AN EXTENSION PROBLEM FOR CANCELLATIVE SEMIGROUPS[1]

BY

CHARLES V. HEUER[2] AND DONALD W. MILLER

1. **Introduction and summary**. If S is a cancellative semigroup with idempotent e then e is necessarily the identity element of S, and the set G of all elements of S having inverses with respect to e in S is the unique maximal subgroup of S. Furthermore if S is not a group then the complement, T, of G in S is a maximal proper ideal of S and is, in fact, the only maximal proper ideal of S.

Henceforth whenever we write $S = G \cup T$, where S is a cancellative semigroup with idempotent, it will be assumed that S is not a group and that G and T denote the unique maximal subgroup of S and the unique maximal proper ideal of S, respectively.

These considerations suggest the following problems:

(I) Given a group G, under what conditions does there exist a cancellative semigroup $S = G \cup T$ for some cancellative semigroup T?

(II) Given a cancellative semigroup T without idempotent, under what conditions does there exist a cancellative semigroup $S = G \cup T$ for some nontrivial group G?

(III) Given a group G and a cancellative semigroup T without idempotent, under what conditions does there exist a cancellative semigroup $S = G \cup T$?

The restriction of Problem (II) to nontrivial groups is desirable since, given a cancellative semigroup T without idempotent, the semigroup S obtained by adjoining an identity element to T has trivial maximal subgroup and has T as the complementary maximal ideal.

Each of these problems is readily seen to be equivalent to an extension problem for cancellative semigroups[3]. This is a consequence of the fact that a cancellative semigroup S with idempotent is not a group if and only if S is an extension of the cancellative semigroup T by the group with zero G^0, where G and T are as defined above.

Presented to the Society, August 30, 1963; received by the editors December 2, 1963.

(1) The authors are indebted to Trevor Evans for raising some of the questions on which the paper is based.

(2) Under the partial support of a National Science Foundation Cooperative Fellowship and a National Science Foundation Graduate Fellowship.

(3) The reader is referred to [1] for notation and terminology.

It is shown in §2 that every group is the maximal subgroup of some cancellative semigroup which is not itself a group.

§3 is devoted to a consideration of commutative cancellative semigroups which have a basis. It is shown that if T is a finite-dimensional commutative cancellative semigroup without idempotent and G is a group, then there exists a cancellative semigroup S which is an extension of T by G^0 if and only if G is commutative of order dividing the dimension of T and T is a homomorph of one of a class of specified finitely generated cancellative semigroups. An analogous result is obtained if the assumption that T is finite-dimensional is replaced by the hypothesis that T possesses a basis; in this case, however, we also assume that G is finitely generated.

§4 is concerned with commutative cancellative semigroups which are not assumed to possess a basis, and problem (II) is solved for such semigroups. Specifically, if T is a given commutative cancellative semigroup without idempotent then a cancellative semigroup $S = G \cup T$ exists for some nontrivial group G if and only if there exist distinct elements x, y in T such that $xT = yT$.

In the final section noncommutative cancellative semigroups which possess a basis are considered. It is shown that given an arbitrary pair m, n of positive integers there exists a cancellative semigroup $S = G \cup T$, where G has order n and T has dimension m, if and only if $n \leqq m$.

2. **Preliminary remarks.** As in [1] the cardinal of a set A will be denoted by $|A|$. If B is a subset of a set A then $A \backslash B$ will denote the complement of B in A. The empty set will be denoted by $\varnothing$. If S is a semigroup without identity then S^1 will denote the semigroup obtained by adjoining an identity element, say 1, to S.

Now let S be a cancellative semigroup with idempotent e. Then for all elements x of S, $xe^2 = xe$ which, by cancellativity, implies that $xe = x$. Similarly $ex = x$ so e is the identity element of S.

Let a, b be elements of S such that $ab = e$. Then $bab = be = b = eb$ so, by cancellativity, it follows that $ba = e$. Thus if $x \in S$ then any one-sided inverse of x relative to e in S is necessarily a two-sided inverse. If an element x of S possesses a (necessarily unique) inverse y relative to e in S we will write $y = x^{-1}$. Then also $y^{-1} = x$, i.e. $(x^{-1})^{-1} = x$ whenever x^{-1} exists in S.

Denote by G the subset of S consisting of all elements of S which have an inverse relative to e in S. If $g \in G$ then $gg^{-1} = g^{-1}g = e$ so $g^{-1} \in G$, and if also $h \in G$ then $(gh)(h^{-1}g^{-1}) = e$ so gh is in G. Hence G is a subgroup of S, maximal by definition since e is the only idempotent in S.

Assuming that S is not a group, let $T = S \backslash G$. Suppose there exist $a \in T$ and $x \in S$ such that $ax \in G$. Then, setting $g = (ax)^{-1}$, $a(xg) = e$ so $a \in G$, a contradiction. Similarly $xa \in T$ for all $a \in T$ and $x \in S$, so T is an ideal of S.

Let A be any proper ideal of S. If $A \cap G \neq \varnothing$ let $g \in A \cap G$. Then

$G = Gg \subseteq GA \subseteq A$, so $e \in A$. Hence $S = Se \subseteq A$, a contradiction. Thus $A \cap G = \emptyset$ so $A \subseteq T$. Consequently T is a maximal proper ideal of S and is unique with this property.

Thus we have established that a cancellative semigroup S which contains an idempotent and is not a group must contain a unique maximal subgroup G and a unique maximal proper ideal T. Furthermore G and T partition S.

The following two lemmas, the first of which was proved in §1, are stated for later reference.

LEMMA 2.1. *Let S be a cancellative semigroup. If S contains an element f such that $af = a$ or $fa = a$ for some a in S, then f is an identity element for S.*

LEMMA 2.2. *Let $S = G \cup T$ be a cancellative semigroup with idempotent. Then T contains no idempotent.*

Proof. An immediate consequence of Lemma 2.1 and the definitions of G and T.

The next lemma provides a solution to problem (I).

LEMMA 2.3. *If H is an arbitrary group then there exists a cancellative semigroup $S = G \cup T$ for some cancellative semigroup T without idempotent such that G is isomorphic to H.*

Proof. Let U be any cancellative semigroup without idempotent and let S be the direct product of H and U^1. Then, writing $S = G \cup T$ we see at once that G and T are respectively isomorphic to H and $H \times U$.

LEMMA 2.4. *Let S be a cancellative semigroup and let I be an ideal of S. If I is commutative then S is commutative.*

Proof. Let $s_1, s_2 \in S$ and $t_1, t_2 \in I$. Then

$$\begin{aligned}(s_1s_2)(t_1t_2) &= s_1((s_2t_1)t_2) = s_1(t_2(s_2t_1)) = (s_1t_2)(s_2t_1)\\ &= (s_2t_1)(s_1t_2) = s_2(t_1(s_1t_2)) = s_2((s_1t_2)t_1)\\ &= (s_2s_1)(t_2t_1) = (s_2s_1)(t_1t_2)\end{aligned}$$

so, by cancellativity, $s_1s_2 = s_2s_1$.

With respect to problem (III), it follows from Lemma 2.4 that if T is commutative then G must also be commutative and in fact that any cancellative semigroup $S = G \cup T$ (if such exists) must be commutative.

3. **Problem (III): the commutative case.** A nonempty subset W of a semigroup S is said to *generate* S if no proper subsemigroup of S contains W. Equivalently, W generates S if and only if every element a of S is expressible as a finite product $a = w_1w_2 \cdots w_m$, where each w_i is contained in W.

A subset B of a semigroup S is called a *basis* for S if (i) B generates S and (ii) no proper subset of B generates S.

LEMMA 3.1. *A commutative cancellative semigroup S without idempotent has at most one basis.*

Proof. Let $A = \{a_1, a_2, \cdots\}$ and $B = \{b_1, b_2, \cdots\}$ be bases for S(4). It is sufficient to show that an arbitrary element, say a_1, of A must also lie in B.

Since B is a basis for S there exist elements $b_1, b_2, \cdots, b_k$, say, in B and positive integers $\alpha_1, \alpha_2, \cdots, \alpha_k$ such that

$$a_1 = b_1^{\alpha_1} b_2^{\alpha_2} \cdots b_k^{\alpha_k}. \tag{3.1}$$

Similarly since A is a basis for S there exist elements $a_1, a_2, \cdots, a_n$ in A and non-negative integers β_{ij} $(i = 1, 2, \cdots, k;\ j = 1, 2, \cdots, n)$ such that

$$b_i = a_1^{\beta_{i1}} a_2^{\beta_{i2}} \cdots a_n^{\beta_{in}} \qquad (i = 1, 2, \cdots, k)\ (5). \tag{3.2}$$

Combining (3.1) and (3.2) we obtain

$$a_1 = a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n}, \tag{3.3}$$

where

$$e_j = \sum_{i=1}^{k} \beta_{ij}\alpha_i \qquad (j = 1, 2, \cdots, n).$$

From (3.3) and the fact that A is a basis for S it follows that $e_1 > 0$. However S has no idempotent so, by Lemma 2.1, $e_1 = 1$ and $e_j = 0$ for $j = 2, \cdots, n$.

Since $\alpha_i > 0$ and $\beta_{i1} \geqq 0$ for $i = 1, 2, \cdots, k$, there must exist an integer m, $1 \leqq m \leqq k$, such that

$$\beta_{m1}\alpha_m = 1 \text{ and } \beta_{i1}\alpha_i = 0 \text{ for all } i \neq m.$$

Therefore $\beta_{m1} = \alpha_m = 1$. It then follows from (3.1) that $a_1 = b_m y$ and from (3.2) that $b_m = a_1 z$, where y and z are suitable elements of S^1. Hence $a_1 = b_m y = a_1 zy$ so, by Lemma 2.1, $z = y = 1$. Thus $a_1 = b_m \in B$, which completes the proof.

If S is a semigroup with a basis of n elements (where n is a positive integer) and no basis of fewer than n elements, then n will be called the *dimension* of S. S will then be called *finite-dimensional* or, more specifically, *n-dimensional.*

LEMMA 3.2. *Let S be a commutative cancellative semigroup with idempotent and write $S = G \cup T$. If T has a basis B then $GB = B$.*

(4) The use of integral subscripts is solely for notational convenience; nowhere in the remainder of the proof will it be assumed that A or B is countable.

(5) For any s in S, s^0 will be interpreted as the identity element, 1, of S^1. It is not an element of S.

Proof. Let B be a basis of T. It is clear that $B \subseteq GB$ since, by Lemma 2.1, the identity element e of G is an identity element for all of S. Hence we need only show that $GB \subseteq B$.

Let $b_1 \in B$ and $g \in G$. If $g = e$ then trivially $gB \subseteq B$ so assume the contrary. There must exist distinct elements $b_1, b_2, \cdots, b_n$ of B and nonnegative integers $r_1, r_2, \cdots, r_n$ such that $gb_1 = b_1^{r_1} \cdots b_n^{r_n}$. If $r_1 > 0$ then, by cancellativity, $g = b_1^{r_1 - 1} b_2^{r_2} \cdots b_n^{r_n}$. But this implies that either $g \in T$ or $g = 1$ (i.e. g is the empty word), both of which are impossible. Hence $r_1 = 0$, so

$$gb_1 = b_2^{r_2} \cdots b_n^{r_n}, \tag{3.4}$$

where we can assume without loss of generality that $r_i > 0$ for $i = 2, \cdots, n$.

Now consider the element $g^{-1}b_2 = y$ of T. By (3.4),

$$b_1 b_2 = gg^{-1} b_1 b_2 = (gb_1)(g^{-1}b_2) = b_2^{r_2} \cdots b_n^{r_n} y.$$

Since $r_2 > 0$ it follows that

$$b_1 = b_2^{r_2 - 1} \cdots b_n^{r_n} y.$$

Because the b_i are distinct and B is a basis for T, we must have that $y = zb_1$ for some z in T^1. Furthermore, since T contains no idempotent, it follows from Lemma 2.1 that $b_2^{r_2 - 1} \cdots b_n^{r_n} z$ is the empty word. Hence $r_2 = 1$ and $n = 2$. We conclude from (3.4) that $gb_1 = b_2 \in B$. Consequently $gB \subseteq B$ for all g in G, proving the lemma.

LEMMA 3.3. *Let $S = G \cup T$ be a commutative cancellative semigroup with idempotent. If T has a basis B then $|G| \leqq |B|$. Furthermore if B is finite then $|G|$ divides $|B|$.*

Proof. Let B be a basis of T and let b be an arbitrary but fixed element of B. By Lemma 3.2 the mapping $g \to gb$ carries G into B. Furthermore the mapping is one-to-one since S is cancellative. Hence $|G| \leqq |B|$.

Suppose now that B is finite. Define the binary relation ρ on B by

$$b_i \rho b_j \text{ if and only if } Gb_i = Gb_j, \quad \text{all } b_i, b_j \in B.$$

Clearly ρ is an equivalence relation on B, so ρ induces a partition of B into equivalence classes, say $B_1, \cdots, B_n$. For each i, $1 \leqq i \leqq n$, let b_i be an arbitrary but fixed element of B_i and consider the mapping ϕ_i of G defined by

$$\phi_i \colon g \to gb_i, \quad \text{all} \quad \in G.$$

By the cancellativity of S, ϕ_i is one-to-one. Furthermore ϕ_i maps G onto B_i since for $x, y \in B$, $x\rho y$ if and only if $gx = y$ for some $g \in G$. Hence $|G| = |B_i|$ for $i = 1, \cdots, n$ so $|B| = n\,|G|$.

For use in a later theorem we will now construct a particular commutative cancellative semigroup T.

Let $r_0, r_1, \cdots, r_n$ be a set of integers such that $r_0 \geqq 1$ and, for $i = 1, \cdots, n$, $r_i \geqq 2$. Let X be the set of all vectors $x = (x_0, x_1, \cdots, x_n)$, where $0 \leqq x_i < r_i$ for $i = 0, 1, \cdots, n$, and let

$$m = |X| = \prod_{i=0}^{n} r_i.$$

Let T be a commutative cancellative semigroup generated by X subject to the following defining relations. For any x, y, u, v in X, we require that

$$xy = uv \tag{3.5}$$

be a relation in T whenever we have for some integer i, $1 \leqq i \leqq n$,

$$x_i + y_i \equiv u_i + z_i \pmod{r_i} \tag{i}$$

and

$$x_j = u_j \text{ and } y_j = v_j, \text{ all } j = 1, \cdots, n \text{ such that } j \neq i. \tag{ii}$$

If $w_1 = w_2$ and $w_3 = w_4$ are relations in an arbitrary semigroup S then the relation $w_1 w_3 = w_2 w_4$ will be called the *product of the relations* $w_1 = w_2$ *and* $w_3 = w_4$.

LEMMA 3.4. *The cancellative semigroup T has dimension m.*

Proof. By Lemma 3.1 it is sufficient to show that X is a basis of T. Since X generates T we need only show that, for $x \in X$, the relation $x = \prod_{y \in Y} y$, where $Y \subseteq X \backslash \{x\}$ and where the elements y of Y may appear any finite number of times or not at all, is not a consequence of the generating relations (3.5).

Note that each of the relations (3.5) is of the form

$$\prod_{x \in X_1} x = \prod_{y \in Y_1} y, \tag{3.6}$$

where X_1 and Y_1 are subsets of X such that, for $i = 0, 1, \cdots, n$,

$$\sum_{x \in X_1} x_i \equiv \sum_{y \in Y_1} y_i \pmod{r_i}, \tag{3.7}$$

and

$$|X_1| = |Y_1|.$$

Furthermore any product of relations of the form (3.6) is again of the form (3.6), as is any relation obtained from a relation of the form (3.6) by cancellation. Consequently every relation which is a consequence of the relations (3.5) must be of the form (3.6). Thus if the relation $x = \prod_{y \in Y} y$ is a consequence of the relations (3.5) then $|Y| = 1$, i.e., the relation must be $x = y$ for some y in X. To complete the proof we therefore need only show that the relation $x = y$ is a consequence of the relations (3.5) only if $x_i = y_i$ for $i = 0, 1, \cdots, n$.

Accordingly, suppose that the relation $x = y$, where $x, y \in X$, is a consequence of the relations (3.5). Then this relation must be of the form (3.6) with $X_1 = \{x\}$ and $Y_1 = \{y\}$. But then, since $|X_1| = |Y_1| = 1$, the congruences (3.7) take the form

$$x_i \equiv y_i \pmod{r_i}, \quad i = 0, 1, \cdots, n,$$

from which it follows that $x_i = y_i, \quad i = 0, 1, \cdots, n$.

We now arrive at the principal theorem obtained for the case in which T is commutative and finite-dimensional. This theorem states in effect that given a group G and a finite-dimensional commutative cancellative semigroup T without idempotent, there exists a cancellative semigroup $S = G \cup T$ if and only if G is finite and commutative and T is a homomorph of one of a specified class of finitely generated cancellative semigroups.

THEOREM 3.5. *Let T be a commutative cancellative semigroup without idempotent; let T have finite dimension m and basis B, and let G be a group. Then there exists a cancellative semigroup $S = G \cup T$ if and only if the following three conditions are satisfied:*

(C1) *G is commutative;*

(C2) *$|G|$ divides m;*

(C3) *Let G be the direct product of t cyclic groups of orders $r_1, \cdots, r_t$, and let X be the set of all vectors $(x_0, x_1, \cdots, x_t)$ with integral components satisfying*

$$0 \leqq x_i < r_i \qquad (i = 0, 1, \cdots, t),$$

where $r_0 = m/|G|$. Then there is a one-to-one mapping, $x \to (x_0, x_1, \cdots, x_t)$, of B onto X such that $xy = uv$ is a relation in T whenever there exists an integer i, $1 \leqq i \leqq t$, such that

(i) $x_i + y_i \equiv u_i + v_i \pmod{r_i}$;

(ii) *$x_j = v_j$ and $y_j = u_j$, all $j = 0, 1, \cdots, t$; $j \neq i$.*

Proof. Suppose there exists a cancellative semigroup $S = G \cup T$. Conditions (C1) and (C2) are then consequences of Lemmas 2.4 and 3.3, respectively. It remains to establish (C3).

Let G have order n and suppose that G is the direct product of the t cyclic groups $G_1, \cdots, G_t$, where G_i is generated by g_i and has order r_i $(i = 1, \cdots, t)$. Let X be the set of vectors defined in the statement of the theorem. Partition B into subsets $B_0, B_1, \cdots, B_{k-1}$ by means of the equivalence relation ρ defined in the proof of Lemma 3.3; thus $k = r_0 = m/|G|$. Choose an arbitrary element from each B_i, $i = 0, 1, \cdots, k-1$, and represent it by the vector $(i, 0, \cdots, 0)$. Let $g \in G$; then g is uniquely representable in the form

$$g = g_1^{x_1} g_2^{x_2} \cdots g_t^{x_t}, \qquad 0 \leqq x_i < r_i \qquad (i = 1, \cdots, t).$$

Represent $g(i,0,\cdots,0)$ by the vector $(i,x_1,\cdots,x_t)$. By definition of ρ and cancellativity in S, every element of B can be written uniquely in the form $g(i,0,\cdots,0)$ for some $g \in G$ and some i, $1 \leqq i \leqq k-1$. Hence every element of B is represented by exactly one vector of X.

Now suppose that for some integer i, $1 \leqq i \leqq t$, there exist vectors x, y, u, v in X whose components satisfy (i) and (ii) of condition (C3). It follows from the way in which the elements of B are represented that

$$\begin{aligned} g_i^{v_i}x &= g_i^{v_i}(g_1^{x_1}\cdots g_t^{x_t})(x_0,0,\cdots,0) \\ &= (g_1^{x_1}\cdots g_{i-1}^{x_{i-1}}g_i^{v_i+x_i}g_{i+1}^{x_{i+1}}\cdots g_t^{x_t})(x_0,0,\cdots,0) \\ &= (x_0,x_1,\cdots,x_{i-1},x_i+v_i,x_{i+1},\cdots,x_t) \end{aligned}$$

where the component $x_i + v_i$ is reduced modulo r_i. Similarly

$$g_i^{x_i}v = (v_0,v_1,\cdots,v_{i-1},v_i+x_i,v_{i+1},\cdots,v_t)$$

where, again, the component $v_i + x_i$ is reduced modulo r_i. Hence, by (ii) of condition (C3),

$$(g_i^{v_i})x = (g_i^{x_i})v.$$

Similarly

$$(g_i^{u_i})y = (g_i^{y_i})u.$$

Hence

$$(g_i^{u_i+v_i})xy = (g_i^{x_i+y_i})uv.$$

But since g_i has order r_i, it follows from (i) that $g_i^{u_i+v_i} = g_i^{x_i+y_i}$. Hence $xy = uv$.

Conversely let T be a commutative cancellative semigroup without idempotent and of finite dimension m and basis B, and let G be a group which satisfies conditions (C1), (C2) and (C3). Assume that B is represented by the set X as described in (C3). (That T can simultaneously have dimension m and satisfy the relations given in (C3) is a consequence of Lemma 3.4.) Let $g_1,\cdots,g_t$ be a basis for the group G, where g_i has order r_i for $i=1,\cdots,t$. Let S be the set-theoretic union of G and T (with G and T assumed to be disjoint). The proof will be completed if we extend the multiplications in G and T to S in such a way that S becomes a cancellative semigroup having G as its maximal subgroup. With this in mind we define multiplication in S as follows:

(M1) Each two elements of G multiply in S as in the group G.

(M2) Each two elements of T multiply in S as in the cancellative semigroup T.

(M3) $(g_1^{e_1}\cdots g_t^{e_t})x = x(g_1^{e_1}\cdots g_t^{e_t}) = y$, where $y_0 = x_0$ and, for $1 \leqq i \leqq n$, $y_i \equiv x_i + e_i \pmod{r_i}$; here x is arbitrary in X.

(M4) $g(t_1xt_2) = (t_1xt_2)g = (gx)(t_1t_2)$ for all $g \in G$, all $x \in X$, and all $t_1, t_2 \in T^1$.

It must be shown at this point that the definition of multiplication given in (M4) is independent of the choice of x in representing the element t_1xt_2 of T, and that multiplication in S is well defined. We first establish

$$\left.\begin{matrix} gx = v \\ gu = y \end{matrix}\right\} \text{ imply } xy = uv, \quad \text{all } x, y, u, v \in X, \quad \text{all } g \in G. \tag{3.8}$$

Every element g of G is uniquely expressible in the form $g = g_1^{e_1} \cdots g_t^{e_t}$, where $0 \leqq e_i < r_i$ $(i = 1, \cdots, t)$. For each $g \in G$ define $N(g)$ to be the number of positive exponents e_i, $1 \leqq i \leqq t$, in this expression for g. The proof of (3.8) will be by induction on $N(g)$.

Suppose $(g_i^{e_i})x = v$ and $(g_i^{e_i})u = y$ for some x, y, u, v in X and some g_i, $1 \leqq i \leqq t$, where $0 < e_i < r_i$. By (M3),

$$x_i + e_i \equiv v_i \pmod{r_i} \text{ and } x_j = v_j, \quad \text{all } j \neq i$$

and

$$u_i + e_i \equiv y_i \pmod{r_i} \text{ and } u_j = y_j, \quad \text{all } j \neq i.$$

Consequently $x_i + y_i \equiv u_i + v_i \pmod{r_i}$. Therefore both (i) and (ii) of condition (C3) of our hypothesis are satisfied. Hence it follows from (C3) that $xy = uv$. This completes the proof of (3.8) for the case $N(g) = 1$.

Assume inductively that (3.8) holds for all g such that $N(g) < p$ for some fixed positive integer p. Let g be an element of G such that $N(g) = p$, say $g = g_1^{e_1} \cdots g_t^{e_t}$, and assume without loss of generality that $e_t > 0$. Suppose $gx = v$ and $gu = y$ Then, by (M3),

$$h(g_t^{e_t}x) = v \text{ and } h(g_t^{e_t}u) = y,$$

where $h = g_1^{e_1} \cdots g_{t-1}^{e_{t-1}}$ and $N(h) = p - 1$. Hence by the induction hypothesis

$$(g_t^{e_t}x)y = (g_t^{e_t}u)v. \tag{3.9}$$

Let $x' = g_t^{e_t}x$ and $u' = g_t^{e_t}u$. Then, since $N(g_t^{e_t}) = 1$, we can apply (3.7), obtaining

$$xu' = ux'. \tag{3.10}$$

Also (3.9) can be written in the form

$$x'y = u'v. \tag{3.11}$$

Since the elements x, y, u, v, x', and u' are elements of the commutative semigroup T, multiplication of equations (3.10) and (3.11) yields

$$xyx'u' = uvx'u',$$

which, by the cancellativity of T, implies

$$xy = uv.$$

This proves (3.8). Note that (3.8) can be stated equivalently as

(3.12) $$x(gu) = (gx)u, \quad \text{all } x, u \in X, \quad \text{all } g \in G.$$

Now let $t_1xt_2ut_3 \in T$, where $t_1, t_2, t_3 \in T^1$ and $x, u \in X$. Then by the commutativity of T, together with (3.12),

$$(gx)t_1t_2ut_3 = (gx)ut_1t_2t_3 = x(gu)t_1t_2t_3 = (gu)t_1xt_2t_3.$$

Hence (M4) is independent of the generator used.

To show that multiplication in S is well defined, suppose $g = g'$ and $xt = yt'$, where $g, g' \in G$ and xt, $yt' \in T$. Since there is only one expression for $g = g'$ of the form $g_1^{e_1} \cdots g_t^{e_t}$ all that need be shown is that $g(xt) = g(yt')$.

Let $z \in X$. Then $(gz)(xt) = (gz)(yt')$. But from (M4),

$$(gz)(xt) = g(zxt) = (gx)(zt) = ((gx)t)z = (g(xt))z.$$

Similarly

$$(gz)(yt') = g(zyt') = (gy)(zt') = ((gy)t')z = (g(yt'))z.$$

Hence $(g(xt))z = (g(yt'))z$ so, by cancellativity in T, $g(xt) = g(yt')$.

To complete the proof of the theorem it remains to establish that multiplication in S is associative and cancellative. Because of the commutativity of S and the associativity of G and T, we need to consider only the following two cases to establish the associativity of S:

(i) gtt' $(g \in G; t, t' \in T)$;

(ii) $gg't$ $(g, g' \in G; t \in T)$.

Case (i). Let $t = xt_1$, where $x \in X$ and $t_1 \in T^1$. Then

$$\begin{aligned} (gt)t' &= ((gx)t_1)t' && \text{by (M4)} \\ &= (gx)(t_1t') && \text{by associativity in } T^1 \\ &= g(xt_1t') && \text{by (M4)} \\ &= g(tt'). \end{aligned}$$

Case (ii). Let $x \in X$. Let $g = g_1^{e_1} \cdots g_t^{e_t}$ and $g' = g_1^{f_1} \cdots g_t^{f_t}$ be arbitrary elements of G. Then it is clear from (M3) that

(3.13) $$(gg')x = y = g(g'x),$$

where $y_i \equiv x_i + e_i + f_i \pmod{r_i}$ for $i = 1, \cdots, t$, and $y_0 = x_0$. Now let $t = xt'$ be an arbitrary element of $T \backslash B$. Then

$$\begin{aligned} (gg')t &= ((gg')x)t' && \text{by (M4)} \\ &= (g(g'x))t' && \text{by (3.13)} \\ &= g((g'x)t') && \text{by Case (i)} \\ &= g(g'(xt')) && \text{by (M4)} \\ &= g(g't). \end{aligned}$$

Hence S is a semigroup.

To verify that S is cancellative the following four cases must be considered (for $g, g' \in G; t, t' \in T$):

(i) $gt = g't$;

(ii) $gt = t't$;

(iii) $gt = gt'$;

(iv) $gt = gg'$.

Case (i). Suppose $gt = g't$, and write $t = xt_1$, where $x \in X$ and $t_1 \in T^1$. Then $(gx)t_1 = (g'x)t_1$ so, by cancellativity in T^1, $gx = g'x$, or equivalently $g^{-1}g'x = x$. Let $g^{-1}g' = g_1^{e_1} \cdots g_t^{e_t}$. It follows from (M3) that $x_i \equiv x_i + e_i \pmod{r_i}$ for $i = 1, \cdots, t$. But $0 \leqq e_i < r_i$ for each i, so $e_i = 0$ for $i = 1, \cdots, t$. Hence $g^{-1}g' = e$, the identity element of G, so $g = g'$.

Case (ii). Suppose $gt = t't$. Then $t = (g^{-1}t')t$ which by Lemma 2.1 implies that $g^{-1}t'$ is idempotent. But $g^{-1}t' \in GT = T$, contrary to the assumption that T contains no idempotent. Hence Case (ii) cannot occur.

Case (iii). Suppose $gt = gt'$. Then $g^{-1}gt = g^{-1}gt'$ so $t = t'$.

Case (iv). This case cannot occur since, by (M3) and (M4), $gt \in T$ while $gg' \in G$.

Hence S is a cancellative semigroup. It is apparent that G is the maximal subgroup of S and that T is an ideal of S. This completes the proof of the theorem.

We may now state a theorem very similar to Theorem 3.5 but without the restriction that T is finite-dimensional. It is assumed, however, that T has a basis and that G is finitely generated. The proof differs from that of Theorem 3.5 in only minor details, and will be omitted.

THEOREM 3.6. *Let T be a commutative cancellative semigroup without idempotent and with basis B, and let G be a finitely generated group. Then there exists a cancellative semigroup $S = G \cup T$ if and only if the following three conditions are satisfied*:

(C1) *G is commutative*;

(C2) $|G| \leqq |B|$;

(C3) *Let G be the direct product of t cyclic groups of orders $r_1, \cdots, r_t$ (any number of which may be infinite), and let X be the set of all vectors $(x_0, x_1, \cdots, x_t)$ with integral components satisfying*

$$\begin{array}{ll} 0 \leqq x_i < r_i & \textit{if } r_i \textit{ is finite}, \\ -\infty < x_i < \infty & \textit{if } r_i \textit{ is infinite}, \\ x_0 \in \Lambda, & \end{array}$$

where Λ is an indexing set of cardinality such that $|X| = |B|$. Then there is a one-to-one mapping $x \to (x_0, \cdots, x_t)$ of B onto X such that $xy = uv$ is a relation in T whenever there exists an integer i, $1 \leqq i \leqq t$, such that

$$\text{(i)} \qquad \begin{cases} x_i + y_i \equiv u_i + v_i \ (\text{mod } r_i), & \textit{if } r_i \textit{ is finite}, \\ x_i + y_i = u_i + v_i, & \text{if } r_i \text{ is } \textit{infinite}; \end{cases}$$

$$\text{(ii)} \qquad x_j = v_j \textit{ and } y_j = u_j \textit{ for all } j = 0, 1, \cdots, t;\ j \neq i.$$

4. **Problems (II) and (III): the commutative case.** Using a somewhat different approach we obtain necessary and sufficient conditions for the existence of a cancellative semigroup $S = G \cup T$ given a commutative cancellative semigroup T without idempotent and a finitely generated commutative group G. The theorems apply to a larger class of cancellative semigroups T than do those of the preceding section since it is not assumed that T has a basis.

LEMMA 4.1. *Let T be a commutative cancellative semigroup without idempotent and let Q be its group of quotients. Let G be a group. If there exists a cancellative semigroup $S = G \cup T$ then S is imbeddable in Q. Conversely if T is identified with its natural isomorph in Q and if G is any subgroup of Q such that $GT \subseteq T$ then there exists a cancellative semigroup $S = G \cup T$.*

Proof. Recall that Q is the set of all pairs (a, b) of elements a and b of T, with equality defined by

$$(a_1, b_1) = (a_2, b_2) \text{ if and only if } a_1 b_2 = a_2 b_1.$$

Multiplication in Q is componentwise and (a, a) is the identity element of Q for every element a of T. If t is an arbitrary but fixed element of T then the mapping

$$\phi: x \to (xt, t), \qquad \text{all } x \in T,$$

is called the *natural isomorphism* of T into Q; clearly ϕ is independent of the choice of t in T.

Suppose there exists a cancellative semigroup $S = G \cup T$. Define the mapping α of S into Q by

$$\alpha: s \to (sa, a), \qquad \text{all } s \in S, \tag{4.1}$$

where a is an arbitrary but fixed element of T. Then by (4.1) and the definitions of multiplication and equality in Q,

$$(s_1\alpha)(s_2\alpha) = (s_1 a, a)(s_2 a, a) = (s_1 s_2 a^2, a^2) = (s_1 s_2 a, a) = (s_1 s_2)\alpha$$

for all $s_1, s_2 \in S$, so α is a homomorphism. Furthermore if $s_1\alpha = s_2\alpha$, i.e., if $(s_1 a, a) = (s_2 a, a)$, then $s_1 a^2 = s_2 a^2$ so $s_1 = s_2$. Thus α is an isomorphism.

The converse is immediate if one observes that $GT \subseteq T$ implies $G \cap T = \varnothing$. Indeed if $g \in G \cap T$ then $e = g^{-1}g \in GT \subseteq T$, which contradicts the assumption that T contains no idempotent. Hence the subset $S = G \cup T$ of Q is the required cancellative semigroup. This completes the proof of the lemma.

LEMMA 4.2. *Let T be a commutative cancellative semigroup without idempotent. Let G be the finite cyclic group of order m. Then there exists a cancellative semigroup $S = G \cup T$ if and only if there exists a pair of elements a, b in T such that*

(i) *m is the least positive integer for which $a^m = b^m$, and*

(ii) *$aT = bT$.*

Proof. Suppose there exists a cancellative semigroup $S = G \cup T$, which, by Lemma 2.4, is necessarily commutative. Let a be an arbitrary element of T and let $b = ga$, where g is a generator of the cyclic group G. Then

$$b^m = (ga)^m = g^m a^m = ea^m = a^m,$$

where e is the identity element of G. Furthermore if $a^n = b^n$ for some positive integer n then $a^n = b^n = g^n a^n$. Hence $g^n = e$ so m divides n, proving (i).

Let $t \in T$. Then $at = agg^{-1}t = bg^{-1}t \in bT$, so $aT \subseteq bT$. Also $bt = agt \in aT$ so $bT \subseteq aT$. This proves (ii).

Conversely suppose there exists a pair of elements a, b in T which satisfy (i) and (ii). Consider the element (a, b) of the group of quotients Q of T. Since $(a, b)^n = (a^n, b^n)$ is the identity element of Q if and only if $a^n = b^n$, it follows from (i) that (a, b) has order m in Q. Let G' denote the cyclic subgroup of Q generated by (a, b) and let T' be the natural isomorph of T in Q. By Lemma 4.1 the proof will be complete if we show that $G'T' \subseteq T'$.

Suppose then that (zt, t) is an arbitrary element of T', where $z, t \in T$. By (ii) there exists an element w in T such that $az = bw$. Hence $(a, b)(zt, t) = (azt, bt) = (bwt, bt) \in T'$, so $(a, b)T' \subseteq T'$. By induction $(a, b)^n T' \subseteq T'$ for every positive integer n, so $G'T' \subseteq T'$.

We next prove the infinite analogue of Lemma 4.2.

LEMMA 4.3. *Let T be a commutative cancellative semigroup without idempotent and let G be the infinite cyclic group. Then there exists a cancellative semigroup $S = G \cup T$ if and only if there exists a pair of elements a, b in T such that*

(i) *$a^n \neq b^n$ for every positive integer n, and*

(ii) *$aT = bT$.*

Proof. Suppose there exists a (necessarily commutative) cancellative semigroup $S = G \cup T$. Let a be an arbitrary element of T and let $b = ga$, where g is a generator of G. If $a^n = b^n$ for some positive integer n then $a^n = b^n = g^n a^n$ so $g^n = e$, a contradiction. This proves (i), while (ii) is proved as in Lemma 4.2.

Conversely suppose T contains elements a, b which satisfy (i) and (ii). Let Q be the group of quotients of T and consider the element (a, b) of Q. By (i), (a, b) has infinite order in Q. Let G' be the cyclic subgroup of Q generated by (a, b) and let T'

be the natural isomorph of T in Q. Again we need only show that $G'T' \subseteq T'$, and this follows just as in the proof of Lemma 4.2.

By applying the two preceding lemmas we can now give a solution to Problem (II) in the commutative case.

THEOREM 4.4. *Let T be a commutative cancellative semigroup without idempotent. Then a necessary and sufficent condition for the existence of a cancellative semigroup $S = G \cup T$, where G is nontrivial, is that there exist a pair of distinct elements x, y in T such that $xT = yT$.*

Proof. Suppose that $S = G \cup T$ exists for some nontrivial group G. Let $h \in G$, $h \neq e$, and let H be the cyclic subgroup of G generated by h. Let $S' = H \cup T$ be the subsemigroup of S defined by the set-theoretic union of H and T. We note that S' is cancellative, H is the maximal subgroup of S', and $T = S' \backslash H$ is the maximal proper ideal of S'.

If H is finite it follows from Lemma 4.2 that there exist distinct elements a and b of T such that $aT = bT$. The same conclusion follows from Lemma 4.3 if H is infinite.

Conversely if $xT = yT$ for distinct elements x, y of T then condition (ii) of Lemmas 4.2 and 4.3 is valid. Since $x \neq y$, either $x^n \neq y^n$ for every positive integer n, in which case there exists a cancellative semigroup $S = G \cup T$ with G the infinite cyclic group, or there exists a least positive integer m, $m > 1$, such that $x^m = y^m$, in which case there exists a cancellative semigroup $S = G \cup T$ with G cyclic of order m.

We next give a solution to the commutative case of Problem (III).

THEOREM 4.5. *Let T be a commutative cancellative semigroup without idempotent and let G be a commutative group. Then there exists a cancellative semigroup $S = G \cup T$ if and only if there is a homomorphism α of G into Q, the group of quotients of T, such that for $g \in G$,*

$$g\alpha = (a, b)$$

implies

(i) *$a^n = b^n$ (n a positive integer) if and only if the order of g is finite and divides n, and*

(ii) *$aT = bT$.*

Proof. Suppose there exists a cancellative semigroup $S = G \cup T$. Let b be an arbitrary but fixed element of T, and define the mapping α of G into Q by

$$\alpha: g \to (gb, b), \quad \text{all } g \in G.$$

Then $(g_1\alpha)(g_2\alpha) = (g_1 b, b)(g_2 b, b) = (g_1 g_2 b^2, b^2) = (g_1 g_2 b, b) = (g_1 g_2)\alpha$, so α is a homomorphism. Furthermore $(gb)^n = b^n$ if and only if $g^n b^n = b^n$ if and only if $g^n = e$ (the identity element of G) if and only if the order of g is finite and divides n, Moreover, for any t in T, $(gb)t = (bg)t = b(gt) \in bT$ and $bt = (bg)(g^{-1}t) \in gbT$. Hence (i) and (ii) are satisfied.

Conversely suppose that there exists a homomorphism α of G into Q which satisfies (i) and (ii). Suppose $g_1, g_2 \in G$, with $g_1\alpha = (a_1, b_1)$ and $g_2\alpha = (a_2, b_2)$. If $g\alpha = (a, a)$, the identity element of Q, then, by (i), $g = e$. Thus α is an isomorphism.

By Lemma 4.1 the proof will be complete if we establish that $G'T' \subseteq T'$, where $G' = G\alpha$ and where T' is the natural isomorph of T in Q. Let (t_1x, x) be an arbitrary element of T' and let (a, b) be an arbitrary element of G'. By (ii) there exists an element t_2 in T such that

$$at_1 = bt_2. \tag{4.2}$$

Thus, by (4.2),

$$(a, b)(t_1x, x) = (at_1x, bx) = (bt_2x, bx) = (t_2bx, bx),$$

which is in T'. Hence $G'T' \subseteq T'$, proving the theorem.

5. **Noncommutative cancellative semigroups.** We recall from Lemma 3.3 that if T is a finite-dimensional commutative cancellative semigroup without idempotent and G is a group then a necessary condition for the existence of a cancellative semigroup $S = G \cup T$ is that $|G|$ divide the dimension of T. If T is not commutative this condition is no longer necessary for the existence of $S = G \cup T$; however it is still necessary that $|G|$ not exceed the dimension of T.

THEOREM 5.1. *Let m and n be positive integers. Then there exists a cancellative semigroup $S = G \cup T$, where T has dimension m and G has order n, if and only if $m \geqq n$.*

Proof. Let $S = G \cup T$ be a cancellative semigroup such that G has order n and T has dimension m, and let B be a basis for T such that $|B| = m$. To show that $m \geqq n$ it is sufficient to show that $Gb \subseteq B$ for some $b \in B$ since, by cancellativity, $|Gb| = |G|$.

Suppose by way of contradiction that this is not the case for any b in B, i.e.,

$$Gb \nsubseteq B, \quad \text{all } b \in B. \tag{5.1}$$

Let b_1 be an arbitrary but fixed element of B. By (5.1) there exists $g \in G$ such that $gb_1 = w_1u_1$, where $u_1 \in B$ and $w_1 \in T$. Again by (5.1), there exists $g_1 \in G$ such that $g_1u_1 \notin B$. Hence $g_1u_1 = w_2'u_2$, where $w_2' \in T$ and $u_2 \in B$. Then $gb_1 = w_1u_1 = w_1g_1^{-1}g_1u_1 = w_1g_1^{-1}w_2'u_2$. Setting $w_1g_1^{-1}w_2' = w_2$, we have

$$gb_1 = w_1u_1 = w_2u_2,$$

where w_1 is a left divisor of w_2 in T. Repetition of this process yields

$$gb_1 = w_1u_1 = w_2u_2 = \cdots = w_mu_m, \tag{5.2}$$

where $u_i \in B$ and $w_i \in T$ for $i = 1,2,\cdots,m$. Furthermore if $1 \leqq i < j \leqq m$ then w_i is a left divisor of w_j in T.

If $b_1 = u_k$ for some integer k, $1 \leqq k \leqq m$, then $gb_1 = w_k u_k = w_k b_1$. By cancellativity in S it follows that $g = w_k \in T$, contradicting that $G \cap T = \varnothing$. Hence $b_1 \neq u_i$ for $i = 1,2,\cdots,m$. Therefore, since $|B| = m$, there must exist integers r and s, with $1 \leqq r < s \leqq m$, such that $u_r = u_s$. It then follows from (5.2) that $w_r = w_s$. Since $r < s$ we also have that $w_s = w_r w$ for some w in T. Hence $w_s = w_s w$, which by Lemma 2.1 implies that w is an identity element for T. This contradicts the assumption that T contains no idempotent, so necessarily $Gb \subseteq B$ for some b in B. It follows that $m \geqq n$.

To prove the converse we will sketch the construction, corresponding to an arbitrary pair of positive integers m and n such that $m \geqq n$, of a cancellative semigroup $S = G \cup T$ where G is the cyclic group of order n and T is a cancellative semigroup of dimension m without idempotent.

Let m,n be fixed integers with $m \geqq n > 0$. Let α be the permutation $(1,2,\cdots,n)$ and, for each positive integer k, define permutations β_k and $\bar{\beta}_k$ by

$$\beta_k = (n + k^2 - k + 1,\ n + k^2 - k + 2,\cdots,n + k^2),$$

and

$$\bar{\beta}_k = (n + k^2 + 1,\ n + k^2 + 2,\cdots,n + k^2 + k).$$

These expressions for β_k and $\bar{\beta}_k$, in which the first integer which appears is the smallest integer in that cycle, will be called *canonical forms* for β_k and $\bar{\beta}_k$. Assuming $\beta_k = (b_1,\cdots,b_k)$ and $\bar{\beta}_k = (\bar{b}_1,\cdots,\bar{b}_k)$ to be in canonical form, define, for each positive integer k,

$$\gamma_k = (c_1, c_2, \cdots, c_{2k}),$$

where $c_{2i-1} = b_i$ and $c_{2i} = \bar{b}_{k+2-i}$ $(i = 1,\cdots,k)$, with each subscript of the components of γ_k reduced to its least positive residue modulo k. Define

$$\sigma_k = \alpha^k \left(\prod_{i=1}^{\infty} \beta_i \bar{\beta}_i \right) \qquad (k = 0,1,\cdots,n-1) \tag{5.3}$$

and, for each positive integer k,

$$\delta_k = \left(-\frac{(k-1)k}{2} - 1,\ -\frac{(k-1)k}{2} - 2,\cdots, -\frac{k(k+1)}{2} \right).$$

Finally define

$$\sigma_k = \left(\prod_{i=1;i\neq k}^{\infty} \delta_i \right) \left(\prod_{i=1}^{\infty} \gamma_i \right) \qquad (k = n, n+1,\cdots,m-1).$$

Let T be the multiplicative semigroup generated by the set $\{\sigma_0, \sigma_1, \cdots, \sigma_{m-1}\}$. Then it can be verified that

(5.4) $$\sigma_0\sigma_i\sigma_0 = \sigma_i \quad \text{if } n \leqq i \leqq m-1;$$

(5.5) T is a cancellative semigroup without idempotent and of dimension m.

Thus if G denotes the cyclic group of order n generated by α, it follows from (5.3) that

$$\alpha\sigma_i = \sigma_i\alpha = \sigma_j \qquad \text{for } 0 \leqq i \leqq n-1,$$

where j is the least positive residue of $i+1$ modulo n. Furthermore, by (5.4),

$$\alpha\sigma_i = \sigma_1\sigma_i\sigma_0 \quad \text{and} \quad \sigma_i\alpha = \sigma_0\sigma_i\sigma_1 \qquad \text{for } n \leqq i < m.$$

Hence T is an ideal of $S = G \cup T$. Clearly G is the maximal subgroup of S, and S, being a subsemigroup of a group, is cancellative. Furthermore T has dimension m and G has order n, so the proof of the theorem is complete.

Reference

1. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vol. 1, Math. Surveys No. 7, Amer. Math. Soc., Providence, R. I., 1961.

The University of Missouri,
Columbia, Missouri
The University of Nebraska,
Lincoln, Nebraska