

# Quadratic Modelings of Syndrome Decoding

Alessio Caminata<sup>1</sup>, Ryann Cartor<sup>2</sup>, Alessio Meneghetti<sup>3</sup>, Rocco Mora<sup>4</sup>, and Alex Pellegrini<sup>5</sup>

<sup>1</sup> Università di Genova

<sup>2</sup> Clemson University

<sup>3</sup> Università di Trento

<sup>4</sup> CISA Helmholtz Center for Information Security

<sup>5</sup> Eindhoven University of Technology

**Abstract.** This paper presents enhanced reductions of the bounded-weight and exact-weight Syndrome Decoding Problem (SDP) to a system of quadratic equations. Over  $\mathbb{F}_2$ , we improve on a previous work and study the degree of regularity of the modeling of the exact weight SDP. Additionally, we introduce a novel technique that transforms SDP instances over  $\mathbb{F}_q$  into systems of polynomial equations and thoroughly investigate the dimension of their varieties. Experimental results are provided to evaluate the complexity of solving SDP instances using our models through Gröbner bases techniques.

**Keywords:** Syndrome Decoding · Gröbner Basis · Cryptanalysis · Code-Based Cryptography · Multivariate Cryptography

## 1 Introduction

As widespread quantum computing becomes closer to reality, accurate cryptanalysis of post-quantum cryptosystems is of the utmost importance. Code-based cryptography is one of the main areas of focus in the search for quantum-secure cryptosystems. This is well represented by the NIST Post-Quantum Standardization Process, where as many as three finalists, namely Classic McEliece [9] (an IND-CCA2 secure variation of McEliece’s very first code-based scheme [31]), HQC [32] and BIKE [2], belong to this family. Similarly, NIST’s additional call for digital signatures has numerous proposals that make use of linear codes. Many of the proposed schemes are based on the hardness of (sometimes structured variants of) the syndrome decoding problem.

The parameters of many code-based schemes are carefully chosen to align with the latest advancements with respect to this computational problem. Despite decades of intensive research in this direction, all the algorithms developed so far exhibit exponential complexity. This is not surprising, since the problem has been shown to be NP-hard [8]. In particular, after more than 60 years of investigation since the groundbreaking paper of Prange [34], the reduction in the exponent for most parameters of interest has been minimal [7, 10, 12, 23, 27, 29, 30, 37]. All the works mentioned fall into the family of Information Set Decoding (ISD) algorithms, whose basic observation is that it is easier

to guess error-free positions, and guessing enough of them is sufficient to decode. This resilience against ISD algorithms adds to the robustness of the syndrome decoding problem as the underlying assumption for code-based cryptosystems.

To comprehensively assess security, it is imperative to consider attacks stemming from various other realms of post-quantum cryptography. For instance, attacks typically associated with multivariate or lattice-based schemes should also be taken into account for code-based schemes, when applicable. A remarkable example is offered by dual attacks, originally introduced in lattice-based cryptography, but strongly questioned in that context. In contrast, their code-based counterpart [17, 18] has recently outperformed ISD techniques for a non-negligible regime of parameters, by reducing the decoding problem to the closely related Learning Parity with Noise problem. Concerning polynomial system solving strategies, another notable illustration of this is the algebraic MinRank attack, which broke the rank-metric code-based schemes RQC and Rollo [4, 5] and now represents the state-of-the-art for MinRank cryptanalysis, beating combinatorial approaches.

In the Hamming metric, a reduction that transforms an instance of the syndrome decoding problem into a system of quadratic equations over  $\mathbb{F}_q$  was introduced in [33]. The goal of [33] was to provide explicit reductions between the Syndrome Decoding Problem (SDP) and the Multivariate Quadratic (MQ) problem, thus proving an isomorphism between these two NP-complete problems. Focusing on the reduction from MLD to MQ, the most expensive step of the transformation, in terms of numbers of new variables and new equations introduced, is the so-called *Hamming-weight computation encoding*. Indeed, for a binary linear code of length  $n$ , the procedure dominates the overall complexity of the reduction with a complexity of  $\mathcal{O}(n \log_2(n)^2)$ .

Despite the considerable theoretical interest in this transformation, the latter is too inefficient to be of practical interest in solving the syndrome decoding problem. Thus, the problem of improving the reduction in order to obtain a more effectively solvable system remains open. Moreover, [33] covers only the binary case, leaving unanswered the challenge of modeling through algebraic equations the decoding problem for codes defined over finite fields with more than two elements.

*Our contribution.* In this work, we improve on the reduction presented in [33] by a factor of  $\log_2(n)$ , thereby reducing the number of introduced variables and equations and achieving an overall reduction cost of  $\mathcal{O}(n \log_2(n))$ . This improvement is achieved by leveraging the recursive structure of the equations generated by the Hamming-weight computation encoding and by transforming the equations similarly to the reduction procedure in Buchberger’s algorithm [14] for Gröbner basis computation. When considering a version of the syndrome decoding problem that requires an error vector with a specified Hamming weight, we derive a further improved modeling, for which we study the degree of regularity.

As a second contribution, we present a novel approach that transforms an instance of the syndrome decoding problem over  $\mathbb{F}_q$  for  $q \geq 2$  into a system of polynomial equations. This significantly broadens the applicability of our meth-

ods to a wider range of code-based cryptosystems. A common feature of our algebraic modelings is that if the decoding problem admits multiple solutions, the Gröbner basis naturally determines all of them.

We also provide theoretical and experimental data to analyze the complexity of solving syndrome decoding instances using our modelings, demonstrating that, at least for small parameters, our new strategy is practical and successful. Software (MAGMA scripts) supporting the work in this chapter can be found [here](#).

*Structure of the paper.* The next section recalls the background and notions necessary for this work. In Section 3, we review the reduction described in [33] from the syndrome decoding problem to that of finding the zeroes of a set of polynomials. In Section 4, we describe two modelings that improve upon [33]. We study the degree of regularity of the modeling for the exact weight syndrome decoding problem, along with experimental results, in Section 5. Finally, in Section 6, we present a novel modeling of the syndrome decoding problem over  $\mathbb{F}_q$  with  $q \geq 2$ , for which we provide a theoretical study of the variety and experimental analysis of the solving complexity with Gröbner bases techniques.

## 2 Preliminaries

This paper investigates the reduction of the Syndrome Decoding Problem into a Polynomial System Solving Problem (PoSSo). In this section, we briefly recall the definitions of both problems, as well as the notions of solving degree and degree of regularity, which are commonly used to estimate the computational complexity of the PoSSo problem.

### 2.1 The Syndrome Decoding Problem

An  $[n, k]$ -linear code  $\mathcal{C}$  is a  $k$ -dimensional subspace of  $\mathbb{F}_q^n$ . We call  $n$  the length of the code, and  $k$  its dimension. An element  $\mathbf{x} \in \mathbb{F}_q^n$  is called a codeword if  $\mathbf{x} \in \mathcal{C}$ . The number of nonzero elements in  $\mathbf{x}$  is called the Hamming weight of  $\mathbf{x}$  and we denote it as  $\text{wt}(\mathbf{x})$ . Given a code  $\mathcal{C}$  we define a parity check matrix of  $\mathcal{C}$  as  $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$  such that the right kernel of  $\mathbf{H}$  is the code  $\mathcal{C}$ . The subspace spanned by the rows of  $\mathbf{H}$  is called the dual code of  $\mathcal{C}$ . Many code-based cryptosystems rely on the hardness of solving the Syndrome Decoding Problem (SDP), see Problems 1 and 2 described below.

*Problem 1 (SDP: Syndrome Decoding Problem).* Given integers  $n, k, t$  such that  $k \leq n$  and  $t \leq n$ , an instance of the problem  $\text{SD}(\mathbf{H}, \mathbf{s}, t)$  consists of a parity check matrix  $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$  and a vector  $\mathbf{s} \in \mathbb{F}_q^{n-k}$  (called the syndrome). A solution to the problem is a vector  $\mathbf{e} \in \mathbb{F}_q^n$  such that  $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$  and  $\text{wt}(\mathbf{e}) \leq t$ .

In later sections, we will also refer to Problem 1 as the ‘‘Bounded Syndrome Decoding’’ Problem. In this paper, we will also consider the following variant of SDP.

*Problem 2 (ESDP: Exact Weight Syndrome Decoding Problem).* Given integers  $n, k, t$  such that  $k \leq n$  and  $t \leq n$ , an instance of the problem  $\text{ESD}(\mathbf{H}, \mathbf{s}, t)$  consists of a parity check matrix  $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$  and a vector  $\mathbf{s} \in \mathbb{F}_q^{n-k}$  (called the syndrome). A solution to the problem is a vector  $\mathbf{e} \in \mathbb{F}_q^n$  such that  $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$  and  $\text{wt}(\mathbf{e}) = t$ .

Additionally, a close variant of the Syndrome Decoding Problem is the *Code-word Finding Problem*, where the syndrome  $\mathbf{s}$  is the zero vector  $\mathbf{0}$ . Since the null vector is always a solution of the parity-check equations  $\mathbf{H}\mathbf{e}^\top = \mathbf{0}^\top$ , a nonzero  $\mathbf{e}$  of weight at most (or exactly)  $t$  is sought. The name of the problem refers to the fact that any element in the right kernel of  $\mathbf{H}$  belongs to the code  $\mathcal{C}$  having  $\mathbf{H}$  as parity-check matrix. We will later need to distinguish this variant in the analysis of one of our modelings.

In addition to length and dimension, a fundamental notion in coding theory and consequently in code-based cryptography is the minimum distance  $d$  of an  $\mathbb{F}_q$ -linear code, i.e. the Hamming weight of the smallest nonzero codeword in the code. Such a quantity is strictly related to the number of solutions to the syndrome decoding problem.

Knowing the expected number of solutions from given parameters is extremely important in cryptography, in order to assess the security correctly. It is guaranteed that the problem does not admit more than one solution as long as the number of errors is upper bounded by  $\frac{d-1}{2}$ . However, in practice, much better can be done for randomly generated codes. Indeed, it turns out that random codes achieve the so-called Gilbert-Varshamov (GV) distance  $d_{GV}$ , defined as the largest integer such that

$$\sum_{i=0}^{d_{GV}-1} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

It can be shown that, as long as the number of errors is below half the Gilbert-Varshamov distance, the Syndrome Decoding problem *typically* has a unique solution. Moreover, the instances where the number of errors attains the GV distance are those supposed to be the most difficult.

## 2.2 The Polynomial System Solving Problem

The Polynomial System Solving Problem (PoSSo) is the following. We define it over a finite field  $\mathbb{F}_q$ , although it can be more generally considered over any field.

*Problem 3 (PoSSo: Polynomial System Solving).* Given integers  $n, r \geq 2$ , an instance of the PoSSo problem consists of a system of polynomials  $\mathcal{F} = \{f_1, \dots, f_r\}$  in  $R = \mathbb{F}_q[x_1, \dots, x_n]$  with  $n$  variables and coefficients in  $\mathbb{F}_q$ . A solution to the problem is a vector  $\mathbf{a} \in \mathbb{F}_q^n$  such that  $f_1(\mathbf{a}) = \dots = f_r(\mathbf{a}) = 0$ .

*Remark 1.* A special case of PoSSo when  $\deg(f_i) = 2$  for  $1 \leq i \leq r$  is called MQ (Multivariate Quadratic) and is the basis for multivariate cryptography.

The following outlines a standard strategy for finding the solutions of a polynomial system  $\mathcal{F}$  by means of Gröbner bases.

1. Find a degree reverse lexicographic (**degrevlex**) Gröbner basis of the ideal  $\langle \mathcal{F} \rangle$ ;
2. Convert the obtained **degrevlex** Gröbner basis into a lexicographic (**lex**) Gröbner basis, where the solutions of the system can be easily read from the ideal in this form.

The second step can be done by FGLM [24], or a similar algorithm, whose complexity depends on the degree of the ideal. This is usually faster than the first step, especially when the system  $\mathcal{F}$  has few solutions. Therefore, we focus on the first step.

The fastest known algorithms to compute a **degrevlex** Gröbner basis are the linear algebra based algorithms such as F4 [25], F5 [26], or XL [20]. These transform the problem of computing a Gröbner basis into one or more instances of Gaussian elimination of the Macaulay matrices. The complexity of these algorithms is dominated by the Gaussian elimination on the largest Macaulay matrix encountered during the process. The size of a Macaulay matrix depends on the degrees of the input polynomials  $f_1, \dots, f_r$ , on the number of variables  $n$ , and on a degree  $d$ . In a nutshell, the *Macaulay matrix*  $M_{\leq d}$  of degree  $d$  of  $\mathcal{F}$  has columns indexed by the monic monomials of degree  $\leq d$ , sorted in decreasing order from left to right (with respect to the chosen **degrevlex** term order). The rows of  $M_{\leq d}$  are indexed by the polynomials  $m_{i,j}f_j$ , where  $m_{i,j}$  is a monic monomial such that  $\deg(m_{i,j}f_j) \leq d$ . The entry  $(i, j)$  of  $M_{\leq d}$  is the coefficient of the monomial of column  $j$  in the polynomial corresponding to the  $i$ -th row.

The *solving degree* of  $\mathcal{F}$  is defined as the least degree  $d$  such that Gaussian elimination on the Macaulay matrix  $M_{\leq d}$  produces a **degrevlex** Gröbner basis of  $\mathcal{F}$ . We denote the solving degree of  $\mathcal{F}$  by  $d_{\text{sol}}(\mathcal{F})$ . We have to compute Macaulay matrices up to degree  $d_{\text{sol}} = d_{\text{sol}}(\mathcal{F})$ , and the largest one we encounter has  $a = \sum_{i=1}^r \binom{n+d_{\text{sol}}-d_i}{d_{\text{sol}}-d_i}$  many rows and  $b = \binom{n+d_{\text{sol}}}{d_{\text{sol}}}$  many columns, where  $d_i = \deg f_i$ . Therefore, taking into account the complexity of Gaussian elimination of this matrix, an upper bound on the complexity of solving the system  $\mathcal{F}$  with this method is

$$\mathcal{O} \left( \binom{n+d_{\text{sol}}}{d_{\text{sol}}}^\omega \right), \quad (1)$$

with  $2 \leq \omega \leq 3$ .

Since the solving degree of a polynomial system may be difficult to estimate, several invariants related to the solving degree (that are hopefully easier to compute) have been introduced. One of the most important is the *degree of regularity* introduced by Bardet, Faugère, and Salvy [6]. We briefly recall its definition and connection with the solving degree.

Let  $\langle \mathcal{F}^{\text{top}} \rangle = \langle f_1^{\text{top}}, \dots, f_r^{\text{top}} \rangle$  be the ideal of the polynomial ring  $R$  generated by the homogeneous part of highest degree of the polynomial system  $\mathcal{F}$ . Assume that  $\langle \mathcal{F}^{\text{top}} \rangle_d = R_d$  for  $d \gg 0$ . The *degree of regularity* of  $\mathcal{F}$  is

$$d_{\text{reg}}(\mathcal{F}) = \min\{d \in \mathbb{N} \mid \langle \mathcal{F}^{\text{top}} \rangle_e = R_e \ \forall e \geq d\}.$$

The degree of regularity can be read off from the Hilbert series of  $\langle \mathcal{F}^{\text{top}} \rangle$ . Let  $I$  be a homogeneous ideal of  $R$ , and let  $A = R/I$ . For an integer  $d \geq 0$ , we denote by  $A_d$  the homogeneous component of degree  $d$  of  $A$ . The function  $\text{HF}_A(-) : \mathbb{N} \rightarrow \mathbb{N}$ ,  $\text{HF}_A(d) = \dim_{\mathbb{F}_q} A_d$  is called *Hilbert function* of  $A$ . The generating series of  $\text{HF}_A$  is called *Hilbert series* of  $A$ . We denote it by  $\text{HS}_A(z) = \sum_{d \in \mathbb{N}} \text{HF}_A(d)z^d$ .

*Remark 2.* Under the assumption that  $\langle \mathcal{F}^{\text{top}} \rangle_d = R_d$  for  $d \gg 0$ , the Hilbert series of  $A = R/\langle \mathcal{F}^{\text{top}} \rangle$  is a polynomial. Then, the degree of regularity of  $\mathcal{F}$  is given by  $d_{\text{reg}}(\mathcal{F}) = \deg \text{HS}_A(z) + 1$  (see [15, Theorem 12]).

Under suitable assumptions, the degree of regularity provides an upper bound for the solving degree [16, 35, 36]. Moreover, it is often assumed that the two values of the degree of regularity and the solving degree are close. Although this occurs in many relevant situations, there are examples where these two invariants can be arbitrarily far apart (see [11, 15, 22]). We will see in Section 5 that the degree of regularity of the system presented in Section 4.2 seems to yield a much higher value than the solving degree achieved during the Gröbner basis algorithm.

### 3 The MPS Modeling

This section is devoted to an overview of the algebraic modeling of the syndrome decoding problem proposed in [33] (referred to as the MPS modeling). We fix the following notation for this section.

**Notation 1** Let  $n \geq 2$  and let  $\mathcal{C} \subseteq \mathbb{F}_2^n$  be a  $[n, k, d]$ -linear code having a parity check matrix  $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ . We define  $\ell = \lfloor \log_2(n) \rfloor + 1$ . Let  $\mathbf{s} \in \mathbb{F}_2^{n-k}$  play the role of the syndrome and let  $0 \leq t \leq \lfloor (d-1)/2 \rfloor$  be the target error weight. Let  $X = (x_1, \dots, x_n)$  and  $Y = (Y_1, \dots, Y_n)$  with  $Y_j = (y_{j,1}, \dots, y_{j,\ell})$  be two sets of variables and we consider the polynomial ring  $\mathbb{F}_2[X, Y]$ .

We define the following maps  $\pi_i$  for  $i = 1, \dots, n$ ,

$$\begin{aligned} \pi_i : \mathbb{F}_2^n &\rightarrow \mathbb{F}_2^i \\ (v_1, \dots, v_n) &\mapsto (v_1, \dots, v_i). \end{aligned}$$

The construction of the proposed algebraic modeling consists of four steps and uses the variables contained in  $X$  and  $Y$  to express relations and dependencies. Each of these steps produces a set of polynomials in  $\mathbb{F}_2[X, Y]$ . An extra step of the construction reduces the aforementioned polynomials to quadratic polynomials.

The idea is to construct an algebraic system having a variety containing elements  $(\mathbf{x} \mid \mathbf{y}_1 \mid \dots \mid \mathbf{y}_n) \in \mathbb{F}_2^{n(\ell+1)}$  whose first  $n$  coordinates represent an element  $\mathbf{x}$  of  $\mathbb{F}_2^n$  such that  $\mathbf{H}\mathbf{x}^\top = \mathbf{s}^\top$ . The remaining  $n\ell$  coordinates are considered to be the concatenation of  $n$  elements  $\mathbf{y}_i \in \mathbb{F}_2^\ell$  where the elements of  $\mathbf{y}_i$  represent the binary expansion of  $\text{wt}(\pi_i(\mathbf{x}))$  for every  $i = 1, \dots, n$ , with  $\pi_i(\mathbf{x}) = (x_1, \dots, x_i)$ .

By this definition, the list  $\mathbf{y}_n$  represents the binary expansion of  $\text{wt}(\mathbf{x})$ . The system finally enforces that  $\mathbf{y}_n$  represents the binary expansion of an integer  $t'$  such that  $t' \leq t$ . The elements of the variety corresponding to the ideal generated by this algebraic modeling are finally projected onto their first  $n$  coordinates, revealing the solutions to the original syndrome decoding problem.

Here is a description of the four steps of reduction of the MPS modeling. We describe the set obtained in each step as a set of polynomials in  $\mathbb{F}_2[X, Y]$ .

- *Parity check encoding.* This step ensures that the solution of the algebraic system satisfies the parity check equations imposed by the parity check matrix  $\mathbf{H}$  and the syndrome vector  $\mathbf{s}$ . Here, we compute the set of  $n - k$  linear polynomials

$$\left\{ \sum_{i=1}^n h_{i,j} x_i + s_j \mid j \in \{1, \dots, n - k\} \right\}. \quad (2)$$

- *Hamming weight computation encoding.* This part of the modeling provides a set of polynomials that describe the binary encoding of  $\text{wt}(\pi_i(\mathbf{x}))$  for every  $i = 1, \dots, n$  described above. The set of polynomials achieving this goal, is given by the union of the three following sets consisting of the  $\ell + n - 1$  polynomials in the sets

$$\begin{aligned} & \{f_{1,1} = x_1 + y_{1,1}, f_{1,2} = y_{1,2}, \dots, f_{1,\ell} = y_{1,\ell}\}, \\ & \{f_{i,1} = x_i + y_{i,1} + y_{i-1,1} \mid i = 2, \dots, n\} \end{aligned} \quad (3)$$

and the  $(n - 1)(\ell - 1)$  polynomials

$$\left\{ f_{i,j} = \left( \prod_{h=1}^{j-1} y_{i-1,h} \right) x_i + y_{i,j} + y_{i-1,j} \mid i = 2, \dots, n, j = 2, \dots, \ell \right\}. \quad (4)$$

We labeled the polynomials of the sets in (3) and in (4) because the improvements in the next sections will mainly involve them.

- *Weight constraint encoding.* This part produces a set consisting of a single polynomial that enforces the constraint  $\text{wt}(\mathbf{x}) \leq t$  by dealing with the variables in  $Y_n$ . Let  $\mathbf{v} \in \mathbb{F}_2^\ell$  represent the binary expansion of  $t$ . Consider the  $\ell$  polynomials in  $\mathbb{F}_2[X, Y]$  defined as

$$f_j = (y_{n,j} + v_j) \prod_{h=j+1}^{\ell} y_{n,h} + v_h + 1$$

for  $j = 1, \dots, \ell$ . The output set is the singleton

$$\left\{ \sum_{j=1}^{\ell} (v_j + 1) f_j \right\}. \quad (5)$$

- *Finite field equations.* The set of  $n + n\ell$  finite field polynomials of  $\mathbb{F}_2[X, Y]$  is

$$\{x_i^2 - x_i \mid i = 1, \dots, n\} \cup \{y_{i,j}^2 - y_{i,j} \mid i = 1, \dots, n, j = 1, \dots, \ell\}, \quad (6)$$

and ensures that the elements of the variety are restricted to elements of  $\mathbb{F}_2^{n(\ell+1)}$ .

The algebraic system corresponding to an instance of the syndrome decoding problem is then the union of the four sets described above. Clearly, this is not a quadratic system; thus the authors apply a linearization strategy that introduces a number of auxiliary variables used to label monomials of degree 2. This eventually results in a large quadratic system in many more than just  $n(\ell + 1)$  variables. In fact, the final quadratic system ends up having equations and variables bounded by  $\mathcal{O}(n \log_2(n)^2)$ .

## 4 Improving the MPS modeling

In this section, we provide improvements of the MPS modeling that reduce the number of equations and variables in the final algebraic system. We keep the same notation as in Notation 1. First, we consider the case of the syndrome decoding problem, i.e. with a bounded weight error. We then consider the case of the exact weight syndrome decoding problem. We observe that one can avoid the linearization step as the resulting system is already quadratic.

### 4.1 Improved Modeling for the Case of SDP

We consider the degrevlex monomial ordering on  $\mathbb{F}_2[X, Y]$  and denote by  $\text{lm}(p)$  the leading monomial of a polynomial  $p$ . Notice that since we are in the binary case, the notions of leading monomial and that of leading term coincide.

Denote by  $F = \{f_{i,j} \mid i = 1, \dots, n, j = 1, \dots, \ell\} \subset \mathbb{F}_2[X, Y]$  the set of polynomials of cardinality  $n\ell$  given by (3) and (4) for a code of length  $n$ . We aim at building a set  $G = \{g_{i,j} \mid i = 1, \dots, n, j = 1, \dots, \ell\} \subset \mathbb{F}_2[X, Y]$  consisting of polynomials of degree at most 2 such that  $\langle G \rangle = \langle F \rangle$ . Denote with  $F[i, j]$  the polynomial  $f_{i,j}$ , similarly for  $G$ . We first give a description of the set  $G$  and then formally describe the new modeling.

Construct  $G$  as follows:

- Put  $G[1, 1] = x_1 + y_1$  and  $G[1, h] = y_{1,h}$  for  $h = 2, \dots, \ell$ ;
- Set  $G[i, 1] = F[i, 1] = x_i + y_{i,1} + y_{i-1,1}$  for every  $i = 2, \dots, n$ ;
- Compute

$$\begin{aligned} G[i, j] &= F[i, j] + y_{i-1, j-1} F[i, j-1] \\ &= F[i, j] + \text{lm}(F[i, j]) + y_{i-1, j-1} (y_{i, j-1} + y_{i-1, j-1}) \\ &= y_{i, j} + y_{i-1, j} + y_{i, j-1}^2 + y_{i, j-1} y_{i-1, j-1}. \end{aligned}$$

for every  $i = 2, \dots, n$  and  $j = 2, \dots, \ell$ , where equality holds because  $\text{lm}(F[i, j]) = y_{i-1, j-1} \text{lm}(F[i, j-1])$ .

*Remark 3.* The algebraic system we are going to construct contains the field polynomials  $x_i^2 - x_i$  for each  $i = 1, \dots, n$  and  $y_{i,j}^2 - y_{i,j}$  for every  $i = 1, \dots, n$  and  $j = 1, \dots, \ell$ . Therefore, in terms of generating elements of the ideal, any squared term in  $G[i, j]$  can be reduced to a linear term.



The set  $G \subset \mathbb{F}_2[X, Y]$  contains  $n\ell$  polynomials of degree at most two. The following proposition proves that the set  $G \subset \mathbb{F}_2[X, Y]$  computed as above and  $F$  generate the same ideal of  $\mathbb{F}_2[X, Y]$ .

**Proposition 1.** *We have  $\langle G \rangle = \langle F \rangle$ .*

*Proof.* The inclusion  $\langle G \rangle \subseteq \langle F \rangle$  is trivial. To prove the other inclusion, we show that we can write any element of the basis  $F$  as an  $\mathbb{F}_2[X, Y]$ -linear combination of elements of the basis  $G$ . By construction,  $G[1, j] = F[1, j]$  for every  $j = 1, \dots, \ell$ . For every  $i = 2, \dots, n$  we prove  $F[i, j] \in \langle G \rangle$  by induction on  $j$ .

For  $j = 1$  we have  $F[i, 1] = G[i, 1]$ .

Assume that  $F[i, j] = \sum_{h=1}^j p_{i,j,h} G[i, h]$  with  $p_{i,j,h} \in \mathbb{F}_2[X, Y]$ . Then by construction we have

$$\begin{aligned} F[i, j+1] &= G[i, j+1] - y_{i-1, j-1} F[i, j-1] \\ &= G[i, j+1] - y_{i-1, j-1} \sum_{h=1}^j p_{i,j,h} G[i, h] \end{aligned}$$

proving the claim.  $\square$

We thus redefine the Hamming weight computation encoding as follows:

- *Hamming weight computation encoding.* Compute the following union of subsets of  $\mathbb{F}_2[X, Y]$ :

$$\begin{aligned} &\{x_1 + y_{1,1}, y_{1,2}, \dots, y_{1,\ell}\} \cup \{x_i + y_{i,1} + y_{i-1,1} \mid i = 2, \dots, n\} \\ &\cup \{y_{i,j-1}y_{i-1,j-1} + y_{i,j} + y_{i-1,j-1} + y_{i-1,j} \\ &\quad \mid i = 2, \dots, n, j = 2, \dots, \ell\}, \end{aligned}$$

**Further improvement.** Set now  $\ell_t = \lfloor \log_2(t) \rfloor + 1$ . A further improvement to the MPS modeling (described in Equation 7) follows by observing that in the non-trivial case where  $t < n$ , we can impose that the last  $\ell - \ell_t$  entries of  $\mathbf{y}_i$  must be 0 for every  $i = 1, \dots, n$ . This means that we can add the linear equations  $y_{i,j} = 0$  for every  $i = 0, \dots, n-1$  and  $j = \ell_t + 1, \dots, \ell$ . By inspection, setting the aforementioned variables to 0 will make part of the equations of the Hamming weight computation encoding vanish. We can equivalently simply consider the equations that remain, and get rid of the variables which have been set to 0. Consider the following updated notation.

**Notation 2** *Let  $n \geq 2$  and let  $\mathcal{C} \subseteq \mathbb{F}_2^n$  be a  $[n, k, d]$ -linear code having a parity check matrix  $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ . We define  $\ell_t = \lfloor \log_2(t) \rfloor + 1$ . Let  $\mathbf{s} \in \mathbb{F}_2^{n-k}$  play the role of the syndrome and let  $0 \leq t \leq \lfloor (d-1)/2 \rfloor$  be the target error weight. Let  $X = (x_1, \dots, x_n)$  and  $Y = (Y_1, \dots, Y_n)$  with  $Y_j = (y_{j,1}, \dots, y_{j,\ell_t})$  be two sets of variables and consider the polynomial ring  $\mathbb{F}_2[X, Y]$ .*

Under Notation 2, the effect of our improvement on the set of polynomials produced by the Hamming weight computation encoding is the following.

- *Hamming weight computation encoding.* Compute the following union of subsets of  $\mathbb{F}_2[X, Y]$ :

$$\begin{aligned} & \{x_1 + y_{1,1}, y_{1,2}, \dots, y_{1,\ell_t}\} \cup \{x_i + y_{i,1} + y_{i-1,1} \mid i = 2, \dots, n\} \\ & \cup \{y_{i,j-1}y_{i-1,j-1} + y_{i,j} + y_{i-1,j-1} + y_{i-1,j} \\ & \quad \mid i = 2, \dots, n, j = 2, \dots, \ell_t\} \cup \{y_{i,\ell_t}y_{i-1,\ell_t} + y_{i-1,\ell_t} \mid i = 2, \dots, n\}. \end{aligned} \quad (7)$$

The effect on the weight constraint encoding is simply the decrease in the degree from  $\ell$  to  $\ell_t$  of the produced polynomial. This is the only non-quadratic polynomial left in the modeling. We can turn this polynomial into a set of  $\mathcal{O}(t\ell_t)$  polynomials of degree up to 2 in  $\mathcal{O}(t\ell_t)$  variables with the same linearization techniques described in [33, Fact 1 and Lemma 11].

To summarize, our modeling is defined in the following way.

**Modeling 1 (Improved modeling for the SDP over  $\mathbb{F}_2$ )** *Given an instance  $(\mathbf{H}, \mathbf{s}, t)$  of Problem 1 over  $\mathbb{F}_2$ , Modeling 1 is the union of the sets of polynomials (2), (5), (6) and (7).*

The improved modeling is an algebraic system of  $\mathcal{O}(n(\ell_t + 2) - k + t\ell_t)$  polynomials of degree at most 2 in  $\mathcal{O}(n(\ell_t + 1) + t\ell_t)$  variables. Note that usual applications of the SDP to code-based cryptography choose  $t \ll n$ , hence the asymptotic bounds on the number of polynomials and variables in the improved modeling are both  $\mathcal{O}(n\ell_t)$ . As shown in Table 1, our modeling improves over MPS by a factor of  $\log_2(n) \log_t(n)$ .

	# Polynomials	# Variables
[33]	$\mathcal{O}(n \log_2(n)^2)$	$\mathcal{O}(n \log_2(n)^2)$
Modeling 1	$\mathcal{O}(n \log_2(t))$	$\mathcal{O}(n \log_2(t))$

**Table 1.** Comparison with the asymptotic size of the polynomial system in [33, Theorem 13], where  $n$  is the length of the code and  $t$  the bound on the weight of the target vector, that is  $\text{wt}(\mathbf{e}) \leq t$ .

## 4.2 Improved Modeling for the Case of ESDP

It is possible to obtain an algebraic modeling for the ESDP by tweaking the modeling described in the previous section. In fact, it is enough to redefine the weight constraint encoding to enforce that  $\mathbf{y}_n$  represents the binary expansion of an integer  $t'$  such that  $t' = t$  exactly. To this end, let  $\mathbf{v} \in \mathbb{F}_2^{\ell_t}$  represent the binary expansion of an integer  $t$ . Under the same notation as in Notation 2, the following version of the weight constraint encoding describes the ESDP modeling with  $\text{wt}(\mathbf{e}) = t$ .

- *Weight constraint encoding.* Compute the following set of linear polynomials:

$$\{y_{n,j} + v_j \mid j = 1, \dots, \ell_t\}. \quad (8)$$

Using these polynomials leads to Modeling

**Modeling 2 (Improved modeling for the ESDP over  $\mathbb{F}_2$ )** *Given an instance  $(\mathbf{H}, \mathbf{s}, t)$  of Problem 2 over  $\mathbb{F}_2$ , Modeling 2 is the union of the sets of polynomials (2), (6), (7) and (8).*

Observe that, replacing the original Hamming weight computation encoding with that in (7) and the weight constraint encoding with that in (8), we obtain an algebraic system of polynomials of degree at most 2 for ESDP. Hence, linearization is not needed, moreover, we can give the exact number of equations and variables of this system. We report these values in Table 2.

	# Polynomials	# Variables
Modeling 2	$2n\ell_t + 3n + \ell_t - k - 1$	$n(\ell_t + 1)$

**Table 2.** Number of equations and variables of the algebraic modeling of ESDP with  $\text{wt}(\mathbf{e}) = t$ . The value of  $\ell_t$  is  $\lceil \log_2(t) \rceil + 1$ .

## 5 Complexity Analysis of Modeling 2

In this section, we investigate the complexity of solving the algebraic system for the ESDP given in Modeling 2 using standard Gröbner basis methods. An upper bound on the complexity is given by the formula (1) which depends on both the number of variables and the solving degree. Typically, the solving degree of the system is estimated by assessing its degree of regularity. However, in our analysis, we experimentally show that the degree of regularity often significantly exceeds the solving degree for systems given in Section 4.2 (see the results in Table 3). This distinction is crucial in cryptography, where these concepts are frequently used interchangeably. Our findings underscore the importance of thoroughly verifying such claims to ensure accurate security assessments and parameter selection.

*Remark 4.* We point out that the study in [13] investigates a particular case of the problem that this paper deals with, that is the *regular* syndrome decoding problem. The regular syndrome decoding problem considers error vectors having a regular distribution of non-zero entries. The algebraic modeling proposed in [13] has been conjectured to behave semi-regularly when the linear parity-check constraints and the fixed and structured quadratic polynomials are considered separately. Despite the fact that the problem tackled in [13] is a particular case of the problem we consider, our modeling has not been devised as a generalization of their modeling. Furthermore, we show that for the more general case, our modeling yields different results.

For the rest of this section, we retain the notation defined in Notation 2. Let  $S \subset \mathbb{F}_2[X, Y]$  be the set of polynomials of Modeling 2 as described in Section 4.2.

Let  $L$  and  $Q$  denote the sets of linear and quadratic polynomials, respectively. Clearly  $S = L \cup Q$ . Write also  $L = L_{\mathbf{H}} \cup P$ , where  $L_{\mathbf{H}}$  denotes the set of linear polynomials in (2) introduced with the parity check matrix  $\mathbf{H}$ , and  $P$  denotes the remaining linear polynomials in  $S$ . In other words,  $P$  is the following set

$$P = \{x_1 + y_{1,1}, y_{1,2}, \dots, y_{1,\ell_t}\} \cup \{x_i + y_{i,1} + y_{i-1,1} \mid i = 2, \dots, n\}.$$

We want to estimate the degree of regularity of  $S$ . As mentioned in Section 2, this can be done by computing the degree of the Hilbert series of  $\mathbb{F}_2[X, Y]/\langle S^{\text{top}} \rangle$ . Since we do not know  $L_{\mathbf{H}}$  a priori, we first consider the set  $S \setminus L_{\mathbf{H}} = Q \cup P$  and compute its degree of regularity. After, we will shortly argue the effect of adding  $L_{\mathbf{H}}$  back to the set on the degree of regularity. We break down the problem even further by first computing the degree of regularity of  $Q$  and then that of  $Q \cup P$ . We take advantage of the fact that the Hilbert series of  $Q$  and of  $Q \cup P$  are polynomials and compute their degree, i.e. for instance,  $d_{\text{reg}}(Q) = \deg \text{HS}_{\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle}(z) + 1$  as per Remark 2, similarly for  $Q \cup P$ . To this end, we are going to compute the maximum degree of a monomial in  $\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle$ , similarly we do for  $Q \cup P$ .

**The quadratic polynomials.** We begin by studying the degree of regularity of the quadratic part  $Q$  of the system  $S$  of Modeling 2. The highest degree part of  $Q$  has a very nice structure, as explained in the following remark.

*Remark 5.* The set  $Q^{\text{top}}$  is the union of the following three sets

$$\{x_i^2 \mid i = 1, \dots, n\}, \{y_{i,j}^2 \mid i = 1, \dots, n, j = 1, \dots, \ell_t\}$$

and

$$\{y_{i-1,j}y_{i,j} \mid i = 2, \dots, n, j = 1, \dots, \ell_t\}.$$

and the ideal  $\langle Q^{\text{top}} \rangle \subseteq \mathbb{F}_2[X, Y]$  is thus a monomial ideal.

The following lemma gives the structure of the quotient ring  $\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle$ .

**Lemma 1.** *The set  $Q^{\text{top}}$  is a Gröbner basis of the ideal  $\langle Q^{\text{top}} \rangle$ .*

*Proof.* As observed in Remark 5,  $Q^{\text{top}}$  is a monomial ideal. Given any two elements of  $m_1, m_2 \in Q^{\text{top}}$  it is clear that for  $a = \text{lcm}(m_1, m_2)/m_1 \in \mathbb{F}_2[X, Y]$  and  $b = \text{lcm}(m_1, m_2)/m_2 \in \mathbb{F}_2[X, Y]$  we have that  $am_1 - bm_2 = 0$ .  $\square$

*Example 1.* Let  $n = 4$  be the length of a code, then  $\ell_t = 2$ . A Gröbner basis of  $\langle Q^{\text{top}} \rangle$  is the union of

$$\{y_{1,1}y_{2,1}, y_{1,2}y_{2,2}, y_{2,1}y_{3,1}, y_{2,2}y_{3,2}, y_{3,1}y_{4,1}, y_{3,2}y_{4,2}\}$$

and

$$\{x_1^2, x_2^2, x_3^2, x_4^2, y_{1,1}^2, y_{1,2}^2, y_{2,1}^2, y_{2,2}^2, y_{3,1}^2, y_{3,2}^2, y_{4,1}^2, y_{4,2}^2\}.$$

The following simple lemma is crucial for computing the degree of regularity of  $Q$ . For the sake of simplicity, we state it in terms of sets, and it ultimately provides a method to construct maximal monomials in the quotient ring  $\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle$ .

**Lemma 2.** *Let  $\mathcal{N} = \{1, 2, 3, \dots, n\}$  and  $\mathcal{P} = \{\{1, 2\}, \{2, 3\}, \dots, \{n-1, n\}\}$ , where  $\mathcal{P}$  consists of consecutive pairs of elements from  $\mathcal{N}$ . Then:*

- *If  $n$  is even, there are exactly two maximal sets  $\mathcal{S} \subseteq \mathcal{N}$  such that no set in  $\mathcal{P}$  is a subset of  $\mathcal{S}$ .*
- *If  $n$  is odd, there is exactly one maximal set  $\mathcal{S} \subseteq \mathcal{N}$  such that no set in  $\mathcal{P}$  is a subset of  $\mathcal{S}$ .*

*Proof.* We aim to find the number of maximal sets  $\mathcal{S} \subseteq \mathcal{N}$  such that no pair from  $\mathcal{P}$  (i.e., no two consecutive elements) appears in  $\mathcal{S}$ . In order to avoid pairs of consecutive elements, we can only select non-consecutive elements from  $\mathcal{N}$ . To maximize the size of  $\mathcal{S}$ , we select every other element from  $\mathcal{N}$ . The size of such a maximal set  $\mathcal{S}$  is:

$$|\mathcal{S}| = \left\lceil \frac{n}{2} \right\rceil.$$

Thus:

- If  $n$  is even, a maximal set contains  $\frac{n}{2}$  elements.
- If  $n$  is odd, the maximal set contains  $\frac{n+1}{2}$  elements.

**Case 1:  $n$  is even.** Let  $n = 2k$ . The largest possible set  $\mathcal{S}$  will contain  $k = \frac{n}{2}$  elements. There are exactly two ways to construct such a set:

1. Start with 1 and select every other element:

$$\mathcal{S}_1 = \{1, 3, 5, \dots, n-1\}.$$

This set contains all the odd-numbered elements of  $\mathcal{N}$ , and its size is  $k$ .

2. Start with 2 and select every other element:

$$\mathcal{S}_2 = \{2, 4, 6, \dots, n\}.$$

This set contains all the even-numbered elements of  $\mathcal{N}$ , and its size is also  $k$ .

Since there are no other ways to select  $k$  elements without picking consecutive elements, these are the only two maximal sets for  $n$  even.

**Case 2:  $n$  is odd.** Let  $n = 2k + 1$ . The largest possible set  $\mathcal{S}$  will contain  $k + 1 = \frac{n+1}{2}$  elements. In this case, there is only one way to construct a set of size  $k + 1$  that avoids consecutive elements, i.e. start with 1 and select every other element:

$$\mathcal{S}_1 = \{1, 3, 5, \dots, n\}.$$

This set contains  $k + 1$  elements and avoids consecutive pairs. If we were to start with 2 and select every other element, we would only get  $k$  elements:

$$\mathcal{S}_2 = \{2, 4, 6, \dots, n-1\}.$$

This is not maximal, as it contains fewer than  $k + 1$  elements. Thus, for  $n$  odd, there is exactly one maximal set.  $\square$

Lemma 2 can be used to prove the following corollary, which we will use to construct a maximal degree monomial in  $\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle$ .

**Corollary 1.** *Let  $n \in \mathbb{N}$  with  $n \geq 2$ , and define*

$$Q_{j,n}^{\text{top}} := \{y_{1,j}y_{2,j}, y_{2,j}y_{3,j}, \dots, y_{n-1,j}y_{n,j}\} \cup \{y_{i,j}^2 \mid i = 1, \dots, n\} \subset \mathbb{F}_2[y_{1,j}, \dots, y_{n,j}],$$

for some  $j \in \mathbb{N}$ . If  $n$  is even then there exists two monomials of maximal degree  $\lceil \frac{n}{2} \rceil$  in  $\mathbb{F}_2[y_{1,j}, \dots, y_{n,j}]/\langle Q_{j,n}^{\text{top}} \rangle$ , namely

$$m_1 = \prod_{\substack{i=1, \dots, n-1, \\ i \text{ odd}}} y_{i,j} \quad \text{and} \quad m_2 = \prod_{\substack{i=2, \dots, n, \\ i \text{ even}}} y_{i,j}.$$

If  $n$  is odd, then there exists a unique monomial of maximal degree  $\lceil \frac{n}{2} \rceil$  in  $\mathbb{F}_2[y_{1,j}, \dots, y_{n,j}]/\langle Q_{j,n}^{\text{top}} \rangle$ , namely

$$m = \prod_{\substack{i=1, \dots, n, \\ i \text{ odd}}} y_{i,j}.$$

We are ready to prove the following theorem, which provides the degree of regularity of  $Q$ .

**Theorem 1.**

$$d_{\text{reg}}(Q) = \begin{cases} n + \ell_t n/2 + 1 & \text{if } n \equiv 0 \pmod{2} \\ n + \ell_t(n+1)/2 + 1 & \text{if } n \equiv 1 \pmod{2} \end{cases}.$$

Equivalently,

$$d_{\text{reg}}(Q) = n + \ell_t \lceil n/2 \rceil + 1.$$

*Proof.* Let  $Q_{j,n}^{\text{top}} \subset \mathbb{F}_2[y_{1,j}, \dots, y_{n,j}]$  as in Corollary 1, for every  $j = 1, \dots, \ell_t$ . Observe that

$$Q^{\text{top}} = \bigcup_{j=1}^{\ell_t} Q_{j,n}^{\text{top}} \cup \{x_i^2 \mid i = 1, \dots, n\}. \quad (9)$$

Corollary 1 computes a monomial  $m_j \in \mathbb{F}_2[y_{1,j}, \dots, y_{n,j}]$  of maximal degree  $\lceil n/2 \rceil$  such that  $m_j \notin \langle Q_h^{\text{top}} \rangle$  for every  $j = 1, \dots, \ell_t$  and every  $h = 1, \dots, \ell_t$ . This implies that  $m_j \notin \langle Q^{\text{top}} \rangle$  for every  $j$ . It is now clear that the monomial

$$m := \prod_{i=1}^n x_i \prod_{j=1}^{\ell_t} m_j \in \mathbb{F}_2[X, Y]$$

is such that  $m \notin \langle Q^{\text{top}} \rangle$ . Note that the set  $\{x_i^2 \mid i = 1, \dots, n\}$  in (9) enforces that  $m$  must be squarefree in the variables  $x_1, \dots, x_n$ . By the maximality of each  $m_j$  and that of  $\prod_{i=1}^n x_i$ , any multiple of  $m$  by a non-constant term would trivially be in  $\langle Q^{\text{top}} \rangle$ . Since

$$d := \deg m = n + \ell_t \lceil n/2 \rceil,$$

we have that the  $(d+1)$ -th coefficient of the Hilbert series of  $\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle$  is 0. The result on the degree of regularity  $d_{\text{reg}}(Q)$  follows.  $\square$

*Example 2.* Let  $n = 8$  and  $\ell_t = 3$ . According to Theorem 2 the degree of regularity of  $Q$  is

$$d_{\text{reg}}(Q) = 8 + 3 \left\lceil \frac{8}{2} \right\rceil + 1 = 21.$$

Using MAGMA, we compute and report the Hilbert series of the quotient ring  $\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle$ , i.e.

$$\begin{aligned} \text{HS}_{\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle}(z) = & 125z^{20} + 2500z^{19} + 23075z^{18} + 130800z^{17} + \\ & 511140z^{16} + 1465020z^{15} + 3198081z^{14} + \\ & 5448312z^{13} + 7360635z^{12} + 7966528z^{11} + \\ & 6946904z^{10} + 4889800z^9 + 2773415z^8 + \\ & 1260580z^7 + 454625z^6 + 128080z^5 + 27524z^4 + \\ & 4348z^3 + 475z^2 + 32z + 1, \end{aligned}$$

thus  $d_{\text{reg}}(Q) = \deg \text{HS}_{\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \rangle} + 1 = 21$ , matching our results.

**The Linear Polynomials.** In this section, we study how the degree of regularity computed in Theorem 1 changes when we add to the quadratic equations  $Q$  also the fixed linear equations of  $P$ , which do not depend on the specific instance of the problem. Specifically, we compute the degree of regularity of  $Q \cup P$ . For this, we need to consider the ideal  $\langle Q^{\text{top}} \cup P^{\text{top}} \rangle$ . Note that this ideal contains  $\langle Q^{\text{top}} \rangle$ , which means that the variety of the former is a subset of the variety of the latter. In particular, the ideal  $\langle Q^{\text{top}} \cup P^{\text{top}} \rangle$  is also zero-dimensional, so its degree of regularity is well-defined. We will use similar arguments to those applied to  $\langle Q^{\text{top}} \rangle$  to study it.

*Remark 6.* The set  $Q^{\text{top}} \cup P^{\text{top}}$  is the union of the following sets

$$\begin{aligned} & \{x_i^2 \mid i = 1, \dots, n\}, \{x_i \mid i = 1, \dots, n\}, \{y_{i,j}^2 \mid i = 1, \dots, n, j = 1, \dots, \ell_t\}, \\ & \{y_{1,j} \mid j = 2, \dots, \ell_t\}, \{y_{n,j} \mid j = 1, \dots, \ell_t\} \end{aligned}$$

and

$$\{y_{i-1,j}y_{i,j} \mid i = 2, \dots, n, j = 1, \dots, \ell_t\}.$$

and the ideal  $\langle Q^{\text{top}} \cup P^{\text{top}} \rangle \subseteq \mathbb{F}_2[X, Y]$  is thus a monomial ideal.

Next lemma provides a Gröbner basis of the ideal  $\langle Q^{\text{top}} \cup P^{\text{top}} \rangle \subseteq \mathbb{F}_2[X, Y]$ .

**Lemma 3.** *A Gröbner basis  $G$  for  $\langle Q^{\text{top}} \cup P^{\text{top}} \rangle \subseteq \mathbb{F}_2[X, Y]$  is*

$$\begin{aligned} G = & \{x_i \mid i = 1, \dots, n\} \cup \{y_{i-1,j}y_{i,j} \mid i = 3, \dots, n-1, j = 1, \dots, \ell_t\} \cup \\ & \{y_{1,1}y_{2,1}\} \cup \{y_{1,j} \mid j = 2, \dots, \ell_t\} \cup \{y_{n,j} \mid j = 1, \dots, \ell_t\} \cup \\ & \{y_{i,j}^2 \mid i = 2, \dots, n-1, j = 1, \dots, \ell_t\} \cup \{y_{1,1}^2\}. \end{aligned}$$

*Proof.* The proof of this statements follows directly from inspecting Remark 6 and the same observations as in proof of Lemma 1.  $\square$

The next theorem gives the exact value of the degree of regularity of the system  $Q \cup P$ . The proof uses similar arguments to those used for the proof of Theorem 1.

**Theorem 2.** *The degree of regularity of  $Q \cup P$  is*

$$d_{\text{reg}}(Q \cup P) = \left\lceil \frac{n-1}{2} \right\rceil + (\ell_t - 1) \left\lceil \frac{n-2}{2} \right\rceil + 1.$$

*Proof.* Define the set

$$\tilde{Q}_{j,n}^{\text{top}} := Q_{j,n-1}^{\text{top}} \setminus \{y_{1,j}y_{2,j}\} \subset \mathbb{F}_2[y_{2,j}, \dots, y_{n-1,j}].$$

Let  $G$  be a Gröbner basis of  $\langle Q^{\text{top}} \cup P^{\text{top}} \rangle$  as in Lemma 3. Due to the presence of the linear monomials contributed by  $P^{\text{top}}$  we observe that

$$G = Q_{1,n-1}^{\text{top}} \cup \bigcup_{j=2}^{\ell_t} \tilde{Q}_{j,n-1}^{\text{top}} \cup \{x_i^2 \mid i = 1, \dots, n\}. \quad (10)$$

Applying Corollary 1, we can get a monomial  $m_1 \in \mathbb{F}_2[y_{1,1}, \dots, y_{n-1,1}]$  of maximal degree  $\deg m_1 = \lceil (n-1)/2 \rceil$  such that  $m_1 \notin \mathbb{F}_2[y_{1,1}, \dots, y_{n-1,1}]/\langle Q_{1,n-1}^{\text{top}} \rangle$ . We can obtain other  $\ell_t - 1$  monomials  $m_j$  of maximal degree  $d = \lceil (n-2)/2 \rceil$ , such that  $m_j \notin \langle \tilde{Q}_{h,n-1}^{\text{top}} \rangle$  for every  $h = 1, \dots, \ell_t$  and every  $j = 2, \dots, \ell_t$ . Let now

$$m := \prod_{j=1}^{\ell_t} m_j \in \mathbb{F}_2[X, Y]/\langle G \rangle$$

then

$$d := \deg m = \left\lceil \frac{n-1}{2} \right\rceil + (\ell_t - 1) \left\lceil \frac{n-2}{2} \right\rceil,$$

meaning that the  $(d+1)$ -th coefficient of the Hilbert series of  $\mathbb{F}_2[X, Y]/\langle G \rangle$  is 0. The result on the degree of regularity  $d_{\text{reg}}(Q \cup P)$  follows.  $\square$

*Example 3.* Let  $n = 8$  and  $\ell_t = 3$ . According to Theorem 2 the degree of regularity of  $Q \cup P$  is

$$d_{\text{reg}}(Q \cup P) = \left\lceil \frac{7}{2} \right\rceil + (3-1) \left\lceil \frac{6}{2} \right\rceil + 1 = 11.$$

Using MAGMA, we compute and report the Hilbert series of the quotient ring  $\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \cup P^{\text{top}} \rangle$ , i.e.

$$\text{HS}_{\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \cup P^{\text{top}} \rangle}(z) = 16z^{10} + 240z^9 + 1188z^8 + 2920z^7 + 4132z^6 + 3608z^5 + 2005z^4 + 710z^3 + 155z^2 + 19z + 1,$$

thus  $d_{\text{reg}}(Q \cup P) = \deg \text{HS}_{\mathbb{F}_2[X, Y]/\langle Q^{\text{top}} \cup P^{\text{top}} \rangle} + 1 = 11$ , matching our results.



*Remark 7.* Since Theorem 2 considers the set  $Q^{\text{top}} \cup P^{\text{top}} = S^{\text{top}} \setminus L_H^{\text{top}}$ , it only gives an upper bound to the degree of regularity  $d_{\text{reg}}(S)$ .

In the next section, we provide some experimental data showing the gap between the value computed in Theorem 2 and that of the actual solving degree.

### 5.1 Experimental results

We performed several experiments for Modeling 2 taking as input both random and Goppa codes, and we obtained a solving degree which is much smaller than the upper bound for the degree of regularity computed in Theorem 2. This results in a much lower complexity estimate. To give a taste of our results, we report a selection of our experiments in Table 3. The MAGMA code used for our experiments can be found at [this link](#).

$n$	$k$	$t$	Code Type	# Lin Eqs	# Quad Eqs	# Vars	$d_{\text{reg}}$	SR $d_{\text{reg}}$	SD
8	2	2	Goppa	17	38	24	$\leq 8$	3	2
10	5	4	Random*	20	67	40	$\leq 14$	5	3
16	8	2	Goppa	27	78	48	$\leq 16$	5	3
20	10	5	Random*	35	137	80	$\leq 29$	7	3
30	15	7	Random*	50	207	120	$\leq 44$	10	4
32	12	4	Goppa	57	221	128	$\leq 47$	10	3
32	17	3	Goppa	50	158	96	$\leq 32$	5	4
32	22	2	Goppa	45	158	96	$\leq 32$	7	3
40	20	8	Random*	67	356	160	$\leq 78$	16	5
50	30	5	Random	75	347	200	$\leq 74$	15	4
50	40	4	Random	65	347	200	$\leq 74$	17	4
64	52	2	Goppa	79	318	192	$\leq 64$	14	4
64	40	4	Goppa	93	445	256	$\leq 95$	19	4
64	16	8	Goppa	119	572	320	$\leq 126$	21	4

**Table 3.** This table gives information from experiments of  $\mathbb{F}_2$ -linear codes using Modeling 2 for the ESDP. The values in the SD column represent the highest step degree achieved when directly computing the Gröbner basis of the system in MAGMA. This is typically regarded as a proxy for the solving degree  $d_{\text{sol}}$ . The SR  $d_{\text{reg}}$  column gives the degree of regularity of a semi-regular system of equations with the associated number of linear equations, quadratic equations, and variables, using [3, Corollary 3.3.8]. The values in  $d_{\text{reg}}$  column are upper bounds for the degree of regularity of the system as provided by Theorem 2 and Remark 7. Random codes with “\*” are decoding challenges from <https://decodingchallenge.org/syndrome>, with a number of errors slightly above Gilbert-Varshamov distance. Several solutions are indeed found. The other random code instances are below GV distance instead. Instances with “Goppa” Code Type are random full-length binary Goppa codes with a number of errors equal to the Goppa polynomial degree. These parameters have also been tested with random codes and always provide the same solving degree in the two cases.

## 6 Modelings over $\mathbb{F}_q$

Each of the modelings we have discussed thus far (MPS, Modeling 1, and Modeling 2) are limited to the binary case. To the best of our knowledge, there is no modeling of the general syndrome decoding problem over  $\mathbb{F}_q$  for  $q > 2$  in the literature. In this section, we adapt the previous modelings to a generic finite field  $\mathbb{F}_q$ , for some prime power  $q \geq 2$ , and explain how to efficiently (i.e. in polynomial time) obtain a polynomial system encoding an instance of the Syndrome Decoding problem.

We will adopt the following notation throughout this section.

**Notation 3** *Let  $n \geq 2$  and let  $\mathcal{C} \subseteq \mathbb{F}_q^n$  be a  $[n, k, d]$ -linear code having a parity check matrix  $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ . The vector  $\mathbf{s} \in \mathbb{F}_q^{n-k}$  denotes the syndrome and  $0 \leq t \leq \lfloor (d-1)/2 \rfloor$  is the target error weight. Let  $r_1, r_2 > 0$  be two integers. We will work over the polynomial ring  $\mathbb{F}_{q^{r_1}}[X, Y, Z]$ , where  $X = (x_1, \dots, x_n)$ ,  $Y = (Y_1, \dots, Y_n)$ ,  $Y_j = (y_{j,1}, \dots, y_{j,r_2})$ , and  $Z = (z_1, \dots, z_n)$  are variables.*

As in the previous sections,  $\mathbf{x} = (x_1, \dots, x_n)$  is the vector of variables corresponding to the solution of the syndrome decoding problem. On the other hand, the role of the integers  $r_1, r_2$  and of the variables  $Y$  and  $Z$  will be illustrated later.

We separately describe and explain the sets of polynomials that, together, model Problems 1 and 2. Then we provide an analysis of the correctness of our modelings.

### 6.1 Construction of the Equations

**Identifying the support of a vector of  $\mathbb{F}_q^n$ .** Unlike the Boolean case, the value of an element in the support of  $\mathbf{x}$  is not uniquely determined when  $q \geq 3$ . In order to count the number of nonzero coordinates with algebraic equations, we first need to map all nonzero elements to a unique element of  $\mathbb{F}_q^*$ , say 1. Thus, in addition to the  $Y$ 's variables encoding the partial Hamming weights, we introduce here another length- $n$  vector of variables  $Z = (z_1, \dots, z_n)$ , each of which can only assume two values, 0 or 1, depending on whether the corresponding  $X$  coordinate is nonzero. First, we tackle the problem of describing the relation between  $X$  and  $Z$  through algebraic equations. We distinguish two cases, depending on the target version of the problem, and then prove the sets of polynomials correctly describe our target.

- *Support constraint encoding for Problem 1.* Compute the following set of  $2n$  quadratic polynomials

$$\{x_j(z_j - 1) \mid j = 1, \dots, n\} \cup \{z_j^2 - z_j \mid j = 1, \dots, n\}. \quad (11)$$

- *Support constraint encoding for Problem 2.* Compute the following set of  $n$  polynomials of degree  $q - 1$

$$\{z_j - x_j^{q-1} \mid j = 1, \dots, n\}. \quad (12)$$

In the first case, the condition  $z_j = 1$  if  $x_j \neq 0$  is given from the first set of polynomials. Otherwise, the second set implies  $z_j \in \{0, 1\}$ . Therefore, the support of  $(z_1, \dots, z_n)$  contains the support of  $(x_1, \dots, x_n)$  and thus  $\text{wt}((z_1, \dots, z_n)) \geq \text{wt}((x_1, \dots, x_n))$ . In the second case, in order for the corresponding equations to be satisfied,  $z_j = 1$  if and only if  $x_j \neq 0$ , and  $z_j = 0$  otherwise. Hence  $\text{wt}((z_1, \dots, z_n)) = \text{wt}((x_1, \dots, x_n))$ .

From a computational point of view, the support constraint encoding for Problem 2 has a strong limitation, that is the high degree of the polynomials. A Gröbner basis computation would need to reach at least degree  $q - 1$  before taking into account such polynomials, leading to infeasible calculations unless  $q$  is very small. This is reminiscent of the problem of including field equations in modelings over large fields. Yet, this issue does not appear in the support constraint encoding for Problem 1: the polynomials have constant degree 2 regardless of the field size  $q$ , making a modeling for Problem 1 more realistic and valuable for effective computations.

**Hamming weight computation encoding.** A difficulty arising from a direct generalization to large fields of the previous approach is the update of the weight registers, i.e. of the vectors  $\mathbf{y}_i$ 's. In order to overcome this limitation, we introduce a different strategy for encoding the partial weights. More precisely, we substitute their binary expansion with the representation of finite field elements through companion matrices. This approach associates intervals of integers with powers of matrices and naturally allows for the choice of different trade-offs between the number of variables and finite field size.

We first recall some known results about (univariate) polynomials over finite fields, companion matrices, and linear recurring sequences. We mainly refer to [28] for this part.

**Definition 1 (Companion matrix, Chapter 2, §5 [28]).** Let  $f(x) = x^d + f_{d-1}x^{d-1} + \dots + f_0 \in \mathbb{F}_q[x]$  be a monic polynomial. Its companion matrix is

$$\mathbf{C}_f = \begin{bmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & \cdots & 0 & -f_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -f_{d-1} \end{bmatrix}. \quad (13)$$

It is well known that the equation  $f(\mathbf{C}_f) = 0$  is satisfied, hence, if  $f$  is a monic irreducible polynomial over  $\mathbb{F}_q$ , then its companion matrix  $\mathbf{C}_f$  plays the role of a root of  $f$ . It follows that the elements of the extension field  $\mathbb{F}_{q^d}$  can be written, according to this representation, as polynomials in  $\mathbf{C}_f$  of degree strictly less than  $d$ .

We also recall that the order of a nonzero polynomial  $f$  with  $f_0 = 0$  is the least positive integer  $e$  such that  $f(x) \mid x^e - 1$ . A polynomial in  $\mathbb{F}_q[x]$  of degree  $d$  is said primitive if it is monic,  $f(0) \neq 0$ , and  $\text{ord}(f) = q^d - 1$ . Such polynomials can be found from the factorization of  $x^{q^d-1} - 1$ .

The theory of linear recurring sequences says that the least period of the sequence of vectors  $\mathbf{y}_0, \mathbf{C}_f \mathbf{y}_0, \mathbf{C}_f^2 \mathbf{y}_0, \dots$ , for some nonzero  $\mathbf{y}_0$  and companion matrix with  $f_0 \neq 0$ , is periodic with least period equal to the order of  $f$ , when the latter is irreducible (cf. [28, Theorem 6.28]). Therefore, by choosing  $f$  primitive, we obtain a sequence of vectors  $\mathbf{y}_0, \mathbf{C}_f \mathbf{y}_0, \mathbf{C}_f^2 \mathbf{y}_0, \dots$  of maximal order  $q^d - 1$ . On the other hand, the choice of  $\mathbf{y}_0$  does not seem to affect any property of our modeling. Without loss of generality, we thus fix the initial state vector

$$\mathbf{y}_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad (14)$$

from now on.

As already anticipated, our strategy allows different ways to choose the number of variables used for the Hamming weight computation encoding, at the cost of working over more or less large field extensions. More precisely, take

$$m := \min\{i \in \mathbb{N} \mid q^i > \max(t, n - t) + 1\},$$

and let  $r_1, r_2$  be two positive integers such that  $m \leq r_1 r_2$ .

Then, let  $f \in \mathbb{F}_{q^{r_1}}[x]$  be a primitive polynomial of degree  $r_2$  and  $\mathbf{C}_f \in \mathbb{F}_{q^{r_1}}^{r_2 \times r_2}$  its companion matrix. For convenience sake, we will use the column vector notation for the  $Y_j$ 's blocks of variables, i.e.

$$Y_j = \begin{pmatrix} y_{j,1} \\ \vdots \\ y_{j,r_2} \end{pmatrix}.$$

The polynomial encoding the partial Hamming weight is the following.

- *Hamming weight computation encoding.* Compute the  $nr_2$  affine bilinear (in  $Y$  and  $Z$ ) polynomials from the expansion of

$$Y_1 - (1 - z_1) \cdot \mathbf{y}_0 - z_1 \cdot \mathbf{C}_f \cdot \mathbf{y}_0 \quad (15)$$

and

$$\{Y_j - (1 - z_j) \cdot Y_{j-1} - z_j \cdot \mathbf{C}_f \cdot Y_{j-1}, \quad \text{for } j \in \{2, \dots, n\}\}. \quad (16)$$

*Remark 8.* Each element in the set corresponds to  $r_2$  polynomial equations over  $\mathbb{F}_{r_1}$ , as each entry of the length- $r_2$  vectors must be equal to 0.

The next proposition shows that the Hamming weight of  $\mathbf{z}$  is correctly computed.

**Proposition 2.** *Consider the system given by (15) and (16) over  $\mathbb{F}_{q^{r_1}}[Y, Z]$ . Any solution  $(\mathbf{y}, \mathbf{z}) = (\mathbf{y}_1, \dots, \mathbf{y}_n, \mathbf{z}) \in \mathbb{F}_{q^{r_1}}^{nr_2} \times \{0, 1\}^n$  of the system satisfies*

$$\mathbf{y}_j = \mathbf{C}_f^{\text{wt}(\pi_j(\mathbf{z}))} \mathbf{y}_0.$$

*In particular,  $\mathbf{y}_n = \mathbf{C}_f^{\text{wt}(\mathbf{z})} \mathbf{y}_0$ .*

*Proof.* It follows directly from the hypotheses by an inductive argument. The first step is considering  $\mathbf{y}_1 := (y_{1,1}, \dots, y_{1,r_2})^\top$ , which by definition is

$$\mathbf{y}_1 = (1 - z_1)\mathbf{y}_0 + z_1\mathbf{C}_f\mathbf{y}_0 = \begin{cases} \mathbf{y}_0 & \text{if } z_1 = 0 \\ \mathbf{C}_f\mathbf{y}_0 & \text{if } z_1 \neq 0 \end{cases},$$

namely,  $\mathbf{y}_1 = \mathbf{C}_f^{\text{wt}(z_1)}\mathbf{y}_0 = \mathbf{C}_f^{\text{wt}(\pi_1(\mathbf{z}))}\mathbf{y}_0$ .

For the inductive step, we consider  $\mathbf{y}_{j-1} := (y_{j-1,1}, \dots, y_{j-1,r_2})^\top$  to be equal to  $\mathbf{C}_f^{\text{wt}(\pi_{j-1}(\mathbf{z}))}\mathbf{y}_0$ , and we look at the definition of  $\mathbf{y}_j$ . We have

$$\mathbf{y}_j = (1 - z_j)\mathbf{y}_{j-1} + z_j\mathbf{C}_f\mathbf{y}_{j-1} = \begin{cases} \mathbf{y}_{j-1} & \text{if } z_j = 0 \\ \mathbf{C}_f\mathbf{y}_{j-1} & \text{if } z_j \neq 0 \end{cases},$$

and either way, we obtain

$$\mathbf{y}_j = \mathbf{C}_f^{z_j} \cdot \mathbf{y}_{j-1} = \mathbf{C}_f^{z_j} \mathbf{C}_f^{\text{wt}(\pi_{j-1}(\mathbf{z}))} \mathbf{y}_0 = \mathbf{C}_f^{\text{wt}(z_j) + \text{wt}(\pi_{j-1}(\mathbf{z}))} \mathbf{y}_0 = \mathbf{C}_f^{\text{wt}(\pi_j(\mathbf{z}))} \mathbf{y}_0.$$

□

**Weight constraint encoding.** As for the previous modelings, the weight constraint encoding simply ensures that the representation of the last partial Hamming weight coincides with the representation of the total Hamming weight.

– *Weight constraint encoding.* Compute the  $r_2$  affine linear polynomials in  $Y$  from the expansion of

$$\mathbf{y}_n - \mathbf{C}_f^t \mathbf{y}_0. \quad (17)$$

**Corollary 2.** Consider the system given by (15), (16) and (17) over  $\mathbb{F}_{q^{r_1}}[Y, Z]$  and let  $z_1, \dots, z_n$  be either 0 or 1. Then

1. The number of solutions  $(\mathbf{y}, \mathbf{z}) \in \mathbb{F}_{q^{r_1}}^{r_2 n} \times \{0, 1\}^n$  of the system is equal to the number of binary vectors of Hamming weight equal to  $t$ , i.e.  $\binom{n}{t}$ ;
2. If  $(\tilde{\mathbf{y}}, \tilde{\mathbf{z}})$  and  $(\hat{\mathbf{y}}, \hat{\mathbf{z}})$  are two distinct solutions, then  $\tilde{\mathbf{z}} \neq \hat{\mathbf{z}}$ .

*Proof.* From Proposition 2 and (17), it follows that any solution  $(\mathbf{y}, \mathbf{z})$  satisfies

$$\mathbf{C}_f^t \mathbf{y}_0 = \begin{pmatrix} y_{n,1} \\ \vdots \\ y_{n,r_2} \end{pmatrix} = \mathbf{C}_f^{\text{wt}(\mathbf{z})} \mathbf{y}_0,$$

which implies  $\text{ord}(f) \mid |t - \text{wt}(\mathbf{z})|$ . Since  $f$  is primitive, we obtain

$$\text{ord}(f) = (q^{r_1})^{r_2} - 1 \geq q^m - 1 > \max(t, n - t).$$

On the other hand,  $0 \leq \text{wt}(\mathbf{z}) \leq n$ , hence  $|t - \text{wt}(\mathbf{z})| \leq \min(t, n - t)$ . Therefore, the only way  $\text{ord}(f)$  can divide  $|t - \text{wt}(\mathbf{z})|$ , is that  $|t - \text{wt}(\mathbf{z})| = 0$ , i.e.  $\text{wt}(\mathbf{z}) = t$ .

Substituting  $\mathbf{z}$  in (15) uniquely determines all the values  $y_{1,1}, \dots, y_{1,r_2}$  by linear equations of the form  $y_{1,i} = c_i$ . Moreover, substituting  $y_{j-1,1}, \dots, y_{j-1,r_2}$  in (16) recursively determines all the values  $y_{j,1}, \dots, y_{j,r_2}$  in a similar manner. Therefore, if  $\tilde{\mathbf{z}} = \hat{\mathbf{z}}$  are the projections over the last  $n$  coordinate of two solutions, then also  $(\tilde{\mathbf{y}}, \tilde{\mathbf{z}}) = (\hat{\mathbf{y}}, \hat{\mathbf{z}})$ , which concludes the proof. □

**Field equations.** The field equations concern only the  $X$  part of the variables.

– *Field equations.* The equations are obtained from the  $n$  polynomials

$$\{x_j^q - x_j \mid j = 1, \dots, n\}. \quad (18)$$

Indeed,  $\mathbf{z}$  already lies over  $\{0, 1\}^n$  because of the support constraint equations (and (18)), while (15) and (16) force  $Y$  to lie over  $\mathbb{F}_{q^{r_1}}$ .

## 6.2 The Modelings

We are finally ready to describe the algebraic systems over  $\mathbb{F}_{q^{r_1}}[X, Y, Z]$  for Problems 2 and 1 and prove their correctness.

**Modeling 3 (Modeling for the SDP over  $\mathbb{F}_q$ )** *Given an instance  $(\mathbf{H}, \mathbf{s}, t)$  of Problem 1 over  $\mathbb{F}_q$ , Modeling 3 is the union of the sets of polynomials (2), (11), (15), (16), (17) and (18).*

**Modeling 4 (Modeling for the ESDP over  $\mathbb{F}_q$ )** *Given an instance  $(\mathbf{H}, \mathbf{s}, t)$  of Problem 2 over  $\mathbb{F}_q$ , Modeling 4 is the union of the sets of polynomials (2), (12), (15), (16), (17) and (18).*

As already said, finite field equations cannot be efficiently taken into account when dealing with large fields. In the exact weight syndrome decoding modeling, the support constraint equations are high-degree as well, so the problem would persist. On the other hand, it becomes convenient to remove the field equations in the bounded syndrome decoding problem. This leads to a new quadratic modeling.

**Modeling 5 (Quadratic modeling for the SDP over  $\mathbb{F}_q$ )** *Given an instance  $(\mathbf{H}, \mathbf{s}, t)$  of Problem 1 over  $\mathbb{F}_q$ , Modeling 5 is the union of the sets of polynomials (2), (11), (15), (16), (17).*

In the next section we thoroughly investigate the effect of removing the field equations from Modeling 4. We find, that at least for the parameter choices interesting for cryptography, the solutions of our modeling without field equations still lie over  $\mathbb{F}_q$  with high probability.

Table 4 provides the number of variables and equations for the three modelings over  $\mathbb{F}_q$ .

	# Polynomials	# Variables	Degree
Modeling 3	$4n - k + nr_2 + r_2$	$n(r_2 + 2)$	$q$
Modeling 4	$3n - k + nr_2 + r_2$	$n(r_2 + 2)$	$q$
Modeling 5	$3n - k + nr_2 + r_2$	$n(r_2 + 2)$	2

**Table 4.** Number of equations, number of variables and maximum degree of the algebraic modelings over  $\mathbb{F}_{q^{r_1}}$ .

*Remark 9.* Since  $r_2$  can be chosen as at most  $m = \mathcal{O}(\log_q(n))$ , both the number of polynomials and variables are quasi-linear in the code-length  $n$  in all the three modelings, namely they are  $\mathcal{O}(\log_2(n))$ . At the cost of defining the system over  $\mathbb{F}_{q^{r_1}} = \mathbb{F}_{q^m}$ , these quantities become linear in  $n$ , as the choice  $r_2 = 1$  is possible.

The modelings above capture exactly the corresponding syndrome decoding problem variants.

**Theorem 3.** *Given an instance  $(\mathbf{H}, \mathbf{s}, t)$ ,*

1. *The vector  $(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is a solution of Modeling 3 if and only if  $\mathbf{x}$  is a solution of Problem 1 and  $\mathbf{x} \in \mathbb{F}_q$ ;*
2. *The vector  $(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is a solution of Modeling 4 if and only if  $\mathbf{x}$  is a solution of Problem 2 and  $\mathbf{x} \in \mathbb{F}_q$ ;*
3. *The vector  $(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is a solution of Modeling 5 if and only if  $\mathbf{x}$  is a solution of Problem 1 and  $\mathbf{x} \in \overline{\mathbb{F}_q}$ , where  $\overline{\mathbb{F}_q}$  denotes the algebraic closure of  $\mathbb{F}_q$ .*

*Proof.* Since the parity-check equations (2) belong to all three modelings, it remains to prove the conditions on the weight of  $\mathbf{x}$  and to determine the base field over the vector can lie.

*Proof of 1.* Modeling 3 contains the field equations, therefore  $\mathbf{x} \in \mathbb{F}_q^n$ . It has already been proved that (11) implies  $\text{wt}(\mathbf{x}) \leq \text{wt}(\mathbf{z})$ . By Corollary 2, (15), (16) and (17) imply that  $\text{wt}(\mathbf{z}) = t$ , hence  $\text{wt}(\mathbf{x}) \leq t$ .

*Proof of 2.* Modeling 4 contains the field equations, therefore  $\mathbf{x} \in \mathbb{F}_q^n$ . It has already been proved that (12) implies  $\text{wt}(\mathbf{x}) = \text{wt}(\mathbf{z})$ . By Corollary 2, (15), (16) and (17) imply that  $\text{wt}(\mathbf{z}) = t$ , hence  $\text{wt}(\mathbf{x}) = t$ .

*Proof of 3.* The proof is analogous to the proof of 1., with the only exception that Modeling 5 does not contain the field equations. Hence, the solutions of the system are all the vectors defined over the algebraic closure  $\overline{\mathbb{F}_q}$  that satisfy the parity-check equations and have weight at most  $t$ .  $\square$

### 6.3 The Dimension of the Variety Associated with Modeling 5

Unlike the modelings that include the field equations, Modeling 5 is not a priori associated with a zero-dimensional ideal. This represents the main drawback of Modeling 5 compared to Modeling 3. The zero-dimensional property is desirable because it is necessary for defining the degree of regularity and for applying the FGLM algorithm to convert the degrevlex Gröbner basis into a lex basis. While it is possible to convert non-zero dimensional ideals using methods such as Gröbner walk or others, the process may not be as straightforward [1, 19].

In this subsection, we analyze the dimension of the variety associated with the ideal corresponding to Modeling 5. We will explore the conditions under which the variety is zero-dimensional, as well as the probability of this occurring. We begin with the following reduction.

**Proposition 3.** *Let  $\mathbf{x} \in \mathbb{F}_q^n$  be a vector which is a solution of Problem 1 for a given instance  $(\mathbf{H}, \mathbf{s}, t)$ . In other words,  $\mathbf{x}$  satisfies  $\mathbf{H}\mathbf{x}^\top = \mathbf{s}^\top$  and  $\text{wt}(\mathbf{x}) \leq t$ . Then, there exist finitely many  $(\mathbf{y}, \mathbf{z})$  such that  $(\mathbf{x}, \mathbf{y}, \mathbf{z})$  is a solution of Modeling 5.*

*Proof.* Let us first consider a vector  $\mathbf{x}$  satisfying the parity-check equations and such that  $\text{wt}(\mathbf{x}) = t$ . Then, in Modeling 5, the  $z_i$  must detect exactly the support of  $\mathbf{x}$ , and  $\mathbf{x}$  uniquely determines a solution  $(\mathbf{x}, \mathbf{y}, \mathbf{z})$  of the system. If instead  $\text{wt}(\mathbf{x}) = \bar{t} < t$ , then there exist  $t - \bar{t}$  indexes where the  $Z$  variables can have value 1 while  $\mathbf{x}_i = 0$ . Thus, for any solution  $\bar{\mathbf{x}} \in \mathbb{F}_q^n$  of the parity check matrix of weight  $\bar{t}$ , there exist

$$\binom{n - \bar{t}}{t - \bar{t}}$$

different solutions  $(\bar{\mathbf{x}}, \mathbf{y}, \mathbf{z})$ .

A special case is given by the codeword finding problem, i.e. where the syndrome  $\mathbf{s}$  is the zero vector. Here the the null vector is a solution of Problem 1 and leads to  $\binom{n}{t}$  solutions, thus likely increasing a lot the solving degree and the cost of the Gröbner basis computation. We can get rid of all these solutions by fixing one variable  $z_i = 1$ , thus forcing any solution to have weight at least 1 and removing the null vector. If the target solution has weight  $t$ , then the guess has success with probability  $t/n$ . We will discuss this strategy in more detail at the end of this subsection.  $\square$

Proposition 3 implies that each solution to the decoding problem (Problem 1) corresponds to a finite number of solutions for Modeling 5. This allows us to conduct an analysis that is independent of the specific modeling, as long as it accurately encodes the decoding problem in the sense of Theorem 3. Therefore, we will focus on the Krull dimension of the solution set of Problem 1 and provide a probability estimate for this dimension being zero.

First, in the following remark we briefly collect the definition of Krull dimension and some important properties we will use in the sequel. Expanded details and proofs can be found e.g. in [21, §4, Chapter 9] or other standard references in commutative algebra and algebraic geometry.

*Remark 10 (Krull dimension).* Let  $\mathbb{K}$  be an algebraically closed field (we will apply the following definitions and results to  $\mathbb{K} = \overline{\mathbb{F}_q}$ ). An affine variety  $V$  is the zero locus in  $\mathbb{K}^m$  of a proper ideal  $I$  of the polynomial ring  $\mathbb{K}[x_1, \dots, x_m]$ . We say that  $V$  is irreducible if it is not possible to write  $V = V_1 \cup V_2$  where  $V_1, V_2 \subsetneq V$  are two proper subvarieties. Irreducibility of  $V$  is equivalent to the corresponding ideal  $I$  being prime. The *Krull dimension* or simply the dimension of a variety  $V$  is defined as the maximal length  $d$  of the chains  $V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_d$ , of distinct nonempty irreducible subvarieties of  $V$ . This is also equivalent to the supremum of the lengths of all chains of prime ideals containing the defining ideal  $I$  of  $V$ . For example, the Krull dimension of an affine linear space  $\mathcal{L}$  generated by  $a$  linearly independent affine linear polynomials  $L_1, \dots, L_a$  is precisely  $m - a$ . This can be seen by completing the polynomials to a maximal linearly independent system of  $m$  equations (in  $m$  variables)  $L_1, \dots, L_a, L_{a+1}, \dots, L_m$  and then considering the following maximal chain of prime ideals

$$\mathcal{L} = \langle L_1, \dots, L_a \rangle \subsetneq \langle L_1, \dots, L_a, L_{a+1} \rangle \subsetneq \dots \subsetneq \langle L_1, \dots, L_m \rangle.$$



Notice that each ideal in this chain is prime, being generated by linearly independent polynomials of degree 1. Finally, we mention that, thanks to the Noetherian property of the polynomial ring, a variety  $V$  can be written uniquely as the union of irreducible varieties, which are called the irreducible components of  $V$ . Thus, the dimension of  $V$  coincides with the largest of the dimensions of its irreducible components (see [21, §4, Chapter 9, Corollary 9]).

Let  $S \subseteq [n]$ . Given a matrix  $\mathbf{H}$  with  $n$  columns and a vector  $\mathbf{x} \in \mathbb{F}_q^n$ , we denote by  $\mathbf{H}_S$  the submatrix of  $\mathbf{H}$  of columns indexed by  $S$  and by  $\mathbf{x}_S \in \mathbb{F}_q^{|S|}$  the vector obtained by deleting the coordinates corresponding to  $[n] \setminus S$  from  $\mathbf{x} \in \mathbb{F}_q^n$ . On the contrary, let  $\text{pad}_S(\mathbf{x}) \in \mathbb{F}_q^n$  be the vector obtained from  $\mathbf{x} \in \mathbb{F}_q^{|S|}$  by padding with 0's the positions corresponding to  $[n] \setminus S$ .

**Proposition 4.** *Let  $\mathcal{C}$  be an  $[n, k]$  code with parity-check matrix  $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ . Then the set of solutions of the Problem 1 with target weight  $t$  and syndrome  $\mathbf{s}$  for the code  $\mathcal{C}$  is the finite union of irreducible components, namely*

$$\bigcup_{S \subseteq [n], |S|=t} \{\text{pad}_S(\mathbf{x}) \in \mathbb{F}_q^n \mid \mathbf{H}_S \mathbf{x} = \mathbf{s}\}.$$

*Proof.* For any  $S$  of cardinality  $t$ ,  $\text{wt}(\text{pad}_S(\mathbf{x})) = \text{wt}(\mathbf{x}) \leq t$  and  $\mathbf{H} \cdot \text{pad}_S(\mathbf{x}) = \mathbf{H}_S \mathbf{x} = \mathbf{s}$ . Thus, the set of solutions of the decoding problem contains

$$\bigcup_{S \subseteq [n], |S|=t} \{\text{pad}_S(\mathbf{x}) \in \mathbb{F}_q^n \mid \mathbf{H}_S \mathbf{x} = \mathbf{s}\}.$$

On the other hand, for any solution  $\mathbf{x} \in \mathbb{F}_q^n$  to the decoding problem, let  $S$  be a set of cardinality  $t$  containing the support of  $\mathbf{x}$ . Then,  $\mathbf{x} \in \{\text{pad}_S(\mathbf{x}) \in \mathbb{F}_q^n \mid \mathbf{H}_S \mathbf{x} = \mathbf{s}\}$ . Finally, all the sets  $\{\text{pad}_S(\mathbf{x}) \in \mathbb{F}_q^n \mid \mathbf{H}_S \mathbf{x} = \mathbf{s}\}$  are irreducible being linear subspaces.  $\square$

The next proposition characterizes the dimension of the irreducible components of the set of solutions of the decoding problem and the finite field extension over which solutions are defined.

**Proposition 5.** *The Krull dimension of the solution set of Problem 1 with target weight  $t$  and syndrome  $\mathbf{s}$  for the linear code with parity-check matrix  $\mathbf{H}$  is*

$$t - \min\{\text{rk}(\mathbf{H}_S) \mid S \subseteq [n], |S| = t, \text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S)\}. \quad (19)$$

Moreover, if the dimension is 0, then all solutions lie over  $\mathbb{F}_q$ .

*Proof.* Let us fix the support  $S$  of  $t$  possible error positions. By Remark 10, the Krull dimension of the irreducible components coincides with their dimensions as vector spaces. The case study of the set of solutions of

$$\mathbf{H}_S \mathbf{x} = \mathbf{s},$$

seen as a variety, thus becomes the following:

- If  $t > n - k$ :
  - if  $\text{rk}(\mathbf{H}_S) = n - k \Rightarrow$  the variety has dimension  $t - n + k$ ;
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S) < n - k \Rightarrow$  the variety has dimension  $t - \text{rk}(\mathbf{H}_S)$ ;
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) > \text{rk}(\mathbf{H}_S) < n - k \Rightarrow$  the variety is empty;
- If  $t = n - k$ :
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S) = t \Rightarrow$  the variety has a unique element, and it belongs to  $\mathbb{F}_q^n$ ;
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) > \text{rk}(\mathbf{H}_S) = t \Rightarrow$  the variety is empty;
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S) < t \Rightarrow$  the variety has dimension  $t - \text{rk}(\mathbf{H}_S)$ ;
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) > \text{rk}(\mathbf{H}_S) < t \Rightarrow$  the variety is empty;
- If  $t < n - k$ :
  - if  $\text{rk}(\mathbf{H}_S) = t \Rightarrow$  the variety has a unique element, and it belongs to  $\mathbb{F}_q$ ;
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S) < t \Rightarrow$  the variety has dimension  $t - \text{rk}(\mathbf{H}_S)$ ;
  - if  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) > \text{rk}(\mathbf{H}_S) < t \Rightarrow$  the variety is empty.

We observe that the solution vector  $\mathbf{x}$  can have 0 entries, i.e. a weight smaller than  $t$ . This will increase the solutions of the algebraic system but not the dimension of the variety. Therefore, by Remark 10, the dimension of the solutions set is obtained as the maximum dimension over all the irreducible components corresponding to some  $S$  for which  $\text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S)$ :

$$\begin{aligned} & \max\{t - \text{rk}(\mathbf{H}_S) \mid S \subseteq [n], |S| = t, \text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S)\} \\ & = t - \min\{\text{rk}(\mathbf{H}_S) \mid S \subseteq [n], |S| = t, \text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S)\}. \end{aligned}$$

Let us now consider the case of a zero-dimensional ideal. Then for any choice of  $S$ , there is at most a solution and it must belong to  $\mathbb{F}_q^n$ . Hence, all solutions belong to  $\mathbb{F}_q^n$ .  $\square$

**Corollary 3.** *The dimension of the variety associated with Modeling 5 is*

$$t - \min\{\text{rk}(\mathbf{H}_S) \mid S \subseteq [n], |S| = t, \text{rk}((\mathbf{H}_S \mid \mathbf{s})) = \text{rk}(\mathbf{H}_S)\}. \quad (20)$$

*Proof.* It readily follows from Propositions 10 and 5 and the fact that each solution of Problem 1 corresponds to a finite number of solutions of Modeling 5.  $\square$

For relevant and not too-small parameters, we usually have  $t \ll n - k$ . Assuming the weight distribution of a linear code follows closely the Bernoulli one, we can estimate the probability that the ideal is zero-dimensional, and thus, by exploiting the proof of Proposition 5, that all the solutions  $\mathbf{x}$  lie over  $\mathbb{F}_q$ .

**Proposition 6.** *Let  $\mathcal{C}$  be an  $\mathbb{F}_q$ -linear code and let  $W_i(\mathcal{C})$  the number of codewords of weight exactly  $i$  in  $\mathcal{C}$ . Then the probability that Modeling 5 provides a variety of strictly positive dimension when  $t < n - k$  is upper bounded by*

$$\sum_{i=1}^t W_i(\mathcal{C}) \left( \frac{1}{q^{n-k-i+1}} + \binom{n-i}{t-i} \left( \frac{1}{q^{n-k-t+1}} - \frac{1}{q^{n-k-i+1}} \right) \right)$$

for a randomly sampled syndrome. For the codeword finding problem, the same probability is upper bounded by

$$\sum_{i=1}^t W_i(\mathcal{C}) \binom{n-i}{t-i}.$$

*Proof.* The parity-check matrix  $\mathbf{H}$  has  $i$  linearly dependent columns indexed by the set  $S$  iff the corresponding code  $\mathcal{C}$  has a codeword of weight  $\leq i$  with support contained in  $S$ . Hence any codeword of positive weight  $i \leq t$  with support  $S'$  identifies a set of  $\binom{n-i}{t-i}$  supersets  $S \supseteq S'$ . For each of such  $S$ , the inequality  $\text{rk}(H_S) < i + (t - i) = t$  holds. If the syndrome  $\mathbf{s} \in \mathbb{F}_q^{n-k}$  is sampled at random, then it belongs to the column space of  $S'$  with probability  $\frac{1}{q^{n-k-i+1}}$ . Otherwise, for any of the  $\binom{n-i}{t-i}$  possible choices of  $S$ , the probability that  $\mathbf{s}$  lies in the column space of  $\mathbf{H}_S$  but not in that of  $\mathbf{H}_{S'}$  is  $\frac{1}{q^{n-k-t+1}} - \frac{1}{q^{n-k-i+1}}$ . Let  $W_i(\mathcal{C})$  be the number of codewords in  $\mathcal{C}$  of weight exactly  $i$ . By summing the probabilities of the two mutually disjoint events and from the proof of Proposition 5, we can thus upper bound the probability that the ideal is positive-dimensional for a random syndrome as

$$\sum_{i=1}^t W_i(\mathcal{C}) \left( \frac{1}{q^{n-k-i+1}} + \binom{n-i}{t-i} \left( \frac{1}{q^{n-k-t+1}} - \frac{1}{q^{n-k-i+1}} \right) \right).$$

In the case of the codeword finding problem, i.e. if the syndrome is the zero vector, then the upper bound on the sought probability simplifies to

$$\sum_{i=1}^t W_i(\mathcal{C}) \binom{n-i}{t-i},$$

since the zero vector syndrome belongs to any column space.  $\square$

*Remark 11.* For random codes, the weight distribution follows closely the Bernoulli one, i.e.  $W_i(\mathcal{C}) \approx \frac{\binom{n}{i}(q-1)^i}{q^{n-k}}$ . Under this assumption, the probability of having a zero-dimensional ideal for the decoding modeling with a random syndrome can be estimated as

$$\frac{1}{q^{n-k}} \sum_{i=1}^t \binom{n}{i} (q-1)^i \left( \frac{1}{q^{n-k-i+1}} + \binom{n-i}{t-i} \left( \frac{1}{q^{n-k-t+1}} - \frac{1}{q^{n-k-i+1}} \right) \right),$$

while for the codeword finding problem as

$$\frac{1}{q^{n-k}} \sum_{i=1}^t \binom{n}{i} \binom{n-i}{t-i} (q-1)^i.$$

We remark in particular that the bound is independent from the choice of  $(r_1, r_2)$ . Different admissible pairs provide of course different solutions, but the projections of the varieties with respect to the  $x_i$ 's variables are the same over the field closure, which is what determines the dimension of the associated ideals.

In Appendix A, Tables 6 and 7, we provide examples of such bounds for concrete parameters. In the case of syndrome decoding, these probabilities are very small even at Gilbert-Varshamov distance and the issue of having ideals of positive dimension is thus absolutely negligible for the purpose of cryptanalysis. On the opposite, the bound on the probability of the same event for the codeword finding problem becomes completely useless when approaching the Gilbert-Varshamov distance. Indeed, the trivial upper bound “ $\mathbb{P} \leq 1$ ” entries from the two tables mean that the bound given by Proposition 6 gives a number larger than 1. A possible workaround for the described issue with the codeword finding version is to make use of hybrid methods. Indeed, it is enough to guess a number of nonzero positions equal or greater than the ideal dimension to decrease the latter to 0 with high probability. Recalling that the solution space is projective and one the value of one nonzero entry can be chosen arbitrarily, specializing  $l$  coordinates has a success probability of  $\frac{\binom{n-l}{t-l}}{\binom{n}{t}(q-1)^{l-1}}$ . In cryptanalysis, however, it is usually assumed to know the minimal weight of a (nonzero) solution. This is because, if there exists a solution of weight smaller than the target, then the challenge is actually easier. The next corollary thus implies a strategy to obtain a zero-dimensional ideal in this setting. If we suppose to know a lower bound  $d'$  the minimum distance  $d(C)$  of the code, then it means that any  $d' - 1$  columns of the parity-check matrix  $\mathbf{H}$  are linearly independent. Therefore, Equation (19) implies that the dimension of the ideal for the bounded weight modeling with target weight  $d'$  is exactly 1 and thus it is enough to specialize one variable  $x_i$  to any element in  $\mathbb{F}_q$  to obtain a zero-dimensional ideal.

#### 6.4 Experimental results.

We solved the quadratic system associated with Modeling 5 for several random codes. We show in Table 5 that, similarly to the case over  $\mathbb{F}_2$ , the solving degree is surprisingly small. MAGMA code used for our experiments with Modeling 5 can be found at [this link](#).

## 7 Conclusion and Future Directions

We have presented a new algebraic cryptanalysis for both the bounded and the exact versions of the Syndrome Decoding problem.

In the binary case, our modelings significantly improved the previous attempt of [33], by capturing the weight condition on the solution vector with quadratic polynomials. We have also experimentally shown that the behavior of the associated Gröbner basis is very different from that of a random system with the same number of variables and equations, *leading to a much better complexity*. We have thus taken an important step towards making algebraic algorithms potentially competitive for the decoding problem.

We introduced algebraic modelings for the first time in the case of the general syndrome decoding problem over larger finite fields. Notably, one of them is

$n$	$k$	$t$	#Lin	$q = 7$			$q = 16, 17$			$q = 127$									
				$r_1$	$r_2$	#Quad	#Vars	SD	$r_1$	$r_2$	#Quad	#Vars	SD	$r_1$	$r_2$	#Quad	#Vars	SD	
10	5	2	5	$m = 2$			$m = 1$			$m = 1$									
				2	1	30	30	4	1	1	30	30	4	1	1	30	30	4	
				1	2	40	40	3											
15	9	3	6	$m = 2$			$m = 1$			$m = 1$									
				2	1	45	45	4	1	1	45	45	4	1	1	45	45	4	
				1	2	60	60	4											
19	10	5	9	$m = 2$			$m = 1$			$m = 1$									
				2	1	57	57	5	1	1	57	57	5	1	1	57	57	5	
				1	2	76	76	4											
22	14	4	8	$m = 2$			$m = 2$			$m = 1$									
				2	1	66	66	5	2	1	66	66	5	1	1	66	66	4	
				1	2	88	88	4	1	2	88	88	4						
30	20	4	10	$m = 3$			$m = 2$			$m = 1$									
				3	1	90	90	$\geq 6$	2	1	90	90	$\geq 6$	1	1	90	90	$\geq 6$	
				2	2	120	120	4	1	2	120	120	5						
				1	3	150	150	4											

**Table 5.** This table gives information from experiments using random  $\mathbb{F}_q$ -linear codes using Modeling 5. The values in the SD column represent the highest step degree achieved when directly computing the Gröbner basis of the system in MAGMA. This is typically regarded as a proxy for the solving degree  $d_{\text{sol}}$ . The column “#lin” denotes the number of linear equations, i.e. of parity-check equations, which is independent from the field size. The columns “#quad” and “#vars” stand for the number of quadratic equations and the number of variables, which depend on the value  $r_2$  instead. The integer  $r_1$  is the extension field degree over which the equations are defined. We recall that the value  $m$  leads to different possible choices of  $(r_1, r_2)$  and we give all minima with respect to the standard partial order on pairs.

quadratic with a number of variables and equations that is linear or quasi-linear in the code length, *independently from the field size*. We have analyzed that, despite the constant degree of the equations involved, the system correctly solves the decoding problem and with high probability does not have spurious solutions for all parameters that are relevant to the problem.

An open question to this work is to understand more clearly the behavior of the Gröbner basis computation both in the binary and in the general finite field cases and to get a theoretical estimate of the complexity that better matches with the one obtained from the experiments. This is a difficult task, as it is often the case for very structured algebraic systems, and probably requires to develop dedicated tools to analyze such behavior.

Another interesting and natural follow-up to this work can be to analyze the impact of hybrid strategies on solving the proposed systems. Since the weight of the solution sought is relatively low, a convenient choice is to set most of the

variables of  $X$  to 0. It is not difficult to see that this approach is reminiscent of the guess part in Prange or later ISD algorithms.

In the case of binary systems, we have verified experimentally that the best hybrid trade-off actually boils down to the Prange algorithm, the best complexity being indeed obtained when enough zeros to linearize the system are guessed.

However, the system hides a lot of structure and offers many different ways to specialize variables. For example, the auxiliary variables from the vector  $\mathbf{y}$  can also be fixed and they too have different probabilities of taking a value equal to 0 or 1. It is therefore not at all unrealistic to speculate that an ad-hoc and smart hybridization technique may lead to a better trade-off than a fully combinatorial approach.

### Acknowledgments.

This publication was created with the co-financing of the European Union FSE-REACT-EU, PON Research and Innovation 2014-2020 DM1062/2021. A. Caminata is supported by the PRIN 2020 grant 2020355B8Y “Squarefree Gröbner degenerations, special varieties and related topics”, by the PRIN PNRR 2022 grant P2022J4HRR “Mathematical Primitives for Post Quantum Digital Signatures”, by the MUR Excellence Department Project awarded to Dipartimento di Matematica, Università di Genova, CUP D33C23001110001, and by the European Union within the program NextGenerationEU. A. Meneghetti acknowledges support from Ripple’s University Blockchain Research Initiative. A. Caminata and A. Meneghetti are members of the INdAM Research Group GNSAGA.

### References

1. Amrhein, B., Gloor, O., Küchlin, W.: On the walk. *Theoretical Computer Science* **187**(1), 179–202 (1997)
2. Aragon, N., Barreto, P., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Ghosh, S., Gueron, S., Güneysu, T., et al.: BIKE: bit flipping key encapsulation (2022)
3. Bardet, M.: Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie. Ph.D. thesis, Université Pierre et Marie Curie-Paris VI (2004)
4. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.P.: An algebraic attack on rank metric code-based cryptosystems. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 64–93. Springer (2020)
5. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D., Tillich, J., Verbel, J.A.: Improvements of algebraic attacks for solving the rank decoding and minrank problems. In: Moriai, S., Wang, H. (eds.) *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security*, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I. *Lecture Notes in Computer Science*, vol. 12491, pp. 507–536. Springer (2020)

6. Bardet, M., Faugere, J.C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving. pp. 71–74 (2004)
7. Becker, A., Joux, A., May, A., Meurer, A.: Decoding random binary linear codes in  $2^{n/20}$ : How  $1 + 1 = 0$  improves information set decoding. In: Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15–19, 2012. Proceedings 31. pp. 520–536. Springer (2012)
8. Berlekamp, E., McEliece, R., Van Tilborg, H.: On the inherent intractability of certain coding problems (corresp.). IEEE Transactions on Information theory **24**(3), 384–386 (1978)
9. Bernstein, D.J., Chou, T., Lange, T., von Maurich, I., Misoczki, R., Niederhagen, R., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., et al.: Classic McEliece: conservative code-based cryptography. fhal-04288769 (2017)
10. Bernstein, D.J., Lange, T., Peters, C.: Smaller decoding exponents: ball-collision decoding. In: Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14–18, 2011. Proceedings 31. pp. 743–760. Springer (2011)
11. Bigdeli, M., De Negri, E., Dizdarevic, M.M., Gorla, E., Minko, R., Tsakou, S.: Semi-regular sequences and other random systems of equations. Association for Women in Mathematics Series **24**, 75 – 114 (2021)
12. Both, L., May, A.: Decoding linear codes with high error rate and its impact for lpn security. In: International Conference on Post-Quantum Cryptography. pp. 25–46. Springer (2018)
13. Briaud, P., Øygarden, M.: A new algebraic approach to the regular syndrome decoding problem and implications for PCG constructions. In: EUROCRYPT (5). Lecture Notes in Computer Science, vol. 14008, pp. 391–422. Springer (2023)
14. Buchberger, B.: Bruno Buchberger’s PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symb. Comput. **41**(3–4), 475–511 (2006)
15. Caminata, A., Gorla, E.: Solving multivariate polynomial systems and an invariant from commutative algebra. In: Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 12542, pp. 3–36. Springer, Cham (2021)
16. Caminata, A., Gorla, E.: Solving degree, last fall degree, and related invariants. J. Symb. Comput. **114**, 322–335 (2023)
17. Carrier, K., Debris-Alazard, T., Meyer-Hilfiger, C., Tillich, J.P.: Statistical decoding 2.0: reducing decoding to lpn. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 477–507. Springer (2022)
18. Carrier, K., Debris-Alazard, T., Meyer-Hilfiger, C., Tillich, J.P.: Reduction from sparse lpn to lpn, dual attack 3.0. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 286–315. Springer (2024)
19. Collart, S., Kalkbrener, M., Mall, D.: Converting bases with the Gröbner walk. Journal of Symbolic Computation **24**(3), 465–469 (1997)
20. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Advances in cryptology—EUROCRYPT 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, pp. 392–407. Springer, Berlin (2000)
21. Cox, D., Little, J., O’Shea, D., Sweedler, M.: Ideals, Varieties, and Algorithms, vol. 3. Springer (1997)
22. Ding, J., Schmidt, D.: Solving degree and degree of regularity for polynomial systems over a finite fields. Lecture Notes in Computer Science **8260**, 34 – 49 (2013)

23. Dumer, I.: Two decoding algorithms for linear codes **25**(1), 17–23 (1989)
24. Faugère, J.C., Gianni, P., Lazard, D., Mora, T.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.* **16**(4), 329–344 (1993)
25. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases ( $F_4$ ). vol. 139, pp. 61–88 (1999), *effective methods in algebraic geometry* (Saint-Malo, 1998)
26. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero ( $F_5$ ). p. 75 – 83 (2002)
27. Finiasz, M., Sendrier, N.: Security bounds for the design of code-based cryptosystems. In: *Advances in Cryptology–ASIACRYPT 2009: 15th International Conference on the Theory and Application of Cryptology and Information Security*, Tokyo, Japan, December 6–10, 2009. *Proceedings 15*. pp. 88–105. Springer (2009)
28. Lidl, R., Niederreiter, H.: *Introduction to Finite Fields and their Applications*. Cambridge University Press, 2 edn. (1994)
29. May, A., Meurer, A., Thomae, E.: Decoding random linear codes in. In: *International Conference on the Theory and Application of Cryptology and Information Security*. pp. 107–124. Springer (2011)
30. May, A., Ozerov, I.: On computing nearest neighbors with applications to decoding of binary linear codes. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. pp. 203–228. Springer (2015)
31. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. *Coding Thv* **4244**, 114–116 (1978)
32. Melchor, C.A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Persichetti, E., Zémor, G., Bourges, I.: Hamming quasi-cyclic (hq). *NIST PQC Round 2*(4), 13 (2018)
33. Meneghetti, A., Pellegrini, A., Sala, M.: On the equivalence of two post-quantum cryptographic families. *Annali di Matematica Pura ed Applicata (1923 -)* **202**, 967–991 (2021)
34. Prange, E.: The use of information sets in decoding cyclic codes. *IRE Trans. Inf. Theory* **8**(5), 5–9 (1962)
35. Salizzoni, F.: An upper bound for the solving degree in terms of the degree of regularity. *arXiv:2304.13485* (2023)
36. Semaev, I., Tenti, A.: Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases. *Journal of Algebra* **565**, 651 – 674 (2021)
37. Stern, J.: A method for finding codewords of small weight. In: *Coding Theory and Applications: 3rd International Colloquium Toulon, France, November 2–4, 1988 Proceedings 3*. pp. 106–113. Springer (1989)



**A Section 6.3 Bounds on the zero-dimensionality**

	$t = \lfloor (d_{GV} - 1)/2 \rfloor$	$t = \lfloor (n - k)/2 \rfloor$	$t = d_{GV}$	$t = d_{GV} + 1$
$[100, 50]_2$	$t = 5,$ $\mathbb{P} \leq 2.32 \cdot 10^{-20}$	$t = 25,$ $\mathbb{P} \leq 1$	$t = 12,$ $\mathbb{P} \leq 6.73 \cdot 10^{-9}$	$t = 13,$ $\mathbb{P} \leq 1.84 \cdot 10^{-7}$
$[100, 50]_7$	$t = 12,$ $\mathbb{P} \leq 8.44 \cdot 10^{-51}$	$t = 25,$ $\mathbb{P} \leq 1.89 \cdot 10^{-20}$	$t = 25,$ $\mathbb{P} \leq 1.89 \cdot 10^{-20}$	$t = 26,$ $\mathbb{P} \leq 2.68 \cdot 10^{-18}$
$[100, 50]_{127}$	$t = 18,$ $\mathbb{P} \leq 5.48 \cdot 10^{-118}$	$t = 25,$ $\mathbb{P} \leq 1.23 \cdot 10^{-84}$	$t = 37,$ $\mathbb{P} \leq 5.38 \cdot 10^{-30}$	$t = 38,$ $\mathbb{P} \leq 1.44 \cdot 10^{-25}$
$[100, 80]_2$	$t = 1,$ $\mathbb{P} \leq 9.09 \cdot 10^{-11}$	$t = 10,$ $\mathbb{P} \leq 1$	$t = 4,$ $\mathbb{P} \leq 3.14 \cdot 10^{-4}$	$t = 5,$ $\mathbb{P} \leq 0.0268$
$[100, 80]_7$	$t = 3,$ $\mathbb{P} \leq 4.06 \cdot 10^{-25}$	$t = 10,$ $\mathbb{P} \leq 2.92 \cdot 10^{-5}$	$t = 8,$ $\mathbb{P} \leq 1.30 \cdot 10^{-10}$	$t = 9,$ $\mathbb{P} \leq 6.55 \cdot 10^{-8}$
$[100, 80]_{127}$	$t = 6,$ $\mathbb{P} \leq 1.16 \cdot 10^{-52}$	$t = 10,$ $\mathbb{P} \leq 1.14 \cdot 10^{-31}$	$t = 13,$ $\mathbb{P} \leq 1.97 \cdot 10^{-16}$	$t = 14,$ $\mathbb{P} \leq 1.97 \cdot 10^{-11}$
$[1000, 500]_2$	$t = 55,$ $\mathbb{P} \leq 1.05 \cdot 10^{-177}$	$t = 250,$ $\mathbb{P} \leq 1$	$t = 112,$ $\mathbb{P} \leq 9.96 \cdot 10^{-84}$	$t = 113,$ $\mathbb{P} \leq 3.13 \cdot 10^{-82}$
$[1000, 500]_7$	$t = 119,$ $\mathbb{P} \leq 1.85 \cdot 10^{-488}$	$t = 250,$ $\mathbb{P} \leq 1.95 \cdot 10^{-181}$	$t = 239,$ $\mathbb{P} \leq 2.06 \cdot 10^{-205}$	$t = 240,$ $\mathbb{P} \leq 3.20 \cdot 10^{-203}$
$[1000, 500]_{127}$	$t = 182,$ $\mathbb{P} \leq 2.66 \cdot 10^{-1136}$	$t = 250,$ $\mathbb{P} \leq 4.75 \cdot 10^{-812}$	$t = 366,$ $\mathbb{P} \leq 5.44 \cdot 10^{-283}$	$t = 367,$ $\mathbb{P} \leq 1.52 \cdot 10^{-278}$
$[1000, 800]_2$	$t = 16,$ $\mathbb{P} \leq 1.41 \cdot 10^{-79}$	$t = 100,$ $\mathbb{P} \leq 1$	$t = 32,$ $\mathbb{P} \leq 8.22 \cdot 10^{-42}$	$t = 33,$ $\mathbb{P} \leq 9.65 \cdot 10^{-40}$
$[1000, 800]_7$	$t = 36,$ $\mathbb{P} \leq 1.30 \cdot 10^{-212}$	$t = 100,$ $\mathbb{P} \leq 8.72 \cdot 10^{-31}$	$t = 74,$ $\mathbb{P} \leq 2.94 \cdot 10^{-101}$	$t = 75,$ $\mathbb{P} \leq 1.78 \cdot 10^{-98}$
$[1000, 800]_{127}$	$t = 61,$ $\mathbb{P} \leq 3.32 \cdot 10^{-489}$	$t = 100,$ $\mathbb{P} \leq 8.70 \cdot 10^{-284}$	$t = 124,$ $\mathbb{P} \leq 3.03 \cdot 10^{-161}$	$t = 125,$ $\mathbb{P} \leq 3.43 \cdot 10^{-156}$

**Table 6.** Bound on the probability  $\mathbb{P}$  that the ideal associated with the system has a strictly positive dimension for the decoding problem with a randomly sampled syndrome.

	$t = \lfloor (d_{GV} - 1)/2 \rfloor$	$t = \lfloor (n - k)/2 \rfloor$	$t = d_{GV} - 2$	$t = d_{GV} - 1$	$t = d_{GV}$
$[100, 50]_2$	$t = 5,$ $\mathbb{P} \leq 2.07 \cdot 10^{-6}$	$t = 25,$ $\mathbb{P} \leq 1$	$t = 10,$ $\mathbb{P} \leq 1$	$t = 11,$ $\mathbb{P} \leq 1$	$t = 12,$ $\mathbb{P} \leq 1$
$[100, 50]_7$	$t = 12,$ $\mathbb{P} \leq 8.08 \cdot 10^{-18}$	$t = 25,$ $\mathbb{P} \leq 1$	$t = 23,$ $\mathbb{P} \leq 0.378$	$t = 24,$ $\mathbb{P} \leq 1$	$t = 25,$ $\mathbb{P} \leq 1$
$[100, 50]_{127}$	$t = 18,$ $\mathbb{P} \leq 1.46 \cdot 10^{-48}$	$t = 25,$ $\mathbb{P} \leq 6.16 \cdot 10^{-30}$	$t = 35,$ $\mathbb{P} \leq 3.04 \cdot 10^{-5}$	$t = 36,$ $\mathbb{P} \leq 0.00696$	$t = 37,$ $\mathbb{P} \leq 1$
$[100, 80]_2$	$t = 1,$ $\mathbb{P} \leq 9.54 \cdot 10^{-5}$	$t = 10,$ $\mathbb{P} \leq 1$	$t = 2,$ $\mathbb{P} \leq 0.0142$	$t = 3,$ $\mathbb{P} \leq 1$	$t = 4,$ $\mathbb{P} \leq 1$
$[100, 80]_7$	$t = 3,$ $\mathbb{P} \leq 6.93 \cdot 10^{-10}$	$t = 10,$ $\mathbb{P} \leq 1$	$t = 6,$ $\mathbb{P} \leq 0.00176$	$t = 7,$ $\mathbb{P} \leq 0.165$	$t = 8,$ $\mathbb{P} \leq 1$
$[100, 80]_{127}$	$t = 6,$ $\mathbb{P} \leq 4.20 \cdot 10^{-21}$	$t = 10,$ $\mathbb{P} \leq 1.59 \cdot 10^{-8}$	$t = 11,$ $\mathbb{P} \leq 1.65 \cdot 10^{-5}$	$t = 12,$ $\mathbb{P} \leq 0.0155$	$t = 13,$ $\mathbb{P} \leq 1$
$[1000, 500]_2$	$t = 55,$ $\mathbb{P} \leq 1.91 \cdot 10^{-43}$	$t = 250,$ $\mathbb{P} \leq 1$	$t = 110,$ $\mathbb{P} \leq 1$	$t = 111,$ $\mathbb{P} \leq 1$	$t = 112,$ $\mathbb{P} \leq 1$
$[1000, 500]_7$	$t = 120,$ $\mathbb{P} \leq 1.24 \cdot 10^{-165}$	$t = 250,$ $\mathbb{P} \leq 1$	$t = 237,$ $\mathbb{P} \leq 1$	$t = 238,$ $\mathbb{P} \leq 1$	$t = 239,$ $\mathbb{P} \leq 1$
$[1000, 500]_{127}$	$t = 182,$ $\mathbb{P} \leq 3.46 \cdot 10^{-463}$	$t = 250,$ $\mathbb{P} \leq 5.40 \cdot 10^{-284}$	$t = 364,$ $\mathbb{P} \leq 0.00115$	$t = 365,$ $\mathbb{P} \leq 0.255$	$t = 366,$ $\mathbb{P} \leq 1$
$[1000, 800]_2$	$t = 15,$ $\mathbb{P} \leq 1.40 \cdot 10^{-23}$	$t = 100,$ $\mathbb{P} \leq 1$	$t = 30,$ $\mathbb{P} \leq 1$	$t = 31,$ $\mathbb{P} \leq 1$	$t = 32,$ $\mathbb{P} \leq 1$
$[1000, 800]_7$	$t = 36,$ $\mathbb{P} \leq 3.60 \cdot 10^{-73}$	$t = 100,$ $\mathbb{P} \leq 1$	$t = 72,$ $\mathbb{P} \leq 1$	$t = 73,$ $\mathbb{P} \leq 1$	$t = 74,$ $\mathbb{P} \leq 1$
$[1000, 800]_{127}$	$t = 61,$ $\mathbb{P} \leq 1.13 \cdot 10^{-194}$	$t = 100,$ $\mathbb{P} \leq 2.66 \cdot 10^{-71}$	$t = 122,$ $\mathbb{P} \leq 3.67 \cdot 10^{-5}$	$t = 123,$ $\mathbb{P} \leq 0.0333$	$t = 124,$ $\mathbb{P} \leq 1$

**Table 7.** Bound on the probability  $\mathbb{P}$  that the ideal associated with the system has strictly positive dimension for the codeword finding problem (i.e. with null syndrome).