arXiv:1802.10139v2 [math.AC] 7 Jan 2019

STILLMAN'S CONJECTURE VIA GENERIC INITIAL IDEALS

JAN DRAISMA AND MICHAŁ LASOŃ AND ANTON LEYKIN

ABSTRACT. Using recent work by Erman-Sam-Snowden, we show that finitely generated ideals in the ring of bounded-degree formal power series in infinitely many variables have finitely generated Gröbner bases relative to the graded reverse lexicographic order. We then combine this result with the first author's work on topological Noetherianity of polynomial functors to give an algorithmic proof of the following statement: ideals in polynomial rings generated by a fixed number of homogeneous polynomials of fixed degrees only have a finite number of possible generic initial ideals, independently of the number of variables that they involve and independently of the characteristic of the ground field. Our algorithm outputs not only a finite list of possible generic initial ideals, but also finite descriptions of the corresponding strata in the space of coefficients.

1. INTRODUCTION

Grevlex series and Gröbner bases. Let A be a ring and let R_A be the A-algebra of formal power series over A of bounded degree in the infinitely many variables $x_1, x_2, \ldots$. In other words, each element of R_A is a formal infinite sum

$$\sum_{\alpha \in \mathbb{N}^{\mathbb{Z}_{\geq 0}}, |\alpha| \leq d} c_\alpha x^\alpha$$

where d is some nonnegative integer and $c_\alpha \in A$ for each sequence $\alpha = (\alpha_1, \alpha_2, \ldots)$ of nonnegative integers whose sum $|\alpha|$ is (finite and) at most d. Addition and multiplication are as usual.

We equip the polynomial ring R_A with the graded reverse lexicographic order grevlex, in which $x^\alpha > x^\beta$ if either $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the last non-zero entry of $\alpha - \beta$ is negative. So, for instance, the monomials of degree 3 are ordered as follows:

$$x_1^3 > x_1^2x_2 > x_1x_2^2 > x_2^3 > x_1^2x_3 > x_1x_2x_3 > x_2^2x_3 > x_1x_3^2 > x_2x_3^2 > x_3^3 > x_1^2x_4 > \ldots$$

To remind the reader that this is the only monomial order considered in this paper, we call the elements of R_A *grevlex series* over A. If f is a nonzero element of R, then $\mathrm{lm}(f)$ denotes the largest monomial that has a nonzero coefficient in f, $\mathrm{lc}(f)$ denotes that coefficient, and $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lm}(f)$ is the leading term. The ring R_A carries a unique topology in which a basis of open neighborhoods of $f \in R_A$ is given by all sets $\{g \in R_A \mid \mathrm{lm}(f - g) < x^\alpha\}$ as α varies.

Let L be a field. A *Gröbner basis* of an ideal $I \subseteq R_L$ is a subset $B \subseteq I$ such that for each $h \in L$ there exists an $f \in B$ with $\mathrm{lm}(f)|\mathrm{lm}(h)$. We do not require that B be finite. As in the classical setting, a Gröbner basis B of I generates I as an ideal (Lemma 7). Our first main result is the following.

JD is partially supported by a Vici grant from the Netherlands Organisation for Scientific Research (NWO).

Research of AL is supported in part by DMS-1719968 award from NSF.

Theorem 1. *For every field L, every finitely generated homogeneous ideal in the ring R_L has a finite Gröbner basis with respect to grevlex.*

The analogous statement certainly does not hold for all monomial orders: in [Sne98a, Appendix A.2] it is shown that the ideal generated by a generic quadric and a generic cubic has a non-finitely generated initial ideal relative to the lexicographic order. Theorem 1 implies a positive answer to [Sne98b, Question 7.1]; in that paper a positive answer is given in the case where the ideal is generated by series $\sum_{|\alpha|=d_i} c_{i,\alpha}x^\alpha,\ i = 1,\ldots,k$ whose coefficients $(c_{i,\alpha})_{i\in[k],|\alpha|=d_i}$ are algebraically independent over the prime field of L.

The natural question arises whether a Gröbner basis as in the theorem can be computed in finite time. A straightforward variant SeriesBuchberger of Buchberger's algorithm shows that this would, indeed, be the case—*if only we could work effectively with infinite series*.

Next we focus on the following setting where we can indeed work with such series. Let $S_\infty = \bigcup_n S_n$ be the union of all symmetric groups, and let $S_{>n}$ be the subgroup of all permutations fixing $1,\ldots,n$ elementwise. Suppose that we are given an action of $S_{>n_0}$ on A by means of ring automorphisms, and let $S_{>n_0}$ act on the variables $x_1, x_2, \ldots$ via $\pi x_i = x_{\pi(i)}$. This action extends to an action of $S_{>n_0}$ by (continuous) ring automorphisms on R_A via

$$\pi\left(\sum_\alpha c_\alpha x^\alpha\right) = \pi\left(\sum_\alpha c_\alpha \prod_i x_i^{\alpha_i}\right) = \sum_\alpha \pi(c_\alpha)\prod_i x_{\pi(i)}^{\alpha_i} = \sum_\alpha \pi(c_\alpha)x^{\alpha\circ\pi^{-1}}.$$

We call an $f \in R_A$ *eventually invariant* if there exists an $n \geq n_0$ such that $\pi(f) = f$ for all $\pi \in S_{>n}$. To specify an eventually invariant grevlex series we need only a finite number of coefficients: if f is invariant under $S_{>n}$ and has degree d, then $S_{>n}$ has only finitely many orbits on monomials in $x_1, x_2, \ldots$ of degree at most d—the grevlex-largest element in each orbit is of the form x^α where $\alpha(n+1) \geq \alpha(n+2) \geq \ldots$. Then f is uniquely determined by its coefficients on these grevlex-largest representatives $x^{\alpha_1}, \ldots, x^{\alpha_s}$. We call $\hat{f} := \sum_{i=1}^s c_{\alpha_i}x^{\alpha_i}$ the *n-representation* of $f = \sum_\alpha c_\alpha x^\alpha$. Often we will suppress n from this notation.

Theorem 2. *Suppose that $A = L$ is a field. There exist a finite algorithm that on input a finite list $\hat{f}_1, \ldots, \hat{f}_k$ of representations of eventually invariant grevlex series $f_1, \ldots, f_k$ outputs a finite list $\hat{g}_1, \ldots, \hat{g}_l$ representing an eventually invariant Gröbner basis $g_1, \ldots, g_l$ of $\langle f_1, \ldots, f_k\rangle_{R_L}$.*

Stillman's conjecture. The condition of eventual invariance seems rather restrictive, but it is tailored to a proof of the following theorem.

Theorem 3. *There exists a finite algorithm that on input $k \in \mathbb{Z}$ and $d_1, \ldots, d_k \in \mathbb{Z}_{\geq 0}$ outputs a finite sequence $S_1, \ldots, S_t$, each S_i a finite set of monomials in the x_j, such that the following holds: For every infinite field K, all $n \in \mathbb{N}$, and all homogeneous polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_k$, respectively, the generic grevlex initial ideal of $\langle f_1, \ldots, f_k\rangle_{K[x_1,\ldots,x_n]}$ equals $\langle S_i\rangle_{K[x_1,\ldots,x_n]}$ for some i.*

In short: ideals in polynomial rings generated by homogeneous polynomials of degrees $d_1, \ldots, d_k$ have only finitely many possible generic grevlex initial ideals, independently of the number of variables. Via [Eis95, Corollary 19.11], which is based on [BS87], this implies that the projective dimension of an ideal generated by homogeneous forms of fixed degrees but in an arbitrary number of variables and in arbitrary characteristic is uniformly bounded. This is Stillman's conjecture from the title; see [PS09].

This is the fourth proof of Stillman's conjecture, after the first proof by Ananyan-Hochster [AH16] and two recent proofs by Erman-Sam-Snowden [ESS18]. Our proof is the same in spirit as the second proof in the latter paper in that it uses Draisma's theorem on topological Noetherianity of polynomial functors [Dra17]. However, unlike the second proof in [ESS18] (but like the first proof there, and like Ananyan-Hochster's proof), our theorem yields $S_1, \dots, S_t$ that are valid in all characteristics. Also, our theorem is constructive in the sense that we give an algorithm for computing the possible initial ideals and the corresponding strata given by equations and disequations for field characteristics and coefficients of the input series. All these are represented finitely.

In [ESS18] the authors raise the question whether a version over $\mathbb{Z}$ of Draisma's theorem holds, as this would also make their second proof characteristic-independent. We do not settle this question. Instead, the algorithm of Theorem 3 simulates a generic ideal computation in all characteristics, branching along constructible subsets of $\operatorname{Spec}\mathbb{Z}$ whenever necessary. We argue that, if there were an infinite branch in this computation, then this branch would also be infinite over some field; and that this would contradict Draisma's theorem over that field.

In [ESS17] (see also [DES17, Theorem 1.9]), using Stillman's conjecture and Draisma's theorem, the same authors establish a generalization of Stillman's conjecture to ideal invariants that are upper semicontinuous in flat families and preserved under adding a variable to the polynomial ring. We have not pursued the question to what extent (an algorithmic version of) this generalisation also follows from our Theorem 3.

Organization. This paper is organized as follows. In Section 2 we prove Theorem 1 using work from [ESS18]. In Section 3 we use this existence result to prove that a version of Buchberger's algorithm for eventually invariant series terminates; this yields Theorem 2. In Section 4 we review topological Noetherianity of a specific polynomial functor, which follows from [Dra17]. Finally, in Section 5 we derive Theorem 3 from Theorem 2 and Draisma's theorem.

2. The existence of finite Gröbner bases

We will use two results from [ESS18], the first of which is the following.

Theorem 4 (Theorem 1.2 from [ESS18]). *If L is perfect, then R_L contains an (uncountable) set of homogeneous elements $\{g_j : j \in J\}$ such that the unique L-algebra homomorphism $L[(x_j)_{j\in J}] \to R_L$ sending x_j to g_j is an L-algebra isomorphism.*

For each $n \in \mathbb{Z}_{\geq 0}$ we write $R_L^{(n)} := L[x_1, \dots, x_n]$. There is a natural L-algebra homomorphism $R_L \to R_L^{(n)}, f \mapsto f^{(n)}$ that retains only the terms involving only the variables $x_1, \dots, x_n$. We may think of a degree-at-most-d element of R_L as a sequence $(f^{(0)}, f^{(1)}, \dots)$ in which each $f^{(n)}$ is a polynomial in $R_L^{(n)}$ of degree at most d such that $f^{(n)}$ is the image of $f^{(n+1)}$ under discarding all terms divisible by x_{n+1}. Conversely, $R_L^{(n)}$ is an L-subalgebra of R_L. Observe that, for any $f \in R_L$ and $n \in \mathbb{Z}_{\geq 0}$, the image $(\operatorname{lm}(f))^{(n)}$ is either zero or equal to $\operatorname{lm}(f^{(n)})$ in the grevlex order on $L[x_1, \dots, x_n]$.

Theorem 5 (Theorem 5.4 from [ESS18])**.** *A sequence $g_1, \dots, g_l \in R_L$ of homogeneous elements is a regular sequence in R_L if and only if $g_1^{(n)}, \dots, g_l^{(n)}$ is a regular sequence in $R_L^{(n)}$ for all $n \gg 0$.*

The following lemma is straightforward from [ESS18, Section 5], but we include its proof using the two results above.

Lemma 6. *Let $f_1, \dots, f_k \in R_L$. Then the natural map between first syzygies*

$$\mathrm{Syz}_{R_L^{(n+1)}}(f_1^{(n+1)}, \dots, f_k^{(n+1)}) \to \mathrm{Syz}_{R_L^{(n)}}(f_1^{(n)}, \dots, f_k^{(n)})$$

is surjective for all $n \gg 0$.

Proof. This surjectivity is not affected by enlarging the field, so we may assume that L is perfect. By Theorem 4, there exist homogeneous $g_1, \dots, g_l \in R_L$ such that $f_1, \dots, f_k \in L[g_1, \dots, g_l]$ and such that $g_1, \dots, g_l$ are part of a system of variables for the polynomial ring R_L. In particular, they are a regular sequence in R_L, and hence by Theorem 5 the polynomials $g_1^{(n)}, \dots, g_l^{(n)}$ are a regular sequence in $R_L^{(n)}$ for $n \gg 0$. We draw two conclusions from this. First, for $n \gg 0$, $g_1^{(n)}, \dots, g_l^{(n)}$ are algebraically independent over L, $f_1^{(n)}, \dots, f_k^{(n)}$ are elements of the polynomial ring $A^{(n)} := L[g_1^{(n)}, \dots, g_l^{(n)}]$, and

$$\mathrm{Syz}_{A^{(n+1)}}(f_1^{(n+1)}, \dots, f_k^{(n+1)}) \to \mathrm{Syz}_{A^{(n)}}(f_1^{(n)}, \dots, f_k^{(n)})$$

is a bijection. Second, still for $n \gg 0$, $R^{(n)}$ is a free module over $A^{(n)}$. Therefore, $\mathrm{Syz}_{A^{(n)}}(f_1^{(n)}, \dots, f_k^{(n)}) \subseteq (A^{(n)})^k$ generates $\mathrm{Syz}_{R^{(n)}}(f_1^{(n)}, \dots, f_k^{(n)}) \subseteq (R^{(n)})^k$ as an $R^{(n)}$-module. Combining these two statements we find the surjectivity claimed in the lemma. □

Proof of Theorem 1. Let $f_1, \dots, f_k \in R_L$ be nonzero, homogeneous, and let $n \in \mathbb{Z}_{\geq 0}$. Set $I := \langle f_1, \dots, f_k \rangle \subseteq R_L$. Consider a monomial $u \in \mathrm{lm}(I) \cap R^{(n+1)}$ divisible by x_{n+1}. There exist homogeneous $a_1, \dots, a_k \in R^{(n)}$ with $\deg(a_i) = \deg(u) - \deg(f_i)$ and homogeneous $b_1, \dots, b_k \in R^{(n+1)}$ with $\deg(b_i) = deg(u) - deg(f_i) - 1$ such that

$$u = \mathrm{lm}((a_1 + b_1 x_{n+1}) f_1^{(n+1)} + \dots + (a_k + b_k x_{n+1}) f_k^{(n+1)}).$$

Now $(a_1, \dots, a_k) \in \mathrm{Syz}_{R^{(n)}}(f_1^{(n)}, \dots, f_k^{(n)})$—otherwise, the right-hand side would equal $\mathrm{lm}(\sum_i a_i f_i^{(n)})$, which is not divisible by x_{n+1}. By Lemma 6, if $n \gg 0$, the syzygy $(a_1, \dots, a_k)$ can be lifted to a syzygy $(c_1, \dots, c_k) \in \mathrm{Syz}_{R_L^{(n+1)}}(f_1^{(n+1)}, \dots, f_k^{(n+1)})$. Write $c_i = a_i + x_{n+1} b_i'$ for each i. Then

$$u = \mathrm{lm}((b_1 - b_1') x_{n+1} f_1^{(n+1)} + \dots + (b_k - b_k') x_{n+1} f^{(n+1)}),$$

but then we see that $u/x_{n+1} \in \mathrm{lm}(I)$. Hence for $n \gg 0$, $\mathrm{lm}(I)$ does not contain minimal generators divisible by x_{n+1}. It follows that for such an n, $\mathrm{lm}(I)$ is generated by any finite generating list $m_1, \dots, m_t$ of $\mathrm{lm}(I^{(n)})$. Now $h_1, \dots, h_t \in I$ such that $\mathrm{lm}(h_i) = m_i$ form a Gröbner basis of I. □

Buchberger's algorithm for grevlex series

To turn Theorem 1 into an algorithm, we derive a version of Buchberger's algorithm.

Lemma 7 (Division with remainder)**.** *Let $f_1, \ldots, f_k \in R_L$ be monic and $h \in R_L$. Then there exist $q_1, \ldots, q_k \in R_L$ such that $\mathrm{lm}(q_i f_i) \leq \mathrm{lm}(h)$ for all i and such that no term of the remainder $h - \sum_i q_i f_i$ is divisible by any $\mathrm{lm}(f_i)$.*

In particular, if $f_1, \ldots, f_k$ is a Gröbner basis of the ideal that they generate, then the remainder must be zero.

Proof. Initialize $r := h$ and $q_i := 0$ for all i. While some term of r is divisible by some $\mathrm{lm}(f_i)$, pick the grevlex-largest such term cx^α in r, subtract $c(x^\alpha/\mathrm{lm}(f_i))f_i$ from r and add $cx^\alpha/\mathrm{lm}(f_i)$ to q_i. This does not change terms in q_i larger than the term just added, and hence in the product topology on R_L^k the vector q converges a solution vector q as desired. □

---

function SeriesBuchberger($f_1, \ldots, f_k$)
  assume $f_1, \ldots, f_k \in R_L$ homogeneous grevlex series.
  $m := 1$; $B := \emptyset$ (the basis); $Q := \{f_1, \ldots, f_k\}$ (the queue);
  while $Q \neq \emptyset$ **do**
    while Q contains an f with $f^{(m)} \neq 0$ **do**
      $Q := Q \setminus \{f\}$;
      $f := f/\mathrm{lc}(f)$;
      $B := B \cup \{f\}$;
      for $h \in B \setminus \{f\}$ **do**
        $\gamma := \mathrm{lcm}(\mathrm{lm}(h), \mathrm{lm}(f))$;
        $s := (\gamma/\mathrm{lm}(h))h - (\gamma/\mathrm{lm}(f))f$;
        compute a remainder r of s after division by B;
        if $r \neq 0$ **then**
          $Q := Q \cup \{r\}$;
        end if;
      end for;
    end while;
    $m := m + 1$;
  end while;
  return B;
end function

Proposition 8. *Assuming an implementation for addition, multiplication, and division with remainder of grevlex series,* SeriesBuchberger *on page 5 terminates after a finite number of steps and outputs a Gröbner basis of the ideal generated by the series in the input.*

Proof. Fix any natural number n. The loops with m ranging from 1 to n really compute a Gröbner basis for $I := \langle f_1^{(n)}, \ldots, f_k^{(n)} \rangle$ while dragging the tails of the series along. In particular, these n loops terminate. If an element is added to the queue Q in the $(n+1)$st run of the loop, then this implies that $\mathrm{lm}(I) \cap R_L^{(n)}$ does not generate $\mathrm{lm}(I)$. By Theorem 1, this cannot happen infinitely often, so the algorithm terminates. That the output is, indeed, a Gröbner basis, follows from the ordinary Buchberger criterion. □

3. Buchberger's algorithm for eventually invariant series

Recall that $S_{>n_0}$ acts on L, on variables, and on R_L. Given representations $\hat{f_1}, \ldots, \hat{f_k}$ of eventually invariant $f_1, \ldots, f_k \in R_L$, we want to compute the representation of an eventually invariant Gröbner basis of $I := \langle f_1, \ldots, f_k \rangle$.

The first ingredient in our variant of Buchberger's algorithm is an analogue of Lemma 7.

Lemma 9 (Division with remainder on representations.). *Let $f_1, \ldots, f_k \in R_L$ be monic and $h \in R_L$. Assume that $h, f_1, \ldots, f_k, \mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_k)$ are invariant under $S_{>n}$. Then $q_1, \ldots, q_k$ and r from Lemma 7 can be chosen $S_{>n}$-invariant, and the representations $\hat{q}_1, \ldots, \hat{q}_k, \hat{r}$ can be effectively computed from $\hat{h}, \hat{f_1}, \ldots, \hat{f_r}$.*

Proof. Set $r := h$. While some term of r is divisible by some $\mathrm{lm}(f_i)$, pick the grevlex-largest such term cx^α in r, let $x^{\alpha_1}, x^{\alpha_2}, \ldots$ be the (countably infinite) orbit of x^α under $S_{>n}$ and for each i let c_i be the coefficient of x^{α_i} in r. Since r is $S_{>n}$-invariant, so is $a := \sum_i c_i x^{\alpha_i}$. Moreover, as $\mathrm{lm}(f_i)$ is $S_{>n}$-invariant, a is divisible by $\mathrm{lm}(f_i)$. Replace r by $r - (a/\mathrm{lm}(f_i))f_i$ and q_i by $q_i + (a/\mathrm{lm}(f_i))$; each of these are $S_{>n}$-invariant. This does not effect the terms of r larger than x^α and gets rid of this particular term. In this process, r and the q_i remain $S_{>n}$-invariant and converge to series as in Lemma 7.

For effectiveness, we need to be able to compute the representation of $r - (a/\mathrm{lm}(f_i))f_i$ from $\hat{r}, \hat{a} = cx^\alpha$, and $\hat{f_i}$. The representation depends linearly on the series, so it suffices to have a procedure for computing the representation of a product. The function Product does just that—it uses that no monomial of degree e that is grevlex-maximal in its $S_{>n}$-orbit contains any of the variables $x_{n+e+1}, x_{n+e+2}, \ldots$. □

---

function Product($n, \hat{f}, \hat{h}$)
  input: n-representations $\hat{f}, \hat{h}$ of $S_{>n}$-invariant series f, h.
  output: n-representation $\widehat{fh}$ of fh.
  $e := \deg f + \deg h$;
  compute the truncations $f^{(n+e)}, h^{(n+e)}$ from $\hat{f}, \hat{h}$;
  $u := f^{(n+e)} h^{(n+e)}$;
  remove all terms in u not grevlex-maximal in their $S_{>n}$-orbit;
  return u;
end function

The next ingredient is S-series: if f, g are monic $S_{>n}$-invariant series whose leading monomials are also $S_{>n}$-invariant, and $x^\gamma = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$, then we set $S(f, g) := (x^\gamma/\mathrm{lm}(f))f - (x^\gamma/\mathrm{lm}(g))g$. We note that $S(f, g)$ is also $S_{>n}$-invariant, and the n-representation of $S(f, g)$ can be computed from the n-representations $\hat{f}, \hat{g}$, as follows.

From the n-representation $\hat{f} = \sum_{i=1}^{s} c_{\alpha_i} x^{\alpha_i}$ of an $S_{>n}$-invariant grevlex series one can compute the m-representation $\tilde{f}$ with $m > n$ as follows. For each $i = 1, \ldots, s$, the group $S_{>m}$ has only finitely many orbits on $S_{>n} x^{\alpha_i}$. Let $x^{\beta_{i1}}, \ldots, x^{\beta_{is_i}}$ be the grevlex-maximal representatives of these orbits, and let $\pi_{i1}, \ldots, \pi_{is_i} \in S_{>m}$ be such that $\pi_{ij} x^{\alpha_i} = x^{\beta_{ij}}$. Then define

$$\tilde{f} := \sum_{i=1}^{s} \sum_{j=1}^{s_i} \pi_{ij}(c_{\alpha_i}) x^{\beta_{ij}}.$$

function REMAINDER($n, \hat{h}, \{\hat{f}_1, \dots, \hat{f}_k\}$)
  input: n-representations $\hat{h}, \hat{f}_1, \dots, \hat{f}_k$ of $S_{>n}$-invariant series, with $\hat{f}_i$ monic and $\mathrm{lm}(\hat{f}_i)$ $S_{>n}$-invariant;
  output: the n-representation of a remainder of h after division by $f_1, \dots, f_k$.
  assume $\mathrm{lm}(\hat{f}_1), \dots, \mathrm{lm}(\hat{f}_k)$ are $S_{>n}$-invariant.
  $\hat{r} := \hat{h}$;
  while $\hat{r}$ contains a term cx^α divisible by some $\mathrm{lm}(\hat{f}_i)$ **do**
    $\hat{r} := \hat{r} - $PRODUCT$(cx^\alpha/\mathrm{lm}(\hat{f}_i), x\hat{f}_i)$;
  end while;
  return $\hat{r}$;
end function

function S($n, \hat{f}, \hat{g}$)
  input: n-representations $\hat{f}, \hat{g}$ of monic $S_{>n}$-invariant series with $\mathrm{lm}(\hat{f}), \mathrm{lm}(\hat{g})$ $S_{>n}$-invariant.
  output: n-representation of $S(f, g)$.
  $x^\gamma := \mathrm{lcm}(\mathrm{lm}(\hat{f}), \mathrm{lm}(\hat{g}))$;
  $\hat{s} := (x^\gamma/\mathrm{lm}(\hat{f}))\hat{f} - (x^\gamma/\mathrm{lm}(\hat{g}))\hat{g}$;
  return $\hat{s}$;
end function

We call $\tilde{f}$ the *m-expansion* of $\hat{f}$. So we may freely increase n when desirable; we will use this to ensure that the leading monomial of f is $S_{>n}$-invariant.

Proof of Theorem 2. The algorithm SYMMETRICBUCHBERGER above called with arguments $(n, \hat{f}_1, \dots, \hat{f}_k)$ performs the same operations as the algorithm SERIESBUCHBERGER on page 5 on input $(f_1, \dots, f_k)$, except that it works with finite data structures capturing the series f_i. Hence Proposition 8 implies both the termination and the fact that the output of SYMMETRICBUCHBERGER is the representation of a Gröbner basis of $\langle f_1, \dots, f_k \rangle$. □

Remark 10. Should one consider implementing SYMMETRICBUCHBERGER, it may be practical to allow series to have m-representations with varying values of m, as opposed to the uniform m for every iteration of the outer loop above.

In order to perform binary operations, i.e., additions and multiplications, representations would then need to be expanded to a matching value of m. Furthermore, to ensure termination, the order of S-pairs needs to ensure that each leading monomial is eventually encountered. In SYMMETRICBUCHBERGER, this is done by increasing m only after all the leading monomials in $x_1, \dots, x_m$ have been collected.

4. A POLYNOMIAL FUNCTOR

Let K be an infinite field. Let $\mathrm{GL}_n(K)$ act on the space K^n with basis $x_1, \dots, x_n$ by left multiplication, and for each $d \in \mathbb{Z}_{\geq 0}$ on the d-th symmetric power $S^d K^n$ in the natural manner. Fix $d_1, \dots, d_k \in \mathbb{Z}_{\geq 0}$ and set

$$P^{(n)}(K) := S^{d_1} K^n \oplus \cdots \oplus S^{d_k} K^n,$$

```
function SymmetricBuchberger(n, f̂_1, ..., f̂_k)
    input: n-representations f̂_1, ..., f̂_k S_{>n}-invariant series.
    output: the m-representation of a Gröbner basis of ⟨f_1, ..., f_k⟩ for some m ≥ n.
    m := n; B̂ := ∅ (the basis); Q := {f̂_1, ..., f̂_k} (the queue);
    while Q ≠ ∅ do
        while Q contains an f̂ with f̂^(m) ≠ 0 do
            Q := Q \ {f̂};
            f̂ := f̂/lc(f̂);
            B̂ := B̂ ∪ {f̂};
            for ĥ ∈ B̂ \ {f̂} do
                r̂ :=Remainder(m,S(m, ĥ, f̂), B̂);
            end for;
            if r̂ ≠ 0 then
                Q := Q ∪ {r̂};
            end if;
        end while;
        Replace B̂ and Q̂ by their (m + 1)-expansions;
        m := m + 1;
    end while;
    return B̂;
end function
```

the space of tuples of forms of degrees $d_1, \ldots, d_k$ in n variables. Now define $P(K) := \lim_{\leftarrow n} P^{(n)}(K)$, the projective limit along the maps $P^{(n+1)}(K) \to P^{(n)}(K)$ coming from the projection $K^{n+1} \to K^n$ forgetting the last coordinate. The map $P^{(n+1)}(K) \to P^{(n)}(K)$ is $\mathrm{GL}_n(K)$-equivariant if we think of $\mathrm{GL}_n(K)$ as embedded in $\mathrm{GL}_{n+1}(K)$ via the map $g \mapsto \mathrm{diag}(g, 1)$, and hence $P(K)$ is a module for the group $\mathrm{GL}_\infty(K) := \bigcup_n \mathrm{GL}_n(K)$. The space $P(K)$ is the subspace of $(R_K)^k$ consisting of all tuples where the i-th element is homogeneous of degree d_i for each $i \in [k]$.

Dually, let $V := \lim_{n\to}(P^{(n)}(K))^*$. Then V is a countable-dimensional space, $P(K)$ is canonically isomorphic to V^*, and hence $K[P] := SV$, the symmetric algebra on V, serves as a coordinate ring of $P(K)$ in that the set of K-algebra homomorphisms $K[P] \to K$ is canonically identified with $P(K)$. We equip $P(K)$ with the Zariski topology in which closed subsets are characterized by polynomial equations from $K[P]$. Also V and $K[P]$ are modules for $\mathrm{GL}_\infty(K)$. The following is an instance of a general result on polynomial functors from [Dra17].

Theorem 11. *Let K be an infinite field, and fix integers $d_1, \ldots, d_N$. Then any chain $P(K) \supseteq X_1 \supseteq \cdots$ of $\mathrm{GL}_\infty(K)$-stable Zariski-closed subsets stabilizes eventually. Equivalently, any sequence $a_1, a_2, a_3, \ldots$ in $K[P]$ has the property that for $t \gg 0$ we have*

$$a_t \in \sqrt{\left\langle \bigcup_{i=1}^{t-1} \mathrm{GL}_\infty(K) a_i \right\rangle}.$$

Remark 12. Two comments are in order. First, the implication $\Rightarrow$ between the two statements in the theorem follows from the Nullstellensatz, since the first sentence also holds for any algebraic closure of K. Second, each a_i is an element of $K[P^{(n_i)}]$

for some finite n_i. If $n \geq \max_{i\in[t]} n_i$, then the property of a_t above is equivalent to

$$a_t \in \sqrt{\left\langle \bigcup_{i=1}^{t-1} \mathrm{GL}_n(K) a_i \right\rangle},$$

where we have replaced ∞ by n.

5. Finitely many generic initial ideals

We now prepare for the proof of Theorem 3. For $i = 1, \ldots, k$ let f_i be the homogeneous degree-d_i series

$$f_i = \sum_{|\alpha|=d_i} c_{i,\alpha} x^\alpha$$

whose coefficients live in the polynomial ring

$$A = \mathbb{Z}[c_{i,\alpha} \mid i \in [k], \alpha \in \mathbb{Z}_{\geq 0}^{\mathbb{N}}, |\alpha| = d_i]$$

in which the $c_{i,\alpha}$ are variables. We note that if K is a field, then $K \otimes A$ is the coordinate ring $K[P]$ of the space $P(K)$ introduced in Section 4.

On A acts S_∞ via ring automorphisms determined by $\pi c_{i,\alpha} = c_{i,\alpha\circ\pi^{-1}}$, and each f_i is S_∞-invariant. In the 0-representation $\hat{f}_i$ of f_i, we have

$$\hat{f}_i = \sum_{|\alpha|=d_i, \alpha(1)\geq\alpha(2)\geq\ldots} c_{i,\alpha} x^\alpha,$$

a polynomial with as many terms as there are partitions of d_i. Write $A^{(n)}$ for the subring of A generated by those $c_{i,\alpha}$ such that $\forall m > n : \alpha(m) = 0$.

Let g be an $n \times n$-matrix of variables. Replacing, in f_i, each x_h with $h \leq n$ by $\sum_j g_{hj} x_j$ and each x_h with $h > n$ by x_h yields a series $g f_i$ in the x_h whose coefficients are polynomials that are linear in the $c_{i,\alpha}$ and homogeneous of degree d_i in the g_{hj}. We use the formal notation $g^{-1} c_{i,\alpha}$ for the coefficient of x^α in $g f_i$. This notation is chosen so that if we specialize g to be the matrix of a permutation $\pi \in \mathrm{S}_n$, then $g^{-1} c_{i,\alpha}$ specializes to $\pi^{-1} c_{i,\alpha}$ in the S_n-action above. For a polynomial $r = r(c) \in A$ (in the $c_{i,\alpha}$ with varying i and α) write $g^{-1} r \in \mathbb{Z}[g_{hj} \mid h, j \in [n]] \otimes_{\mathbb{Z}} A$ for the polynomial obtained by replacing each $c_{i,\alpha}$ with $g^{-1} c_{i,\alpha}$. Regarding $g^{-1} r$ as a polynomial in the entries g_{hj} whose coefficients are in A, we write $E_n(r) \subseteq A$ for the set of all nonzero coefficients. It is easy to see that if $r \in A^{(n)}$, then also $E_n(r) \subseteq A^{(n)}$. The following easy lemma explains the significance of this construction.

Lemma 13. *If K is an infinite field, then the K-span of the orbit of $1 \otimes r \in K \otimes_{\mathbb{Z}} A$ under $\mathrm{GL}_n(K)$ equals the K-span of $1 \otimes E_n(r(c))$.* □

Proof of Theorem 3. In the recursive variant Stillman of SymmetricBuchberger on page 10, we write $\mathbb{F}_p$, where p is either zero or a prime, for the prime field of characteristic p. We prove that Stillman terminates on input

$$(0, \emptyset, \{\hat{f}_1, \ldots, \hat{f}_d\}, \mathrm{Spec}(\mathbb{Z}), \emptyset, \emptyset)$$

and that it prints out the sets S_i as in the theorem.

First we clarify the role of the variables. The symbols $m, \hat{B}, \hat{Q}$ carry the same meaning as in SymmetricBuchberger. The meaning of Z and N, finite subsets of A, is that of vanishing and nonvanishing elements, respectively, at the current run

```
procedure Stillman(n, B̂, Q̂, Y, Z, N)
    m := n;
    Q := Q \ {0};
    while Y ≠ ∅ and Q̂ ≠ ∅ do
        while Y ≠ ∅ and Q̂ contains an f̂ with f̂^(m) ≠ 0 do
            Q̂ := Q̂ \ {f̂};
            b := lc(f̂) ∈ A[N^{-1}];
            a :=numerator(b) ∈ A;
            Y_1 := {(p) ∈ Y : a ∈ sqrt(⟨⋃_{r∈Z} E_m(r)⟩_{F_p⊗A^(m)[N^{-1}]})};
            Stillman(m, B̂, Q̂ ∪ {f̂ − lt(f̂)}, Y_1, Z, N);                    (I)
            Y := Y \ Y_1;
            Y_2 := {(p) ∈ Y : 1 ∉ ⟨⋃_{r∈Z∪{a}} E_m(r)⟩_{F_p⊗A^(m)[N^{-1}]}};
            Stillman(m, B̂, Q̂ ∪ {f̂ − lt(f̂)}, Y_2, Z ∪ {a}, N);              (II)
            f̂ := f̂/b;
            N := N ∪ {a};
            B̂ := B̂ ∪ {f̂};
            for ĥ ∈ B̂ \ {f̂} do
                r̂ :=Remainder(m,S(m, ĥ, f̂), B);
                if r̂ ≠ 0 then
                    Q̂ := Q̂ ∪ {r̂};
                end if;
            end for;
        end while;
        Replace B and Q̂ by their (m + 1)-expansions;
        m := m + 1;
    end while;
    if Y ≠ ∅ then
        print lm(B̂);
    end if;
end procedure
```

of the algorithm. While Z stays constant throughout the run (Z is extended only when recursive calls are made), N is augmented as it accumulates elements due to presumed nonvanishing of the leading coefficients.

The current run considers only primes in the set $Y \subseteq \operatorname{Spec}(\mathbb{Z})$. Furthermore, it deals with the specializations of the truncations $f_1^{(m)}, \ldots, f_k^{(m)}$ with coefficients in

$$\bar{A}^{(m)} := A^{(m)}[N^{-1}] / \sqrt{\left\langle \bigcup_{r \in Z} E_m(r) \right\rangle}.$$

We discuss the computations of Y_1, Y_2.

For Y_1, one starts running the ordinary Buchberger algorithm on the ideal in the localization $A^{(m)}[N^{-1}][t]$ generated by $\bigcup_{r \in Z} E_m(r)$ and $ta - 1$ (Rabinowitsch' trick), where t is an auxiliary variable. Whenever an integer leading coefficient is divisible by a nonzero prime (p) in Y, the algorithm branches into a branch where multiples of p are zero and a branch where p is invertible. Assuming that Y is constructible to begin with, each leaf of this finite tree yields a constructible set of primes leading to that leaf, and Y_1 is the union of the primes corresponding to leaves where the aforementioned ideal contains 1.

A similar algorithm is used to compute Y_2. Since we start with $Y = \operatorname{Spec}\mathbb{Z}$, it follows that in any of the further calls of Stillman the set Y is constructible. In other words, Y is either a finite set of nonzero primes in $\operatorname{Spec}(\mathbb{Z})$ or a cofinite set in $\operatorname{Spec}(\mathbb{Z})$ containing (0).

Furthermore, in each run of Stillman, for each $(p) \in Y$, the algebra $\mathbb{F}_p \otimes \bar{A}^{(m)}$ has $0 \neq 1$. This is true at the initial call, it remains true in call (I) since m, Z, N do not change, and it remains true in call (II) since we explicitly test for this condition. Furthermore, it remains true later in the loop, since there we have already removed from Y the primes in Y_1, which are those where inverting a would cause the algebra to collapse.

Let T be the rooted tree whose vertices are the runs of Stillman and whose edges are labelled (I) or (II) according to which call in the algorithm leads from one run to the other. We claim that every path in T away from the root is finite. Indeed, consider an infinite path γ in T. The argument Y remains nonempty and weakly decreases along γ and since it is locally closed in $\operatorname{Spec}(\mathbb{Z})$, so there exists a prime $(p_0) \in \operatorname{Spec}\mathbb{Z}$ that is in the intersection of all the arguments Y along γ.

If infinitely many edges in γ are labelled (II), then Z records $a_1, a_2, a_3, \ldots$ with $a_i \in A^{(m_i)}$ and $m_1 \leq m_2 \leq \ldots$ and

$$a_i \notin \sqrt{\langle E_{n_i}(a_1) \cup \cdots \cup E_{n_i}(a_{i-1})\rangle_{\mathbb{F}_{p_0}\otimes A^{(m_i)}}} \text{ for all } i = 1, 2, 3, \ldots$$

By Lemma 13 and Remark 12 this contradicts the Noetherianity of $K[P]$ over any infinite field K of characteristic p_0 (Theorem 11).

Hence only finitely many edges in γ are labelled (II). We analyse the computation along γ beyond the last edge e labelled (II). Let $m_\infty \in \mathbb{N} \cup \{\infty\}$ be the supremum of the values of m along γ, let Z_0 be the (fixed) value of Z along γ from e onwards, and let N_∞ the union of all N's seen along γ. Define

$$\tilde{A} := \mathbb{F}_{p_0} \otimes A[N_\infty^{-1}] / \sqrt{\left\langle \bigcup_{m \leq m_\infty, r \in Z} E_m(r) \right\rangle}.$$

By construction, $1 \neq 0$ in $\tilde{A}$, hence there exists an epimorphism from $\tilde{A}$ to some field L of characteristic p_0. Then the call of SeriesBuchberger with input the images of the f_i in R_L performs the same operations as the algorithm Stillman along γ. Since the former algorithm terminates by Proposition 8, so does the latter.

We conclude that T is finite. Let K be an infinite field, n a natural number, and let $f'_1, \ldots, f'_k$ be homogeneous polynomials in $K[x_1, \ldots, x_n]$ of degrees $d_1, \ldots, d_k$, respectively. We claim that, at the leaf of some path γ in T away from the root, generators for the generic initial ideal of $\langle f'_1, \ldots, f'_k\rangle$ are printed. To see this, let g be an $n \times n$-matrix of variables, set $L := K((g_{hj})_{h,j})$, and consider the ideal J in $L[x_1, \ldots, x_n]$ generated by the polynomials $gf'_1, \ldots, gf'_k$ obtained by replacing x_h in each f'_i by $\sum_h g_{hj}x_j$. Then the generic initial ideal of $\langle f'_1, \ldots, f'_k\rangle \subseteq K[x_1, \ldots, x_n]$ equals the initial ideal of J, and the latter is computed by Buchberger (or SymmetricBuchberger) on input (n and) $gf'_1, \ldots, gf'_k$. To find γ, proceed as follows: whenever $a \in A$ is defined as the numerator of a leading coefficient of $\hat{f}$, check if under the specialization

$f_i \mapsto g f_i'$ the element a specializes in K to zero or to a nonzero element. If a specializes to zero, then follow call (I) or call (II) according as $(\mathrm{char}\, K) \in Y_1$ or not. If a does not specialize to zero, then follow neither of these calls and continue with the loop. Along this γ, Stillman performs the same operations as SeriesBuchberger, and hence terminates with the generic initial ideal of $\langle f_1', \ldots, f_k' \rangle$. □

Remark 14. Apart from printing $\mathrm{lm}(\hat{B})$ at each leaf of T we may also print Y, Z, N, which together describe a locally closed stratum of $P(K)$, for any infinite K with $(\mathrm{char}\, K) \in Y$, consisting of k-tuples with generic initial ideal generated by $\mathrm{lm}(\hat{B})$.

Acknowledgements. The authors thank Institut Mittag-Leffler for the hospitality during their stay in the early 2018.

The first author thanks Diane Maclagan, who introduced Stillman's conjecture to him many years ago and suggested that it might be related to Noetherianity up to symmetry.

The third author thanks MSRI for the Fall of 2017 stay, during which "The Fellowship of the Ring" and Craig Huneke rekindled his interest in Stillman's conjecture. Last but the most, the thanks go to Gennady Lyubeznik and Mike Stillman. When they both were 40 years young, Gennady suggested a problem that involved a certain constructible stratification and Mike helped solving it via parametric Gröbner bases. The intuition gained 20 years ago was instrumental in the present work.

References

[AH16] Tigran Ananyan and Melvin Hochster. Small subalgebras of polynomial rings and Stillman's conjecture. 2016. Preprint, arXiv:1610.09268.

[BS87] David Bayer and Michael Stillman. A theorem on refining division orders by the reverse lexicographic order. *Duke Math. J.*, 55:321–328, 1987.

[DES17] Harm Derksen, Rob Eggermont, and Andrew Snowden. Topological noetherianity for cubic polynomials. *Algebra Number Theory*, 11(9):2197–2212, 2017.

[Dra17] Jan Draisma. Topological Noetherianity of polynomial functors. 2017. Preprint, arXiv:1705.01419.

[Eis95] David Eisenbud. *Commutative Algebra. With a View toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1995.

[ESS17] Daniel Erman, Steven Sam, and Andrew Snowden. Generalizations of Stillman's conjecture via twisted commutative algebras. 2017. Preprint, arXiv:1804.09807.

[ESS18] Daniel Erman, Steven V. Sam, and Andrew Snowden. Big polynomial rings and Stillman's conjecture. 2018. Preprint, arXiv:1801.09852.

[PS09] Irena Peeva and Mike Stillman. Open problems on syzygies and Hilbert functions. *J. Commut. Algebra*, 1(1):159–195, 2009.

[Sne98a] Jan Snellman. Gröbner bases and normal forms in a subring of the power series ring on countably many variables. *J. Symb. Comput.*, 25(3):315–328, 1998.

[Sne98b] Jan Snellman. Reverse lexicographic initial ideals of generic ideals are finitely generated. In *Gröbner bases and applications. Based on a course for young researchers, January 1998, and the conference "33 years of Gröbner bases", Linz, Austria, February 2–4, 1998*, pages 504–518. Cambridge: Cambridge University Press, 1998.

(Jan Draisma) Mathematical Institute, University of Bern, Sidlerstrasse 5, 3012 Bern, Switzerland; and Eindhoven University of Technology, The Netherlands

E-mail address: jan.draisma@math.unibe.ch

(Michał Lasoń) Mathematical Institute, University of Bern, Sidlerstrasse 5, 3012 Bern, Switzerland; Institute of Mathematics of the Polish Academy of Sciences, ul.Śniadeckich 8, 00-656 Warszawa, Poland
E-mail address: michalason@gmail.com

(Anton Leykin) School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332-0160, USA
E-mail address: leykin@math.gatech.edu