Computations with Frobenius Powers

Susan Hermiller and Irena Swanson

CONTENTS

It is an open question whether tight closure commutes with localization in quotients of a polynomial ring in finitely many variables over a field. Katzman [Katzman 98] showed that tight closure of ideals in these rings commutes with localization at one element, if for all ideals I and J in a polynomial ring there is a linear upper bound in q on the degree in the least variable of reduced Grobner bases in reverse lexicographic ordering of the ideals of the form $J + I^{[q]}$. Katzman conjectured that this property would always be satisfied. In this paper we prove several cases of Katzman's conjecture. We also provide an experimental analysis (with proofs) of asymptotic properties of Grobner bases connected with Katzman's conjectures.

1. INTRODUCTION

Throughout this paper, F is a field of prime characteristic p, R is a finitely generated polynomial ring $F[x_1, \ldots, x_n]$ over F, J and I denote ideals of R, and $q = p^e$ denotes a power of p, where e is a nonnegative integer. Then $I^{[q]}$ is the *e th Frobenius power of* I, defined by

$$I^{[q]} := (i^q | i \in I).$$

It follows that if I is generated by $f_1, \ldots, f_r$, then $I^{[q]}$ is generated by $f_1^q, \ldots, f_r^q$.

The main motivation for our work in this paper is the theory of tight closure, in which Frobenius powers of ideals play a central role. In particular, we address the question of whether tight closure commutes with localization. The basics of tight closure can be found in the first few sections of [Hochster and Huneke 90]; however, in the following paper no knowledge of tight closure will be needed.

The polynomial ring R is a regular ring, so every ideal in R, and in the localizations of R, is tightly closed [Hochster and Huneke 90, Theorem 4.4], and thus tight closure commutes with localization in R. However, it is not known if tight closure commutes with localization in quotient rings R/J of R, even for the special case of localization at a multiplicatively closed set $\{1, r, r^2, r^3, \ldots\}$,

2000 AMS Subject Classification: Primary 13P10, 13A35

Keywords: Frobenius powers, Gröbner bases, tight closure, binomial ideals

generated by one element $r \in R/J$. Katzman [Katzman 98] showed that for this special case it suffices to consider the case $r = x_n$ (by possibly modifying R, I, and J). Katzman also proved that a positive answer to the question of tight closure commuting with localization at x_n would be provided by a positive answer to the following conjecture.

Conjecture 1.1. [Katzman 98, Conjecture 4] *Let $R = F[x_1, ..., x_n]$ where F is a field of characteristic p, and let I and J be ideals of R. Let G_q be the reduced Gröbner basis for the ideal $J + I^{[q]}$ with respect to the reverse lexicographic ordering. Then there exists an integer α such that the degrees in x_n of the elements of G_q are bounded above by αq.*

The *(graded) reverse lexicographic ordering* on monomials in $x_1, \dots, x_n$ is defined by $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} < x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$ if $\sum_i a_i < \sum_i b_i$, or if $\sum_i a_i = \sum_i b_i$ and $a_i > b_i$ for the last index i at which a_i and b_i differ. For background on reduced Gröbner bases and Buchberger's algorithm for finding these bases, see, for example, [Cox et al. 92].

Katzman's conjecture holds trivially when $J = (0)$, since Frobenius powers commute with sums in rings of characteristic p, and hence the reduced reverse lexicographic Gröbner basis for $I^{[q]}$ consists of the qth powers of elements of the reduced Gröbner basis for I. The other known cases are due to Katzman, who proved that the conjecture also holds whenever J is generated by monomials [Katzman 98, Theorem 8], and whenever J is generated by binomials and simultaneously I is generated by monomials [Katzman 98, Corollary 11]. There are classes of examples for which it is known that tight closure commutes with localization but for which Katzman's conjecture has not been proved; in particular, one such class, due to Smith [Smith 01], consists of ideals I and J for which J is a binomial ideal and I is arbitrary. Since the question of whether tight closure commutes with localization has so far defied proof for quotient rings of polynomial rings, the proof of Katzman's conjecture is expected to be hard. Difficulties in finding a general proof include the dependence of Gröbner bases on the characteristic of the field F and the dependence of Gröbner bases on raising a subset of the generators to powers.

In this paper, we study the asymptotic behavior of three functions of q associated with the family of reduced reverse lexicographic Gröbner bases G_q for the ideals $J + I^{[q]}$, namely:

(1) the maximum of the x_n-degrees of the elements of G_q (as in Katzman's conjecture), also written as the x_n-degree of G_q and denoted $\delta(q)$;

(2) the maximum of the total degrees of the elements of G_q, also referred to as the total degree of G_q and denoted $\Delta(q)$; and

(3) the cardinality $c(q)$ of G_q.

Since for any ideals I and J we have $\delta(q) \leq \Delta(q)$ for all q, a linear upper bound for $\Delta(q)$ also implies Katzman's conjecture.

In Section 2 of this paper, we prove (Theorem 2.1) that Katzman's conjecture holds for polynomial rings in one or two variables with arbitrary ideals I and J, and we find a linear upper bound for $\Delta(q)$ and a constant upper bound for $c(q)$ as well. (As part of the proof of this theorem, we include a review of the steps of the Buchberger algorithm for reduced Gröbner basis computation.)

In Sections 3 and 4, we provide further information about the specific form of the functions $\delta(q)$ and $\Delta(q)$, as well as the function $c(q)$, in the more restrictive case in which I and J are both principal binomial (and not monomial) ideals, and in the even more restrictive case of monoidal ideals, both to gain better understanding of these functions and to find constructive proofs of special cases of Katzman's conjecture with potential for application in more general cases. A *binomial* ideal is an ideal generated by binomials, i.e., polynomials of the form $x^v - gx^w$, where x^v and x^w are (monic) terms, and $g \in F$. Such a polynomial is called a *monomial* if $g = 0$, and it is called *monoidal* if $g = 1$ so that the coefficients of the polynomial are restricted to $+1$ and -1. We refer to an ideal generated by monoidal polynomials as a *monoidal ideal*. When I and J are monoidal ideals, the quotient rings $R/(J + I^{[q]})$ are monoid rings over F for finitely presented commutative monoids, and the Gröbner bases for the ideals $J + I^{[q]}$ can also be considered to be finite complete rewriting systems in the category of commutative monoids.

In Section 3, we compute (in Theorem 3.2) Gröbner bases for the ideals $J + I^{[q]}$ for ideals $I = (x^u(x^v - gx^w))$ and $J = (x^a(x^b - hx^c))$ whenever g and h are units, $\gcd(x^u, x^w) = 1 = \gcd(x^b, x^c)$, and $(x^v - gx^w, x^b - hx^c) = R$, and hence obtain a constructive proof of upper bounds for $\delta(q)$, $\Delta(q)$, and $c(q)$ in this case. In Theorem 3.3 we prove that for "most" principal binomial ideals I and J, there is a change of variables that converts I and J into monoidal ideals. This change of variables preserves both the reverse lexicographic ordering on the monomials and on all three of the functions $\delta(q)$, $\Delta(q)$, and $c(q)$.

In Section 4, we study the asymptotic behavior of the three functions $\delta(q)$, $\Delta(q)$, and $c(q)$ for constructions of the reduced Gröbner bases G_q for a wide range of examples of principal monoidal ideals I and J. We give examples illustrating that the three functions can be linear, periodic, or have linear expressions holding only for q sufficiently large. In addition, we show examples in which the cardinality and the x_n-degree of the Gröbner bases can be bounded above by a constant for all q. We also discuss the dependence of the three functions on the characteristic p of the field F for several of the examples. Section 4 ends with a table summarizing the range of types of behavior of the Gröbner bases we computed. Finally, in Section 5, we include a sample of the Macaulay2 [Grayson and Stillman 03] code we used to generate Gröbner bases for small values of q as an aid to our proofs.

2. SPECIAL CASES OF KATZMAN'S CONJECTURE

As mentioned in the introduction, several special cases of Katzman's conjecture are known to be true: when $J = (0)$, or J is generated by monomials (with arbitrary ideal I), or J is generated by binomials and I by monomials [Katzman 98]. In all three cases, Katzman's proof also shows a linear upper bound for the function $\Delta(q)$.

We prove in this section another special case of Katzman's conjecture, namely for $n \leq 2$.

Theorem 2.1. *Katzman's conjecture holds when R is a polynomial ring in one or two variables over F. Moreover, for any ideals I and J in R and reduced Gröbner basis G_q for the ideal $J + I^{[q]}$ with respect to the reverse lexicographic ordering, there exist integers α and β such that the x_n-degree and total degree functions satisfy $\delta(q) \leq \Delta(q) \leq \alpha q$ and the cardinality function satisfies $c(q) \leq \beta$ for all q.*

Proof: If R is a polynomial ring in one variable, then R is a principal ideal domain, so $I = (f)$ and $J = (g)$ for some $f, g \in R$. In this case, $J + I^{[q]}$ is also a principal ideal, and the reduced Gröbner basis of $J + I^{[q]}$ consists of the element $\gcd(g, f^q)$, whose total degree is bounded above by $\deg g$. Then if we define $\alpha := \deg g$ and $\beta := 1$, we obtain constant bounds for all three functions given by $\delta(q) \leq \Delta(q) \leq \alpha$ and $c(q) = \beta$ for all q.

Next, suppose that R is a polynomial ring in two variables x and y over F. By earlier observations, we may assume that I and J are nonzero ideals. Let S be a generating set for the ideal J, and T a generating set for I. Choose S and T so that the leading coefficients of all of their elements are 1. Define $T_q := \{t^q \mid t \in T\}$ to be the corresponding generating set for $I^{[q]}$.

We apply the Buchberger algorithm with the reverse lexicographic ordering to compute a Gröbner basis of $J + I^{[q]}$, starting with the generating set $S \cup T_q$. At each step, a partial Gröbner basis $B_{i-1} := S \cup T_q \cup \{p_1, ..., p_{i-1}\}$ has been found, and an S-polynomial of a pair of elements in B_{i-1} is computed and reduced with respect to all of the elements in this basis. If the result is nonzero, the polynomial is divided by its leading coefficient and the resulting monic polynomial is added as the element p_i to form the basis B_i. When there are no nonzero reduced S-polynomials remaining, this creates a Gröbner basis $B := S \cup T_q \cup \{p_1, ..., p_k\}$ for $J + I^{[q]}$ with respect to the reverse lexicographic ordering, where each element of B is a monic polynomial, and for each $1 \leq i \leq k$, all of the terms of the polynomial p_i are reduced with respect to $S \cup T_q \cup \{p_1, ..., p_{i-1}\}$.

In order to compute the reduced Gröbner basis G_q of $J + I^{[q]}$, we need to reduce the Gröbner basis B. For each polynomial $r \in B$, replace r in the basis with the monic polynomial obtained by reducing all of the terms of r with respect to the elements of $B \setminus \{r\}$, and dividing by the resulting leading coefficient. Repeat this process for all of the polynomials in the basis, removing any zero polynomials that result, until no further reduction can be done. This gives the reduced Gröbner basis G_q for $J + I^{[q]}$ [Cox et al. 92, Proposition 2.7.6].

The total degree of the reduced Gröbner basis G_q for $J + I^{[q]}$ will be at most the total degree for the basis B. To compute bounds on these degrees, we first need to describe the polynomials p_i more carefully.

Let $x^a y^b$ be the leading term of a nonzero element p of S. In particular, since $J = (S) \neq (0)$, there is a nonzero monic polynomial $p' \in J$, and by adding the element $xyp' \in J$ to the set S if necessary, we may assume (for ease of notation) that both a and b are nonzero. For each $1 \leq i \leq k$, let $x^{a_i} y^{b_i}$ be the leading term of the polynomial p_i in B. Since p_i is reduced with respect to S, either $0 \leq a_i < a$ or $0 \leq b_i < b$, or both. If $i > j$, then p_i is also reduced with respect to p_j. More specifically, at each step of the algorithm described above, when p_i is computed, (at least) one of four possible cases occurs. Either

(1) $0 \leq a_i < a$ and $a_i \neq a_j$ for all $1 \leq j \leq i-1$,

(2) $0 \leq a_i < a$ and for some $j < i$, $a_i = a_j$ and $b_i < b_j$,

(3) $0 \leq b_i < b$ and $b_i \neq b_j$ for all $1 \leq j \leq i-1$, or

(4) $0 \leq b_i < b$ and for some $j < i$, $b_i = b_j$ and $a_i < a_j$.

In Cases (2) and (4), the total degree of p_i is strictly less than the maximal total degree of the previous basis $S \cup T_q \cup \{p_1, ..., p_{i-1}\}$. In Cases (1) and (3), the total degree of the polynomial p_i, which is a reduction of an S-polynomial of a pair of elements in the previous basis, can be at most twice the maximal total degree of the previous basis (by definition of S-polynomials). Note that Cases (1) and (3) can occur at most $a+b$ times during the algorithm. The maximal total degree of elements in $S \cup T_q$ satisfies

$$\begin{aligned}\deg(S \cup T_q) &= \max\{\deg(S), \deg(T_q)\}\\ &= \max\{\deg(S), q \cdot \deg(T)\}\\ &\leq q \cdot \max\{\deg(S), \deg(T)\}.\end{aligned}$$

Thus the total degree of the basis B is at most $2^{a+b} \cdot q \cdot \max\{\deg(S), \deg(T)\}$. If we define the constant $\alpha := 2^{a+b} \cdot \max\{\deg(S), \deg(T)\}$, then this proves that $\Delta(q) \leq \alpha q$. For all q, $\delta(q) \leq \Delta(q) \leq \alpha q$, therefore Katzman's conjecture holds in the case in which the polynomial ring has two variables.

Finally, to get the bound on the cardinality of the reduced Gröbner basis G_q of $J + I^{[q]}$, note that although the element $p \in S$ with leading term $x^a y^b$ may have been reduced or removed in the reduction process to construct G_q from B, no polynomial that remains in G_q may have leading term divisible by $x^a y^b$. For each number $0 \leq a' < a$ and $0 \leq b' < b$, there can be at most one polynomial in G_q with leading term of the form $x^{a'} y^*$ for any number $*$, and at most one polynomial in G_q with leading term $x^* y^{b'}$. Hence the cardinality of G_q satisfies $|G_q| \leq a+b$. Then by defining the constant $\beta := a+b$, we obtain $c(q) \leq \beta$. □

3. PRINCIPAL BINOMIAL IDEALS: GENERAL CONSTRUCTIONS

For the remainder of the paper we direct our attention to the case in which the ideals I and J are principal and binomial, and obtain more detailed information about the specific form of the degree functions $\delta(q)$ and $\Delta(q)$, as well as the cardinality function $c(q)$. We begin by considering arbitrary pairs of monoidal binomials which generate the whole ring.

Lemma 3.1. *Let F be a field and let $R = F[x_1, \dots, x_n]$ be a polynomial ring in n variables over F. Let $x^v - gx^w, x^b - hx^c \in R$, where v, w, b, c are n-tuples of nonnegative integers, g and h are nonzero elements in F, $\gcd(x^v, x^w) = 1 = \gcd(x^b, x^c)$, and in reverse lexicographic ordering, $x^v > x^w$ and $x^b > x^c$. Assume that $(x^v - gx^w, x^b - hx^c) = R$. Then $w = c = \underline{0}$, and there is a positive rational number l such that $v_i = lb_i$ for all i.*

Proof: If the conclusion holds after tensoring with the algebraic closure $\overline{F}$ of F over F, then it also holds in R. So without loss of generality we may assume that F is algebraically closed.

The hypothesis on the ordering implies that v and b are both nonzero. If both w and c are nonzero, then $R = (x^v - gx^w, x^b - hx^c) \subseteq (x_1, \dots, x_n)R$, which is a contradiction. So either w or c is zero; without loss of generality suppose that $w = \underline{0}$.

Choose any root $k = (k_1, \dots, k_n) \in F^n$ of $x^v - gx^w$; thus $k^v = g$. Further, choose i such that $v_i > 0$. Since $v_i > 0$, then $k_i \neq 0$ and k_i depends on the choices of the other k_j by the relation

$$k_i = g^{1/v_i} \prod_{j \neq i, v_j \neq 0} k_j^{-v_j/v_i}$$

(for some choice of the v_ith roots).

The assumption that $(x^v - g, x^b - hx^c) = R$ implies that the two binomials cannot have a common root, so $k^b - hk^c$ is a nonzero element in F. Hence for all indices j with $v_j = 0$, any choice of $x_j = k_j \in F$ for these indices must make $k^b - hk^c$ equal to

$$\begin{aligned} & g^{b_i/v_i} \prod_{j \neq i, v_j \neq 0} k_j^{b_j - b_i(v_j/v_i)} \\ & \times \prod_{v_j = 0} x_j^{b_j} - hg^{c_i/v_i} \\ & \times \prod_{j \neq i, v_j \neq 0} k_j^{c_j - c_i(v_j/v_i)} \\ & \times \prod_{v_j = 0} x_j^{c_j}, \end{aligned} \tag{3–1}$$

which is a nonzero element in F.

Suppose that m is an index such that $m \neq i$ and $v_m = 0$. If $b_m > 0$ and $c_m > 0$, then for $k_m = 0$, Expression (3–1) is $k^b - hk^c = 0$, giving a contradiction. If $b_m = 0$ and $c_m \neq 0$, then for $k_j = 1$ for all $j \neq i, m$ and $k_m = (h^{-1} g^{(b_i - c_i)/v_i})^{1/c_m}$, the expression is again zero, giving a contradiction. Similar choices show that the case in which $b_m \neq 0$ and $c_m = 0$ cannot occur. Therefore, when $v_m = 0$, we have that $b_m = c_m = 0$. Thus $b_m - c_m = 0 = (b_i - c_i)(v_m/v_i)$ for all indices $m \neq i$ with $v_m = 0$.

Next, let m be any index such that $m \neq i$ and $v_m \neq 0$. If, in addition, $k_1, \ldots, k_n$ are all chosen to be nonzero, then

$$k^{b-c} - h = g^{(b_i-c_i)/v_i} \prod_{j\neq i} k_j^{b_j-c_j-(b_i-c_i)(v_j/v_i)} - h$$

is also a nonzero element in F. If $b_m - c_m - (b_i - c_i)(v_m/v_i) \neq 0$, then letting $k_j = 1$ for all $j \neq i, m$, and

$$k_m = [hg^{-(b_i-c_i)/v_i}]^{1/(b_m-c_m-(b_i-c_i)(v_m/v_i))},$$

we have $k^{b-c}-h = 0$, giving a contradiction. So $b_m-c_m-(b_i-c_i)(v_m/v_i) = 0$, and hence $b_m-c_m = (b_i-c_i)(v_m/v_i)$, when $v_m \neq 0$ also.

Thus for all $j \neq i$, we have that $b_j-c_j = (b_i-c_i)(v_j/v_i)$ and v_j/v_i is nonnegative. By the hypothesis $x^b > x^c$ in the reverse lexicographic ordering, so we must have $b_i - c_i > 0$ and $b_j \geq c_j$ for all j. By the assumption that $\gcd(x^b, x^c) = 1$, it follows that $c = \underline{0}$. Then $b_i v_j = b_j v_i$ for all j, and since $v_i \neq 0$ and $b \neq \underline{0}$, $b_i \neq 0$ as well. Therefore, if we define the positive rational number $l := v_i/b_i$, then $v_j = lb_j$ for all j. □

This result leads to the following definition. Two binomials $x^u(x^v - gx^w)$ and $x^a(x^b - hx^c)$ with $x^v > x^w$ and $x^b > x^c$ are of the *same type* if there are nonnegative integers l and m and n-tuples B and C of nonnegative integers with $x^B > x^C$ such that $v = lB$, $w = lC$, $b = mB$, and $c = mC$; in this case, we say the binomials are of *type* (B, C). With this notation, Lemma 3.1 says that if the ideal generated by two nonmonomial binomials is the whole ring, then the two binomials are both of type $(B, (0, \ldots, 0))$ for some B, and neither binomial is a multiple of any variable. The corresponding result fails for a 3-generated binomial ideal; for example, the three binomials $x_1 - 1$, $x_2 - 1$, $x_1x_2 - 2$ generate the whole ring, yet no two of the three binomials are of the same type.

The following theorem shows that for principal ideals generated by binomials of the same type as those considered in Lemma 3.1, one can bound the number of elements in the reduced Gröbner bases, as well as give constructive upper bounds for the x_n-degree and total degree.

Theorem 3.2. *Let F be a field of positive prime characteristic p and $R = F[x_1, \ldots, x_n]$ a polynomial ring in n variables over F. Let $I = (x^u(x^v - gx^w))$ and $J = (x^a(x^b - hx^c))$ be ideals in R, where $u, v, w, a, b,$ and c are n-tuples of nonnegative integers, g and h are units in F, $\gcd(x^v, x^w) = 1 = \gcd(x^b, x^c)$, and in reverse lexicographic ordering, $x^v > x^w$ and $x^b > x^c$. Assume that $(x^v - gx^w, x^b - hx^c) = R$. Then for q sufficiently large, the maximal x_n-degree of the Gröbner basis of $J+I^{[q]}$ satisfies $\delta(q) \leq \max((u_n + v_n)q, a_n + b_n)$, the maximal total degree satisfies $\Delta(q) \leq \max((|u|+|v|)q, |a|+|b|)$, and the cardinality of the Gröbner basis satisfies $c(q) \leq 4$.*

Proof: By Lemma 3.1, $w = c = 0$ and the generators of I and J have the same type. Then $I^{[q]} = (x^{qu}(x^{qv} - g^q))$ and $J = (x^a(x^b - h))$. We will explicitly compute a Gröbner basis for $J + I^{[q]}$.

The hypothesis that $(x^v - g, x^b - h) = R$ implies that there are polynomials $r, s \in R$ with $r(x^v - g) + s(x^b - h) = 1$. Taking qth powers of both sides and then multiplying by lcm (x^{qu}, x^a) yields

$$r^q \frac{\operatorname{lcm}\,(x^{qu}, x^a)}{x^{qu}} x^{qu}(x^{qv} - g^q) + [s^q(x^b - h)^{q-1}] \frac{\operatorname{lcm}\,(x^{qu}, x^a)}{x^a} x^a(x^b - h),$$

which equals lcm (x^{qu}, x^a). Thus $J + I^{[q]}$ contains lcm (x^{qu}, x^a). Computation of the S-polynomials of this monomial with the two generators of $J + I^{[q]}$ shows that

$$\begin{aligned}\frac{1}{g^q} S(x^{q(u+v)} - g^q x^{qu}, \operatorname{lcm}\,(x^{qu}, x^a)) &= \frac{1}{g^q} \frac{\operatorname{lcm}\,(x^{q(u+v)}, x^a)}{x^{q(u+v)}} g^q x^{qu} \\ &= \frac{\operatorname{lcm}\,(x^{q(u+v)}, x^a)}{x^{qv}}\end{aligned}$$

and

$$\begin{aligned}\frac{1}{h} S(x^{a+b} - hx^a, \operatorname{lcm}\,(x^{qu}, x^a)) &= \frac{1}{h} \frac{\operatorname{lcm}\,(x^{a+b}, x^{qu})}{x^{a+b}} hx^a \\ &= \frac{\operatorname{lcm}\,(x^{a+b}, x^{qu})}{x^b}\end{aligned}$$

are also in $J + I^{[q]}$.

Let $E_j := \frac{\operatorname{lcm}\,(x^{a+jb}, x^{qu})}{x^{jb}}$. By the S-polynomial calculation above, $E_1 \in J + I^{[q]}$. If $E_j \in J + I^{[q]}$, then so is

$$\frac{1}{h} S(x^a(x^b - h), E_j) = \frac{\operatorname{lcm}\,(x^{a+b}, \frac{\operatorname{lcm}\,(x^{a+jb}, x^{qu})}{x^{jb}})}{x^b}. \quad (3\text{–}2)$$

The exponent of x_i in Equation (3–2) equals $\max(a_i + b_i, \max(a_i+jb_i, qu_i)-jb_i)-b_i = \max(a_i, \max(a_i-b_i, qu_i-(j+1)b_i)) = \max(a_i, qu_i-(j+1)b_i)$, which is the same as the exponent of x_i in E_{j+1}. Thus the monic S-polynomial in Equation (3–2) is $\frac{1}{h}S(x^a(x^b-h),E_j)=E_{j+1}$. Therefore all the E_j are in $J+I^{[q]}$. Note that the exponent $\max(a_i, qu_i - jb_i)$ of x_i in E_j is at least as large as the exponent of x_i in E_{j+1} for all i, so E_j is a multiple of E_{j+1} for each j. Thus for sufficiently large j, $E_j = E_{j+1} = E_{j+2} = \ldots$, and we denote this eventual monomial as E_∞. All of the E_j are multiples of E_∞.

Define the set

$$B := \left\{ \begin{matrix} x^{qu}(x^{qv}-g^q), x^a(x^b-h), \\ \dfrac{\text{lcm }(x^{q(u+v)}, x^a)}{x^{qv}}, E_\infty \end{matrix} \right\},$$

then B is a basis of $J+I^{[q]}$. The S-polynomial of the first two elements is $\frac{\text{lcm }(x^{q(u+v)},x^{a+b})}{x^{qv}}g^q - \frac{\text{lcm }(x^{q(u+v)},x^{a+b})}{x^b}h$, which reduces modulo the third element in B and modulo E_1 (i.e., modulo E_∞) to zero. The S-polynomial of the first and the third elements in B is

$$S\left(x^{qu}(x^{qv}-g^q), \frac{\text{lcm }(x^{q(u+v)},x^a)}{x^{qv}}\right) = \frac{\text{lcm }(x^{q(u+v)}, \frac{\text{lcm }(x^{q(u+v)},x^a)}{x^{qv}})}{x^{qv}} g^q. \quad (3\text{–}3)$$

The exponent of x_i in Equation (3–3) equals

$$\max(qu_i+qv_i, \max(qu_i+qv_i,a_i)-qv_i)-qv_i = \max(qu_i, a_i-2qv_i).$$

For sufficiently large q, if $v_i \neq 0$ then $\max(qu_i, a_i - 2qv_i) = qu_i = \max(qu_i, a_i - qv_i)$, and if $v_i = 0$ then $\max(qu_i, a_i-2qv_i) = \max(qu_i,a_i) = \max(qu_i, a_i-qv_i)$. Since $\max(qu_i, a_i-qv_i)$ also equals the exponent of x_i in the third element of the basis B, this shows that the S-polynomial of the first and the third elements of B reduces to 0. The S-polynomial of the first and the fourth elements in B is

$$S\left(x^{qu}(x^{qv}-g^q), E_\infty)\right) = \frac{\text{lcm }(x^{q(u+v)},E_\infty)}{x^{qv}}g^q. \quad (3\text{–}4)$$

The exponent of x_i in Equation (3–4) equals, for j sufficiently large,

$$\max(qu_i, \max(a_i-qv_i, qu_i-jb_i-qv_i)) = \max(qu_i, a_i-qv_i),$$

which is the same as the exponent of x_i in the third element of B. Thus the S-polynomial of the first element of B with any other element of B reduces to 0. The S-polynomial of the second and third elements is the monomial

$$\frac{\text{lcm }\left(x^{a+b}, \frac{\text{lcm }(x^{q(u+v)},x^a)}{x^{qv}}\right)}{x^b}h, \quad (3\text{–}5)$$

for which the exponent of x_i is $\max(a_i, \max(qu_i-b_i, a_i-qv_i-b_i)) = \max(a_i, qu_i-b_i)$, so the S-polynomial in Equation (3–5) is a multiple of E_1 and thus of E_∞, and hence reduces to zero. We have previously established that the S-polynomial of the second and the fourth elements reduces to 0 modulo the given basis. The last two elements of the basis B are both monomials, so their S-polynomial is 0 as well. This proves that, for q sufficiently large, the set B is a Gröbner basis of $J+I^{[q]}$ with respect to the reverse lexicographic ordering.

Although the Gröbner basis B may not be reduced, the reduced reverse lexicographic Gröbner basis G_q for $J+I^{[q]}$ will have cardinality and degrees at most those of B. Thus we can read off upper bounds for the three functions for q sufficiently large, and find that $\delta(q) \leq \max((u_n+v_n)q, a_n+b_n)$, $\Delta(q) \leq \max((|u|+|v|)q, |a|+|b|)$, and $c(q) \leq 4$. □

Next, we use Lemma 3.1 to show that the principal monoidal ideals cover "most" of the possibilities for principal binomial ideals.

Theorem 3.3. *For any principal binomial (nonmonomial) ideals I and J which are generated by binomials that are not of the same type, there is a change of variables under which I and J become principal monoidal ideals. Furthermore, this change of variables preserves the reverse lexicographic ordering and the three functions $\delta(q)$, $\Delta(q)$, and $c(q)$.*

Proof: Let F be a field of positive prime characteristic p and $R = F[x_1,\ldots,x_n]$ a polynomial ring in n variables over F. Since Gröbner bases are unchanged if we pass to $\overline{F}[x_1,\ldots,x_n]$, where $\overline{F}$ is the algebraic closure of F, without loss of generality we may assume that F is algebraically closed.

Let I and J be arbitrary principal binomial (nonmonomial) ideals that are not of the same type. We can write $I = (x^u(x^v - gx^w))$ and $J = (x^a(x^b - hx^c))$, where u, v, w, a, b, and c are n-tuples of nonnegative integers, g and h are units in F, $x^v > x^w$ and $x^b > x^c$ in the reverse lexicographic ordering, and $\gcd(x^v, x^w) = 1 = \gcd(x^b, x^c)$.

Case I. Suppose there exist nonzero elements $k_1, \ldots, k_n$ in F such that $k^v - gk^w = 0 = k^b - hk^c$. In this case, under the variable change $x_i \mapsto k_i x_i$ for all i, the reverse lexicographic ordering is preserved, and the generator of the image $\widetilde{I}$ of I under this ring automorphism is $k^u x^u(k^v x^v - gk^w x^w)$. After dividing through by the nonzero element $k^u k^v = k^u g k^w$ of F, this generator becomes $x^u(x^v - x^w)$. A similar computation holds for the generator of the image $\widetilde{J}$ of J; hence the generators of $\widetilde{I}$ and $\widetilde{J}$ are monoidal. Since this ring automorphism preserves the reverse lexicographic ordering, it maps Gröbner bases to Gröbner bases. Since this change of variables is linear, the functions $\delta(q)$, $\Delta(q)$, and $c(q)$ will also be preserved.

Case II. Suppose that there do not exist nonzero elements $k_1, \ldots, k_n$ in F such that $k^v - gk^w = 0 = k^b - hk^c$.

Case IIa. Suppose Case II holds and also that $v_i + w_i > 0$ and $b_i + c_i = 0$ for some index i. There is another index j for which either $b_j > 0$ or $c_j > 0$, but not both, since $x^b > x^c$ and $\gcd(x^b, x^c) = 1$. By performing the change of variables $x_j \mapsto h^{1/b_j}$ (respectively $x_j \mapsto (h^{-1})^{1/c_j}$) and $x_m \mapsto x_m$ for all $m \neq j$, the generator $x^a(x^b - hx^c)$ of J is mapped to a scalar multiple of $x^a(x^b - \tilde{h}x^c) = x^a(x^b - x^c)$ with unit $\tilde{h} = 1$. At the same time, the generator of I changes to a scalar multiple of $x^u(x^v - \tilde{g}x^w)$ for another unit $\tilde{g}$ in F. Since either $v_i > 0$ or $w_i > 0$, we can similarly replace x_i by an appropriate scalar multiple of itself so that $x^u(x^v - \tilde{g}x^w)$ is mapped to a scalar multiple of $x^u(x^v - x^w)$. Since $b_i = c_i = 0$, the unit $\tilde{h} = 1$ remains unchanged under this second map. As in Case I, this change of variables preserves the ordering and the three functions associated to the Gröbner bases.

Case IIb. Suppose Case II holds and $v_i + w_i = 0$ and $b_i + c_i > 0$ for some index i. An argument similar to Case IIa also demonstrates this case.

Case IIc. Suppose Case II holds and that for all indices i, $v_i + w_i > 0$ if and only if $b_i + c_i > 0$. Let T be the set of indices m for which $v_m > 0$, let U be the set of indices m for which $w_m > 0$, and let $S := T \cup U$. Let

$$b_+ := \begin{cases} b_j & \text{if } j \in T \\ 0 & \text{if } j \notin T \end{cases} \quad \text{and} \quad b_- := \begin{cases} b_j & \text{if } j \in U \\ 0 & \text{if } j \notin U, \end{cases}$$

and define c_+ and c_- similarly. Then $b = b_+ + b_-$ and $c = c_+ + c_-$.

Define new variables y_m over F, where m varies over the set S. We will denote the restrictions of the tuples v, w, b_+, b_-, c_+, and c_- to tuples in the indices of S by the same notation. Consider the ideal $(y^{v+w} - g, y^{b_+ + c_-} - hy^{b_- + c_+})$ in $F[y_m | m \in S]$.

Since the nonleading (monic) term of the first generator is 1, it follows directly that $y^{v+w} > 1$ and $\gcd(y^{v+w}, 1) = 1$. Note that the indices m for which $(b_+)_m > 0$ or $(c_-)_m > 0$ also satisfy the property that $(b_-)_m = 0 = (c_+)_m$, so the supports of the two terms of the second generator are disjoint. Then $\gcd(y^{b_+ + c_-}, y^{b_- + c_+}) = 1$ and either $y^{b_+ + c_-} > y^{b_- + c_+}$ or $y^{b_- + c_+} > y^{b_+ + c_-}$.

Suppose that $\underline{\tilde{k}}$ is a tuple with entries in F (and indices in S) for which $\tilde{k}^{v+w} - g = 0 = \tilde{k}^{b_+ + c_-} - h\tilde{k}^{b_- + c_+}$. Since the product of all of the $\tilde{k}_m$ divides $\tilde{k}^{v+w}$, the first equation shows that all of the entries of $\underline{\tilde{k}}$ are nonzero. Define the n-tuple $\underline{k} \in F^n$ by $k_j := \tilde{k}_j$ for $j \in T$, $k_j := \tilde{k}_j^{-1}$ for $j \in U$, and $k_j := 1$ for $j \notin S$. Then $k_1, \ldots, k_n$ are nonzero elements in F for which $0 = k^w(\tilde{k}^{v+w} - g) = k^w(k^{v-w} - g) = k^v - gk^w$ and $0 = k^{b_- + c_-}(\tilde{k}^{b_+ + c_-} - h\tilde{k}^{b_- + c_+}) = k^{b_- + c_-}(k^{b_+ - c_-} - hk^{-b_- + c_+}) = k^b - hk^c$, contradicting the hypothesis of Case II. Therefore the equations $y^{v+w} - g = 0 = y^{b_+ + c_-} - hy^{b_- + c_+}$ have no solutions over F. Then Hilbert's Nullstellensatz says that $(y^{v+w} - g, y^{b_+ + c_-} - hy^{b_- + c_+}) = F[y_m | m \in S]$.

Applying Lemma 3.1, we get that either $b_+ + c_- = 0$ or $b_- + c_+ = 0$, and we can write $y^{b_+ + c_-} - hy^{b_- + c_+}$ as a scalar multiple of $y^{\hat{b} + \hat{c}} - \hat{h}$ where $\hat{b} + \hat{c}$ is either $b_+ + c_-$ or $b_- + c_+$, and $\hat{h}$ is h or h^{-1}, respectively. The last conclusion of Lemma 3.1 says there is a positive rational number l such that $v + w = l(\hat{b} + \hat{c})$. If $b_+ + c_- = 0$, then $b = b_-$, $c = c_+$, and $v + w = l(b_- + c_+)$, so $v = lc_+$ and $w = lb_-$, which contradicts the assumption that both $x^v > x^w$ and $x^b > x^c$. Therefore $b_- + c_+ = 0$, so $b = b_+$, $c = c_-$, $v = lb$, and $w = lc$. Therefore the generator $x^u(x^v - gx^w)$ of the ideal I is of the same type as the generator $x^a(x^b - hx^c)$ of J. But this contradicts the hypothesis that the generators of I and J are of distinct types, so Case IIc cannot occur. $\square$

Motivated by the preceding theorem, for the remainder of the paper, we consider the case in which the ideals I and J are principal and monoidal.

4. PRINCIPAL MONOIDAL IDEALS: EXAMPLES

In this section, we report on our calculations of reduced reverse lexicographic Gröbner bases, together with the functions $\delta(q)$, $\Delta(q)$, and $c(q)$, for ideals of the form $J + I^{[q]}$, where I and J are fixed principal monoidal ideals and q varies over powers of the characteristic of the base field F. In every example, the three functions either are eventually (for $q >> 0$) linear or constant functions, or else eventually vary periodically between linear or constant functions. For several of the examples, we also explore in more detail the dependence of the three functions on the characteristic p of the field F. The examples included in this section were chosen from among all of our computations to illustrate all of the possible behaviors we observed for the three functions.

In the process of finding each of the following examples, we used the symbolic computer algebra program Macaulay2 [Grayson and Stillman 03] to generate Gröbner bases for ideals $J + I^{[q]}$ for small values of q (usually three or four values), and studied the patterns in these bases to guide us in proving the structure of the Gröbner bases for all values of q. A sample of the Macaulay2 code used in our calculations is provided in Section 5.

We begin with an example in which the degree functions are linear functions and the cardinality is a constant.

Proposition 4.1. *Let $R = \mathbb{Z}/3\mathbb{Z}[x, y, z]$, $I = (y^2z - x^2)$, $J = (y^3 - xy)$, $p = 3$, and $q = 3^e$. Then the Gröbner basis of $J + I^{[q]}$ with respect to the reverse lexicographic ordering (with $x_1 = x$, $x_2 = y$, and $x_3 = z$, so that $z < y < x$) is*

$$\{y^3 - xy, x^{q-1}y^2z^q - x^{2q}, x^{2q}y - x^q yz^q, x^{3q+1} - x^{2q+1}z^q\}.$$

Therefore the maximal z-degree of the Gröbner basis elements for $J + I^{[q]}$ is $\delta(q) = q$, the maximal total degree of the elements is $\Delta(q) = 3q + 1$, and the number of elements in the Gröbner basis is $c(q) = 4$ for all q.

Proof: Define $f := y^3 - xy$ and $g := y^{2q}z^q - x^{2q}$, so that f and g generate J and $I^{[q]}$, respectively. Before computing S-polynomials, we reduce g modulo $(y^3 - xy)$. Note that for any monomial $x^ay^bz^c$ with $b \geq 3$, the monomial reduces to $x^{a+1}y^{b-2}z^c$. Then the normal form of $x^ay^bz^c$ modulo f is $x^{a+k}y^{b-2k}z^c$, where $b - 2(k - 1) \geq 3$ and $b - 2k < 3$; that is, $(b - 3)/2 < k \leq (b - 1)/2$. Then, to find the normal form for $y^{2q}z^q$, where $b = 2q$, we need $q - \frac{3}{2} < k \leq q - \frac{1}{2}$, so $k = q - 1$, and the normal form is $x^{q-1}y^2z^q$. Therefore the polynomial g reduces to $g' := x^{q-1}y^2z^q - x^{2q}$.

The polynomials f and g' are a basis for $J + I^{[q]}$. Let h denote their S-polynomial

$$h := S(f, g') = x^{q-1}z^q f - yg' = -x^q yz^q + x^{2q}y.$$

The S-polynomial

$$\begin{aligned} S(g', h) &= x^{q+1}g' - yz^q h = -x^{3q+1} + x^q y^2 z^{2q} \\ &\equiv -x^{3q+1} + x^{2q+1}z^q, \end{aligned}$$

where $\equiv$ denotes a reduction using g'; let $i := x^{3q+1} - x^{2q+1}z^q$ denote the monic scalar multiple of this polynomial. All of the remaining S-polynomials in the basis $\{f, g', h, i\}$ reduce to 0. Therefore the four elements indeed generate a Gröbner basis, and since no element of the basis may be reduced by any other, this Gröbner basis is also reduced. This proves that the maximal z-degree is of the elements of the Gröbner basis $\delta(q) = q$, the maximal total degree is $\Delta(q) = 3q + 1$, and the cardinality is $c(q) = 4$. $\square$

Note 4.2. Let $R = \mathbb{Z}/p\mathbb{Z}[x, y, z]$, with x, y, z variables over $\mathbb{Z}/p\mathbb{Z}$, where p is any prime and q varies over powers of p. Let $I = (y^2z - x^2)$ and $J = (y^3 - xy)$ be the same ideals as in the example above. In this case, the same sets as in Proposition 4.1 are the reduced Gröbner bases of the ideals $J + I^{[q]}$ also in characteristic p. Indeed, the proof above applies, since the hypothesis that $p = 3$ was never used in the proof.

The number of elements in the Gröbner bases need not remain constant, as we prove next with the ideals I and J from Proposition 4.1, but with their roles switched.

Proposition 4.3. *Let $R = \mathbb{Z}/3\mathbb{Z}[x, y, z]$, $I = (y^2z - x^2)$, $J = (y^3 - xy)$, and $q = 3^e$. Then the Gröbner basis of $I + J^{[q]}$ with respect to the reverse lexicographic ordering (with $z < y < x$) is*

$$\left\{ \begin{array}{l} y^2z - x^2, \\ y^{3q} - x^q y^q, \\ x^{2k}y^{3q-2k} - x^{q+2k}y^{q-2k} \end{array} \;\middle|\; 1 \leq k \leq (q-1)/2 \right\}$$
$$\cup \left\{ x^{q-1+2j}y^{2q+1-2j} - x^{2q-1}yz^j \mid 1 \leq j \leq q \right\}$$
$$\cup \left\{ x^{3q+1} - x^{2q+1}z^q \right\}.$$

The corresponding functions for these ideals are $\delta(q) = q$, $\Delta(q) = 3q + 1$, and $c(q) = (3q + 5)/2$ for all q.

Proof: Define the polynomials $f := y^2z - x^2$, $g := y^{3q} - x^q y^q$, $h_k := x^{2k}y^{3q-2k} - x^{q+2k}y^{q-2k}$ when $1 \leq k \leq (q - 1)/2$, $r_j := x^{q-1+2j}y^{2q+1-2j} - x^{2q-1}yz^j$ when $1 \leq j \leq q$, and $s := x^{3q+1} - x^{2q+1}z^q$. Since $q = 3^e$, q is odd, so $(q - 1)/2$ is an integer for all values of e.

Note that if $q = 1$, there are no elements of the form h_k. In this case, the Gröbner basis is already included in the proof of Proposition 4.1.

Next assume that $q > 1$. In this example each of the generators of both I and $J^{[q]}$ is in normal form with respect to the other, giving the first two elements f and g of the basis. The S-polynomial

$$\begin{aligned} S(f, g) &= y^{3q-2}f - zg = -x^2y^{3q-2} + x^q y^q z \\ &\equiv -x^2y^{3q-2} + x^{q+2}y^{q-2} = -h_1, \end{aligned}$$

where $\equiv$ denotes a reduction using f. Repeating this for $1 \leq k \leq (q-3)/2$, we get

$$\begin{aligned} S(f, h_k) &= x^{2k} y^{3q-2k-2} f - z h_k \\ &= -x^{2k+2} y^{3q-2k-2} + x^{q+2k} y^{q-2k} z \\ &\equiv -x^{2(k+1)} y^{3q-2(k+1)} + x^{q+2(k+1)} y^{q-2(k+1)} \\ &= -h_{k+1}, \end{aligned}$$

where $\equiv$ denotes a reduction of the second term using f. Note that in this S-polynomial computation, we required that the first y-exponent $3q - 2k - 2 \geq 0$, and to do the later reduction by f, we needed the fact that y^2 divides y^{q-2k}. Then $3q - 2k \geq 2$ and $q - 2k \geq 2$, so the first inequality is redundant, and the second inequality says $k \leq (q-2)/2$. In this proposition, we are assuming that $p = 3$, so $q = 3^e$ is always odd and the largest value that k can actually reach in this S-polynomial computation is $(q-3)/2$. So the largest value of k for which a basis element h_k is produced is $(q-1)/2$. Thus the entire set of elements h_k is generated in the Buchberger algorithm.

The last element generated this way is $h_{(q-1)/2} = x^{q-1} y^{2q+1} - x^{2q-1} y$. Computing the S-polynomial of this and f gives $S(f, h_{(q-1)/2}) = -r_1$. Again computing S-polynomials inductively for $1 \leq j \leq q-1$, we get $S(f, r_j) = -r_{j+1}$. The last element generated in this latter step is $r_q = x^{3q-1} y - x^{2q-1} y z^q$.

Finally, the S-polynomial $S(f, r_q)$ reduces (using f) to the polynomial $-s$, resulting in the last element in the list of the basis elements. It is straightforward to check that, with these basis elements, all remaining S-polynomials reduce to 0, hence the set is a Gröbner basis, and the Gröbner basis is reduced. The results for the three functions then follow directly. $\square$

Note 4.4. Let $R = \mathbb{Z}/2\mathbb{Z}[x, y, z]$, so that the characteristic is $p = 2$, and let $I = (y^2 z - x^2)$ and $J = (y^3 - xy)$ be the same ideals as in Proposition 4.3. In the proof above, in the computation of the S-polynomials $S(f, h_k)$, we noted that the number of polynomials of the form h_k produced satisfies $k \leq (q-2)/2$. When the characteristic p is even, then, the Gröbner basis computation at this point can differ from the proof above. In fact, a proof very similar to the one above shows that for $p = 2$ the reduced Gröbner basis of $I + J^{[q]}$ is

$$\left\{ \begin{array}{l|l} y^2 z - x^2, & \\ x^{2k} y^{3q-2k} - x^{q+2k} y^{q-2k}, & 0 \leq k \leq \dfrac{(q-2)}{2}, \\ x^{q+2j} y^{2q-2j} - x^{2q} z^j & 0 \leq j \leq q \end{array} \right\}$$

when $q > 1$. Then the functions $\Delta(q) = 3q$ and $c(q) = \frac{3}{2} q + 2$ for $q > 1$ associated to these Gröbner bases differ from the functions $\Delta(q)$ and $c(q)$ computed in Proposition 4.3 with $p = 3$. Thus, not surprisingly, the reduced Gröbner bases, in general, depend on the characteristic of the underlying field. In this example though, the x_n-degree $\delta(q) = q$ is the same function in both characteristics.

The proofs of the next three examples, in Propositions 4.5 and 4.6, computing S-polynomials to produce the Gröbner basis and to check that remaining S-polynomials are 0, utilize reasoning similar to the two previous proofs. To avoid repetition, we omit these proofs.

In part (a) of the next proposition, we show that the function $\delta(q)$ can also equal a constant. In the previous propositions, the functions $\delta(q)$ and $\Delta(q)$ are exactly equal to linear functions, and $c(q)$ equals either a linear or constant function, for all q. As mentioned earlier, these functions are not always this regular. Part (b) of the next proposition illustrates functions $\Delta(q)$ and $c(q)$ that are polynomials eventually but not at the start.

Proposition 4.5. *Let $R = \mathbb{Z}/2\mathbb{Z}[x, y, z]$, $I = (x^2 - y^2)$, $J = (xy - z^2)$, and $q = 2^e$. With the reverse lexicographic ordering (with $z < y < x$),*

(a) the reduced Gröbner basis for $J + I^{[q]}$ is

$$\{xy - z^2, x^{2q} - y^{2q}, y^{2q+1} - x^{2q-1} z^2\},$$

so that $\delta(q) = 2$, $\Delta(q) = 2q + 1$, and $c(q) = 3$ for all q, and

(b) the reduced Gröbner basis for $I + J^{[q]}$ with $q \geq 2$ is

$$\{x^2 - y^2, y^{2q} - z^{2q}\},$$

so in this case $\delta(q) = 2q$,

$$\Delta(q) = \begin{cases} 3 & \text{if } q = 1, \\ 2q & \text{if } q \geq 2 \end{cases}, \text{ and } c(q) = \begin{cases} 3 & \text{if } q = 1, \\ 2 & \text{if } q \geq 2 \end{cases}$$

for all q.

The next example shows that the function $\delta(q)$ may also be a function that is eventually linear but not for small q.

Proposition 4.6. *Let $R = \mathbb{Z}/3\mathbb{Z}[x, y, z, w]$, $I = (x^5 y^2 z w - x y^3 z^2 w)$, $J = (x y^2 z^3 w^2 - x^3 y z w^3)$, and $q = 3^e$. Then with the reverse lexicographic ordering (with $w < z <$*

$y < x$), the reduced Gröbner basis of $J + I$ is

$$\left\{ \begin{array}{l} xy^2z^3w^2 - x^3yzw^3, \\ x^5y^2zw - xy^3z^2w, \\ x^7yzw^3 - x^3y^2z^2w^3 \end{array} \right\},$$

and for $q \geq 3$, the reduced Gröbner basis of $J + I^{[q]}$ is

$$\left\{ \begin{array}{l} xy^2z^3w^2 - x^3yzw^3, \\ x^{6q-1+2i}y^{\frac{3q+1}{2}-i}zw^{\frac{3q-1}{2}+i} \\ \quad - x^{3q-2+2i}y^{2q+1-i}z^2w^{2q-1+i} \end{array} \;\middle|\; 0 \leq i \leq \frac{3q-1}{2} \right\}.$$

Thus

$$\delta(q) = \begin{cases} 3 & \text{if } q = 1, \\ \frac{7q-3}{2} & \text{if } q \geq 3, \end{cases}$$

$$\Delta(q) = \begin{cases} 12 & \text{if } q = 1, \\ 12q - 1 & \text{if } q \geq 3, \end{cases}$$

and $c(q) = \frac{3q+3}{2}$ for all q.

In the following example, we again use the ideals I and J from the previous proposition and exchange their roles, in order to exhibit periodic behavior of both the cardinality function $c(q)$ and the total degree function $\Delta(q)$ of the elements of the reduced Gröbner basis of $I + J^{[q]}$, with periodic behavior starting not with $q = 1$ but at the next level, at $q = p$. The proof of Proposition 4.7 is similar to, but somewhat less complicated than, the proof of Proposition 4.8; again to avoid repetition, we include only the proof of the latter result.

Proposition 4.7. *Let $R = \mathbb{Z}/3\mathbb{Z}[x, y, z, w]$, $I = (x^5y^2zw - xy^3z^2w)$, $J = (xy^2z^3w^2 - x^3yzw^3)$, and $q = 3^e$. Using the reverse lexicographic ordering (with $w < z < x < y$) the reduced Gröbner basis of $I + J$ is*

$$\left\{ \begin{array}{l} x^5y^2zw - xy^3z^2w, \\ xy^2z^3w^2 - x^3yzw^3, \\ x^7yzw^3 - x^3y^2z^2w^3 \end{array} \right\};$$

the reduced Gröbner basis of $I + J^{[q]}$ for q a positive even power of 3 is

$$\left\{ \begin{array}{l} x^5y^2zw - xy^3z^2w, \\ xy^{\frac{9}{4}q-\frac{1}{4}}z^{\frac{13}{4}q-\frac{1}{4}}w^{2q} - x^3y^{\frac{7}{4}q-\frac{3}{4}}z^{\frac{7}{4}q-\frac{3}{4}}w^{3q} \end{array} \right\};$$

and the reduced Gröbner basis of $I + J^{[q]}$ for q an odd power of 3 is

$$\left\{ \begin{array}{l} x^5y^2zw - xy^3z^2w, \\ x^3y^{\frac{9}{4}q-\frac{3}{4}}z^{\frac{13}{4}q-\frac{3}{4}}w^{2q} - xy^{\frac{7}{4}q-\frac{1}{4}}z^{\frac{7}{4}q-\frac{1}{4}}w^{3q}, \\ xy^{\frac{9}{4}q+\frac{1}{4}}z^{\frac{13}{4}q+\frac{1}{4}}w^{2q} - x^3y^{\frac{7}{4}q-\frac{1}{4}}z^{\frac{7}{4}q-\frac{1}{4}}w^{3q} \end{array} \right\}.$$

The corresponding functions are given by $\delta(q) = 3q$,

$$\Delta(q) = \begin{cases} 12 & \text{if } q = 1, \\ \frac{15}{2}q + \frac{3}{2} & \text{if } q = 3^e,\ e \text{ odd}, \\ \frac{15}{2}q + \frac{1}{2} & \text{if } q = 3^e,\ e > 0 \text{ even}, \end{cases}$$

and

$$c(q) = \begin{cases} 3 & \text{if } q = 1 \text{ or } q = 3^e,\ e \text{ odd}, \\ 2 & \text{if } q = 3^e,\ e > 0 \text{ even} \end{cases}$$

for all q.

In the next example, we show that the function $\delta(q)$ also can vary periodically. In the example in Proposition 4.7, $c(q)$ alternated between constant functions for the ideals $J + I^{[q]}$. The next example shows that the function $c(q)$ can vary periodically between linear functions as well. Moreover, the asymptotic patterns for all three functions of the ideals $J + I^{[q]}$ begin further along, at $q = p^2$.

Proposition 4.8. *Let $R = \mathbb{Z}/3\mathbb{Z}[x, y, z]$, $I = (x^2y^2z - xyz^2)$, $J = (xy^2z^5 - x^2yz)$, and $q = 3^e$. Then with the reverse lexicographic ordering (with $z < y < x$) the reduced Gröbner basis for $J + I$ is*

$$\{xy^2z^5 - x^2yz, x^2y^2z - xyz^2, xyz^6 - x^3yz\};$$

the reduced Gröbner basis for $J + I^{[3]}$ is

$$\left\{ \begin{array}{l} xy^2z^5 - x^2yz, \\ x^6y^6z^3 - x^4y^2z^2, \\ x^7y^5z - x^4y^2z^4, \\ x^8y^4z - x^5yz^4, \\ x^5yz^8 - x^9y^3z \end{array} \right\};$$

if $e \geq 2$ is even the reduced Gröbner basis for $J + I^{[q]}$ is

$$\left\{ \begin{array}{l} xy^2z^5 - x^2yz, \\ x^{\frac{9}{4}q-\frac{1}{4}+k}y^{\frac{7}{4}q+\frac{1}{4}-k}z \\ \quad - x^{\frac{3}{2}q-\frac{1}{2}+k}y^{\frac{1}{2}q+\frac{1}{2}-k}z^2, \\ x^{\frac{11}{4}q+\frac{1}{4}+j}y^{\frac{5}{4}q-\frac{1}{4}-j}z \\ \quad - x^{2q-1}yz^{6+4j}, \\ x^{2q-1}yz^{2q+4} - x^{\frac{13}{4}q-\frac{1}{4}}y^{\frac{3}{4}q+\frac{1}{4}}z \end{array} \;\middle|\; \begin{array}{l} 0 \leq k \leq \frac{(q-1)}{2}, \\ 0 \leq j \leq \frac{(q-3)}{2} \end{array} \right\};$$

and if $e \geq 3$ is odd then the reduced Gröbner basis for $J + I^{[q]}$ is

$$\left\{\begin{array}{l|l} xy^2z^5 - x^2yz, & \\ x^{\frac{9}{4}q-\frac{3}{4}}y^{\frac{7}{4}q+\frac{3}{4}}z^3 & \\ \quad - x^{\frac{3}{2}q-\frac{1}{2}}y^{\frac{1}{2}q+\frac{1}{2}}z^2, & \\ x^{\frac{9}{4}q+\frac{1}{4}+k}y^{\frac{7}{4}q-\frac{1}{4}-k}z & 0 \leq k \leq \dfrac{(q-1)}{2}, \\ \quad - x^{\frac{3}{2}q-\frac{1}{2}+k}y^{\frac{1}{2}q+\frac{1}{2}-k}z^4, & 0 \leq j \leq \dfrac{(q-3)}{2} \\ x^{\frac{11}{4}q+\frac{3}{4}+j}y^{\frac{5}{4}q-\frac{3}{4}-j}z & \\ \quad - x^{2q-1}yz^{8+4j}, & \\ x^{2q-1}yz^{2q+6} - x^{\frac{13}{4}q+\frac{1}{4}}y^{\frac{3}{4}q-\frac{1}{4}}z & \end{array}\right\}.$$

The associated functions are

$$\delta(q) = \begin{cases} 8 & \text{if } q = 3, \\ 2q+4 & \text{if } q = 3^e,\ e \geq 0 \text{ even}, \\ 2q+6 & \text{if } q = 3^e,\ e \geq 3 \text{ odd}, \end{cases}$$

$$\Delta(q) = \begin{cases} 15 & \text{if } q = 3, \\ 4q+4 & \text{if } q = 3^e,\ e \geq 0 \text{ even}, \\ 4q+6 & \text{if } q = 3^e,\ e \geq 3 \text{ odd}, \end{cases}$$

and

$$c(q) = \begin{cases} 5 & \text{if } q = 3, \\ q+2 & \text{if } q = 3^e,\ e \geq 0 \text{ even}, \\ q+3 & \text{if } q = 3^e,\ e \geq 3 \text{ odd}. \end{cases}$$

Proof: The Gröbner bases for $J + I$ and $J + I^{[3]}$ can be computed with Macaulay2, and are left to the reader. For the rest of the proof, assume $q = p^e$ with $e \geq 2$. Let $g = xy^2z^5 - x^2yz$ be the generator of the ideal J. We need to reduce the generator $x^{2q}y^{2q}z^q - x^qy^qz^{2q}$ of $I^{[q]}$ to normal form modulo g. Observe that whenever $a \geq 1$, $b \geq 2$, and $c \geq 5$, then $x^ay^bz^c$ reduces to $x^{a+1}y^{b-1}z^{c-4}$, so the normal form of the monomial $x^ay^bz^c$ is the monomial $x^{a+k}y^{b-k}z^{c-4k}$, where k is the largest integer such that $b-(k-1) \geq 2$ and $c - 4(k-1) \geq 5$; i.e., $b \geq k+1$ and $c \geq 4k+1$. For the monomial $x^{2q}y^{2q}z^q$, k is the largest integer such that $2q \geq k+1$ and $q \geq 4k+1$; in this case, if the latter inequality holds, then the former is true as well, so we only need to find the largest integer k for which $q \geq 4k+1$. If e is even, then $q \equiv 1$ modulo 4, so $k = (q-1)/4$ and the normal form of $x^{2q}y^{2q}z^q$ is $x^{\frac{9}{4}q-\frac{1}{4}}y^{\frac{7}{4}q+\frac{1}{4}}z$. If e is odd, then $q \equiv 3$ modulo 4, so $k = (q-3)/4$ and the normal form of $x^{2q}y^{2q}z^q$ is $x^{\frac{9}{4}q-\frac{3}{4}}y^{\frac{7}{4}q+\frac{3}{4}}z^3$. Similarly, $x^qy^qz^{2q}$ reduces k times using g to its normal form when k is the largest integer such that $q \geq k+1$ and $2q \geq 4k+1$. As before, we can ignore the first inequality. For all $e \geq 2$, we get $k = (2q-2)/4 = (q-1)/2$, so the normal form of $x^qy^qz^{2q}$ is $x^{\frac{3}{2}q-\frac{1}{2}}y^{\frac{1}{2}q+\frac{1}{2}}z^2$. The the normal form for the generator $x^{2q}y^{2q}z^q - x^qy^qz^{2q}$ of $I^{[q]}$ is

$$f' := \begin{cases} x^{\frac{9}{4}q-\frac{1}{4}}y^{\frac{7}{4}q+\frac{1}{4}}z - x^{\frac{3}{2}q-\frac{1}{2}}y^{\frac{1}{2}q+\frac{1}{2}}z^2 & e \text{ even} \\ x^{\frac{9}{4}q-\frac{3}{4}}y^{\frac{7}{4}q+\frac{3}{4}}z^3 - x^{\frac{3}{2}q-\frac{1}{2}}y^{\frac{1}{2}q+\frac{1}{2}}z^2 & e \text{ odd}. \end{cases}$$

Suppose that $e \geq 2$ is even. Define the polynomials

$$f_k := x^{\frac{9}{4}q-\frac{1}{4}+k}y^{\frac{7}{4}q+\frac{1}{4}-k}z - x^{\frac{3}{2}q-\frac{1}{2}+k}y^{\frac{1}{2}q+\frac{1}{2}-k}z^2 \quad \text{for } 0 \leq k \leq (q-1)/2,$$

$$h_j := x^{\frac{11}{4}q+\frac{1}{4}+j}y^{\frac{5}{4}q-\frac{1}{4}-j}z - x^{2q-1}yz^{6+4j} \quad \text{for } 0 \leq j \leq (q-3)/2, \text{ and}$$

$$r := x^{2q-1}yz^{2q+4} - x^{\frac{13}{4}q-\frac{1}{4}}y^{\frac{3}{4}q+\frac{1}{4}}z.$$

Note that $f' = f_0$. When $0 \leq k \leq (q-3)/2$, the S-polynomial

$$\begin{aligned} S(g, f_k) &= x^{\frac{9}{4}q-\frac{5}{4}+k}y^{\frac{7}{4}q-\frac{7}{4}-k}g - z^4 f_k \\ &= -x^{\frac{9}{4}q-\frac{1}{4}+(k+1)}y^{\frac{7}{4}q+\frac{1}{4}-(k+1)}z \\ &\quad + x^{\frac{3}{2}q-\frac{1}{2}+k}y^{\frac{1}{2}q+\frac{1}{2}-k}z^6 \\ &\equiv -x^{\frac{9}{4}q-\frac{1}{4}+(k+1)}y^{\frac{7}{4}q+\frac{1}{4}-(k+1)}z \\ &\quad + x^{\frac{3}{2}q-\frac{1}{2}+(k+1)}y^{\frac{1}{2}q+\frac{1}{2}-(k+1)}z^2 \\ &= -f_{k+1}, \end{aligned}$$

where $\equiv$ denotes a reduction using g on the second term. Therefore, the polynomials f_k for $0 \leq k \leq (q-1)/2$ are included with g and f' in the procedure to compute the Gröbner basis. The last polynomial in this family is $f_{(q-1)/2} = x^{\frac{11}{4}q-\frac{3}{4}}y^{\frac{5}{4}q+\frac{3}{4}}z - x^{2q-1}yz^2$. Then

$$\begin{aligned} S(g, f_{(q-1)/2}) &= x^{\frac{11}{4}q-\frac{7}{4}}y^{\frac{5}{4}q-\frac{5}{4}}g - z^4 f_{(q-1)/2} \\ &= -x^{\frac{11}{4}q+\frac{1}{4}}y^{\frac{5}{4}q-\frac{1}{4}}z + x^{2q-1}yz^6 = -h_0. \end{aligned}$$

Similarly, the S-polynomial $S(g, h_j) = -h_{j+1}$ for all $0 \leq j \leq (q-5)/2$, so the polynomials h_j for $0 \leq j \leq (q-3)/2$ are appended to the basis. The final polynomial in this list is $h_{(q-3)/2} = x^{\frac{13}{4}q-\frac{5}{4}}y^{\frac{3}{4}q+\frac{5}{4}}z - x^{2q-1}yz^{2q}$. Then

$$\begin{aligned} S(g, h_{(q-3)/2}) &= x^{\frac{13}{4}q-\frac{9}{4}}y^{\frac{3}{4}q-\frac{3}{4}}g - z^4 h_{(q-3)/2} \\ &= -x^{\frac{13}{4}q-\frac{1}{4}}y^{\frac{3}{4}q+\frac{1}{4}}z + x^{2q-1}yz^{2q+4} = r. \end{aligned}$$

Therefore, r is also added to the basis by the Buchberger algorithm. All of the remaining S-polynomials reduce to zero modulo this set of polynomials, so the set

Example	$\delta(q)$	$\Delta(q)$	$c(q)$
Prop. 4.1	linear	linear	constant
Prop. 4.3	linear	linear	linear
Prop. 4.5(a)	constant	linear	constant
Prop. 4.5(b)	linear	linear ($q \geq p$)	constant ($q \geq p$)
Prop. 4.6	linear ($q \geq p$)	linear ($q \geq p$)	linear
Prop. 4.7	linear	periodically linear ($q \geq p$)	periodically constant ($q \geq p$)
Prop. 4.8	periodically linear ($q \geq p^2$)	periodically linear ($q \geq p^2$)	periodically linear ($q \geq p^2$)
Prop. 4.10	linear	linear (high coeff.)	linear

TABLE 1. Summary.

$\{g, f_k, h_j, r \mid 0 \leq k \leq (q-1)/2, 0 \leq j \leq (q-3)/2\}$ is a Gröbner basis for $J + I^{[q]}$ in the case that $e \geq 2$ is even.

Finally, suppose that $e \geq 3$ is odd. We have already shown that the polynomials $g = xy^2z^5 - x^2yz$ and $f' = x^{\frac{9}{4}q-\frac{3}{4}}y^{\frac{7}{4}q+\frac{3}{4}}z^3 - x^{\frac{3}{2}q-\frac{1}{2}}y^{\frac{1}{2}q+\frac{1}{2}}z^2$ are a basis for $J + I^{[q]}$. Define the polynomials

$$\begin{aligned} s_k &:= x^{\frac{9}{4}q+\frac{1}{4}+k}y^{\frac{7}{4}q-\frac{1}{4}-k}z - x^{\frac{3}{2}q-\frac{1}{2}+k}y^{\frac{1}{2}q+\frac{1}{2}-k}z^4 \\ &\qquad\qquad \text{for } 0 \leq k \leq (q-1)/2, \\ t_j &:= x^{\frac{11}{4}q+\frac{3}{4}+j}y^{\frac{5}{4}q-\frac{3}{4}-j}z - x^{2q-1}yz^{8+4j} \\ &\qquad\qquad \text{for } 0 \leq j \leq (q-3)/2, \text{ and} \\ u &:= x^{2q-1}yz^{2q+6} - x^{\frac{13}{4}q+\frac{1}{4}}y^{\frac{3}{4}q-\frac{1}{4}}z. \end{aligned}$$

By an argument very similar to the proof of the case when $e \geq 2$ is even, we get that $S(g, f') = -s_0$ and $S(g, s_k) \equiv -s_{k+1}$ for all $0 \leq k \leq (q-3)/2$, where $\equiv$ denotes a reduction by g. Then $S(g, s_{(q-1)/2}) = t_0$ and $S(g, t_j) = -t_{j+1}$ when $0 \leq j \leq (q-5)/2$. Taking one further S-polynomial with g, $S(g, t_{(q-3)/2}) = u$. Finally, all of the remaining S-polynomials reduce to 0 modulo these polynomials, so the set $\{g, f', s_k, t_j, u \mid 0 \leq k \leq (q-1)/2, 0 \leq j \leq (q-3)/2\}$ is a Gröbner basis for $J + I^{[q]}$ when $e \geq 3$ is odd.

Since, in each case the Gröbner basis we computed is also reduced, the results on the functions associated to these ideals then follow immediately from these bases. $\square$

Note 4.9. If we change the characteristic in Proposition 4.8 to $p = 2$, we find that the x_n-degree function $\delta(q)$ is dependent on the characteristic of the field F as well; in fact, all three functions $\delta(q)$, $\Delta(q)$, and $c(q)$ are altered, and the periodicity is lost. In particular, if $R = \mathbb{Z}/2\mathbb{Z}[x, y, z]$, and $I = (x^2y^2z - xyz^2)$ and $J = (xy^2z^5 - x^2yz)$ are the same ideals as in Proposition 4.8, a computation similar to the one above shows that the reduced Gröbner basis for $J + I^{[q]}$ with $q = 2^e$ and $e \geq 3$ is

$$\left\{ \begin{array}{l|l} xy^2z^5 - x^2yz, & \\ x^{\frac{9}{4}q-1}y^{\frac{7}{4}q+1}z^4 - x^{\frac{3}{2}q-1}y^{\frac{1}{2}q+1}z^4, & 0 \leq j \leq \dfrac{(q-2)}{2}, \\ x^{\frac{9}{4}q+j}y^{\frac{7}{4}q-j}z - x^{\frac{3}{2}q+j}y^{\frac{1}{2}q-j}z, & \\ x^{\frac{11}{4}q+k}y^{\frac{5}{4}q-k}z - x^{2q-1}yz^{5+4k}, & 0 \leq k \leq \dfrac{(q-2)}{2} \\ x^{2q-1}yz^{2q+5} - x^{\frac{13}{4}q-1}y^{\frac{3}{4}q+1}z^5 & \end{array} \right\}.$$

Thus the associated functions satisfy $\delta(q) = 2q + 5$, $\Delta(q) = 4q + 5$, and $c(q) = q + 3$ for $q \geq 2^3$. The main difference in the proofs lies in the reduction of the generator $x^{2q}y^{2q}z^q - x^qy^qz^{2q}$ of $I^{[q]}$ modulo the generator $g = xy^2z^5 - x^2yz$ of J.

In the final example, we show that it need not be the case that the total degree of the Gröbner basis of $J + I^{[q]}$ is bounded above by $q \cdot \max\{\text{Gbdeg } I, \text{Gbdeg } J\}$, where Gbdeg denotes the total degree of the reduced Gröbner basis (with the reverse lexicographic ordering). The proof follows the lines of reasoning developed in the other proofs of this section, and is left to the reader.

Proposition 4.10. *Let $R = \mathbb{Z}/3\mathbb{Z}[x, y, z, w]$. The ideal $J + I^{[q]}$ with $I = (x^2y^2zw^5 - xyz^2w^2)$, $J = (xy^2z^3w - xyzw^3)$, and $q = 3^e$ has the reduced Gröbner basis*

$$\left\{ \begin{array}{l|l} xy^2z^3w - xyzw^3, & \\ x^{2q}y^{(3q+1-2k)/2}zw^{6q-1+2k} & 0 \leq k \leq \dfrac{(3q-1)}{2} \\ \quad - x^qyz^{2k+2}w^{4q-2} & \end{array} \right\}$$

with respect to the reverse lexicographic ordering with $w < z < y < x$. Therefore, the maximal w-degree of the Gröbner basis is $\delta(q) = 9q - 2$, the maximal total degree is $\Delta(q) = 11q$, and the number of elements is $c(q) = 3(q+1)/2$ for all q.

Therefore $q \cdot \max\{\text{Gbdeg } I, \text{Gbdeg } J\} = q \cdot \max\{10, 7\} < 11q = \text{Gbdeg } (J + I^{[q]})$.

In Table 1, we summarize the examples in this section. All of these examples satisfy Katzman's conjecture that the x_n-degree $\delta(q)$ of the reduced Gröbner basis of $J + I^{[q]}$ is bounded above linearly in q. Furthermore, in all of these examples the total degree and cardinality of the Gröbner basis are also bounded above linearly in q. However, we are left with the open question of whether the behavior of the functions $\delta(q)$, $\Delta(q)$, and $c(q)$ (eventually) follows one of the patterns in the table above, and whether linear upper bounds on $\delta(q)$, $\Delta(q)$, and $c(q)$ hold, for all ideals I and J in a polynomial ring.

5. MACAULAY2 CODE

We used variations of the following Macaulay2 code for our calculations, included for the readers interested in making further computations.

Input: polynomial ring R, ideals I, J
Output: $\text{fn}(e) =$ Gröbner basis of $J + I^{[p^e]}$,
$\text{df}(e) =$ maximal total degree of an element of the Gröbner basis.

```
p = 3
R = ZZ/p[x,y,z,MonomialSize=>16];
I = ideal(y^2*z-x^2); J = ideal(y^3-x*y);
fn = e -> (transpose gens gb (J+I^(p^e)))
df = e -> (L = {}; i = 0;
           G = gens gb (J + I^(p^e));
           l = rank source G;
           while i < l do (
              L = prepend (degree G_(0,i), L);
              i = i + 1; );
           max L)
```

ACKNOWLEDGMENTS

The authors thank Aldo Conca and Enrico Sbarra for helpful discussions of an earlier version of this paper. The first author acknowledges support from NSF grant DMS-0071037. The second author acknowledges support from NSF grant DMS-9970566.

REFERENCES

[Cox et al. 92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. New York: Springer-Verlag, 1992.

[Grayson and Stillman 03] D. R. Grayson and M. E. Stillman. "Macaulay2, a Software System for Research in Algebraic Geometry." Available from World Wide Web (http://www.math.uiuc.edu/Macaulay2/), 2003.

[Hochster and Huneke 90] M. Hochster and C. Huneke. "Tight Closure, Invariant Theory, and the Briançon-Skoda Theorem." *J. Amer. Math. Soc.* 3 (1990), 31–116.

[Katzman 98] M. Katzman. "The Complexity of Frobenius Powers of Ideals." *J. Algebra* 203 (1998), 211–225.

[Smith 01] K. E. Smith. "Tight Closure Commutes with Localization in Binomial Rings." *Proc. Amer. Math. Soc.* 129 (2001) 667–669.

Susan Hermiller, Department of Mathematics, University of Nebraska, Lincoln, Nebraska 68588-0130 (smh@math.unl.edu)

Irena Swanson, Department of Mathematical Sciences, New Mexico State University, Las Cruces, NM 88003-8001 (iswanson@nmsu.edu)

Submitted June 17, 2003; accepted in revised form December 15, 2004.