The Complexity of Algebraic Algorithms for LWE

Matthias Johann Steiner ⬤

Alpen-Adria-Universität Klagenfurt, Klagenfurt am Wörthersee, Austria
`matthias.steiner@aau.at`

Abstract. Arora & Ge introduced a noise-free polynomial system to compute the secret of a Learning With Errors (LWE) instance via linearization. Albrecht et al. later utilized the Arora-Ge polynomial model to study the complexity of Gröbner basis computations on LWE polynomial systems under the assumption of semi-regularity. In this paper we revisit the Arora-Ge polynomial and prove that it satisfies a genericity condition recently introduced by Caminata & Gorla, called being in generic coordinates. For polynomial systems in generic coordinates one can always estimate the complexity of DRL Gröbner basis computations in terms of the Castelnuovo-Mumford regularity and henceforth also via the Macaulay bound.

Moreover, we generalize the Gröbner basis algorithm of Semaev & Tenti to arbitrary polynomial systems with a finite degree of regularity. In particular, existence of this algorithm yields another approach to estimate the complexity of DRL Gröbner basis computations in terms of the degree of regularity. In practice, the degree of regularity of LWE polynomial systems is not known, though one can always estimate the lowest achievable degree of regularity. Consequently, from a designer's worst case perspective this approach yields sub-exponential complexity estimates for general, binary secret and binary error LWE.

In recent works by Dachman-Soled et al. the hardness of LWE in the presence of side information was analyzed. Utilizing their framework we discuss how hints can be incorporated into LWE polynomial systems and how they affect the complexity of Gröbner basis computations.

Keywords: LWE · LWE with hints · Gröbner bases

1 Introduction

With the emerging threat of Shor's quantum polynomial time algorithms for factoring and discrete logarithms [34] on the horizon, cryptographers in the past 20 years have been in desperate search for new cryptographic problems that cannot be solved in polynomial time on classical as well as quantum computers. So far, lattice-based cryptography built on *Learning With Errors* (LWE) and the *Short Integer Solution* (SIS) [1] has emerged as most promising candidate for cryptography in the presence of quantum computers.

In this paper we revisit polynomial models to solve the Search-LWE problem via Gröbner basis computations. Solving LWE via a polynomial system was

first done by Arora & Ge [6], though they solved the system via linearization not via Gröbner bases. Albrecht et al. [2,3] studied the complexity of Gröbner basis computations for the Arora-Ge polynomial model under the assumption that the polynomial system is *semi-regular* [24,29]. Moreover, for binary error LWE Sun et al. [37] refined the complexity estimates for linearization under the semi-regularity assumption. For a general review of the computational hardness of LWE we refer to [4].

We stress that the complexity estimates of [2,3,37] are still hypothetical since both works do not provide a proof that a LWE polynomial system is semi-regular except for very special cases, see e.g. [3, Theorem 11]. Moreover, the complexity bounds rely on asymptotic studies of the Hilbert series of a semi-regular polynomial system. Needless to say that a priori is not guaranteed that these complexity estimates apply for practical LWE instantiations.

In this paper we consider two new approaches to estimate the complexity of Gröbner basis computations. Caminata & Gorla [12] revealed that the solving degree of polynomial system in *generic coordinates* is always upper bounded by the Castelnuovo-Mumford regularity and henceforth also by the Macaulay bound, see [12, Theorem 10]. For our first approach we prove that any fully determined LWE polynomial system is in generic coordinates. In particular this implies that for any LWE polynomial system there exists a Gröbner basis algorithm in exponential time as well as memory complexity. Semaev & Tenti [33] revealed that the complexity of Gröbner basis algorithms can also be estimated via the *degree of regularity* of a polynomial system. Though, their bound is only applicable over finite fields and the polynomial system must contain the field equations, see [33, Theorem 2.1] and [38, Theorem 3.65]. We generalize their result to any polynomial system that admits a finite degree of regularity regardless of the underlying field. For a fixed degree of regularity we will determine the minimal number of LWE samples necessary so that the polynomial system could achieve the degree of regularity. Hence, for a designer this implies that there *could* exist Gröbner basis algorithms in sub-exponential time as well as memory to solve Search-LWE.

In two recent works Dachman-Soled et al. [18,19] introduced a framework to study the complexity of attacks on Search-LWE in the presence of side information. In Section 6 we shortly review their framework and describe how hints can be incorporated into LWE polynomial systems. Moreover, in Example 28 we showcase the complexity impact of hints on Gröbner basis computations.

Finally, Semaev & Tenti [33] also investigated the probability that a uniformly and independently distributed polynomial system $\mathcal{F} \subset \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$ achieves a certain degree of regularity. Their proof depends only on combinatorial properties, hence we expect that a similar result can be proven for uniformly and independently distributed polynomial system $\mathcal{F} \subset \mathbb{F}_q[x_1, \ldots, x_n]/\big(f(x_1), \ldots, f(x_n)\big)$, where f is univariate and $\deg(f) \geq 2$ is arbitrary. In Appendix A we study the related problem whether a LWE polynomial is close to the uniform distribution or not. We find a negative answer for this question, in particular we show that the statistical distance between the highest

degree component of a LWE polynomial and the uniform distribution is always $\geq \frac{1}{2}$ and has limit 1 if the degree of the LWE polynomial goes to infinity. Hence, even if Semaev & Tenti's generalizes it is not applicable to LWE polynomial systems.

2 Preliminaries

By k we will always denote a field, by $\bar{k}$ we denote its algebraic closure, and by $\mathbb{F}_q$ we denote the finite field with q elements. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, then we denote the zero locus of I over $\bar{k}$ as

$$\mathcal{Z}(I) = \left\{ \mathbf{x} \in \bar{k}^n \mid f(\mathbf{x}) = 0, \ \forall f \in I \right\} \subset \mathbb{A}_{\bar{k}}^n. \tag{1}$$

If in addition I is homogeneous, then we denote the projective zero locus over $\bar{k}$ by $\mathcal{Z}_+(I) \subset \mathbb{P}_{\bar{k}}^{n-1}$.

Let $f \in K[x_1, \ldots, x_n]$ be a polynomial, and let x_0 be an additional variable, we call

$$f^{\mathrm{hom}}(x_0, \ldots, x_n) = x_0^{\deg(f)} \cdot f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in K[x_0, \ldots, x_n] \tag{2}$$

the homogenization of f with respect to x_0, and analog for the homogenization of ideals $I^{\mathrm{hom}} = \left\{ f^{\mathrm{hom}} \mid f \in I \right\}$ and finite systems of polynomials $\mathcal{F}^{\mathrm{hom}} = \left\{ f_1^{\mathrm{hom}}, \ldots, f_m^{\mathrm{hom}} \right\}$. Further, we will always assume that we can extend a term order on $k[x_1, \ldots, x_n]$ to a term order on $k[x_0, \ldots, x_n]$ according to [12, Definition 8].

For a term order $>$ and an ideal $I \subset k[x_1, \ldots, x_n]$ we denote with

$$\mathrm{in}_>(I) = \{\mathrm{LT}_>(f) \mid f \in I\} \tag{3}$$

the initial ideal of I, i.e. the ideal of leading terms of I, with respect to $>$.

Every polynomial $f \in [x_1, \ldots, x_n]$ can be written as $f = f_d + f_{d-1} + \ldots + f_0$, where f_i is homogeneous of degree i. We denote the highest degree component f_d of f with f^{top}, and analog we denote $\mathcal{F}^{\mathrm{top}} = \left\{ f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}} \right\}$.

For a homogeneous ideal $I \subset P$ and an integer $d \geq 0$ we denote

$$I_d = \{f \in I \mid \deg(f) = d, \ f \text{ homogeneous}\}, \tag{4}$$

and analog for the polynomial ring P.

Let $I, J \subset k[x_1, \ldots, x_n]$ be ideals, then we denote with

$$I : J = \{f \in k[x_1, \ldots, x_n] \mid \forall g \in J \colon f \cdot g \in I\} \tag{5}$$

the usual ideal quotient, and with $I : J^\infty = \bigcup_{i \geq 1} I : J^i$ the saturation of I with respect to J.

Let $I, \mathfrak{m} \in k[x_0, \ldots, x_n]$ be homogeneous ideals where $\mathfrak{m} = (x_0, \ldots, x_n)$, then we call $I^{\mathrm{sat}} = I : \mathfrak{m}^\infty$ the saturation of I.

We will often encounter the lexicographic and the degree reverse lexicographic term order which we will abbreviate as LEX and DRL respectively.

For $\mathbf{x}, \mathbf{y} \in k^n$ we denote the standard inner product as

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^\mathsf{T} \mathbf{y} = \sum_{i=1}^{n} x_i \cdot y_i. \tag{6}$$

By log we denote the natural logarithm and by $\log_2$ the logarithm in base 2.

2.1 Learning With Errors

Learning With Errors (LWE) was introduced by Ajtai in his seminal work [1]. In its base form it can be formulated as a simple computational linear algebra problem.

Definition 1 (Learning with errors, [1]). *Let q be a prime, let $n \geq 1$ be an integer, and let χ be a probability distribution on $\mathbb{Z}$. For a secret vector $\mathbf{s} \in \mathbb{F}_q^n$ the LWE distribution $A_{\mathbf{s},\chi}$ over $\mathbb{F}_q^n \times \mathbb{F}_q$ is sampled by choosing $\mathbf{a} \in \mathbb{F}_q^n$ uniformly at random, choosing $e \leftarrow \chi$, and outputting $(\mathbf{a}, \langle \mathbf{s}, \mathbf{a} \rangle + e \in \mathbb{F}_q)$.*

In Search-LWE we are given m LWE samples $(\mathbf{a}_i, b_i)$ sampled according to some probability distribution. Our task is then to recover the secret vector $\mathbf{s} \in \mathbb{F}_q^n$ that has been used to generate the samples.

As probability distribution one typically chooses a discrete Gaussian distribution with mean 0 and standard deviation σ. For ease of computation in this paper, we ignore the discretization and assume $\chi = \mathcal{N}(0, \sigma)$ if not specified otherwise, hence we do not discuss discretization techniques further. Assume that $X \sim \mathcal{N}(0, \sigma)$, we will utilize the following well-known property of the Gaussian distribution several times in this paper

$$\mathbb{P}\left[|X| > t \cdot \sigma\right] \leq \frac{2}{t \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{t^2}{2}\right). \tag{7}$$

It is well-known that solving Search-LWE for a discrete Gaussian error distribution and $\sigma \in \mathcal{O}(\sqrt{n})$ is at least as hard as solving several computational lattice problems, see e.g. [31,30,10,28].

Moreover, on top of LWE many cryptographic functions can be built, e.g. Regev's public key cryptosystem [31] as well as a key exchange mechanism [9].

2.2 Gröbner Bases

For an ideal $I \subset k[x_1, \ldots, x_n]$ and a term order $>$ on the polynomial ring, a $>$-Gröbner basis $\mathcal{G} = \{g_1, \ldots, g_m\}$ is a finite set of generators such that

$$\mathrm{in}_{>}(I) = \big(\mathrm{LT}_{>}(g_1), \ldots, \mathrm{LT}_{>}(g_m) \big). \tag{8}$$

Gröbner bases were introduced by Bruno Buchberger in his PhD thesis [11]. With Gröbner bases one can solve many computational problems on ideals like

the ideal membership problem or the computation of the zero locus [17]. For a general introduction to the theory of Gröbner bases we refer to [17].

Today, two classes of Gröbner basis algorithms are known: *Buchberger's algorithm* and *linear algebra-based algorithms*. In this paper we only study the latter family.

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = k[x_1, \ldots, x_n]$ be a homogeneous polynomial system, and let $>$ be a term order on P. The *homogeneous Macaulay matrix* in degree d, denoted as M_d, has columns indexed by monomials in P_d sorted from left to right with respect to $>$. The rows of M_d are indexed by polynomials $s \cdot f_i$, where $s \in P$ is a monomial such that $\deg(s \cdot f_i) = d$. The entry of row $s \cdot f_i$ at column t is the coefficient of $s \cdot f_i$ at the monomial t. For an inhomogeneous polynomial system M_d is replaced by $M_{\leq d}$ and the degree equalities by inequalities. By performing Gaussian elimination on $M_0, \ldots, M_d$ respectively $M_{\leq d}$ for d big enough one will produce a $>$-Gröbner basis of $\mathcal{F}$. This idea can be traced back to Lazard [26]. Since d determines the complexity of this algorithm in space and time, the least suitable d is of special interest [20].

Definition 2 (Solving degree, [12, Definition 6]). *Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$ and let $>$ be a term order. The solving degree of $\mathcal{F}$ is the least degree d such that Gaussian elimination on the Macaulay matrix $M_{\leq d}$ produces a Gröbner basis of $\mathcal{F}$ with respect to $>$. We denote it by $\mathrm{sd}_>(\mathcal{F})$.*

If $\mathcal{F}$ is homogeneous, we consider the homogeneous Macaulay matrix M_d and let the solving degree of $\mathcal{F}$ be the least degree d such that Gaussian elimination on $M_0, \ldots, M_d$ produces a Gröbner basis of $\mathcal{F}$ with respect to $>$.

Today, the most efficient variants of linear algebra-based Gröbner basis algorithms are Faugére's F4 [22] and Matrix-F5 [23] algorithms. These algorithms utilize efficient selection criteria to avoid redundant rows in the Macaulay matrices. Moreover, they construct the matrices for increasing values of d. Therefore, they also need stopping criteria, though one could artificially stop the computation once the solving degree is reached since then a Gröbner basis must already be contained in the system produced by Gaussian elimination. Hence, we do not discuss termination criteria further.

Let $\mathcal{F} \subset k[x_1, \ldots, x_n]$ be a polynomial system, and let $\mathcal{F}^{\mathrm{hom}}$ be its homogenization. We always have that, see [12, Theorem 7],

$$\mathrm{sd}_{DRL}(\mathcal{F}) \leq \mathrm{sd}_{DRL}\left(\mathcal{F}^{\mathrm{hom}}\right). \tag{9}$$

Complexity Estimate via the Solving Degree. For a matrix $\mathbf{A} \in k^{n \times m}$ of rank r the reduced row echelon form can be computed in $\mathcal{O}\left(n \cdot m \cdot r^{\omega-2}\right)$ [36, §2.2], where $2 \leq \omega < 2.37286$ is a linear algebra constant [5].

Let $\mathcal{F} \subset P = k[x_1, \ldots, x_n]$ be a system of m homogeneous polynomials, it is well-known that the number of monomials in P_d is given by $\binom{n+d-1}{d}$. Moreover, at most $\binom{n+d-\deg(f_i)-1}{d-\deg(f_i)} \leq \binom{n+d-1}{d}$ many columns can stem from the polynomial f_i. Therefore, the cost of Gaussian elimination on $M_0, \ldots, M_d$ is bounded by

$$\mathcal{O}\left(m \cdot d \cdot \binom{n+d-1}{d}^{\omega}\right). \tag{10}$$

Thus, by estimating the solving degree $\mathrm{sd}_{DRL}(\mathcal{F})$ we yield a complexity upper bound for linear algebra-based Gröbner basis computations.

2.3 Generic Coordinates & the Solving Degree

For completeness, we shortly recall the definition of the Castelnuovo-Mumford regularity [21, Chapter 4], a well-established invariant from commutative algebra and algebraic geometry. Let $P = k[x_0, \ldots, x_n]$ be the polynomial ring and let

$$\mathbf{F} : \cdots \to F_i \to F_{i-1} \to \cdots \tag{11}$$

be a graded complex of free P-modules, where $F_i = \sum_j P(-a_{i,j})$.

Definition 3. *The Castelnuovo-Mumford regularity of $\mathbf{F}$ is defined as*

$$\mathrm{reg}\,(\mathbf{F}) = \sup_i a_{i,j} - i.$$

By Hilbert's Syzygy theorem [21, Theorem 1.1] any finitely graded P-module has a finite free graded resolution. I.e., for every homogeneous ideal $I \subset P$ the regularity of I is computable.

Next we introduce the notion of generic coordinates which first appeared in the seminal work of Bayer & Stillman [8]. Let $I \subset P$ be an ideal, and let $r \in P$. We use the shorthand notation "$r \nmid 0 \mod I$" for expressing that r is not a zero-divisor on P/I.

Definition 4 ([12,13, Definition 5]). *Let k be an infinite field. Let $I \subset k[x_0, \ldots, x_n]$ be a homogeneous ideal with $|\mathcal{Z}_+(I)| < \infty$. We say that I is in generic coordinates if either $|\mathcal{Z}_+(I)| = 0$ or $x_0 \nmid 0 \mod I^{\mathrm{sat}}$.*

Let k be any field, and let $k \subset K$ be an infinite field extension. I is in generic coordinates over K if $I \otimes_k K[x_0, \ldots, x_n] \subset K[x_0, \ldots, x_n]$ is in generic coordinates.

Provided a polynomial system is in generic coordinates, then the solving degree is always upper bounded by the Castelnuovo-Mumford regularity.

Theorem 5 ([12, Theorem 9, 10]). *Let K be an algebraically closed field, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset K[x_1, \ldots, x_n]$ be an inhomogeneous polynomial system such that $(\mathcal{F}^{\mathrm{hom}})$ is in generic coordinates. Then*

$$\mathrm{sd}_{DRL}\,(\mathcal{F}) \leq \mathrm{reg}\,(\mathcal{F}^{\mathrm{hom}})\,.$$

By a classical result one can always bound the regularity of an ideal with the Macaulay bound (see [15, Theorem 1.12.4]).

Corollary 6 (Macaulay bound, [26, Theorem 2], [12, Corollary 2]). *Consider a system of equations $\mathcal{F} = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$ with $d_i = \deg(f_i)$ and $d_1 \geq \ldots \geq d_m$. Set $l = \min\{n+1, m\}$. Assume that $\left|\mathcal{Z}_+\left(\mathcal{F}^{\mathrm{hom}}\right)\right| < \infty$ and that (F^{hom}) is in generic coordinates over $\bar{k}$. Then*

$$\mathrm{sd}_{DRL}\,(\mathcal{F}) \leq \mathrm{reg}\,(\mathcal{F}^{\mathrm{hom}}) \leq d_1 + \ldots + d_l - l + 1.$$

In particular, if $m > n$ and $d = d_1$, then

$$\mathrm{sd}_{DRL}\left(\mathcal{F}\right) \leq (n+1) \cdot (d-1) + 1.$$

In the proof of [12, Theorem 11] Caminata & Gorla implicitly revealed an efficient criterion to prove that a polynomial system is in generic coordinates. This observation was later formalized by Steiner in terms of the highest degree components of a polynomial system [35].

Theorem 7 ([35, Theorem 3.2]). *Let k be an algebraically closed field, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$ be an inhomogeneous polynomial system such that*

(i) $(\mathcal{F}) \neq (1)$, and
(ii) $\dim(\mathcal{F}) = 0$.

Then the following are equivalent.

(1) $\left(\mathcal{F}^{\mathrm{hom}}\right)$ is in generic coordinates and $\left|\mathcal{Z}_+\left(\mathcal{F}^{\mathrm{hom}}\right)\right| \neq 0$.
(2) $\sqrt{\mathcal{F}^{\mathrm{top}}} = (x_1, \ldots, x_n)$.
(3) $(\mathcal{F}^{\mathrm{top}})$ is zero-dimensional in $k[x_1, \ldots, x_n]$.
(4) For every $1 \leq i \leq n$ there exists an integer $d_i \geq 1$ such that $x_i^{d_i} \in \mathrm{in}_{DRL}\left(\mathcal{F}^{\mathrm{hom}}\right)$.

In particular, (4) implies that every inhomogeneous polynomial system that contains a zero-dimensional DRL Gröbner basis is already in generic coordinates.

2.4 A Refined Solving Degree

In the Gröbner basis complexity literature there is another quantity that is also known as solving degree that refines Definition 2, cf. [14, §1]. Again let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P = k[x_1, \ldots, x_n]$ be a finite set of polynomials, and let $>$ be a term order on P. We start with $M_{\leq d}$ the Macaulay matrix for $\mathcal{F}$ up to degree d and compute a basis $\mathcal{B}$ of the row space of $M_{\leq d}$ via Gaussian elimination. Now we construct the Macaulay matrix $M_{\leq d}$ for the polynomial system $\mathcal{B}$ and again compute the basis $\mathcal{B}'$ of the row space via Gaussian elimination. We repeat this procedure until $\mathcal{B} = \mathcal{B}'$, at this point multiplying the polynomials in $\mathcal{B}'$ with all monomials up to degree $\leq d$ does not add any new elements to the basis after Gaussian elimination. We denote the final Macaulay matrix for $\mathcal{F}$ with $\hat{M}_d$, and we also denote $\hat{M}_d$'s row space via $\mathrm{rowsp}\left(\hat{M}_d\right)$. It is clear that

$$\mathrm{rowsp}\left(\hat{M}_d\right) \subset (\mathcal{F})_{\leq d} = \left\{ f \in (\mathcal{F}) \;\middle|\; f = \sum_{i=1}^{m} g_i \cdot f_i, \; \deg\left(g_i \cdot f_i\right) \leq d \right\}, \quad (12)$$

and for d big enough $\mathrm{rowsp}\left(\hat{M}_d\right)$ will contain a $>$-Gröbner basis for $\mathcal{F}$. This motivates the following definition.

Definition 8 (Refined solving degree, see [14, Definition 1.1]). *Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$ and let $>$ be a term order. The refined solving degree of $\mathcal{F}$ is the least degree d such that $\mathrm{rowsp}\left(\hat{M}_d\right)$ contains a Gröbner basis of $\mathcal{F}$ with respect to $>$. We denote it by $\overline{\mathrm{sd}}_>(\mathcal{F})$.*

It is clear from the definitions that

$$\overline{\mathrm{sd}}_>(\mathcal{F}) \leq \mathrm{sd}_>(\mathcal{F}), \tag{13}$$

but the inequality might be strict.

Complexity Estimate via the Refined Solving Degree. Let $\mathcal{F} \subset P = k[x_1, \ldots, x_n]$ be a system of m homogeneous polynomials, let $\overline{\mathrm{sd}}_>(\mathcal{F}) \leq d$ for some term order $>$ on P, and let D denote the number of monomials in P of degree $\leq d$. Then the dimensions of the Macaulay matrix $M_{\leq d}$ for $\mathcal{F}$ are bounded by $D \cdot m \times D$. Without loss of generality we can assume that $\mathcal{F}$ does not contain redundant elements, then the row space basis of $M_{\leq d}$ has either at least $m + 1$ elements or it contains a Gröbner basis with $\leq m$ many elements. In the first case, we have to build a new Macaulay matrix whose size is bounded by $D \cdot (m + 1) \times D$. Iterating this argument we can build at most $(D - m)$ many Macaulay matrices, and we have to perform Gaussian elimination at most $D - m$ times. With $D \leq d \cdot \binom{n+d-1}{d}$ and our estimation from Equation (10) we obtain the following worst case complexity estimate

$$\mathcal{O}\left(\sum_{i=0}^{D-m-1} (m+i) \cdot d \cdot \binom{n+d-1}{d}^{\omega}\right) \tag{14}$$

$$\in \mathcal{O}\left(\left(m \cdot D + \frac{(D-m-1) \cdot (D-m-2)}{2}\right) \cdot d \cdot \binom{n+d-1}{d}^{\omega}\right) \tag{15}$$

$$\in \mathcal{O}\left(m \cdot D^2 \cdot d \cdot \binom{n+d-1}{d}^{\omega}\right) \tag{16}$$

$$\in \mathcal{O}\left(m \cdot d^3 \cdot \binom{n+d-1}{d}^{\omega+2}\right). \tag{17}$$

2.5 Approximation of Binomial Coefficients

We recall the following well-known approximation of binomial coefficients.

Lemma 9 ([16, Lemma 17.5.1]). *For $0 < p < 1$, $q = 1 - p$ such that $n \cdot p$ is an integer*

$$\frac{1}{\sqrt{8 \cdot n \cdot p \cdot q}} \leq \binom{n}{n \cdot p} \cdot 2^{-n \cdot H_2(p)} \leq \frac{1}{\sqrt{\pi \cdot n \cdot p \cdot q}}.$$

With $p = \frac{k}{n}$ the inequality then becomes

$$\sqrt{\frac{n}{8 \cdot k \cdot (n-k)}} \leq \binom{n}{k} \cdot 2^{-n \cdot H_2\left(\frac{k}{n}\right)} \leq \sqrt{\frac{n}{\pi \cdot k \cdot (n-k)}}. \tag{18}$$

In case the solving degree is an integer polynomial in the number of variables, then we have the following generic estimation for the binomial coefficient.

Proposition 10. *Let $n \geq 2$ be an integer, let $\alpha \geq 1$, and let $p \in \mathbb{Z}[x]$.*

(1) If $p(n) \geq n - 1$ for all $n \geq 2$, then

$$\left(\frac{n + p(n) - 1}{p(n) \cdot (n-1)} \right)^{\alpha} \leq \frac{2^{\alpha}}{n-1}.$$

(2) If $p(n) \geq 0$ for all $n \geq 2$, then

$$H_2 \left(\frac{p(n)}{n + p(n) - 1} \right) \leq \left(4 \cdot \frac{(n-1) \cdot p(n)}{(n + p(n) - 1)^2} \right)^{\frac{1}{\log(4)}} \leq \left(4 \cdot \frac{p(n)}{n-1} \right)^{\frac{1}{\log(4)}}.$$

In particular if $\alpha \geq 2$ and $p(n) \geq n - 1$ for all $n \geq 2$, then

$$\binom{n + p(n) - 1}{p(n)}^{\alpha} \in \mathcal{O} \left(\frac{1}{n-1} \cdot 2^{\alpha \cdot \left(\frac{4 \cdot (n-1) \cdot p(n)}{\left(n + p(n) - 1 \right)^{2 - \log(4)}} \right)^{\frac{1}{\log(4)}}} \right).$$

Proof. For (1), since $\alpha \geq 1$ and $n \geq 2$ we have that

$$\left(\frac{n + p(n) - 1}{p(n) \cdot (n-1)} \right)^{\alpha} = \left(\frac{1}{p(n)} + \frac{1}{n-1} \right)^{\alpha} \leq \left(\frac{2}{n-1} \right)^{\alpha} \leq \frac{2^{\alpha}}{n-1},$$

which proves the claim.

For (2), let $0 < p < 1$ we recall the following inequality for the binary entropy [39, Theorem 1.2]

$$H_2(p) \leq \left(4 \cdot p \cdot (1 - p) \right)^{\frac{1}{\log(4)}}.$$

Then

$$H_2 \left(\frac{p(n)}{n + p(n) - 1} \right) \leq \left(4 \cdot \frac{(n-1) \cdot p(n)}{(n + p(n) - 1)^2} \right)^{\frac{1}{\log(4)}}.$$

Since $\log(4) \approx 1.3863$ we have that $n - 1 \leq n + p(n) - 1 \Rightarrow (n-1)^{\frac{1}{\log(4)}} \leq (n + p(n) - 1)^{\frac{1}{\log(4)}}$, so the second inequality follows.

The last claim follows from Equation (18) combined with the two inequalities. $\square$

3 Refined Solving Degree & Degree of Regularity

Another measure to estimate the complexity of linear algebra-based Gröbner basis algorithms is the so-called degree of regularity.

Definition 11 (Degree of regularity, [7, Definition 4]). *Let k be a field, and let $\mathcal{F} \subset P = k[x_1, \ldots, x_n]$. Assume that $\left(\mathcal{F}^{\mathrm{top}}\right)_d = P_d$ for some integer $d \geq 0$. The degree of regularity is defined as*

$$d_{\mathrm{reg}}\left(\mathcal{F}\right) = \min\left\{d \geq 0 \mid \left(\mathcal{F}^{\mathrm{top}}\right)_d = P_d\right\}.$$

Note that by Theorem 7 and the projective weak Nullstellensatz [17, Chapter 8 §3 Theorem 8] $\mathcal{F}$ is in generic coordinates if and only if $d_{\mathrm{reg}}(\mathcal{F}) < \infty$.

Let $\mathcal{F} = \{f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n\} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a polynomial system such that $d_{\mathrm{reg}}\left(\mathcal{F}\right) \geq \max\{q, \deg\left(f_1\right), \ldots, \deg\left(f_m\right)\}$, Semaev & Tenti [33, Theorem 2.1] showed that all S-polynomials appearing in Buchberger's algorithm have degree $\leq 2 \cdot d_{\mathrm{reg}}\left(\mathcal{F}\right) - 2$. Due to the requirement $d_{\mathrm{reg}}\left(\mathcal{F}\right) \geq q$ we do not expect that Semaev & Tenti's bound outperforms the Macaulay bound in practice. On the other hand, the inclusion of the field equations was only made to restrict to the $\mathbb{F}_q$-valued solutions of a polynomial system, the proof of [33, Theorem 2.1] only requires that $d_{\mathrm{reg}}\left(\mathcal{F}\right) < \infty$. Moreover, we will see that LWE polynomial systems contain a univariate polynomial $f_i \mid x_i^q - x_i$ for all variables x_i. Hence, LWE polynomial systems can restrict to the $\mathbb{F}_q$-valued solutions with polynomials of much smaller degrees than q. Therefore, we will now generalize [33, Theorem 2.1] to the general case $d_{\mathrm{reg}}\left(\mathcal{F}\right) < \infty$.

Let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset k[x_1, \ldots, x_n]$ be such that $d_{\mathrm{reg}}\left(\mathcal{F}\right) < \infty$. Moreover, let $>$ be a degree compatible term order on $k[x_1, \ldots, x_n]$. In principle, we simply repeat the refined analysis presented in [38, §3.4]:

(1) Compute the Macaulay matrices $M_{\leq d_{\mathrm{reg}}(\mathcal{F})}$ of the sequence $f_1, \ldots, f_m$ with respect to $>$, and put the matrix into row echelon form.
(2) Choose a finite set of generators $(\mathcal{B}) = I$ such that every element of $\mathcal{B}$ has degree $\leq d_{\mathrm{reg}}(\mathcal{F})$, and every monomial in $k[x_1, \ldots, x_n]$ of degree $\geq d_{\mathrm{reg}}(\mathcal{F})$ is divisible by at least one monomial in $\left(\mathrm{LM}_>(\mathcal{B})\right)$. [1] Then we perform Buchberger's algorithm on $\mathcal{B}$ to obtain a Gröbner basis $\mathcal{G}$.
(3) Compute a reduced Gröbner basis of $(\mathcal{F})$ via $\mathcal{G}$.

Let us now collect some properties of the basis $\mathcal{B}$.

Proposition 12. *Let k be a field, let $>$ be a degree compatible term order on $P = k[x_1, \ldots, x_n]$, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P$ be such that $d_{\mathrm{reg}}\left(\mathcal{F}\right) < \infty$. There exists a finite generating set $\mathcal{B}$ for $(\mathcal{F})$ such that*

(1) $\max_{f \in \mathcal{B}} \deg\left(f\right) \leq d_{\mathrm{reg}}\left(\mathcal{F}\right)$.
(2) Every monomial $m \in k[x_1, \ldots, x_n]$ with $\deg\left(m\right) \geq d_{\mathrm{reg}}\left(\mathcal{F}\right)$ is divisible by some $\mathrm{LM}_>(f)$, where $f \in \mathcal{B}$.
(3) For $f \in \mathcal{B}$ with $\deg\left(f\right) = d_{\mathrm{reg}}(\mathcal{F})$ one has $\deg\left(f - \mathrm{LT}_>(f)\right) < d_{\mathrm{reg}}(\mathcal{F})$.

Proof. We abbreviate $d_{\mathrm{reg}}\left(\mathcal{F}\right) = d_{\mathrm{reg}}$. First we construct the Macaulay matrix $M_{\leq d_{\mathrm{reg}}}$ of $\mathcal{F}$ with respect to $>$ and denote with $\mathcal{B}$ basis of the row space of $M_{\leq d_{\mathrm{reg}}}$. By assumption, we have that $d_{\mathrm{reg}} = d_{\mathrm{reg}}\left(\mathcal{B}\right)$.

---

[1] For ease of writing we introduce the shorthand notation: $\mathcal{B} = \{h_1, \ldots, h_r\}$, then $\left(\mathrm{LM}_>(\mathcal{B})\right) = \left(\mathrm{LM}_>(h_1), \ldots, \mathrm{LM}_>(h_m)\right)$.

For $f \in \mathcal{F}$, if $\deg(f) \leq d_{\mathrm{reg}}$, then by construction $f \in (\mathcal{B})_{\leq d_{\mathrm{reg}}}$. If $\deg(f) > d_{\mathrm{reg}}$, then we compute the remainder r_f of f modulo $\mathcal{B}$ with respect to $>$ and add it to $\mathcal{B}$. By elementary properties of multivariate polynomial division, see [17, Chapter 2 §3 Theorem 3], and the degree of regularity we then have that $\deg(r_f) < d_{\mathrm{reg}}$.

Obviously, we have that $(\mathcal{B}) = (\mathcal{F})$ and (1) follows by construction, (2) follows from $d_{\mathrm{reg}} = d_{\mathrm{reg}}(\mathcal{B})$, and lastly basis elements that satisfy (3) can always be constructed with another round of Gaussian elimination on the elements of $\mathcal{B}$ of degree d_{reg}. $\qquad\square$

Now we can prove the generalization of Semaev & Tenti's bound. Also, recall that a term order $>$ on P is called degree compatible if for $f, g \in P$ with $\deg(f) > \deg(f)$ one also has that $f > g$.

Theorem 13. *Let k be a field, let $>$ be a degree compatible term order on $P = k[x_1, \ldots, x_n]$, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset P$ such that $d_{\mathrm{reg}}(\mathcal{F}) < \infty$. If $d_{\mathrm{reg}}(\mathcal{F}) \geq \max\big\{ \deg(f_1), \ldots, \deg(f_m) \big\}$, then*

$$\overline{\mathrm{sd}}_> (\mathcal{F}) \leq 2 \cdot d_{\mathrm{reg}}(\mathcal{F}) - 1.$$

Proof. We abbreviate $d_{\mathrm{reg}}(\mathcal{F}) = d_{\mathrm{reg}}$. Let $\mathcal{B} = \{g_1, \ldots, g_t\}$ be the ideal basis from Proposition 12 for $(\mathcal{F})$. By assumption, we have that $\mathcal{F} \subset (\mathcal{B})_{\leq d_{\mathrm{reg}}}$, and by construction $\mathcal{B} \subset \mathrm{rowsp}\big(M_{d_{\mathrm{reg}}}(\mathcal{F})\big)$. Starting from $\mathcal{B}$ we compute a $>$-Gröbner basis via Buchberger's algorithm, see [17, Chapter 2 §7]. Let $g_i, g_j \in \mathcal{B}$, we consider their $>$-S-polynomial

$$S_>(g_i, g_j) = \frac{x^\gamma}{\mathrm{LM}_>(g_i)} \cdot g_i - \frac{x^\gamma}{\mathrm{LM}_>(g_j)} \cdot g_j,$$

where $x^\gamma = \mathrm{lcm}\big(\mathrm{LM}_>(g_i), \mathrm{LM}_>(g_j)\big)$. Note that by [17, Chapter 2 §9 Proposition 4] we only have to consider the pairs with $\gcd\big(\mathrm{LM}_>(g_i), \mathrm{LM}_>(g_j)\big) \neq 1$. Since $\mathrm{LM}_>(g_i)$ and $\mathrm{LM}_>(g_j)$ must coincide in at least one variable and their degree is $\leq d_{\mathrm{reg}}$ we can conclude that

$$\deg\left(\frac{x^\gamma}{\mathrm{LM}_>(g_i)} \cdot g_i\right), \deg\left(\frac{x^\gamma}{\mathrm{LM}_>(g_j)} \cdot g_j\right) \leq 2 \cdot d_{\mathrm{reg}} - 1.$$

After performing division by remainder of the S-polynomial with respect to $\mathcal{B}$ we then also have that the remainder has degree $< d_{\mathrm{reg}}$ since $\big(\mathrm{LM}_>(\mathcal{B})\big)_d = \big(k[x_1, \ldots, x_n]\big)_d$ for all $d \geq d_{\mathrm{reg}}$. Therefore, we can construct all S-polynomials within Buchberger's algorithm with non-trivial remainder via polynomials whose degree is $\leq 2 \cdot d_{\mathrm{reg}} - 1$. Since Buchberger's algorithm always produces a $>$-Gröbner basis we can conclude that $\overline{\mathrm{sd}}_>(\mathcal{F}) \leq 2 \cdot d_{\mathrm{reg}} - 1$. $\qquad\square$

Corollary 14. *In the scenario of Theorem 13, the largest degree of S-polynomials appearing in Buchberger's algorithm is less than or equal to $2 \cdot d_{\mathrm{reg}}(\mathcal{F}) - 2$.*

Proof. Let us take another look at the S-polynomial

$$S_>(g_i, g_j) = \frac{x^\gamma}{\mathrm{LM}_>(g_i)} \cdot g_i - \frac{x^\gamma}{\mathrm{LM}_>(g_j)} \cdot g_j$$
$$= \frac{x^\gamma}{\mathrm{LM}_>(g_i)} \cdot \tilde{g}_i - \frac{x^\gamma}{\mathrm{LM}_>(g_j)} \cdot \tilde{g}_j,$$

where $x^\gamma = \mathrm{lcm}\left(\mathrm{LM}_>(g_i), \mathrm{LM}_>(g_j)\right)$ and $\tilde{g}_l = g_l - \mathrm{LM}_>(g_l)$ for $l = i, j$. Since the leading monomials are not coprime we have that

$$\deg\left(\frac{x^\gamma}{\mathrm{LM}_>(g_i)}\right), \deg\left(\frac{x^\gamma}{\mathrm{LM}_>(g_j)}\right) \leq d_{\mathrm{reg}} - 1.$$

Moreover, by Proposition 12 we have that $\deg(\tilde{g}_i), \deg(\tilde{g}_j) < d_{\mathrm{reg}}$. $\qquad\square$

4 Affinely Derived Polynomial Systems

LWE polynomial systems follow a very special structure. To construct one polynomial one starts with a univariate polynomial f and then substitutes a multivariate affine equation $\langle \mathbf{a}, \mathbf{x} \rangle + b$ into f. Many properties of LWE polynomial systems solely stem from this substitution, this motivates the following definition.

Definition 15 (Affinely derived polynomial systems). *Let k be a field, let $n, m \geq 1$ be integers, let $g_1, \ldots, g_m \in k[x]$ be non-constant polynomials, let $\mathbf{a}_1, \ldots, \mathbf{a}_m \in k^n$, and let $b_1, \ldots, b_m \in k$. In the polynomial ring $k[x_1, \ldots, x_n]$, we call*

$$g_1\left(\mathbf{a}_1^\mathsf{T}\mathbf{x} + b_1\right) = 0,$$
$$\ldots$$
$$g_m\left(\mathbf{a}_m^\mathsf{T}\mathbf{x} + b_m\right) = 0,$$

where $\mathbf{x} = (x_1, \ldots, x_n)^\mathsf{T}$, the affinely derived polynomial system of $g_1, \ldots, g_m$ by $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_m, b_m)$. We also abbreviate affinely derived polynomial systems as tuple $\left((g_1, \mathbf{a}_1, b_1), \ldots, (g_m, \mathbf{a}_m, b_m)\right)$.

Next let us collect some properties of zero-dimensional affinely derived polynomial systems.

Theorem 16. *Let k be a field and let $\bar{k}$ be its algebraic closure, let $n \geq 1$ be an integer, and let $\mathcal{F} = \left((g_1, \mathbf{a}_1, b_1), \ldots, (g_n, \mathbf{a}_n, b_n)\right) \subset k[x_1, \ldots, x_n]$ be an affinely derived polynomial system. Assume that the matrix*

$$\mathbf{A} = \left(\mathbf{a}_1 \ldots \mathbf{a}_n\right)^\mathsf{T} \in k^{n \times n}$$

has rank n. Then

(1) *LEX and DRL Gröbner bases of $\mathcal{F}$ can be computed via an affine transformation.*
(2) $\mathcal{F}$ *is a 0-dimensional polynomial system.*
(3) $\dim_k \left(k[x_1, \ldots, x_n]/(\mathcal{F}) \right) = \prod_{i=1}^n \deg(g)_i.$
(4) *Let $\mathcal{G} \subset \bar{k}[x_1, \ldots, x_n]$ be such that $\mathcal{F} \subset \mathcal{G}$ and $(\mathcal{G}) \neq (1)$. Then $\mathcal{G}^{\mathrm{hom}}$ is in generic coordinates.*

If in addition k is a finite field with q elements, and $g_i \mid x^q - x$ for all $1 \leq i \leq n$. Then

(5) *Any ideal $I \subset k[x_1, \ldots, x_n]$ such that $\mathcal{F} \subset I$ is radical.*

Proof. For (1), we define new variables via

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \left(\mathbf{a}_1 \ \ldots \ \mathbf{a}_n \right)^{\intercal} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

and since the matrix $\mathbf{A}$ has full rank this construction is invertible. Then the polynomial system is of the form $g_1(y_1) = \ldots = g_n(y_n) = 0$, so under any LEX and DRL term order the leading monomials of the polynomials are pairwise coprime, so by [17, Chapter 2 §9 Theorem 3, Proposition 4] we have found a Gröbner basis.

For (2), follows from [17, Chapter 5 §3 Theorem 6].

For (3), the quotient space dimension can be computed by counting the number of monomials not contained in $\left(y_1^{\deg(g_1)}, \ldots, y_n^{\deg(g_n)} \right)$.

For (4), follows from Theorem 7.

For (5), let $F = (x_1^q - x_1, \ldots, x_n^q - x_n) \subset k[x_1, \ldots, x_n]$ be the ideal of field equations. It is well-known that for any ideal $I \subset k[x_1, \ldots, x_n]$ the ideal $I + F$ is radical, see for example [25, Lemma 3.1.1]. Since $g_i \mid x^q - x$ we have for all $1 \leq i \leq n$ that

$$(\mathbf{a}_1^{\intercal} \mathbf{x} + c_1)^q - (\mathbf{a}_1^{\intercal} \mathbf{x} + c_1) = (\mathbf{a}_1^{\intercal} \mathbf{x})^q - (\mathbf{a}_1^{\intercal} \mathbf{x})$$

$$= \sum_{i=1}^n a_i \cdot (x_i^q - x_i) = \mathbf{a}_i^{\intercal} \begin{pmatrix} x_1^q - x_1 \\ \vdots \\ x_n^q - x_1 \end{pmatrix} \in (\mathcal{F}).$$

So by invertibility $\mathbf{A}$ we have that $x_i^q - x_i \in (\mathcal{F})$ for all $1 \leq i \leq n$ which proves the claim. $\qquad\square$

Remark 17. Note that being in generic coordinates also follows from [12, Remark 13].

Corollary 18. *Let k be an algebraically closed field, let $m > n \geq 1$, let $\mathcal{F} = \left(\left(g_1, \mathbf{a}_1, b_1 \right), \ldots, \left(g_m, \mathbf{a}_m, b_m \right) \right) \subset k[x_1, \ldots, x_n]$ be an affinely derived polynomial system such that $\deg(g_1) \geq \ldots \geq \deg(g_m)$. Assume that the matrix*

$$\mathbf{A} = \left(\mathbf{a}_1 \ \ldots \ \mathbf{a}_m \right)^{\intercal} \in k^{m \times n}$$

13

has rank n. Then

$$\text{sd}_{DRL}(\mathcal{F}) \leq \sum_{i=1}^{n+1} (\deg(g_i) - 1) + 1.$$

In particular if $d \geq \deg(g_1)$, then

$$\text{sd}_{DRL}(\mathcal{F}) \leq (n+1) \cdot (d-1) + 1$$

Proof. Follows from Theorem 16 and the Macaulay bound Corollary 6. □

4.1 LWE Polynomial Systems

Arora & Ge proposed a noise-free polynomial system to solve the Search-LWE problem [6]. If the error is distributed via a Gaussian distribution $\mathcal{N}(0, \sigma)$, then one assumes that the error always falls in the range $[-t \cdot \sigma, t \cdot \sigma]$ for some $t \in \mathbb{Z}$ such that $d = 2 \cdot t + 1 < q$. As we saw in Equation (7), the probability of falling outside this interval decreases exponentially in t. Therefore, up to some probability, in $\mathbb{F}_q$ the error is then always a root of the polynomial

$$f(x) = x \cdot \prod_{i=1}^{t} (x+i) \cdot (x-i) \in \mathbb{F}_q[x]. \tag{19}$$

Since by construction $2 \cdot t + 1 < q$ there cannot exist $1 \leq i < j \leq t$ such that $i \equiv -j \mod q$. So f is a square-free polynomial and therefore divides the field equation $x^q - x$. For LWE samples $(\mathbf{a}_i, c_i) = (\mathbf{a}_i, \mathbf{a}_i^\mathsf{T} \mathbf{s} + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ one then has that in $\mathbb{F}_q[x_1, \dots, x_n]$

$$f(c_i - \mathbf{a}_i^\mathsf{T} \mathbf{x}) = 0 \tag{20}$$

with probability $\geq 1 - \frac{2}{t \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{t^2}{2}\right)$. Given m LWE samples one then constructs m polynomials of the form of Equation (20), we call this polynomial system the LWE polynomial system $\mathcal{F}_{\text{LWE}}$. Obviously, the LWE polynomial system is an affinely derived polynomial system. The failure probability, i.e. the probability that at least one error term does not lie in the interval $[-t \cdot \sigma, t \cdot \sigma]$, can be estimated via the union bound

$$p_{fail} = m \cdot \mathbb{P}\left[|X| > t \cdot \sigma\right] \leq m \cdot \frac{2}{t \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{t^2}{2}\right). \tag{21}$$

Moreover, by Theorem 16 for the polynomial system to be fully determined we have to require that $m \geq n$ and that n sample vectors are linearly independent.

To devise the complexity of Gröbner basis computations we in principle follow the strategy of [3, §5]. We assume that $\sigma = n^\epsilon$, where $0 \leq \epsilon \leq 1$, and let θ be such that $0 \leq \theta \leq \epsilon \leq 1$. We consider sample numbers of the following form

$$m_{\text{GB}} = e^{\gamma_\theta}, \tag{22}$$

where $\gamma_\theta = 2^{2 \cdot (\epsilon - \theta)}$.

Lemma 19 ([3, Lemma 5]). *Let q, n, σ be parameters of an LWE instance. Let $(\mathbf{a}_1, b_1), \ldots, (\mathbf{a}_m, b_m)$ be elements of $\mathbb{Z}_q^n \times \mathbb{Z}$ sampled according to LWE. If $t = \sqrt{2 \cdot \log(m)}$, then the LWE polynomial system vanishes with probability at least*

$$p_g = 1 - \sqrt{\frac{1}{\pi \cdot \log(m)}}.$$

By [3, Remark 1] $m \in \mathcal{O}(n)$ implies that $p_g \in 1 - o(1)$.

Therefore, we can deduce the degree D_{GB} required for $m_{\mathrm{GB}} = e^{\gamma_\theta}$ equations in the LWE polynomial system. By the previous lemma, we have to fix $t_{\mathrm{GB}} = \sqrt{2 \cdot \log(m_{\mathrm{GB}})} = \sqrt{2 \cdot \gamma_\theta}$, so

$$
\begin{aligned}
D_{\mathrm{GB}} &= 2 \cdot \sqrt{2 \cdot \log(m_{\mathrm{GB}})} \cdot \sigma + 1 \\
&\in \mathcal{O}\left(\sqrt{\log(m_{\mathrm{GB}}) \cdot \sigma}\right) = \mathcal{O}\left(\sqrt{\gamma_\theta} \cdot \sigma\right) = \mathcal{O}\left(n^{2 \cdot \epsilon - \theta}\right) = \mathcal{O}\left(\gamma_\theta \cdot n^\theta\right).
\end{aligned}
\tag{23}
$$

Theorem 20. *Let $q, n \geq 2, \sigma = \sqrt{\frac{n}{2 \cdot \pi}}$ be parameters of an LWE instance. Let $m_{GB} = e^{\frac{\pi \cdot n}{4}}$, and let $(\mathbf{a}_i, b_i)_{1 \leq i \leq m_{GB}}$ be elements of $\mathbb{F}_q^n \times \mathbb{F}_q$ sampled according to LWE. If the matrix $\mathbf{A} = \left(\mathbf{a}_1 \ldots \mathbf{a}_m\right)^\mathsf{T}$ has rank n, then a linear algebra-based Gröbner basis algorithm that computes a DRL Gröbner basis has time complexity*

$$\mathcal{O}\left(n \cdot 2^{\omega \cdot 2^{\frac{1}{\log(2)}} \cdot n^{2 - \frac{1}{\log(4)}} + \frac{\pi \cdot \log_2(e)}{4} \cdot n}\right)$$

and memory complexity

$$\mathcal{O}\left(n \cdot 2^{2^{1 + \frac{1}{\log(2)}} \cdot n^{2 - \frac{1}{\log(4)}} + \frac{\pi \cdot \log_2(e)}{4} \cdot n}\right).$$

The algorithm has success probability $\geq 1 - \frac{2}{\pi \cdot \sqrt{n}}$.

Proof. As in Lemma 19 let $t = \sqrt{2 \cdot \log(m_{\mathrm{GB}})}$. By our assumptions and Equation (23) we have that

$$D_{\mathrm{GB}} = 2 \cdot \sqrt{2 \cdot \log(m_{\mathrm{GB}})} \cdot \sigma + 1 = 2 \cdot \sqrt{2 \cdot \frac{\pi \cdot n}{4}} \cdot \sqrt{\frac{n}{2 \cdot \pi}} + 1 = n + 1.$$

Since the matrix $\mathbf{A}$ has full rank we can apply Corollary 18 to estimate the solving degree of the LWE polynomial system

$$\mathrm{sd}_{DRL}\left(\mathcal{F}_{\mathrm{LWE}}\right) \leq (n + 1) \cdot (D_{\mathrm{GB}} - 1) + 1 = n^2 + n + 1.$$

Now we apply Proposition 10 with $p(n) = n^2 + n + 1$, then we perform the additional estimations

$$n^3 - 1 < n^3,$$
$$\left(n^2\right)^{2 - \log(4)} \leq \left(n^2 + 2 \cdot n\right)^{2 - \log(4)},$$

for all $n \geq 1$. Also note that $2 - \log(4) \approx 0.6137$, so we can divide by the expressions in the last inequality without affecting the sign. Therefore,

$$\left(n + p(n) - 1\right) \cdot H_2 \left(\frac{p(n)}{n + p(n) - 1}\right) \leq 2^{\frac{1}{\log(2)}} \cdot n^{2 - \frac{1}{\log(4)}}.$$

The final claim then follows by converting m_{GB} into base 2. $\square$

Numerically we have that $2 - \frac{1}{\log(4)} \approx 1.2787$.

4.2 LWE With Small Errors

Suppose that the LWE error distribution χ can only take values in $\mathcal{E} \subset \mathbb{F}_q$ with $|\mathcal{E}| = D \ll \sqrt{n}$. Then the error polynomial is

$$f(x) = \prod_{e \in \mathcal{E}} (x - e) \tag{24}$$

of degree D. Moreover, for any LWE sample $(\mathbf{a}, b)$ we have $f(b - \mathbf{a}^\intercal \mathbf{x}) = 0$ with probability 1. Analog to Theorem 20 we can estimate the complexity of a DRL Gröbner basis computation.

Theorem 21. *Let q be a prime, and let $m > n \geq 2$ be integers. Let $(\mathbf{a}_i, b_i)_{1 \leq i \leq m}$ be elements of $\mathbb{F}_q^n \times \mathbb{F}_q$ sampled according to a LWE distribution $A_{\mathbf{s}, \chi}$ such that the error distribution that χ can take at most D values. If the matrix $\mathbf{A} = \left(\mathbf{a}_1 \ldots \mathbf{a}_m\right)^\intercal$ has rank n, then a linear algebra-based Gröbner basis algorithm that computes a DRL Gröbner basis has time complexity*

$$\mathcal{O}\left(m \cdot (D - 1) \cdot n \cdot 2^{\omega \cdot \left(8 \cdot D^{\log(4) - 1}\right)^{\frac{1}{\log(4)}} \cdot n}\right)$$

and memory complexity

$$\mathcal{O}\left(m \cdot (D - 1) \cdot n \cdot 2^{2 \cdot \left(8 \cdot D^{\log(4) - 1}\right)^{\frac{1}{\log(4)}} \cdot n}\right).$$

Proof. The LWE polynomial has degree D, therefore by Corollary 18

$$\mathrm{sd}_{DRL}(\mathcal{F}_{\mathrm{LWE}}) \leq (n + 1) \cdot (D - 1) + 1.$$

We apply Proposition 10 with $p(n) = (n + 1) \cdot (D - 1) + 1$ and do the estimations

$$\frac{(n + 1) \cdot (D - 1) + 1}{n - 1} = \frac{(n - 1) \cdot (D - 1) + 2 \cdot D - 1}{n - 1} \in \mathcal{O}(1),$$

for all $n \geq 2$,

$$\left((n + 1) \cdot (D - 1) + 1\right) \cdot (n - 1) = \left(n^2 - 1\right) \cdot (D - 1) + n - 1 \leq 2 \cdot n^2 \cdot D,$$
$$(n \cdot D)^{2 - \log(4)} \leq (n \cdot D + D - 1)^{2 - \log(4)},$$

for all $n \geq 1$. $\square$

4.3 LWE With Small Secrets

Suppose that the entries of the secret $\mathbf{s}$ of a LWE distribution $A_{\mathbf{s},\chi}$ can only take values in $\mathcal{S} \subset \mathbb{F}_q$ with $|\mathcal{S}| = D$. Then for $1 \leq i \leq n$ we can add the equations

$$f_i(x_i) = \prod_{s \in \mathcal{S}}(x_i - s) \tag{25}$$

to the LWE polynomial system. Trivially, $f_1, \ldots, f_n$ is a DRL Gröbner basis, so the monomials $g \notin \text{in}_{DRL}(f_1, \ldots, f_n)$ have degree $\leq n \cdot (D - 1)$. Moreover, any univariate polynomial is trivially affinely derived.

Theorem 22. *Let q be a prime, and let $m > n \geq 2$ be integers. Let $(\mathbf{a}_i, b_i)_{1 \leq i \leq m}$ be elements of $\mathbb{Z}_q^n \times \mathbb{Z}_q$ sampled according to a LWE distribution $A_{\mathbf{s},\chi}$ such that the components of the secret can only take values in a set of size D. If the matrix $\mathbf{A} = \begin{pmatrix} \mathbf{a}_1 & \ldots & \mathbf{a}_m \end{pmatrix}^{\mathsf{T}}$ has rank n and the error polynomial f has $\deg(f) > D$, then a linear algebra-based Gröbner basis algorithm that computes a DRL Gröbner basis has time complexity*

$$\mathcal{O}\left(m \cdot (D-1) \cdot n^2 \cdot 2^{\omega \cdot 2^{\frac{1}{\log(2)}} \cdot (D-1)^{1 - \frac{1}{\log(4)}} \cdot n^{2 - \frac{1}{\log(4)}}}\right)$$

and memory complexity

$$\mathcal{O}\left(m \cdot (D-1)^2 \cdot n^3 \cdot 2^{2^{1 + \frac{1}{\log(2)}} \cdot (D-1)^{1 - \frac{1}{\log(4)}} \cdot n^{2 - \frac{1}{\log(4)}}}\right).$$

Proof. Let $\mathcal{F}_{\text{LWE}}$ be the affinely derived LWE polynomial system, and let $\mathcal{F}_{\mathcal{S}}$ be the polynomials that have all possible values of the secret components as zeros, see Equation (25). As preprocessing we compute the remainder of all polynomials in $\mathcal{F}_{\text{LWE}}$ with respect to $\mathcal{F}_{\mathcal{S}}$ and DRL, then the remainder polynomials can at most have degree $n \cdot (D - 1)$, see [17, Chapter 2 §6 Proposition 1]. Now we join the remainders and $\mathcal{F}_{\mathcal{S}}$ in a single system $\mathcal{F}$ and start the Gröbner basis computation. By Theorem 7 this polynomial system is in generic coordinates, therefore

$$\text{sd}_{DRL}(\mathcal{F}) \leq (n+1) \cdot \big(n \cdot (D-1) - 1\big) + 1.$$

Now we apply Proposition 10 with $p(n) = (n+1) \cdot n \cdot (D-1) + 1$ and perform the additional estimations

$$\frac{(n+1) \cdot \big(n \cdot (D-1) - 1\big) + 1}{n - 1} \leq \frac{(D-1) \cdot (n+1)^2}{n - 1} \in \mathcal{O}\left((D-1) \cdot n\right)$$

for all $n \geq 2$, and

$$\big((n+1) \cdot n \cdot (D-1) + 1\big) \cdot (n - 1) \leq n^3 \cdot (D-1),$$
$$n^2 \cdot (D-1) \leq n + (n+1) \cdot n \cdot (D-1),$$

for all $n \geq 1$. Then

$$\frac{n^3 \cdot (D-1)}{\big(n^2 \cdot (D-1)\big)^{2 - \log(4)}} = n^{2 \cdot \log(4) - 1} \cdot (D-1)^{\log(4) - 1}$$

which proves the claim. $\qquad\square$

LWE With Small Secrets & Small Errors. Lastly, let us shortly analyze the case of small secret small error LWE. Suppose that the errors are drawn from a set of size $D_{\mathcal{E}}$ and that the secrets are drawn from a set of size $D_{\mathcal{S}}$. As for Theorem 22 we can compute the DRL remainder of the LWE polynomials with respect to the n univariate polynomials limiting the possible solutions for the secret.

- If $D_{\mathcal{E}} \gg D_{\mathcal{S}}$, then we can estimate the degrees of the remainders as $\leq n \cdot (D_{\mathcal{S}} - 1)$, then we obtain the Macaulay bound

$$\mathrm{sd}_{DRL}(\mathcal{F}) \leq (n+1) \cdot n \cdot (D_{\mathcal{S}} - 1) + 1. \tag{26}$$

- If $n \cdot (D_{\mathcal{S}} - 1) \gg D_{\mathcal{E}} \geq D_{\mathcal{S}}$, then we can always estimate the degrees of the remainders as $\leq D_{\mathcal{E}}$, then

$$\mathrm{sd}_{DRL}(\mathcal{F}) \leq (n+1) \cdot (D_{\mathcal{E}} - 1) + 1. \tag{27}$$

- If $n \cdot (D_{\mathcal{S}} - 1) \gg D_{\mathcal{S}} > D_{\mathcal{E}}$, then we perform a variable transformation so that the LWE polynomials $\mathcal{F}_{\mathrm{LWE}}$ include n univariate polynomials, i.e. we exchange the roles of $\mathcal{F}_{\mathcal{S}}$ and $\mathcal{F}_{\mathrm{LWE}}$. The degrees of the remainders of $\mathcal{F}_{\mathcal{S}}$ are then bounded by $\leq D_{\mathcal{S}}$, and we obtain

$$\mathrm{sd}_{DRL}(\mathcal{F}) \leq n \cdot (D_{\mathcal{S}} - 1) + D_{\mathcal{E}}. \tag{28}$$

So the first case reduces to Theorem 22 and the second and the third one to Theorem 21, though the third case has a different constant term in the solving degree bound than small error LWE.

5 Sub-Exponential Complexity Estimates via the Refined Solving Degree

In this section we use Theorem 13 to show that in an ideal scenario general LWE, binary secret LWE and binary error LWE admit sub-exponential Gröbner basis algorithms.

5.1 LWE With Exponential Many Samples

For general LWE the lowest achievable degree of regularity is the degree D of the error polynomial. In that degree there exist $\binom{n+D-1}{D}$ many monomials, hence to achieve degree of regularity m the number of samples m has to be at least the aforementioned binomial coefficient.

Theorem 23. *Let q, n, σ be parameters of an LWE instance, and let $D = 2 \cdot t \cdot \sigma + 1$ be the degree of the LWE polynomial. Let $m \in \mathcal{O}\left(\binom{n+D-1}{D}\right)$ be such that $d_{\mathrm{reg}}\left(\mathcal{F}_{LWE}^{\mathrm{top}}\right) = D$. Then a linear algebra-based Gröbner basis algorithm that computes a DRL Gröbner basis has time complexity*

$$\mathcal{O}\left(D^3 \cdot 2^{(\omega+3) \cdot 2^{\frac{1}{\log(2)}} \cdot (2 \cdot D - 1)^{\frac{1}{\log(4)}} \cdot (n-1)^{1 - \frac{1}{\log(4)}}}\right)$$

18

and memory complexity

$$\mathcal{O}\left(D^3 \cdot 2^{5 \cdot 2^{\frac{1}{\log(2)}} \cdot (2 \cdot D - 1)^{\frac{1}{\log(4)}} \cdot (n-1)^{1 - \frac{1}{\log(4)}}}\right).$$

For $t \to \infty$ the success probability of the algorithm approaches 1.

Proof. We can use Theorem 13 and Equation (17) to estimate the complexity of a linear algebra based Gröbner basis algorithm. Then

$$\mathcal{O}\left(m \cdot (2 \cdot D - 1)^3 \cdot \binom{n + 2 \cdot D - 2}{2 \cdot D - 1}^{\omega+2}\right) \in \mathcal{O}\left(D^3 \cdot \binom{n + 2 \cdot D - 2}{2 \cdot D - 1}^{\omega+3}\right).$$

To estimate the binomial coefficient we use Equation (18) and [39, Theorem 1.2]. Similar to Proposition 10, the term in the square root is estimated by $\mathcal{O}(1)$. For the entropy term we have that

$$(n + 2 \cdot D - 2) \cdot H_2\left(\frac{2 \cdot D - 1}{n + 2 \cdot D - 2}\right) \leq \left(4 \cdot \frac{(2 \cdot D - 1) \cdot (n - 1)}{(n + 2 \cdot D - 2)^{2 - \log(4)}}\right)^{\frac{1}{\log(4)}}.$$

Without loss of generality $D \geq 1$, so $n - 1 \leq n + 2 \cdot D - 2$ which implies the complexity claim.

For the success probability, recall that by Equation (21)

$$
\begin{aligned}
p_{fail} &\in \mathcal{O}\left(m \cdot \frac{2}{t \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{t^2}{2}\right)\right) \\
&\in \mathcal{O}\left(\binom{n + D - 1}{D} \cdot \frac{2}{t \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{t^2}{2}\right)\right) \\
&\in \mathcal{O}\left(\sqrt{\frac{n + D - 1}{D \cdot (n - 1)}} \cdot 2^{2 \cdot \sqrt{D \cdot n}} \cdot \frac{2}{t \cdot \sqrt{2 \cdot \pi}} \cdot \exp\left(-\frac{t^2}{2}\right)\right) \\
&\in \mathcal{O}\left(\exp\left(2 \cdot \log(2) \cdot \sqrt{2 \cdot t \cdot \sigma \cdot n} - \frac{t^2}{2}\right)\right),
\end{aligned}
$$

which proves the claim. □

In particular, for $\sigma = \sqrt{n}$ and $t = \frac{k}{\sqrt{\sigma}}$, where $k \in \mathbb{Z}$ we obtain the complexity estimate

$$\mathcal{O}\left(\left(k \cdot \sqrt{n}\right)^3 \cdot 2^{(\omega+3) \cdot 2^{\frac{1}{\log(2)}} \cdot (4 \cdot k + 1)^{\frac{1}{\log(4)}} \cdot n^{1 - \frac{1}{2 \cdot \log(4)}}}\right). \tag{29}$$

Since $1 - \frac{1}{2 \cdot \log(4)} \approx 0.6393$ this complexity estimate is sub-exponential.

5.2 Sub-Exponential Complexity for Binary Secret LWE

Recall the binary secret LWE is the simplest case of small secret LWE, see Section 4.3. Let $F = (x_1^2 - x_1, \ldots, x_n^2 - x_n)$, and let $\mathcal{F}_{\text{LWE}} = \{f_1, \ldots, f_m\}$

be a binary secret LWE polynomial system where the (univariate) LWE error polynomial is of degree D. Without loss of generality we can first reduce the polynomials in $\mathcal{F}_{\mathrm{LWE}}$ modulo F with respect to the DRL term order. Let $f \in \mathcal{F}_{\mathrm{LWE}}$, after the preprocessing step only monomials of the form

$$m = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \tag{30}$$

where $\alpha_i \in \{0, 1\}$ for all i, are present in f and by elementary properties of multivariate polynomial division, see [17, Chapter 2 §3] also $\deg(f) \leq D$ after the reduction.

Suppose that all $f \in \mathcal{F}_{\mathrm{LWE}}$ are of degree D after the reduction, we want to find the minimal achievable degree of regularity $d_{\mathrm{reg}}\big((\mathcal{F}_{\mathrm{LWE}}) + F\big)$. Let $g \in P = \mathbb{F}_q[x_1, \ldots, x_n]$ be a monomial such that $x_i^2 \mid g$ for some i. Such a monomial can always be generated by some element in F^{top}, therefore we only have to consider monomials as in Equation (30). Necessarily, these monomials must be generated by the elements in $\mathcal{F}_{\mathrm{LWE}}^{\mathrm{top}}$. Moreover, by elementary combinatorics there exist $\binom{n}{d}$ many monomials of the form of Equation (30) in degree d.

To compute $d_{\mathrm{reg}}\big((\mathcal{F}_{\mathrm{LWE}}) + F\big)$ one iterates through:

(1) Let $d = 0$, and $\mathcal{G} = \left(\mathcal{F}_{\mathrm{LWE}}^{\mathrm{top}}\right)$.
(2) Perform Gaussian elimination on $\mathcal{G}$ to obtain a minimal generating set. If $|\mathcal{G}| = \binom{n}{D+d}$ return $D + d$, else set $d = d + 1$.
(3) Compute $\mathcal{G} = \sum_{i=1}^{n} x_i \cdot (\mathcal{G}) \mod (x_1^2, \ldots, x_n^2)$, and return to step (2).

In order to achieve $d_{\mathrm{reg}}\big((\mathcal{F}_{\mathrm{LWE}}) + F\big) \leq D + d$, for some $d \geq 0$, we must require that

$$m \cdot \binom{n}{d} \overset{!}{\geq} \binom{n}{D+d} \tag{31}$$

$$\Leftrightarrow m \overset{!}{\geq} \frac{\binom{n}{D+d}}{\binom{n}{d}} = \prod_{i=1}^{D} \frac{n - d - i + 1}{d + i}. \tag{32}$$

I.e., $m \in \mathcal{O}\left(n^D\right)$ many samples can be sufficient to achieve $d_{\mathrm{reg}}\big((\mathcal{F}_{\mathrm{LWE}}) + F\big) \leq D + 1$.

Provided that $m \in \mathcal{O}\left(n^D\right)$ and $d_{\mathrm{reg}}(\mathcal{F}_{\mathrm{LWE}}) \leq D + 1$, then we obtain analog to Theorem 23 the following complexity estimate

$$\mathcal{O}\left(n^D \cdot D^3 \cdot 2^{(\omega+2) \cdot 2^{\frac{1}{\log(2)}} \cdot (2 \cdot D + 1)^{\frac{1}{\log(4)}} \cdot (n-1)^{1 - \frac{1}{\log(4)}}}\right). \tag{33}$$

If $D = 2 \cdot t \cdot \sigma + 1$ and $\sigma = \sqrt{n}$, then we can further estimate $2 \cdot D + 1 \in \mathcal{O}\left(\sqrt{n}\right)$. In particular, the exponent of n then becomes

$$\frac{1}{2 \cdot \log(4)} + 1 - \frac{1}{\log(4)} = 1 - \frac{1}{2 \cdot \log(4)} \approx 0.6393, \tag{34}$$

so the complexity estimate is indeed sub-exponential.

5.3 Polynomial Complexity for Binary Error LWE

Recall that binary error LWE is the simplest case of small error LWE, see Section 4.2. Every polynomial has degree 2. Analog to Theorem 21, we first pick n linearly independent samples $(\mathbf{a}_i, b_i)$ and perform a coordinate transformation. So without loss of generality we can assume that $\mathbf{a}_i$ is the ith standard basis vector of $\mathbb{F}_q^n$. After the transformation these n LWE equations become $x_i^2 - x_i = 0$. We allocate them in the ideal $F = (x_1^2 - x_1, \ldots, x_n^2 - x_n)$, the remaining $m - n$ LWE polynomials we collect in $\mathcal{F}_{\text{LWE}}$. Therefore, we can interpret binary error LWE as special case of binary secret LWE, see Section 5.2. Suppose that we want to achieve $d_{\text{reg}}\big((\mathcal{F}_{\text{LWE}}) + F\big) \leq 2 + d$ for some $d \geq 0$, then by Equation (32)

$$m - n \overset{!}{\geq} \frac{(n - d - 1) \cdot (n - d)}{(d + 1) \cdot (d + 2)} \tag{35}$$

many LWE samples are necessary. In particular, for $d = 0$ this reduces to Arora & Ge's analysis [6]. Analog to Theorem 23 and Equation (33), for $m \in \mathcal{O}\left(n^2\right)$ we then obtain the complexity estimate

$$\mathcal{O}\left(n^2 \cdot d^3 \cdot \binom{n + 2 \cdot d + 2}{2 \cdot d + 3}^{\omega + 2}\right) \in \mathcal{O}\left(d^3 \cdot n^{(\omega + 2) \cdot (2 \cdot d + 3) + 2}\right). \tag{36}$$

It is easy to see from Equation (35) that the higher the value of d the fewer samples are necessary to achieve a certain degree of regularity. Let us see an example.

Example 24. Let q be a prime, and let $n = 256$, and

(1) Let $m = 2 \cdot n$. The minimum $d \in \mathbb{Z}_{\geq 0}$ such that Equation (35) is satisfied is $d = 14$. Analog to Equation (36) with $m = 2 \cdot n$ we yield the complexity of a DRL Gröbner basis computation

$$\mathcal{O}\left(2 \cdot n \cdot d^3 \cdot \binom{n + 30}{31}^{\omega + 2}\right) \in \mathcal{O}\left(n^{31 \cdot \omega + 64}\right).$$

If we use $\omega \leq 3$, then direct evaluation of the left complexity yields 434 bits.

(2) Let $m = n^{\frac{3}{2}}$. The minimum $d \in \mathbb{Z}_{\geq 0}$ such that Equation (35) is satisfied is $d = 3$. Then we yield the complexity of a DRL Gröbner basis computation

$$\mathcal{O}\left(n^{\frac{3}{2}} \cdot d^3 \cdot \binom{n + 8}{9}^{\omega + 2}\right) \in \mathcal{O}\left(n^{9 \cdot \omega + 19.5}\right).$$

If we use $\omega \leq 3$, then direct evaluation of the left complexity yields 178 bits.

5.4 A Conjecture on the Castelnuovo-Mumford Regularity

Experimentally we observed the following property for all LWE polynomial systems studied in this paper.

Conjecture 25. *Let $\mathbb{F}_q$ be a finite field, and let $\mathcal{F}_{LWE} \subset \mathbb{F}_q[x_1, \ldots, x_n]$ be a LWE polynomial system.*

(1) For small secret LWE where the error is drawn from the interval $[-N, N]$

$$\mathrm{reg}\left(\mathcal{F}_{LWE}^{\mathrm{hom}}\right) \leq d_{\mathrm{reg}}\left(\mathcal{F}_{LWE}\right) + N - 1.$$

(2) For binary secret or binary error LWE

$$\mathrm{reg}\left(\mathcal{F}_{LWE}^{\mathrm{hom}}\right) \leq d_{\mathrm{reg}}\left(\mathcal{F}_{LWE}\right) + 1.$$

In case the conjecture holds, then the complexity estimates discussed in this section improve significantly since we can utilize the complexity estimate for Gaussian elimination on a *single* Macaulay matrix (Equation (10)).

– The binary error LWE estimate from Equation (33) improves to

$$\mathcal{O}\left(n^D \cdot D \cdot 2^{\omega \cdot 2^{\frac{1}{\log(2)}} \cdot (D+2)^{\frac{1}{\log(4)}} \cdot (n-1)^{1-\frac{1}{\log(4)}}}\right). \tag{37}$$

– The binary secret LWE estimate from Equation (36) improves to

$$\mathcal{O}\left(d \cdot n^{\omega \cdot (d+3)+2}\right). \tag{38}$$

E.g., under the conjecture the numeric complexities of Example 24 improve to 279 bits and 96 bits respectively.

We also note that for the conservative cryptanalyst there is a non-hypothetical alternative to Conjecture 25. By [14, Theorem 5.3] for a polynomial system $\mathcal{F}^{\mathrm{hom}} \subset P[x_0]$ in generic coordinates one always has that

$$d_{\mathrm{reg}}\left(\mathcal{F}\right) \leq \mathrm{reg}\left(\mathcal{F}^{\mathrm{hom}}\right). \tag{39}$$

Thus, one can estimate the lowest achievable complexity estimate for Gaussian elimination on the Macaulay matrix to produce a Gröbner basis of $\mathcal{F}_{\mathrm{LWE}}$ as follows:

(1) Compute/Estimate the lowest achievable degree of regularity $\hat{d}$ for $\mathcal{F}_{\mathrm{LWE}}$.
(2) Use Equation (10) with $d = \hat{d}$ and $\omega = 2$ to estimate the lowest achievable complexity upper bound of a Gröbner basis computation for $\mathcal{F}_{\mathrm{LWE}}$.

We also recommend utilizing Equation (10) itself for numerical computations rather than our complexity estimations. Our estimations are not tight but merely showcase the complexity class, i.e. exponential, sub-exponential & polynomial, for various LWE Gröbner basis computations.

5.5 Complexity Estimation of Kyber768

Finally, let us showcase our complexity estimation methods for a concrete cryptographic example: Kyber768 [32], a selected algorithm in the NIST post-quantum competition. Kyber768 is based on the Module-LWE problem, it has parameters $q = 3329$, $n = 3 \cdot 256$, $m = n$, $D = 2$ and errors as well as secrets are drawn from the interval $[-D, D]$. I.e., it is an instance of small error and small secret LWE. Thus, it induces a polynomial system of 15446 equations in 768 variables, where 768 polynomials stem from LWE samples. The lowest achievable degree of regularity for Kyber768 is estimated via

$$m \cdot \binom{n+d-1}{d} \overset{!}{\geq} \binom{n+D+d-1}{D+d}. \tag{40}$$

In Table 2 we list our complexity estimates together with estimates for various lattice-based attacks. The complexities for lattice-based attacks have been computed via the lattice estimator tool[2] by Albrecht et al. [4].

Table 1. Bit complexity estimation for various attack strategies on Kyber768. Complexity of lattice-based attacks are computed via the lattice estimator [4]. For attacks where the lattice estimator provides estimations for multiple steps in an attack the most difficult step is shown in the table. For Gröbner basis attacks, the proven complexity estimate is computed via Equation (10) and the Macaulay bound (Corollary 6). The optimistic complexity estimate is computed via Equation (17), Theorem 13 and the lowest achievable degree of regularity. The lowest achievable complexity estimate is computed via Equation (10) with $\mathrm{sd}_{DRL}\left(\mathcal{F}_{\mathrm{Kyber768}}\right) = d_{\mathrm{reg}}\left(\mathcal{F}_{\mathrm{Kyber768}}\right) + D - 1$ (Conjecture 25). Gröbner basis complexity estimates are computed with $\omega = 2$.

Method	BKW	USVP	BDD	BDD Hybrid	BDD MiTM Hybrid	Dual	Dual Hybrid	Proven complexity estimate		Optimistic complexity estimate		Lowest achievable complexity estimate	
Samples	2^{226}	768	768	768	768	768	768	768	768^4	768	768^4	768	768^4
Complexity (bits)	239	205	201	201	357	214	206	5554	5581	4717	419	1588	203
Solving degree				n.a.				3077		n.a.		n.a.	
Lowest achievable degree of regularity				n.a.				n.a.		232	7	232	7

6 Integrating Hints into LWE Polynomial Models

In two recent works Dachman-Soled et al. [18,19] introduced a framework for cryptanalysis of LWE in the presence of side information. E.g., in presence of a side-channel the information can come from the power consumption, electromagnetic

---

[2] https://github.com/malb/lattice-estimator

ration, sound emission, etc. of a device. Once side information has been obtained it has to be modeled as mathematical hints. Dachman-Soled et al. categorize hints for LWE into four classes [18, §1]:

– Perfect hints: $\langle \mathbf{s}, \mathbf{v} \rangle = l \in \mathbb{F}_q$.[3]
– Modular hints: $\langle \mathbf{s}, \mathbf{v} \rangle \equiv l \mod k$.
– Approximate hints: $\langle \mathbf{s}, \mathbf{v} \rangle + e_\sigma = l \in \mathbb{F}_q$.
– Short vector hints: $\mathbf{v} \in \Lambda$, where Λ is the lattice associated to a LWE instance.

Dachman-Soled et al. [18,19] then discuss how these hints can be incorporated into Distorted Bounded Distance Decoding (DBDD) problems and lattice reduction algorithms to attack LWE. For readers interested how such hints can be obtained in practice we refer to [18, §4, 6]. Except for short vector hints that do not involve the LWE secret, we can incorporate these hints into LWE polynomial models.

Integrating a perfect hint is straight-forward since including an affine equation to the polynomial systems simply eliminates one variable.

If we are given a modular hint, then in principle one can compute a subset $\Omega \in \mathbb{F}_q$ such that $\langle \mathbf{s}, \mathbf{v} \rangle - l \in \Omega$ (in $\mathbb{F}_q$). Hence, we can set up a new polynomial with roots in Ω, substitute $\langle \mathbf{s}, \mathbf{v} \rangle - l$ into the polynomial and add it to the LWE polynomial system. Although this sounds simple, in practice the computation of Ω can be a challenge. In particular, if $\mathbf{s}$ and $\mathbf{v}$ can take all values in $\mathbb{F}_q^n$, then we expect the set Ω to be too big to improve Gröbner basis computations. On the other hand, if $\mathbf{s}, \mathbf{v} \in \{0,1\}^n$ and we have the modular equation $\langle \mathbf{s}, \mathbf{v} \rangle \equiv 1 \mod 2$, then only the odd numbers in the interval $\left[0, \left\lfloor \frac{n}{2} \right\rfloor\right]$ can be in Ω, so the univariate polynomial with roots in Ω is of degree $\leq \left\lfloor \frac{n}{2} \right\rfloor$.

More interesting are approximate hints. Such hints are obtained from noisy side-channel information. In case the probability distribution of e_σ has smaller width than the one of the LWE error, then we can reduce the degree of a polynomial in the LWE polynomial system. Another class of hints that we interpret as approximate hints are Hamming weight hints. Suppose that the LWE secret entry s_1 is drawn from $D \subset \mathbb{F}_q$ and that we know the Hamming weight $H(s_1) = k$. Then we can add a univariate polynomial in x_1 to the LWE polynomial system whose roots are exactly the elements of D of Hamming weight k. I.e., Hamming weight hints restrict the number of possible solutions. We illustrate this with an example.

Example 26. Let q be a 16 bit prime number, and let $(\mathbf{a}_i, b_i)_{1 \leq i \leq m} \subset \mathbb{F}_q^n \times \mathbb{F}_q$ be a LWE sample generated with secret $\mathbf{s} \subset [-5, 5]^n$. As discussed in Section 4.3, for every variable x_i we can add a polynomial of degree 11 to the polynomial system to restrict the solutions to the interval. Suppose that s_i is represented by a signed 16 bit integer and that we learned its Hamming weight $H(s_i) = 2$,

---

[3] Dachman Soled et al. [18] considered perfect hints over $\mathbb{Z}^n$, our notion of perfect hint corresponds to their modular hint, where the modulus is the characteristic of $\mathbb{F}_q$. They made this distinction, because affine equations over $\mathbb{Z}^n$ and $\mathbb{F}_q^n$ require different integration into lattice algorithms, see [18, §4.1, 4.2]. Though, for integration into polynomial systems perfect hints are always projected to $\mathbb{F}_q$.

then $s_i \in \{3, 5\}$ and we can replace the degree 11 polynomial by a polynomial of degree 2.

Note that such Hamming weight biases can also persist if one opts for a more efficient memory representation of the secret entries.

Example 27. Let q be a 16 bit prime number, and let $(\mathbf{a}_i, b_i)_{1 \leq i \leq m} \subset \mathbb{F}_q^n \times \mathbb{F}_q$ be a LWE sample generated with secret $\mathbf{s} \subset [-2, 2]^n$. As discussed in Section 4.3, for every variable x_i we can add a polynomial of degree 5 to the polynomial system to restrict the solutions to the interval. Assume that the entries of $\mathbf{s}$ are stored as signed integers in the interval $\left[-\frac{q}{2}, \frac{q}{2}\right]$, then

- if $H(s_i) = 0$, then $s_1 = 0$,
- if $H(s_i) = 1$, then $s_1 \in \{1, 2\}$, and
- if $H(s_i) = 2$, then $s_1 \in \{-1, -2\}$.

So if one can learn the Hamming weight of s_i, then one either obtains a perfect hint or one can replace the degree 5 polynomial by a degree 2 polynomial.

Moreover, modular and approximate hints can be combined in a hybrid manner.

Example 28. Let q be a 16 bit prime number, and let $(\mathbf{a}_i, b_i)_{1 \leq i \leq m} \subset \mathbb{F}_q^n \times \mathbb{F}_q$ be a LWE sample generated with secret $\mathbf{s} \subset [-5, 5]^n$. Assume that the entries of $\mathbf{s}$ are stored as signed integers in the interval $\left[-\frac{q}{2}, \frac{q}{2}\right]$. If $H(s_i) = 2$ and $s_i \equiv 1$ mod 3, then $s_i \in \{-2, 4\}$. So we can replace the degree 11 polynomial by a polynomial of degree 2.

In practice this can have devastating consequences. If we can reduce a small secret LWE instance to binary secret LWE or even worse to binary secret binary error LWE, then we expect to achieve a lower degree of regularity with less number of samples necessary compared to the plain polynomial system. We numerically showcase this in the following example.

Example 29. Let q be a 16 bit prime number, assume that we are given small secret small error LWE over $\mathbb{F}_q^{256}$ whose secrets and error are drawn from $[-2, 2]$. Let $m = 256^{\frac{3}{2}}$ samples be given, and assume that we have enough Hamming weight hints for the secret and the error terms to transform the LWE polynomial system to either

(i) binary secret LWE, or
(ii) binary secret binary error LWE.

In Table 2 we record the least integer d such that $d_{\mathrm{reg}}\left(\mathcal{F}_{\mathrm{LWE}}\right) \leq D + d$ together with the optimistic complexity estimate from Equation (17) and the lowest achievable complexity estimate implied by Equation (39) for various numbers of perfect hints.

Table 2. Complexity estimates for binary secret LWE with error polynomial degree $D = 5$ and binary secret binary error LWE over $\mathbb{F}_q^{256}$. The column d lists the least integer such that $d_{\mathrm{reg}}\,(\mathcal{F}_{\mathrm{LWE}}) \leq D + d$ for a given number of perfect hints. The optimistic complexity estimate is computed via Equation (17) and the lowest achievable complexity estimate is computed via Equation (10) with $\mathrm{sd}_{DRL}\,(\mathcal{F}_{\mathrm{LWE}}) = d_{\mathrm{reg}}\,(\mathcal{F}_{\mathrm{LWE}}) + D - 1$ where $D = 5, 2$ (Conjecture 25).

Perfect hints	Small Secret Small Error LWE $D = 5$			Binary Secret LWE $D = 5$			Binary Secret Binary Error LWE $D = 2$		
	d	Optimistic complexity estimate (bits)	Lowest achievable complexity estimate (bits)	d	Optimistic complexity estimate (bits)	Lowest achievable complexity estimate (bits)	d	Optimistic complexity estimate (bits)	Lowest achievable complexity estimate (bits)
$\omega = 2$									
0	57	1391	481	38	1118	370	3	237	92
50	45	1122	393	30	906	303	2	188	78
150	22	596	221	15	499	174	1	127	59
190	13	387	152	8	320	117	0	80	45
$\omega = 3$									
0	57	1731	712	38	1389	547	3	291	131
50	45	1394	580	30	1125	336	2	229	110
210	8	339	165	5	290	127	0	88	56

7 Discussion

In this paper we proved that any fully-determined LWE polynomial system is in generic coordinates. Therefore, bounds for the complexity of DRL Gröbner basis computations can be found via the Castelnuovo-Mumford regularity. In particular, this permits provable complexity estimates without relying on strong but unproven theoretical assumptions like semi-regularity [24,29].

We also demonstrated how the degree of regularity of a LWE polynomial system can be used to derive complexity estimates. Though, in practice one has to keep in mind that a degree of regularity computation usually requires a non-trivial Gröbner basis computation for the highest degree components. Hence, we interpret complexity bounds based on the lowest achievable degree of regularity as worst-case bounds from a designer's perspective that *could* be achievable by an adversary.

Based on the lowest achievable degree of regularity, we discussed that a conservative cryptanalyst should assume that Gaussian elimination on a single Macaulay matrix in the degree of regularity is sufficient to solve Search-LWE.

Moreover, we discussed how side information can be incorporated into LWE polynomial systems, and we showcased how it can affect the complexity of Gröbner basis computations.

Overall, we have presented a new framework to aid algebraic cryptanalysis for LWE-based cryptosystems under minimal theoretical assumptions on the polynomial system.

Acknowledgments

A   Semaev & Tenti's Probability Analysis

Let $P = \mathbb{F}_q[x_1, \ldots, x_n]$ and $R = P/\left(x_1^q, \ldots, x_n^q\right)$, and let $\mathcal{F} = \{f_1, \ldots, f_m\} \subset R$ be a homogeneous polynomial system such $\deg\left(f_i\right) = D$ for all i. Additionally, we define the notation

$$l_e(n,d) = \left| \left\{ (a_1, \ldots, a_n) \in \mathbb{Z}^n \;\middle|\; 0 \leq a_i < e, \; \sum_{i=1}^{n} a_i = d \right\} \right|. \tag{41}$$

Moreover, if we refer to the degree of regularity in the following paragraph, then we implicitly mean the extension of the degree of regularity to R (see [38, Definition 3.48, Theorem 3.53]).

Semaev & Tenti analyzed the probability that a uniformly random polynomial system $\mathcal{F}$ achieves a certain degree of regularity. In particular, they proved that for $D > d > 0$ and $m \geq \frac{l_q(n, D+d)}{l_q(n,d)}$ the probability that $d_{\mathrm{reg}}\left(\mathcal{F}\right) \leq D+d$ converges to 1 for $n \to \infty$ [33, Theorem 1.1]. For $q = D = 2$ Tenti also provided an explicit probability in his PhD thesis [38, Theorem 4.2]

$$\mathbb{P}\left[d_{\mathrm{reg}}\left(\mathcal{F}\right) \leq 3\right] \geq 1 - \sum_{v=0}^{n-1} q^{\binom{n-v}{3} + (n-v+1)\cdot v - (n-v)\cdot m}. \tag{42}$$

For LWE polynomial systems we encounter a very similar scenario, since in all scenarios in Sections 4.1 to 4.3 we can find a set of univariate polynomials $F = \left(f(x_1), \ldots, f(x_n)\right)$, where f is univariate and $\deg\left(f\right) = e \geq 2$, that restricts the number of possible solutions. Moreover, in all our scenarios $f(x_i) \mid x_i^q - x_i$. Thus, to analyze the degree of regularity analog to Semaev & Tenti we first construct the polynomials F, and then we replace the polynomials in $\mathcal{F}_{\mathrm{LWE}}$ by their remainders modulo F. Finally, for the degree of regularity only the highest degree components matter, so we can restrict the analysis to $\mathcal{F}_{\mathrm{LWE}}^{\mathrm{top}} \in \mathbb{F}_q[x_1, \ldots, x_n]/\left(x_1^e, \ldots, x_n^e\right)$.

The proof of Semaev & Tenti is combinatorial, i.e. in principle it does not depend on $e = q$ nor the characteristic of the finite field. Therefore, we expect that their results can be generalized to arbitrary rings $\mathbb{F}_q[x_1, \ldots, x_n]/\left(x_1^e, \ldots, x_n^e\right)$.

Instead of repeating their analysis now, we will investigate a simpler problem. Can we consider the highest degree components of LWE polynomial systems as uniformly distributed in $\mathbb{F}_q[x_1, \ldots, x_n]$?

A.1 On The Distance Of LWE Highest Degree Components To The Uniform Distribution

The highest degree components of LWE polynomials are of the form $\left(\langle \mathbf{a}_i, \mathbf{x} \rangle\right)^d$, for some uniform and independent distributed $\mathbf{a}_i \in \mathbb{F}_q^n$. In this section we compute the distance of the coefficient distribution of $\left(\langle \mathbf{a}_i, \mathbf{x} \rangle\right)^d$ to the uniform distribution over $\mathbb{F}_q^{\binom{n+d-1}{d}}$. Let us first recall the notion of statistical distance also known as total variation distance.

Definition 30 ([27, §4.1]). *Let μ and ν be two probability distributions on a finite set Ω. The statistical distance (or total variation distance) between μ and ν is defined as*

$$\mathrm{d}_{\mathrm{TV}}\left(\mu, \nu\right) = \frac{1}{2} \cdot \sum_{x \in \Omega} |\mu(x) - \nu(x)|.$$

The following identity will be useful to compute the statistical distance.

Lemma 31 ([27, Remark 4.3]). *Let μ and ν be two probability distributions on a finite set Ω. Then*

$$\mathrm{d}_{\mathrm{TV}}\left(\mu, \nu\right) = \sum_{\substack{x \in \Omega, \\ \mu(x) \geq \nu(x)}} \mu(x) - \nu(x).$$

The following lemma is an easy consequence of the previous lemma.

Lemma 32. *Let μ and ν be two probability distributions on a finite set Ω, and assume that $\mathrm{d}_{\mathrm{TV}}\left(\mu, \nu\right) \leq \epsilon$ for some $\epsilon > 0$. Then*

$$\nu(x) - \epsilon \leq \mu(x) \leq \nu(x) + \epsilon,$$
$$\mu(x) - \epsilon \leq \nu(x) \leq \mu(x) + \epsilon.$$

Proof. If $\mu(x) - \nu(x) \geq 0$, then by Lemma 31 $\mu(x) - \nu(x) \leq \sum_{\substack{x \in \Omega, \\ \mu(x) \geq \nu(x)}} \mu(x) - \nu(x) = \mathrm{d}_{\mathrm{TV}}\left(\mu, \nu\right) \leq \epsilon$. If $\nu(x) - \mu(x) \geq 0$, then $\nu(x) - \mu(x) \leq \sum_{\substack{x \in \Omega, \\ \nu(x) \geq \mu(x)}} \nu(x) - \mu(x) = \mathrm{d}_{\mathrm{TV}}\left(\mu, \nu\right) \leq \epsilon$. By combining these two inequalities we derive the claims. $\square$

Hence, if some property holds for the distribution ν, then in principle one can extend this property to the distribution μ up to some error term that depends on ϵ.

Let us now return to $\left(\langle \mathbf{a}_i, \mathbf{x} \rangle\right)^d$, for ease of notation we abbreviate $N_{n,d} = \binom{n+d-1}{d}$. We consider the function

$$\phi_{n,d} : \mathbb{F}_q^n \to \mathbb{F}_q^{N_{n,d}},$$
$$(a_1, \ldots, a_n) \mapsto \left(\frac{d!}{i_1! \cdots i_n!} \cdot a_1^{i_1} \cdots a_n^{i_n} \right)_{\substack{0 \leq i_j \leq d, \\ \sum_{j=1}^n i_j = d}}. \tag{43}$$

Obviously, ϕ maps $\mathbf{a} \in \mathbb{F}_q^n$ to the coefficient vector of $(\langle \mathbf{a}, \mathbf{x} \rangle)^d$. Moreover, we assume that $\frac{n!}{i_1! \cdots i_n!} \neq 0$ in $\mathbb{F}_q$ for all possible $(i_1, \ldots, i_n)$. This condition is for example satisfied if q is prime and $d < q$. Then

$$\mu(\mathbf{b}) = \mathbb{P}\left[\mathbf{b} \in \mathrm{im}(\phi_{n,d})\right] = \frac{\left|\phi_{n,d}^{-1}(\mathbf{b})\right|}{q^n}. \tag{44}$$

In particular, if $\left|\phi_{n,d}^{-1}(\mathbf{b})\right| \neq 0$, then $\mu(\mathbf{b}) \geq \frac{1}{q^n}$. Also, for $d \geq 1$ we have that $N_{n,d} \geq n$. Then with Lemma 31 we have that

$$\mathrm{d}_{\mathrm{TV}}\left(\mu, \frac{1}{q^{N_{n,d}}}\right) = \sum_{\substack{\mathbf{b} \in \mathbb{F}_q^{N_{n,d}}, \\ \mu(\mathbf{b}) \geq \frac{1}{q^{N_{n,d}}}}} \mu(\mathbf{b}) - \frac{1}{q^{N_{n,d}}} \tag{45}$$

$$= \sum_{\mathbf{b} \in \mathrm{im}(\phi_{n,d})} \frac{\left|\phi_{n,d}^{-1}(\mathbf{b})\right|}{q^n} - \frac{1}{q^{N_{n,d}}} \tag{46}$$

$$= 1 - \frac{\left|\mathrm{im}(\phi_{n,d})\right|}{q^{N_{n,d}}} \tag{47}$$

$$\geq 1 - \frac{q^n}{q^{N_{n,d}}}. \tag{48}$$

Obviously, the last expression has limit 1 for $d \to \infty$. Now let $\mathbf{a} \in \mathbb{F}_q^n$ be uniformly random and let $\mathbf{b} \in \mathbb{F}_q^{N_{n,d}}$, then

$$\mathbb{P}\left[\phi_{n,d}(\mathbf{a}) = \mathbf{b}\right] = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \mathbb{P}\left[\mathbf{c}\right] \cdot \mathbb{P}\left[\phi_{n,d}(\mathbf{a}) = \mathbf{b} \mid \mathbf{a} = \mathbf{c}\right]. \tag{49}$$

Note that $\mathbb{P}\left[\phi_{n,d}(\mathbf{a}) = \mathbf{b} \mid \mathbf{a} = \mathbf{c}\right] \in \{0, 1\}$, and it is equal to 1 exactly $\left|\phi_{n,d}^{-1}(\mathbf{b})\right|$-many times. Therefore,

$$\mathbb{P}\left[\phi_{n,d}(\mathbf{a}) = \mathbf{b}\right] = \mathbb{P}\left[\mathbf{b} \in \mathrm{im}(\phi_{n,d})\right]. \tag{50}$$

Hence, in general we consider the distribution of $\phi_{n,d}(\mathbf{a})$, where $\mathbf{a} \in \mathbb{F}_q^n$ is uniformly random, to be far from the uniform distribution over $\mathbb{F}_q^{N_{n,d}}$. For example for $d = 2$ we have that

$$\mathrm{d}_{\mathrm{TV}}\left(\mu, \frac{1}{q^{N_{n,2}}}\right) \geq 1 - \frac{q^n}{q^{\frac{(n-1) \cdot n}{2}}} = 1 - q^{\frac{-n^2+n}{2}} \geq \frac{1}{2}, \tag{51}$$

where the last inequality follows by $n, q \geq 2$.

Hence, probability estimations for uniformly distributed highest degree components, like the one of Semaev & Tenti, are not applicable to LWE polynomial systems.

References

1. Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: 28th Annual ACM Symposium on Theory of Computing. pp. 99–108. ACM Press, Philadephia, PA, USA (May 22–24, 1996). https://doi.org/10.1145/237814.237838
2. Albrecht, M.R., Cid, C., Faugère, J.C., Fitzpatrick, R., Perret, L.: Algebraic algorithms for LWE problems. ACM Commun. Comput. Algebra **49**(2), 62 (aug 2015). https://doi.org/10.1145/2815111.2815158
3. Albrecht, M.R., Cid, C., Faugère, J.C., Perret, L.: Algebraic algorithms for LWE. Cryptology ePrint Archive, Report 2014/1018 (2014), https://eprint.iacr.org/2014/1018
4. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of Learning with Errors. J. Math. Cryptol. **9**(3), 169–203 (2015). https://doi.org/10.1515/jmc-2015-0016
5. Alman, J., Williams, V.V.: A refined laser method and faster matrix multiplication. In: Marx, D. (ed.) 32nd Annual ACM-SIAM Symposium on Discrete Algorithms. pp. 522–539. ACM-SIAM, Virtual Conference (Jan 10–13, 2021). https://doi.org/10.1137/1.9781611976465.32
6. Arora, S., Ge, R.: New algorithms for learning in presence of errors. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) ICALP 2011: 38th International Colloquium on Automata, Languages and Programming, Part I. Lecture Notes in Computer Science, vol. 6755, pp. 403–415. Springer, Heidelberg, Germany, Zurich, Switzerland (Jul 4–8, 2011). https://doi.org/10.1007/978-3-642-22006-7_34
7. Bardet, M., Faugère, J.C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving. pp. 71–74 (2004)
8. Bayer, D., Stillman, M.: A criterion for detecting m-regularity. Invent. Math. **87**(1), 1–11 (2 1987). https://doi.org/10.1007/BF01389151
9. Bos, J.W., Costello, C., Ducas, L., Mironov, I., Naehrig, M., Nikolaenko, V., Raghunathan, A., Stebila, D.: Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In: Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S. (eds.) ACM CCS 2016: 23rd Conference on Computer and Communications Security. pp. 1006–1018. ACM Press, Vienna, Austria (Oct 24–28, 2016). https://doi.org/10.1145/2976749.2978425
10. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.: Classical hardness of learning with errors. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) 45th Annual ACM Symposium on Theory of Computing. pp. 575–584. ACM Press, Palo Alto, CA, USA (Jun 1–4, 2013). https://doi.org/10.1145/2488608.2488680
11. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. thesis, Universität Innsbruck (1965)
12. Caminata, A., Gorla, E.: Solving multivariate polynomial systems and an invariant from commutative algebra. In: Bajard, J.C., Topuzoğlu, A. (eds.) Arithmetic of Finite Fields. pp. 3–36. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-68869-1_1
13. Caminata, A., Gorla, E.: Solving multivariate polynomial systems and an invariant from commutative algebra. arXiv: 1706.06319 (2022), Version: 7
14. Caminata, A., Gorla, E.: Solving degree, last fall degree, and related invariants. J. Symb. Comput. **114**, 322–335 (2023). https://doi.org/10.1016/j.jsc.2022.05.001

15. Chardin, M.: Some results and questions on Castelnuovo-Mumford regularity. In: Peeva, I. (ed.) Syzygies and Hilbert Functions. Lecture Notes in Pure and Applied Mathematics, vol. 254, pp. 1–40. Chapman and Hall/CRC (2007)

16. Cover, T.M., Joy, T.A.: Elements of Information Theory. John Wiley & Sons, Ltd, Hoboken, New Jersey, 2 edn. (2006). https://doi.org/10.1002/0471200611

17. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Undergraduate Texts in Mathematics, Springer International Publishing, 4 edn. (2015). https://doi.org/10.1007/978-3-319-16721-3

18. Dachman-Soled, D., Ducas, L., Gong, H., Rossi, M.: LWE with side information: Attacks and concrete security estimation. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020, Part II. Lecture Notes in Computer Science, vol. 12171, pp. 329–358. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2020). https://doi.org/10.1007/978-3-030-56880-1_12

19. Dachman-Soled, D., Gong, H., Hanson, T., Kippen, H.: Revisiting security estimation for LWE with hints from a geometric perspective. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023, Part V. Lecture Notes in Computer Science, vol. 14085, pp. 748–781. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2023). https://doi.org/10.1007/978-3-031-38554-4_24

20. Ding, J., Schmidt, D.: Solving degree and degree of regularity for polynomial systems over a finite fields. In: Fischlin, M., Katzenbeisser, S. (eds.) Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday. pp. 34–49. Springer Berlin Heidelberg, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42001-6_4

21. Eisenbud, D.: The Geometry of Syzygies: A Second Course Commutative Algebra and Algebraic Geometry. Springer New York, 1 edn. (2005). https://doi.org/10.1007/b137572

22. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra **139**(1), 61–88 (1999). https://doi.org/10.1016/S0022-4049(99)00005-5

23. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. p. 75–83. ISSAC '02, Association for Computing Machinery (2002). https://doi.org/10.1145/780506.780516

24. Fröberg, R.: An inequality for Hilbert series of graded algebras. Math. Scand. **56**, 117–144 (12 1985). https://doi.org/10.7146/math.scand.a-12092

25. Gao, S.: Counting Zeros over Finite Fields Using Gröbner Bases. Master's thesis, Carnegie Mellon University (2009), https://www.cs.cmu.edu/~sicung/papers/MS_thesis.pdf

26. Lazard, D.: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: van Hulzen, J.A. (ed.) Computer Algebra, EUROCAL '83, European Computer Algebra Conference, London, England, March 28-30, 1983, Proceedings. Lecture Notes in Computer Science, vol. 162, pp. 146–156. Springer Berlin Heidelberg (1983). https://doi.org/10.1007/3-540-12868-9_99

27. Levin, D.A., Peres, Y.: Markov Chains and Mixing Times. American Mathematical Society, 2 edn. (2017). https://doi.org/10.1090/mbk/107

28. Micciancio, D.: On the hardness of learning with errors with binary secrets. Theory Comput. **14**(13), 1–17 (2018). https://doi.org/10.4086/toc.2018.v014a013

29. Pardue, K.: Generic sequences of polynomials. J. Algebra **324**(4), 579–590 (2010). https://doi.org/10.1016/j.jalgebra.2010.04.018

30. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: Mitzenmacher, M. (ed.) 41st Annual ACM Symposium on Theory of Computing. pp. 333–342. ACM Press, Bethesda, MD, USA (May 31 – Jun 2, 2009). https://doi.org/10.1145/1536414.1536461

31. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th Annual ACM Symposium on Theory of Computing. pp. 84–93. ACM Press, Baltimore, MA, USA (May 22–24, 2005). https://doi.org/10.1145/1060590.1060603

32. Schwabe, P., Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Seiler, G., Stehlé, D., Ding, J.: CRYSTALS-KYBER. Tech. rep., National Institute of Standards and Technology (2022), available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

33. Semaev, I., Tenti, A.: Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases. J. Algebra **565**, 651–674 (2021). https://doi.org/10.1016/j.jalgebra.2020.08.035

34. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science. pp. 124–134. IEEE Computer Society Press, Santa Fe, NM, USA (Nov 20–22, 1994). https://doi.org/10.1109/SFCS.1994.365700

35. Steiner, M.J.: Solving degree bounds for iterated polynomial systems. arXiv: 2310.03637 (2023). https://doi.org/10.48550/ARXIV.2310.03637, Accepted into IACR Trans. Symm. Cryptol. 2024(1)

36. Storjohann, A.: Algorithms for matrix canonical forms. Doctoral thesis, ETH Zurich, Zürich (2000). https://doi.org/10.3929/ethz-a-004141007, diss., Technische Wissenschaften ETH Zürich, Nr. 13922, 2001.

37. Sun, C., Tibouchi, M., Abe, M.: Revisiting the hardness of binary error LWE. In: Liu, J.K., Cui, H. (eds.) ACISP 20: 25th Australasian Conference on Information Security and Privacy. Lecture Notes in Computer Science, vol. 12248, pp. 425–444. Springer, Heidelberg, Germany, Perth, WA, Australia (Nov 30 – Dec 2, 2020). https://doi.org/10.1007/978-3-030-55304-3_22

38. Tenti, A.: Sufficiently overdetermined random polynomial systems behave like semiregular ones. Ph.D. thesis, University of Bergen (2019), https://hdl.handle.net/1956/21158

39. Topsøe, F.: Bounds for entropy and divergence for distributions over a two-element set. J. Ineq. Pure Appl. Math. **2**(2), Paper No. 25, 13 p.–Paper No. 25, 13 p. (2001), http://eudml.org/doc/122035