ON SUBSEMIGROUPS OF SEMIGROUPS

JURAJ BOSÁK, Bratislava

The first part of the present paper is concerned with the investigation of subsemigroups of the cyclic and of the free semigroups. The cardinality of the system of all subsemigroups of such semigroups is determined.

The second part is concerned with the semigroups in which we obtain from subsemigroups by set-theoretical operations either subsemigroups again or the empty set.

In the paper we use the following symbols: The symbol $\delta(N)$ denotes the greatest common divisor of all elements of a given set N of natural numbers. The symbol $\tau(n)$ denotes the number of all natural divisors of the natural number n. ([1]) If $h > 1$ is a natural number, then the symbol $\mathbf{V}(h)$ denotes the system of all the sets $V \subseteq \subseteq \{1, 2, \ldots, h-1\}$ containing no number that is a linear combination of the others with natural coefficients.([2]) Put $\mathbf{V}(1) = \{\emptyset\}$. Evidently, $\emptyset \in \mathbf{V}(h)$ for each natural number h. The union or the difference and the symmetric difference of the sets A, B is denoted by the symbols $A \cup B$, $A \setminus B$, and $A \triangle B$, respectively. The complement of the set A will be denoted by A^*. The symbol $C(h, g)$, where h, g are natural numbers, denotes the cyclic (monogenic) semigroup of the type (h, g), i.e. the finite cyclic semigroup consisting of mutually distinct elements $a, a^2, \ldots, a^{h+g-1}$, where $a^{h+g} = = a^h$. The symbol $\sigma(h, g)$ denotes the number of all subsemigroups of the semigroup $C(h, g)$. The other terms and notations are used mostly according to [3, 7].

1. SUBSEMIGROUPS OF CYCLIC SEMIGROUPS

Lemma 1. *A necessary and sufficient condition for the subset T of the semigroup $C(h, g)$ to be (with respect to the given multiplication) a subsemigroup of the semigroup $C(h, g)$, is that there exists a set $V \in \mathbf{V}(h)$ and a natural $x \mid \delta(V \cup g)$ such that $T = = [a^V] \cup e[a^x]$, where e is the idempotent, a the generator of the semigroup $C(h, g)$.([3])*

([1]) It is well-known that if the natural $n > 1$ has the canonical decomposition into primes $n = = p^k q^l \ldots r^m$, then $\tau(n) = (k+1)(l+1)\ldots(m+1)$. Evidently, $\tau(1) = 1$.

([2]) i.e., no number $v \in V$ can be written in the form $v = ks + lt + \ldots + mu$, where $k, l \ldots, m$ are naturals, $s, t, \ldots, u$ are elements of the set V, different from v.

([3]) We write $a \mid b$, if a divides b. We also use the symbol $a^V = \{a^v : v \in V\}$. The symbol $[T]$ denotes the subsemigroup generated by the set T. The braces will be omitted where any misunderstanding is out of the question.

Proof. I. Prove that for each $V \in \mathbf{V}(h)$, $x \mid \delta(V \cup g)$ the set

$$T = [a^V] \cup e[a^x]$$

is a subsemigroup of the semigroup S. Evidently, it is sufficient to prove that:

$$b \in [a^V], \quad c \in e[a^x] \Rightarrow bc \in e[a^x].$$

There exist naturals m, n such that $b = a^m$, $c = ea^{nx}$. Since $a^m \in [a^V]$, m is a linear combination of the elements from V; as x divides all elements from V, we have $x \mid m$. Further, $x \mid g$, i.e. $\delta(x, g) = x \mid m$ and evidently also $\delta(x, g) \mid nx$ so that $\delta(x, g) \mid m + nx$, therefore the Diophantine equation

$$m + nx = ix - jg$$

has natural solutions i, j. Therefore $bc = a^m ea^{nx} = ea^{m+nx} = ea^{m+nx+jg} = ea^{ix} = e(a^x)^i \in e[a^x]$.

II. Let T be a subsemigroup of the semigroup $C(h, g)$. Let T_2 be the maximal group of the semigroup T; put $T_1 = T \setminus T_2$. Form the set of all naturals k such that $a^k \in T_1$ and delete those which are linear combinations (with natural coefficients) of the others. In this way we obtain a certain set $V \in \mathbf{V}(h)$. Denote by the symbol x the least natural number with the property $ea^x \in T$. Prove that $x \mid \delta(V \cup g)$. If we denote $ea = d$, then $\{d, d^2, \ldots, d^g = e\}$ is the maximal group of the semigroup $C(h, g)$, T_2 is its subgroup. Therefore T_2 is the cyclic group generated by $d^x = ea^x$, where x is the least natural number for which $d^x \in T_2$; from this it easily follows that $x \mid g$. If $x \mid v$ did not hold for some $v \in V$, then the Diophantine equation

$$ix + jg = v$$

would not have integer solutions i, j. On the other hand the element

$$a^{v+vhg} = (a^v)^{gh+1} \in T_2$$

so that it can be written in the form $(d^x)^m = ea^{mx} = a^{ghx} a^{mx} = a^{(gh+m)x}$ where m is a natural number. Hence $a^{(gh+m)x} = a^{v+vhg}$. Two elements of the finite cyclic semigroup, written as powers of the same generator, can be equal only if their exponents differ by the integer multiple of the "period" (g in our case). Consequently, $v + vgh - (gh + m)x = ng$ where n is an integer. Hence the equation (2) has the solution $i = gh + m$, $j = n - vh$, which is a contradiction. Thus it is proved that x divides all elements from V, and since $x \mid g$, we have also $x \mid \delta(V \cup g)$.

Let us prove further that under the given choice of V and x the equality (1) is valid.

Choose $b \in T$. If $b \in T_1$, then evidently $b \in [a^V]$. It is therefore sufficient to consider the case where $b \in T_2$. According to what has been said, $T_2 = [ea^x] = e[a^x]$, so that $b \in [ea^x]$. Hence in both cases $b \in [a^V] \cup e[a^x]$.

Conversely, pick $c \in [a^V] \cup e[a^x]$. If $c \in [a^V]$, then evidently $c \in T$. Further if

$c \in e[a^x] = [ea^x]$, since $ea^x \in T$ and T is a semigroup, we have $[ea^x] \subseteq [T] = T$, whence it follows that $c \in T$.

The proof is accomplished.

Theorem 1. *The number $\sigma(h, g)$ of all subsemigroups of the finite cyclic semigroup $C(h, g)$ is*

$$\sum_{V \in \mathbf{V}(h)} \tau[\delta(V \cup g)].$$

Proof. Let a be the generator, e the idempotent of the semigroup $C(h, g)$. According to lemma 1 all subsemigroups of the semigroup $C(h, g)$ have the form

$$T = [a^V] \cup e[a^x],$$

where $V \in \mathbf{V}(h)$, $x \mid \delta(V \cup g)$.

Let us prove first that by the choice of the subsemigroup T, V and x are uniquely determined. Let us assume that $W \in \mathbf{V}(h)$ and the natural number $y \mid \delta(W \cup g)$ also determine the subsemigroup T. As $[a^V] \cup e[a^x] = [a^W] \cup e[a^y]$, we have $V = W$. Assume that $x \neq y$. Let e.g., $x < y$. We have $ea^x \in T = [a^W] \cup e[a^y]$. Without loos of generality we can write $ea^x \in e[a^y]$, for if $ea^x \in [a^W]$, then $ea^x = a^w$, where w is a linear combination (with natural coefficients) of the elements of W. Since $y \mid \delta(W \cup g)$, we have $y \mid w$, so that we can write $a^w = a^{yz}$, where z is a natural number. Consequently, we have $ea^x = e^2 a^x = e(ea^x) = ea^w = ea^{yz} \in e[a^y]$. Hence always $ea^x \in e[a^y]$, so that $ea^x = ea^{ly}$, where l is a natural number. Pick the natural number n such that $a^n = e$. From the condition $ea^x = ea^{ly}$ we obtain $a^{n+x} = a^{n+ly}$. We therefore have $n + x - (n + ly) = kg$ where k is an integer. Thus the Diophantine equation

$$kg + ly = x$$

has integer solutions k, l. Therefore $y = \delta(y, g) \mid x$, which is according to the condition $x < y$ not possible (x, y are naturals!).

The assumption of theorem 1 can now be easily proved, if, with each fixed chosen $V \in \mathbf{V}(h)$, we count all possible subsemigroups; there are as many as there are divisors of the number $\delta(V \cup g)$, i.e. $\tau(\delta(V \cup g))$.

Corollaries. 1. *The number $\sigma(1, g)$ of all subsemigroups of the semigroup $C(1, g)$, i.e., of the cyclic group of the finite order g, is $\tau(g)$. The number of all subgroups of the semigroup $C(h, g)$ is $\tau(g)$.*

2. $\sigma(2, g) = \tau(g) + 1$.

3. $\sigma(3, g) = \begin{cases} \tau(g) + 2, \text{ if } g \text{ is odd,} \\ \tau(g) + 3, \text{ if } g \text{ is even.} \end{cases}$

4. $\sigma(4, g) = \begin{cases} \tau(g) + 4, \text{ if } g \text{ is divisible neither by 2 nor by 3,} \\ \tau(g) + 5, \text{ if } g \text{ is divisible either by 2 or by 3, but not by 6,} \\ \tau(g) + 6, \text{ if } g \text{ is divisible by 6.} \end{cases}$

5. $\sigma(5, g) = \begin{cases} \tau(g) + 6, \text{ if } g \text{ is divisible neither by 2 nor by 3,} \\ \tau(g) + 7, \text{ if } g \text{ is divisible by 3, but not by 2,} \\ \tau(g) + 8, \text{ if } g \text{ is divisible by 2, but neither by 3 nor by 4,} \\ \tau(g) + 9, \text{ if } g \text{ is divisible either by 4 or by 6, but not by 12,} \\ \tau(g) + 10, \text{ if } g \text{ is divisible by 12.} \end{cases}$

The proof of corollaries 1–5 can be established with the help of the formula from theorem 1. Considering corollary 1, however, we must remember that each subgroup of the semigroup $C(h, g)$ is contained in the maximal subgroup, isomorphic with the semigroup $C(1, g)$ and that each subsemigroup of the finite group is a group.

Theorem 2. *Denote the number of sets of the system* $V(h)$ *by the symbol* $\omega(h)$. *We then have:*

$$\tau(g) + \omega(h) - 1 \leqq \sigma(h, g) \leqq \tau(g) + \sum_{\substack{V \in V(h) \\ V \neq 0}} \tau(\delta(V)).$$

Proof. From theorem 1 it follows that the difference $\varrho_h(g) = \sigma(h, g) - \tau(g)$ reaches a minimum with a fixed h, if $g = 1$, namely $\varrho_h(1) = \omega(h) - 1$. $\varrho_h(g)$ reaches a maximum, if $g = h!$, namely $\varrho_h(h!) = \Sigma\, \tau(\delta(V))$ where the summation is taken over all $V \in V(h)$ not equal to $\emptyset$. Whence follow the proved inequalities.

Corollary. $\tau(g) + h - 1 \leqq \sigma(h, g) \leqq \tau(g) + (2^{h-1} - 1)(h - 1)$.

The proof follows if we use elementary estimates for the expressions in the inequalities of theorem 2.

Theorem 3. *Let* S *be a free semigroup over the set* M. *Then it is true for the cardinality* f *of the system of all subsemigroups of the semigroup* S *that:*(4)

$$f = \begin{cases} \aleph_0, & \text{if } |M| = 1, \\ \aleph, & \text{if } 1 < |M| < \aleph_0, \\ 2^{|M|} & \text{if } |M| \geqq \aleph_0. \end{cases}$$

Proof. I. Let $|M| = 1$. Denote the (single) element of the set M by the symbol a; then $S = \{a, a^2, a^3, \ldots\}$ is an infinite cyclic semigroup. Since $[a]$, $[a^2]$, $[a^3]$, ... are mutually different subsemigroups of the semigroup S, $f \geqq \aleph_0$. To prove that $f \leqq \aleph_0$, let us assign to any subsemigroup T of the semigroup S a finite set T' of naturals thus: Let n be the smallest natural number such that $a^n \in T$. T' will then consist of the number n and of all naturals $t > n$ such that $a^t \in T$, but $a^{t-n} \bar{\in} T$. T' is a finite set, since from each residue class modulo n it contains at most one element. Evidently, different finite sets are assigned to different subsemigroups. Hence the number f of all subsemigroups of the semigroup S can be only less than or equal to the number of all finite sets of naturals. Therefore $f \leqq \aleph_0$. From the assertions $f \leqq \aleph_0$, $f \geqq \aleph_0$ it follows that $f = \aleph_0$.

(4) The symbol $|M|$ denotes the cardinality of the set M.

II. Let $1 < |M| < \aleph_0$. Then $|S| = \aleph_0$, therefore the cardinality of the system of all subsets of the set S is $2^{|S|} = 2^{\aleph_0} = \aleph$, so that $f \leqq \aleph$. It is therefore sufficient to prove that $f \geqq \aleph$. Let us choose $a, b \in M$ $(a \neq b)$. Let us form the set $M^* = \{ab, ab^2, ab^3, \ldots\}$. The set M^* has $\aleph$ subsets, each of which generates a different subsemigroup of the semigroup S. Therefore $f \geqq \aleph$.

III. Let $|M| \geqq \aleph_0$. Then $|S| = |M|$, so that $f \leqq 2^{|S|} = 2^{|M|}$. The set M has $2^{|M|}$ subsets, each of which generates a different subsemigroup of the semigroup S. Therefore $f \geqq 2^{|M|}$, and hence $f = 2^{|M|}$.

Note 1. It evidently follows from the proof that the theorem remains valid if, in addition, we suppose the validity of the commutative law in S.

Note 2. The first assertion of theorem 3 (case $|M| = 1$) says that the infinite cyclic semigroup has exactly $\aleph_0$ subsemigroups.

Theorem 4. *All cyclic semigroups* S, *including exactly* n *subsemigroups* $(n \leqq 5)$ *are given in table* 1 *(where* p, q *are primes).*

Table 1

n	S	
1	$C(1,1)$	
2	$C(2,1)$ $C(1,p)$	
3	$C(3,1)$ $C(2,p)$ $C(1,p^2)$	
4	$C(3,p)$ $C(2,p^2)$ $C(1,p^3)$ $C(1,pq)$	$p \neq 2$ $p \neq q$
5	$C(4,1)$ $C(3,2)$ $C(3,p^2)$ $C(2,p^3)$ $C(2,pq)$ $C(1,p^4)$	 $p \neq 2$ $p \neq q$

The proof follows from the inequalities $h \geqq 1$, $\tau(g) \geqq 1$, $\tau(g) + h - 1 \leqq \sigma(h, g) \leqq 5$ (corollary of theorem 2) and from the evaluation of the function $\tau(g)$ according to(1). The semigroups that can be considered under these conditions will be verified

according to the corollaries of theorem 1 and the number of their subsemigroups will be found. We shall see that, apart from $C(3, 4)$ and $C(4, p)$, all of them have less than 6 subsemigroups.

Note. The mentioned results were used in [2] to obtain some results formulated and partly also deduced with the help of the theory of graphs. Conversely, using [2], we can easily establish some results, closely related to the subject of our investigation and not using any terms from the theory of graphs. These are the results:

1. A semigroup has no proper subsemigroups if and only if it has a single element. It follows from lemma 2 in [2]; this result, of course, is evident directly; we are mentioning it for the sake of completeness.

2. A semigroup has no proper subsemigroups([5]) apart from one-element subsemigroups if and only if it has less than three elements or if it is a cyclic group of a prime order. (This follows from theorems 2 and 3 in [2].) Tamura devotes his paper [13] to another proof of this assertion. Both assertions are found in Chion [5], generalized for convex subsemigroups of partially ordered semigroups.

3. A semigroup has a finite number of subsemigroups if and only if it is finite. This follows from lemma 2 in article [2].

4. If a semigroup has less than 5 subsemigroups then it either consists of two idempotents or has a single idempotent. All semigroups with less than 5 subsemigroup are determined in theorem 3 in [2].

2. SEMIGROUPS WHOSE SYSTEM OF SUBSEMIGROUPS IS CLOSED WITH RESPECT TO CERTAIN SET OPERATIONS

It is well-known that the system of all subsemigroups of a given semigroup (with the empty set added) is closed with respect to the operation of intersection so that the intersection of two subsemigroups is always a subsemigroup or an empty set $\emptyset$. In [1] we considered semigroups with a system of subsemigroups closed with respect to the operation of union. Such semigroups are a special case of semigroups with a distributive lattice of subsemigroups (with the empty set added and with the ordering by means of the set inclusion); this lattice will be denoted by Σ' – see, e.g. [10]. With the investigation of semigroups S, for which $\Sigma'(S)$ is a distributive lattice, papers [4, 10] are concerned. Now we shall consider semigroups with a system of subsemigroups (and $\emptyset$) closed with respect to other set operations. I wish to mention that the systems of sets closed with respect to certain set operations were studied by Kluvánek [6] from an abstract point of view.

([5]) Tamura [13] does not consider one-element subsemigroups as proper subsemigroups. We use the term proper subsemigroups of the semigroup S in the sense of Lyapin [7], i.e., as subsemigroups that are different from S.

Theorem 5. *The following five assertions are equivalent:*

(1) *The set difference of any two subsemigroups of the semigroup S is either a subsemigroup of the semigroup S or $\emptyset$;*

(2) *The symmetric difference of any two subsemigroups of the semigroup S is either a subsemigroup of the semigroup S or $\emptyset$;*

(3) *The complement of any proper subsemigroup of the semigroup S is the proper subsemigroup of the semigroup S;*

(4) *It is true for any two elements a,b of the semigroup S that $ab \in \{a, b\}$;*

(5) *All non-empty subsets of the semigroup S are, with respect to the given multiplication, subsemigroups.*

Proof. It is evidently true that (4) $\Rightarrow$ (5), (5) $\Rightarrow$ (1). The implication (1) $\Rightarrow$ (2) follows from the relation

$$A \triangle B = \{S \setminus [(S \setminus A) \setminus B]\} \setminus [A \setminus (A \setminus B)],$$

valid for any $A \subseteq S$, $B \subseteq S$. The implication (2) $\Rightarrow$ (3) follows from the relation

$$A^* = S \triangle A,$$

valid for any $A \subseteq S$. Therefore only the implication (3) $\Rightarrow$ (4) remains to be proved.

Let (3) hold. We shall prove first that any element $a \in S$ is an idempotent. Since $[a^2]$ is a semigroup, $[a^2]^*$ must also be either a semigroup or the empty set. If $a \in [a^2]^*$, then would $a^2 \in [a^2]^*$, which is impossible. Therefore $a \bar{\in} [a^2]^*$, so that $a \in [a^2]$. Whence it follows that the element a has a finite order and the semigroup $[a]$ contains an idempotent; denote it by e. $\{e\}$ is a semigroup, therefore also $\{e\}^*$ is a semigroup or the empty set. If $a \neq e$, then would $a \in \{e\}^*$, and consequently $\{e\}^* \neq \emptyset$. Therefore e (i. e., a power of the element a) also belongs to the semigroup $\{e\}^*$, which is not possible, since $e \in \{e\}$. There remains the only possibility that $a = e$, i.e., a is an idempotent.

Let $a,b \in S$. The element ab is an idempotent; therefore $\{ab\}$ is a semigroup, $\{ab\}^*$ is either a semigroup or an $\emptyset$. If $a \in \{ab\}^*$, and $b \in \{ab\}^*$ as well, then $\{ab\}^* \neq \emptyset$, i.e. $\{ab\}^*$ would be a semigroup; in that case also $ab \in \{ab\}^*$, which is impossible. Therefore either a or b belongs to $\{ab\}$, i.e. $ab \in \{a, b\}$.

Notes. Shevrin [9, 10, 11] proved that conditions (4) or (5) are equivalent with any of the following conditions (he calls such semigroups a "strong band of one-element semigroups"):

(6) $\Sigma'(S)$ is a complemented lattice with unique complements;

(7) $\Sigma'(S)$ is a modular lattice with complements;

(8) $\Sigma'(S)$ is a Boolean algebra;

and in case of a commutative semigroup S even with the following condition:

(9) $\Sigma'(S)$ is a complemented lattice.

Ego [4, theorem 8.4] mentions similar results. The structure of all semigroups,

fulfilling condition (5) was described by Rédei [8, theorem 50, p. 85]. The semigroups S, whose system $\Sigma(S)$ of all subsemigroups (without $\emptyset$) is a Boolean algebra, are considered in [12].

REFERENCES

[1] Bosák J., *B-pologrupy*, Mat.-fyz. časopis *11* (1961), 32—44.

[2] Bosák J., *The graphs of semigroups*, Theory of graphs and its applications, Proceedings of the Symposium held in Smolenice in June 1963, Praha 1964, 119—125.

[3] Clifford A. H., Preston G. B., *The Algebraic Theory of Semigroups I.*, Mathematical Surveys 7, Providence 1961.

[4] Ego M., *Structure des demi-groupes dont le treilis des sous-demi-groupes satisfait a certaines conditions*, Bull. Soc. math. France *91* (1963), 137—201.

[5] Хион Я. В., *О частично упорядоченных полугруппах, в которых собственные выпуклые подполугруппы не пересекаются*, Известия АН СССР 27 (1963), 67—74.

[6] Kluvánek I., *O množinových systémoch uzavretých vzhľadom na niektoré množinové operácie*, Mat.-fyz. časopis *5* (1955), 191—211.

[7] Ляпин Е. С., *Полугруппы*, Москва 1960.

[8] Rédei L., *Algebra I.*, Leipzig 1959.

[9] Шеврин Л. Н., *Полугруппы, структура подполугрупп которых обладает относительными дополнениями*, ДАН СССР *144* (1962), 72—75.

[10] Шеврин Л. Н., *О структурных свойствах полугрупп*, Сибирский матем. журн. *3* (1962), 446—470.

[11] Шеврин Л. Н., *Полугруппы, структура подполугрупп которых есть структура с единственными дополнениями*, Сибирский матем. журн. *4* (1963), 709—711.

[12] Tamura T., *On semigroup whose subsemigroup semilattice is the Boolean algebra of all subsets of a set*, J. Gakugei Tokushima Univ. *12* (1961), 1—3.

[13] Tamura T., *Note on semigroup having no proper subsemigroup*, Proc. Jap. Acad. *37* (1961), 72—74.

Received August 15, 1963.

ČSAV, Kabinet matematiky
Slovenskej akadémie vied,
Bratislava

О ПОДПОЛУГРУППАХ ПОЛУГРУПП

Юрай Босак

Резюме

В статье устанавливается мощность множества всех подполугрупп циклической полугруппы и свободной полугруппы с произвольным числом образующих. В работе найдены все циклические полугруппы с меньше, чем 6 подполугруппами, и дана характеризация полугрупп, система подполугрупп которых замкнута относительно некоторых теоретико-множественных операций. Указывается, какие дальнейшие результаты можно получить из [2] при помощи теории графов. Полученные результаты сравниваются с результатами других авторов.