ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 4, 2006

THE MINIMAL GENERATING SETS OF THE MULTIPLICATIVE MONOID OF A FINITE COMMUTATIVE RING

DAVID E. DOBBS AND BRIAN C. IRICK

ABSTRACT. For any finite commutative multiplicative monoid S with an element 0 such that $S0 = \{0\} \neq S$, some decompositions of S are given as the disjoint union of a submonoid of S and some prime ideals of some submonoids of S. These decompositions lead to an algorithm producing all the minimal generating sets of S in terms of semigroup-theoretic generating sets of minimal prime ideals of some submonoids of S and minimal generating sets of the group of invertible elements of S. This algorithm is applied in case S is the multipicative monoid of a finite nonzero commutative ring R. For any such R, each application of the algorithm terminates in the same number of steps, namely, the number of prime ideals of R, that is, the number of minimal prime ideals of S.

1. Introduction. All rings considered below are commutative with identity; all semigroups and monoids considered below are commutative. Our interest is in developing some semigroup- and monoid-theoretic results that have applications to ring theory. Perhaps the most useful monoid associated to a ring R is the *multiplicative monoid* of R, i.e., the structure consisting of the underlying set of R and its binary operation of multiplication. One sees this topic in the current *renaissance* in factorization theory, but it was already apparent in Jacobson's approach to unique factorization domains via Gaussian monoids [**7**, pp. 115–127].

In dealing with the semigroup-ring interface, one must exercise caution, as the semigroup-theoretic ideal theory of S may differ from the ring-theoretic ideal theory of R. A result of Aubert [**3**] characterizes the rings R such that each (semigroup-theoretic) ideal of S is an (ring-theoretic) ideal of R. One such class of rings consists of the special principal ideal rings, or SPIRs; this follows from a well-known factorization result [**10**, Example, p. 245]. (Recall from [**10**, p. 245] that a ring R is called an SPIR in the case where R is a quasilocal principal ideal

Received by the editors on July 7, 2003, and in revised form on May 19, 2004.

Copyright ©2006 Rocky Mountain Mathematics Consortium

ring whose unique maximal ideal is nilpotent.) As Bullington [**4**] has recently determined the minimal generating sets of submodules of any free module over a finite SPIR, we are motivated to seek the minimal generating sets of S in case R is a finite SPIR. More generally, Corollary 2.6 (b), see also the commentary following Proposition 2.4, constructs all the minimal generating sets of the multiplicative monoid S of any finite local ring R. This is generalized in Theorem 4.2 (a), which shows that we have constructed all the minimal generating sets of the multiplicative monoid of any finite nonzero ring that is not a field.

There is a ring-theoretic reason to be interested in determining the minimal generating sets of the multiplicative monoid of a ring. According to a result of Isbell [**6**], cf. alternate proofs in [**1**, Corollary 1 and Remark 3], [**2**, Theorem 2.3], a ring is finite if (and only if) its multiplicative monoid is finitely generated, and hence if and only if its multiplicative monoid has a finite minimal generating set. One is thus led to ask for the structure of all the minimal generating sets of the multiplicative monoid of a finite ring R. Apart from the trivial cases in which R is either 0 or a finite field, this question is answered in Theorem 4.2.

Our work is couched more generally than may be apparent from the above summary. Our main context is a *nontrivial finite semigroup with zero*, in the sense of [**9**, p. 49], i.e., a (multiplicatively written) finite monoid S containing an element 0 such that $0S = \{0\} \neq S$. (An example of such an S is provided by the multiplicative monoid of any finite nonzero ring.) In Algorithm 2.5, we construct a family of minimal generating sets of S in terms of semigroup-theoretic generating sets of minimal prime ideals of some submonoids of S and minimal generating sets of the group of invertible elements of S. The case in which $\{0\}$ is a maximal ideal of S is dispatched in Proposition 2.4 and the ensuing commentary; the associated ring-theoretic application of Proposition 2.4 reduces to the context of a finite field.

Section 3 is devoted to proving the converse of Algorithm 2.5. In Theorem 3.3, we establish that every minimal generating set of a nontrivial finite semigroup with zero can be obtained by applying the algorithm in Algorithm 2.5. To facilitate this proof, Section 3 begins by introducing some standing hypotheses and giving some technical lemmas. The most general ring-theoretic applications of Theorems 2.5 and 3.3 are given in Theorem 4.2. The purpose of Remark 4.3

is twofold. Its part (a) gives two examples that underscore the need for care in the earlier proofs in case the given semigroup with zero does not arise as the multiplicative monoid of a finite ring. Remark 4.3 (b) indicates that it is not straightforward to develop a direct proof of the ring-theoretic applications in Theorem 4.2 that would avoid some of the semigroup-theoretic complexities in the proof of Theorem 3.3.

Some of the supporting technical details that we develop may seem counterintuitive to a ring-theorist accustomed to the fact that any finite nonzero ring has Krull dimension 0, cf. [**10**, Theorem 2, p. 203] and Lemma 2.2 (b). However, some noteworthy semigroup-ring compatibility is established in Lemma 4.1, namely, the fact that if R is a finite nonzero ring with multiplicative monoid S, then the minimal (semigroup-theoretic) prime ideals of S coincide with the (minimal ring-theoretic) prime ideals of R.

The proof of Theorem 4.2 depends on the decomposition [**10**, Theorem 3, p. 205] of any nonzero Artinian ring R as an internal direct product of finitely many, say k, local rings. One upshot, in Theorem 4.2 (d), is that if R is any nonzero finite ring, other than a field, with multiplicative monoid S and k is as above, then any application to S of the algorithm in Algorithm 2.5 that constructs minimal generating sets of S must terminate in exactly k steps. In particular, the process terminates in just one step if and only if the finite nonzero nonfield R is a local ring. Another application, in Theorem 4.2 (c), is that the internal direct product decomposition of any finite nonzero nonfield R determines much of the data in any application of the algorithm in Algorithm 2.5 to the multiplicative monoid of R. Theorem 4.2 (d) shows that some of that data need not be so determined, even if R is an SPIR.

To avoid confusion when considering both a ring R and its multiplicative monoid S, we refer to ideals or prime ideals or maximal ideals *of* S, respectively *of* R, to mean the corresponding semigroup- (respectively, ring-) theoretic concept. As to our other notational conventions, $\subset$ denotes proper inclusion. If n is a positive integer, then $[n] := \{1, \ldots, n\}$; and $[0] := \{0\}$. Also, if A is a ring, we let $\mathrm{Spec}\,(A)$ denote the set of prime ideals of A; $\mathrm{Max}\,(A)$ the set of maximal ideals of A; $\mathrm{Min}\,(A)$ the set of minimal ideals of A; and $U(A)$ the group of units of A. Any unexplained material is standard, as in [**5, 9, 10**].

2. Minimal prime ideals lead to minimal generating sets. All semigroups considered below are written multiplicatively. Rather than seeking maximum generality, we tailor the assertions in Lemmas 2.1–2.3 to facilitate the proofs of Theorems 2.5 and 3.3 and the ring-theoretic applications in Corollary 2.6 and Theorem 4.2.

We recall some semigroup-theoretic notation and terminology, cf. [**5**, pp. 2, 3], [**9**, pp. 91, 138]. Let S be a (commutative) semigroup. If H, K are nonempty subsets of S, then $HK := \{g \in S \mid \text{there exist } h \in H,\ k \in K \text{ such that } g = hk\}$; $H^2 := HH$; and if $h \in H$, then $hK := \{h\}K$. A nonempty subset H of S is said to be an *ideal of* S if $SH \subseteq H$; and a *proper ideal of* S if H is an ideal of S such that $H \subset S$. A proper ideal H of S is said to be a *prime ideal of* S if $x, y \in S,\ xy \in H$ implies that either $x \in H$ or $y \in H$, i.e., if $S \setminus H$ is a subsemigroup of S; and a *maximal ideal of* S in case no ideal K of S satisfies $H \subset K \subset S$.

Lemma 2.1 shows that in discussing the notions of "prime ideal" and "maximal ideal," we must specify whether we are working in the ring-theoretic or the semigroup-theoretic context. Lemmas 2.2 and 2.3 then give useful semigroup-theoretic analogues of the facts that $\operatorname{Max}(R) \subseteq \operatorname{Spec}(R)$ for any ring R, with the reverse inclusion holding if R is finite.

Lemma 2.1. *Let R be a ring and H a subset of R. Let S denote the multiplicative monoid of R. Then*:

(a) *If $H \in \operatorname{Spec}(R)$, then H is a prime ideal of S.*

(b) *If H is a prime ideal of S, then it need not be the case that $H \in \operatorname{Spec}(R)$.*

(c) *If $H \in \operatorname{Max}(R)$, then it need not be the case that H is a maximal ideal of S.*

(d) *If H is a maximal ideal of S, then it need not be the case that $H \in \operatorname{Max}(R)$.*

Proof. (a) $H \in \operatorname{Spec}(R) \Rightarrow K := R \setminus H$ is a multiplicatively closed subset of R that contains $1 \Rightarrow K$ is a submonoid of $S \Rightarrow H$ is a prime ideal of S.

(b) Consider $R := \mathbf{Z}$, and let $H := 2\mathbf{Z} \cup 3\mathbf{Z}$. Then H is a prime ideal of S, but $H \notin \mathrm{Spec}\,(R)$ since H is not closed under addition.

(c) Consider $R := \mathbf{Z}$, and let $H := 2\mathbf{Z}$. Of course, $H \in \mathrm{Max}\,(R)$. However, H is not a maximal ideal of S since $K := 2\mathbf{Z} \cup 3\mathbf{Z}$ is an ideal of S such that $H \subset K \subset S$.

(d) Consider $R := \mathbf{Z}$, and let $H := \mathbf{Z} \setminus \{1, -1\}$. Then H is a maximal ideal of S, since H is the set of all the nonunits of R, but $H \notin \mathrm{Max}\,(R)$ since $H + H \not\subseteq H$. □

The reasoning in the proof of Lemma 2.1 (d) applies if R is any nonzero nonlocal ring and H is the set of nonunits of R. In such an example, R can be taken finite. When combined with Lemma 2.1 (a), the assertions in Lemma 2.2 (b) imply that any finite nonzero nonlocal ring illustrates the phenomena in parts (b), (c) and (d) of Lemma 2.1.

If S is a (commutative) monoid, let $U(S) := \{x \in S \mid \text{there exists } y \in S \text{ such that } xy = 1\}$, the group of invertible elements of S. This terminology follows usage in [**5**, p. 4], rather than the contemporary ring-theoretic usage of "units," in view of the different meaning accorded to the word "unit" in some of the literature on semigroups, cf. [**9**, item 2.6].

Lemma 2.2. (a) *Let S be a commutative semigroup such that $S^2 = S$ (for instance, a commutative monoid). If H is a maximal ideal of S, then H is a prime ideal of S.*

(b) *Let S be a commutative monoid consisting of more than one element and suppose that S contains a (uniquely determined) element 0 such that $0S = \{0\}$. Then S has a unique maximal ideal, namely, $S \setminus U(S)$, the set of all the noninvertible elements of S.*

Proof. (a) Since H is a maximal ideal of S, H is a proper ideal of S. It suffices to show that if $x, y \in S$ satisfy $xy \in H$, then either $x \in H$ or $y \in H$. Suppose not. Since $x \notin H$ and H is a maximal ideal of S, the ideal of S generated by $H \cup \{x\}$ is all of S; that is, $H \cup \{x\} \cup (H \cup \{x\})S = S$, cf. [**5**, p. 3]. As $HS \subseteq H$, it follows that $H \cup \{x\} \cup xS = S$. Similarly, $H \cup \{y\} \cup yS = S$. Then

$$S = S^2 = (H \cup \{x\} \cup xS)(H \cup \{y\} \cup yS).$$

Since $SH = HS \subseteq H$ and $xy \in H$, we have the (desired) contradiction:

$$S \subseteq H^2 \cup yH \cup ySH \cup xH \cup \{xy\} \cup xyS \cup xSH \cup xyS \cup xyS^2 \subseteq H \subset S.$$

(b) Any factor of an invertible element is an invertible element; and 1 is invertible. It follows that $S \setminus U(S)$ is a proper ideal of S. It suffices to show that this ideal contains each proper ideal H of S. Suppose not, and choose $h \in H \cap (S \setminus (S \setminus U(S))) = H \cap U(S)$. Then $S = h^{-1}hS \subseteq SHS = H \subset S$. This (desired) contradiction completes the proof of (b). □

Lemma 2.3. *Let (R, M) be a finite local ring and S the multiplicative monoid of R. Then*:

(a) *M is the only prime ideal of S.*

(b) *M is the only maximal ideal of S.*

(c) *A subset H of S is a prime ideal of S if and only if H is a maximal ideal of S.*

Proof. Note that $0S = \{0\} \neq S$. By Lemma 2.2 (b), S has a unique maximal ideal, $S\setminus U(S) = R\setminus U(R) = M$, proving (b). Also, by Lemma 2.2 (a), M is a prime ideal of S.

Next, note, as in the proof of Lemma 2.2 (b), that no proper ideal of S can contain an element of $U(S)$. Thus, if H is any prime ideal of S, then $H \subseteq S \setminus U(S)$. To complete the proof, it suffices to establish the reverse inclusion.

Define a binary relation $\sim$ on S via: if $s_1, s_2 \in S$, then $s_1 \sim s_2$ if and only if $H + s_1 = H + s_2$. (If $s \in S$ and $V \subseteq S$, then $V + s := \{x \in S \mid$ there exists $v \in V$ such that $x = v + s\}$.) Clearly, $\sim$ is an equivalence relation on S. For each $s \in S$, let $[s]$ denote the $\sim$-equivalence class of s; put $T := \{[s] \mid s \in S\}$, the set of all the $\sim$-equivalence classes.

If the prime ideal H is not a maximal ideal of S, the above claim allows us to choose $m \in M \setminus H$. Define a function $f : T \to T$ by $f([s]) = [sm]$ for each $s \in S$. To show that f is well-defined, we prove that if $s_1, s_2 \in S$ satisfy $H+s_1 = H+s_2$, then $H+s_1m = H+s_2m$. We next take advantage of the fact that each element of S has an additive inverse in S. In fact, by considering $s := s_1 - s_2$, we see that it is

enough to prove that if $s \in S$ satisfies $H + s = H$, then $H + sm = H$. Since $m - 1 \in U(R)$ and H is an ideal of S, we have $H = H(m-1)$. It follows that f is a well-defined function, since

$$\begin{aligned} H + sm &= H(m-1) + s(m-1) + s = (H+s)(m-1) + s \\ &= H(m-1) + s = H + s = H. \end{aligned}$$

In fact, f is an injection. To see this, our task is to show that if $s_1, s_2 \in S$ satisfy $H + s_1 m = H + s_2 m$, then $H + s_1 = H + s_2$. By considering $s := s_1 - s_2$, we see that it is enough to prove that if $s \in S$ satisfies $H + sm = H$, then $H + s = H$. Since $h \mapsto h + s$ establishes a bijection $H \to H + s$ and H is finite, it follows from the pigeonhole principle that we need only prove that $H + s \subseteq H$. Observe that $(H+s)m \subseteq Hm + sm \subseteq H + sm = H$. Since H is a prime ideal of S and $m \in S \setminus H$, it follows that $H + s \subseteq H$, as desired.

By the pigeonhole principle, f is a bijection. In particular, there exists $y \in S$ such that $f([y]) = [1]$. In other words, $ym \sim 1$; that is, $H + ym = H + 1$. As $0 \in 0H \subseteq SH = H$, it follows that $1 \in H + ym \subseteq M + M = M$. This (desired) contradiction completes the proof. □

We pause to isolate a limiting case of the situation that is to be treated in Algorithm 2.5.

Proposition 2.4. *Let S be a commutative monoid consisting of more than one element and suppose that S contains an (uniquely determined) element 0 such that $0S = \{0\}$. Then $\{0\}$ is a (the) maximal ideal of S if and only if there exists a group G such that S is the (necessarily disjoint) union of $\{0\}$ and G.*

Proof. If $\{0\}$ is a maximal ideal of S, then by Lemma 2.2 (b), $\{0\} = S \setminus U(S)$, whence $G := S \setminus \{0\} = U(S)$, a group. Clearly, S is the disjoint union of $\{0\}$ and G.

Conversely, suppose that S is the union of $\{0\}$ and some group G. Then this a disjoint union, for otherwise, $0 \in S = G$ and $S = 1S = 0^{-1}0S = 0^{-1}\{0\} = \{0\}$, contrary to hypothesis. Moreover, as in the proofs of Lemmas 2.2 (b) and 2.3, no proper ideal H of S can

contain an invertible element of S, whence $H \subseteq S \setminus G = \{0\}$. As the hypotheses ensure that $\{0\}$ is a proper ideal of S, it follows that $\{0\}$ is the maximal ideal of S. □

If $S, 0$ and G satisfy the equivalent conditions in the statement of Proposition 2.4, the typical minimal generating set of S is of the form $\{0\} \cup W$, where W is a minimal generating set of G as a monoid. Since each element in a finite group has finite order, it follows that if S is finite and contains more than one element, then the typical minimal generating set of S is of the form $\{0\} \cup W$, where W is a minimal generating set of G as a group. Note also that if R is a finite nonzero ring, then the multiplicative monoid S of R satisfies the equivalent conditions in the statement of Proposition 2.4 if and only if R is a finite field. The comments in this paragraph are generalized in Algorithm 2.5 (e) and Corollary 2.6.

Henceforth, if H is a nonempty subset of a semigroup S, we let $\langle H \rangle$ denote the subsemigroup of S generated by H. We next present our first main result.

Algorithm 2.5. *Let S be a commutative nontrivial finite semigroup with zero. Suppose that $\{0\}$ is not a maximal ideal of S. Put $S_0 := S$. Choose P_1 to be a minimal prime ideal of S_0; consider the monoid $S_1 := S_0 \setminus P_1$. Choose B_1 to be minimal among nonempty subsets of P_1 such that $\langle B_1 S_1 \rangle = P_1$. If S_1 is not a group, choose P_2 to be a minimal prime ideal of S_1, and consider the monoid $S_2 := S_1 \setminus P_2$. Choose B_2 to be minimal among nonempty subsets of P_2 such that $\langle B_2 S_2 \rangle = P_2$. Iterate, so that if $i \geq 1$ and S_i is not a group, then P_{i+1} is chosen to be a minimal prime ideal of S_i, the monoid $S_{i+1} := S_i \setminus P_{i+1}$, and B_{i+1} is chosen to be minimal among nonempty subsets of P_{i+1} such that $\langle B_{i+1} S_{i+1} \rangle = P_{i+1}$. Then*:

(a) *For any choice of the P_i and B_i as above, the process terminates*; *that is, there exists a positive integer n such that S_n is a group and, in fact, $S_n = U(S)$.*

(b) *If $1 \leq i \leq j \leq n$ (where n is as in* (a)*), then $P_i P_j \subseteq P_i$ and $P_i S_n = P_i$.*

(c) *If* $1 \leq i \leq n$ (*where* n *is as in* (a)), *then* S *can be expressed as the disjoint union* $S = Q_i \cup S_i$, *where* $Q_i := \cup\{P_j \mid 1 \leq j \leq i\}$ *is a prime ideal of* S.

(d) *If* n *is as in (a), then* $S \setminus U(S)$, *the set of noninvertible elements of* S, *is the prime ideal* (*indeed, the unique maximal ideal*) Q_n *that can be described as the disjoint union* $Q_n := \cup\{P_j \mid 1 \leq j \leq n\}$.

(e) *If* n *is as in* (a) *and* B *is any minimal generating set of* $U(S)$ *as a semigroup* (*respectively, as a group if* $U(S) \neq \{1\}$), *then* $\bigcup\{B_i \mid 1 \leq i \leq n\} \cup B$ *is a minimal generating set of* S.

Proof. (a) Since S is finite, each proper ideal (in particular, each prime ideal) of S is contained in a (the) maximal ideal of S. Therefore, by Lemma 2.2, we can choose a minimal prime ideal P_1 of S. Since P_1 is a prime ideal of S, $S_1 := S_0 \setminus P_1$ is a subsemigroup of S. As $1 \notin P_1$, it follows that S_1 is a monoid. Consequently, $\langle P_1 S_1 \rangle = P_1$, and so since P_1 is finite, we can choose a minimal nonempty subset B_1 of P_1 such that $\langle B_1 S_1 \rangle = P_1$.

If S_1 is not a group, then S_1 has a proper ideal cf. [**9**, item 1.8, p. 142], [**5**, Theorem 1.1 (1)], hence a maximal ideal, hence a prime ideal, by Lemma 2.2 (a), hence a minimal prime ideal (since S_1 is finite). Choose P_2 to be a minimal prime ideal of S_1. Since P_2 is prime, reasoning as above shows that $S_2 := S_1 \setminus P_2$ is a monoid. For much the same reason that B_1 existed, we can choose B_2 to be minimal among the nonempty subsets of P_2 such that $\langle B_2 S_2 \rangle = P_2$. Iterating leads to sequences $\{S_i\}, \{P_i\}$ and $\{B_i\}$ as in the assertion.

It is easy to prove by mathematical induction on i that $Q_i := \cup\{P_j \mid 1 \leq j \leq i\}$ is expressed as a disjoint union; and that $S = Q_i \cup S_i$ is also a disjoint union. In particular, $\{Q_i\}$ is a strictly increasing sequence of subsets of the finite set S. Therefore, this sequence is finite (as are the other sequences noted above); that is, the process terminates, as asserted.

(b) The first assertion follows since $P_i P_j \subseteq P_i S_{j-1} \subseteq P_i S_{i-1} = P_i$. (In detail, the first inclusion holds because P_j is an ideal of S_{j-1}; the second inclusion holds because $S_{j-1} \subseteq S_{i-1}$; and the equality holds because P_i is an ideal of the monoid S_{i-1}.) In addition, the assertion that $P_i S_n = P_i$ follows from the facts that P_i is an ideal of S_{i-1}, $S_n \subseteq S_{i-1}$, and $1 \in S_n$.

(c) It follows from the comments in the final paragraph of the proof of (a) that $S = Q_n \cup S_n$. Therefore, (b), together with the definition of the Q_j, yields that each Q_i is an ideal of S. It remains only to show that each Q_i is a prime ideal of S. We proceed by mathematical induction on i. The induction basis is clear, for $Q_1 = P_1$ was chosen to be a certain kind of prime ideal of $S_0 = S$. Suppose inductively that Q_{i-1} is a prime ideal of S, for some $i \geq 2$. If the assertion fails, there exist $x, y \in S \setminus Q_i = S_i$ such that $xy \in Q_i$. By the inductive hypothesis, we may suppose that $xy \in Q_i \setminus Q_{i-1} = P_i$. As P_i is a prime ideal of S_{i-1}, we may assume without loss of generality that $x \in S \setminus S_{i-1} = Q_{i-1}$. But then $xy \in Q_{i-1}S \subseteq Q_{i-1}$. This (desired) contradiction completes the induction step and finishes the proof of (c).

(d) It was shown in the proof of (a) that $Q_n := \cup\{P_j \mid 1 \leq j \leq n\}$ is a disjoint union. Moreover, by (c), Q_n is a prime ideal of S. In addition, by (a) and (c), $S \setminus U(S) = S \setminus S_n = Q_n$. Finally, the parenthetical assertion is now a consequence of Lemma 3.2 (b).

(e) We begin by noting two facts that will be important later in the proof. The first of these, which follows easily from the definitions of the P_j and the S_j, states that if $0 \leq i \leq n-1$, then we have $S_i = \cup\{P_j \mid i+1 \leq j \leq n\} \cup S_n$, expressed as a disjoint union.

Second, by (a) and the choice of B, we have that $\langle B \rangle = S_n = U(S)$. Indeed, if $U(S) \neq \{1\}$, there is no difference in considering the generation of $U(S)$ by B as a semigroup or as a group, since every element of $U(S)$ has finite order.

Next, we claim $P_i \subseteq \langle \cup\{B_j \mid i \leq j \leq n\} \cup B \rangle$ for all $i = 1, \ldots, n$. This will be proved by decreasing induction on i. The case $i = n$ is clear, for $P_n = \langle B_n S_n \rangle \subseteq \langle B_n \cup S_n \rangle = \langle B_n \cup B \rangle$, the final step following from the second fact noted above. For the induction step, suppose that $1 \leq i \leq n-1$ and $\cup\{P_j \mid i+1 \leq j \leq n\} \cup S_n \subseteq \langle \cup\{B_j \mid i+1 \leq j \leq n\} \cup B \rangle$. Then, by the first fact noted above and the induction hypothesis, $P_i = \langle B_i S_i \rangle \subseteq \langle B_i \cup S_i \rangle = \langle B_i \cup \cup\{P_j \mid i+1 \leq j \leq n\} \cup S_n \} \rangle \subseteq \langle \cup\{B_j \mid i \leq j \leq n\} \cup B \rangle$. This completes the induction step and finishes the proof of the above claim. By (c),

$$S = Q_n \cup S_n = \bigcup\{P_j \mid 1 \leq j \leq n\} \cup S_n \subseteq \left\langle \bigcup\{B_j \mid 1 \leq j \leq n\} \cup B \right\rangle.$$

As the reverse inclusion is trivial, it follows that $\mathcal{T} := \cup\{B_i \mid 1 \leq i \leq n\} \cup B$ is a generating set of S. It remains only to prove the minimality of $\mathcal{T}$ as a generating set of S.

If the assertion fails, choose $x \in \mathcal{T}$ such that $\langle \mathcal{T} \setminus \{x\} \rangle = S$. There are two cases. Suppose first that $x \in B$. By the choice of B, we have that $x \notin \langle B \setminus \{x\} \rangle$. However, it follows from (c) and (d) that no element of S_n can be expressed as a product of elements in $\mathcal{T}$ at least one of whose factors lies in Q_n. Thus, $x \notin \langle \mathcal{T} \setminus \{x\} \rangle$, the desired contradiction.

If $x \in \mathcal{T} \setminus B = \cup\{B_j \mid 1 \leq j \leq n\}$, there exists $i, 1 \leq i \leq n$, such that $x \in B_i \subseteq P_i$. As $B_{i+1}, B_{i+2}, \ldots, B_n, S_n \subseteq S_i$, it follows from (b), (c), and the first fact noted above that

$$P_i = P_i \cap \langle \mathcal{T} \setminus \{x\} \rangle \subseteq \langle ((\mathcal{T} \setminus \{x\}) \cap B_i) \cdot S_i \rangle = \langle (B_i \setminus \{x\}) \cdot S_i \rangle.$$

However, it is clear that $\langle (B_i \setminus \{x\}) \cdot S_i \rangle \subseteq \langle B_i S_i \rangle = P_i$. Hence, $\langle (B_i \setminus \{x\}) \cdot S_i \rangle = P_i$, contradicting the minimality of B_i. This (desired) contradiction completes the proof. □

The most important application of Algorithm 2.5 arises for S the multiplicative monoid of a finite nonzero ring R that is not a field. For this context, Corollary 2.6 (a) establishes, i.e., that the case $n = 1$ of Algorithm 2.5 corresponds to R being local.

Corollary 2.6. *Let R be a finite nonzero ring which is not a field, and let S be the multiplicative monoid of R. Then*:

a) *The following five conditions are equivalent*:

(1) *Each application of the algorithm in Algorithm* 2.5 *terminates at* $n = 1$;

(2) *Some application of the algorithm in Algorithm* 2.5 *terminates at* $n = 1$;

(3) *S has a unique nonzero prime ideal*;

(4) *S has a unique prime ideal*;

(5) *R is a local ring.*

(b) *If R is a local ring, for instance, an* SPIR*, then each minimal generating set of S can be obtained as an application of the algorithm in Algorithm* 2.5.

Proof. (a) Since R is not an integral domain, $\{0\} \notin \mathrm{Spec}\,(R)$. As $\{0\}$ is closed under addition, $\{0\}$ is not a prime ideal of S. Therefore, (4) $\Leftrightarrow$ (3). Moreover, (1) $\Rightarrow$ (2) because the beginning of the proof of Algorithm 2.5 (a) showed that the algorithm can be realized.

(2) $\Rightarrow$ (4). Assume (2). By Algorithm 2.5 (d), the set of noninvertible elements of S form a minimal (nonzero) prime ideal, say Q, of S. We show that if P is a prime ideal of S, then $P = Q$. In fact, P cannot contain any element $h \in U(S)$ (lest $S = h^{-1}hS \subseteq h^{-1}P = P \subset S$, a contradiction), whence $P \subseteq S \backslash U(S) = Q$ and $P = Q$ by the minimality of Q.

(4) $\Rightarrow$ (5). Apply Lemma 2.1 (a).

It now suffices to prove that (5) $\Rightarrow$ (1). Assume (5), with M denoting the unique maximal ideal of R. Since R is local, $R \backslash M = U(R) = U(S)$. By Lemma 2.3 (a), M is the only prime ideal of S. Thus, in any application of the algorithm in Algorithm 2.5, $P_1 = M$, whence $S_1 := S \setminus P_1 = R \setminus M = U(S)$ is a group and the algorithm terminates at $n = 1$.

(b) Any factor of an invertible element is invertible; and any product of invertible elements is invertible. Thus, the set B of the invertible elements in any given generating set V of S generates $U(S)$ as a semigroup; since $S \neq \{1\}$ and every element of $U(S)$ has finite order, this generation is actually as a group. As above, let M denote the maximal ideal of R, and now suppose that V is a minimal generating set of S. By (a) and the above comments, it suffices to observe that $B_1 := V \cap M$ is minimal with the property that $\langle B_1 U(S) \rangle = M$. □

Remark 2.7. The referee has suggested that it would be of interest to illustrate the algorithm in Algorithm 2.5 with an example at this point. We consider here the multiplicative monoid S of $R := \mathbf{Z}/6\mathbf{Z}$. (In Example 4.3 (a), the algorithm is illustrated for some monoids S that do not arise as multiplicative monoids of rings.) It turns out that 6 is the smallest n such that applications of the algorithm to the multiplicative monoid of $\mathbf{Z}/n\mathbf{Z}$ require (at least) two steps before terminating. In applying the algorithm to this example, one can choose P_1 to be either $\{0, 2, 4\}$ or $\{0, 3\}$. The first of these choices can be followed by choosing B_1 to be either $\{2\}$ or $\{4\}$; then $P_2 = \{3\}$, $B_2 = \{3\}$, $B = \{5\}$ and, in this way, one obtains the minimal

generating sets $\{2,3,5\}$ and $\{4,3,5\}$ of S. On the other hand, the choice $P_1 = \{0,3\}$ is followed by $B_1 = \{3\}$ and $P_2 = \{2,4\}$, with B_2 either $\{2\}$ or $\{4\}$, and $B = \{5\}$, and the algorithm thus produces the same two minimal generating sets as before, namely, $\{3,2,5\}$ and $\{3,4,5\}$, albeit with their elements permuted. For a more general explanation of this example, apply Theorem 4.2 (a)–(d) to the canonical isomorphism $\mathbf{Z}/6\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. The reader can check directly that in this example, S has exactly two minimal generating sets. Thus (in anticipation of Theorems 3.3 and 4.2 (a)), each such set has been obtained by a suitable application of the algorithm in Algorithm 2.5. The diligent reader can verify directly that the same conclusion holds if $R := \mathbf{Z}/30\mathbf{Z}$ and that 30 is the smallest value of n such that applications of the algorithm to the multiplicative monoid of $\mathbf{Z}/n\mathbf{Z}$ require (at least) three steps before terminating.

Corollary 2.6 left open the case of R a finite field, with multiplicative monoid S. In this case, one can apply the algorithm in Algorithm 2.5 with $P_1 := \{0\}$, with the result that such R and S then satisfy analogues of the assertions in Corollary 2.6. The details of these analogues were essentially given in the comments following the proof of Proposition 2.4.

Corollary 2.6 also left open the interpretation of the algorithm in Algorithm 2.5 in case $n > 1$, equivalently, if R is nonlocal. Theorem 4.2 settles such matters in general by relating the number of steps (n) in an application of that algorithm to the intrinsic structure of R as an Artinian ring. One may view Theorem 4.2 as a generalization of Corollary 2.6 (a). First, we devote Section 3 to proving the underlying semigroup-theoretic result, Theorem 3.3.

3. Minimal generating sets come from minimal prime ideals. The main result of this section, Theorem 3.3, is essentially the converse of Algorithm 2.5 (e). It is convenient now to set up the following *standing hypotheses and notation for Section* 3. S denotes a commutative finite nontrivial semigroup with zero. There are exactly m, semigroup-theoretic, prime ideals of S, and these are denoted $A_1, \ldots, A_m$. (Note that Lemma 2.2 (a) ensures that m is a positive integer.) W is a given minimal generating set of S. For each permutation σ on $[m]$, that is, for each permutation σ in the symmetric group on m letters, we have the following six sets of definitions:

1) $B := W \cap U(S)$.

(2) $\mathcal{P}_k := A_{\sigma(k)} \setminus \cup\{A_{\sigma(\mu)} \mid \mu < k\}$ for each $k \in [m]$.

(3) $\mathcal{S}_k := U(S) \cup \cup\{\mathcal{P}_\mu \mid \mu > k\}$ for each $k \in \{0\} \cup [m]$.

(4) $B^{(k)} := B \cup \cup\{W \cap \mathcal{P}_\mu \mid \mu > k\}$ for each $k \in [m]$.

(5) $V^{(k)} := W \setminus B^{(k)}$ for each $k \in [m]$.

(6) $\mathcal{B}_k := V^{(k)} \cap \mathcal{P}_k$ for each $k \in [m]$.

Each of the above definitions (2)–(6) depends on σ, which does not appear explicitly in the above notation. For instance, $\mathcal{P}_k$ should be understood as $\mathcal{P}_{\sigma,k}$. In view of context clues, we trust that the less cumbersome notation in (2)–(6) above will not lead to confusion.

Lemmas 3.1 and 3.2 establish some useful technical facts about the above-defined items. To prove Lemma 3.1, repeat the beginning of the proof of Corollary 2.6 (b).

Lemma 3.1. *Under the above standing hypotheses and notation, B is a minimal generating set of $U(S)$.*

Lemma 3.2. *Under the above standing hypotheses and notation, including the given permutation σ, one has the following conclusions for the above-defined items.*

(a) $\cup\{\mathcal{P}_k \mid 1 \leq k \leq \mu\} = \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu\}$ *for each* $\mu \in [m]$.

(b) $\mathcal{P}_k \cap \mathcal{P}_j = \varnothing$ if $k \neq j$.

(c) $\cup\{\mathcal{P}_k \mid i+1 \leq k \leq m\} = \cup\{A_{\sigma(k)} \mid 1 \leq k \leq m\} \setminus \cup\{A_{\sigma(k)} \mid 1 \leq k \leq i\}$ *for each* $i \in [m-1]$.

(d) $\mathcal{S}_0 = S$.

(e) $\mathcal{S}_m = U(S)$.

(f) $\mathcal{S}_k = S \setminus \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq k\}$ *is a monoid for each* $k \in [m]$.

(g) $\mathcal{S}_{k-1} = \mathcal{S}_k \cup \mathcal{P}_k$, *expressed as a disjoint union, for each* $k \in [m]$.

(h) *If $\mathcal{P}_k$ is nonempty, then it is a prime ideal of $\mathcal{S}_{k-1}$ for each* $k \in [m]$.

(i) *If $\mathcal{P}_k$ is nonempty, then* $\langle \mathcal{B}_k \mathcal{S}_k \rangle = \mathcal{P}_k$ *for each* $k \in [m]$.

(j) $W = V^{(k)} \cup B^{(k)}$, *expressed as a disjoint union, for each* $k \in [m]$.

(k) $\langle \mathcal{S}_k \cup (W \cap \mathcal{P}_k) \rangle = \mathcal{S}_{k-1}$ *for each* $k \in [m]$.

(l) $\langle B^{(k)} \rangle = \mathcal{S}_k$ *for each* $k \in [m]$.

(m) $\mathcal{B}_k \cap \mathcal{B}_j = \varnothing$ if $k \neq j$.

(n) $\cup\{\mathcal{B}_k \mid 1 \leq k \leq m\} = W \setminus B$ *and* $\cup\{B_i \mid 1 \leq i \leq m\} \cup B = W$.

Proof. (a) Induct on μ. The induction basis (the case $\mu = 1$) follows easily from (2) above, since a union indexed by the empty set is empty. For the induction step, suppose that $\cup\{\mathcal{P}_k \mid 1 \leq k \leq \mu\} = \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu\}$, and observe that $\cup\{\mathcal{P}_k \mid 1 \leq k \leq \mu+1\} = \mathcal{P}_{\mu+1} \cup \cup\{\mathcal{P}_k \mid 1 \leq k \leq \mu\} = \mathcal{P}_{\mu+1} \cup \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu\} = (A_{\sigma(\mu+1)} \setminus \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu\}) \cup \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu\} = \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu+1\}$.

(b) Without loss of generality, $\mathcal{P}_k$ and $\mathcal{P}_j$ are each nonempty and $j < k$. Using (2), observe that $\mathcal{P}_k \cap \mathcal{P}_j = (A_{\sigma(k)} \setminus \cup\{A_{\sigma(\mu)} \mid \mu < k\}) \cap (A_{\sigma(j)} \setminus \cup\{A_{\sigma(\mu)} \mid \mu < j\}) \subseteq (A_{\sigma(k)} \setminus \cup\{A_{\sigma(\mu)} \mid \mu < k\}) \cap A_{\sigma(j)} = \varnothing$. The assertion follows.

(c) The assertion follows directly from (a) and (b).

(d) In view of (3) with $k := 0$, we need only show that each nonunit x of S lies in some $\mathcal{P}_\mu$. Thus, by (a), it suffices to show that x lies in some A_j. This, in turn, follows from the consequence of parts (b) and (a) of Lemma 2.2 that $S \setminus U(S)$ is a prime ideal of S.

(e) Apply (3) with $k := m$ and the convention about unions indexed by the empty set.

(f) By (3), (c) and the proof of (d), $\mathcal{S}_k := U(S) \cup \cup\{\mathcal{P}_\mu \mid k+1 \leq \mu \leq m\} = U(S) \cup (\cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq m\} \setminus \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq k\}) = (U(S) \cup \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq m\}) \setminus \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq k\} = S \setminus \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq k\}$. The assertion follows, as $1 \in \mathcal{S}_k$ and the complement in S of any union of prime ideals of S is closed under multiplication.

(g) The definitions of $\mathcal{S}_k$ and $\mathcal{S}_{k-1}$ in (3) easily lead to the fact that $\mathcal{S}_{k-1} = \mathcal{S}_k \cup \mathcal{P}_k$. To see that $\mathcal{P}_k$ is disjoint from $\mathcal{S}_k$, combine (3) and (2).

(h) By (g), $\mathcal{P}_k \subseteq \mathcal{S}_{k-1}$. Suppose $\mathcal{P}_k$ is nonempty. By combining (2), (3) and (b), one verifies that $\mathcal{P}_k$ is an ideal of $\mathcal{S}_{k-1}$. Also, it follows from (f) and (g) that a product of two elements of $\mathcal{S}_k$ cannot lie in $\mathcal{P}_k$, and so it follows from (g) that $\mathcal{P}_k$ is a prime ideal of $\mathcal{S}_{k-1}$.

(i) By (a) and (b), it follows from (5) and (1) that $V^{(k)} = W \cap \bigcup\{\mathcal{P}_\mu \mid 1 \leq \mu \leq k\}$. Hence, by (b), $\mathcal{B}_k = W \cap \mathcal{P}_k$. Moreover, $\mathcal{S}_k \subseteq \mathcal{S}_{k-1}$, by (g). Then (h) ensures that $\langle \mathcal{B}_k \mathcal{S}_k \rangle \subseteq \mathcal{P}_k$. It remains only to prove the reverse inclusion.

Note that if $x, y \in S \setminus U(S)$ are such that $xy \in \mathcal{P}_k$, then both x and y belong to $\mathcal{S}_{k-1}$. (Otherwise, either x or y would be in $\cup\{\mathcal{P}_\mu \mid 1 \leq \mu \leq k-1\}$ and, hence by (a), in $A_{\sigma(j)}$ for some $j < k$, a contradiction to (2) since $A_{\sigma(j)}$ is an ideal of S.) Hence, by (h) and (g), at least one of x, y is in $\mathcal{P}_k$, while the other is in either $\mathcal{P}_k$ or $\mathcal{S}_{k-1} \setminus \mathcal{P}_k = \mathcal{S}_k$. Now, by the hypothesis on W, each element of $\mathcal{P}_k$ is either in W or is a product of elements of W. As we saw above that $W \cap \mathcal{P}_k = \mathcal{B}_k$, it now follows easily that $\mathcal{P}_k \subseteq \langle \mathcal{B}_k \mathcal{S}_k \rangle$, as required.

(j) By (4) and (1), $B^{(k)} \subseteq W$. The assertion now follows from (5).

(k) If $\mathcal{P}_k$ is empty, the assertion is immediate from (g), (f) and (d). Assume henceforth that $\mathcal{P}_k$ is nonempty. Then, by (j) and (6), $\langle \mathcal{S}_k \cup (W \cap \mathcal{P}_k) \rangle = \langle \mathcal{S}_k \cup \mathcal{B}_k \cup (B^{(k)} \cap \mathcal{P}_k) \rangle = \langle \mathcal{S}_k \cup \mathcal{B}_k \mathcal{S}_k \cup (B^{(k)} \cap \mathcal{P}_k) \rangle$. By (i), this simplifies to $\langle \mathcal{S}_k \cup \mathcal{P}_k \rangle$; and by (g), (f) and (d), this is just $\langle \mathcal{S}_{k-1} \rangle = \mathcal{S}_{k-1}$.

(l) By (4), Lemma 3.1 and (e), $\langle B^{(k)} \rangle = \langle \langle B \rangle \cup \cup\{W \cap \mathcal{P}_\mu \mid \mu > k\} \rangle = \langle U(S) \cup \cup\{W \cap \mathcal{P}_\mu \mid \mu > k\} \rangle = \langle \mathcal{S}_m \cup \cup\{W \cap \mathcal{P}_\mu \mid k+1 \leq \mu \leq m\} \rangle = \langle \mathcal{S}_m \cup (W \cap \mathcal{P}_m) \cup \cup\{W \cap \mathcal{P}_\mu \mid k+1 \leq \mu \leq m-1\} \rangle$. By (k), this simplifies to $\langle \mathcal{S}_{m-1} \cup \cup\{W \cap \mathcal{P}_\mu \mid k+1 \leq \mu \leq m-1\} \rangle$. By iterating the argument, we further simplify this expression to $\langle \mathcal{S}_{m-2} \cup \cup\{W \cap \mathcal{P}_\mu \mid k+1 \leq \mu \leq m-2\} \rangle = \cdots = \langle \mathcal{S}_{k+1} \cup (W \cap \mathcal{P}_{k+1}) \rangle$, which, by (k), is just $\langle \mathcal{S}_k \rangle = \mathcal{S}_k$.

(m) By (6) and (b), $\mathcal{B}_k \cap \mathcal{B}_j = V^{(k)} \cap V^{(j)} \cap \mathcal{P}_k \cap \mathcal{P}_j = V^{(k)} \cap V^{(j)} \cap \varnothing = \varnothing$.

(n) It suffices to prove the first assertion. It was shown in the proof of (i) that $\mathcal{B}_k = W \cap \mathcal{P}_k$ if $\mathcal{P}_k$ is nonempty; and it is clear from (6) that this equation also holds if $\mathcal{P}_k$ is empty. Also, by (3) and (d), $\cup\{\mathcal{P}_k \mid 1 \leq k \leq m\} = \mathcal{S}_0 \setminus U(S) = S \setminus U(S)$. Therefore, $\cup\{\mathcal{B}_k \mid 1 \leq k \leq m\} = W \cap (\cup\{\mathcal{P}_k \mid 1 \leq k \leq m\}) = W \cap (S \setminus U(S)) = W \setminus (W \cap U(S)) = W \setminus B$. □

Theorem 3.3. *Under the above standing hypotheses and notation, W can be obtained as in Algorithm* 2.5 (e)*. In other words, there exists an application of the algorithm in Algorithm* 2.5 *to S so that, in the notation of Algorithm* 2.5*, $W = \cup\{B_i \mid 1 \leq i \leq n\} \cup B$.*

Proof. It suffices to show that there exists a permutation σ on $[m]$ such that for each k for which $\mathcal{P}_k$ is nonempty, we have that $\mathcal{P}_k$ is a minimal prime ideal of $\mathcal{S}_{k-1}$ and $\mathcal{B}_k$ is minimal among the nonempty subsets of $\mathcal{P}_k$ such that $\langle \mathcal{B}_k \mathcal{S}_k \rangle = \mathcal{P}_k$. Indeed, given such a permutation σ, let $k_1 < \cdots < k_j$ denote the indexes of the nonempty $\mathcal{P}_k$'s. (In the notation developed below, $j = m - \eta(\sigma)$.) Then, by defining $P_i := \mathcal{P}_{k_i}$, $S_i := \mathcal{S}_{k_i}$ and $B_i := \mathcal{B}_{k_i}$, we obtain sequences of P_i's, S_i's and B_i's behaving as described in Algorithm 2.5, as desired.

First, we claim that for each permutation σ on $[m]$, if $\mathcal{P}_k$ is nonempty for some k, then we have that $\mathcal{B}_k$ is minimal such that $\langle \mathcal{B}_k \mathcal{S}_k \rangle = \mathcal{P}_k$. (Note that it was shown implicitly in the proof of Lemma 3.2 (i) that $\mathcal{B}_k$ is nonempty whenever $\mathcal{P}_k$ is nonempty.) In view of Lemma 3.2 (i), only the "minimality" assertion remains at issue.

Suppose that the above claim fails. Then, for some permutation σ on $[m]$ and some k such that $\mathcal{P}_k$ is nonempty, there exists a proper nonempty subset $\mathcal{B}' \subset \mathcal{B}_k$ such that $\langle \mathcal{B}' \mathcal{S}_k \rangle = \mathcal{P}_k$. It follows from Lemma 3.2 (j) that $W' := (V^{(k)} \setminus \mathcal{B}_k) \cup \mathcal{B}' \cup B^{(k)}$ is a proper subset of W. However, using parts (l), (f) and (j) of Lemma 3.2, we find that $\langle W' \rangle = \langle (V^{(k)} \setminus \mathcal{B}_k) \cup \mathcal{B}' \cup \mathcal{S}_k \rangle = \langle (V^{(k)} \setminus \mathcal{B}_k) \cup \mathcal{B}' \mathcal{S}_k \cup \mathcal{S}_k \rangle = \langle (V^{(k)} \setminus \mathcal{B}_k) \cup \mathcal{B}_k \mathcal{S}_k \cup \mathcal{S}_k \rangle = \langle (V^{(k)} \setminus \mathcal{B}_k) \cup \mathcal{B}_k \cup \mathcal{S}_k \rangle = \langle (V^{(k)} \setminus \mathcal{B}_k) \cup \mathcal{B}_k \cup B^{(k)} \rangle = \langle V^{(k)} \cup B^{(k)} \rangle = \langle W \rangle = S$. This contradicts the supposed minimality of W, and so the above claim has been proved.

It remains only to show that there is a permutation σ on $[m]$ such that each nonempty $\mathcal{P}_k$ is a minimal prime ideal of $\mathcal{S}_{k-1}$. For each permutation σ on $[m]$, let $\eta(\sigma)$ denote the number of indexes k for which $\mathcal{P}_k$ is empty, in the sequence determined by σ. We claim that if the permutation σ is chosen such that $\eta(\sigma)$ is minimal, then each nonempty $\mathcal{P}_k$, arising from σ, must be a minimal prime ideal of $\mathcal{S}_{k-1}$.

Suppose, on the contrary, that despite $\eta(\sigma)$ being minimal, we can find an index i such that $\mathcal{P}_i$ is nonempty but not minimal as a prime ideal of $\mathcal{S}_{i-1}$. Since S is finite, we can choose a minimal prime ideal $\mathcal{P}'$ of $\mathcal{S}_{i-1}$ such that $\mathcal{P}' \subset \mathcal{P}_i$. It follows from (2) that

$\mathcal{D} := \mathcal{P}' \cup \ \cup \{A_{\sigma(\mu)} \mid 1 \leq \mu \leq i-1\}$ is expressed as a disjoint union, and it is easy to use Lemma 3.2 (f) to verify that $\mathcal{D}$ is a prime ideal of S. Therefore, $\mathcal{D} = A_{\sigma(j)}$ for some index j.

If $j < i$, then parts (a) and (b) of Lemma 3.2 would lead to a contradiction to the fact that $\varnothing \neq \mathcal{P}' \subseteq \mathcal{P}_i$. Also, if $j = i$, then it follows from (2) and the definition of $\mathcal{D}$ that $\mathcal{P}_i = \mathcal{D} \setminus \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq i-1\} = \mathcal{P}'$, contradicting the choice of $\mathcal{P}'$. Therefore, $j > i$. However, since Lemma 3.2 (a) and the definition of $\mathcal{D}$ ensure that $A_{\sigma(j)} \subseteq \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq i\}$, we see that $\mathcal{P}_j = A_{\sigma(j)} \setminus \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq j-1\} = \varnothing$. In particular, there exists an index k such that $k > i$ and $\mathcal{P}_k$ is empty.

Define a permutation τ on $[m]$ as follows:

$$\tau(\mu) = \begin{cases} \sigma(\mu) & \text{if } 1 \leq \mu < i \\ \sigma(j) & \text{if } \mu = i \\ \sigma(\mu - 1) & \text{if } i < \mu \leq j \\ \sigma(\mu) & \text{if } j < \mu \leq m. \end{cases}$$

Then, with $\mathcal{P}_\mu$ continuing to denote $\mathcal{P}_{\sigma,\mu}$ as above, we claim that

$$\mathcal{P}_{\tau,\mu} = \begin{cases} \mathcal{P}_\mu & \text{if } 1 \leq \mu < i \\ \mathcal{P}' & \text{if } \mu = i \\ \mathcal{P}_i \setminus \mathcal{P}' & \text{if } \mu = i+1 \\ \mathcal{P}_{\mu-1} & \text{if } i+1 < \mu \leq j \\ \mathcal{P}_\mu & \text{if } j < \mu \leq m. \end{cases}$$

Some of the five values that were just claimed may be verified without too much difficulty. For instance, if $1 \leq \mu < i$, then it follows from (2) and the definition of τ that $\mathcal{P}_{\tau,\mu} = A_{\tau(\mu)} \setminus \cup\{A_{\tau(k)} \mid k < \mu\} = A_{\sigma(\mu)} \setminus \cup\{A_{\sigma(k)} \mid k < \mu\} = \mathcal{P}_\mu$. Similarly, for the case $\mu = i$, we have $\mathcal{P}_{\tau,i} = A_{\sigma(j)} \setminus \cup\{A_{\tau(k)} \mid k < i\} = \mathcal{D} \setminus \cup\{A_{\sigma(k)} \mid k < i\} = \mathcal{P}'$. Moreover, using similar reasoning, it is routine to verify that if $j < \mu \leq m$, then $\mathcal{P}_{\tau,\mu} = \mathcal{P}_\mu$.

The verifications in the two remaining cases are more intricate. Consider first the case $\mu = i+1$. Then $\mathcal{P}_{\tau,i+1} = A_{\sigma(i)} \setminus (A_{\sigma(j)} \cup \cup\{A_{\sigma(k)} \mid k \leq i-1\}) = A_{\sigma(i)} \setminus \mathcal{D} = (A_{\sigma(i)} \setminus \mathcal{P}') \cap \mathcal{P}_i = \mathcal{P}_i \setminus \mathcal{P}'$. Finally, we consider the case whose analysis is the most difficult, $i+1 < \mu \leq j$.

Then, by reasoning as above with (2) and the definition of τ, we find that $\mathcal{P}_{\tau,\mu} = A_{\sigma(\mu-1)} \setminus (A_{\sigma(j)} \cup \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu - 2\})$. On the other hand, $\mathcal{P}_{\mu-1} = A_{\sigma(\mu-1)} \setminus \cup\{A_{\sigma(k)} \mid 1 \leq k \leq \mu - 2\}$. Therefore, to prove the claim that $\mathcal{P}_{\tau,\mu} = \mathcal{P}_{\mu-1}$, it suffices to prove that $\mathcal{P}_{\mu-1}$ is disjoint from $A_{\sigma(j)}$. This, in turn, follows easily from parts (a) and (b) of Lemma 3.2, when taken in conjunction with the above-proved fact that $A_{\sigma(j)} \subseteq \cup\{A_{\sigma(\mu)} \mid 1 \leq \mu \leq i\}$. This completes the proof of all the cases in the above claim regarding the values of $\mathcal{P}_{\tau,\mu}$.

One may now use the above-displayed values of $\mathcal{P}_{\tau,\mu}$ to compare $\eta(\sigma)$ and $\eta(\tau)$. In doing so, notice especially the following facts: $\mathcal{P}_i$ and $\mathcal{P}_{\tau,i} = \mathcal{P}'$ are each nonempty; $\mathcal{P}_{\tau,i+1} = \mathcal{P}_i \setminus \mathcal{P}'$ is nonempty; and (as proved above) $\mathcal{P}_j = \varnothing$. The upshot is that $\eta(\sigma) = \eta(\tau) + 1 > \eta(\tau)$, contradicting the minimality of $\eta(\sigma)$. Thus, no such i exists, and the proof is complete. □

Remark 3.4. The proof of Algorithm 2.5 goes thorough even if one does not require that the prime ideal P_{i+1} of S_i is chosen to be minimal. However, there is no real gain in doing so. Indeed, Theorem 3.3 shows that any minimal generating set that could be obtained from a variant of Algorithm 2.5 in which the prime ideals P_{i+1} are not necessarily chosen to be minimal could also be obtained directly from Algorithm 2.5.

4. Ring-theoretic applications. Recall that $\mathrm{Max}\,(R) = \mathrm{Min}\,(R) = \mathrm{Spec}\,(R)$ for any nonzero finite ring R, cf. [**10**, Theorem 2, p. 203]. However, Lemmas 2.1 (a) and 2.2 (b) combine to show that the analogue fails for semigroup-theoretic ideals of S, the multiplicative monoid of R, if R is nonlocal. Moreover, we see by combining Lemmas 2.1 (a) and 2.2 (a) that if R is nonlocal, then the prime ideals of S are not the same as the prime ideals of R, in contrast to the situation for local rings as described in Lemma 2.3. In particular, the restriction to local rings in Lemma 2.3 is essential. Nevertheless, Lemma 4.1 identifies some compatibility between the semigroup- and the ring-theoretic concepts in the general case, by establishing that the set of *minimal* prime ideals of S coincides with $\mathrm{Min}\,(R)$, for any nonzero finite ring R. Lemma 4.1 also provides the technical key to proving Theorem 4.2.

Lemma 4.1. *Let R be a finite nonzero ring and let S be the multiplicative monoid of R. Then a subset H of S is a minimal prime ideal of S if and only if H is a necessarily minimal, prime ideal of R. In other words,* $\mathrm{Min}\,(R) = \mathrm{Spec}\,(R)$ *is the set of minimal prime ideals of S.*

Proof. If R is a field, then $\{0\}$ is the only semigroup- or ring-theoretic proper ideal, whence it is the only semigroup- or ring-theoretic prime ideal and the assertion follows in this case. Thus, we may assume henceforth that R is not a field. In fact, because of Lemma 2.3, we may often use notation below that tacitly assumes that R is nonlocal.

Since R is Artinian, it can be expressed uniquely as the internal direct product of finitely many local, nonzero, rings (R_j, J_j), $1 \leq j \leq k$, [**10**, Theorem 3, p. 205]; identify R with the external direct product $R_1 \times \cdots \times R_k$. By the above remarks, each prime ideal of R is minimal; and it is well known that the typical such prime ideal is given by $I_j := R_1 \times \cdots \times R_{j-1} \times J_j \times R_{j+1} \times \cdots \times R_k$, where $1 \leq j \leq k$. For each j, let e_j denote the multiplicative identity element of R_j. Note that $e_1 + \cdots + e_k = 1$ and $Re_j = R_j$ for each j.

We show first that if H is a minimal prime ideal of S, then H coincides with some I_j. To do this, we show that there is a permutation of $\{R_1, \ldots, R_k\}$ such that $H = I_k$.

In fact, since $I_k \in \mathrm{Spec}\,(R)$, it follows from Lemma 2.1 (a) and the minimality of H that it suffices to show that $I_j \subseteq H$. As a final reduction of the task, it suffices to show that $R_1 \times \cdots \times R_{k-1} \times \{0\} \subseteq H$. Indeed, if $\xi \in J_k$, then $\xi^\nu = 0$ for some positive integer ν, cf. [**10**, Note II, p. 151], whence the primeness of H ensures that any element of the form $x := (r_1, \ldots, r_{k-1}, \xi) \in H$ since $x^\nu = (r_1^\nu, \ldots, r_{k-1}^\nu, 0) \in R_1 \times \cdots \times R_{k-1} \times \{0\} \subseteq H$.

For any indexes $i \neq j$, we have $e_i e_j = 0 \in H$ and so, since H is a prime ideal of S, either $e_i \in H$ or $e_j \in H$. Thus, some $e_i \in H$ and, by permuting $\{R_1, \ldots, R_k\}$, we may suppose without loss of generality that $e_1 \in H$. Therefore, $R_1 \times \{0\} \times \cdots \times \{0\} = R_1 = Re_1 \subseteq H$. Next, consider the elements $f_2 := (e_1, e_2, 0, \ldots, 0), f_3 := (e_1, 0, e_3, 0, \ldots, 0), \ldots, f_k := (e_1, 0, \ldots, 0, e_k)$ of R. For all $2 \leq i < j \leq k$, we have that $f_i f_j \in R_1 \times \{0\} \times \cdots \times \{0\} = R_1 \subseteq H$. As H is a prime ideal of S, some $f_i \in H$. By permuting $\{R_2, \ldots, R_k\}$

(notice that R_1 is unchanged), we may suppose that $f_2 \in H$. Therefore, $R_1 \times R_2 \times \{0\} \times \cdots \times \{0\} = Rf_2 \subseteq H$.

Repeating the argument, next consider the elements $g_3 := (e_1, e_2, e_3, 0, \ldots, 0)$, $g_4 := (e_1, e_2, 0, e_4, 0, \ldots, 0)$, $\ldots$, $g_k := (e_1, e_2, 0, \ldots, 0, e_k)$ of R. For all $3 \leq i < j \leq k$, we have that $g_i g_j \in R_1 \times R_2 \times \{0\} \times \cdots \times \{0\} \subseteq H$. As H is a prime ideal of S, some $g_i \in H$. By permuting $\{R_3, \ldots, R_k\}$ (notice that R_1 and R_2 are each unchanged), we may suppose that $g_3 \in H$. Therefore, $R_1 \times R_2 \times R_3 \times \{0\} \times \cdots \times \{0\} = Rg_3 \subseteq H$. Iterating the argument, we see that there is a permutation of $\{R_1, \ldots, R_k\}$ such that $R_1 \times \cdots \times R_{k-1} \times \{0\} \subseteq H$. As explained above, this is enough to complete the proof that $H \in \operatorname{Min}(R) = \operatorname{Spec}(R)$.

Conversely, it remains to show that if K is a necessarily minimal, prime ideal of R, then K is a minimal prime ideal of S. By Lemma 2.1 (a), K is a prime ideal of S, and so, since S is finite, there exists a minimal prime ideal H of S such that $H \subseteq K$. By the preceding three paragraphs, $H = I_j$ for some j. In other words, $I_j \subseteq K$. By the minimality of K, it follows that $K = I_j$; that is, $K = H$, a minimal prime ideal of S. □

We next give our most important ring-theoretic applications.

Theorem 4.2. *Let R be a finite nonzero ring which is not a field, and let S be the multiplicative monoid of R. Consider the unique expression of R as the internal direct product of finitely many local, nonzero, rings (R_j, J_j), $1 \leq j \leq k$; for convenience, identify R with the external direct product $R_1 \times \cdots \times R_k$. The list of prime ideals of R is given by $I_1, \ldots, I_k$, where $I_j := R_1 \times \cdots \times R_{i-1} \times J_j \times R_{j+1} \times \cdots \times R_k$ for all $1 \leq j \leq k$. Then:*

(a) *The set of all the minimal generating sets of S is the same as the set of all the outputs resulting from applications of the algorithm in Algorithm* 2.5 *to R and S.*

(b) *In each application of the algorithm in Algorithm* 2.5 *to R and S, the integer n described in Algorithm* 2.5 (a) *as counting the number of steps in the process is given by $n = k$.*

(c) *For any application of the algorithm in Algorithm* 2.5 *to* R *and* S, *it is possible to permute* $\{R_j \mid 1 \leq j \leq k\}$ *so that, for all* $1 \leq i \leq k$, $S_i = U(R_1) \times \cdots \times U(R_i) \times R_{i+1} \times \cdots \times R_k$ *and* $P_i = U(R_1) \times \cdots \times U(R_{i-1}) \times J_i \times R_{i+1} \times \cdots \times R_k$.

(d) *In the applications of the algorithm in Algorithm* 2.5 *to* R *and* S, *there are exactly* $k!$ *possible sequences of the form* $\{S_i \mid 1 \leq i \leq k\}$. *Each such sequence determines the associated sequence* $\{P_i \mid 1 \leq i \leq k\}$ *but need not determine the sequence* $\{B_i \mid 1 \leq i \leq k\}$.

Proof. The list of, necessarily minimal, prime ideals of R was verified in the second paragraph of the proof of Lemma 4.1. A proof of (a) follows by combining Algorithm 2.5 (e) and Theorem 3.3. We turn now to the proofs of (b) and (c). Consider any application of the algorithm in Algorithm 2.5 to R and S. As P_1 is a minimal (nonzero) prime of S, Lemma 4.1 shows that, after a suitable permutation of $\{R_1, \ldots, R_k\}$, we may assume $P_1 = I_1 = J_1 \times R_2 \times \cdots \times R_k$. Therefore, $S_1 := S \setminus P_1 = R \setminus I_1 = (R_1 \setminus J_1) \times R_2 \times \cdots \times R_k = U(R_1) \times R_2 \times \cdots \times R_k$. This verifies the assertions in (c) for $i = 1$.

Next, recall that P_2 was chosen to be a minimal prime ideal of S_1. Given the above description of S_1, the reader can easily verify that P_2 must take the form $P_2 = U(R_1) \times K$, where K is necessarily some minimal prime ideal of the multiplicative monoid of the ring $A := R_2 \times \cdots \times R_k$. By applying Lemma 4.1 to A and its multiplicative monoid, we see that there exists a permutation of $\{R_2, \ldots, R_k\}$ such that $K = J_2 \times R_3 \times \cdots \times R_k$. Therefore, $P_2 = U(R_1) \times J_2 \times R_3 \times \cdots \times R_k$. Moreover, $S_2 := S_1 \setminus P_2 = U(R_1) \times (R_2 \setminus J_2) \times R_3 \times \cdots \times R_k = U(R_1) \times U(R_2) \times R_3 \times \cdots \times R_k$. This verifies the assertions in (c) for $i = 2$.

Assuming that $k > 2$, we provide the details for one more iteration of the above argument. Recall that P_3 was chosen to be a minimal prime ideal of S_2. Given the above description of S_2, one can verify that P_3 must take the form $P_3 = U(R_1) \times U(R_2) \times L$, where L is necessarily some minimal prime ideal of the multiplicative monoid of the ring $B := R_3 \times \cdots \times R_k$. By applying Lemma 4.1 to B and its multiplicative monoid, we see that there exists a permutation of $\{R_3, \ldots, R_k\}$ such that $L = J_3 \times R_4 \times \cdots \times R_k$. Thus, $P_3 = U(R_1) \times U(R_2) \times J_3 \times R_4 \times \cdots \times R_k$. Also, $S_3 := S_2 \setminus P_3 = U(R_1) \times U(R_2) \times (R_3 \setminus J_3) \times R_4 \times \cdots \times R_k =$

$U(R_1) \times U(R_2) \times U(R_3) \times R_4 \times \cdots \times R_k$. This verifies the assertions in (c) for $i = 3$.

Iterating the above argument, we obtain external direct product descriptions of all the P_i and S_i, thus completing the proof of (c). In particular, by taking $i = k$, we have $S_k = U(R_1) \times \cdots \times U(R_k) = U(R)$, which is a group. Therefore, by the description of the process in the statement of Algorithm 2.5, the number of steps in the application is $n = k$, thus completing the proof of (b). It remains only to prove (d).

(d) By Lemma 4.1, the typical minimal prime of S is of the form I_j, where $1 \leq j \leq k$. It is easy to verify that each of the $k!$ permutations of $\{1, \ldots, k\}$ provides, via the prescriptions in (c), an implementation of the algorithm in Algorithm 2.5. Different permutations of $\{1, \ldots, k\}$ produce different sequences $\{S_i\}$, because no R_j is a group under multiplication; and we see via (b) that the sequence $\{S_i\}$ determines the sequence $\{P_i\}$.

It remains only to give an example that establishes the final assertion. Perhaps the simplest such example can be built by taking (R, M) as an SPIR whose maximal ideal $M = R\pi$ has index of nilpotency 3. (For a non-local example, see Remark 2.7.) For specificity, take $R := \mathbf{F}_2[X]/(X^3) = \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\}$, where $\pi := x := X + (X^3)$. Since R is local, it follows from (c) that there is only one possible sequence $\{S_i\}$ appearing in the applications of the algorithm in Algorithm 2.5 to R. By Lemma 4.1, or the final paragraph of the proof of Corollary 2.6 (a), any such application of this algorithm involves choosing a minimal nonempty set $B_1 \subseteq M$ such that $\langle B_1 U(R) \rangle = P_1 = M$; that is, a minimal nonempty set $B_1 \subseteq \{0, x, x^2, x + x^2\}$ such that $\langle B_1 \{1, 1 + x, 1 + x^2, 1 + x + x^2\} \rangle = \{0, x, x^2, x + x^2\}$. A routine calculation reveals that there are exactly two such B_1, namely, $\{x\}$ and $\{x + x^2\}$. The proof is complete. □

Remark 4.3 (a). The semigroup-theoretic analogue of Theorem 4.2 (b) is literally false. More precisely, the number of steps needed in an application of the algorithm in Algorithm 2.5 to S, the given nontrivial semigroup with zero, *need not be* the number of minimal prime ideals of S. Perhaps the simplest nontrivial example that illustrates this phenomenon is given by the three-element, commutative, monoid $S := \{0, a, 1\}$, where $a^2 = a$ and multiplication by 0 or 1 is as expected

from the notation. Indeed, this S has exactly one minimal prime ideal, namely, $H := \{0\}$, and so any application of the algorithm in Algorithm 2.5 to S must involve the choice of $P_1 := H$. In any such application, the number of steps required is 2, as P_2 is necessarily chosen to be $\{a\}$, which is the complement of P_1 in the unique maximal ideal $K := \{0, a\}$ of S. This example also shows that the method of proof of Theorem 3.3 is efficient inasmuch as the number of steps needed above, namely, 2, is precisely the number of prime ideals of S (which was denoted m in the standing notation of Section 3).

There are several ways to see that the monoid S introduced above is not the multiplicative monoid of any finite ring R. First, if such an R existed, then Lemma 4.1 and Theorem 4.2 (b) would combine to show that any application of the algorithm in Algorithm 2.5 to S terminates in one step, contrary to the preceding paragraph. Second, if such an R existed, then $K = S \setminus U(S)$, by Lemma 2.2, would be the union of the minimal prime ideals of R (since $\mathrm{Spec}\,(R) = \mathrm{Min}\,(R)$), which, in view of Lemma 4.1, would contradict the fact that $K \neq H$. Third, if such an R existed, one would contradict Lagrange's theorem, for the index of K in, the additive group of, R would be $|R|/|K| = 3/2$, which is not an integer.

One may object that the monoid S constructed above is quite special, given that $U(S) = \{1\}$. Another, less trivial example illustrating the points made above concerning S is the five-element commutative monoid $T := \{0, a, b, 1, c\}$, where $a^2 = 0$, $b^2 = b$, $c^2 = 1$, $ab = 0$, $ac = a$, $bc = b$, and multiplication by 0 or 1 is as expected from the notation. Indeed, $U(T)$ has cardinality 2; T has exactly one minimal prime ideal, namely, $\{0, a\}$; T has exactly one nonminimal prime ideal, namely, $T \setminus U(T) = \{0, a, b\}$; and any application of the algorithm in Algorithm 2.5 to T must terminate in exactly two steps.

(b) At first blush, it might seem possible to avoid some of the above semigroup-theoretic reasoning if one is interested in only the ring-theoretic applications in Theorem 4.2. For instance, suppose, to mix the notations of Sections 3 and 4, that one takes $\{A_1, \ldots, A_k\}$ to be $\mathrm{Min}\,(R)$. (Such an ordering is permitted, thanks to Lemma 4.1.) Then, taking σ to be the identity permutation (for simplicity), we find via the prime avoidance lemma [**8**, Theorem 81] that $\mathcal{P}_i$ is nonempty whenever $1 \leq i \leq k$ and $\mathcal{P}_i$ is empty whenever $k + 1 \leq i \leq m$. In view of Theorem 4.2 (b), one may choose instead to proceed along a

related, but somewhat different, tack by seeking to modify the proof of Theorem 3.3 in the ring-theoretic context by replacing $\{A_1, \ldots, A_m\}$ and the meaning of m with $\mathrm{Min}\,(R)$ and k, respectively. Then, the suitably redefined $\mathcal{P}_k$ are never empty, by virtue of Lemma 4.1 and the prime avoidance lemma.

However, we next identify three obstacles that arise if one tries to replace $\{A_1, \ldots, A_m\}$ with $\mathrm{Min}\,(R)$ in the above proofs. First, the proof of Lemma 3.2 (d) would not carry over, as it depends on Lemma 2.2. Thus, we find a second obstacle: the proof of Lemma 3.2 (n) would not carry over. Finally, a third obstacle would arise in modifying the proof of Theorem 3.3 itself, for it can be shown that the prime ideal $\mathcal{D}$ constructed there is not minimal.

In closing, we indicate a possible direction for future work. It would be of interest to replace the restriction to finite semigroups, monoids and rings in this paper by considering semigroups, monoids and rings that satisfy suitable chain conditions.

REFERENCES

1. D.D. Anderson, *Finitely presented multiplicative semigroups of rings*, Semigroup Forum **55** (1997), 294–298.

2. D.D. Anderson and J. Stickles, *Commutative rings with finitely presented multiplicative semigroup*, Semigroup Forum **60** (2000), 436–443.

3. K.E. Aubert, *On the ideal theory of commutative semi-groups*, Math. Scand. **1** (1953), 39–54.

4. G.D. Bullington, *On the expected number of generators of a submodule of a free module over a finite special principal ideal ring*, Rend. Circ. Mat. Palermo (2) **51** (2002), 5–50.

5. R. Gilmer, *Commutative semigroup rings*, Chicago Lectures in Math., Univ. Chicago Press, Chicago, 1984.

6. J. R. Isbell, *On the multiplicative semigroup of a commutative ring*, Proc. Amer. Math. Soc. **10** (1959), 908–909.

7. N. Jacobson, *Lectures in abstract algebra*, Vol. I, Van Nostrand, Princeton, 1951.

8. I. Kaplansky, *Commutative rings*, rev. ed., Univ. Chicago Press, Chicago, 1974.

9. E.S. Ljapin, *Semigroups*, Transl. Math. Monogr., vol. 3, Amer. Math. Soc., Providence, 1974.

10. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Van Nostrand, Princeton, 1958.

Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1300
E-mail address: dobbs@math.utk.edu

Department of Mathematics, University of Tennessee, Knoxville, Tennessee 37996-1300