

PRIME AND SEMIPRIME SEMIGROUP ALGEBRAS OF CANCELLATIVE SEMIGROUPS

M. V. CLASE

ABSTRACT. Necessary and sufficient conditions are given for a semigroup algebra of a cancellative semigroup to be prime and semiprime. These conditions were proved necessary by Okniński; our contribution is to show that they are also sufficient. The techniques used in the proof are a new variation on the Δ -methods which were developed originally for group algebras.

1. INTRODUCTION

An open question from [8, Chapter 9] is to characterise those semigroup algebras $K[S]$, for cancellative semigroups S , which are prime and semiprime. Of particular interest are necessary and sufficient conditions at the semigroup level which parallel those known for group algebras. A complete answer is provided by the following theorem.

Theorem 1. *Let S be a cancellative semigroup and let K be a field of characteristic $p \geq 0$.*

- (i) *$K[S]$ is prime if and only if there do not exist distinct commuting elements s and t in S such that $(s, t) \in \omega$ and $s^n = t^n$ for some $n > 1$.*
- (ii) *If $p = 0$ then $K[S]$ is semiprime.*
- (iii) *If $p > 0$ then $K[S]$ is semiprime if and only if there do not exist distinct commuting elements s and t in S such that $(s, t) \in \omega$ and $s^p = t^p$.*

We defer definition of ω until Section 2; it is a congruence that generalises the notion of the FC-centre of a group.

The conditions given in Theorem 1 were shown to be necessary by Okniński [9], and were conjectured by him to be sufficient. The goal of this paper is to show that these conditions are indeed sufficient. Note that [9] contained some partial results on sufficiency: assertion (ii) was proved, and the conditions were shown to be necessary and sufficient in the special case that S has a group of right fractions.

In the case that S is a group, the corresponding results were proved in the early 1960's by Connell [6] and Passman [10]. We give this result below for comparison purposes and because we shall use it later in our proof.

Connell-Passman Theorem. *Let G be a group and let K be a field of characteristic $p \geq 0$.*

Received by the editors November 17, 1995 and, in revised form, August 1, 1996.

1991 *Mathematics Subject Classification.* Primary 16S36; Secondary 16N60, 20M25.

This work was completed while the author held an NSERC Postdoctoral Fellowship at McMaster University, Hamilton, Canada.

- (i) $K[G]$ is prime if and only if $\Delta(G)$ is a torsion-free group.
- (ii) If $p = 0$ then $K[G]$ is semiprime.
- (iii) If $p > 0$ then $K[G]$ is semiprime if and only if $\Delta(G)$ contains no elements of order p .

Here $\Delta(G)$ is the subgroup $\Delta(G) = \{g \in G \mid g \text{ has finitely many conjugates}\}$; this is called the FC-centre of G .

The similarity between these conditions and those of Theorem 1 is apparent. Indeed, if S is a group, then it turns out that $(s, t) \in \omega$ if and only if $s\Delta(S) = t\Delta(S)$, from which the equivalence of these conditions follows easily.

The techniques used in the original proof of the Connell-Passman Theorem have become known as Δ -methods. Variations of these methods have been used to extend the Connell-Passman Theorem to twisted group rings [11], crossed-products [13], and strongly group-graded rings [14]. Nice expositions of this work can be found in [12] and [15]. Further generalisations of Δ -methods have been developed for enveloping algebras of Lie algebras and Lie superalgebras in a series of papers by Bergen and Passman [1, 2, 3, 4].

Since Δ -methods have been used successfully to attack other ring theoretic problems concerning group rings and enveloping algebras, the methods of the current paper may find other applications to the study of semigroup algebras of cancellative semigroups.

We mention also an earlier attempt by Okniński in [8] to settle this question for cancellative semigroups using a notion of the FC-centre of a cancellative semigroup due to Krempa [7]. Again, necessary conditions similar to those of the Connell-Passman Theorem were obtained, but an example in [9] showed that these conditions were not sufficient.

2. PRELIMINARIES

Throughout the paper, S is a cancellative semigroup and K is a field. We do not require S to have an identity, but make occasional use of the notation S^1 to signify the semigroup S with an identity adjoined if it did not already have one. We shall need only a few elementary facts about semigroups, all of which can be found in Chapter 1 of [5].

We begin with a few congruences.

Definition 2 ([9]). Let S be a cancellative semigroup. Define congruences ρ , ρ' , and τ by:

- (i) $(s, t) \in \rho$ if and only if for all $x \in S^1$, $sxS \cap txS \neq \emptyset$.
- (ii) $(s, t) \in \rho'$ if and only if for all $x \in S^1$, $Sxs \cap Sxt \neq \emptyset$.
- (iii) $\tau = \rho \cap \rho'$.

These relations are easily seen to be congruences. Another easily established and very important fact is that ρ is left cancellative (i.e. $(us, vt) \in \rho$ and $(u, v) \in \rho$ implies $(s, t) \in \rho$) and ρ' is right cancellative. Note that $\rho = S \times S$ if and only if S satisfies the right Ore condition if and only if S has a group of right fractions.

Let σ be a congruence (or more generally, an equivalence relation) on S . We write $\sigma(x)$ for the equivalence class of σ which contains x . We call a subset T of S a σ -constant subset if all elements of T belong to a single σ -class. An element $\alpha \in K[S]$ is called σ -constant if $\text{supp}(\alpha)$ is a σ -constant subset of S .

The relation ω used in Theorem 1 is defined as follows.

Definition 3 ([9]). Let S be a cancellative semigroup. Define a relation ω on S by $(s, t) \in \omega$ if and only if there is a finite τ -constant set $F \subseteq S$ such that for each $x \in S$, there are $b, d \in F$ with $sxb = txd$.

Note that the definition of ω in [9] differs slightly in that x is allowed to be an element of S^1 rather than S . Our definition is occasionally more convenient for our purposes and is easily seen to be equivalent: a pair (s, t) satisfying our definition witnessed by a set F will satisfy the definition of [9] provided we replace F by zF for any element $z \in S$; the converse is clear.

A crucial fact from [9] that we require about ω is that the definition is left-right symmetric (i.e. the congruence ω' defined as above except that the final equation reads $bxs = dxt$ is the same as ω). From this it follows that ω is cancellative (indeed, it is easily seen to be left cancellative, and so right cancellativity follows from the left-right symmetry), and that $\omega \subseteq \tau$ (an equation $sxb = txd$ with $b, d \in F$ forces $(s, t) \in \rho'$ since ρ' is right cancellative, and $(s, t) \in \rho$ follows by symmetry). We shall use these facts from time to time without further comment.

If S is a group, then it is not difficult to see that $(s, t) \in \omega$ if and only if $s\Delta(S) = t\Delta(S)$, for each equation $sxb = txd$ can be rewritten in the form $(t^{-1}s)^x = db^{-1}$. Taking this a little further, Okniński demonstrates in [9] that if S has a group of right fractions G , then for $s, t \in S$, we have $(s, t) \in \omega$ if and only if $s\Delta(G) = t\Delta(G)$.

Throughout this paper, we deal extensively with subsets of $S \times S$ of various sorts. One point of notation to which we occasionally resort is the following: if A is such a subset and s is an element of S , then As denotes the set $\{(as, bs) \mid (a, b) \in A\}$, and sA is defined similarly. If A happens to be an indexed family of pairs, then we agree that the families As and sA are indexed in the same way.

3. OUTLINE OF PROOF

If $K[S]$ is not prime, then there exist non-zero elements α and β in $K[S]$ such that S satisfies the identity

$$(1) \quad \alpha x \beta = 0 \quad \text{for all } x \in S.$$

If $K[S]$ is not semiprime, then we may take $\alpha = \beta$ in (1).

A good account of the group case is given in [12]. That proof proceeds by showing that one may reduce the identity (1) to the case that $\text{supp}(\alpha) \subseteq \Delta(G)$ and $\text{supp}(\beta) \subseteq \Delta(G)$.

In the semigroup case, the bulk of the work is to show that we may similarly assume that α and β are ω -constant elements. The first stage of this process is to reduce (1) to τ -constant elements. We present a short account of this reduction in Section 4; it was first performed by Okniński [9]. Note that this step is unnecessary in the group case since $\tau = G \times G$ for a group G .

The difficult part of the proof is the further reduction of (1) to ω -constant elements. We are guided by the method of proof in the group case: one shows that if it is not possible to reduce α to an element in $K[\Delta(G)]$, then one can cover the group G by a finite union of cosets of subgroups of infinite index (the subgroups in question being centralisers of elements not in $\Delta(G)$), which is an impossibility. In the semigroup case, the centraliser of an element is replaced by a certain equivalence relation which we call a generalised centraliser (see Section 5), and a covering by a union of cosets is replaced by a collection of elements of S called a covering system (see Section 6).

Even with these definitions in hand, the proof is technically more difficult than the group case. A reduction argument allows us to produce pairs of ω -related elements from a covering system (Section 7). If we cannot find ω -constant elements α and β satisfying (1) then we construct a covering system; the pair of ω -related elements that this covering system produces leads to a contradiction (see Section 10).

Once we have obtained the reduction to ω -constant elements, the proof is easily completed (in Section 11) by localisation and applying the Connell-Passman Theorem.

4. REDUCTION TO τ -CLASSES

For any pair of elements (s, t) of S , exactly one of the following three possibilities occurs: (i) $(s, t) \in \rho$, (ii) $sS \cap tS = \emptyset$, or (iii) $sS \cap tS \neq \emptyset$ but there is a $u \in S$ such that $suS \cap tuS = \emptyset$. Note that properties (i) and (ii) are preserved by left and right multiplications: $(s, t) \mapsto (asb, atb)$, while a pair (s, t) satisfying (iii) becomes a pair (su, tu) satisfying (ii) after right multiplication by the appropriate u .

So for any finite set $F \subset S \times S$, we can successively convert case (iii) pairs to case (ii) pairs by suitable right multiplications. Hence there is some u in S such that Fu contains no case (iii) pairs. In particular, if we apply this to $\text{supp}(\alpha) \times \text{supp}(\alpha)$ we obtain:

Lemma 4. *Let $\alpha \in K[S]$. There is an element $u \in S$ such that $\beta = \alpha u$ satisfies the following condition:*

$$\text{for all } s, t \in \text{supp}(\beta), \text{ either } (s, t) \in \rho \text{ or } sS \cap tS = \emptyset.$$

The same condition is true of $\beta = v\alpha u$ for any $v \in S$. □

Suppose that there is an identity of the form $\alpha x \beta = 0$ satisfied by all $x \in S$. Clearly, we may replace α and β by any left or right multiples by semigroup elements and still have such an identity. The next proposition shows that we may reduce such an identity to τ -constant elements α and β .

Proposition 5 ([9, Lemma 2]). *Suppose that there are non-zero elements $\alpha, \beta \in K[S]$ such that $\alpha x \beta = 0$ for all $x \in S$. Then there are τ -constant elements α' and β' such that $\alpha' x \beta' = 0$ for all $x \in S$. If $\alpha = \beta$, then we can take $\alpha' = \beta'$.*

Proof. By Lemma 4 and the corresponding version for ρ' , we may assume that for all $(s, t) \in \text{supp}(\alpha)$, either $(s, t) \in \rho$ or $sS \cap tS = \emptyset$, and for all $(s, t) \in \text{supp}(\beta)$, either $(s, t) \in \rho'$ or $sS \cap tS = \emptyset$. Note that we may preserve the property $\alpha = \beta$ by the last statement of Lemma 4.

Fix $a \in \text{supp}(\alpha)$ and $b \in \text{supp}(\beta)$. Write $\alpha = \alpha' + \alpha''$ and $\beta = \beta' + \beta''$, where $\text{supp}(\alpha') \subseteq \tau(a)$, $\text{supp}(\alpha'') \cap \tau(a) = \emptyset$, $\text{supp}(\beta') \subseteq \tau(b)$, and $\text{supp}(\beta'') \cap \tau(b) = \emptyset$.

Suppose there is an $x \in S$ such that $\alpha' x \beta' \neq 0$. Then there is some element in the support of $\alpha' x \beta'$ which we may assume without loss of generality is axb . Because $\alpha x \beta = 0$, we have

$$\alpha' x \beta' = -\alpha' x \beta'' - \alpha'' x \beta' - \alpha'' x \beta''.$$

Hence $axb = cxd$ for some $c \in \text{supp}(\alpha)$ and $d \in \text{supp}(\beta)$ with either $c \in \text{supp}(\alpha'')$ or $d \in \text{supp}(\beta'')$. Now $axb = cxd$ implies $aS \cap cS \neq \emptyset$. By assumption on α , this implies $(a, c) \in \rho$. Since ρ is left cancellative, the equality $axb = cxd$ implies $(b, d) \in \rho$. Similarly, by assumption on β , we get $(b, d) \in \rho'$ and $(a, c) \in \rho'$. This

means that $(a, c) \in \tau$, so that $c \notin \text{supp}(\alpha'')$ and $(b, d) \in \tau$, so that $d \notin \text{supp}(\beta'')$, a contradiction.

So we have $\alpha'x\beta' = 0$ for all $x \in S$, and α' and β' are τ -constant elements, as desired. If $\alpha = \beta$, then we can take $a = b$, so that $\alpha' = \beta'$. $\square$

5. GENERALISED CENTRALISERS

As remarked earlier, we need a notion analogous to the centraliser of an element of a group.

Definition 6. Fix a right ideal T of S and elements $a, c \in S$. Define a relation $\gamma = \gamma_{a,c}^T$ as follows: $(x, y) \in \gamma$ if and only if for all pairs $b, d \in T$ we have

$$axb = cxd \Leftrightarrow ayb = cyd.$$

The need for dependency on T will become clear as we proceed. In particular, it is required so that we can make use of Lemma 8 below.

Note also that the definition makes sense for an arbitrary subset T of S , but all of the applications and some of the properties given below require that T is a right ideal of S .

If S is a group, then $axb = cxd$ if and only if $(c^{-1}a)^x = db^{-1}$, so $(x, y) \in \gamma_{a,c}^S$ if and only if x and y are in the same right coset of the centraliser of $c^{-1}a$. For this reason we call $\gamma_{a,c}^T$ a *generalised centraliser*.

Let T be a subset of S . We say that an equivalence relation σ is a *right T -congruence* if $(x, y) \in \sigma$ implies $(xt, yt) \in \sigma$ for all $t \in T$.

Lemma 7. Let $a, c \in S$ and let T and T' be right ideals of S . Let $\gamma = \gamma_{a,c}^T$ and $\gamma' = \gamma_{a,c}^{T'}$.

- (i) γ is a right T -congruence.
- (ii) If $T' \subseteq T$ then $\gamma \subseteq \gamma'$.

Proof. It is immediate from Definition 6 that γ is an equivalence relation. Suppose $(x, y) \in \gamma$ and $t \in T$. If $b, d \in T$ with $axtb = cxtd$, then $tb, td \in T$, so $(x, y) \in \gamma$ implies $aytb = cytd$. So $(xt, yt) \in \gamma$. This proves (i), and (ii) follows straight from Definition 6. $\square$

The next result is extremely important. It allows us to conclude that elements are γ -related using a single pair of equations, rather than having to check all pairs of elements of T as the definition of γ suggests.

Lemma 8. Fix $t \in S$ and let $T = \tau(t)S^1$, the right ideal generated by the τ -class of t . Let $\gamma = \gamma_{a,c}^T$ for elements $a \neq c$ with $(a, c) \in \tau$. Suppose $b, d \in \tau(t)$ and $x, y \in S$ satisfy $axb = cxd$ and $ayb = cyd$. Then $(x, y) \in \gamma$.

Proof. It suffices to show that for any pair $e, f \in T$ with $axe = cxf$, we have $aye = cyf$ also. Let e, f be such a pair.

Since $(a, c) \in \tau \subseteq \rho$ and ρ is left cancellative, the equation $axe = cxf$ implies $(e, f) \in \rho$. We have $e \in \tau(t)S^1$ and $b \in \tau(t)$, so there is a $u \in S^1$ such that $(e, bu) \in \tau \subseteq \rho$. From the latter, and the relations $(b, d) \in \tau$ and $(e, f) \in \rho$, we obtain $(f, du) \in \rho$. By definition of ρ , there are elements $p, q, r, s \in S$ such that

$$ep = buq \quad \text{and} \quad duqr = fqs.$$

Combining these with the equation $axb = cxd$, we obtain

$$axepr = axbuqr = cxduqr = cxfqs.$$

But S is cancellative and we are given $axe = cxf$; therefore $pr = qs$. Using the equation $ayb = cyd$, we similarly obtain

$$ayepr = aybuqr = cyduqr = cyfqs.$$

Cancelling $pr = qs$, we get the desired equation $aye = cyf$. $\square$

6. COVERING SYSTEMS

In this section, we introduce the notion of a covering system; this fills the role occupied by a union of cosets of centralisers in the group case. Rather than using the obvious analogue, a union of equivalence classes of generalised centralisers, we find it more convenient to work with a concept that is closer in spirit to a linear identity of the form $\alpha x \beta = 0$.

Suppose $\alpha x \beta = 0$ for some non-zero elements α and β of $K[S]$ and all elements x in some subset U of S . Fix $a \in \text{supp}(\alpha)$ and $b \in \text{supp}(\beta)$. Then for any $x \in U$, there must be a $c \in \text{supp}(\alpha)$ and a $d \in \text{supp}(\beta)$ with $a \neq c$ and $b \neq d$ such that $axb = cxd$; otherwise axb would appear with non-zero coefficient in the product $\alpha x \beta$. This is the notion we capture in the definition of a covering system.

Definition 9. A *covering system* (a, b, A, B) for a subset U of S consists of elements $a, b \in S$ and finite subsets $A, B \subseteq S$ with $a \notin A$ and $b \notin B$ satisfying the following property:

for each $x \in U$, there are elements $c \in A$ and $d \in B$ such that $axb = cxd$.

If (a, b, A, B) is a covering system for U and, in addition, $A \subseteq \tau(a)$ and $B \subseteq \tau(b)$, then we call (a, b, A, B) a τ -covering system.

Example 1. Suppose, as above, that $\alpha x \beta = 0$ is an identity in $K[S]$ holding for all x in a subset U of S . Fix $a \in \text{supp}(\alpha)$ and $b \in \text{supp}(\beta)$ and put $A = \text{supp}(\alpha) \setminus \{a\}$ and $B = \text{supp}(\beta) \setminus \{b\}$. Then (a, b, A, B) is a covering system for U . If, in addition, α and β are τ -constant elements, then (a, b, A, B) is a τ -covering system for U .

A further important example of a covering system is provided by the following lemma, which shows a relationship between pairs of ω -related elements and τ -covering systems.

Lemma 10. Let (a, b, A, B) be a τ -covering system for S such that $A = \{c\}$ is a singleton. Then $(a, c) \in \omega$. Conversely, if $(a, c) \in \omega$ and $a \neq c$, then we can find an element b and a finite subset B of S such that $(a, b, \{c\}, B)$ is a τ -covering system.

Proof. Recall that $(a, c) \in \omega$ means that there is a finite τ -constant subset $F \subseteq S$ such that for each $x \in S$, $axF \cap cxF \neq \emptyset$. If $(a, b, \{c\}, B)$ is a τ -covering system, then $F = \{b\} \cup B$ will do.

Conversely, suppose that $(a, c) \in \omega$ and F is such a set. Let $F = \{f_1, f_2, \dots, f_n\}$. Since elements of F are τ -related, we claim that there is a common right multiple of the elements of F : $b = f_1 g_1 = f_2 g_2 = \dots = f_n g_n$. Indeed, f_1 and f_2 have a common multiple $f_1 h_1 = f_2 h_2$. Now, $\{f_2 h_2, f_3 h_2, \dots, f_n h_2\}$ is a smaller τ -constant set, which has a common right multiple by induction, say $b = f_2 h_2 k_2 = f_3 h_2 k_3 = \dots = f_n h_2 k_n$. Put $g_1 = h_1 k_2$ and $g_i = h_2 k_i$ for $i > 1$.

For any i, j, k, l , note that $(f_i g_j, f_j g_j) \in \tau$ and $(f_k g_l, f_l g_l) \in \tau$ because τ is a congruence. But $f_j g_j = b = f_l g_l$, so we conclude that $(f_i g_j, f_k g_l) \in \tau$.

Put $B = \{f_i g_j \mid 1 \leq i, j \leq n, i \neq j\}$. Put $A = \{c\}$. Then (a, b, A, B) is a τ -covering system for S . $\square$

In Section 10, we re-examine linear identities and construct another more complicated covering system.

Given a τ -covering system for U , we can construct a collection of classes of certain generalised centralisers whose union includes U . This is illustrated in the following lemma.

Lemma 11. *Let (a, b, A, B) be a τ -covering system for a subset U of S . Let $I \subseteq A \times B$ be the subset of pairs $(c, d) \in A \times B$ for which there is an element $x \in U$ such that $axb = cxd$, and for each such pair fix such an element $x_{c,d} = x$. Let $T = \tau(b)S^1$. Then,*

$$U \subseteq \bigcup_{(c,d) \in I} \gamma_{a,c}^T(x_{c,d}).$$

Proof. Let $u \in U$. By the definition of covering system, there are elements $c \in A$ and $d \in B$ such that $aub = cud$. Note that $a \neq c$ since the definition of covering system requires $a \notin A$. By Lemma 8, it follows that $(u, x_{c,d}) \in \gamma_{a,c}^T$, or, in other words, that $u \in \gamma_{a,c}^T(x_{c,d})$. $\square$

It is also possible to go the other way: to pass from a union of classes of generalised centralisers to a covering system. This is demonstrated, in the form that we shall later need, by the next lemma.

Lemma 12. *Let T be a right ideal of S , let $a \in S$, and let A be a finite subset of the τ -class of a with $a \notin A$. Suppose that $\{c_i \mid 1 \leq i \leq n\}$ and $\{x_i \mid 1 \leq i \leq n\}$ are two families (possibly with repeated elements) with each $c_i \in A$ and $x_i \in S$. Further suppose that there is an $x \in S$ such that*

$$Sx \subseteq \bigcup_{i=1}^n \gamma_{a,c_i}^T(x_i).$$

Then there are elements $\hat{b}$ and $\hat{d}_i$, $1 \leq i \leq n$, with the following properties:

- (i) *For any $s \in S$ there is an i for which $as\hat{b} = c_is\hat{d}_i$.*
- (ii) *For each i , if there is an $s \in S$ such that $as\hat{b} = c_is\hat{d}_i$, then $(\hat{d}_i, \hat{b}) \in \tau$.*

If we put $B = \{\hat{d}_i \mid 1 \leq i \leq n\}$, then condition (i) of the lemma tells us that $(a, \hat{b}, A, B)$ is a covering system for S . Condition (ii) allows us to improve this to a τ -covering system by simply throwing out all elements of B which are not actually needed to cover S . Note that we did not state the conclusion of the lemma in the form “there is an element $\hat{b}$ and a set B such that $(a, \hat{b}, A, B)$ is a τ -covering system for S ” because we shall need the extra information that links the $\hat{d}_i$ ’s to specific c_i ’s when we come to apply it.

Proof. Fix an element $t \in T$, so that $tS^1 \subseteq T$.

Because $(a, c_i) \in \rho$ for each i , we can inductively define elements b_i and e_i , for $1 \leq i \leq n$, such that

$$(2) \quad ax_itb_1b_2 \cdots b_{i-1}b_i = c_ix_itb_1b_2 \cdots b_{i-1}e_i.$$

Put $b = tb_1b_2 \cdots b_n$ and for $1 \leq i \leq n$ put $d_i = tb_1b_2 \cdots b_{i-1}e_ib_{i+1} \cdots b_n$. Note that $b, d_i \in T$. Multiplying (2) on the right by $b_{i+1}b_{i+2} \cdots b_n$, we obtain, for each i ,

$$(3) \quad ax_ib = c_ix_id_i.$$

By the remarks preceding Lemma 4, there is an element $y \in S$ such that, for each i , either $(yxb, yxd_i) \in \rho'$ or $Syxb \cap Syxd_i = \emptyset$. Put $\hat{b} = yxb$ and $\hat{d}_i = yxd_i$.

Let $s \in S$. Then $syx \in Sx$, so there is an i for which $syx \in \gamma_{a,c_i}^T(x_i)$. By (3) and the definition of γ_{a,c_i}^T , we have

$$as\hat{b} = asyxb = c_isyxd_i = c_is\hat{d}_i.$$

This proves (i).

For (ii), note that if there is an $s \in S$ such that $as\hat{b} = c_is\hat{d}_i$, then $as\hat{b} \in S\hat{b} \cap S\hat{d}_i = Syxb \cap Syxd_i$. By choice of y , this means that $(\hat{b}, \hat{d}_i) = (yxb, yxd_i) \in \rho'$. Notice, from (3) and the fact that ρ is left-cancellative, that $(b, d_i) \in \rho$ for all i . Since ρ is a congruence, we see that $(\hat{b}, \hat{d}_i) \in \rho$. Thus, $(\hat{b}, \hat{d}_i) \in \tau$, as claimed. $\square$

7. REDUCTION OF COVERING SYSTEMS

If a group G is covered by a finite union of cosets of subgroups, then one of those subgroups has finite index [12, Lemma 4.2.1], which is to say that G can be covered by a finite union of cosets of a single one of those subgroups. This fact is crucial to the proof of the Connell-Passman Theorem (see [12, §4.2]), where it is applied in the case that the subgroups in question are centralisers.

In the present situation, the corresponding result takes the following form.

Proposition 13. *Let S be a cancellative semigroup and let (a, b, A, B) be a τ -covering system for S . Then there is an element $c \in A$ such that $(a, c) \in \omega$.*

We defer the proof until the next section. The rest of the current section is devoted to a discussion of the result, to a new ingredient required for its proof, and to a simple consequence of the proposition.

By Lemma 10, we may rephrase the conclusion of the proposition to say that there is a one-element subset $A' \subseteq A$ (namely, $A' = \{c\}$) for which there exists a τ -covering system (a, b', A', B') . So the proposition can be understood to say that we may reduce A to a singleton and still form a τ -covering system.

If we associate unions of classes of generalised centralisers with these τ -covering systems (cf. Lemma 11), then we can interpret the proposition as saying that a given covering of S by a finite union of classes of several generalised centralisers $\gamma_{a,c}^T$ (with c varying) can be reduced to a covering of S by a finite union of classes of a single generalised centraliser $\gamma_{a,c}^{T'}$. Note however, that the parameter T may change to some other T' . In this form, the corresponding statement about covering a group by cosets is recognisable.

We follow this route in the proof: after translating the covering system into a union of γ -classes, we eliminate one of those classes, and translate the information back to a new covering system, which is, in some sense, smaller than the original covering system. In order to explain precisely what we mean by ‘smaller’ in this context, we must augment the definition of covering system as follows.

Definition 14. An *indexed covering system* for S , written $(a, b, A, \{B_c\}_{c \in A})$, consists of two elements $a, b \in S$, a finite subset A of S with $a \notin A$, and a family $\{B_c \mid c \in A\}$ of finite subsets of S with $b \notin \bigcup_{c \in A} B_c$, such that the following property holds: for any $s \in S$ there is a $c \in A$ and a $d \in B_c$ with $asb = csd$.

If, in addition, $A \subseteq \tau(a)$ and $B_c \subseteq \tau(b)$ for each $c \in A$, then $(a, b, A, \{B_c\}_{c \in A})$ is an *indexed τ -covering system* for S .

Given an indexed τ -covering system $(a, b, A, \{B_c\}_{c \in A})$, we define its *width* to be $\min_{c \in A} |B_c|$.

It is convenient to permit $B_c = \emptyset$ in the definition of indexed covering system; of course, such an indexed covering system would have width zero.

We can turn a τ -covering system (a, b, A, B) into an indexed τ -covering system by putting $B_c = B$ for each $c \in A$, or, more economically, taking $B_c = \{d \in B \mid \text{there exists an } s \in S \text{ such that } asb = csd\}$. Conversely, if $(a, b, A, \{B_c\}_{c \in A})$ is an indexed τ -covering system, then $(a, b, A, \bigcup_{c \in A} B_c)$ is a τ -covering system.

The following special case of Theorem 1 is immediately deduced from Proposition 13.

Corollary 15. *Let S be a cancellative semigroup and suppose that ω is trivial. Then $K[S]$ is prime.*

Proof. If $K[S]$ is not prime, then S satisfies an identity $\alpha x \beta = 0$. By Proposition 5, we may assume that α and β are τ -constant elements. Using Example 1, we construct a τ -covering system (a, b, A, B) for S . Proposition 13 shows that ω is non-trivial. $\square$

8. PROOF OF PROPOSITION 13

Let (a, b, A, B) be a τ -covering system for S .

Among all τ -covering systems (a, b', A', B') for S with $A' \subseteq A$, choose one with $|A'|$ as small as possible. Without loss of generality, we may assume that (a, b, A, B) is this covering system.

If $|A| = 1$, say $A = \{c\}$, then by Lemma 10 we have $(a, c) \in \omega$ as required.

Suppose instead that $|A| > 1$. Under this assumption Lemma 10 and the minimality of (a, b, A, B) imply that there is no $c \in A$ for which $(a, c) \in \omega$.

Now consider all possible indexed τ -covering systems $(a, b', A, \{B'_c\}_{c \in A})$ with a and A fixed, and choose one of minimal width. To keep the notation as simple as possible, let us assume that this minimal width system is $(a, b, A, \{B_c\}_{c \in A})$. Let m be its width, and fix $e \in A$ with $m = |B_e|$. Note that we cannot have $m = 0$ here, for otherwise $(a, b, A \setminus \{e\}, \bigcup_{c \in A} B_c)$ would be a τ -covering system, and this contradicts the minimality of $|A|$. So $B_e \neq \emptyset$.

We may assume without loss of generality that for each $c \in A$ and each $d \in B_c$, there is an element $x_{c,d} \in S$ with

$$(4) \quad ax_{c,d}b = cx_{c,d}d;$$

otherwise we could remove d from B_c and still have an indexed τ -covering system for S . If we put $T = \tau(b)S^1$, then, as in Lemma 11, we have

$$(5) \quad S \subseteq \bigcup_{c \in A} \bigcup_{d \in B_c} \gamma_{a,c}^T(x_{c,d}).$$

We claim that for any $x \in S$, we cannot have

$$(6) \quad xS \subseteq \bigcup_{d \in B_e} \gamma_{a,e}^T(x_{e,d}).$$

Suppose that this were so for some x . Then for any $s \in S$, we have $(xs, x_{e,d}) \in \gamma_{a,e}^T$ for some $d \in B_e$, and, from (4), we conclude that $axsb = exsd$. But this says that $(ax, ex) \in \omega$, witnessed by the τ -constant set $\{b\} \cup B_e$. Since ω is cancellative, we obtain $(a, e) \in \omega$, which is a contradiction.

Fix an element $f \in B_e$. Since (6) is not satisfied for $x = x_{e,f}b$, there is an $s \in S$ with $x_{e,f}bs \notin \bigcup_{d \in B_e} \gamma_{a,e}^T(x_{e,d})$. Put $t = bs \in T$; then $x_{e,f}bs = x_{e,f}t$. Since $\gamma_{a,e}^T$ is an equivalence relation, different $\gamma_{a,e}^T$ -classes are disjoint. Thus

$$\gamma_{a,e}^T(x_{e,f}t) \cap \bigcup_{d \in B_e} \gamma_{a,e}^T(x_{e,d}) = \emptyset,$$

so that, by (5),

$$(7) \quad \gamma_{a,e}^T(x_{e,f}t) \subseteq \bigcup_{\substack{c \in A \\ c \neq e}} \bigcup_{d \in B_c} \gamma_{a,c}^T(x_{c,d}).$$

Let $s \in S$. If $s \in \gamma_{a,e}^T(x_{e,f})$, then $st \in \gamma_{a,e}^T(x_{e,f}t)$ by Lemma 7(i), and using (7) we see that

$$st \in \bigcup_{\substack{c \in A \\ c \neq e}} \bigcup_{d \in B_c} \gamma_{a,c}^T(x_{c,d}).$$

Otherwise, by (5), we have $s \in \gamma_{a,c}^T(x_{c,d})$ for a pair $(c,d) \neq (e,f)$, and then $st \in \gamma_{a,c}^T(x_{c,d}t)$. Combining these two cases, we conclude that

$$(8) \quad St \subseteq \bigcup_{\substack{c \in A \\ c \neq e}} \bigcup_{d \in B_c} \gamma_{a,c}^T(x_{c,d}) \cup \bigcup_{\substack{c \in A \\ c \neq e}} \bigcup_{d \in B_c} \gamma_{a,c}^T(x_{c,d}t) \cup \bigcup_{\substack{d \in B_e \\ d \neq f}} \gamma_{a,e}^T(x_{e,d}t).$$

The next step is to apply Lemma 12 to (8). Each γ -class in the above union corresponds to a class $\gamma_{a,c_i}^T(x_i)$ in the notation of Lemma 12. The lemma produces for us the element $\hat{b}$ and a family of elements $\{\hat{d}_i\}$, one for each γ -class in the union. We shall adopt a different notation for this family to better indicate the γ -class correspondence: for each class in (8) of the form $\gamma_{a,c}^T(x_{c,d})$, write $\hat{g}_{c,d}$ for the corresponding $\hat{d}_i$, and for each class of the form $\gamma_{a,c}^T(x_{c,d}t)$, write $\hat{h}_{c,d}$ for the corresponding $\hat{d}_i$.

Thus, translating conclusion (i) of Lemma 12 into this notation, we see that for any $s \in S$, at least one of the following holds:

- (i) For some $c \in A$, $c \neq e$, and some $d \in B_c$, we have $as\hat{b} = cs\hat{g}_{c,d}$.
- (ii) For some $c \in A$, $c \neq e$, and some $d \in B_c$, we have $as\hat{b} = cs\hat{h}_{c,d}$.
- (iii) For some $d \in B_e$, $d \neq f$, we have $as\hat{b} = es\hat{h}_{e,d}$.

For $c \in A$, $c \neq e$, put $\hat{B}_c = \{\hat{g}_{c,d}, \hat{h}_{c,d} \mid d \in B_c\}$, and put $\hat{B}_e = \{\hat{h}_{e,d} \mid d \in B_e, d \neq f\}$. By (i)–(iii) above, we conclude that $(a, \hat{b}, A, \{\hat{B}_c\}_{c \in A})$ is an indexed covering system for S . By Lemma 12(ii), after possibly discarding some elements of some of the sets $\hat{B}_c$, we can assume that $(a, \hat{b}, A, \{\hat{B}_c\}_{c \in A})$ is an indexed τ -covering system for S .

But note that $|\hat{B}_e| \leq |B_e \setminus \{f\}| < |B_e| = m$, so that $(a, \hat{b}, A, \{\hat{B}_c\}_{c \in A})$ has width strictly smaller than the width of $(a, b, A, \{B_c\}_{c \in A})$, a contradiction.

This final contradiction completes the proof of Proposition 13. $\square$

9. FINITE INDEX

An element of the FC-centre of a group G has the property that its centraliser is a subgroup of finite index in G . In this section we develop a notion of finite index for relations in cancellative semigroups and apply it to generalised centralisers.

Although the definition and many of the elementary results make sense for arbitrary equivalence relations, we shall restrict our attention to right T -congruences.

Fix a right ideal T of S and a right T -congruence σ . We write S/σ for the set of σ -classes of S , and if W is any subsemigroup of S , we write W/σ for the set of σ -classes restricted to W (excluding those classes which do not intersect W). We say that σ has finite index in S if $|S/\sigma| < \infty$, that is, if there are finitely many σ -classes. Finite index is preserved under finite intersections:

Lemma 16. *Let σ_i , $1 \leq i \leq n$, be a family of right T -congruences each of which has finite index in S . Then $\xi = \bigcap_{i=1}^n \sigma_i$ is also a right T -congruence of finite index.*

Proof. Clearly ξ is a right T -congruence. There is a natural set injection $S/\xi \rightarrow S/\sigma_1 \times S/\sigma_2 \times \cdots \times S/\sigma_n$. $\square$

Drawing on the analogy with the group situation, we should expect a generalised centraliser $\gamma_{a,c}^T$ to have finite index if $(a, c) \in \omega$. This is indeed the case, provided that we choose the right ideal T appropriately. We state the result in the form in which we shall need it later.

Lemma 17. *Let $a \neq c$ with $(a, c) \in \omega$, let $b \in S$, and let $u \in S^1$. Then there is a $v \in S$ such that, putting $T = \tau(b)uvS^1$, the relation $\gamma_{a,c}^T$ has finite index in S .*

Proof. Since $(a, c) \in \omega$, there is a finite τ -constant set F such that $axF \cap cxF \neq \emptyset$ for all $x \in S$. In particular, $axbuF \cap cxbuF \neq \emptyset$ for all $x \in S$. Fix $v \in F$ and put $T = \tau(b)uvS^1$.

For elements $g, h \in F$, define $A(g, h) = \{x \in S \mid axbug = cxbuh\}$. (We need only consider $g \neq h$, since cancellativity forces $A(g, g) = \emptyset$.) Let $x, y \in A(g, h)$. Note that $bug, buh \in \tau(buv)$, so by Lemma 8 we have $(x, y) \in \gamma_{a,c}^{T'}$, where $T' = \tau(buv)S^1$. Since $T \subseteq T'$, we have $(x, y) \in \gamma_{a,c}^T$ by Lemma 7(ii).

By choice of F we see that $S \subseteq \bigcup_{g,h \in F} A(g, h)$. Since each non-empty $A(g, h)$ is contained in a $\gamma_{a,c}^T$ -class, the union of the finite number of $\gamma_{a,c}^T$ -classes so determined covers S . Hence $\gamma_{a,c}^T$ has finite index. $\square$

Let $s \in S$, and let σ be a right T -congruence. Define a relation $s^{-1}\sigma$ by $(x, y) \in s^{-1}\sigma$ if and only if $(sx, sy) \in \sigma$. It is easily seen that $s^{-1}\sigma$ is also a right T -congruence. (If s has an inverse in S , then this notation agrees with the interpretation of $s^{-1}\sigma$ as the product of the element s^{-1} with the subset $\sigma \subseteq S \times S$.)

Lemma 18. *Let σ be a right T -congruence for some right ideal T of S and let $s \in S$. Then $|S/s^{-1}\sigma| = |sS/\sigma| \leq |S/\sigma|$. If σ has finite index in S , then so does $s^{-1}\sigma$.*

Proof. The map $x \mapsto sx$ induces a bijection of sets $S/s^{-1}\sigma \rightarrow sS/\sigma$. $\square$

The following lemma shows that $s^{-1}\gamma$ remains a generalised centraliser. If specialised to a group, this lemma merely states the trivial fact that the centraliser of a conjugate g^s is the conjugate by s of the centraliser of g .

Lemma 19. *Let T be a right ideal of S , and let a, c , and s be elements of S . Then $s^{-1}\gamma_{a,c}^T = \gamma_{as,cs}^T$.*

Proof. From the definitions we have:

$$\begin{aligned} (x, y) \in s^{-1}\gamma_{a,c}^T & \text{ if and only if } (sx, sy) \in \gamma_{a,c}^T \\ & \text{ if and only if } asxb = csxd \Leftrightarrow asyb = csyd \quad \text{for all } b, d \in T \\ & \text{ if and only if } (x, y) \in \gamma_{as,cs}^T. \quad \square \end{aligned}$$

10. REDUCTION TO ω -CLASSES

We show that if $K[S]$ satisfies an identity of the form $\alpha x \beta = 0$, then we may assume that α and β are ω -constants.

We adopt the following notational convention: if $\alpha = \sum_{s \in S} k_s s$ and $W \subseteq S$, then $\alpha_W = \sum_{s \in W} k_s s$.

Lemma 20. *Suppose that α and β are non-zero τ -constant elements of $K[S]$ and that $\alpha x \beta = 0$ for all $x \in S$. Let W be an ω -class of S which meets $\text{supp}(\alpha)$. Then there is an element $z \in S^1$ such that $\alpha_W z x \beta = 0$ for all $x \in S$.*

Before giving the proof, which is the main substance of this section, we quickly derive from it the result that we want.

Proposition 21. *Suppose that α and β are non-zero τ -constant elements of $K[S]$ and that $\alpha x \beta = 0$ for all $x \in S$. Then there are non-zero ω -constant elements α' and β' such that $\alpha' x \beta' = 0$ for all $x \in S$. If, in addition, $\alpha = \beta$, then we may take $\alpha' = \beta'$.*

Proof. Let W be an ω -class which meets $\text{supp}(\alpha)$, and let V be an ω -class which meets $\text{supp}(\beta)$. By Lemma 20, there is an element $z \in S^1$ such that $\alpha_W z x \beta = 0$ for all $x \in S$. Applying the left-right dual of the lemma to this new identity, there is an element $y \in S^1$ such that $\alpha_W z x y \beta_V = 0$ for all $x \in S$. Put $\alpha' = \alpha_W z$ and $\beta' = y \beta_V$; these are ω -constant elements of $K[S]$ since ω is a congruence.

If $\alpha = \beta$, we may take $W = V$, and put $\alpha' = \beta' = y \alpha_W z$. $\square$

Suppose that Lemma 20 is not true; then there is no z such that S satisfies the identity $\alpha_W z x \beta = 0$. We shall derive a contradiction in several steps. Notation introduced as we go is fixed until the end of the proof.

Let $\text{supp}(\alpha_W) = \{a_i \mid 1 \leq i \leq k\}$. Let u be an element of S , for the moment unspecified, let $b_0 \in \text{supp}(\beta)$, and let $T = \tau(b_0)uS^1$. For each pair (i, j) with $1 \leq i < j \leq k$, define $\gamma_{i,j} = \gamma_{a_i,a_j}^T$, and let $\xi = \bigcap_{i,j} \gamma_{i,j}$.

Step 1. *There is a choice of u so that ξ has finite index in S .*

Proof. By Lemma 16, we need only find a u such that each $\gamma_{i,j}$ has finite index.

Totally order the pairs (i, j) , for $i < j$, lexicographically: $(1, 2) < (1, 3) < \dots < (1, k) < (2, 3) < \dots < (k-1, k)$. Using Lemma 17, there is a $T_{1,2} = \tau(b)v_{1,2}S^1$ such that $\gamma_{a_1,a_2}^{T_{1,2}}$ has finite index in S . Applying the lemma again, there is a $T_{1,3} = \tau(b)v_{1,2}v_{1,3}S^1$ such that $\gamma_{a_1,a_3}^{T_{1,3}}$ has finite index. We have $\gamma_{a_1,a_2}^{T_{1,2}} \subseteq \gamma_{a_1,a_2}^{T_{1,3}}$ by Lemma 7(ii), since $T_{1,3} \subseteq T_{1,2}$, and so $\gamma_{a_1,a_2}^{T_{1,3}}$ still has finite index.

Continuing in this way, through all pairs (i, j) in order, we get a sequence of right ideals $T_{i,j} = \tau(b)v_{1,2}v_{1,3} \dots v_{i,j}S^1$ such that each relation $\gamma_{a_k,a_l}^{T_{i,j}}$ has finite index for $(k, l) \leq (i, j)$. Put $u = v_{1,2}v_{1,3} \dots v_{k-1,k}$ and $T = T_{k-1,k}$. $\square$

Let $z \in S$. Because ω is cancellative, we see that $\alpha_W z = (\alpha z)_V$, where $V = \omega(a_1 z)$. Of course, we have $\alpha z y \beta = 0$ for all $y \in S$. So it suffices to prove the lemma

for αz and V instead of α and W , for if there is a $w \in S$ such that $(\alpha z)_V w y \beta = 0$ for all $y \in S$, then $\alpha_W z' y \beta = 0$ for all $y \in S$, where $z' = zw$.

By Lemma 19,

$$z^{-1}\xi = \bigcap_{i,j} z^{-1}\gamma_{i,j} = \bigcap_{i,j} \gamma_{a_i z, a_j z}^T$$

and by Lemma 18 and Step 1, the relation $z^{-1}\xi$ has finite index in S . Since $\text{supp}(\alpha z) \cap V = \{a_1 z, a_1 z, \dots, a_k z\}$, we see that $z^{-1}\xi$ has the same relation to αz as ξ does to α .

Choose z so that the index $|S/z^{-1}\xi|$ is as small as possible. Replacing α by αz , W by V , $\gamma_{i,j}$ by $z^{-1}\gamma_{i,j}$, and ξ by $z^{-1}\xi$, we may assume that for all $s \in S$ we have $|S/s^{-1}\xi| = |S/\xi|$.

A consequence of this is:

Step 2. *We may assume that for all $s \in S$, the right ideal sS intersects each ξ -class of S non-trivially.*

Proof. Otherwise, the embedding $S/s^{-1}\xi \rightarrow sS/\xi \rightarrow S/\xi$ would not be a bijection. $\square$

By assumption, there is an element $x \in S$ such that $\alpha_W x \beta \neq 0$. Let $U = \xi(x)$, the ξ -class containing x . Our next task is to construct a τ -covering system for U . Since $\alpha_W x \beta \neq 0$, there are elements $a \in \text{supp}(\alpha_W)$ and $b \in \text{supp}(\beta)$ such that $axb \in \text{supp}(\alpha_W x \beta)$. Without loss of generality, suppose that $a = a_1$. Let $A = \text{supp}(\alpha - \alpha_W)$ and let $B = \text{supp}(\beta) \setminus \{b\}$.

Step 3. *The system (a, b, A, B) is a τ -covering system for U .*

Proof. Let $y \in U$, so that $(y, x) \in \xi$. Write $B = \{d_1, d_2, \dots, d_m\}$.

Let i and j be arbitrary indices with $2 \leq i \leq k$ and $1 \leq j \leq m$. We have $(y, x) \in \gamma_{1,i}$, since $\xi \subseteq \gamma_{1,i}$. Note that $bu, d_j u \in T$, so by definition of $\gamma_{1,i}$, $axbu = a_i x d_j u$ if and only if $aybu = a_i y d_j u$. Cancelling u , we obtain

$$(9) \quad axb = a_i x d_j \quad \text{if and only if} \quad ayb = a_i y d_j.$$

Let $\alpha_W = \lambda_0 a + \lambda_2 a_2 + \dots + \lambda_k a_k$ and $\beta = \mu_0 b + \mu_1 d_1 + \dots + \mu_m d_m$, with each λ_i and μ_i an element of the field K . Then the coefficient of axb in $\alpha_W x \beta$ is

$$\lambda_0 \mu_0 + \sum_{axb=a_i x d_j} \lambda_i \mu_j.$$

But by (9), this is exactly the same as the coefficient of ayb in $\alpha_W y \beta$. Since $axb \in \text{supp}(\alpha_W x \beta)$ by choice of x , a , and b , we conclude that this coefficient is non-zero and so $ayb \in \text{supp}(\alpha_W y \beta)$.

Now, $\alpha y \beta = 0$ and $\alpha = \alpha_W + \alpha_A$, so

$$\alpha_W y \beta = -\alpha_A y \beta,$$

which means that $ayb \in \text{supp}(\alpha_A y \beta)$. Hence, there is a $c \in A$ and a $d \in \text{supp}(\beta)$ such that $ayb = cyd$. Since $a \neq c$ we must have $d \neq b$, and so $d \in B$. In other words, there is a pair $c \in A$ and $d \in B$ such that $ayb = cyd$.

Since y is an arbitrary element of U , this shows that (a, b, A, B) is a covering system for U . That (a, b, A, B) is a τ -covering system follows at once, since the elements of A and B come from the supports of τ -constant semigroup algebra elements. $\square$

Our goal now is to extend the τ -covering system (a, b, A, B) for U to a τ -covering system $(a, \hat{b}, A, \hat{B})$ of S . We shall do so by covering each ξ -class in turn. Accordingly, let $x_1 = x, x_2, x_3, \dots, x_r$ be representatives from the ξ -classes, and let $U_i = \xi(x_i)$.

We single out a few elementary manipulations of covering systems, the validity of which is easily checked from the definition.

Lemma 22. *Let $X \subseteq S$ and let (a, b, A, B) be a τ -covering system for X .*

- (i) *For any $s \in S$, the collection (a, bs, A, Bs) is also a τ -covering system for X .*
- (ii) *If $Yy \subseteq X$ for some $y \in S$ and $Y \subseteq S$, then (a, yb, A, yB) is a τ -covering system for Y .*
- (iii) *If (a, b, A, B') is a τ -covering system for another set X' , then $(a, b, A, B \cup B')$ is a τ -covering system for $X \cup X'$. $\square$*

We shall extend (a, b, A, B) to cover each U_i in turn, using the following induction step.

Step 4. *Let (a, b_i, A, B_i) be a τ -covering system for $U_1 \cup U_2 \cup \dots \cup U_i$ with $b_i \in T$ and $B_i \subseteq T$. Then there is a $b_{i+1} \in T$ and a set $B_{i+1} \subseteq T$ so that (a, b_{i+1}, A, B_{i+1}) is a τ -covering system for $U_1 \cup U_2 \cup \dots \cup U_{i+1}$.*

Proof. Recall that $U_{i+1} = \xi(x_{i+1})$.

By the assumption of Step 2, $x_{i+1}b_iS \cap \xi(x) \neq \emptyset$, so there is an element $s \in S$ such that $x_{i+1}b_is \in \xi(x)$.

Let $y \in U_{i+1}$. Then $(y, x_{i+1}) \in \xi$ and $b_is \in T$, so, ξ being a right T -congruence, we have $(yb_is, x_{i+1}b_is) \in \xi$. But $x_{i+1}b_is \in \xi(x)$, so $yb_is \in \xi(x) = U_1$. This shows that $U_{i+1}b_is \subseteq U_1$.

By Lemma 22(ii), (a, b_isb_i, A, b_isB_i) is a τ -covering system for U_{i+1} . But, by Lemma 22(i), (a, b_isb_i, A, B_isb_i) is a τ -covering system for $U_1 \cup U_2 \cup \dots \cup U_i$. Put $b_{i+1} = b_isb_i$ and $B_{i+1} = b_isB_i \cup B_isb_i$. Then Lemma 22(iii) says that the combined system (a, b_{i+1}, A, B_{i+1}) is a τ -covering system for $U_1 \cup U_2 \cup \dots \cup U_{i+1}$.

Note that $b_{i+1} \in T$ and $B_{i+1} \subseteq T$, because T is a right ideal of S . $\square$

Step 5. *There is an element $\hat{b}$ and a set $\hat{B}$ such that $(a, \hat{b}, A, \hat{B})$ is a τ -covering system for S .*

Proof. Put $b_1 = bu$ and $B_1 = Bu$; then $\{b_1\} \cup B_1 \subseteq T$, and (a, b_1, A, B_1) is a τ -covering system for $U = U_1$ by Lemma 22(i). Inductively define $b_2, b_3, \dots, b_r$ and $B_2, B_3, \dots, B_r$ according to Step 4. Put $\hat{b} = b_r$ and $\hat{B} = B_r$. Since $U_1, U_2, \dots, U_r$ are all the ξ -classes, $S = U_1 \cup U_2 \cup \dots \cup U_r$. Hence, $(a, \hat{b}, A, \hat{B})$ is a τ -covering system for S , as desired. $\square$

Applying Proposition 13 to this τ -covering system $(a, \hat{b}, A, \hat{B})$, we conclude that there is a $c \in A$ with $(a, c) \in \omega$. But this is not possible since $A \cap \omega(a) = A \cap W = \emptyset$.

This contradiction completes the proof of Lemma 20.

11. PROOF OF THEOREM 1

Having reduced the identity $\alpha x \beta = 0$ to ω -constant elements, it is now relatively simple to complete the proof of Theorem 1. Okniński [9, Theorem 2] has furnished a proof of the necessity of the conditions of Theorem 1, so it remains only to show that they are sufficient.

We begin by collecting together a few preliminary results, all of which are due to Okniński. The first is a triviality which will eventually give us the commutativity of the pair of elements required in the conditions of Theorem 1.

Lemma 23. *Let S be a cancellative semigroup and let $s, t \in S$.*

- (i) *If S has a group of right fractions, G , and $st^{-1} \in \Delta(G)$, then there is an n such that $st^n = t^n s$.*
- (ii) *If $(s, t) \in \omega$, then there is an n such that $st^n = t^n s$.*

Proof. We can prove (i) directly by noting that some power of t must be contained in the centraliser of st^{-1} because the latter is a subgroup of finite index. Alternatively, it follows from (ii) since Okniński [9, Remark 2] observed that $st^{-1} \in \Delta(G)$ implies $(s, t) \in \omega$.

For (ii), let F be a finite τ -constant set such that $sxF \cap txF \neq \emptyset$ for all $x \in S$. If we replace x by various powers of t , the finiteness of F ensures that there must be positive integers $i < j$ such that $st^i c = tt^i d$ and $st^j c = tt^j d$ for some $c, d \in F$. We conclude that $t^{j-i} st^i c = t^{j-i} tt^i d = tt^j d = st^j c$, and, cancelling on the right, that $t^{j-i} s = st^{j-i}$. (This argument is given in [9, Page 6].) $\square$

We construct a group of fractions, not from the whole cancellative semigroup S , which is not always possible, but from a certain subsemigroup.

Lemma 24 ([9, Lemma 4]). *Fix $a \in S$ and let $T = \{s \in S \mid (s, a^n) \in \omega \text{ for some } n > 0\}$. Then T is a subsemigroup and has a group of right fractions.*

In fact, T has a two-sided group of fractions, but a right group of fractions suffices for our purposes.

Proof. Let $s, t \in T$, so that $(s, a^n) \in \omega$ and $(t, a^m) \in \omega$ for some n and m . Then $(st, a^{n+m}) \in \omega$, so T is a subsemigroup. To show that T has a group of right fractions, it suffices to show that T satisfies the Ore condition: $sT \cap tT \neq \emptyset$. Assume that $m \geq n$. Then $(sa^{m-n}, t) \in \omega$, and by Lemma 23(ii), there is a k so that t^k and sa^{m-n} commute. Hence, $sa^{m-n}t^k = t^k sa^{m-n} \in sT \cap tT$. $\square$

The final preliminary result enables us to transfer an identity from a semigroup to its group of fractions. The proof, due to Okniński, involves showing that a generating subsemigroup of a group is a “very large subset” in the sense of [12, §4.2], and will be omitted.

Lemma 25 ([8, Corollary 7.18]). *Let G be a group generated by a subsemigroup S . If an identity $\alpha x \beta = 0$, with $\alpha, \beta \in K[G]$, holds for all $x \in S$, then it holds for all $x \in G$.* $\square$

Proof of Theorem 1 (sufficiency). Suppose that $K[S]$ is not prime. Then there are non-zero elements α and $\beta \in K[S]$ such that $\alpha x \beta = 0$ for all $x \in S$. By Propositions 5 and 21, we may assume that α and β are ω -constant elements. Fix $a \in \text{supp}(\alpha)$ and $b \in \text{supp}(\beta)$; then the identity $bax\beta a = 0$ is satisfied for all $x \in S$, and ba is an element of both $\text{supp}(b\alpha)$ and $\text{supp}(\beta a)$. Replacing α by $b\alpha$ and β by βa , we may assume that there is an element $a \in \text{supp}(\alpha) \cap \text{supp}(\beta)$, and since α and β are ω -constants, we have $\text{supp}(\alpha) \cup \text{supp}(\beta) \subseteq \omega(a)$.

Consider the quotient semigroup $\bar{S} = S/\omega$. Let $\bar{a}$ be the image of a in $\bar{S}$, and let $C = \langle \bar{a} \rangle$ be the cyclic subsemigroup of $\bar{S}$ generated by $\bar{a}$. Since ω is a cancellative congruence, C is cancellative, and is either a finite cyclic group or a free cyclic semigroup.

In the former case, $\bar{a}^q$ is an idempotent for some $q > 0$. Replacing α by $a^{q-1}\alpha$, β by $a^{q-1}\beta$, and a by a^q , we may assume that $\bar{a}$ is idempotent. This means that $(a, a^k) \in \omega$ for all $k > 0$.

Otherwise, if C is free, then the powers $\bar{a}, \bar{a}^2, \dots$ are distinct, which means that $a, a^2, a^3, \dots$ fall into different ω -classes of S .

Let $T = \{s \in S \mid (s, a^n) \in \omega \text{ for some } n > 0\}$. Since $\text{supp}(\alpha) \cup \text{supp}(\beta) \subseteq \omega(a) \subseteq T$, we may regard α and β as elements of $K[T]$, and we have the identity $\alpha x \beta = 0$ for all $x \in T$.

By Lemma 24, T has a group of right fractions G , and by Lemma 25, we have $\alpha x \beta = 0$ for all $x \in G$. Thus, the group algebra $K[G]$ is not prime. By the Connell-Passman Theorem, there is an element $1 \neq g \in \Delta(G)$ of finite order n , say. Write $g = st^{-1}$ with $s, t \in T$. By Lemma 23(i), there is a k such that s and t^k commute. Note that $g = st^{-1} = (st^{k-1})(t^k)^{-1}$. Replacing s by st^{k-1} and t by t^k , we may assume that s and t commute. Since $g \neq 1$, we have $s \neq t$. Since $g^n = 1$, we have $s^n = t^n$.

It remains to show that $(s, t) \in \omega$. In the first case above, when $(a, a^k) \in \omega$ for all $k > 0$, we have $T = \omega(a)$, so certainly $(s, t) \in \omega$. Otherwise, the various powers of a fall into distinct ω -classes. Suppose that $(s, a^i) \in \omega$ and $(t, a^j) \in \omega$. Then $s^n = t^n$ implies $(a^{in}, a^{jn}) \in \omega$, whence $in = jn$ and $i = j$. So in the second case, we again get $(s, t) \in \omega$.

The pair (s, t) satisfies the required conditions of Theorem 1, completing the proof of the prime case.

The semiprime case is similar. If $K[S]$ is not semiprime, then we proceed as before, except that $\alpha = \beta$ throughout. The Connell-Passman Theorem tells us that $\text{char}(K) = p > 0$, and produces an element $g \in \Delta(G)$ of order p . We obtain s and t as before, with $s^p = t^p$. $\square$

ACKNOWLEDGEMENT

The author would like to thank Professor Bruno Müller for his encouragement of the research which lead to this paper.

REFERENCES

1. J. Bergen and D. S. Passman, *Delta methods in enveloping rings*, J. Algebra **133** (1990), 277–312. MR **92b**:16056
2. ———, *Delta methods in enveloping algebras of Lie superalgebras*, Trans. Amer. Math. Soc. **334** (1992), 259–280. MR **93a**:17008
3. ———, *Delta methods in enveloping rings II*, J. Algebra **156** (1993), 494–534. MR **94j**:16044
4. ———, *Delta methods in enveloping algebras of Lie superalgebras II*, J. Algebra **166** (1994), 568–610. MR **95j**:17007
5. A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*. Vols. I, II, American Mathematical Society, Providence, Rhode Island, 1961, 1967. MR **24**:A2627; MR **36**:1558
6. I. G. Connell, *On the group ring*, Canad. J. Math. **15** (1963), 650–685. MR **27**:3666
7. J. Krempa, *Special elements in semigroup rings*, Bull. Acad. Polon. Sci. Sér. Sci. Math. **28** (1980), 17–23. MR **82g**:20103
8. J. Okniński, *Semigroup algebras*, Marcel Dekker, New York, 1991. MR **92f**:20076
9. ———, *Prime and semiprime semigroup rings of cancellative semigroups*, Glasgow Math. J. **35** (1993), 1–12. MR **93j**:16012
10. D. S. Passman, *Nil ideals in group rings*, Michigan Math. J. **9** (1962), 375–384. MR **26**:2470
11. ———, *Radicals of twisted group rings*, Proc. London Math. Soc. (3) **20** (1970), 409–437. MR **42**:6129
12. ———, *The algebraic structure of group rings*, John Wiley and Sons, New York, 1977. MR **81d**:16001

13. ———, *Semiprime and prime crossed products*, J. Algebra **83** (1983), 158–178. MR **85b**:16008
14. ———, *Infinite crossed products and group-graded rings*, Trans. Amer. Math. Soc. **284** (1984), 707–727. MR **85j**:16012
15. ———, *Infinite crossed products*, Academic Press, Boston, 1989. MR **90g**:16002

86 HERKIMER ST., APT. A, HAMILTON, ONTARIO, CANADA L8P 2G7

Current address: Andyne Computing Ltd., 1 Research Drive, Dartmouth, Nova Scotia, B2Y 4M9 Canada

E-mail address: michael.clase@ns.sympatico.ca