modulo n defines a number λ in the sense of theorem II. Let us denote $2^\lambda - 1$ by τ_n. Then any positive integer with more than τ_n divisors can be written as

$$q_1 \circ q_2 \circ \ldots \circ q_\mu,$$

where each q_i is a prime number, not necessarily different from the other ones, and where $\mu \geq \lambda$. Theorem II, applied on the word $q_1\, q_2 \circ\circ\circ q_\lambda$ modulo n leads up to a divisor $d \geq 2$ with $d^2 \equiv d \bmod n$. The latter congruence implies that $d(d-1)$ is divisible by n.

§6. Proof of theorem IV A

The proof is based upon lemma 3 - lemma 8.

Given $(H,*)$, let X be a subset of H, such that X does not contain idempotent elements.

A function $f(z)$, defined on H, is called an order-function with respect to X, if the following properties (5) hold true.

$$(5)\qquad \begin{cases} f(z) = 0 \quad \text{for } z \in H \setminus X. \\ f(z) \text{ is a positive integer for } z \in X. \\ f(x) > f(y) \text{ for all } x, y \text{ with } x \in X \text{ and } x * y = x. \end{cases}$$

If an order-function $f(z)$ with respect to X has been given, the number of solutions of the equation $f(z) = k$ will be denoted by s_k. Hence we have

(6) s_k is the number of elements $z \in H$, such that $f(z) = k$.

Lemma 3.

Definitions: Let $(H,*)$ be a finite semigroup;
W a word over H without subwords of idempotent value;
X the set of all values of all subwords of W;
$f(z)$ an order-function with respect to X.

Assumption : Each central set of subwords W contains less than N words w such that $f(|w|) \leq k-1$.
Here N and k are arbitrary positive integers.

Assertion : Any central set of subwords of W will contain less than $N(s_k+1)$ words w such that $f(|w|) \leq k$.

Proof. Due to the assumption we need only to prove that a central set contains a t m o s t Ns_k words w for which $f(|w|) = k$.

If $s_k = 0$, the assumption is identical with the assertion, whence we may assume that $s_k \geq 1$. If a wordset C (which need not be central) contains $Ns_k + 1$ words w with $f(|w|) = k$, it will certainly contain, by the pigeon-hole principle, a subset C_1 of N + 1 words, all of which have one and the same value in H.

Hence, if such a set C is moreover central, it will have a central subset

$$C_1 = \{w_1, w_1w_2, \ldots, w_1w_2\ldots w_{N+1}\},$$

in which each word has the value $|w_1|$. Denoting $|w_1|$ by x, we have $x \in X$ and $f(x) = k$.

Next, let us consider the "derived" set

$$C_2 = \{w_2, w_2w_3, \ldots, w_2w_3\ldots w_{N+1}\}$$

and let y be the value of one of its words. Then we have $x * y = x$ and hence, by (5),

$$f(x) > f(y).$$

This means that $f(|w|) \leq k-1$ for all $w \in C_2$. But C_2 has exactly N elements, which is contradictory to the assumption of the lemma.

Lemma 4. Let H, W, X and f(z) be defined as in the previous lemma. Then the length of W is less than

(7) $$(1 + s_1)(1 + s_2) \ldots (1 + s_M),$$

where M is the maximum value of f(z), or any integer exceeding that maximum value.

Proof. The assumption of lemma 3 is true for N = 1, k = 1. Hence, by the same lemma, it is also true for $N = 1+s_1$, k = 2; hence too for $N = (1+s_1)(1+s_2)$, k = 3; and so on. Since $s_k = 0$ for any k which exceeds the maximum value of f(z), one may proceed as long as one wishes, the final result being, that the amount of words in any central set is less than the positive integer (7). As the number of letters in W is equal to the number of words in the largest possible central set, lemma 4 has has been proved.

The following diophantine statement and its proof are independent of the previous text.

Lemma 5. Given $M \geq 1$ and $T \geq 1$. Then the function

$$\phi = (1 + t_1)(1 + t_2) \cdots (1 + t_M), \tag{8}$$

considered in the lattice-point region

$$\begin{cases} t_1 \geq 0, \ t_2 \geq 0, \ \cdots, \ t_M \geq 0 \\ t_1 + t_2 + \cdots + t_M \leq T, \end{cases} \tag{9}$$

takes the maximum value

$$(1 + p)^{M-\sigma} \cdot (2 + p)^{\sigma}, \tag{10}$$

where p and σ are determined by the quotient-residue formula

$$T = pM + \sigma \quad (0 \leq \sigma \leq M-1). \tag{11}$$

Proof. As the result is trivial for $M = 1$ and all T, let us assume that $M \geq 2$.

(i). Let P be a point $(t_1, t_2, \cdots, t_M)$ of (9), such that $\sum t_i < T$, then $\phi(P)$ is certainly not maximal: t_1 can be augmented by 1 and ϕ will increase.

(ii). Let P be such that $t_i - t_j \geq 2$ for at least one pair i, j, then $\phi(P)$ is not maximal: t_i can be replaced by $t_i - 1$ and t_j by $t_j + 1$; then ϕ will certainly increase. Hence, the coordinates of a maximizing point of (9) either have all the same value, or they are distributed over two consecutive integral values. In the first case, denote that value by p; in the second case, denote the two values by p and p+1.

It follows by (i) and (ii) that a maximum value can be reached only in such points, where τ coordinates have a certain value p and σ coordinates have the value p+1, whilst moreover

$$\begin{cases} \tau + \sigma = M, \\ \tau p + \sigma(p+1) = T, \\ \tau \geq 1. \end{cases}$$

Eliminating τ from these relations, we find as a necessary condition: $T = pM + \sigma$, $0 \leq \sigma \leq M-1$, which is formula (11). For the maximal value (which certainly exists) we find (10) and this proves the lemma.

Applying lemma 5 on lemma 4, we find at once the following result:

Lemma 6. Let M, W, X and $f(z)$ be defined as in lemma 3.
Let M be an integer $\geq$ the maximum value of $f(z)$.
Let T be an integer $\geq$ the number of elements of the set X.
Let p and σ be defined by the quotient-residue formula
$T = pM + \sigma$, $0 \leq \sigma \leq M-1$.

Then we have $p \geq 0$, and the length of W is less than

$$(1 + p)^{M-\sigma} \cdot (2 + p)^{\sigma}.$$

The above lemma may look like a statement which is "biting its own tail". One might remark that the set X has been defined with help of the word W, that the function $f(z)$ depends on the structure of X and hence, that all the parameters in the final estimate are depending on the word W itself, possibly in a bad way.

Luckily this is not true. We know that X is free of idempotents, so that we may take $T = n - \theta$, where n is the order of H and θ is the number of its idempotents. The indeterminate constant M will be dealt with, likewise, in the following lemma's 7 and 8. It will be shown that we may take $M = 2\theta$ in all relevant cases.

Lemma 7. Let $(H,*)$ be a finite semigroup with $\theta < n$. Let

(12) $$x_1, x_2, \ldots, x_\pi$$

be a sequence of non-idempotent elements of H, such that

(13) $$x_i * x_j = x_i \quad \text{for all pairs } i, j \text{ with } i < j.$$

Then we have: $\pi \leq 2\theta$.

Proof. Take an arbitrary x_i from the sequence (12) and consider its powers

$$x_i, x_i^2, x_i^3, \ldots\ldots .$$

It is well-known and easy to prove that this sequence contains a term which is an idempotent element of H. (This is easily seen, for instance, by applying theorem II on a word $x_i x_i \ldots x_i$ of sufficient length; but we have promised that our proof of theorem IV A would be independent of II.) Denote such an idempotent by $e(x_i)$, then $e(x_i) = x_i^p$ for some p. (The fact that there is only one element $e(x_i)$ for each x_i is not relevant here.)

If the length of (12) exceeds 2θ, there will certainly exist a sub-sequence of (12), say x, y, z, such that $e(x) = e(y) = e(z)$; this follows from the pigeon-hole principle. We have then, for some triple of positive integers q, r, s:

$$e(x) = x^q \quad , \quad e(y) = y^r \quad , \quad e(z) = z^s$$

and hence, by (13):

$$(14) \qquad \begin{cases} x * y = x, \\ y * z = y \\ x^q = y^r = z^s. \end{cases}$$

The relations (14) imply, in any semigroup, that

$$y^r = y,$$

as we have

$$y^r = x^q = x^q * y = y^r * y = y * y^r = y * z^s = y.$$

In our present case the element y, which occurs as a term in (12), would be equal to e(y), which is an idempotent. This would contradict our assumption on (12); hence the length of (12) does never exceed 2θ.

Lemma 8. Let $(H,*)$ be a finite semigroup with $\theta < n$.
Let X be a non-empty subset of H without idempotents.
Then there exists an order-function f(z) with respect to X such that

$f(z) \leq 2\theta$ for all z.

Proof. A sequence (12) with property (13) will be called an X-tail of z, if $x_1 = z$ and if moreover all the x_i (including z) are elements of X. Since (13) holds trivially true for $\pi = 1$, any $z \in X$ has at least one X-tail, a tail with length 1.

For any $z \in X$ we define $\pi(z)$ as the maximal length, which is realized among the X-tails of z. For any $z \in H \setminus X$ we define $\pi(z) = 0$. We shall now prove that $\pi(x) > \pi(y)$ for all x, y with $x \in X$ and $x * y = x$.

The assertion is trivial for $y \in H \setminus X$. For $y \in X$, let $x_1, \ldots, x_\pi$ be an X-tail of y, then we have $x_1 = y$ and it follows from $x * y = x$, that $x, x_1, \ldots, x_\pi$ is an X-tail of x. Hence we have certainly $\pi(x) > \pi(y)$.

In view of lemma 7 we have moreover: $\pi(z) \leq 2\theta$ for all z.

Thus we have proved lemma 8, with $f(z) = \pi(z)$.

Theorem IV A follows easily from lemma's 6 and 8. For $\theta = n$ the assertion is trivial. For $\theta < n$, choose a word W over H without subwords of idempotent value; define X as the set of all values of all subwords of W; define $f(z)$ according to lemma 8; take in lemma 6: $T = n - \theta$ and $M = 2\theta$. Then the formula $T = pM + \sigma$ gives $n = (2q-1)\theta + \sigma$ with $0 \leq \sigma \leq 2\theta - 1$, where $q = p+1 \geq 1$. Finally the estimate function of lemma 6 yields $L(n,\theta)$. Thus we have proved IV A.

Remark. The underlying ideas in the foregoing proof are as follows:

Let X be any subset of an arbitrary, finite semigroup $(H,*)$, which contains θ idempotents.

Define $S_0 = H \setminus X$. Define for $k \geq 0$, by induction:

$$S_{k+1} = \{x \in X \setminus \bigcup_{i=0}^{k} S_i : x * y = x \rightarrow y \in \bigcup_{i=0}^{k} S_i\}.$$

Then the following statements hold true:

(a) X will be free of idempotents if and only if the union of all S_k equals H.

(b) The number of non-empty classes S_k with $k \geq 1$ is at most 2θ.

§7. Proof of theorem IV B and the supplementary theorem

First, let us consider the indeterminate boundary length λ, as given in theorem II. Let us denote by $\lambda(H)$ the least possible value of λ for a given H. Further, let us denote the order of H by $n(H)$ and the number of its idempotents by $\theta(H)$.

Assertion IV A, which has been proved in the previous section, is equivalent to the statement that $\lambda(H)$ exists and is $\leq L(n,\theta)$, where $n = n(H)$, $\theta = \theta(H)$, for every H.

Likewise, assertion IV B can be restated as follows:

Theorem IV B*

Given a pair n, θ with $1 \leq \theta \leq n$, there is a commutative H such that

$$(14)\quad \begin{cases} n(H) = n, \\ \theta(H) = \theta, \\ \lambda(H) \geq L(n,\theta). \end{cases}$$

To prove IV B* and hence IV B, we need three lemma's. They provide information for the supplementary theorem as well.

Lemma 9. Let H_1 and H_2 be disjunct finite semigroups of an arbitrary structure. Then there is a semigroup H with the following properties:

(a) $n(H) = n(H_1) + n(H_2)$,

(b) $\theta(H) = \theta(H_1) + \theta(H_2)$,

(c) $\lambda(H) \geq \lambda(H_1)\lambda(H_2)$.

(d) If both H_1 and H_2 are commutative, so is H.

(e) H contains a sub-semigroup, which is isomorphic with H_1 and a sub-semigroup which is isomorphic with H_2.

Proof. Let us denote the operations in H_1 and H_2 by $\circ$ and Δ, respectively. We define a set H by $H = H_1 \cup H_2$ and we define in H an operation $*$ as follows:

$$(15)\qquad \begin{cases} a * b = a \circ b & \text{if } a \in H_1,\ b \in H_1. \\ a * b = a \Delta b & \text{if } a \in H_2,\ b \in H_2. \\ a * b = b * a = a & \text{if } a \in H_1,\ b \in H_2. \end{cases}$$

Then $(H,*)$ is a semigroup, satisfying (a), (b), (d) and (e). So far, the procedure is not altogether unknown, but now (c) has to be proved.

If $\lambda(H_1) = 1$ or $\lambda(H_2) = 1$, (c) is implied by (e); hence we may assume that $\lambda_1 - 1 \geq 1$ and $\lambda_2 - 1 \geq 1$, where λ_i is an abbreviation of $\lambda(H_i)$.

Let $a_1 a_2 \circ\circ\circ a_{\lambda_1 - 1}$ be a word over H, without subwords of idempotent value. Let W be a word over H_2, of length $\lambda_2 - 1$ and likewise free of subwords of idempotent value. Such words exist, by the definition of λ_i. Then the word

$$(16)\qquad W a_1 W a_2 W \circ\circ\circ W a_{\lambda_1 - 1} W \quad \text{over } H$$

consists of exactly $\lambda_1 \lambda_2 - 1$ letters; we shall prove that it has no subwords of idempotent value in H. The statement is trivial for those subwords w of (16), which are contained in one of its subwords of the form W. Next, let w be a subword of (16) which is not contained in one of the W. Then the sequence w (for w is a sequence!) certainly contains a subsequence

$$a_p,\ a_{p+1},\ \circ\circ\circ,\ a_q \qquad (1 \leq p \leq q \leq \lambda_1 - 1)$$

such that a_{p-1} and a_{q+1}, if they exist, do not occur in the sequence w. It follows then by (15) and the law of associativity, that

$$|w| = a_p * \circ\circ\circ * a_q = a_p \circ \circ\circ \circ a_q.$$

Hence $|w|$ is not idempotent.

Thus we have proved (c). It should be noted that the semigroups H_1 and H_2 may not change places in this proof, although the result is symmetric.

Lemma 10. Let $\{H_1, H_2, \ldots, H_t\}$ be a non-empty collection of disjunct finite semigroups. Then there exists a semigroup H with the following properties:

(a) $n(H) = \sum_i n(H_i)$,

(b) $\theta(H) = \sum_i \theta(H_i)$,

(c) $\lambda(H) \geq \prod_i \lambda(H_i)$.

(d) If all the H_i are commutative, so is H.

(e) H contains a sub-semigroup $\cong H_i$, for all i.

Proof. The statement is trivial for $t = 1$; the case $t = 2$ is covered by lemma 9; for $t \geq 3$ it can be proved by repeated application of lemma 9.

Lemma 10 suggests already the construction of a semigroup H, which has a critical word-length of exponential order. It is, however, not strong enough to reach the estimate (14); we shall bolster it up by the following lemma.

Lemma 11.

(a) For any positive integer q there are semigroups S, T and U such that

$n(S) = 2q-1$ $\quad$ $n(T) = 2q$ $\quad$ $n(U) = 2q+1$

$\theta(S) = 1$ $\quad$ $\theta(T) = 1$ $\quad$ $\theta(U) = 1$

$\lambda(S) \geq q^2$ $\quad$ $\lambda(T) \geq q(q+1)$ $\quad$ $\lambda(U) \geq (q+1)^2$.

(b) S can be chosen such that it is commutative.
The same holds for T and for U.

(c) S can be chosen such, that it contains a sub-semigroup which is isomorphic with an arbitrarily prescribed group G of order q.
The same holds for T.

(d) U can be chosen such as to contain a sub-semigroup, which is isomorphic with an arbitrarily prescribed group G of order q+1.

Proof. The assertions on U in the above statement are superfluous, from a logical point of view. As soon as we have verified any assertion on S for all q, the corresponding property of U has been proved as well.

For $q = 1$, the assertions on S are trivial and those on T are easy to verify. Now let $q \geq 2$. Choose an arbitrary group $(G, \circ)$ of order q and let e be its unit-element. Apart from G, choose a non-empty set

$$V = \{d_1, d_2, \ldots, d_r\}$$

of objects, which are not elements of G.
In the set $G \cup V$ we define an operation $*$ as follows:

$$(17) \qquad \begin{cases} a * b = a \circ b & \text{if } a \in G,\ b \in G, \\ a * d_i = d_i * a = a & \text{if } a \in G, \\ d_i * d_j = d_{i+j} & \text{if } i+j \leq r, \\ d_i * d_j = e & \text{if } i+j > r. \end{cases}$$

Then $G \cup V$ is a semigroup under the operation $*$. Denoting $G \cup V$ by H, we have

$$(18) \qquad n(H) = q + r,$$

$$(19) \qquad \theta(H) = 1 \quad (e \text{ is the unique idempotent});$$

(20) if G is commutative, so is H;

(21) H contains a sub-semigroup $\cong G$.

For this semigroup $(H, *)$ we shall prove:

$$(22) \qquad \lambda(H) \geq q(r+1).$$

To that end we need theorem Ib. It shows the existence of a word $a_1 a_2 \ldots a_{q-1}$ over G, without subwords of unit-value in G, hence without subwords of idempotent value in H.

Apart from this word, let us consider a word

$$W = d_1 d_1 d_1 \ldots d_1 d_1,$$

which contains exactly r letters. Then W has evidently no subwords of idempotent value.

It is easy to verify, that now the word

$$Wa_1Wa_2W \ldots Wa_{q-1}W$$

consists of exactly $q(r+1)-1$ letters. Moreover it has no subwords of idempotent value in H, as may be seen from an argument, similar to the one we have used when dealing with (16).
Thus we have proved (22). The semigroups S and T are obtained as special semigroups H by taking $r = q-1$ and $r = q$, respectively.
Their properties follow at once from (18), (19), (20), (21), (22).

Remark. The foregoing proof has many features in common with the proof of lemma 9, and our reference to (16), at the end of the proof, is perhaps somewhat disturbing. This slackness can be avoided by the following procedure: in lemma 9, take $H_1 = G$ and $H_2 = V \cup \{z\}$, where z is a zero-element which makes a semigroup of $V \cup \{z\}$. Thereupon, identify the elements z and e of $H_1 \cup H_2$ and lemma 9 will lead to lemma 11. The exact procedure requires some care, but is not unknown in the theory of semigroups.

Using lemma's 11 and 10, we are now able to prove IV B^*, which is another form of IV B.

Given a pair n, θ with $1 \leq \theta \leq n$, we define q and σ by

$$n = (2q-1)\theta + \sigma \qquad (0 \leq \sigma \leq 2\theta-1)$$

and recall that

$$L(n,\theta) = q^{2\theta-\sigma} \cdot (q+1)^{\sigma}.$$

Defining three integers α, β, γ by

$$\theta - \sigma + \left[\tfrac{1}{2}\sigma\right] = \alpha,$$

$$\sigma - 2\left[\tfrac{1}{2}\sigma\right] = \beta,$$

$$\left[\tfrac{1}{2}\sigma\right] = \gamma,$$

we find the following properties (which may justify the curious choice of these integers):

(23) $$\alpha + \beta + \gamma = \theta;$$

(24) $$\begin{cases} 2\alpha + \beta = 2\theta - \sigma \\ \beta + 2\gamma = \sigma \end{cases};$$

(25) $$\alpha \geq 0 , \quad \beta \geq 0 , \quad \gamma \geq 0;$$

(26) $$\alpha + \beta \geq 1.$$

Now we consider a collection of disjunct semigroups

(27) $$\{H_1 , H_2 , \ldots , H_\theta\},$$

such that

α semigroups are of the type S (order $2q-1$),
β semigroups are of the type T (order $2q$)
γ semigroups are of the type U (order $2q+1$),

as described in lemma 11. By the same lemma, we may take each H_i to be commutative. Then lemma (10), applied on the collection (27), leads to a commutative H with property (14). Thus theorem IV B has been proved.

For the supplementary theorem we have to make a little change of tactics, though the main procedure remains unaltered. We do not require the commutativity of the H_i in (27), but we try to make at least one of them non-commutative; in view of lemma 10 (e) this is a sufficient condition for the validity of the supplementary assertion.

In which cases can this be done?

(i) If q is even and ≥ 6, there exists a non-commutative group of order q (for instance, the symmetry group of the regular polygon with $\frac{1}{2}q$ vertices). By lemma 11(c) this group can be embedded in a semigroup of the type S, as well as in a semigroup of the type T. Now it follows from (26) that $\alpha \geq 1$ or $\beta \geq 1$. Hence, for at least one H_i a non-commutative semigroup can be taken.

(ii) If q is odd and ≥ 5, there exists a non-commutative group of order $q+1$. By lemma 11(d) this group can be embedded in a semigroup of the type U. Now suppose that $\sigma \geq 2$, then we have $\gamma = \left[\frac{1}{2}\sigma\right] \geq 1$. Hence, for at least one H_i a non-commutative semigroup may be taken.

Thus we have proved the supplementary theorem.

Remark. Our construction depends on the diophantine system (24), (25), which implies (23) and (26). If θ and σ are given and if, for the moment, we consider α, β and γ as unknowns, all the solutions of the system are given by

$$\left.\begin{aligned} \alpha_k &= \alpha_0 - k \\ \beta_k &= \beta_0 + 2k \\ \gamma_k &= \gamma_0 - k \end{aligned}\right\} \qquad (0 \leq k \leq \mathrm{Min}(\alpha_0, \gamma_0)),$$

where α_0, β_0, γ_0 is the particular solution which we have employed in our proof. In all cases where $\sigma = 0$, $\sigma = 1$ or $\sigma = 2\theta - 1$, the system (24), (25) has no other solutions than α_0, β_0, γ_0.

§8. Proof of theorem III

A necessary and sufficient condition for the validity of theorem III is the following one:

$$\max_{\theta} L(n,\theta) = L(n) \quad \text{for all } n. \tag{28}$$

The verification is easy for $n = 1$ and $n = 2$, as we have: $L(1,1) = L(1)$; $L(2,1) = L(2) = 2$; $L(2,2) = 1$.

For the rest of our proof we assume $n \geq 3$, though most of our argument will be valid for $n = 1$ and $n = 2$ as well.

Defining the integer q as before, we have

$$(2q-1)\theta \leq n \leq (2q+1)\theta - 1. \tag{29}$$

Furthermore we have, after a slight rearrangement of the definition-formula:

$$L(n,\theta) = \left(1 + \frac{1}{q}\right)^n \{E(q)\}^\theta, \tag{30}$$

where

$$E(q) = \frac{q^{2q+1}}{(q+1)^{2q-1}} = \frac{q(q+1)}{\left(1 + \frac{1}{q}\right)^{2q}} > \frac{q(q+1)}{e^2} > \frac{q(q+1)}{10}. \tag{31}$$

Hence we have, in particular,

$$E(2) = \frac{32}{27} \tag{32}$$

and

$$E(q) > 1 \quad \text{for all } q \geq 2. \tag{33}$$

After these preparations, let us first prove that

$$L(n,\theta) \leq L(n) \tag{34}$$

for all pairs n, θ. We distinguish three cases.

First we consider all pairs n, θ for which $q = 1$.

In this case we find by (29) that $\theta \geq \frac{1}{3} n + \frac{1}{3}$ and it follows that

$$L(n,\theta) = 2^{n-\theta} \leq 2^{\frac{2}{3}n} \cdot 2^{-\frac{1}{3}} < 2^{\frac{2}{3}n} \cdot \left(\frac{27}{32}\right)^{\frac{2}{3}} \leq L(n). \tag{35}$$

Next, we consider all pairs n, θ for which $q \geq 2$.

Here the other part of (29) implies that $\theta \leq \frac{n}{2q-1}$ and hence, as θ is an integer, that

$$\theta \leq \left[\frac{n}{2q-1}\right] . \tag{36}$$

By (30), (33) and (36) we conclude that

$$L(n,\theta) \leq \left(1 + \frac{1}{q}\right)^n \{E(q)\}^{\left[\frac{n}{2q-1}\right]} = q^{\frac{2n}{2q-1}} \left\{\frac{1}{E(q)}\right\}^{\frac{n}{2q-1} - \left[\frac{n}{2q-1}\right]}, \tag{37}$$

where the latter equality is a consequence of the definition of $E(q)$ in (31).

The following property is easily verified, in view of (32):

(38) For $q = 2$, the right-hand side of (37) equals $L(n)$.

This implies that (34) holds for all pairs n, θ for which $q = 2$.

Finally we consider all pairs n, θ for which $q \geq 3$.

Here (37) yields, in view of (33):

$$L(n,\theta) \leq q^{\frac{2n}{2q-1}} . \tag{39}$$

Now $q^{\frac{1}{2q-1}}$ is a decreasing function of q for $q \geq 3$; hence we find from (39):

$$L(n,\theta) \leq 3^{\frac{2n}{5}} < 2^{\frac{2n}{3}} \left(\frac{27}{32}\right)^{\frac{2}{3}} \leq L(n), \tag{40}$$

where the middle inequality requires some elementary calculation (it may be reduced to $3^3 < 2^5$).

Thus we have proved (34), but not yet (28).
The truth of (28) can be seen by a supplementary argument, from the foregoing formulae. To that end one should observe that, if in (36) the sign of equality holds, the same will be true for the first sign in (37). Thereupon, property (38) shows at once that

$$L(n, \left[\frac{n}{3}\right]) = L(n) \qquad (n \geq 3).$$

This completes the proof of theorem III.