Genericity Definitions

Ben Clingenpeel

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 $\mathfrak{m} = (x_1, \dots, x_n) \subset R$, or $\mathfrak{m} = (x_1, \dots, x_n, h) \subset S$ 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 [BS87].

Definition 1. 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, for $j > 0$ we define the set $U_j(I) \subset R_1^j$ by

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

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

It is shown in [CG20] 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 $\mathrm{sd}_{1,DRL}(\mathcal{F}) \le \mathrm{reg}(\mathcal{F}^h)$. The proof of this result uses the following definition, which differs slightly from the one given above:

Definition 2. Let $I \subset S = k[x_1, \dots, x_n, h]$ be a homogeneous ideal with $|\mathcal{Z}_+(I)| < \infty$. 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}.

However, an earlier version of the [CG20] paper uses 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, $S = k[x_1, \dots, x_n]$. 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 1. Let $I \subset k[x, y]$ be given by $I = (x^2, y^2)$. Then the matrix

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

yields the ideal gI, generated by

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

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

We 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 [Gal74] shows that the number of equivalence classes is finite, and that one of them is a Zariski open set in $GL_n(k)$ (see also [MS05]). 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 3. Let $I \subset S = k[x_1, \dots, x_n]$ 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 [BS87] that this Zariski open equivalence class is contained in the open set $V = \{g \in GL_n(k) : (x_n, \dots, x_{n-r+1}) \in U_r(gI)\}$ using the notation of Definition 1. This means that if I is in generic coordinates in the sense of Definition 3, then the identity matrix is in this set V, meaning $(x_n, \dots, x_{n-r+1}) \in U_r(I)$ for $r = \dim(S/I)$, and we have that I is in generic coordinates in the sense of Definition 1, which in turn implies being in generic coordinates in the sense of Definition 2. The implication (1) $\implies$ (2) is strict since Definition 2 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 (3) $\implies$ (1) 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 [Frö85]. 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 [Par10], which involves the idea of a "generic sequence" of polynomials:

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

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

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” the conjecture asserts that

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

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

Definition 4. 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. 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 $U \subset \prod_{i=1}^{r} S_{d_i}$. A sequence with coefficients in U is then said to be a **generic sequence**. See [Par10].

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 [Par10], Section 2:

Proposition 1. *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 4 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 opend, 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.

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 [Fau02], 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

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

arithmetic operations, where $2 \leq \omega < 2.39$ is the linear algebra constant [BFS04]. 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, and we will discuss this shortly, along with the relevant definitions. 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 [Par10] 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 [Tru19]), 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 4, and (if Fröberg's conjecture is true) it gives us good results about the complexity of at least one Gröbner basis algorithm. Our other definitions are slightly easier to work with, so it would be nice if one of them would imply Definition 4. Unfortunately, we can show that none of them imply Definition 4 with the following example:

Example 2. 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 3. 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 1. 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 4. 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 3. Hence Definition 3 does not imply Definition 4.

Now because Definition 3 implies Definitions 1 and 2, we cannot have that either of these imply Definition 4.

Questions

- Does Definition 4 imply any of the others? [BDND$^+$21] seems to suggest so on page 11.
- The form suggested by Fröberg's conjecture would imply that any ideal defined by an overdermined generic sequence (in the sense of Definition 4) is zero-dimensional. We have examples of generic ideals (in the sense of Definition 3) that don't satisfy Fröberg's conjecture, but these all have positive dimension—does Fröberg's conjecture hold for a zero-dimensional generic ideal?
- The ideal $I = (x^2, y^2, z^2)$ has Hilbert series of the form in Fröberg's conjecture, which is known to hold in $k[x, y, z]$ for an infinite field k. However, I is not generic in the sense of Definition 3 (it is not Borel-fixed). This could be a counterexample to Definition 4 implying Definition 3, but even though its Hilbert series is generic, we don't know necessarily whether the coefficients of I are in the open set V_1 on which the Hilbert series is constant—is there a way to figure this out?

References

[BDND$^+$21] Mina Bigdeli, Emanuela De Negri, Manuela Muzika Dizdarevic, Elisa Gorla, Romy Minko, and Sulamithe Tsakou. Semi-regular sequences and other random systems of equations. In *Women in Numbers Europe III: Research Directions in Number Theory*, pages 75–114. Springer, 2021.

[BFS04] Magali Bardet, Jean-Charles Faugere, and Bruno Salvy. 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, 2004.

[BS87] David Bayer and Michael Stillman. A criterion for detecting m-regularity. *Inventiones mathematicae*, 87(1):1–11, 1987.

[CG20] Alessio Caminata and Elisa Gorla. Solving multivariate polynomial systems and an invariant from commutative algebra. In *International Workshop on the Arithmetic of Finite Fields*, pages 3–36. Springer, 2020.

[Fau02] Jean Charles Faugere. 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, 2002.

[Frö85] Ralf Fröberg. An inequality for hilbert series of graded algebras. *Mathematica Scandinavica*, 56(2):117–144, 1985.

[Gal74] André Galligo. 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). 1974.

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

[MS05] Ezra Miller and Bernd Sturmfels. *Combinatorial commutative algebra*, volume 227. Springer, 2005.

[Par10] Keith Pardue. Generic sequences of polynomials. *Journal of Algebra*, 324(4):579–590, 2010.

[S$^+$22] W. A. Stein et al. *Sage Mathematics Software (Version 9.6)*. The Sage Development Team, 2022. `http://www.sagemath.org`.

[Tru19] Van Duc Trung. The initial ideal of generic sequences and fröberg's conjecture. *Journal of Algebra*, 524:79–96, 2019.