These things *might* be different!

A disoriented amateur's guide to the algorithms and assumptions of multivariate polynomial based cryptography

Ben Clingenpeel

4/26/23

Abstract

In this thesis we walk through some of the notions at play in solving systems of polynomial equations. The motivation for this comes from cryptosystems based on the difficulty of solving such systems. In the first section, we explore a main tool used to solve systems of polynomials: Gröbner bases. We will look at two algorithms used to compute Gröbner bases, prove that they work, and show that they lead to distinct notions of the solving degree of a system. In the second section, we explain some ideas from commutative algebra used to obtain bounds on the solving degree, and the genericity assumptions needed to guarantee these bounds. Here we give two versions of what it means for a system to be in generic coordinates and show that one is strictly stronger than the other. In the final section, we give two more definitions of genericity, with connections to Fröberg's Conjecture and the notion of the generic initial ideal of a system. We show that none of these definitions are exactly the same, and end with questions about the relationships between them.

1 Gröbner bases and solving degree

Notation. We will use R to mean $k[x_1, \ldots, x_n]$ for a field k. When discussing initial ideals of ideals I with a specified generating set $\mathcal{F} = \{f_1, \ldots, f_s\}$, we will use $\mathbf{in}(I)$ or $\mathbf{in}(\mathcal{F})$ to mean the initial ideal $(\text{in}(f) : f \in I)$ and $\text{in}(\mathcal{F})$ (without boldface) to mean the monomial ideal with generators $\{\text{in}(f) : f \in \mathcal{F}\} = \{\text{in}(f_1), \ldots, \text{in}(f_s)\}$. We recall that a set $\mathcal{G} = \{g_1, \ldots, g_t\}$ is a **Gröbner basis** for I if $(\mathcal{G}) = I$ and $\text{in}(\mathcal{G}) = \mathbf{in}(\mathcal{G})$.

Given a system of of equations $\mathcal{F} = \{f_1, \ldots, f_s\}$ in variables $x_1, \ldots, x_n$ and the ideal $I = (f_1, \ldots, f_s) \subset R$ it defines, we are interested in finding the corresponding solution set, the affine variety $\mathcal{Z}(I)$. A general way to do this is to compute a Gröbner basis with respect to the lexicographic (LEX) order. This yields a system of equations with the same solution set, but crucially, it includes an equation in a single variable, allowing us to solve the system. This approach is outlined in section 2 of [Caminata and Gorla, 2020]. In general, computing a LEX Gröbner basis is more

computationally demanding, and so it is often easier to compute a Gröbner basis with respect to the degree reverse lexicographic (DRL) ordering, and then convert the resulting basis to a LEX basis, for example using the FGLM algorithm [Faugere et al., 1993].

The complexity of computing a Gröbner basis is therefore of interest, and there are several algorithms to do this. There is Buchberger's algorithm, which uses Buchberger's criterion to gradually add elements to a basis until it is a Gröbner basis (see [Cox et al., 2013]), but many faster algorithms take an approach based on Gaussian elimination, converting the problem of finding a Gröbner basis to finding a reduced row-echelon form (RREF) of a matrix. Among these linear algebra based approaches, there are a number that use Macaulay matrices or Macaulay-like matrices. We will analyze two such algorithms, and will use the following definition:

Definition 1. Let k be a field and let $\mathcal{F} = \{f_1, \ldots, f_s\} \subset R$ be a system of equations. Fixing a term order τ on R and using $(\mathcal{F})$ to denote the ideal $(f_1, \ldots, f_s)$ generated by this system, we define for a degree $d \geq 0$ the **Macaulay matrix of $\mathcal{F}$ in degree** d, denoted $M_{\leq d}$, to be the matrix whose columns are indexed by all monomials of degree at most d, arranged in decreasing order with respect to τ and whose rows are indexed by all monomial multiples of elements of $\mathcal{F}$ with degree at most d, such that every entry is the coefficient of its column index monomial in the row index polynomial.

Example 1. Let $f_1 = x$ and $f_2 = x^2 - y$. Then the degree $d = 2$ Macaulay matrix of $\mathcal{F} = \{f_1, f_2\}$ with respect to the degree reverse lexicographic (DRL) order is

$$M_{\leq 2} = \begin{array}{c} \\ f_1 \\ xf_1 \\ yf_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & x & y & 1 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & \mathbf{-1} & 0 \end{pmatrix} \end{array}.$$

Notation. Given any matrix A, we will denote its reduced row-echelon form by A^r. Noting that any matrix A whose columns are indexed by monomials has its rows represent polynomials (using each entry as the coefficient of its corresponding column index monomial), we will use $\mathscr{P}(A)$ to mean the set of polynomials obtained from the rows of A, and $(\mathscr{P}(A))$ will denote the ideal they generate. We will use $\mathscr{R}(A)$ to mean the set of polynomials obtained from all rows in the row space of A, that is, $\mathscr{R}(A)$ is the free k-vector space with generating set $\mathscr{P}(A)$.

Example 2. Continuing the previous example, using $M_{\leq 2}$ above, we have that

$$M^r_{\leq 2} = \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \end{pmatrix}.$$

Then $\mathscr{P}(M^r_{\leq 2}) = \{x^2, xy, x, y\}$ and so $(\mathscr{P}(M^r_{\leq 2})) = (x, y)$.

Since ideals are closed under k-linear combinations, we always have the inclusions $\mathscr{P}(M_{\leq d}) \subset \mathscr{R}(M_{\leq d}) \subset (\mathscr{P}(M_{\leq d}))$. We also have that $\mathscr{R}(M^r_{\leq d}) = \mathscr{R}(M_{\leq d})$, so we see that

$$\mathscr{P}(M_{\leq d}) \subset \mathscr{R}(M^r_{\leq d}) \subset (\mathscr{P}(M^r_{\leq d})) \quad \text{and} \quad \mathscr{P}(M^r_{\leq d}) \subset \mathscr{R}(M_{\leq d}) \subset (\mathscr{P}(M_{\leq d})),$$

meaning $(\mathscr{P}(M^r_{\leq d})) = (\mathscr{P}(M_{\leq d}))$. From this, we also see that taking $D = \max\{\deg(f) : f \in \mathcal{F}\}$ gives $(\mathscr{P}(M^r_{\leq D})) = (\mathcal{F})$. We will soon show that there exists a $d \geq D$ for which $\mathscr{P}(M^r_{\leq d})$ is a Gröbner basis for $(\mathcal{F})$, and this existence gives us the first algorithm for computing a Gröbner basis by performing Gaussian elimination on Macaulay matrices: for large enough d, construct $M_{\leq d}$ and compute $M^r_{\leq d}$ to obtain the Gröbner basis $\mathscr{P}(M^r_{\leq d})$. This algorithm is analyzed in [Caminata and Gorla, 2020]. We will refer to it as **Algorithm I**. In practice, we do not know a priori what degree $d \geq 0$ we should use to run this algorithm, and so one approach is to simply try all degrees starting from $D = \max\{\deg(f) : f \in \mathcal{F}\}$. Many algorithms for computing Gröbner bases work similarly in the sense that, while we know there exists some degree for which the algorithm returns a Gröbner basis, we do not know which. The smallest degree d for which which the algorithm returns a Gröbner basis is called the **solving degree** of the system, which in the above example is denoted $\mathrm{sd}_{1,DRL}(\mathcal{F})$ where the 1 refers to Algorithm 1, and DRL refers to the term order. We have not yet seen enough examples to justify the distinctions, but we will soon, and we will drop the subscripts when the algorithms and term orders are clear from the context.

Since the complexity of such algorithms can be thought of as a function of the size of the largest matrix involved, which in turn is determined by the solving degree, we would like some methods to estimate it, since it is difficult to compute on its own without simply running the Gröbner basis algorithm. These estimations are done using various different invariants, but before we discuss them, we will first finish showing that Algorithm I does indeed produce a Gröbner basis. We will then introduce a second algorithm whose correctness follows from the correctness of Algorithm I, and we will compare the two to show that the solving degree is algorithm-dependent, something not always made explicit in discussions of the solving degree. In Section 2, we will begin to explore some of the different invariants used to estimate the solving degree.

Notation. Let $\mathrm{piv}(M_{\leq d})$ denote the set of monomials indexing the pivot columns of the matrix $M_{\leq d}$, and define $\mathrm{in}(d) = \mathrm{in}(\mathscr{P}(M^r_{\leq d}))$ for ease of notation. Note that because each initial term of

a polynomial in $\mathscr{P}(M^r_{\leq d})$ is a monomial that indexes a pivot column of $M^r_{\leq d}$, we see that $\mathrm{in}(d)$ can also be defined to be the ideal $(\mathrm{piv}(M_{\leq d}))$ generated by the monomials indexing the pivot columns of $M_{\leq d}$ (since these are the same as the pivot columns of $M^r_{\leq d}$).

Example 3. Using the DRL ordering, let $\mathcal{F} = \{f_1, f_2\}$ with $f_1 = x^2 - 1$ and $f_2 = xy + x$, as in Example 8 of [Caminata and Gorla, 2020]. Then we have that $\mathrm{in}(\mathcal{F}) = (x^2, xy)$, but

$$y + 1 = -x^2y + y - x^2 + 1 + x^2y + x^2 = -(y+1)f_1 + xf_2 \in (\mathcal{F})$$

implies that $y \in \mathbf{in}(\mathcal{F}) \setminus \mathrm{in}(\mathcal{F})$, so we have that $\mathrm{in}(\mathcal{F}) \neq \mathbf{in}(\mathcal{F})$, and therefore $\mathcal{F}$ is not a Gröbner basis for the ideal it generates. Continuing this example, we can compute that

$$M_{\leq 2} = \begin{array}{c} \\ f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{cccccc} x^2 & xy & y^2 & x & y & 1 \end{array} \\ \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{-1} \\ 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 \end{pmatrix} \end{array} = M^r_{\leq 2},$$

which is already reduced. Therefore $\mathrm{piv}(M_{\leq 2}) = \{x^2, xy\}$, and so $\mathrm{in}(2) = (x^2, xy)$ which we see does indeed equal the ideal generated by the initial terms of the polynomials in $\mathscr{P}(M^r_{\leq 2}) = \{x^2 - 1, xy + x\}$. Hence $\mathscr{P}(M^r_{\leq 2})$ is the same as our starting generating set, and is not a Gröbner basis for $(\mathcal{F})$, but if instead we do the same computations with degree $d = 3$, we have the following:

$$M_{\leq 3} = \begin{array}{c} \\ f_1 \\ f_2 \\ xf_1 \\ yf_1 \\ xf_2 \\ yf_2 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2 & xy & y^2 & x & y & 1 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{-1} \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{-1} & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{-1} & 0 \\ 0 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \end{pmatrix} \end{array},$$

and bringing this into RREF, we have

$$M^r_{\leq 3} = \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{-1} & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{-1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{-1} \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} \end{pmatrix},$$

so that $\mathrm{in}(3) = (x^3, x^2y, xy^2, x^2, xy, y) = (x^2, y) = \mathbf{in}(\mathcal{F})$. Therefore $\mathrm{in}(\mathscr{P}(M^r_{\leq 3})) = \mathrm{in}(3) = \mathbf{in}(\mathcal{F})$,

and since the original generating set $\mathcal{F} = \{f_1, f_2\}$ is included in $\mathscr{P}(M_{\leq 3})$ and therefore also in $(\mathscr{P}(M^r_{\leq 3})) = (\mathcal{F})$. Therefore

$$\mathscr{P}(M^r_{\leq 3}) = \{x^3 - x, x^2y + 1, xy^2 - x, x^2 - 1, xy + x, y + 1\}$$

is a Gröbner basis for $(\mathcal{F})$.

Lemma 1. *Given an ideal $(\mathcal{F})$ and degrees d_1 and d_2 with $0 \leq d_1 \leq d_2$, we have that $\text{in}(d_1) \subset \text{in}(d_2)$.*

Proof. Since $\text{in}(d_1)$ and $\text{in}(d_2)$ are monomial ideals, it is a Corollary of Lemma 3 of section 2.4 of [Cox et al., 2013] that $\text{in}(d_1) \subset \text{in}(d_2)$ if and only if all monomials of $\text{in}(d_1)$ lie in $\text{in}(d_2)$. Therefore let $m \in \text{in}(d_1)$ be a monomial. Lemma 2 of the same section in [Cox et al., 2013] says that $m \in \text{in}(d_1) = (\text{piv}(M_{\leq d_1}))$, means that there is some generating monomial $m^* \in \text{piv}(M_{\leq d_1})$ that divides m. Therefore, if we can show that $m^* \in \text{in}(d_2)$, we will have that $m \in \text{in}(d_2)$. To this end, note that $m^* \in \text{piv}(M_{\leq d_1})$ means that the column of $M_{\leq d_1}$ indexed by m^* is a pivot column, so the corresponding column in $M^r_{\leq d_1}$ is all zeros except for a 1 in a row that corresponds to a polynomial p with $\text{in}(p) = m^*$. This row corresponding to p is in the row space $\mathscr{R}(M^r_{\leq d_1}) = \mathscr{R}(M_{\leq d_1})$, and so p can be written as a k-linear combination of the polynomials in $\mathscr{P}(M_{\leq d_1})$. Note that the polynomials involved in this k-linear combination all have degree less than or equal to d_1, which is in turn less than or equal to d_2. Therefore these polynomials also correspond to rows of $M_{\leq d_2}$, and we have that p is a k-linear combination of the elements of $\mathscr{P}(M_{\leq d_2})$.

That p is a k-linear combination of the elements of $\mathscr{P}(M_{\leq d_2})$ means that the row vector corresponding to p with the same length as the length of the rows of $M_{\leq d_2}$ (that is, the row vector representation of p whose entries are indexed by monomials of degree less than or equal to d_2) is in the row space $\mathscr{R}(M_{\leq d_2}) = \mathscr{R}(M^r_{\leq d_2})$, and so this row is a k-linear combination of the nonzero rows of $M^r_{\leq d_2}$. That $m^* = \text{in}(p)$ means that any rows of $M^r_{\leq d_2}$ with pivots further left than the column indexed by m^* are not involved in this k-linear combination (if they were, there would need to be cancellation involved, and such cancellation occurring would contradict $M^r_{\leq d_2}$) being in RREF). Then because the row corresponding to p has 1 as an entry in the m^* column, this column cannot consist entirely of zeros—there exists at least one row involved in the k-linear combination associated to p with a nonzero entry in the m^* column. Because this row is part of this k-linear combination, it cannot have a pivot further left than the m^* column, and so we conclude that the m^* entry of this row is a pivot since all nonzero rows of RREF matrices must have a pivot. Therefore $m^* \in \text{piv}(M_{\leq d_2})$ and since m^* divides m, we see that $m \in (\text{piv}(M_{\leq d_2})) = \text{in}(d_2)$. Hence $\text{in}(d_1) \subset \text{in}(d_2)$, as claimed. □

Theorem 1. *For an ideal $(\mathcal{F})$, there exists a $D \geq 0$ such that $\mathscr{P}(M^r_{\leq D})$ is a Gröbner basis of $(\mathcal{F})$.*

Proof. By the Lemma, we have that ascending chain of ideals $\text{in}(0) \subset \text{in}(1) \subset \text{in}(2) \subset \ldots$ contained in $R = k[x_1, \ldots, x_n]$. Because R is Noetherian, there exists a $D' \geq 0$ such that for all $d \geq D'$,

$\text{in}(d) = \text{in}(D')$. As in the discussion following Example 2, for any $d \geq \max\{\deg(f) : f \in \mathcal{F}\}$, $\mathscr{P}(M_{\leq d})$ contains $\mathcal{F}$ and so $(\mathscr{P}(M_{\leq d})) = (\mathscr{P}(M^r_{\leq d})) = (\mathcal{F})$. Therefore we may choose some $D \in \mathbb{N}$ large enough such that $D \geq D'$ and that $(\mathscr{P}(M^r_{\leq D})) = (\mathcal{F})$. We claim that $\mathscr{P}(M^r_{\leq D})$ is a Gröbner basis for $(\mathcal{F})$, which means proving that $\text{in}(\mathscr{P}(M_{\leq D})) = \mathbf{in}(\mathscr{P}(M_{\leq D}))$, that is, that $\text{in}(D) = \mathbf{in}(\mathcal{F})$. Because the ideal $(\mathscr{P}(M^r_{\leq D}))$ is the ideal $(\mathcal{F})$, all initial terms of polynomials in $\mathscr{P}(M^r_{\leq D})$ are initial terms of polynomials in $(\mathcal{F})$, and so $\text{in}(D) = \text{in}(\mathscr{P}(M^r_{\leq D})) \subset \mathbf{in}(\mathcal{F})$.

To show the other containment, recall from the proof of the Lemma that $\text{in}(D)$ and $\text{in}(I)$ being monomial ideals means it is sufficient to show that all monomials $m \in \mathbf{in}(\mathcal{F})$ are in $\text{in}(D)$ in order to show that $\text{in}(I) \subset \text{in}(D)$. Therefore let $m \in \mathbf{in}(\mathcal{F})$ be an arbitrary monomial. Then there exists some $p \in (\mathcal{F})$ with initial term $\text{in}(p) = m$. Then $p \in (\mathcal{F}) = (\mathscr{P}(M^r_{\leq D})) = (\mathscr{P}(M_{\leq D}))$ means p can be written as $p = \sum_{q \in \mathscr{P}(M_{\leq D})} h_q q$ where $h_q \in R$. Then because each h_q is a k-linear combination of monomials, we have that $h_q = \sum_{\alpha \in N_q} a_\alpha x^\alpha$ for some finite index set N_q. Therefore

$$p = \sum_{q \in \mathscr{P}(M_{\leq D})} \sum_{\alpha \in N_q} a_\alpha x^\alpha q.$$

Since $\mathscr{P}(M_{\leq D})$ is finite and each index set N_q is finite, we may set

$$d^* = \max \left\{ \deg(x^\alpha q) \,\middle|\, \alpha \in \bigcup_{q \in \mathscr{P}(M_{\leq D})} N_q,\ q \in \mathscr{P}(M_{\leq D}) \right\} \geq D.$$

Then because each q is a monomial times one of the polynomials $f \in \mathcal{F}$, so is each each $x^\alpha q$, and therefore p as written above is a k-linear combination of polynomials corresponding to rows in the Macaulay matrix $M_{\leq d^*}$. Therefore if r_p is the row vector corresponding to p whose entries are indexed by monomials of degree less than or equal to d^*, we have that r_p is an element of the row space $\mathscr{R}(M_{\leq d^*}) = \mathscr{R}(M^r_{\leq d^*})$. Therefore we have the same situation as in Lemma 1: we have a polynomial p with leading term m satisfying $\deg(m) \leq d^*$ such that r_p is a k-linear combination of the nonzero rows of $M^r_{\leq d^*}$. As in the proof of Lemma 1, then, we have that the column indexed by m is a pivot column of $M_{\leq d^*}$, which means that $m \in \text{piv}(M_{\leq d^*}) \subset (\text{piv}(M_{\leq d^*})) = \text{in}(d^*)$. Because $d^* \geq D$, we also have that $m \in \text{in}(d^*) = \text{in}(D)$ since the ascending chain $\text{in}(0) \subset \text{in}(1) \subset \text{in}(2) \subset \ldots$ stabilizes at or before D. Therefore $\mathbf{in}(\mathcal{F}) \subset \text{in}(D)$, and since we have shown both containments, the set $\mathscr{P}(M^r_{\leq D})$ is a Gröbner basis for I. □

Now that we have shown Algorithm I does indeed produce a Gröbner basis, we introduce a variant which we will call **Algorithm II**. This algorithm is considered in [Caminata and Gorla, 2023] and differs from Algorithm I only in that after row reducing a matrix $M_{\leq d}$, Algorithm II adds new rows for each polynomial uf where f is a polynomial of degree strictly less than d corresponding to a row in $M_{\leq d}$ and u is a monomial such that $\deg(uf) \leq d$ and $uf \notin \mathscr{R}(M_{\leq d})$. This algorithm then repeats the row reduction of the matrix $M_{\leq d}$ with its new rows until no new rows are added.

We have shown that Algorithm I does produce a Gröbner basis. If we suppose for a system $\mathcal{F}$ and term order τ that Algorithm I produces a Gröbner basis in degree d and run Algorithm II also in degree d, then the matrix the algorithm starts with already has a Gröbner basis in its row space, meaning now new rows are added, and Algorithm II terminates at least by degree d, and so we have that $\mathrm{sd}_{2,\tau}(\mathcal{F}) \leq \mathrm{sd}_{1,\tau}(\mathcal{F})$. The question that naturally arises is: do these two algorithms yield *the same* solving degree? That is, given a system $\mathcal{F}$, is it true that the largest degree involved in computing a Gröbner basis is the same from algorithm to algorithm? To show the answer is *no*, we give the following example.

Example 4. Let

$$\mathcal{F} = \{f_1, f_2\} \subset k[x, y, z] \quad \text{for} \quad f_1 = y^2,\ f_2 = yz + x,$$

and consider the Macaulay matrix $M_{\leq 3}$:

	x^3	x^2y	xy^2	y^3	x^2z	xyz	y^2z	xz^2	yz^2	z^3	x^2	xy	y^2	xz	yz	z^2	x	y	z	1
f_1	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0
f_2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	**1**	0	0	0
xf_1	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
yf_1	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
zf_1	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0
xf_2	0	0	0	0	0	**1**	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0
yf_2	0	0	0	0	0	0	**1**	0	0	0	0	**1**	0	0	0	0	0	0	0	0
zf_2	0	0	0	0	0	0	0	0	**1**	0	0	0	0	**1**	0	0	0	0	0	0

which in RREF is

x^3	x^2y	xy^2	y^3	x^2z	xyz	y^2z	xz^2	yz^2	z^3	x^2	xy	y^2	xz	yz	z^2	x	y	z	1
0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	**1**	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	**1**	0	0	0	0	**1**	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	0	**1**	0	0	0

We note now that $x^2 = z^2 f_1 + (x - yz) f_2 \in (\mathcal{F})$ and so $x^2 \in \mathbf{in}(\mathcal{F})$ but that the rows of the above

matrix correspond to polynomials

$$\{xy^2, y^3, xyz + x^2, y^2z, yz^2 + xz, xy, y^2, yz + x\},$$

whose leading terms generate the ideal $(xy^2, y^3, xyz, y^2z, yz^2, xy, y^2, yz) = (xy, y^2, yz)$. Since $x^2 \notin (xy, y^2, yz)$, we have that $(xy, y^2, yz) \neq \mathbf{in}(\mathcal{F})$, meaning the above collection of polynomials we obtained from the RREF form of $M_{\leq 3}$ is not a Gröbner basis. Therefore $\mathrm{sd}_1(\mathcal{F}) > 3$.

Now using Algorithm II, the first stage of degree 3 computations involves the same matrices as above, though this time instead of checking whether the collection $\{xy^2, y^3, xyz + x^2, y^2z, yz^2 + xz, xy, y^2, yz + x\}$ obtained from the reduced row-echelon form is a Gröbner basis, we check whether there are any monomial multiples of these polynomials that still have degree less than 3 that correspond to row vectors not originally in the row space of the above matrices. For the polynomial xy, we consider the polynomials x^2y, xy^2, and xyz. Since x^2y and xyz are not in the row space of the above matrices, we add new rows for them. For y^2, we consider xy^2, y^3, and y^2z, but these are all already in the row space, so we do not add new rows for them. Similarly, we do not add rows for $xyz + x^2$, $y^2z + xy$, or $yz^2 + xz$. After adding these rows and performing Gaussian elimination, we get the resulting RREF matrix:

$$\begin{array}{c}
\begin{array}{ccccccccccccccccccc}
x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 & x^2 & xy & y^2 & xz & yz & z^2 & x & y & z & 1
\end{array} \\
\begin{pmatrix}
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0
\end{pmatrix}
\end{array}$$

whose rows correspond to the set $\{x^2y, xy^2, y^3, xyz, y^2z, yz^2 + xz, x^2, xy, y^2, yz + x\}$. We now do the same procedure, looking at monomial multiples of these polynomials to see if there are any that are not already contained in the row space of the above matrix. Looking to the degree 2 polynomials here for candidates, we check x^3, x^2y, and x^2z, and see that x^3 and x^2z are not already in the row space. The remaining candidates xy^2, y^3, y^2z, $xyz + x^2$, $y^2z + xy$, and $yz^2 + xz$ are all already in the row space, so we only add rows corresponding to x^3 and x^2z. After adding these rows and

performing Gaussian elimination again, we see that the new RREF form is

$$\begin{array}{cccccccccccccccccccc}
x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 & x^2 & xy & y^2 & xz & yz & z^2 & x & y & z & 1 \\
\left(\begin{array}{cccccccccccccccccccc}
\mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0
\end{array}\right)
\end{array}$$

The rows of the above correspond to the polynomials

$$\{x^3, x^2y, xy^2, y^3, x^2z, xyz, y^2z, yz^2 + xz, x^2, xy, y^2, yz + x\},$$

and we note that all monomial multiples of the polynomials in this set with total degree not more than 3 are now contained in the row space of the above matrix. Since this condition is met, we end the calculations for degree 3, and return this set of polynomials. This set is, in fact, a Gröbner basis (in particular, note that it now contains the x^2 polynomial that posed a problem for the other algorithm in degree 3), and so we end calculations entirely. Thus $\mathrm{sd}_2(\mathcal{F}) = 3 < \mathrm{sd}_1(\mathcal{F})$.

Now that we have two different algorithms for computing Gröbner bases with two different notions of the solving degree, we will now explore some of the invariants used to estimate them in the next section.

2 Estimating the solving degree(s)

Some bounds on the solving degree require certain assumptions about either the system $\mathcal{F}$ or the term order τ. We introduce the following notion of a degree-compatible term order below, which is required for a lower bound on the solving degree:

Definition 2. A term order τ is called **degree-compatible** if $\deg(x^\alpha) < \deg(x^\beta)$ implies $x^\alpha <_\tau x^\beta$. Sometimes such term orders are called **graded** term orders.

For example, the DRL term order is degree-compatible. If we restrict our attention to DRL or to any other degree-compatible term order τ, we have the inequality

$$\text{max. GB. deg}_\tau(\mathcal{F}) \leq \text{sd}_{2,\tau}(\mathcal{F})$$

where $\text{max. GB. deg}_\tau(\mathcal{F})$ is the largest degree of any polynomial appearing in a *reduced* Gröbner basis for $(\mathcal{F})$ with respect to τ. This inequality follows because we have a Gröbner basis computed by a Macaulay matrix based algorithm in degree d, which means the elements of the output basis have degree at most d. In the division required to obtain the reduced Gröbner basis from the output basis, the degree-compatibility of τ ensures that no remainders have degree greater than their corresponding dividends. Hence all terms of polynomials in the reduced Gröbner basis have degree at most $d = \text{sd}_{2,\tau}(\mathcal{F})$. And since $\text{sd}_{2,\tau}(\mathcal{F}) \leq \text{sd}_{1,\tau}(\mathcal{F})$, we also have that

$$\text{max. GB. deg}_\tau(\mathcal{F}) \leq \text{sd}_{1,\tau}(\mathcal{F})$$

as well. Going further, it is shown in [Caminata and Gorla, 2023] that

$$\text{sd}_{2,\tau}(\mathcal{F}) = \max\{d_\mathcal{F}, \text{max. GB. deg}_\tau(\mathcal{F})\}$$

where $d_\mathcal{F}$ is the last fall degree of the system.

Caminata and Gorla show in [Caminata and Gorla, 2020] that certain systems (satisfying a certain genericity requirement) have their solving degrees bounded above by an invariant called the Castelnuovo-Mumford regularity. In what follows, we explain the background necessary for this bound, state the bound, and then give a weaker version that requires no genericity assumption.

Definition 3. An ideal $(\mathcal{F}) \subset R$ for $\mathcal{F} = \{f_1, \ldots, f_s\}$ is said to be **homogeneous** if all of the f_i are homogeneous polynomials. A nonhomogeneous polynomial f of degree d can be made into a homogeneous polynomial in the ring $S = R[h] = k[x_1, \ldots, x_n, h]$ by considering the **homogenization** of f, obtained by writing $f = \sum_{j=0}^{d} f_j$ as the sum of its homogeneous components and setting $f^h = \sum_{j=0}^{d} f_j h^{d-j}$ so that all terms of f^h have degree d.

Example 5. The polynomial $f \in k[x, y, z]$ given by $f = xy^3 + y^2 + yz - 1$ is not homogeneous. We can decompose it into homogeneous components as in the above definition by taking $f_0 = -1$, $f_1 = 0$, $f_2 = y^2 + yz$, $f_3 = 0$, and $f_4 = xy^2$. Then $f^h = xy^3 + y^2h^2 + yzh^2 - h^4 \in k[x, y, z, h]$.

Definition 4. A map $\varphi : M \to N$ of graded R-modules is **homogeneous of degree 0** if for all homogeneous elements $f \in M$, $\deg(\varphi(f)) = \deg(f)$, that is, φ preserves the degrees of homogeneous elements.

Given a polynomial ring $R = k[x_1, \ldots, x_n]$, many of the maps we will consider will not be homogeneous of degree zero, so we may "re-grade" elements of R by considering variables to have

degrees other than the standard $\deg(x_i) = 1$. We denote the ring R with degrees shifted by d by $R(-d)$ and define the jth homogeneous component of $R(-d)$ to be $R(-d)_j = R_{-d+j}$. By degrees "shifted by d" we mean that the variables have degree $1 + d$, so for example if we would like the variables to have degree 3, we will consider the ring $R(-2)$, where $R(-2)_3 = R_1$ contains the variables.

Definition 5. Let $I \subset R$ be a homogeneous ideal. The **minimal free resolution** of I is the exact sequence

$$0 \longrightarrow F_m \xrightarrow{\varphi_m} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} I \longrightarrow 0$$

of free R-modules obtained by choosing a minimal set of generators for I, constructing φ_0 to map a free module F_0 onto I sending the generators of F_0 to the generators of I, constructing φ_1 to map a free module F_1 onto $\ker \varphi_0 \subset F_0$ by sending the generators of F_1 to a minimal set of generators for $\ker \varphi_0$, and continuing this procedure until it terminates. Termination is guaranteed by the Hilbert Syzygy Theorem—a proof using Gröbner bases can be found in section 15.5 of [Eisenbud, 1995] Each time we construct a map φ_i, we take the free modules to be $F_i = \bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{i,j}}$ with the degree shifts chosen so that each φ is homogeneous of degree 0. The numbers $\beta_{i,j}$ are called the **graded Betti numbers** of I, and the **Castelnuovo-Mumford regularity** of I is defined to be $\operatorname{reg} I = \max\{j - i : \beta_{i,j} \neq 0\}$.

Example 6. Consider the ideal $I = (xy^2, x^2, yz) \subset k[x, y, z]$. A minimal free resolution then is

$$0 \longrightarrow R(-5) \xrightarrow{\varphi_2} R(-4)^3 \xrightarrow{\varphi_1} R(-3) \oplus R(-2)^2 \xrightarrow{\varphi_0} I \longrightarrow 0$$

with the maps

$$\varphi_0 = \begin{pmatrix} xy^2 & x^2 & yz \end{pmatrix}, \quad \varphi_1 = \begin{pmatrix} x & z & 0 \\ -y^2 & 0 & yz \\ 0 & -xy & -x^2 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} z \\ -x \\ y \end{pmatrix}.$$

We know that this resolution is minimal because the matrices above do not contain any invertible elements—all elements there are in the irrelevant maximal ideal $\mathfrak{m} = (x, y, z)$. This condition, that for each map φ_i, the image $\operatorname{im} \varphi_i$ is contained in $\mathfrak{m}F_{i-1}$, is taken as a definition of minimality in [Eisenbud, 2005]. Following that text's conventions, the graded Betti numbers are then shown in the table below:

	0	1	2
2	2	—	—
3	1	3	1

where the entry in the ith column and jth row is the graded Betti number $\beta_{i,i+j}$. Then the

regularity, the largest $j - i$ for which $\beta_{i,j} \neq 0$, is simply the index of the last nonzero row, and so we see that in this case $\operatorname{reg} I = 3$.

Definition 6. Given a nonhomogeneous ideal $(\mathcal{F}) \subset R$ with $\mathcal{F} = \{f_1, \ldots, f_s\}$, we can obtain a homogeneous ideal in S either by considering the ideal $(\mathcal{F}^h)$, obtained by considering the generating set $\mathcal{F}^h = \{f_1^h, \ldots, f_s^h\}$, or by considering the **homogenization** of $(\mathcal{F})$, denoted $(\mathcal{F})^h$, which is the ideal $(\mathcal{F})^h = (f^h \mid f \in (\mathcal{F}))$ generated by the homogenizations of *all* elements in $(\mathcal{F})$, not just the elements in $\mathcal{F}$.

In [Caminata and Gorla, 2020], it is shown that the solving degree for a system with respect to the DRL term order can often be bounded above by the regularity of the ideal $(\mathcal{F}^h)$, but this requires the ideal $(\mathcal{F}^h)$ to be in *generic coordinates*, a concept that requires the use of the notions of the *saturation* of an ideal with respect to another and the *dimension* of ideals and varieties. We first define saturations, and the related notion of a quotient ideal:

Definition 7. Let $\mathcal{R}$ be a ring. Given ideals $I, J \subset \mathcal{R}$, we define the **quotient** or **colon ideal**

$$I : J = \{r \in \mathcal{R} \mid \text{for all } s \in J, rs \in I\}$$

and the **saturation**

$$I : J^\infty = \{r \in \mathcal{R} \mid \text{for all } s \in J, \text{ there exists an } n \geq 0 \text{ such that } rs^n \in I\}.$$

When $J = (x)$ for some $x \in \mathcal{R}$, we write $I : x$ instead of $I : (x)$. Then

$$I : x = \{r \in \mathcal{R} \mid \text{for all } s \in (x), rs \in I\} = \{r \in \mathcal{R} \mid rx \in I\}.$$

Example 7. In $\mathcal{R} = \mathbb{Z}$, let $I = (4)$ and $J = (6)$. Then

$$\begin{aligned} I : J &= \{m \in \mathbb{Z} \mid \forall a \in (6), ma \in (4)\} \\ &= \{m \in \mathbb{Z} \mid \forall k \in \mathbb{Z}, 4 | m \cdot (6k)\} = (2), \end{aligned}$$

and

$$\begin{aligned} I : J^\infty &= \{m \in \mathbb{Z} \mid \forall a \in (6), \exists n \geq 0 \text{ s.t. } ma^n \in (4)\} \\ &= \{m \in \mathbb{Z} \mid \forall k \in \mathbb{Z}, \exists n \geq 0 \text{ s.t. } 4 | m \cdot (6k)^n\} = \mathbb{Z} \end{aligned}$$

since choosing $n = 2$ suffices for any m.

For an example with $\mathcal{R} = k[x, y, z]$, we will use the following Proposition, which is Proposition 4.4.13 in [Cox et al., 2013].

Proposition 1. *Let I and $J_1, \ldots, J_n$ be ideals in R. Then*

$$I : \left(\sum_{i=1}^{n} J_i \right) = \bigcap_{i=1}^{n} I : J_i \quad \textit{and} \quad I : \left(\sum_{i=1}^{n} J_i \right)^{\infty} = \bigcap_{i=1}^{n} I : J_i^{\infty}.$$

Example 8. In $R = k[x, y, z]$, let $I = (xy^4z, x^2z^3)$ and $J = (xz, y)$. Then

$$\begin{aligned} I : J &= (I : xz) \cap (I : y) \\ &= (y^4, xz^2) \cap (xy^3z, x^2z^3) \\ &= (xy^4z, x^2y^4z^3, xy^3z^2, x^2z^3) \\ &= (xy^4z, xy^3z^2, x^2z^3). \end{aligned}$$

Where we have used the above proposition. We compute the saturation similarly:

$$\begin{aligned} I : J^{\infty} &= (I : (xz)^{\infty}) \cap (I : y^{\infty}) \\ &= k[x, y, z] \cap (xz) = (xz) \end{aligned}$$

where $I : (xz)^{\infty} = k[x, y, z]$ because we can choose $n = 3$ in the defition of a saturation to show that $1 \in I : (xz)^{\infty}$.

In discussing ideas of dimension, we will need to use Hilbert functions:

Definition 8. Let I be an ideal in R, and consider the sets $R_{\leq s}$ of polynomials in R with degree at most s and $I_{\leq s} = I \cap R_{\leq s}$. Viewing these sets as vector spaces over k, we note that $I_{\leq s}$ is a subspace of $R_{\leq s}$ and define the **affine Hilbert function** of I to be the dimension of their quotient:

$$^{a}\operatorname{HF}_{R/I}(s) = \dim R_{\leq s}/I_{\leq s}.$$

In the projective case, we use the vector space S_s of homogeneous polynomials of degree s, together with the zero polynomial, and we define $I_s = I \cap S_s$ for a homogeneous ideal $I \subset S$.

Definition 9. Let I be a homogeneous ideal in S. The **projective Hilbert function** of I is

$$\operatorname{HF}_{S/I}(s) = \dim S_s/I_s.$$

We know state a few propositions from [Cox et al., 2013] on the behavior of these Hilbert functions. These propositions will allow us to define the dimension of a variety.

Proposition 2. *Let $I \subset R$ be a proper monomial ideal. Then $^{a}\operatorname{HF}_{R/I}(s)$ is the number of monomials of degree at most s not contained in I. If $I \subset S$ is homogeneous, then $\operatorname{HF}_{S/I}(s)$ is the number of monomials of degree exactly s not contained in I.*

Theorem 2. *For s sufficiently large, the Hilbert functions agree with polynomial functions of s in that there is some polynomial $f(s)$ such that the Hilbert function of I evaluated at s is equal to $f(s)$. We call these polynomials the Hilbert polynomials, and we denote them ${}^a\mathrm{HP}(s)$ for the affine case and $\mathrm{HP}(s)$ for the projective case.*

Remark 1. The Hilbert polynomial of an ideal can be computed from its Hilbert series, the formal power series

$$ {}^a\mathrm{HS}_{R/I}(t) := \sum_{s=0}^{\infty} {}^a\mathrm{HF}_{R/I}(s)t^s. $$

This is a corollary of the Hilbert-Serre Theorem, giving a representation of the series as a rational function (Corollary 11.10 in [Kemper, 2011].) The series can be computed via an algorithm involving Gröbner bases (Algorithm 11.8 in [Kemper, 2011]).

Proposition 3. *For an ideal $I \subset R$, we have that*

$$ {}^a\mathrm{HF}_{R/I}(s) = {}^a\mathrm{HF}_{R/\,\mathbf{in}(I)}(s) $$

where $\mathbf{in}(I)$ is taken with respect to any degree-compatible term order. Similarly, for a homogeneous $I \subset S$, we have that

$$ \mathrm{HF}_{S/I}(s) = \mathrm{HF}_{S/\,\mathbf{in}(I)}(s). $$

This means that I and $\mathbf{in}(I)$ also share Hilbert series and Hilbert polynomials.

Definition 10. Given an affine variety V, we define $\dim V$, the **dimension** of V, to be the degree of the affine Hilbert polynomial of $\mathbf{I}(V)$, where $\mathbf{I}(V)$ is the ideal of polynomials that vanish on V. If V is a projective variety, we instead use the degree of the projective Hilbert polynomial of $\mathbf{I}(V)$.

Example 9. Consider the affine variety V consisting of the lines $y = x$ and $x = 0$ in $\mathbb{R}^2$. Then $\mathbf{I}(V) = (x(x-y)) \subset R = \mathbb{R}[x,y]$. Using the degree reverse lexicographic (DRL) term order, we see that $\{x^2 - xy\}$ is already a Gröbner basis, and we have that $\mathbf{in}(\mathbf{I}(V)) = (x^2)$. Then the only monomials not in $\mathbf{in}(\mathbf{I}(V))$ are those of the form y^k or xy^k for $k = 0, 1, \ldots$, meaning there are $2s+1$ monomials of degree at most s not contained in $\mathbf{in}(\mathbf{I}(V))$. Therefore

$$ {}^a\mathrm{HF}_{R/\,\mathbf{I}(V)}(s) = {}^a\mathrm{HF}_{R/\,\mathbf{in}(\mathbf{I}(V))}(s) = 2s+1, $$

and because this is already a polynomial in s, we have that this is also the affine Hilbert polynomial. It has degree 1, so $\dim V = 1$ as an affine variety.

However, because the lines making up V are lines through the origin, we can also consider V as the projective variety $\{(1:1),(0:1)\} \subset \mathbb{P}^1(\mathbb{R})$ and get the same ideal $\mathbf{I}(V)$ back, but this time we will think of it as being $\mathbf{I}(V) = (x(x-h)) \subset S = \mathbb{R}[x,h]$. As before, we have that $\mathbf{in}(\mathbf{I}(V)) = (x^2)$ with respect to the DRL order, but now to compute the projective Hilbert function,

we are interested in those monomials of degree exactly s not contained in $\mathbf{in}(\mathbf{I}(V))$. For $s = 0$, there is the monomial 1, and for $s > 0$, there are the monomials y^s and xy^{s-1}, meaning

$$\mathrm{HF}_{S/\,\mathbf{I}(V)}(s) = \mathrm{HF}_{S/\,\mathbf{in}(\mathbf{I}(V))} = \begin{cases} 1 & s = 0 \\ 2 & s > 0. \end{cases}$$

Therefore $\mathrm{HP}_{S/\,\mathbf{I}(V)}(s) = 2$ is a degree zero polynomial, and so $\dim V = 0$ as a projective variety. In this case, viewing a set as a projective variety rather than an affine variety decreased its dimension by 1, and the following theorem ([Cox et al., 2013] Theorem 12 of section 9.3) says that this is always the case.

Theorem 3. *Let $I \subset S$ be homogeneous. Then for $s \geq 1$, we have that*

$$\mathrm{HF}_{S/I}(s) = {}^a\mathrm{HF}_{S/I}(s) - {}^a\mathrm{HF}_{S/I}(s-1).$$

Therefore for a projective variety $V \subset \mathbb{P}^n(k)$, the affine variety $C_V \subset k^{n+1}$ (called its affine cone) with the same associated ideal I has $\dim C_V = \dim V + 1$.

In the second part of Example 9, we had the projective variety $V = \{(1:1),(0:1)\} \subset \mathbb{P}^1(\mathbb{R})$, and saw that the associated ideal was $\mathbf{I}(V) = (x^2 - xh)$, the same ideal we got by considering V as an affine variety (which is denoted C_V in the language of Theorem 3). We said that ${}^a\mathrm{HF}_{S/\,\mathbf{I}(V)}(s)$ was $2s + 1$, and indeed, we see that for $s \geq 1$, we have that

$${}^a\mathrm{HF}_{S/\,\mathbf{I}(V)}(s) - {}^a\mathrm{HF}_{S/\,\mathbf{I}(V)}(s-1) = 2s + 1 - (2(s-1)+1) = 2 = \mathrm{HF}_{S/\,\mathbf{I}(V)}(s).$$

We also see in this example that this finite projective variety had dimension 0. Proposition 6 of section 9.4 in [Cox et al., 2013] asserts that nonempty finite varieties always have dimension 0, but the proof is only given in the affine case. We give details for the projective version below, but first state another proposition from [Cox et al., 2013].

Proposition 4. *Let V and W be nonempty varieties, either both projective or both affine, then*

$$\dim(V \cup W) = \max\{\dim V, \dim W\},$$

where the notion of dimension is affine if $V, W \subset k^n$ or projective if $V, W \subset \mathbb{P}^n(k)$.

Proposition 5. *If V is a nonempty projective variety with $|V| < \infty$, then $\dim V = 0$.*

Proof. If V consists of finitely many points, then

$$V = \{p_1, \ldots, p_r\} = V_1 \cup \cdots \cup V_r$$

where V_j is the projective variety $\{p_j\}$. By the above Proposition 4, it suffices to show that $\dim V_j = 0$ for all $1 \leq j \leq r$. Therefore let $W = \{p\}$ be a projective variety consisting of exactly one point, and suppose p has homogeneous coordinates $p = (a_1 : \cdots : a_n : a_{n+1})$. Then at least one a_i is nonzero, and without loss of generality, we will assume that $a_{n+1} \neq 0$. (If this is not the case, there is some $1 \leq j \leq n$ for which a_j is nonzero, and we will later consider the DRL term ordering with variables ordered so that $x_j < x_k$ for all $k \neq j$—assuming $a_{n+1} \neq 0$ allows us to use the normal DRL ordering). Then also

$$p = \left(\frac{a_1}{a_{n+1}} : \cdots : \frac{a_n}{a_{n+1}} : 1 \right)$$

and we have that $f \in k[x_1, \ldots, x_n, h]$ therefore vanishes on all homogeneous coordinates of p if and only if $x_i - (a_i/a_{n+1})h = 0$ for all $1 \leq i \leq n$. Therefore

$$\mathbf{I}(W) = \left(x_1 - \frac{a_1}{a_{n+1}} h, \ldots, x_n - \frac{a_n}{a_{n+1}} h \right).$$

The polynomials above already form a Gröbner basis for $\mathbf{I}(W)$, and so we have that the initial ideal is $\mathbf{in}(\mathbf{I}(W)) = (x_1, \ldots, x_n)$. To compute the projective Hilbert function of $\mathbf{I}(W)$, we therefore need to determine the number of monomials of degree exactly s not contained in $(x_1, \ldots, x_n)$. But the only such monomial is h^s, meaning $\mathrm{HF}_{S/\mathbf{I}(W)}(s) = 1$. Since this is already a polynomial, we see that $\mathbf{I}(W)$ has a projective Hilbert polynomial of degree 0, meaning $\dim W = 0$. Therefore any variety that is the union of finitely many points has dimension zero as well. □

We now consider another way of defining the dimension of a ring, called the Krull dimension:

Definition 11. Let $\mathcal{R}$ be a ring and let $\operatorname{Spec} \mathcal{R}$ be its collection of prime ideals. We say a **chain** $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ in $\operatorname{Spec} \mathcal{R}$ has **length** n (the number of strict inclusions), and we define the **Krull dimension** of $\mathcal{R}$ to be

$$\dim \mathcal{R} = \sup\{ \text{ length}(C) \mid C \text{ is a chain in } \operatorname{Spec} \mathcal{R} \}.$$

Note that if we have an ideal $I \subset R$, we now have two notions of the dimension of a quotient R/I. We can look at the degree of the affine Hilbert polynomial, or we can consider the Krull dimension. For the next example, recall that a chain of prime ideals in R/I corresponds to a chain of prime ideals in R all containing the ideal I.

Example 10. We continue Example 9, in which $\mathbf{I}(V) = (x^2 - xy)$. This ideal is not prime, so any chain of prime ideals containing $\mathbf{I}(V)$ cannot begin with the ideal $\mathbf{I}(V)$ itself. Suppose P is a prime ideal containing $\mathbf{I}(V)$. Then $x^2 - xy \in \mathbf{I}(V) \subset P$, which means either $x \in P$ or $x - y \in P$. Then P must contain either the prime ideal (x) or the prime ideal $(x - y)$, so any chain of primes containing

$\mathbf{I}(V)$ and maximal in length must start either with (x) or with $(x-y)$. But the only prime ideal containing either (x) or $(x-y)$ is the maximal ideal (x,y), and so the only possible chains are

$$(x) \subset (x,y) \quad \text{or} \quad (x-y) \subset (x,y),$$

meaning the Krull dimension of R/I is 1. This is the same as the degree of the affine Hilbert polynomial of I, and this is not a coincidence, as the next Theorem from [Kemper, 2011] asserts.

Theorem 4. *Let $I \subset R$ be an ideal. Then the Krull dimension of R/I is the degree of the affine Hilbert polynomial.*

With this discussion of dimension out of the way, we can now say what it means for a homogeneous ideal I (in either of the rings R or S over an infinite field k) to be in *generic coordinates*. For a homogeneous ideal $I \subset R$ or $I \subset S$, we define I^{sat} to be the saturation $I : \mathfrak{m}^\infty$ with respect to the irrelevant maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n) \subset R$, or $\mathfrak{m} = (x_1, \ldots, x_n, h) \subset S$ depending on which ring I is contained in. Although we will be considering homogeneous ideals here, when we refer to the dimension $\dim(R/I)$, we mean the Krull dimension, which agrees with the degree of the *affine* Hilbert polynomial, rather than the projective Hilbert polynomial. We have the following definitions for genericity and generic coordinates from [Bayer and Stillman, 1987].

Definition 12. Let $I \subset R$ be a homogeneous ideal. We say that an element $g \in R$ is **generic** for I if either

(1) $\dim(R/I) = 0$, or
(2) g is not a zero-divisor on R/I^{sat}.

Further, recall that by R_d we mean the set of degree d elements in R, and for $j > 0$ define the set $U_j(I) \subset R_1^j$ by

$$U_j(I) = \{(g_1, \ldots, g_j) \in R_1^j \mid g_i \text{ is generic for } I + (g_1, \ldots, g_{i-1}), 1 \leq i \leq j\},$$

and we say that I is in **generic coordinates** if $(x_n, \ldots, x_{n-r+1}) \in U_r$ for $r = \dim(R/I)$.

It is shown in [Caminata and Gorla, 2020] that for the DRL order and a system $\mathcal{F}$ for which the ideal $(\mathcal{F}^h) \subset S$ is in generic coordinates, we have that $\text{sd}_{1,DRL}(\mathcal{F}) \leq \text{reg}(\mathcal{F}^h)$. The proof of this result uses the following definition, which differs slightly from the one given above:

Definition 13. Let $I \subset S = k[x_1, \ldots, x_n, h]$ be a homogeneous ideal with finite projective zero locus $|\mathcal{Z}_+(I)| < \infty$. Then I is in **generic coordinates** if either

(i) $|\mathcal{Z}_+(I)| = 0$, or
(ii) h is not a zero-divisor on S/I^{sat}.

Since the proof of the result that $\mathrm{sd}_{1,DRL}(\mathcal{F}) \leq \mathrm{reg}(\mathcal{F}^h)$ uses the results in [Bayer and Stillman, 1987], we will show that the definition in [Caminata and Gorla, 2020] is just a special case of that in [Bayer and Stillman, 1987].

Proposition 6. *Let $I \subset S$ be a homogeneous ideal in generic coordinates in the sense of Definition 13 from [Caminata and Gorla, 2020]. Then I is also in generic coordinates in the sense of Definition 12 from [Bayer and Stillman, 1987].*

Proof. Assume the hypotheses of the claim, and also assume I is a proper ideal (if not, $\dim(S/I) = \dim(S/S) = 0$ and so I is in generic coordinates). There are two cases to consider. In the first, suppose $|\mathcal{Z}_+(I)| = 0$. Because I is a homogeneous ideal, the polynomials in I all vanish at $(0, 0, \ldots, 0)$, so $(0, 0, \ldots, 0) \in \mathcal{Z}(I)$. If there is any other point in $p \in \mathcal{Z}(I)$, then any function in I vanishes along the line in k^{n+1} through $(0, 0, \ldots, 0)$ and p, since each point on the line has the same homogeneous coordinates as p. But the point with these homogeneous coordinates is then in $\mathcal{Z}_+(I) = \emptyset$, which cannot be the case. Therefore $\mathcal{Z}(I) = \{(0, 0, \ldots, 0)\}$, and so in particular, $|\mathcal{Z}(I)| < \infty$. Then by the affine version of Proposition 5 (the proof of which is given in [Cox et al., 2013]), the degree of the affine Hilbert polynomial is 0. By Theorem 4, this means $\dim(S/I) = 0$, and so I is in generic coordinates in the sense of [Bayer and Stillman, 1987] since it meets (1) of Definition 12.

Now for the second case, assume that h is not a zero-divisor on S/I^{sat}. Then in the language of Definition 12, this means that h is generic for I. Since $h \in S_1$, this in turn means that $h \in U_1(I)$. Because I is in generic coordinates in the sense of Definition 13, we have that $|\mathcal{Z}_+(I)| < \infty$. Since this projective variety is finite, Proposition 5 implies that the degree of the projective Hilbert polynomial is 0. By Theorem 2, the degree of the projective Hilbert polynomial is one less than that of the affine Hilbert polynomial, and therefore the Krull dimension $\dim(S/I)$ is equal to 1 by Theorem 3. Then because $h \in U_1(I)$ and h is the smallest variable (with respect to the DRL ordering) in the polynomial ring $S = k[x_1, \ldots, x_n, h]$, we have that I is in generic coordinates in the sense of Definition 12 from [Bayer and Stillman, 1987]. □

In addition, the argument used in [Caminata and Gorla, 2020] uses that for an ideal J in generic coordinates and over a field k of characteristic zero, the equalities $\mathrm{max.\,GB.\,deg}_{DRL}(J) = \mathrm{reg}(\mathbf{in}_{DRL}(J)) = \mathrm{reg}(J)$ hold, both of which come from [Bayer and Stillman, 1987]. Additionally, they note that in characteristic p, $\mathrm{max.\,GB.\,deg}_{DRL}(J) \leq \mathrm{reg}(\mathbf{in}_{DRL}(J))$ still holds. We give an argument for this inequality (in arbitrary characteristic) to show a weaker version of the result that $\mathrm{sd}_{1,DRL}(\mathcal{F}) \leq \mathrm{reg}(\mathcal{F}^h)$ without any genericity assumptions.

Proposition 7. *Let $\mathcal{F} = \{f_1, \ldots, f_s\} \subset R$. Then $\mathrm{sd}_{1,DRL}(\mathcal{F}) \leq \mathrm{reg}(\mathbf{in}_{DRL}(\mathcal{F}^h))$.*

Proof. We follow the proof of given for the stronger result in [Caminata and Gorla, 2020], noting that the genericity of $(\mathcal{F}^h)$ is not needed for the result of Theorem 7 that $\mathrm{sd}_{1,DRL}(\mathcal{F}) \leq \mathrm{max.\,GB.\,deg}_{DRL}(\mathcal{F}^h)$, so it does indeed suffice to show that $\mathrm{max.\,GB.\,deg}(J) \leq \mathrm{reg}(\mathbf{in}(J))$ for a

proper homogeneous ideal $J \subset S$, and this can be shown for a more general degree-compatible term order. Let τ be such a term order. Let $\mathcal{G} = \{g_1, \ldots, g_r\}$ be a reduced Gröbner basis of J, with degrees $d_1, \ldots, d_r$, so that $\text{max. GB. deg}_\tau(J) = \max\{d_1, \ldots, d_r\}$. Since $\mathcal{G}$ is a reduced Gröbner basis, the leading monomials $m_1, \ldots, m_r$ of its elements minimally generate $\mathbf{in}_\tau(J)$, and so we can define the map

$$\varphi_0 : \bigoplus_{j=1}^{r} S(-d_j) \to J$$

by sending the ith generator to the monomial m_i. Because J is proper, the degrees satisfy $d_j \geq 1$, and so this map shows us that all the Betti numbers β_{0,d_j} are nonzero. Therefore the regularity is at least

$$\text{reg}(\mathbf{in}_\tau(J)) = \max\{j - i : \beta_{i,j} \neq 0\} \geq \max\{d_j - 0 : 1 \leq j \leq r\} = \text{max. GB. deg}_\tau(J).$$

Choosing $J = \mathcal{F}^h$ gives us a proper homogeneous ideal and taking $\tau = DRL$ gives us $\text{sd}_{1,DRL}(\mathcal{F}) \leq \text{max. GB. deg}_{DRL}(\mathcal{F}^h) \leq \text{reg}(\mathbf{in}_{DRL}(F^h))$, as claimed. □

So summing up, we have that

$$\text{sd}_{2,DRL}(\mathcal{F}) \leq \text{sd}_{1,DRL}(\mathcal{F}) \leq \text{reg}(\mathbf{in}_{DRL}(\mathcal{F}^h))$$

for any system $\mathcal{F}$, and if $(\mathcal{F}^h)$ is known or assumed to be in generic coordinates, then we have the stronger result that

$$\text{sd}_{2,DRL}(\mathcal{F}) \leq \text{sd}_{1,DRL}(\mathcal{F}) \leq \text{reg}(\mathbf{in}_{DRL}(\mathcal{F}^h)) = \text{reg}(\mathcal{F}^h)$$

since for a homogeneous ideal J in generic coordinates, we have that $\text{reg}(J) = \text{reg}(\mathbf{in}_{DRL}(J))$, whereas without genericity assumptions we only have that $\text{reg}(J) \leq \text{reg}(\mathbf{in}_{DRL}(J))$.

Example 11. We continue Example 4, where we showed that it is possible to have the strict inequality $\text{sd}_{2,\tau}(\mathcal{F}) < \text{sd}_{1,\tau}(\mathcal{F})$ using the system $\mathcal{F} = \{y^2, yz + x\}$ with $\tau = DRL$. We can also use this example to show that the genericity condition is indeed needed to have $\text{sd}_{1,\tau}(\mathcal{F}) \leq \text{reg}(\mathcal{F}^h)$. The ideal $(\mathcal{F}^h)$ has dimension 2, so checking genericity means checking that h is generic for $(\mathcal{F}^h)$ and z is generic for $(\mathcal{F}^h) + (h)$. To check that h is generic for $(\mathcal{F}^h)$, we first compute the saturation $(\mathcal{F}^h) : \mathfrak{m}^\infty = (\mathcal{F}^h)$, and then note that neither h nor xy is an element of $\mathcal{F}^h$, but

$$hxy = y^2z + hxy - y^2z = y(yz + xh) - z(y^2) = yf_2^h - zf_1^h \in (\mathcal{F}^h).$$

Therefore h is a zero-divisor on $S/(\mathcal{F}^h)$, and so $(\mathcal{F}^h)$ is not in generic coordinates in the sense of

either definition. For the regularity, we have that $(\mathcal{F}^h) = (y^2, yz + xh)$ with minimal free resolution

$$0 \longrightarrow S(-4) \xrightarrow{\varphi_1} S(-2)^2 \xrightarrow{\varphi_0} (\mathcal{F}^h) \longrightarrow 0$$

given by the maps

$$\varphi_0 = \begin{pmatrix} y^2 & yz + xh \end{pmatrix} \quad \text{and} \quad \varphi_1 = \begin{pmatrix} yz + xh \\ -y^2 \end{pmatrix}.$$

The nonzero Betti numbers are $\beta_{0,2} = 2$ and $\beta_{1,4} = 1$, and so $\operatorname{reg}(\mathcal{F}^h) = 3$. We showed earlier that $\operatorname{sd}_{1,DRL}(\mathcal{F}) > 3$, and so we have an example for which $\operatorname{sd}_{1,DRL}(\mathcal{F}) \not\leq \operatorname{reg}(\mathcal{F}^h)$.

In Example 4, it was shown that $\operatorname{sd}_{2,DRL}(\mathcal{F}) = 3$, which is the regularity of $(\mathcal{F}^h)$. In general, however, the genericity assumption is also needed to show the $\operatorname{sd}_{2,DRL}(\mathcal{F}) \leq \operatorname{reg}(\mathcal{F}^h)$ version of the inequality for Algorithm II. We show this with the following Example, modifying the above slightly.

Example 12. Consider now the system $\mathcal{F} = \{y^2 + 1, yz + xw\} \subset R = k[x, y, z, w]$. The ideal $(\mathcal{F}^h) = (y^2 + h^2, yz + xw)$ now has dimension 3. First we note that $(\mathcal{F}^h) : \mathfrak{m}^\infty = (\mathcal{F}^h)$, as previously, but this time h is not a zero-divisor in $S/(\mathcal{F}^h)$ (this can be checked by confirming that h is not in any of the associated primes of $(\mathcal{F}^h)$), so h is generic for $(\mathcal{F}^h)$. However, w is not generic for $(\mathcal{F}^h) + (h)$, since $\big((\mathcal{F}^h) + (h)\big) : \mathfrak{m}^\infty = (\mathcal{F}^h) + (h)$ and

$$\begin{aligned} wxy &= y^2z + wxy - y^2z - zh^2 + zh^2 \\ &= y(yz + wx) - z(y^2 + h^2) - zh(h) \\ &= yf_2^h - zf_1^h - zh(h) \in (\mathcal{F}^h) + (h) \end{aligned}$$

with $w, xy \notin (\mathcal{F}^h) + (h)$. Once again, $(\mathcal{F}^h)$ is not in generic coordinates, and we have an almost identical minimal free resolution:

$$0 \longrightarrow S(-4) \xrightarrow{\varphi_1} S(-2)^2 \xrightarrow{\varphi_0} (\mathcal{F}^h) \longrightarrow 0,$$

the difference being in the maps

$$\varphi_0 = \begin{pmatrix} y^2 + h^2 & yz + xh \end{pmatrix} \quad \text{and} \quad \varphi_1 = \begin{pmatrix} yz + xh \\ -y^2 - h^2 \end{pmatrix}.$$

This means $\operatorname{reg}(\mathcal{F}^h)$ is still 3, but what changes in this example is that we have

$$\operatorname{sd}_{2,DRL}(\mathcal{F}) = \operatorname{sd}_{1,DRL}(\mathcal{F}) = 4 > \operatorname{reg}(\mathcal{F}^h).$$

Hence being in generic coordinates is still a requirement for the inequality to hold.

We have shown that Algorithms I and II are indeed different, but with the notion of generic coordinates, we can ask whether they are still "generically" the same. That is, do we have that $\mathrm{sd}_{1,\tau}(\mathcal{F}) = \mathrm{sd}_{2,\tau}(\mathcal{F})$ for a system $\mathcal{F}$ for which $(\mathcal{F}^h)$ is in generic coordinates? To see that the answer is *no*, we use the following example from [Minko, 2021].

Example 13. Take the polynomials in $\mathcal{F}_7[x, y, z]$ defined by

$$f_1 = x^5 + y^5 + z^5 - 1, \quad f_2 = x^3 + y^3 + z^2 - 1, \quad f_3 = y^6 - 1, \quad f_4 = z^6 - 1,$$

and take $\mathcal{F}$ to consist of all possible products of these polynomials with indices in (not strictly) ascending order, together with the *field equations* $f_x = x^7 - x$, $f_y = y^7 - y$, $f_z = z^7 - z$. That is, we are considering the system

$$\begin{aligned}\mathcal{F} &= \left\{ \prod_{j=1}^{3} f_{i_j} : 1 \leq i_1 \leq i_2 \leq i_3 \leq 4 \right\} \cup \{f_x, f_y, f_z\} \\ &= \{f_1 f_1 f_1,\ f_1 f_1 f_2,\ f_1 f_1 f_3,\ \ldots,\ f_3 f_4 f_4,\ f_4 f_4 f_4,\ f_x,\ f_y,\ f_z\}.\end{aligned}$$

Then one can compute (using e.g. Sage or Macaulay2) that $\mathrm{sd}_{2,DRL}(\mathcal{F}) = 18 < 22 = \mathrm{sd}_{1,DRL}(\mathcal{F})$.[1] We can also check that the system is indeed in generic coordinates, and that $\mathrm{reg}(\mathcal{F}^h) = 22$ bounds both solving degrees above, as we would expect. So we see that even with a general choice of coordinates, Algorithms I and II may produce different results for the solving degree of the system.

3 Further definitions of genericity

We have already seen two definitions of what it means to be "generic," one from [Bayer and Stillman, 1987], and one from [Caminata and Gorla, 2020]. However, more are used in practice. In fact, an earlier version of the [Caminata and Gorla, 2020] paper used a different definition of genericity, which involves the idea of the *generic initial ideal*. Consider a homogeneous ideal I in a polynomial ring of n variables, $S = k[x_1, \ldots, x_n]$. Then an element $g \in GL_n(k)$ with entries g_{ij} acts on I by the mapping $x_i \mapsto \sum_{j=1}^{n} g_{ij} x_j$.

Example 14. Let $I \subset k[x, y]$ be given by $I = (x^2, y^2)$. Then the matrix

$$g = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$$

[1] In [Minko, 2021], d_{solve}, the notion of solving degree considered, is said to be 24, but this is based on the way the computer algebra system Magma computes the *maximum step degree* of a system in its F5 algorithm, which is another Gröbner basis algorithm distinct from the two presented here.

yields the ideal gI, generated by

$$gI = \left((2x-y)^2 + (x)^2\right) = (4x^2 - 4xy + y^2, x^2) = (x^2, 4xy - y^2).$$

Note that $\mathbf{in}_{DRL}(I) = (x^2, y^2)$, but $\mathbf{in}_{DRL}(gI) = (y^3, x^2, xy)$.

We will now use this action of $GL_n(k)$ on an ideal $I \subset S$ to define another version of genericity, as well as what it means for an ideal to be *Borel-fixed*.

Definition 14. The **Borel subgroup** $B = \{g \in GL_n(k) : g_{ij} = 0 \text{ for all } j < i\}$ consists of all the upper triangular matrices, and we say that an ideal is **Borel-fixed** if $I = gI$ for all $g \in B$.

The next Definition and the subsequent Proposition give an easier way to check if an ideal is Borel-fixed, one that we will use later on.

Definition 15. An **elementary move** e_k for $1 \leq k \leq n-1$ on a monomial $x_1^{m_1} \cdots x_n^{m_n}$ is defined by

$$e_k(x_1^{m_1} \cdots x_n^{m_n}) = \begin{cases} x_1^{m_1} \cdots x_k^{m_k+1} x_{k+1}^{m_{k+1}-1} \cdot x_n^{m_n} & m_{k+1} - 1 \geq 0 \\ 0 & m_{k+1} - 1 < 0. \end{cases}$$

Proposition 8. *[Green et al., 1998] An ideal $I \subset S$ is Borel-fixed if and only if for all monomials $m \in I$, $e_k(m) \in I$ for all $1 \leq k \leq n-1$.*

We can think of I as being the identity of $GL_n(k)$ acting on I, and can define an equivalence relation on $GL_n(k)$ by $g_1 \sim g_2$ if and only if $\mathbf{in}_{DRL}(g_1 I) = \mathbf{in}_{DRL}(g_2 I)$. A theorem of Galligo [Galligo, 1974] shows that the number of equivalence classes is finite, and that one of them is a Zariski open set in $GL_n(k)$ and that $\mathbf{in}_{DRL}(gI)$ is Borel-fixed for any g in this equivalence class (see also [Miller and Sturmfels, 2005]). We define the **generic initial ideal** of I, denoted $\mathbf{gin}_\tau(I)$ for a term order τ by $\mathbf{gin}_\tau(I) = \mathbf{in}_\tau(gI)$ for any g in this Zariski open equivalence class of $GL_n(k)$.

Definition 16. Let $I \subset S = k[x_1, \ldots, x_n]$ be a homogeneous ideal. Then I is said to be in **generic coordinates** if and only if $\mathbf{in}_{DRL}(I) = \mathbf{gin}_{DRL}(I)$, that is, if the identity matrix is in the Zariski open equivalence class guaranteed to exist by Galligo's Theorem.

In the example above, it turns out that there are exactly two equivalences classes, with the one yielding (y^3, x^2, xy) being the Zariski open one. Therefore (x^2, y^2) is not in generic coordinates. Bayer and Stillman show in [Bayer and Stillman, 1987] that this Zariski open equivalence class is contained in the open set $V = \{g \in GL_n(k) : (x_n, \ldots, x_{n-r+1}) \in U_r(gI)\}$ using the notation of Definition 12. This means that if I is in generic coordinates in the sense of Definition 16, then the identity matrix is in this set V, meaning $(x_n, \ldots, x_{n-r+1}) \in U_r(I)$ for $r = \dim(S/I)$, and we have that I is in generic coordinates in the sense of Definition 12, which in turn implies being in generic coordinates in the sense of Definition 13. The implication (12) $\implies$ (13) is strict since

Definition 13 applies only to homogeneous ideals with dimension 1 or 0, and Bayer and Stillman give the example $I = (x^3, y^5)$ to show that the implication (16) $\implies$ (12) is strict as well.

We now introduce a conjecture due to Fröberg concerning what the Hilbert series of an ideal should look like when it is sufficiently generic [Fröberg, 1985]. In the original, the conjecture uses a notion of genericity concerning the algebraic independence of the coefficients of the ideal's generators, but we will consider the version of the conjecture studied in [Pardue, 2010], which involves the idea of a "generic sequence" of polynomials:

Conjecture 1. *If k is an infinite field and $I \subset S = k[x_1, \ldots, x_n]$ is an ideal generated by a generic sequence of polynomials $f_1, \ldots, f_r$ of degrees $d_1, \ldots, d_r$, then*

$$\mathrm{HS}_{S/I}(t) = \left| \frac{\prod_{i=1}^{r}(1-t^{d_i})}{(1-t)^n} \right|.$$

Here, the absolute value bars mean truncating the series to exclude all terms after and including the first one with a negative coefficient, so for example, if we had an ideal I in $k[x, y, z]$ generated by a "generic sequence" of degrees $d_1 = 3$, $d_2 = 2$, $d_3 = 2$, and $d_4 = 2$, the conjecture asserts that

$$\begin{aligned}\mathrm{HS}_{S/I}(t) &= \left| \frac{(1-t^3)(1-t^2)^3}{(1-t)^3} \right| = \left| \frac{(1-t^3)(1-t)^3(1+t)^3}{(1-t)^3} \right| \\ &= |1 + 3t + 3t^2 - 3t^4 - 3t^5 - t^6| = 1 + 3t + 3t^2.\end{aligned}$$

We now define what is meant by a generic sequence, as it differs from the previous definitions of genericity.

Definition 17. Given a sequence of degrees $d_1, \ldots, d_r$, we may identify any given generating set $f_1, \ldots, f_r$ of homogeneous polynomials of these degrees with their coefficients. Any f_i of degree d_i (that is, $f_i \in S_{d_i}$) is a tuple of its $\binom{n+d_i-1}{d_i}$ coefficients, and so any sequence $f_1, \ldots, f_r$ is a tuple of all of the $\sum_{i=1}^{r}\binom{n+d_i-1}{d_i}$ coefficients involved. If $I = (f_1, \ldots, f_r)$, then we will denote this tuple of all $\sum_{i=1}^{r}\binom{n+d_i-1}{d_i}$ coefficients by **coeff**(I). In this way, we may put the Zariski topology on the space $\prod_{i=1}^{r} S_{d_i}$, and we will say that some property P is **generic** if it holds for all sequences $f_1, \ldots, f_r$ whose coefficients lie in a Zariski open $V \subset \prod_{i=1}^{r} S_{d_i}$. A sequence with coefficients in V is then said to be a **generic sequence**. See [Pardue, 2010].

Note that when a generic sequence is mentioned, this kind of genericity is relative to a certain generic property P. In the case of the generic sequences involved in Fröberg's conjecture, the conjecture is asserting that the property of having Hilbert series equal to the specified

$$\left| \frac{\prod_{i=1}^{r}(1-t^{d_i})}{(1-t)^n} \right|$$

is a generic property. This conjecture is open, but what is known is the following, from [Pardue, 2010],

Section 2:

Proposition 9. *For a specified sequence of degrees $d_1, \ldots, d_r$, there exist nonempty, Zariski open sets $V_1, V_2 \subset \prod_{i=1}^{r} S_{d_i}$ such that the Hilbert series is constant on V_1 and the initial ideal is constant on V_2.*

Since the Hilbert series of an ideal is equal to that of its initial ideal, having the same initial ideal means having the same Hilbert series, so in the above, we have that $V_2 \subset V_1$. Suppose $H(t)$ is the Hilbert series of any homogeneous ideal whose generators' coefficients are in V_1. Then Definition 17 says that having Hilbert series equal to $H(t)$ is a generic property. If Fröberg's conjecture holds, we would need to have

$$H(t) = \left| \frac{\prod_{i=1}^{r}(1-t^{d_i})}{(1-t)^n} \right|,$$

as we would have two nonempty Zariski open sets, V_1 on which the Hilbert series is $H(t)$, and V_1' on which the Hilbert series has the conjectured form. Since V_1 and V_1' are nonempty and Zariski open, they must therefore intersect nontrivially, and so there would be some ideal with coefficients in $V_1 \cap V_1'$ having Hilbert series of the conjectured form *and* equal to $H(t)$, meaning the two series must be equal. Hence there is known to be *some* "generic" Hilbert series $H(t)$, and Fröberg's conjecture is that it has the form given in Conjecture 1.

Remark 2. Unless otherwise specified, when we refer to a generic sequence in the sense of Definition 17, we mean a sequence satisfying the known generic property of having Hilbert series equal to $H(t)$, that is, a sequence whose coefficients are in this corresponding Zariski open set $V_1 \subset \prod_{i=1}^{r} S_{d_i}$.

The interest in Fröberg's conjecture in cryptography stems from another conjecture concerning *semi-regular sequences*. These sequences generate ideals that play particularly nicely with the F5 Gröbner basis algorithm [Faugere, 2002], and lead to the notion of the *degree of regularity* of a system, denoted d_{reg}. Bardet, Faugère, and Salvy show that for a semi-regular system in $k[x_1, \ldots, x_n]$, the F5 algorithm performs at most

$$O\left(\binom{n+d_{\text{reg}}}{n}^{\omega}\right)$$

arithmetic operations, where $2 \leq \omega < 2.39$ is the linear algebra constant [Bardet et al., 2004]. This estimate is used for analyzing the security of cryptosystems using multivariate polynomials, but rests on the assumptions that 1) the algorithm being used is F5, and 2) that the input is semi-regular. The validity of using the degree of regularity as an upper bound for the solving degree when the algorithm in use is not F5 has been the subject of some recent work (see for example [Caminata and Gorla, 2023] and [Minko, 2021]), and it is known that the inequality can fail. For instance, in the system $\mathcal{F}$ from Example 13, it was shown that $\text{sd}_1(\mathcal{F}) = 22$ and $\text{sd}_2(\mathcal{F}) = 18$, whereas one can compute that $d_{\text{reg}}(\mathcal{F}) = 15$, failing to bound either notion of solving degree.

If the algorithm used is F5, then Fröberg's conjecture enters the picture in addressing the second assumption that the input is semi-regular: Pardue shows in [Pardue, 2010] that Fröberg's conjecture is equivalent to the following:

Conjecture 2. *If k is an infinite field and $I \subset S = k[x_1, \ldots, x_n]$ is an ideal generated by a generic sequence of polynomials $f_1, \ldots, f_r$ of degrees $d_1, \ldots, d_r$, then $f_1, \ldots, f_r$ is a semi-regular sequence.*

Hence if Fröberg's conjectures holds (and it is known to hold for several classes of ideals—see [Trung, 2019]), the F5 algorithm performs very efficiently on a *generic sequence* of polynomials, that is, on a sequence of polynomials whose coefficients come from a Zariski open set in $\prod_{i=1}^{r} S_{d_i}$. With an infinite field k, this means that if the coefficients are "random," we should expect F5 to perform quite well. This is the concept of genericity in Definition 17, and (if Fröberg's conjecture is true) it gives us good results about the complexity of at least one Gröbner basis algorithm. For an example of this being used in practice, see [Thomae and Wolf, 2012], where Thomae and Wolf make use of the semi-regularity assumption and the associated complexity result in their analysis of the Unbalanced Oil and Vinegar public key signature scheme.

The results from Definition 17 are useful, but our other genericity definitions are slightly easier to work with, so it would be nice if one of them would imply Definition 17. Unfortunately, we can show that none of them imply Definition 17 with the following example:

Example 15. We consider two different sequences of polynomials of degrees $d_1 = 3$, $d_2 = 2$, $d_3 = 2$, and $d_4 = 2$, both generic in the sense of Definition 16. We will show that they have different Hilbert functions, meaning at least one of their Hilbert series is not equal to $H(t)$, the generic Hilbert series of Proposition 9. Define the ideals I and J by $I = (y^3, x^2, xy)$ and $J = (xz^2, x^2, xy)$. Recall that $\mathrm{HF}_{S/I}(s)$ and $\mathrm{HF}_{S/J}(s)$ are the number of degree s monomials not contained in I and J, respectively. Thus to show they have different Hilbert series, it suffices to show that their Hilbert functions differ at $s = 4$. The ideal $I = (y^3, x^2, xy)$ contains powers of x and y of degrees greater than or equal to 3 and the cross term xy, so I contains all degree monomials in x and y of degrees greater than or equal to 3. Hence any monomials not in I involve z, and must have a power of z at least 2, as otherwise the monomial would be z times a degree 3 monomial in x and y, which would be in I. Hence there are 4 monomials of degree 4 not in I, namely y^2z^2, xz^3, yz^3, and z^4. For $J = (xz^2, x^2, xy)$, we see that any monomial in J must be divisible by x. Since $x^2 \in J$, so is any degree 4 monomial divisible by x^2, and if a degree 4 monomial is divisible by at most x, then it is xm where m is a monomial of degree 3 in y and z. Hence m is divisible by z^2 or y, so xm is divisible by xz^2 or xy and is therefore in J. Hence the degree 4 monomials not in J are exactly the degree 4 monomials that do not involve x, of which there are 5: y^4, y^3z, y^2z^2, yz^3, and z^4. Hence we have that

$$\mathrm{HF}_{S/I}(4) = 4 \neq 5 = \mathrm{HF}_{S/J}(4),$$

so I and J do not have the same Hilbert series, and therefore at least one of them is not equal to the

generic series $H(t)$. Hence I or J does not meet Definition 17. However, a Macaulay2 computation shows that

$$\mathbf{gin}\, I = (y^3, x^2, xy) = I = \mathbf{in}\, I \quad \text{and} \quad \mathbf{gin}\, J = (xz^2, x^2, xy) = J = \mathbf{in}\, J,$$

meaning I and J are both generic in the sense of Definition 16. Hence Definition 16 does not imply Definition 17.

Now because Definition 16 implies Definitions 12 and 13, we cannot have that either of these imply Definition 17. Hence even if we assume that some system is "generic" in the sense of any of Definitions 12-16, we may not have access to the complexity bounds given by Definition 17. The next question is whether Definition 17 is strictly stronger than the others. That is, if we take an ideal $I = (f_1, \ldots, f_r)$ where the generators have degrees $d_1, \ldots, d_r$ and we assume that the coefficient tuple $\mathbf{coeff}(I)$ belongs to the open V_1 on which the Hilbert function is constant, then is it the case that $\mathbf{in}(I) = \mathbf{gin}(I)$?

Example 16. Take $I = (x^2, y^2, z^2) \subset k[x, y, z]$. It is known that Fröberg's conjecture holds in this context (with $S = k[x, y, z]$ a polynomial ring of three variables [Trung, 2019]), so if $\mathbf{coeff}(I) \in V_1$, then we have that

$$HS_{S/I}(t) = \left| \frac{(1-t^2)^3}{(1-t)^3} \right| = |(1+t)^3| = 1 + 3t + 3t^2 + t^3.$$

Indeed, I does have the required Hilbert series, so it is possible that

$$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) = \mathbf{coeff}\, I \in V_1$$

and I is therefore generic in the sense of Definition 17. However, I is certainly not generic in the sense of Definition 16, because $\mathbf{in}(I) = I$ and I cannot be the generic initial ideal because it is not Borel-fixed—for example, $z^2 \in I$ but the elementary move $e_2(z^2) = yz \notin I$.

Question 1. The difficulty with the above example is that it is hard to say whether $\mathbf{coeff}(I) \in V_1$ or not. Is there a simpler characterization for when a system has its coefficients in the open set V_1 on which Hilbert series are constnt?

Question 2. Is it true that Definition 17 implies the others? The authors of [Bigdeli et al., 2021] seem to suggest that being generated by a "generic sequence" (Definition 17) implies being "in generic coordinates" (Definition 16—they reference an earlier version of [Caminata and Gorla, 2020] for this defintion).

References

[Atiyah and MacDonald, 1969] Atiyah, M. and MacDonald, I. (1969). *Introduction to Commutative Algebra*. Addison-Wesley.

[Bardet et al., 2004] Bardet, M., Faugere, J.-C., and Salvy, B. (2004). On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74.

[Bayer and Stillman, 1987] Bayer, D. and Stillman, M. (1987). A criterion for detecting m-regularity. *Inventiones mathematicae*, 87(1):1–11.

[Bigdeli et al., 2021] Bigdeli, M., De Negri, E., Dizdarevic, M. M., Gorla, E., Minko, R., and Tsakou, S. (2021). Semi-regular sequences and other random systems of equations. In *Women in Numbers Europe III: Research Directions in Number Theory*, pages 75–114. Springer.

[Caminata and Gorla, 2020] Caminata, A. and Gorla, E. (2020). Solving multivariate polynomial systems and an invariant from commutative algebra. In *International Workshop on the Arithmetic of Finite Fields*, pages 3–36. Springer.

[Caminata and Gorla, 2023] Caminata, A. and Gorla, E. (2023). Solving degree, last fall degree, and related invariants. *Journal of Symbolic Computation*, 114:322–335.

[Cox et al., 2013] Cox, D., Little, J., and OShea, D. (2013). *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media.

[Eisenbud, 1995] Eisenbud, D. (1995). *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer-Verlag.

[Eisenbud, 2005] Eisenbud, D. (2005). *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, volume 229. Springer.

[Faugere, 2002] Faugere, J. C. (2002). A new efficient algorithm for computing gröbner bases without reduction to zero (f 5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83.

[Faugere et al., 1993] Faugere, J.-C., Gianni, P., Lazard, D., and Mora, T. (1993). Efficient computation of zero-dimensional gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344.

[Fröberg, 1985] Fröberg, R. (1985). An inequality for hilbert series of graded algebras. *Mathematica Scandinavica*, 56(2):117–144.

[Galligo, 1974] Galligo, A. (1974). À propos du théorème de-préparation de weierstrass, fonctions de plusieurs variables complexes (sém. françois norguet, octobre 1970–décembre 1973; à la mémoire d'andré martineau).

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

[Green et al., 1998] Green, M. L. et al. (1998). Generic initial ideals. *Six lectures on commutative algebra*, 166:119–185.

[Kemper, 2011] Kemper, G. (2011). *A course in commutative algebra*, volume 1. Springer.

[Miller and Sturmfels, 2005] Miller, E. and Sturmfels, B. (2005). *Combinatorial commutative algebra*, volume 227. Springer.

[Minko, 2021] Minko, R. (2021). *Security assumptions in post-quantum cryptography*. PhD thesis, University of Oxford.

[Pardue, 2010] Pardue, K. (2010). Generic sequences of polynomials. *Journal of Algebra*, 324(4):579–590.

[Stein et al., 2022] Stein, W. et al. (2022). *Sage Mathematics Software (Version 9.6)*. The Sage Development Team. `http://www.sagemath.org`.

[Thomae and Wolf, 2012] Thomae, E. and Wolf, C. (2012). Solving underdetermined systems of multivariate quadratic equations revisited. In *International Workshop on Public Key Cryptography*, pages 156–171. Springer.

[Trung, 2019] Trung, V. D. (2019). The initial ideal of generic sequences and fröberg's conjecture. *Journal of Algebra*, 524:79–96.