V. Ponomarenko (San Diego State Univ., USA)

ARITHMETIC OF SEMIGROUP SEMIRINGS

АРИФМЕТИКА НАПІВГРУПОВИХ НАПІВКІЛЕЦЬ

We define semigroup semirings by analogy with group rings and semigroup rings. We study the arithmetic properties and determine sufficient conditions under which a semigroup semiring is atomic, has finite factorization, or has bounded factorization. We also present a semigroup-semiring analog (although not a generalization) of the Gauss lemma on primitive polynomials.

Напівгрупові напівкільця визначаються по аналогії з груповими кільцями та напівгруповими кільцями. Вивчено арифметичні властивості та отримано достатні умови, за яких напівгрупове напівкільце є атомним, має скінченну факторизацію або має обмежену факторизацію. Також наведено напівгрупово-напівкільцевий аналог (хоча і не узагальнення) гауссівської леми про примітивні поліноми.

1. Introduction. The study of group rings is very popular and active, see, e.g., [7]. Similarly, the study of semigroup rings has a rich history, see, e.g., [8]. Also, the study of semirings is very active not only in mathematics but in computer science and control theory, see, e.g., [10]. In this context, it seems natural to study semigroup semirings; however relatively little work (see, e.g., [4, 15]) has been done in this area. We propose to study the arithmetic properties of semigroup semirings, specifically factorization into irreducibles and primes. As tools we will use tools from semirings as well as from semigroups.

This work is organized as follows. Section 1 collects basic facts and tools about semirings and factorization theory. Section 2 introduces semigroup semirings and develops several tools to find atoms. Section 3 introduces content sets and maximal common divisors, which generalize the notion of greatest common divisors. These tools are sufficient to determine necessary conditions for a semigroup semiring to be atomic, finite factorization, and bounded factorization. We also prove a semiring analog of the Gauss lemma on primitive polynomials.

Definition 1.1. *We call* $R = (R, +, \times)$ *a semiring if it satisfies the following*:

(1) $(R, +)$ *is a commutative monoid with identity* 0;

(2) $(R, \times)$ *is a commutative monoid with identity* 1. *We abbreviate* $\times$ *via juxtaposition*;

(3) *for all* $a \in R$, $a0 = 0$;

(4) *for all* $a, b, c \in R$, $a(b + c) = (ab) + (ac)$.

Following [10], *we call* R *an information algebra if it also satisfies the following*:

(5) *for all* $a, b \in R$, *if* $a + b = 0$ *then* $a = b = 0$;

(6) *for all* $a, b \in R$, *if* $ab = 0$ *then* $a = 0$ *or* $b = 0$.

For convenience, set $R^* = R \setminus \{0\}$. Properties (5), (6) are equivalent to R^* being closed under $+, \times$.

Lemma 1.1. *Let* R *be an information algebra, and let* $a_1, a_2, \ldots, a_k,\ b_1, b_2, \ldots, b_k \in R$. *Then* $\sum_{i=1}^{k} a_i b_i$ *is nonzero if and only if there is some* $i \in [1, k]$ *with* a_i *and* b_i *each nonzero*.

Proof. If the sum is zero, then each summand is zero by property (5), and hence for each i either $a_i = 0$ or $b_i = 0$ by property (6). The other direction is trivial.

Let $(M, \cdot)$ be a commutative monoid with identity e. We say that binary relation R on M *respects* $\cdot$ if for all $a, b, c \in M$, aRb implies that $(a \cdot c)R(b \cdot c)$. We define the relation $\mid$ on M via $a \mid b$ if there is some $c \in M$ with $a \cdot c = b$. We say that a is a *unit* if $a \mid e$ and a *nonunit* otherwise. It is easy to see that the product of units is a unit and the product of nonunits is a nonunit. We say that a and b are *associates* if $a \mid b$ and $b \mid a$.

We now recall terms from the arithmetical theory of semigroups. For an introduction, see [6]. We say that nonunit a is an *atom* if $a = b \cdot c$ implies that either b or c is a unit. We say that $(M, \cdot)$ is *atomic* if every nonunit may be factored into atoms in at least one way. We say that nonunit a is *prime* if $a \mid b \cdot c$ implies that $a \mid b$ or $a \mid c$. We say that $(M, \cdot)$ is *reduced* if e is the only unit.

For a in atomic $(M, \cdot)$, we say that $a_1 \cdot a_2 \ldots a_k$ is a *factorization* of a if the product is a and each a_i is an atom. Two factorizations $a_1 \cdot a_2 \ldots a_k$ and $a'_1 \cdot a'_2 \ldots a'_k$ are *equivalent* if there is some permutation $\pi \in S_k$, and $a_i, a'_{\pi(i)}$ are associates for $1 \le i \le k$. This is an equivalence relation on the set of all factorizations of an element. For nonunit a, we call $F(a)$ a *factorization set* of a if every equivalence class of factorizations of a has exactly one representative in $F(a)$. We define the *length set* $\mathcal{L}(a) = \{k : a_1 \cdot a_2 \ldots a_k \in F(a)\}$. Note that $|F(a)|$ and $\mathcal{L}(a)$ are independent of the choice of equivalence class representatives for $F(a)$. We say that a has *unique factorization* (*UF*) if $|F(a)| = 1$; we say that a has *finite factorization* (*FF*) if $|F(a)| < \infty$; we say that a has *bounded factorization* (*BF*) if $|\mathcal{L}(a)| < \infty$. We say that $(M, \cdot)$ is UF, FF, BF if each nonunit in M is. We define the *elasticity* ρ of $a \in M$ via $\rho(a) = \dfrac{\sup \mathcal{L}(a)}{\min \mathcal{L}(a)}$. We define the elasticity $\rho(M) = \sup_{a \in M} \rho(a)$, and say M is *fully elastic* if every $x \in \mathbb{Q} \cap [1, \rho(M))$ is the elasticity of some element in M.

We say that $(M, \cdot)$ is *yoked* if for all $a, b \in M$ there is some $c \in M$ where either $a \cdot c = b$ or $a = b \cdot c$. We say that $(M, \cdot)$ is *cancellative* if $a \cdot c = b \cdot c$ implies that $a = b$. Following [3], we say that $(M, \cdot)$ is *weakly cancellative* if $a \cdot b = a$ implies that $b = e$. This property has also been called plain, in [10].

Lemma 1.2. *$(M, \cdot)$ is weakly cancellative if and only if the following holds*:

$$\forall a, b, c \in M, \quad with\ unit\ a. \quad If\ a \cdot c = b \cdot c, \quad then \quad a = b.$$

Proof. Let $d \in M$ with $d \cdot a = e$. Then $c = d \cdot a \cdot c = d \cdot b \cdot c$. Applying weak cancellativity, $d \cdot b = e$ and hence $b = a \cdot d \cdot b = a \cdot e = a$. The other direction follows by taking $a = e$.

Our primary focus is on information algebras R. We study the multiplicative monoid $(R^*, \times)$, and say that R is atomic, cancellative, reduced, etc. if $(R^*, \times)$ is. We say that $a \in R^*$ is a unit, atom, prime, etc. if it is in $(R^*, \times)$.

Example 1.1. The set of nonnegative integers $\mathbb{N}_0$ is a UF, cancellative, reduced, information algebra under the usual $+, \times$.

Example 1.2. For $\mathbb{B} = \{0, 1\}$, we set $0 + 0 = 0 \times 0 = 0 \times 1 = 1 \times 0 = 0$, $0 + 1 = 1 + 0 = 1 + 1 = 1 \times 1 = 1$, and $1 > 0$. This is an UF, cancellative, reduced, yoked information algebra known as the *Boolean semiring*.

Example 1.3. Let $(R, +, \times)$ be the set of fractional ideals of a Dedekind domain D. $+$ has identity (0), and $\times$ has identity D. $(R, +, \times)$ is an atomic information algebra.

***Example* 1.4.** Let R be a partially-ordered semiring (or ring). Set $R^+ = \{r \in R : r \geq 0\}$, the positive cone of R. R^+ is an information algebra.

***Example* 1.5.** Let R be a semiring that is not a ring. Then $\{1 + r : r \in R\} \cup \{0\}$ is an information algebra.

Proposition 1.1. *Let $(M, \cdot)$ be a commutative monoid. Then the following hold*:

1. *The relation $|$ is a preorder, with $u \mid a$ for all units u and all $a \in M$.*

2. *If $a = u \cdot b$ for some unit u, then a, b are associates. If $(M, \cdot)$ is also weakly cancellative, then the opposite implication also holds.*

3. *Let $a \in M$. If a is an atom, then for all $b \mid a$, either b is a unit or an associate of a. If $(M, \cdot)$ is also weakly cancellative, then the opposite implication also holds.*

4. *Let $a, b \in M$ be associates. If a is an atom, then b is an atom.*

5. *If $(M, \cdot)$ is weakly cancellative, then every prime is an atom.*

6. *If $(M, \cdot)$ is UF, then every atom is prime.*

7. *If $(M, \cdot)$ is reduced and weakly cancellative, then $|$ is a partial order. If $(M, \cdot)$ is yoked, then $|$ is a weak order. If $(M, \cdot)$ is reduced, weakly cancellative, and yoked, then $|$ is a total order.*

8. *The relation $|$ respects $\cdot$.*

9. *If there exists a partial order $\leq$ on M with least element e that respects $\cdot$, then $(M, \cdot)$ is reduced. Further, $\leq$ is a refinement of $|$. That is, if $a \mid b$ then $a \leq b$.*

Proof. (1) Straightforward.

(2) Suppose that $a = b \cdot u$ for some unit u. Hence $b \mid a$. Let v be such that $u \cdot v = e$. We have $a \cdot v = b \cdot u \cdot v = b$, and thus $a \mid b$ so a, b are associates. Suppose now that $(M, \cdot)$ is weakly cancellative and a, b are associates. Then there are d, d' with $a = b \cdot d$, $b = a \cdot d'$. Combining, we have $a = b \cdot d = a \cdot (d' \cdot d)$, and hence $e = d' \cdot d$. Thus d is a unit and $a = b \cdot d$.

(3) Suppose that a is an atom. Let $b \mid a$ for nonunit b that is a nonassociate of a. Then $a = b \cdot c$ for some $c \in M$. Since a is an atom and b is a nonunit, then c must be a unit. By (2), a, b are associates, contrary to hypothesis.

Now let a be a nonatom that satisfies the condition. Write $a = b \cdot c$, a product of two nonunits. By hypothesis, b must be a unit or associate of a, hence an associate of a. By (2), $b = a \cdot u$ for some $u \in M$. Hence $a = b \cdot c = a \cdot (u \cdot c)$, and by weak cancellativity $u \cdot c = e$. Hence c is a unit, in violation of hypothesis.

(4) Suppose otherwise; we write $b = u \cdot v$ for some nonunits u, v. Since a, b are associates there is some $c \in M$ with $a = b \cdot c = u \cdot v \cdot c$. Hence a is a product of nonunits $u, (v \cdot c)$, a contradiction.

(5) Let $a \in M$ be prime. Suppose $a = b \cdot c$ for nonunits b, c. Since a is prime, we assume without loss that $a \mid b$. Hence a, b are associates and by (2) there is some unit u with $b = a \cdot u$. Now $a = b \cdot c = a \cdot u \cdot c$, and by weak cancellativity $u \cdot c = e$ and hence c is a unit. This contradiction shows that a is an atom.

(6) Let $a \in M$ be an atom, and suppose $a \mid b \cdot c$. There is some $d \in M$ with $a \cdot d = b \cdot c$. We take factorizations $d = (d_1 \cdot d_2 \ldots)$, $b = (b_1 \cdot b_2 \ldots)$, $c = (c_1 \cdot c_2 \ldots)$. We have two factorizations $a \cdot (d_1 \cdot d_2 \ldots) = (b_1 \cdot b_2 \ldots) \cdot (c_1 \cdot c_2 \ldots)$; by UF these must be equivalent. Without loss we may assume that a, b_1 are associates; but then $a \mid b$. Hence a is prime.

(7) Suppose that $a \mid b$ and $b \mid a$. Then by (2), $a = u \cdot b$ for some unit u, and $u = e$ since $(M, \cdot)$ is reduced. Therefore $a = b$ and $\mid$ is antisymmetric. Suppose that $(M, \cdot)$ is yoked. Then for all $a, b \in M$, either $a \mid b$ or $b \mid a$ and hence $\mid$ is a total preorder (aka a weak order). A total partial order is a total order.

(8) Straightforward.

(9) First, note that if u is a unit different from e we have $u \cdot v = e$ and $e < u = u \cdot e < u \cdot v = e$, a contradiction. Hence $(M, \cdot)$ is reduced. Suppose now that $a \mid b$. Then there is some $c \in M$ with $b = a \cdot c$. We now have $a = a \cdot e \le a \cdot c = b$.

For information algebras R, we will use $\mid_+$ to denote the preorder $\mid$ on the reduced monoid $(R, +)$.

Proposition 1.2. *Suppose that $(M, \cdot)$ has UF. Then $(M, \cdot)$ is weakly cancellative if and only if it is cancellative.*

Proof. One direction is trivial. For the other, suppose that a, b are nonunits and $a \cdot c = b \cdot c$. If c is a unit we multiply by c^{-1} and get $a = b$; otherwise we take factorizations $a = (a_1 \cdot a_2 \ldots)$, $b = (b_1 \cdot b_2 \ldots)$, $c = (c_1 \cdot c_2 \ldots)$. By UF the factorization $(a_1 \cdot a_2 \ldots) \cdot (c_1 \cdot c_2 \ldots)$ is equivalent to $(b_1 \cdot b_2 \ldots) \cdot (c_1 \cdot c_2 \ldots)$. Hence we may assume without loss that a_i, b_i are associates for all i, and thus a, b are associates. By Proposition 1.1(2), there is some unit u with $a = u \cdot b$. But then $u \cdot b \cdot c = b \cdot c$, and by weak cancellativity $u = e$ and hence $a = e \cdot b = b$.

Definition 1.2. *Given semirings R_1, R_2, we say $\phi \colon R_1 \to R_2$ is a morphism if it satisfies the following, for all $a, b \in R_1$:*

(1) $\phi(a + b) = \phi(a) + \phi(b)$,

(2) $\phi(ab) = \phi(a)\phi(b)$,

(3) $\phi(0) = 0$, $\phi(1) = 1$.

For morphism ϕ and property P, we say that P *carries forward* if $P(a)$ implies $P(\phi(a))$. We say that P *carries backward* if $P(\phi(a))$ implies $P(a)$. We say that P *is preserved* if it carries forward and backward. We make similar statements for semiring properties.

Proposition 1.3. *Let $\phi \colon R_1 \to R_2$ be a morphism. Then units and associates carry forward. If units are preserved, then atoms carry backward. If ϕ is injective, then cancellation and weak cancellation carries backward. If ϕ is surjective, then yoked carries forward.*

Proof. (Units) Let $a \in R_1$ be a unit. Choose $b \in R_1$ with $ab = 1$. Then $\phi(a)\phi(b) = \phi(1) = 1$, so $\phi(a)$ is a unit.

(Associates) Let $a, b \in R_1$ be associates. There must be $c, d \in R_1$ with $a = bc$, $b = ad$. We have $\phi(a) = \phi(b)\phi(c)$ and $\phi(b) = \phi(a)\phi(d)$.

(Atoms) Suppose that $\phi(a)$ is an atom. a cannot be a unit since units carry forward. Suppose that a is not an atom. Then we write $a = a_1 a_2$ for nonunits $a_1, a_2 \in R_1$. Then $\phi(a) = \phi(a_1)\phi(a_2)$, a product of nonunits since units carry backward. Hence $\phi(a)$ is a nonatom, contrary to hypothesis.

(Cancellation) Suppose that $ac = bc$. Then $\phi(a)\phi(c) = \phi(b)\phi(c)$, and by cancellation on R_2, $\phi(a) = \phi(b)$. Since ϕ is injective, $a = b$.

(Weak cancellation) Suppose that $ab = a$. Then $\phi(a)\phi(b) = \phi(a)$, and by weak cancellation on R_2, $\phi(b) = 1$. Since ϕ is injective, $b = 1$.

(Yoked) Let $a, b \in R_2$. Since ϕ is surjective, there are $a', b' \in R_1$ with $\phi(a') = a$, $\phi(b') = b$. Since R_1 is yoked, without loss we let $c \in R_1$ with $a'c = b'$. Then $\phi(a')\phi(c) = \phi(b')$ and $a\phi(c) = b$. Hence R_2 is yoked.

Proposition 1.4. *Let R_1, R_2 be semirings. Let $\phi \colon R_1 \to R_2$ be a bijective morphism. Then $\phi^{-1} \colon R_2 \to R_1$ is a (bijective) morphism. Also, ϕ preserves units, associates, atoms, primes, and UF.*

Proof. Let $a, b \in R_2$. $\phi(\phi^{-1}(a) + \phi^{-1}(b)) = \phi(\phi^{-1}(a)) + \phi(\phi^{-1}(b)) = a + b$. Hence $\phi^{-1}(a + b) = \phi^{-1}(\phi(\phi^{-1}(a) + \phi^{-1}(b))) = \phi^{-1}(a) + \phi^{-1}(b)$. Similarly, $\phi(\phi^{-1}(a)\phi^{-1}(b)) = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b)) = ab$. Hence $\phi^{-1}(ab) = \phi^{-1}(\phi(\phi^{-1}(a)\phi^{-1}(b))) = \phi^{-1}(a)\phi^{-1}(b)$. Hence ϕ^{-1} is a morphism.

ϕ preserves units, associates, and atoms by applying Proposition 1.3 to ϕ and ϕ^{-1}.

(Primes) Suppose that a is a prime but $\phi(a)$ is a nonprime. Hence there are $b, c, d \in R_2$ with $\phi(a)d = bc$, but $\phi(a) \nmid b$ and $\phi(a) \nmid c$. Because ϕ is surjective, there are $b', c', d' \in R_1$ with $\phi(b') = b$, $\phi(c') = c$, $\phi(d') = d$. $\phi(ad') = \phi(a)\phi(d') = \phi(a)d = bc = \phi(b')\phi(c') = \phi(b'c')$, hence since ϕ is injective $ad' = b'c'$. Since a is prime, without loss $a \mid b'$, i.e., there is some $h \in R_1$ with $ah = b'$. Now $\phi(a)\phi(h) = \phi(b') = b$, so $\phi(a) \mid b$, a contradiction. Hence ϕ carries primes forward; the other direction follows from ϕ^{-1}.

(UF) Suppose R_2 is UF. Let $a \in R_1$ have two inequivalent factorizations $a_1 a_2 \ldots a_k$, $a_1' a_2' \ldots a_j'$. But then $\phi(a_1)\phi(a_2)\ldots\phi(a_k)$, $\phi(a_1')\phi(a_2')\ldots\phi(a_j')$ are inequivalent factorizations of $\phi(a)$, a contradiction. Hence ϕ carries UF backward; the other direction follows from ϕ^{-1}.

Note that for any morphism ϕ, if $a \mid b$ then $\phi(a) \mid \phi(b)$. Recalling an important tool from factorization theory, we say that ϕ is a *divisor morphism* if the converse also holds.

Definition 1.3. *We say that morphism $\phi \colon R_1 \to R_2$ is a divisor morphism if it satisfies the following: For all $a, b \in R_1$, if $\phi(a) \mid \phi(b)$ (in R_2), then $a \mid b$ (in R_1).*

Proposition 1.5. *Let $\phi \colon R_1 \to R_2$ be a divisor morphism. Then units and associates are preserved, while atoms and primes carry backward. If ϕ is surjective, then atoms and primes are preserved.*

Proof. It is straightforward to prove that units, associates, and primes carry forward.

Let $a \in R_1$ and suppose that $\phi(a)$ is a nonatom. Write $\phi(a) = bc$, and by surjectivity there are $b', c' \in R_1$ with $\phi(b') = b, \phi(c') = c$. Hence $\phi(a) = \phi(b'c')$ and $\phi(a) \mid \phi(b'c')$, $\phi(b'c') \mid \phi(a)$. Therefore $a, b'c'$ are associates. b', c' cannot be units since units carry forward; hence a is a nonatom.

Let $a \in R_1$ be prime. Suppose that $\phi(a) \mid bc$; by surjectivity there are $b', c' \in R_1$ with $\phi(b') = b$, $\phi(c') = c$. Because $\phi(a) \mid bc = \phi(b'c')$, $a \mid b'c'$; since a is prime we may assume without loss that $a \mid b'$. But then $\phi(a) \mid \phi(b') = b$.

Proposition 1.6. *Let R_1, R_2 be atomic semirings, and let $\phi \colon R_1 \to R_2$ be a divisor morphism. For all $a \in R_1$, $\sup \mathcal{L}(a) \leq \sup \mathcal{L}(\phi(a))$. Further, BF and FF carry backward.*

Proof. Let $a \in R_1$, $k \in \mathcal{L}(a)$. Choose $a_1 a_2 \ldots a_k \in F(a)$. $\phi(a) = \phi(a_1)\phi(a_2)\ldots\phi(a_k)$. $\mathcal{L}(\phi(a)) \supseteq \mathcal{L}(\phi(a_1)) + \mathcal{L}(\phi(a_2)) + \ldots + \mathcal{L}(\phi(a_k)) \geq 1 + 1 + \ldots + 1 \geq k$. Hence $\sup \mathcal{L}(a) \leq \sup \mathcal{L}(\phi(a))$, and if the right-hand side is finite (i.e., a is BF) then so is the left-hand side.

Let $a \in R_1$, $a_1 a_2 \ldots a_k \in F(a)$. Since ϕ preserves units, $\phi(a) = \phi(a_1)\phi(a_2)\ldots\phi(a_k)$, a product of nonunits. Suppose now that $F(\phi(a))$ is finite, but $F(a)$ is infinite. Since each element of $F(\phi(a))$ has only finitely many partitions as above, there must be at least two (in fact infinitely many) partitions

$a_1 a_2 \ldots a_k$, $a'_1 a'_2 \ldots a'_k \in F(a)$ both mapping to $(b_1^1 b_1^2 \ldots)(b_2^1 b_2^2 \ldots) \ldots (b_k^1 b_k^2 \ldots) \in F(\phi(a))$, where $(b_i^1 b_i^2 \ldots) \in F(\phi(a_i)) \cap F(\phi(a'_i))$. But then $\phi(a_i) = \phi(a'_i)$, and hence a_i, a'_i are associates, and hence $a_1 a_2 \ldots a_k$, $a'_1 a'_2 \ldots a_k$ are equivalent yet both in $F(a)$, a contradiction.

The following result may be found in [9]; we include its short proof for completeness.

Proposition 1.7. *Let R be an information algebra. Then $\phi \colon R \to \mathbb{B}$ given by $\phi(0) = 0$, $\phi(r) = 1$ (for all other r) is a morphism.*

Proof. If $a = b = 0$, then $\phi(a+b) = \phi(ab) = 0 = \phi(a) + \phi(b) = \phi(a)\phi(b)$. If a, b are nonzero, then $a + b$, ab are both nonzero, so $\phi(a+b) = \phi(ab) = 1 = \phi(a) + \phi(b) = \phi(a)\phi(b)$. If one of a, b is zero, but the other is nonzero, then $a + b$ is nonzero and $ab = 0$. So $\phi(a+b) = 1 = \phi(a) + \phi(b)$ while $\phi(ab) = 0 = \phi(a)\phi(b)$.

2. Semigroup semirings. Semigroup semirings may be seen as analogous to group rings and semigroup rings. We propose to study their arithmetic properties, namely factorization into atoms.

Definition 2.1. *Given information algebra R and reduced commutative monoid $(S, +)$ with identity e, we define the semigroup semiring $R[X; S] = \left\{ \sum_{s \in S} r_s X^s : r_s \in R \right\}$, where we insist that all but finitely many coefficients $r_s = 0$. Notationally, we write $A = \sum_{s \in S} a_s X^s$, where elements of $R[X; S]$ are denoted by capital letters and their coefficients by lower case versions. We will often abbreviate $\sum_{s \in S}$ by just $\sum$. We define $+, \times$ as follows:*

(1) $A + B = \sum (a_s + b_s) X^s$, with identity $0 = \sum 0 X^s$,

(2) $A \times B = \sum r_s X^s$, where $r_s = \sum_{u+v=s} a_u b_v$. This has identity $1 = 1 X^e$.

Example 2.1. Let R be an arbitrary information algebra, and let $S = \mathbb{N}_0$. Then $R[X; S]$ is the semiring of polynomials with coefficients from R. These have been studied in [2, 14].

Example 2.2. Let S be an arbitrary reduced commutative monoid, and let $R = \mathbb{B}$. Then $R[X; S]$ models the semiring of subsets of S, with operations union $(+)$ and Minkowski addition $(\times)$. These have been studied in [5, 13].

Example 2.3. Let S be an arbitrary reduced commutative monoid, and let $R = \mathbb{N}_0$. Then $R[X; S]$ models the semiring of multisets from S, with operations multiset union $(+)$ and multiset addition $(\times)$.

Proposition 2.1. *Semigroup semiring $R[X; S]$ is an information algebra.*

Proof. (1) $(R[X; S], +)$ is closed and commutative with identity 0 because $(R, +)$ is.

(2) $(R[X; S], \times)$ is closed and commutative because R is a semiring. We have $1 = 1X^e + + \sum 0 X^s$, so $1A = \sum r_s X^s$ where r_s has only one nonzero summand, namely $1 a_s$. Hence $1A = A$.

(3) $A0 = \sum r_s X^s$, where $r_s = \sum_{u+v=s} a_u 0 = 0$. Hence $A0 = 0$.

(4) $A(B + C) = \sum r_s X^s$, where $r_s = \sum_{u+v=s} a_u (b_v + c_v) = \sum_{u+v=s} (a_u b_v) + (a_u c_v) = \sum_{u+v=s} a_u b_v + \sum_{u+v=s} a_u c_v$, repeatedly using the semiring properties of R. Hence $A(B+C) = (AB) + (AC)$.

(5) Let $A, B \in R[X; S]$. If $A + B = 0$, then $(a+b)_s = 0$ for all $s \in S$; hence since R is positive $a_s = b_s = 0$ and thus $A = B = 0$.

(6) Let $A, B \in R[X; S]$, and set $C = AB$. If $C = 0$, then $\sum_{u+v=s} a_u b_v = 0$ for all $s \in S$. Suppose that $A \neq 0$ and $B \neq 0$. Then there are $u, v \in S$ with $a_u \neq 0$ and $b_v \neq 0$. By Lemma 1.1, $c_{u+v} \neq 0$ and hence $C \neq 0$, which contradicts hypothesis. Hence either $A = 0$ or $B = 0$.

Proposition 2.2. *Let $R[X; S]$ be a semigroup semiring. The natural embedding $\phi \colon R \to$* $\to R[X; S]$ *given by $\phi(a) = aX^e$ is a divisor morphism. Also, the natural projection $\psi \colon R[X; S] \to$* $\to R$ *given by $\psi \left(\sum a_s X^s \right) = a_e$ is a morphism.*

Proof. (1) Let $a, b \in R$. $\phi(ab) = (ab)X^e = abX^{e+e} = (aX^e)(bX^e) = \phi(a)\phi(b)$. $\phi(a + b) =$ $= (a + b)X^e = aX^e + bX^e = \phi(a) + \phi(b)$. If $\phi(a) \mid \phi(b)$ then there is some $C \in R[X; S]$ with $\phi(a)C = \phi(b)$. Since S is reduced, $c_s = 0$ for $s \neq e$, and hence $C = c_e X^e$. We have $a_e c_e = b_e$, so $a \mid b$.

(2) Let $A, B \in R[X; S]$. $\psi(A+B) = (A+B)_e = A_e + B_e = \psi(A) + \psi(B)$. $\psi(AB) = (AB)_e =$ $= \sum_{u+v=e} a_u b_v = a_e b_e = \psi(A)\psi(B)$, where $u + v = e$ implies $u = v = e$ since S is reduced.

Proposition 2.3. *Let $R[X; S]$ be a semigroup semiring. Then the following hold*:

(1) aX^e *is a unit in $R[X; S]$ if and only if a is a unit in R;*

(2) aX^e *is an atom in $R[X; S]$ if and only if a is an atom in R;*

(3) *if $R[X; S]$ is cancellative/weakly cancellative/yoked, then so is R.*

Proof. Propositions 1.3, 1.5, and 2.2.

Definition 2.2. *Let $R[X; S]$ be a semigroup semiring, and let $A \in R[X; S]$. Set $\operatorname{Supp}(A) =$* $= \{s \in S \colon a_s \neq 0\}$, *the support of A. If $e \in \operatorname{Supp}(A)$, then we call A elementary. If $|\operatorname{Supp}(A)| = 1$,* *then we call A monomial. We call elementary monomials constants.*

The product of two elementary elements is elementary, and the product of two monomials is a monomial. The converses of these statements are given in Propositions 2.4 and 2.6.

Proposition 2.4. *Let $R[X; S]$ be a semigroup semiring. The following are equivalent*:

1. *For all $A, B \in R[X; S]$, if AB is a monomial then A, B are each monomials.*

2. *S is cancellative.*

Proof. If S is not cancellative, let $a, b, c \in S$ satisfy $a + b = a + c$ and $b \neq c$. Then $(1X^a)(1X^b + 1X^c) = 1X^{a+b} + 1X^{a+c} = 2X^{a+b}$ gives a monomial product, yet $1X^b + 1X^c$ is not a monomial. Conversely, suppose that S is cancellative and B is not a monomial. Let $a \in \operatorname{Supp}(A), b \neq c \in \operatorname{Supp}(B)$. Both $a + b$ and $a + c$ are in $\operatorname{Supp}(AB)$, and $a + b \neq a + c$ since S is cancellative and $b \neq c$. Hence AB is not a monomial.

Proposition 2.5. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. Then* $\operatorname{Supp}(A + B) = \operatorname{Supp}(A) \cup \operatorname{Supp}(B)$ *and $\operatorname{Supp}(AB) = \operatorname{Supp}(A) + \operatorname{Supp}(B)$.*

Proof. Set $C = A + B$. Let $s \in \operatorname{Supp}(C)$. Then $c_s = a_s + b_s$, and since $c_s \neq 0$, either $a_s \neq 0$ $\big($and $s \in \operatorname{Supp}(A)\big)$ or $b_s \neq 0$ $\big($and $s \in \operatorname{Supp}(B)\big)$. Hence $s \in \operatorname{Supp}(A) \cup \operatorname{Supp}(B)$. Now let $s \in \operatorname{Supp}(A) \cup \operatorname{Supp}(B)$. Without loss $s \in \operatorname{Supp}(A)$. We have $c_s = a_s + b_s$. Since $a_s \neq 0$, $c_s \neq 0$ so $s \in \operatorname{Supp}(C)$.

Now, set $D = AB$. Let $s \in \operatorname{Supp}(D)$. Then $d_s = \sum_{u+v=s} a_u b_v$. Since $d_s \neq 0$, some summand corresponding to $u' + v' = s$ is nonzero. Hence $a_{u'}, b_{v'}$ are nonzero, so $u' \in \operatorname{Supp}(A), v' \in \operatorname{Supp}(B)$ and $s = u' + v' \in \operatorname{Supp}(A) + \operatorname{Supp}(B)$. Now let $u + v \in \operatorname{Supp}(A) + \operatorname{Supp}(B)$. By Lemma 1.1, since a_u, b_v are nonzero, $d_{u+v} \neq 0$, and so $u + v \in \operatorname{Supp}(D)$.

Lemma 2.1. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. AB is a constant* *if and only if A, B are.*

Proof. Set $C = AB$. If C is a constant, then $\operatorname{Supp}(C) = \{e\} = \operatorname{Supp}(A) + \operatorname{Supp}(B)$, by Proposition 2.5. Since S is reduced, $\operatorname{Supp}(A) = \operatorname{Supp}(B) = \{e\}$, and hence A, B are constant. The other direction is similar.

Proposition 2.6. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. If $A + B$ is elementary, then at least one of A, B is elementary. If AB is elementary, then both A, B are elementary.*

Proof. The first statement follows from Proposition 2.5. Let $e \in \text{Supp}(AB) = \text{Supp}(A) + \text{Supp}(B)$. By Proposition 2.5 again, there are $a \in \text{Supp}(A)$, $b \in \text{Supp}(B)$ with $a + b = e$. Since S is reduced, $a = b = e$.

Proposition 2.7. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. Suppose that S is cancellative. Then $|\text{Supp}(AB)| \geq \max(|\text{Supp}(A)|, |\text{Supp}(B)|)$, with equality if one of A, B is a monomial.*

Proof. Without loss we assume $|\text{Supp}(A)| \geq |\text{Supp}(B)|$. Let $r \in \text{Supp}(B)$. We have $|\text{Supp}(AB)| = |\text{Supp}(A) + \text{Supp}(B)| \geq |\text{Supp}(A) + \{r\}|$. For $a, b \in \text{Supp}(A)$, if $a + r = b + r$ then $a = b$ since S is cancellative. Therefore $|\text{Supp}(A) + \{r\}| = |\text{Supp}(A)|$. If B is a monomial, then the inequality is an equality.

Corollary 2.1. *Let $R[X; S]$ be a semigroup semiring with S cancellative. Then every divisor of a monomial is again a monomial.*

Theorem 2.1. *Let $R[X; S]$ be a semigroup semiring. The set of units of $R[X; S]$ is $U = \{rX^e : r$ is a unit of $R\}$. In particular, each unit is a constant.*

Proof. By Proposition 2.3, each element of U is a unit in $R[X; S]$. Suppose now that $1 = AB$. By Proposition 2.5, $\text{Supp}(A) + \text{Supp}(B) = \{e\}$. Since S is reduced, $\text{Supp}(A) = \text{Supp}(B) = \{e\}$. Hence $A = aX^e$, $B = bX^e$, and $AB = (ab)X^e$. Hence $A, B \in U$.

Proposition 2.8. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. If AB is elementary, then $(b_e A + a_e B) \mid_+ (AB + (a_e b_e)X^e)$ and $b_e A \mid_+ AB$.*

Proof. Let $s \in \text{Supp}(A)$. By Proposition 2.6, B is elementary and hence $e \in \text{Supp}(B)$. Thus $s = s + e \in \text{Supp}(A) + \text{Supp}(B) = \text{Supp}(AB)$. Set $C = AB$. We have $a_s b_e \mid_+ c_s$. Further, for all $s \neq e$, $a_s b_e + b_s a_e \mid_+ c_s$, while for $s = e$, $a_s b_e = c_s$ so $a_s b_e + a_e b_s = c_s + a_e b_e$.

The following result simplifies the search for divisors of an elementary element, and is the key to finding elementary atoms (as will be seen in Corollary 3.1).

Theorem 2.2. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. If AB is elementary, then $\text{Supp}(A) \cup \text{Supp}(B) \subseteq \text{Supp}(AB)$.*

Proof. Apply Proposition 2.8 to A, B.

Proposition 2.9. *Let $R_1[X; S], R_2[X; S]$ be semigroup semirings, and let $\phi\colon R_1 \to R_2$ be a morphism. Define $\phi'\colon R_1[X; S] \to R_2[X; S]$ via $\phi'\left(\sum a_s X^s\right) = \sum \phi(a_s)X^s$. Then ϕ' is a morphism. Further, if ϕ preserves units, then so does ϕ'.*

Proof. Let $A, B \in R_1[X; S]$. Then

$$\phi'(A + B) = \phi'\left(\sum(a_s + b_s)X^s\right) = \sum \phi(a_s + b_s)X^s =$$

$$= \sum \left(\phi(a_s) + \phi(b_s)\right)X^s = \sum \phi(a_s)X^s + \sum \phi(b_s)X^s = \phi'(A) + \phi'(B),$$

$$\phi'(AB) = \phi'\left(\sum c_s X^s\right) = \sum_{s \in S} \phi(c_s)X^s =$$

$$= \sum_{s \in S} X^s \sum_{u+v=s} \phi(a_u)\phi(b_v) =$$

$$= \sum \phi(a_s)X^s \sum \phi(b_s)X^s = \phi'(A)\phi'(B),$$

$\phi'(0) = \phi'(0X^e) = \phi(0)X^e = 0X^e = 0$, and $\phi'(1) = \phi'(1X^e) = \phi(1)X^e = 1X^e = 1$.

Suppose now that ϕ preserves units. By Proposition 1.3, ϕ' carries units forward. Suppose now that $A \in R_1[X;S]$ and $\phi'(A)$ is a unit. By Theorem 2.1, $\phi'(A) = rX^e = \phi(a_e)X^e$, and $\phi(a_e)$ is a unit in R_2. Since ϕ preserves units, a_e is a unit, and hence $A = a_eX^e$ is a unit.

Definition 2.3. *Let S be a reduced commutative monoid with identity e. We call $\nu \colon S \to \mathbb{N}_0$ a valuation if $\nu(s \cdot t) = \nu(s) + \nu(t)$ for all $s, t \in S$.*

Note that if ν is a valuation then $\nu(e) = \nu(e \cdot e) = \nu(e) + \nu(e)$, so $\nu(e) = 0$. Valuations are useful in our context because of the following.

Proposition 2.10. *Let $R[X;S]$ be a semigroup semiring, let ν be a valuation on S, and let $\rho \in R$. Set $\nu \colon R[X;S] \to R$ via $\nu(A) = \sum_{s \in \mathrm{Supp}(A)} a_s\rho^{\nu(s)}$. Then $\nu \colon R[X;S] \to R$ is a morphism.*

Proof. We have

$$\nu(A+B) = \sum_{s \in \mathrm{Supp}(A+B)} (a_s + b_s)\rho^{\nu(s)} =$$

$$= \sum_{s \in \mathrm{Supp}(A)} a_s\rho^{\nu(s)} + \sum_{s \in \mathrm{Supp}(B)} b_s\rho^{\nu(s)} = \nu(A) + \nu(B),$$

$$\nu(1) = \nu(1X^e) = 1\rho^{\nu(e)} = 1\rho^0 = 1,$$

and $\nu(0)$ is an empty sum so $\nu(0) = 0$,

$$\nu(AB) = \sum_{s \in \mathrm{Supp}(A)+\mathrm{Supp}(B)} \sum_{u+v=s} a_ub_v\rho^{\nu(s)} =$$

$$= \sum_{s \in \mathrm{Supp}(A)+\mathrm{Supp}(B)} \sum_{u+v=s} a_u\rho^{\nu(u)}b_v\rho^{\nu(v)} = \sum_{s \in \mathrm{Supp}(A)} a_u\rho^{\nu(u)} \sum_{s \in \mathrm{Supp}(B)} b_v\rho^{\nu(v)} = \nu(A)\nu(B).$$

Proposition 2.11. *Let $(S, \cdot)$ be a a reduced commutative monoid with identity e. Let $\sigma \in S$ be prime. For all $s \in S$, set $\nu(s) = \sup\{n \colon \sigma^n \mid s\}$. Suppose that the following two conditions hold:*

(1) for all $s \in S$, $\nu(s) \in \mathbb{N}_0$;

(2) for all $s, t \in S$, if $\sigma \cdot s = \sigma \cdot t$ then $s = t$.

The ν is a valuation on S.

Proof. Let $u \cdot v = s$; we write $u = \sigma^{\nu(u)} \cdot u'$, $v = \sigma^{\nu(v)} \cdot v'$ for some $u', v' \in S$. Certainly $\nu(u') = \nu(v') = 0$, by maximality of ν. We have $s = u \cdot v = \sigma^{\nu(u)+\nu(v)} \cdot u' \cdot v'$, so $\nu(s) \geq \nu(u) + \nu(v)$, and we write $s = \sigma^{\nu(u)+\nu(v)} \cdot s' = \sigma^{\nu(u)+\nu(v)} \cdot u' \cdot v'$. By hypothesis (2), $s' = u' \cdot v'$. Since σ is prime, if $\sigma \mid s'$ then $\sigma \mid u'$ or $\sigma \mid v'$, contrary to $\nu(u') = \nu(v') = 0$. Hence $\nu(s') = 0$ and thus $\nu(s) = \nu(u) + \nu(v)$.

Note that if S is BF, then the first condition of Proposition 2.11 holds. If S is cancellative, then the second condition of Proposition 2.11 holds.

***Example* 2.4.** Consider the multiplicative submonoid of the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. It has units $U = \{1, -1\}$. Set $S = (\mathbb{Z}[\sqrt{-5}]/U, \cdot)$, a reduced commutative semigroup with identity $e = [1]$. Set $\sigma = [6 + \sqrt{-5}] \in S$. It is prime since it has norm $36 + 5 = 41$, a rational prime. S is BF and cancellative, hence we define ν as in Proposition 2.11. Consider $\mathbb{N}[X;S]$, the semiring of

multisets from S. Set $A = 1X^e + 2X^\sigma + 3X^{\sigma \cdot \sigma}$. Taking $\rho = 1$, we have $\nu(A) = 6$, which is not helpful. However, if we take $\rho = 2$ we have $\nu(A) = 17$, a rational prime. ν preserves units, since if $\nu(B) = 0$ then $b_s = 0$ for all s. Hence by Proposition 1.3, A is an atom.

Proposition 2.12. *Let S be a reduced commutative semigroup with identity e. For valuations ν_1, ν_2, we define operation $\circ$ via $(\nu_1 \circ \nu_2)(s) = \nu_1(s) + \nu_2(s)$. Under this operation, the set of valuations on S is a nonempty reduced commutative semigroup with identity $\nu_0 \colon S \to \{0\}$.*

Proof. We have $(\nu_1 \circ \nu_2)(s \cdot t) = \nu_1(s \cdot t) + \nu_2(s \cdot t) = \nu_1(s) + \nu_1(t) + \nu_2(s) + \nu_2(t) = (\nu_1(s) + \nu_2(s)) + (\nu_1(t) + \nu_2(t)) = (\nu_1 \circ \nu_2)(s) + (\nu_1 \circ \nu_2)(t)$, so $\nu_1 \circ \nu_2$ is a valuation. $\circ$ is commutative by symmetry. We have $(\nu_0 \circ \nu)(s) = \nu_0(s) + \nu(s) = 0 + \nu(s) = \nu(s)$, so ν_0 is neutral. Lastly, if $\nu_1 \circ \nu_2 = \nu_0$, then $\nu_1(s) + \nu_2(s) = 0$ for all s, but since $\nu_1(s), \nu_2(s) \in \mathbb{N}_0$, $\nu_1(s) = \nu_2(s) = 0$ and $\nu_1 = \nu_2 = \nu_0$.

3. Primitivity and maximal common divisors.

Definition 3.1. *Let $R[X; S]$ be a semigroup semiring, and $A \in R[X; S]$ be nonzero. We call the R-content of A the set $Rc(A) = \{r \in R \colon r \mid a_s \text{ for all } s \in \mathrm{Supp}(A)\}$. We say that A is R-primitive if there is no nonunit in $Rc(A)$. We call the S-content of A the set $Sc(A) = \{t \in S \colon t \mid s \text{ for all } s \in \mathrm{Supp}(A)\}$. We say that A is S-primitive if $Sc(A) = \{e\}$. We say that A is primitive if it is both R-primitive and S-primitive.*

Lemma 3.1. *Let $R[X; S]$ be a semigroup semiring, and let $A \in R[X; S]$ be nonzero. $r \in Rc(A)$ if and only if $rX^e \mid A$. $s \in Sc(A)$ if and only if $1X^s \mid A$.*

Proof. If $r \in Rc(A)$, then for all $s \in \mathrm{Supp}(A)$ we define a'_s via $a_s = ra'_s$. We have $A = \sum_{s \in \mathrm{Supp}(A)} ra'_s X^s = (rX^e) \sum_{s \in \mathrm{Supp}(A)} a'_s X^s$. If $A = (rX^e)B = \sum_{s \in \mathrm{Supp}(B)} rb_s X^s$, so $r \mid a_s$ for all $s \in \mathrm{Supp}(A) = \mathrm{Supp}(B)$ and hence $r \in Rc(A)$.

If $s \in Sc(A)$, then for all $t \in \mathrm{Supp}(A)$ we define t' via $t = s + t'$. We have

$$A = \sum_{t \in \mathrm{Supp}(A)} a_t X^t = \sum_{t' \colon s + t' \in \mathrm{Supp}(A)} a_t X^{s+t'} = (1X^s) \sum_{t' \colon s + t' \in \mathrm{Supp}(A)} a_{s+t'} X^{t'}.$$

Now, if $A = (1X^s)B = \sum_{t \in \mathrm{Supp}(B)} b_t X^{s+t}$, then $\mathrm{Supp}(A) = s + \mathrm{Supp}(B)$, so $s \in Sc(A)$.

Proposition 3.1. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. Then $Rc(A)Rc(B) \subseteq Rc(AB)$, $Rc(A) \cap Rc(B) \subseteq Rc(A + B)$, and $Sc(A) + Sc(B) \subseteq Sc(AB)$.*

Proof. We apply Lemma 3.1 repeatedly. If $d_a \in Rc(A)$, $d_b \in Rc(B)$, then $d_a X^e \mid A$, $d_b X^e \mid B$ and hence $(d_a X^e)(d_b X^e) = (d_a d_b) X^e \mid AB$ so $d_a d_b \in Rc(AB)$. If $d \in Rc(A) \cap Rc(B)$, then $dX^e \mid A$, $dX^e \mid B$ so $A = dX^e A'$, $B = dX^e B'$ and $A + B = dX^e(A' + B')$, so $dX^e \mid (A + B)$ and hence $d \in Rc(A + B)$. If $t_a \in Sc(A)$, $t_b \in Sc(B)$, then $1X^{t_a} \mid A, 1X^{t_b} \mid B$ and hence $(1X^{t_a})(1X^{t_b}) = 1X^{t_a + t_b} \mid AB$ so $t_a + t_b \in Sc(AB)$.

Corollary 3.1. *Let $R[X; S]$ be a semigroup semiring, and let $A, B \in R[X; S]$. If AB is R-primitive (resp. S-primitive), then A and B are each R-primitive (resp. S-primitive).*

Theorem 3.1. *Let $R[X; S]$ be a semigroup semiring, and let $A \in R[X; S]$ be primitive. Let $B \in \mathbb{B}[X; S]$ with $\mathrm{Supp}(A) = \mathrm{Supp}(B)$. Suppose B is an atom. Then A is an atom.*

Proof. Combining Propositions 1.7 and 2.9, we get morphism $\phi \colon R[X; S] \to \mathbb{B}[X; S]$ that maps A to B. Suppose that $A = A_1 A_2$, a product of nonunits. Then $\phi(A) = B = \phi(A_1)\phi(A_2)$. Since B is an atom, without loss $\phi(A_1)$ is a unit. The only unit of $\mathbb{B}[X; S]$ is $1X^e$, and hence $A_1 = rX^e$ for some nonzero r. By Corollary 3.1, A_1 is primitive and thus r is a unit in R. But then A_1 is a unit by Proposition 2.3, which is a contradiction. Hence A is an atom.

Proposition 3.2. *Let $R[X; S]$ be a semigroup semiring. Every elementary element is S-primitive. If S is also yoked, then the opposite implication also holds.*

Proof. Let $A \in R[X; S]$. Suppose that A is elementary, and let $t \in Sc(A)$. $e \in \mathrm{Supp}(A)$ since A is elementary, so $t \mid e$ and $t = e$ since S is reduced. Hence $Sc(A)$ contains no nonunits, and A is S-primitive. Suppose now that S is yoked and A is S-primitive. By Proposition 1.1, $\mid$ is a total preorder on S, hence on $\mathrm{Supp}(A)$. We may therefore choose some $t \in \mathrm{Supp}(A)$ (not necessarily uniquely) that is a common divisor of each element of $\mathrm{Supp}(A)$. Since A is S-primitive, t is a unit. Since S is reduced, $t = e$. Therefore $e \in \mathrm{Supp}(A)$ and A is elementary.

The following result is a major tool for construction of elementary atoms in semigroup semirings. We have no similarly simple construction for primitive non elementary atoms, lacking an analog to Theorem 2.2.

Theorem 3.2. *Let $R[X; S]$ be a semigroup semiring, let $A \in R[X; S]$ be elementary, and set $T = \mathrm{Supp}(A) \setminus \{e\}$. Let $s \in T$ be "maximal" in the sense that for all $t \in T$, $s + t \notin T$. Suppose that for all $u, v \in T$, $u + v \neq s$. Then A is an atom.*

Proof. Suppose otherwise, that $A = BC$, a product of nonunits. We first prove that B is not a monomial. Suppose otherwise, that $B = bX^t$. We have $b \in Rc(A), t \in Sc(A)$. Since A is elementary, by Proposition 3.2, A is primitive and so b, t are units, and by Proposition 2.3, B is a unit, contrary to hypothesis. Hence B (and, similarly, C) is not a monomial. Since $s \in \mathrm{Supp}(A)$, by Proposition 2.5 there are $u \in \mathrm{Supp}(B)$, $v \in \mathrm{Supp}(C)$ with $u + v = s$. If $u = e$, then $s \in \mathrm{Supp}(C)$. Choose any $u' \in \mathrm{Supp}(B) \setminus \{e\}$, which is nonempty since B is not a monomial. Then $u' + v = u' + s \in T$, which contradicts the "maximality" of s. Hence $u \neq e$, and similarly $v \neq e$. Now by Theorem 2.2, $u, v \in T$ and $u + v = s$. This contradicts hypothesis, and hence A is an atom.

Example 3.1. Consider $R[X; \mathbb{N}_0]$, which are polynomials and admit a degree. Let $A \in R[X; \mathbb{N}_0]$ be elementary with $\deg(A) = n$. Suppose that either $\left[1, \dfrac{n}{2}\right]$ or $\left[\dfrac{n}{2}, n-1\right]$ has no intersection with $\mathrm{Supp}(A)$. Taking $s = n$ in Theorem 3.2, we conclude that A is an atom.

The following is derived from an example in [14].

Proposition 3.3. *Let $R[X; S]$ be a semigroup semiring. Suppose that $1, 2(= 1 + 1), 3$ are pairwise distinct in R. Suppose further that there is some $s \in S$ with $s, 2s(= s + s), \ldots, 12s$ all distinct. Then the elasticity of $R[X; S]$ is at least $3/2$. In particular, $R[X; S]$ is not UF.*

Proof. Note that $X^e + X^s + X^{2s} + X^{3s} + 2X^{4s} + 2X^{5s} + 2X^{6s} + 3X^{7s} + X^{8s} + X^{9s} + X^{10s} = AB = CDE$, for $A = X^e + X^{3s} + X^{5s} + X^{6s}$, $B = X^e + X^s + X^{2s} + X^{4s}$, $C = X^e + X^s$, $D = X^e + X^{2s}$, $E = X^e + 2X^{4s} + X^{7s}$. C, D, E are all atoms by Theorem 3.2. If A were not an atom, we write $A = A_1 A_2$, and applying Proposition 2.2 we get $\mathrm{Supp}(A_1) \cup \mathrm{Supp}(A_2) \subseteq \mathrm{Supp}(A) = \{e, 3s, 5s, 6s\}$. Within this set $5s + e$ is the only factorization of $5s$. Hence without loss we assume that $5s \in \mathrm{Supp}(A_1)$, $e \in \mathrm{Supp}(A_2)$. But now $\mathrm{Supp}(A_2) = \{e\}$ else $\mathrm{Supp}(A) \neq \{e, 3s, 5s, 6s\}$. Hence $A_2 = uX^e$ and $A_1 = aX^e + bX^{3s} + cX^{5s} + dX^{6s}$. Since $ua = 1$, u is a unit in R, and hence A_2 is a unit in $R[X; S]$. By a similar argument, if B is not an atom, then $B = (aX^e + bX^s + cX^{2s})(a'X^e + b'X^s + c'X^{2s})$. So $aa' = 1$, $ab' + ba' = 1$, $ac' + bb' + ca' = 1$, $bc' + cb' = 0$, $cc' = 1$. So a, a', c, c' are units. But $bc' = 0$ and $cb' = 0$, so $b = b' = 0$ and hence $ab' + ba' = 0$, a contradiction.

Proposition 3.4. *Let $R[X; S]$ be a semigroup semiring. Suppose there is some $r \in R^*$ with $r + r = rr = r$. Suppose there is some $s \in S$ with $s, 2s, 3s, \ldots$ all distinct. Then $R[X; S]$ has infinite elasticity. Further, if there is some prime $P \in R[X; S]$, then $R[X; S]$ is fully elastic.*

Proof. Let $n \in \mathbb{N}$. Set $A = 1X^e + rX^s$, $B = 1X^e + rX^s + rX^{2s} + \ldots + rX^{ns} + rX^{(2n+1)s}$, $C = 1X^e + rX^{(n+1)s} + rX^{(n+2)s} + \ldots + rX^{(2n+1)s}$. By Theorem 3.2, A, B, C are each atoms. We have $BC = 1X^e + rX^s + rX^{2s} + \ldots + rX^{(4n+2)s} = A^{4n+2}$, hence $\rho(R[X; S]) \geq \dfrac{4n+2}{2} = 2n+1$, so $\rho(R[X; S]) = \infty$. Now, let $\dfrac{p}{q} \geq 1$. If $p = q$ we have $\rho(P) = \dfrac{p}{q}$, otherwise we take $n = p - q$ and consider $BCP^{4q-2} = A^{4n+2}P^{4q-2}$. We have $\rho(BCP^{4q-2}) = \dfrac{4(p-q) + 2 + 4q - 2}{2 + 4q - 2} = \dfrac{p}{q}$.

Note that an r such as in Proposition 3.4 may be appended to any semiring R, defining $x + r = xr = r$ for all nonzero $x \in R$. Further, in [2] it is shown that $\mathbb{N}_0[X; \mathbb{N}_0]$ has infinite elasticity. Hence even for these very well-behaved R, S (cancellative, reduced, UF, greatest common divisors, totally ordered), the resulting semigroup semiring has infinite elasticity.

At the other extreme, if $|S| = 1$ then we call $R[X; S]$ *trivial*. Then the natural embedding $\phi \colon R[X; S] \to R$ is bijective, so by Proposition 1.4, $R[X; S]$ inherits the properties of R, such as elasticity and UF.

The evidence collected above and in Propositions 3.3 and 3.4 leads us to the following conjecture. It stands in contrast to the (semi)group ring case, where UF is achievable (e.g., $D[X]$ for any unique factorization domain D).

Conjecture 3.1. *All nontrivial atomic semigroup semirings have infinite elasticity. In particular, no semigroup semiring is UF.*

Proposition 3.5. *Let $R[X; S]$ be a semigroup semiring. $1X^s$ is an atom in $R[X; S]$ if and only if s is an atom in S. $1X^s$ is prime in $R[X; S]$ if and only if s is prime in S.*

Proof. Suppose $s = r + t$, for nonzero $r, t \in S$. Then $1X^s = (1X^r)(1X^t)$, a product of nonunits by Theorem 2.1. Suppose now that $1X^s = AB$, for nonunits A, B. If $\text{Supp}(A) = \{e\}$, then a_e is a nonunit in R by Theorem 2.1. However, $a_e \in Rc(AB)$ by Proposition 3.1, hence $a_e \mid 1$, a contradiction. Hence there is some $t \in \text{Supp}(A)$ with $t \neq e$. Similarly, there is some $r \in \text{Supp}(B)$ with $r \neq e$. By Proposition 2.5, $r + t \in \text{Supp}(AB) = \{s\}$, and hence $r + t = s$. Therefore s is not an atom in S.

Suppose now that $1X^s$ is prime in $R[X; S]$, and there are $a, b, c \in S$ with $a + s = b + c$. Then $(1X^a)(1X^s) = (1X^b)(1X^c)$, and since $1X^s$ is prime, then without loss there is some $A \in R[X; S]$ with $A(1X^s) = 1X^b$. Then for all $t \in \text{Supp}(A)$, $t + s = b$, so in particular $s \mid b$. Hence s is prime in S. Suppose next that s is prime in S, and that there are $A, B, C \in R[X; S]$ with $A(1X^s) = BC$. Suppose there are $u \in \text{Supp}(B)$, $v \in \text{Supp}(C)$ with $s \nmid u$ and $s \nmid v$. But then $u + v \in \text{Supp}(BC) = \text{Supp}(A) + s$, so $s \mid u + v$ yet $s \nmid u$, $s \nmid v$, which contradicts the primality of S. Hence either $s \in Sc(B)$ or $s \in Sc(C)$ and hence $1X^s \mid B$ or $1X^s \mid C$, and so $1X^s$ is prime.

Proposition 3.6. *Let $R[X; S]$ be a semigroup semiring. Let $A = aX^s$ be an arbitrary monomial. A is an atom if exactly one of the following holds*:

(1) *a is an atom in R, and $s = e$*

or

(2) *a is a unit in R, and s is an atom in S.*

Proof. One direction is given by Propositions 2.3 and 3.5. If neither a nor s is a unit, then we write $A = (aX^e)(1X^s)$, a product of nonunits. Hence if A is an atom either a or s is a unit; then by Propositions 2.3 and 3.5 again, one of the above must hold.

Proposition 3.7. *Let $R[X; S]$ be a semigroup semiring. Let $r, r' \in R$, $s, s' \in S$. Monomials rX^s, $r'X^{s'}$ are associates in $R[X; S]$ if and only if*

(1) r, r' are associates in R, and

(2) s, s' are associates in S.

Proof. Suppose first (1) + (2). Choose $r'' \in R$, $s'' \in S$ with $r = r'r''$, $s = s's''$. We have $rX^s = (r'X^{s'})(r''X^{s''})$; hence $rX^s \mid r'X^{s'}$. Repeating in the other direction proves (1) and (2).

Suppose now $rX^s, r'X^{s'}$ are associates. Choose $A \in R[X; S]$ with $rX^s A = r'X^{s'}$. Then $(rX^e)(1X^s)A = r'X^{s'}$, so by Lemma 3.1, (1) $r \in Rc(r'X^{s'})$ so $r \mid r'$, and (2) $s \in Sc(r'X^{s'})$ so $s \mid s'$. Repeating in the other direction proves (1) and (2).

Proposition 3.8. *Let $R[X; S]$ be a semigroup semiring, with R, S atomic. If all monomials of $R[X; S]$ have UF/FF/BF, then R, S are also UF/FF/BF. If S is also cancellative, then the opposite implication also holds.*

Proof. Consider monomial rX^s. By Proposition 3.6, we may reorder any factorization of rX^s into monomials canonically, as $(r_1X^e)(r_2X^e)\ldots(r_kX^e)$ $(1X^{s_1})(1X^{s_2})\ldots(1X^{s_j})$, where $r_1r_2\ldots r_k$ is a factorization of r and $s_1 + s_2 + \ldots + s_j$ is a factorization of s. By Proposition 3.7, two such factorizations are equivalent in $R[X; S]$ if and only if the corresponding factorizations are each equivalent in R, S. Hence the set of factorizations of rX^s into monomials is UF/FF/BF, if and only if the same conditions hold on both factorizations of r, s. This gives one direction, since if all factorizations of rX^s are UF/FF/BF then surely all factorizations into monomials are. If S is cancellative, then by Proposition 2.4, all factorizations of rX^s are into monomials, which gives the other direction.

Proposition 3.9. *Let $R[X; S]$ be a semigroup semiring, and let $A \in R[X; S]$. If A is an atom then either A is a monomial or primitive.*

Proof. Suppose otherwise. If A is not R-primitive, there is some nonunit $r \in Rc(A)$, and by Lemma 3.1, we write $A = (rX^e)B$. If instead A is not S-primitive, there is some nonunit $t \in Sc(A)$ and by Lemma 3.1, we write $A = (1X^t)B$. In both cases, B is a nonunit by Theorem 2.1 since $|\operatorname{Supp}(B)| = |\operatorname{Supp}(A)|$, which is greater than 1. Hence we have factored A into two nonunits, which contradicts the hypothesis.

Hence, every atomic factorization of $A \in R[X; S]$ is the product of monomial atoms (whose product may or may not be a monomial) and the product of primitive atoms (whose product may or may not be primitive). The former can be resolved by Corollary 2.1, and the latter by Theorem 3.11.

However another approach to factoring A into atoms is to first factor A into a monomial (each factor of which must be monomial) times a primitive element (each factor of which must be primitive). Then, we factor each part into atoms. We take this approach, with a sequence of results leading up to Theorem 3.6, which gives sufficient conditions for $R[X; S]$ to be atomic.

Definition 3.2. *Given monoid $(M, \cdot)$, suppose that for each finite set $S \subseteq M$, there is some d that satisfies the following*:

(1) *for all $s \in S$, $d \mid s$*;

(2) *if there is some d' with $d \mid d'$ and $d' \mid s$ (for all $s \in S$), then d, d' are associates.*

In this case we say that $(M, \cdot)$ has maximal common divisors.

In the ring theoretic context, maximal common divisors have been considered in [1, 11]. Every FF monoid has maximal common divisors. A monoid may have maximal common divisors but no greatest common divisors, as shown by the following.

Example 3.2. Consider the numerical monoid $(M, +)$ for $M = \{0, 3, 4, 5, 6, \ldots\}$. For $S = \{9, 10\}$, the set of common divisors is $\{0, 3, 4, 5, 6\}$, and the set of maximal common divisors is $\{4, 5, 6\}$. There is no greatest common divisor of S.

Theorem 3.3. *Let $R[X; S]$ be a semigroup semiring, where R and S each have maximal common divisors and are weakly cancellative. Let $A \in R[X; S]$. Then we may write $A = BC$, where B is monomial and C is primitive.*

Proof. Let b be a maximal common divisor of $\{a_s : s \in \operatorname{Supp}(A)\}$, and let t be a maximal common divisor of $\operatorname{Supp}(A)$. Set $B = bX^t$, and $C = \sum_{s \in \operatorname{Supp}(A)} (a_s/b)X^{(s-t)}$. Evidently $A = BC$ and B is a monomial; it remains to prove that C is primitive. Suppose d is a common divisor of $\{c_s : s \in \operatorname{Supp}(C)\}$. But then bd is a common divisor of $\{a_s : s \in \operatorname{Supp}(A)\}$. Since b is maximal, in fact $b = bde$ for some unit e; hence d is a unit by weak cancellativity of R. Hence C is R-primitive. Suppose now that r is a common divisor of $\operatorname{Supp}(C)$. But then $r+t$ is a common divisor of $\operatorname{Supp}(A)$. Since t is maximal, in fact $t = t + r + e$ for some unit e; hence r is a unit by weak cancellativity of S. Hence C is S-primitive, and thus primitive.

Theorem 3.4. *Let $R[X; S]$ be a semigroup semiring, where R and S are each atomic. Let $A \in R[X; S]$ be a monomial. Then we may write A as a product of monomial atoms. Further, if both R, S are UF/FF/BF, then so is A.*

Proof. Let $A = aX^s$. We factor into atoms $a = a_1 a_2 \ldots a_m$ and also $s = s_1 + s_2 + \ldots \ldots + s_n$. By Proposition 3.6, we have a factorization of A into $k = m + n$ atoms given by $(a_1 X^e)(a_2 X^e) \ldots (a_m X^e)(1X^{s_1})(1X^{s_2}) \ldots (1X^{s_n})$. On the other hand, if $A = A_1 A_2 \ldots A_k$, then by Proposition 3.6, for some $m + n = k$ this corresponds to a factorization of a into m atoms, and a factorization of s into n atoms. Hence $|F(A)| \leq |F(a)|\,|F(s)|$ and $\sup \mathcal{L}(A) \leq \sup \mathcal{L}(a) + \sup \mathcal{L}(s)$.

Note that if S is also cancellative, Corollary 2.1 provides a partial converse to Theorem 3.4: all factorizations of a monomial are into other monomials.

The following surprising theorem gives a factorization of any primitive element into a bounded number of atoms, even if R, S are not BF or atomic themselves.

Theorem 3.5. *Let $R[X; S]$ be a semigroup semiring, with S cancellative. Let $A \in R[X; S]$ be a primitive nonunit. Then we may write A as a product of k primitive atoms, for some $k \leq 2^{|\operatorname{Supp}(A)|}$.*

Proof. The proof is by induction on $|\operatorname{Supp}(A)|$. If $|\operatorname{Supp}(A)| = 1$, then A is a primitive monomial, hence a unit by Proposition 2.3, which is contrary to hypothesis. Now suppose that $|\operatorname{Supp}(A)| > 1$. If A is an atom, there is nothing to prove. If not, write $A = BC$ for nonunits B, C. By Corollary 3.1, both B and C are primitive. If either were a monomial, then again by Proposition 2.3 it would be a unit, contrary to supposition. By Proposition 2.7, $|\operatorname{Supp}(A)| \geq \geq |\operatorname{Supp}(B)|$ and $|\operatorname{Supp}(A)| \geq |\operatorname{Supp}(C)|$. We now prove that these inequalities are strict. Suppose that instead $|\operatorname{Supp}(B) + \operatorname{Supp}(C)| = |\operatorname{Supp}(A)| = |\operatorname{Supp}(B)|$. Let $c \in \operatorname{Supp}(C) \setminus \{e\}$; we must have $\operatorname{Supp}(B) + \{c\} = \operatorname{Supp}(B) + \operatorname{Supp}(C)$. For all $a \in \operatorname{Supp}(A)$, we write $a = u + v$ for some $u \in \operatorname{Supp}(B)$, $v \in \operatorname{Supp}(C)$. Since $u + v \in \operatorname{Supp}(A) = \operatorname{Supp}(B) + \{c\}$, there is some $u' \in \operatorname{Supp}(B)$ with $a = u' + c$. Therefore $c \in Sc(A)$, contradicting the primitivity of A. Hence $|\operatorname{Supp}(A)| > |\operatorname{Supp}(B)|$ and similarly $|\operatorname{Supp}(A)| > |\operatorname{Supp}(C)|$. The inductive hypothesis now gives us two factorizations into primitive atoms $B = B_1 B_2 \ldots B_m$, $C = C_1 C_2 \ldots C_n$. Combining and setting $k = m + n$, we have $A = B_1 B_2 \ldots B_m C_1 C_2 \ldots C_n$. By the inductive hypothesis $m \leq 2^{|\operatorname{Supp}(B)|} \leq 2^{|\operatorname{Supp}(A)|-1}$ and also $n \leq 2^{|\operatorname{Supp}(A)|-1}$ so $k = m + n \leq 2^{|\operatorname{Supp}(A)|}$.

Theorem 3.6 provides sufficient conditions for semigroup semiring $R[X; S]$ to be atomic, and also BF. UF was addressed in Conjecture 3.1, while FF requires some machinery and will be addressed in Theorem 3.7.

Theorem 3.6. *Suppose that R, S are atomic and have maximal common divisors. Suppose that R is weakly cancellative, and S is cancellative. Then semigroup semiring $R[X; S]$ is atomic. Further, if R, S are each BF, then so is $R[X; S]$.*

Proof. We first factor $A \in R[X; S]$ into monomial and primitive parts with Theorem 3.3, then factor each part into atoms with Theorem 3.4 and Theorem 3.5, respectively.

Definition 3.3. *Let $(M, \cdot)$ be a commutative monoid. Suppose that M admits a total order $\geq$ with least element e that respects $\cdot$. Suppose further that M does not contain any infinite descending chain $s_1 > s_2 > \ldots$. We then call M well-ordered. For semiring R, if $(R, +)$ is well-ordered, and also $\geq$ respects $\times$, then we call R well-ordered.*

Well-ordered semigroups are characterized in [12]. A well-ordering on R yields a natural partial ordering on $R[X; S]$ via $A \geq B$ if $a_s \geq b_s$ for all $s \in S$.

Let R be a well-ordered semiring, and let $r \in R$. Then there are finitely many $r' \in R$ with $r' \mid_+ r$.

Theorem 3.7. *Let $R[X; S]$ be a BF semigroup semiring. Suppose that R is well-ordered, $(R, +)$ is FF, and S is cancellative, yoked, and FF. Then $R[X; S]$ is FF.*

Proof. Let $A \in R[X; S]$. Suppose we have factorization set $F(A)$ with $|F(A)| = \infty$. By Proposition 3.9, either infinitely many nonassociate monomial atoms divide A, or infinitely many nonassociate primitive atoms divide A. In the first case, by Proposition 3.6, either R or S lacks FF. We therefore suppose the second case. By Proposition 3.2, A is elementary, and by Proposition 2.8 if $B \mid A$ then there is some constant $c \in R$ with $cB \mid_+ A$. Since $(R, +)$ is FF, there are only finitely many $r \in R$ with $r \mid_+ a_s$ for each $s \in \mathrm{Supp}(A)$. Since there are infinitely many nonassociate B dividing A, we may construct $c_1, c_2, \ldots \in R$ and nonassociate $B_1, B_2, \ldots$ such that $B_i \mid A$ and $c_1 B_1 = c_2 B_2 = \ldots$. If some $c_i = c_j$, then $B_i = B_j$, contrary to hypothesis. Because $\geq$ is a well-ordering, $c_1 > c_2 > \ldots$ is impossible, hence we assume without loss that $c_1 < c_2 < \ldots$. Let $s \in \mathrm{Supp}(B_1)$, and set $b_i = (B_i)_s$. We have $c_1 b_1 = c_2 b_2 = \ldots$. If $b_1 \leq b_2$ then $c_1 b_1 < c_2 b_1 \leq c_2 b_2$, a contradiction. Hence $b_1 > b_2 > \ldots$, which contradicts the well-ordering of R.

The gap between Theorems 3.6, 3.7, and the following partial converse remains open. Note also Conjecture 3.1.

Theorem 3.8. *Suppose that $R[X; S]$ is an atomic semigroup semiring. Then R, S are atomic. Further, if $R[X; S]$ is UF/FF/BF, then so are R, S.*

Proof. Propositions 2.3 and 3.8.

We turn now toward a semiring analog of the Gauss lemma on primitive polynomials. Note that this does not directly generalize Gauss lemma since semigroup semirings as we define them are information algebras (hence cannot be rings). In Theorem 3.11 we present the desired result, but first we need some machinery.

Proposition 3.10. *Let $(M, \cdot)$ be a commutative monoid with UF. Then $(M, \cdot)$ has greatest common divisors. Further, if $X, Y \subseteq M$ are nonempty and finite, then $\gcd(X \cdot Y) = \gcd(X) \cdot \gcd(Y)$, up to associates.*

Proof. Let $S \subseteq M$ be finite. Choose a factorization of $\prod S$, and let Q be the finite set of primes from this factorization. Choose $P \subseteq Q$ so that each $q \in Q$ has some associate $p \in P$, but the elements of P are pairwise nonassociate. By UF, any prime from any factorization of an element of S is associate to some element of Q, hence some element of P. Hence for each $s \in S$ we have a unique associated prime factorization $\prod_{p \in P} p^{\nu(p)}$, where $\nu(p) \in \mathbb{N}_0$.

We claim that $d \mid s$ if and only if d is associated to some $\prod_{p \in P} p^{\gamma(p)}$, where $0 \leq \gamma(p) \leq \nu(p)$. If d is associated to an element of this form, then s is associated to $d \prod_{p \in P} p^{\nu(p)-\gamma(p)}$, so $d \mid s$.

Suppose that $d \mid s$. If some prime divides d that is not associate to any prime in P, that prime divides $\prod S$, which contradicts the UF property. Hence d is associated to $\prod_{p \in P} p^{\gamma(p)}$, where $\gamma(p) \in \mathbb{N}_0$. Suppose that $\gamma(p) > \nu(p)$ for some p. Then $p^{\gamma(p)} \mid s$, so we write $s = p^{\gamma(p)}a$, for some $a \in M$. But this contradicts UF, since any factorization of $p^{\gamma(p)}a$ must have at least $\gamma(p)$ primes associate to p, and so p is associate to some other element of P. Now, set $\mu(p) = \min_{s \in S}\{\nu(p)\}$, $d = \prod_{p \in P} p^{\mu(p)}$. By the above, d is a common divisor for S, and if d' is any other divisor of s, then $d' \mid d$.

Next, for $S = X \cup Y$, we set $\mu_X(p) = \min_{s \in X}\{\nu(p)\}$, $\mu_Y(p) = \min_{s \in Y}\{\nu(p)\}$, $\mu_{X \cdot Y}(p) = {} = \min_{s \in X \cdot Y}\{\nu(p)\}$. Choose $x \in X$ with $x = p^{\mu_X(p)}x'$ and $\nu(x') = 0$, and $y \in Y$ with $y = p^{\mu_Y(p)}y'$ and $\nu(y') = 0$. We have $p^{\mu_X(p) + \mu_Y(p)} \mid xy$, so $\mu_{X \cdot Y}(p) \geq \mu_X(p) + \mu_Y(p)$. Suppose that $p^s \mid xy$ with $s > \mu_X(p) + \mu_Y(p)$. We write $p^s \mid p^{\mu_X(p) + \mu_Y(p)}x'y'$. But now, by UF, $p \mid x'y'$ and so $p \mid x'$ or $p \mid y'$, which contradicts $\nu(x') = \nu(y') = 0$. Hence $\mu_{X \cdot Y}(p) = \mu_X(p) + \mu_Y(p)$ and hence $\prod_{p \in P} p^{\mu_{X \cdot Y}(p)} = \prod_{p \in P} p^{\mu_X(p)} \cdot \prod_{p \in P} p^{\mu_Y(p)}$. Each element of $\gcd(X \cdot Y)$ is associated to this product, as is each element of $\gcd(X) \cdot \gcd(Y)$.

The following is an Sc-analog of the Gauss lemma on primitive polynomials.

Theorem 3.9. *Let $R[X; S]$ be a semigroup semiring. Suppose that S has UF. Then $Sc(AB) = {} = Sc(A) + Sc(B)$. In particular, if A, B are both S-primitive, then AB is S-primitive.*

Proof. $\gcd(\mathrm{Supp}(AB)) = \gcd(\mathrm{Supp}(A) + \mathrm{Supp}(B))$ by Proposition 2.5. By Proposition 3.10, this is associate to $\gcd(\mathrm{Supp}(A)) + \gcd(\mathrm{Supp}(B))$. If $c \in Sc(AB)$, then c divides each element of $\mathrm{Supp}(AB)$, hence $c \mid \gcd(\mathrm{Supp}(AB)) = \gcd(\mathrm{Supp}(A)) + \gcd(\mathrm{Supp}(B))$. Hence there is some $a \in \gcd(\mathrm{Supp}(A))$, $b \in \gcd(\mathrm{Supp}(B))$ with $c \mid a + b$ and hence $c \in Sc(A) + Sc(B)$. On the other hand, if $a \in Sc(A), b \in Sc(B)$, then $a + b$ divides each element of $\mathrm{Supp}(AB)$, hence $a + b \in Sc(AB)$.

Definition 3.4. *Let R be a semiring. Following [10], we call R a PLIS-semiring if the following property holds: For all $a, b \in R$, if d is a common divisor of a, $a + b$, then d is a divisor of b.*

Note that every ring is a PLIS-semiring. The following lemma extends Proposition 3.1, for PLIS-semirings.

Lemma 3.2. *Let $R[X; S]$ be a semigroup semiring, where R is a PLIS-semiring. Let $A, B \in {} \in R[X; S]$. Then $Rc(A) \cap Rc(A + B) \subseteq Rc(B)$.*

Proof. Let $d \in Rc(A) \cap Rc(A + B)$. Hence, for each $s \in S$, we have $d \mid a_s$, $d \mid (a_s + b_s)$. Because R is a PLIS-semiring, $d \mid b_s$; hence $d \in Rc(B)$.

Definition 3.5. *Let $R[X; S]$ be a semigroup semiring. Suppose that S is well-ordered. We define the degree function, $\deg \colon R[X; S] \to S$ via $\deg(A) = \max\{s \colon s \in \mathrm{Supp}(A)\}$.*

We now present an Rc-analog of the Gauss lemma on primitive polynomials.

Theorem 3.10. *Let $R[X; S]$ be a semigroup semiring. Suppose that R is a UF PLIS-semiring, and S is well-ordered. Then $Rc(AB) = Rc(A)Rc(B)$. In particular, if A, B are both R-primitive, then AB is R-primitive.*

Proof. If A, B are not R-primitive, we choose a to be a greatest common divisor of $Rc(A)$, b to be a greatest common divisor of $Rc(B)$. By Lemma 3.1 we consider $A/(aX^e)$, $B/(bX^e)$. We claim that these are each R-primitive; suppose $d \in Rc(A/(aX^e))$. But then $da \in Rc(A)$, and hence $da \mid a$. By unique factorization, d is a unit. Applying the theorem to R-primitive $A/(aX^e)$, $B/(bX^e)$, we conclude that $AB/(abX^e)$ is R-primitive, and hence $Rc(AB) = Rc(A)Rc(B)$.

We assume henceforth that A, B are R-primitive. Set $C = AB$. The proof proceeds by recursion on $\deg(C)$. If $\deg(C) = e$, then C is a constant. By Proposition 2.6, A, B are also constants and hence $Rc(C) = Rc(A)Rc(B)$. If either A or B is a monomial, then again $Rc(C) = Rc(A)Rc(B)$.

Suppose $\deg(C) > e$, and some nonunit $r \in Rc(C)$. Since R has UF, we choose prime p dividing r. Let $u \in \operatorname{Supp}(A)$, $v \in \operatorname{Supp}(B)$. We have $\deg(A) + \deg(B) \geq \deg(A) + v \geq u + v$, with equality only if $\deg(A) = u$, $\deg(B) = v$. Hence $c_{\deg(C)} = a_{\deg(A)} b_{\deg(B)}$. Since $p \mid c_{\deg(C)}$ and p is prime, without loss we may assume that $p \mid a_{\deg(A)}$. Set $A' = \sum_{s \in \operatorname{Supp}(A) \setminus \{\deg(A)\}} a_s X^s$, $A'' = a_{\deg(A)} X^{\deg(A)}$. These are each nontrivial since A is not a monomial. We have $p \in Rc(A'') = Rc(A'')\{1\} \subseteq Rc(A''B)$. But also $p \in Rc(C) = Rc(A'B + A''B)$, so by Lemma 3.2, $p \in Rc(A'B)$.

But now we have $A', B, A'B$ with $\deg(C) > \deg(A'B)$. We continue recursively; however since S is well-ordered there cannot be an infinite descending chain. Hence we may assume by recursion that $Rc(A'B) = Rc(A')Rc(B) = Rc(A')$. We have $p \in Rc(A') \cap Rc(A'') \subseteq Rc(A' + A'') = Rc(A)$, which contradicts the R-primitivity of A.

Theorem 3.11. *Let $R[X; S]$ be a semigroup semiring. Suppose that R is a UF PLIS-semiring, and S is UF and well-ordered. Then $Rc(AB) = Rc(A)Rc(B)$ and $Sc(AB) = Sc(A) + Sc(B)$. In particular, if A, B are both primitive, then AB is primitive.*

Proof. Combine Theorems 3.9 and 3.10.

1. *Anderson D. D.* GCD domains, Gauss' lemma, and contents of polynomials, non-Noetherian commutative ring theory // Math. Appl. – 2000. – **520**. – P. 1 – 31.
2. *Cesarz Patrick, Chapman S. T., Stephen McAdam, Schaeffer George J.* Elastic properties of some semirings defined by positive systems // Commut. Algebra and Appl. – Berlin: Walter de Gruyter, 2009. – P. 89 – 101.
3. *Charles Ching-an Cheng, Wong Roman W.* Hereditary monoid rings // Amer. J. Math. – 1982. – **104**, № 5. – P. 935 – 942.
4. *Duchamp G., Thibon J.-Y.* Théorèmes de transfert pour les polynômes partiellement commutatifs // Theor. and Comput. Sci. – 1988. – **57**, № 2-3. – P. 239 – 249.
5. *Gallagher Peter.* In the finite and non-finite generation of finitary power semigroups // Semigroup Forum. – 2005. – **71**, № 3. – P. 481 – 494.
6. *Geroldinger A., Halter-Koch F.* Non-unique factorizations // Pure and Appl. Math. – Boca Raton, FL: Chapman & Hall/CRC, 2006. – **278**.
7. *Giambruno A., César Polcino Milies, Sudarshan K. Sehgal (eds.)* Groups, rings and group rings // Contemp. Math. – Providence, RI: Amer. Math. Soc., 2009. – **499**.
8. *Gilmer R.* Commutative semigroup rings // Chicago Lect. Math. – Chicago, IL: Univ. Chicago Press, 1984.
9. *Golan J. S.* The theory of semirings with applications in mathematics and theoretical computer science // Pitman Monogr. and Surv. in Pure and Appl. Math. – Harlow: Longman Sci. & Techn., 1992. – **54**.
10. *Golan J. S.* Semirings and affine equations over them: theory and applications // Math. and Appl. – 2003. – **556**.
11. *Halter-Koch F.* Ideal systems // Monogr. and Textbooks in Pure and Appll. Math. – New York: Marcel Dekker Inc., 1998. – **211**.
12. *Révész G.* When is a total ordering of a semigroup a well-ordering? // Semigroup Forum. – 1990. – **41**, № 1. – P. 123 – 126.
13. *Schwarz S.* Powers of subsets in a finite semigroup // Semigroup Forum. – 1995. – **51**, № 1. – P. 1 – 22.
14. *van de Woestijne Ch. E.* Factors of disconnected graphs and polynomials with nonnegative integer coefficients (to appear).
15. *Weinert H. J.* On 0-simple semirings, semigroup semirings and two kinds of division semirings // Semigroup Forum. – 1984. – **28**, № 1-3. – P. 313 – 333.