MATHEMATICS OF COMPUTATION
http://dx.doi.org/10.1090/mcom/3321
Article electronically published on April 6, 2018

GRÖBNER BASES OVER FIELDS WITH VALUATIONS

ANDREW J. CHAN AND DIANE MACLAGAN

Abstract. Let K be a field with a valuation and let S be the polynomial ring $S := K[x_1, \ldots, x_n]$. We discuss the extension of Gröbner theory to ideals in S, taking the valuations of coefficients into account, and describe the Buchberger algorithm in this context. In addition we discuss some implementation and complexity issues. The main motivation comes from tropical geometry, as tropical varieties can be defined using these Gröbner bases, but we also give examples showing that the resulting Gröbner bases can be substantially smaller than traditional Gröbner bases. In the case $K = \mathbb{Q}$ with the p-adic valuation the algorithms have been implemented in a Macaulay 2 package.

1. Introduction

Most work in computational algebraic geometry makes fundamental use of the theory of Gröbner bases. In this paper we consider algorithms for a variant of Gröbner bases for ideals in a polynomial ring with coefficients in a valued field.

A major application for these results is in the rapidly growing field of tropical geometry. Let X be the subvariety of $\mathbb{P}^{n-1}$ defined by a homogeneous ideal I in $S = K[x_1, \ldots, x_n]$, where K is a field with a valuation $\mathrm{val}\colon K^* \to \mathbb{R}$. Let X^0 be the intersection of X with the torus $T \cong (K^*)^{n-1}$ of $\mathbb{P}^{n-1}$. The tropicalization of X^0 is the set of $w \in \mathbb{R}^n/\mathbb{R}(1, \ldots, 1)$ for which the modified initial ideal $\mathrm{in}_w(I)$ does not contain a monomial. This has the structure of a polyhedral complex, and many invariants of X can be recovered from the tropical variety.

Prior computational work in tropical geometry has focused on ideals with coefficients in either $\mathbb{Q}$ with the trivial valuation or $\overline{\mathbb{Q}(t)}$, as those cases can be treated using standard Gröbner techniques. See the software `gfan` [Jen] for details. Standard Gröbner techniques do not suffice for the case of $\mathbb{Q}$ with the p-adic valuation val_p, which is of increasing interest thanks to the connections between tropical geometry and Berkovich spaces; see, for example, [BPR16].

Section 2 explains how the standard Gröbner algorithms need to be modified to handle general valued fields K, such as $(\mathbb{Q}, \mathrm{val}_p)$. The main issue is that the standard normal form algorithm need not terminate. The solution is to replace it by a modification of Mora's tangent cone algorithm; the main contribution of this part of the paper is the suggestion of an appropriate écart function. Unlike the standard basis case, we get a strong normal form; see Remark 2.7. In Sections 3 and 4 we discuss complexity and implementation issues. Degree bounds are as for usual Gröbner bases (Theorem 3.1). While the valuations of coefficients in a reduced Gröbner basis cannot be bounded by the valuations of the original generators (Example 3.2), for coefficients in $(\mathbb{Q}, \mathrm{val}_p)$ we can bound the valuations

Received by the editor October 28, 2016, and, in revised form, July 29, 2017.
2010 *Mathematics Subject Classification.* Primary 13P10; Secondary 14T05.
The second author was partially supported by EPSRC grant EP/I008071/1.

of coefficients in a reduced Gröbner basis using the valuations and absolute values of coefficients of the generators; see Proposition 3.3.

A theoretical consequence of these results is a computational proof that the tropical variety of an ideal only depends on the field defined by the coefficients of the generators; see Corollary 2.12. We expect these algorithms to also have applications outside tropical geometry. In particular, they can lead to smaller Gröbner bases. In Section 5 we give a family of ideals in $\mathbb{Q}[x_1, x_2, x_3]$ for which the size of the p-adic Gröbner basis is constant but the smallest size of a traditional Gröbner basis grows unboundedly.

The algorithms have been implemented in a package `GrobnerValuations` [AJC13] for the computational algebraic geometry system `Macaulay2` [GS], which is available from the authors' webpages. A preliminary implementation is also available in `gfan` [Jen]. For a different approach to this problem, see [MR16].

2. Gröbner theory

In this section we generalize the standard Buchberger algorithm for Gröbner bases so that it takes the valuations of coefficients into account. The key algorithm is Algorithm 2.4, which computes the normal form of a polynomial.

Let K be a field with a valuation $\mathrm{val}\colon K^* \to \mathbb{R}$. We denote by $R := \{a \in K : \mathrm{val}(a) \geq 0\} \cup \{0\}$ the valuation ring of K, by $\mathfrak{m} := \{a \in K : \mathrm{val}(a) > 0\} \cup \{0\}$ the maximal ideal of the local ring R, and by $\Bbbk := R/\mathfrak{m}$ the residue field. For $a \in R$ we denote by $\overline{a}$ the image of a in $\Bbbk$. The image of the valuation map is denoted by Γ, and is an additive subgroup of $\mathbb{R}$. We assume that there exists a group homomorphism $\phi : \Gamma \to K^*$ with $\mathrm{val}(\phi(w)) = w$. This always exists if K is algebraically closed (see [MS15, Lemma 2.1.15]). For example, the field $K = \mathbb{Q}(t)$ has valuation $\mathrm{val}(f/g) = a$ when the Taylor series for f/g is $\alpha t^a +$ higher order terms. In this case we can set $\phi(w) = t^w$. We use the notation $w \mapsto t^w$ for the homomorphism ϕ for an arbitrary field. We make frequent use of the p-adic valuation val_p on $\mathbb{Q}$. If $a = p^m b/c$, where p does not divide b or c, then $\mathrm{val}_p(a) = m$. In this case $\Gamma = \mathbb{Z}$, and we can take ϕ to be $\phi(w) = p^w$. Another standard, though less computationally effective, choice of field is the Puiseux series $\mathbb{C}\{\{t\}\}$ with valuation the lowest exponent occurring.

Let S be the polynomial ring $K[x_1, \ldots, x_n]$, and fix a weight vector $w \in \mathbb{R}^n$. For $f = \sum_{u \in \mathbb{N}^n} c_u x^u \in S$, let $W := \mathrm{trop}(f)(w) = \min(\mathrm{val}(c_u) + w \cdot u : c_u \neq 0)$. The initial term of f with respect to w is

$$\mathrm{in}_w(f) = \sum_{\mathrm{val}(c_u)+w\cdot u = W} \overline{t^{-\mathrm{val}(c_u)} c_u} x^u \in \Bbbk[x_1, \ldots, x_n].$$

The initial ideal of a homogeneous ideal $I \subset S$ with respect to $w \in \mathbb{R}^n$ is

$$\mathrm{in}_w(I) = \langle \mathrm{in}_w(f) : f \in I \rangle \subseteq \Bbbk[x_1, \ldots, x_n].$$

Note that $\mathrm{in}_w(I)$ is an ideal in $\Bbbk[x_1, \ldots, x_n]$. A finite set $\mathcal{G} = \{g_1, \ldots, g_s\} \subset I$ is called a *Gröbner basis* for I with respect to w if $\mathrm{in}_w(I) = \langle \mathrm{in}_w(g_1), \ldots, \mathrm{in}_w(g_s) \rangle$. The requirement that the ideal I be homogeneous is not necessary to define an initial ideal, but is for a Gröbner basis to have expected properties; see Remark 2.11.

This modification of the original definition of a Gröbner basis comes from tropical geometry; see [Spe05]. When the valuation on K is trivial this initial ideal is the standard initial ideal of I with respect to the weight vector $-w$. While many properties of these Gröbner bases are well understood when the valuation is nontrivial, computational issues have not yet been addressed in the literature.

Example 2.1. Let $f = 3x^2+xy+18y^2 \in \mathbb{Q}[x,y]$, where $\mathbb{Q}$ has the 3-adic valuation. For $w = (0,0)$ we have $W = 0$, and $\mathrm{in}_w(f) = xy \in \mathbb{Z}/3\mathbb{Z}[x,y]$. For $w = (1,4)$ we have $W = 3$, and $\mathrm{in}_w(f) = x^2$, and for $w = (2,0)$ we have $W = 2$ and $\mathrm{in}_w(f) = xy + \overline{3^{-2}18}y^2 = xy + 2y^2$.

A Gröbner basis for an ideal I can be computed by a modification of the standard Buchberger algorithm as we explain below. The main difference is in the normal form algorithm for the remainder of a polynomial on division by a set of other polynomials. The difficulty is that a naive implementation of the normal form algorithm need not terminate, as the following example shows.

Example 2.2. Let $K = \mathbb{Q}$ with the 2-adic valuation. Consider the standard normal form algorithm, where the term to be canceled at each stage is taken to be the term with the lowest valuation of the coefficient. Using this to compute the remainder of $x \in \mathbb{Q}[x,y,z]$ on division by $\{x-2y, y-2z, z-2x\}$, we reduce x by $x-2y$ to get $2y$. This is then reduced by $y-2z$ to get $4z$, which in turn is reduced by $z-2x$ to get $8x$. This reduction continues indefinitely.

This problem also arises in the theory of standard bases; see for example [CLO05, §4.3]. The solution in that setting, Mora's tangent cone algorithm, is to allow division by previous partial quotients. Termination is assured by a descending nonnegative integer invariant called the écart which measures the difference in degrees between two possible initial terms of a polynomial. A difficulty in generalizing this function to Gröbner bases with valuations is that this difference must take the valuations of the coefficients into account, so would naturally lie in the not-necessarily-well-ordered group Γ. Even for the valuation val_p on $\mathbb{Q}$, where $\Gamma = \mathbb{Z}$, the standard écart function does not work directly.

The following algorithm modifies Mora's algorithm to take into account the valuations of the coefficients. It uses a function $E(f,g)$, which takes two homogeneous polynomials and returns a nonnegative integer. In Lemma 2.6 we give one option for this function that ensures termination. We present the algorithm with the function E unspecified as more efficient functions E may exist.

As in all normal form algorithms this is a generalization of long division, which works by canceling the "leading term" of the polynomial f. An added complication is that we do not assume that the weight vector w is generic, so the leading term $\mathrm{in}_w(f)$ is not necessarily a monomial. For this reason we also fix an arbitrary monomial term order $\prec$ (in the sense of usual Gröbner theory) to determine which term of $\mathrm{in}_w(f)$ to cancel. If w is sufficiently generic with respect to the input polynomials $\prec$ will play no role. For $f \in K[x_1,\dots,x_n]$, $\mathrm{in}_\prec(\mathrm{in}_w(f)) = \alpha x^u$ denotes the leading term, including the coefficient. We denote by $\mathrm{lm}(f)$ the monomial x^u occurring in $\mathrm{in}_\prec(\mathrm{in}_w(f))$, and by $\mathrm{lc}(f)$ the coefficient of x^u in f. Note that $\mathrm{lc}(f) \in K$, not $\Bbbk$, and that $\mathrm{lc}(f)$ and $\mathrm{lm}(f)$ depend on both w and $\prec$.

We also use the following partial order on polynomials, which plays the role of comparing initial monomials in usual Gröbner bases.

Definition 2.3. Fix homogeneous polynomials $f, g \in K[x_1,\dots,x_n]$, $w \in \mathbb{R}^n$, and a term order $\prec$. Write $\mathrm{lm}(f) = x^u$, $\mathrm{lm}(g) = x^v$, $\mathrm{lc}(f) = a$, and $\mathrm{lc}(g) = b$. Then $f < g$ if $\mathrm{val}(a) + w\cdot u < \mathrm{val}(b) + w\cdot v$ or $\mathrm{val}(a) + w\cdot u = \mathrm{val}(b) + w\cdot v$ and $x^u \succ x^v$. In addition we set $f < 0$ for all nonzero f. This is consistent with the first part of the definition if we regard the valuation as a function $\mathrm{val}\colon K \to \mathbb{R}\cup\{\infty\}$.

For example, if $\mathbb{Q}$ has the 2-adic valuation, $w = (1, 2)$ and $\prec$ is the lexicographic term order with $x_1 \succ x_2$, then $x_1^2 < x_2^2 < x_1^5 < 2x_2^2$. Note that if $f \geq h$ and $g \geq h$, then $f \pm g \geq h$.

Algorithm 2.4. Input: Homogeneous polynomials $\{g_1, \ldots, g_s\}$, a homogeneous polynomial f in $S = K[x_1, \ldots, x_n]$, a weight vector $w \in \mathbb{R}^n$, and a term order $\prec$.
Output: Homogeneous polynomials $h_1, \ldots, h_s, r \in S$ satisfying

$$f = \sum_{i=1}^{s} h_i g_i + r,$$

where $h_i g_i \geq f$ for $1 \leq i \leq s$, and $r \geq f$. Write $r = \sum b_v x^v$ with $b_v \in K$. Then in addition $b_v \neq 0$ implies x^v is not divisible by any $\operatorname{lm}(g_i)$.

We call r a *remainder*, or *normal form*, of dividing f by $\{g_1, \ldots, g_s\}$.

(1) **Initialize:** Set $T = \{g_1, \ldots, g_s\}, h_{10} = \cdots = h_{s0} = 0, q_0 = f, r_0 = 0$. Set $j = 0$.
(2) **Loop:** While $q_j \neq 0$ do:
  (a) **Move to remainder:** If there is no $g \in T$ with $\operatorname{lm}(g)$ dividing $\operatorname{lm}(q_j)$, then set $r_{j+1} = r_j + \operatorname{lc}(q_j)\operatorname{lm}(q_j)$, $q_{j+1} = q_j - \operatorname{lc}(q_j)\operatorname{lm}(q_j)$, and $h_{ij+1} = h_{ij}$ for all i. Set $T = T \cup \{q_j\}$.
  (b) **Divide:** Otherwise:
    (i) Choose $g \in T$ such that $\operatorname{lm}(g)$ divides $\operatorname{lm}(q_j)$ with $E(q_j, g)$ minimal among all such choices.
    (ii) If $E(q_j, g) > 0$, then set $T = T \cup \{q_j\}$.
    (iii) Since $\operatorname{lm}(g)$ divides $\operatorname{lm}(q_j)$ there is a monomial x^v with $\operatorname{lm}(x^v g) = \operatorname{lm}(q_j)$. Set $c_v = \operatorname{lc}(q_j)/\operatorname{lc}(x^v g) \in K$. Let $p = q_j - c_v x^v g$.
    (iv) If $g = g_m$ for some $1 \leq m \leq s$, then set $q_{j+1} = p$, $h_{mj+1} = h_{mj} + c_v x^v$, $h_{ij+1} = h_{ij}$ for $i \neq m$, and $r_{j+1} = r_j$.
    (v) If g was added to T at some previous iteration of the algorithm, so $g = q_m$ for some $m < j$, then set $q_{j+1} = 1/(1 - c_v)p$, $h_{ij+1} = 1/(1 - c_v)(h_{ij} - c_v h_{im})$, and $r_{j+1} = 1/(1 - c_v)(r_j - c_v r_m)$.
  (c) $j = j + 1$.
(3) **Output:** Output $h_i = h_{ij}$ for $1 \leq i \leq s$, and $r = r_j$.

Example 2.5. Let $f = x^2 + y^2 + z^2 \in \mathbb{Q}[x, y, z]$ where $\mathbb{Q}$ has the 2-adic valuation, and let $g_1 = y + 16z$. Fix $w = (3, 2, 1)$, and let $\prec$ be the lexicographic order with $x \prec y \prec z$. For clarity we underline the term of a polynomial f containing $\operatorname{lm}(f)$. We do not specify the function $E(f, g)$, assuming that it is always positive. Then the algorithm proceeds as follows:

(1) $T = \{\underline{y} + 16z\}$, $h_{10} = 0$, $q_0 = x^2 + y^2 + \underline{z^2}$, $r_0 = 0$, $j = 0$.
(2) $T = \{\underline{y} + 16z, x^2 + y^2 + \underline{z^2}\}$, $h_{11} = 0$, $q_1 = x^2 + \underline{y^2}$, $r_1 = z^2$, $j = 1$.
(3) $T = \{\underline{y} + 16z, x^2 + y^2 + \underline{z^2}, x^2 + \underline{y^2}\}$, $h_{12} = y$, $q_2 = \underline{x^2} - 16yz$, $r_2 = z^2$, $j = 2$.
(4) $T = \{\underline{y} + 16z, x^2 + y^2 + \underline{z^2}, x^2 + \underline{y^2}, \underline{x^2} - 16yz\}$, $h_{13} = y$, $q_3 = -16yz$, $r_3 = x^2 + z^2$, $j = 3$.
(5) $T = \{\underline{y} + 16z, x^2 + y^2 + \underline{z^2}, x^2 + \underline{y^2}, \underline{x^2} - 16yz, -16yz\}$, $h_{14} = y - 16z$, $q_4 = 256z^2$, $r_4 = x^2 + z^2$, $j = 4$.
(6) $T = \{\underline{y} + 16z, x^2 + y^2 + \underline{z^2}, x^2 + \underline{y^2}, \underline{x^2} - 16yz, -16yz, 256z^2\}$. In this case we divide by $g = x^2 + y^2 + z^2 = q_0$, so $c_v = 256$. Thus $h_{15} = -1/255(y - 16z)$, $q_5 = 1/255(256x^2 + \underline{256y^2})$, $r_5 = -1/255(x^2 + z^2)$, and $j = 5$.

(7) $T = \{\underline{y} + 16z, x^2 + y^2 + \underline{z}^2, x^2 + \underline{y}^2, \underline{x}^2 - 16yz, -16yz, -16z^2, 256/255x^2 + \underline{255/256y^2}\}$. Then $g = x^2 + y^2 = q_1$, so $c_v = 256/255$. Thus $h_{16} = \underline{255}(1/255(y - 16z)) = y - 16z$, $q_6 = 0$, $r_6 = -255(-1/255(x^2 + z^2) - 256/255z^2) = x^2 + 257z^2$, and $j = 6$.
(8) Output $h_1 = y - 16z$ and $r = x^2 + 257z^2$.

Note that $x^2+y^2+z^2 = (y-16z)(y+16z)+x^2+257z^2$ and no term of x^2+257z^2 is divisible by $\mathrm{lm}(y + 16z) = y$.

Proof of correctness. We show correctness assuming termination.

We show that the following properties hold at each stage of the algorithm:

(1) $f = q_j + \sum_{i=1}^{s} h_{ij}g_i + r_j$;
(2) $h_{ij}g_i \geq f$;
(3) $r_j \geq f$;
(4) No term of r_j is divisible by any $\mathrm{lm}(g_i)$;
(5) $q_j \geq f$;
(6) If $q_{j+1} \neq 0$, then $q_{j+1} > q_j$.

These properties all hold at the initialization step by construction. We now show they continue to hold after each of the three types of iteration step. We also show that in step 2(b)(v) of the algorithm we have $1 - c_v \neq 0$. In all cases, write $\mathrm{lc}(q_j)\,\mathrm{lm}(q_j) = c_j x^{\alpha_j}$. There are three possibilities for the division step, which we consider separately.

Case 1. **Move to remainder**. Suppose there is no $g \in T$ with $\mathrm{lm}(g)$ dividing $\mathrm{lm}(q_j)$. Then the only values that change are q_j and r_j, but we have $q_j + r_j = q_{j+1} + r_{j+1}$ by construction, so the equality (1) holds. Condition (2) holds at stage $j + 1$ since it held at stage j. Since properties (3) and (5) hold for j, property (3) holds for $j + 1$. The term that is added to r_{j+1} is not divisible by any $\mathrm{lm}(g_i)$, so property (4) still holds. The term $c_{j+1}x^{\alpha_{j+1}}$ is a nonleading term of q_j, so property (6) follows, which also implies property (5).

Case 2. **Divide, with** $g = g_m$. Suppose the chosen g with $\mathrm{lm}(g)$ dividing $\mathrm{lm}(q_j)$ is g_m for some $1 \leq m \leq s$. Since $q_j + h_{mj}g_m = q_{j+1} + h_{mj+1}g_m$ by construction, the equality (1) holds in this case as well. Since $h_{mj}g_m \geq f$, and $q_j \geq f$, we have $h_{mj+1}g_m \geq f$. As the remainder term does not change properties (3) and (4) still hold. Since $q_{j+1} = q_j - c_v x^v g_m$, we cancel the leading term of q_j, so all terms of q_{j+1} are the sum of a nonleading term of q_j and a term of $c_v x^v q_m$ that is larger than $c_j x^{\alpha_j}$. This implies that $q_j < q_{j+1}$ (property (6)), which implies property (5) for $j + 1$ as above.

Case 3. **Divide, with** $g = q_m$. Finally, we consider the case that the chosen g with $\mathrm{lm}(g)$ dividing $\mathrm{lm}(q_j)$ is q_m for some $m < j$. Since all q_i are homogeneous of the same degree, $x^v = 1$ in this setting, and $c_v = c_j/c_m$. Since property (6) holds for all smaller values, we have $\mathrm{val}(c_j) + w \cdot \alpha_j > \mathrm{val}(c_m) + w \cdot \alpha_m$. Thus $x^{\alpha_m} = x^{\alpha_j}$ implies $\mathrm{val}(c_v) > 0$, so $1 - c_v \neq 0$.

Now $f = q_m + \sum_{i=1}^{s} h_{im}g_i + r_m$, so $q_{j+1} = 1/(1 - c_v)(q_j - c_v q_m)$, which equals $1/(1 - c_v)((f - \sum_{i=1}^{s} h_{ij}g_i - r_j) - c_v(f - \sum_{i=1}^{s} h_{im}g_i - r_m))$. Thus $f = q_{j+1} + \sum_{i=1}^{s} 1/(1-c_v)(h_{ij} - c_v h_{im})g_i + 1/(1-c_v)(r_j - c_v r_m) = q_{j+1} + \sum_{i=1}^{s} h_{ij+1}g_i + r_{j+1}$. This is equality (1).

Since $\mathrm{val}(1 - c_v) = 0$, we have $\mathrm{val}(1/(1 - c_v)) = 0$. Note the following property of the order $<$ of Definition 2.3: If $p_1 \geq p_2$ and $c \in K$ satisfies $\mathrm{val}(c) \geq 0$, then

$cp_1 \geq p_2$. Then properties (2) and (3) for $j+1$ follow from the analogous properties for j and m. No term in either r_j or r_m is divisible by any $\mathrm{lm}(g_i)$, so the same is true for r_{j+1}. Finally, $p > q_j$ by construction, so $q_{j+1} = 1/(1-c_v)p > q_j$ as above, so properties (5) and (6) also hold. □

Lemma 2.6. *For homogeneous polynomials $f, g \in S$ with $f = \sum c_u x^u$ and $g = \sum b_u x^u$, set $E(f,g) := |\{u : b_u \neq 0, c_u = 0\}|$. Algorithm 2.4 terminates for this choice of function E.*

Proof. There are only a finite number of possible supports $\mathrm{supp}(q_j) = \{u : c_u \neq 0\}$ of the polynomials $q_j = \sum c_u x^u$, as they all have the same degree. Thus after some step j no new support will occur, so there will be $q_m \in T_j$ with $\mathrm{supp}(q_m) \subseteq \mathrm{supp}(q_j)$, and so $E(q_j, q_m) = 0$. Since we remove the leading term of q_j at the jth step, either by moving it to the remainder, or by canceling it, when $\mathrm{supp}(q_m) \subseteq \mathrm{supp}(q_j)$ we have $\mathrm{supp}(q_{j+1}) \subsetneq \mathrm{supp}(q_j)$. Since the size of the support cannot decrease indefinitely, the algorithm must terminate. □

Remark 2.7. Note that Algorithm 2.4 gives a strong normal form (no term of the remainder is divisible by any of the monomials $\{\mathrm{lm}(g_i) : 1 \leq i \leq s\}$), as opposed to the weak normal form that occurs in the standard basis case. This is a consequence of restricting to homogeneous input; see Remark 2.11 for more on this topic. See [GP08, §1.6] for details of normal forms in the standard basis case.

Remark 2.8. Algorithm 2.4 also holds, with the same proof, in the following modified setting. Let $K = \mathbb{Q}$ with the p-adic valuation. The valuation val_p restricts to a function, which we also denote by val_p, from $\mathbb{Z}/p^m\mathbb{Z}$ to the semigroup $\{0, 1, \ldots, m-1\} \cup \{\infty\}$, where ∞ acts as an absorbing element. Note that $\mathrm{val}_p(ab) = \mathrm{val}_p(a) + \mathrm{val}_p(b)$ and $\mathrm{val}_p(a+b) \geq \min(\mathrm{val}_p(a), \mathrm{val}_p(b))$ for $a, b \in \mathbb{Z}/p^m\mathbb{Z}$. We can then define the partial order $<$ on polynomials in $\mathbb{Z}/p^m\mathbb{Z}[x_1, \ldots, x_n]$ in the same way as in Definition 2.3. Also note that in step 2(b)(v) of the algorithm, since $1 - c_v$ has valuation zero (as shown in the proof), it is not divisible by p, so is a unit in $\mathbb{Z}/p^m\mathbb{Z}$. This means that the algorithm and its proof go through in this setting. This variant is used in Section 4.2.

As in the usual Gröbner setting, we can use the normal form algorithm to compute a Gröbner basis using the Buchberger algorithm. Let f, g be two polynomials in $K[x_1, \ldots, x_n]$. We define the S-polynomial of f and g to be

$$S(f,g) := \mathrm{lc}(g)\frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(f)} f - \mathrm{lc}(f)\frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(g)} g.$$

Algorithm 2.9. Input: A list $\{f_1, \ldots, f_l\}$ of homogeneous polynomials in S, a weight-vector $w \in \mathbb{R}^n$, and a term order $\prec$.
Output: A list $\{g_1, \ldots, g_s\}$ of homogeneous polynomials in $I = \langle f_1, \ldots, f_l \rangle$ such that $\{\mathrm{in}_\prec(\mathrm{in}_w(g_i)) : 1 \leq i \leq s\}$ generates $\mathrm{in}_\prec(\mathrm{in}_w(I))$.

(1) Set $\mathcal{G} = \{f_1, \ldots, f_l\}$. Set $\mathcal{P} = \{(g, g') : g, g' \in \mathcal{G}\}$.
(2) While $\mathcal{P} \neq \emptyset$:
    (a) Pick $(g, g') \in \mathcal{P}$.
    (b) Let r be the normal form on dividing $S(g, g')$ by $\mathcal{G}$. If $r \neq 0$, then set $\mathcal{G} = \mathcal{G} \cup \{r\}$, and $\mathcal{P} = \mathcal{P} \cup \{(r, g) : g \in \mathcal{G}\}$.
(3) Return $\mathcal{G}$.

The proof of the termination and correctness of this algorithm is almost exactly the same as the proof for usual Gröbner bases, which can be found for example in [CLO07]. We indicate below the necessary changes, which use the following lemma.

Lemma 2.10. *Fix $v_1, \dots, v_m \in K^n$, and $\beta_1, \dots, \beta_m \in \mathbb{R}$. For $\lambda \in K^m$, write $s(\lambda) = \min(\mathrm{val}(\lambda_i) + \beta_i)$. Then for fixed $v \in \mathrm{span}(v_1, \dots, v_m)$ there is a choice of $\lambda \in K^m$ with $\sum \lambda_i v_i = v$ that maximizes $s(\lambda)$ among all such choices.*

Proof. We first show that for any λ with $\sum \lambda_i v_i = v$ there is a λ' with $\sum \lambda'_i v_i = v$, $\{v_i : \lambda'_i \neq 0\}$ linearly independent, and $s(\lambda') \geq s(\lambda)$. Indeed, if $\{v_i : \lambda_i \neq 0\}$ is linearly dependent, then there is a nonzero $c \in K^m$ with $\sum c_i v_i = 0$ and $c_i \neq 0$ only when $\lambda_i \neq 0$. After relabeling we may assume that $\mathrm{val}(c_1) + \beta_1 = \min(\mathrm{val}(c_i) + \beta_i)$. Since this then implies that $\mathrm{val}(c_1) \neq \infty$, we have $c_1 \neq 0$, so we may rescale so that $c_1 = \lambda_1$. Let $\lambda' = \lambda - c$. Then for every j,

$$\begin{aligned}
\mathrm{val}(\lambda'_j) + \beta_j &= \mathrm{val}(\lambda_j - c_j) + \beta_j \\
&\geq \min(\mathrm{val}(\lambda_j), \mathrm{val}(c_j)) + \beta_j \\
&= \min(\mathrm{val}(\lambda_j) + \beta_j, \mathrm{val}(c_j) + \beta_j) \\
&\geq \min(\mathrm{val}(\lambda_j) + \beta_j, \mathrm{val}(\lambda_1) + \beta_1) \\
&\geq s(\lambda),
\end{aligned}$$

so $s(\lambda') \geq s(\lambda)$. Since $\{i : \lambda'_i \neq 0\} \subsetneq \{i : \lambda_i \neq 0\}$, after iterating a finite number of times $\{v_i : \lambda'_i \neq 0\}$ is linearly independent. The lemma then follows from the observation that if $\{v_i : \lambda_i \neq 0\}$ is linearly independent, then the λ_i are determined, so the maximum $s(\lambda)$ is achieved at one of these finitely many choices. □

Proof of termination and correctness of Algorithm 2.9. Since at each stage the ideal $\langle \mathrm{in}_\prec(\mathrm{in}_w(g)) : g \in \mathcal{G} \rangle$ strictly increases, termination follows as in the standard case from the fact that the polynomial ring is Noetherian.

The proof of correctness is also essentially the same as in the standard case; we include it as it takes essentially the same amount of space as indicating the changes. Suppose at the end of the algorithm $\mathrm{in}_\prec(\mathrm{in}_w(f)) \notin \langle \mathrm{in}_\prec(\mathrm{in}_w(g_i)) : 1 \leq i \leq s \rangle$ for some homogeneous $f \in I$. Since the f_i are contained in $\mathcal{G}$, we can write $f = \sum h_i g_i$ for some homogeneous polynomials h_i. Write $\mathrm{lm}(h_i g_i) = x^{u_i}$. We may assume that $\min(\mathrm{val}(\mathrm{lc}(h_i g_i)) + w \cdot u_i)$ is maximal over all choices of counterexample f and description $f = \sum h_i g_i$. That a maximum exists follows from Lemma 2.10 applied to the vector space $S_{\deg(f)}$, with the v_i all polynomials of the form $x^u g_j$, where x^u is a monomial of degree $\deg(f) - \deg(g_j)$, and $\beta_i = w \cdot u'$ for $\mathrm{lm}(x^u g_j) = x^{u'}$. After renumbering we may assume that $\min(\mathrm{val}(\mathrm{lc}(h_i g_i)) + w \cdot u_i) = \mathrm{val}(\mathrm{lc}(h_j g_j)) + w \cdot u_j$ for $1 \leq j \leq d$, and that in addition $x^{u_1} = x^{u_i}$ for $1 \leq i \leq d' \leq d$ with x^{u_1} the largest x^{u_i} among those $i \leq d$. We may further assume that d' is as small as possible among descriptions achieving the maximum. Since $\mathrm{in}_\prec(\mathrm{in}_w(h_i g_i)) = \mathrm{in}_\prec(\mathrm{in}_w(h_i))\,\mathrm{in}_\prec(\mathrm{in}_w(g_i)) \in \langle \mathrm{in}_\prec(\mathrm{in}_w(g_1)), \dots, \mathrm{in}_\prec(\mathrm{in}_w(g_s)) \rangle$, $x^{u_1} \neq \mathrm{lm}(f)$. This means that $\mathrm{lm}(\sum_{i=1}^{d'} h_i g_i) \neq \mathrm{lm}(f)$, so $\mathrm{val}(\sum_{i=1}^{d'} \mathrm{lc}(h_i g_i)) \geq \min(\mathrm{val}(\mathrm{lc}(h_i g_i)))$, and so in particular $d' \geq 2$. By hypothesis we can write $S(g_1, g_2) = \sum_{i=1}^{s} h'_i g_i$ with

$h_i' g_i \geq S(g_1, g_2)$. Then

$$\begin{aligned} f &= \sum_{i=1}^{s} h_i g_i \\ &= \sum_{i=1}^{s} h_i g_i - \frac{\operatorname{lc}(h_1 g_1) x^{u_1}}{\operatorname{lc}(g_1)\operatorname{lc}(g_2)\operatorname{lcm}(\operatorname{lm}(g_1), \operatorname{lm}(g_2))}(S(g_1, g_2) - \sum_{i=1}^{s} h_i' g_i) \\ &= (h_1 - \frac{\operatorname{lc}(h_1 g_1) x^{u_1}}{\operatorname{lc}(g_1)\operatorname{lm}(g_1)} + \frac{\operatorname{lc}(h_1 g_2) x^{u_1}}{\operatorname{lc}(g_1)\operatorname{lc}(g_2)\operatorname{lcm}(\operatorname{lm}(g_1), \operatorname{lm}(g_2))} h_1') g_1 \\ &\qquad + (h_2 - \frac{\operatorname{lc}(h_1 g_1) x^{u_1}}{\operatorname{lc}(g_1)\operatorname{lm}(g_2)} + \frac{\operatorname{lc}(h_1 g_2) x^{u_1}}{\operatorname{lc}(g_1)\operatorname{lc}(g_2)\operatorname{lcm}(\operatorname{lm}(g_1), \operatorname{lm}(g_2))} h_2') g_2 \\ &\qquad + \sum_{i=3}^{s} (h_i + \frac{\operatorname{lc}(h_1 g_2) x^{u_1}}{\operatorname{lc}(g_1)\operatorname{lc}(g_2)\operatorname{lcm}(\operatorname{lm}(g_1), \operatorname{lm}(g_2))} h_i') g_i \\ &= \sum_{i=1}^{s} \tilde{h}_i g_i, \end{aligned}$$

where $\tilde{h}_i$ is defined to be the polynomial multiplying g_i in the previous line. By construction $\tilde{h}_1 > h_1$ and $\tilde{h}_i \geq h_i$ for all $i \geq 2$. Write $x^{\tilde{u}_i}$ for $\operatorname{lm}(\tilde{h}_i g_i)$. Thus we have a new expression for f with either $\min(\operatorname{val}(\operatorname{lc}(\tilde{h}_i g_i)) + w \cdot \tilde{u}_i)$ larger or this minimum the same and d' smaller, which contradicts our assumptions on the respective maximality and minimality of these quantities. We thus conclude that f does not exist, so $\operatorname{in}_\prec(\operatorname{in}_w(I)) = \langle \operatorname{in}_\prec(\operatorname{in}_w(g_1)), \ldots, \operatorname{in}_\prec(\operatorname{in}_w(g_s)) \rangle$ as required. □

Note that Algorithm 2.9 and the proof above also holds in the variation discussed in Remark 2.8.

After applying Algorithm 2.9 we have found a set $\{g_1, \ldots, g_s\} \subset I$ such that $\{\operatorname{in}_\prec(\operatorname{in}_w(g_i)) : 1 \leq i \leq s\}$ generates $\operatorname{in}_\prec(\operatorname{in}_w(I))$. This means that $\{\operatorname{in}_w(g_i) : 1 \leq i \leq s\}$ is a (usual) Gröbner basis for $\operatorname{in}_w(I)$ with respect to $\prec$, so in particular this set generates $\operatorname{in}_w(I)$. We thus conclude that the set $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I with respect to w.

This Gröbner theory shares many of the properties of standard Gröbner bases:

(1) The Gröbner basis $\{g_1, \ldots, g_s\}$ generates I. The proof here is the standard one: If $f \in I$, then the normal form r of f with respect to $\{g_1, \ldots, g_s\}$ lies in I, but $\operatorname{in}_\prec(\operatorname{in}_w(r)) \notin \operatorname{in}_\prec(\operatorname{in}_w(I))$ unless $r = 0$.
(2) For any homogeneous ideal I, $w \in \mathbb{R}^n$, and monomial term order $\prec$ there is a unique reduced Gröbner basis. This is a Gröbner basis $\{g_1, \ldots, g_s\}$ with the property that the $\operatorname{in}_\prec(\operatorname{in}_w(g_i))$ minimally generate $\operatorname{in}_\prec(\operatorname{in}_w(I))$, and no monomial in g_i except $\operatorname{lm}(g_i)$ is divisible by any $\operatorname{lm}(g_j)$. This follows, as in the standard case, from the existence of a strong normal form. Specifically, if $\operatorname{in}_\prec(\operatorname{in}_w(I)) = \langle x^{u_1}, \ldots, x^{u_s} \rangle$, then let r_i be the remainder on dividing x^{u_i} by any Gröbner basis for I with respect to w and $\prec$. Set $g_i = x^{u_i} - r_i$.
(3) The Hilbert function of the two ideals I and $\operatorname{in}_w(I)$ (which live in different polynomial rings) agree. While this follows, as in the standard case, from the existence of a strong normal form, there are other proofs; see, for example, [Spe05, Chapter 2] or [MS15, Corollary 2.4.9].

Remark 2.11. We remark that the assumption that the ideal I, and the Gröbner basis $\{g_1, \ldots, g_s\}$, are homogeneous is necessary for many of these properties of

Gröbner bases. For example, a set $\{g_1, \dots, g_s\} \subset I$ with $\mathrm{in}_w(I) = \langle \mathrm{in}_w(g_1), \dots, \mathrm{in}_w(g_s)\rangle$ need not generate I if it is not homogeneous. A simple example is given by $I = \langle x\rangle \subseteq \mathbb{Q}[x]$ with the 2-adic valuation: For $w = 0$ the set $\{g_1 = x + 2x^2\}$ satisfies $\mathrm{in}_w(I) = \langle x\rangle = \langle \mathrm{in}_w(g_1)\rangle$, but $\langle x\rangle \neq \langle x + 2x^2\rangle$.

This algorithmic approach to these initial ideals also allows a short computational proof of the following theorem of tropical geometry. See [MS15] for background definitions.

Corollary 2.12. *Let K be a field with a valuation* val *for which there is a homomorphism $\phi : \Gamma \to K^*$ with* $\mathrm{val}(\phi(w)) = w$. *Let L be an extension field of K with a valuation that restricts to* val *on K. Let $Y \subseteq (K^*)^n$, and let $Y_L = Y \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L)$. Then* $\mathrm{trop}(Y) = \mathrm{trop}(Y_L)$.

Proof. Let $I \subset K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be the ideal of $Y \subset (K^*)^n$. Then the ideal of Y_L is $I_L = IL[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$. Let $J = I \cap K[x_1, \dots, x_n]$, and $J_L = I_L \cap L[x_1, \dots, x_n]$. This intersection can be calculated by a (standard) Gröbner computation, so the ideals J and J_L have the same generators: $J_L = JL[x_1, \dots, x_n]$. The definition of the initial ideal of an ideal taking the valuation of the coefficients into account extends naturally to the Laurent polynomial ring. By the fundamental theorem of tropical geometry (see, for example [MS15, Theorem 3.2.3]) $w \in \mathbb{R}^n$ lies in $\mathrm{trop}(Y)$ if and only if $\mathrm{in}_w(I) = \langle 1\rangle$, and thus if and only if $\mathrm{in}_w(J)$ contains a monomial. Since J and J_L have the same generators, Algorithm 2.9 implies that regarding the elements of a Gröbner basis for I with respect to w as living in $L[x_1, \dots, x_n]$ gives a Gröbner basis for I_L with respect to w. The residue field $\mathbb{L}$ of L is an extension field of $\Bbbk$, so this means that $\mathrm{in}_w(I_L) = \mathrm{in}_w(I)\mathbb{L}[x_1, \dots, x_n]$. An ideal contains a monomial if and only if the saturation by the product of all the variables is the unit ideal. Since this can be decided by a (standard) Gröbner basis computation, this means that $\mathrm{in}_w(I_L)$ contains a monomial if and only if $\mathrm{in}_w(I)$ does. This implies that $\mathrm{trop}(Y) = \mathrm{trop}(Y_L)$. □

3. Complexity

Given a bound on the degrees of generators for I, it is useful to have a bound on the degrees of elements in a reduced Gröbner basis. The degree bounds in this context are the same as for usual Gröbner bases [MM84], [Dub90], as we show below. We also give a bound on the valuations of coefficients occurring in a reduced Gröbner basis when working over $\mathbb{Q}$ with the p-adic valuation. For the degree bounds we use the formulation of Dubé [Dub90].

Theorem 3.1. *Let $I = \langle f_1, \dots, f_l\rangle \subset K[x_1, \dots, x_n]$ be a homogeneous ideal, with* $\deg(f_i) \leq d$ *for $1 \leq i \leq l$. Fix $w \in \mathbb{R}^n$. Then there is a Gröbner basis $\{g_1, \dots, g_s\}$ for I with respect to w with* $\deg(g_i) \leq 2(d^2/2 + d)^{2^{n-2}}$.

Proof. In [Dub90] it is shown that if $\deg(f_i) \leq d$ for $1 \leq i \leq l$, and $\{g_1', \dots, g_s'\}$ is a standard homogeneous Gröbner basis with respect to some term order $\prec$, then the degree of each g_i' is bounded by $2(d^2/2 + d)^{2^{n-2}}$. The proof given actually shows more: If M is any monomial ideal whose Hilbert function agrees with that of I, then M is generated in degrees at most $2(d^2/2 + d)^{2^{n-2}}$. Denote by S_K the polynomial ring $K[x_1, \dots, x_n]$ and by $S_{\Bbbk}$ the polynomial ring $\Bbbk[x_1, \dots, x_n]$. By [MS15, Corollary 2.4.9] we have $\dim_{\Bbbk}(S_{\Bbbk}/\mathrm{in}_w(I))_\delta = \dim_K(S_K/I)_\delta$ for all degrees δ. Since the initial

ideal $\mathrm{in}_w(I)$ is again a homogeneous ideal, all of its monomial initial ideals have the same Hilbert function, so we have

$$\dim_{\Bbbk}(S_{\Bbbk}/\operatorname{in}_{\prec}(\mathrm{in}_w(I)))_\delta = \dim_{\Bbbk}(S_{\Bbbk}/\operatorname{in}_w(I))_\delta = \dim_K(S_K/I)_\delta.$$

Let M be the monomial ideal in S_K with the same generators as $\operatorname{in}_{\prec}(\mathrm{in}_w(I)) \subset S_{\Bbbk}$. As the Hilbert function of a monomial ideal does not depend on the coefficient field, M has the same Hilbert function as I, so by [Dub90] M is generated in degrees at most $2(d^2/2+d)^{2^{n-2}}$. Choose homogeneous polynomials $\{g_1,\dots,g_s\} \subset I$ such that $\{\operatorname{in}_{\prec}(\mathrm{in}_w(g_1)),\dots,\operatorname{in}_{\prec}(\mathrm{in}_w(g_s))\}$ is a minimal generating set for $\operatorname{in}_{\prec}(\mathrm{in}_w(I))$. Then $\mathrm{in}_w(I) = \langle \mathrm{in}_w(g_1),\dots,\mathrm{in}_w(g_s)\rangle$ so $\{g_1,\dots,g_s\}$ is a Gröbner basis for I with respect to w. Since we have $\deg(\operatorname{in}_{\prec}(\mathrm{in}_w(g_i))) \le 2(d^2/2+d)^{2^{n-2}}$ by above, we deduce that $\{g_1,\dots,g_s\}$ is a Gröbner basis for I with respect to w with $\deg(g_i) \le 2(d^2/2+d)^{2^{n-2}}$ for $1 \le i \le s$ as required. □

Since the valuations of coefficients also play an important role in computing these Gröbner bases, it is also useful to bound the valuations that may occur. This is not possible in full generality, as the following example shows.

Example 3.2. Let $K = \mathbb{Q}(t)$ with the valuation of a rational function given by taking the lowest exponent occurring in a Taylor series for the function. Fix an integer $a \gg 0$ and weight vector $w = (1, a, 2a)$. Let I be the ideal in $K[x,y,z]$ generated by the two polynomials $f = x + z$ and $g = x^2 + (1+t^a)xz + xy$. We compute a Gröbner basis by looking at the S-polynomial $S(f,g) = xf - g = -xy - t^a xz$. Computing the remainder on division by $\{f,g\}$ we obtain $yz + t^a z^2$ which is a nonzero polynomial with initial term yz. It is added to the Gröbner basis at this stage by the Buchberger algorithm (Algorithm 2.9). Further running of this algorithm shows that $\{x+z, yz+t^az^2\}$ is a Gröbner basis for I. This can also be seen from applying Buchberger's criterion (B1); see Section 4.1. Notice that we started with polynomials where the valuations of all the coefficients were zero and we have an element of the reduced Gröbner basis which has a coefficient with valuation a showing that unbounded valuations may potentially occur when computing Gröbner bases. The field $K = \mathbb{Q}(t)$ is only chosen for concreteness; such an example exists for any nontrivially-valued field.

When $K = \mathbb{Q}$ with the p-adic valuation the valuation of coefficients that can occur in a reduced Gröbner basis can be bounded in terms of the absolute values of the original coefficients.

Let $I = \langle f_1,\dots,f_l\rangle$ be a homogeneous ideal in $\mathbb{Q}[x_1,\dots,x_n]$ with $\deg(f_i) \le \delta$ for $1 \le i \le l$. Fix val to be the p-adic valuation on $\mathbb{Q}$. Write $f_i = \sum c_{u,i}x^u$ where we assume (by clearing denominators or dividing by a common factor) that $c_{u,i} \in \mathbb{Z}$ and that for each i we have $\min_u \mathrm{val}(c_{u,i}) = 0$.

Proposition 3.3. *Let $I = \langle f_1,\dots,f_l\rangle$ be a homogeneous ideal in $\mathbb{Q}[x_1,\dots,x_n]$ with assumptions as above. Let $C = \max_{u,i}|c_{u,i}|$. Fix $w \in \mathbb{R}^n$. Then there is a Gröbner basis $\{g_1,\dots,g_s\}$ for I with respect to w, with $g_i = \sum_{u,i} b_{u,i}x^u$, that satisfies*

$$\mathrm{val}(b_{u,i}) \le A/2\log_p(C^2A),$$

where $A = \dim_{\mathbb{Q}}(I_D)$ for $D = 2(\delta^2/2+\delta)^{2^{n-2}}$.

Proof. As the Hilbert functions of I and $\mathrm{in}_w(I)$ agree [MS15, Corollary 2.4.9] we have that $\dim_{\mathbb{Q}} I_d = \dim_{\mathbb{Z}/p\mathbb{Z}}(\mathrm{in}_w(I)_d)$ for all d. Fix a term order $\prec$ on $\mathbb{Z}/p\mathbb{Z}[x_1, \ldots, x_n]$. Let $H(d) = \dim_{\mathbb{Q}}(I_d)$.

For $d \leq D$, form an $H(d) \times \binom{n+d-1}{d}$ matrix A_d with columns indexed by the monomials of degree d ordered so that those in $\mathrm{in}_\prec(\mathrm{in}_w(I))_d$ come first. The rows of A_d are the coefficients of polynomials forming a $\mathbb{Q}$-basis for I_d; we may take these polynomials to be monomial multiples of the generators f_i, so all entries of A_d have absolute value at most C.

Let the submatrix of A_d indexed by the first $H(d)$ columns be denoted by M_d. Note that M_d has full rank; if not, since A_d has rank $H(d)$, there would be a vector in the row-space of A_d with its first $H(d)$ entries zero, and thus there would be a nonzero polynomial f in I_d for which $\mathrm{in}_\prec(\mathrm{in}_w(f))$ does not lie in $\mathrm{in}_\prec(\mathrm{in}_w(I))$, which is a contradiction.

Set $B_d = M_d^{-1} A_d$. Note that the first $H(d)$ columns of B_d are an identity matrix, so the minor $\det((B_d)_J)$ of B_d indexed by the set $J := (\{1, \ldots, H(d)\} \cup \{j\}) \backslash \{i\}$ equals $(-1)^{H(d)-i}(B_d)_{ij}$. Since $(B_d)_J = M_d^{-1}(A_d)_J$,

$$\begin{aligned} \mathrm{val}((B_d)_{ij}) &= \mathrm{val}(\det((B_d)_J)) \\ &= \mathrm{val}(\det(M_d^{-1}(A_d)_J)) \\ &= -\mathrm{val}(\det(M_d)) + \mathrm{val}(\det((A_d)_J)). \end{aligned}$$

Hadamard's inequality (see for example [Gar07, Corollary 14.2.1]) states that if M is an $N \times N$ matrix with the absolute value of the entries bounded by C, then $|\det(M)| \leq C^N N^{N/2}$. Thus $|\det((A_d)_J)| \leq C^{H(d)} H(d)^{H(d)/2}$. Since $\det(A_d)_J$ is an integer, $\mathrm{val}(\det((A_d)_J) \leq \log_p(|\det((A_d)_J)|)$. By construction all entries of M_d have nonnegative valuation, so $\mathrm{val}(\det(M_d)) \geq 0$. Thus,

$$\mathrm{val}((B_d)_{ij})) \leq \log_p(C^{H(d)} H(d)^{H(d)/2}) = H(d)/2 \log_p(C^2 H(d)).$$

By Theorem 3.1 there is a Gröbner basis $\{g_1, \ldots, g_s\}$ for I with respect to w with $\deg(g_i) \leq D$, which can be chosen so $\{\mathrm{in}_w(g_1), \ldots, \mathrm{in}_w(g_s)\}$ is a Gröbner basis for $\mathrm{in}_w(I)$ with respect to $\prec$. The construction of the matrix B_d guarantees that if g_i has degree d, then the coefficients of g_i form a row of the matrix B_d. This follows from the fact that there is a unique homogeneous polynomial f in I with $\mathrm{in}_\prec(\mathrm{in}_w(f))$ equal to a prescribed monomial x^u with the property that the coefficient of x^u in f is one, and no other term of f lies in $\mathrm{in}_\prec(\mathrm{in}_w(I))$. Thus the valuation of the coefficients of g_i is bounded as above. Since $H(d)$ is an increasing function of d, the bound is largest when $d = D$, so $H(d) = A$, from which we see that the valuations of any of the coefficients of any g_i is bounded by $A/2 \log_p(C^2 A)$ as required. □

4. Implementation issues

We focus on $K = \mathbb{Q}$ with the p-adic valuation. This has been implemented as a package in `Macaulay2` [AJC13]. As is common for Gröbner algorithms with coefficients in $\mathbb{Q}$, a major issue in practical implementations is coefficient blow-up. We found examples where coefficients became so large that computations would not terminate within the memory space limitations. Thus it was necessary to consider ways to improve the speed and efficiency of the algorithms, the two main ways of which are:

(1) using criteria to decide a priori that certain S-polynomials reduce to zero;
(2) working over $\mathbb{Z}/p^m\mathbb{Z}$ for some suitably large $m \in \mathbb{N}$.

4.1. **Choice of S-polynomials—Buchberger's criteria.** Suppose we are at some intermediate stage of the Buchberger algorithm where we have a set $\mathcal{P}$ of critical pairs still to consider and we are about to compute the S-polynomial of the pair (f_i, f_j). Then

- **B1:** holds if $\operatorname{lcm}(\operatorname{lm}(f_i), \operatorname{lm}(f_j)) = \operatorname{lm}(f_i)\operatorname{lm}(f_j)$;
- **B2:** holds if there exists some $k \neq i, j$ such that the pairs (f_i, f_k) and (f_j, f_k) are not in $\mathcal{P}$ and $\operatorname{lm}(f_k)$ divides $\operatorname{lcm}(\operatorname{lm}(f_i), \operatorname{lm}(f_j))$.

From the work of Buchberger [Buc79] for usual Gröbner bases, if either of these conditions hold then we know a priori that the S-polynomial reduces to zero. The proof can be found for example in [CLO07]: the proof for 4.1 is Proposition 4, and the proof for 4.1 is Proposition 10 of [CLO07, §2.9]. The first proof follows through verbatim in this situation, while the second requires the same modifications as in the proof of Algorithm 2.9. We illustrate the usefulness of the criteria with an example.

Example 4.1. Let $K = \mathbb{Q}$ with the 2-adic valuation and let S be the polynomial ring $\mathbb{Q}[x_1, \ldots, x_9]$. Let I be the ideal generated by polynomials $\{-3x_1x_4 + 6x_3x_4 + 3x_1x_5 + 92x_2x_5 + 2x_3x_5 - 23x_2x_6 - 2x_3x_6, x_1x_8 + 7x_2x_8 - 4x_3x_8 - 6x_1x_9 - 3x_2x_9, x_4x_8 + 3x_5x_8 - 3x_6x_8 - 24x_5x_9 - 3x_6x_9, -x_2x_4 - 4x_3x_4 + x_2x_5 + 4x_3x_5 + 23x_2x_6 + 2x_3x_6, -13x_1x_7 - 4x_3x_7 + 7x_2x_8 + 28x_3x_8 - 65x_1x_9 - 3x_2x_9 - 32x_3x_9, x_4x_7 + 27x_5x_7 - 9x_6x_8 + 5x_4x_9 + 135x_5x_9 - 9x_6x_9, -4x_2x_5 - 16x_3x_5 + 3x_1x_6 + x_2x_6 - 2x_3x_6, 13x_2x_7 - 8x_3x_7 + x_2x_8 + 4x_3x_8 + 59x_2x_9 - 64x_3x_9, 8x_5x_7 + x_6x_7 - 3x_6x_8 + 40x_5x_9 + 5x_6x_9, 4x_2x_5x_8 + 16x_3x_5x_8 + 20x_2x_6x_8 - 10x_3x_6x_8 - 24x_2x_5x_9 - 96x_3x_5x_9 - 3x_2x_6x_9 - 12x_3x_6x_9\}$. This is the general fiber of a Mustafin variety in the sense of [CHSW11]. Its special fiber is the initial ideal with respect to $w = 0$.

At some intermediate step of the Buchberger algorithm (Algorithm 2.9) we compute the normal form of the S-polynomial $6x_3x_4x_6x_7 + 3x_1x_5x_6x_7 + 24x_1x_4x_5x_7 + 92x_2x_5x_6x_7 + 2x_3x_5x_6x_7 - 23x_2x_6^2x_7 - 2x_3x_6^2x_7 - 9x_1x_4x_6x_8 + 120x_1x_4x_5x_9 + 15x_1x_4x_6x_9$ of the polynomials $-3x_1x_4 + 6x_3x_4 + 3x_1x_5 + 92x_2x_5 + 2x_3x_5 - 23x_2x_6 - 2x_3x_6$ and $x_6x_7 + 8x_5x_7 - 3x_6x_8 + 40x_5x_9 + 5x_6x_9$. Notice that the condition B1 holds, so we know a priori that this S-polynomial will reduce to zero, however, when we try to compute the normal form, after a few divisions we obtain a leading coefficient of $1.02624\cdots \times 10^{37,746}$ and after a few more divisions we have exceeded the memory capabilities of the computer.

By implementing Buchberger's criterion B1, the algorithm no longer considers this critical pair and we compute the Gröbner basis to be $\{3x_1x_4 - 6x_3x_4 - 3x_1x_5 - 92x_2x_5 - 2x_3x_5 + 23x_2x_6 + 2x_3x_6, x_1x_8 + 7x_2x_8 - 4x_3x_8 - 6x_1x_9 - 3x_2x_9, x_4x_8 + 3x_5x_8 - 3x_6x_8 - 24x_5x_9 - 3x_6x_9, x_2x_4 + 4x_3x_4 - x_2x_5 - 4x_3x_5 - 23x_2x_6 - 2x_3x_6, 13x_1x_7 + 4x_3x_7 - 7x_2x_8 - 28x_3x_8 + 65x_1x_9 + 3x_2x_9 + 32x_3x_9, x_4x_7 + 27x_5x_7 - 9x_6x_8 + 5x_4x_9 + 135x_5x_9 - 9x_6x_9, -4x_2x_5 - 16x_3x_5 + 3x_1x_6 + x_2x_6 - 2x_3x_6, 13x_2x_7 - 8x_3x_7 + x_2x_8 + 4x_3x_8 + 59x_2x_9 - 64x_3x_9, 8x_5x_7 - 3x_6x_8 + 40x_5x_9 + 5x_6x_9 + x_6x_7, -4x_2x_5x_8 - 16x_3x_5x_8 - 20x_2x_6x_8 + 10x_3x_6x_8 + 24x_2x_5x_9 + 3x_2x_6x_9 + 96x_3x_5x_9 + 12x_3x_6x_9\}$.

4.2. **Working over $\mathbb{Z}/p^m\mathbb{Z}$.** While it is sometimes unavoidable to get large coefficients when computing a Gröbner basis over $\mathbb{Q}$, these coefficients do not always have large p-adic valuation. This motivates working in $\mathbb{Z}/p^m\mathbb{Z}$ via the method suggested in Remark 2.8.

This requires the following standard subroutine, which details how to compute a Gröbner basis for I given generators for $\operatorname{in}_\prec(\operatorname{in}_w(I))$. This is the usual linear

algebra for reconstructing Gröbner bases as in the nonvaluation case; we include it for completeness.

Algorithm 4.2. Input: Homogeneous generators $\{f_1, \dots, f_l\}$ for an ideal $I \subseteq \mathbb{Q}[x_1, \dots, x_n]$. A weight vector $w \in \mathbb{R}^n$ and a term order $\prec$. Generators $\mathcal{I} = \{x^{u_1}, \dots, x^{u_s}\}$ for $\mathrm{in}_\prec(\mathrm{in}_w(I))$.
Output: A reduced Gröbner basis for I with respect to w and $\prec$.

(1) $\mathcal{G} = \emptyset$.
(2) For each degree d of a monomial $x^{u_i} \in \mathcal{I}$ do:
   (a) Let $h = \dim_{\mathbb{Q}} I_d$. Form the $h \times \binom{n+d-1}{d}$ matrix A_d whose rows are the coefficients of a $\mathbb{Q}$-basis for I_d. The columns of A_d are indexed by the monomials of degree d, and we assume that the monomials in $\mathrm{in}_\prec(\mathrm{in}_w(I))_d$ come first in the ordering. The rows can be taken to be monomial multiples of the f_i.
   (b) Let B_d be the result of multiplying A_d by the inverse of the first $h \times h$ submatrix of A_d. This submatrix is invertible by the argument of the proof of Proposition 3.3.
   (c) For each $x^{u_i} \in \mathcal{I}$ of degree d, let g_i be the polynomial corresponding to the row of B_d that contains a 1 in the column corresponding to x^{u_i}. Add g_i to $\mathcal{G}$.
(3) Output $\mathcal{G}$.

Proof of correctness of Algorithm 4.2. The chosen polynomials have the property that no monomial other than x^{u_i} lies in $\mathrm{in}_\prec(\mathrm{in}_w(I))$, so $\mathrm{in}_\prec(\mathrm{in}_w(g_i)) = x^{u_i}$. Thus the initial ideal $\mathrm{in}_\prec(\mathrm{in}_w(I))$ equals $\langle \mathrm{in}_\prec(\mathrm{in}_w(g_1)), \dots, \mathrm{in}_\prec(\mathrm{in}_w(g_r))\rangle$, so the output is a reduced Gröbner basis as required. □

We incorporate this into the following algorithm, which computes a Gröbner basis modulo p^m for large m.

Algorithm 4.3.
Input: A list $\{f_1, \dots, f_l\}$ of homogeneous polynomials in $\mathbb{Q}[x_1, \dots, x_n]$, a prime p, a weight-vector $w \in \mathbb{R}^n$, and a term order $\prec$.
Output: A Gröbner basis for $\langle f_1, \dots, f_l\rangle$.

(1) Let $I = \langle f_1, \dots, f_l\rangle$. Let $f_i^w = f_i(p^{w_1}x_1, \dots, p^{w_n}x_n)$ for $1 \le i \le l$. Clear denominators in the f_i^w, and saturate the resulting ideal in $\mathbb{Z}[x_1, \dots, x_n]$ by $\langle p\rangle$. Let $\tilde{I}_w$ be the image of this ideal in $\mathbb{Z}/p^m\mathbb{Z}[x_1, \dots, x_n]$.
(2) Compute $\mathrm{in}_\prec(\mathrm{in}_0(\tilde{I}_w))$ using Algorithm 2.9.
(3) Lift the resulting initial ideal to a Gröbner basis for I using Algorithm 4.2.

Note that the fact that Algorithm 2.9 does compute $\mathrm{in}_\prec(\mathrm{in}_0(\tilde{I}_w))$ follows from Remark 2.8. The following lemma shows that for m sufficiently large this initial ideal equals $\mathrm{in}_\prec(\mathrm{in}_w(I))$, so Algorithm 4.2 will terminate with the correct answer.

Lemma 4.4. *For $m \gg 0$ Algorithm* 4.3 *terminates with the correct answer.*

Proof. We first show that for $m \gg 0$ we have $\mathrm{in}_\prec(\mathrm{in}_0(\tilde{I}_w)) = \mathrm{in}_\prec(\mathrm{in}_w(I))$. Note that if $f = \sum c_u x^u$ with $c_u \in \mathbb{Z}$ with $\mathrm{val}(c_u) < m$, then the image $\tilde{f}$ of f in $\mathbb{Z}/p^m\mathbb{Z}[x_1, \dots, x_n]$ satisfies $\mathrm{in}_\prec(\mathrm{in}_0(\tilde{f})) = \mathrm{in}_\prec(\mathrm{in}_0(f))$. Let $I_w = \langle f_i^w : 1 \le i \le l\rangle \subseteq \mathbb{Q}[x_1, \dots, x_n]$, so $\mathrm{in}_w(I) = \mathrm{in}_0(I_w)$. By Proposition 3.3 there is a bound in terms of the absolute value of the coefficients of the generators of I on the maximum

valuation that occurs in a reduced Gröbner basis. For m larger than this bound we have $\text{in}_\prec(\text{in}_w(I)) \subseteq \text{in}_\prec(\text{in}_0(\tilde{I}_w))$.

For the reverse inclusion, fix $x^u \in \text{in}_\prec(\text{in}_0(\tilde{I}_w))$. Choose $f \in \tilde{I}_w$ with $\text{in}_\prec(\text{in}_w(f)) = x^u$. By the definition of $\tilde{I}_w$ there is $g \in I_w$ with $f = \tilde{g}$. By construction $\text{in}_0(g) = \text{in}_0(f)$, so $x^u = \text{in}_\prec(\text{in}_0(g)) \in \text{in}_\prec(\text{in}_0(I_w)) = \text{in}_\prec(\text{in}_w(I))$.

In the first step of the algorithm, note that generators of the ideal obtained by clearing denominators and saturating by $\langle p \rangle$ generate $I_w \cap \mathbb{Z}_{\langle p \rangle}[x_1, \ldots, x_n]$. Since the image of an ideal $J \subset \mathbb{Z}[x_1, \ldots, x_n]$ in $\mathbb{Z}/p^m\mathbb{Z}[x_1, \ldots, x_n]$ equals the ideal obtained by first taking the image of J in $\mathbb{Z}_{\langle p \rangle}[x_1, \ldots, x_n]$ and then taking the image in $\mathbb{Z}/p^m\mathbb{Z}[x_1, \ldots, x_n]$ (using that $\mathbb{Z}_{\langle p \rangle}/\langle p^m \rangle \cong \mathbb{Z}/p^m\mathbb{Z}$), $\tilde{I}_w$ is the image of $I_w \cap \mathbb{Z}[x_1, \ldots, x_n]$ in $\mathbb{Z}/p^m\mathbb{Z}[x_1, \ldots, x_n]$. The second step computes $\text{in}_\prec(\text{in}_0(\tilde{I}_w))$ by Remark 2.8. The equality $\text{in}_\prec(\text{in}_0(\tilde{I}_w)) = \text{in}_\prec(\text{in}_w(I))$ then guarantees that we have the correct input for Algorithm 4.2, so the algorithm terminates correctly. □

The bound on m to guarantee that we are in the situation given in Proposition 3.3, may be ridiculously large, and not tight. If instead one uses an ad hoc choice for m, step (3) of Algorithm 4.3 will fail if the bound chosen was too low. We can thus iterate, repeating the computation with a larger value of m. This seems often to be the best choice in practice.

5. Cardinality

In this section we give an example which shows that a p-adic Gröbner basis may be significantly smaller than any standard Gröbner basis. This gives another motivation to study such Gröbner bases.

Recall that a monomial ideal M is strongly stable, or Borel fixed, if for all $x^u \in M$ with $u_j > 0$ and $i < j$ we have $x_i/x_j x^u \in M$. Our construction requires a special case of the following elementary lemma.

Lemma 5.1. *Fix degrees $d_1, \ldots, d_l$, and let $\mathbb{P} = \prod_{i=1}^{l} \mathbb{P}^{\binom{d_i+n-1}{d_i}-1}$ be the parameter space for sequences of homogeneous polynomials $f_1, \ldots, f_l \subset K[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_l$, where K has characteristic zero. Then there is a Zariski open set $U \subseteq \mathbb{P}$ for which, if $p \in U$, then the ideal $I = \langle f_1, \ldots, f_l \rangle$ generated by the polynomials corresponding to p has the property that $\text{in}_\prec(I)$ is strongly stable for all term orders $\prec$. There are points in U with any prescribed valuations.*

Proof. Fix a term order $\prec$. Note that $G = \text{PGL}(n, K)$ acts on $\mathbb{P}$ by change of coordinates on each factor. There is a nonempty open set $V \subset G \times \mathbb{P}$ for which $\text{in}_\prec(gI)$ is constant for all $(g, p) \in V$. Denote this initial ideal by $M_\prec$. The existence of this open set V follows from the theory of comprehensive Gröbner bases [Wei92]. For a fixed $p \in \mathbb{P}$, there is an open set $V' \subset G$ for which the initial ideal $\text{in}_\prec(gI)$ equals the generic initial ideal $\text{gin}_\prec(I)$, which is strongly stable; see for example [Eis95, Theorem 15.23]. By considering any $p \in \mathbb{P}$ for which there is some $g \in G$ with $(g, p) \in V$, we see that the initial ideal $M_\prec$ is strongly stable.

Since V is open in $G \times \mathbb{P}$, the set $U_\prec = \{p \in \mathbb{P} : (\text{id}, p) \in V\}$ is open in $\mathbb{P}$, and $\text{in}_\prec(I) = M_\prec$ for all $p \in U_\prec$. The group G acts on $G \times \mathbb{P}$ by $h \cdot (g, p) = (gh^{-1}, hp)$. Note that the set $V \subset G \times \mathbb{P}$ is invariant under this action. This means that the set $U_\prec$ is nonempty, as given any $(g, p) \in V$, we also have $(\text{id}, g^{-1}p) \in V$. If $M_\prec = M_{\prec'}$ for two different term orders $\prec, \prec'$, then we can take $U_\prec = U_{\prec'}$, as the two term orders agree on the initial terms of a reduced Gröbner basis of any $I = I(p)$ with

$p \in U_\prec$. The first part of the lemma then follows from the observation that the Hilbert functions of all initial ideals $M_\prec$ agree and there are only a finite number of strongly stable ideals with a given Hilbert function, so there are only a finite number of open sets $U_\prec$ to intersect to obtain an open set $U \subset \mathbb{P}$ with $\text{in}_\prec(I)$ strongly stable for any $p \in U$ and any term order $\prec$.

Since $U \subset \mathbb{P}$ is open, so is its intersection with an affine chart $\mathbb{A}^{\sum_{i=1}^{l}\binom{d_i+n-1}{d_i}-l}$. Let $N = \sum_{i=1}^{l}\binom{d_i+n-1}{d_i} - l$. This open set contains the complement of a hypersurface $V(f)$, where $f \in K[x_1, \ldots, x_N]$. We now show by induction on N that the valuations of a point outside $V(f)$ can be prescribed. When $N = 1$, $V(f)$ is a finite set, so the base case follows from the fact that there are infinitely many elements of K with a given valuation. Now assume that the claim is true for smaller N, and write $f = gx_1^m +$ lower order terms, where $g \in K[x_2, \ldots, x_N]$. Then by induction there is $x' = (x_2, \ldots, x_N)$ with $g(x') \neq 0$ and with $\text{val}(x')$ prescribed. By the base case there is x_1 with prescribed valuation for which the univariate polynomial $f(x_1, x')$ is nonzero. Then $(x_1, x') \in U$ is the desired point. □

The other ingredient needed for the construction is the notion of a Stanley decomposition for a monomial ideal $M \subseteq K[x_1, \ldots, x_n]$. For $\sigma \subseteq \{1, \ldots, n\}$ and a monomial x^u we denote by (x^u, σ) the set of monomials $\{x^{u+v} : v_i = 0 \text{ for } i \notin \sigma\}$. A Stanley decomposition for M is a union $\{(x^{u_i}, \sigma_i) : 1 \leq i \leq s\}$ such that every monomial in M lies in a unique set (x^{u_i}, σ_i). The key fact about Stanley decompositions is that the Hilbert function $\dim_K I_t$ of I is the sum $\sum_{i=1}^{s}\binom{t-|u_i|+|\sigma_i|-1}{|\sigma_i|}$.

Theorem 5.2. *Fix an even integer $d = 2e$. Let $I = \langle f, g\rangle \subseteq \mathbb{Q}[x_1, x_2, x_3]$ be two generic polynomials of degree d where every coefficient of f except x_1^d and every coefficient of g except $x_2^e x_3^e$ has positive 2-adic valuation, and the remaining two coefficients have valuation zero. Then $\text{in}_0(I) = \langle x_1^d, x_2^e x_3^e\rangle$ with the 2-adic valuation, but any standard initial ideal $\text{in}_\prec(I)$ has at least $1/2(d+3)$ generators.*

Proof. Note first that the existence of f, g satisfying these conditions follows from Lemma 5.1, from which it also follows that every standard initial ideal $\text{in}_\prec(I)$ is Borel-fixed. That $\{f, g\}$ is a 2-adic Gröbner basis for I with respect to $w = 0$ follows from Buchberger's criterion B1.

Fix a term order $\prec$, and let $\text{in}_\prec(I) = \langle x^{u_1}, \ldots, x^{u_s}\rangle$. Write $\{1, 2, 3\} = \{i_1, i_2, i_3\}$ so that $x_{i_1} \succ x_{i_2} \succ x_{i_3}$. For $u \in \mathbb{N}^3$, denote by $m(u)$ the index $m(u) = \max(j : u_{i_j} \neq 0) \in \{1, 2, 3\}$. Since $\text{in}_\prec(I)$ is Borel-fixed, the decomposition

$$\{(x^{u_i}, \{i_{m(u_i)}, \ldots, i_3\}) : 1 \leq i \leq s\}$$

is a Stanley decomposition for $\text{in}_\prec(I)$. This means that

$$\dim_{\mathbb{Q}}(\text{in}_\prec(I)_t) = \sum_{i=1}^{s}\binom{t-|u_i|+3-m(u_i)}{3-m(u_i)}.$$

Without loss of generality, we may assume that $x^{u_1} = x_{i_1}^d$, and $m(u_i) \geq 2$ for $i \geq 2$. Since I is generated in degree d, $|u_i| \geq d$ for all i. Since the Hilbert function of I and any initial ideal (standard or 2-adic) agree, the fact that the 2-adic initial ideal of I is $\langle x_1^d, x_2^e x_3^e\rangle$ implies that $\dim_{\mathbb{Q}}(I_t) = 2\binom{t-d+2}{2}$ for $d \leq t < 2d$. Thus for

$d \leq t < 2d$ we have

$$2\binom{t-d+2}{2} = \sum_{i=1}^{s} \binom{t-|u_i|+3-m(u_i)}{3-m(u_i)} \leq \binom{t-d+2}{2} + (s-1)\binom{t-d+1}{1}$$

so

$$1/2(t-d+2)(t-d+1) \leq (s-1)(t-d+1).$$

This means that $s \geq 1/2(d+3)$, as required. □

Acknowledgments

We thank Spencer Backman and Anders Jensen for comments on an earlier draft of this paper.

References

[BPR16] M. Baker, S. Payne, and J. Rabinoff, *Nonarchimedean geometry, tropicalization, and metrics on curves*, Algebr. Geom. **3** (2016), no. 1, 63–105, DOI 10.14231/AG-2016-004. MR3455421

[Buc79] B. Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner-bases*, Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin-New York, 1979, pp. 3–21. MR575678

[CHSW11] D. Cartwright, M. Häbich, B. Sturmfels, and A. Werner, *Mustafin varieties*, Selecta Math. (N.S.) **17** (2011), no. 4, 757–793, DOI 10.1007/s00029-011-0075-x. MR2861606

[AJC13] Andrew J. Chan, *GrobnerValuations*, 2013. A Macaulay 2 package available at `http://homepages.warwick.ac.uk/staff/D.Maclagan/papers/GrobnerValuations.m2`.

[CLO07] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*: *An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd ed., Undergraduate Texts in Mathematics, Springer, New York, 2007. MR2290010

[CLO05] D. A. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, 2nd ed., Graduate Texts in Mathematics, vol. 185, Springer, New York, 2005. MR2122859

[Dub90] T. W. Dubé, *The structure of polynomial ideals and Gröbner bases*, SIAM J. Comput. **19** (1990), no. 4, 750–775, DOI 10.1137/0219053. MR1053942

[Eis95] D. Eisenbud, *Commutative Algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995. With a view toward algebraic geometry. MR1322960

[Gar07] D. J. H. Garling, *Inequalities: A Journey into Linear Analysis*, Cambridge University Press, Cambridge, 2007. MR2343341

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

[GP08] G.-M. Greuel and G. Pfister, *A Singular Introduction to Commutative Algebra*, Second, extended edition, Springer, Berlin, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann; With 1 CD-ROM (Windows, Macintosh and UNIX). MR2363237

[Jen] A. N. Jensen, *Gfan, a software system for Gröbner fans and tropical varieties*, Available at `http://home.imf.au.dk/jensen/software/gfan/gfan.html`.

[MS15] D. Maclagan and B. Sturmfels, *Introduction to Tropical Geometry*, Graduate Studies in Mathematics, vol. 161, American Mathematical Society, Providence, RI, 2015. MR3287221

[MR16] T. Markwig and Y. Ren, *Computing tropical varieties over fields with valuation*, 2016. arXiv:1612.01762.

[MM84] H. M. Möller and F. Mora, *Upper and Lower Bounds for the Degree of Groebner Bases*, EUROSAM 84 (Cambridge, 1984), Lecture Notes in Comput. Sci., vol. 174, Springer, Berlin, 1984, pp. 172–183, DOI 10.1007/BFb0032840. MR779124

[Spe05] D. E. Speyer, *Tropical Geometry*, ProQuest LLC, Ann Arbor, MI, 2005. Thesis (Ph.D.)–University of California, Berkeley. MR2707751

[Wei92] V. Weispfenning, *Comprehensive Gröbner bases*, J. Symbolic Comput. **14** (1992), no. 1, 1–29, DOI 10.1016/0747-7171(92)90023-W. MR1177987

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
Email address: andrew.john.chan@gmail.com

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
Email address: D.Maclagan@warwick.ac.uk