

# Notions of regularity

10/13/22

## Maximum degree of a reduced Gröbner basis element

**Definition.** Given an ideal  $I \subset k[x_1, \dots, x_n]$  and a term order  $\tau$ , we denote by  $\text{max.GB.deg}_\tau(I)$  the maximum of the degrees of all polynomials in the reduced Gröbner basis of  $I$  with respect to the term order  $\tau$ .

## Solving degree

Given a system of equations  $\mathcal{F} = \{f_1, \dots, f_s\}$  in variables  $x_1, \dots, x_n$  and the ideal  $I = (f_1, \dots, f_s) \subset k[x_1, \dots, x_n]$  it defines, we are interested in finding the corresponding solution set  $\mathcal{Z}(I)$ . 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 outline in section 2 of [CG20]. 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.

The complexity of computing a Gröbner basis is therefore of interest. Many algorithms to do this use row reduction on Macaulay matrices of increasing size, and so the complexity can be thought of as a function of the size of the largest matrix involve. This in turn, is determined by the **solving degree** of a system. There are a few different definitions of the solving degree, but generally speaking this is the largest degree of any Macaulay matrix involved in computing a Gröbner basis. One definition is as follows:

[CG20] **Definition 6.** Let  $\mathcal{F} = \{f_1, \dots, f_s\} \subset k[x_1, \dots, x_n]$  and let  $\tau$  be a term order. The **solving degree** of  $\mathcal{F}$ , denoted  $\text{solv.deg}_\tau(\mathcal{F})$ , is the least degree  $d$  such that Gaussian elimination on the Macaulay matrix  $M_{\leq d}$  produces a Gröbner basis with respect to  $\tau$ .

We also have the following notion that allows us to relate the solving degree and the largest degree of an element in a Gröbner basis:

**Definition.** A term order  $\tau$  is called **degree-compatible** if  $\deg(x^\alpha) < \deg(x^\beta)$  implies  $x^\alpha <_\tau x^\beta$ .

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

$$\max.\text{GB}.\deg_\tau(\mathcal{F}) \leq \text{solv}.\deg_\tau(\mathcal{F}).$$

This is 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  $\tau$  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  $d = \text{solv}.\deg_\tau(\mathcal{F})$ .

[Min21] **Definition 3.3.1.** The **solving degree** of  $\mathcal{F} = \{f_1, \dots, f_s\}$ ,  $d_{\text{solve}}(\mathcal{F})$ , is the degree  $d$  at which a Gröbner basis algorithm returns a *DRL* Gröbner basis of  $I = (f_1, \dots, f_s)$ .

[CG23] **Definition 1.1.** Let  $\mathcal{F} \subset k[x_1, \dots, x_n]$  be a polynomial system. The **solving degree** of  $\mathcal{F}$  with respect to a term order  $\tau$  is the least degree  $d$  such that  $\text{rowsp}(M_d)$  contains a Gröbner basis of  $(\mathcal{F})$  with respect to  $\tau$ . We denote it by  $\text{sd}_\tau(\mathcal{F})$ .

In this last definition,  $M_d$  is the RREF matrix the algorithm being used outputs in degree  $d$ . As we can see, some definitions consider all possible term orders, some only *DRL*; some definitions consider any Gröbner basis algorithms, some only certain explicitly mentioned algorithms. In the case of the first and third definitions, the algorithm being used differs only in that after row reducing a matrix  $M_{\leq d}$ , the algorithm in the third definition adds new rows to the starting matrix  $M$  for each polynomial  $uf$  where  $f$  is a polynomial of degree strictly less than  $d$  corresponding to a vector in  $M_{\leq d}$  and  $u$  is a monomial such that  $\deg(uf) \leq d$ . This algorithm then repeats the row reduction of the matrix  $M$  with its new rows until no new rows are added. In the algorithm used in the first definition, however, the degree  $d$  step ends after the row reduction of the degree  $d$  Macaulay matrix—no new rows are added. 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. 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  $M_{\leq 3}$ :

$$\begin{array}{c}
f_1 \\
f_2 \\
xf_1 \\
yf_1 \\
zf_1 \\
xf_2 \\
yf_2 \\
zf_2
\end{array}
\begin{pmatrix}
x^3 & x^2y & xy^2 & y^3 & x^2z & xyz & y^2z & xz^2 & yz^2 & z^3 & x^2 & xy & y^2 & xz & yz & z^2 & x & y & z & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 \\
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

which in RREF is

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

We note now that  $x^2 = z^2f_1 + (x - yz)f_2 \in (\mathcal{F})$  and so  $x^2 \in \text{in}_{DRL}(\mathcal{F})$  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  $(xy, y^2, yz) \neq \text{in}_{DRL}(\mathcal{F})$ , meaning the above collection of polynomials we obtained from the RREF form of  $M_{\leq 3}$  is not a Gröbner basis. Therefore  $\text{solv.deg}_{DRL}(\mathcal{F}) > 3$ .

We now consider the case in which we base our notion of solving degree on the Gröbner basis algorithm discussed in [CG23] rather than in [CG20]. The first stage of degree 3 computations in this algorithm 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 or equal to 3 that correspond to row vectors not originally in the row space of the above matrices. For the degree 3 polynomials in the above collection, the only

monomial we may multiply by to keep the degree at most 3 is the monomial 1, and if we multiply by this, the polynomials are coming from the row space of these matrices. Therefore we look only at the polynomials of degree strictly less than three for candidates. For instance, 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:

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

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

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

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  $\text{sd}_{DRL}(\mathcal{F}) = 3 < \text{solv.deg}_{DRL}(\mathcal{F})$ .

Thus it is not always the case that these two notions of solving degree, although they are both based on Macaulay matrices, agree. We can note, however, that if  $\text{solv.deg}_{DRL}(\mathcal{F}) = d$  for some system  $\mathcal{F}$ , then the Macaulay matrix  $M_{\leq d}$ , when row reduced, contains a Gröbner basis in its rows. Therefore running the procedure in [CG23] with the starting matrix  $M_{\leq d}$  may add more rows to the matrix, but will still contain the rows that form a Gröbner basis. Hence  $\text{sd}_{DRL}(\mathcal{F}) \leq d = \text{solv.deg}_{DRL}(\mathcal{F})$ . So we have an inequality that holds generally, and the next question is when equality holds. We have the following conjecture:

**Conjecture 1.** Let  $\mathcal{F} = \{f_1, \dots, f_r\} \subset k[x_1, \dots, x_n]$  and assume  $(\mathcal{F})$  is in generic coordinates. Then  $\text{sd}_{DRL}(\mathcal{F}) = \text{solv.deg}_{DRL}(\mathcal{F})$ .

Perhaps the next question is what does this mean for the main result of [CG20], that  $\text{solv.deg}_{DRL}(\mathcal{F}) \leq \text{reg}(\mathcal{F}^h)$ ? By our inequality, we have that  $\text{sd}_{DRL}(\mathcal{F}) \leq \text{solv.deg}_{DRL}(\mathcal{F}) \leq \text{reg}(\mathcal{F}^h)$ , so this bound holds for both notions of the solving degree, but we note that this relies on the assumption that  $(\mathcal{F})$

is in generic coordinates. Caminata and Gorla note in [CG20] that for a system  $\mathcal{F} \subset \mathbb{F}_q$ , adding the field equations to the system will ensure that the genericity assumption is satisfied, but also that the addition of these equations may increase the solving degree. We would like to extend the result to the non-generic case, and so we have the following conjectures:

**Conjecture 2.** Let  $\mathcal{F} = \{f_1, \dots, f_r\} \subset k[x_1, \dots, x_n]$ . Then

$$\text{solv.deg}_{DRL}(\mathcal{F}) \leq \text{reg}(\text{in}_{DRL}(\mathcal{F}^h)).$$

Note that if  $(\mathcal{F})$  is in generic coordinates, we recover Caminata and Gorla's result that

$$\text{solv.deg}_{DRL}(\mathcal{F}) \leq \text{reg}(\text{in}_{DRL}(\mathcal{F}^h)) = \text{reg}(\mathcal{F}^h).$$

**Conjecture 3.** Let  $\mathcal{F} = \{f_1, \dots, f_r\} \subset k[x_1, \dots, x_n]$ . Then  $\text{sd}_{DRL}(\mathcal{F}) \leq \text{reg}(\mathcal{F}^h)$ .

To illustrate these conjectures, we give the results computations with Sage on the examples given in [CG23], as well as on Minko's Example 3.4.1 [Min21]. The  $DRL$  term order is used throughout.

	max.GB.deg( $\mathcal{F}$ )	solv.deg( $\mathcal{F}$ )	sd( $\mathcal{F}$ )	$d_{\mathcal{F}}$	reg(in( $\mathcal{F}^h$ ))	reg( $\mathcal{F}^h$ )
Example 2.4	5	$\geq 20^1$	11	11	20	15
Example 4.1 over $\mathbb{F}_{11}$	2	3	3	3	11	11
Example 4.2 over $\mathbb{F}_7$	6	6	6	3	8	8
Example 4.3 over $\mathbb{F}_{13}$	2	2	2	0	3	3
Example 4.4 over $\mathbb{F}_5$	4	16	9	9	17	13
Minko 3.4.1	6	22	18	18	22	18

As can be seen from the table,  $\text{sd}_{DRL}(\mathcal{F}) \leq \text{reg}(\mathcal{F}^h)$  in every case, as Conjecture 3 would suggest. For Conjecture 2, it remains to finish checking whether row reduction on  $M_{\leq 20}$  yields a Gröbner basis in Example 2.4, but otherwise we see that  $\text{solv.deg}_{DRL}(\mathcal{F}) \leq \text{reg}(\text{in}_{DRL}(\mathcal{F}^h))$ . Lastly, to show there are no counterexamples here to Conjecture 1, we must verify that the systems in Examples 2.4 and 4.4 from [CG23] and 3.4.1 from [Min21] are not in generic coordinates, since these are the examples for which  $\text{sd}_{DRL}(\mathcal{F}) < \text{solv.deg}_{DRL}(\mathcal{F})$ .

---

<sup>1</sup>We have  $\geq 20$  here rather than 20, because the matrices involved in checking the case  $d = 20$  appear to be too large for Sage to work with well. We have checked that row reducing the Macaulay matrix  $M_{\leq 19}$  does not yield a Gröbner basis for  $(\mathcal{F})$ , so we know only that  $\text{solv.deg}(\mathcal{F}) \geq 20$ . Conjecture 2 asserts that this should be  $\leq 20$ , so we'd like to confirm that in fact  $\text{solv.deg}(\mathcal{F}) = 20$ , but this involves row reducing a roughly  $10000 \times 10000$  matrix.

## Degree of Regularity (Bardet, et al)

The degree of regularity as first defined in [Bar04] and [BFS04] is not an upper bound for the solving degree, but is often close. Before giving definitions for the degree of regularity, we first give the following prerequisite definitions:

### Hilbert (function / polynomial / series) definition

### index of regularity definition

We now have the following definitions for the degree of regularity, taking  $R = k[x_1, \dots, x_n]$ :

**[BFS04] Definition 4.** Given a zero-dimensional ideal  $I = (f_1, \dots, f_m) \subset R$  with  $m \geq n$ , we define the **degree of regularity** to be

$$d_{\text{reg}}(\mathcal{F}) = \min \left\{ d \geq 0 \mid \dim_k I_d = \binom{n+d-1}{d} \right\}$$

where  $I_d = \{f \in I \mid \deg(f) = d\}$  and we are considering its dimension as a  $k$ -vector space.

**[CG20] Definition 12.** Let  $\mathcal{F} = \{f_1, \dots, f_s\} \subset R$  such that  $(\mathcal{F}^{\text{top}})_d = R_d$  for some  $d \gg 0$ . Then the **degree of regularity** of  $\mathcal{F}$  is  $d_{\text{reg}}(\mathcal{F}) = i_{\text{reg}}(\mathcal{F}^{\text{top}})$ .

**[Min21] Definition 3.3.9.** Let  $\mathcal{F} = \{f_1, \dots, f_s\} \subset R$ . The **degree of regularity** of  $\mathcal{F}$  is

$$d_{\text{reg}}(\mathcal{F}) = \min\{d \geq 0 \mid (\mathcal{F}^{\text{top}})_d = R_d\}.$$

If this minimum does not exist, that is, if  $(\mathcal{F}^{\text{top}})_d \neq R_d$  for all  $d \geq 0$ , then define  $d_{\text{reg}}(\mathcal{F}) = \infty$ .

As we can see, some authors require that the number of polynomials in the system is greater than the number of variables (requiring an *overdetermined* system), some authors require that there does exist some  $d \gg 0$  for which  $(\mathcal{F}^{\text{top}})_d = R_d$ , and, in the case of the last definition, some authors use this condition as the definition of degree of regularity.

## References

- [Bar04] Magali Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie*. PhD thesis, Université Pierre et Marie Curie-Paris VI, 2004.
- [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.
- [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.
- [CG23] Alessio Caminata and Elisa Gorla. Solving degree, last fall degree, and related invariants. *Journal of Symbolic Computation*, 114:322–335, 2023.
- [Min21] Romy Minko. *Security assumptions in post-quantum cryptography*. PhD thesis, University of Oxford, 2021.