On the Soundness of Algebraic Attacks against Code-based Assumptions

Miguel Cueto Noval [*],
Simon-Philipp Merz [†],
Patrick Stählin[†],
and Akin Ünal[*‡]

[*]ISTA, Klosterneuburg, Austria
[†]ETH Zurich, Zurich, Switzerland

{mcuetono,auenal}@ista.ac.at
research@simon-philipp.com
stpatric@ethz.ch

March 4, 2025

Abstract

We study recent algebraic attacks (Briaud-Øygarden EC'23) on the Regular Syndrome Decoding (RSD) problem and the assumptions underlying the correctness of their attacks' complexity estimates. By relating these assumptions to interesting algebraic-combinatorial problems, we prove that they do not hold in full generality. However, we show that they are (asymptotically) true for most parameter sets, supporting the soundness of algebraic attacks on RSD. Further, we prove—without any heuristics or assumptions—that RSD can be broken in polynomial time whenever the number of error blocks times the square of the size of error blocks is larger than 2 times the square of the dimension of the code.

Additionally, we use our methodology to attack a variant of the Learning With Errors problem where each error term lies in a fixed set of constant size. We prove that this problem can be broken in polynomial time, given a sufficient number of samples. This result improves on the seminal work by Arora and Ge (ICALP'11), as the attack's time complexity is independent of the LWE modulus.

1 Introduction

Regular Syndrome Decoding. The Syndrome Decoding (SD) resp. Learning Parity with Noise (LPN) problem is one of the foundational problems at the heart of coding theory, and it is used as a standard assumption to prove the security of a multitude of cryptographic constructions in code-based cryptography. Further fueled by the surge of interest in post-quantum cryptography,

[‡]Part of this work was done while Ünal worked at ETH Zurich, Zurich, Switzerland.

research on constructing and analysing cryptographic schemes based on specific parameter sets for these foundational assumptions has gained increasing traction.

Let $\mathbf{e} \in \mathbb{F}^n$ be a vector with low Hamming weight, at most w, over a finite field $\mathbb{F}$. Given the parity-check matrix $\mathbf{H} \leftarrow \mathbb{F}^{(n-k)\times n}$ of a linear code over $\mathbb{F}$ and the syndrome, defined as $\mathbf{s} \coloneqq \mathbf{He}$, the SD problem asks to recover the error vector $\mathbf{e}$.

A more structured version of this problem, known as the Regular Syndrome Decoding (RSD) problem[1], with additional information about the error distribution in $\mathbf{e}$ was introduced two decades ago by Augot, Finiasz and Sendrier in the context of fast syndrome-based hash functions [AFS03]. For parameters (b, k, w), with $n = bw$, the RSD problem asks again to decode $(\mathbf{H}, \mathbf{He})$. This time, the error vector $\mathbf{e} = (\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)})$ consists of w consecutive chunks $\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)} \in \mathbb{F}^b$ of Hamming[2] weight ≤ 1.

During the past 5 years, the popularity of the structured RSD problem has grown as it allowed to increase the efficiency of cryptographic schemes and to design new advanced cryptographic constructions. For instance, RSD was used in the *TinyKeys* MPC-protocol [Haz+18], to introduce new signatures with reduced signature size [CCJ23] or to construct Vector Oblivious Linear Evaluation (VOLE) [Boy+18] and Pseudorandom Correlation Generators (PCG) [Boy+19] which in turn can be used to construct more involved MPC and ZK applications and have sparked an entire series of works on the topic, e.g. [Boy+20; Wen+21; Yan+20]. Additionally, RSD (besides LPN) implies local PRGs, which enjoy application in the construction of indistinguishability obfuscation [RVV24; BCM24].

Apart from the regular structure of the error vector, several of these constructions diverge from the standard syndrome decoding problem which is often stated over the binary field $\mathbb{Z}_2$ by considering instances over larger fields [Boy+18; Boy+19; Wen+21] or even over polynomial rings [Boy+20].

Cryptanalysis on RSD. Cryptanalysis of RSD was done by Liu, Wang, Yang and Yu [Liu+24] with advanced information set decoding (ISD) algorithms, by Briaud and Øygarden with algebraic attacks [BØ23] based on assumptions and by Esser and Santini with combinatorial ISD attacks [ES24]. In Table 1, we provide an overview of the estimated time complexities of their attacks for special parameters put forth by Boyle, Couteau, Gilboa and Ishai [Boy+18].

While recent attacks could catch up with the algebraic solvers of [BØ23] over $\mathbb{Z}_2$, we can see that the performance of algebraic attacks for large parameters over big fields is still far out reach for linear and combinatorial attacks. Given that the proof of correctness provided in [BØ23] relies on assumptions, one may raise concerns about the actual soundness of algebraic attacks on RSD. Indeed, Briaud and Øygarden base the soundness of their attacks on the semi-regularity of the polynomial systems they solve. Semi-regularity is a complicated algebraic concept inspired by Fröberg's [Frö85] work and put forth by Pardue in

[1] Note that RSD is equivalent to Regular Learning Parity with Noise (RLPN).

[2] For simplicity, we deviate in this work from the standard convention of each block having Hamming weight exactly 1, and allow for blocks of weight 0 or 1. We do this to simplify our analysis in the following. We think this relaxation is justified as in the big-field setting, this difference is negligible. In the case of $\mathbb{F} = \mathbb{Z}_2$, the exact Hamming-weight case (for parameters (b, k, w)) can be reduced to the relaxed case (for parameters $(b-1, k-w, w)$) by extracting one correct linear equation per block.

			LWYY	**BØ**	**ES**	**LWYY**	**BØ**
			[Liu+24]	[BØ23]	[ES24]	[Liu+24]	[BØ23]
n	k	w	RSD over $\mathbb{F}_2$			RSD over $\mathbb{F}_{2^{128}}$	
2^{10}	652	106	176	145	**113**	194	**179**
2^{12}	1589	172	131	135	**109**	155	**150**
2^{14}	3482	338	132	138	**118**	150	**150**
2^{16}	7391	667	135	139	**126**	151	**150**
2^{18}	15336	1312	139	**122**	**122**	153	**133**
2^{20}	32771	2467	143	**125**	**125**	155	**131**
2^{22}	64770	4788	147	**103**	**103**	156	**110**

Table 1: Overview of logarithms of runtimes for different attacks on RSD over $\mathbb{F}_2$ and $\mathbb{F}_{2^{128}}$.

algebra [Par10] and Bardet [BFS03] in cryptography. While most random systems of polynomials are semi-regular, Fröberg already pointed out that there are special polynomial systems that can never be semi-regular [FH94] (independently of their randomness). Additionally, Hodges, Molina and Schlather [HMS17] investigated semi-regular sequences over $\mathbb{Z}_2$ and noted that for certain parameters semi-regular sequences can never exist. All of these leads us to the following question:

> *Do algebraic attacks on RSD actually work, or are they too good to be true and their analysis based on faulty assumptions?*

Contribution. Our contribution lies in answering the above question positively by demonstrating that one can replace the semi-regularity assumptions in several works by concrete proofs. Concretely, we investigate under which conditions the equation systems in [BØ23] have a degree of regularity or witness degree[3] of 2. While our first result is negative and proves that the assumptions of [BØ23] do not hold in full generality, we prove that they hold *asymptotically* for all relevant parameters. We think these results strongly support the soundness of the algebraic attacks on RSD of [BØ23] for all cases where they target[4] a witness degree of 2. Additionally, as a reward, we get a polynomial-time algebraic attack on RSD for certain parameter ranges over big fields whose correctness is fully proven without any assumptions.

Main Theorem 1 (Theorem 2)**.** *Let $\mathbb{F}$ be a large enough field. For each constant $c > 1$, there is a PPT algorithm that can solve RSD over $\mathbb{F}$ with parameters (b, k, w) with high probability if*

$$w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2}.$$

[3] Briaud and Øygarden [BØ23] bound their complexities by the witness degree, which is bounded by the degree of regularity of a homogenized system. In the hybrid attacks of [BØ23], where a lot of incorrect guesses happen, the degree of regularity of the homogenized system can be bounded by the hypothesis we study here.

[4] Verifying witness degrees of 3 or higher poses another interesting, but even more complicated open problem. We give details to the different assumptions used in [BØ23] in Section F.

We strongly suspect that the assumptions of [BØ23] are already fulfilled whenever $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ and $w \geq 4$. Hence, we think that RSD is cryptographically weak whenever the tighter inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ holds.

Conjecture 1. There is a PPT algorithm that can solve RSD with parameters (b, k, w) with high probability whenever

$$w \cdot \binom{b}{2} \geq \binom{k+1}{2}.$$

As advice for protocol designers, we recommend keeping a large distance between wb^2 and k^2 when deploying RSD.

The insecurity of RSD for $w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2}$ was not known[5] before. In particular, this result shows that there are parameter ranges for which algebraic attacks on RSD excel while linear attacks will need super-polynomial time. This is a big difference to the normal Syndrome Decoding problem where algebraic attacks do not appear to surpass linear attacks [LSS22; Stä23].

Additionally, we will apply the methodology we developed for algebraic attacks on RSD to algebraic attacks on the Learning With Bounded Errors (LWBE) problem. LWBE is a generalization of the Learning With Binary Errors problem and asks to recover $\mathbf{x}$ from $(\mathbf{G} \in \mathbb{F}^{n \times k}, \mathbf{Gx} + \mathbf{e} \in \mathbb{F}^n)$ where each term of the noise-vector $\mathbf{e}$ lies in some fixed set of size d. While Learning With Errors is the gold standard in theory, LWBE is more relevant in reality, as it is more suitable to sample noise from small instead of Gaussian distributions. As an example, we can give the standardized post-quantum ML-KEM (Crystal Kyber) whose noise terms lie in sets of size 5 and 7 [Lyu24]. LWBE has been studied multiple times with either relinearization attacks [AG11] or algebraic attacks relying on different assumptions [MP13; Alb+14; STA20; Ste24]. The attack we devise in this paper will be free of assumptions and optimal with respect to its runtime in relation to the number of samples it needs. Concretely, we show:

Main Theorem 2 (Theorem 4)**.** *Let $n = \binom{k+d-1}{d}$ and let $\mathbb{F}$ be large enough with characteristic $> d$. There is an algorithm that solves LWBE, with n samples and code dimension k where each error-term lies in a set of size d, with high probability. The time complexity of this algorithm is $O(dkM)$ where M is the cost of inverting an $n \times n$ matrix.*

We give an overview of existing attacks on LWBE in Table 2. Note that the soundness of most attacks relies on assumptions. The only exceptions are one attack with exponential runtime [Ste24], and the attack of Arora and Ge [AG11], whose time complexity grows superlinear in q. In contrast to our attack, whose time complexity is independent of q, this is suboptimal for large moduli, which appear, for example, in the LWR problem.

The same analysis done for the LWBE problem applies to the case of the Learning with Rounding (LWR) Problem 5 introduced by Banerjee, Peikert and Rosen [BPR12]. The LWR problem uses deterministic noise instead of the randomly sampled noise used in LWE which means it is more suitable for

[5] Briaud and Øygarden already proved the soundness of their attacks when the code-rate is n^{-b} and the error-rate n^{-a} for $a + 2b > 1$. However, these proofs needed assumptions and the parameter ranges we give are asymptotically tighter.

Work	Size of Errors	Number of Samples n	Time Complexity	Without Heuristics?
AG [AG11]	d	$O\left(\log(q) \cdot q \cdot k^d\right)$	$O\left(\log(q) \cdot q \cdot k^{\omega d}\right)$	**YES**
ACFP [Alb+14]	2	$O\left(k \log\log k\right)$	$O\left(k^2 \cdot 2^{\frac{\omega k \log\log\log k}{8 \log\log k}}\right)$	NO
ACFP [Alb+14]	2	$c \cdot k$	$O\left(k^2 \cdot 2^{\omega k(1+\beta)H_2(\beta/(1+\beta))}\right)$ for $\beta = c - 0.5 - \sqrt{c(c-1)}$	NO
STA [STA20]	2	$c \cdot k^2$	$k^{O(1/c)}$	NO
STA [STA20]	2	$k^{1+\alpha}$	$2^{\widetilde{O}\left(n^{1-\alpha}\right)}$	NO
Steiner [Ste24]	d	$> k$	$O\begin{pmatrix} n \cdot (d-1) \cdot k \\ \cdot 2^{\omega \cdot (8d^{\ln(4)-1})^{1/\ln(4)} \cdot k} \end{pmatrix}$	**YES**
Steiner [Ste24]	d	$O\left(\binom{k+d-1}{d}\right)$	$O\left(d^3 \cdot c_d^{(k-1)^{1-1/\ln(4)}}\right)$	NO
Steiner [Ste24]	2	$O\left(k^2\right)$	$O\left(k^2 \cdot \binom{k+3}{3}^{\omega+2}\right)$	NO
This Work	d	$\binom{k+d-1}{d}$	$O\left(dk^{1+d\omega}\right)$	**YES**

Table 2: An overview of attacks on LWBE with secret key length k and number of samples n. Each error term must lie in a fixed set of size d. Note that $H_2(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy function and $\ln = \log_e$ the natural logarithm. ω denotes the linear algebra constant, which lies between 2 and 3. To save space, we had to set $c_d := 2^{(\omega+3)\cdot 2^{1/\ln(2)} \cdot (2d-1)^{1/\ln(4)}}$.

constructing primitives that are inherently deterministic such as PRFs. Our results imply that LWR with primes $q > p$ can be broken in time $O(qk^{1+\omega q/p}/p)$ when given $O(k^{q/p})$ samples.

1.1 Technical Overview

1.1.1 Equivalence of Primal and Dual Modelings.

Let $(\mathbf{H} \in \mathbb{F}^{n \times k}, \mathbf{s} = \mathbf{He} \in \mathbb{F}^{n-k})$ be an RSD instance over a large field, e.g. $\mathbb{F} = \mathbb{F}_{2^{128}}$, where $\mathbf{e} = (\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)})$ consists of w blocks $\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)} \in \mathbb{F}^b$. To extract $\mathbf{e}$ out of $(\mathbf{H}, \mathbf{s})$, Briaud and Øygarden [BØ23] consider the following **dual** polynomial equation system

$$\begin{aligned} E_\alpha^{(i)} \cdot E_\beta^{(i)} &= 0, && \text{for } i \in [w], 1 \leq \alpha < \beta \leq b, \\ h_j(E) &= s_j, && \text{for } j \in [n-k], \end{aligned}$$

where $E = (E_\alpha^{(i)})_{\alpha \in [b], i \in [w]}$ is a vector of $n = wb$ formal variables. The $h_j(E) := \mathbf{h}_j^\intercal \cdot E$ are linear polynomials that compute the rows $\mathbf{h}_1^\intercal, \ldots, \mathbf{h}_{n-k}^\intercal$ of $\mathbf{H}$. The equations $E_\alpha^{(i)} E_\beta^{(i)} = 0$ ensure that each solution $(\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)})$ has Hamming weight at most 1 per block, while the equations $h_j(E) = 0$ ensure that $\mathbf{e}$ lies in the kernel of $\mathbf{H}$.

Remember that the degree of regularity of a system of polynomials is the smallest degree d such that the ideal generated by the top terms[6] of all polynomials contains all monomials of degree d. To estimate the time complexity of algebraic algorithms for solving the above equation system, the authors of [BØ23] assume that the linear forms $h_1, \ldots, h_{n-k}$ form a semi-regular[7] sequence with respect to the quotient ring

$$R := \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)} \mid i \in [w], 1 \leq \alpha < \beta \leq b).$$

This assumption implies that the Hilbert series of the quotient ring $R/(h_1, \ldots, h_{n-k})$ is given by the truncation[8] of

$$(1-T)^{n-k} \cdot \mathcal{H}_R(T) = (1-T)^{n-k} \cdot (1 + bT + bT^2 + \ldots)^w,$$

where $\mathcal{H}_R(T)$ is the Hilbert series of R. We will show that the first three coefficients of this power series are given by

$$1 + k \cdot T + \left(\binom{k+1}{2} - w\binom{b}{2} \right) \cdot T^2 + O(T^3).$$

This means, the assumptions underlying [BØ23] imply a degree of regularity of 2 for the above polynomial equation system whenever the inequality

$$w\binom{b}{2} \geq \binom{k+1}{2}$$

holds. We claim that this is no coincidence. In fact, let us show that the polynomial system above is equivalent to a primal system with $w\binom{b}{2}$ degree-2 equations over k variables. For the dual RSD problem $(\mathbf{H}, \mathbf{s} = \mathbf{He})$, consider an equivalent RLPN problem $(\mathbf{G} \in \mathbb{F}^{n \times k}, \mathbf{y} = \mathbf{Gx} + \mathbf{e} \in \mathbb{F}^n)$, where $\mathbf{G}$ is a generator matrix for the code of $\mathbf{H}$. Let $X_1, \ldots, X_k$ be new variables that represent the unknown entries of $\mathbf{x}$. Denote by $(\mathbf{g}_\alpha^{(i)})^\intercal$, $i \in [w], \alpha \in [b]$, the rows of $\mathbf{G}$ (indexed according to error blocks of $\mathbf{e}$), and denote by $g_\alpha^{(i)} \in \mathbb{F}[X]$ linear forms that compute the rows of $\mathbf{G}$, i.e., $g_\alpha^{(i)}(X) := (\mathbf{g}_\alpha^{(i)})^\intercal \cdot X$. To extract $\mathbf{x}$ (and therefore $\mathbf{e}$) from $(\mathbf{G}, \mathbf{y})$, we consider the following **primal** system of degree-2 polynomials

$$\left(g_\alpha^{(i)}(X) - y_\alpha^{(i)} \right) \cdot \left(g_\beta^{(i)}(X) - y_\beta^{(i)} \right) = 0, \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

This modeling is very similar to the systems studied by Arora and Ge [AG11]. However, the key difference is that we extract a maximum number of $\binom{b}{2}$ equations per error block $\mathbf{e}^{(i)}$, while [AG11] usually extracts only one equation per error block.

We will prove that both modelings are equivalent. This means that algebraic algorithms solving those models have similar runtimes. In particular, both models have the same degree of regularity. Note that the primal model is significantly simpler than the dual model. This simplicity allows us to determine its degree

[6] The top term of a polynomial f is the sum of all monomials of f of degree $\deg(f)$.

[7] We define semi-regularity in Section D.

[8] Truncation means we cut the formal power series off before the first non-positive coefficient.

of regularity. Indeed, the primal modeling has degree of regularity 2 (with overwhelming probability over $\mathbf{G} \leftarrow \mathbb{F}^{n\times k}$) whenever the following hypothesis holds:

Hypothesis (Hypothesis 3). There exist linear forms $g_\alpha^{(i)} \in \mathbb{F}[X]^1$ for $i \in [w], \alpha \in [b]$ such that

$$\operatorname{span}_{\mathbb{F}} \left\{ g_\alpha^{(i)} \cdot g_\beta^{(i)} \;\middle|\; i \in [w], 1 \leq \alpha < \beta \leq b \right\} = \mathbb{F}[X]^2,$$

where

$$\mathbb{F}[X]^1 \coloneqq \operatorname{span}_{\mathbb{F}}\{X_1, \ldots, X_k\} \quad \text{and} \quad \mathbb{F}[X]^2 \coloneqq \operatorname{span}_{\mathbb{F}}\{X_i X_j \mid i, j \in [k]\}$$

denote the spaces of 1-forms and 2-forms, respectively.

This hypothesis constitutes an interesting algebraic-combinatorial problem. The assumptions of [BØ23] imply that this hypothesis must be true whenever $w\binom{b}{2} \geq \binom{k+1}{2}$. In the following, we will examine when this is the case:

Negative Results. Our first results are negative. Indeed, we will prove that the hypothesis must be wrong for $w = 2, b < k$ and $w = 3, b < 2k/3$. This implies that the assumptions of [BØ23] are false whenever $w \in \{2, 3\}$.

Let us sketch our proof in the case $w = 2$ and $b = k - 1$. In this case, we are given two blocks $g_1^{(1)}, \ldots, g_{k-1}^{(1)} \in \mathbb{F}[X]^1$ and $g_1^{(2)}, \ldots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$. Assume, for the sake of contradiction, that we would have

$$\operatorname{span}_{\mathbb{F}} \left\{ g_\alpha^{(1)} \cdot g_\beta^{(1)} \;\middle|\; \alpha < \beta \right\} + \operatorname{span}_{\mathbb{F}} \left\{ g_\alpha^{(2)} \cdot g_\beta^{(2)} \;\middle|\; \alpha < \beta \right\} = \mathbb{F}[X]^2.$$

Now, without loss of generality, the intersection of $A \coloneqq \operatorname{span}\{g_1^{(1)}, \ldots, g_{k-1}^{(1)}\}$ and $B \coloneqq \operatorname{span}\{g_1^{(2)}, \ldots, g_{k-1}^{(2)}\}$ has exactly dimension $k - 2$. Denote this space by C. Since C is generated by $k-2$ linearly independent linear forms, $\mathbb{F}[X]/(C)$ is isomorphic to a polynomial ring in two variables. In particular, the set of homogeneous degree-2 polynomials of $\mathbb{F}[X]/(C)$ has exactly dimension 3. However, A and B modulo C have only one dimension. This means, modulo C they are generated by single elements γ and $\delta \in \mathbb{F}[X]/(C)$, respectively. In particular, the spaces $\operatorname{span}_{\mathbb{F}} \left\{ g_\alpha^{(1)} \cdot g_\beta^{(1)} \;\middle|\; \alpha < \beta \right\} \subset A^2$ and $\operatorname{span}_{\mathbb{F}} \left\{ g_\alpha^{(2)} \cdot g_\beta^{(2)} \;\middle|\; \alpha < \beta \right\} \subset B^2$ modulo C are generated by the elements γ^2 and δ^2, i.e. they are one-dimensional. Now, our assumption would imply that the sum of two one-dimensional spaces equals a three-dimensional space, which is clearly a contradiction.

The proof in the case $w = 3$ and $b < 2k/3$ works similarly. In this case, we have three blocks $A_i = \operatorname{span}\{g_1^{(i)}, \ldots, g_b^{(i)}\}$, $i \in \{1, 2, 3\}$, and consider the sum of intersections $C = (A_1 \cap A_2) + (A_1 \cap A_3) + (A_2 \cap A_3)$.

Positive Results. Besides the cases $w = 2$ and $w = 3$, we could not find any more parameters for which the hypothesis does not hold when $w\binom{b}{2} \geq \binom{k+1}{2}$. In fact, we think that the hypothesis is true whenever $w \geq 4$ and $w\binom{b}{2} \geq \binom{k+1}{2}$. Note that in the cases $w = 2$ and $w = 3$, the block size b needs to be larger than $k/2$. This implies in those cases that the different blocks of linear forms intersect, which leads to non-trivial dependencies for their generated 2-forms. Now, in the case $w \geq 4$ and $w\binom{b}{2} \geq \binom{k+1}{2}$, the block size b can be lower than $k/2 + 1$, which leads to (almost) no intersection of blocks. This seems to be the reason why there are no dependencies between the two-forms generated by different blocks of linear forms for $w \geq 4$. While we cannot prove this conjecture tightly, we prove the following asymptotically equivalent statement.

For all constants $c > 1$, there is a constant w_c such that the hypothesis holds whenever $w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2}$ and $w \geq w_c$ (for fields $\mathbb{F}$ of large enough size $|\mathbb{F}| \geq b$).

We prove this by considering the case of a square number of blocks $w = a^2$ of size $b \geq k/a + 1$. In this case, it is possible to give concrete candidates for the linear forms $g_1^{(i)}, \ldots, g_b^{(i)}$ of each block $i \in [w]$ and prove that

$$\sum_{i \in [w]} \operatorname{span}_{\mathbb{F}} \left\{ g_\alpha^{(i)} g_\beta^{(i)} \;\middle|\; 1 \leq \alpha < \beta \leq b \right\} = \mathbb{F}[X]^2.$$

Again, this implies that we have a degree of regularity of 2 whenever $w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2}$ and $w \geq w_c$. Since a polynomial equation system can be efficiently solved whenever it has a constant degree of regularity [ST21; Sal23; Ste24], this yields directly PPT algorithms for RSD, leading to our first main result, Theorem 2.

Learning With Bounded Errors. We can apply the same methodology as outlined above to the LWBE problem. Given an instance $(\mathbf{G} \in \mathbb{F}^{n \times k}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e} \in \mathbb{F}^n)$ where each entry of $\mathbf{e}$ lies in some set S, the Arora-Ge [AG11] modeling of the problem is given by

$$\prod_{z \in S} (y_i - g_i(X) - z) = 0, \qquad\qquad \text{for } i \in [n],$$

where $g_1, \ldots, g_n \in \mathbb{F}[X]^1$ are the linear forms that compute the rows of $\mathbf{G}$. This problem admits a PPT algorithm if its polynomial equation system has a constant degree of regularity. We will show that for $n \geq \binom{k+d-1}{d}$, the above system has a degree of regularity of d (with high probability over the size of $\mathbb{F}$). Note that the top terms of the system are given by the powers $(-g_1)^d, \ldots, (-g_n)^d$. Hence, it suffices to show that these powers of linear forms generate the space of all homogeneous polynomials of degree d. We will do so by constructing an explicit system of linear forms $g_1, \ldots, g_n$ with this property by using multivariate Vandermonde matrices.

1.2 Overview.

In the next Section 2, we will give preliminaries on code-based problems and systems of polynomial equations. Preliminaries on semi-regularity can be found in Section D. In Sections 3 and 5, we will prove our main results for RSD and LWBE, respectively. In Sections C and 4, we will provide positive and negative results for block hypotheses; in Section E, we will relate those hypotheses on polynomials to hypotheses on tensors. In Sections A, B and G, we will provide additional details for our proofs. In Section B, we will relate more assumptions of Briaud and Øygarden [BØ23] to certain polynomial block hypotheses.

Acknowledgments. We thank Pierre Briaud and Morten Øygarden for helpful discussions on algebraic attacks on RSD, and the EC reviewers for helpful comments.

2 Preliminaries

2.1 Notation

Throughout this work, $\mathbb{F}$ denotes a finite field and $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ its multiplicative group. By $\mathbb{F}_q$ we denote the field of size q. Further, $\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of natural numbers and $\mathbb{N}_0 \coloneqq \mathbb{N} \cup \{0\}$.

For $n \in \mathbb{N}$, we use the shorthand notation $[n] \coloneqq \{1, 2, \ldots, n\}$. Given a finite set S, we denote by $|S|$ its cardinality. By log, we denote the logarithm to base 2.

Matrices are denoted by upper-case bold letters $\mathbf{M}$, vectors by lower-case letters $\mathbf{v}$. Vectors $\mathbf{v} = (v_1, \ldots, v_k)$ are always column vectors, row vectors are given by their transpose $\mathbf{v}^\mathsf{T}$. The inner product of $\mathbf{v}, \mathbf{w} \in \mathbb{F}^k$ is given by $\mathbf{v}^\mathsf{T} \cdot \mathbf{w}$. Unless stated otherwise, $\mathbf{m}_i^\mathsf{T}$ denotes the i-th row of $\mathbf{M}$, $m_{i,j}$ denotes the (i, j)-th entry of $\mathbf{M}$ and v_i denotes the i-th entry of $\mathbf{v}$.

Variables are denoted by italic upper case letters, e.g. $X_1, \ldots, X_k$ and $E_1, \ldots, E_n$. Given variables $X_1, \ldots, X_k$ and $E_1, \ldots, E_n$ we denote the corresponding column vectors of variables by $X = (X_1, \ldots, X_k)$ and $E = (E_1, \ldots, E_n)$, respectively.

2.2 Regular Syndrome Decoding

Definition 1. Let $n, k \in \mathbb{N}$, $n \geq k$. Let $\mathbb{F}$ be a field. An $[n, k]$-**code** over $\mathbb{F}$ is a vector space $\mathcal{C} \subset \mathbb{F}^n$ of dimension k.

A matrix $\mathbf{G} \in \mathbb{F}^{n \times k}$ is called a **generator matrix** for $\mathcal{C}$ if $\mathcal{C}$ equals the image of $\mathbf{G}$, i.e.

$$\mathcal{C} = \left\{ \mathbf{G} \cdot \mathbf{x} \;\middle|\; \mathbf{x} \in \mathbb{F}^k \right\}.$$

A matrix $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$ is called a **parity-check matrix** for $\mathcal{C}$ if $\mathcal{C}$ equals the kernel of $\mathbf{H}$, i.e.

$$\mathcal{C} = \{\mathbf{y} \in \mathbb{F}^n \mid \mathbf{H} \cdot \mathbf{y} = 0\}.$$

Definition 2. Let $\mathbf{e} \in \mathbb{F}^n$. We define the **Hamming weight** of $\mathbf{e} = (e_1, \ldots, e_n)$ as the number of coordinates which are not zero, i.e.

$$\operatorname{hw}(\mathbf{e}) \coloneqq |\{i \in [n] \mid e_i \neq 0\}|.$$

Definition 3. Let $b, w \in \mathbb{N}$, set $n = bw$. A vector $\mathbf{e} \in \mathbb{F}^n$ is called b**-regular** if there exist vectors $\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)} \in \mathbb{F}^b$ of Hamming weight ≤ 1 such that $\mathbf{e}$ is the concatenation

$$\mathbf{e}^\mathsf{T} = \left(\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)} \right).$$

Problem 1 (Regular Syndrome Decoding)**.** Let $b, k, w \in \mathbb{N}$, $n = b \cdot w$, and let $\mathbf{H}$ be a parity check matrix $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$. The **Regular Syndrome Decoding** (RSD) problem consists of extracting a b-regular vector $\mathbf{e} \in \mathbb{F}^n$ given the parity check matrix $\mathbf{H}$ and syndrome $\mathbf{s} = \mathbf{H} \cdot \mathbf{e}$.

Remark 1. Note that we deviate from the usual notion of RSD. Usually, in the literature, each error block must contain exactly one noise term. We allow error blocks to be of Hamming-weight 0. This generalises the usual notion, and it simplifies our notation later.

In the big-field setting, this difference is (almost) not relevant. In the binary case (i.e. $\mathbb{F} = \mathbb{Z}_2$), the exact Hamming-weight case can be reduced to the problem studied by us. Indeed, given $\mathbf{H} \in \mathbb{Z}_2^{(n-k)\times n}$ and $\mathbf{s} = \mathbf{He}$ with $\mathrm{hw}(\mathbf{e}^{(1)}) = \ldots = \mathrm{hw}(\mathbf{e}^{(w)}) = 1$, we can use the linear equations

$$e_1^{(i)} + \ldots + e_b^{(i)} = 1$$

to eliminate one noise term per block. This leads to an equivalent problem $\mathbf{H}' \in \mathbb{Z}_2^{(n-k)\times(n-w)}$, $\mathbf{s}' = \mathbf{H}'\mathbf{e}'$ where $\mathbf{e}' \in \mathbb{Z}_2^{n-w}$ is $(b-1)$-regular in the sense of Definition 3. Hence, our definition of RSD is indeed a generalisation of the usual notion in literature.

RSD is the dual version of the following variation of Learning Parity with Noise.

Problem 2 (Regular Learning Parity with Noise)**.** Let $b, k, w \in \mathbb{N}$, $n = b \cdot w$, and let $\mathbf{G} \in \mathbb{F}^{n\times k}$ be a generator matrix. The **Regular Learning Parity with Noise** (RLPN) problem consists of extracting a b-regular vector $\mathbf{e} \in \mathbb{F}^n$ and a secret vector $\mathbf{x} \in \mathbb{F}^k$ from $\mathbf{G}$ and a noisy code word $\mathbf{y} = \mathbf{G} \cdot \mathbf{x} + \mathbf{e}$.

The following lemma shows that RSD has a unique solution, even over any field extension of $\mathbb{F}$, with overwhelming probability if n is large enough. Taking extensions of $\mathbb{F}$ into account is important, since this way we know exactly how the Groebner basis of a corresponding algebraic modeling of RSD looks like (cf. Corollary 1).

Lemma 1. *Let $\mathbb{F}$ be a field of size q. Denote by $\overline{\mathbb{F}}$ the algebraic closure of $\mathbb{F}$. Let $A \subset \overline{\mathbb{F}}^n$ be the set of all b-regular vectors over $\overline{\mathbb{F}}$. For $\mathbf{H} \leftarrow \mathbb{F}^{(n-k)\times n}$, we have*

$$\Pr\left[\exists \mathbf{e}, \mathbf{e}' \in A : \ \mathbf{He} = \mathbf{He}', \mathbf{e} \neq \mathbf{e}'\right] \in O\left(b^{2w} q^{2w+k-n}\right).$$

Proof. Let $\mathbf{e}, \mathbf{e}' \in A$ such that $\mathbf{He} = \mathbf{He}'$ but $\mathbf{e} \neq \mathbf{e}'$. Since $\mathbf{H}$ has only values over $\mathbb{F}$, we can assume without loss of generality that $\mathbf{e}, \mathbf{e}' \in \mathbb{F}^n$. Set $\mathbf{f} := \mathbf{e} - \mathbf{e}'$ and note that $\mathbf{f} = (\mathbf{f}^{(1)}, \ldots, \mathbf{f}^{(w)})$ admits a decomposition into blocks of length b and Hamming weight ≤ 2. If we fix $\mathbf{f} \neq 0$ and sample $\mathbf{H}$ uniformly at random, then the probability of $\mathbf{Hf} = 0$ is exactly q^{k-n}. Now, let B be the set of all such $\mathbf{f}$ that are not zero, i.e.

$$B = \left\{\mathbf{f} = (\mathbf{f}^{(1)}, \ldots, \mathbf{f}^{(w)}) \in \mathbb{F}^n \;\middle|\; \mathbf{f} \neq 0, \ \mathrm{hw}(\mathbf{f}^{(i)}) \leq 2 \ \forall i \in [w]\right\}.$$

We have for $\mathbf{H} \leftarrow \mathbb{F}^{(n-k)\times n}$

$$\Pr\left[\exists \mathbf{e}, \mathbf{e}' \in A : \ \mathbf{He} = \mathbf{He}', \mathbf{e} \neq \mathbf{e}'\right] = \Pr\left[\exists \mathbf{f} \in B : \ \mathbf{Hf} = 0\right]$$

$$\leq \sum_{\mathbf{f} \in B} \Pr\left[\mathbf{Hf} = 0\right] = \frac{|B|}{q^{n-k}} \leq \frac{\left(\binom{b+1}{2} \cdot q^2\right)^w}{q^{n-k}}. \qquad \square$$

2.3 Learning With Bounded Errors

Problem 3 (Learning With Bounded Errors)**.** Let $\mathbb{F}$ be a field. Let $k, n, d \in \mathbb{N}$, and choose subsets $S_1, \dots, S_n \subset \mathbb{F}$ each of size d.

For a generator matrix $\mathbf{G} \in \mathbb{F}^{n \times k}$, the **Learning With Bounded Errors** (LWBE) problem asks to extract $\mathbf{x} \in \mathbb{F}^k$ from $(\mathbf{G}, \mathbf{b} = \mathbf{G}\mathbf{x} + \mathbf{e})$, where $\mathbf{e} \in S_1 \times \ldots \times S_n$.

It is easy to see that the LWBE problem is equivalent to its dual version:

Problem 4 (Bounded Syndrome Decoding)**.** For a parity-check matrix $\mathbf{H} \in \mathbb{F}^{(n-k)\times n}$, the **Bounded Syndrome Decoding** (BSD) problem asks to extract $\mathbf{e}$ from $(\mathbf{H}, \mathbf{s} = \mathbf{H}\mathbf{e})$, where $\mathbf{e} \in S_1 \times \ldots \times S_n$.

The BSD problem generalises the restricted syndrome decoding problem [Bit+23] and the inhomogeneous short integer problem [Ajt96].

Lemma 2. *Let $\mathbb{F}$ be a field of size q. Denote by $\overline{\mathbb{F}}$ the algebraic closure of $\mathbb{F}$. Let $S_1, \dots, S_n \subset \mathbb{F}$ be of size d. Set $A := S_1 \times \cdots \times S_n$. For $\mathbf{H} \leftarrow \mathbb{F}^{(n-k)\times n}$, we have*

$$\Pr\left[\exists \mathbf{e}, \mathbf{e}' \in A : \ \mathbf{H}\mathbf{e} = \mathbf{H}\mathbf{e}', \mathbf{e} \neq \mathbf{e}'\right] \in O\left(d^{2n}/q^{n-k}\right).$$

Proof. We will proceed analogously to Lemma 1. Let $\mathbf{e}, \mathbf{e}' \in A$ such that $\mathbf{H}\mathbf{e} = \mathbf{H}\mathbf{e}'$ but $\mathbf{e} \neq \mathbf{e}'$. Set $\mathbf{f} := \mathbf{e} - \mathbf{e}'$ and note that $\mathbf{f}$ lies in the set

$$B := \{\alpha - \gamma \mid \alpha, \gamma \in S_1\} \times \cdots \times \{\alpha - \gamma \mid \alpha, \gamma \in S_n\}$$

of size $\leq d^{2n}$. For $\mathbf{H} \leftarrow \mathbb{F}^{(n-k)\times n}$ we have

$$\Pr\left[\exists \mathbf{e}, \mathbf{e}' \in A : \ \mathbf{H}\mathbf{e} = \mathbf{H}\mathbf{e}', \mathbf{e} \neq \mathbf{e}'\right] \leq \sum_{\mathbf{f} \in B} \Pr\left[\mathbf{H}\mathbf{f} = 0\right] = \frac{|B|}{q^{n-k}} \leq \frac{d^{2n}}{q^{n-k}}. \qquad \square$$

2.4 Learning With Rounding

Problem 5 (Learning With Rounding)**.** Let $k, n \in \mathbb{N}$, and $p < q$ be two prime numbers. If $\lceil \cdot \rfloor$ denotes the usual rounding function over the integers, we define $\lceil \cdot \rfloor_p : \mathbb{Z}_q \to \mathbb{Z}_p$ as the function that maps a to $\lceil p \cdot a/q \rfloor$. We extend $\lceil \cdot \rfloor_p$ to vectors by applying it component-wise. For a generator matrix $\mathbf{G} \in \mathbb{Z}_q^{n\times k}$, the **Learning With Rounding** (LWR) problem asks to extract $\mathbf{x} \in \mathbb{Z}_q^k$ from $(\mathbf{G}, \mathbf{b} = \lceil \mathbf{G}\mathbf{x} \rfloor_p) \in \mathbb{Z}_q^{n\times k} \times \mathbb{Z}_p^n$.

We omit the dual version of Problem 5.

2.5 Algebraic Preliminaries

Lemma 3 (Schwartz-Zippel [DL78; Zip79; Sch80])**.** *Let $\mathbb{F}$ be a field of size q. Let $f \in \mathbb{F}[X]$ such that $f \neq 0$. For $\mathbf{x} \leftarrow \mathbb{F}^n$, we have*

$$\Pr[f(\mathbf{x}) = 0] \leq \deg(f)/q.$$

Lemma 4 (Poor Man's Schwartz-Zippel)**.** *Let $\mathbb{F}$ be a field of size q. Let $f \in \mathbb{F}[X]$ such that $f \notin (X_1^q - X_1, \dots, X_n^q - X_n)$. For $\mathbf{x} \leftarrow \mathbb{F}^n$, we have*

$$\Pr[f(\mathbf{x}) = 0] \leq 1 - q^{-\deg f}.$$

A proof of Lemma 4 can be found in [Üna24].

Definition 4 (Graded Rings, Homogeneous Elements, Isomorphisms)**.** Let R be an $\mathbb{F}$-algebra. We call R a **graded** ring if it admits a decomposition into vector spaces

$$R = \bigoplus_{i=0}^{\infty} R^i$$

such that

1. $R^0 = \mathbb{F}$,
2. every R^i has a finite dimension as $\mathbb{F}$-vector space,
3. $R^i \cdot R^j \subseteq R^{i+j}$,
4. the elements of R^1 generate R as $\mathbb{F}$-algbera.

An isomorphism of two graded $\mathbb{F}$-algebras R, S is a ring isomorphism $\phi : R \to S$ that preserves the grading, i.e., we have for each i

$$\phi\left(R^i\right) = S^i.$$

We call elements in R^d **homogeneous** (for any d). The **degree** of a homogeneous element $r \in R^d$ is defined to be d. Set

$$R^{\leq d} \coloneqq \bigoplus_{i=0}^{d} R^i.$$

An ideal $I \subseteq R$ is called **homogeneous** if it is generated by homogeneous elements. This is equivalent to the existence of a decomposition $I = \bigoplus_{i=0}^{\infty} I^i$ with $I^i \subset R^i$.

Definition 5 (Formal Power Series)**.** For a formal variable T, **formal power series** are defined to be infinite sums $\sum_{i=0}^{\infty} c_i \cdot T^i$ of powers of T with integer coefficients $c_i \in \mathbb{Z}$. The set of formal power series forms a local ring.

For a power series $\mathcal{H}(T) = \sum_{i=0}^{\infty} c_i \cdot T^i$, we define its **truncation** by

$$\left[\mathcal{H}(T)\right]_+ = \sum_{i=0}^{\min\{n \in \mathbb{N}_0 \ \mid \ c_{n+1} \leq 0\}} c_i \cdot T^i.$$

Definition 6 (Hilbert Series)**.** Let R be a graded $\mathbb{F}$-algebra. The **Hilbert-series** of R is given by

$$\mathcal{H}_R(T) \coloneqq \sum_{i=0}^{\infty} \dim_{\mathbb{F}}\left(R^i\right) \cdot T^i.$$

Definition 7 (Degree of Regularity)**.** Let $I \subseteq R$ be a homogeneous ideal. The **degree of regularity** of I is given by

$$\mathrm{d}_{\mathsf{reg}}(I) = \min\left(\left\{d \in \mathbb{N}_0 \;\middle|\; I^d = R^d\right\} \cup \{\infty\}\right).$$

For an element $f \in R$ of degree d, there is a unique decomposition

$$f = f^{(0)} + \ldots + f^{(d)}$$

with $f^{(0)} \in R^0, \ldots, f^{(d)} \in R^d$ and $f^{(d)} \neq 0$. We define the **top-term** of f by

$$f^{\mathsf{top}} := f^{(d)}$$

We define the **degree of regularity** of a sequence $f_1, \ldots, f_m \in R$ by

$$\mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m) := \mathrm{d}_{\mathsf{reg}}((f_1^{\mathsf{top}}, \ldots, f_m^{\mathsf{top}})).$$

Lemma 5. *Let $M(X) \in (\mathbb{F}[X_1, \ldots, X_n])^{m_1 \times m_2}$ be such that the degree of each entry of M is bounded by d.*

If there exists $x \in \mathbb{F}^n$, such that $M(x)$ has full rank $m = \min(m_1, m_2)$, then we have

$$\Pr_{x \leftarrow \mathbb{F}^n}[M(x) \text{ has full rank}] \geq \max\left(1 - \frac{d \cdot m}{|\mathbb{F}|}, |\mathbb{F}|^{-d \cdot m}\right).$$

Proof. Let $A(X) \in (\mathbb{F}[X])^{m \times m}$ be a submatrix of $M(X)$ such that $A(x)$ is invertible. Since $\det A(x) \neq 0$, $\det A(X) \in \mathbb{F}[X]$ is not the zero polynomial. The claim now follows by Lemmas 3 and 4 and observing that $\deg(\det A(X)) \leq m \cdot d$. □

For large fields, a minimal degree of regularity is persistent:

Lemma 6. *Let $f_1, \ldots, f_m \in R$ be homogeneous of degrees $d_1, \ldots, d_m$. For $g_1 \leftarrow R^{d_1}, \ldots, g_m \leftarrow R^{d_m}$, we have*

$$\Pr\left[\mathrm{d}_{\mathsf{reg}}(g_1, \ldots, g_m) > \mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m)\right] \leq \min\left(\frac{D}{|\mathbb{F}|}, 1 - |\mathbb{F}|^{-D}\right),$$

where $D = \dim_{\mathbb{F}} R^{\mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m)}$.

Proof. Set $d := \mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m)$. Consider the linear map

$$\begin{aligned} \mu : R^{d_1} \times \cdots \times R^{d_m} &\longrightarrow \mathrm{Hom}_{\mathbb{F}}\left(R^{d-d_1} \times \cdots \times R^{d-d_m}, R^d\right) \\ (a_1, \ldots, a_m) &\longmapsto \left[(h_1, \ldots, h_m) \mapsto a_1 \cdot h_1 + \ldots + a_m \cdot h_m\right]. \end{aligned}$$

For each $(g_1, \ldots, g_m) \in R^{d_1} \times \cdots \times R^{d_m}$, $\mu(g_1, \ldots, g_m)$ is a linear map of type $R^{d-d_1} \times \cdots \times R^{d-d_m} \to R^d$. Let ϕ be a linear isomorphism

$$\phi : \mathbb{F}^N \longrightarrow R^{d_1} \times \cdots \times R^{d_m}$$

and let ψ be a canonical linear isomorphism

$$\psi : \mathrm{Hom}_{\mathbb{F}}\left(R^{d-d_1} \times \cdots \times R^{d-d_m}, R^d\right) \longrightarrow \mathbb{F}^{M \times D}$$

that maps each linear $L : R^{d-d_1} \times \cdots \times R^{d-d_m} \to R^d$ to its matrix representation in $\mathbb{F}^{\dim_{\mathbb{F}}(R^{d-d_1} \times \cdots \times R^{d-d_m}) \times \dim_{\mathbb{F}}(R^d)} = \mathbb{F}^{M \times D}$. The composition $\psi \circ \mu \circ \phi$ is linear and maps vectors to matrices. Hence, we can interpret it as a matrix whose entries are degree-1 polynomials in a polynomial ring over $\mathbb{F}$. The claim now follows from Lemma 5 (where the full rank is D). □

Salizzoni and Steiner both proved that Mutant-XL algorithms [Din+08] can compute Groebner bases in polynomial time if the degree of regularity is constant [Sal23; Ste24]. We recall the results of Salizzoni here.

Theorem 1 ([Sal23]). *There exists an algorithm $\mathcal{A}$ that on input $f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ outputs the minimal Groebner basis of $(f_1, \ldots, f_m)$ (with respect to some monomial degree-ordering) if $\mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m) \geq \deg(f_i)$ for all $i \in [m]$.*

The time complexity of $\mathcal{A}$ lies in $O(n^{4(1+\mathrm{d}_{\mathsf{reg}}(f_1,\ldots,f_m))})$.

Corollary 1. *Let $f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ with $\mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m) \geq \deg(f_i)$ for all $i \in [m]$.*

1. *If the system $f_1(X) = \ldots = f_m(X) = 0$ is insatisfiable over the algebraic closure of $\mathbb{F}$, then algorithm $\mathcal{A}$ of Theorem 1 outputs 1 as Groebner basis.*
2. *If $f_1(X) = \ldots = f_m(X) = 0$ has exactly one solution $\mathbf{x}$ over the algebraic closure of $\mathbb{F}$, then $\mathbf{x}$ lies in $\mathbb{F}^n$ and $\mathcal{A}$ outputs*

$$(X_1 - x_1)^{e_1}, \ldots, (X_n - x_n)^{e_n}$$

for some $e_1, \ldots, e_n \leq \mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m)$.

Proof. For the first claim, note that $f_1(X) = \ldots = f_m(X) = 0$ is satisfiable if and only if $1 \notin (f_1, \ldots, f_m)$.

For the second claim, note that solutions of $f_1(X) = \ldots = f_m(X) = 0$ are invariant under the action of the Galois group of the algebraic closure over $\mathbb{F}$. Hence, $\mathbf{x}$ needs to have entries in $\mathbb{F}$. Because of Hilbert's Nullstellensatz, we have

$$(f_1, \ldots, f_m) = ((X_1 - x_1)^{e_1}, \ldots, (X_n - x_n)^{e_n})$$

for some $e_1, \ldots, e_n \in \mathbb{N}$. Naturally, we must have $e_1, \ldots, e_n \leq \mathrm{d}_{\mathsf{reg}}(f_1, \ldots, f_m)$. Since $(X_1 - x_1)^{e_1}, \ldots, (X_n - x_n)^{e_n}$ is the minimal Groebner basis of $(f_1, \ldots, f_m)$, the claim follows. □

3 Regular Syndrome Decoding

Let $\mathbb{F}$ be a field of size q and let $b, k, w \in \mathbb{N}$. Set $n = bw$. The main result of this section are given by the following two claims.

Theorem 2.

1. *For every constant $c > 1$, there exists a poly-time algorithm $\mathcal{S}_c$ that solves RSD instances $(\mathbf{H} \in \mathbb{F}^{(n-k)\times n}, \mathbf{s} \in \mathbb{F}^n)$ with w blocks of size b. The success probability of $\mathcal{S}_c$ is at least*

$$\geq 1 - \frac{(k+1)k}{2q} - \frac{b^{2w} q^{2w+k}}{q^n},$$

over the randomness of $\mathbf{H} \leftarrow \mathbb{F}^{(n-k)\times n}$ whenever $q \geq b - 1$ and

$$w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2}.$$

2. *For every constant $c > 1$, there exists a poly-time algorithm $\mathcal{S}'_c$ that solves RSD instances $(\mathbf{H} \in \mathbb{F}^{(n-k)\times n}, \mathbf{s} \in \mathbb{F}^n)$ with w blocks of size b. The success probability of $\mathcal{S}'_c$ is at least*

$$\geq 1 - \frac{(k+1)k}{2q} - \frac{b^{2w} q^{2w+k}}{q^n},$$

over the randomness of $\mathbf{H} \leftarrow \mathbb{F}^{(n-k)\times n}$ *whenever* $q \geq \sqrt{b}$ *and*

$$w \cdot \binom{b}{2} \geq c \cdot \frac{9}{4} \cdot \binom{k+1}{2}.$$

Note that both claims differ in minor technical points. The first claim allows for a tighter inequality, but requires a larger field of size b. The second claim requires a larger constant in the inequality, but allows for smaller fields of size $\sqrt{b}$.

To solve the RSD problem, Briaud and Øygarden introduced the following system of polynomial equations.

Modeling 1 (Dual modeling, Briaud-Øygarden [BØ23])**.** Let $(\mathbf{H}, \mathbf{s} = \mathbf{He})$ be an instance of the RSD problem such that $\mathbf{H} \in \mathbb{F}^{n-k\times n}$ and $\mathbf{e} = (\mathbf{e}^{(1)}, \ldots, \mathbf{e}^{(w)}) \in \mathbb{F}^n$ is b-regular. Introduce formal variables

$$E_1^{(1)}, \ldots, E_b^{(1)}, \ldots, E_1^{(w)}, \ldots, E_b^{(w)}.$$

Denote by $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]^1$ linear forms that correspond to the rows of H, i.e.

$$h_i(E) \coloneqq \mathbf{h}_i^{\mathsf{T}} \cdot \left(E_1^{(1)}, \ldots, E_b^{(1)}, \ldots, E_1^{(w)}, \ldots, E_b^{(w)}\right).$$

The **dual** or **Briaud-Øygarden** modeling of the problem $(\mathbf{H}, \mathbf{s} = \mathbf{He})$ is given by the polynomial equations

$$\begin{aligned} E_\alpha^{(i)} \cdot E_\beta^{(i)} &= 0, &&\text{for } i \in [w], 1 \leq \alpha < \beta \leq b,\\ h_i(E) - s_i &= 0, &&\text{for } i \in [n-k]. \end{aligned}$$

To bound the time complexity of algebraic algorithms solving Modeling 1, Briaud and Øygarden [BØ23] assume the following for all parameters $b, k, w \in \mathbb{N}$.

Hypothesis 1 ([BØ23], Assumption 1)**.** Set

$$Q' \coloneqq \mathbb{F}[E_1^{(1)}, \ldots, E_b^{(1)}, \ldots, E_1^{(w)}, \ldots, E_b^{(w)}]/(E_\alpha^{(i)} \cdot E_\beta^{(i)} | i \in [w], 1 \leq \alpha < \beta \leq b).$$

If we draw $h_1, \ldots, h_{n-k} \leftarrow \mathbb{F}[E]^1$ uniformly at random, then the sequence $h_1, \ldots, h_{n-k}$ is semi-regular with respect to Q' with high probability.

Note that Hypothesis 1 implies that the Hilbert-series of $Q \coloneqq Q'/(h_1, \ldots, h_{n-k})$ for $h_1, \ldots, h_{n-k} \leftarrow \mathbb{F}[E]^1$ is given by

$$\mathcal{H}_Q(T) = \left[(1-T)^{n-k} \cdot \left(1 + bT + bT^2 + \ldots\right)^w\right]_+$$

with some high probability (cf. Section D for details). Because of Lemma 6, this is equivalent to the following hypothesis for parameters $b, k, w, \mathbb{F}$.

Hypothesis 2. There exist linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]^1$ such that we have for $Q = Q'/(h_1, \ldots, h_{n-k})$

$$\mathcal{H}_Q(T) = \left[(1-T)^{n-k} \cdot \left(1 + bT + bT^2 + \ldots\right)^w\right]_+.$$

Lemma 18, which we prove in Section A, implies that we have

$$(1-T)^{n-k} \cdot \left(1 + bT + bT^2 + \ldots\right)^w = 1 + kT + \left(\binom{k+1}{2} - w \cdot \binom{b}{2}\right) T^2 + O(T^3).$$

I.e., Hypothesis 1 implies a degree of regularity 2 whenever we have $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$. This is no coincidence. In the following, we will relate Modeling 1 by the use of ring isomorphisms to another modeling with $w \cdot \binom{b}{2}$ quadratic equations over k variables. For parameters $k, b, w \in \mathbb{N}$, $n = bw$, and a field $\mathbb{F}$, let $\mathbf{H} \in \mathbb{F}^{(n-k)\times n}$, $\mathbf{G} \in \mathbb{F}^{n\times k}$ be a parity-check and a generator matrix of the same code. Given an RSD problem $(\mathbf{H}, \mathbf{s} = \mathbf{H})$, we can convert it to a regular LPN problem $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e})$ and consider the following modeling for it.

Modeling 2. For a regular LPN problem $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e})$, decompose $\mathbf{G}$ into blocks

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}^{(1)} \\ \vdots \\ \mathbf{G}^{(w)} \end{pmatrix} \quad \text{of shape } b \times k \text{ with rows} \quad \mathbf{G}^{(i)} = \begin{pmatrix} \mathbf{g}_1^{(i)} \\ \vdots \\ \mathbf{g}_b^{(i)} \end{pmatrix}.$$

Also, decompose $\mathbf{y} = (\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(w)}) = ((y_1^{(1)}, \ldots, y_b^{(1)}), \ldots, (y_1^{(w)}, \ldots, y_b^{(w)}))$. Let $g_1^{(1)}, \ldots, g_b^{(1)}, \ldots, g_1^{(w)}, \ldots, g_b^{(w)} \in \mathbb{F}[X_1, \ldots, X_k]^1$ be linear forms that correspond to the rows of $\mathbf{G}$, i.e.

$$g_\alpha^{(i)}(X) \coloneqq (\mathbf{g}_\alpha^{(i)})^\intercal \cdot X.$$

The **primal** or **Arora-Ge** modeling is given by

$$(g_\alpha^{(i)}(X) - y_\alpha^{(i)}) \cdot (g_\beta^{(i)}(X) - y_\beta^{(i)}) = 0, \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

Both modelings share the same degree of regularity as the following lemma shows.

Lemma 7. *The ring Q from Hypothesis 1 is isomorphic to the ring R given by*

$$R \coloneqq \mathbb{F}[X] / \left((g_\alpha^{(i)}(X) \cdot g_\beta^{(i)}(X)) | i \in [w], 1 \leq \alpha < \beta \leq b\right).$$

This isomorphism preserves the gradings of both rings.

Proof. The map $\mathbf{G} : \mathbb{F}^k \to \mathbb{F}^n$ induces a dual ring morphism

$$\mathbf{G}^* : \mathbb{F}[E] \longrightarrow \mathbb{F}[X]$$

on the coordinate rings by

$$E_\alpha^{(i)} \longmapsto g_\alpha^{(i)}.$$

Since $\mathbf{G}$ is linear, it preserves the degree of its inputs. The kernel of $\mathbf{G}^*$ is given by $(h_1, \ldots, h_{n-k})$, hence, we have the isomorphism

$$\mathbb{F}[E]/(h_1, \ldots, h_{n-k}) \xrightarrow{\sim} \mathbb{F}[X].$$

Under this isomorphism, the element $E^{(i)}_\alpha \cdot E^{(i)}_\beta$ gets mapped to $g^{(i)}_\alpha \cdot g^{(i)}_\beta$. In particular, the ideal

$$(E^{(i)}_\alpha \cdot E^{(i)}_\beta | i \in [w], 1 \leq \alpha < \beta \leq b) \subset \mathbb{F}[E]$$

gets mapped to the ideal

$$(g^{(i)}_\alpha \cdot g^{(i)}_\beta | i \in [w], 1 \leq \alpha < \beta \leq b) \subset \mathbb{F}[X].$$

Hence, we have a grade-preserving isomorphism $Q \to R$. □

A more general version of Lemma 7 is given in Section B. Now, consider the following hypothesis for the primal modeling:

Hypothesis 3. For parameters $b, k, w \in \mathbb{N}$ and a field $\mathbb{F}$, there are linear forms

$$g^{(1)}_1, \ldots, g^{(1)}_b, \ldots, g^{(w)}_1, \ldots, g^{(w)}_b \in \mathbb{F}[X_1, \ldots, X_k]^1$$

such that

$$V_1 + \ldots + V_w = \mathbb{F}[X]^2,$$

where

$$V_i = \operatorname{span}_{\mathbb{F}} \left\{ g^{(i)}_\alpha \cdot g^{(i)}_\beta \;\middle|\; 1 \leq \alpha < \beta \leq b \right\}.$$

Note that a necessary condition for Hypothesis 3 to be true is the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$. On the other hand, Lemma 18 and Hypothesis 2 imply that Hypothesis 3 must hold whenever $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$. Hence, to study the correctness of Hypotheses 1 and 2 it suffices to study Hypothesis 3. We will do this in more generality in Section 4. We will show the following theorem, i.e. Hypothesis 3 is wrong in general, however, correct for all relevant cases in practice.

Theorem 3. *Let $b, k, w \in \mathbb{N}$, $n = bw$. Let $\mathbb{F}$ be a finite field of size q. Hypotheses 2 and 3 are wrong if:*

1. $w = 2$, $b < k$,
2. $w = 3$, $b < 2k/3$.

Hypotheses 2 and 3 are true if:

3. $w = 2$, $b \geq k$, $b > 1$,
4. $w = 3$, $b \geq 2k/3 + 1$,
5. $w \geq \binom{k+1}{2}$ *and* $b \geq 2$,
6. $w \geq a^2$ *for some* $a \in \mathbb{N}$ *and* $b \geq k/a + 1$, $q \geq b - 1$,
7. $w \geq \lceil k/(b-1) \rceil^2$ *and* $q \geq b - 1$,
8. $w \geq a + 3\binom{a}{2}$ *for some* $a \in \mathbb{N}$, $b \geq k/a + 1$, $q^2 \geq b - 1$,
9. $w \geq \frac{c}{(\sqrt{c}-1)^2}$, $q \geq b - 1$ *and* $w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2}$ *for each constant* $c > 1$.
10. $w \geq 3\frac{c}{(\sqrt{c}-1)^2}$, $q^2 \geq b$ *and* $w \cdot \binom{b}{2} \geq c \cdot \frac{9}{4} \cdot \binom{k+1}{2}$ *for each constant* $c > 1$.

Proof. The statements for two blocks follow from Lemmas 9 to 11. The statements for three blocks follow from Lemmas 9, 25 and 26. The statement for blocks of size at least 2 follows from Lemmas 9 and 30. The statements for a square number of blocks follow from Lemmas 9, 12 and 27. The seventh statement follows from the fourth by setting $a = \lceil k/(b-1) \rceil$. The eighth statement follows from Lemma 28 and Lemma 29 depending on the characteristic of the field. The ninth and tenth statements assert that the hypothesis is asymptotically true. I.e., for each constant $c > 1$, the hypothesis is true if $w \cdot \binom{b}{2} \geq c \cdot 1.5 \cdot \binom{k+1}{2}$ respectively $w \cdot \binom{b}{2} \geq c \cdot 2.25 \cdot \binom{k+1}{2}$, and w is large enough. We prove these results in Lemmas 13 and 31 by bootstrapping them on the case of $w = a^2$ and $w = a + \binom{a}{2}$, respectively. The general cases of $w \geq a^2$ and $w \geq a + \binom{a}{2}$ follow from Lemma 9. □

Let us conclude this section with the proof of Theorem 2:

Theorem 2. 1. Let $c > 1$ be constant. Let $w_c = \frac{c}{(\sqrt{c}-1)^2}$ be the constant from Lemma 13. Let $\mathbb{F}$ be a field of size $q \geq b-1$. Let $(\mathbf{G} \in \mathbb{F}^{n \times k}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e} \in \mathbb{F})$ be an RLPN instance with $w \geq w_c$ error blocks of size b. Lemmas 6 and 13 imply that Modeling 2 for $(\mathbf{G}, \mathbf{y})$ has degree of regularity 2 with probability $\geq 1 - \frac{\dim_{\mathbb{F}}(\mathbb{F}[X]^2)}{q} = 1 - \binom{k+1}{2}/q$ if we draw $\mathbf{G} \leftarrow \mathbb{F}^{n \times k}$ uniformly at random. Lemma 1 implies that $(\mathbf{G}, \mathbf{y})$ has a unique solution $\mathbf{x}$ with probability $\geq 1 - \frac{b^{2w}q^{2w+k}}{q^n}$. Corollary 1 implies now that an algebraic algorithm can solve $(\mathbf{G}, \mathbf{y})$ in time $O(k^{12})$ with probability at least $\geq 1 - \frac{\dim_{\mathbb{F}}(\mathbb{F}[X]^2)}{q} - \frac{b^{2w}q^{2w+k}}{q^n}$.

   On input an RLPN instance $(\mathbf{G}, \mathbf{y})$ for w blocks of size b and k secret dimensions, $\mathcal{S}_c$ now proceeds as follows: If $w < w_c$, then $\mathcal{S}_c$ guesses $b-1$ error-free positions in each block and tries to solve the RSD instance by linear algebra. This has a time complexity of $O(k^3 b^{w_c})$, which is polynomial, since w_c is constant. If $w \geq w_c$, $\mathcal{S}_c$ uses Salizzoni's algorithm to solve Modeling 2 for $(\mathbf{G}, \mathbf{y})$. Because of Lemmas 1, 6 and 13 and Corollary 1, this has a success probability of at least

$$\geq 1 - \frac{\dim_{\mathbb{F}}(\mathbb{F}[X]^2)}{q} - \frac{b^{2w}q^{2w+k}}{q^n}$$

   and a time complexity in $O(k^{12})$.

2. Let $c > 1$ and $w_c = 3 \cdot \frac{c}{(\sqrt{c}-1)^2}$. On input an RLPN instance with w blocks of size b and code dimension k, $\mathcal{S}'_c$ proceeds similarly to $\mathcal{S}_c$: If $w < w_c$, $\mathcal{S}'_c$ solves the problem by brute-force in time $O(k^3 b^{w_c})$. Otherwise, it uses Mutant-XL to solve Modeling 2. Because of Lemmas 1, 6 and 31 and Corollary 1, this has a success probability of $1 - \frac{\dim_{\mathbb{F}}(\mathbb{F}[X]^2)}{q} - \frac{b^{2w}q^{2w+k}}{q^n}$ and a time complexity in $O(k^{12})$ if $q^2 \geq b$, $w \cdot \binom{b}{2} \geq c \cdot \frac{9}{4} \cdot \binom{k+1}{2}$ and the generator matrix of the problem is sampled uniformly at random. □

4 Block Hypotheses

In this section, we study for which parameter ranges Hypothesis 3 is true or false. Remember that Hypothesis 3 is true for $b, k, w \in \mathbb{N}$ and a field $\mathbb{F}$ if there are linear forms $f_\alpha^{(i)} \in \mathbb{F}[X]^1 = \mathbb{F}[X_1, \ldots, X_k]^1$, $i \in [w], \alpha \in [b]$ such that

$$V_1 + \ldots + V_w = \mathbb{F}[X]^2$$

where for $i \in [w]$

$$V_i \coloneqq \operatorname{span}_{\mathbb{F}} \left\{ f^{(i)}_\alpha \cdot f^{(i)}_\beta \;\middle|\; 1 \le \alpha < \beta \le b \right\}.$$

Since the dimension of each V_i is bounded by $\binom{b}{2}$, a necessary condition for Hypothesis 3 to be true is the inequality

$$w \cdot \binom{b}{2} \ge \dim_{\mathbb{F}}(V_1 + \ldots + V_w) = \dim_{\mathbb{F}}(\mathbb{F}[X]^2) = \binom{k+1}{2}.$$

Since a space V_i does not need to contain the square elements $(f^{(i)}_1)^2, \ldots, (f^{(i)}_b)^2$, Hypothesis 3 is a bit complicated to understand. Therefore, we will introduce the following simpler hypothesis.

Hypothesis 4. For parameters $b, k, w \in \mathbb{N}$ and a field $\mathbb{F}$, there are linear forms

$$f^{(1)}_1, \ldots, f^{(1)}_b, \ldots, f^{(w)}_1, \ldots, f^{(w)}_b \in \mathbb{F}[X_1, \ldots, X_k]^1$$

such that

$$\overline{V_1} + \ldots + \overline{V_w} = \mathbb{F}[X]^2$$

where $\overline{V_i} = \operatorname{span}_{\mathbb{F}} \left\{ f^{(i)}_\alpha \cdot f^{(i)}_\beta \;\middle|\; 1 \le \alpha \le \beta \le b \right\}$.

Note that the inequality $w \cdot \binom{b+1}{2} \ge \binom{k+1}{2}$ must hold for Hypothesis 4 to be true. Hypotheses 3 and 4 are related as the following lemma shows:

Lemma 8. *Hypothesis 3 for $(b, k, w, \mathbb{F})$ implies Hypothesis 4 for $(b, k, w, \mathbb{F})$.*

Hypothesis 4 for $(b, k, w, \mathbb{F})$ implies Hypothesis 3 for $(b + 1, k, w, \mathbb{F})$.

Proof. The first direction is easy to see, as $V_i \subseteq \overline{V_i}$.

For the other direction, let $f^{(1)}_1, \ldots, f^{(1)}_b, \ldots, f^{(w)}_1, \ldots, f^{(w)}_b \in \mathbb{F}[X]^1$ such that

$$\overline{V}_1 + \ldots + \overline{V}_w = \mathbb{F}[X]^2.$$

For each $i \in [w]$, we define

$$f^{(i)}_{b+1} \coloneqq f^{(i)}_1 + \ldots + f^{(i)}_b.$$

Now, let $V_i = \operatorname{span}_{\mathbb{F}} \left\{ f^{(i)}_\alpha \cdot f^{(i)}_\beta \;\middle|\; 1 \le \alpha < \beta \le b + 1 \right\}$. We claim that $\overline{V}_i = V_i$. Indeed, it is easy to see that $V_i \subseteq \overline{V}_i$. On the other hand, all squares $(f^{(i)}_1)^2, \ldots, (f^{(i)}_b)^2$ are contained in V_i, since

$$(f^{(i)}_j)^2 = f^{(i)}_{b+1} \cdot f^{(i)}_j - \sum_{\ell \in [b] \setminus \{j\}} f^{(i)}_\ell \cdot f^{(i)}_j$$

and V_i contains $f^{(i)}_{b+1} f^{(i)}_j, f^{(i)}_1 \cdot f^{(i)}_j, \ldots, f^{(i)}_b \cdot f^{(i)}_j$. It follows $\overline{V}_i = V_i$, and therefore

$$V_1 + \ldots + V_w = \overline{V}_1 + \ldots + \overline{V}_w = \mathbb{F}[X]^2. \qquad \square$$

We will now turn to proving several negative and positive results for different parameter ranges. Because of limited space, most of the lemmas have been moved to Section C. The following observation will prove useful in general:

Lemma 9. *Let $b, b', k, k', w, w' \in \mathbb{N}$ such that $b \leq b'$, $k \geq k'$, $w \leq w'$. Let $\mathbb{F} \subseteq \mathbb{F}'$ be an extension of fields.*

Hypothesis 3 and Hypothesis 4 for $(b, k, w, \mathbb{F})$ imply Hypothesis 3 and Hypothesis 4 for $(b', k', w', \mathbb{F}')$, respectively.

Proof. We show the claim only for Hypothesis 3, as the proof for Hypothesis 4.

If Hypothesis 3 holds for $(b, k, w, \mathbb{F})$, then there are linear forms $f_\alpha^{(i)} \in \mathbb{F}[X_1, \ldots, X_k]^1$, $i \in [w]$,$\alpha \in [b]$, s.t. $V_1 + \ldots + V_w = \mathbb{F}[X_1, \ldots, X_k]^2$ where $V_i = \operatorname{span}_{\mathbb{F}}\{f_\alpha^{(i)} \cdot f_\beta^{(i)} \mid 1 \leq \alpha < \beta \leq b\}$. Denote by $\phi : \mathbb{F}[X_1, \ldots, X_k] \to \mathbb{F}[X_1, \ldots, X_{k'}]$ the surjective morphism that sends X_i to X_i, if $i \leq k'$, and to 0, if $i > k'$. We define linear forms $g_\alpha^{(i)} \in \mathbb{F}[X_1, \ldots, X_{k'}]^1$, $\alpha \in [b']$, $i \in [w']$, by

$$g_\alpha^{(i)}(X_1, \ldots, X_{k'}) \coloneqq \begin{cases} \phi(f_\alpha^{(i)}(X)), & \text{if } \alpha \leq b \text{ and } i \leq w, \\ 0, & \text{if } \alpha > b \text{ or } i > w. \end{cases}$$

Further, set $W_i \coloneqq \operatorname{span}_{\mathbb{F}}\{g_\alpha^{(i)} \cdot g_\beta^{(i)} \mid 1 \leq \alpha < \beta \leq b'\}$ for $i \in [w']$. We have $W_i = \phi(V_i)$ for $i \in [w]$. Hence,

$$W_1 + \ldots + W_{w'} = \phi(V_1 + \ldots + V_w) + 0 + \ldots + 0 = \phi(\mathbb{F}[X_1, \ldots, X_k]^2) = \mathbb{F}[X_1, \ldots, X_{k'}]^2$$

and Hypothesis 3 is true for $(b', k', w', \mathbb{F})$. The soundness of Hypothesis 3 for $(b', k', w', \mathbb{F}')$ follows from the fact that $\operatorname{span}_{\mathbb{F}}(W_1 + \ldots + W_{w'})$ contains all monomials X_iX_j for $1 \leq i, j \leq k'$. □

Lemma 10. *Let $b, k \in \mathbb{N}$, $k > 2$, $w = 2$ and let $\mathbb{F}$ be any field. If $b < k$, then Hypotheses 3 and 4 are false.*

Proof. It suffices to refute Hypothesis 4 in the case $b = k - 1$.

Assume that Hypothesis 4 does hold and let $f_1^{(1)}, \ldots, f_{k-1}^{(1)}, f_1^{(2)}, \ldots, f_{k-1}^{(2)} \in \mathbb{F}[X]^1$ be such that $\overline{V_1} + \overline{V_2} = \mathbb{F}[X]^2$. Set

$$A \coloneqq \operatorname{span}_{\mathbb{F}}\{f_1^{(1)}, \ldots, f_{k-1}^{(1)}\} \qquad \text{and} \qquad B \coloneqq \operatorname{span}_{\mathbb{F}}\{f_1^{(2)}, \ldots, f_{k-1}^{(2)}\}.$$

Without loss of generality, we can assume that we have

$$\dim_{\mathbb{F}} A = \dim_{\mathbb{F}} B = k - 1.$$

Indeed, if, let's say, A does not have full dimensions, we could replace $f_1^{(1)}, \ldots, f_{k-1}^{(1)}$ by linear independent $g_1, \ldots, g_{k-1} \in \mathbb{F}[X]^1$ such that

$$\begin{aligned} A &\subset \operatorname{span}_{\mathbb{F}}\{g_1, \ldots, g_{k-1}\}, \\ \overline{V_1} &\subset \operatorname{span}_{\mathbb{F}}\{g_\alpha \cdot g_\beta \mid 1 \leq \alpha \leq \beta \leq k-1\}. \end{aligned}$$

It would then suffice to refute the hypothesis for $g_1, \ldots, g_{k-1}$ and $f_1^{(2)}, \ldots, f_{k-1}^{(2)}$.

Hence, we assume that A and B have full dimension $k - 1$. We can further assume that A and B are different vector spaces, since, otherwise, the dimension of $\overline{V}_1 + \overline{V}_2 = \overline{V}_1$ would be smaller than the dimension of $\mathbb{F}[X]^2$. Thus,

$$\dim_{\mathbb{F}}(A \cap B) = k - 2.$$

Let $h_1, \dots, h_{k-2}$ be a basis of $A \cap B$ and choose $f_*^{(1)}, f_*^{(2)} \in \mathbb{F}[X]^1$ such that

$$A = \mathrm{span}_{\mathbb{F}}\{h_1, \dots, h_{k-2}, f_*^{(1)}\}, \qquad B = \mathrm{span}_{\mathbb{F}}\{h_1, \dots, h_{k-2}, f_*^{(2)}\}.$$

For $i \in \{1, 2\}$, we then have

$$\begin{aligned} \overline{V}_i &= \mathrm{span}_{\mathbb{F}} \left\{ f_\alpha^{(i)} \cdot f_\beta^{(i)} \;\middle|\; 1 \le \alpha \le \beta \le b \right\} \\ =&\mathrm{span}_{\mathbb{F}} \left\{ h_\alpha \cdot h_\beta \mid 1 \le \alpha \le \beta \le k-2 \right\} + \mathrm{span}_{\mathbb{F}} \left\{ h_\alpha \cdot f_*^{(i)} \;\middle|\; \alpha \in [k-2] \right\} + \mathrm{span}_{\mathbb{F}}\{(f_*^{(i)})^2\}. \end{aligned}$$

In particular, we have

$$\begin{aligned} \overline{V}_1 + \overline{V}_2 = &\mathrm{span}_{\mathbb{F}} \left\{ h_\alpha \cdot h_\beta \mid 1 \le \alpha \le \beta \le k-2 \right\} + \mathrm{span}_{\mathbb{F}} \left\{ h_\alpha \cdot f_*^{(1)} \;\middle|\; \alpha \in [k-2] \right\} \\ &+ \mathrm{span}_{\mathbb{F}} \left\{ h_\alpha \cdot f_*^{(2)} \;\middle|\; \alpha \in [k-2] \right\} + \mathrm{span}_{\mathbb{F}}\{(f_*^{(1)})^2\} + \mathrm{span}_{\mathbb{F}}\{(f_*^{(2)})^2\}. \end{aligned}$$

Now, the dimension of $\overline{V}_1 + \overline{V}_2$ can be upper-bounded by

$$\begin{aligned} &\dim_{\mathbb{F}}(\overline{V}_1 + \overline{V}_2) \le \binom{k-1}{2} + 2(k-2) + 2 \\ =&\frac{(k-1)(k-2)}{2} + 2k - 2 = \frac{k^2}{2} - \frac{3}{2}k + 1 + 2k - 2 = \frac{k^2 + k}{2} - 1. \end{aligned}$$

This is smaller than the dimension $\binom{k+1}{2}$ of $\mathbb{F}[X]^2$. This contradicts Hypothesis 4. □

Lemma 11. *Let $b, k \in \mathbb{N}$, $k > 2$, $w = 2$ and let $\mathbb{F}$ be any field. If $b \ge k$, then Hypotheses 3 and 4 are true.*

Proof. It suffices to prove Hypothesis 3 in the case $b = k$.

In this case, we can choose for the first block

$$f_1^{(1)}(X) \coloneqq X_1, \qquad f_2^{(1)}(X) \coloneqq X_2, \qquad \dots, \qquad f_k^{(1)}(X) = X_k,$$

and for the second block

$$f_1^{(2)}(X) \coloneqq X_1 + X_2, \quad f_2^{(2)}(X) \coloneqq X_2 + X_3, \quad \dots, \quad f_k^{(2)}(X) = X_k + X_1.$$

Now, the first block

$$V_1 = \mathrm{span}_{\mathbb{F}} \left\{ f_\alpha^{(1)} \cdot f_\beta^{(1)} \;\middle|\; 1 \le \alpha < \beta \le b \right\} = \mathrm{span}_{\mathbb{F}} \left\{ X_\alpha \cdot X_\beta \mid 1 \le \alpha < \beta \le k \right\}$$

contains all degree-2 monomials of different variables. To prove $V_1 + V_2 = \mathbb{F}[X]^2$, we need to argue that the remaining square monomials $X_1^2, \dots, X_k^2$ are contained in $V_1 + V_2$.

Let $i \in [k]$, $i > 1$, and consider

$$f_{i-1}^{(2)}(X) \cdot f_i^{(2)}(X) = (X_{i-1} + X_i)(X_i + X_{i+1}) = X_i^2 + X_{i-1}X_i + X_iX_{i+1} + X_{i-1}X_{i+1}.$$

$X_i^2 + X_{i-1}X_i + X_iX_{i+1} + X_{i-1}X_{i+1}$ is contained in V_2. Since V_1 contains $X_{i-1}X_i, X_iX_{i+1}$ and $X_{i-1}X_{i+1}$, it follows that $V_1 + V_2$ contains X_i^2 for $i = 2, \dots, k$. For X_1^2, note that V_2 contains

$$f_1^{(2)}(X) \cdot f_k^{(2)}(X) = (X_1 + X_2)(X_k + X_1) = X_1^2 + X_1X_2 + X_1X_k + X_2X_k.$$

Since V_1 contains $X_1X_2 + X_1X_k + X_2X_k$, $V_1 + V_2$ contains X_1^2. It follows that $V_1 + V_2$ contains all degree-2 monomials and we have

$$V_1 + V_2 = \mathbb{F}[X]^2. \qquad \square$$

Because of limited space, we had to move the proofs for $w = 3$ to Section C. We now prove the correctness of the hypothesis for a square number of blocks:

Lemma 12. *Let $a \in \mathbb{N}$ and assume*

$$w = a^2, \qquad b \geq k/a, \qquad |\mathbb{F}| \geq b.$$

Then, Hypothesis 4 is true for $(b, k, w, \mathbb{F})$ and Hypothesis 3 is true for $(b + 1, k, w, \mathbb{F})$.

Proof. We will prove here only the case $\mathsf{char}\,\mathbb{F} \neq 2$. The proof in the case $\mathsf{char}\,\mathbb{F} = 2$ works similarly and is given in Section C.

It suffices to prove Hypothesis 4. We only need to prove Hypothesis 4 in the case[9] where $k = ab$. To prove the hypothesis, let us divide the $k = ab$ variables of $\mathbb{F}[X]$ into a groups:

$$Y_1^{(1)}, \ldots, Y_b^{(1)}, \qquad \ldots, \qquad Y_1^{(a)}, \ldots, Y_b^{(a)}.$$

Let $\kappa_1, \ldots, \kappa_b$ be b distinct elements of $\mathbb{F}$. We construct three groups of blocks: the first group contains a blocks $A_1, \ldots, A_a \subset \mathbb{F}[X]^1$, the second and third group contain $\binom{a}{2}$ blocks, which we denote by $(B_{\alpha,\beta})_{\alpha,\beta\in[a],\alpha<\beta}$ and $(C_{\alpha,\beta})_{\alpha,\beta\in[a],\alpha<\beta}$. For $\alpha \in [a]$, we set

$$A_\alpha \coloneqq \{Y_1^{(\alpha)}, \ldots, Y_b^{(\alpha)}\}.$$

For $\alpha, \beta \in [a]$ with $\alpha < \beta$, we set

$$\begin{aligned} B_{\alpha,\beta} &\coloneqq \{Y_1^{(\alpha)} + Y_1^{(\beta)}, \ldots, Y_b^{(\alpha)} + Y_b^{(\beta)}\}, \\ C_{\alpha,\beta} &\coloneqq \{Y_1^{(\alpha)} + \kappa_1 \cdot Y_1^{(\beta)}, \ldots, Y_b^{(\alpha)} + \kappa_b \cdot Y_b^{(\beta)}\}. \end{aligned}$$

Further, let us set

$$\begin{aligned} \overline{U}_\alpha &\coloneqq \mathrm{span}_\mathbb{F} \{f \cdot g \mid f, g \in A_\alpha\}, \\ \overline{V}_{\alpha,\beta} &\coloneqq \mathrm{span}_\mathbb{F} \{f \cdot g \mid f, g \in B_{\alpha,\beta}\}, \\ \overline{W}_{\alpha,\beta} &\coloneqq \mathrm{span}_\mathbb{F} \{f \cdot g \mid f, g \in C_{\alpha,\beta}\}. \end{aligned}$$

Then, we have for all $i, j \in [b]$ and $\alpha, \beta \in [a]$

$$\begin{aligned} Y_i^{(\alpha)} \cdot Y_j^{(\alpha)} &\in \overline{U}_\alpha, \\ (Y_i^{(\alpha)} + Y_i^{(\beta)})(Y_j^{(\alpha)} + Y_j^{(\beta)}) &\in \overline{V}_{\alpha,\beta}, \\ (Y_i^{(\alpha)} + \kappa_i \cdot Y_i^{(\beta)})(Y_j^{(\alpha)} + \kappa_j \cdot Y_j^{(\beta)}) &\in \overline{W}_{\alpha,\beta}. \end{aligned}$$

It is left to prove that all cross-monomials $Y_i^{(\alpha)} \cdot Y_j^{(\beta)}$ for $i, j \in [b], \alpha, \beta \in [a]$ with $\alpha < \beta$ are contained in $\sum_\alpha \overline{U}_\alpha + \sum_{\alpha,\beta} \overline{V}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{W}_{\alpha,\beta}$.

[9] If a does not divide k, the claim follows by the correctness of the hypothesis for $k' = a \cdot \lceil k/a \rceil$, $b' = \lceil k/a \rceil \leq b$ and setting the last coordinates $X_{k+1}, \ldots, X_{k'}$ to zero.

For $i = j$, we point out that $\overline{V}_{\alpha,\beta}$ contains

$$(Y_i^{(\alpha)} + Y_i^{(\beta)})^2 = (Y_i^{(\alpha)})^2 + 2Y_i^{(\alpha)}Y_i^{(\beta)} + (Y_i^{(\beta)})^2.$$

Since $(Y_i^{(\alpha)})^2, (Y_i^{(\beta)})^2 \in \overline{U}_\alpha + \overline{U}_\beta$ and the characteristic of $\mathbb{F}$ is not 2, it follows that $\sum_\alpha \overline{U}_\alpha + \sum_{\alpha,\beta} \overline{V}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{W}_{\alpha,\beta}$ contains $Y_i^{(\alpha)} \cdot Y_i^{(\beta)}$.

Now, let $i \neq j$. Then, we have

$$\begin{aligned} (Y_i^{(\alpha)} + Y_i^{(\beta)}) \cdot (Y_j^{(\alpha)} + Y_j^{(\beta)}) &\in \overline{V}_{\alpha,\beta}, \\ (Y_i^{(\alpha)} + \kappa_i \cdot Y_i^{(\beta)}) \cdot (Y_j^{(\alpha)} + \kappa_j \cdot Y_j^{(\beta)}) &\in \overline{W}_{\alpha,\beta}. \end{aligned}$$

It follows

$$\begin{aligned} Y_i^{(\alpha)} \cdot Y_j^{(\beta)} + Y_i^{(\beta)} \cdot Y_j^{(\alpha)} &\in \overline{V}_{\alpha,\beta} + \overline{U}_\alpha + \overline{U}_\beta, \\ \kappa_j \cdot Y_i^{(\alpha)} \cdot Y_j^{(\beta)} + \kappa_i \cdot Y_i^{(\beta)} \cdot Y_j^{(\alpha)} &\in \overline{W}_{\alpha,\beta} + \overline{U}_\alpha + \overline{U}_\beta. \end{aligned}$$

Since $\kappa_i \neq \kappa_j$, it follows

$$Y_i^{(\alpha)} \cdot Y_j^{(\beta)}, Y_i^{(\beta)} \cdot Y_j^{(\alpha)} \in \overline{W}_{\alpha,\beta} + \overline{V}_{\alpha,\beta} + \overline{U}_\alpha + \overline{U}_\beta.$$

Hence, $\sum_\alpha \overline{U}_\alpha + \sum_{\alpha,\beta} \overline{V}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{W}_{\alpha,\beta}$ contains all monomials of $\mathbb{F}[X]^2$. □

Lemma 13. *Let $c > 1$ and set $w_c := \frac{c}{(\sqrt{c}-1)^2}$. We have for all $w \geq w_c$, $k \in \mathbb{N}$, $b > 2$ and fields $\mathbb{F}$ with $|\mathbb{F}| \geq b - 1$*

$$w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2} \implies \textit{Hypothesis } 3 \textit{ is true for } (b, k, w, \mathbb{F}).$$

Proof. Let $w \geq w_c$, $b > 1$, $k \in \mathbb{N}$ such that $w \cdot \binom{b}{2} \geq c \cdot \frac{3}{2} \cdot \binom{k+1}{2}$. We have

$$w \geq c \cdot \frac{3}{2} \cdot \frac{(k+1) \cdot k}{b \cdot (b-1)} \geq c \cdot \left(\frac{k}{b-1}\right)^2,$$

since $\frac{3}{2} \cdot \frac{k+1}{b} \geq \frac{k}{b-1}$ (which holds because $b \geq 3$). Set $a := \left\lceil \frac{k}{b-1} \right\rceil$. We claim that we have $w \geq a^2$. This follows because

$$a^2 \leq \left(\frac{k}{b-1} + 1\right)^2 \leq \left(\frac{\sqrt{w}}{\sqrt{c}} + 1\right)^2 = w\left(\frac{1}{\sqrt{w}} + \frac{1}{\sqrt{c}}\right)^2 \leq w,$$

where the last inequality follows from

$$\frac{1}{\sqrt{w}} + \frac{1}{\sqrt{c}} \leq \frac{1}{\sqrt{w_c}} + \frac{1}{\sqrt{c}} \leq \frac{\sqrt{c}-1}{\sqrt{c}} + \frac{1}{\sqrt{c}} = 1.$$

Since $|\mathbb{F}| \geq b-1$, Lemmas 9 and 12 imply now Hypothesis 3 for $(b, k, a^2, \mathbb{F})$. □

5 Learning With Bounded Errors

In this section, we use the methods developed above to study the LWBE problem. Let $\mathbf{G} \in \mathbb{F}^{n \times k}, \mathbf{H} \in \mathbb{F}^{(n-k)\times n}$ be the generator and parity-check matrix of a code $\mathcal{C}$. As in Problems 3 and 4, let $S_1, \ldots, S_n$ be the sets of size d containing the errors $e_1, \ldots, e_n$. For $i \in [n]$, let f_i be the following univariate polynomial.

$$f_i(Z_1) := \prod_{e \in S_i} (Z_1 - e).$$

Our main result is the following:

Theorem 4. *Let $\mathbb{F}$ be a field of size $q \geq dn + 2$ and characteristic $\mathsf{char}\,\mathbb{F} > d$.*

1. *Let $n = \binom{k+d}{d}$. There is an algorithm $\mathcal{D}$ that on input $(\mathbf{G}, \mathbf{Gx} + \mathbf{e})$ will always output 0 if $\mathbf{e} \in S_1 \times \ldots \times S_n$. However, for uniform random inputs, we have*

$$\Pr_{\mathbf{G} \leftarrow \mathbb{F}^{n \times k}, \mathbf{y} \leftarrow \mathbb{F}^n} [\mathcal{D}(\mathbf{G}, \mathbf{y}) = 1] \geq 1 - dn/q.$$

   The time complexity of $\mathcal{D}$ is dominated by inverting an $n \times n$ matrix.

2. *Let $n = \binom{k+d-1}{d}$. There is an algorithm $\mathcal{S}$ that on input $(\mathbf{G}, \mathbf{Gx} + \mathbf{e})$ outputs $\mathbf{e} \in S_1 \times \ldots \times S_n$ with success probability $\geq 1 - (d^2 n + 1) \cdot k/q$ over the randomness of $\mathbf{G} \leftarrow \mathbb{F}^{n \times k}$. The time complexity of $\mathcal{S}$ is $O(dkM)$, where M is the cost of inverting an $n \times n$ matrix.*

Before proving this result, we observe that it implies that the LWR Problem 5 with primes $q > p$ can be solved in time $O(qk^{1+\omega q/p}/p)$ when given $\binom{k+\lceil q/p \rfloor}{\lceil q/p \rfloor + 1}$ samples. Indeed, it suffices to consider the polynomials

$$f_i(Z_1) := \prod_{e = -\lceil (q+p)/2p \rfloor}^{\lceil (q+p)/2p \rfloor - 1} (Z_1 - e), \qquad \text{for all } i,$$

which have degree $\lceil q/p \rfloor + 1$. We can map the samples $(\mathbf{G}, \mathbf{b} = \lceil \mathbf{Gx} \rfloor_p) \in \mathbb{F}_q^{n \times k} \times \mathbb{F}_p^n$ to samples $(\mathbf{G}, \mathbf{b}') \in \mathbb{F}_q^{n \times k} \times \mathbb{F}_q^n$ where $\mathbf{b}' := \lceil q/p \cdot \mathbf{b} \rfloor$ can be written as $\mathbf{b}' = \mathbf{Gx} + \mathbf{e}$ for some error $\mathbf{e} \in \{- \lceil (q+p)/2p \rfloor, \ldots, \lceil (q+p)/2p \rfloor - 1\}^n$. This follows from the fact that if $a \in \mathbb{Z}_q$ and $b = \lceil a \rfloor_p = \lceil ap/q \rfloor$, then

$$\left| a - \left\lceil \frac{q}{p} b \right\rfloor \right| \leq \left| a - \frac{q}{p} b \right| + \left| \frac{q}{p} b - \left\lceil \frac{q}{p} b \right\rfloor \right| \leq \frac{q}{p} \left| a \frac{p}{q} - b \right| + \frac{1}{2} \leq \frac{q}{p} \frac{1}{2} + \frac{1}{2} = \frac{q+p}{2p}.$$

Now we proceed to study the LWBE problem in order to prove Theorem 4. The primal and dual modeling of LWBE and BSD are given by:

Modeling 3. Denote by $g_1, \ldots, g_n \in \mathbb{F}[X]^1$ linear forms that compute the rows of $\mathbf{G}$, i.e.

$$g_i(X) := \mathbf{g}_i^{\mathsf{T}} \cdot X.$$

The **primal** modeling of $(\mathbf{G}, \mathbf{y} = \mathbf{Gx} + \mathbf{e})$ is given by

$$f_1(y_1 - g_1(X)) = 0, \qquad \ldots, \qquad f_n(y_n - g_n(X)) = 0.$$

Modeling 4. Denote by $h_1, \ldots, h_{n-k} \in \mathbb{F}[X]^1$ linear forms that compute the rows of $\mathbf{H}$, i.e.

$$h_i(X) := \mathbf{h}_i^\mathsf{T} \cdot X.$$

The **dual** modeling of $(\mathbf{H}, \mathbf{s} = \mathbf{He})$ is given by

$$\begin{aligned} f_1(E_1) &= 0, & \ldots, && f_n(E_n) &= 0, \\ h_1(E) - s_1 &= 0, & \ldots, && h_{n-k}(E) - s_{n-k} &= 0. \end{aligned}$$

By the following lemma, both modelings are equivalent in the sense that the ideals of their top terms are isomorphic.

Lemma 14. *Let*

$$\begin{aligned} I &:= \left((-g_1)^d, \ldots, (-g_n)^d\right), \\ J &:= \left(E_1^d, \ldots, E_n^d, h_1, \ldots, h_{n-k}\right). \end{aligned}$$

Then, $\mathbb{F}[X]/I$ and $\mathbb{F}[E]/J$ are isomorphic as graded rings.

We omit the proof of Lemma 14 as it is analogous to the proof of Lemma 7. A more general lemma is proven in Section B. To ease notation, we will consider the polynomials $g_1^d, \ldots, g_n^d \in \mathbb{F}[X]^d$ instead of $(-g_1)^d, \ldots, (-g_n)^d$ in the following. Note that this is equivalent, since

$$\operatorname{span}_{\mathbb{F}}\{(-g_1)^d, \ldots, (-g_n)^d\} = \operatorname{span}_{\mathbb{F}}\{g_1^d, \ldots, g_n^d\}.$$

Theorem 5. *Let $d, k \in \mathbb{N}$. Let $\mathbb{F}$ be a field with $\mathsf{char}(\mathbb{F}) > d$.*

There are $n = \binom{k+d-1}{d}$ linear forms $g_1, \ldots, g_n \in \mathbb{F}[X]^1$ such that

$$\operatorname{span}_{\mathbb{F}}\{g_1^d, \ldots, g_n^d\} = \mathbb{F}[X]^d.$$

For this n, Theorem 5 implies that Modelings 3 and 4 have a degree of regularity d with high probability (see Lemma 6). There are multiple ways to prove Theorem 5. Our strategy here utilizes multivariate Vandermonde matrices, as those matrices naturally capture the combinatorics of multivariate degree-d polynomials.

For an **index** $\beta \in \mathbb{N}_0^k$, denote its **weight** by $|\beta| = \beta_1 + \ldots + \beta_k$. Let $\alpha(1), \ldots, \alpha(n)$ be an enumeration of the set of indices of weight $\leq d$

$$\left\{\alpha \in \mathbb{N}_0^{k-1} \;\middle|\; |\alpha| \leq d\right\}.$$

We define $\beta(1), \ldots, \beta(n)$ to be corresponding homogenized indices of weight d. Concretely, for $i \in [n]$, we set $\beta(i) := (\alpha(i), d - |\alpha(i)|) \in \mathbb{N}_0^k$.

We use the following theorem from the PhD thesis of Ünal [Üna24, Thm. 54]:

Theorem 6. *Let $m_1, \ldots, m_n \in \mathbb{Z}[X_1, \ldots, X_{k-1}]$ be an enumeration of all monomials of degree $\leq d$, given by*

$$m_i = X^{\alpha(i)} = X_1^{\alpha(i)_1} \cdots X_{k-1}^{\alpha(i)_{k-1}}.$$

We have for the determinant of the multivariate Vandermonde matrix $\mathbf{V} = (m_j(\alpha(i)))_{i,j \in [n]}$ for inhomogeneous polynomials of degree d over $k-1$ variables

$$\det \mathbf{V} = \prod_{i=1}^{d} (d + 1 - i)^{i \cdot \binom{k-2+i}{i}}.$$

Lemma 15. *Define* $\gamma_1, \ldots, \gamma_n \in \mathbb{F}$ *by*

$$(X_1 + \ldots + X_k)^d = \sum_{j=1}^{n} \gamma_j \cdot X^{\beta(j)}.$$

If $\mathsf{char}\, \mathbb{F} > d$*, then no* γ_i *can be zero.*

Proof. We prove the statement by induction on k and d. Note that we have

$$(X_1 + \ldots + X_k)^d = \sum_{i=0}^{d} \binom{d}{i} \cdot X_k^i \cdot (X_1 + \ldots + X_{k-1})^{d-i}.$$

Let us study the coefficient of $X_1^{i_1} \cdots X_k^{i_k}$. It is given by $\binom{d}{i_k}$ times the coefficient $\gamma' \in \mathbb{F}$ of the monomial $X_1^{i_1} \cdots X_{k-1}^{i_{k-1}}$ in the polynomial $(X_1 + \ldots + X_{k-1})^{d-i_k}$. By induction, $\gamma' \neq 0$. The coefficient of $X_1^{i_1} \cdots X_k^{i_k}$ is hence given by $\gamma' \cdot \binom{d}{i}$, which is not zero in $\mathbb{F}$, since $\mathsf{char}\, \mathbb{F} > d$. □

Theorem 5. We set each g_i to be

$$g_i := X_k + \sum_{j=1}^{k-1} \alpha(i)_j \cdot X_j.$$

Note that we have

$$g_i^d = \sum_{j=1}^{n} \gamma_j \cdot (\alpha(i), 1)^{\beta(j)} \cdot X^{\beta(j)} = \sum_{j=1}^{n} \gamma_j \cdot \alpha(i)^{\alpha(j)} \cdot X^{\beta(j)}.$$

Let $\mathbf{M} \in \mathbb{F}^{n \times n}$ be the matrix where the i-th row contains the coefficients of g_i^d. Concretely, the i-th row of $\mathbf{M}$ is given by

$$(\gamma_1 \cdot \alpha(i)^{\alpha(1)} \qquad \cdots \qquad \gamma_n \cdot \alpha(i)^{\alpha(n)}).$$

We can see that $\mathbf{M}$ equals $\mathbf{V} \cdot \mathbf{D}$ where $\mathbf{V}$ is the Vandermonde matrix from Theorem 6 and $\mathbf{D}$ is a diagonal matrix with $\gamma_1, \ldots, \gamma_n$ on its diagonal. Since $\gamma_1, \ldots, \gamma_n$ are all non-zero, the determinant of $\mathbf{M}$ is not zero. It follows that the homogeneous polynomials $g_1^d, \ldots, g_n^d \in \mathbb{F}[X]^d$ are linearly independent. As $\dim_{\mathbb{F}} \mathbb{F}[X]^d = n$, they span the whole space. □

Theorem 4. A naive approach would be to use the theorem of Salizzoni Theorem 1 and bound the runtime of the Mutant-XL algorithm. However, we can do better by using the degree of regularity and a search-to-decision reduction. Let $n = \binom{k+d}{d}$. For the first claim, let $\mathcal{D}$ act as follows: On input $\mathbf{G}$ and $\mathbf{y}$, $\mathcal{D}$ computes the polynomials $f_1(y_1 - g_1(X)), \ldots, f_n(y_n - g_n(X))$, where n is as specified in Theorem 4. It computes a basis of the space

$$V := \mathrm{span}_{\mathbb{F}}\{f_1(y_1 - g_1(X)), \ldots, f_n(y_n - g_n(X))\} \subseteq \mathbb{F}[X]^{\leq d}.$$

If $1 \in V$, it outputs 1, otherwise, it outputs 0. Now, if $\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e}$ for some $\mathbf{e} \in S_1 \times \cdots \times S_n$, then $V \subset (f_1(y_1 - g_1(X)), \ldots, f_n(y_n - g_n(X)))$ can never contain 1. On the other hand, draw $\mathbf{G}$ and $\mathbf{y}$ uniformly at random. Introduce a homogenization variable H_1 and set for $i \in [n]$

$$g_i'(X, H_1) := y_i \cdot H_1 - g_i(X).$$

The $g_1', \ldots, g_n'$ are distributed uniformly at random in $\mathbb{F}[X, H_1]^1$. Additionally, let $f_i'(Z_1, H_1) = \prod_{e \in S_i}(Z_1 - eH_1)$ be the homogenization of f_i for $i \in [n]$. In Lemma 36, we show that the space

$$V' := \mathrm{span}_{\mathbb{F}}\{f_1'(g_1'), \ldots, f_n'(g_n')\}$$

equals $\mathbb{F}[X, H_1]^d$ with probability $\geq 1 - dn/q$. Now, we have $H^d \in V'$ iff $1 \in V$. Hence, if $\mathbf{G}$ and $\mathbf{y}$ are uniformly random, then $\mathcal{D}$ will output 1 with probability $\geq 1 - dn/q$.

For the second claim, let $n = \binom{k+d-1}{d}$. Given $\mathcal{D}$, $\mathcal{S}$ acts as follows on input $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e})$: For $i \in [k]$ and $z \in S_i$, $\mathcal{S}$ guesses that $\mathbf{e}$ has the value $e_i = z$ at position i. By this, it reduces[10] n and k of the LWBE problem by one by using the equation $g_i(\mathbf{x}) + z = y_i$ to reduce the dimension of $\mathbf{x}$. Additionally, it removes the i-th row of $\mathbf{G}$ and $\mathbf{y}$. It ends with a smaller LWBE instance $(\mathbf{G}' \in \mathbb{F}^{(n-1)\times(k-1)}, \mathbf{y}' \in \mathbb{F}^{n-1})$. Now, it runs $\mathcal{D}$ on $(\mathbf{G}', \mathbf{y}')$. If $\mathcal{D}(\mathbf{G}', \mathbf{y}') = 0$, then $\mathcal{S}$ assumes that $e_i = z$. If the guess $e_i = z$ is incorrect, then $\mathbf{G}'$ and $\mathbf{y}'$ are distributed uniformly at random, and we have $\mathcal{D}(\mathbf{G}', \mathbf{y}') = 1$ with probability $\geq 1 - dn/q$. By a union bound, the probability that $\mathcal{D}$ outputs 1 for every wrong guess of $\mathcal{S}$ is at least $1 - d^2kn/q$. At the end, $\mathcal{S}$ learns $e_1, \ldots, e_k$. With probability $\geq 1 - k/q$, the first k rows of $\mathbf{G}$ are linearly independent. In this case, $\mathcal{S}$ can solve for $\mathbf{x}$, since it knows the first k values of $\mathbf{e}$. □

References

[AFS03] Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. *A Fast Provably Secure Cryptographic Hash Function.* Cryptology ePrint Archive, Report 2003/230. 2003. URL: `https://eprint.iacr.org/2003/230`.

[AG11] Sanjeev Arora and Rong Ge. "New Algorithms for Learning in Presence of Errors". In: *ICALP 2011, Part I.* Ed. by Luca Aceto, Monika Henzinger, and Jiri Sgall. Vol. 6755. LNCS. Springer, Berlin, Heidelberg, July 2011, pp. 403–415. DOI: `10.1007/978-3-642-22006-7_34`.

[Ajt96] Miklós Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *28th ACM STOC.* ACM Press, May 1996, pp. 99–108. DOI: `10.1145/237814.237838`.

[Alb+14] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. *Algebraic Algorithms for LWE.* Cryptology ePrint Archive, Report 2014/1018. 2014. URL: `https://eprint.iacr.org/2014/1018`.

[Bar04] Magali Bardet. "Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie". Theses. Université Pierre et Marie Curie - Paris VI, Dec. 2004. URL: `https://theses.hal.science/tel-00449609`.

[10] We detail this reduction in Section G.

[BCM24] Dung Bui, Geoffroy Couteau, and Nikolas Melissaris. *Structured-Seed Local Pseudorandom Generators and their Applications.* Cryptology ePrint Archive, Report 2024/1027. 2024. URL: https://eprint.iacr.org/2024/1027.

[BFS03] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. *Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over F_2 with solutions in F_2.* Research Report RR-5049. INRIA, 2003. URL: https://inria.hal.science/inria-00071534.

[Big+20] M. Bigdeli, E. De Negri, M. M. Dizdarevic, E. Gorla, R. Minko, and S. Tsakou. *Semi-regular sequences and other random systems of equations.* Cryptology ePrint Archive, Report 2020/1375. 2020. URL: https://eprint.iacr.org/2020/1375.

[Bit+23] Sebastian Bitzer, Alessio Pavoni, Violetta Weger, Paolo Santini, Marco Baldi, and Antonia Wachter-Zeh. "Generic Decoding of Restricted Errors". In: *2023 IEEE International Symposium on Information Theory (ISIT).* 2023, pp. 246–251. DOI: 10.1109/ISIT54713.2023.10206983.

[BØ23] Pierre Briaud and Morten Øygarden. "A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions". In: *EUROCRYPT 2023, Part V.* Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. LNCS. Springer, Cham, Apr. 2023, pp. 391–422. DOI: 10.1007/978-3-031-30589-4_14.

[Boy+18] Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai. "Compressing Vector OLE". In: *ACM CCS 2018.* Ed. by David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang. ACM Press, Oct. 2018, pp. 896–912. DOI: 10.1145/3243734.3243868.

[Boy+19] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. "Efficient Pseudorandom Correlation Generators: Silent OT Extension and More". In: *CRYPTO 2019, Part III.* Ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11694. LNCS. Springer, Cham, Aug. 2019, pp. 489–518. DOI: 10.1007/978-3-030-26954-8_16.

[Boy+20] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. "Efficient Pseudorandom Correlation Generators from Ring-LPN". In: *CRYPTO 2020, Part II.* Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 387–416. DOI: 10.1007/978-3-030-56880-1_14.

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. "Pseudorandom Functions and Lattices". In: *EUROCRYPT 2012.* Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. LNCS. Springer, Berlin, Heidelberg, Apr. 2012, pp. 719–737. DOI: 10.1007/978-3-642-29011-4_42.

[CCJ23] Eliana Carozza, Geoffroy Couteau, and Antoine Joux. "Short Signatures from Regular Syndrome Decoding in the Head". In: *EUROCRYPT 2023, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. LNCS. Springer, Cham, Apr. 2023, pp. 532–563. DOI: 10.1007/978-3-031-30589-4_19.

[Din+08] Jintai Ding, Johannes Buchmann, Mohamed Saied Emam Mohamed, Wael Said Abd Elmageed Mohamed, and Ralf-Philipp Weinmann. "MutantXL". de. In: *SCC* TUD-CS-2009-0142 (Jan. 2008), pp. 16–22. URL: http://tubiblio.ulb.tu-darmstadt.de/100617/.

[DL78] Richard A. Demillo and Richard J. Lipton. "A probabilistic remark on algebraic program testing". In: *Information Processing Letters* 7.4 (1978), pp. 193–195. ISSN: 0020-0190. DOI: 10.1016/0020-0190(78)90067-4.

[ES24] Andre Esser and Paolo Santini. "Not Just Regular Decoding: Asymptotics and Improvements of Regular Syndrome Decoding Attacks". In: *CRYPTO 2024, Part VI*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14925. LNCS. Springer, Cham, Aug. 2024, pp. 183–217. DOI: 10.1007/978-3-031-68391-6_6.

[FBS04] Jean-Charles Faugère, Magali Bardet, 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*. 2004. URL: https://api.semanticscholar.org/CorpusID:7982329.

[FH94] Ralf Fröberg and Joachim Hollman. "Hilbert Series for Ideals Generated by Generic Forms". In: *Journal of Symbolic Computation* 17.2 (1994), pp. 149–157. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.1994.1008. URL: https://www.sciencedirect.com/science/article/pii/S074771718471008X.

[Frö85] Ralf Fröberg. "An inequality for Hilbert series of graded algebras." In: *MATHEMATICA SCANDINAVICA* 56 (Dec. 1985), pp. 117–144. DOI: 10.7146/math.scand.a-12092. URL: https://www.mscand.dk/article/view/12092.

[Haz+18] Carmit Hazay, Emmanuela Orsini, Peter Scholl, and Eduardo Soria-Vazquez. "TinyKeys: A New Approach to Efficient Multi-Party Computation". In: *CRYPTO 2018, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. LNCS. Springer, Cham, Aug. 2018, pp. 3–33. DOI: 10.1007/978-3-319-96878-0_1.

[HMS17] Timothy J. Hodges, Sergio D. Molina, and Jacob Schlather. "On the existence of homogeneous semi-regular sequences in F2[X1,...,Xn]/(X12,...,Xn2)". In: *Journal of Algebra* 476 (2017), pp. 519–547. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2016.11.025. URL: https://www.sciencedirect.com/science/article/pii/S0021869316304732.

[Liu+24] Hanlin Liu, Xiao Wang, Kang Yang, and Yu Yu. "The Hardness of LPN over Any Integer Ring and Field for PCG Applications". In: *EUROCRYPT 2024, Part VI.* Ed. by Marc Joye and Gregor Leander. Vol. 14656. LNCS. Springer, Cham, May 2024, pp. 149–179. DOI: 10.1007/978-3-031-58751-1_6.

[LSS22] Paul Lou, Amit Sahai, and Varun Sivashankar. "Relinearization Attack on LPN over Large Fields". In: 2022. URL: https://www.cfail.org/_files/ugd/6a3e24_bdd034dc2a264d4a8b0fb1856daa823a.pdf.

[Lyu24] Vadim Lyubashevsky. *Basic Lattice Cryptography: The concepts behind Kyber (ML-KEM) and Dilithium (ML-DSA).* Cryptology ePrint Archive, Report 2024/1287. 2024. URL: https://eprint.iacr.org/2024/1287.

[MP13] Daniele Micciancio and Chris Peikert. "Hardness of SIS and LWE with Small Parameters". In: *CRYPTO 2013, Part I.* Ed. by Ran Canetti and Juan A. Garay. Vol. 8042. LNCS. Springer, Berlin, Heidelberg, Aug. 2013, pp. 21–39. DOI: 10.1007/978-3-642-40041-4_2.

[Par10] Keith Pardue. "Generic sequences of polynomials". In: *Journal of Algebra* 324.4 (2010), pp. 579–590. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2010.04.018. URL: https://www.sciencedirect.com/science/article/pii/S0021869310001948.

[RVV24] Seyoon Ragavan, Neekon Vafa, and Vinod Vaikuntanathan. *Indistinguishability Obfuscation from Bilinear Maps and LPN Variants.* Cryptology ePrint Archive, Report 2024/856. 2024. URL: https://eprint.iacr.org/2024/856.

[Sal23] Flavio Salizzoni. *An upper bound for the solving degree in terms of the degree of regularity.* 2023. arXiv: 2304.13485 [math.AC]. URL: https://arxiv.org/abs/2304.13485.

[Sch80] J. T. Schwartz. "Fast Probabilistic Algorithms for Verification of Polynomial Identities". In: *J. ACM* 27.4 (Oct. 1980), pp. 701–717. ISSN: 0004-5411. DOI: 10.1145/322217.322225.

[ST21] Igor Semaev and Andrea Tenti. "Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases". In: *Journal of Algebra* 565 (2021), pp. 651–674. ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2020.08.035. URL: https://www.sciencedirect.com/science/article/pii/S0021869320304737.

[STA20] Chao Sun, Mehdi Tibouchi, and Masayuki Abe. "Revisiting the Hardness of Binary Error LWE". In: *ACISP 20.* Ed. by Joseph K. Liu and Hui Cui. Vol. 12248. LNCS. Springer, Cham, Nov. 2020, pp. 425–444. DOI: 10.1007/978-3-030-55304-3_22.

[Stä23] Patrick Stählin. "Subexponential Attacks on Variational LPN". en. Master Thesis. Zurich: ETH Zurich, 2023. DOI: 10.3929/ethz-b-000643453.

[Ste24] Matthias Johann Steiner. "The Complexity of Algebraic Algorithms for LWE". In: *EUROCRYPT 2024, Part III*. Ed. by Marc Joye and Gregor Leander. Vol. 14653. LNCS. Springer, Cham, May 2024, pp. 375–403. DOI: 10.1007/978-3-031-58734-4_13.

[Üna24] Akin Ünal. "Cryptanalysis by Algebraic Relations". en. Doctoral Thesis. Zurich: ETH Zurich, 2024. DOI: 10.3929/ethz-b-000679381.

[Wen+21] Chenkai Weng, Kang Yang, Jonathan Katz, and Xiao Wang. "Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits". In: *2021 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2021, pp. 1074–1091. DOI: 10.1109/SP40001.2021.00056.

[Yan+20] Kang Yang, Chenkai Weng, Xiao Lan, Jiang Zhang, and Xiao Wang. "Ferret: Fast Extension for Correlated OT with Small Communication". In: *ACM CCS 2020*. Ed. by Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna. ACM Press, Nov. 2020, pp. 1607–1626. DOI: 10.1145/3372297.3417276.

[Zip79] Richard Zippel. "Probabilistic algorithms for sparse polynomials". In: *Symbolic and Algebraic Computation*. Ed. by Edward W. Ng. Berlin, Heidelberg: Springer Berlin Heidelberg, 1979, pp. 216–226. ISBN: 978-3-540-35128-3. DOI: 10.1007/3-540-09519-5_73.

Supplementary Material

A Computations on Power Series

First note that we have the following for parameters $b, k, w, n \in \mathbb{N}$

$$\begin{aligned}
(1-T)^n &= \sum_{i=0}^{n} \binom{n}{i} \cdot (-T)^i \\
&= 1 - nT + \binom{n}{2} T^2 + O(T^3), \\
\left(1 + bT + bT^2 + \ldots\right)^w &= \left(1 + bT + bT^2\right)^w + O(T^3) \\
&= \sum_{i=0}^{w} \binom{w}{i} \cdot b^i \cdot (T + T^2)^i + O(T^3) \\
&= 1 + wb(T + T^2) + \binom{w}{2} b^2 \cdot (T + T^2)^2 + O(T^3) \\
&= 1 + wbT + \left(bw + \binom{w}{2} b^2\right) \cdot T^2 + O(T^3), \\
\frac{1}{(1+T)^n} &= (1 - T + T^2 - \ldots)^n \\
&= \sum_{i=0}^{n} \binom{n}{i} \cdot (T^2 - T)^i + O(T^3) \\
&= 1 + n \cdot (T^2 - T) + \binom{n}{2} \cdot (T^2 - T)^2 + O(T^3) \\
&= 1 - nT + \left(n + \binom{n}{2}\right) T^2 + O(T^3) \\
&= 1 - nT + \binom{n+1}{2} T^2 + O(T^3), \\
(1 + bT)^w &= \sum_{i=0}^{w} \binom{w}{i} \cdot b^i \cdot T^i \\
&= 1 + wbT + b^2 \cdot \binom{w}{2} \cdot T^2 + O(T^3), \\
(1-T)^{-k} &= \left(\frac{1}{1-T}\right)^k \\
&= \left(1 + T + T^2 + \ldots\right)^k \\
&= 1 + kT + \binom{k+1}{2} T^2 + O(T^3).
\end{aligned}$$

Lemma 16. *We have*

$$\binom{wb}{2} + bw + b^2 \binom{w}{2} - (wb)^2 = -w \binom{b}{2}.$$

Proof.

$$\binom{wb}{2} + bw + b^2 \binom{w}{2} - (wb)^2$$

$$\begin{aligned}
&= \frac{wb(wb-1) + 2bw + b^2w(w-1) - 2(wb)^2}{2} \\
&= \frac{-wb + 2bw - b^2w}{w} \\
&= -\frac{b^2w - bw}{2} = -w\binom{b}{2}.
\end{aligned}$$ □

Lemma 17. *We have*

$$(1-T)^{wb} \cdot (1 + bT + bT^2 + \ldots)^w = 1 - w\binom{b}{2}T^2 + O(T^3)$$

Proof.

$$\begin{aligned}
&(1-T)^{wb} \cdot (1 + bT + bT^2 + \ldots)^w \\
&\quad = \left(1 - wbT + \binom{wb}{2}T^2\right) \cdot \left(1 + wbT + \left(bw + \binom{w}{2}b^2\right) \cdot T^2\right) + O(T^3) \\
&\quad = 1 + \left(\binom{wb}{2} + bw + \binom{w}{2}b^2 - (wb)^2\right)T^2 + O(T^3) \\
&\quad = 1 - w\binom{b}{2}T^2 + O(T^3).
\end{aligned}$$ □

Lemma 18. *We have with* $n = bw$

$$(1-T)^{n-k} \cdot \left(1 + bT + bT^2 + \ldots\right)^w = 1 + k \cdot T + \left(\binom{k+1}{2} - w \cdot \binom{b}{2}\right) \cdot T^2 + O(T^3).$$

Proof.

$$\begin{aligned}
&(1-T)^{n-k} \cdot \left(1 + bT + bT^2 + \ldots\right)^w \\
&\quad = (1-T)^{-k} \cdot (1-T)^{bw} \cdot \left(1 + bT + bT^2 + \ldots\right)^w \\
&\quad = \left(1 + kT + \binom{k+1}{2}T^2\right) \cdot \left(1 - w\binom{b}{2}T^2\right) + O(T^3) \\
&\quad = 1 + kT + \left(\binom{k+1}{2} - w \cdot \binom{b}{2}\right) \cdot T^2 + O(T^3).
\end{aligned}$$ □

Lemma 19. *We have*

$$\frac{(1 + b \cdot T)^w}{(1+T)^{bw}} = 1 - w \cdot \binom{b}{2}T^2 + O(T^3).$$

Proof. We have

$$\begin{aligned}
\frac{(1 + b \cdot T)^w}{(1+T)^{bw}} &= \left(1 + wbT + b^2\binom{w}{2}T^2\right) \cdot \left(1 - bwT + \left(bw + \binom{bw}{2}\right)T^2\right) + O(T^3) \\
&= 1 + \left(b^2\binom{w}{2} + bw + \binom{bw}{2} - (bw)^2\right)T^2 + O(T^3).
\end{aligned}$$

With Lemma 16, it follows

$$\begin{aligned}
1+&\left(b^2\binom{w}{2} + bw + \binom{bw}{2} - (bw)^2\right)T^2 + O(T^3) \\
&= 1 - w\binom{b}{2}T^2 + O(T^3).
\end{aligned}$$ □

Lemma 20. *With $n = bw$, we have*

$$\begin{aligned}\frac{(1+b\cdot T)^w}{(1+T)^{n-k}} &= 1 + k\cdot T + \left(\binom{k+1}{2} - k - w\cdot\binom{b}{2}\right)\cdot T^2 + O(T^3)\\ &= 1 + k\cdot T + \left(\binom{k}{2} - w\cdot\binom{b}{2}\right)\cdot T^2 + O(T^3).\end{aligned}$$

Proof. We have

$$\begin{aligned}\frac{(1+b\cdot T)^w}{(1+T)^{n-k}} &= \frac{(1+b\cdot T)^w}{(1+T)^{bw}}\cdot(1+T)^k\\ &= \left(1 - w\binom{b}{2}T^2\right)\cdot\left(1 + kT + \binom{k}{2}T^2\right) + O(T^3)\\ &= 1 + kT + \left(\binom{k}{2} - w\binom{b}{2}\right)T^2 + O(T^3). \qquad \square\end{aligned}$$

A.1 The Hybrid Setting

For the hybrid approach of Briaud and Øygarden [BØ23], where one guesses $u < b$ error-free positions in $f \leq w$ blocks, the following computations are relevant:

Lemma 21. *For $n = bw$, we have*

$$\begin{aligned}&(1-T)^{n-k}\cdot\left(1 + bT + bT^2 + \ldots\right)^{w-f}\cdot(1 + (b-u)T + (b-u)T^2 + \ldots)^f\\ &\qquad = 1 + (k - fu)T + \left(\binom{k-fu+1}{2} - (w-f)\binom{b}{2} - f\binom{b-u}{2}\right)T^2 + O(T^3).\end{aligned}$$

Proof. Note that we have

$$n - fu = b(w-f) + (b-u)f.$$

It follows with Lemma 17

$$\begin{aligned}&(1-T)^{n-fu}\cdot\left(1 + bT + bT^2 + \ldots\right)^{w-f}\cdot(1 + (b-u)T + (b-u)T^2 + \ldots)^f\\ &= (1-T)^{b(w-f)}\left(1 + bT + bT^2\right)^{w-f}\cdot(1-T)^{(b-u)f}(1 + (b-u)T + (b-u)T^2)^f + O(T^3)\\ &= \left(1 - (w-f)\binom{b}{2}T^2\right)\cdot\left(1 - f\binom{b-u}{2}T^2\right) + O(T^3)\\ &= 1 - \left((w-f)\binom{b}{2} + f\binom{b-u}{2}\right)T^2 + O(T^3).\end{aligned}$$

Hence, we have

$$\begin{aligned}&(1-T)^{n-k}\cdot\left(1 + bT + bT^2 + \ldots\right)^{w-f}\cdot(1 + (b-u)T + (b-u)T^2 + \ldots)^f\\ &= (1-T)^{uf-k}\cdot\left(1 - \left((w-f)\binom{b}{2} + f\binom{b-u}{2}\right)T^2\right) + O(T^3)\\ &= \left(1 + (k-fu)T + \binom{k-fu+1}{2}T^2\right)\cdot\left(1 - \left((w-f)\binom{b}{2} + f\binom{b-u}{2}\right)T^2\right) + O(T^3)\\ &= 1 + (k-fu)T + \left(\binom{k-fu+1}{2} - (w-f)\binom{b}{2} - f\binom{b-u}{2}\right)T^2 + O(T^3). \quad \square\end{aligned}$$

Lemma 22. *For $n = bw$, we have*

$$\begin{aligned}
&\frac{(1+bT)^{w-f} \cdot (1+(b-u)T)^{f}}{(1+T)^{n-k}} \\
&= 1 + (k-fu)T + \left(\binom{k-fu}{2} - (w-f)\binom{b}{2} - f\binom{b-u}{2} \right) T^2 + O(T^3).
\end{aligned}$$

Proof. Again, we use $n - fu = b(w-f) + (b-u)f$ to consider

$$\begin{aligned}
&\frac{(1+bT)^{w-f} \cdot (1+(b-u)T)^{f}}{(1+T)^{n-fu}} \\
&= \frac{(1+bT)^{w-f}}{(1+T)^{b(w-f)}} \cdot \frac{(1+(b-u)T)^{f}}{(1+T)^{(b-u)f}} \\
&= \left(1 - (w-f)\binom{b}{2}T^2\right) \cdot \left(1 - f\binom{b-u}{2}T^2\right) + O(T^3) \\
&= 1 - \left((w-f)\binom{b}{2} + f\binom{b-u}{2}\right) T^2 + O(T^3).
\end{aligned}$$

It follows

$$\begin{aligned}
&\frac{(1+bT)^{w-f} \cdot (1+(b-u)T)^{f}}{(1+T)^{n-k}} \\
&= (1+T)^{k-fu} \cdot \frac{(1+bT)^{w-f} \cdot (1+(b-u)T)^{f}}{(1+T)^{n-fu}} \\
&= \left(1 + (k-fu)T + \binom{k-fu}{2}T^2\right) \cdot \left(1 - \left((w-f)\binom{b}{2} + f\binom{b-u}{2}\right) T^2\right) + O(T^3) \\
&= 1 + (k-fu)T + \left(\binom{k-fu}{2} - (w-f)\binom{b}{2} - f\binom{b-u}{2} \right) T^2 + O(T^3). \qquad \square
\end{aligned}$$

B Equivalence of Primal and Dual Modelings

Let $\mathbb{F}$ be a finite field. We introduce here general learning and syndrome decoding problems:

Problem 6 (General Learning)**.** Let $k, n, m \in \mathbb{N}$, and fix polynomials $f_1, \ldots, f_m \in \mathbb{F}[E_1, \ldots, E_n]$.

For a generator matrix $\mathbf{G} \in \mathbb{F}^{n \times k}$, the **General Learning** problem asks to extract $\mathbf{x} \in \mathbb{F}^k$ from $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e})$ where $\mathbf{e} \in \mathbb{F}^n$ fulfils

$$f_1(\mathbf{e}) = \ldots = f_m(\mathbf{e}) = 0.$$

Its dual problem is given as follows:

Problem 7 (General Syndrome Decoding)**.** For a parity-check matrix $\mathbf{H} \in \mathbb{F}^{(n-k)\times n}$, the **General Syndrome Decoding** problem asks to extract $\mathbf{e} \in \mathbb{F}^n$ from $(\mathbf{H}, \mathbf{s} = \mathbf{H}\mathbf{e})$ s.t.

$$f_1(\mathbf{e}) = \ldots = f_m(\mathbf{e}) = 0.$$

Lemma 23. *Let* $\mathbf{G} \in \mathbb{F}^{n \times k}$ *and* $\mathbf{H} \in \mathbb{F}^{(n-k) \times k}$ *be a generator and a parity-check matrix for a* k*-dimensional code* $\mathcal{C}$*. The General Learning problem for* $\mathbf{G}$ *and the General Syndrome Decoding for* $\mathbf{H}$ *problem are equivalent via reductions that have a time complexity in* $O(n^3)$*.*

Proof. First note that we have the following short exact sequence of linear spaces

$$0 \longrightarrow \mathbb{F}^k \xrightarrow{\mathbf{G}} \mathbb{F}^n \xrightarrow{\mathbf{H}} \mathbb{F}^{n-k} \longrightarrow 0.$$

Now, let $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e})$ be an instance of the General Learning problem for the polynomials $f_1, \dots, f_m \in \mathbb{F}[E]$. By applying $\mathbf{H}$ to $\mathbf{y}$, we get the General Syndrome Decoding problem $(\mathbf{H}, \mathbf{H}\mathbf{y} = \mathbf{H}\mathbf{e})$. Because of our short exact sequence, any solution $\mathbf{e}'$ for $(\mathbf{H}, \mathbf{H}\mathbf{e})$ yields a solution $(\mathbf{x}', \mathbf{e}')$ for $(\mathbf{G}, \mathbf{y})$.

On the other hand, let $(\mathbf{H}, \mathbf{s} = \mathbf{H}\mathbf{e})$ be an instance of the General Syndrome Decoding problem for the polynomials $f_1, \dots, f_m \in \mathbb{F}[E]$. Compute any $\mathbf{y} \in \mathbb{F}^n$ s.t. $\mathbf{H}\mathbf{y} = \mathbf{s}$. Because of our short exact sequence, there exists an $\mathbf{x} \in \mathbb{F}^k$ s.t. $\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e}$. Hence, we get a General Learning instance $(\mathbf{G}, \mathbf{y})$. Any solution $(\mathbf{x}', \mathbf{e}')$ for $(\mathbf{G}, \mathbf{y})$ yields a solution $\mathbf{e}'$ for $(\mathbf{H}, \mathbf{s})$. □

Modeling 5 (General Primal Modeling)**.** Let $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e})$ be an instance of the General Learning problem for polynomials $f_1, \dots, f_m \in \mathbb{F}[E_1, \dots, E_n]$. Denote by $g_1, \dots, g_n \in \mathbb{F}[X_1, \dots, X_k]^1$ the linear forms that compute the rows of $\mathbf{G}$, i.e.

$$g_i(X) = \mathbf{g}_i^\mathsf{T} \cdot X.$$

The **primal** modeling of $(\mathbf{G}, \mathbf{y})$ is given by

$$\begin{aligned} f_1(y_1 - g_1(X), \dots, y_n - g_n(X)) &= 0, \\ &\vdots \\ f_m(y_1 - g_1(X), \dots, y_n - g_n(X)) &= 0. \end{aligned}$$

Modeling 6 (General Dual Modeling)**.** Let $(\mathbf{H}, \mathbf{s} = \mathbf{H}\mathbf{e})$ be an instance of the General Syndrome Decoding problem for polynomials $f_1, \dots, f_m \in \mathbb{F}[E_1, \dots, E_n]$. Denote by $h_1, \dots, h_{n-k} \in \mathbb{F}[E_1, \dots, E_n]^1$ the linear forms that compute the rows of $\mathbf{H}$, i.e.

$$h_i(X) = \mathbf{h}_i^\mathsf{T} \cdot E.$$

The **dual** modeling of $(\mathbf{H}, \mathbf{s})$ is given by

$$\begin{aligned} f_1(E) &= 0, & h_1(E) - s_1 &= 0, \\ &\vdots & &\vdots \\ f_m(E) &= 0, & h_{n-k}(E) - s_{n-k} &= 0. \end{aligned}$$

Lemma 24. *There is a grade-preserving ring isomorphism*

$$\mathbb{F}[E]/(f_1^{\mathsf{top}}, \dots, f_m^{\mathsf{top}}, h_1, \dots, h_{n-k}) \longrightarrow \mathbb{F}[X]/(f_1^{\mathsf{top}}(g_1(X), \dots, g_n(X)), \dots, f_m^{\mathsf{top}}(g_1(X), \dots, g_n(X))).$$

This isomorphism implies that the primal Modeling 5 and the dual Modeling 6 have the same degree of regularity with probability $\geq 1 - \frac{nd+k}{|\mathbb{F}|}$ *over the randomness of* $g_1, \dots, g_n \leftarrow \mathbb{F}[X]^1$ *where* $d = \max_{i \in [n]}(\deg f_i)$*.*

Proof. Let us first prove the existence of the isomorphism. Denote by I the homogeneous ideal generated by these terms and set

$$\begin{aligned} Q := \mathbb{F}[X]/I =& \mathbb{F}[X]/(f_1^{\mathsf{top}}(-g_1(X), \dots, -g_n(X)), \dots, f_m^{\mathsf{top}}(-g_1(X), \dots, -g_n(X))) \\ =& \mathbb{F}[X]/(f_1^{\mathsf{top}}(g_1(X), \dots, g_n(X)), \dots, f_m^{\mathsf{top}}(g_1(X), \dots, g_n(X))). \end{aligned}$$

(Note that the minus signs are irrelevant, since $f_1^{\mathsf{top}}, \dots, f_m^{\mathsf{top}}$ are homogeneous polynomials.) Denote by J the homogeneous ideal generated by

$$f_1^{\mathsf{top}}(E), \dots, f_m^{\mathsf{top}}(E), h_1(E), \dots, h_{n-k}(E),$$

and set

$$R := \mathbb{F}[E]/J = \mathbb{F}[E]/(f_1^{\mathsf{top}}, \dots, f_m^{\mathsf{top}}, h_1, \dots, h_{n-k}).$$

For the isomorphism, note that the short exact sequence

$$0 \longrightarrow \mathbb{F}^k \xrightarrow{\mathbf{G}} \mathbb{F}^n \xrightarrow{\mathbf{H}} \mathbb{F}^{n-k} \longrightarrow 0$$

induces a sequence of dual ring morphisms

$$0 \longrightarrow \mathbb{F}[S_1, \dots, S_{n-k}] \xrightarrow{\mathbf{H}^*} \mathbb{F}[E] \xrightarrow{\mathbf{G}^*} \mathbb{F}[X] \longrightarrow 0.$$

The maps

$$\begin{aligned} \mathbf{H}^* : \mathbb{F}[S] &\longrightarrow \mathbb{F}[E] \\ S_i &\longmapsto h_i(E) \end{aligned}$$

and

$$\begin{aligned} \mathbf{G}^* : \mathbb{F}[E] &\longrightarrow \mathbb{F}[X] \\ E_i &\longmapsto g_i(X) \end{aligned}$$

preserve degrees since $\mathbf{G}$ and $\mathbf{H}$ are linear. Further, $\mathbf{G}^*$ is surjective, since $\mathbf{G}$ is injective, and $\mathbf{H}^*$ is injective, since $\mathbf{H}$ is surjective. The sequence of rings is not exact, anymore, but the image of $\mathbf{H}^*$ still lies in the kernel of $\mathbf{G}^*$. In particular, the kernel of $\mathbf{G}^*$ is given by $(h_1, \dots, h_{n-k})$, hence, $\mathbf{G}^*$ induces the isomorphism

$$\mathbb{F}[E]/(h_1, \dots, h_{n-k}) \xrightarrow{\sim} \mathbb{F}[X].$$

Under this isomorphism, the element $f_i^{\mathsf{top}}(E)$ gets mapped to $f_i^{\mathsf{top}}(g_1(X), \dots, g_n(X))$. In particular, the ideal

$$(f_1^{\mathsf{top}}(E), \dots, f_m^{\mathsf{top}}(E)) \subset \mathbb{F}[E]/(h_1, \dots, h_{n-k})$$

gets mapped to the ideal

$$(f_1^{\mathsf{top}}(g_1(X), \dots, g_n(X)), \dots, f_m^{\mathsf{top}}(g_1(X), \dots, g_n(X))) \subset \mathbb{F}[X].$$

Hence, we have a grade-preserving isomorphism $Q \to R$.

The second claim follows whenever the top terms of the primal modeling are given by

$$f_1^{\mathsf{top}}(-g_1(X), \dots, -g_n(X)), \dots, f_m^{\mathsf{top}}(-g_1(X), \dots, -g_n(X))$$

and the top terms of the dual modeling are given by

$$f_1^{\mathsf{top}}(E), \ldots, f_m^{\mathsf{top}}(E), h_1(E), \ldots, h_{n-k}(E).$$

Both events do not need to hold in general[11]. Hence, we need to upper bound the probability of

$$(f_i(y_1 - g_1(X), \ldots, y_n - g_n(X)))^{\mathsf{top}} \neq f_i^{\mathsf{top}}(-g_1(X), \ldots, -g_n(X)).$$

By the Schwartz-Zippel lemma, this probability is bounded by $\leq \frac{d}{|\mathbb{F}|}$ for one $i \in [n]$. By a union bound, all top terms coincide with the generators of I with probability at least $\geq 1 - \frac{dn}{|\mathbb{F}|}$.

Now, the polynomials $f_1^{\mathsf{top}}, \ldots, f_n^{\mathsf{top}}, h_1, \ldots, h_{n-k}$ can only deviate from the top terms of Modeling 6 if one of the h_i is zero. This can only happen, if $\mathbf{G}$ does not have full rank, which may happen with probability at most $\frac{k}{|\mathbb{F}|}$.

Hence, the top terms of both modelings are given by the generators of I and J with probability at least $\geq 1 - \frac{dn+k}{|\mathbb{F}|}$.

Whenever that is the case, the degree of regularity of the primal and dual modeling is the minimal d s.t. $Q^d = 0$ and $R^d = 0$, respectively. Since Q and R are isomorphic, we have $Q^d = 0$ iff $R^d = 0$ for all d. Hence, the second claim follows. □

C More Block Hypotheses

Lemma 25. *Let $b, k \in \mathbb{N}$, $k \geq 3$, $w = 3$ and let $\mathbb{F}$ be any field. If $b < \frac{2}{3}k$, then Hypotheses 3 and 4 are false.*

Proof. It suffices to show that if

$$A = \operatorname{span}_{\mathbb{F}} \left\{ f_\alpha^{(1)} \;\middle|\; 1 \leq \alpha \leq \frac{2}{3}k \right\}, \qquad B = \operatorname{span}_{\mathbb{F}} \left\{ f_\alpha^{(2)} \;\middle|\; 1 \leq \alpha \leq \frac{2}{3}k \right\}$$

are subspaces of $\mathbb{F}[X]^1$ and have dimension $\frac{2}{3}k$ and

$$C = \operatorname{span}_{\mathbb{F}} \left\{ f_\alpha^{(3)} \;\middle|\; 1 \leq \alpha \leq \frac{2}{3}k - 1 \right\}$$

is a subspace of $\mathbb{F}[X]^1$ and has dimension $\frac{2}{3}k - 1$, then $\overline{V_1} + \overline{V_2} + \overline{V_3} \neq \mathbb{F}[X]^2$ where

$$\overline{V_i} = \operatorname{span}_{\mathbb{F}} \left\{ f_\alpha^{(i)} \cdot f_\beta^{(i)} \;\middle|\; 1 \leq \alpha \leq \beta \leq b \right\}.$$

Without loss of generality, we can assume that we have

$$\dim_{\mathbb{F}} A \cap B = \frac{1}{3}k, \qquad \dim_{\mathbb{F}} A \cap C = \dim_{\mathbb{F}} B \cap C = \frac{1}{3}k - 1.$$

Therefore, there exist a basis $H_{A \cap B}$ of $A \cap B$, a basis $H_{A \cap C}$ of $A \cap C$, a basis $H_{B \cap C}$ of $B \cap C$ and elements $a \in A \setminus ((A \cap B) + (A \cap C))$ and $b \in B \setminus ((A \cap B) + (B \cap C))$ such that

$$A = \operatorname{span}_{\mathbb{F}}\{H_{A \cap B}\} \oplus \operatorname{span}_{\mathbb{F}}\{H_{A \cap C}\} \oplus \operatorname{span}_{\mathbb{F}}\{a\}$$

[11] For example, if $s_1 \neq 0$, but $h_1 = 0$, then $(h_1(X) - s_1)^{\mathsf{top}} = -s_1 \neq 0 = h_1^{\mathsf{top}}(X)$.

$$B = \mathrm{span}_{\mathbb{F}}\{H_{A\cap B}\} \oplus \mathrm{span}_{\mathbb{F}}\{H_{B\cap C}\} \oplus \mathrm{span}_{\mathbb{F}}\{b\}$$
$$C = \mathrm{span}_{\mathbb{F}}\{H_{A\cap C}\} \oplus \mathrm{span}_{\mathbb{F}}\{H_{B\cap C}\}.$$

If we consider the ideal $I = (A \cap B) + (A \cap C) + (B \cap C)$ and the morphism it induces, namely,

$$\begin{aligned} \phi\colon\ \mathbb{F}[X] &\longrightarrow \mathbb{F}[X]/I \\ x &\longmapsto x + I \end{aligned}$$

we have that

$$\begin{aligned} \phi(\overline{V_1}) &= \mathrm{span}_{\mathbb{F}}\{a^2 + I\}, \\ \phi(\overline{V_2}) &= \mathrm{span}_{\mathbb{F}}\{b^2 + I\}, \\ \phi(\overline{V_3}) &= 0. \end{aligned}$$

However, $\phi(\mathbb{F}[X]^2) \simeq \mathbb{F}[Y_1, Y_2]^2$ has dimension 3. Whence $\overline{V_1} + \overline{V_2} + \overline{V_3} \neq \mathbb{F}[X]^2$. □

Lemma 26. *Let $b, k \in \mathbb{N}$, $k \geq 3$, $w = 3$ and let $\mathbb{F}$ be any field. If $b \geq 2k/3$, then Hypothesis 4 is true for $(b, k, w, \mathbb{F})$ and Hypothesis 3 is true for $(b + 1, k, w, \mathbb{F})$.*

Proof. Let us first assume $k = 3a$ and $b = 2a$ for some $a \in \mathbb{N}$. In this case, divide $X_1, \ldots, X_k$ into three groups $Y_1, \ldots, Y_a$, $Z_1, \ldots, Z_a$, $W_1, \ldots, W_a$. Let

$$\begin{aligned} A_1 &:= \mathrm{span}_{\mathbb{F}}\{Y_1, \ldots, Y_a, Z_1, \ldots, Z_a\}, \\ A_2 &:= \mathrm{span}_{\mathbb{F}}\{Y_1, \ldots, Y_a, W_1, \ldots, W_a\}, \\ A_3 &:= \mathrm{span}_{\mathbb{F}}\{Z_1, \ldots, Z_a, W_1, \ldots, W_a\}. \end{aligned}$$

It holds $\mathbb{F}[X]^2 = \overline{V_1} + \overline{V_2} + \overline{V_3}$ where

$$\overline{V_i} := \mathrm{span}_{\mathbb{F}}\left\{f \cdot g \mid f, g \in A_i\right\}.$$

Indeed, all monomials $Y_i Z_j$ are contained in $\overline{V_1}$, while all monomials $Y_i W_j$ lie in $\overline{V_2}$ and all monomials $Z_i W_j$ are in $\overline{V_3}$.

Now, assume $k = 3a + 2$, $b = 2a + 2$. This case follows from the above case by setting $k' = k + 1 = 3a + 3$. If $(f_1^{(1)}, \ldots, f_b^{(1)})$, $(f_1^{(2)}, \ldots, f_b^{(2)})$, $(f_1^{(3)}, \ldots, f_b^{(3)})$ is a solution for b, k', w over $\mathbb{F}[X_1, \ldots, X_{k'}]$, we can set $X_{k'}$ to zero and get a solution for b, k, w.

Now, consider the case $k = 3a + 1$, $b = 2a + 1$. In this case, we subdivide $X_1, \ldots, X_k$ into three groups $Y_1, \ldots, Y_a$, $Z_1, \ldots, Z_a$, $W_1, \ldots, W_a$ plus an extra variable U and set

$$\begin{aligned} A_1 &:= \mathrm{span}_{\mathbb{F}}\{Y_1, \ldots, Y_a, Z_1, \ldots, Z_a, U\}, \\ A_2 &:= \mathrm{span}_{\mathbb{F}}\{Y_1, \ldots, Y_a, W_1, \ldots, W_a, U\}, \\ A_3 &:= \mathrm{span}_{\mathbb{F}}\{Z_1, \ldots, Z_a, W_1, \ldots, W_a, U\}. \end{aligned}$$

It is now easy to verify, that $A_1 \cdot A_1 + A_2 \cdot A_2 + A_3 \cdot A_3 = \mathbb{F}[X]^2$. □

Lemma 27. *Let $a \in \mathbb{N}$ and assume*

$$w = a^2, \qquad b \geq k/a, \qquad |\mathbb{F}| \geq b, \qquad \mathsf{char}\,\mathbb{F} = 2.$$

Then, Hypothesis 4 is true for $(b, k, w, \mathbb{F})$ and Hypothesis 3 is true for $(b + 1, k, w, \mathbb{F})$.

Proof. As in Lemma 12, we can assume without loss of generality $k = ab$. Again, we divide the variables $X_1, \ldots, X_k$ into a groups:

$$Y_1^{(1)}, \ldots, Y_b^{(1)}, \qquad \ldots, \qquad Y_1^{(a)}, \ldots, Y_b^{(a)}.$$

Let $\kappa_1, \ldots, \kappa_b$ be b distinct elements of $\mathbb{F}$. We again construct blocks $(A_\alpha)_\alpha$, $(B_{\alpha,\beta})_{\alpha,\beta\in[a],\alpha<\beta}$, and $(C_{\alpha,\beta})_{\alpha,\beta\in[a],\alpha<\beta}$ of size $b+1$. For $\alpha \in [a]$, we set

$$A_\alpha := \{Y_1^{(\alpha)}, \ldots, Y_b^{(\alpha)}, Y_1^{(\alpha)} + \ldots + Y_b^{(\alpha)}\}.$$

For $\alpha, \beta \in [a]$ with $\alpha < \beta$, we set

$$\begin{aligned} B_{\alpha,\beta} &:= \{Y_1^{(\alpha)} + Y_1^{(\beta)}, \ldots, Y_b^{(\alpha)} + Y_b^{(\beta)}, Y_1^{(\alpha)} + \ldots + Y_b^{(\alpha)}\}, \\ C_{\alpha,\beta} &:= \{Y_1^{(\alpha)} + \kappa_1 \cdot Y_1^{(\beta)}, \ldots, Y_b^{(\alpha)} + \kappa_b \cdot Y_b^{(\beta)}, Y_1^{(\alpha)} + \ldots + Y_b^{(\alpha)}\}. \end{aligned}$$

Further,

$$\begin{aligned} \overline{U}_\alpha &:= \operatorname{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in A_\alpha\}, \\ \overline{V}_{\alpha,\beta} &:= \operatorname{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in B_{\alpha,\beta}\}, \\ \overline{W}_{\alpha,\beta} &:= \operatorname{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in C_{\alpha,\beta}\}. \end{aligned}$$

Because of our reasoning in Lemma 12, we know that all cross-monomials $Y_i^{(\alpha)} \cdot Y_j^{(\beta)}$ for $i \neq j$ are contained in $\sum_\alpha \overline{U}_\alpha + \sum_{\alpha,\beta} \overline{V}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{W}_{\alpha,\beta}$.

Now, let $i = j$. If $\alpha = \beta$, then $Y_i^{(\alpha)} \cdot Y_i^{(\alpha)}$ is contained in $\overline{U}_\alpha$. For $\alpha \neq \beta$, note that we have

$$(Y_i^{(\alpha)} + Y_i^{(\beta)}) \cdot (Y_1^{(\alpha)} + \ldots + Y_b^{(\alpha)}) \in \overline{V}_{\alpha,\beta}.$$

Since $\sum_\alpha \overline{U}_\alpha + \sum_{\alpha,\beta} \overline{V}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{W}_{\alpha,\beta}$ contains all cross-monomials $Y_i^{(\beta)} Y_{i'}^{(\alpha)}$ for $i' \neq i$, it also contains

$$(Y_i^{(\alpha)} + Y_i^{(\beta)}) \cdot Y_i^{(\alpha)} = Y_i^{(\alpha)} \cdot Y_i^{(\alpha)} + Y_i^{(\alpha)} \cdot Y_i^{(\beta)}.$$

Since the squares $(Y_i^{(\alpha)})^2$ are also contained in $\overline{U}_\alpha$, it follows that $\sum_\alpha \overline{U}_\alpha + \sum_{\alpha,\beta} \overline{V}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{W}_{\alpha,\beta}$ also contains $Y_i^{(\alpha)} \cdot Y_i^{(\beta)}$. Hence, it contains all monomials. □

Lemma 28. *Let $a \in \mathbb{N}$ and assume*

$$w \geq a + 3\binom{a}{2}, \qquad |\mathbb{F}|^2 \geq b, \qquad b \geq k/a, \qquad \mathsf{char}\, \mathbb{F} \neq 2.$$

Then, Hypothesis 4 is true for $(b, k, w, \mathbb{F})$ and Hypothesis 3 is true for $(b + 1, k, w, \mathbb{F})$.

Proof. It suffices to prove Hypothesis 4. Again, we can assume that $k = ba$ and $w = a + 3\binom{a}{2}$. Further, set $r := \left\lceil \sqrt{b} \right\rceil$ and note $|\mathbb{F}| \geq r$.

To prove the hypothesis, let us divide the $k = ba$ variables of $\mathbb{F}[X]$ into a groups:

$$Y_1^{(1)}, \ldots, Y_b^{(1)}, \qquad \cdots \qquad Y_1^{(a)}, \ldots, Y_b^{(a)}.$$

Let $\kappa_1, \ldots, \kappa_r$ be r distinct elements of $\mathbb{F}$. We construct four groups of blocks: the first group contains a blocks $A_1, \ldots, A_a \subset \mathbb{F}[X]^1$, the second, third and fourth groups contain $\binom{a}{2}$ blocks, which we denote by $(B_{\alpha,\beta})_{\alpha,\beta\in[a],\alpha<\beta}$, $(C_{\alpha,\beta})_{\alpha,\beta\in[a],\alpha<\beta}$ and $(D_{\alpha,\beta})_{\alpha,\beta\in[a],\alpha<\beta}$.

For $\alpha \in [a]$, we set

$$A_\alpha \coloneqq \{Y_1^{(\alpha)}, \ldots, Y_b^{(\alpha)}\}.$$

For $\alpha, \beta \in [a]$ with $\alpha < \beta$, we set

$$\begin{aligned}
B_{\alpha,\beta} \coloneqq &\{Y_1^{(\alpha)} + Y_1^{(\beta)}, \ldots, Y_b^{(\alpha)} + Y_b^{(\beta)}\},\\
C_{\alpha,\beta} \coloneqq &\{Y_{t+sr}^{(\alpha)} + \kappa_t \cdot Y_{t+sr}^{(\beta)}, \mid t \in [r], s \in [r-1]_0 \text{ s.t. } t + sr \leq b\},\\
D_{\alpha,\beta} \coloneqq &\{Y_{t+sr}^{(\alpha)} + \kappa_{t+s \bmod r} \cdot Y_{t+sr}^{(\beta)} \mid t \in [r], s \in [r-1]_0 \text{ s.t. } t + sr \leq b\}.
\end{aligned}$$

Further, we define

$$\begin{aligned}
\overline{U}_\alpha \coloneqq &\operatorname{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in A_\alpha\},\\
\overline{V}_{\alpha,\beta} \coloneqq &\operatorname{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in B_{\alpha,\beta}\},\\
\overline{W}_{\alpha,\beta} \coloneqq &\operatorname{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in C_{\alpha,\beta}\},\\
\overline{R}_{\alpha,\beta} \coloneqq &\operatorname{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in D_{\alpha,\beta}\}.
\end{aligned}$$

Then, we have for all $i, j \in [b]$ and $\alpha, \beta \in [a]$

$$\begin{aligned}
&Y_i^{(\alpha)} \cdot Y_j^{(\alpha)} \in \overline{U}_\alpha,\\
&(Y_i^{(\alpha)} + Y_i^{(\beta)})(Y_j^{(\alpha)} + Y_j^{(\beta)}) \in \overline{V}_{\alpha,\beta},\\
&(Y_i^{(\alpha)} + \kappa_{i \bmod r} \cdot Y_i^{(\beta)})(Y_j^{(\beta)} + \kappa_{j \bmod r} \cdot Y_j^{(\beta)}) \in \overline{W}_{\alpha,\beta},
\end{aligned}$$

and for $i \in \{1 + sr, \ldots, r + sr\}$ and $j \in \{1 + s'r, \ldots, r + s'r\}$ where $s \neq s'$ and $\alpha < \beta \in [a]$

$$(Y_i^{(\alpha)} + \kappa_{i+s \bmod r} \cdot Y_i^{(\beta)})(Y_j^{(\beta)} + \kappa_{j+s' \bmod r} \cdot Y_j^{(\beta)}) \in \overline{R}_{\alpha,\beta}.$$

Set $\overline{S} = \sum_\alpha \overline{U}_\alpha + \sum_{\alpha,\beta} \overline{V}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{W}_{\alpha,\beta} + \sum_{\alpha,\beta} \overline{R}_{\alpha,\beta}$. It remains to show that $Y_i^{(\alpha)} \cdot Y_j^{(\beta)} \in \overline{S}$ for $i, j \in [b]$ and $\alpha < \beta \in [a]$. Following the same arguments as in Lemma 12, it follows that

1. for all $i \in [b]$ and $\alpha < \beta \in [a]$, we have
$$Y_i^{(\alpha)} Y_i^{(\beta)} \in \overline{V}_{\alpha,\beta} + \overline{U}_\alpha + \overline{U}_\beta \subseteq \overline{S},$$
2. for all $i, j \in [b]$ with $i \neq j \bmod r$ and $\alpha, \beta \in [a]$ we have
$$Y_i^{(\alpha)} Y_j^{(\beta)} \in \overline{W}_{\alpha,\beta} + \overline{V}_{\alpha,\beta} + \overline{U}_\alpha + \overline{U}_\beta \subseteq \overline{S}.$$

In order to show that $Y_i^{(\alpha)} Y_j^{(\beta)} \in \overline{S}$ for $i = j \bmod r$ but $i \neq j$ we can repeat the argument used in Lemma 12. Indeed, we can assume without loss of generality that $i \in \{1+sr, \dots, r+sr\}$ and $j \in \{1+s'r, \dots, r+s'r\}$ where $s, s' \in \{0, \dots, r-1\}$ and $s < s'$. Then, we have

$$(Y_i^{(\alpha)} + Y_i^{(\beta)}) \cdot (Y_j^{(\alpha)} + Y_j^{(\beta)}) \in \overline{V}_{\alpha,\beta},$$
$$(Y_i^{(\alpha)} + \kappa_{i+s \bmod r} \cdot Y_i^{(\beta)})(Y_j^{(\beta)} + \kappa_{j+s' \bmod r} \cdot Y_j^{(\beta)}) \in \overline{R}_{\alpha,\beta}.$$

Now using the fact that $i = j \bmod r$ and $s \neq s' \bmod r$ we obtain that $\kappa_{i+s \bmod r} \neq \kappa_{j+s' \bmod r}$ and therefore $Y_i^{(\alpha)} Y_j^{(\beta)} \in \overline{S}$. Hence, $\overline{S}$ contains all monomials in $\mathbb{F}[X]^2$. □

We now proceed to combine the ideas of Lemma 28 and Lemma 27 to obtain a result that works in characteristic 2 and fields that satisfy the inequality $|\mathbb{F}|^2 \geq b$.

Lemma 29. *Let $a \in \mathbb{N}$ and assume*

$$w \geq a + 3\binom{a}{2}, \qquad |\mathbb{F}|^2 \geq b, \qquad b \geq k/a, \qquad \mathsf{char}\,\mathbb{F} = 2.$$

Then, Hypothesis 3 is true for $(b+1, k, w, \mathbb{F})$.

Proof. We can assume that $k = ba$ and $w = a + 3\binom{a}{2}$. To prove the hypothesis, let us divide the $k = ba$ variables of $\mathbb{F}[X]$ into a groups:

$$Y_1^{(1)}, \dots, Y_b^{(1)}, \qquad \dots \qquad Y_1^{(a)}, \dots, Y_b^{(a)}.$$

Let $c = \lceil \sqrt{b} \rceil$. Let $\kappa_1, \dots, \kappa_c$ be distinct elements of $\mathbb{F}$ which exist since $|\mathbb{F}|^2 \geq b$. We construct four groups of blocks; for $\alpha \in [a]$, we set

$$A_\alpha := \{Y_1^{(\alpha)}, \dots, Y_b^{(\alpha)}, Y_1^{(\alpha)} + \dots + Y_b^{(\alpha)}\},$$

for $\alpha, \beta \in [a]$ with $\alpha < \beta$, we set

$$B_{\alpha,\beta} := \{Y_1^{(\alpha)} + Y_1^{(\beta)}, \dots, Y_b^{(\alpha)} + Y_b^{(\beta)}, Y_1^{(\alpha)} + \dots + Y_b^{(\alpha)}\},$$
$$C_{\alpha,\beta} := \{Y_{t+sc}^{(\alpha)} + \kappa_t \cdot Y_{t+sc}^{(\beta)} \mid s \in [c-1]_0, t \in [c] \text{ s.t. } t + sc \leq b\} \cup \{\sum_{j=1}^{b} Y_j^{(\alpha)}\},$$
$$D_{\alpha,\beta} := \{Y_{t+sc}^{(\alpha)} + \kappa_{t+s \bmod c} \cdot Y_{t+sc}^{(\beta)} \mid s \in [c-1]_0, t \in [c] \text{ s.t. } t + sc \leq b\} \cup \{\sum_{j=1}^{b} Y_j^{(\alpha)}\}.$$

Further, we define

$$U_\alpha := \mathrm{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in A_\alpha \text{ s.t. } f \neq g\},$$
$$V_{\alpha,\beta} := \mathrm{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in B_{\alpha,\beta} \text{ s.t. } f \neq g\},$$
$$W_{\alpha,\beta} := \mathrm{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in C_{\alpha,\beta} \text{ s.t. } f \neq g\},$$
$$R_{\alpha,\beta} := \mathrm{span}_{\mathbb{F}} \{f \cdot g \mid f, g \in D_{\alpha,\beta} \text{ s.t. } f \neq g\}.$$

Set $S = \sum_\alpha U_\alpha + \sum_{\alpha,\beta} V_{\alpha,\beta} + \sum_{\alpha,\beta} W_{\alpha,\beta} + \sum_{\alpha,\beta} R_{\alpha,\beta}$. By construction, $Y_i^{(\alpha)} Y_j^{(\alpha)} \in U_\alpha$ for all $i \neq j$ and all α. If $i = j$, then $Y_i^{(\alpha)} Y_i^{(\alpha)}$ is contained in U_α, since

$$Y_i^{(\alpha)} \cdot Y_i^{(\alpha)} = Y_i^{(\alpha)} \cdot (Y_1^{(\alpha)} + \dots + Y_b^{(\alpha)}) - \sum_{i' \neq i} Y_i^{(\alpha)} \cdot Y_{i'}^{(\alpha)} \in U_\alpha.$$

Following the same arguments as in Lemma 12 and Lemma 28, it follows that $Y_i^{(\alpha)} Y_j^{(\beta)} \in S$ for all $i \neq j$ and $\alpha \leq \beta$. Finally, we can use the same arguments as in Lemma 27 in order to show that all cross-monomials $Y_i^{(\alpha)} Y_i^{(\beta)} \in S$. □

Lemma 30. *Let $k \in \mathbb{N}$, $w \geq \binom{k+1}{2}$ and $\mathbb{F}$ be any field. Hypothesis 3 is true for $(2, k, w, \mathbb{F})$.*

Proof. Let $m_1, \dots, m_{\binom{k+1}{2}}$ be all degree-2 monomials of $\mathbb{F}[X]$. We can choose both linear forms $f_1^{(i)}, f_2^{(i)}$ of the i-th block s.t.

$$f_1^{(i)} \cdot f_2^{(i)} = m_i.$$

Hence, we have $V_1 + \ldots + V_{\binom{k+1}{2}} = \mathbb{F}[X]^2$ where $V_i = \operatorname{span}_{\mathbb{F}}\{f_1^{(i)} \cdot f_2^{(i)}\}$ □

Lemma 31. *Let $c > 1$ and set $w_c := \frac{3}{2} \cdot \frac{c}{(\sqrt{c}-1)^2}$. We have for all $w \geq w_c$, $k \in \mathbb{N}$, $b > 2$ and fields $\mathbb{F}$ with $|\mathbb{F}| \geq \sqrt{b}$*

$$w \cdot \binom{b}{2} \geq c \cdot \frac{9}{4} \cdot \binom{k+1}{2} \implies \textit{Hypothesis } 3 \textit{ is true for } (b, k, w, \mathbb{F}).$$

Proof. Let $w \geq w_c$, $b > 2$, $k \in \mathbb{N}$ s.t. $w \cdot \binom{b}{2} \geq c \cdot \binom{k+1}{2}$. As in the proof of Lemma 13, we have (since $b \geq 3$)

$$w \geq c \cdot \frac{9}{4} \cdot \frac{(k+1) \cdot k}{b \cdot (b-1)} \geq c \cdot \frac{3}{2} \left(\frac{k}{b-1}\right)^2,$$

Set $a := \left\lceil \frac{k}{b-1} \right\rceil$. We claim that we have $w \geq a + 3\binom{a}{2} = \frac{3a^2 - a}{2}$. This follows because

$$\begin{aligned}
\frac{3a^2 - a}{2} &\leq \frac{3\left(\frac{k}{b-1} + 1\right)^2 - \frac{k}{b-1}}{2} \\
&= \frac{3}{2}\left(\frac{k}{b-1}\right)^2 + \frac{5}{2} \cdot \frac{k}{b-1} + \frac{3}{2} \\
&\leq \frac{w}{c} + 2 \cdot \frac{\sqrt{3}}{\sqrt{2}} \cdot \frac{\sqrt{w}}{\sqrt{c}} + \left(\frac{\sqrt{3}}{\sqrt{2}}\right)^2 \\
&\leq \left(\frac{\sqrt{w}}{\sqrt{c}} + \frac{\sqrt{3}}{\sqrt{2}}\right)^2 \\
&\leq w
\end{aligned}$$

where the last inequality follows from

$$\begin{aligned}
\left(\frac{1}{\sqrt{c}} + \frac{\sqrt{3}}{\sqrt{2w}}\right)^2 &\leq \left(\frac{1}{\sqrt{c}} + \frac{\sqrt{3}}{\sqrt{2w_c}}\right)^2 \\
&= \left(\frac{1}{\sqrt{c}} + \frac{\sqrt{c}-1}{\sqrt{c}}\right)^2 \\
&= 1.
\end{aligned}$$

Since $|\mathbb{F}|^2 \geq b$, Lemmas 28 and 29 imply now Hypothesis 3 for $(b, k, a + 3\binom{a}{2}, \mathbb{F})$. □

D On Semi-Regularity

There are four different notions of semi-regularity [Big+20]. The original definition goes back to Pardue:

Definition 8 (Semi-Regular Sequence [Par10])**.** Let R be a graded ring. An element $f \in R^d$ is called **semi-regular** with respect to R if for each $e \in \mathbb{N}_0$ the map

$$\begin{aligned} R^e &\longrightarrow R^{d+e} \\ r &\longmapsto r \cdot f \end{aligned}$$

has full rank (as linear map of finite dimensional vector spaces).

A sequence of homogeneous elements $f_1 \in R^{d_1}, \dots, f_m \in R^{d_m}$ is **semi-regular** if each f_i (as element of $R^{d_i}/(f_1, \dots, f_{i-1})^{d_i}$) is semi-regular with respect to $R/(f_1, \dots, f_{i-1})$.

Over small fields (like $\mathbb{Z}_2$), the following relaxation seems to be more appropriate [Bar04].

Definition 9 (Binary Semi-Regular Sequence)**.** Let R be a graded $\mathbb{Z}_2$-algebra s.t. $f^2 = 0$ for all $f \in R$. Let $f \in R^d$ be homogeneous. f is called **semi-regular over** $\mathbb{Z}_2$ with respect to R if for each $e \in \mathbb{N}_0$ the map

$$\begin{aligned} R^e/(f) &\longrightarrow R^{d+e} \\ r &\longmapsto r \cdot f \end{aligned}$$

has full rank (as linear map of finite dimensional vector spaces).

A sequence of homogeneous elements $f_1 \in R^{d_1}, \dots, f_m \in R^{d_m}$ is **semi-regular over** $\mathbb{Z}_2$ if each f_i (as element of $R^{d_i}/(f_1, \dots, f_{i-1})^{d_i}$) is semi-regular over $\mathbb{Z}_2$ with respect to $R/(f_1, \dots, f_{i-1})$.

Besides the original definitions of semi-regularity, there exist two additional definitions that are more popular in cryptography [FBS04]:

Definition 10 (Cryptographic Semi-Regular Sequence [FBS04])**.** Let R be a graded ring and $f_1 \in R^{d_1}, \dots, f_m \in R^{d_m}$ be homogeneous. $f_1, \dots, f_m$ is called a **cryptographic semi-regular sequence** if for all $i \in [m]$ and $e < \mathrm{d}_{\mathsf{reg}}(f_1, \dots, f_m) - d_i$ the map

$$\begin{aligned} (R/(f_1, \dots, f_{i-1}))^e &\longrightarrow (R/(f_1, \dots, f_{i-1}))^{e+d_i} \\ r &\longmapsto r \cdot f_i \end{aligned}$$

has full rank (as linear map of finite dimensional vector spaces).

The relaxation over $\mathbb{Z}_2$ goes back to Bardet [BFS03; Bar04].

Definition 11 (Binary Cryptographic Semi-Regular Sequence [BFS03; Bar04])**.** Let R be a graded $\mathbb{Z}_2$-algebra s.t. $f^2 = 0$ for each $f \in R$. Let $f_1 \in R^{d_1}, \dots, f_m \in R^{d_m}$ be homogeneous. $f_1, \dots, f_m$ is called a **cryptographic semi-regular sequence over** $\mathbb{Z}_2$ if for all $i \in [m]$ and $e < \mathrm{d}_{\mathsf{reg}}(f_1, \dots, f_m) - d_i$ the map

$$\begin{aligned} (R/(f_1, \dots, f_{i-1}, f_i))^e &\longrightarrow (R/(f_1, \dots, f_{i-1}))^{e+d_i} \\ r &\longmapsto r \cdot f_i \end{aligned}$$

has full rank (as linear map of finite dimensional vector spaces).

Both definitions of semi-regularity (the normal and the cryptographic one) have separate shortcomings. The definition due to Pardue is not stable under permutations: for example, X, Y, X is a semi-regular[12] sequence with respect to $\mathbb{F}[X, Y]$ according to Definition 8, but the permutated sequence X, X, Y cannot be semi-regular[13]. On the other hand, subsequences $f_1, \ldots, f_t$ of semi-regular sequences $f_1, \ldots, f_m$, $t \leq m$, will always stay semi-regular.

Cryptographic semi-regular sequences are always stable under permutations (as the next lemma will show). However, subsequences of cryptographic semi-regular sequences do not need to be cryptographic semi-regular, anymore. This leads to absurd situations where cryptographic semi-regular sequences over $\mathbb{Z}_2$ of length 1 in $\mathbb{Z}_2[X_1, \ldots, X_n]/(X_1^2, \ldots, X_n^2)$ of degree $1 < d < n/3$ cannot exist [HMS17].

Ultimately, for estimating the Hilbert series of a quotient ring, it does not matter which definition one uses:

Lemma 32. *Let R be a graded $\mathbb{F}$-algebra and $f_1 \in R^{d_1}, \ldots, f_m \in R^{d_m}$.*

1. *If $f_1, \ldots, f_m$ are semi-regular, we have*

$$\mathcal{H}_{R/(f_1,\ldots,f_m)}(T) = \left[\prod_{i=1}^{m}(1 - T^{d_i}) \cdot \mathcal{H}_R(T)\right]_+ .$$

2. *$f_1, \ldots, f_m$ are cryptographic semi-regular iff*

$$\mathcal{H}_{R/(f_1,\ldots,f_m)}(T) = \left[\prod_{i=1}^{m}(1 - T^{d_i}) \cdot \mathcal{H}_R(T)\right]_+ .$$

Now, assume $\mathbb{F} = \mathbb{Z}_2$ and that we have $f^2 = 0$ for each $f \in R$:

1. *If $\mathbb{F} = \mathbb{Z}_2$ and $f_1, \ldots, f_m$ are semi-regular over $\mathbb{Z}_2$, we have*

$$\mathcal{H}_{R/(f_1,\ldots,f_m)}(T) = \left[\frac{\mathcal{H}_R(T)}{\prod_{i=1}^{m}(1 + T^{d_i})\cdot}\right]_+ .$$

2. *If $\mathbb{F} = \mathbb{Z}_2$, then $f_1, \ldots, f_m$ are cryptographic semi-regular over $\mathbb{Z}_2$ iff*

$$\mathcal{H}_{R/(f_1,\ldots,f_m)}(T) = \left[\frac{\mathcal{H}_R(T)}{\prod_{i=1}^{m}(1 + T^{d_i})\cdot}\right]_+ .$$

Proofs for the claims in Lemma 32 can be found in [Par10; BFS03; Bar04; HMS17].

[12] Indeed, X is not a zero-divisor in $\mathbb{F}[X, Y]$ and Y is not a zero-divisor in $\mathbb{F}[X, Y]/(X) = \mathbb{F}[X]$. While X is zero in $\mathbb{F}[X, Y]/(X, Y) = \mathbb{F}$, this does not hurt semi-regularity, as we have $(\mathbb{F}[X, Y]/(X, Y))^d = 0$ for $d > 0$. Hence, multiplication with X is always surjective as a linear map $(\mathbb{F}[X, Y]/(X, Y))^d \to (\mathbb{F}[X, Y]/(X, Y))^{d+1}$.

[13] Indeed, X is zero in $\mathbb{F}[X, Y]/(X) = \mathbb{F}[Y]$ and, hence, the linear map $\mathbb{F}[Y]^d \to \mathbb{F}[Y]^{d+1}$ given by multiplication with X does not have full rank.

E Tensor Hypotheses

We will show here an equivalence between Hypotheses 3 and 4 for homogeneous polynomials and similar hypotheses for tensors. Denote by

$$\otimes : \mathbb{F}^k \times \mathbb{F}^k \to \mathbb{F}^k \otimes \mathbb{F}^k \simeq \mathbb{F}^{k \times k}$$

the tensor product in the following. We first formulate the following hypotheses:

Hypothesis 5. For $b, k, w \in \mathbb{N}$ and a field $\mathbb{F}$, there exist vectors $v_\alpha^{(i)} \in \mathbb{F}^k$, $\alpha \in [b]$, $i \in [w]$, s.t.

$$V_1 + \ldots + V_w = \mathbb{F}^{k \times k}$$

where

$$V_i := \operatorname{span}_{\mathbb{F}} \left\{ v_\alpha^{(i)} \otimes v_\beta^{(i)} \;\middle|\; \alpha, \beta \in [b], \alpha \neq \beta \right\}.$$

Hypothesis 6. For $b, k, w \in \mathbb{N}$ and a field $\mathbb{F}$, there exist vectors $v_\alpha^{(i)} \in \mathbb{F}^k$, $\alpha \in [b]$, $i \in [w]$, s.t.

$$\overline{V_1} + \ldots + \overline{V_w} = \mathbb{F}^{k \times k}$$

where

$$\overline{V_i} := \operatorname{span}_{\mathbb{F}} \left\{ v_\alpha^{(i)} \otimes v_\beta^{(i)} \;\middle|\; \alpha, \beta \in [b] \right\}.$$

Usually, Hypothesis 5 and Hypothesis 6 do not need to be equivalent to their polynomial counterparts Hypothesis 3 and Hypothesis 4. However, in the special case of characteristic 2, an equivalence can be established, as the next lemma implies:

Lemma 33. *Let $\mathbb{F}$ be a field of characteristic two, $b, k, w \in \mathbb{N}$ and consider the morphism*

$$\begin{aligned} \phi : \mathbb{F}^{k \times k} &\longrightarrow \mathbb{F}[X]^2 \\ \mathbf{M} &\longmapsto X^{\mathsf{T}} \cdot \mathbf{M} \cdot X. \end{aligned}$$

Let $V \subset \mathbb{F}^{k \times k}$ be a subspace that is invariant under transposing matrices. The following two statements are equivalent:

1. *$\mathbb{F}^{k \times k} = V$,*
2. *$\mathbb{F}[X]^2 = \phi(V)$.*

Proof. It suffices to observe that ϕ is surjective in order to prove that the first statement implies the second. So it remains to show that $\mathbb{F}[X]^2 = \phi(V)$ implies $\mathbb{F}^{k \times k} = V$.

We first show that $\ker \phi$ is contained in the space spanned by $\mathbf{a} \otimes \mathbf{b} + \mathbf{b} \otimes \mathbf{a}$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}^k$. Indeed, if $\mathbf{M} \in \ker \phi$, then we must have

$$\mathbf{x}^{\mathsf{T}} \cdot \mathbf{M} \cdot \mathbf{x} = 0$$

for every $\mathbf{x} \in \mathbb{F}^k$. By letting $\mathbf{x} = \mathbf{e}_i + \mathbf{e}_j$ be the sum of the i-th and j-th unit vector, it follows

$$\mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_i + \mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j + \mathbf{e}_j^\mathsf{T}\mathbf{M}\mathbf{e}_i + \mathbf{e}_j^\mathsf{T}\mathbf{M}\mathbf{e}_j = \mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j + \mathbf{e}_j^\mathsf{T}\mathbf{M}\mathbf{e}_i = 0.$$

Ergo, $\mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j = -\mathbf{e}_j^\mathsf{T}\mathbf{M}\mathbf{e}_i$. Since $\mathsf{char}\,\mathbb{F} = 2$, we have $\mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j = \mathbf{e}_j^\mathsf{T}\mathbf{M}\mathbf{e}_i$. It now follows

$$\begin{aligned}\mathbf{M} = &\sum_{i,j=1}^{k} \mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j \cdot \mathbf{e}_i \otimes \mathbf{e}_j \\ =&\sum_{i=1}^{k} \mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_i \cdot \mathbf{e}_i \otimes \mathbf{e}_i + \sum_{i\neq j} \mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j \cdot \mathbf{e}_i \otimes \mathbf{e}_j \\ =&0 + \sum_{i\neq j} \mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j \cdot \mathbf{e}_i \otimes \mathbf{e}_j \\ =&\sum_{i<j} \mathbf{e}_i^\mathsf{T}\mathbf{M}\mathbf{e}_j \cdot (\mathbf{e}_i \otimes \mathbf{e}_j + \mathbf{e}_j \otimes \mathbf{e}_i).\end{aligned}$$

Hence, $\ker\phi$ is generated by all $\mathbf{e}_i \otimes \mathbf{e}_j + \mathbf{e}_j \otimes \mathbf{e}_i$.

Now, let $\mathbf{M} \in \mathbb{F}^{k\times k}$. By assumption, there exists $\mathbf{P} \in V$ such that $\phi(\mathbf{M}) = \phi(\mathbf{P})$. Therefore, there exists $\mathbf{K} \in \ker\phi$ such that $\mathbf{M} = \mathbf{P} + \mathbf{K}$. Moreover, we also obtain that

$$\mathbf{M} + \mathbf{M}^\mathsf{T} = \mathbf{P} + \mathbf{P}^\mathsf{T} + \mathbf{K} + \mathbf{K}^\mathsf{T}.$$

Since $\mathbf{K}$ must be symmetric and $\mathsf{char}\,\mathbb{F} = 2$, we have $\mathbf{K} + \mathbf{K}^\mathsf{T} = 0$. Since V is stable under transposition, it also contains $\mathbf{P}^\mathsf{T}$. It follows $\mathbf{M} + \mathbf{M}^\mathsf{T} \in V$ for all $\mathbf{M} \in \mathbb{F}^{k\times k}$. This implies that V contains all $\mathbf{e}_i \otimes \mathbf{e}_j + \mathbf{e}_j \otimes \mathbf{e}_i$. In particular, it contains $\ker\phi$. The claim now follows by $V = V + \ker\phi = \mathbb{F}^{k\times k}$. □

The above equivalence can be generalized to tensors of any order. For this end, let us introduce some additional notation: If V is a vector space over $\mathbb{F}$, we denote by V^* its dual. If $\{V_i\}_{i\in[d]}$ are vector spaces over $\mathbb{F}$ we denote by $V_1 \otimes \ldots \otimes V_d$ the tensor product whose elements $\mathbf{T} = \sum \mathbf{v}_1 \otimes \ldots \otimes \mathbf{v}_d$ correspond to multilinear maps $f_\mathbf{T}\colon V_1^* \times \ldots \times V_d^* \to \mathbb{F}$ defined as $f_\mathbf{T}(a_1, \ldots, a_d) = \sum a_1(\mathbf{v}_1)\cdots a_d(\mathbf{v}_d)$. If $\{\mathbf{u}_j^i\}_j$ is a basis for each vector space V_i, then $\{\mathbf{u}_{j_1}^1 \otimes \ldots \otimes \mathbf{u}_{j_d}^d\}_{j_1,\ldots,j_d}$ is a basis for $V_1 \otimes \ldots \otimes V_d$.

In the case when $V_i = V$ for all i, we write $V^{\otimes d}$ and refer to d as the degree of a tensor in $V^{\otimes d}$. We define the action of the symmetric group S_d on $V^{\otimes d}$ by mapping a permutation σ and a tensor $\mathbf{T} = \sum \mathbf{v}_1 \otimes \ldots \otimes \mathbf{v}_d$ to the tensor $\sigma\mathbf{T} = \sum \mathbf{v}_{\sigma^{-1}1} \otimes \ldots \otimes \mathbf{v}_{\sigma^{-1}d}$ which corresponds to the map defined as $f_{\sigma\mathbf{T}}(a_1, \ldots, a_d) = f_\mathbf{T}(a_{\sigma(1)}, \ldots, a_{\sigma(d)})$. We say that a tensor $\mathbf{T} \in V^{\otimes d}$ is symmetric if for all permutations $\sigma \in S_d$, $\sigma\mathbf{T} = \mathbf{T}$. If V has dimension k and $\{\mathbf{u}_i\}_{i\in[k]}$ is a basis, then any symmetric tensor can be written as $\sum_{i_1,\ldots,i_d=1}^{k} T_{i_1,\ldots,i_d} \mathbf{u}_{i_1} \otimes \ldots \otimes \mathbf{u}_{i_d}$ with the property that $T_{i_1,\ldots,i_d} = T_{\sigma i_1,\ldots,\sigma i_d}$ for all $\sigma \in S_d$.

For the vector space $\mathbb{F}^k$ we denote by $\{\mathbf{e}_i\}_{i\in[k]}$ the standard basis, that is, the entries $(\mathbf{e}_i)_j$ are zero for every $j \neq i$ and $(\mathbf{e}_i)_i = 1$. We use the notation $\{\mathbf{e}_i^*\}_{i\in[k]}$ for the dual basis given by $\mathbf{e}_i^*(\mathbf{e}_j) = 0$ for $j \neq i$ and $\mathbf{e}_i^*(\mathbf{e}_i) = 1$.

Lemma 34. *Let $\mathbb{F}$ be a field of characteristic two, $b, k, w, d \in \mathbb{N}$ and consider the morphism*

$$\begin{aligned}\phi\colon (\mathbb{F}^k)^{\otimes d} &\longrightarrow \mathbb{F}[X]^d \\ \mathbf{T} &\longmapsto \sum_{i_1,\dots,i_d \in [k]} \mathbf{T}(\mathbf{e}^*_{i_1}, \dots, \mathbf{e}^*_{i_d}) \cdot X_{i_1} \cdots X_{i_d}.\end{aligned}$$

Let $V \subset (\mathbb{F}^k)^{\otimes d}$ be a subspace of $(\mathbb{F}^k)^{\otimes d}$ that is invariant under the action of S_d. The following two statements are equivalent:

1. $(\mathbb{F}^k)^{\otimes d} = V$,
2. $\mathbb{F}[X]^d = \phi(V)$.

Proof. It suffices to observe that ϕ is surjective in order to prove that the first statement implies the second. So it remains to show that $\mathbb{F}[X]^d = \phi(V)$ implies that $(\mathbb{F}^k)^{\otimes d} = V$.

Let $\mathbf{T} = \sum_{i_1,\dots,i_d=1}^{k} T_{i_1,\dots,i_d} \mathbf{e}_{i_1} \otimes \dots \otimes \mathbf{e}_{i_d} \in \ker \phi$ and $(j_1, \dots, j_d) \in [k]^w$. Then $\sum_{(i_1,\dots,i_d) \in \{(\sigma j_1,\dots,\sigma j_d)\colon \sigma \in S_d\}} T_{(i_1,\dots,i_d)} = 0$. Therefore, we have that $\sum_{\sigma \in S_d} \sigma \mathbf{T} = 0$. In particular, $\ker \phi$ is generated by all tensors $\sum_{\sigma \in S_d} \mathbf{e}_{\sigma(i_1)} \otimes \cdots \otimes \mathbf{e}_{\sigma(i_d)}$ for $i_1, \dots, i_d \in [k]$.

Let $\mathbf{T} \in (\mathbb{F}^k)^{\otimes d}$. By assumption, there exists $\mathbf{P} \in V$ such that $\phi(\mathbf{T}) = \phi(\mathbf{P})$. Therefore, there exists $\mathbf{K} \in \ker \phi$ such that $\mathbf{T} = \mathbf{P} + \mathbf{K}$. Moreover, we also obtain that

$$\begin{aligned}\sum_{\sigma \in S_d} \sigma \mathbf{T} &= \sum_{\sigma \in S_d} \sigma \mathbf{P} + \sum_{\sigma \in S_d} \sigma \mathbf{K} \\ &= \sum_{\sigma \in S_d} \sigma \mathbf{P}\end{aligned}$$

since $\mathbf{K} \in \ker \phi$. By assumption, V is invariant under the action of S_d and $\mathbf{P} \in V$. This shows that $\sum_{\sigma \in S_d} \sigma \mathbf{T} \in V$.

In order to complete the proof it suffices to show that $\ker \phi \subseteq V$. However, this follows now since V contains each generator $\sum_{\sigma \in S_d} \mathbf{e}_{\sigma(i_1)} \otimes \cdots \otimes \mathbf{e}_{\sigma(i_d)}$ of $\ker \phi$. □

F More Attacks of Briaud and Øygarden

F.1 On Hybrid Attacks over Big Fields

To achieve concrete fast runtimes for solving RSD instances for selected parameters, Briaud and Øygarden [BØ23] devise a hybrid algebraic attack: for parameters (f, u) they guess u error-free positions in f of w blocks. The parameters f and u are so optimized such that the resulting system has a low witness degree and degree of regularity (2 or 3).

To analyse this, set $n = (w - f) \cdot b + f \cdot (b - u)$ and consider variables

$$\begin{aligned}&E_1^{(i)}, \dots, E_b^{(i)} && \text{for } i \in [w - f], \\ &F_1^{(i)}, \dots, F_{b-u}^{(i)} && \text{for } i \in [f],\end{aligned}$$

and the ring

$$R := \mathbb{F}[E,F]/((E_\alpha^{(i)}E_\beta^{(i)} \mid i \in [w-f], 1 \le \alpha < \beta \le b) + (F_\alpha^{(i)}F_\beta^{(i)} \mid i \in [f], 1 \le \alpha < \beta \le b-u)).$$

The Hilbert series of this ring is given by

$$\mathcal{H}_R(T) = (1 + bT + bT^2 + \dots)^{w-f} \cdot (1 + (b-u)T + (b-u)T^2 + \dots)^f.$$

The hypothesis underlying the hybrid attack of [BØ23] can now be formalized as:

Hypothesis 7. There exist linear forms $h_1, \dots, h_{n-k} \in R^1$ s.t.

$$\mathcal{H}_{R/(h_1,\dots,h_{n-k})}(T) = \left[(1-T)^{n-k} \cdot (1 + bT + bT^2 + \dots)^{w-f} \cdot (1 + (b-u)T + (b-u)T^2 + \dots)^f\right]_+.$$

In Lemma 21, we show

$$\begin{aligned}&(1-T)^{n-k} \cdot \left(1 + bT + bT^2 + \dots\right)^{w-f} \cdot (1 + (b-u)T + (b-u)T^2 + \dots)^f \\ &= 1 + (k - fu)T + \left(\binom{k - fu + 1}{2} - (w-f)\binom{b}{2} - f\binom{b-u}{2}\right)T^2 + O(T^3).\end{aligned}$$

Hence, Hypothesis 7 implies a degree of regularity 2 whenever

$$(w-f)\binom{b}{2} + f\binom{b-u}{2} \ge \binom{k-fu+1}{2}.$$

Let us set

$$w_1 = w - f, \qquad b_1 = b, \qquad w_2 = f, \qquad b_2 = b - u, \qquad k' = k - fu.$$

By going to a primal model, Hypothesis 7 implies the following hypothesis whenever $w_1\binom{b_1}{2} + w_2\binom{b_2}{2} \ge \binom{k'+1}{2}$:

Hypothesis 8. For parameters $b_1, b_2, k', w_1, w_2 \in \mathbb{N}$, there exist $f_\alpha^{(i)}, g_\beta^{(j)} \in \mathbb{F}[X_1, \dots, X_{k'}]^1$, $i \in [w_1], \alpha \in [b_1], j \in [w_2], \beta \in [b_2]$, s.t.

$$\operatorname{span}_{\mathbb{F}}\left\{f_\alpha^{(i)} \cdot f_\beta^{(i)} \;\middle|\; i \in [w_1], 1 \le \alpha < \beta \le b_1\right\} + \operatorname{span}_{\mathbb{F}}\left\{g_\alpha^{(i)} \cdot g_\beta^{(i)} \;\middle|\; i \in [w_2], 1 \le \alpha < \beta \le b_2\right\} = \mathbb{F}[X]^2.$$

We suspect that Hypothesis 8 is true as long as $b_1, b_2 \le k'/2$ (and $(w - f)\binom{b}{2} + f\binom{b-u}{2} \ge \binom{k-fu+1}{2}$.) This is indeed the case for the parameters analysed in [BØ23].

F.2 On Plain Attacks over the Binaries

Let us now consider the plain binary setting: let $E_\alpha^{(i)}$, $\alpha \in [b]$, $i \in [w]$, be $n = bw$ variables and set

$$\begin{aligned}R &:= \mathbb{Z}_2[E]/(((E_\alpha^{(i)})^2 | i \in [w], \alpha \in [b]) + (E_\alpha^{(i)}E_\beta^{(i)} \mid i \in [w], 1 \le \alpha < \beta \le b)) \\ &= \mathbb{Z}_2[E]/(E_\alpha^{(i)}E_\beta^{(i)} \mid i \in [w], \alpha, \beta \in [b]).\end{aligned}$$

The Hilbert series of R is given by

$$\mathcal{H}_R(T) = (1 + bT)^w.$$

Assumption 2 of [BØ23] corresponds to

Hypothesis 9. There exist linear forms $h_1, \ldots, h_{n-k} \in R^1$ s.t.

$$\mathcal{H}_{R/(h_1,\ldots,h_{n-k})}(T) = \left[\frac{(1+bT)^w}{(1+T)^{n-k}} \right]_+ .$$

Note that Lemma 20 shows

$$\frac{(1+bT)^w}{(1+T)^{n-k}} = 1 + k \cdot T + \left(\binom{k}{2} - w \cdot \binom{b}{2} \right) \cdot T^2 + O(T^3).$$

By shifting to a primal modeling again, one arrives at Hypothesis 4. Indeed, Hypothesis 9 implies Hypothesis 4 whenever

$$w \cdot \binom{b}{2} \geq \binom{k}{2}.$$

On the other hand, this inequality is necessary, as the following lemma shows:

Lemma 35. *Let $\mathbb{F}$ be of characteristic two and $b, k, w \in \mathbb{N}$. Then, Hypothesis 4 can only be true if*

$$w \cdot \binom{b}{2} \geq \binom{k}{2}.$$

Proof. Let $(f_i^{(\alpha)})_{i \in [b], \alpha \in [w]}$ s.t.

$$\mathbb{F}[X]^2 = \mathrm{span}_{\mathbb{F}}\{f_i^{(\alpha)} \cdot f_j^{(\alpha)} | \alpha \in [w], i, j \in [b]\}.$$

Note that the squares $(f_i^{(\alpha)})^2$ are all contained in the k-dimensional space

$$\mathrm{span}_{\mathbb{F}}\{X_1^2, \ldots, X_k^2\}.$$

Hence, the $w \cdot b$ squares of the list $(f_i^{(\alpha)} f_j^{(\alpha)})_{i,j \in [b], \alpha \in [w]}$ can contribute at most k many independent polynomials. The maximum achievable dimension of $\mathrm{span}_{\mathbb{F}}\{f_i^{(\alpha)} \cdot f_j^{(\alpha)} | \alpha \in [w], i, j \in [b]\}$ is hence bounded from above by $w \cdot \binom{b+1}{2} - bw + k = w \cdot \binom{b}{2} + k$. □

In Section 4, we refuted Hypothesis 4 for $w = 2$ and $w = 3$. Ergo, Hypothesis 9 (Assumption 2 in [BØ23]) is wrong for those cases. We suspect however that Hypothesis 4 is true when $w \geq 4$.

F.3 On Hybrid Binary Attacks

Finally, we consider the hybrid binary setting.

Set $n = (f - w) \cdot b + f \cdot (b - u)$ and consider again the variables

$$E_1^{(i)}, \ldots, E_b^{(i)} \qquad \text{for } i \in [w - f],$$
$$F_1^{(i)}, \ldots, F_{b-u}^{(i)} \qquad \text{for } i \in [f].$$

Set

$$R := \mathbb{F}[E, F]/((E_\alpha^{(i)} E_\beta^{(i)} \mid i \in [w - f], \alpha, \beta \in [b]) + (F_\alpha^{(i)} F_\beta^{(i)} \mid i \in [f], \alpha, \beta \in [b - u])).$$

The Hilbert series of this ring is given by

$$\mathcal{H}_R(T) = (1 + bT)^{w-f} \cdot (1 + (b - u)T)^f.$$

The assumption underlying the hybrid binary attack of [BØ23] is now given by:

Hypothesis 10. There exist linear forms $h_1, \dots, h_{n-k} \in R^1$ s.t.

$$\mathcal{H}_{R/(h_1,\dots,h_{n-k})}(T) = \left[\frac{(1+bT)^{w-f} \cdot (1+(b-u)T)^f}{(1+T)^{n-k}}\right]_+ .$$

In Lemma 22, we show

$$\frac{(1+bT)^{w-f} \cdot (1+(b-u)T)^f}{(1+T)^{n-k}}$$
$$= 1 + (k-fu)T + \left(\binom{k-fu}{2} - (w-f)\binom{b}{2} - f\binom{b-u}{2}\right)T^2 + O(T^3).$$

Hence, Hypothesis 10 implies a degree of regularity 2 whenever

$$(w-f)\binom{b}{2} + f\binom{b-u}{2} \geq \binom{k-fu}{2}.$$

Again, set

$$w_1 = w-f, \qquad b_1 = b, \qquad w_2 = f, \qquad b_2 = b-u, \qquad k' = k-fu.$$

By going to a primal model, Hypothesis 10 implies the following hypothesis whenever $w_1\binom{b_1}{2} + w_2\binom{b_2}{2} \geq \binom{k'}{2}$:

Hypothesis 11. For parameters $b_1, b_2, k', w_1, w_2 \in \mathbb{N}$, there exist $f_\alpha^{(i)}, g_\beta^{(j)} \in \mathbb{F}[X_1, \dots, X_{k'}]^1$, $i \in [w_1], \alpha \in [b_1], j \in [w_2], \beta \in [b_2]$, s.t.

$$\mathrm{span}_{\mathbb{F}}\left\{f_\alpha^{(i)} \cdot f_\beta^{(i)} \;\middle|\; i \in [w_1], \alpha, \beta \in [b_1]\right\} + \mathrm{span}_{\mathbb{F}}\left\{g_\alpha^{(i)} \cdot g_\beta^{(i)} \;\middle|\; i \in [w_2], \alpha, \beta \in [b_2]\right\} = \mathbb{F}[X]^2.$$

Again, from all we have seen, we think Hypothesis 11 is true as long as $b_1, b_2 \leq k'/2$ and $(w-f)\binom{b}{2} + f\binom{b-u}{2} \geq \binom{k-fu}{2}$.

G Details on the LWBE Solving Algorithm

Lemma 36. *Set $n = \binom{k+d}{d}$. Let $\mathbb{F}$ be a finite field of characteristic $> d$ and size $\geq dn+2$. Let $f_1', \dots, f_n' \in \mathbb{F}[Z_1, H_1]^d$ be given by*

$$f_i'(Z_1, H_1) = Z_1^d + \sum_{j=1}^{d} c_{i,j} \cdot Z_1^{d-j} \cdot H_1^j$$

for arbitrary coefficients $c_{i,1}, \dots, c_{i,d} \in \mathbb{F}$. If we draw $g_1', \dots, g_n' \leftarrow \mathbb{F}[X_1, \dots, X_k, H_1]^1$ uniformly at random, we have

$$\mathrm{span}_{\mathbb{F}}\{f_1'(g_1'(X_1, \dots, X_k, H_1), H_1), \dots, f_n'(g_n'(X_1, \dots, X_k, H_1), H_1)\} = \mathbb{F}[X_1, \dots, X_k]^d$$

with probability

$$\geq 1 - \frac{dn}{|\mathbb{F}|}.$$

Proof. We need to prove that $g'_1, \ldots, g'_n$ with

$$\mathrm{span}_{\mathbb{F}}\{f'_1(g'_1(X_1, \ldots, X_k, H_1), H_1), \ldots, f'_n(g'_n(X_1, \ldots, X_k, H_1), H_1)\} = \mathbb{F}[X_1, \ldots, X_k, H_1]^d$$

exist. Note that $f'_i(g'_i(X, H_1), 0) = g'_i(X, H_1)^d$. Because of Theorem 5, it follows that there exist $g_1, \ldots, g_n$ with

$$\mathrm{span}_{\mathbb{F}}\{f'_1(g_1(X_1, \ldots, X_k, H_1), 0), \ldots, f'_n(g_n(X_1, \ldots, X_k, H_1), 0)\} = \mathbb{F}[X_1, \ldots, X_k, H_1]^d.$$

Because of Lemma 5, if we draw $\alpha \leftarrow \mathbb{F}$ we have

$$\mathrm{span}_{\mathbb{F}}\{f'_1(g_1(X_1, \ldots, X_k, H_1), \alpha \cdot H_1), \ldots, f'_n(g_n(X_1, \ldots, X_k, H_1), \alpha \cdot H_1)\} = \mathbb{F}[X_1, \ldots, X_k, H_1]^d$$

with probability at least $\geq 1 - \frac{dn}{|\mathbb{F}|}$. Since $|\mathbb{F}| \geq dn + 2$, there is one $\alpha \neq 0$ such that the above equality does hold. Set $g'_1 \coloneqq g_1/\alpha$ and note that

$$\alpha^d \cdot f'_1(g'_1, H_1) = f'_1(g_1, \alpha \cdot H_1).$$

It follows now

$$\begin{aligned}
&\mathrm{span}_{\mathbb{F}}\{f'_1(g'_1(X_1, \ldots, X_k, H_1), H_1), \ldots, f'_n(g'_n(X_1, \ldots, X_k, H_1), \cdot H_1)\} \\
&\mathrm{span}_{\mathbb{F}}\left\{\frac{f'_1(g_1(X_1, \ldots, X_k, H_1), \alpha H_1)}{\alpha^d}, \ldots, \frac{f'_n(g_n(X_1, \ldots, X_k, H_1), \alpha H_1)}{\alpha^d}\right\} \\
&= \frac{1}{\alpha^d} \cdot \mathbb{F}[X_1, \ldots, X_k, H_1]^d = \mathbb{F}[X_1, \ldots, X_k, H_1]^d.
\end{aligned}$$

For the probability bound, note that the entries of the matrix with the coefficients of $f'_1(g'_1(X_1, \ldots, X_k, H_1), H_1)$, $\ldots$, $f'_n(g'_n(X_1, \ldots, X_k, H_1), H_1)$ have degree $\leq d$ in the coefficients of $g'_1, \ldots, g'_n$. Hence, the claim follows by Lemma 5 again. □

G.1 Search-To-Decision Reduction

We detail here the reduction of an LWBE instance in the proof of Theorem 5.

Let $\mathbf{G} \leftarrow \mathbb{F}^{n \times k}$ be a uniformly random generator matrix. Further, let $\mathbf{e} \in S_1 \times \ldots \times S_n$ for subsets $S_1, \ldots, S_n \subset \mathbb{F}$ of size d and let $\mathbf{x} \in \mathbb{F}^k$. Set

$$\mathbf{y} \coloneqq \mathbf{G}\mathbf{x} + \mathbf{e}.$$

Now, given $\mathbf{G}$ and $\mathbf{y}$, let us guess that the i-th entry e_i of $\mathbf{e}$ equals some value $z \in S_i$. The guess $e_i \overset{!}{=} z$ gives us the (potentially incorrect) knowledge

$$y_i \overset{!}{=} \mathbf{g}_i^{\mathsf{T}} \cdot \mathbf{x} + z.$$

With overwhelming probability, one of the entries of $\mathbf{g}_i$ is non-zero[14]. Without loss of generality, we can assume[15] that the first entry of $\mathbf{g}_i$ equals 1. Hence, our guess implies

$$x_1 = y_i - e_i - \sum_{j=2}^{k} g_{i,j} x_j \overset{!}{=} y_i - z - \sum_{j=2}^{k} g_{i,j} x_j.$$

[14] If $\mathbf{g}_i = \mathbf{0}$, then we have $y_i = e_i$ and can directly read off a correct value for e_i.

[15] Otherwise, we scale $\mathbf{g}_i$ and permute the columns of $\mathbf{G}$

Denote the columns of $\mathbf{G}$ by $\mathbf{c}_1, \ldots, \mathbf{c}_k \in \mathbb{F}^k$, i.e.

$$\mathbf{G} = \left(\mathbf{c}_1 | \cdots | \mathbf{c}_k\right).$$

Our guess $e_i \overset{!}{=} z$ implies now

$$\begin{aligned}
\mathbf{y} &= \mathbf{c}_1 x_1 + \sum_{j=2}^{k} \mathbf{c}_j x_j + \mathbf{e} \\
&\overset{!}{=} \mathbf{c}_1 (y_i - z - \sum_{j=2}^{k} g_{i,j} x_j) + \sum_{j=2}^{k} \mathbf{c}_j x_j + \mathbf{e} \\
&= \mathbf{c}_1 (y_i - z) + \sum_{j=2}^{k} (\mathbf{c}_j - g_{i,j} \mathbf{c}_1) x_j + \mathbf{e}.
\end{aligned}$$

Rearranging yields the smaller problem with unknowns $x_2, \ldots, x_k$ and $e_1, \ldots, e_{i-1}$, $e_{i+1}, \ldots, e_n$

$$(\mathbf{c}_2 - g_{i,2}\mathbf{c}_1)x_2 + \ldots + (\mathbf{c}_k - g_{i,k}\mathbf{c}_1)x_k + \mathbf{e} \overset{!}{=} \mathbf{y} - \mathbf{c}_1(y_i - z).$$

The i-th entry of $\mathbf{y} - \mathbf{c}_1(y_i - z)$ will always be z, since the i-th entry of $\mathbf{c}_1$ is one (as it is the first entry of $\mathbf{g}_i$). Further, the i-th entry of each $\mathbf{c}_j - g_{i,2}\mathbf{c}_1$ must be zero. Besides that, all other entries of $\mathbf{c}_2 - g_{i,2}\mathbf{c}_1, \ldots, \mathbf{c}_k - g_{i,k}\mathbf{c}_1$ are uniformly random, since $\mathbf{c}_2, \ldots, \mathbf{c}_k$ are distributed uniformly and independently at random (and all of their entries except the i-ths are independent of $\mathbf{g}_i$). Denote by $\mathbf{c}'_1, \ldots, \mathbf{c}'_k \in \mathbb{F}^{n-1}$ the vectors $\mathbf{c}_1, \ldots, \mathbf{c}_k \in \mathbb{F}^n$ without their i-th entry. Now, we let $\mathbf{G}' \in \mathbb{F}^{(n-1)\times(k-1)}$ be the matrix

$$\mathbf{G}' = \left(\mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1 | \cdots | \mathbf{c}'_k - g_{i,k}\mathbf{c}'_1\right).$$

Further, let $\mathbf{y}' \in \mathbb{F}^{n-1}$ be the vector that contains all entries of $\mathbf{y} - \mathbf{c}_1(y_i - z)$ except the i-th. The reduced LWBE problem is given by

$$\mathbf{G}' \cdot \begin{pmatrix} x_2 \\ \vdots \\ x_k \end{pmatrix} + \mathbf{e}' \overset{!}{=} \mathbf{y}' \tag{1}$$

where $\mathbf{e}' = (e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n)$.

We distinguish three cases:

Case 1: *We guessed correctly $z = e_i$.*
In this case, $(\mathbf{G}', \mathbf{y}')$ is a correct LWBE instance. Any solution $\mathbf{e}' \in S_1 \times \cdots \times S_{i-1} \times S_{i+1} \times \cdots \times S_n$ can be lifted to a solution $\mathbf{e} \in \mathbb{F}^n$ by setting

$$\mathbf{e} := (e'_1, \ldots, e'_{i-1}, z, e'_i, \ldots, e'_{n-1}).$$

Case 2: *We guessed incorrectly $z \neq e_i$ and $z \neq y_i$.*
We claim that in this case $(\mathbf{G}', \mathbf{y}')$ is distributed uniformly at random in $\mathbb{F}^{(n-1)\times k}$. Indeed, the uniform randomness of $\mathbf{G}'$ follows from the uniform randomness of $\mathbf{c}'_2, \ldots, \mathbf{c}'_k$. In particular, $\mathbf{G}'$ is independent of $\mathbf{c}_1$.

The uniform randomness of

$$\mathbf{y}' = \begin{pmatrix} y_1 - g_{1,1}(y_i - z) \\ \vdots \\ y_{i-1} - g_{i-1,1}(y_i - z) \\ y_{i+1} - g_{i+1,1}(y_i - z) \\ \vdots \\ y_n - g_{n,1}(y_i - z) \end{pmatrix}$$

follows from the fact that the random values $g_{1,1}, \dots, g_{i-1,1}, g_{i+1,1}, \dots, g_{n,1}$ are independent of $\mathbf{c}_2, \dots, \mathbf{c}_k, \mathbf{g}_i$ and that $y_i - z \neq 0$.

Case 3: *We guessed incorrectly $z \neq e_i$, $z = y_i$.*

If $z = y_i$, $\mathbf{y}'$ equals $\mathbf{y}$, except its i-th entry. Note that we can rewrite $\mathbf{y}$ as

$$\begin{aligned} \mathbf{y} &= \mathbf{c}_1 x_1 + \ldots + \mathbf{c}_k x_k + \mathbf{e} \\ &= \mathbf{c}_1 \cdot (y_i - e_i - \sum_{j=2}^{k} g_{i,j} x_j) + \mathbf{c}_2 x_2 + \ldots + \mathbf{c}_k x_k + \mathbf{e} \\ &= \mathbf{c}_1 \cdot (y_i - e_i) + (\mathbf{c}_2 - g_{i,2}\mathbf{c}_1) \cdot x_2 + \ldots + (\mathbf{c}_k - g_{i,k}\mathbf{c}_1) \cdot x_k + \mathbf{e}. \end{aligned}$$

Also note that $y_i - e_i$ is not zero, since $y_i = z \neq e_i$. Note that the columns of $\mathbf{G}'$, which are $\mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1, \ldots, \mathbf{c}'_k - g_{i,k}\mathbf{c}'_1$, are distributed uniformly and independently at random. In particular, they are statistically independent of $\mathbf{c}_1$. Since $y_i - e_i \neq 0$, the vector $\mathbf{c}'_1 \cdot (y_i - e_i) + (\mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1) \cdot x_2 + \ldots + (\mathbf{c}'_k - g_{i,k}\mathbf{c}'_1) \cdot x_k$ is independent of $\mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1, \ldots, \mathbf{c}'_k - g_{i,k}\mathbf{c}'_1$. To make this argument precise, note that we have

$$\begin{aligned} &\big(\mathbf{c}'_1 \cdot (y_i - e_i) + (\mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1) \cdot x_2 + \ldots + (\mathbf{c}'_k - g_{i,k}\mathbf{c}'_1) \cdot x_k | \mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1 | \cdots | \mathbf{c}'_k - g_{i,k}\mathbf{c}'_1\big) \\ &= \big(\mathbf{c}'_1 | \mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1 | \cdots | \mathbf{c}'_k - g_{i,k}\mathbf{c}'_1\big) \cdot \begin{pmatrix} y_i - e_i & & & & & \\ x_2 & 1 & & & & \\ x_3 & & 1 & & & \\ \vdots & & & \ddots & & \\ x_{k-1} & & & & 1 & \\ x_k & & & & & 1 \end{pmatrix} \\ &= \big(\mathbf{c}'_1 | \mathbf{c}'_2 | \cdots | \mathbf{c}'_k\big) \cdot \begin{pmatrix} 1 & -g_{i,2} & & & & \\ & 1 & -g_{i,3} & & & \\ & & 1 & -g_{i,4} & & \\ & & & \ddots & & \\ & & & & 1 & -g_{i,k} \\ & & & & & 1 \end{pmatrix} \cdot \begin{pmatrix} y_i - e_i & & & & & \\ x_2 & 1 & & & & \\ x_3 & & 1 & & & \\ \vdots & & & \ddots & & \\ x_{k-1} & & & & 1 & \\ x_k & & & & & 1 \end{pmatrix} \end{aligned}$$

The uniform randomness of the left-hand side now follows by the uniform randomness of $(\mathbf{c}'_1 | \mathbf{c}'_2 | \cdots | \mathbf{c}'_k)$ and the fact that both matrices multiplied to it in the right-hand side are invertible.

Since the columns

$$\mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1, \quad \ldots, \quad \mathbf{c}'_k - g_{i,k}\mathbf{c}'_1, \quad \mathbf{c}'_1 \cdot (y_i - e_i) + (\mathbf{c}'_2 - g_{i,2}\mathbf{c}'_1) \cdot x_1 + \ldots + (\mathbf{c}'_k - g_{i,k}\mathbf{c}'_1) \cdot x_k$$

are distributed uniformly at random, it follows that $(\mathbf{G}', \mathbf{y}')$ is distributed uniformly at random in $\mathbb{F}^{(n-1)\times k}$ as $\mathbf{y}'$ equals the last column plus $\mathbf{e}'$.