Decompositions of commutative monoid
congruences and binomial ideals

Thomas Kahle and Ezra Miller

Decompositions of commutative monoid congruences and binomial ideals

Thomas Kahle and Ezra Miller

Primary decomposition of commutative monoid congruences is insensitive to certain features of primary decomposition in commutative rings. These features are captured by the more refined theory of *mesoprimary decomposition* of congruences, introduced here complete with witnesses and associated prime objects. The combinatorial theory of mesoprimary decomposition lifts to arbitrary binomial ideals in monoid algebras. The resulting *binomial mesoprimary decomposition* is a new type of intersection decomposition for binomial ideals that enjoys computational efficiency and independence from ground field hypotheses. Binomial primary decompositions are easily recovered from mesoprimary decomposition.

1. Introduction

Overview. Primary decomposition of ideals and modules has been a mainstay of commutative algebra since Emmy Noether's unification of scattered results [1921]. A formally analogous theory for congruences on commutative monoids made its first appearance in [Drbohlav 1963], and subsequently the topic of decompositions has similarly played a central role in commutative semigroup theory [Grillet 2001]. Our first goal is to demonstrate that the formal analogy in the setting of finitely generated monoids and congruences — the *combinatorial setting* — fails to capture the essence of primary decomposition in noetherian rings and modules. We justify this claim, and rectify it, by exhibiting a more sensitive theory of *mesoprimary decomposition* of congruences, complete with witnesses, associated prime objects, and other facets of control afforded in parallel with primary decomposition in rings. We then proceed beyond formal analogy by lifting our witnessed theory of mesoprimary decomposition to the *arithmetic setting* of binomial ideals in semigroup rings, at the interface of commutative ring theory with finitely generated monoids.

Mesoprimary decomposition of binomial ideals is not binomial primary decomposition, but a new type of intersection decomposition for binomial ideals, with numerous advantages over ordinary primary decomposition, such as combinatorial clarity, independence from properties of the ground field, and computational efficiency. Nevertheless, binomial primary decomposition is easily recovered from mesoprimary decomposition. In essence, by lifting mesoprimary decomposition of congruences, binomial mesoprimary decomposition distills the coefficient-free combinatorics inherent in primary decomposition of binomial ideals and isolates the precise manner in which coefficients subsequently determine the primary components. The subtlety of coefficient arithmetic causes the lifting procedure to fail verbatim translation, particularly where redundancy is involved. Part of our study therefore contrasts the slightly different notions of witness and associatedness in the combinatorial and arithmetic settings.

General motivation. The need for natural decompositions in the monoid and binomial contexts has become increasingly important in recent years, in view of appearances and applications in numerous areas. Some of these directly involve commutative monoids, such as schemes over $\mathbb{F}_1$ [Connes and Consani 2011; Deitmar 2005], where monoids form the foundation just as rings do for usual schemes. Another instance is the arrival of misère quotients in combinatorial game theory, where monoids provide data structures for recording and computing winning strategies [Plambeck 2005; Plambeck and Siegel 2008] (see also [Miller 2011] for an algebraic introduction). At the same time, binomial ideals interact with other parts of mathematics and the sciences, motivating research into applicable descriptions of their decompositions. For example, dynamics of mass-action kinetics, where

steady states in detailed-balanced cases are described by vanishing of binomial trajectories, arise from stoichiometric exponential growth and decay [Adleman et al. 2014]; binomial decompositions in mass-action kinetics can identify which species persist or become extinct [Shiu and Sturmfels 2010]. In algebraic statistics, decompositions of binomial ideals give insight into how a set of conditional independence statements among random variables can be realized [Drton et al. 2009; Herzog et al. 2010]. More generally, the connectivity of lattice point walks in polyhedra can be analyzed using decompositions of binomial ideals [Diaconis et al. 1998; Kahle et al. 2014b]. These applications rely on decompositions of *unital* ideals — generated by monomials and differences of monomials — into unital ideals; these are mesoprimary decompositions. The algebra, geometry, and combinatorics of binomial primary decomposition interact with systems of differential equations of hypergeometric type [Gelfand et al. 1987; Gelfand et al. 1989], whose solutions are eigenfunctions for binomial differential operators encoding the infinitesimal action of an algebraic torus. In fact, it was in the hypergeometric framework that the combinatorics of binomial primary decomposition had its origin [Matusevich et al. 2005; Dickenstein et al. 2010a; 2010b], providing tight control over series solutions. In the meantime, mesoprimary decomposition serves as an improved method for presenting and visualizing binomial primary decomposition in algorithmic output [Kahle 2012]. Beyond that, the methods here have already found a theoretical application to combinatorial game theory [Guo and Miller 2011; Miller 2013].

Conventions. Unless otherwise stated, Q denotes a finitely generated (equivalently, noetherian) commutative monoid, and $\Bbbk$ denotes an arbitrary field.

Gathering primary components rationally. Staring at output of binomial primary decomposition algorithms intimates that certain primary components belong together.

Example 1.1. During investigations of presentations of misère quotients of combinatorial games (culminating in the definition of lattice games [Guo et al. 2009; Guo and Miller 2011]), Macaulay2 [Grayson and Stillman] produced long lists of primary binomial ideals. In one instance, eight of the components were

$$\langle e-1, d-1, b-1, a-1, c^3 \rangle, \quad \langle e-1, d-1, b-1, a+1, c^3 \rangle,$$
$$\langle e-1, d+1, b-1, a-1, c^3 \rangle, \quad \langle e-1, d+1, b-1, a+1, c^3 \rangle,$$
$$\langle e+1, d-1, b+1, a-1, c^3 \rangle, \quad \langle e+1, d-1, b+1, a+1, c^3 \rangle,$$
$$\langle e+1, d+1, b+1, a-1, c^3 \rangle, \quad \langle e+1, d+1, b+1, a+1, c^3 \rangle.$$

The urge to gather these eight into one piece (a piece of eight?), namely their intersection

$$\langle b-e, e^2-1, d^2-1, a^2-1, c^3 \rangle,$$

is irresistible. (Who would rather sift through the big list?) And it would have become more so had the exponents in the single gathered component been larger integers, for then the coefficients in the long list of primary ideals would not even have been rational numbers, though the intersection would still have been rational.

An arbitrary binomial prime ideal $I_{\rho,P}$ in a finitely generated monoid algebra $\Bbbk[Q]$ is determined by a monoid prime ideal $P \subset Q$ and a character $\rho : K \to \Bbbk^*$ defined on a subgroup of the unit group $G_P \subseteq Q_P$ in the localization of Q along P (Definition 3.9 and Theorem 11.14). A binomial ideal $I \subseteq \Bbbk[Q]$ might possess many associated primes sharing the same P and K, differing only in the character ρ. *Mesoprimary ideals* (Definition 10.4; see also Propositions 12.10 and 15.1) are data structures for keeping track of primary components for such groups of associated binomial primes. The term "group" here is used in the ordinary nonmathematical sense, but it is appropriate mathematically: the primary components of a meso-primary ideal over an algebraically closed field are indexed by the characters of a finite abelian group, namely the quotient sat$(K)/K$ of the saturation of K in G_P (Propositions 11.9 and 15.4). Gathering primary components into mesoprimary ideals saves space just as writing the presentation for a finite abelian group instead of listing every one of its characters does.

The situation is not typically as simple as in Example 1.1. Indeed, upon inspecting a binomial primary decomposition, it can be difficult to determine which mesopri-mary ideals ought to occur, and which mesoprimary ideal each primary component ought to contribute to. Furthermore, some primary components of a mesoprimary ideal can be absent, even if the mesoprimary ideal clearly ought to appear.

Example 1.2. If char$(\Bbbk) \neq 2$, the ideal $I = \langle y - x^2y, y^2 - xy^2, y^3 \rangle \subseteq \Bbbk[x, y]$ has primary decomposition $I = \langle y \rangle \cap \langle 1+x, y^2 \rangle \cap \langle 1-x, y^3 \rangle$. The ideal I is unital, being generated by differences of monomials, so the component $\langle 1+x, y^2 \rangle$ feels out of place. Yet there are no obvious components to gather. What's missing is a "phantom" component $\langle 1 - x, y^2 \rangle$, hidden by $\langle 1 - x, y^3 \rangle$. Gathering yields $\langle 1 + x, y^2 \rangle \cap \langle 1-x, y^2 \rangle = \langle 1-x^2, y^2 \rangle$. If char$(\Bbbk) = 2$, then $I = \langle y \rangle \cap \langle 1-x^2, y^2 - xy^2, y^3 \rangle$ is a primary decomposition of I. While this decomposition is forced to be unital, it feels not fine enough. Indeed, $1 - x^2$ and $1 - x$ look like they should contribute two associated objects, and in all but a single characteristic they do. Independent of the characteristic the mesoprimary decomposition splits the second component: $I = \langle y \rangle \cap \langle 1-x^2, y^2 \rangle \cap \langle 1-x, y^3 \rangle$.

A *mesoprimary decomposition* of a binomial ideal I is an expression of I as an intersection of *mesoprimary components* (Definition 12.14), each of which is a mesoprimary ideal. Mesoprimary decompositions of binomial ideals always exist (Definition 13.1 and Theorem 13.2) in a form that realizes our initial intent (Theorems 15.6 and 15.9). However, an arbitrary intersection of mesoprimary

ideals is not a mesoprimary decomposition, even if the intersection is a binomial ideal; exigent additional conditions must be met regarding the interaction of the combinatorics and the arithmetic of the mesoprimary components, as compared with that of I (Remark 13.6). In summary, mesoprimary decomposition gathers primary components so that:

(1) The decomposition into binomial ideals requires no hypotheses on the field $\Bbbk$.

(2) Specifying one mesoprimary component takes the place of individually listing all primary components arising from saturated extensions of a fixed character.

(3) The combinatorics of the components and their associated prime objects reflects accurately and faithfully the combinatorics of the decomposed binomial ideal.

Congruences: binomial combinatorics. The simple (and not new) idea of binomial combinatorics is that a binomial ideal $I \subseteq \Bbbk[Q]$ determines an equivalence relation $\sim$ on Q that sets $u \sim v$ if I contains a two-term binomial $t^u - \lambda t^v$ (Definition 2.15). The quotient $\overline{Q} = Q/\sim$ modulo this relation is a monoid.

Example 1.3. The following ideals induce the depicted congruences on $\mathbb{N}^2$ and quotient monoids. The congruence classes are the connected components of the graphs drawn in the left-hand pictures. Each element labeled 0 is the identity of the quotient monoid. Each element labeled ∞ in the right-hand picture is *nil* (Definition 2.9 and Remark 2.10) in the quotient monoid; its congruence class comprises all monomials in the given binomial ideal. In items (2) and (4), the groups labeling the rows indicate how the group in the bottom row acts on the higher rows. In all four items, every element outside of the bottom row of the quotient monoid is *nilpotent* (Definition 2.9).
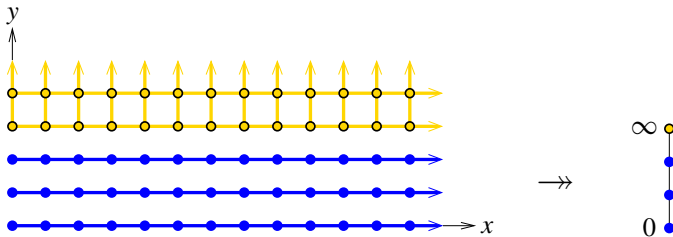
(1) For the ideal $\langle y \rangle \subset \Bbbk[x, y]$, the quotient monoid is $\mathbb{N} \cup \infty$:
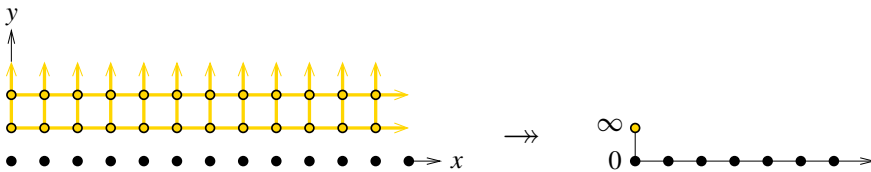

(2) For the ideal $\langle 1 - x^2, y^2 \rangle \subset \Bbbk[x, y]$, the quotient monoid is a copy of the group $\mathbb{Z}/2\mathbb{Z}$ (the bottom row), a free module over $\mathbb{Z}/2\mathbb{Z}$ (the middle row), and a nil:
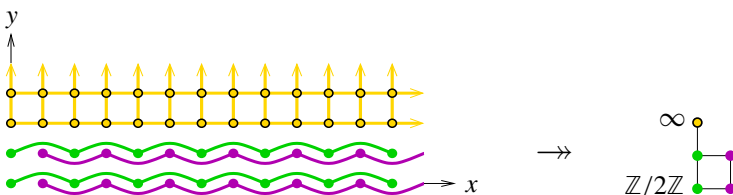
(3) For the ideal $\langle 1-x, y^3 \rangle \subset \Bbbk[x, y]$, the quotient monoid is the quotient $\mathbb{N}/(3+\mathbb{N})$ of the natural numbers modulo the *Rees congruence* of the ideal $3+\mathbb{N}$, which makes all elements of the ideal equivalent and leaves the other elements of $\mathbb{N}$ alone:

(4) For the ideal $\langle y-x^2y, y^2-xy^2, y^3 \rangle \subset \Bbbk[x, y]$, the quotient monoid is a disjoint union of the group $\mathbb{Z}$ and three $\mathbb{Z}$-modules:
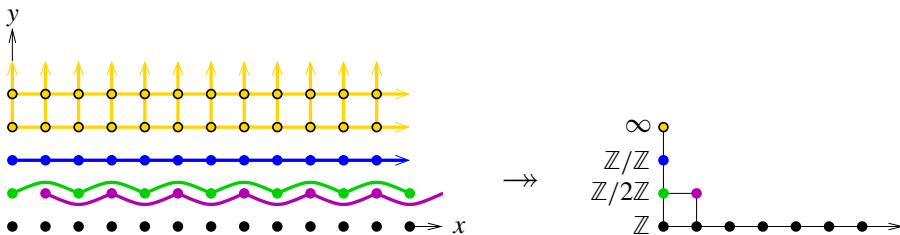
We examined (the literature on) monoid congruences on the premise that an appropriate decomposition theory for them should lift, either directly or analogously, to the desired mesoprimary theory for binomial ideals. However, although we found rich decomposition theories for commutative semigroups [Grillet 2001], the expected analogue of binomial primary decomposition was absent.

The most promising development we encountered along these lines is Grillet's discovery of conditions guaranteeing that a commutative semigroup can be realized as a subsemigroup of the multiplicative semigroup of a primary ring — that is, a ring with just one associated prime [Grillet 1975]. That work covers ground anticipating — in a more general setting — the characterization of primary binomial ideals over algebraically closed fields of characteristic zero [Dickenstein et al. 2010b].

The closest monoid relative in the literature to primary decomposition in rings seems to be primary decomposition of congruences [Drbohlav 1963] (see [Gilmer 1984] for a treatment in the context of semigroup rings). However, one of our motivating discoveries is that primary decomposition of congruences, being much closer to a shadow of cellular binomial decomposition (see Theorem 10.6), falls short of serving as a rubric for either primary or mesoprimary decomposition of binomial ideals. Indeed, congruences that are *prime*, meaning that quotients modulo them are cancellative except perhaps for a nil (Definition 2.12.4), fail to be irreducible

(Example 2.22). Furthermore, congruences that are *primary*, meaning that every element in the quotient is either nilpotent or cancellative (Definition 2.12.1), admit further decompositions into pieces that are visibly more "homogeneous", in a manner more analogous to primary decomposition in the presence of embedded primes than to irreducible decomposition of primary ideals.

Example 1.4. All of the congruences depicted in Example 1.3 are primary, but the first three are visibly more homogeneous: in each one, the nonnil rows all look the same. In fact, the fourth congruence is the *common refinement* (Section 3) of the first three. This is equivalent, given that all of the ideals (and their intersection) are binomial, to saying that the fourth binomial ideal equals the intersection of the first three, since the ideals in question are all unital and contain monomials; see Remark 2.16 and Theorem 9.12. This intersection is the mesoprimary decomposition from Example 1.2.

Primary binomial ideals in characteristic zero induce *primitive* congruences (Definition 2.12 and Theorem 10.6), but congruences usually do not admit expressions as intersections (common refinements) of primitive congruences. The reason stems from the same phenomenon that requires one to assume, for binomial primary decomposition, that the base field is algebraically closed: decompositions of ideals generated by binomials — even unital ones — usually require nontrivial roots of unity. Viewed another way, the arithmetic part of binomial primary decomposition has a combinatorial ramification: intersecting multiple primary ideals inducing the same primitive congruence results in a single mesoprimary ideal whose associated prime congruence has finite index in the primitive one (Proposition 15.4). In essence, primary congruences on Q are too coarse to reflect binomial primary decomposition in $\Bbbk[Q]$ accurately, and primitive congruences on Q are too fine, requiring additional arithmetic data from $\Bbbk$ to resolve otherwise indistinguishable associated primes in $\Bbbk[Q]$.

An additional layer of complication arises from the fact that primary binomial ideals in positive characteristic need not induce nicely filtered congruences (Example 10.8). The reason for this failure is not under our control: the ideal $\langle (x-1)^p, y(x-1), y^2 \rangle$ happens to be primary, the ideal $\langle x^p - 1, y(x-1), y^2 \rangle$ happens to be binomial, and — accidentally, one may conclude — they coincide in characteristic p. This highlights that even the "binomiality" of a ring-theoretic construction can depend on the characteristic, and consequently no study of binomial ideals can skirt the resulting distinctions.

The true monoid congruence analogue of primary decomposition in rings is a suitable compromise, developed (in Sections 2–8) as *mesoprimary decomposition for congruences* (Definition 8.1 and Theorem 8.3). The type of homogeneity mentioned before Example 1.4, discovered by Grillet [1975] (Remark 2.13(4)),

characterizes mesoprimary congruences (Corollary 6.7 and Remark 6.8). These are also distinguished (Theorem 6.1) as those with just one *associated prime congruence* (Definitions 2.12.4 and 5.2), a notion new to monoid theory. For comparison, a congruence is primary precisely when it has just one *associated prime ideal* (Definition 4.7 and Corollary 4.21).

The development of binomial mesoprimary decomposition in the latter half of the paper (Sections 9–16) mirrors the first half directly. Arithmetic existence statements build on combinatorial ones by exhibiting lifts of statements or requirements concerning elements equivalent under congruences to statements or requirements concerning binomials with nonzero coefficients.

It is worth warning the reader at this juncture of the inevitable clash of terminology in translating between combinatorics and arithmetic; see the table in Section 10, which in particular explains the source of our term *mesoprimary* to mean "between the two occurrences of 'primary'". To aid readers coming from commutative ring theory, the basic notions from semigroup theory are reviewed from scratch (Sections 2 and 3). For readers interested primarily in monoids, we complete the entire combinatorial theory in Section 8, before starting the arithmetic theory in Section 9.

Witnessed associated objects. In ordinary primary decomposition, a witness is an element whose annihilator is (an associated) prime. Our *witnesses* also have *associated* prime objects (Definitions 4.7, 5.2, and 12.1). Continuing the parallel, our notions of associatedness are defined by local combinatorial or algebraic conditions but equivalently characterized by the consistent appearance of prime objects in every primary decomposition (Theorems 4.20 and 15.11). The local conditions defining witnesses incorporate the combinatorial quiddity of having prime annihilator in ordinary ring theory.

The proof of concept for mesoprimary decomposition as a mode to connect the combinatorial and arithmetic settings lies in a fundamental discovery: there is a combinatorially defined set of witnesses that captures decompositions of both a binomial ideal and its induced congruence. To yield finite decompositions, however, not all witnesses are to be believed. The *key witnesses* for congruences (Definition 4.7) and *essential witnesses* for binomial ideals (Definition 12.1) yield finitely many components whose intersections suffice. These key and essential decompositions can generally fail to be minimal in ways that even retain symmetry. In the cellular binomial ideal case, we demonstrate a systematic reduction to *character witnesses* (Definition 16.3) that should have an extension to general binomial ideals. The dichotomy between key and essential witnesses demands care, as do other subtle distinctions between the combinatorial and arithmetic aspects of the theory, since they necessitate occasional slight weakenings, or failures of the combinatorics to lift; see Remarks 12.20 and 12.21, for instance.

2. Taxonomy of congruences on monoids

Fix a *commutative semigroup* Q: a set with an associative, commutative binary operation (usually denoted by $+$ here). Assume that Q has an identity, usually denoted by 0 here, so Q is a *monoid*. An *ideal* $T \subseteq Q$ is a subset such that $T + Q \subseteq T$, and T is *prime* if $t + s \in T$ implies $t \in T$ or $s \in T$. The ideal generated by elements $q_1, \ldots, q_s$ is written $\langle q_1, \ldots, q_s \rangle$. A *congruence* $\sim$ on Q is an equivalence relation that is additively closed: $a \sim b \Longrightarrow a + c \sim b + c$ for all $a, b, c \in Q$. The quotient $Q/\sim$ by any congruence is a monoid. The minimal relation satisfying this definition is equality itself, called the *identity congruence*. The congruence that equates all pairs of elements in Q, and has trivial quotient, is the *universal congruence*. For any ideal $T \subseteq Q$, under the *Rees congruence* $\sim_T$ all elements of T form one class, while all elements outside of T are singletons.

Definition 2.1. A *module* over a commutative monoid Q is a nonempty set T with an *action* of Q, which means a map $Q \times T \to T$, written $(q, t) \mapsto q + t$, that satisfies

- $0 + t = t$ for all $t \in T$, and
- $(q + q') + t = q + (q' + t)$,

the latter meaning that the action respects addition. A *congruence* on a module is an equivalence relation that is preserved by the action. A *module homomorphism* over a given monoid is a set map that respects the actions. For any element $q \in Q$, the *addition morphism* $\phi_q : Q \to \langle q \rangle$ is the module morphism defined by $p \mapsto p + q$. The *kernel* $\ker(\phi)$ of a module homomorphism $\phi : T_1 \to T_2$ is the congruence on T_1 under which $t \sim s \Longleftrightarrow \phi(t) = \phi(s)$.

Remark 2.2. For general semigroups Grillet [2007] defines an *act* as a set with an action of a semigroup that satisfies only the second bullet in Definition 2.1, even if the semigroup was a monoid to start with. To every semigroup S a formal identity element e can be adjoined (even if S is already a monoid) to form the monoid $S \cup \{e\}$. Upon this operation an S-act turns into an $(S \cup \{e\})$-module as it automatically satisfies the first item in Definition 2.1.

Remark 2.3. A subsemigroup of a monoid may have an identity, and in that case it may or may not be the identity of the monoid. To the contrary, a submonoid is required to have the same identity as its ambient monoid. In this sense a subsemigroup of a monoid can be a monoid without being a submonoid.

Definition 2.4. A *subgroup of a monoid* is a subsemigroup that is a group.

Definition 2.5. *Green's preorder* on a monoid is the divisibility preorder $p \preceq q \Longleftrightarrow \langle p \rangle \supseteq \langle q \rangle$. *Green's relation* on a monoid is $p \sim q \Longleftrightarrow \langle p \rangle = \langle q \rangle$.

Lemma 2.6 [Grillet 2001, Proposition I.4.1]. *The quotient of a commutative monoid modulo Green's relation is partially ordered by divisibility.*

Remark 2.7. Green's relation measures the extent to which group-like behavior occurs in a monoid. Idempotents and nontrivial units are obstructions to partially ordering a monoid by divisibility. In particular, a monoid with trivial unit group is partially ordered if Green's relation is trivial. Note that our divisibility preorder is the opposite direction compared to Grillet's, to be compatible with divisibility of monomials.

The following observation, which relies crucially on the noetherian hypothesis, is applied in the proof of Proposition 7.9.

Lemma 2.8. *Fix a noetherian commutative monoid Q. If $p \in Q$ and the Green's class of w satisfies $[w] = [p+w]$, then the map $[w] \to [p+w]$ of Green's classes induced by adding p is bijective.*

Proof. Suppose that $v \in [w] = [p+w]$. For surjectivity, first note that $v \in p + \langle w \rangle$, because $v \in \langle v \rangle = \langle p+w \rangle = p + \langle w \rangle$. Consequently $v \in p + [w]$ because $[v] = [w]$ is the (unique) minimal element in the poset of Green's classes with representatives in $\langle w \rangle$ (that is, $[v]$ can't lie in $p + [u]$ if $[u] \succ [w]$).

Since the sets in question can be infinite, injectivity requires additional reasoning. Suppose that $v \in [w]$ satisfies $p+w = p+v$. By surjectivity, for $k \in \mathbb{N}$ choose $w_k, w'_k \in [w]$ so that $k \cdot p + w_k = w$ and $k \cdot p + w'_k = v$. If $\sim_k$ is the kernel congruence of addition by $k \cdot p$, then $\sim_k$ refines $\sim_\ell$ whenever $k \leq \ell$. The noetherian property implies that the chain of kernel congruences stabilizes: $\sim_k = \sim_{k+1}$ for $k \gg 0$. But $w_k \sim_{k+1} w'_k$ for all k because $p+w = p+v$, whence $w_k \sim_k w'_k$ for $k \gg 0$ by stability. For $k \gg 0$, then, $w = k \cdot p + w_k \sim k \cdot p + w'_k = v$. $\square$

Definition 2.9. A nonidentity element ∞ in a monoid Q is *nil* if $q + \infty = \infty$ for all $q \in Q$. An element $q \in Q$ is

- *nilpotent* if one of its multiples nq is nil for some nonnegative integer $n \in \mathbb{N}$,
- *cancellative* if addition by it is injective: $q + a = q + b \Longrightarrow a = b$ in Q,
- *partly cancellative* if $q + a = q + b \neq \infty \Longrightarrow a = b$ for all cancellative $a, b \in Q$.

A set S of elements in a monoid is *torsion-free* if $na = nb \Longrightarrow a = b$ for all $n \in \mathbb{N}$ whenever $a, b \in S$. An *affine semigroup* is a monoid isomorphic to a finitely generated submonoid of a free abelian group. A *nilmonoid* is a monoid whose nonidentity elements are all nilpotent.

Remark 2.10. In the literature a nil is often called a zero instead; but when we work with monoid algebras, we need to distinguish the nil monomial t^∞ from the zero element 0 of the algebra (see Section 9 for ramifications of this distinction), and we need to identify the identity monomial t^0 with the unit element 1 of the algebra.

Remark 2.11. The condition $a + c = b + c'$ for cancellative c, c' means that a and b are off by a unit in the localization Q' of Q obtained by inverting all of its cancellative elements. Note that the natural map $Q \to Q'$ is injective.

Definition 2.12. Fix a commutative monoid Q, a congruence $\sim$, and use a bar to denote passage to the quotient $\overline{Q} = Q/\sim$. The congruence $\sim$ is

(1) *primary* if every element of $\overline{Q}$ is either nilpotent or cancellative,

(2) *mesoprimary* if it is primary and every element of $\overline{Q}$ is partly cancellative,

(3) *primitive* if it is mesoprimary and the cancellative subset of $\overline{Q}$ is torsion-free,

(4) *prime* if every element of $\overline{Q}$ is either nil or cancellative,

(5) *toric* if the nonnil elements of $\overline{Q}$ form an affine semigroup.

Remark 2.13. The notions just defined are nearly or exactly the same as concepts that have appeared in the literature on monoids.

(1) Our definitions of prime and primary congruences agree with those in the literature [Gilmer 1984, §5]. In the case of prime congruences, where the nonnil elements of $\overline{Q}$ form a cancellative monoid, this is easy. In the case of primary congruences, for $q \in Q$ the condition Gilmer expresses as $q + a \sim q + b$ for all a, $b \in Q$ is equivalent to the class $\overline{q}$ being a nil in $\overline{Q} = Q/\sim$, so q lies in the nil class, and the condition that Gilmer expresses by saying that q lies in the radical of the nil class is equivalent to $\overline{q}$ being nilpotent in $\overline{Q}$.

(2) Our definition of affine semigroup differs slightly from [Grillet 2001, §II.7]: Grillet requires the unit group to be trivial, whereas we do not. Equivalently, our affine semigroups are the finitely generated, cancellative, torsion-free commutative monoids, while Grillet additionally requires affine semigroups to be reduced (that is, to have trivial unit group).

(3) A congruence on Q is primary if and only if $\overline{Q}$ is a *subelementary* monoid, by definition [Grillet 2001, §VI.2.2].

(4) A congruence on Q is mesoprimary if and only if the subelementary monoid $\overline{Q}'$, obtained from the monoid $\overline{Q}$ in the previous item by inverting its cancellative elements, is *homogeneous* [Grillet 2001, §VI.5.3]; this is Corollary 6.7, below.

Lemma 2.14. *For monoid congruences,*

- *toric $\Longrightarrow$ prime $\Longrightarrow$ mesoprimary $\Longrightarrow$ primary, and*
- *toric $\Longrightarrow$ primitive $\Longrightarrow$ mesoprimary $\Longrightarrow$ primary.*

Proof. The only implication that is not immediate from the definitions is that prime implies mesoprimary. For this, assume $\sim$ is a prime congruence and $\overline{q} + \overline{a} = \overline{q} + \overline{b}$ in $\overline{Q}$ with neither side being nil. Then $\overline{q}$ is not nil, whence $\overline{a} = \overline{b}$ by cancellativity. $\square$

Definition 2.15. The *semigroup algebra* $\Bbbk[Q] = \bigoplus_{q \in Q} \Bbbk \cdot t^q$ is the direct sum with multiplication $t^p t^q = t^{p+q}$. Any congruence $\sim$ on Q induces a grading of $\Bbbk[Q]$ by $\overline{Q} = Q/\sim$ in which the *monomial* t^q has degree $\overline{q} \in \overline{Q}$ whenever $q \mapsto \overline{q}$ under the quotient map $Q \to \overline{Q}$. A *binomial ideal* $I \subseteq \Bbbk[Q]$ is an ideal generated by *binomials* $t^p - \lambda t^q$, where $\lambda \in \Bbbk$ is a scalar possibly equal to $0 \in \Bbbk$. A binomial ideal is *unital* if all coefficients λ are equal to either 0 or 1. The ideal I *induces* the congruence $\sim_I$ in which $p \sim_I q$ whenever $t^p - \lambda t^q \in I$ for some unit $\lambda \in \Bbbk^*$.

Remark 2.16. Giving a congruence on Q is the same as giving a unital ideal in $\Bbbk[Q]$ that is generated by unital binomials $t^p - t^q$ (and no monomials). In particular, every congruence is induced by some binomial ideal. That said, other binomial ideals can induce the same congruence as the canonical unital ideal, by rescaling the variables or via Theorem 9.12, for instance.

Example 2.17 (some congruences from unital ideals).

(1) The prime ideal $\langle x - y \rangle \subset \Bbbk[x, y]$ induces a toric congruence such that $\overline{\mathbb{N}^2} \cong \mathbb{N}$.

(2) The ideal $\langle x^2 - y^2 \rangle \subset \Bbbk[x, y]$ induces a prime congruence with $\overline{\mathbb{N}^2}$ isomorphic to the submonoid $Q \subseteq G = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ generated by $(1, 0)$ and $(1, 1)$. The monoid is not torsion-free, since $x^2 = y^2$ but $x \neq y$ in $\Bbbk[Q]$. Therefore the congruence on $\mathbb{N}^2$ is not toric, since Q generates G as a group.

(3) The ideal $\langle x^2 - x \rangle \subset \Bbbk[x]$ induces the same toric congruence on $\mathbb{N}$ as the prime ideal $\langle x \rangle$ does, but $\langle x^2 - x \rangle$ is not primary (in fact, not even cellular; see Definition 10.4). Nevertheless $\sim_{\langle x^2 - 1 \rangle} = \sim_{\langle x \rangle}$ is irreducible according to Definition 2.21.

(4) The $\langle x, y \rangle$-primary ideal $\langle x^2, x - y \rangle$ induces the primitive congruence on $\mathbb{N}^2$ with $\overline{\mathbb{N}^2} \cong \{0, x, \infty\} =: Q$. The monoid algebra $\Bbbk[Q]$ has a presentation $\Bbbk[x, y]/J$, where $J = \langle x - y, x - x^2 \rangle = \langle x - 1, y - 1 \rangle \cap \langle x, y \rangle$ induces the same congruence.

(5) The binomial ideal $\langle y - x^2 y, y^2 - xy^2, y^3 \rangle$ induces a primary congruence whose classes are depicted as connected components of the graph in the following figure.
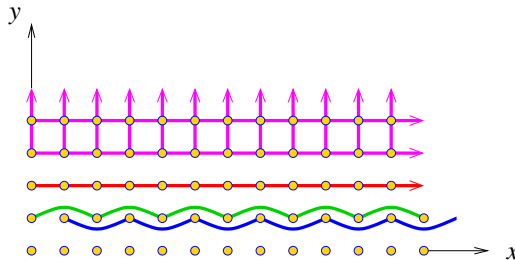

This congruence exhibits the distinction between primary and mesoprimary congruences: for a primary congruence, no injectivity is required of addition

by a nilpotent element. In the picture, this means that translating two dots in different classes upward by one unit can force them into the same nonnil class. To make the congruence mesoprimary, homogenize the bottom three rows by replacing any two of them with the third; after that, upward translation on two dots keeps them in separate classes unless both land in the nil class. This replacement procedure also exhibits the distinction between mesoprimary and primitive congruences: it results in a primitive congruence only if the bottom row or the third row is preserved; preserving the second row yields torsion in the cancellative part of $\overline{Q}$.

The following example demonstrates the partly cancellative property.

Example 2.18. Partly cancellative elements can still merge congruence classes. For instance, consider the congruence on $\mathbb{N}^2$ induced by $I = \langle x^2 - xy, \, xy - y^2, \, x^3, \, y^3 \rangle \subseteq \Bbbk[x, y]$. In the figure
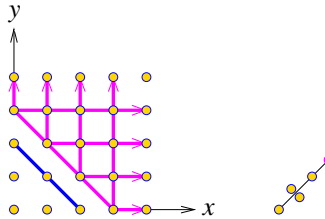
the congruence on $\mathbb{N}^2$ appears at left, and the quotient $\overline{\mathbb{N}^2}$ appears at right. The quotient is the monoid $\mathbb{N}$ with two copies of 1 modulo the Rees congruence of $\langle 3 \rangle$ (declare all elements in $\langle 3 \rangle$ congruent). The two copies of 1 become identified upon addition by either: $1 + 1 = 1 + 1' = 1' + 1' = 2$. Nonetheless, both 1 and $1'$ are partly cancellative and the congruence is mesoprimary.

The next result will be applied in the proofs of Theorems 8.4 and 10.6. The conclusion says that Q/F is a nilmonoid whose Green's preorder is an order (i.e., is antisymmetric). Equivalently, it says that Q/F is *naturally partially ordered*, or a *holoid* [Grillet 2001, §V.2.2].

Lemma 2.19. *Fix a monoid Q whose identity congruence is primary, so the non-nilpotent elements of Q constitute a cancellative submonoid $F \subseteq Q$. The quotient monoid Q/F defined by the congruence*

$$p \sim q \iff p + f = q + g \text{ for some } f, g \in F$$

is a nilmonoid partially ordered by divisibility. If Q is finitely generated, Q/F is finite.

Proof. This is more or less [Grillet 2001, Proposition VI.3.3], but the proof is simple. Every nonidentity element of Q/F is nilpotent by definition, so when Q is finitely generated, Q/F is finite. The rest follows because every nilmonoid is

partially ordered by divisibility; this is easy, and can be found in [Grillet 2001, Proposition IV.3.1]. □

Remark 2.20. It is a crucial assumption for Lemma 2.19 that every element is nilpotent or cancellative, excluding idempotents. If every cancellative element is a unit, e.g., after localizing at the nilpotent ideal (see Section 4), then Q/F equals Q modulo Green's relation.

Concluding this section, we comment on the notion of irreducibility for congruences, which is, despite the close connection between binomial ideals and their congruences, quite different from irreducibility for ideals.

Definition 2.21. A congruence is *irreducible* if it cannot be expressed as the common refinement of two congruences neither of which equals the given one.

The theories of irreducible and primary decomposition for congruences in commutative monoids are not as nice as for (binomial) ideals in rings. The following example might come as a nasty surprise (it did to us). Quotients by irreducible congruences are characterized in [Grillet 2001, Theorem VI.5.3].

Example 2.22. The identity congruence on $\mathbb{N}^2$ is reducible: it is the common refinement of the congruences induced by $\langle x - 1 \rangle$ and $\langle y - 1 \rangle$. Ring-theoretically, this is due to the fact that $\langle x - 1 \rangle \cap \langle y - 1 \rangle$ does not contain binomials.

Example 2.22 demonstrates the sad reality that prime congruences need not be irreducible. In a wider sense, unrestricted primary or irreducible decomposition of congruences decomposes them into components that are too fine to provide nuanced information about their combinatorics. The theory of mesoprimary decomposition, with its well-founded notions of associatedness for prime ideals and prime congruences, is our remedy.

3. Primary decomposition and localization in monoids

We review the notion of primary decomposition for congruences on finitely generated commutative monoids, which traces back to Drbohlav [1963]. This decomposition is only a coarse approximation of mesoprimary decomposition, a central goal of this paper. In general, a *decomposition* of a congruence is an expression of it as a common refinement of congruences. The notion of refinement here is standard: formally, an equivalence relation on Q is a reflexive, symmetric, transitive subset of $Q \times Q$; one relation $\sim$ *refines* another relation $\approx$ if $\approx$ contains $\sim$ (we also say $\approx$ *coarsens* $\sim$); and the *common refinement* of a family of equivalence relations is their intersection in $Q \times Q$.

Remark 3.1. Every congruence in this setting admits a *primary decomposition*: an expression as the common refinement of finitely many primary congruences

[Gilmer 1984, Theorem 5.7]. Similarly to the case of rings, this follows from the existence of irreducible decomposition using a noetherian induction argument. Any decomposition theory that is finer than primary decomposition — that is, any theory that further decomposes each primary component — yields a greater number of congruences, each of which is coarser than some primary component.

Remark 3.2. The preimage under any monoid homomorphism of a prime ideal is prime. Since $\mathbb{N}^n$ has only finitely many prime ideals and a finitely generated commutative monoid Q has a presentation $\mathbb{N}^n \twoheadrightarrow Q$, it follows that Q has only finitely many prime ideals. Precisely one of these is the *maximal ideal* of Q.

Convention 3.3. To avoid tedious case distinctions in the following, we consider the empty set as an ideal of any monoid, and in fact we declare it to be a prime ideal (its complement is, after all, a submonoid). The empty set considered as an ideal will be denoted by $\varnothing \subset Q$; this symbol is never used for any other purpose in this paper.

Definition 3.4. The *nilpotent ideal* of a congruence $\sim$ on Q is the ideal of Q consisting of all elements with nilpotent image in $Q/\sim$. If P is the nilpotent ideal of a primary congruence $\sim$, then $\sim$ is *P-primary*.

Lemma 3.5. *If $\sim$ is a primary congruence, then the nilpotent ideal is prime. If $Q/\sim$ is cancellative, then $\sim$ is $\varnothing$-primary.* □

Remark 3.6. If $q_1, \ldots, q_n$ generate Q, then a primary congruence defines a partition of $\{q_1, \ldots, q_n\}$ into generators with cancellative and nilpotent images, respectively. In this case the nilpotent ideal is generated by the generators q_i with nilpotent images.

Proposition 3.7. *The common refinement of finitely many P-primary congruences is P-primary.*

Proof. It suffices by induction to show this for two P-primary congruences $\sim_1$ and $\sim_2$. Reducing modulo their intersection, we can assume that the intersection is the identity congruence on Q. Denote by Q_1 and Q_2 the quotients modulo $\sim_1$ and $\sim_2$, respectively. By assumption $P \subset Q$ is the nilpotent ideal of both $\sim_1$ and $\sim_2$. We claim that if $p \in P$ then p is nilpotent already in Q. Indeed, a sufficiently high multiple of p is congruent to nil under both $\sim_1$ and $\sim_2$, and since their intersection is trivial this can only happen if that multiple is nil. On the other hand, if $p \notin P$, then it must be cancellative: if there exist $a, b \in Q$ with $a+p = b+p$, then $a \sim_1 b$ and $a \sim_2 b$ both hold — whence $a = b$, in fact — since p is cancellative modulo $\sim_1$ and $\sim_2$. □

Remark 3.8. Albeit in different language, [Gilmer 1984, Theorem 5.6.2] contains a variant of the statement of Proposition 3.7.

Passing from the theory surrounding P-primary congruences to that for general congruences is best accomplished by localizing.

Definition 3.9. The *localization* T_P of a Q-module T at a prime ideal $P \subset Q$ is the set of formal differences $t - q$ for $t \in T$ and $q \notin P$, with $t - q$ and $t' - q'$ identified when $w + q' + t = w + q + t'$ for some $w \in Q \setminus P$. Conventions for this are as follows:

- The localization Q_P of Q itself is naturally a monoid, and T_P is a Q_P-module.

- The image of P in Q_P is the maximal ideal P_P of Q_P.

- Any given congruence $\sim$ on Q induces a congruence on Q_P, also denoted $\sim$.

- If $\bar{Q} = Q/\sim$ then we write $\bar{Q}_P = Q_P/\sim$.

- The *unit group at P* is the subgroup $G_P = Q_P \setminus P_P$.

Example 3.10. Localizing Q at the empty prime ideal yields the universal group $Q_\varnothing$. When Q has a nil, $Q_\varnothing$ is trivial. In fact, the universal group $Q_\varnothing$ is trivial precisely when Q has a nil. (Proof: If $Q_\varnothing$ is trivial, then q becomes equal to 0 after inverting every element of Q. Thus there is an element $x_q \in Q$ such that $x_q + q = x_q$. As Q is generated by a finite set $S \subseteq Q$, the sum of the elements x_s for $s \in S$ exists, and it is nil in Q.)

By definition, the group of units of Q_P acts on itself and also on the set $\bar{Q}_P$ of equivalence classes modulo any congruence on Q_P. Here and in what follows, we often think of the quotient $\bar{Q}$ explicitly as a set of congruence classes in Q. Thus $\bar{Q}_P$ is a set of congruence classes in Q_P. We record this fact for future reference.

Lemma 3.11. *Let $P \subset Q$ be a prime ideal. Given any congruence on Q, the unit group of Q_P acts on the quotient $\bar{Q}_P$ modulo the induced congruence on Q_P.* $\square$

In analogy with what happens over rings, primary decomposition of congruences behaves well under localization.

Theorem 3.12. *Primary decomposition of congruences commutes with localization: if $\sim = \sim_1 \cap \cdots \cap \sim_r$ is a primary decomposition of the congruence $\sim$ on Q, and $P \subset Q$ is a prime ideal, then each of the congruences induced by $\sim_1, \ldots, \sim_r$ on Q_P is primary or universal, and their common refinement is the congruence induced by $\sim$ on Q_P.*

Proof. If some element of Q lies outside of P but becomes nilpotent in $Q/\sim_j$, then $\sim_j$ induces the universal congruence on Q_P, so assume no such element exists. Suppose that $q - u \in Q_P$. Our assumption means that u has cancellative image in $Q/\sim_j$. It follows that $q - u \in Q_P$ becomes cancellative in $Q_P/\sim_j$ as long as $q - u$ does not become nilpotent in $Q_P/\sim_j$. Therefore $\sim_j$ induces a primary congruence on Q_P. The rest of the proof is covered by the following lemma. $\square$

Lemma 3.13. *Localization commutes with finite common refinement of congruences*: *if* $\sim\, =\, \sim_1 \cap \cdots \cap \sim_r$ *as congruences on* Q, *and* $P \subset Q$ *is a prime ideal*, *then the induced congruences on the localization* Q_P *still satisfy* $\sim\, =\, \sim_1 \cap \cdots \cap \sim_r$.

Proof. For the duration of this proof, a dot denotes passage to Q_P, so $\dot\sim$ is the congruence on Q_P induced by $\sim$ on Q. If $v \dot\sim_j w$ in Q_P for all j, then for each j there is an element $u_j \in Q \setminus P$ with $u_j + v \sim_j u_j + w$. Summing these elements u_j yields an element $u = u_1 + \cdots + u_r$ such that $u + v \sim_j u + w$ for all j, whence $u + v \sim u + w$ by definition of $\sim$ as the common refinement. Therefore $v \dot\sim w$. This logic easily reverses to show that $v \dot\sim w \Longrightarrow v \dot\sim_j w$ for all j. We conclude that $\dot\sim\, =\, \dot\sim_1 \cap \cdots \cap \dot\sim_r$, as desired. $\qquad\square$

4. Witnesses and associated prime ideals of congruences

Our aim in this section is to show that primary decompositions of congruences in finitely generated commutative monoids have well-defined associated prime ideals. These, and their witnesses, reflect the combinatorial features of a given congruence more accurately than does primary decomposition alone.

Definition 4.1. For any ideal $T \subseteq Q$, the *annihilator modulo* T is the common refinement $\mathrm{ann}(T) = \bigcap_{t \in T} \ker(\phi_t)$ of the kernels of the addition morphisms ϕ_t for $t \in T$.

Remark 4.2. If $q_1 + v = q_2$ then $\ker(\phi_{q_1})$ refines $\ker(\phi_{q_2})$. Therefore, in the definition of $\mathrm{ann}(T)$, it suffices to intersect only over generators of T. Equivalently, if T is generated by $t_1, \ldots, t_r$, then $\mathrm{ann}(T) = \ker(\phi_{t_1} \oplus \cdots \oplus \phi_{t_r} : Q \to T^{\oplus r})$. If $T = \varnothing$ is the empty ideal, then $\mathrm{ann}(T)$ is the universal congruence (that has just one class).

Example 4.3. To explain the "annihilator" terminology, let Q be a monoid with nil ∞ and write $\Bbbk[Q]^- := \Bbbk[Q]/\langle t^\infty \rangle$. If $T \subseteq Q$ is a monoid ideal, then $\mathrm{ann}(T)$ is the congruence induced by the binomials (and the monomials) in the ideal $(0 : \Bbbk\{T\}) = \{f \in \Bbbk[Q] \mid f\,\Bbbk\{T\} = 0 \text{ in } \Bbbk[Q]^-\}$.

Definition 4.4. Fix a prime ideal $P \subset Q$ with $P_P \subset Q_P$ minimally generated by $p_1, \ldots, p_r$. The *P-covers* of $q \in Q$ are the elements $q + p_i \in Q_P$ for $i = 1, \ldots, r$. The *cover morphisms at* P are the morphisms $\phi_i : Q_P \to \langle p_i \rangle_P$ defined via $q \mapsto q + p_i$; if P is the maximal ideal, then the ϕ_i are called simply *the cover morphisms* of Q.

Remark 4.5. The set of P-cover morphisms depends on the choice of generators $p_1, \ldots, p_r$ and may be infinite if, for example, Q_P has a lot of units. However, modulo Green's relation on Q_P there is a unique finite minimal generating set of any ideal, and every minimal generating set for P_P maps bijectively to it.

Lemma 4.6. *For a fixed prime P, the set of kernels of P-cover morphisms is finite.*

Proof. Two cover morphisms ϕ_p and $\phi_{p'}$ for elements p, p' that are Green's-equivalent in Q_P have the same kernel, because if $p \in \langle p' \rangle$ then there exists an element u such that $p = p' + u$, and thus the kernel of $\phi_{p'}$ refines the kernel of ϕ_p and vice versa. □

Next comes the first main new definition of the paper (note that the concept of mesoprimary congruence in Definition 2.12 is equivalent to a notion already available in the literature; cf. Remark 2.13(4), whose details can best be seen in action in the proofs of Proposition 7.9 and Theorem 8.4.

Definition 4.7. Let $\sim$ be a congruence on Q and $P \subset Q$ a prime ideal. Consider the localized quotient $\overline{Q}_P$. For each $q \in Q$ let $\overline{q}$ be its image in $\overline{Q}_P$. An element $\overline{q}$ is *exclusively maximal* in a subset $S \subseteq \overline{Q}_P$ if $\overline{q}$ is the unique maximal element of S under Green's preorder. An element $w \in Q$ is a:

(1) *witness for P* if the class of $\overline{w}$ is nonsingleton under the kernel of each cover morphism (i.e., the class $\overline{p} + \overline{w}$ is nonsingleton for all $p \in P$) and in each of its nonsingleton kernel classes, $\overline{w}$ is not exclusively maximal.

(2) *key witness for P* if the class of $\overline{w}$ is nonsingleton under the intersection of the kernels of all cover morphisms (i.e., if the class of $\overline{w}$ is nonsingleton under $\text{ann}(\overline{P}_P)$) and $\overline{w}$ is not exclusively maximal in the nonsingleton class;

The ideal P is an *associated prime ideal of* $\sim$ if the annihilator modulo $\overline{P}_P \subset \overline{Q}_P$ is not the identity congruence.

Convention 4.8. A (key) witness is a (key) witness for some prime ideal P. When we speak of the set of (key) witnesses for a given congruence we mean the set of pairs (w, P) where $w \in Q$ is a (key) witness for a prime ideal $P \subset Q$. If the congruence $\sim$ is not clear from context, a (key) witness may be called a (key) $\sim$-witness.

Lemma 4.9. *A prime ideal $P \subset Q$ is associated to a congruence $\sim$ on Q if and only if Q has a key witness for P.*

Proof. Once the annihilator $\text{ann}(\overline{P}_P)$ does not equal the identity congruence, it has a class of size 2 or more; at least one element therein avoids being exclusively maximal. □

Definition 4.10. Fix the notation of Definition 4.7.

(1) An *aide*[1] for a witness w and a generator $p \in P$ is an element $w' \in Q$ whose image $\overline{w}' \in \overline{Q}_P$ is (i) distinct from $\overline{w}$, but (ii) congruent to $\overline{w}$ in the kernel of

---

[1]The English word "aide" is fortuitously a transliteration of the Hebrew word for "witness". In talmudic courts, a pair of witnesses was required for any conviction.

the cover morphism ϕ_p, and (iii) maximal (under Green's preorder) in the set $\{\overline{w}, \overline{w}'\}$.

(2) A *key aide* for a key witness w is an element $w' \in Q$ whose image $\overline{w}' \in \overline{Q}_P$ is (i) distinct from $\overline{w}$, but (ii) congruent to $\overline{w}$ in the intersection of the kernels of all cover morphisms, and (iii) maximal (under Green's preorder) in the set $\{\overline{w}, \overline{w}'\}$.

Lemma 4.11. *Every witness for P and generator $p \in P$ has an aide. Every key witness has a key aide.*

Proof. In each case, there is a nonsingleton class containing $\overline{w} \in \overline{Q}_P$, so there exists an element $\overline{w}' \neq \overline{w}$ in this class. The point is to choose $\overline{w}'$ so that it does not precede $\overline{w}$ under Green's preorder and so that $\overline{w}'$ lies in the image of the composite morphism $Q \to \overline{Q} \to \overline{Q}_P$. The existence of $\overline{w}'$ not preceding $\overline{w}$ is a consequence of $\overline{w}$ not being exclusively maximal. Now use that every element of $\overline{Q}_P$ is off from the image of $\overline{Q}$ by an element of P, and that $Q \to \overline{Q}$ is surjective. $\square$

Remark 4.12. Every key witness is a witness, because any key aide is an aide for all generators of P.

Remark 4.13. An aide w' for a witness w and $p \in P$ can be a witness but need not be:

- Adding $\overline{p}$ could join $\overline{w}$ to $\overline{w}'$ while some other element of P fails to join $\overline{w}$ to $\overline{w}'$.

- $\overline{w}'$ can be exclusively maximal in its class under the kernel of the cover morphism.

Similarly, a key aide can be a witness (and hence a key witness) but need not be; however, in the key case only the second circumstance (i.e., exclusive maximality) can occur.

In the set of (key) witnesses for a congruence, a single $w \in Q$ can occur multiple times for different P. For instance, this happens when $\varnothing$ is associated.

Example 4.14. The condition for an element to be a witness for the empty prime ideal $\varnothing$ is vacuous: there are no cover morphisms. Furthermore, the congruence $\text{ann}(\varnothing)$ in the definition of key witness is an empty intersection of congruences, so it is the universal congruence on $\overline{Q}_\varnothing$. Thus the empty ideal is associated to a congruence if and only if the universal group $\overline{Q}_\varnothing$ of the quotient modulo that congruence is nontrivial, and that occurs precisely when $\overline{Q}$ has no nil (see Example 3.10). Every $q \in Q$ is a (key) witness in this case but at the same time $\overline{Q}_\varnothing$ has only one class under Green's relation.

The following series of examples demonstrates various features of associatedness of prime ideals and their witnesses.

Example 4.15. As usual it will be convenient to describe congruences on $\mathbb{N}^n$ by unital binomial ideals in polynomial rings. We use $e_x, e_y, \ldots$ to denote the generators of $\mathbb{N}^n$ corresponding to variables $x, y, \ldots$ in the polynomial ring $\Bbbk[\mathbb{N}^n]$, but we write the addition morphisms as $\phi_x, \phi_y, \ldots$ instead of $\phi_{e_x}, \phi_{e_y}, \ldots$, for simplicity.

(1) Let $\sim$ be the congruence on $\mathbb{N}^2$ induced by the binomial ideal $\langle x^2 - xy, xy - y^2 \rangle$ of $\Bbbk[x, y]$. The set of associated prime ideals in $\mathbb{N}^2$ consists of the empty ideal $\varnothing$ and the maximal ideal $P = \langle e_x, e_y \rangle$. Localization at the maximal ideal does nothing and there are only two cover morphisms, given by adding e_x and e_y, respectively. To establish that P is associated, note that e_x and e_y themselves are key witnesses for P, congruent under $\mathrm{ann}(P)$, and serve as aides for one another. Indeed, $\mathrm{ann}(P)$, the intersection of the two kernels, contains the pair (e_x, e_y) since $e_x + e_x \sim e_y + e_x$ and also $e_x + e_y \sim e_y + e_y$. The identity $0 \in \mathbb{N}^2$ is not a witness for P. Neither $\langle e_x \rangle$ nor $\langle e_y \rangle$ is associated since adjoining inverses to either turns the quotient $\mathbb{N}^2/\sim$ into a cancellative monoid. In this case all kernels of addition morphisms are trivial. Finally, localizing at the empty prime ideal amounts to considering the induced congruence on $\mathbb{Z}^2$, which is induced by the binomial ideal $\langle x - y \rangle \subset \Bbbk[x^{\pm}, y^{\pm}]$. Since the quotient is nontrivial, $\varnothing$ is associated too. Every element of $\mathbb{N}^2$ is a witness for $\varnothing$, but taken together they form only one Green's class in $\mathbb{Z}^2$.

(2) Let $\sim$ be the congruence on $\mathbb{N}^3$ induced by $\langle x^2 - xy, y^2 - xy, x(z - 1) \rangle \subset \Bbbk[x, y, z]$. The associated prime ideals are $\langle e_x, e_y \rangle$ and $\varnothing$. The argument for $\varnothing$ is the same as in item (1). The localization of $\sim$ at $\langle e_x, e_y \rangle$ is induced by the same ideal, considered in $\Bbbk[x, y, z^{\pm}]$. This says that e_z is cancellative, i.e., that the addition morphism $\phi_z : q \mapsto q + e_z$ is injective. The set of key witnesses is invariant under the ϕ_z-action. It consists of $e_y + k e_z$ and $e_x + k e_z$ for $k \in \mathbb{N}$. The translates of e_y all become equivalent when adding e_x or e_y. Any translates of e_x are witnesses since they are each joined to a translate of e_y. No e_z-translate of 0 is a witness, though. Again, all witnesses are key.

(3) Let $\sim$ be the congruence on $\mathbb{N}^4$ induced by

$$\langle x^2 - xy, y^2 - xy, x(z - 1), y(w - 1) \rangle \subset \Bbbk[x, y, z, w].$$

The associated prime ideals are again $\varnothing$ and $P = \langle e_x, e_y \rangle$. The set of witnesses for P is determined as follows. The element $0 \in \mathbb{N}^4$ is a witness that is not key. The kernel congruences of ϕ_x and ϕ_y are generated by $\{(0, e_z), (e_x, e_y)\}$ and $\{(0, e_w), (e_x, e_y)\}$ in $\mathbb{N}^4 \times \mathbb{N}^4$, respectively. This shows the witness property and also, because their common refinement leaves it singleton similarly to Example 2.22, that 0 is not key. In contrast, e_x and e_y are key witnesses because $\phi_x(e_x) = \phi_x(e_y)$ and likewise for ϕ_y. A mesoprimary decomposition (Theorem 13.2) of the binomial ideal defining $\sim$ has components corresponding to all three witnesses, while a mesoprimary decomposition of the congruence $\sim$ itself needs components only for

the two key witnesses (Theorem 8.4). Why the extra binomial component? The common refinement of the congruences induced by $\langle z-1, x^2, y \rangle$ and $\langle w-1, x, y^2 \rangle$ leaves the class of 0 singleton, but the intersection of the ideals is merely free of binomials, rather than being altogether zero.

This next example demonstrates how the monoid prime ideal P matters in the definition of a (key) witness for P, and how the same element can be a witness for different P.

Example 4.16. Fix the congruence $\sim$ induced on $\mathbb{N}^4$ by the unital binomial ideal $\langle x(z-1), x(w-1), y(z-1), y^2 \rangle \subset \Bbbk[x, y, z, w]$. The associated prime ideals of $\sim$ are $\langle e_x, e_y \rangle$ and $\langle e_y \rangle$. Consider the addition morphisms ϕ_x and ϕ_y. The key witnesses for $\langle e_y \rangle$ are $e_y + ke_x$ and all their translates in the e_z and e_w directions. No element in the ideal $\langle e_x \rangle$ can be a witness for a monoid prime containing e_x because ϕ_x acts injectively on that ideal. Indeed, the witnesses for $\langle e_x, e_y \rangle$ are $0 \in \mathbb{N}^4$ together with all its translates in the e_z direction, and e_y together with its translates in the e_z and e_w directions.

The final example on witnesses demonstrates the prohibition on exclusive maximality, which in particular bars ∞ and idempotents from being witnesses. See Remark 7.10 for a deeper explanation of the ban on exclusive maximality.

Example 4.17. Let $P = \langle e_x, e_y \rangle$ be the maximal ideal of $\mathbb{N}^2$.

(1) Under the Rees congruence induced by the monomial ideal $\langle x^2, y^2 \rangle$, the element $e_x + e_y$ is joined to nil under both cover morphisms. Only $e_x + e_y$ is a P-witness, and is in fact a key witness. In contrast, ∞ is a key aide but not a witness, and hence certainly not a key witness.

(2) Under the congruence induced by the unital binomial ideal $\langle y, x^2 - x \rangle$, both cover morphisms join the identity 0 to e_x. However, only the identity is a witness, because e_x lies in the ideal that 0 generates.

Lemma 4.18. *If P is maximal among the prime ideals associated to the components in a primary decomposition, then* $\mathrm{ann}(P)$ *refines all P'-primary components with* $P' \subsetneq P$.

Proof. Fix a P'-primary component $\approx$ with $P' \subsetneq P$, and choose $p \in P \setminus P'$, so that $\bar{p} \in Q/\approx$ is cancellative. By definition, if $a, b \in Q$ are congruent modulo $\mathrm{ann}(P)$ then $a+p$ and $b+p$ are congruent modulo the original congruence, so $a+p \approx b+p$, and therefore $a \approx b$ by the cancellative property of $\bar{p}$. Thus $\mathrm{ann}(P)$ refines $\approx$. □

Lemma 4.19. *For all primes $P \not\supseteq P'$, the congruence on Q_P induced by any P'-primary congruence on Q is universal on Q_P.*

Proof. Localization adjoins an inverse for a nilpotent element. □

Despite the oddities in Example 2.22, primary decomposition of congruences is combinatorially well-behaved: the associated prime ideals of a congruence reflect which components are necessary in every primary decomposition.

Theorem 4.20. *A prime $P \subset Q$ is associated to a congruence $\sim$ on Q if and only if every primary decomposition of $\sim$ has a P-primary component. Moreover, if P is not associated to $\sim$, then every P-primary component in every primary decomposition of $\sim$ is* **redundant**: *omitting it leaves another primary decomposition of $\sim$.*

Proof. Suppose that a primary decomposition with no P-primary component is given. Working modulo $\sim$, assume that the congruence to be decomposed is the identity congruence on Q. After localizing along P, the induced congruences on Q_P form a primary decomposition of the identity congruence there by Theorem 3.12, with all P'-primary components for $P' \nsubseteq P$ being universal and thus redundant by Lemma 4.19. That is to say, we can assume that P is the maximal monoid prime ideal of Q. Since the primary decomposition has no P-primary component, Lemma 4.18 implies that $\operatorname{ann}(P)$ refines all primary components, and thus it refines their intersection. Thus $\operatorname{ann}(P)$ is trivial and P is not associated.

To prove the rest of the statement, it suffices to show that P is an associated prime of $\sim$ if some primary decomposition of $\sim$ has a P-primary component $\sim_P$ that is *irredundant* in the sense that omitting $\sim_P$ yields a coarser congruence than $\sim$. Write $\approx$ for the (not necessarily primary) common refinement of all other congruences in the decomposition. Thus $\sim_P \cap \approx$ is a nontrivial decomposition of the identity congruence. Choose $a \neq b \in Q$ with $a \approx b$ but $a \nsim_P b$. Let $T = \{t \in Q \mid t+a \sim_P t+b\}$. Since $\sim_P$ is P-primary, the radical of T is P. Modulo Green's relation on Q_P, find a maximal element $\hat{t}$ not in the image of T. If $t \in Q$ maps to $\hat{t}$ then the images of $t+a$ and $t+b$ in Q_P are joined under each cover morphism. Therefore their class is nonsingleton under $\operatorname{ann}(P)$, so one of them is a key witness for P. $\qquad\square$

Theorem 4.20 implies a natural characterization of primary congruences.

Corollary 4.21. *A congruence is primary if and only if it has exactly one associated prime ideal.*

Remark 4.22. Via the Rees congruence construction, primary decomposition of congruences is a refinement of primary decomposition of ideals in monoids. There is an extensive literature on the second type of decomposition surveyed in [Anderson and Johnson 1984]. Our definitions are aligned with those in the literature: the Rees congruence of a monoid ideal is primary if and only if that monoid ideal is primary. In this case its unique associated monoid prime ideal is the unique associated monoid prime ideal of the congruence.

5. Associated prime congruences

Each primary congruence on a finitely generated commutative monoid Q has a unique associated prime ideal. One of the most basic insights in this paper is that a single primary congruence can have several associated prime congruences. The first definition says how a congruence looks near a given $q \in Q$.

Definition 5.1. Fix a prime ideal $P \subseteq Q$, a congruence $\sim$ on Q, and an element $q \in Q$. The *P-prime congruence* of $\sim$ *at q* is the kernel of the morphism $Q \to (\langle \bar{q} \rangle / \langle \bar{q} + P \rangle)_P$ induced by the quotient $Q \to Q/\!\sim\, = \bar{Q}$, addition $\phi_{\bar{q}} : \bar{Q} \to \langle \bar{q} \rangle$, and localization at P.

Definition 5.2. A prime congruence $\approx$ on Q is *associated* to an arbitrary congruence $\sim$ if $\approx$ equals the P-prime congruence of $\sim$ at a key witness for P.

Remark 5.3. The definition implies that the associated prime P of $\approx$ is associated to $\sim$ too. If P is clear from the context, such as after $\approx$ is fixed, then we also speak of a key witness for P simply as a *key witness*.

Lemma 5.4. *If $p, q \in Q$ are equivalent under Green's relation, that is, if $\langle p \rangle = \langle q \rangle$, then their P-prime congruences agree for each P.*

Proof. The same argument as for Lemma 4.6 applies. □

Example 5.5. In the situation of Example 4.16, the associated prime congruences are induced by the ideals $\langle x, y \rangle$, $\langle x, y, z - 1 \rangle$, and $\langle y, z - 1, w - 1 \rangle$. The first two correspond to witnesses for $\langle e_x, e_y \rangle$, while the third corresponds to all of the witnesses for $\langle e_y \rangle$.

The following and Lemma 2.19 are the central finiteness results, reflected in all of the following development, particularly Theorem 8.4.

Theorem 5.6. *Fix a congruence $\sim$ on a finitely generated commutative monoid Q. For each of the finitely many primes P of Q, the key $\sim$-witnesses for P generate only finitely many Green's classes in the localization Q_P along P. Consequently, each congruence on Q has only finitely many associated prime congruences.*

Proof. Since the definition of key witness for P is already local, it suffices to treat the case where P is the maximal ideal of Q. Form a relation on Q by joining every key witness w to a key aide a. This relation is a congruence by the definitions of key witness and key aide. The claim about Green's classes holds because Q is noetherian. To prove the consequence for associated prime congruences, use Lemma 5.4. □

Example 5.7. The congruence in Example 2.18 is primary with respect to the maximal ideal. The (key) witnesses are e_x, e_y, and also $2e_x$, $e_x + e_y$, and $2e_y$, since their class gets joined to nil under ϕ_x and ϕ_y. Although the witnesses look combinatorially different, the only associated prime congruence is the identity

congruence on the monoid $\{0, \infty\}$. This is forced, as the identity is the only cancellative element in $\overline{Q}$.

If on Q the identity congruence is primary, then the assignment of witnesses to their P-prime congruences is order-preserving. It would be interesting to understand which posets of witnesses and associated prime congruences can occur (Problem 17.4).

6. Characterization of mesoprimary congruences

In parallel with the theory of ordinary primary ideals in commutative rings, the mesoprimary condition admits a characterization in terms of associated prime congruences. Definition 2.12 was made with this proposition in mind.

Theorem 6.1. *A congruence is mesoprimary if and only if it has exactly one associated prime congruence.*

Proof. Fix a P-primary congruence $\sim$ on Q. If $\sim$ is mesoprimary and w is not nil, then the P-prime congruence of $\sim$ at w coincides with the P-prime congruence of $\sim$ at the identity because $\overline{w}$ is partly cancellative. The uniqueness of the associated prime congruence follows from the special case where w is a key witness.

On the other hand, assume $\sim$ has a unique associated prime congruence. Then $\sim$ is primary by Corollary 4.21. Replacing Q with $\overline{q}$, assume $\sim$ is the identity congruence on Q. Suppose that a and b are distinct elements whose images in Q_P satisfy $a + u = b$ for some unit $u \in Q_P$. Using the partial order from Lemma 2.19, let $w \in Q$ be any element such that $w + a \neq w + b$ and the image of w modulo the cancellative elements $F \subseteq Q$ is maximal with this property. Let w' be any maximal nonnil element whose image in the poset Q/F is comparable to w but not below. The choices of w and w' make them both key witnesses: w' has ∞ as an aide, and w is verified directly to be a key witness since $p + w = p + (w + a - b)$ in Q_P for all $p \in P$. Replacing w' with $w' + c$ for some cancellative element c if necessary, assume that $w' = w + q$ for some $q \in Q$. Uniqueness of the associated prime congruence, combined with the relation $\phi_{w'} = \phi_q \circ \phi_w$ among addition morphisms, implies that $w' + a \neq w' + b$. By maximality of w' in Q/F, the relation $v + a = v + b$ can only hold for v such that $v + a = \infty$. Thus $\sim$ is partly cancellative. $\square$

Remark 6.2. A primary congruence has only one associated monoid prime ideal by Corollary 4.21. Theorem 6.1 makes precise the notion that further decomposition along the associated prime congruences is natural, as is visible already in Example 1.3.

Quotients by mesoprimary congruences can be described fairly explicitly in terms related to the action in Lemma 3.11. Making this description into a precise

alternative characterization of mesoprimary congruences requires some specialized notions involving monoid actions.

Definition 6.3. The action of a monoid F on an F-module T is *semifree* if

- $t \mapsto f + t$ is an injection $T \hookrightarrow T$ for all $f \in F$, and
- $f \mapsto f + t$ is an injection $F \hookrightarrow T$ for all $t \in T$.

Remark 6.4. The letter "F" stands for "face": in practice, the monoid F is often a face of an affine semigroup, and thinking of it that way is good for intuition.

Lemma 6.5. *An action of a cancellative monoid F on an F-module T is semifree if and only if the localization map $T \hookrightarrow T_\varnothing$ is injective and the universal group $F_\varnothing$ acts freely on $T_\varnothing$.*

Proof. The cancellative condition means that the natural map $F \hookrightarrow F_\varnothing$ is injective. Using this fact, the "if" direction is elementary, and omitted. In the other direction, the semifree case, the first injectivity condition guarantees that $t - f = t' - f' \iff f' + t = f + t'$. In particular, $t - 0 = t' - 0 \iff t = t'$, so the natural map $T \hookrightarrow T_\varnothing$ is injective. The second injectivity condition guarantees that the action of $F_\varnothing$ is free: $(f - f') + (t - w) = t - w \iff (f + t) - (f' + w) = t - w \iff (w + f) + t = (f' + w) + t$, and by the second injectivity condition this occurs if and only if $f + w = f' + w$, which is equivalent to $f = f'$ because F is cancellative. $\square$

In contrast to group actions, monoid actions need not define equivalence relations, because the relation $t \sim f + t$ can fail to be symmetric. The relation is already reflexive and transitive, however, precisely by the two axioms for monoid actions.

Definition 6.6. An *orbit* of a monoid action of F on T is an equivalence class under the symmetrization of the relation $\{(s, t) \mid f + s = t$ for some $f \in F\} \subseteq T \times T$.

Combinatorially, from an F-module T, one can construct a directed graph with vertex set T and an edge from s to t if $t = f + s$ for some $f \in F$. Then an orbit is a connected component of the underlying undirected graph.

Corollary 6.7. *A congruence $\sim$ on a finitely generated commutative monoid Q is mesoprimary if and only if the set F of nonnilpotent elements in $\bar{Q} = Q/\!\sim$ is a cancellative monoid that acts semifreely on $\bar{Q} \setminus \{\infty\}$ with finitely many orbits.*

Proof. Whether we assume the mesoprimary condition on $\sim$ or the condition on the nonnilpotent elements in $\bar{Q}$, we can in each case deduce that $\sim$ is P-primary for some prime $P \subset Q$. The image of $Q \setminus P$ in $\bar{Q}$ is the cancellative submonoid F by definition, which has finitely many orbits by Lemma 2.19. The only feature of the corollary's statement that distinguishes mesoprimary congruences from general primary ones is semifreeness, which we claim is equivalent to uniqueness of the associated prime congruence in Theorem 6.1. Indeed, F acts semifreely if and only if the P-prime congruences at all nonnil elements of $\bar{Q}$ coincide. Those coincidences

certainly imply that the P-prime congruences at all witnesses coincide, in which case $\sim$ is mesoprimary. On the other hand, if $\sim$ is mesoprimary, then the P-prime congruences at all key witnesses coincide. They all coincide with the P-prime congruence at the identity, or else there would be two key witnesses, one sharing its P-prime congruence with the identity and the other not. Since the image in Q/F of every nonnil element of Q lies between the identity and a key witness, the P-prime congruence of every nonnil element is forced to agree with the one shared by the identity and the key witnesses. □

Remark 6.8. As the proof of Corollary 6.7 shows, one interpretation of the structure theorem in the statement is that a P-primary congruence has the same P-prime congruence at every nonnil element as soon as it has the same P-prime congruence at every key witness, and that is what it means to be mesoprimary.

Proposition 6.9. *Given a finite set of congruences on Q, all of which are mesoprimary with the same associated prime congruence, their common refinement is also mesoprimary with the same associated prime congruence.*

Proof. Let $\sim$ be the common refinement of finitely many P-mesoprimary congruences. Then $\sim$ is P-primary by Proposition 3.7. Applying Theorem 6.1, it suffices to show that the P-prime congruence of $\sim$ at any element $q \in Q$ that lies outside the nil class of $\sim$ is the same as the P-prime congruence of $\sim$ at the identity.

Lemma 3.13 implies that we may assume P is the maximal ideal of Q with unit group $G = Q \setminus P$. Under each of the given mesoprimary congruences, Corollary 6.7 (in the guise of Remark 6.8) implies that the class of q is either nil or its intersection with the orbit $G + q$ equals $K + q$, where $K \subseteq G$ is the subgroup that stabilizes (fixes as a set, but not necessarily pointwise) the class of the identity under each of the mesoprimary congruences. Since the nil class contains $K + q$ once it contains q, the class of q under $\sim$ is either nil or its intersection with the orbit $G + q$ equals $K + q$. Having excluded nil by our choice of q, the intersection must be $K + q$. Thus the P-prime congruence at q under $\sim$ coincides with the P-prime congruence at q under (every) one of the mesoprimary congruences modulo which q is not nil.

In particular, letting q be the identity shows that K is the intersection of the identity class of $\sim$ with G. Consequently, the P-prime congruence of $\sim$ at q coincides with the P-prime congruence of $\sim$ at the identity, as desired. □

7. Coprincipal congruences

In commutative rings, irreducible decomposition underlies primary decomposition. Analogously, coprincipal decomposition underlies mesoprimary decomposition of commutative monoid congruences (but see the remarks and examples after Theorem 8.4).

Definition 7.1. A *peak* of a monoid Q is a nonnil element $q \in Q$ such that $q + a = \infty$ for all nonunit $a \in Q$. The *cogenerators* of a P-primary congruence on Q are the elements of Q whose images in $\bar{Q}_P$ are peaks.

Definition 7.2. A congruence $\sim$ on Q is *coprincipal* if it is P-mesoprimary for some monoid prime P and additionally the quotient of $\bar{Q}_P$ modulo its Green's relation has precisely one peak.

Example 7.3. The congruence in Example 2.18 is coprincipal. It is P-mesoprimary for $P = Q \setminus \{0\}$ and its unique peak is the class of 2.

Definition 7.4. Fix a congruence on Q with quotient $\bar{Q}$. The *order ideal* $Q^P_{\preceq q}$ *cogenerated by* $q \in Q$ *at a prime ideal* $P \subset Q$ consists of those $a \in Q$ whose image precedes that of q in the partially ordered quotient of $\bar{Q}_P$ modulo its Green's relation (Lemma 2.6).

Example 7.5. Let $\sim$ be the congruence on $\mathbb{N}$ induced by the binomial ideal $\langle x^3 - x^6 \rangle \subset \Bbbk[x]$. Set $P = \langle e \rangle$, where $e = e_x$ is the generator of $\mathbb{N}$.

(1) The order ideal $\mathbb{N}^P_{\preceq e}$ consists of e itself and $0 \in \mathbb{N}$.

(2) Including $2e$ yields the order ideal $\mathbb{N}^P_{\preceq 2e} = \{0, e, 2e\}$.

(3) The order ideals $\mathbb{N}^P_{\preceq q}$ for $q = me$ with $m \geq 3$ all coincide with $\mathbb{N}$ itself. Thus, in general, order ideals $Q^P_{\preceq q} \subseteq Q$ need not be finite, although their images in $\bar{Q}_P$ modulo Green's relation always are.

(4) The order ideals $\mathbb{N}^{\varnothing}_{\preceq q}$ for $q \in \mathbb{N}$ all coincide with $\mathbb{N}$ itself.

Example 7.6. Let $\sim$ be the identity congruence on $Q = \mathbb{N}^3$, and set $P = \langle e, f \rangle$, where e, f are two of the three generators of $\mathbb{N}^3$, the third being g. The order ideal $Q^P_{\preceq e+f+2g}$ consists of the lattice points on the nonnegative g-axis together with their translates by e, f, and $e + f$. The answer would have been the same had $e + f + 2g$ been replaced by $e + f$, or $e + f + g$, or $e + f + mg$ for any $m \in \mathbb{N}$.

Definition 7.7. Fix a congruence $\sim$. The congruence *cogenerated by q along P* is the coarsening $\sim^P_q$ of $\sim$ obtained by first joining any pair of elements in $Q \setminus Q^P_{\preceq q}$ and also joining any pair $(a, b) \in Q$ such that

(i) the images $\bar{a}$ and $\bar{b}$ in $\bar{Q}_P$ differ by a unit in $\bar{Q}_P$, and

(ii) $\bar{c} + \bar{a} = \bar{c} + \bar{b} = \bar{q} \in \bar{Q}_P$ for some $c \in Q_P$.

Example 7.8. The congruence $\sim^P_q$ in Definition 7.7 need not be primary, and hence it need not be coprincipal. Essentially, the prime P has to be small enough to foster the mesoprimary condition. In Example 4.17.2, the congruence cogenerated by $q = e_x$ along $P' = \{e_x, \infty\}$ is not primary. However, along $P = \{\infty\}$, localization inverts more, causing e_x to be joined with 0, resulting in a primary — and hence coprincipal — congruence.

Proposition 7.9. *Fix a congruence $\sim$ and a witness w for a prime P. All elements of P are nilpotent modulo the congruence $\sim_w^P$, whose nil class is $Q \setminus Q_{\leq w}^P$.*

Proof. Given an aide w' for w and a generator p of P, one of two things must happen, and in both cases $p + w$ is nil modulo $\sim_w^P$. Write $[q]$ for the Green's class of $\bar{q} \in \bar{Q}_P$.

(1) $[w] \neq [w']$. In this case, either $[w] < [w']$ or $[w]$ and $[w']$ are incomparable, but these both imply that w' maps to nil modulo the coprincipal congruence $\sim_w^P$, so $p + w = p + w'$ is nil modulo $\sim_w^P$.

(2) $[w] = [w']$; that is, their images lie in the same Green's class. In this case, $[p + w] > [w]$ by Lemma 2.8, since addition by p joins $[w]$ to $[w']$.

Since p is an arbitrary generator of P, it follows that $P + w$ is nil modulo $\sim_w^P$. This implies that every element of P is nilpotent modulo $\sim_w^P$, as follows. There are only finitely many Green's classes beneath $[w]$, so the Green's classes of multiples of any given nonunit element $a \in Q_P / \sim_w^P$ are not all distinct: there must be repeats. Suppose $[\alpha \cdot a] = [\beta \cdot a]$ for some positive integers $\alpha < \beta$. Every nonnil element of $Q_P / \sim_w^P$ precedes $\bar{w}$ in Green's preorder. Therefore, if neither $\alpha \cdot a$ nor $\beta \cdot a$ is nil, then there is some $c \in Q$ such that $[\alpha \cdot a] + c = [w]$, whence

$$[w] = [\beta \cdot a] + c = (\beta - \alpha) \cdot a + [\alpha \cdot a] + c = (\beta - \alpha) \cdot a + [w] \subseteq P + [w]$$

is nil modulo $\sim_w^P$, contradicting the choice of w.

The statement about the nil class holds because $Q \setminus Q_{\leq w}^P$ is an ideal of Q (so its image is nil) that does not contain w itself (so the image of w is not made nil by the first relations in Definition 7.7) or any element in $Q_{\leq w}^P$ (so none of the relations defined by (i) and (ii) in Definition 7.7 make w or any other element of $Q_{\leq w}^P$ nil). $\square$

Remark 7.10. Proposition 7.9 can fail if w is merely an aide — even a key aide. The not-exclusively-maximal property of a witness guarantees existence of an aide that can be set congruent to nil modulo the coprincipal congruence without forcing w to be nil as well. In Example 4.17.2, for instance, there is no way to define a coprincipal congruence cogenerated by e_x in such a way that e_x is nilpotent without it being nil.

Theorem 7.11. *Given a congruence $\sim$, the congruence $\sim_w^P$ cogenerated by any witness w for P is coprincipal, with associated prime ideal P.*

Proof. Every nonunit in the localization $Q_P / \sim_w^P$ of the quotient monoid $Q / \sim_w^P$ along P is nilpotent by Proposition 7.9. The statement about the nil class in that same proposition implies that the Green's class of w is the unique peak. The localization morphism $Q / \sim_w^P \to Q_P / \sim_w^P$ is injective by condition (i) in Definition 7.7. Condition (ii) there forces the P-prime congruence at the identity to equal the P-prime congruence at w, which consequently forces the P-prime congruences at

all nonnil elements to coincide, since they lie between the P-prime congruences at the identity and at w. Therefore the action of the unit group of $Q_P/\sim_w^P$ on its nonnilpotent elements is free. The proof is complete by Corollary 6.7, using the characterization of semifreeness in Lemma 6.5. $\square$

Definition 7.12. If w is a witness for an associated P-prime congruence of $\sim$, then the congruence $\sim_w^P$ is the *coprincipal component* of $\sim$ cogenerated by w along P. If the prime ideal P is clear from context, e.g., if w is already specified to be a witness for P, then we simply speak of the coprincipal component cogenerated by w.

Example 7.13. Consider the congruence on $\mathbb{N}^2$ induced by $I = \langle x^3 - x^2, y^3 - y^2 \rangle$. The quotient $Q = \mathbb{N}^2/\sim_I$ has nine elements, with the class of $2e_x + 2e_y$ being nil. The quotient also has two idempotents, namely the classes of $2e_x$ and $2e_y$. Neither of the congruences cogenerated by $q = e_x + 2e_y$ and $q = e_y + 2e_x$ along $P = \langle e_x, e_y \rangle$ is primary; however, these elements are not P-witnesses. In fact, there are no P-witnesses: the maximal ideal is not associated. In contrast, the coprincipal components for the witnesses $(2e_2, \langle e_1 \rangle)$ and $(2e_1, \langle e_2 \rangle)$ are mesoprimary, as per Theorem 7.11.

Example 7.14. In the setting of Example 7.5, the coprincipal component of $\sim$ cogenerated by any $q \in \mathbb{N}$ along $\varnothing$ is induced by the binomial ideal $\langle 1 - x^3 \rangle$. The component cogenerated by the key witness $2e$ along $\langle e \rangle$ is induced by the binomial ideal $\langle x^3 \rangle$.

Proposition 7.15. *Given any witness w for an associated P-prime congruence of $\sim$, the coprincipal component of $\sim$ cogenerated by w along P is refined by $\sim$.*

Proof. Starting from $\sim$ the coprincipal component is formed by identifying additional pairs of elements. $\square$

Proposition 7.16. *Any mesoprimary congruence $\sim$ equals the common refinement of the coprincipal components of $\sim$ cogenerated by the cogenerators of $\sim$.*

Proof. Fix a P-mesoprimary congruence $\sim$. By Proposition 7.15 each coprincipal component at a cogenerator coarsens $\sim$. On the other hand, suppose that $q \not\sim q'$. Let $\bar{q}$ and $\bar{q}'$ denote their images in the localized quotient $\bar{q}_P$. By mesoprimariness, $\bar{q} \neq \bar{q}'$. Modulo Green's relation on $\bar{q}_P$, every element precedes a peak. If exactly one of $\bar{q}$ and $\bar{q}'$ precedes some peak $\bar{w}$, then modulo $\sim_w^P$ exactly one of q and q' maps to nil, so they are incongruent. If no such peak exists, then $\bar{q}$ and $\bar{q}'$ both precede some peak $\bar{w}$. For $\bar{q}$ and $\bar{q}'$ to be joined by $\sim_w^P$ they must differ by a unit and satisfy $\bar{q} + \bar{c} = \bar{q}' + \bar{c} = \bar{w}$ for some $c \in Q_P$, all by Definition 7.7. However, since $\sim$ is mesoprimary, $\bar{q} + \bar{c} = \bar{q}' + \bar{c}$ implies that both sides are nil. Consequently, $q \not\sim_w^P q'$. $\square$

8. Mesoprimary decompositions of congruences

Definition 8.1. Fix a congruence $\sim$ on a finitely generated commutative monoid Q.

(1) An expression of $\sim$ as the common refinement of finitely many mesoprimary congruences is a *mesoprimary decomposition* if, for each mesoprimary congruence $\approx$ that appears in the decomposition with associated prime ideal $P \subset Q$, the P-prime congruences of $\sim$ and $\approx$ at every cogenerator of $\approx$ coincide.

(2) Each mesoprimary congruence that appears is a *mesoprimary component* of $\sim$.

(3) If every cogenerator of every P-mesoprimary component $\approx$ is a key $\sim$-witness for P, then the decomposition is a *key* mesoprimary decomposition.

Example 8.2. According to Definition 8.1, the decomposition in Example 2.22 is not a mesoprimary decomposition because the intersectands are not components of the identity congruence: the combinatorics at the witnesses for the mesoprimary congruences in the decomposition do not agree with the combinatorics of the identity congruence. More precisely, the $\varnothing$-prime congruence at each element of $\mathbb{N}^2$ is the identity congruence, not the congruence induced by $\langle x - 1 \rangle$ or $\langle y - 1 \rangle$.

Theorem 8.3. *Every congruence on a finitely generated commutative monoid admits a key mesoprimary decomposition.*

Proof. Two examples are the decompositions in Theorem 8.4 and Corollary 8.11, by Remark 8.5 and finiteness of the set of Green's classes of witnesses in Theorem 5.6. □

In the remainder of this section, Convention 4.8 leads to some simplification of terminology. The first statement to benefit is our first main decomposition theorem (the other being Corollary 8.11), which generalizes to arbitrary monoid congruences the notion of irreducible decomposition for monoid ideals; see Examples 8.6 and 8.7.

Theorem 8.4. *Every congruence on a finitely generated commutative monoid is the common refinement of the coprincipal congruences cogenerated by its key witnesses.*

Proof. Fix a congruence $\sim$ on Q. Proposition 7.15 implies that the intersection of all of the coprincipal congruences for witnesses is refined by $\sim$. On the other hand, suppose that $q \not\sim q'$ for two elements $q, q' \in Q$. The proof is done once we find a prime $P \subset Q$ and a key witness $w \in Q$ whose coprincipal congruence $\sim_w^P$ on Q fails to join q to q'.

Let $T = \{t \in Q \mid t + q \sim t + q'\}$ be the ideal of elements joining q to q'. Fix a prime ideal P minimal among primes of Q containing T. The images $\hat{q}$ and $\hat{q}'$ of q and q' in the localization Q_P remain incongruent because P contains T. In contrast, every element in the localized image T_P joins $\hat{q}$ to $\hat{q}'$; that is, $\hat{t} + \hat{q} \sim \hat{t} + \hat{q}'$ for all $\hat{t} \in T_P$. Since the maximal ideal P_P of Q_P is minimal over T_P by minimality of P over T, there is a maximal Green's class among those represented by the elements

$\{\hat{t} \in Q_P \mid \hat{t} + \hat{q} \not\succ \hat{t} + \hat{q}'\}$. If the image of t lies in such a maximal Green's class, then in Q at least one of the elements $w = t + q$ and $w' = t + q'$ — namely one whose image in $\bar{Q}_P$ is not strictly greater than the other under Green's preorder — is a key witness by definition. Assuming, by symmetry, that w is a key witness, the localization of the congruence $\sim_w^P$ satisfies $\hat{q} \not\succ_w^P \hat{q}'$, so $q \not\succ_w^P q'$ before localization. $\qquad\square$

Remark 8.5. In Theorem 8.4 it makes no difference whether one uses all the key witnesses or just one per Green's class. This follows instantly from the definition of a coprincipal component; indeed, for a given Green's class of key witnesses, the coprincipal components are all equal — not just equivalent, but literally the same congruence.

Example 8.6. For a monomial ideal in an affine semigroup ring, the coprincipal decomposition of the Rees congruence afforded by Theorem 8.4 arises equivalently from the Rees congruences of the components in the unique irredundant irreducible decomposition into monomial ideals [Miller 2002, Theorem 2.4]; see also [Miller and Sturmfels 2005, Corollary 11.5 and Proposition 11.41].

Example 8.7. Unlike the case in Example 8.6, the decomposition in Theorem 8.4 can be redundant in general. This happens for the congruence in Example 4.15(1). The decomposition produced by Theorem 8.4 has three mesoprimary components: $\sim_w^P$ for $P = \langle e_x, e_y \rangle$ and $w \in \{(e_x, 0), (0, e_y)\}$ arise from joining e_y and e_x, respectively, to nil. A third component $\sim^\varnothing$ arises for $P = \varnothing$ (with any element as a witness) and is induced by $\langle x - y \rangle$. The decomposition into three congruences is redundant: the given congruence is already the common refinement of $\sim^\varnothing$ and either of $\sim_w^P$, the point being that once $\sim^\varnothing$ is given, one only needs to separate $(1, 0)$ from $(0, 1)$. That said, the points $(1, 0)$ and $(0, 1)$ represent distinct Green's classes of key witnesses for the associated prime congruence induced by the binomial ideal $\langle x, y \rangle$. There is simply no way of constructing an irredundant coprincipal decomposition without breaking the symmetry: no systematic method of eliminating one of the redundant components in this example would have a way to choose between them.

Remark 8.8. A coprincipal congruence can have more than one Green's class of key witnesses, such as Example 2.18. In any such case the mesoprimary decomposition from Theorem 8.4 produces more than one coprincipal component. By Proposition 7.16, however, it is guaranteed that the original congruence appears as the component for the Green's class of the unique peak, and thus all other components are redundant. This phenomenon prevents arbitrary coprincipal congruences from accurately reflecting the combinatorics of irreducible decomposition of binomial ideals. One irreducible decomposition of the coprincipal ideal $I = \langle x^2 - xy, xy - y^2, x^3 \rangle$ from Example 2.18 is $I = \langle x - y, x^3 \rangle \cap \langle x^2, y \rangle \cap \langle x, y^2 \rangle$, as can be seen by applying [Vasconcelos 1998, Proposition 3.1.7].

Remark 8.9. Any irreducible congruence is mesoprimary: if a congruence is not mesoprimary then it has at least two associated prime congruences by Theorem 6.1, and then it is reducible by mesoprimary decomposition. However, irreducible decompositions of congruences do not, in general, reflect the combinatorics of congruences in a manner that is witnessed combinatorially by the congruence itself.

Lemma 8.10. *Every cogenerator of the common refinement of a finite set of P-mesoprimary congruences is a cogenerator of one of the given mesoprimary congruences.*

Proof. If w is a cogenerator of the common refinement $\sim$, then w is not nil modulo $\sim$, so w is not nil modulo (at least) one of the given mesoprimary congruences. On the other hand, $p+w$ is nil modulo $\sim$ for all $p \in P$, whence $P+w$ is nil modulo each one of the given mesoprimary congruences. Therefore w is a cogenerator of each of the given mesoprimary congruences modulo which it is not nil. □

Combining Theorem 8.4 with Proposition 6.9 and Lemma 8.10 yields the next result, culminating our study of commutative monoid congruence decompositions.

Corollary 8.11. *Every congruence on a finitely generated commutative monoid admits a key mesoprimary decomposition with one component per associated prime congruence.*

Example 8.12. In general, the set of key witnesses is properly contained in the set of witnesses. Example 4.15(3) shows one way this can happen. Exploiting the weirdness of irreducible decomposition of the identity congruence is not necessary: consider the primary congruence induced by the (cellular) binomial ideal

$$I = \langle a^2 - 1,\, b^2 - 1,\, x(b-1),\, y(a-1),\, z(a-b),\, x^2,\, y^2,\, z^2 \rangle.$$

The geometry of the quotient is shown here, where $\mathbb{Z}_2^\delta$ is the diagonal copy of $\mathbb{Z}_2$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$, i.e., the copy generated by $(1, 1)$:
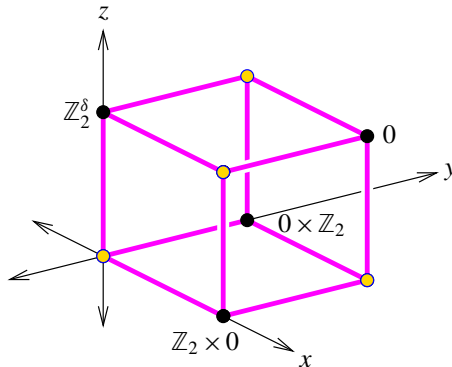
The solid dots indicate key witnesses and are labeled with quotients of $\overline{Q}$ modulo the corresponding stabilizers, under the action from Lemma 3.11. The origin is not a

key witness because the common refinement of the three kernels of the addition morphisms is trivial. According to Theorem 8.4, a coprincipal mesoprimary decomposition of $\sim_I$ is induced by the following decomposition of I into unital binomial ideals:

$$I = \langle a-1, b-1, z^2, y^2, x^2 \rangle \cap \langle a^2-1, b-1, z, y, x^2 \rangle$$
$$\cap \langle a-1, b^2-1, z, x, y^2 \rangle \cap \langle ab-1, a-b, y, x, z^2 \rangle.$$

The heart of the remainder of this paper — the ring-theoretic part — is to make the corresponding decomposition of arbitrary (nonunital) binomial ideals precise. For reference, the primary decomposition of I is

$$I = \langle a-1, b-1, z^2, y^2, x^2 \rangle \cap \langle a+1, b-1, z, y, x^2 \rangle$$
$$\cap \langle a-1, b+1, z, x, y^2 \rangle \cap \langle a+1, b+1, y, x, z^2 \rangle.$$

9. Augmentation ideals, kernels, and nils

One of our goals is to compare the combinatorics of congruences on a commutative monoid Q in purely monoid-theoretic settings with their ring-theoretic counterparts. It is therefore important to note that various binomial ideals $I \subset \Bbbk[Q]$ can induce the same congruence on Q. One way for this to happen is an arithmetic way, via binomials involving the same monomials but different sets of coefficients; this occurs for binomial primes $I_{\rho, P}$ whose characters share their domain of definition (see Section 12).

Example 9.1. Let $\mathrm{char}(\Bbbk) \neq 2$. In the polynomial ring $\Bbbk[x, y, z]$, both of the ideals $I = \langle x(z-1), y(z-1), z^2-1, x^2, xy, y^2 \rangle$ and $I' = \langle x(z-1), y(z+1), z^2-1, x^2, y^2 \rangle$ induce the same congruence; note that I' contains $\langle xy \rangle$, so the only difference between these two ideals is the character on $\mathbb{Z} = \{0\} \times \{0\} \times \mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ induced by the monomials $y, zy, z^2y, \ldots$ due to the generator $y(z+1)$ instead of $y(z-1)$.

Another way, demonstrated in parts (3) and (4) of Example 2.17, is combinatorial: when Q has a nil ∞, the binomial ideal $\langle t^\infty \rangle$ induces the same (trivial) congruence on Q as the zero ideal $\langle 0 \rangle \subseteq \Bbbk[Q]$. Nils are the only way for this to occur.

Lemma 9.2. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$ whose congruence $\sim_I$ is trivial (every class is a singleton). Then $I = 0$ or $I = \langle t^\infty \rangle$ for a nil $\infty \in Q$.*

Proof. If $I \neq 0$ then I must be a monomial ideal with a unique monomial, or else the congruence $\sim_I$ has a class of size at least 2. Hence the result follows because a monoid can have at most one nil. $\square$

Definition 9.3. If $\infty \in Q$ is a nil, then the *truncated algebra* is $\Bbbk[Q]^- := \Bbbk[Q]/\langle t^\infty \rangle$. By convention, if Q has no nil, then we set $\Bbbk[Q]^- := \Bbbk[Q]$.

Remark 9.4. Truncated algebras arise naturally from monoid algebras because of differences in the way quotients of monoids and monoid algebras by ideals are formed. If $F \subseteq Q$ is a monoid ideal and $\sim_F$ its Rees congruence, the quotient $\Bbbk[Q] \to \Bbbk[Q]/M_F$ modulo the monomial ideal $M_F = \langle t^f \mid f \in F \rangle$ equals $\Bbbk[Q/\sim_F]^-$ rather than $\Bbbk[Q/\sim_F]$ itself. We shall see that if Q has a nil, then $\Bbbk[Q]$ and $\Bbbk[Q]^-$ reflect certain aspects of the algebra of Q to varying degrees of accuracy.

More generally, if the congruence induced by a (not necessarily unital) binomial ideal I results in a quotient $Q/\sim_I$ that has a nil, then throwing in monomials from the nil class results in an ideal that determines the same congruence.

Proposition 9.5. *Fix a binomial ideal* $I \subseteq \Bbbk[Q]$. *The only binomial ideals containing* I *that determine the same congruence* $\sim_I$ *are* I *itself and, if* $\overline{Q} = Q/\sim_I$ *has a nil* ∞, *the ideal* $I + \langle t^q \mid \overline{q} = \infty \rangle$, *where the bar denotes passage from* $q \in Q$ *to its image* $\overline{q} \in \overline{Q}$.

Proof. Under the grading of the quotient algebra $\Bbbk[Q]/I$ by $\overline{Q} = Q/\sim_I$, the dimension of the graded piece $(\Bbbk[Q]/I)_{\overline{q}}$ as a vector space over $\Bbbk$ is either 0 or 1, depending on whether I contains a monomial in the corresponding class. Since the (exponents on) monomials in I form a single class, the dimension can only be 0 for at most one $\overline{q}$, and $\overline{q}$ must be a nil in $\overline{Q}$. Now note that $\Bbbk[Q]/I$ is close enough to the monoid algebra $\Bbbk[\overline{Q}]$ for the argument from Lemma 9.2 to work, and lift the result from $\Bbbk[Q]/I$ to $\Bbbk[Q]$. $\square$

The two binomial ideals in Proposition 9.5 are unequal precisely when I contains no monomials, and in this case it is trivial to form the second ideal by inserting monomials. In special circumstances, it is possible to reverse this procedure. To this end, we wish to examine the transition from $\Bbbk[Q]$ to the truncated algebra $\Bbbk[Q]^-$ (when Q has a nil) in terms of primary decomposition of binomial ideals. This naturally leads to the following concept refining that of a nil.

Definition 9.6. A *kernel* of a commutative monoid Q is a nonempty ideal contained in all nonempty ideals of Q. (Such an ideal might not exist.)

Example 9.7. A nil is the same thing as a kernel of cardinality 1.

The existence of a nil in Q, or a finite kernel more generally, is reflected by a certain kind of maximal ideal of $\Bbbk[Q]$ being an associated prime of $\Bbbk[Q]$.

Definition 9.8. Fix a commutative monoid Q, and write $\Bbbk^* = \Bbbk \setminus \{0\}$. The *unital augmentation ideal* in the monoid algebra $\Bbbk[Q]$ is the ideal

$$I^1_{\mathrm{aug}} := \langle t^q - 1 \mid q \in Q \rangle$$

generated by all monomial differences. More generally, an *augmentation ideal* for a given binomial ideal $I \subseteq \Bbbk[Q]$ is a proper ideal of the form

$$I_{\mathrm{aug}} := \langle t^q - \lambda_q \mid q \in Q, \lambda_q \in \Bbbk^* \rangle \subseteq \Bbbk[Q]$$

such that $I \cap I_{\text{aug}}$ is a binomial ideal.

Example 9.9. The ideal $I = \langle x^2 \rangle \subset \Bbbk[x, y]$ induces a primary congruence (a Rees congruence) identifying all monomials in I. A compatible augmentation ideal is $I_{\text{aug}} = \langle x-1, y-1 \rangle$, which satisfies $I \cap I_{\text{aug}} = \langle x^2 - x^3, yx^2 - x^2 \rangle$. This intersection induces the same congruence $\sim$ as I does. Note that $\Bbbk[x, y]/(I \cap I_{\text{aug}}) \cong \Bbbk[\mathbb{N}^2/\sim]$ is isomorphic to the semigroup algebra of $\mathbb{N}^2/\sim$ while $\Bbbk[\mathbb{N}^2]/I \cong \Bbbk[\mathbb{N}^2/\sim]^-$ is the truncated algebra.

Lemma 9.10. *Given an augmentation ideal I_{aug} as in Definition 9.8, the association $q \mapsto \lambda_q$ constitutes a monoid homomorphism $\phi : Q \to \Bbbk^*$.*

Proof. The maximal ideals of $\Bbbk[Q]$ with residue field $\Bbbk$ are in bijection with the monoid homomorphisms $Q \to \Bbbk$; Definition 9.8 guarantees that the image lies in $\Bbbk^*$. □

Proposition 9.11. *Fix a monoid algebra $\Bbbk[Q]$ over a field $\Bbbk$, with Q finitely generated. An augmentation ideal is associated to $\Bbbk[Q]$ if and only if Q has a finite kernel, and in that case the unital augmentation ideal is associated to $\Bbbk[Q]$.*

Proof. If Q has a finite kernel K, then I_{aug}^1 is the annihilator of the sum $f = \sum_{k \in K} t^k$. Indeed, $q + K \subseteq K$ is an ideal of $Q \implies q + K = K$ for all $q \in Q \implies t^q f = f$ for all $q \in Q \implies (t^q - 1)f = 0$ for all $q \in Q \implies I_{\text{aug}}^1 \subseteq \text{ann}(f)$; but I_{aug}^1 is a maximal ideal.

Now suppose that an augmentation ideal I_{aug} is associated to $\Bbbk[Q]$. The homomorphism $q \mapsto \lambda_q$ in Lemma 9.10 induces an automorphism of $\Bbbk[Q]$ that rescales the monomials by $t^q \mapsto \lambda_q t^q$. This automorphism takes I_{aug} to I_{aug}^1. Therefore, we may as well assume $I_{\text{aug}} = I_{\text{aug}}^1$ is the unital augmentation ideal. Let $K \subseteq Q$ be a nonempty subset such that $f = \sum_{k \in K} \mu_k t^k$ is annihilated by I_{aug}^1, where $\mu_k \in \Bbbk^*$ for all $k \in K$. It suffices to show that K is a kernel of Q. But $t^q f = f$ for all $q \in Q$ implies that $q + K = K$ for all $q \in Q$, which implies both that K is an ideal of Q (since $q + K \subseteq K$ for all q) and also that K is contained in every ideal of Q (since $K + q \supseteq K$). □

Theorem 9.12. *If $I_\ell \supset \cdots \supset I_0$ is a chain of distinct binomial ideals in $\Bbbk[Q]$ inducing the same congruence on Q, then $\ell \leq 1$. Moreover, if $\ell = 1$ then I_1 contains monomials and I_0 does not: $I_0 = I_1 \cap I_{\text{aug}}$ for an augmentation ideal I_{aug} compatible with I_1.*

Proof. The first sentence follows from Proposition 9.5, as does the statement about monomials when $\ell = 1$. It remains to show that $I_0 = I_1 \cap I_{\text{aug}}$ if $\ell = 1$. Set $I = I_0$. Under the grading of the quotient algebra $\Bbbk[Q]/I$ by $\bar{Q} = Q/\sim_I$, the dimension of the graded piece $(\Bbbk[Q]/I)_{\bar{q}}$ as a vector space over $\Bbbk$ is 1 for all $\bar{q} \in \bar{Q}$. Let $\overline{\infty} \in \bar{Q}$ be the nil, which exists because it is the class of all exponents on monomials in I_1. Fix a nonzero element $t^{\overline{\infty}} \in \Bbbk[Q]/I$ of degree $\overline{\infty}$. Then $t^q t^{\overline{\infty}} = \lambda_q t^{\overline{\infty}}$ for each

$q \in Q$. Set $I_{\text{aug}} = \langle t^q - \lambda_q \mid q \in Q \rangle$. Then $I_{\text{aug}} \supseteq I$ by construction, but $I_{\text{aug}} \not\supseteq I_1$, since I_1 contains monomials and I_{aug} does not. Therefore $I_1 \supsetneq I_1 \cap I_{\text{aug}} \supseteq I$, whence $I_1 \cap I_{\text{aug}} = I$, because $I_1/I = \langle t^{\overline{\infty}} \rangle \subseteq \Bbbk[Q]/I$ has dimension 1 as a vector space over $\Bbbk$ by Proposition 9.5. $\qquad\square$

Example 9.13. The ideal $I = \langle x^2 - xy, xy - 2y^2 \rangle \subseteq \Bbbk[x, y]$ contains monomials even when char($\Bbbk$) $\neq 2$, because I contains both of $x^2 y - xy^2$ and $x^2 y - 2xy^2$, so $x^2 y$ and xy^2 lie in I. However, Theorem 9.12 implies that there is no augmentation ideal compatible with I. Indeed, every binomial ideal I' contained in I and inducing the same congruence necessarily contains a binomial of the form $x^2 - \lambda xy$ and one of the form $xy - \mu y^2$, so I' contains both $x^2 - xy$ and $xy - 2y^2$ (and therefore $I' = I$) since $xy \notin I$.

10. Taxonomy of binomial ideals in monoid algebras

The concepts of primary, mesoprimary, primitive, prime, and toric congruence from Definition 2.12 have precise analogues for binomial ideals in monoid algebras. As a small measure to aid the reader with conflicting usages of the terms "primary" and "prime", long since immovably set in the literature, the items in the following definition are listed in the order corresponding exactly to Definition 2.12, as Theorem 10.6 makes precise; for quick reference, consult the following table.

…congruence on Q	…binomial ideal in $\Bbbk[Q]$
primary	cellular
mesoprimary	mesoprimary
primitive	primary
prime	mesoprime
toric	prime

This table explains our choice of terminology: "mesoprimary" sits between the two occurrences of "primary", being stronger than one and weaker than the other.

Our choice to work over fields that need not be algebraically closed forces us to consider slight generalizations of group algebras.

Definition 10.1. A *twisted group algebra* over a field $\Bbbk$ is a $\Bbbk$-algebra that is graded by a group G and, after tensoring with the algebraic closure $\overline{\Bbbk}$, is isomorphic to the group algebra $\overline{\Bbbk}[G]$ via a G-graded isomorphism. A *monomial homomorphism* from a monoid algebra to a twisted group algebra takes each monomial to a homogeneous element (possibly 0).

Example 10.2. The ring $R = \mathbb{Q}[x]/\langle x^3 - 2 \rangle$ is not isomorphic to the group algebra $\mathbb{Q}[G]$ for $G = \mathbb{Z}/3\mathbb{Z}$ over $\mathbb{Q}$, because no element of R is a cube root of 2. On the other hand, the element $y = x\sqrt[3]{2} \in R_{\mathbb{C}} := R \otimes_{\mathbb{Q}} \mathbb{C}$ generates $R_{\mathbb{C}}$, yielding the

presentation $R_{\mathbb{C}} = \mathbb{C}[y]/\langle y^3 - 1 \rangle \cong \mathbb{C}[G]$. Therefore R is a nontrivial twisted group algebra for the group $G = \mathbb{Z}/3\mathbb{Z}$ over the rational numbers $\mathbb{Q}$.

Generalizing the manipulations in Example 10.2 yields the following.

Proposition 10.3. *The twisted group algebras R over $\Bbbk$ (for a finitely generated group G) are precisely the quotients of Laurent polynomial rings over $\Bbbk$ by binomial ideals.*

Proof. Let R be a twisted group algebra. Every G-graded piece of R has dimension $\dim_{\Bbbk}(R_g) = 1$ for all $g \in G$, because this is true after tensoring with $\bar{\Bbbk}$ by definition. Thus R admits a binomial presentation $R \cong \Bbbk[\mathbb{N}^n]/I$ [Eisenbud and Sturmfels 1996, Proposition 1.11]. Every monomial $x^u \in \Bbbk[\mathbb{N}^n]$ becomes invertible in R because every such monomial becomes invertible in $R\bar{\Bbbk} := R \otimes_{\Bbbk} \bar{\Bbbk}$. Therefore $R \cong \Bbbk[\mathbb{Z}^n]/I$ is a binomial quotient of a Laurent polynomial ring. On the other hand, the characterization of Laurent binomial ideals I [Eisenbud and Sturmfels 1996, Theorem 2.1] (or see Lemma 11.10, below) implies that there is a unique sublattice $L \subseteq \mathbb{Z}^n$ and character $\sigma : L \to \Bbbk$ such that $I = \langle x^q - \sigma(q) \mid q \in L \rangle$. Over $\Bbbk$, not much more can be said, in general; but over $\bar{\Bbbk}$, the fact that $\bar{\Bbbk}^*$ is an injective abelian group implies that σ extends to a character $\rho : \mathbb{Z}^n \to \bar{\Bbbk}^*$. If y_i is the image in $R\bar{\Bbbk}$ of $\rho(x_i)x_i \in \bar{\Bbbk}[\mathbb{Z}^n]$, then naturally $R\bar{\Bbbk} = \bar{\Bbbk}[y_1, \ldots, y_n] = \bar{\Bbbk}[G]$ for $G = \mathbb{Z}^n/L$. $\square$

Definition 10.4. A binomial ideal $I \subset \Bbbk[Q]$ in the monoid algebra for a monoid Q is

(1) *cellular* if every monomial $t^q \in \Bbbk[Q]/I$ is either nilpotent or a nonzerodivisor;

(2) *mesoprimary* if it is maximal among the proper binomial ideals inducing a given mesoprimary congruence (as per Theorem 9.12);

(3) *primary* if the quotient $\Bbbk[Q]/I$ has precisely one associated prime ideal;

(4) *mesoprime* if I is the kernel of a monomial homomorphism from $\Bbbk[Q]$ to a twisted group algebra over $\Bbbk$;

(5) *prime* if $\Bbbk[Q]/I$ is an integral domain: $fg = 0$ in $\Bbbk[Q]/I$ implies $f = 0$ or $g = 0$.

Remark 10.5. The maximality for a mesoprimary ideal $I \subseteq \Bbbk[Q]$ amounts to stipulating that the nil class of $\sim_I$ consists of elements $q \in Q$ with $t^q \in I$, the alternative being that none of these monomials lie in I but differences of scalar multiples thereof do.

Theorem 10.6. *For* $\alpha \in \{1, 2, 4\}$, *a binomial ideal* I *satisfies condition* (α) *of Definition 10.4 if and only if its induced congruence satisfies condition* (α) *of Definition 2.12 and* I *is maximal among proper ideals inducing that congruence. For* $\alpha = 5$, *the same holds if* $\Bbbk$ *is algebraically closed. For* $\alpha = 3$, *the condition in Definition 2.12 implies the one in Definition 10.4 in general, and the converse holds if* $\Bbbk$ *is algebraically closed of characteristic* 0.

Proof. Fix a binomial ideal I and use notation as in Definition 2.12 for $\sim\, = \,\sim_I$. We first assume that I satisfies Definition 10.4(α) and show that I satisfies Definition 2.12(α).

(1) If a monomial $t^q \in \Bbbk[Q]/I$ is nilpotent or a nonzerodivisor then the image $\bar{q} \in \bar{Q}$ of q is nilpotent or cancellative, respectively.

(2) By definition.

(3) Pick a presentation $\mathbb{N}^n \twoheadrightarrow Q$. The kernel of the induced surjection $\Bbbk[\mathbb{N}^n] \twoheadrightarrow \Bbbk[Q]$ is a binomial ideal [Gilmer 1984, §7], so the preimage of I in $\Bbbk[\mathbb{N}^n]$ is a primary binomial ideal $I' \subseteq \Bbbk[\mathbb{N}^n]$ such that $\mathbb{N}^n/\!\sim_{I'}\, = \bar{Q}$. Replacing I by I' if necessary, we therefore may as well assume $Q = \mathbb{N}^n$, since the definitions of primitive congruence and primary ideal depend only on the quotients $\overline{\mathbb{N}^n} = \bar{Q}$ and $\Bbbk[\mathbb{N}^n]/I' = \Bbbk[Q]/I$.

Each binomial prime in $\Bbbk[\mathbb{N}^n] = \Bbbk[x_1, \ldots, x_n]$ can be expressed as a sum $\mathfrak{p}_b + \mathfrak{m}_J \subseteq \Bbbk[\mathbb{N}^n]$ of its "binomial portion" $\mathfrak{p}_b$, which is a prime binomial ideal containing no monomials, and a monomial prime $\mathfrak{m}_J := \langle x_i \mid i \notin J \rangle$, which is generated by the variables whose indices are *not* contained in $J \subseteq \{1, \ldots, n\}$ [Eisenbud and Sturmfels 1996, Corollary 2.6]; this deduction relies on the algebraically closed hypothesis. Rescaling the variables of $\Bbbk[\mathbb{N}^n]$ if necessary, we can assume that the unique associated prime $\mathfrak{p} = \mathfrak{p}_b + \mathfrak{m}_J$ of $\Bbbk[\mathbb{N}^n]/I$ is *unital* — that is, $\mathfrak{p}_b$ is a unital ideal. Given that $\Bbbk$ is algebraically closed of characteristic 0, the $\mathfrak{p}$-primary condition on I implies that it contains $\mathfrak{p}_b$ [Eisenbud and Sturmfels 1996, Theorem 7.1']. Therefore, replacing $\Bbbk[\mathbb{N}^n]$ by $\Bbbk[\mathbb{N}^n]/\mathfrak{p}_b$ and I by $I/\mathfrak{p}_b$, we assume that Q is an affine semigroup and $\mathfrak{p}$ is generated by monomials. The desired result now follows from [Dickenstein et al. 2010b, Theorem 2.15 and Proposition 2.13] or [Miller 2011, Theorem 2.23], the latter being an equivalent statement that directly implies the characterization of mesoprimary congruences in Corollary 6.7.

(4) If $\bar{q}$ is not nil then $t^q \in \Bbbk[Q]$ lies outside of I, so t^q maps to a nonzero monomial in the twisted group algebra, whence $\bar{q}$ is cancellative because G is cancellative.

(5) When I is a monomial prime in an affine semigroup ring, the result is obvious. But prime $\Longrightarrow$ primary, so the reduction to that case in part (3) applies.

Moreover, since $I = \mathfrak{p}$ contains $\mathfrak{p}_b$ already, the characteristic 0 hypothesis is superfluous.

For this half of the theorem, it remains to explain, for $\alpha \neq 2$, why I is maximal among ideals inducing $\sim$. For that, it suffices by Theorem 9.12 to show that I contains a monomial if $\overline{Q}$ has a nil ∞. For part (1) (the cellular case), if $\overline{q} = \infty$, then by definition of nil there is for each $r \in \mathbb{N}$ a binomial $t^q - \lambda_r t^{rq} \in I$ for some $\lambda_r \in \Bbbk^*$, so $t^q(1 - \lambda_r t^{(r-1)q}) \in I$, whence t^q is a zerodivisor modulo I and thus nilpotent modulo I — say $t^{rq} \in I$; then $t^q - \lambda_r t^{rq} \in I \implies t^q \in I$. For part (3) (the primary case), Theorem 9.12 implies that I has at least two associated primes — one or more arising from an augmentation ideal — if maximality fails. For part (4) (the mesoprime case), any monomial t^q with $\overline{q} = \infty$ must lie in I because a group has no nil. For part (5) (the prime case), the maximality is a special case of part (1), because prime $\implies$ cellular for binomial ideals.

Next, assuming that I is maximal among the binomial ideals inducing a congruence $\sim$ on Q satisfying Definition 2.12(α), we prove that I satisfies Definition 10.4(α). As a matter of notation, write $\overline{t}^q$ for the image of t^q in $\Bbbk[Q]/I$. In all cases, if $q \in Q$ is an element whose image $\overline{q} \in \overline{Q}$ is nil, then $\overline{t}^q = 0$ by Theorem 9.12, using the maximality property of I. Consequently, if $q \in Q$ is nilpotent, then $\overline{t}^q$ is nilpotent in $\Bbbk[Q]/I$.

(1) By the previous paragraph, if $q \in Q$, then either the monomial $\overline{t}^q$ is nilpotent or $\overline{q}$ is cancellative. In the latter case, multiplication by $\overline{t}^q$ is injective on $\Bbbk[Q]/I$ because $\Bbbk[Q]/I$ is $\overline{Q}$-graded and addition by $\overline{q}$ is injective on $\overline{Q}$.

(2) By definition.

(3) The quotient $\overline{Q}$ satisfies the condition of Corollary 6.7 in which the cancellative monoid $F \subseteq \overline{Q}$ is an affine semigroup. Each orbit is a finite union of translates $\overline{q} + F$ because $\overline{Q}$ itself is generated by F and finitely many nilpotent elements. The proof now proceeds as in [Dickenstein et al. 2010b, Proposition 2.13]: owing to the partial order on the set of orbits afforded by Lemma 2.19, the $\overline{Q}/F$-grading on $\Bbbk[Q]/I$ induces a filtration by $\Bbbk[Q]$-submodules with associated graded module

$$\operatorname{gr}(\Bbbk[Q]/I) \cong \bigoplus_{F\text{-orbits } T} \Bbbk\{T\},$$

where $\Bbbk\{T\}$ is the vector space over $\Bbbk$ with basis T. The isomorphism above is as $\Bbbk[F]$-modules, or equivalently, as $\Bbbk[Q]$-modules annihilated by the kernel $\mathfrak{p}_F$ of the surjection $\Bbbk[Q] \twoheadrightarrow \Bbbk[F]$, with the $\Bbbk[F]$-module structure on $\Bbbk\{T\}$ induced by the F-action on T. Since $\Bbbk\{T\}$ is torsion-free as a $\Bbbk[F]$-module, the direct sum over T has only one associated prime, namely $\mathfrak{p}_F$, whence $\Bbbk[Q]/I$ does too.

(4) Set $\bar{Q}' = \bar{Q} \setminus \{\infty\}$ if $\bar{Q}$ has a nil, and $\bar{Q}' = \bar{Q}$ otherwise. By maximality of I, the quotient $\Bbbk[Q]/I$ is $\bar{Q}'$-graded. By part (1), every nonzero monomial $\bar{t}^q \in \Bbbk[Q]/I$ is a nonzerodivisor. Therefore $\Bbbk[Q]/I$ injects into its localization R obtained by inverting the nonzero monomials. Any presentation $\mathbb{Z}^n \twoheadrightarrow G$ for the universal group G of Q results in a presentation $\Bbbk[\mathbb{Z}^n] \twoheadrightarrow \Bbbk[G] \twoheadrightarrow \Bbbk[G]/I = R$ whose kernel is a binomial ideal. Thus R is a twisted group algebra over $\Bbbk$ by Proposition 10.3.

(5) The argument for part (4) works in this case, too, but now $\bar{Q}'$ is an affine semigroup, so that $\bar{\Bbbk} \otimes_\Bbbk R$, and hence also $\Bbbk[Q]/I$, are integral domains. $\square$

Corollary 10.7. *For binomial ideals in $\Bbbk[Q]$, over an arbitrary field except where noted,*

- *prime $\implies$ mesoprime $\implies$ mesoprimary $\implies$ cellular; and*

- *prime $\implies$ primary $\implies$ mesoprimary $\implies$ cellular (we only claim the second implication when $\Bbbk$ is algebraically closed of characteristic 0).*

Proof. Use Theorem 10.6: if I is maximal among binomial ideals inducing a congruence from Definition 2.12, then it is maximal among binomial ideals inducing any of the weaker congruences from Lemma 2.14. This proves every implication except for prime $\implies$ mesoprime, which a priori requires $\Bbbk$ to be algebraically closed, if Theorem 10.6 is being applied. But in fact the implication holds in general, even though the quotient by a prime binomial ideal I need not be an affine semigroup ring if $\Bbbk$ is not algebraically closed. This is a consequence of the stronger statement in Theorem 11.14, below. $\square$

Example 10.8. In general a primary ideal need not be mesoprimary. For instance, $\langle 1 - x^p, y - xy, y^2 \rangle$ is primary in characteristic p, but the congruence it induces has two associated prime congruences regardless of the characteristic.

Remark 10.9. The given proof of the implication Definition 10.4(3) $\implies$ Definition 2.12(3) fails in characteristic p, even if the field $\Bbbk$ is algebraically closed, because primary binomial ideals in characteristic p do not necessarily contain the binomial part of their associated prime [Eisenbud and Sturmfels 1996, Theorem 7.1′].

Theorem 10.6 implies the following result, which reflects the table on page 1332 homogeneously across all of its rows, and shows that all of the richness in Definition 10.4 is already exhibited by *unital ideals*: those generated by monomials and unital binomials.

Corollary 10.10. *A congruence satisfies a part of Definition 2.12 if and only if the kernel of the surjection $\Bbbk[Q] \twoheadrightarrow \Bbbk[\bar{Q}]^-$ satisfies the corresponding part of Definition 10.4.* $\square$

11. Monomial localization, characters, and mesoprimes

For arithmetic reasons, intersections of binomial ideals need not reflect their combinatorics completely accurately. The simplest example is $\langle x^2 - 1 \rangle = \langle x - 1 \rangle \cap \langle x + 1 \rangle$, whose congruence fails to equal the common refinement of the congruences induced by $\langle x - 1 \rangle$ and $\langle x + 1 \rangle$. Precise statements about relations between combinatorics and arithmetic use characters on subgroups of the unit groups of localizations of Q.

Localizations of monoids at their prime ideals corresponds to inverting monomials in their monoid algebras.

Definition 11.1. For a prime ideal $P \subset Q$, the corresponding monomial ideal in $\Bbbk[Q]$ is $\mathfrak{m}_P = \langle t^p \mid p \in P \rangle$.

Remark 11.2. When P is maximal, $\mathfrak{m}_P$ is the maximal proper Q-graded ideal in the monoid algebra $\Bbbk[Q]$, but it need not be maximal in the set of all proper ideals of $\Bbbk[Q]$.

Definition 11.3. The *monomial localization* $\Bbbk[Q]_P$ *of* $\Bbbk[Q]$ *along* P is the monoid algebra of the localization Q_P, arising by adjoining inverses to all monomials outside of $\mathfrak{m}_P$. The *monomial localization* of any $\Bbbk[Q]$-module M *along* P is $M_P = M \otimes_{\Bbbk[Q]} \Bbbk[Q]_P$.

Localization behaves well upon passing between algebra and combinatorics; it forms part of the justification for characterizing algebraic notions, such as the concept of I-witness in the next section, in combinatorial terms.

Lemma 11.4. *If $I \subseteq \Bbbk[Q]$ is a binomial ideal inducing the congruence $\sim$ on Q with quotient $\bar{Q}$, then for any monoid prime $P \subset Q$, the quotient of Q_P modulo the congruence induced by I_P is the monoid localization $\bar{Q}_P$ from Definition 3.9.*

Proof. Immediate from the definitions. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Definition 11.5. For any group L, a *character* is a homomorphism $\rho : L \to \Bbbk^*$. A character $\rho' : L' \to \Bbbk^*$ *extends* ρ if $L \subseteq L'$ is a subgroup and $\rho'(\ell) = \rho(\ell)$ for $\ell \in L$. The extension is *finite* if L'/L is finite.

Convention 11.6. The domain L is part of the data of a character $\rho : L \to \Bbbk^*$; that is, we simply speak of the character ρ, and write L_ρ if it is necessary to specify L.

Definition 11.7. Fix a subgroup $K \subseteq G_P$ of the unit group G_P at P. For any character $\rho : K \to \Bbbk^*$, the *P-mesoprime of ρ* is the preimage $I_{\rho,P}$ in $\Bbbk[Q]$ of the ideal

$$(I_{\rho,P})_P := \langle t^u - \rho(u-v)t^v \mid u - v \in K \rangle + \mathfrak{m}_P \subseteq \Bbbk[Q]_P.$$

Viewing P as implicit in the definition of ρ, the symbol I_ρ refers to the preimage in $\Bbbk[Q]$ of the ideal $\langle t^u - \rho(u-v)t^v \mid u - v \in K \rangle \subseteq \Bbbk[Q]_P$.

Definition 11.8. A subgroup $L \subseteq G$ of an abelian group is *saturated* in G if there is no subgroup of G in which L is properly contained with finite index. The *saturation* $\mathrm{sat}(L)$ of L is the intersection of all saturated subgroups of G that contain L. For any prime number $p \in \mathbb{N}$, the largest subgroup of $\mathrm{sat}(L)$ whose quotient modulo L has order

- a power of p is denoted $\mathrm{sat}_p(L)$,
- coprime to p is denoted $\mathrm{sat}'_p(L)$.

For $p = 0$, set $\mathrm{sat}_p(L) = L$ and $\mathrm{sat}'_p(L) = \mathrm{sat}(L)$.

The following implies, in particular, that the set of saturations of a character is finite. The statement is actually a slight generalization of [Eisenbud and Sturmfels 1996, Corollary 2.2], in that the domain L of ρ is allowed to be a subgroup of an arbitrary finitely generated abelian unit group G_P, and $I_{\rho,P}$ is not an arbitrary ideal in a finitely generated group algebra, but rather an ideal containing the maximal monomial ideal in an arbitrary finitely generated monoid algebra. However, the generalization follows from the original by working modulo the maximal monomial ideal and lifting to any presentation of G_P, taking note that all of the characters in question are trivial on the kernel of the presentation.

Proposition 11.9 [Eisenbud and Sturmfels 1996, Corollary 2.2]. *Fix an algebraically closed field $\Bbbk$ of characteristic $p \geq 0$. Let $\rho : L \to \Bbbk^*$ be a character on a subgroup $L \subseteq G_P$, and write g for the order of $\mathrm{sat}'_p(L)/L$. There are g distinct characters $\rho_1, \ldots, \rho_g$ on $\mathrm{sat}'_p(L)$ that extend ρ. For each ρ_j there is a unique character ρ'_j on $\mathrm{sat}(L)$ extending ρ_j. There is a unique character ρ' that extends ρ and is defined on $\mathrm{sat}_p(L)$. Moreover,*

(1) $\sqrt{I_{\rho,P}} = I_{\rho',P}$,

(2) $\mathrm{Ass}(S/I_{\rho,P}) = \{I_{\rho'_j,P} \mid j = 1, \ldots, g\}$, *and*

(3) $I_{\rho,P} = \bigcap_{j=1}^{g} I_{\rho_j,P}$.

The following lemma is a variant of [Dickenstein et al. 2010a, Lemma 2.9] and [Eisenbud and Sturmfels 1996, Theorem 2.1].

Lemma 11.10. *If $\Bbbk[\Phi]$ is the group algebra of a finitely generated abelian group Φ, then for any proper binomial ideal $I \subset \Bbbk[\Phi]$ there is a subgroup $L \subseteq \Phi$ and a character $\rho : L \to \Bbbk^*$ such that $I = I_\rho$.*

Proof. The binomial ideal is of the form $\langle 1 - \lambda_u t^u \mid u \in \mathcal{U} \rangle$ for some finite $\mathcal{U} \subseteq \Phi$. First off, $\mathcal{U}$ is a subgroup of Φ since $1 - \lambda\mu t^{u+v} = \mu t^v(1 - \lambda t^u) + (1 - \mu t^v)$ for all $\lambda, \mu \in \Bbbk$, including $\lambda = \lambda_u$ and $\mu = \lambda_v$. The set $\mathcal{U}$ is closed under inverses because $(1 - \lambda t^u)/\lambda t^u = -(1 - t^{-u}/\lambda)$ when $\lambda \neq 0$, and $I \neq \Bbbk[\Phi] \Longrightarrow \lambda_u \neq 0$. The very same arguments show that the map $\rho : \mathcal{U} \to \Bbbk^*$ defined by $u \mapsto \lambda_u$ is a homomorphism. $\square$

Definition 11.11. Fix a binomial ideal $I \subseteq \Bbbk[Q]$.

(1) The *stabilizer* of an element $q \in Q$ along a prime ideal $P \subset Q$ is the subgroup $K_q^P \subseteq G_P$ (sometimes denoted by K_q if P is clear from context) fixing the class of $q \in Q_P$ under the action from Lemma 3.11 for the congruence $\sim_I$.

(2) For $t^q \notin I_P$, the *character (of I_P) at q* is the homomorphism $\rho = \rho_q^P : K_q^P \to \Bbbk^*$ such that the $\Bbbk[G_P]$-module map $\Bbbk[G_P] \to \Bbbk[Q_P]/I_P$ taking $1 \mapsto t^q$ has kernel I_ρ.

(3) The ideal $I_q^P := I_{\rho, P} \subseteq \Bbbk[Q]$ is the *P-mesoprime of I at q*.

Remark 11.12. The homomorphism $\Bbbk[G_P] \to \Bbbk[Q_P]/I_P$ in Definition 11.11(2) has kernel of the form I_ρ by Lemma 11.10. Indeed, the kernel is a priori the binomial ideal $(I_P : t^q) \cap \Bbbk[G_P]$, which is not the unit ideal in $\Bbbk[G_P]$ because t^q lies outside of I_P.

Saturations of subgroups (Definition 11.8) are more or less combinatorial in nature. Saturations of characters, on the other hand, are more subtle, because arithmetic properties of the target field $\Bbbk$ can enter.

Definition 11.13. Fix a subgroup L of an abelian group G. A character $\rho : L \to \Bbbk^*$ is

- *saturated* if the subgroup L is saturated, and
- *arithmetically saturated* if ρ has no finite proper extensions.

A *saturation* of ρ is an extension of ρ to $\mathrm{sat}(L)$.

The importance of saturated characters has been demonstrated in Proposition 11.9, which required the algebraically closed hypothesis. Without it, the arithmetically saturated condition holds sway, and equivalence of primality with saturation can break.

Theorem 11.14. *If a binomial ideal in $\Bbbk[Q]$ over an arbitrary field $\Bbbk$ is prime then it is a mesoprime $I_{\rho, P}$ for an arithmetically saturated character ρ. The converse holds if $\Bbbk$ is algebraically closed, and it can fail if not.*

Proof. Suppose that $\Bbbk[Q]/I$ is a domain. The ideal of monoid elements $p \in Q$ such that $t^p \in I$ is a monoid prime P. Replacing Q with the monoid $Q \setminus P$ and I with its image in $\Bbbk[Q \setminus P] = \Bbbk[Q]/\langle t^p \mid p \in P \rangle$, it suffices to prove that $I = I_\rho$ for an arithmetically saturated character when Q is cancellative and I contains no monomials. Since $\Bbbk[Q]$ injects into its localization $\Bbbk[Q]_\varnothing = \Bbbk[\Phi]$ for the universal group $\Phi = Q_\varnothing$, and I contains no monomials, Lemma 11.10 implies the existence of a subgroup $L \subseteq \Phi$ and a character $\rho : L \to \Bbbk^*$ such that $I = I_\rho$. It remains to show that I_ρ is not prime if ρ is not arithmetically saturated. Suppose $\sigma : K \to \Bbbk^*$ properly extends ρ to a subgroup $K \subseteq \mathrm{sat}(L)$. Then $I_\sigma \supsetneq I_\rho$. By restricting σ to a subgroup of K that still properly contains L, we can assume that $|K/L| > 1$ and one of the following occurs:

- $\Bbbk$ has positive characteristic p and $|K/L|$ is a power of p.
- $\Bbbk$ has positive characteristic p and $|K/L|$ is relatively prime to p.
- $\Bbbk$ has characteristic 0.

Proposition 11.9 implies that in the first case, the extension $\overline{I}_\sigma$ of I_σ to $\overline{\Bbbk}$ has the same radical as the extension $\overline{I}_\rho$, in which case I_ρ itself is not a radical ideal. In the remaining two cases, Proposition 11.9 implies that $\overline{I}_\rho = \overline{I}_\sigma \cap \overline{J}$, with no associated prime of either intersectand containing an associated prime of the other. It follows that $I_\rho = I_\sigma \cap J$, where I_σ and $J := (I_\rho \mid I_\sigma)$ both properly contain I_ρ, so I_ρ is not prime.

The $\Bbbk = \overline{\Bbbk}$ converse is implicit in Proposition 11.9, and anyway follows easily from [Eisenbud and Sturmfels 1996, Theorem 2.1]. Example 11.15 demonstrates failure of the general converse. $\qquad\square$

Example 11.15. The ideal $I_\rho \subset \mathbb{Q}[x]$ for the character $\rho : 4\mathbb{Z} \to \mathbb{Q}^*$ defined by $\rho(4) = -4$ is $\langle x^4 + 4 \rangle$. This ideal is not prime because it factors as $\langle x^4 + 4 \rangle = \langle x^2 - 2x + 2 \rangle \cap \langle x^2 + 2x + 2 \rangle$. Nonetheless, ρ is arithmetically saturated because $x^4 + 4$ has no binomial factors of degree 2.

Example 11.16. The ideal $\langle x^3 - 2 \rangle$ in Example 10.2 is prime (by Eisenstein's criterion, for example). Therefore the character $\rho : 3\mathbb{Z} \to \mathbb{Q}^*$ sending $3 \mapsto 2$ is arithmetically saturated, viewing $3\mathbb{Z}$ as a subgroup of $\mathbb{Z}$: any proper extension of ρ to a character $\mathbb{Z} \to \mathbb{Q}^*$ would require a cube root of 2.

12. Coprincipal and mesoprimary components of binomial ideals

Definition 12.1. Fix a binomial ideal $I \subseteq \Bbbk[Q]$ inducing a congruence $\sim$ on Q.

(1) An element $w \in Q$ is an *I-witness* for a monoid prime P if it is a $\sim$-witness for P or if $P = \varnothing$ is the empty monoid ideal and I contains no monomials.

(2) An element $w \in Q$ is an *essential I-witness* for a monoid prime P if w is a key $\sim_I$-witness or some polynomial annihilated by $\mathfrak{m}_P$ in $\Bbbk[Q_P]/I_P$ (Definitions 11.1 and 11.3) has t^w minimal (under Green's preorder) among its nonzero monomials.

(3) If $I_{\rho,P}$ is the P-mesoprime of I (Definition 11.11) at some I-witness w for P, then w is an *I-witness for $I_{\rho,P}$*.

(4) $I_{\rho,P}$ is an *associated mesoprime* of I if there is an essential I-witness for $I_{\rho,P}$.

Lemma 12.2. *Every essential I-witness for P is an I-witness for P.*

Proof. Assume that $f \in \Bbbk[Q]$ such that $\mathfrak{m}_P f \subseteq I_P$. Let $m = \lambda t^w$ be a term of f (that is, a nonzero constant times a monomial) minimal under Green's preorder on Q_P restricted to the terms of f. Fix a nonunit monoid element $p \in Q_P$.

Since $t^p f \in I_P$, the term $t^p m$ must equal, modulo I_P, some sum of terms whose monomials t^{p+a} have t^a appearing with nonzero coefficient in f. It follows that $t^p m$ shares its $\bar{Q}_P$-graded degree with at least one of these monomials t^{p+a}, where $\bar{Q} = Q/\sim_I$. Thus w is a witness by minimality of m: at least one of the elements a is an aide for w and p. $\square$

Example 12.3. If $I = \langle y - x^2 y, y^2 - xy^2, y^3 \rangle$ is the binomial ideal from Example 2.17(5) then $I_{\rho,P} = \langle x^2 - \lambda, y \rangle$ for $P = \langle e_y \rangle$ and $\rho : \langle (2,0) \rangle \to \Bbbk^*$ defined by $\rho(2,0) = \lambda$ induces the associated prime congruence of $\sim_I$ for any $\lambda \in \Bbbk^*$. The monomial $x^a y \in \Bbbk[x, y]$ is a witness for any $a \in \mathbb{N}$, and it lies in one of two possible essential witness classes, depending on the parity of a; see the figure in Example 2.17. However, only $\lambda = 1$ gives the associated mesoprime itself, as opposed to merely inducing its congruence.

Lemma 12.4. *Every binomial ideal in $\Bbbk[Q]$ has only finitely many essential witnesses.*

Proof. Theorem 5.6 takes care of key witnesses, so it is enough to treat witnesses arising from annihilation by $\mathfrak{m}_P$. As Q has finitely many prime ideals, it suffices to bound the number of essential witnesses for a fixed prime ideal P. By definition, $\mathfrak{m}_P$ annihilates the $\Bbbk[Q_P]$-submodule of $\Bbbk[Q_P]/I_P$ consisting of polynomials giving rise to essential I-witnesses. Hence the $\Bbbk[Q_P]$-submodule in question is finitely generated over $\Bbbk[G_P] = \Bbbk[Q_P]/\mathfrak{m}_P$, so only finitely G_P-orbits of (exponents on) monomials are involved. $\square$

Remark 12.5. All associated mesoprimes of a unital binomial ideal (generated by differences of monomials with unit coefficients) are unital.

Remark 12.6. When I contains no monomials, every monomial is an essential I-witness for the empty monoid ideal $\varnothing \subset Q$. The condition that $I_{\rho,\varnothing}$ be an associated mesoprime of I for some (unique) character ρ is similar to the condition that $\varnothing$ be associated to the congruence $\sim$ induced by I, but it is not equivalent. These conditions differ only when I is minimal and not maximal among binomial ideals inducing $\sim$ (see Theorem 9.12) — that is, when $\sim$ has a nil class but I nonetheless contains no monomials — in which case I has an associated mesoprime $I_{\rho,\varnothing}$ but $\varnothing$ is not associated to $\sim$.

Lemma 12.7. *If w is an I-witness for $I_{\rho,P}$, then the localization along P of the P-mesoprime I_w^P of I at w satisfies $(I_w^P)_P = (I_{\rho,P})_P = (I_P : t^w) + \mathfrak{m}_P$.*

Proof. The first equality is by Definition 11.11. For the second, use Theorem 7.11, which implies that I and $I_P + t^w \mathfrak{m}_P$ have the same P-mesoprime at w. It follows that the natural isomorphism $\Bbbk[G_P] \to \Bbbk[Q_P]/\mathfrak{m}_P$ induced by the inclusion $\Bbbk[G_P] \to \Bbbk[Q_P]$ descends to an isomorphism

$$\Bbbk[G_P]/(I_P : t^w) \cap \Bbbk[G_P] \to \Bbbk[Q_P]/((I_P : t^w) + \mathfrak{m}_P).$$

Now apply Remark 11.12.   □

Remark 12.8. If $Q = \mathbb{N}^n$ and I is unital, then all information about associated mesoprimes is contained in the set of *associated lattices* $L \subset \mathbb{Z}^J$, each of which comes with an *associated subset* $J \subseteq \{1, \ldots, n\}$. Indeed, a prime ideal P of $\mathbb{N}^n$ is the complement of a face $\mathbb{N}^J$ of $\mathbb{N}^n$, and specifying a prime congruence on $\mathbb{N}^n$ amounts to choosing such a face along with a lattice $L \subset \mathbb{Z}^J$. To see why, first observe that localization along P inverts the face, turning $\mathbb{N}^n$ into $\mathbb{Z}^J \times \mathbb{N}^{\bar{J}} = G_P \times \mathbb{N}^{\bar{J}}$. Subsequently passing to the quotient by a given prime congruence, the complement of the face maps to nil, and the subgroup L is the stabilizer of any class under the action of $\mathbb{Z}^J = G_P$ on the quotient. We were led to associated lattices (before the more general associated prime congruences) in part by [Eisenbud and Sturmfels 1996, Theorem 8.1]. Although that theorem only covers cellular cases, the upshot is that a collection of associated lattice ideals contributes associated primes.

Remark 12.9. When the domain K of a character $\rho : K \to \Bbbk^*$ is a saturated subgroup of G_P, the ideal $I_{\rho, P}$ is often an associated prime of a binomial ideal I without being an associated mesoprime of I. The reason is that the congruences induced by associated P-mesoprimes are immediately visible in the congruence induced by I_P, whereas the associated primes of I usually induce coarser congruences (larger congruence classes) than those visible. The quintessential example to consider is the lattice ideal I for an unsaturated sublattice of $\mathbb{Z}^n$: the lattice ideal for the saturation is an associated prime of I, but the unique associated mesoprime of I is I itself.

Proposition 12.10. *A binomial ideal $I \subseteq \Bbbk[Q]$ is mesoprimary if and only if I has exactly one associated mesoprime.*

Proof. If I is mesoprimary then it is cellular by Corollary 10.7 and the congruence $\sim_I$ is mesoprimary by Definition 10.4. If w is any witness (essential or not) for the unique associated prime congruence and $I' = (I : t^w)$ is the annihilator of the image of t^w in $\Bbbk[Q]/I$, then multiplication by t^w induces an isomorphism $I_P + \mathfrak{m}_P \to I'_P + \mathfrak{m}_P$, so every associated mesoprime of I is equal to $I + \mathfrak{m}_P$.

On the other hand, assume that I has only one associated mesoprime, and that its associated monoid prime is $P \subset Q$. The congruence $\sim$ induced by I is mesoprimary by Lemma 4.9 and Theorem 6.1. Either I contains a monomial, in which case it is already maximal among ideals inducing its congruence by Theorem 9.12, or else I contains no monomials, in which case the unique associated monoid prime ideal is $P = \varnothing$ by definition. When $P = \varnothing$, if I is not maximal then $\sim$ has a witness for some monoid prime ideal other than $\varnothing$ by Remark 12.6, as $\sim$ has an associated monoid prime but $\varnothing$ is not one of them. Thus uniqueness of the associated mesoprime implies maximality.   □

Remark 12.11. Building on Remark 6.8, Proposition 12.10 says that the character of I_P is the same at every nonzero monomial as soon as it is the same at every essential witness monomial, and that is what it means to be a mesoprimary ideal.

Definition 12.12. Given a monoid prime $P \subset Q$, a mesoprimary binomial ideal in $\Bbbk[Q]$ is *P-mesoprimary* if the associated prime ideal of its induced congruence is P.

The principal use of the following definition, which builds on the notion of order ideal from Definition 7.4, concerns the case where the set $\boldsymbol{w}$ consists of a single witness. The more general case arises during the construction of mesoprimary decompositions with as few components as possible (Corollary 13.5).

Definition 12.13. Fix a binomial ideal $I \subseteq \Bbbk[Q]$, a prime $P \subset Q$, and a finite subset $\boldsymbol{w} \subseteq Q$. The *monomial ideal* $M_{\boldsymbol{w}}^P(I) \subseteq \Bbbk[Q]$ *cogenerated by $\boldsymbol{w}$ along P* is generated by the monomials $\boldsymbol{t}^u \in \Bbbk[Q]$ such that u lies outside of the order ideal $Q_{\preceq w}^P$ cogenerated by w at P (Definition 7.4) under the congruence $\sim_I$ for all $w \in \boldsymbol{w}$.

Definition 12.14. Fix a binomial ideal $I \subseteq \Bbbk[Q]$ and a finite set $\boldsymbol{w} \subseteq Q$ such that the *P-mesoprime* I_w^P of I at w is $I_{\rho,P}$ for all $w \in \boldsymbol{w}$. The *P-mesoprimary component of I cogenerated by $\boldsymbol{w}$* is the preimage $W_{\boldsymbol{w}}^P(I)$ in $\Bbbk[Q]$ of the ideal $I_P + I_\rho + M_{\boldsymbol{w}}^P(I) \subseteq \Bbbk[Q]_P$.

Remark 12.15. Comparing to Definition 7.7, adding $M_{\boldsymbol{w}}^P(I)$ in Definition 12.14 joins all pairs of elements in $Q \setminus Q_{\preceq q}^P$, while adding I_ρ joins the pairs $(a, b) \in Q$ satisfying conditions (i) and (ii) in Definition 7.7.

Definition 12.16. A *cogenerator* of a mesoprimary binomial ideal $I \subseteq \Bbbk[Q]$, or of the quotient $\Bbbk[Q]/I$, is a monoid element that is a cogenerator of the induced congruence. A *monomial cogenerator* is a monomial in $\Bbbk[Q]$ whose exponent is a cogenerator.

The nomenclature in Definition 12.14 is justified by the following result, which arithmetizes the combination of Theorem 7.11 and Lemma 8.10.

Proposition 12.17. *If $\boldsymbol{w}$ consists of I-witnesses for P, then the ideal $W_{\boldsymbol{w}}^P(I)$ in Definition 12.14 is mesoprimary with associated mesoprime $I_{\rho,P}$. Moreover, if I induces $\sim$ on Q, then $W_{\boldsymbol{w}}^P(I)$ induces the common refinement of the coprincipal components $\sim_{\boldsymbol{w}}^P$ cogenerated by the elements in $\boldsymbol{w}$ along P. Every cogenerator of $W_{\boldsymbol{w}}^P(I)$ lies in $\boldsymbol{w}$.*

Proof. The claim has little content if $P = \varnothing$, as then $I_{\rho,P} = I_\rho = I_P$, so assume $P \neq \varnothing$. Since $W_{\boldsymbol{w}}^P(I)$ contains monomials by definition, it suffices by Theorem 9.12 to verify that $W_{\boldsymbol{w}}^P(I)$ induces the common refinement $\approx$ of coprincipal congruences in question, given that $\approx$ is mesoprimary by Theorem 7.11 and Proposition 6.9.

By construction (specifically, Definition 7.7; see also Remark 12.15), the mesoprimary congruence $\approx$ refines the congruence $\approx'$ induced by $W_{\boldsymbol{w}}^P(I)$: the monomial

ideal $M_{\boldsymbol{w}}^P(I)$ sets all elements outside of the order ideal equivalent to one another, and the generators of I_ρ carry out the remaining required identifications. The harder direction is showing that no more relations are introduced.

Since $W_{\boldsymbol{w}}^P(I)$ is obtained from an extension to the localization $\Bbbk[Q]_P$ along P, we may as well assume that $Q = Q_P$, so P is the maximal ideal of Q. The congruences induced by I and I_ρ each individually refine the congruence $\approx$ (not to be confused with $\approx'$ here); for I this is by Theorem 8.4, and for I_ρ this is by Corollary 6.7 (see also Remark 6.8). Therefore both I and I_ρ are ideals graded by $Q/\approx$. We deduce that $W_{\boldsymbol{w}}^P(I)$ is graded by $Q/\approx$ as well, since $M_{\boldsymbol{w}}^P(I)$ is a monomial ideal and hence is automatically graded by $Q/\approx$. Consequently, each nonnil congruence class of $\approx'$ is contained in some congruence class of $\approx$.

It remains to treat the nil class of $\approx'$. Assuming $a \in Q$ with $t^a \notin M_{\boldsymbol{w}}^P(I)$, it suffices to show $t^a \notin W_{\boldsymbol{w}}^P(I)$. Choose $w \in \boldsymbol{w}$ with a in the order ideal $Q_{\preceq w}^P = Q_{\preceq w}^P(\sim)$, which can be done by definition of $M_{\boldsymbol{w}}^P(I)$. Next pick $u \in Q$ such that the images of $u + a$ and w in $Q/\approx$ are Green's-equivalent to one another; this is possible by definition of the order ideal $Q_{\preceq w}^P$. Use a double bar to denote passage from Q to $Q/\approx$, so $\overline{\overline{q}} \in Q/\approx$ is the image of q for any $q \in Q$. The choice of the character ρ was made precisely so that the graded piece $(I)_{\overline{\overline{q}}}$ of the ideal I contains the graded piece $(I_\rho)_{\overline{\overline{q}}}$ whenever $\overline{\overline{q}}$ is Green's-equivalent to $\overline{\overline{w}}$ in $Q/\approx$. This means that I_ρ adds no new relations to I in degree $\overline{\overline{q}}$. Since $M_{\boldsymbol{w}}^P(I)$ adds no new relations to I in degree $\overline{\overline{q}}$ by definition, $W_{\boldsymbol{w}}^P(I)_{\overline{\overline{q}}} = (I)_{\overline{\overline{q}}}$ for $q = u + a$. The class of $u + a$ is not nil in $Q/\sim$ because the character of I_P at $u + a$ is ρ. Hence $t^a \notin W_{\boldsymbol{w}}^P(I)$.

The final claim of the Proposition follows from Lemma 8.10. $\qquad\square$

Definition 12.18. A binomial ideal is *coprincipal* if it is mesoprimary and its induced congruence is coprincipal. A *coprincipal component* $W_q^P(I)$ *of* I *cogenerated by* q *at* P is a P-mesoprimary component $W_{\{q\}}^P(I)$ cogenerated by a single element q.

Corollary 12.19. *If* $I \subseteq \Bbbk[Q]$ *is a binomial ideal and* w *is an* I-*witness for* P, *then the coprincipal component of* I *cogenerated by* w *at* P *is a coprincipal binomial ideal.*

Proof. Immediate from Proposition 12.17 and the definitions. $\qquad\square$

Remark 12.20. It would be superb if intersecting any pair of mesoprimary ideals with the same associated mesoprime resulted in another mesoprimary ideal. More precisely, a direct binomial ideal analogue of Proposition 6.9 would be desirable. Unfortunately, the binomial analogue is false in general: in $\Bbbk[x, y]$, the intersection of the mesoprimary ideals $\langle x - 2y \rangle + \langle x, y \rangle^3$ and $\langle x - y \rangle + \langle x, y \rangle^3$ is not mesoprimary when $\operatorname{char}(\Bbbk) \neq 2$; it is not even a binomial ideal. Heuristically, if I_1 and I_2 are mesoprimary ideals in $\Bbbk[Q_P]$ with associated mesoprime $I_{\rho, P}$, then in each of I_1 and I_2 there are "vertical" binomials from I_ρ, whose coefficients are

dictated by the character ρ, and "horizontal" binomials conglomerating the vertical fibers, with more arbitrary coefficients. (The vertical and horizontal directions in Examples 1.3 and 2.17 are reversed for aesthetic reasons; the usage here makes sense in Examples 4.15, 4.16, 8.12, 9.1, and 17.5.) When the horizontal coefficients from I_1 and I_2 conflict, the intersection need not be binomial.

That said, the analogue of Proposition 6.9 is true once control is granted over binomiality, and that comes for free when I_1 and I_2 both arise from a single ideal via sets of witnesses as in Proposition 12.17. In that sense, the binomial analogue of Proposition 6.9 is "true enough" for the relevant aspects of the theory of mesoprimary decomposition to succeed, namely Corollary 13.5.

Remark 12.21. The existence of a mesoprimary ideal inducing a given congruence is automatic by Remark 2.16. However, the question becomes more subtle when a given associated mesoprime other than the unital one is desired. Roughly speaking, we do not know how to construct mesoprimary ideals with given associated mesoprimes de novo, although by Proposition 12.17 we do know how to construct mesoprimary ideals given the foundation of a binomial ideal to start from. More precisely, fix a monoid prime $P \subset Q$, a P-mesoprimary congruence $\approx$ on Q, and a character $\rho : K \to \Bbbk^*$ on the stabilizer K of some element that is not nil in the localization of $Q/\approx$ along P. It would be convenient to say that there exists a mesoprimary ideal J inducing $\approx$ with associated mesoprime $I_{\rho,P}$, but it is not clear to us whether this should be true. What guarantees existence in the cases we care about, namely Proposition 12.17, is the I-witnessed nature of $\approx$: each I-witness prefers a particular character over all others — the one it sees by virtue of it being an I-witness — and that is the only one required for the theory of mesoprimary decomposition.

In a different light, the problem is one of automorphisms. The associated mesoprime of any unital P-mesoprimary ideal I is $I_{1,P}$ for the trivial character. Suppose, for simplicity, that the ground field $\Bbbk$ is algebraically closed. Then, for any mesoprime $I_{\rho,P}$, there is an automorphism of $\Bbbk[Q]$ taking $I_{1,P}$ to $I_{\rho,P}$; this amounts to the feasibility of extending the character $\rho : K \to \Bbbk^*$ to the entire group G_P of units of Q_P. To transform I into a mesoprimary ideal with associated mesoprime $I_{\rho,P}$, however, the character must be extended appropriately to all of Q_P, not just to G_P. It is not clear to us whether issues of horizontal coefficients (see Remark 12.20) can intervene, particularly when the inclusion of G_P into Q_P fails to split.

Remark 12.22. Independent of the existence question, it is not clear how to describe the class of mesoprimary ideals inducing a given congruence and with a given associated mesoprime. Certainly, a solution to the problem in Remark 12.21 need not be unique. For instance in the nilpotent situation, the one-parameter family $\langle x - \lambda y, x^2, xy, y^2 \rangle$ (for $\lambda \neq 0$) consists of mesoprimary ideals over the associated mesoprime $\langle x, y \rangle$, all inducing the same congruence.

13. Mesoprimary decomposition of binomial ideals

This section makes precise the sense in which mesoprimary decomposition of congruences lifts to a parallel combinatorial theory for binomial ideals in monoid algebras.

Definition 13.1. Fix a binomial ideal $I \subseteq \Bbbk[Q]$ in a finitely generated commutative monoid algebra over a field $\Bbbk$.

(1) An expression of I as an intersection of finitely many mesoprimary ideals is a *mesoprimary decomposition* if, for each prime $P \subset Q$ and P-mesoprimary intersectand J, the P-mesoprimes of I and J at every cogenerator of J coincide.

(2) The decomposition is a *combinatorial* mesoprimary decomposition if every cogenerator of every component J in the decomposition is an essential I-witness.

Theorem 13.2. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal in the algebra $\Bbbk[Q]$ admits a combinatorial mesoprimary decomposition.*

Proof. Examples include those in Theorem 13.3 and Corollary 13.5, below, where the finiteness of the intersection in Theorem 13.3 is Lemma 12.4. $\square$

The use of all essential witnesses and not merely key witnesses in the next result stems from the element f in the proof, which can have more than two terms. See also Example 16.6, which shows that nonkey witnesses can be necessary for the intersection of the corresponding coprincipal components to be a binomial ideal. On the other hand, the restriction to essential witnesses instead of all witnesses ensures finiteness of the number of intersectands, according to Lemma 12.4.

Theorem 13.3. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal in the monoid algebra $\Bbbk[Q]$ is the intersection of the coprincipal components cogenerated by its essential witnesses.*

Proof. Pick an element f outside of I. The goal is to show that f lies outside of the coprincipal component of I cogenerated by some essential witness. First assume that f lies in the monomial localization $I_{P'}$ along every nonmaximal prime P'. Thus f is annihilated, modulo I, by some power of the maximal monomial ideal $\mathfrak{m}_P \subseteq \Bbbk[Q]$. Replacing f by a monomial multiple of f, assume that f is annihilated, modulo I, by the entire maximal monomial ideal; that is, assume $\mathfrak{m}_P f \subseteq I$. By Definition 12.1, some essential I-witness w for P is the exponent on a monomial t^w with nonzero coefficient in f. Minimality of w ensures that all terms of f other than t^w itself vanish modulo $W_w^P(I)$, whence $f \notin W_w^P(I)$.

The argument just completed proves, in particular, the case where Q has only one prime ideal. Now assume that Q has more than one prime ideal. By the argument already given, assume the image of f under monomial localization along some

nonmaximal monoid prime P lies outside of I_P. Induction on the number of prime ideals of Q implies that the localized image of f lies outside of some P-coprincipal component of I_P. By Definition 12.14, a P-coprincipal component of I_P is the localization along P of a P-coprincipal component of I. Lemma 13.4 implies that f lies outside of that P-coprincipal component before localization, as desired. $\square$

Lemma 13.4. *If I is a P-mesoprimary ideal, then localization along a monoid prime is either injective or 0 on $\Bbbk[Q]/I$, with injectivity precisely when the prime contains P.*

Proof. By Definition 2.12, any P-mesoprimary congruence on Q is P-primary, whence the quotient $\bar{Q}$ either injects into its localization along the given prime (if the prime contains P) or else $\bar{Q}$ becomes trivial upon localization (if some element of P — which is nilpotent in $\bar{Q}$ — is inverted). Lemma 11.4 implies that the result for congruences lifts to binomial ideals. $\square$

Using Theorem 13.3 and Proposition 12.17, one can find a mesoprimary decomposition that minimizes the number of components by intersecting all coprincipal components for a given associated mesoprime.

Corollary 13.5. *Fix a finitely generated commutative monoid Q and a field $\Bbbk$. Every binomial ideal in the monoid algebra $\Bbbk[Q]$ admits a combinatorial mesoprimary decomposition with one component per associated mesoprime.*

Remark 13.6. The existence of any mesoprimary decomposition — let alone a combinatorial one as in Theorem 13.2 — is much stronger than mere existence of a decomposition as an intersection of mesoprimary ideals, essentially because of the phenomenon in Remark 12.9. The strength is particularly visible when the field $\Bbbk$ is algebraically closed of characteristic 0. In that case, every binomial primary decomposition of I expresses I as an intersection of mesoprimary ideals by Corollary 10.7, but a mesoprime must honor stringent combinatorial conditions to be an associated mesoprime of I, and a mesoprimary ideal for an associated mesoprime must honor stringent combinatorial conditions to be an intersectand in a mesoprimary decomposition of I. The difference between ordinary and combinatorial mesoprimary decompositions is a relatively slight distinction among potential cogenerator locations: in the ordinary case, I is merely required to possess the correct characters at the cogenerators of the intersectands, whereas in the combinatorial case only certain intrinsically defined elements possessing the correct characters from I are allowed as cogenerators of components.

14. Binomial localization

Upon localization of a binomial quotient $\Bbbk[Q]/I$ at a binomial prime, some monomials become units and others are annihilated. The units are easy: if the prime

is $I_{\sigma,P}$, then the monomials outside of $\mathfrak{m}_P$ become units. The question of which monomials die is much more subtle. There are two potential reasons that a monomial gets killed upon ordinary localization (Theorem 14.9): a combinatorial one and an arithmetic one. Combinatorially, a monomial dies if its class under $\sim_I$ points into P (Definition 14.1); arithmetically, a monomial dies if the character of I_P at it is incommensurate with ρ (Definition 14.6). These annihilations result from the inversion of two different types of binomials: in the combinatorial case the inverted binomials have one monomial outside of $\mathfrak{m}_P$, and in the arithmetic case the inverted binomials lie along the unit group G_P locally at P. The relevant monomials die because locally each becomes a binomial unit multiple of a binomial in I; see the proof of Theorem 14.9.

Definition 14.1. Given a prime $P \subset Q$, and a congruence $\sim$ on Q, the congruence class of $q \in Q$ *points into P* if $q + p \sim q$ in the localization Q_P for some $p \in P$.

Lemma 14.2. *Given a prime $P \subset Q$ and a congruence $\sim$ on Q, the set of elements in Q whose class points into P is an ideal of Q.*

Proof. If $q + p \sim q$ then $u + q + p \sim u + q$ by additivity of $\sim$. $\qquad\square$

Definition 14.3. The *P-infinite ideal* $M_\infty^P(\sim) \subseteq Q$ for a prime $P \subset Q$ and congruence $\sim$ on Q is generated by the elements of Q whose classes point into P. If $\sim \, = \, \sim_I$ is induced by a binomial ideal $I \subseteq \Bbbk[Q]$, then $M_\infty^P(I) \subseteq \Bbbk[Q]$ is the corresponding *P-infinite monomial ideal*.

Remark 14.4. The terminology involving infinity stems from [Dickenstein et al. 2010b, Lemma 2.10], which concerns binomial localization at a monomial prime of an affine semigroup ring: when the ambient monoid Q is an affine semigroup, a class that points into P is infinite. The focus on monomial primes in affine semigroup rings arises there because the field is algebraically closed of characteristic 0 and the ideals to be localized are $I_{\rho,P}$-primary (and hence contain I_ρ), so the binomial localization procedure can be carried out in the affine semigroup ring $\Bbbk[Q]/I_\rho$. Definitions 14.1 and 14.3 lift the picture from $(I + I_\rho)/I_\rho \subseteq \Bbbk[Q]/I_\rho$ to $I + I_\rho \subseteq \Bbbk[Q]$ itself; but see Remark 14.7.

Lemma 14.5. *Let R be a set of characters on subgroups of the unit group G_P of Q_P. Given a binomial ideal $I \subseteq \Bbbk[Q]$, the set*

$$\{q \in Q \mid \text{the character } \rho_q^P \text{ of } I_P \text{ at } q \text{ is not a restriction of every character from } R\}$$

is an ideal of Q.

Proof. The character ρ_{p+q}^P of I_P at $p + q$ is an extension of ρ_q^P. $\qquad\square$

Definition 14.6. Given a binomial ideal $I \subseteq \Bbbk[Q]$ and a mesoprime $I_{\rho,P}$, the *incommensurate ideal* of I at ρ is the ideal $M_\rho^P(I) \subseteq \Bbbk[Q]$ spanned over $\Bbbk$ by all monomials t^q such that the character of I_P at q is not a restriction of ρ.

Remark 14.7. The condition for a monomial to lie in the incommensurate ideal is phrased arithmetically, but in reality many monomials in it are there for combinatorial reasons: if the domain of the character of I_P at q fails to be contained in the (saturation of) the domain of ρ — that is, if the stabilizer of the class of q in $Q/\sim_I$ is too big — then q has no hope of being commensurate with ρ. This type of combinatorial obstruction to commensurability also contributes infinite classes in [Dickenstein et al. 2010b, Lemma 2.10].

Definition 14.8. The *binomial localization* of $I \subseteq \Bbbk[Q]$ at a binomial prime $I_{\sigma,P}$ is the sum $I + M_\infty^P(I) + M_\sigma^P(I) \subseteq \Bbbk[Q]$ of I plus its P-infinite and incommensurate ideals.

The point of this section is to compare the previous definition with ordinary (inhomogeneous) localization of a $\Bbbk[Q]$-module at a binomial prime $I_{\sigma,P}$, obtained by inverting all elements of $\Bbbk[Q]$ outside of $I_{\sigma,P}$.

Theorem 14.9. *Given a binomial ideal $I \subseteq \Bbbk[Q]$ over an arbitrary field $\Bbbk$, the kernel of the localization homomorphism from $\Bbbk[Q]$ to the ordinary localization of $\Bbbk[Q]/I$ at a binomial prime $I_{\sigma,P}$ contains the binomial localization of I at $I_{\sigma,P}$.*

Proof. First suppose that the class of $q \in Q$ points into P. Pick $p \in P$ such that $q + p \sim q$. This congruence means that there is a binomial $t^q - \lambda t^{q+p} = t^q(1 - \lambda t^p)$ in I. But $1 - \lambda t^p$ lies outside of $I_{\sigma,P}$ because its image modulo $\mathfrak{m}_P$ is already 1. Therefore $1 - \lambda t^p$ is a unit in the ordinary localization of $\Bbbk[Q]/I$ at $I_{\sigma,P}$, so t^q is 0 there.

Next suppose that $t^q \in M_\sigma^P(I)$. By definition, there is a binomial $1 - \lambda t^g$ for some $g \in G_P$ such that $\lambda \neq \sigma(g)$ and $t^q(1 - \lambda t^g) \in I_P$. The element $1 - \lambda t^g$ lies outside of $I_{\sigma,P}$ by definition. Therefore the argument in the previous paragraph works in this case, too. We conclude that the binomial localization of I is contained in the kernel. $\square$

Remark 14.10. How is Theorem 14.9 to be applied? While the binomial localization I' of I at $I_{\sigma,P}$ might not coincide with the kernel of ordinary localization at $I_{\sigma,P}$, it is always the case, by Theorem 14.9, that I and I' have the same ordinary localization at $I_{\sigma,P}$. Therefore, for the purpose of detecting $I_{\sigma,P}$-primary components, I' is just as good as I was in the first place. But the combinatorics of I' might be much simplified, thereby clarifying the role of $I_{\sigma,P}$ in the primary decomposition of I. See the proof of Theorem 15.11 for a quintessential example.

15. Primary decomposition of binomial ideals

Passing from mesoprimary and coprincipal ideals and decompositions to primary ideals and decompositions requires a minimal amount of knowledge concerning primary decomposition of mesoprimary ideals themselves. To speak about binomial

primary decomposition of binomial ideals in $\Bbbk[Q]$, we are forced to assume, in appropriate locations, that $\Bbbk$ is algebraically closed (Example 11.15); we write $\Bbbk = \overline{\Bbbk}$ in that case. Doing so guarantees that each binomial ideal $I \subset \Bbbk[Q]$ has binomial associated primes [Eisenbud and Sturmfels 1996, Theorem 6.1]. However, most of this section works for an arbitrary ground field, so we are explicit about our hypotheses in this section. One reason is that the characterization of binomial prime ideals (Theorem 11.14) does not rely on properties of $\Bbbk$: every binomial prime can be expressed as a sum $\mathfrak{p} + \mathfrak{m}_P$ in which $P \subset Q$ is a monoid prime ideal and $\mathfrak{p}$ is a binomial ideal (unique and prime modulo $\mathfrak{m}_P$, but not necessarily in $\Bbbk[Q]$) that contains no monomials.

Proposition 15.1. *Fix an arbitrary field $\Bbbk$. If $I \subset \Bbbk[Q]$ is mesoprimary with associated mesoprime $I_{\rho,P}$, and the localized quotient monoid $\overline{Q}_P = Q_P/\sim_I$ has unit group G, then* (i) *localizing along P induces an injection $\Bbbk[Q]/I \hookrightarrow (\Bbbk[Q]/I)_P$, and* (ii) *$(\Bbbk[Q]/I)_P$ has finitely many nonzero $(\overline{Q}_P/G)$-graded pieces, all isomorphic to $(\Bbbk[Q]/I_{\rho,P})_P$. Conditions* (i) *and* (ii) *characterize mesoprimary ideals I with associated mesoprime $I_{\rho,P}$.*

Proof. The monomials outside of $\mathfrak{m}_P$ are nonzerodivisors on the quotient modulo any P-mesoprimary ideal by definition; hence the injection (i). Claim (ii) and the statement about characterizing mesoprimary ideals follow from Proposition 12.10 (see also Definition 11.11, Remark 11.12, and Lemma 12.7). □

Corollary 15.2. *Fix an arbitrary field $\Bbbk$. If $I \subset \Bbbk[Q]$ is mesoprimary, then the associated primes of I are exactly the minimal primes of its unique associated mesoprime. In particular, I is primary if it is mesoprimary and its associated mesoprime is prime.*

Proof. The partial order on the monoid $\overline{Q}_P/G$ afforded by Lemma 2.19 induces a filtration of $(\Bbbk[Q]/I)_P$ by $\Bbbk[Q]_P$-submodules whose associated graded module is free of finite rank — in fact isomorphic to $(\Bbbk[Q]/I)_P$ itself — as a module over $(\Bbbk[Q]/I_{\rho,P})_P$. □

Remark 15.3. Corollary 15.2 says that, although one expects to derive information about associated primes of I from the characters at its witnesses, when I is mesoprimary the appropriate characters appear at the identity $1 \in \Bbbk[Q]$. This is another manifestation of semifreeness (Remark 6.8), detailed in the present case in Proposition 15.1.

Primary decomposition of mesoprimary ideals reduces to that of mesoprimes.

Proposition 15.4. *Fix $\Bbbk = \overline{\Bbbk}$. Any mesoprimary ideal $I \subset \Bbbk[Q]$ with associated mesoprime $I_{\rho,P}$ has unique minimal primary decomposition $I = \bigcap_\sigma (I + I_\sigma)$, if $I_{\rho,P} = \bigcap_\sigma I_{\sigma,P}$ is the unique minimal primary decomposition of $I_{\rho,P}$ from Proposition 11.9.*

Proof. Adding the binomials I_σ to the mesoprimary ideal I coarsens its congruence to another mesoprimary one, so each ideal $I + I_\sigma$ is mesoprimary, and hence primary by Corollary 15.2. The intersection $J = \bigcap_\sigma (I + I_\sigma)$ obviously contains I, and we need that $J \subseteq I$, or equivalently that $I_\rho = \bigcap_\sigma I_\sigma$ maps to 0 in the quotient $\Bbbk[Q]/I$. This is a consequence of Proposition 15.1, completing the proof. $\qquad\square$

Remark 15.5. If I is coprincipal in Proposition 15.4, then every primary component there is a coprincipal ideal. Indeed, the partially ordered monoid of Green's classes that is used to detect (or construct) coprincipal ideals is the same for I and for $I + I_\sigma$.

The remainder of this section outlines the main consequences of mesoprimary decomposition for primary decomposition.

Theorem 15.6. *Fix a binomial ideal $I \subseteq \overline{\Bbbk}[Q]$ over an algebraically closed field $\overline{\Bbbk}$. Refining any mesoprimary decomposition of I by canonical primary decomposition of its components yields a binomial primary decomposition of I. In characteristic 0, each primary component in this decomposition induces a primitive congruence on Q.*

Proof. Proposition 15.4 implies binomiality of the primary decomposition. For the final claim, it suffices to prove that every component $I + I_\sigma$ in Proposition 15.4 induces a primitive congruence in characteristic 0. But since σ is a saturation of ρ, the quotient of Q_P modulo the congruence induced by $I + I_\sigma$ is exactly the quotient of $Q_P/\sim_I$ by the torsion subgroup of its unit group. $\qquad\square$

Remark 15.7. No choices are necessary to construct the coprincipal decomposition in Theorem 13.3 or the combinatorial mesoprimary decomposition in Corollary 13.5, and hence no choices are necessary to construct the primary decomposition in Theorem 15.6: these decompositions are all canonically recovered from essentially combinatorial data — a set of witnesses and monoid primes, plus the congruence induced by the binomial ideal — just as in the monomial case. Canonicality in the binomial context, however, comes at the price of nonminimality. Some redundancy can be eliminated using Section 16, but without arbitrary, unmotivated (and often symmetry-breaking) choices, redundancy can stubbornly persist. The reason is that the redundancy is already inherent in the combinatorics; that is, it happens at the level of monoids, congruences, and witnesses, before coefficients enter the picture. Note that by "canonical" we mean in the sense of "determined without extra data or requirements". In contrast, Ortiz [1959] uses the adjective "canonical" to refer to primary decompositions that minimize a certain index of nilpotency. Regardless of the name, Ojeda [2011] proves that the components in Ortiz's "canonical" decompositions are binomial when the original ideal is binomial, but these decompositions generally differ from the ones here, which rely solely on intrinsic data.

Remark 15.8. In positive characteristic p, primary binomial ideals need not be mesoprimary. This feature of mesoprimary decomposition reflects its freedom from characteristic. For instance, according to Hasse's local-to-global principle the ideal $\langle x^p - 1, y(x-1), y^2 \rangle$ has no business being primary: in all but one characteristic it has two or more associated objects that accidentally coincide in characteristic p.

When the base field $\Bbbk$ is not algebraically closed, the binomial ideal I need not possess a binomial primary decomposition over $\Bbbk$ (see Example 11.15, for instance), but it does have one over the algebraic closure $\overline{\Bbbk}$. One of our original motivations for seeking a theory of mesoprimary decomposition was to gather primary components in such a way that Galois automorphisms (of $\overline{\Bbbk}$ over $\Bbbk$) permute them. In particular, if two primes are Galois translates of one another, then we wanted their corresponding primary components to look combinatorially the same.

Theorem 15.9. *If the ideal I in Theorem 15.6 is defined over a subfield $\Bbbk$ of its algebraic closure $\overline{\Bbbk}$, then the primary decomposition there is fixed by the Galois group $\mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. More precisely, if $\pi \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ is a Galois automorphism and C is one of the primary components of I from Theorem 15.6, then $\pi(C)$ is another one of them.*

Proof. The Galois group fixes every mesoprimary component of I, and the primary decomposition of a mesoprimary ideal (Proposition 15.4) is canonical. $\square$

Our final result on the primary-to-mesoprimary correspondence shows that, for general binomial ideals, every associated prime is detected by an associated mesoprime. For cellular binomial ideals, the relationship between associated mesoprimes and associated primes is even more perfectly precise. The cellular case of the following result over an algebraically closed field is [Eisenbud and Sturmfels 1996, Theorem 8.1] and its converse; the latter was stated and used without proof after [Eisenbud and Sturmfels 1996, Algorithm 9.5]. First, a matter of notation.

Definition 15.10. Fix a cellular binomial ideal $I \subset \Bbbk[Q]$. If $P \subset Q$ is the prime ideal of exponents on monomials that are nilpotent modulo I, then I is *P-cellular*.

Theorem 15.11. *Fix a binomial ideal $I \subseteq \Bbbk[Q]$ over an arbitrary field $\Bbbk$.*

(1) *Each associated prime of I is minimal over some associated mesoprime of I.*

(2) *If I is cellular, then the binomial converse holds: every binomial prime that is minimal over an associated mesoprime of I is an associated prime of I.*

Proof. For part (1), apply Corollary 15.2 to the components of I under any mesoprimary decomposition from Theorem 13.2.

For the cellular converse, suppose that I is P-cellular, and that a binomial prime $I_{\sigma,P}$ is minimal over some associated mesoprime $I_{\rho,P}$ of I. The submodule of $\Bbbk[Q]/I$ generated by a witness for $I_{\rho,P}$ is isomorphic to a quotient $\Bbbk[Q]/I'$, for a

binomial ideal I' all of whose witness characters are extensions of ρ. After subsequently binomially localizing at $I_{\sigma,P}$, the only surviving characters are restrictions of σ, and hence sit between σ and ρ. In particular, this is true for the character at any given monomial t^q such that q is a cogenerator of the induced congruence. Such a monomial generates a mesoprime submodule with $I_{\sigma,P}$ among its associated primes by Corollary 15.2. Therefore $I_{\sigma,P}$ is associated to I', and hence to I by Theorem 14.9; see Remark 14.10. $\qquad\square$

Example 15.12. Given an associated prime of I as in Theorem 5.11(1), the associated mesoprime guaranteed by the theorem need not be unique. This phenomenon is illustrated by Example 2.17.5. The binomial prime $\langle x - 1, y \rangle$ for the trivial character on the x-axis $\mathbb{N} \times \{0\}$ is associated to I and has two possible choices of associated mesoprime, namely $\langle x - 1, y \rangle$ and $\langle x^2 - 1, y \rangle$. Combinatorially, the row of dots at height 1 consists of two classes, each being the nonnegative points in a coset of an unsaturated lattice, while the row of dots at height 2 comprise just one class, the nonnegative points in a coset of the saturation. In general, when the group of units G_P acts, there could be a whole G_P-orbit of classes corresponding to an unsaturated subgroup K, and a higher G_P-orbit with an associated subgroup anything between K and its saturation.

Example 15.13. Unmixed (cellular) binomial ideals need not be mesoprimary. Consider the cellular binomial ideal $\langle x^2 - 1, y(x - 1), y^2 \rangle \subset \Bbbk[x, y]$. It is not mesoprimary, but because its associated primes are $\langle x - 1, y \rangle$ and $\langle x + 1, y \rangle$, it is unmixed (even primary if $\mathrm{char}(\Bbbk) = 2$). Consequently, the unmixed decompositions of [Eisenbud and Sturmfels 1996, Corollary 8.2] and [Ojeda Martínez de Castilla and Piedra-Sánchez 2000, Algorithm A4] do not decompose this ideal and thus do not lead to mesoprimary — let alone coprincipal — decompositions, even in cellular cases.

16. Character witnesses and false witnesses

The set of I-witnesses in the arithmetic setting of a binomial ideal I in a monoid algebra can be redundant in a manner that parallels the redundancy of witnesses in the combinatorial setting of monoid congruences. In the combinatorial setting, some of the redundancy is naturally eliminated by restricting to key witnesses; in the arithmetic setting here, character witnesses (Definition 16.3) play an analogous role. For cellular binomial ideals this is Theorem 16.9. Lifting to the general (i.e., noncellular) case is possible but would take us too far afield to be included here.

Definition 16.1. Fix a binomial ideal $I \subset \Bbbk[Q]$, an element $q \in Q$, and a monoid prime ideal $P \subset Q$. A *P-cover extension at q* is an extension of the character $\rho_q^P : K_q \to \Bbbk^*$ of I_P at q to the character $\rho_{p+q}^P : K_{p+q} \to \Bbbk^*$ at a P-cover $p+q$ of q (Definitions 4.4 and 11.11).

There can be many — even infinitely many — choices of minimal generating sets for P (Remark 4.5), but just as in Lemma 4.6, there are not too many P-cover extensions.

Lemma 16.2. *In the situation of Definition 16.1, the set of P-cover extensions at q is finite, in the sense that only finitely many stabilizers K_{p+q} occur, and only finitely many characters defined on each stabilizer occur among the characters ρ^P_{p+q}.*

Proof. Let $\bar{Q}$ be the quotient of Q modulo the congruence determined by I. If the images of p and p' are Green's-equivalent in $\bar{Q}$, then the stabilizers K_{p+q} and $K_{p'+q}$ coincide, as do the extensions to ρ^P_{p+q} and $\rho^P_{p'+q}$. Now apply Remark 4.5. $\square$

Definition 16.3. Fix a prime $P \subset Q$, a P-cellular binomial ideal $I \subset \Bbbk[Q]$, and $w \in Q$.

(1) The *testimony* of w at P is the set $T_P(w)$ of P-cover extension characters.

(2) The testimony $T_P(w)$ is *suspicious* if the intersection of the corresponding mesoprimes equals the P-mesoprime I^P_w (Definition 11.7); that is, if
$$I^P_w = \bigcap_{\rho \in T_P(w)} I_{\rho,P}.$$

(3) A *false witness* is an I-witness w for P that is not maximal (under Green's preorder) among I-witnesses for P and whose testimony at P is suspicious.

(4) An I-witness that is not false is a *character witness*.

Remark 16.4. For algebraically closed $\Bbbk = \bar{\Bbbk}$, Definition 16.3(4) becomes transparent, as follows. Minimal primary decompositions of mesoprimes $I_{\rho,P}$ (Proposition 11.9) are easy and canonical in that case: every saturated finite extension of ρ appears exactly once. A finite intersection of mesoprimes $I_{\sigma,P}$, each containing $I_{\rho,P}$, equals $I_{\rho,P}$ when, among all of the saturated finite extensions of the characters σ, every saturated finite extension of ρ appears at least once. A character witness for P with associated mesoprime $I_{\rho,P}$ is a witness in possession of a new character (a saturated finite extension) not present in its testimony. By the same token, a witness is false if it has no new characters to mention: the set of characters in its testimony is suspiciously complete.

The relation between the different types of witnesses from monoid land (key witnesses) and binomial land (character witnesses) is not as strong as one may hope. For example, a key witness can be a false witness (Example 16.5), and a character witness might not be a key witness (Example 16.6). It is also possible for a nonkey witness to be a false witness (Example 16.7). All of these examples are cellular binomial ideals.

Example 16.5. Consider the ideal $I' = \langle x(z-1), y(z+1), z^2 - 1, x^2, y^2 \rangle$ from Example 9.1 and let P be the monoid prime of $\mathbb{N}^3$ such that $\mathfrak{m}_P = \langle x, y \rangle$. Then $0 \in \mathbb{N}^3$ is a key I'-witness for P that is a false I'-witness: the P-mesoprimes at the

P-covers of 0 are $\langle z-1 \rangle$ and $\langle z+1 \rangle$, whose characters form the complete set of saturated finite extensions of the character for $\langle z^2-1 \rangle$. The testimony is suspicious because $\langle z-1 \rangle \cap \langle z+1 \rangle = \langle z^2-1 \rangle$. In contrast, $0 \in \mathbb{N}^3$ is a character I-witness for P, where the ideal $I = \langle x(z-1), y(z-1), z^2-1, x^2, xy, y^2 \rangle$ induces the same congruence as I'.

Example 16.6. In Definition 16.3, the intersection of the mesoprimes is the analogue of intersecting the kernels of the cover morphisms in Definition 4.7. The necessity of allowing all (nonkey) witnesses as potential character witnesses stems from the phenomenon in Example 2.22 (the common refinement of the congruences induced by $\langle x-1 \rangle$ and $\langle y-1 \rangle$ is trivial whereas the intersection of these ideals not) but is better illustrated by $I = \langle x^2-xy, y^2-xy, x(z-1), y(w-1), x^3 \rangle \subset \Bbbk[x, y, z, w]$, which throws an extra generator x^3 into the ideal from Example 4.15(3). In contrast with that example, the extra monomial causes I to be cellular: the primary congruence it induces has associated monoid prime $P = \langle e_x, e_y \rangle$. But the P-prime congruence at the character I-witness $0 \in \mathbb{N}^4$ remains trivial, being the common refinement of the congruences induced by $\langle z-1 \rangle$ and $\langle w-1 \rangle$. This trivial P-prime congruence at 0 indicates a total lack of binomials in the $\bar{Q}$-degree 0 part of the intersection $\langle z-1, x^2, y \rangle \cap \langle w-1, x, y^2 \rangle$, but this lack is accompanied by nonbinomial elements. An additional intersectand, namely the prime ideal $\langle x, y \rangle$ itself, is required to enforce binomiality.

In terms of Definition 16.3, the testimony consists entirely of saturated but infinite extensions of the character of I_P at $0 \in \mathbb{N}^4$. Therefore no saturated finite extensions occur, in the sense of Remark 16.4, making $0 \in \mathbb{N}^4$ a rather strong character I-witness, even though it is not a key witness for the congruence induced by I.

Example 16.7. Nonkey witnesses can be false witnesses. In Example 8.12 the origin is a false witness because $\langle a^2-1, b-1 \rangle \cap \langle a-1, b^2-1 \rangle \cap \langle ab-1, a-b \rangle = \langle a^2-1, b^2-1 \rangle$ exhibits suspicious testimony.

Definition 16.8. Fix a cellular binomial ideal $I \subseteq \Bbbk[Q]$ in a finitely generated commutative monoid algebra over a field $\Bbbk$. A mesoprimary decomposition of I is *characteristic* if every cogenerator for every mesoprimary component is a character I-witness.

Theorem 16.9. *Fix I, a cellular binomial ideal. I admits a characteristic mesoprimary decomposition. In fact, I is the intersection of the coprincipal ideals cogenerated by its character witnesses. More generally, if I is expressed as an intersection of coprincipal components of I, then any component cogenerated by a false witness is redundant.*

In particular, the components for false witnesses can be thrown out (with their testimony) from the coprincipal decomposition in Theorem 13.3 for a cellular binomial ideal.

Proof. P-cellular ideals have only finitely many Green's classes of witnesses for P, because their induced congruences have only finitely many Green's classes to begin with by Lemma 2.19. Therefore the intersection over character witnesses is finite.

Express I as an intersection of mesoprimary components of I cogenerated by single witnesses, one of which is $W = W_w^P(I)$, cogenerated by a false witness w. Given an element $f \notin W$, we need f to lie outside of the intersection I' of the other components. It suffices to show that f lies outside at least one of the other components. To that end, there is no harm in localizing along P, because by Lemma 13.4 if f lies outside of a coprincipal component after localizing then it does so before localizing. Henceforth, therefore, assume P is the maximal monoid ideal. Furthermore, if f' is a monomial multiple of f that remains outside of W, then concluding that $f' \notin I'$ is enough. Therefore, replacing f by a monomial multiple of f, assume f is annihilated, modulo W, by the entire maximal monomial ideal. Write $f = f_{\preceq w} + f_{\npreceq w}$, where $f_{\preceq w}$ is the sum of the terms of f whose exponents lie in $w + G$ for $G = Q \setminus P$, the unit group of Q.

The first goal is to show that $f \in I' \implies f_{\preceq w} \in I'$. Let v be any I-witness and set $W' = W_v^P(I)$. When $w \nprec v$ in Green's preorder, it is automatic that $f_{\preceq w} \in W'$, for then all monomials with exponents in $w + G$ lie in W'. Therefore assume $w \prec v$ and $f \in W'$. The relation $w \prec v$ implies that w is not nil modulo the congruence $\sim_{W'}$ induced by W', and consequently no term of $f_{\preceq w}$ has an exponent that is congruent under $\sim_{W'}$ to the exponent on a term of $f_{\npreceq w}$. Therefore $f \in W' \implies f_{\preceq w} \in W'$.

We have reduced to showing that $f \notin W \implies f \notin I'$ when $f = f_{\preceq w}$, so assume $f = f_{\preceq w} \notin W$. For each generator $p \in P$, let $\sigma_p \in T_P(w)$ be the corresponding P-cover extension character. The crucial observation is that, since f is a sum over $w + G$,

$$t^p f \in I \iff f \in W + I_{\sigma_p}.$$

This equivalence holds by tracing through all of the definitions; it implies that $t^p f \in I$ for all generators $p \in P$ precisely when

$$f \in \bigcap_p (W + I_{\sigma_p}) = W + \bigcap_p I_{\sigma_p} = W + I_w^P = W,$$

where the first displayed equality is a consequence of Proposition 15.1. Since $f \notin W$, it follows that there is some generator $p \in P$ such that $t^p f \notin I$. But $t^p f \in W$ by construction, so $t^p f$ lies outside of some other coprincipal component of I, and hence so does f itself, as desired.   □

Where did cellularity enter the proof of the preceding proposition? Beyond finiteness of witnesses, the conclusion that no term of $f_{\preceq w}$ has an exponent congruent under $\sim_{W'}$ to the exponent on a term of $f_{\npreceq w}$ would be false if W' were allowed to be a coprincipal component for a monoid prime strictly contained in P; see the next example.

Example 16.10. Let

$$I = \langle x^2 - x\dot{x},\, x\dot{x} - \dot{x}^2,\, x^3,\, x^2 y,\, z^2 - 1,\, x^2(z-1),\, y(z+1),\, y(x - \dot{x}) \rangle \subseteq \Bbbk[x, \dot{x}, y, z].$$

(The variables x and $\dot{x}$ correspond to x and y in Example 2.18.) Then $\dot{x}$ is a false I-witness monomial for the monoid prime P corresponding to $\mathfrak{m}_P = \langle x, \dot{x}, y \rangle$: the character at $\dot{x}$ is $z^2 - 1$, while at $x\dot{x}$ it is $z - 1$ and at $y\dot{x}$ it is $z + 1$. Omitting the coprincipal component $\langle x^2, x\dot{x}, \dot{x}^2, y, z^2 - 1 \rangle$ of I cogenerated by $\dot{x}$ from the coprincipal decomposition of I in Theorem 13.3 leaves $\langle x^3, x^2 - x\dot{x}, x\dot{x} - \dot{x}^2, y, z - 1 \rangle \cap \langle x^2, x - \dot{x}, z + 1 \rangle$, which is not a binomial ideal. The element $f = x - \dot{x}$ has a monomial $\dot{x} = t^w$ whose exponent w is congruent to the exponent of $x = t^q$ under $\sim_{W'}$ for $W' = \langle x^2, x - \dot{x}, z + 1 \rangle$ even though q and w are incomparable. W' is P'-mesoprimary for $\mathfrak{m}_{P'} = \langle x, \dot{x} \rangle \subsetneq \mathfrak{m}_P$.

Remark 16.11. One reason Theorem 16.9 restricts to the cellular case is the automatic finiteness for witnesses. In contrast, in Section 12 the notion of essential witness does the job by Lemma 12.4. In general, even modulo Green's equivalence the set of I-witnesses can be infinite. For example, infiniteness causes Proposition 12.17 to fail when $I = \langle x^2 y - y^2 x \rangle$ if one uses all I-witnesses for $\mathfrak{m}_P = \langle x, y \rangle$. The sets of essential and character witnesses do not coincide, because of the false key witnesses in Example 16.5, but it is possible that every character I-witness could be an essential I-witness.

Question 16.12. Are there redundant character witnesses? key witnesses?

17. Open problems

Beyond Question 16.12, the results of this paper raise other problems implicitly in the remarks, and still others that constitute future research directions beyond the scope of this paper. We collect some of these problems here.

17.1. *Intersections of binomial ideals.*

Problem 17.1. Characterize when an intersection of binomial ideals is binomial.

Problem 17.1 was originally posed by Eisenbud and Sturmfels [1996, Problem 4.9], who answered it in the reduced situation [1996, Theorem 4.1]. In our language, that theorem contains information about the associated prime ideals of the congruence induced by a radical binomial ideal. It is possible that the general case could reduce to the radical case, by considering what the congruence or the P-prime characters induced by the intersection could possibly look like at each monoid element. This type of consideration underlies the definition of character witness (Definition 16.3), where nonbinomiality at specific monoid elements would otherwise occur, without specifically throwing in additional binomials, because of incompatibility of congruences or characters arising from covers.

As a stepping stone to a full answer to Problem 17.1, one might consider [Eisenbud and Sturmfels 1996, Problem 6.6]: does intersecting the minimal primary components of a binomial ideal result in another binomial ideal?

17.2. *Choices of vertical coefficients.* Remarks 12.21 and 12.22 raise the following.

Problem 17.2. Characterize the mesoprimary ideals that induce a fixed mesoprimary congruence with a fixed associated mesoprime. In particular, decide when the set of such mesoprimary ideals is nonempty.

17.3. *Primary binomial ideals in positive characteristic.* Lack of knowledge concerning the combinatorics of primary binomial ideals in positive characteristic is an obstacle in our investigations. In particular we do not know exactly which primary binomial ideals are mesoprimary.

Problem 17.3. Characterize primary binomial ideals with nontrivial mesoprimary decompositions.

17.4. *Posets of mesoprimes.*

Problem 17.4. Characterize the posets of associated prime congruences of primary congruences.

The problem could have been stated for arbitrary congruences, but then every finite poset would be possible, because every finite poset occurs as the set of associated primes of a monomial ideal (this is a good exercise, but it follows from [Miller 1998]). Problem 17.4 is equivalent to characterizing posets of associated mesoprimes of unital cellular binomial ideals. Such posets always possess a unique minimal element, represented by the identity element of the finite partially ordered monoid of Green's classes in Lemma 2.19. When devising examples for the present paper, we often used a technique to "place" associated mesoprimes at desired locations, illustrated as follows.

Example 17.5. Let $\Delta \subsetneq \Gamma$ be simplicial complexes on $\{1, \ldots, n\}$ and consider the polynomial ring in $2n$ variables $S = \Bbbk[x_1, \ldots, x_n, y_1, \ldots, y_n]$. For any $A \in \Gamma \setminus \Delta$ write $x_A := \prod_{i \in A} x_i$. The poset of associated mesoprimes of the cellular binomial ideal

$$I_{\Gamma \setminus \Delta} = \sum_{A \in \Gamma \setminus \Delta} I_A + \langle x_i^2 \mid i = 1, \ldots, n \rangle \subset S \quad \text{for} \quad I_A = \langle x_A(y_i - 1) \mid i \in A \rangle$$

is isomorphic to $(\Gamma \setminus \Delta) \cup \{\varnothing\}$.

Remark 17.6. The construction in the previous example is fairly general, and one might hope that complete generality is possible. In practice this problem will be

about understanding what happens to the partial order on $\mathbb{N}^n$ when passing to a quotient and under the order-preserving map assigning to a witness its associated prime congruence.

Remark 17.7. Definition 5.2 requires associated prime congruences to appear at key witnesses. Allowing arbitrary witnesses yields an a priori different notion of associated prime congruence: although the P-prime congruence at an arbitrary witness for P agrees with the P-prime congruence at some key witness, the key witness might be for a monoid prime smaller than P. This phenomenon does not occur for primary congruences, however, as they have only one associated monoid prime. Thus Problem 17.4 would have the same answer if Definition 5.2 had allowed arbitrary witnesses.

Nonetheless, this line of thinking indicates that care must be taken in lifting Problem 17.4 to the arithmetic setting, where Definition 12.1 requires associated mesoprimes to appear at arbitrary witnesses, not at a subset of all witnesses. For instance, a P-mesoprime can be associated to an ideal even though it only appears at a false witness; this occurs in both Example 16.5 and Example 16.7. This idiosyncrasy in the definition of associated mesoprime motivates a new definition.

Definition 17.8. An associated mesoprime of a binomial ideal I is *truly associated* if it is the P-mesoprime of I at a character I-witness for P.

Problem 17.9. Characterize the posets of associated mesoprimes of cellular binomial ideals. Do the same for posets of truly associated mesoprimes.

Remark 17.10. The family of posets referred to in (either version of) Problem 17.9 contains the family of posets in Problem 17.4 by Remark 17.7 applied to the case of unital binomial ideals.

17.5. *Mesoprimary decomposition of modules.* Grillet [2007] shows how subdirect decompositions of semigroups induce subdirect decompositions of sets acted on by semigroups; see Remark 2.2. In a similar vein, mesoprimary decomposition ought to extend to finitely generated monoid actions.

Problem 17.11. Generalize mesoprimary decomposition of congruences to Q-modules.

The generalization ought to parallel the manner in which ordinary primary decomposition of ideals in rings extends to primary decomposition of modules over rings. In the arithmetic setting of mesoprimary decomposition, however, even the first step of the extension requires thought.

Question 17.12. What is a binomial module over a commutative monoid algebra?

A good theory of such modules should yield the desired generalization.

Problem 17.13. Extend mesoprimary decomposition to binomial $\Bbbk[Q]$-modules.

17.6. *Homological invariants of binomial rings.* The combinatorics of the free commutative monoid $\mathbb{N}^n$ gives rise to formulas and constructions for all sorts of homological invariants involving monomial ideals — Betti numbers, Bass numbers, free resolutions, local cohomology, and so on — due to the $\mathbb{N}^n$-grading; see [Miller and Sturmfels 2005]. Gradings by more general affine semigroups yield formulas and constructions for local cohomology over affine semigroup rings (with maximal support [Ishida 1988] as well as with more arbitrary monomial support [Helm and Miller 2003; 2005]), and Betti numbers for toric ideals [Stanley 1996, Theorem I.7.9], etc. Having identified the combinatorics controlling decompositions of binomial ideals, the way is open to generalize monomial homological algebra.

Question 17.14. Do there exist combinatorial (monoid-theoretic) formulas for local cohomology, Tor, and Ext involving binomial quotients of polynomial rings?

Remark 17.15. In contrast, it is unclear to us whether combinatorial formulas for local cohomology with binomial support should exist, partly because of ill-behaved characteristic dependence; see [Iyengar et al. 2007, Example 21.31].

As soon as there is some control over Betti tables, Boij–Söderberg theory [Fløystad 2012] enters the picture. There one decomposes the Betti table $\beta(M)$ of a module M over a polynomial ring S as a rational linear combination of certain *pure tables* π_d:

$$\beta(M) = \sum a_d \pi_d.$$

Question 17.16. What combinatorics, if any, explains the coefficients a_d of $S/I_{\rho,P}$ as an S-module when $I_{\rho,P}$ is a mesoprime?

Even the special case of Boij–Söderberg theory for toric ideals is currently open.

17.7. *Test sets in integer programming.* Let $A \in \mathbb{Z}^{d \times n}$ be an integer matrix. An *integer program* is an optimization problem that seeks, for a given cost vector $\omega \in \mathbb{R}^n$, to maximize $\omega \cdot u$ over the integer points in the polyhedron $\mathcal{F}_b = \{u \in \mathbb{N}^n \mid Au = b\}$ for $b \in \mathbb{N}A := A(\mathbb{N}^n) \subseteq \mathbb{Z}^d$. A solution to this problem is the computation of a *test set*: a set $\mathcal{B}$ of differences between points in $\mathcal{F}_b$ such that for any candidate solution u to the optimization problem, its optimality can be tested by comparing it to $u + v$ for $v \in \mathcal{B}$. Computing a Gröbner basis of the toric ideal $I_A = \langle x^u - x^v \mid u, v \in \mathbb{N}^n$ and $Au = Av \rangle$ provides a simultaneous test set for all right-hand sides b, but this procedure may be computationally prohibitive. The hope behind the following problem is that for many b a test set is significantly simpler than a Gröbner basis.

Problem 17.17. Fix a finite set $\mathcal{B} \subset \ker_{\mathbb{Z}} A$.

(1) Characterize the multidegrees $b \in \mathbb{N}A$ for which $\mathcal{B}$ is a test set.

(2) Quantify the failure of $\mathcal{B}$ to be a test set in large fibers $\mathcal{F}_b$.

Intuition for the second problem comes from the geometry of mesoprimary components, or better yet, coprincipal components: their thicknesses in various directions should provide bounds on how close an integer point in $\mathcal{F}_b$ can get to optimality using $\mathcal{B}$. Indeed, starting at some $u \in \mathbb{Z}^n$ and successively progressing to the (local) optimum achieved by moving along vectors in $\mathcal{B}$ is equivalent to normal form reduction of x^u using binomials in the ideal $I_\mathcal{B} = \langle x^u - x^v \mid u - v \in \mathcal{B} \rangle$. Classes for the congruence induced by $I_\mathcal{B}$ can be thought of, roughly speaking, as polyhedra of the form $\mathcal{F}_b$ with bits (the "skerries" from [Dickenstein et al. 2010b, Section 1.1]) eaten away from the boundary; mesoprimary decomposition controls the missing boundary bits.

Diaconis, Eisenbud, and Sturmfels suggested — though not in the presence of a cost vector — to systematically study lattice walks with step set $\mathcal{B}$ using primary decomposition of $I_\mathcal{B}$ [Diaconis et al. 1998]. Given the unsuitability of primary decomposition for combinatorial purposes, the method should be updated to work with mesoprimary decompositions. This is especially true in the presence of unsaturated lattices among the minimal primes of $I_\mathcal{B}$, in which case the combinatorial flavor of the problem becomes clouded in the arithmetic (rather than combinatorics) of binomial primary decomposition.

A first step toward Problem 17.17 was developed in [Kahle et al. 2014b]. There the authors study only the connectivity of $\mathcal{F}_b$ as a function of the position of b in the cone $\mathbb{Q}_+ A$. Additionally all ideals there are radical, and consequently the subtleties of mesoprimary decomposition play no role.

Acknowledgements

References

[Adleman et al. 2014] L. Adleman, M. Gopalkrishnan, M.-D. Huang, P. Moisset, and D. Reishus, "On the mathematics of the law of mass action", pp. 3–46 in *A systems theoretic approach to systems and synthetic biology, I: Models and system characterizations*, edited by V. V. Kulkarni et al., Springer, Dordrecht, 2014.

[Anderson and Johnson 1984] D. D. Anderson and E. W. Johnson, "Ideal theory in commutative semigroups", *Semigroup Forum* **30**:2 (1984), 127–158. MR 86c:20060 Zbl 0533.20032

[Ojeda Martínez de Castilla and Piedra-Sánchez 2000] I. Ojeda Martínez de Castilla and R. Piedra-Sánchez, "Cellular binomial ideals. Primary decomposition of binomial ideals", *J. Symbolic Comput.* **30**:4 (2000), 383–400. MR 2001g:13058 Zbl 0991.13008

[Connes and Consani 2011] A. Connes and C. Consani, "On the notion of geometry over $\mathbb{F}_1$", *J. Algebraic Geom.* **20**:3 (2011), 525–557. MR 2012d:14079 Zbl 1227.14006

[Deitmar 2005] A. Deitmar, "Schemes over $\mathbb{F}_1$", pp. 87–100 in *Number fields and function fields: two parallel worlds*, edited by G. van der Geer et al., Progress in Mathematics **239**, Birkhäuser, Boston, 2005. MR 2006j:14002 Zbl 1098.14003

[Diaconis et al. 1998] P. Diaconis, D. Eisenbud, and B. Sturmfels, "Lattice walks and primary decomposition", pp. 173–193 in *Mathematical essays in honor of Gian-Carlo Rota* (Cambridge, MA, 1996), edited by B. E. Sagan and R. P. Stanley, Progress in Mathematics **161**, Birkhäuser, Boston, 1998. MR 99i:13035 Zbl 0962.05010

[Dickenstein et al. 2010a] A. Dickenstein, L. F. Matusevich, and E. Miller, "Binomial D-modules", *Duke Math. J.* **151**:3 (2010), 385–429. MR 2011h:14073 Zbl 1205.13031

[Dickenstein et al. 2010b] A. Dickenstein, L. F. Matusevich, and E. Miller, "Combinatorics of binomial primary decomposition", *Math. Z.* **264**:4 (2010), 745–763. MR 2011b:13063 Zbl 1190.13017

[Drbohlav 1963] K. Drbohlav, "On finitely generated commutative semigroups", *Comment. Math. Univ. Carolinae* **4** (1963), 87–92. MR 29 #4821 Zbl 0138.02001

[Drton et al. 2009] M. Drton, B. Sturmfels, and S. Sullivant, *Lectures on algebraic statistics*, Oberwolfach Seminars **39**, Birkhäuser, Basel, 2009. MR 2012d:62004 Zbl 1166.13001

[Eisenbud and Sturmfels 1996] D. Eisenbud and B. Sturmfels, "Binomial ideals", *Duke Math. J.* **84**:1 (1996), 1–45. MR 97d:13031 Zbl 0873.13021

[Fløystad 2012] G. Fløystad, "Boij–Söderberg theory: introduction and survey", pp. 1–54 in *Progress in commutative algebra 1: Combinatorics and homology*, edited by C. Francisco et al., de Gruyter, Berlin, 2012. MR 2932580 Zbl 1260.13020 arXiv 1106.0381

[Gelfand et al. 1987] I. M. Gelfand, M. I. Graev, and A. V. Zelevinsky, "Holonomic systems of equations and series of hypergeometric type", *Dokl. Akad. Nauk SSSR* **295**:1 (1987), 14–19. In Russian; translated in *Sov. Math. Dokl.* **36**:1 (1987), 5–10. MR 88j:58118 Zbl 0661.22005

[Gelfand et al. 1989] I. M. Gelfand, A. V. Zelevinskiĭ, and M. M. Kapranov, "Гипергеометрические функции и торальные многообразия", *Funktsional. Anal. i Prilozhen.* **23**:2 (1989), 12–26. Translated as "Hypergeometric functions and toral manifolds" in *Funct. Anal. Appl.* **23**:2 (1989), 94–106. Correction in the same journals, **27**:4 (1993), p. 91 (Russian), p. 295 (English). MR 90m:22025 Zbl 0721.33006

[Gilmer 1984] R. Gilmer, *Commutative semigroup rings*, University of Chicago Press, Chicago, 1984. MR 85e:20058 Zbl 0566.20050

[Grayson and Stillman] D. R. Grayson and M. E. Stillman, "Macaulay2: a software system for research in algebraic geometry", http://www.math.uiuc.edu/Macaulay2.

[Grillet 1975] P. A. Grillet, "Primary semigroups", *Michigan Math. J.* **22**:4 (1975), 321–336. MR 53 #3159 Zbl 0352.20045

[Grillet 2001] P. A. Grillet, *Commutative semigroups*, Advances in Mathematics (Dordrecht) **2**, Kluwer, Dordrecht, 2001. MR 2004h:20089 Zbl 1040.20048

[Grillet 2007] P. A. Grillet, "Commutative actions", *Acta Sci. Math.* (*Szeged*) **73**:1-2 (2007), 91–112. MR 2008i:20070 Zbl 1135.20039

[Guo and Miller 2011] A. Guo and E. Miller, "Lattice point methods for combinatorial games", *Adv. in Appl. Math.* **46**:1-4 (2011), 363–378. MR 2012f:91047 Zbl 1213.91045

[Guo et al. 2009] A. Guo, E. Miller, and M. Weimerskirch, "Potential applications of commutative algebra to combinatorial game theory", *Oberwolfach Reports* **22** (2009), 1179–1182. Extended abstract.

[Helm and Miller 2003] D. Helm and E. Miller, "Bass numbers of semigroup-graded local cohomology", *Pacific J. Math.* **209**:1 (2003), 41–66. MR 2004c:13028 Zbl 1078.13009

[Helm and Miller 2005] D. Helm and E. Miller, "Algorithms for graded injective resolutions and local cohomology over semigroup rings", *J. Symbolic Comput.* **39**:3-4 (2005), 373–395. MR 2007d:13025 Zbl 1120.13014

[Herzog et al. 2010] J. Herzog, T. Hibi, F. Hreinsdóttir, T. Kahle, and J. Rauh, "Binomial edge ideals and conditional independence statements", *Adv. in Appl. Math.* **45**:3 (2010), 317–333. MR 2011j:13041 Zbl 1196.13018

[Ishida 1988] M.-N. Ishida, "The local cohomology groups of an affine semigroup ring", pp. 141–153 in *Algebraic geometry and commutative algebra in honor of Masayaoshi Nagata*, vol. 1, edited by H. Hijikata et al., Kinokuniya, Tokyo, 1988. MR 90a:13029 Zbl 0687.14002

[Iyengar et al. 2007] S. B. Iyengar, G. J. Leuschke, A. Leykin, C. Miller, E. Miller, A. K. Singh, and U. Walther, *Twenty-four hours of local cohomology*, Graduate Studies in Mathematics **87**, American Mathematical Society, Providence, RI, 2007. MR 2009a:13025 Zbl 1129.13001

[Kahle 2012] T. Kahle, "Decompositions of binomial ideals", *J. Softw. Algebra Geom.* **4** (2012), 1–5. MR 2947669

[Kahle et al. 2014a] T. Kahle, E. Miller, and C. O'Neill, "Irreducible decompositions of binomial ideals", draft, 2014.

[Kahle et al. 2014b] T. Kahle, J. Rauh, and S. Sullivant, "Positive margins and primary decomposition", *J. Commut. Algebra* **6**:2 (2014), 173–208. MR 3249835 arXiv 1201.2591

[Matusevich et al. 2005] L. F. Matusevich, E. Miller, and U. Walther, "Homological methods for hypergeometric families", *J. Amer. Math. Soc.* **18**:4 (2005), 919–941. MR 2007d:13027 Zbl 1095.13033

[Miller 1998] E. Miller, "Multiplicities of ideals in Noetherian rings", *Beiträge Algebra Geom.* **39**:1 (1998), 47–51. MR 99c:13044 Zbl 0908.13001

[Miller 2002] E. Miller, "Cohen–Macaulay quotients of normal semigroup rings via irreducible resolutions", *Math. Res. Lett.* **9**:1 (2002), 117–128. MR 2003a:13015 Zbl 1044.13005

[Miller 2011] E. Miller, "Theory and applications of lattice point methods for binomial ideals", pp. 99–154 in *Combinatorial aspects of commutative algebra and algebraic geometry* (Voss, 2009), edited by G. Fløystad et al., Abel Symp. **6**, Springer, Berlin, 2011. MR 2012f:13045 Zbl 1251.14041

[Miller 2013] E. Miller, "Affine stratifications from finite misère quotients", *J. Algebraic Combin.* **37**:1 (2013), 1–9. MR 3016298 Zbl 1271.20070

[Miller and Sturmfels 2005] E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics **227**, Springer, New York, 2005. MR 2006d:13001 Zbl 1066.13001

[Noether 1921] E. Noether, "Idealtheorie in Ringbereichen", *Math. Ann.* **83**:1-2 (1921), 24–66. MR 1511996 JFM 48.0121.03

[Ojeda 2011] I. Ojeda Martínez de Castilla, "Binomial canonical decompositions of binomial ideals", *Comm. Algebra* **39**:10 (2011), 3722–3735. MR 2012i:13035 Zbl 1242.13024 arXiv 1003.1701

[Ortiz 1959] V. Ortiz, "Sur une certaine décomposition canonique d'un idéal en intersection d'idéaux primaires dans un anneau Noethérien commutatif", *C. R. Acad. Sci. Paris* **248** (1959), 3385–3387. MR 21 #5656 Zbl 0136.02403

[Plambeck 2005] T. E. Plambeck, "Taming the wild in impartial combinatorial games", *Integers* **5**:1 (2005), Article ID #G5. MR 2006g:91044 Zbl 1092.91012

[Plambeck and Siegel 2008] T. E. Plambeck and A. N. Siegel, "Misère quotients for impartial games", *J. Combin. Theory Ser. A* **115**:4 (2008), 593–622. MR 2009m:91036 Zbl 1142.91022 arXiv math.CO/0609825v5

[Shiu and Sturmfels 2010] A. Shiu and B. Sturmfels, "Siphons in chemical reaction networks", *Bull. Math. Biol.* **72**:6 (2010), 1448–1463. MR 2011e:92117 Zbl 1198.92020

[Stanley 1996] R. P. Stanley, *Combinatorics and commutative algebra*, 2nd ed., Progress in Mathematics **41**, Birkhäuser, Boston, 1996. MR 98h:05001 Zbl 0838.13008

[Vasconcelos 1998] W. V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Algorithms and Computation in Mathematics, Springer, Berlin, 1998. MR 99c:13048 Zbl 0896.13021

thomas.kahle@ovgu.de   *Fakultät für Mathematik, Otto-von-Guericke Universität Magdeburg, Institut Algebra und Geometrie, D-39106 Magdeburg, Germany*

ezra@math.duke.edu   *Mathematics Department, Duke University, Durham, NC 27708, United States*

Algebra & Number Theory

msp.org/ant

Algebra & Number Theory