Ideals modulo p

John Abbott

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Anna Maria Bigatti

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Lorenzo Robbiano

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Abstract

The main focus of this paper is on the problem of relating an ideal I in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$ to a corresponding ideal in $\mathbb{F}_p[x_1, \ldots, x_n]$ where p is a prime number; in other words, the *reduction modulo* p of I. We define a new notion of σ-good prime for I which depends on the term ordering σ, and show that all but finitely many primes are good for all term orderings. We relate our notion of σ-good primes to some other similar notions already in the literature. One characteristic of our approach is that enables us to detect some bad primes, a distinct advantage when using modular methods.

Key words: modular
1991 MSC: [2010] 13P25, 13P10, 13-04, 14Q10, 68W30

1. Introduction and Notation

There is a long tradition of using modular techniques for speeding up computations which involve polynomials with rational coefficients (see for instance (16)). Two main interrelated obstacles to the success of this kind of approach are the existence of *bad primes*, and the difficulty of reconstructing the *correct rational coefficients* possibly in the presence of undetected bad primes. We refer to (1) for a discussion of the second

Email addresses: `abbott@dima.unige.it` (John Abbott), `bigatti@dima.unige.it` (Anna Maria Bigatti), `robbiano@dima.unige.it` (Lorenzo Robbiano).

[1] This research was partly supported by the "National Group for Algebraic and Geometric Structures, and their Applications" (GNSAGA – INDAM). J. Abbott is an INdAM–COFUND Marie Curie Fellow.

problem and to (4) for some new results in this direction and applications to the problem of the implicitization of hypersurfaces.

The main focus of this paper is on the problem of relating an ideal I in the polynomial ring $P = \mathbb{Q}[x_1, \ldots, x_n]$ to a corresponding ideal in $\mathbb{F}_p[x_1, \ldots, x_n]$ where p is a prime number. In other words, we face the problem of defining a *reduction modulo p* of I. This is the main theme of Section 2 where we use results proved in (5), and introduce the notions of *σ-good* and *σ-bad primes* for I with respect to a given term ordering σ, which exploit the uniqueness of the reduced σ-gbasis. Notions of good/bad primes in modular computations are ubiquitous, see for instance (8) for a fine discussion, however, in our opinion there is still room for improving the knowledge of this topic. As a first result, we prove Theorem 2.11 which relates the behaviour of good primes with respect to two different term orderings.

From the theory of Gröbner Fans (see (14)) it follows that for any ideal I in P all but finitely many primes are good for all term orderings (see Remark 2.12). In other words there is an integer Δ, called the *universal denominator* (see Definition 2.13), such that for every prime p which does not divide Δ we can define the reduction of I to an ideal in $\mathbb{F}_p[x_1, \ldots, x_n]$ which is independent of any term ordering (see Definition 2.15).

In the context of polynomial ideals there are several notions of good/bad primes in the mathematical literature, and Section 3 is devoted to understanding some of their interrelations. We recall the notion of a *minimal strong Gröbner basis* for ideals in $\mathbb{Z}[x_1, \ldots, x_n]$. Following (15), we say that p is *Pauer-lucky* for a set of polynomials $F \subset P$ if it does not divide the leading coefficients of any polynomial in a minimal strong σ-Gröbner basis of $\langle \mathrm{prim}(F) \rangle$ (see Definition 3.6). Then, given a term ordering σ, the ideal $I = \langle F \rangle$, and its reduced σ-gbasis G, we use the fundamental results contained in Proposition 3.7 and Theorem 3.11 to show that if p is Pauer-lucky for $\mathrm{prim}(F)$ then p is σ-good for I (see Proposition 3.16), and that p is Pauer-lucky for $\mathrm{prim}(G)$ if and only if it is σ-good for I (see Corollary 3.19).

In Section 4 we address the problem of detecting σ-bad primes when the reduced σ-Gröbner basis is not known. In (7) E.A. Arnold restricted her investigation to the case of homogeneous ideals and used suitable Hilbert functions to detect some bad primes. We describe a similar but more general strategy. The main new idea is to use the term ordering σ to order tuples of power products. In particular, we prove Proposition 4.6 and the key Lemma 4.10 which pave the way to the proof of the main Theorem 4.13. In essence given two term orderings σ and τ, and two primes p and q which are both σ-good, but only one is τ-good, then we can determine which is τ-good just doing modular computations. This result implies the relevance of Corollary 4.14 where a nice criterion for detecting relatively bad primes is described. Another interesting application is given in Corollary 4.16 which is the last result of the paper.

Are there practical applications of the theoretical results proved in this paper? First experiments show that a modular approach for the computation of some Gröbner bases can benefit from our results. We plan to implement new algorithms and explain their benefits in a subsequent paper. First naive experiments (see for instance Example 4.18) show that our approach is very promising.

Most examples described in the paper were computed using the computer algebra system CoCoA (see (2) and (3)). The computations of minimal strong Gröbner bases were performed with SINGULAR.

Notation

For the basic notation and definitions about the theory of Gröbner bases see (11), (12), and (13). The monoid of power-products in n indeterminates is denoted by $\mathbb{T}^n$. We use the convention that $\mathrm{LT}_\sigma(\langle 0\rangle) = \langle 0\rangle$. In particular, if $t = x_1^{a_1} \cdots x_n^{a_n} \in \mathbb{T}^n$ is a power-product and c is a coefficient, we say that t is a **term** and $c\,t$ is a **monomial**. Throughout this article, when we use the notation $G = \{g_1, \ldots, g_r\}$, we actually mean that the r elements in G are numbered and distinct. We use the symbol $\mathbb{Z}_\delta$ to represent the localization of $\mathbb{Z}$ at the multiplicative system generated by the integer δ. Sometimes in the literature the symbol $\mathbb{Z}[\frac{1}{\delta}]$ is used instead of $\mathbb{Z}_\delta$.

There are several instances in the paper where we compare the minimal set of generators of two monomial ideals in different rings. Hence we introduce the following definition. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over K, let σ be a term ordering on $\mathbb{T}^n$, and let I be an ideal in P. The unique minimal set of generators of $\mathrm{LT}_\sigma(I)$ is denoted by $\boldsymbol{\mathrm{MinLT}_\sigma(I)}\subset \mathbb{T}^n$. We observe that while $\mathrm{LT}_\sigma(I)$ is a monomial ideal in P, the set $\mathrm{MinLT}_\sigma(I)$ is a subset of $\mathbb{T}^n$. Later we introduce the tuple $\boldsymbol{\mathrm{OrdMinLT}_\sigma(I)}$ which contains the same elements as $\mathrm{MinLT}_\sigma(I)$ placed in increasing σ-order (see Definition 4.1).

Let $T = \{t_1, t_2, \ldots, t_r\}$ be a set of power-products. We define the **interreduction** of T to be the unique maximal subset T' of T with the property that there is no pair (t_i, t_j) of distinct elements in T' such that $t_i \mid t_j$. We say that T is **interreduced** if it is equal to its own interreduction.

2. Reductions modulo p

In this section we analyse the concept of *reduction modulo a prime p*. In particular we give a definition for the reduction mod p of an ideal, which is independent of its generators.

The **radical** of a positive integer N, $\boldsymbol{\mathrm{rad}(N)}$, is the product of all primes dividing N. Obviously from the definition we have $p \,|\, N \iff p \,|\, \mathrm{rad}(N)$ for any prime p. For example, $\mathrm{rad}(240) = 30$. Note that, for any positive integer N, we have $\mathbb{Z}_N = \mathbb{Z}_\delta$ where $\delta = \mathrm{rad}(N)$.

Definition 2.1. Let δ be a positive integer, and p a prime number not dividing δ. We write π_p to denote the canonical homomorphism $\mathbb{Z}_\delta \longrightarrow \mathbb{F}_p$ and all its natural “coefficientwise” extensions to $\mathbb{Z}_\delta[x_1, \ldots, x_n] \longrightarrow \mathbb{F}_p[x_1, \ldots, x_n]$; we call them all **reduction homomorphisms modulo *p***.

Definition 2.2. Let $P = \mathbb{Q}[x_1, \ldots, x_n]$.

(a) Given a polynomial $f \in P$, we define the **denominator of *f***, denoted by $\boldsymbol{\mathrm{den}(f)}$, to be 1 if $f \in \mathbb{Z}[x_1, \ldots, x_n]$, and otherwise the positive least common multiple of the denominators of the coefficients of f. In particular, $\mathrm{den}(0) = 1$.

(b) Given a set of polynomials F in P, we define the **denominator of *F***, denoted by $\boldsymbol{\mathrm{den}(F)}$, to be the least common multiple of $\{\mathrm{den}(f) \mid f \in F\}$. For completeness we define $\mathrm{den}(\emptyset) = 1$ where $\emptyset$ denotes the empty set.

(c) Given a term ordering σ and an ideal I in the ring P with reduced σ-Gröbner basis G_σ, we define the ***σ*-denominator of *I*** to be $\boldsymbol{\mathrm{den}_\sigma(I)}$= $\mathrm{den}(G_\sigma)$.

The following easy example shows that $\mathrm{den}_\sigma(I)$ generally depends on σ.

Example 2.3. Let $P = \mathbb{Q}[x, y]$ and let $g = x + 2y \in P$, and let $I = \langle g \rangle$. Clearly $\{g\}$ is the reduced Gröbner basis of I with respect to any term ordering σ with $x >_\sigma y$. Instead, the reduced Gröbner basis of I with respect to any term ordering τ with $y >_\tau x$ is $\{y + \frac{1}{2}x\}$. Therefore we have $\mathrm{den}_\sigma(I) = 1$ while $\mathrm{den}_\tau(I) = 2$.

The following proposition collects some important results taken from (5).

Lemma 2.4. *Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, let I be an ideal in P, let G_σ be the reduced σ-Gröbner basis of I, and let $f \in P$. Furthermore, let $G_{\sigma,f} = \{g \in G_\sigma \mid \mathrm{LT}_\sigma(g) \leq_\sigma \mathrm{LT}_\sigma(f)\}$, and let δ_f be a common multiple of* $\mathrm{den}(f)$ *and* $\mathrm{den}(G_{\sigma,f})$.

(a) Every intermediate step of rewriting f via G_σ has all coefficients in $\mathbb{Z}_{\delta_f}$.

(b) The polynomial $\mathrm{NF}_{\sigma,I}(f)$ has all coefficients in $\mathbb{Z}_{\delta_f}$.

Proof. The proof follows as an immediate generalization of (5), Lemma 4.1. □

The following proposition is the foundation stone of our investigation. In particular, it set the right context in which the reduction mod p of a Gröbner basis is the Gröbner basis of the ideal it generates (claim c).

Proposition 2.5. *Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, let I be an ideal in P, let G_σ be its reduced σ-Gröbner basis, and let $f \in P$. Then let δ be a positive integer such that f and G_σ have all coefficients in $\mathbb{Z}_\delta$, i.e. δ is a non-zero multiple of* $\mathrm{rad}(\mathrm{den}(f) \cdot \mathrm{den}_\sigma(I))$, *and let p be a prime number which does not divide δ.*

(a) Every intermediate step of rewriting f via G_σ has all coefficients in $\mathbb{Z}_\delta$.

(b) The polynomial $\mathrm{NF}_{\sigma,I}(f)$ has all coefficients in $\mathbb{Z}_\delta$.

(c) The set $\pi_p(G_\sigma)$ is the reduced σ-Gröbner basis of the ideal $\langle \pi_p(G_\sigma) \rangle$.

(d) We have the equality $\pi_p(\mathrm{NF}_{\sigma,I}(f)) = \mathrm{NF}_{\sigma,\langle \pi_p(G_\sigma) \rangle}(\pi_p(f))$.

(e) Let $B = \mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ and let Q_p denote the quotient ring $\mathbb{F}_p[x_1, \ldots, x_n]/\langle \pi_p(G_\sigma) \rangle$. Then the set of the residue classes of B is an $\mathbb{F}_p$-basis of Q_p.

Proof. Clearly claims (a) and (b) are special cases of Lemma 2.4. For the proofs of (c) and (d) we refer to (5), Theorem 4.6. Finally, claim (e) is an immediate consequence of (c) and (d). □

2.1. σ-Good Primes

Along the lines in (5), Proposition 2.5 motivates the following definitions.

Definition 2.6. Let $P = \mathbb{Q}[x_1, \ldots, x_n]$ be a polynomial ring.

(a) Let F be a finite set of polynomials in P. We say that a prime p is **bad** for F if $p \mid \mathrm{den}(F)$, *i.e.* p divides the denominator of at least one coefficient of at least one polynomial in F.

(b) Let σ be a term ordering on $\mathbb{T}^n$, let I be an ideal in P, and let G_σ be the reduced σ-Gröbner basis of I. If p is bad for G_σ we say that p is ***σ*-bad for *I***. Otherwise we say that p is ***σ*-good for *I***.

(c) If p is a σ-good prime for I we define the **(p, σ)-reduction of *I*** to be the ideal $I_{(p,\sigma)} = \langle \pi_p(G_\sigma) \rangle \subseteq \mathbb{F}_p[x_1, \ldots, x_n]$ generated by the reductions modulo p of the polynomials in G_σ.

Now we can reinterpret Proposition 2.5.c as follows.

Remark 2.7. Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, and σ a term ordering on $\mathbb{T}^n$. Let I be an ideal in P, and G_σ its reduced σ-Gröbner basis. For every σ-good prime p for I we have

(a) the set $\pi_p(G_\sigma)$ is the reduced σ-gbasis of $I_{(p,\sigma)}$, *i.e.* the ideal it generates.
(b) $\mathrm{MinLT}_\sigma(I) = \mathrm{MinLT}_\sigma(I_{(p,\sigma)})$.

Remark 2.8. We observe that the apparently simplistic definition, stating that p is σ-good for I if and only if p does not divide $\mathrm{den}(G_\sigma)$, acquires a much deeper meaning after the above remark, and provides further support for the notation $I_{(p,\sigma)}$ since the reduced σ-Gröbner basis of any ideal is unique.

Proposition 2.5 turns out to be the essential tool to prove the following result.

Theorem 2.9. *Let σ be a term ordering on $\mathbb{T}^n$, let $P = \mathbb{Q}[x_1, \ldots, x_n]$, let I be an ideal in P, and let G_σ be its reduced σ-Gröbner basis. Then let F be any finite set of polynomials in the ideal I, and let δ be a positive integer such that both G_σ and F are contained in $\mathbb{Z}_\delta[x_1, \ldots, x_n]$. Let p be a prime number such that $p \nmid \delta$.*

(a) We have $\mathrm{rad}(\mathrm{den}_\sigma(I)) \mid \delta$.
(b) We have $\langle \pi_p(F) \rangle \subseteq I_{(p,\sigma)} \subseteq \mathbb{F}_p[x_1, \ldots, x_n]$.
(c) If there exists a matrix M with entries in $\mathbb{Z}_\delta[x_1, \ldots, x_n]$ such that $G_\sigma = F \cdot M$, then we have $\langle \pi_p(F) \rangle = I_{(p,\sigma)}$.

Proof. To prove claim (a) we observe that the minimal localization of $\mathbb{Z}$ where G_σ is contained is $\mathbb{Z}_{\mathrm{den}_\sigma(I)}[x_1, \ldots, x_n]$, and the conclusion follows.

To prove claim (b) we observe that Proposition 2.5.c implies that every element of F can be written as a linear combination of elements of G_σ where the “coefficients” are polynomials in $\mathbb{Z}_\delta[x_1, \ldots, x_n]$. In general, there will be several ways to reduce each element of F by the basis G_σ, we may pick any one, and use the corresponding linear combination. We can view F and G_σ as row-matrices by ordering their elements in some way. Then writing the linear combinations as columns, we obtain a matrix A over $\mathbb{Z}_\delta[x_1, \ldots, x_n]$ (see 2.5.a) satisfying $F = G_\sigma \cdot A$. This implies that $\pi_p(F) = \pi_p(G_\sigma) \cdot \pi_p(A)$, concluding the proof.

Finally, we prove (c). By claim (a) the prime p is σ-good for I, hence we have the equality $I_{(p,\sigma)} = \langle \pi_p(G_\sigma) \rangle$. Moreover, we have $\pi_p(G_\sigma) = \pi_p(F) \cdot \pi_p(M)$ hence the implication $I_{(p,\sigma)} \subseteq \langle \pi_p(F) \rangle$ follows. The reverse inclusion follows from (b), and the proof is complete. □

The following easy example shows that the inclusion in claim (b) can be strict even when F is a generating set.

Example 2.10. We follow the notation in the proof above.

```
/**/ use P ::= QQ[x,y,z], DegRevLex;
/**/ F_0 := [x+2*z,  x+2*y];  I := ideal(F_0);
/**/ G_0 := ReducedGBasis(I);  G_0;
[x+2*z,  y-z]
/**/ [GenRepr(f, I) | g in G_0];
[[1,  0],  [-1/2,  1/2]]
```

The "new prime" 2 shows up in the denominators of the coefficients representing the reduced σ-Gröbner basis elements as linear combinations of the original generators. Now we look at what happens modulo 2 when we create an ideal from the original generators, and when we create an ideal from the reduced Gröbner basis.

```
/**/ use P_2 ::= ZZ/(2)[x,y,z], DegRevLex;
/**/ pi_2 := PolyRingHom(P, P_2, CanonicalHom(QQ,P_2),indets(P_2));
/**/ J := ideal(apply(pi_2, F_0));
/**/ ReducedGBasis(J);
[x]
/**/ I := ideal(apply(pi_2, G_0));
/**/ ReducedGBasis(I);
[y+z,  x]
```

Here we see that the inclusion in Theorem 2.9.b can be strict even though the prime $p = 2$ is `DegRevLex`-good for I. In the next section we shall see that 2 is not a "lucky prime" for F.

Next we present the main result of this subsection. It examines the situation when a prime is good with respect to two different term orderings.

Theorem 2.11. *Let σ and τ be two term orderings on $\mathbb{T}^n$, let $P = \mathbb{Q}[x_1, \ldots, x_n]$, and let I be an ideal in P. Then let G_σ and G_τ be the reduced Gröbner bases of I with respect to σ and τ, and let p be a prime which is both σ-good and τ-good for I.*

(a) We have the equality $I_{(p,\sigma)} = I_{(p,\tau)}$.

(b) The reduced τ-Gröbner basis of $I_{(p,\sigma)}$ is $\pi_p(G_\tau)$.

Proof. Since claim (b) follows immediately from (a) and Remark 2.7, it is sufficient to prove claim (a). Let $\delta = \operatorname{lcm}(\operatorname{den}_\sigma(I), \operatorname{den}_\tau(I))$, so both G_σ and G_τ are contained in the ring $\mathbb{Z}_\delta[x_1, \ldots, x_n]$. From the assumption about p we may apply Theorem 2.9 with $F = G_\tau$ to deduce that $I_{(p,\tau)} = \langle \pi_p(G_\tau) \rangle \subseteq I_{(p,\sigma)}$. Applying Theorem 2.9 again, after exchanging the roles of σ and τ, shows that $I_{(p,\sigma)} = \langle \pi_p(G_\sigma) \rangle \subseteq I_{(p,\tau)}$. This proves the claim. □

2.2. Universal Denominator

In this subsection we recall some facts from Gröbner Fan Theory (see (14)) and use them to define the *universal denominator* of an ideal.

Remark 2.12. It is well-known that the Gröbner fan of an ideal is finite (*e.g.* see (14)), hence for every ideal in $\mathbb{Q}[x_1, \ldots, x_n]$ there are only finitely many distinct reduced Gröbner bases. Each of these bases has its own corresponding denominator; thus any prime which does not divide any of these denominators is good for all term orderings.

This remark motivates the following definition.

Definition 2.13. Let I be an ideal in $\mathbb{Q}[x_1, \ldots, x_n]$. Then the least common multiple of all $\operatorname{den}_\sigma(I)$, as we vary σ, is called the **universal denominator** of I, and is denoted by $\Delta(I)$.

Next we show the existence of a well-behaved notion of reduction of I modulo p which is independent of the term orderings.

Proposition 2.14. *Let I be an ideal in P, let $\Delta(I)$ be its universal denominator, and let p be a prime not dividing $\Delta(I)$. Then $I_{(p,\sigma)}$ does not depend on σ.*

Proof. For any term orderings σ and τ, the prime p is both σ-good and τ-good. So, by Theorem 2.11, we have $I_{(p,\sigma)} = I_{(p,\tau)}$. □

This proposition motivates the following definition.

Definition 2.15. Let I be a non-zero ideal in P, let $\Delta(I)$ be its universal denominator, and let p be a prime not dividing $\Delta(I)$. Then the **reduction of I modulo p**, denoted I_p, is the ideal $I_{(p,\sigma)}$, for any choice of σ.

The main practical problem related to this definition is the computation of the universal denominator of I which is, in general, not an easy task. Let us see some examples.

Example 2.16. Let $P = \mathbb{Q}[x, y, z]$ and let $I = \langle x^2 - y,\ xy + z + 1,\ z^2 + x\rangle$. It is a zero-dimensional ideal and its Gröbner fan consists of twelve cones.

```
/**/ use P ::= QQ[x,y,z];
I := ideal(x^2 -y,  x*y +z +1,  z^2 +x);
/**/ GF := GroebnerFanIdeals(I);
/**/ [ReducedGBasis(J) | J in GF];
  [z^2 +x,  x*y +z +1,  x^2 -y,  y^2 +x*z +x],
  [x +z^2,  y*z^2 -z -1,  z^4 -y,  y^2 -z^3 -z^2],
  [x*y +z +1,  z^2 +x,  x^2 -y,  x*z +y^2 +x,  y^3 +x -2*z -1,  y^2*z -y^2 -x -y],
  [x +z^2,  y*z^2 -z -1,  z^3 -y^2 +z^2,  y^2*z -y^2 +z^2 -y,  y^3 -z^2 -2*z -1],
  [z +x*y +1,  x^2 -y,  y^3 +2*x*y +x +1],
  [z +(-1/2)*y^3 +(-1/2)*x +1/2,  x^2 -y,  x*y +(1/2)*y^3 +(1/2)*x +1/2,
      y^5 +(-1/2)*y^4 +(1/4)*y^3 +(-7/4)*x -3*y^2 +(-5/2)*y +1/4],
  [z +(-2/7)*y^5 +(1/7)*y^4 +(-4/7)*y^3 +(6/7)*y^2 +(5/7)*y +3/7,
      x +(-4/7)*y^5 +(2/7)*y^4 +(-1/7)*y^3 +(12/7)*y^2 +(10/7)*y -1/7,  y^6 -2*y^3 -4*y^2 -y +1],
  [y -x^2,  z +x^3 +1,  x^6 +2*x^3 +x +1],
  [z^2 -y^3 +2*z +1,  x +y^3 -2*z -1,  y^2*z +y^3 -2*z -y^2 -y -1,  y^4 -2*y*z -z -y -1],
  [z^2 +2*z -y^3 +1,  x -2*z +y^3 -1,  y*z +(-1/2)*y^4 +(1/2)*z +(1/2)*y +1/2,
      y^5 +(-1/2)*y^4 +(-7/2)*z +2*y^3 -3*y^2 +(-5/2)*y -3/2],
  [y -x^2,  x^3 +z +1,  z^2 +x],
  [x +z^2,  y -z^4,  z^6 -z -1]
```

So we have $\Delta(I) = 2^2{\cdot}7$. Consequently the reduction I_p is defined for every prime p other than 2 and 7, and is generated by the reduction modulo p of any of these Gröbner bases.

Example 2.17. While many ideals do have relatively small universal denominators, a few seemingly simple ideals can have surprisingly large ones. This usually arises when the Gröbner fan comprises many cones, which can happen easily when there are many indeterminates. We exhibit two examples with few indeterminates which nevertheless have impressive denominators.

The first example in $\mathbb{Q}[x, y, z]$ is the ideal $\langle x^2y + xy^2 + 1, y^3 + x^2z, z^3 + x^2\rangle$ whose universal denominator is larger than 2×10^{404} and has 105 distinct prime factors (including all primes up to 100 except 79 and 89). The Gröbner fan of this ideal comprises 392 cones. The second example is in the ring $\mathbb{Q}[x, y, z, w]$: it is the apparently innocuous ideal $\langle xyz + yzw + y, z^3 + x^2, y^2z + w^3, x^3 + y^3\rangle$. Its universal denominator is larger than 2×10^{379530}. This number has at least 24539 distinct (probably-)prime factors including more than $\frac{2}{3}$ of all primes less than 2^{15}. The smallest prime not dividing the universal denominator is 4463, and the largest (probable) prime factor is about 3.42×10^{76}. The Gröbner fan of this ideal comprises almost 37000 cones.

3. Good primes vs lucky primes

In this section we recall some notions of *lucky primes* which have a long history, and compare them with our notion of *good primes*. We restrict our attention to the case where the ring of coefficients is $\mathbb{Z}$, although the theory is more general (see for instance (6) and (15)). Several results described in this subsection are known, however we adapt them to our notation, and for some of them we provide new proofs.

In this section we fix a term ordering σ on the monoid $\mathbb{T}^n$ of the power-products in n indeterminates, consequently we sometimes omit the symbol σ. Computations of minimal, strong Gröbner bases were performed by Singular (see (10)).

The first important tool is the following definition (see (6), Definition 4.5.6).

Definition 3.1. Let $G_{\mathbb{Z}} = \{g_1, \ldots, g_s\}$ be a set of non-zero polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$. We say that $G_{\mathbb{Z}}$ is a **strong σ-Gröbner basis** for the ideal $J = \langle G_{\mathbb{Z}} \rangle$, if for each $f \in J$ there exists some $i \in \{1, \ldots, s\}$ such that $\mathrm{LM}_\sigma(g_i)$ divides $\mathrm{LM}_\sigma(f)$. We say that $G_{\mathbb{Z}}$ is a **minimal strong σ-Gröbner basis** if it is a strong σ-Gröbner basis and $\mathrm{LM}_\sigma(g_i)$ does not divide $\mathrm{LM}_\sigma(g_j)$ whenever $i \neq j$.

Remark 3.2. In (6) the theory of minimal strong Gröbner bases is fully developed, in particular it is stated that every non-zero ideal in $\mathbb{Z}[x_1, \ldots, x_n]$ has a minimal strong Gröbner basis (see (6), Exercise 4.5.9).

It is well known that reduced Gröbner bases have the property that the leading terms of their elements are pairwise distinct. This also holds for minimal strong Gröbner bases in $\mathbb{Z}[x_1, \ldots, x_n]$ because the coefficient ring $\mathbb{Z}$ is a principal ideal domain.

The following easy examples show the difference between a minimal strong Gröbner basis of an ideal $J \subset \mathbb{Z}[x_1, \ldots, x_n]$ and the reduced Gröbner basis of the extended ideal $J\,\mathbb{Q}[x_1, \ldots, x_n]$. Note that, whereas the elements of the reduced Gröbner basis are monic, in a strong Gröbner basis the coefficients of the leading monomial play an essential role in divisibility checking.

Example 3.3. Let $G_{\mathbb{Z}} = \{x^2,\ 2x\} \subset \mathbb{Z}[x]$; then $G_{\mathbb{Z}}$ is a minimal strong Gröbner basis of the ideal $\langle G_{\mathbb{Z}} \rangle$, while $\{x\}$ is the reduced Gröbner basis of the extended ideal $\langle G_{\mathbb{Z}} \rangle\, \mathbb{Q}[x]$.

Let $F_{\mathbb{Z}} = \{2x,\ 3y\}$. Then $\{2x,\ 3y,\ xy\}$ is a minimal strong Gröbner basis of the ideal $\langle F_{\mathbb{Z}} \rangle$, while $\{x,\, y\}$ is the reduced Gröbner basis of the extended ideal $\langle F_{\mathbb{Z}} \rangle\, \mathbb{Q}[x]$.

The reduced Gröbner basis is a unique, canonical choice amongst all Gröbner bases; in contrast, a minimal strong Gröbner basis is not unique.

Example 3.4. Let σ be the `DegRevLex` term ordering on $\mathbb{T}^2$. In the ring $\mathbb{Z}[x, y]$ let $G_{\mathbb{Z}} = \{y^2 - x,\ 2x\}$ and $G_{\mathbb{Z}}' = \{y^2 + x,\ 2x\}$. Then clearly $\langle G_{\mathbb{Z}} \rangle = \langle G_{\mathbb{Z}}' \rangle$ and both $G_{\mathbb{Z}}$ and $G_{\mathbb{Z}}'$ are minimal strong σ-Gröbner bases of this ideal. The unique reduced σ-Gröbner basis of the extended ideal is $G = \{x,\ y^2\}$.

Although not unique, we shall now see that two minimal strong σ-Gröbner bases of an ideal J in $\mathbb{Z}[x_1, \ldots, x_n]$ share the same leading monomials.

Lemma 3.5. *Let J be an ideal in $\mathbb{Z}[x_1,\dots,x_n]$, and σ be a term-ordering on $\mathbb{T}^n$. Let $G_\mathbb{Z}$ and ${G_\mathbb{Z}}'$ be two minimal strong σ-Gröbner bases of J. Then $\{\mathrm{LM}_\sigma(g) \mid g \in G_\mathbb{Z}\} = \{\mathrm{LM}_\sigma(g') \mid g' \in {G_\mathbb{Z}}'\}$. Consequently we have $\#G_\mathbb{Z} = \#{G_\mathbb{Z}}'$ and $\{\mathrm{LC}_\sigma(g) \mid g \in G_\mathbb{Z}\} = \{\mathrm{LC}_\sigma(g') \mid g' \in {G_\mathbb{Z}}'\}$.*

Proof. This equality can be proved along the same lines as the proof of the uniqueness of the minimal generating set of a monomial ideal in $K[x_1,\dots,x_n]$ where K is a field – see for instance (11, Proposition 1.3.11.b). □

Given a polynomial in $\mathbb{Q}[x_1,\dots,x_n]$ we define its primitive integral part; it has integer coefficients with no common factor, so its modular reduction is non-zero for any prime p.

Definition 3.6. Let f be a non-zero polynomial in $\mathbb{Q}[x_1,\dots,x_n]$, and let c be the integer content of $f\cdot\mathrm{den}(f) \in \mathbb{Z}[x_1,\dots,x_n]$. Then the **primitive integral part of f**, denoted **prim(f)**, is the primitive polynomial $c^{-1}f\cdot\mathrm{den}(f) \in \mathbb{Z}[x_1,\dots,x_n]$. If F is a set of non-zero polynomials in $\mathbb{Q}[x_1,\dots,x_n]$ then **prim(F)**$= \{\mathrm{prim}(f) \mid f{\in}F\}$.

Note that if σ is any term-ordering then $\mathrm{prim}(f) = \mathrm{den}(f_1)\cdot f_1$ where $f_1 = \frac{f}{\mathrm{LC}_\sigma(f)}$.

Let G be the reduced σ-Gröbner basis of an ideal in $\mathbb{Q}[x_1,\dots,x_n]$. The following proposition shows some important properties of all minimal strong σ-Gröbner bases of the ideal generated by $\mathrm{prim}(G)$ in $\mathbb{Z}[x_1,\dots,x_n]$.

Proposition 3.7. *Let $P = \mathbb{Q}[x_1,\dots,x_n]$ with term-ordering σ on $\mathbb{T}^n$. Let I be a non-zero ideal in P, and let $G = \{g_1,\dots,g_r\}$ be its reduced σ-Gröbner basis, whose elements are indexed so that $\mathrm{LT}_\sigma(g_1) <_\sigma \cdots <_\sigma \mathrm{LT}_\sigma(g_r)$. Then let $G_\mathbb{Z} = \{\tilde{g}_1,\dots,\tilde{g}_s\}$ be a minimal strong σ-Gröbner basis of the ideal $J = \langle\mathrm{prim}(G)\rangle \subset \mathbb{Z}[x_1,\dots,x_n]$.*

(a) The elements in $G_\mathbb{Z}$ can be indexed so that $\mathrm{LT}_\sigma(\tilde{g}_i){=}\mathrm{LT}_\sigma(g_i)$ for $i{=}1,\dots,r$ while for $i{=}r{+}1,\dots,s$ each $\mathrm{LT}_\sigma(\tilde{g}_i)$ is a proper multiple of $\mathrm{LT}_\sigma(g_k)$ for some $k \le r$.

(b) The subset $\{\tilde{g}_1,\dots,\tilde{g}_r\}$ is a minimal σ-Gröbner basis of I in P.

(c) We have $\mathrm{LC}_\sigma(\tilde{g}_i) \mid \mathrm{LC}_\sigma(\mathrm{prim}(g_i))$ for $i = 1,\dots,r$.

(d) If there exists a prime p such that $p\,|\,\mathrm{den}(g_i)$ but $p\!\!\not|\,\mathrm{den}(g_j)$ for every $j{=}1,\dots,i{-}1$ then $p \mid \mathrm{LC}_\sigma(\tilde{g}_i)$.

Proof. We start by proving claims (a) and (b). For each $i = 1,\dots,r$ we have $\mathrm{prim}(g_i) \in J$, hence there is at least one polynomial $\tilde{g}_j \in G_\mathbb{Z}$ such that $\mathrm{LM}_\sigma(\tilde{g}_j) \mid \mathrm{LM}_\sigma(\mathrm{prim}(g_i))$. Now $\tilde{g}_j \in I$, hence there is at least one polynomial $g_k \in G$ such that $\mathrm{LT}_\sigma(g_k) \mid \mathrm{LT}_\sigma(\tilde{g}_j)$. Since G is a reduced Gröbner basis it follows that $k = i$, and then also $\mathrm{LT}_\sigma(\tilde{g}_j) = \mathrm{LT}_\sigma(g_i)$. So by suitably renumbering we may assume $j = i$.

Now we consider $i > r$. Again we observe $\tilde{g}_i \in I$, hence there is at least one polynomial $g_k \in G$ such that $\mathrm{LT}_\sigma(g_k) \mid \mathrm{LT}_\sigma(\tilde{g}_i)$. Since $G_\mathbb{Z}$ is minimal and $\mathrm{LT}_\sigma(\tilde{g}_k) = \mathrm{LT}_\sigma(g_k)$ we deduce from Remark 3.2 that $\mathrm{LT}_\sigma(\tilde{g}_i)$ must be a proper multiple of $\mathrm{LT}_\sigma(g_k)$. We have now proved claims (a) and (b).

Next we prove claim (c). From claim (a) it follows that the two polynomials $\tilde{g}_i$ and $\mathrm{prim}(g_i)$ have the same leading term. Since $\mathrm{prim}(g_i) \in J$ there is at least one polynomial $\tilde{g}_j \in G_\mathbb{Z}$ such that $\mathrm{LM}_\sigma(\tilde{g}_j) \mid \mathrm{LM}_\sigma(\mathrm{prim}(g_i))$. This implies that $\mathrm{LT}_\sigma(\tilde{g}_j)\,|\,\mathrm{LT}_\sigma(g_i)$, which in turn implies that $j = i$. Hence $\mathrm{LC}_\sigma(\tilde{g}_i)\,|\,\mathrm{LC}_\sigma(\mathrm{prim}(g_i))$.

Finally, we prove claim (d). Let $h = \tilde{g}_i - \mathrm{LC}_\sigma(\tilde{g}_i){\cdot}g_i$; observe that $h \in I$. Using the fact that $\mathrm{LM}_\sigma(\tilde{g}_i) = \mathrm{LC}_\sigma(\tilde{g}_i)\cdot\mathrm{LT}_\sigma(g_i)$ we can write

$$h \;=\; \big(\tilde{g}_i - \mathrm{LM}_\sigma(\tilde{g}_i)\big) - \mathrm{LC}_\sigma(\tilde{g}_i)\cdot\big(g_i - \mathrm{LT}_\sigma(g_i)\big) \;=\; \tilde{h}_i - \mathrm{LC}_\sigma(\tilde{g}_i){\cdot}h_i$$

where $\tilde{h}_i = \tilde{g}_i - \mathrm{LM}_\sigma(\tilde{g}_i)$ and $h_i = g_i - \mathrm{LT}_\sigma(g_i)$. Since $h \in I$ we have the equality $\mathrm{NF}_{\sigma,I}(\tilde{h}_i) = \mathrm{LC}_\sigma(\tilde{g}_i) \cdot \mathrm{NF}_{\sigma,I}(h_i)$. Given that $g_i \in G$, the reduced σ-Gröbner basis of I, we have that $\mathrm{NF}_{\sigma,I}(h_i) = h_i$, which implies that $\mathrm{NF}_{\sigma,I}(\tilde{h}_i) = \mathrm{LC}_\sigma(\tilde{g}_i)\cdot h_i$.

Now we look at the denominators of $\mathrm{NF}_{\sigma,I}(\tilde{h}_i)$ and $\mathrm{LC}_\sigma(\tilde{g}_i)\cdot h_i$. By hypothesis we have $p \,|\, \mathrm{den}(g_i)$, so clearly $p \,|\, \mathrm{den}(h_i)$ since g_i is monic. Notice that $\tilde{h}_i$ has integer coefficients; using the fact that $\mathrm{LT}_\sigma(g_k) >_\sigma \mathrm{LT}_\sigma(\tilde{h}_i)$ for all $k \geq i$ we can apply Lemma 2.4 to conclude that $\mathrm{NF}_{\sigma,I}(\tilde{h}_i) \in \mathbb{Z}_{\delta'}[x_1, \ldots, x_n]$ where $\delta' = \mathrm{lcm}(\mathrm{den}(g_1), \ldots, \mathrm{den}(g_{i-1}))$. By hypothesis we know that $p \nmid \delta'$, thus $p \nmid \mathrm{den}(\mathrm{NF}_{\sigma,I}(\tilde{h}_i))$. Consequently $p \nmid \mathrm{den}(\mathrm{LC}_\sigma(\tilde{g}_i) \cdot h_i)$, but since $p \mid \mathrm{den}(h_i)$, we necessarily have $p \mid \mathrm{LC}_\sigma(\tilde{g}_i)$. □

The following example illustrates claim (d).

Example 3.8. Let σ = `DegRevLex` on $\mathbb{T}^2$ and let $g_1 = y - \frac{1}{3}$, $g_2 = x - \frac{1}{6} \in \mathbb{Q}[x, y]$. Then $G = \{g_1, g_2\}$ is the reduced σ-Gröbner basis of $I = \langle G \rangle$, and $G_\mathbb{Z} = \{3y - 1,\, 2x - y,\, xy + y^2 - x\}$ is a minimal strong σ-Gröbner basis of $J = \langle \mathrm{prim}(G) \rangle \subset \mathbb{Z}[x, y]$ indexed according to claim (a). As stated in claim (d):

- since $3 \mid \mathrm{den}(g_1)$, we therefore have $3 \mid \mathrm{LC}_\sigma(\tilde{g}_1)$; indeed $\mathrm{LC}_\sigma(\tilde{g}_1)$=3.
- since $2 \mid \mathrm{den}(g_2)$ and $2 \nmid \mathrm{den}(g_1)$, we therefore have $2 \mid \mathrm{LC}_\sigma(\tilde{g}_2)$; indeed $\mathrm{LC}_\sigma(\tilde{g}_2)$=2.

The following example illustrates the fact that simply sorting the elements of a minimal strong Gröbner basis by increasing LT_σ may not satisfy claim (a).

Example 3.9. Let $P = \mathbb{Q}[x, y, z]$ with term ordering σ = `DegRevLex`. Let $g_1 = y - \frac{1}{3}$, $g_2 = x - \frac{1}{2}$ and $g_3 = z^3$. Then $G = \{g_1, g_2, g_3\}$ is the reduced Gröbner basis of the ideal $I = \langle G \rangle$, and we have $\mathrm{LT}_\sigma(g_1) <_\sigma \mathrm{LT}_\sigma(g_2) <_\sigma \mathrm{LT}_\sigma(g_3)$. A minimal strong Gröbner basis of the ideal $J = \langle \mathrm{prim}(G) \rangle \subset \mathbb{Z}[x, y, z]$ with elements indexed according to claim (a) is $G_\mathbb{Z} = \{3y - 1,\, 2x - 1,\, z^3,\, xy - x + y\}$, but clearly we have $\mathrm{LT}_\sigma(\tilde{g}_3) >_\sigma \mathrm{LT}_\sigma(\tilde{g}_4)$.

Since the set of leading coefficients is independent of the specific choice of minimal strong Gröbner basis of J, we make the following definition.

Definition 3.10. Given a finite set $F_\mathbb{Z}$ of non-zero polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$, we define $\boldsymbol{\mathrm{lcm}_\sigma(F_\mathbb{Z})}$= $\mathrm{lcm}\{\mathrm{LC}_\sigma(f) \mid f \in F_\mathbb{Z}\} \in \mathbb{Z}$, the least common multiple of all the leading coefficients in $F_\mathbb{Z}$. Given an ideal J in $\mathbb{Z}[x_1, \ldots, x_n]$ we define $\boldsymbol{\mathrm{lcm}_\sigma(J)}$= $\mathrm{lcm}_\sigma(G_\mathbb{Z})$, where $G_\mathbb{Z}$ is one of its minimal strong Gröbner bases.

Now we apply Proposition 3.7 to show that the primes appearing in $\mathrm{den}_\sigma(I)$ are the same as those appearing in the leading coefficients of any minimal strong σ-Gröbner basis of the ideal generated by the primitive integral parts of the reduced σ-Gröbner basis of I.

Theorem 3.11. *Let σ be a term ordering on $\mathbb{T}^n$, let I be a non-zero ideal in $\mathbb{Q}[x_1, \ldots, x_n]$, and let G be its reduced σ-Gröbner basis. Then* $\mathrm{rad}(\mathrm{den}(G)) = \mathrm{rad}(\mathrm{lcm}_\sigma(\langle \mathrm{prim}(G) \rangle))$.

Proof. Let $G_\mathbb{Z}$ be a minimal strong Gröbner basis of the ideal $\langle \mathrm{prim}(G) \rangle \subset \mathbb{Z}[x_1, \ldots, x_n]$. The conclusion follows from the following two claims.
Claim (1): We have $\mathrm{lcm}_\sigma(G_\mathbb{Z}) \mid \mathrm{den}_\sigma(I)$ and hence $\mathrm{rad}(\mathrm{lcm}_\sigma(G_\mathbb{Z})) \mid \mathrm{rad}(\mathrm{den}_\sigma(I))$.
Claim (2): We have $\mathrm{rad}(\mathrm{den}_\sigma(I)) \mid \mathrm{rad}(\mathrm{lcm}_\sigma(G_\mathbb{Z}))$.

For the proof we assume that the tuple $G = (g_1, \ldots, g_r)$ is the reduced σ-Gröbner basis of I, and its elements are indexed so that $\mathrm{LT}_\sigma(g_1) <_\sigma \cdots <_\sigma \mathrm{LT}_\sigma(g_r)$. We shall also assume that $G_\mathbb{Z} = \{\tilde{g}_1, \ldots, \tilde{g}_s\}$ is indexed according to Proposition 3.7.a.

Let us prove claim (1). From Proposition 3.7.c we get $\mathrm{LC}_\sigma(\tilde{g}_i) \mid \mathrm{LC}_\sigma(\mathrm{prim}(g_i))$ for every $i = 1, \ldots, r$. Moreover, it is clear that $\mathrm{LC}_\sigma(\mathrm{prim}(g_i)) = \mathrm{den}(g_i)$, hence we get $\mathrm{LC}_\sigma(\tilde{g}_i) \mid \mathrm{den}(g_i)$ for every $i = 1, \ldots, r$. Consequently, to finish the proof of claim (1) we show that $\mathrm{lcm}_\sigma(G_\mathbb{Z}) = \mathrm{lcm}_\sigma(\{\tilde{g}_1, \ldots, \tilde{g}_r\})$. Let j be an index with $s+1 \leq j \leq r$; then by Proposition 3.7.a there exists an index i with $1 \leq i \leq s$ such that $\mathrm{LT}_\sigma(\tilde{g}_i) \mid \mathrm{LT}_\sigma(\tilde{g}_j)$. Since $G_\mathbb{Z}$ is a minimal strong Gröbner basis we have that $\mathrm{LC}_\sigma(\tilde{g}_j) \mid \mathrm{LC}_\sigma(\tilde{g}_i)$. Hence $\mathrm{lcm}_\sigma(G_\mathbb{Z}) = \mathrm{lcm}_\sigma(\{\tilde{g}_1, \ldots, \tilde{g}_r\})$.

Claim (2) is an immediate consequence of Proposition 3.7.d. □

The following example shows that in Theorem 3.11 it is not sufficient that G is just a *minimal* σ-Gröbner basis of I.

Example 3.12. Let $\sigma = \texttt{DegRevLex}$ on $\mathbb{T}^3$, let $I = \langle yz - z^2,\ xy - z^2 \rangle$ be an ideal in the ring $\mathbb{Q}[x, y, z]$, then $G = \{yz - z^2,\ xy - z^2,\ xz^2 - z^3\}$ is its reduced σ-Gröbner basis. Let p be a prime. The set $G_{\min} = \{yz - z^2,\ xy - z^2,\ xz^2 - z^3 + \frac{1}{p}(yz - z^2)\}$ is a minimal, but not reduced, σ-Gröbner basis of I. Clearly $\mathrm{den}(G_{\min}) = p$. On the other hand, a minimal strong σ-Gröbner basis of the ideal $\langle \mathrm{prim}(G_{\min}) \rangle$ is $G_\mathbb{Z} = \{yz - z^2,\ xy - z^2,\ xz^2 - z^3\}$, hence $\mathrm{lcm}_\sigma(\langle \mathrm{prim}(G_{\min}) \rangle) = 1$.

The following example shows that under the assumptions of Theorem 3.11 we do not necessarily have the equality $\mathrm{den}(G) = \mathrm{lcm}_\sigma(\langle \mathrm{prim}(G) \rangle)$.

Example 3.13. Let $\sigma = \texttt{DegRevLex}$, let $I = \langle 2x - y,\ 2y - z \rangle \subset \mathbb{Q}[x, y, z]$. Its reduced σ-Gröbner basis is $G = \{y - \frac{1}{2}z,\ x - \frac{1}{4}z\}$, hence $\mathrm{den}(G) = 4$. A minimal strong Gröbner basis of the ideal $\langle \mathrm{prim}(G) \rangle$ is $G_\mathbb{Z} = \{2y - z,\ 2x - y,\ xz - y^2\}$, hence $\mathrm{lcm}_\sigma(G_\mathbb{Z}) = 2$.

Remark 3.14. We note that we can make claim 3.7.d stronger: if p is a prime satisfying the conditions in 3.7.d then the greatest power of p dividing $\mathrm{den}(g_i)$ is the same as the greatest power dividing $\mathrm{LC}_\sigma(\tilde{g}_i)$. Observe that Example 3.13 does not contradict this stronger claim.

Next we recall, using our setting and language, the definition of lucky primes according to (15). Franz Pauer described *lucky ideals* (in R) when the coefficient ring R of the polynomial ring is very general. Then he considered the case where R is a principal ideal domain. We rephrase his definition for the case $R = \mathbb{Z}$.

Definition 3.15. Let $F_\mathbb{Z} \subset \mathbb{Z}[x_1, \ldots, x_n]$ be a set of non-zero polynomials and let $G_\mathbb{Z}$ be a minimal strong σ-Gröbner basis of the ideal $\langle F_\mathbb{Z} \rangle \subset \mathbb{Z}[x_1, \ldots, x_n]$. A prime p is called **$\boldsymbol{\sigma}$-Pauer-lucky for $\boldsymbol{F}_\mathbb{Z}$** (or simply **Pauer-lucky for $\boldsymbol{F}_\mathbb{Z}$** if σ is clear from the context) if p does not divide the leading coefficient of any polynomial in $G_\mathbb{Z}$.

In (15, Proposition 6.1) Pauer proved the following relation between Pauer-lucky and good primes.

Proposition 3.16. *Let σ be a term ordering on $\mathbb{T}^n$, let $F \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a set of non-zero polynomials, and let p be a prime number. If p is Pauer-lucky for* $\mathrm{prim}(F)$ *then p is σ-good for $\langle F \rangle$.*

The inclusion stated in this proposition can be strict, as the following examples show.

Example 3.17. For instance in Example 2.10 the prime 2 is good for the ideal $\langle F\rangle$. However, the minimal strong Gröbner basis of the ideal $\langle \mathrm{prim}(F)\rangle$ is $\{2y-2z,\ x+2z\}$, hence 2 is not Pauer-lucky for $\mathrm{prim}(F)$.

Example 3.18. Let $\sigma = \mathtt{DegRevLex}$, and let $F = \{x^2y-\frac{7}{2}y,\ xy^2-\frac{3}{5}x\} \subset \mathbb{Q}[x,y]$. The reduced σ-Gröbner basis of the ideal $\langle F\rangle$ is $G = \{xy^2-\frac{3}{5}x,\ x^2-\frac{35}{6}y^2,\ y^3-\frac{3}{5}y\}$. Now we consider the two ideals $\langle \mathrm{prim}(F)\rangle$ and $\langle \mathrm{prim}(G)\rangle$ in $\mathbb{Z}[x,y]$. A minimal strong σ-Gröbner basis of $\langle \mathrm{prim}(G)\rangle$ is

$$\{6x^2-35y^2,\ 5y^3-3y,\ 5xy^2-3x,\ x^2y^2-3x^2+14y^2\}$$

A minimal strong σ-Gröbner basis of $\langle \mathrm{prim}(F)\rangle$ is

$$\{6x^2-35y^2,\ 35y^3-21y,\ 5xy^2-3x,\ 2x^2y-7y,\ x^2y^2-3x^2+14y^2\}$$

Hence $\mathrm{den}_\sigma(\langle F\rangle) = \mathrm{lcm}_\sigma(\langle \mathrm{prim}(G)\rangle) = 2\cdot 3\cdot 5$, in accordance with Theorem 3.11, while $\mathrm{lcm}_\sigma(\langle \mathrm{prim}(F)\rangle) = 2\cdot 3\cdot 5\cdot 7$. Consequently the prime 7 is not Pauer-lucky for $\mathrm{prim}(F)$, while it is a good prime for the ideal $\langle F\rangle$.

In view of the notion of Pauer-luckyness we can rephrase Theorem 3.11 as follows.

Corollary 3.19. *Let σ be a term ordering on $\mathbb{T}^n$, let $F \subset \mathbb{Q}[x_1,\dots,x_n]$ be a set of non-zero polynomials, let G be the reduced σ-Gröbner basis of the ideal $\langle F\rangle$. Then a prime number p is is Pauer-lucky for* $\mathrm{prim}(G)$ *if and only if it is σ-good for $\langle F\rangle$.*

We conclude the section by mentioning another important paper which deals with a notion of lucky primes.

Remark 3.20. In the paper (7), Elisabeth Arnold considered the case where the polynomials in F are homogeneous with respect to the standard grading, and proves that, if G is the reduced Gröbner basis of $\langle F\rangle$, a prime p is Pauer-lucky for $\mathrm{prim}(F)$ if and only if the reduced Gröbner basis of $\langle \pi_p(\mathrm{prim}(F))\rangle$ is $\pi_p(G)$. Moreover, this is also equivalent to p being Hilbert-lucky and good for $\langle F\rangle$.

For a reformulation of this result and a nice example see (8), Theorem 5 and Example 6.

4. Detecting Bad Primes

With the fundamental help of Theorem 2.11, we have seen the nice relation between ideals generated by the reductions modulo p of two reduced Gröbner bases of I when p is good for both term orderings. But what happens when p is good for one and bad for the other? We point out that the situation of knowing whether a prime is good or bad for some particular term ordering does arise in some useful circumstances, see for instance Example 4.18.

In the following we shall find it convenient to order finite sets of distinct power-products. For this reason we introduce the following definition.

Definition 4.1. Let σ be a term ordering on $\mathbb{T}^n$ and let $P = K[x_1,\dots,x_n]$.

(a) A tuple $(t_1, t_2, \dots, t_r)$ of distinct power-products in $\mathbb{T}^n$ is called ***σ*-ordered** if we have $t_1 <_\sigma t_2 <_\sigma \cdots <_\sigma t_r$. The empty tuple is σ-ordered.

(b) Let F be a set or tuple of non-zero polynomials in P. The σ-ordered tuple of the interreduction of $\mathrm{LT}_\sigma(F)$ is denoted by $\mathbf{OrdMinLT}_{\boldsymbol{\sigma}}\boldsymbol{(F)}$.

(c) Let I be an ideal in P. Then the σ-ordered tuple of the leading terms of any minimal σ-Gröbner basis of I is denoted by $\mathbf{OrdMinLT}_{\boldsymbol{\sigma}}\boldsymbol{(I)}$. In particular, if I is the zero ideal then $\mathrm{OrdMinLT}_\sigma(I)$ is the empty tuple.

Example 4.2. Let $P = \mathbb{Q}[x, y]$ and let $\sigma = \texttt{DegRevLex}$. We consider the set of polynomials $F = \{x{+}y{+}1,\ x^2{+}2x{+}y{+}1,\ y^3\}$. Observe that $\mathrm{LT}_\sigma(F) = \{x, x^2, y^3\}$ is not interreduced; interreduction produces $\mathrm{OrdMinLT}_\sigma(F) = (x, y^3)$. In contrast, working with the ideal $I = \langle F \rangle$ gives $\mathrm{OrdMinLT}_\sigma(I) = (y,\ x)$ since the reduced Gröbner basis is $\{x{+}1,\ y\}$.

We define a total ordering on the σ-ordered tuples of distinct power-products.

Definition 4.3. Let σ be a term ordering on the monoid $\mathbb{T}^n$, and let $T = (t_1, \dots, t_r)$ and $T' = (t'_1, \dots, t'_{r'})$ be σ-ordered tuples of distinct power-products in $\mathbb{T}^n$. We say that $\boldsymbol{T}$ ***σ*-precedes** $\boldsymbol{T'}$ and write $\boldsymbol{T \prec_\sigma T'}$ if either T' is a proper prefix of T, *i.e.* $r' < r$ and $t_i = t'_i$ for all $i = 1, \dots, r'$, or there exists an index $k \in \{1, \dots, \min(r, r')\}$ such that $t_i = t'_i$ for every $i = 1, \dots, k{-}1$ and $t_k <_\sigma t'_k$.

We write $\boldsymbol{T \preceq_\sigma T'}$ to mean either $T \prec_\sigma T'$ or $T = T'$.

Remark 4.4. We observe that "σ-precedes" is just the "σ-lexicographical" ordering on the σ-ordered tuples (T, x^∞) where T is a σ-ordered tuple of distinct power-products, and x^∞ is σ-greater than any power-product. For instance, we now easily see that every non-empty tuple σ-precedes the empty tuple.

Example 4.5. Let $\sigma = \texttt{DegRevLex}$; we compare these tuples:

$(x, y, z) \prec_\sigma (x, y)$ — since $z <_\sigma x^\infty$, equiv. (x, y) is a proper prefix

$(x, y) \prec_\sigma (x, y^2, z)$ — since $y <_\sigma y^2$

Proposition 4.6. *Let $P = K[x_1, \dots, x_n]$, and σ be a term ordering on $\mathbb{T}^n$. Let J be an ideal in P, and let F be a set of non-zero polynomials in J.*

(a) $\mathrm{OrdMinLT}_\sigma(J) = \mathrm{OrdMinLT}_\sigma(F)$ *if and only if F is a σ-Gröbner basis of J.*

(b) $\mathrm{OrdMinLT}_\sigma(J) \prec_\sigma \mathrm{OrdMinLT}_\sigma(F)$ *if F is not a σ-Gröbner basis of J.*

Proof. By definition, $F \subseteq J$ is a σ-Gröbner basis of J if and only if $\mathrm{LT}_\sigma(F)$ generates $\mathrm{LT}_\sigma(I)$. Hence claim (a) follows. Now we prove claim (b).

Since F is not a σ-Gröbner basis of J, we have $\mathrm{OrdMinLT}_\sigma(F) \neq \mathrm{OrdMinLT}_\sigma(J)$. If it happens that $\mathrm{OrdMinLT}_\sigma(F)$ is a proper prefix of $\mathrm{OrdMinLT}_\sigma(J)$, the conclusion follows immediately. So we assume that $\mathrm{OrdMinLT}_\sigma(F)$ is not a proper prefix. Note that $\mathrm{OrdMinLT}_\sigma(J)$ cannot be a proper prefix of $\mathrm{OrdMinLT}_\sigma(F)$ as otherwise this would imply that there is $f \in F \subset J$ with $\mathrm{LT}_\sigma(f) \notin \mathrm{LT}_\sigma(J)$.

Let $\mathrm{OrdMinLT}_\sigma(F) = (t_1, t_2, \dots)$, let $\mathrm{OrdMinLT}_\sigma(J) = (t'_1, t'_2, \dots)$, and let k be the first index such that $t_k \neq t'_k$. Since $F \subset J$ we know that $t_k \in \mathrm{LT}_\sigma(J)$, and hence t_k is a multiple of some element of $\mathrm{OrdMinLT}_\sigma(J)$. Since $\mathrm{OrdMinLT}_\sigma(F)$ is interreduced, t_k is not a multiple of any of the other t_j, and thus specifically not a multiple of any of $t'_1, \dots, t'_{k-1}$. Hence t_k can only be a non-trivial multiple of t'_k or a multiple of t'_j for some index $j > k$. Either way $t_k >_\sigma t'_k$, and so $\mathrm{OrdMinLT}_\sigma(J) \prec_\sigma \mathrm{OrdMinLT}_\sigma(F)$ as claimed. □

The next example illustrates the importance of $\mathrm{OrdMinLT}_\sigma(F)$ being interreduced.

Example 4.7. Let $P = K[x, y]$ and let σ=`DegRevLex`. Let $J = \langle x, y^3 \rangle$ and consider the σ-ordered tuple $T = (x, x^2, y^3)$; the elements of T are clearly non-zero polynomials in J. We observe that $\mathrm{OrdMinLT}_\sigma(J) = \mathrm{OrdMinLT}_\sigma(T) = (x, y^3)$. However, the tuple T is not interreduced, and we have $T \prec_\sigma \mathrm{OrdMinLT}_\sigma(J)$.

We recall here a standard result from the theory of Gröbner bases; for the sake of completeness we include the proof.

Lemma 4.8. *Let $P = K[x_1, \dots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, and let I, J be ideals in P. If $I \subsetneq J$ then $\mathrm{LT}_\sigma(I) \subsetneq \mathrm{LT}_\sigma(J)$.*

Proof. Since $I \subsetneq J$ we clearly have $\mathrm{LT}_\sigma(I) \subseteq \mathrm{LT}_\sigma(J)$. Let $f \in J \setminus I$ with minimal σ-leading term, thus $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma(J)$. However, by the minimality of $\mathrm{LT}_\sigma(f)$ we see that f cannot be head-reduced by any element of a σ-Gröbner basis of I. Hence we conclude that $\mathrm{LT}_\sigma(f) \notin \mathrm{LT}_\sigma(I)$. □

We are ready to prove the following interesting result.

Corollary 4.9. *Let $P = K[x_1, \dots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, and let I, J be ideals in P. If $I \subsetneq J$ then $\mathrm{OrdMinLT}_\sigma(J) \prec_\sigma \mathrm{OrdMinLT}_\sigma(I)$.*

Proof. Let G_σ be a σ-Gröbner basis of I. Thus G_σ is a set of non-zero polynomials in J. By Proposition 4.6 we have $\mathrm{OrdMinLT}_\sigma(J) \preceq_\sigma \mathrm{OrdMinLT}_\sigma(G_\sigma) = \mathrm{OrdMinLT}_\sigma(I)$. From Lemma 4.8 and the assumption that $I \subsetneq J$ the conclusion follows. □

Next we prove another useful result.

Lemma 4.10. *Let σ be a term ordering on $\mathbb{T}^n$. Let $T = (t_1, t_2, \dots, t_r)$ be an interreduced σ-ordered tuple of elements in $\mathbb{T}^n$, let T' be a set of elements in $\mathbb{T}^n$. Assume that there exists an index $k \le r$ such that $t_1, \dots, t_{k-1} \in T'$ and there exists $t' \in T'$ satisfying $t' <_\sigma t_k$ and t' is not divisible by any t_i. Then we have $\mathrm{OrdMinLT}_\sigma(T') \prec_\sigma T$ and T is not a proper prefix of $\mathrm{OrdMinLT}_\sigma(T')$.*

Proof. Let $t'_{\min} = \min_\sigma\{t' \in T' \mid t' \text{ not divisible by any } t \in T\}$. Let t_j be the first element of T satisfying $t_j >_\sigma t'_{\min}$. Observe that $j \le k$, so from the definition of k we know that $t_1, \dots, t_{j-1} \in T'$.

Now we define the tuple $\overline{T'} = (t_1, \dots, t_{j-1}, t'_{\min})$, and observe that it is σ-ordered. The set of power-products in $\overline{T'}$ is interreduced: we already know that $\{t_1, \dots, t_{j-1}\}$ is interreduced, and $t'_{\min}$ is not divisible by any of them; on the other hand, we see that $t'_{\min}$ cannot divide any of them because it is the σ-greatest element. We also clearly have that $\overline{T'} \prec_\sigma T$ since $t'_{\min} <_\sigma t_j$.

We conclude by proving that $\mathrm{OrdMinLT}_\sigma(T') \preceq_\sigma \overline{T'}$; to do this we show that $\overline{T'}$ is a prefix of $\mathrm{OrdMinLT}_\sigma(T')$. We have already seen that $\overline{T'}$ is an interreduced subset of T', so it suffices to show that each element of T' (or, equivalently, of $T' \setminus \overline{T'}$) is σ-greater-than $t'_{\min}$ or is a multiple of an element of $\overline{T'}$.

Let $s' \in T'$; we shall argue depending on whether s' is divisible by some element of the tuple T. First we consider the case where s' is not divisible by any $t_i \in T$. By definition of $t'_{\min}$ we see that $s' \geq_\sigma t'_{\min}$; if $s' = t'_{\min}$ it is trivially a multiple of an element of $\overline{T'}$, otherwise $s' >_\sigma t'_{\min}$ as claimed. We address now the case where s' is a multiple of some $t_i \in T$. If $i < j$ then s' is clearly a multiple of an element of $\overline{T'}$; otherwise $i \geq j$, so $s' \geq_\sigma t_i \geq_\sigma t_j >_\sigma t'_{\min}$. □

The following example illustrates the steps in this proof.

Example 4.11. Let $\sigma = \texttt{DegRevLex}$. Consider the interreduced σ-ordered tuple T and the set T':

$$\begin{aligned} T &= (xyz, x^3, \boxed{x^2y^2}, xz^4, y^6, z^7) \\ T' &= \{xyz, x^3, x^2z^2, \boxed{xy^2}, y^7, x^2y^8\}. \end{aligned}$$

We take $k = 3$, so $t_k = x^2y^2$, and $t' = xy^2$, which is not a multiple of any power-product in T: these choices satisfy the hypotheses of the lemma. Following through the proof we have $t'_{\min} = t'$, $j = 2$ and $\overline{T'} = (xyz, \boxed{xy^2})$, and we see clearly that $\overline{T'} \prec_\sigma T$. We compute the tuple $\mathrm{OrdMinLT}_\sigma(T') = (xyz, \boxed{xy^2}, x^3, x^2z^2, y^7)$, and observe that $\overline{T'}$ appears as a (proper) prefix. Consequently $\mathrm{OrdMinLT}_\sigma(T') \prec_\sigma \overline{T'} \prec_\sigma T$.

The following easy example shows the importance of the non-divisibility assumption in the lemma.

Example 4.12. Let $\sigma = \texttt{DegRevLex}$ and let $T = (x, y^3)$, an interreduced σ-ordered tuple. Now let $T' = \{x, x^2, y^4, z^4\}$. For $k = 1$ there is no $t' \in T'$ with $t' <_\sigma t_k$; and for $k = 2$ the only elements of T' which are σ-less-than t_k are x and x^2, but both are divisible by t_1. So we cannot apply the lemma. Indeed, $\mathrm{OrdMinLT}_\sigma(T') = (x, y^4, z^4)$, and we have $T \prec_\sigma \mathrm{OrdMinLT}_\sigma(T')$.

Now we are ready to prove the main theorem.

Theorem 4.13. *Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, let σ, τ be two term orderings on $\mathbb{T}^n$, let I be a non-zero ideal in P, and let p be a prime which is σ-good for I.*

(a) If p is τ-good for I, we have $\mathrm{OrdMinLT}_\tau(I_{(p,\,\sigma)}) = \mathrm{OrdMinLT}_\tau(I)$.

(b) If p is τ-bad for I, we have $\mathrm{OrdMinLT}_\tau(I_{(p,\,\sigma)}) \prec_\tau \mathrm{OrdMinLT}_\tau(I)$, and also that $\mathrm{OrdMinLT}_\tau(I)$ is not a proper prefix of $\mathrm{OrdMinLT}_\tau(I_{(p,\,\sigma)})$.

Proof. Let G_τ be the reduced τ-Gröbner basis of I, and G_σ be the reduced σ-Gröbner basis for I.

We start by proving claim (a). By hypothesis, p is both σ-good and τ-good for I, hence Theorem 2.11.b implies that the reduced τ-Gröbner basis of $I_{(p,\,\sigma)}$ is $\pi_p(G_\tau)$ which has the same leading terms as G_τ, and the conclusion follows immediately from Remark 2.7.b.

Now we prove claim (b). Let $G_\tau = \{g_1, \ldots, g_r\}$ where the elements are indexed so that $\mathrm{LT}_\tau(g_i) <_\tau \mathrm{LT}_\tau(g_{i+1})$ for $i = 1, \ldots, r{-}1$. For $i = 1, \ldots, r$, let $\tilde{g}_i = \mathrm{prim}(g_i)$ so in particular $\pi_p(\tilde{g}_i) \neq 0$. Define the following τ-ordered tuple T and set T'

$$\begin{aligned} T &= (\quad \mathrm{LT}_\tau(g_1) \quad, \ \ldots \ , \quad \mathrm{LT}_\tau(g_r) \quad) \ \text{ which is just } \mathrm{OrdMinLT}_\tau(I) \\ T' &= \{\ \mathrm{LT}_\tau(\pi_p(\tilde{g}_1)) \ , \ \ldots \ , \ \mathrm{LT}_\tau(\pi_p(\tilde{g}_r)) \ \} \end{aligned}$$

By definition of π_p we have $\mathrm{LT}_\tau(\pi_p(\tilde{g}_i)) \leq_\tau \mathrm{LT}_\tau(g_i)$ for all i. Since p is τ-bad, there is at least one index j such that p divides the denominator of $g_j \in G_\tau$, hence it divides also the leading coefficient of $\tilde{g}_j$. Therefore $\mathrm{LT}_\tau(\pi_p(\tilde{g}_j)) <_\tau \mathrm{LT}_\tau(g_j)$; let k be the smallest such index. Moreover, since G_τ is a reduced Gröbner basis, $\mathrm{LT}_\tau(\pi_p(\tilde{g}_k))$ is not a multiple of any element of $\mathrm{LT}_\tau(G_\tau)$. Therefore we can apply Lemma 4.10 to T and T' with the above value of k and deduce that $\mathrm{OrdMinLT}_\tau(T') \prec_\tau T = \mathrm{OrdMinLT}_\tau(I)$, and that $\mathrm{OrdMinLT}_\tau(I)$ is not a proper prefix of $\mathrm{OrdMinLT}_\tau(T')$.

Let $F = \{\pi_p(\tilde{g}_1), \ldots, \pi_p(\tilde{g}_r)\}$. By Proposition 2.5.b we deduce that $F \subseteq I_{(p,\,\sigma)}$. Hence Proposition 4.6 implies that $\mathrm{OrdMinLT}_\tau(I_{(p,\,\sigma)}) \preceq_\tau \mathrm{OrdMinLT}_\tau(F) = \mathrm{OrdMinLT}_\tau(T')$.

Combining the two inequalities, the conclusion follows. □

This theorem enables us to detect some bad primes without having to compute the reduced τ-Gröbner basis of I over the rationals.

Corollary 4.14. *Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, let σ and τ be two term orderings on $\mathbb{T}^n$, and let I be a non-zero ideal in P. Let p and q be σ-good primes for I.*
If $\mathrm{OrdMinLT}_\tau(I_{(q,\,\sigma)}) \prec_\tau \mathrm{OrdMinLT}_\tau(I_{(p,\,\sigma)})$ then q is τ-bad for I.

Proof. By Theorem 4.13 we know that $\mathrm{OrdMinLT}_\tau(I_{(p,\,\sigma)}) \preceq_\tau \mathrm{OrdMinLT}_\tau(I)$. Hence $\mathrm{OrdMinLT}_\tau(I_{(q,\,\sigma)}) \prec_\tau \mathrm{OrdMinLT}_\tau(I)$, so Theorem 4.13(a) implies that the prime q is τ-bad for I. □

Example 4.15. In the polynomial ring $\mathbb{Q}[x,y,z]$ with term ordering $\sigma = \texttt{DegRevLex}$, let $F = \{x^2y + 7xy^2 - 2,\ y^3 + x^2z,\ z^3 + x^2 - y\}$ and let $I = \langle F \rangle$. It turns out that all primes are σ-good for I, and we have

$$\mathrm{OrdMinLT}_\sigma(I) = \mathrm{OrdMinLT}_\sigma(I_{(p,\sigma)}) = (z^3,\ y^3,\ x^2y,\ x^4z,\ x^6) \quad \text{for all primes } p.$$

Now we consider the term ordering $\tau = \texttt{Lex}$. It turns out that the set of τ-bad primes for I smaller than 10^8 is $S = \{2,\ 7,\ 11,\ 55817\}$. We have

$$\mathrm{OrdMinLT}_\tau(I) = \mathrm{OrdMinLT}_\tau(I_{(p,\tau)}) = (z^{26},\ y,\ x) \quad \text{for all primes } p \notin S.$$

For the bad primes we obtain:

- $\mathrm{OrdMinLT}_\tau(I_{(2,\sigma)}) = (z^{17},\ yz,\ y^3,\ xz^6,\ xy^2,\ x^2)$
- $\mathrm{OrdMinLT}_\tau(I_{(7,\sigma)}) = (z^{13},\ y,\ x^2)$
- $\mathrm{OrdMinLT}_\tau(I_{(11,\sigma)}) = \mathrm{OrdMinLT}_\tau(I_{(55817,\sigma)}) = (z^{25},\ yz,\ y^2,\ x)$

Another important consequence of the theorem is that a prime may be "partly good", that is some of the elements in the Gröbner basis have good reductions.

Corollary 4.16. *Let $P = \mathbb{Q}[x_1, \ldots, x_n]$, let σ and τ be two term orderings on $\mathbb{T}^n$, and let I be a non-zero ideal in P. Next, we let G_σ be its reduced σ-Gröbner basis, and let $G_\tau = \{g_1, g_2, \ldots\}$ be its reduced τ-Gröbner basis, whose elements are indexed so that $\mathrm{LT}_\tau(g_1) <_\tau \mathrm{LT}_\tau(g_2) <_\tau \cdots$. Let p be a σ-good but τ-bad prime for I, and let $\widetilde{G}_\tau = \{\tilde{g}_1, \tilde{g}_2, \ldots\}$ be the reduced τ-Gröbner basis of $I_{(p,\sigma)}$ with elements indexed so that $\mathrm{LT}_\tau(\tilde{g}_1) <_\tau \mathrm{LT}_\tau(\tilde{g}_2) <_\tau \cdots$.*

(a) There is an index j such that $\mathrm{LT}_\tau(\tilde{g}_j) \neq \mathrm{LT}_\tau(g_j)$; let k be the smallest such index.

(b) We have $\tilde{g}_j = \pi_p(g_j)$ for $j = 1, \ldots, k-1$.

Proof. By Theorem 4.13 we see that $\mathrm{OrdMinLT}_\tau(I_{(p,\sigma)}) \prec_\tau \mathrm{OrdMinLT}_\tau(I)$ and also that $\mathrm{OrdMinLT}_\tau(I)$ is not a proper prefix of $\mathrm{OrdMinLT}_\tau(I_{(p,\sigma)})$ so it is clear that k exists, and (a) is proved.

Now we prove claim (b). Since p is a τ-bad prime, there is a smallest index j such that $p \,|\, \mathrm{den}(g_j)$. By Proposition 2.5.b we have $\pi_p(\mathrm{prim}(g_j)) \in I_{(p,\sigma)}$, hence $\pi_p(\mathrm{prim}(g_j))$ reduces to zero by $\widetilde{G}_\tau$. By choice of j we have $\mathrm{LT}_\tau(\pi_p(\mathrm{prim}(g_j))) <_\tau \mathrm{LT}_\tau(g_j)$. Now we cannot have $j < k$ because otherwise there must be a $\tilde{g}_i \in \widetilde{G}_\tau$ with index $i < j$ which reduces $\pi_p(\mathrm{prim}(g_j))$, but this cannot happen because g_j came from a reduced τ-Gröbner basis, so $\mathrm{LT}_\tau(\pi_p(\mathrm{prim}(g_j)))$ is not divisible by any element of $\mathrm{OrdMinLT}_\tau(I_{(p,\sigma)})$. Hence we must have $j \geq k$.

For each $i = 1, \ldots, k-1$ we have that $\pi_p(g_i) \in I_{(p,\sigma)}$, so $\pi_p(g_i)$ will reduce to zero upon "Gröbner division" by $\{\tilde{g}_1, \ldots, \tilde{g}_{k-1}\} \subset \widetilde{G}_\tau$. Since $\mathrm{LT}_\tau(\pi_p(g_i)) = \mathrm{LT}(g_i)$ the only reducer for $\pi_p(g_i)$ is $\tilde{g}_i$. Now let $h = \pi_p(g_i) - \tilde{g}_i \in I_{(p,\sigma)}$, so if $h \neq 0$ then $\mathrm{LT}_\tau(h) <_\tau \mathrm{LT}_\tau(g_i)$ and also, since $\widetilde{G}_\tau$ is a reduced τ-Gröbner basis, we know that $\mathrm{LT}_\tau(h)$ is not divisible by any of $\mathrm{LT}_\tau(g_1), \ldots, \mathrm{LT}_\tau(g_i)$ contradicting the fact that h must reduce to zero. □

To conclude the paper we show two examples illustrating the merits of Corollary 4.14.

Example 4.17. Let $P = \mathbb{Q}[x, y, z, w, s, t]$, let $\sigma = \mathtt{Lex}$ and τ be any elimination ordering for $[s, t]$ which restricts to $\mathtt{DegRevLex}$ on $\mathbb{T}(x, y, z, w)$. Let $f_1 = t^3$, $f_2 = st^2 - 2s^2$, $f_3 = s^2t - 5$, $f_4 = s^3 - 7t$, and let $J = \langle x - f_1,\ y - f_2,\ z - f_3,\ w - f_4 \rangle$. Obviously every prime is σ-good, but we do not know which ones are τ-good. A direct computation of the reduced τ-Gröbner basis of J shows that $\mathrm{den}_\tau(J) = 42 = 2 \cdot 3 \cdot 7$. Let us check that a good use of Corollary 4.14 makes it possible to identify these numbers as τ-bad primes *without computing* G_τ over the rationals.

Let use choose $p = 101$. For $\mathrm{OrdMinLT}_\tau(I_{(p,\sigma)})$ we get the following tuple

$$[z^5,\ yz^4,\ y^2z^3,\ y^3z^2,\ xy^2z^2,\ y^4z,\ xy^3z,\ y^5,\ xy^4,\ y^4w^2,\ \boxed{y^2z^2w^3},\ xz^4w^2,\ xyz^3w^2,\ x^2z^3w^2,\ x^2z^4w,$$
$$x^2yz^3w,\ x^3z^3w,\ sz,\ sy,\ sx,\ tz^2,\ tyz,\ txz,\ ty^2,\ txy,\ tx^2,\ tw^3,\ sw^3,\ tzw^2,\ tyw^2,\ txw^2,\ t^2,\ st,\ s^2]$$

For $p = 2$ we compute $\mathrm{OrdMinLT}_\tau(I_{(p,\sigma)})$ obtaining the following tuple

$$[y^2,\ z^5,\ yz^4,\ ty,\ sy,\ tx,\ sx,\ tz^3,\ sz^3,\ t^2,\ stz,\ s^2z,\ s^2t,\ s^3]$$

Clearly $\mathrm{OrdMinLT}_\tau(I_{(2,\sigma)}) \prec_\tau \mathrm{OrdMinLT}_\tau(I_{(101,\sigma)})$ hence 2 is a τ-bad prime for J.

For the prime $p = 7$ we compute the tuple $\mathrm{OrdMinLT}_\tau(I_{(p,\sigma)})$ to be the following

$$[z^3,\ y^2z^2,\ y^3z,\ y^4,\ sz,\ sy,\ sx,\ tw^2,\ sw^2,\ tzw,\ tz^2,\ tyz,\ ty^2,\ t^2w,\ stw,\ s^2w,\ t^3,\ st^2,\ s^2t,\ s^3]$$

Again, $\mathrm{OrdMinLT}_\tau(I_{(2,\sigma)}) \prec_\tau \mathrm{OrdMinLT}_\tau(I_{(101,\sigma)})$ and hence 7 is a τ-bad prime for J.

We observe a more interesting situation for $p = 3$. We compute $\mathrm{OrdMinLT}_\tau(I_{(p,\sigma)})$ to be the following

$$[z^5,\ yz^4,\ y^2z^3,\ y^3z^2,\ xy^2z^2,\ y^4z,\ xy^3z,\ y^5,\ xy^4,\ y^4w^2,\ \boxed{xz^3w^3},\ xz^4w^2,\ xyz^3w^2,\ x^2z^3w^2,\ x^2z^4w,$$
$$x^2yz^3w,\ x^3z^3w,\ sz,\ sy,\ sx,\ tz^2,\ tyz,\ txz,\ ty^2,\ txy,\ tx^2,\ tw^3,\ sw^3,\ tzw^2,\ tyw^2,\ txw^2,\ t^2,\ st,\ s^2]$$

If we compare $\mathrm{OrdMinLT}_\tau(I_{(3,\sigma)})$ with $\mathrm{OrdMinLT}_\tau(I_{(101,\sigma)})$ we observe that the only difference is the boxed entries. Since $xz^3w^3 <_\tau y^2z^2w^3$ we see that $\mathrm{OrdMinLT}_\tau(I_{(3,\sigma)}) \prec_\tau \mathrm{OrdMinLT}_\tau(I_{(101,\sigma)})$ and hence also 3 is a τ-bad prime for J.

It is important to observe that the arguments used to show that 2, 3, and 7 are τ-bad primes for J cannot be used to conclude that 101 is a τ-good prime for J.

The second example shows how some of the new ideas presented in the paper help the computation of an implicitization.

Example 4.18. In the polynomial ring $\mathbb{Q}[s,t]$ we let

$$f_1 = st^5 - st^3 - t, \quad f_2 = s^3 - st - t^2 - 1, \quad f_3 = s^2t^2 - s, \quad f_4 = s^4$$

and in the polynomial ring $\mathbb{Q}[x,y,z,w,s,t]$ we let $I = \langle x - f_1,\ y - f_2,\ z - f_3,\ w - f_4\rangle$. Observe that these generators form a reduced `Lex`-Gröbner basis so we can immediately tell whether a prime is good or bad for `Lex`. Consequently we can use Corollary 4.14 for the computation of the implicitization $I \cap \mathbb{Q}[x,y,z,w]$. Using a first implementation of our modular approach this computation takes about 22 seconds on a MacBook Pro 2.9GHz Intel Core i7. The result is a Gröbner basis of $I \cap \mathbb{Q}[x,y,z,w]$ which contains 62 polynomials. The *biggest* among these polynomials has 517 power products in its support. The *biggest numerator* is an integer with 18 digits and the *biggest denominator* is an integer with 13 digits. We require the computation modulo 5 primes to reconstruct the correct result.

References

[1] J. Abbott, *Fault-Tolerant Modular Reconstruction of Rational Numbers*, `arXiv:1303.2965v2`, 2015; to appear in J. Symb. Comp. **(80)**, 2017, p. 707–718

[2] J. Abbott and A.M. Bigatti, *CoCoALib: a C++ library for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it/cocoalib`

[3] J. Abbott, A.M. Bigatti, L. Robbiano, *CoCoA: a system for doing Computations in Commutative Algebra.* Available at `http://cocoa.dima.unige.it`

[4] J. Abbott, A. Bigatti, L. Robbiano, *Implicitization of Hypersurfaces* J. Symb. Comput. **(81)**, 2017, p. 20–40.

[5] J. Abbott, A. Bigatti, E. Palezzato, L. Robbiano, *Computing and Using Minimal Polynomials*, `arXiv:1704.03680`, 2017.

[6] W.W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathemamatics, Vol 3, American Mathematical Society, 1994.

[7] E.A. Arnold, *Modular algorithms for computing Gröbner bases*, J. Symb. Comput. **(35)**, 2003, p. 403–419.

[8] J. Böhm, W. Decker, C. Fieker, S. Laplagne, G. Pfister, *Bad primes in Computational Algebraic Geometry*, `arXiv:1702.06920v1`, 2017.

[9] B. Buchberger, *Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory*, in: (N.K. Bose, Ed.) *Multidimensional Systems Theory.* D. Reidel Publ. Comp. Pp., 1985, 184–232.

[10] W. Decker, G-M. Greuel, G. Pfister, H. Schönemann, SINGULAR– *A computer algebra system for polynomial computations.* Available at `http://www.singular.uni-kl.de`

[11] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, Springer, Heidelberg, 2000 (second edition 2008).

[12] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 2*, Springer, Heidelberg, 2005.

[13] M. Kreuzer and L. Robbiano, *Computational Linear and Commutative Algebra*, Springer, Heidelberg, 2016.

[14] T. Mora L. Robbiano, *The Gröbner Fan of an Ideal*, J. Symb. Comput. **(6)**, 1988, p. 183–208.

[15] F. Pauer, *On Lucky Ideals for Gröbner basis Computations*, J. Symb. Comput. **(14)**, 1992, p. 471–482.

[16] F. Winkler, *A p-adic Approach to the Computation of Gröbner bases*, J. Symb. Comput. **(6)**, 1978, p. 287–304..