Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT
ELSEVIER
Journal of Combinatorial Theory, Series A 105 (2004) 185–206
Journal of Combinatorial Theory Series A
http://www.elsevier.com/locate/jcta

From monomials to words to graphs

Cristina G. Fernandes,[a,1] Edward L. Green,[b,2] and Arnaldo Mandel[a,3]

[a] *Departamento de Ciência da Computação, Universidade de São Paulo, São Paulo, SP, 05508-970, Brazil*
[b] *Mathematics Department, Virginia Tech University, USA*

Received 26 February 2003

Communicated by Bernd Sturmfels

Abstract

Given a finite alphabet X and an ordering $\prec$ on the letters, the map $\sigma_\prec$ sends each monomial on X to the word that is the ordered product of the letter powers in the monomial. Motivated by a question on Gröbner bases, we characterize ideals I in the free commutative monoid (in terms of a generating set) such that the ideal $\langle \sigma_\prec(I) \rangle$ generated by $\sigma_\prec(I)$ in the free monoid is finitely generated. Whether there exists an $\prec$ such that $\langle \sigma_\prec(I) \rangle$ is finitely generated turns out to be NP-complete. The latter problem is closely related to the recognition problem for comparability graphs.

Keywords: Gröbner bases; Polynomials; Comparability graphs; NP-complete; Blocking polyhedron

1. Introduction

An important structural difference between commutative and noncommutative free monoids is that in a finitely generated free commutative monoid all ideals are finitely generated (Dickson's Lemma), while this is not the case for free monoids (for instance, the ideal generated by $\{xy^nx \mid n \geqslant 0\}$). We will consider questions about

E-mail addresses: cris@ime.usp.br (C.G. Fernandes), green@math.vt.edu (E.L. Green), am@ime.usp.br (A. Mandel).

[1] Research MCT/CNPq through ProNEx Programme (Proc. CNPq 664107/1997–4).
[2] Partially supported by CNPq/NSF Grant no. 910123/99.
[3] Partially supported by CNPq/NSF Grant no. 910123/99 and MCT/CNPq through ProNEx Programme (Proc. CNPq 664107/1997–4).

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2003.11.001

whether some ideals of the free monoid are finitely generated. Those ideals will be described starting with an ideal in a free commutative monoid.

Let X be a finite alphabet (of *letters*). Denote by $[X]$ the free commutative monoid on X and by X^* the free monoid on X; we call the members of $[X]$ *monomials*, and the members of X^* *words*. When convenient, we assume $X = \{x_1, x_2, \dots, x_n\}$, so a monomial can be written multiplicatively as $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. We denote by π the canonical monoid epimorphism $X^* \to [X]$.

The most natural relation between ideals of $[X]$ and X^* is given by the canonical map, so the first question is:

Problem 1. Given an ideal I of $[X]$, is $\pi^{-1}(I)$ finitely-generated?

This first question, while quite natural, seems to be of limited interest, as ideals are not such big players in the structure theory of monoids.

The next questions were motivated by the study of noncommutative presentations of affine algebras and their Gröbner bases. In fact, the problems studied in this paper were motivated by a question posed by Bernd Sturmfels on the finite generation of monomial ideals. We postpone the discussion until Section 2, as the questions can be completely understood within the context of monoids.

For each ordering $\prec$ of the letters, we define a section $\sigma_\prec$ of π as follows. We say that a word is *sorted* if its letters occur in it in increasing order; if $x_1 \prec x_2 \prec \cdots \prec x_n$, such a word can be uniquely written as $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Let $\sigma_\prec : [X] \to X^*$ be the function mapping each monomial m to the unique sorted word in $\pi^{-1}(m)$. So, $\pi\sigma_\prec$ is the identity map on $[X]$, and we define the *sorting map* $S_\prec$ on X^* by $S_\prec = \sigma_\prec \pi$. The subscript $\prec$ will be omitted when implicitly understood.

We will mainly be concerned with ideals of form $\mathscr{I}_\prec(I) = \langle \sigma_\prec(I) \rangle$, that is, the ideal generated by sorted words corresponding to a commutative ideal.

Problem 2. Given an ideal I of $[X]$ and an ordering $\prec$ of X, is $\mathscr{I}_\prec(I)$ finitely generated?

While it is convenient to assume an ordering on the letters so that one can write monomials, that ordering is not part of $[X]$. So, we also consider

Problem 3. Given an ideal I of $[X]$, is there an ordering $\prec$ of X so that $\mathscr{I}_\prec(I)$ is finitely generated?

These problems are very loosely posed, as it is not specified how each ideal is given. We are interested in specification by finite data, so that it makes sense to look for an algorithmic answer to each of the problems. We consider three forms of specifying an ideal of $[X]$: by a finite generating set, as the inverse image of an ideal under a morphism from $[X]$, and as the initial ideal of a polynomial ideal given by its generators. The latter is explained in Section 2; our main results relate to the other two.

Most of this paper will be concerned with a finite set of monomials and the ideal it generates. Let us denote by $\langle M \rangle$ the monoid ideal generated by a set M. So, $\langle M \rangle = M[X]$ if $M \subseteq [X]$, and $\langle M \rangle = X^*MX^*$ if $M \subseteq X^*$. From now on, except where explicitly stated, in each of the problems above, *given an ideal* I is reinterpreted as *given a finite set* M *of monomials, let* $I = \langle M \rangle$. That is the first of the three forms mentioned above.

It is not clear a priori that either problem is even decidable. Section 3 shows that standard methods of Automata Theory suffice to decide each instance of the problems, when the ideal is given by generators. However, this is unsatisfying both mathematically and computationally. From a purely mathematical viewpoint, the automata decision process is so far removed from the initial data that one learns very little about the underlying structure. From the computational viewpoint, what goes wrong is the exponential complexity of the algorithms thus obtained. We heed the fact that a monomial can be given as a vector of exponents, so the run-time of algorithms for the corresponding decision problems should be measured relative to the bit size of the exponents. With that in mind, we summarize the main results:

Problem 1 is solved completely in Section 7. The characterization we obtain yields a polynomial algorithm.

Problem 2 is the central one here, and also has a definite answer. To describe it we need more notation. We suppose an ordering of X is given. For w in $[X]$, say that a letter is *extremal* in w if it is the smallest or the largest letter with a positive exponent there and say that a letter is *internal* to w if it lies strictly between the extremal letters. Notice that an internal letter is not required to occur in w; for instance, using the ordering implied by the indices, the internal letters of $x_2^3x_3x_5^2x_7$ are x_3, x_4, x_5, and x_6. Also denote by $w\backslash x$ the monomial resulting of evaluating x to 1 in the monomial w. In particular, $x^m\backslash x = 1$. A collection of monomials is an *antichain* if no one divides another; clearly, the (unique) minimal generating set of an ideal of $[X]$ is an antichain. Dickson's Lemma, quoted earlier, is equivalent to the statement that every antichain of monomials is finite. For convenience, we will shorten $\mathscr{I}(\langle M \rangle)$ to $\mathscr{I}(M)$ when M is an arbitrary set of monomials.

Theorem 1. *Let M be an antichain in $[X]$. Then, $\mathscr{I}(M)$ is finitely generated if and only if, for every w in M and x in X, there exists s in M such that x is extremal in s and $s\backslash x$ divides w.*

A proof is found in Section 4. The above result immediately yields a polynomial-time decision algorithm for Problem 2. It also implies that Problem 3 is in NP.

When M is square free, Problem 3 can be decided in polynomial time. And that is the end of good news. Problem 3 is shown in Section 6 to be NP-complete even when M consists only of quadratic monomials. So, while the automata-theoretic algorithms where unacceptable for Problems 1 and 2 because of high exponents in the data, NP-completeness of Problem 3 is not related to the possibility of writing numbers succinctly.

In Section 8, using a slightly homological flavor, we turn to another way of presenting an ideal of $[X]$: fix a homomorphism from $[X]$ to another free commutative monoid, and an ideal J in the target, and take the pre-image of that ideal. The homomorphism can be described by a matrix, and when J is given by its minimal generators the ideal of $[X]$ is described as a finite union of integer polyhedra, each one of them an ideal. The theory developed for handling generators is enough to show that Problems 1 and 2 become coNP-complete with this data, while Problem 3 is shown to be NP-hard.

2. Connections with Gröbner bases

Problems 2 and 3 stem from a connection between the commutative and noncommutative Gröbner bases theories. Let K denote a field, $K[X]$ the commutative polynomial ring on the finite set X, and $K\langle X\rangle$ the free associative algebra on the same set (we adhere to the terminology of the first section, and talk about *letters* instead of variables). The linear extension of the monoid morphism π is a ring morphism $K\langle X\rangle \to K[X]$, still denoted by π; its kernel is generated by the commutation relations $\mathscr{C} = \{xy - yx \mid x, y \in X\}$. Also, given an ordering of X, the linear extension of the maps σ and S will be denoted by the same symbols.

Throughout this section, I is an ideal of $K[X]$ and $J = \pi^{-1}(I)$. It is occasionally useful to lift a commutative ring presentation $K[X]/I$ to a noncommutative presentation $K\langle X\rangle/J$ through π. This has been used in [1,2,10,15] for homological computations.

Proposition 2. *Let $A \subseteq \langle X\rangle$ be a set of noncommutative polynomials. The following are equivalent*:

(i) *$\mathscr{C} \cup A$ generates J.*
(ii) *$\pi(A)$ generates I.*
(iii) *For some ordering $\prec$ of X, $\mathscr{C} \cup S_{\prec}(A)$ generates J.*
(iv) *For any ordering $\prec$ of X, $\mathscr{C} \cup S_{\prec}(A)$ generates J.*

In particular, for any ordering $\prec$ of X, $\mathscr{C} \cup \sigma_{\prec}(I)$ generates J.

Proof. Suppose that $\mathscr{C} \cup A$ generates J. Then, $\langle \pi(A)\rangle = \langle \pi(\mathscr{C} \cup A)\rangle = \pi\langle \mathscr{C} \cup A\rangle = \pi(J) = I$. Conversely, suppose that $\pi(A)$ generates I. Since $\ker\pi \subseteq \langle \mathscr{C} \cup A\rangle \subseteq \pi^{-1}(I)$ and $\pi\langle \mathscr{C} \cup A\rangle = I$, it follows that $\langle \mathscr{C} \cup A\rangle = J$.

The equivalence of conditions (iii) and (iv) to the previous ones follows from the observation that $\pi S_{\prec}(A) = \pi(A)$. The last observation is immediate, as $\pi\sigma_{\prec}(I) = I$. $\square$

In many applications, one wants to describe a Gröbner basis for J, preferably related to a Gröbner basis for I. Let us recall quickly what those bases are (see [9,13] for an introduction to the subject). We will say *term* to mean either "word" or "monomial", so we can treat commutative and noncommutative polynomials simultaneously.

A necessary ingredient for a Gröbner bases theory is to fix a *term order*: a total order on the terms, compatible with multiplication and with 1 as minimum, and with no infinite descending chains. In this case, every polynomial has an *initial term*, the maximum term in its support, and to every ideal I one associates its *initial ideal* $In(I)$, the set of all initial terms of polynomials in I. The initial ideal is an ideal of the monoid of terms. A *Gröbner basis* for I is a subset B of I such that the initial terms of the members of B generate $In(I)$.

Eisenbud, et al. [5] took the following approach to relate Gröbner bases for commutative polynomial ideals and their pre-images in the free algebra. Start with a term order $\prec$ on $[X]$, and define its *lexicographic extension*, still denoted here by $\prec$, to X^* by: $u \prec v$ if $\pi(u) \prec \pi(v)$ or $\pi(u) = \pi(v)$ and u precedes v lexicographically, according to the $\prec$ ordering on X.

Proposition 3. *The initial ideal $In(J)$ is generated by*

$$\{xy \mid x, y \in X, \ x \succ y\} \cup \sigma(In(I)).$$

Proof. Since the noncommutative order extends the commutative one, if $p \in K[X]$, the initial term of $\sigma(p)$ is $\sigma(m)$, where m is the initial term of p. Also, from the lexicography, if $x \succ y$ are letters, xy is the initial term of $xy - yx$. The result now follows from Proposition 2. $\square$

It follows from Dickson's Theorem that every ideal of $[X]$ is finitely generated, hence every ideal of $K[X]$ has a finite Gröbner basis. In contrast, not every ideal of X^* is finitely generated, so it is generally interesting to detect whether a given ideal of $K\langle X \rangle$ has a finite Gröbner basis. The preceding proposition implies that J has a finite Gröbner basis with respect to $\succ$ if and only if $\mathscr{I}(In(I))$ is finitely generated. This gives rise to Problem 2.

A word in an ideal of X^* is a minimal generator of that ideal if and only if the words obtained by erasing either the first or the last letter are not in the ideal. Combining it with Proposition 2, we get the next result; it is Theorem 2.1 of [5], stripped of the ring theoretic context (which is handled by Proposition 3):

Theorem 4. *If M is an antichain of monomials, then the minimal generating set of $\mathscr{I}(M)$ is*

$$\{\sigma(mu) | m \in M, u \in [X] \text{ is generated by letters internal to } m,$$
$$\text{and is such that, for each letter } x \text{ extremal to } mux^{-1} \notin \langle M \rangle\}.$$

There seems to be no immediate characterization from the above for when J has a finite Gröbner basis. A sufficient condition is provided in [5], and then the question is finessed: it is shown that, if K is infinite, then, for any I and $\prec$, J will have a finite Gröbner basis after a generic change of variables.

This is of limited computational use if high degree polynomials are being handled, since the supports can grow explosively after generic changes. So, it is still of some interest to detect whether $\pi^{-1}(I)$ has a finite Gröbner basis when I is still expressed in the given coordinates.

If I is generated by a set M of monomials (this is called a *monomial ideal* of $K[X]$), then $In(I) = \langle M \rangle$, irrespective of the term order $\prec$. It follows from Proposition 3 that:

Proposition 5. *Let $M \subseteq [X]$ and let I be the monomial ideal it generates. Then J has a finite Gröbner basis with respect to the lexicographic extension of a term order of $[X]$ if and only if, for the same ordering of X, $\mathscr{I}(M)$ is finitely generated.*

This gives rise to Problem 3.

A similar looking question is, in the notation above, what conditions must M satisfy, so that J has a finite Gröbner basis with respect to the lexicographic extension of any term order of $[X]$? Proposition 5 translates it to a problem of monomials and words, and the answer is in Section 5, Theorem 16.

As a final note, we point out that within this context another way of specifying an ideal of $[X]$ is relevant to Problems 2 and 3. Namely, suppose a term order is given on $[X]$; given a finite set M of polynomials, consider the initial ideal I of the polynomial ideal generated by M. That is the actual motivation for those problems, after all! The usual process of going from M to I is Buchberger's algorithm and its variants. These are all of high complexity, so the question remains whether Problem 2 can be solved efficiently from this data.

3. Using automata

It is not clear from the outset that either of the problems mentioned in the introduction is decidable. This can be shown to be the case by means of the traditional machinery of automata theory (we follow the notation and terminology of [12]). We do it here, mostly for completeness and to underline some of the complexity issues. This section can be skipped, with no loss in understanding of the remaining text.

Suppose J is an ideal of the free monoid X^*; then its unique minimal generating set is $T = J \backslash (XJ \cup JX)$. Hence, if J is a regular language, so is T. The problem of deciding whether T is finite, given a regular expression for J, can be whimsically, although not very accurately, related to two well-known Unix utility programs: given a pattern for a `grep` search, decide whether the same search can be made by `fgrep`.

Problems 1 and 2 refer to ideals that are regular languages. Consider Problem 1. It is a well-known (although nonconstructive) consequence of Higman's Theorem [11] that, for every subset A of $[X]$, $\pi^{-1}(A)$ is regular. For $\pi^{-1}\langle M \rangle$, one can construct a deterministic automaton directly: have n parallel counters, one for each letter and counting up to its maximum degree in M. Each state of the automaton corresponds to an n-tuple of values for the counters, and processing a word x leads to a state whose counters correspond to the exponent vector of $\pi(x)$. The final states are those that show that $\pi(x) \in \langle M \rangle$, and they can be colluded into a single state that is never left after being reached.

For Problem 2, we can write a simple regular expression for $\pi^{-1}\langle M \rangle$. If $w = x_1^{i_1} x_2^{i_2} \cdots x_{n-1}^{i_{n-1}} x_n^{i_n} \in [X]$, then $\mathscr{I}(w) = X^* x_1^{i_1} x_2^{i_2} x_2^* \cdots x_{n-1}^{i_{n-1}} x_{n-1}^* x_n^{i_n} X^*$; and $\mathscr{I}(M) = \bigcup_{w \in M} \mathscr{I}(w)$, so $\mathscr{I}(M)$ is a regular language. A deterministic automaton recognizing $\mathscr{I}(M)$ can also be constructed using parallel bounded counters, although the description would be more complicated than the previous one.

In both cases, there is only one final state, from which no transition leaves. This makes it easy to construct a deterministic automaton for the minimal generating set of each ideal, with direct products of three very similar automata. Then finiteness can be easily checked by a graph search. This approach shows now that Problem 2 is decidable.

From a complexity viewpoint, this does not work. Even though we have scrupulously avoided using nondeterministic automata, there remains a source of exponential complexity: in either case, the automaton described for each ideal has a number of states that is roughly the product N of the maximum degrees of letters in M. This is too large; since a monomial can be represented as a vector of exponents, a reasonable encoding for M would have only $O(n \log N)$ bits, where $n = |X|$. So, the automaton for the minimal generating set has exponentially many states, and the graph search is linear in the number of states.

The solutions we present in the following sections could perhaps be retro-fitted into an automata-theoretical framework. Actually, thinking of automata helped in the discovery of those results: the Pumping Lemma (see [12, Section 2.4]) was a starting point.

There is a rich literature on ideals of the free monoid, from the viewpoint of language theory, with a twist. Instead of concentrating on the ideal, the focus is on its complement. The complement of an ideal is said to be a *factorial language*, and the minimal generators of the ideal appear as *forbidden subwords* in this context. There are many algorithms for problems involving factorial languages (see [3,4]), but they usually take a deterministic automaton like the large ones we described as input, so they are of no use here.

4. When $\mathscr{I}(M)$ is finitely generated

We assume a fixed ordering $\prec$ on the alphabet X. The *support* of a monomial w, denoted $\underline{w}$, is the set of letters with nonzero exponent in w. So, $\min(\underline{w})$ and $\max(\underline{w})$ are the *extremal* letters of w, while the letters x such that $\min(\underline{w}) \prec x \prec \max(\underline{w})$ are *internal* to w. We will use the notation $u|v$ meaning *u divides v*, both in $[X]$ and X^*. So, for monomials $u = x_1^{i_1} \ldots x_n^{i_n}, v = x_1^{j_1} \ldots x_n^{j_n}$, $u \mid v$ means that $i_1 \leqslant j_1, \ldots, i_n \leqslant j_n$; for words u, v, $u \mid v$ means that there exist words w, z such that $v = wuz$.

Example 1. Take $X = \{a, b, c, \dots\}$ with the usual ordering. Then, for $w = b^2df$, $\min(\underline{w}) = b$, $\max(\underline{w}) = f$, and the internal letters are c, d, and e.

Lemma 6. *If u and v are sorted words such that $u \mid v$, then for any x in X, either $u \mid S(vx)$ or $S(ux) \mid S(vx)$.*

Proof. The first case occurs if $x \leqslant \min(\underline{u})$ or $x \geqslant \max(\underline{u})$, and the second case occurs if $\min(\underline{u}) \leqslant x \leqslant \max(\underline{u})$. $\square$

Lemma 7. *Let T be a set of sorted words. If, for every t in T and x in X, $S(tx)$ has a factor in T, then there exists an ideal I of $[X]$ such that $T \subseteq \sigma(I)$ and $\langle T \rangle = \mathscr{I}(I)$.*

Proof. Let $M = \pi(T)$ and $I = \langle M \rangle$; clearly $T \subseteq \sigma(I)$, and we will show that $\langle T \rangle = \mathscr{I}(I)$.

Since $\langle T \rangle \subseteq \mathscr{I}(I)$ is clear, it is enough to show that $\sigma(I) \subseteq \langle T \rangle$. Since any monomial in I can be written as su, with $s \in M$, $u \in [X]$, we will show that $\sigma(su)$ has a factor in T (so, it is in $\langle T \rangle$) by induction in the total degree of u.

There is nothing to prove if the degree is zero. So, we can write $u = vx$, with $v \in [X]$, $x \in X$. By the induction hypothesis, $t \mid \sigma(sv)$ for some $t \in T$. By hypothesis, $S(tx)$ has a factor $y \in T$. Noticing that $S(\sigma(sv)x) = \sigma(svx) = \sigma(su)$, Lemma 6 implies that either $t \mid \sigma(su)$, or $S(tx) | \sigma(su)$, in which case, $y \mid \sigma(su)$. In either case, the result follows. $\square$

From this, it easily follows:

Corollary 8. *Let M be a set of monomials. A sufficient condition for a set T of words to be such that $\langle T \rangle = \mathscr{I}(M)$ is that $\sigma(M) \subseteq T \subseteq \sigma\langle M \rangle$ and for every t in T and x in X, $S(tx)$ has a factor in T.*

We restate Theorem 1 with some additional precision, in order to prove it. First, we recall and introduce some notation.

If w is a monomial and $x \in X$, $w \backslash x$ denotes the monomial obtained from w by erasing the occurrences of x. We denote by $\imath(w)$ the set of internal letters of w, and by $\partial_x w$ the degree of x in w. Given a set M of monomials, let $r_x(M)$ denote the maximum degree x occurs with as an extremal letter in M. To avoid misunderstandings, $[\imath(w)]$ is simply the submonoid of $[X]$ generated by $\imath(w)$.

Example 2. Continuing the earlier example, $w \backslash b = df$ and $w \backslash f = b^2d$. If $M = \{c^3, a^2c^5f^2, cf^3g, a^2b^2c^2\}$, then $r_c(M) = 3$ and $r_f(M) = 2$.

Theorem 9. *Let M be an antichain in $[X]$. The following are equivalent*:

(i) *$\mathscr{I}(M)$ is finitely generated.*

(ii) *For every* w *in* M *and* x *in* $\imath(w)$, *there exists* s *in* M *such that* x *is extremal in* s, *and* $s\backslash x$ *divides* w.

(iii) $\mathscr{I}(M)$ *is generated by* $\sigma\big(\bigcup_{w\in M}\{u\in w[\imath(w)] \mid \forall x\in\imath(w),\ \partial_x u < r_x(M)\}\big)$.

Proof. Let T be the minimal generating set of $\mathscr{I}(M)$, and suppose it is finite. We shall prove condition (ii). Note that $\sigma(M)\subseteq T$. Indeed, if $w\in M$, $\sigma(w)$ has a factor in T, and this has the form $\sigma(su)$, for some $s\in M$ and $u\in[X]$. So, $\sigma(su)|\sigma(w)$, and this clearly implies $su \mid w$. So, $s|w$ and, since M is an antichain and $s\in M$, it follows that $s=w$, $u=1$, hence $\sigma(w)\in T$.

Let $w\in M$ and let x be an internal letter to w. We can uniquely write $\sigma(w)=ux^rv$, with u, v sorted, $\max(\underline{u})\prec x\prec\min(\underline{v})$. Hence, all words ux^nv, with $n\geqslant r$, are in $\mathscr{I}(M)$, so each has a factor in T; it follows that some $t\in T$ is a factor of infinitely many such words. If x is not in the support of t, it must happen that t is a factor of u or of v, hence a proper factor of $\sigma(w)$, but $\sigma(w)\in T$, so this cannot occur. Therefore, x is in the support of t, and necessarily is extremal. Without loss of generality, let us assume that $x=\min(\underline{t})$; so $t=x^kz$ with $x\prec\min(\underline{z})$, and note that z is a factor of $\sigma(w)$, so $\pi(z)|w$. Now, $t=\sigma(sy)$ for some $s\in M$ and $y\in[X]$. If $x\notin\underline{s}$, we would have $s \mid \pi(z)$, hence $s \mid w$, a contradiction. Hence $x=\min(\underline{s})$, so $s\backslash x$ is a factor of w.

Now, suppose that condition (ii) holds and let us prove (iii). Call T the generating set in that statement. Clearly $\sigma(M)\subseteq T\subseteq\sigma\langle M\rangle$. Now, let $t\in T$ and $x\in X$, and let us find a factor of $S(tx)$ in T as required by Corollary 8. Write $t=\sigma(wz)$, with $w\in M$ and $z\in[\imath(w)]$.

If $x\notin\imath(w)=\imath(\pi(t))$, it follows immediately that $t \mid S(tx)$. There remains the case where $x\in\imath(w)$ and $S(tx)\notin T$ (since the case $S(tx)\in T$ is trivial).

Now, $\sigma(wz)\in T$, but $\sigma(wzx)\notin T$, hence $\partial_x wz=r_x(M)-1$. We can write uniquely $wz=ux^{r_x(M)-1}v$, with $\max(\underline{u})\prec x\prec\min(\underline{v})$. By hypothesis, there exists $s\in M$, with x extremal in s (without loss, $x=\max(\underline{s})$) such that $s\backslash x$ divides w. Since $\partial_x s\leqslant r_x(M)$, $s|wzx$, and by maximality of x in $\underline{s}$, $s \mid ux^{r_x(M)}$. Let p result from raising the degree of each internal letter of s to its exponent in u. Then, $p\in s[\imath(s)]$ and its internal letters have small degree, so $\sigma(p)\in T$, and it is the factor of $S(tx)$ we sought after.

Clearly (iii) implies (i), and the theorem is proved. □

Example 3. Consider the set $M=\{ab^2c, a^3b\}$. The ordering $a\prec b\prec c$ does not satisfy the conditions above, since b is internal to ab^2c, and extremal only in a^3b, but $a^3b\backslash b=a^3$ does not divide ab^2c; indeed, $\sigma\langle M\rangle$ comprises all words $a^ib^{j+2}c^k$ and $a^{i+3}b^j$ with $i,j,k\geqslant 0$, and the set $\{ab^{j+2}c \mid j\geqslant 0\}$ cannot be generated as multiples of finitely many of those. Similarly, $a\prec c\prec b$ fails, since c is internal to a^3b, and extremal in none. However, $b\prec a\prec c$ is good: a is internal to b^2ac only, and $ba^3\backslash a=b$ divides b^2ac. In this case, $\mathscr{I}(M)$ is generated by $\{b^2ac, b^2a^2c, ba^3\}$.

Condition (iii) above is a fairly precise description of the minimal generating set of $\mathscr{I}(M)$. One gets a quick and dirty estimate for its size by forgetting most parameters:

Corollary 10. *Let M be a finite set of monomials in $[X]$. Then, if $\mathscr{I}(M)$ is finitely generated, it can be generated by a set of at most*

$$|M'| \prod_{x \in \imath(M)} r_x(M) + |M| - |M'|$$

elements, where $M' = \{w \in M | \imath(w) \neq \emptyset\}$ and $\imath(M) = \bigcup_{w \in M} \imath(w)$.

Even though it is a rough estimate, the result above is best possible. To see this, suppose $X = \{x_1, x_2, \dots, x_n\}$, ordered according to the indices. Choose positive integers $m, r_2, r_3, \dots, r_{n-1}$, and let $M = \{x_1^{i+1} x_n^{m-i} \mid 0 \leqslant i < m\} \cup \{x_i^{r_i} | i = 2, \dots, n-1\}$. Then, the minimal generating set for $\mathscr{I}(M)$ is precisely that described in Theorem 9(iii) and has size $m \prod r_i + n - 2$.

If we are given M as a collection of integer vectors, divisibility is just componentwise comparison, so it can be tested rapidly. A naive check of the condition on Theorem 1 would need at most $|M|^2 |X|$ such comparisons, so Problem 2 can be solved by a polynomial-time algorithm.

We end this section with some constructions that will be useful later and some unexpected consequences of the theorem.

Given a collection M of monomials and an integer k, M_k will denote the subset of M consisting of monomials whose support has size at most k.

Proposition 11. *If an antichain M of monomials is such that $\mathscr{I}(M)$ is finitely generated, so is $\mathscr{I}(M_k)$ for each integer k.*

Proof. Let us show that M_k satisfies condition (ii) of Theorem 9. If $w \in M_k$, and x is internal to w, we know, since $\mathscr{I}(M)$ is finitely generated, that for some monomial $u \in M$, x is extremal in u and $u \backslash x$ is a factor of w. Since x is internal to w and extremal in u, the support of $u \backslash x$ is a proper subset of the support of w, so $|\underline{u}| \leqslant k$; that is, $u \in M_k$. $\square$

Proposition 12. *Let $w \leftrightarrow \hat{w}$ be a bijection between sets M and $\hat{M}$ of monomials, such that:*

(i) *For every w in M, w and $\hat{w}$ have the same extremal letters.*
(ii) *For every u, v in M and x in X, if $\partial_x u \leqslant \partial_x v$, then $\partial_x \hat{u} \leqslant \partial_x \hat{v}$.*

If $\hat{M}$ is an antichain, and $\mathscr{I}(M)$ is finitely generated, then so is $\mathscr{I}\hat{M}$.

Proof. First notice that, from condition (ii), $u \mid v$ implies $\hat{u} \mid \hat{v}$, so M is an antichain. Thus, it must satisfy Theorem 9 (ii). Let $\hat{w} \in \hat{M}$, and $x \in X$ be internal to $\hat{w}$. From condition (i), x is internal to w, so there exists $u \in M$ such that x is extremal in u and $u \backslash x | w$. Again from (i), x is extremal in $\hat{u}$, and from condition (ii), $\hat{u} \backslash x | \hat{w}$. $\square$

5. Cool orderings

Given an antichain M of monomials in $[X]$, we say that an ordering of X is *cool* for M if, for every w in M and letter x internal to w, there exists s in M such that x is extremal in s and $s\backslash x$ divides w.

As we will see in the next section, no good algorithm is forthcoming to decide whether a cool ordering exists. Before giving substance to this, we try to get a better understanding of such orderings. We begin with an immediate consequence of Propositions 11 and 12.

Proposition 13. *Let M be an antichain of monomials. Then, any cool ordering for M is also a cool ordering for*:

1. M_k, *for any integer* k.
2. *Any* $\hat{M}$, *obtained from* M *by changing each* w *to* $\hat{w}$, *so that*:

(a) w *and* $\hat{w}$ *have the same support, and*
(b) *For every* u, v *in* M *and* x *in* X, *if* $\partial_x u \leqslant \partial_x v$, *then* $\partial_x \hat{u} \leqslant \partial_x \hat{v}$.

This gives some necessary conditions for existence of cool orderings. We also get a kind of equivalence between sets of monomials:

Proposition 14. *Let* $w \leftrightarrow \hat{w}$ *be a bijection between set* M *and* $\hat{M}$ *of monomials, such that*:

(i) *For every* w *in* M, $\underline{w} = \underline{\hat{w}}$, *and*
(ii) *For every* u, v *in* M *and* x *in* X, $\partial_x u < \partial_x v$ *if and only if* $\partial_x \hat{u} < \partial_x \hat{v}$.

Then, an ordering of X *is cool for* M *if and only if it is so for* $\hat{M}$.

Proof. It is easily checked that $u \mid v$ if and only if $\hat{u} \mid \hat{v}$. So, the bijection maps minimal monomials to minimal monomials, antichains to antichains, and so on. It is just a matter of applying part 2 of Proposition 13 in both directions. $\square$

From now to the end of the article, an ordering of the letters will not be given at the outset, and the following concept will be useful for the search of cool orderings. A monomial w is said to *help* a monomial m *with* the letter x if $x \in \underline{w}$, $w\backslash x \mid m$ and $\underline{w\backslash x} \subsetneq \underline{m\backslash x}$.

If $\prec$ is a cool ordering for a set M and, for some $Y \subset X$, every monomial in M has support included in Y or disjoint from Y, then $\prec$ is a cool ordering for those monomials with support included in Y. This can be extended to the following easily verified fact:

Proposition 15. *A cool ordering for* M *is also cool for any* $N \subseteq M$ *such that all members on* M *that help some member of* N (*with some letter*) *are in* N.

Next section will consider the problem of finding a cool ordering, given M. We close the section considering a question that is a sort of opposite of that: how must M look like if *every* ordering of X is cool? The answer is surprisingly simple.

Theorem 16. *Let M be an antichain of monomials over X. Then, every ordering of X is cool for M if and only if, for every m in M and x in X such that $|\underline{m\backslash x}| \geqslant 2$, there exists a u in M_2 such that $u\backslash x \mid m$.*

Proof. Suppose that every ordering of X is cool for M. Let m and x be given as in the statement. Then, there exists an ordering $\prec$ on X such that x is internal to m. Since $\prec$ is cool, there is a u in M that helps m with x. Choose u with minimal support, and let us show that $\underline{u}$ has size at most 2. If $|\underline{u}| > 2$, there is another ordering of X that makes x internal to u. Again by Theorem 9, there exists a v in M that helps u with x; clearly, v also helps m with x. Since $x \in \underline{u} \cap \underline{v}$, it follows that $\underline{v} \subsetneq \underline{u}$, so we have contradicted the minimality of $\underline{u}$.

Conversely, suppose the divisibility condition holds, and consider an arbitrary ordering of X. Pick an $m \in M$ and let $x \in \imath(m)$. Choose u in M_2 such that $u\backslash x \mid m$; clearly x is extremal in u. It follows that the ordering is cool. $\square$

6. Finding cool orders is hard

Monoids generated by square-free monomials appear frequently in algebraic combinatorics (related to Stanley–Reisner rings of simplicial complexes), and have been studied in the current context by Peeva and Sturmfels, together with Eisenbud [5] and Reiner [15]. Propositions 18 and 20 tell the same as [5, Proposition 3.2] and [15, Lemma 3.1], although the different jargon may obscure this. After that we move to another direction.

Proposition 17. *Suppose that M is an antichain and the degree of the letter x in $w \in M$ is the largest degree it has in all monomials in M. Then, in any cool ordering for M, x cannot be internal to w.*

Proof. If there is a cool ordering for M where x is internal to w, there exists a $t \in M$ such that $t\backslash x | w$. But since $\partial_x w \geqslant \partial_x t$, it follows that $t \mid w$, a contradiction, as M is an antichain. $\square$

The following is an immediate corollary:

Proposition 18. *If M consists only of square-free monomials and affords a cool ordering, then its monomials have total degree at most* 2.

Degree 1 monomials are trivially handled here, so the square-free sets M of interest consist only of quadratic monomials. Polynomial ideals whose initial ideals are generated by quadratic monomials (mostly square-free) were extensively studied in [15].

We leave now the square-free condition, and consider the case when M consists exclusively of quadratic monomials, that is, we allow monomials of form x^2. This seemingly trivial extension has deep consequences:

Proposition 19. *The problem of deciding, given a set of quadratic monomials M, whether there exists a cool ordering for M is*:

(a) *Solvable in polynomial time, if M is square-free.*
(b) *NP-complete, in general.*

Proof. Part (a) follows from Proposition 20 and part (b) from Proposition 21. □

With quadratic monomials, irrespective of the order of the letters, each letter is extremal in each monomial it occurs, so, an ordering $\prec$ on X is cool for M if and only if whenever $x \prec y \prec z$ and xz is in M, then at least one of y^2, xy, yz is in M.

At this point, it becomes convenient to encode the data and the problem by means of graphs, and it turns out to be convenient to use the complement of what comes naturally. The graph $G(M)$ will have the letters as vertices, xy is an edge if xy is not in M. Let T_M denote the set of letters whose square is *not* in M.

An orientation of a graph is said to be *transitive* at a vertex y if, whenever oriented edges $x \to y$ and $y \to z$ exist, then the edge $x \to z$ must also exist. A graph is a *comparability graph* if it admits an orientation that is transitive at all its vertices; such an orientation is always acyclic. Comparability graphs have been widely studied, and can be recognized efficiently [6] (or [14]), [8,16].

Proposition 20. *A set M of quadratic monomials admits a cool order if and only if $G(M)$ admits an acyclic orientation that is transitive at all vertices of T_M. In particular, if M is square-free, it admits a cool order if and only if $G(M)$ is a comparability graph.*

Proof. Suppose M has a cool ordering. Direct all edges of $G(M)$ from the smallest to the largest vertex. This orientation is trivially acyclic. If $y \in T_M$, and edges $x \to y$ and $y \to z$ exist, then the monomials y^2, xy and yz are not in M. By coolness, $xz \notin M$, so the edge xz is in $G(M)$, and is correctly oriented.

Conversely, suppose that $G(M)$ admits an acyclic orientation that is transitive at all vertices of T_M. With a "topological sort" order its vertices so that all directed edges point from the smaller to the bigger end. One readily verifies that this ordering is cool for M.

When M is square-free, T_M comprises all vertices, so an acyclic orientation that is transitive at all vertices of T_M says that $G(M)$ is a comparability graph. □

We refer the reader to the already classic text [7] as a general reference for NP-completeness, good algorithms and satisfiability. Since good algorithms for recognition of comparability graphs are known, one would expect that testing the condition of Proposition 20 would also be feasible.

Proposition 21. *The problem*:

> given a graph G and a set $T \subseteq VG$, is there an acyclic orientation of G that is transitive at all vertices in T?

is NP-complete.

Proof. Let us shorten "orientation transitive at T" to T-*orientation*. The proof will be by a reduction from NOT-ALL-EQUAL-3SAT [17]. The basic gadget is the graph in Fig. 1, where the vertices in T are black (and labeled a, $\bar{a}$, c).

Fact 1. *The orientation $a \to \bar{a}$ of the edge $a\bar{a}$ can be extended to a unique T-orientation of this graph. In this orientation, a is a source, $\bar{a}$ is a sink, and the bottom edge is directed from r* to *l.*

To see this, notice that since the edge $s\bar{a}$ does not exist, sa must be oriented as $a \to s$, because of transitivity at a. By a similar argument we check that all edges with an end in T can have only one orientation. Finally, since the orientations $r \to c$ and $c \to l$ are forced, $r \to l$ is forced by transitivity at c.

Now we construct the main gadget by gluing three copies of the top hat, identifying cyclically each t with the next s and each r with the next l. The result is in Fig. 2, where only important vertices are labeled.

Fact 2. *Consider an orientation of the edges $a_1\bar{a}_1$, $a_2\bar{a}_2$ and $a_3\bar{a}_3$. It extends to an acyclic T-orientation of the gadget if and only if they are not all directed the same way along the external cycle.*

Indeed, by looking at the top hats we see that any orientation of these edges extends uniquely to a T-orientation of the gadget. If they are all oriented the same way, the inner triangle becomes a directed cycle. Conversely, if they are not all the same way (by symmetry, there is only one case to check), the orientation of the gadget is acyclic.

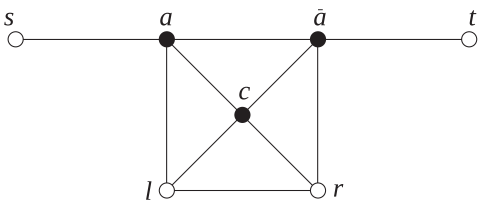

Fig. 1. The top hat.

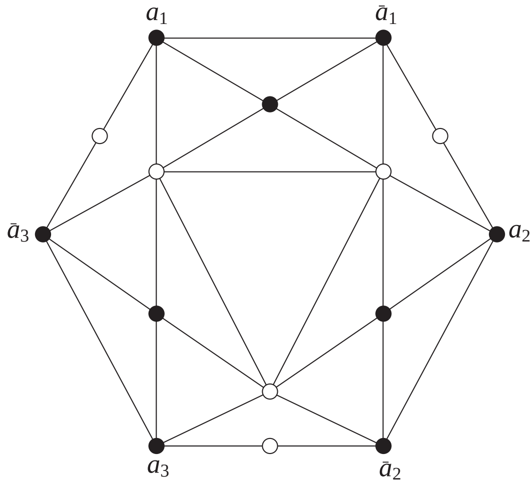

Fig. 2. The gadget.

Now we proceed to the reduction. A typical instance of NOT-ALL-EQUAL-3SAT consists of a set X of variables and a set C of clauses over X, where each clause has three literals, each of form x or $\bar{x}$, for some $x \in X$. The question is whether there exists a truth assignment to X, so that for each clause one literal gets value *true* and one gets value *false*.

For each clause, take a copy of the gadget and replace the labels a_1, a_2 and a_3 by the literals, and $\bar{a}_1$, $\bar{a}_2$ and $\bar{a}_3$ by the complements of the literals in the clause. Add to that a vertex v_x for each variable x, and join it to all vertices labeled x. Call the resulting graph G, and let T be formed by all v_x together with the union of all black vertices from the gadgets.

We will show a 1-1 correspondence between truth assignments for V that solve C and acyclic T-orientations of G. Start with a truth assignment. For each edge labeled $x\bar{x}$, orient it from x if x is assigned *true* and towards x otherwise. Consider a clause and its respective gadget. The three literals in the clause are not all *true* and not all *false*, so the three special edges are not all directed the same way. It follows from Fact 2 that one can orient (uniquely) all gadgets extending these orientations. In this orientation, all vertices labeled with the same literal are sources in their gadgets if that literal is *true*, and sinks otherwise. This T-orientation can now be extended to the whole G, directing all edges incident to v_x towards it if x is *true* and the opposite otherwise.

Conversely, suppose a T-orientation of G is given. Since all neighbors of v_x are pairwise nonadjacent, v_x is either a source or a sink. Assign x *true* if v_x is a sink, *false* otherwise. The fact that each gadget is acyclically T-oriented shows that in the corresponding clause the not-all-equal condition is satisfied. $\square$

Since simple powers have originated the problem in Proposition 19, we tried to look at another extension of its first part, namely, allow only monomials with support size exactly 2. This was short lived, though:

Proposition 22. *The problem*:

> given a collection M of monomials, each with support of size 2, does there exist a cool ordering for M?

is NP-complete.

Proof. We reduce the quadratic case to this. Suppose that M is a collection of quadratic monomials, and let $M' = \{xy \mid xy \in M\} \cup \{x^2y \mid x^2 \in M \text{ and } xy \notin M\}$. It is easy to check that M and M' have precisely the same cool orderings. $\square$

There is a lot of leeway in the reduction in the proof of Proposition 21. For instance, the v_i could be eliminated, and similarly labeled vertices could be merged. One could add irrelevant vertices of both types and show that existence of acyclic T-orientations is NP-complete even if $|T| = \frac{1}{2}|VG|$ (any constant between 0 and 1 would do). On the extremes, the problem can be solved:

When $T = VG$, that is recognition of comparability graphs. When T induces a bipartite graph, any acyclic orientation in which one side of T consists only of sources and the other (if it exists) only of sinks is a T-orientation. This takes care of $|T| \leqslant 2$; actually, for any fixed k, if $|T| \leqslant k$, one can restrict the search for a T-orientation to a polynomial number of acyclic orientations that can be systematically enumerated.

7. Lifting the ideal

Here we present the solution to Problem 1.

Theorem 23. *Given an antichain of monomials $M \subseteq [X]$, the following are equivalent*:

(i) $\pi^{-1}\langle M \rangle$ *is a finitely generated ideal of* X^*.

(ii) *For every m in M and any letters $x \neq z \neq y$ such that $xy|m$, there exists a monomial w in M such that $w\backslash z$ divides either mx^{-1} or my^{-1}.* (*Note that $x = y$ is included.*)

(iii) *For every m in M and any letter z such that no power of it is in M, if $m\backslash z$ has degree $\geqslant 2$, there exists a monomial $z^r t$ in M_2, such that $t \in \underline{m}$.*

(iv) $\pi^{-1}\langle M \rangle$ *is generated by the inverse images of the monomials $m \in \langle M \rangle$ such that, for every letter x, $\partial_x m \leqslant \max_{u \in M_2} \partial_x u$.*

Proof. (i) implies (ii): Given m, x, y, and z, choose $u = xz^r vy \in \pi^{-1}(m)$, where $r \geqslant 0$. Now, for every $s \geqslant r$, $xz^s vy \in \pi^{-1}\langle M \rangle$, and since $\pi^{-1}\langle M \rangle$ is finitely generated, some minimal generator g divides infinitely many of these. This is only possible if g divides some xz^s or some $z^s vy$. So, $\pi(g)\backslash z$ divides either my^{-1} or mx^{-1}. The result follows by taking any w in M that divides $\pi(g)$.

(ii) implies (iii): Given m and z, choose letters x and y such that $xy \mid m\backslash z$. Let w be given by condition (ii), with minimal support. Since M is an antichain, $z \in \underline{w}$. Suppose, by contradiction, that $w\backslash z$ has degree $\geqslant 2$. We apply condition (ii) to w, obtaining a w'; that new monomial could also play the role of w with respect to m, so, by minimality of w, it cannot exist. Since no power of z is in M, $w = z^r t$ for some letter $t \neq z$. As $w\backslash z$ divides either mx^{-1} or my^{-1}, it follows that $t \in \underline{m}$.

(iii) implies (iv): Let W be the set claimed to generate $\pi^{-1}\langle M\rangle$. If this is false, then $\langle W\rangle \subsetneq \pi^{-1}\langle M\rangle$, since $W \subseteq \pi^{-1}\langle M\rangle$. So, there must exist a $w \in \pi^{-1}\langle M\rangle$, of minimum length, with no factor in W. So, for some letter z, $\partial_z \pi(w) > r = \max_{u\in M_2} \partial_z u$.

Suppose that $z^r \in M$. Clearly w has a proper factor u such that $z^r \mid \pi(u)$, so $u \in \pi^{-1}\langle M\rangle$. By minimality of w, u has a factor in W; then, so does w, a contradiction. So, $z^r \notin M$, and by the choice of r and as M is an antichain, no power of z lies in M. Now, let $m \in M$ be such that $m \mid \pi(w)$. By (iii), there exists a $z^s t \in M$ such that $t \in \underline{m}$. Since $s \leqslant r$, w has a proper factor u such that $z^s t \mid \pi(u)$. We get a contradiction again, that finishes the proof.

(iv) implies (i): We deserve the rest. □

We briefly relate this result to the preceding ones. It is easy to check from the definitions that if $\pi^{-1}\langle M\rangle$ is finitely generated, then every ordering of X is cool for M. This can also be seen from the fact that if M satisfies the condition in Theorem 23(iii), then it also satisfies the condition of Theorem 16. The converse is not true; the simplest example is $M = \{a^2, bc\}$—here, every ordering is cool, but $\pi^{-1}\langle M\rangle$ is not finitely generated. Actually, if one starts with any M for which every ordering is cool and substitutes each letter for its square, this property is preserved. But now, $\pi^{-1}\langle M\rangle$ is not finitely generated.

The similarity between Theorems 23 and 9 may suggest that perhaps a restricted form of 9(ii) involving M_2 would hold. That is not likely, as suggested by $M = \{x_1x_2^2, x_1x_2x_3^2, x_1x_2x_3x_4^2, \dots\}$; the natural ordering of $x_1, x_2, \dots, x_n$ is cool for M, for any n, even though M_2 is quite skimpy.

8. Commutative ideals given by inequalities

Another way of giving an ideal of $[X]$ is as the pre-image of an ideal under a morphism from $[X]$ to another commutative monoid. This is useful only if there is a nice way of describing the morphisms and the ideals of the target. We will consider morphisms between free commutative monoids and lift ideals given by generators.

In this setting, it will be convenient to switch to an additive notation for $[X]$. We number the letters of X as $x_1, x_2, \dots, x_n$, and identify $[X]$ with $\mathbb{N}^n$ by the isomorphism given by $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n} \mapsto \mathbf{x} = (i_1, i_2, \dots, i_n)$. In this notation, a set $I \subseteq \mathbb{N}^n$ is an ideal if

$\mathbf{x} \geqslant \mathbf{y} \in I$ implies $\mathbf{x} \in I$ (as usual, $\mathbf{x} \geqslant \mathbf{y}$ means $\mathbf{x}_i \geqslant \mathbf{y}_i$ for every i). Other terms require translation: monomials become vectors, letters become indices or coordinates of vectors, and so on.

Consider a morphism $\varphi : [X] \to [Y]$, where an isomorphism $[Y] \to \mathbb{N}^m$ is already fixed. If $\varphi(x_j) = \prod_i y_i^{a_{ij}}$, then φ is the linear map $\mathbb{N}^n \to \mathbb{N}^m$ given by the matrix $A = (a_{ij})$, where each a_{ij} is a nonnegative integer. If J is an ideal of $\mathbb{N}^m$, then $I = \{\mathbf{x} \in \mathbb{N}^n | A\mathbf{x} \in J\}$ is an ideal of $[X]$; moreover, if J is generated by the finite set W, then that same ideal I can be described as:

$$I(A, W) = \{\mathbf{x} \in \mathbb{N}^n \mid A\mathbf{x} \geqslant w \text{ for some } w \in W\}.$$

When w is a vector in $\mathbb{N}^m$, we write $I(A, w)$ for $I(A, \{w\})$. Also, we stress that we only consider $I(A, w)$ when A is nonnegative.

Given a generating set M of an ideal of $[X]$, one can write down a description $\langle M \rangle = I(I_n, M)$, simply using $Y = X$ and the identity morphism as φ. From the complexity viewpoint, we notice that the new description has size bounded by a polynomial on the size of M; one interesting feature of the new type of description is that it can be much more compact. Just to give a trivial example, consider, for each k in $\mathbb{N}$, the ideal $\{\mathbf{x} \in \mathbb{N}^2 | x_1 + x_2 \geqslant k\}$. The size of this description is $O(\log k)$, while clearly it has $k + 1$ minimal generators.

Clearly, $I(A, w) = \bigcup_{w \in W} I(A, w)$, and this suggests the following definition: we say that an ideal of $[X]$ is *convex* if it is of form $I(A, w)$ for some integer matrix A and vector w. The name is motivated by the following fact, that follows from standard results in the theory of polyhedra (see [18] for terminology and facts about polyhedra that we use).

Proposition 24. *Let $I = \langle M \rangle$ be an ideal of $[X] = \mathbb{N}^n$, with M finite. The following are equivalent*:

(i) *I is convex.*
(ii) *I is the intersection of $\mathbb{N}^n$ with a convex set in $\mathbb{R}^n$.*
(iii) $I = \mathbb{N}^n \cap (\mathrm{conv}(M) + \mathbb{R}^n_+)$ ($\mathrm{conv}(M)$ *is the convex hull of* M).

So, $I(A, w)$ is a union of convex ideals. It turns out that any union of convex ideals can be expressed as an $I(A, w)$. As we see below, this can be done without wasting much space, so we can switch descriptions without penalty in the coarse complexity of the problems we will talk about.

Lemma 25. *Let $I_1 = I(A^{(1)}, w^{(1)})$, $I_2 = I(A^{(2)}, w^{(2)})$, …, $I_r = I(A^{(r)}, w^{(r)})$ be ideals of $[X]$. Then there exist a matrix A and a set W of vectors, with total size polynomial in the total size of the descriptions $I(A^{(i)}, w^{(i)})$, such that $\bigcup_i I_i = I(A, w)$.*

Proof. Let A result from piling up the matrices $A^{(i)}$ on top of each other. For each i, let w^i result from extending $w^{(i)}$ with null entries corresponding to the inequalities of the other systems; so, $I(A, w^i) = I_i$. Finally, let $W = \{w^1, w^2, \ldots, w^r\}$.

For those of a more categorical persuasion, the proof is simply the substitution of a family of morphisms by its direct product. □

Now we consider what happens to the three guiding problems of the introduction when I is given in the form $I(A, w)$. Problem 3 is sort of hopeless, since a description $\langle M \rangle$ can be converted into a description $I(A, w)$ of size polynomial in the size of M, and Problem 3 is NP-complete when M is the given data. It follows that this problem with I given as $I(A, w)$ is NP-hard; to make things worse, we cannot even assert that it is in NP. At this point, we refer the reader again to [7] for a refresher on NP-completeness concepts, and, in particular, to the satisfiability problem, that will play an important role in the remainder of this section.

For the other two problems, our results are similarly bad and more definite. They will be shown to be coNP-complete. Indeed, we will add a new problem to the pack, that is completely trivial if the ideal is given by generators:

Problem 4. Given an ideal I of $[X]$, is it generated by monomials with support of size at most 2? That is, is there a set M such that $M = M_2$ and $\langle M \rangle = I$? □

We register two basic algorithms pertaining to these problems.

Lemma 26. *Given an ideal $I = I(A, w)$ and a vector $\mathbf{x}$, it can be decided in polynomial time whether $\mathbf{x} \in I$ and whether $\mathbf{x}$ is a minimal generator of I.*

Proof. Computing $A\mathbf{x}$ and comparing the result with each member of W, we quickly decide membership in I. To decide whether an $\mathbf{x} \in I$ is minimal, it is enough to verify that each vector obtained from $\mathbf{x}$ by subtracting 1 from a positive coordinate is not in I. □

In what follows, the proofs will be a bit sketchy, with some bare statements; filling in the details is routine handiwork.

Recall that a decision problem is in coNP if, the problem obtained by reversing the answer is in NP; in other words, **no**-instances have short certificates.

Proposition 27. *Problems* 1, 2 *and* 4 *are in coNP, when the ideal is given as* $I(A, w)$.

Proof. For each problem, when the answer to an instance is **no**, we will present a short certificate, verifiable in polynomial time. That will be a minimal generator of the ideal, and some additional information. Notice that any minimal generator has coordinates bounded by the maximum of all coordinates in members of W, so it can be part of a short certificate.

For Problem 4, a certificate is simply a minimal generator with support of size at least 3.

For Problem 1, a certificate is a minimal generator $\mathbf{m}$ and an index z such that item (iii) of Theorem 23 is violated. That amounts to the following:

- There is no vector in I whose support is $\{z\}$ (no power of z is in M). This happens if and only if, for each $w \in W$, there is an index i such that $w_i > 0$ and $a_{iz} = 0$.

- $\sum_{i \neq z} m_i \geqslant 2$ ($m \backslash z$ has degree $\geqslant 2$).
- There is no $\mathbf{x} \in I$ and index $t \neq z$ such that $m_t > 0$, $x_t = 1$ and $x_i = 0$ for every $i \neq t, z$. This is true, for each candidate t, if and only if for every $w \in W$ there exists an i such that $w_i > a_{it}$ and $a_{iz} = 0$.

For Problem 2, we assume, without loss of generality, that the ordering on the letters is that of the indexing. Now, a certificate consists of a minimal generator $\mathbf{m}$ and an index x, interior to $\mathbf{m}$ satisfying the condition: there is no minimal generator $\mathbf{s}$ whose first or last positive entry is in position x, and such that if $\mathbf{s}'$ results from $\mathbf{s}'$ by turning the x-component to 0, then $\mathbf{s}' \leqslant \mathbf{m}$. This condition can be checked as follows. Let $\mathbf{m}_{\leftarrow}$ ($\mathbf{m}_{\rightarrow}$) result from $\mathbf{m}$ by changing to zero all components with index bigger (smaller) than x. Let also A', W' result from eliminating all rows i such that $a_{ix} > 0$. Then, x satisfies the required condition if and only if neither $\mathbf{m}_{\leftarrow}$ nor $\mathbf{m}_{\rightarrow}$ is in $I(A', W')$.

Proposition 28. *Problems* 1, 2 *and* 4 *are coNP-complete, when the ideal is given as* $I(A, w)$.

Proof. We will reduce directly from Sat to the negative of each problem. The reductions will have a lot in common. From each instance of Sat, we will produce a family of convex ideals I_i, like in Lemma 25; instead of presenting them in matrix form, we write them as systems of linear inequalities.

Given an instance S of Sat on variables $x_1, x_2, \ldots, x_n$, (we assume $n \geqslant 3$) our inequalities will involve the variables $x_1, \bar{x}_1, x_2, \bar{x}_2 \ldots, x_n, \bar{x}_n$, in obvious correspondence to the literals. For each clause, the corresponding *clause inequality* is

$$\text{sum of the literals in the clause} \geqslant 1.$$

Let I_0 be defined by the clause inequalities, together with the *boolean inequalities* $x_i + \bar{x}_i \geqslant 1$ for $i = 1, 2, \ldots, n$. The specific use of I_0 is the following: $\mathbf{x}$ *is a solution of* I_0 *in nonnegative integers such that each boolean inequality is satisfied as equality if and only if* $\mathbf{x}$ *is a boolean assignment satisfying* S.

We also define, for each $i = 1, 2, \ldots, n$, the ideal I_i given by the single inequality $x_i + \bar{x}_i \geqslant 2$. Notice that I_i has three minimal generators: two with single support ($x_i = 2$ or $\bar{x}_i = 2$), the other with two-element support ($x_i = \bar{x}_i = 1$).

Reduction to Problem 4: The instance P of Problem 4 consists precisely of the systems $I_0, I_1, \ldots, I_n$.

Suppose that S is satisfiable, and let $\mathbf{x}$ be a boolean assignment satisfying S. Since for each i, exactly one of x_i or $\bar{x}_i$ equals 1, the support of $\mathbf{x}$ has size $n \geqslant 3$, and $\mathbf{x}$ is not in any I_i, $i \geqslant 1$. On the other hand, clearly $\mathbf{x}$ is in I_0. Also, $\mathbf{x}$ is minimal, since zeroing any variable would violate the corresponding boolean inequality. So, P has a negative answer if S is satisfiable.

Conversely, suppose P has a negative answer, that is, the corresponding ideal has a minimal generator $\mathbf{x}$ whose support has size $\geqslant 3$. Clearly it cannot be in any I_i with $i \geqslant 1$, so it is in I_0, and $x_i + \bar{x}_i = 1$ for each i. Hence, S is satisfiable.

Reduction to Problem 2: We introduce two new variables, y and z, besides the ones we already have. The instance P of Problem 2 consists of the systems $I_1, \dots, I_n$, together with I'_0, which is I_0 with the addition of the inequality $y \geqslant 1$. The variables of P will be ordered increasingly as $y, z, x_1, \bar{x}_1, x_2, \bar{x}_2, \dots, x_n, \bar{x}_n$.

Suppose that S is satisfiable, define $\mathbf{x}$ as before, and extend it by setting $y = 1$ and $z = 0$. Then this is a minimal generator and is only in I'_0. Now, z is internal to this vector, but no minimal generator of the ideal has z in its support (let alone, as an extreme entry), so condition (ii) of Theorem 9 is violated, and P has a negative answer.

Conversely, if P has a negative answer, there exists a minimal generator and an internal variable such that condition (ii) of Theorem 9 is violated. This minimal generator cannot be in any of the $I_i, i \geqslant 1$, since those have no internal letters. So it is in I'_0, and must have $y = 1$, $z = 0$, and the other variables must be a boolean assignment that satisfies S. The problematic internal variable must be z, but who cares?

Reduction to Problem 1: We use just one new variable y. The instance P of Problem 1 consists of I_0, a new system I_*, with the single inequality $y \geqslant 2$, systems I'_i, each obtained from I_i by the addition of the inequality $y \geqslant 1$. By arguments similar to the preceding ones and the help of Theorem 23(iii), it can be shown that S is satisfiable if and only if P has a negative answer.

Proposition 24(iii) says that a convex ideal is the set of integer points of a *blocking polyhedron*. Such polyhedra, and mostly their integer points, have been the subject of a lot of attention in the context of combinatorial and integer programming. This, and perhaps sheer curiosity, justify asking what happens to Problems 1–4 if one restricts the questions to convex ideals (given in the form $I(A, w)$). No one of the definite results we presented so far applies to convex ideals; in particular, the proof of Theorem 19 constructs ideals that are not convex, so even Problem 3's status is undecided.

References

[1] D.J. Anick, On the homology of associative algebras, Trans. Amer. Math. Soc. 296 (1986) 641–659.

[2] D. Anick, G.-C. Rota, Higher-order syzygies for the bracket algebra and for the ring of coordinates of the Grassmannian, Proc. Nat. Acad. Sci. USA 88 (1991) 8087–8090.

[3] M.-P. Béal, F. Mignosi, A. Restivo, M. Sciortino, Forbidden words in symbolic dynamics, Adv. Appl. Math. 25 (2000) 163–193.

[4] M. Crochemore, F. Mignosi, A. Restivo, Automata and forbidden words, Inform. Process. Lett. 67 (1998) 111–117.

[5] D. Eisenbud, I. Peeva, B. Sturmfels, Non-commutative Gröbner bases for commutative algebras, Proc. Amer. Math. Soc. 126 (1998) 687–691.

[6] T. Gallai, Graphen mit triangulierbaren ungeraden Vielecken, Magyar Tud. Akad. Mat. Kutat Int. Közl. 7 (1962) 3–36.

[7] M. Garey, D.S. Johnson, Computers and Intractability. A guide to the theory of NP-Completeness, W.H. Freeman and Co., San Francisco, CA, 1979.

[8] M.C. Golumbic, Algorithmic Aspects of Perfect Graphs, North-Holland Mathematical Studies, Vol. 88, North-Holland, Amsterdam, 1984.
[9] E. Green, Noncommutative Gröbner bases and projective resolutions, Progress in Mathematics, Vol. 173, Birkhäuser Verlag, Basel/Switzerland, 1999, pp. 29–60 (Chapter 2).
[10] E. Green, R.Q. Huang, Projective resolutions of straightening closed algebras generated by minors, Adv. in Math. 110 (1995) 314–333.
[11] G. Higman, Ordering by divisibility in abstract algebras, Proc. London Math. Soc. 3 (1952) 326–336.
[12] H.R. Lewis, C.H. Papadimitiou, Elements in the Theory of Computation, 2nd Edition, Prentice-Hall, Englewood Cliffs, NJ, 1998.
[13] T. Mora, An introduction to commutative and noncommutative Gröbner bases, Theoret. Comput. Sci. 134 (1994) 131–173.
[14] F. Maffray, M. Preissmann, A translation of Gallai's paper: Transitiv Orientierbare Graphen, in: J.L. Ramírez-Alfonsín, B.A. Reed (Eds.), Perfect Graphs, Jossey-Bass, New York, 2001.
[15] I. Peeva, V. Reiner, B. Sturmfels, How to shell a monoid, Math. Ann. 310 (1998) 379–393.
[16] J.L. Ramírez-Alfonsín, B.A. Reed (Eds.), Perfect Graphs, Jossey-Bass, New York, 2001.
[17] T.J. Schaefer, The complexity of satisfiability problems, Conference Record of the Tenth Annual ACM Symposium on Theory of Computing (San Diego, CA, 1978), ACM, New York, 1978, pp. 216–226.
[18] A. Schrijver, Theory of Linear and Integer Programming, Wiley-Interscience Series in Discrete Mathematics, Wiley, Chichester, 1986.