Security Analysis on UOV Families with Odd Characteristics: Using Symmetric Algebra

Yi Jin[1], Yuansheng Pan[1], Xiaoou He[1], Boru Gong[1], and Jintai Ding[2]

[1] CCB Fintech Ltd.
[2] Xi'an Jiaotong-Liverpool University

Abstract UOV and its variants have been submitted to NIST's PQC Standardization Project. And security analysis against UOV families (*i.e.*, UOV and its variants) are typically categorized into key-recovery attacks and forgery attacks, with the XL algorithm serving as one of the most significant methods for mounting key-recovery attacks. Recently, Lars Ran introduced a novel key-recovery attack against UOV families that could be seen as an XL attack using exterior algebra; nevertheless, this new XL attack is applicable only when the underlying (finite) field of UOV instances is of characteristic 2.

In this work, we address this limitation by generalizing Lars Ran's approach, and our contributions are three-fold. First, we generalize the notion of exterior algebra and propose the notion of *reduced symmetric algebra* over *any* field, which is essentially symmetric algebra when the characteristic p of the underlying field is 0 and is exterior algebra when $p = 2$. Moreover, based upon the reduced symmetric algebra, we propose a new XL attack against *all* UOV families: as a generalization of Lars Ran's attack, our XL attack also works for those UOV instances with *odd* characteristic; for instance, it works for those 12 recommended QR-UOV instances submitted to NIST's PQC Standardization Project, although its performance does not outperform those of the existing key-recovery attacks. Finally, analysis on our XL attack reveals the connection between the characteristic p and the concrete hardness of UOV instances.

Keywords: MPKC · UOV · XL Algorithm · Symmetric Algebra

1 Introduction

Digital signature schemes are fundamental to cybersecurity, as it provides authenticity, integrity, and non-repudiation for digital communications. Classic digital signature schemes are usually based on the hardness of certain problems in number theory, and they have played a very important role in network security work for decades. Moreover, the emergence of quantum computing has intensified research into post-quantum cryptography (PQC), particularly following Shor's algorithm [22], which threatens traditional cryptographic systems. As such, NIST launched the PQC Standardization Project in the 2010s, aiming to standardize quantum-resistant algorithms. Recently, NIST issued a call for additional digital signature proposals to be considered in the PQC standardization process in September 2022 [16], with

primary interest in additional general-purpose signature schemes that are not based on structured lattices; for certain applications, NIST is also interested in signature schemes that have short signatures and fast verification speed.

1.1 UOV and its variants

The multivariate public key cryptosystems (MPKC) are a family of candidate post quantum cryptographic schemes that usually have short signatures and fast verification speed, and the security of these cryptosystems in MPKC are firmly connected to the computational hardness of solving multivariate polynomial equation systems, The idea of MPKC dates back to 1980s, and many leading cryptographers (Ong, Schnorr, Matsumoto, Imai, Harashima, Diffie, Fell, Miyagawa, Tsujii, Kurosawa, Fujioka and others) built various types of MPKCs. Compared with other types of post-quantum counterparts, multivariate-based digital signature schemes (*e.g.*, UOV and its variants) usually offer signatures whose lengths are comparable to those classic ones.

The Unbalanced Oil and Vinegar (UOV) digital signature scheme was first proposed in 1999 [18]. It leverages the hash-and-sign paradigm underpinned by a trapdoored multivariate quadratic map. Its origin could be traced back to Patarin's groundbreaking linearization equations attack [17] in 1995 against the Matsumoto-Imai cryptosystem [15]. Following this innovative stride, Patarin ingeniously repurposed the attack's underlying principle into the design of the Oil and Vinegar signature scheme (OV) [18] in 1997. However, an invariant subspace attack [14] cracked the *balanced* version of this scheme in 1998. And Kipnis, Patarin, and Goubin promptly introduced the original UOV. Please refer to [9] for more information on UOV. Over two decades, UOV has withstood rigorous cryptanalytic scrutiny, which validates its robust security and consistent reliability.

As a classic multivariate-based scheme, UOV has garnered significant attention over the past decades. And researchers have proposed variants of UOV to improve its efficiency and security properties. Notable examples include MAYO [5], QR-UOV [13], SNOVA [25]. These variants, along with the original UOV scheme, were submitted to NIST's PQC Project in response to the call for additional digital signature schemes. All four candidates successfully advanced to the second round of the PQC process.

1.2 Previous works

Security analysis against UOV families (*i.e.*, UOV and its variants) is usually carried out by listing all the known critical attacks that may influence its concrete hardness estimation result. Historically, those attacks are usually classified into two types: (1) the *key-recovery attacks* that aim to recover the secret key from the given public key, *e.g.*, the Kipnis-Shamir attack [14], the intersection attack [3] and the MinRank attack [24, 1, 23]; (2) the *forgery attacks* that aim to forge a message/signature pair passing the verification test, *e.g.*, the collision attacks against the hash function, and the direct attack. It is worth to noticed that XL algorithm is an important methods which often used in most attacks of UOV.

Recently, Lars Ran [20] proposed a new XL variant that aims to conduct the key-recovery attack against UOV instances whose underlying (finite) fields are of characteristic $p = 2$. This XL attack is based on the observation that when $p = 2$, the public key of a UOV instance

in polar form could be seen as a specific subspace of an exterior algebra. Although the XL attack in [20] outperforms those existing key-recovery attacks in terms of many recommended instances of UOV [6], MAYO [5] and SNOVA [25], it is not applicable to QR-UOV [13] due to its constraint on the characteristic, *i.e.*, $p = 2$.

1.3 Contributions in this work

Our work is motivated by the observation that by employing different algebraic structures, XL attacks usually exhibit varying computational efficiencies. With this observation in mind, we generalize Lars Ran's XL attack [20], and conduct a further security analysis against UOV families (*i.e.*, UOV and its variants). Our contribution in this work is three-fold, as the following indicates.

First and foremost, we propose a new algebra, *i.e.*, the reduced symmetric algebra, over *any* field of characteristic p. This new algebra could be seen as a natural generalization of the exterior algebra used in Lars Ran's XL attack [20]. The strength of this new algebra lies in the facts: (1) when $p = 0$, this algebra is essentially the symmetric algebra; (2) when $p = 2$, this algebra is essentially the exterior algebra; (3) what interests us most is that this algebra is also well-defined for every *odd* characteristic p. This new algebra may be of independent interest in the realm of commutative algebra. Please refer to Section 3 for full details.

Moreover, we construct a new XL attack by fully utilizing the properties of the reduced symmetric algebra, and it is essentially a key-recovery attack against *all* UOV instances. On the one hand, when $p = 2$, our XL attack is equivalent to Lars Ran's XL attack [20]. On the other hand, compared with Lars Ran's XL attack in [20], the strength of our XL attack lies in the fact it is also applicable to UOV instances with *odd* characteristics, *e.g.*, those recommended QR-UOV instances [13]. Please refer to Sections 4 and 5 for full details.

Our final contribution lies in the connection between the characteristic p of the underlying field $\Bbbk$ in a UOV instance and the concrete hardness of that UOV instance. Previous works in MPKC show that for a UOV instance, the order q of its underlying (finite) field $\Bbbk$ is firmly connected to its concrete hardness, and a larger order usually results in a more secure UOV instance, *provided other parameters remain unchanged*; however, the characteristic $p = \mathsf{char}(\Bbbk)$ was usually not taken into the consideration of the concrete hardness analysis of UOV in the past. In contrast, our analysis in Section 5 shows that our XL attack runs faster when the characteristic p of the underlying field $\Bbbk$ of UOV gets smaller. Conversely, this implies that choosing a larger characteristic p may help increase the (concrete) hardness of UOV; for instance, a UOV instance with $\Bbbk = \mathbb{F}_{79}$ is, in general, more secure than a similar UOV instance with $\Bbbk = \mathbb{F}_{81}$. Please refer to Section 5 for full details.

1.4 Organization of this work

The work is organized as follows. Section 2 specifies the notations/conventions used in this work, as well as some preliminary definitions/arguments in MPKC and algebra. In Section 3 a new algebra, *i.e.*, the p-reduced symmetric algebra, is defined that can reveal the hidden structure in UOV problem and could be seen as a generalization of the exterior algebra used in Lars Ran's attack [20]. In Section 4, we first reformulate the UOV problem, and then construct our extended XL attack based upon the p-reduced symmetric algebra that can

solve UOV instances with *odd* characteristics as well as UOV instances with characteristic 2; the time complexity of our XL attack is also conducted. In Section 5 we carry out the bit-cost estimation of recommended QR-UOV instances using our XL attack, analyze the relation between its performance and the choice of characteristics, and compare the performance of our XL attack with those of its key-recovery counterparts. We conclude this work in Section 6 with implications of our contributions for UOV security and future research directions.

2 Preliminaries

2.1 Notations

For every positive integer k, let $[k]$ denote the index set $\{1, 2, ..., k\}$, and let Perm_k denote the set of permutations of over $[k]$. Throughout this work, let V always denote a vector space over $\Bbbk$, where $\Bbbk$ denotes a (possibly infinite) field with characteristic $p = \mathsf{char}(\Bbbk) \in \{0, 2, 3, 5, ...\}$. In most cases $\Bbbk$ denotes a *finite* field $\mathbb{F}_q$, and hence its cardinality q is of the form $q = p^e$, where e is a positive integer. Let V^* always denote the dual space of V.

2.2 UOV-like schemes and the problem

UOV problem is the underlying problem in all UOV-like signature schemes. Here we redefine UOV problem by polar form.

UOV-like scheme. In a UOV-like signature scheme, the public key consists of a system of homogeneous multivariate quadratic polynomials $\mathcal{P} = (p_1, \ldots, p_m)$ over $\mathbb{F}_q$ in n variables. These polynomials are constructed such that there exists a secret o-dimensional subspace $O \subseteq \mathbb{F}_q^n$, called the *Oil space*, satisfying $p_i(\mathbf{x}) = 0$ for all $\mathbf{x} \in O$ and all $i \in [m]$. The security of such schemes relies on the computational hardness of the *UOV problem*: informally speaking, given the public key, recover the oil space.

We define the *Vinegar space* as the $v := n - o$ dimensional subspace $V \subseteq \mathbb{F}_q^n$ that is the orthogonal complement of the Oil space with respect to the standard inner product.

Polar form. For a multivariate quadratic polynomial $p(\mathbf{x})$ over $\mathbb{F}_q$ in n variables, its *polar form* is defined as

$$p'(\mathbf{x}, \mathbf{y}) := p(\mathbf{x} + \mathbf{y}) - p(\mathbf{x}) - p(\mathbf{y}) + p(\mathbf{0})$$

which is a symmetric bilinear form [4].

In the special case when $\mathrm{char}(\mathbb{F}_q) = 2$, this form is additionally anti-symmetric (*i.e.*, alternating) [20].

Similarly, for a system of multivariate quadratic polynomials $\mathcal{P} = (p_1, \ldots, p_m)$ over finite fields $\mathbb{F}_q$ in n variables, we can define its *polar form* as $\mathcal{P}' := (p'_1, \ldots, p'_m)$.

Oil space is a totally isotropic subspace. We define a subspace $O \subseteq \mathbb{F}_q^n$ is *totally isotropic* for a system of polar forms $\mathcal{P}'$ if for all $\mathbf{x}, \mathbf{y} \in V$, $\mathcal{P}'(\mathbf{x}, \mathbf{y}) = \mathbf{0}$, like the definition of totally isotropic subspace for a single bilinear form in [21, 4.1. Definition] and [19].

The following proposition shows that the secret key of UOV is a totally isotropic subspace O of dimension o.

Proposition 1 (Lemma 2.1, [19]). *For UOV public key $\mathcal{P}$, $O \subseteq \mathbb{F}_q^n$ is the Oil space if and only if O is a totally isotropic subspace with dimension o of $\mathcal{P}'$.*

Remark 2. If the characteristic $p \neq 2$, the proposition is obvious. But for characteristic $p = 2$, a totally isotropic subspace with a specialized basis $\mathbf{x}_1, \ldots, \mathbf{x}_o$ satisfying an overdetermined system $\mathcal{P}'(\mathbf{x}_i, \mathbf{x}_j) = 0$. This system has one unique solution in overwhelming cases which explicitly constructs the Oil space.

Definition 3 (UOV problem). *Given (q, n, o, m) and an homogeneous multivariate quadratic system $\mathcal{P} = (p_1, \ldots, p_m)$, find an o-dimensional totally isotropic subspace $O \subseteq \mathbb{F}_q^n$ relative to the polar form of $\mathcal{P}$.*

2.3 Key recovery attacks for UOV-like schemes

A key recovery attack against UOV-like schemes aims to derive a secret key from the given public key.

XL algorithm The XL algorithm is a method for solving systems of multivariate quadratic equations. It serves as a core subroutine in many key-recovery attacks against UOV-like signature schemes.

The XL algorithm [8], named for e**X**tended **L**inearization, originates from the idea to linearize the given system by regarding each monomial as one variable, and then use linear algebra to the coefficient matrix of the linearized system. Furthermore, the most effective improvements of XL are Wiedemann XL (WXL) [27], and the hybrid approaches [2, 26].

Roughly speaking, for a system of m multivariate quadratic equations in n variables over finite fields $\mathbb{F}_q$, and a sufficiently large *degree bound* $D \geq 2$, the plain XL algorithm has complexity

$$\mathcal{O}\left(\binom{n+D}{D}^{\omega}\right)$$

where $2 \leq \omega < 3$ is the exponent of matrix multiplication. WXL has complexity

$$\mathcal{O}\left(\binom{n}{2} \cdot \binom{n+D}{D}^{2}\right)$$

where D can be taken to be the least d such that the coefficient of z^d in $\frac{(1-z^2)^m}{(1-z)^{n+1}}$ does not exceed d, *i.e.*,

$$D := \min\left\{d : \mathrm{coef}\left(\frac{(1-z^2)^m}{(1-z)^{n+1}}, z^d\right) \leq d\right\}.$$

And the hybrid XL has complexity

$$\mathcal{O}\left(q^k \cdot \binom{n-k+D}{D}^{\omega}\right) \text{ and } \mathcal{O}\left(q^k \cdot \binom{n-k}{2} \cdot \binom{n-k+D}{D}^{2}\right)$$

using plain XL and WXL respectively where D can be taken as the least d such that the coefficient of z^d in $\frac{(1-z^2)^m}{(1-z)^{n-k+1}}$ does not exceed d itself, *i.e.*

$$D := \min\left\{d : \mathrm{coef}\left(\tfrac{(1-z^2)^m}{(1-z)^{n-k+1}}, z^d\right) \leq d\right\}.$$

Reconciliation attack [11] Reconciliation attack aims to recover a vector $\mathbf{o}$ in Oil space O by solving the polynomial system $\mathcal{P}(\mathbf{o}) = \mathbf{0}$ which can be done by XL algorithm. Given that $\dim(O) = o$, imposing o generic affine constraints on $\mathbf{o}$ typically yields a unique solution

in O. When $n-o \leq m$, the constrained system $\mathcal{P}(\mathbf{o}) = \mathbf{0}$ becomes an overdetermined system of m equations in fewer than m variables, making it efficiently solvable and superior to direct attacks. When $n - o > m$, we solve $\mathbf{o}_i \in O$ by constructing a underdetermined system:

$$\begin{cases} \mathcal{P}(\mathbf{o}_i) = \mathbf{0}, & 1 \leq i \leq k, \\ \mathcal{P}'(\mathbf{o}_i, \mathbf{o}_j) = \mathbf{0}, & 1 \leq i < j \leq k \end{cases}$$

where P' encodes P's polar form. However, this strategy introduces $k(n-o)$ variables and $m\binom{k+1}{2}$ equations, rendering it generally less efficient than direct attack when k exceeds a small threshold.

Wedge product-based algorithm for characteristic 2 [20] In particular, Lars Ran [20] recently makes use of exterior algebra and introduces a new XL attack for key recovery on UOV instances over finite fields of characteristic 2. It breaks some parameters of UOV-like algorithms : UOV, MAYO and SNOVA. For certain parameter sets, it reduces the effective security margin by more than 30 bits compared to the current best-known attacks.

Specifically, let $V = \langle \mathbf{v}_1, \ldots, \mathbf{v}_v \rangle$ be the vinegar space and $\mathcal{V} = \mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_v$ its associated v-wedge. [20] defines a map

$$\begin{aligned} \mathcal{M} : \bigwedge^{v} \mathbb{F}_q^n &\to \left(\bigwedge^{v+2} \mathbb{F}_q^n \right)^m \\ \mathcal{V} &\mapsto (\mathcal{V} \wedge p'_1, \ldots, \mathcal{V} \wedge p'_m) \end{aligned}$$

where $p'_1, \ldots, p'_m$ are polar forms of the public key. Notice that $\mathcal{M}$ is basically a linear map from $\mathbb{F}_q^{\binom{n}{v}}$ to $\mathbb{F}_q^{m\binom{n}{v+2}}$. Moreover, the matrix corresponding $\mathcal{M}$ can be viewed as a Macaulay matrix on exterior algebra. Since $\mathcal{V}$ lies in the kernel, if the kernel $\mathrm{Ker}(\mathcal{M})$ is of dimension 1, it is exactly the $\mathcal{V}$ and hence we can solve the sparse linear algebra and retrieve the oil space. And Lars Ran has made perfect rank prediction for all 3188 different (non-trivial) parameter sets as

$$\mathrm{rank}(\mathcal{M}) = \sum_{i=0}^{\lfloor \frac{o}{2} \rfloor} (-1)^i \binom{m+i-1}{i} \binom{v+o}{v+2i}$$

except for only 7 exceptions that can further be accounted for with a single rule.

2.4 Graded Frobenius algebra

Here we introduce graded Frobenius algebra, which is a finite dimensional $\mathbb{N}$-graded $\Bbbk$-algebra. The p-reduced symmetric algebra with $p > 0$ is the graded Frobenius algebra.

Definition 4 (Graded Frobenius Algebra). *Let $A = \bigoplus_{i=0}^{u} A_i$ be a finite-dimensional $\mathbb{N}$-graded $\Bbbk$-algebra. A is called a **graded Frobenius algebra** if there exists a homogeneous linear map $\varepsilon : A \to \Bbbk$ of degree $-u$ (the **counit**) such that the bilinear form*

$$\langle a, b \rangle := \varepsilon(a \cdot b)$$

is non-degenerate, i.e., for any homogeneous $a \neq 0$, $\exists b$ with $\langle a, b \rangle \neq 0$.

Proposition 5. *Let $A = \bigoplus_{i=0}^{u} A_i$ be a graded Frobenius algebra over a field $\Bbbk$. For any degree d, the graded components A_d and A_{u-d} are mutually dual vector spaces with* $\dim A_d = \dim A_{u-d}$.

Proof. By the definition of a graded Frobenius algebra, there exists a homogeneous linear map $\varepsilon : A \to \Bbbk$ (of degree $-u$) inducing a non-degenerate bilinear form $\langle a, b\rangle = \varepsilon(ab)$. Consider the linear map $\phi : A_{u-d} \to (A_d)^*$ defined by $\phi(w)(v) = \langle v, w\rangle$. For any nonzero $w \in A_{u-d}$, non-degeneracy guarantees the existence of $a \in A$ such that $\varepsilon(aw) \neq 0$. Decomposing a into homogeneous components $\sum_i a_i$, the homogeneity of ε implies that only the $a_d \in A_d$ term satisfies $\varepsilon(a_d w) \neq 0$ (since for $i \neq d$ we have $\varepsilon(a_i w) = 0$ with $\deg \varepsilon = -u$), proving ϕ is injective. Similarly, we can construct an injection $\psi : A_d \to (A_{u-d})^*$. As A_d and A_{u-d} are finite-dimensional, the injectivity combined with dimension comparison $\dim A_{u-d} \leq \dim(A_d)^* = \dim A_d \leq \dim(A_{u-d})^* = \dim A_{u-d}$ immediately yields $\dim A_d = \dim A_{u-d}$, with ϕ and ψ being isomorphisms. □

3 Reduced Symmetric Algebra

In this section, we propose a p-reduced symmetric algebra and introduce its properties. We then represent polar forms as degree-2 elements within this algebraic structure. This framework will enable us to develop an XL algorithm in the following section.

For ease of description, in this section $\Bbbk$ always denotes a field with characteristic $p \in \{0, 2, 3, 5, ...\}$, whereas V denotes a vector space over $\Bbbk$.

3.1 Symmetric form and p-reduced symmetric algebra

We start by defining symmetric d-form as a generalization of polar forms, so that we have multiplication operation between different forms. Then we present our reduced algebra to reveal some hidden structure of UOV public keys. Recall that polynomial rings could be direct sum of graded polynomials, our new algebra could also be direct sum of different forms.

Symmetric d-form. In this work, we are interested in a *specific* type of symmetric form specified in the following definition.

Definition 6. *Let $d \geq 0$. A* symmetric d-form *of V is a multilinear map $f : V^d \to \Bbbk$ such that:*

- $f(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_d) = f(\mathbf{x}_{\sigma(1)}, \mathbf{x}_{\sigma(2)}, ..., \mathbf{x}_{\sigma(d)})$ *for every permutation σ over the index set $[d] = \{1, 2, ..., d\}$; moreover,*
- *If $d \geq p > 0$, then $f(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_d) = 0$ provided that $\mathbf{x}_1 = \mathbf{x}_2 = \cdots = \mathbf{x}_p$.*

Remark 7. When the characteristic $p = 0$, a symmetric d-form is essentially the classical symmetric form of V. And it is the classical alternating form when $p = 2$.

We now define the multiplication operation between forms (on the same vector space V).

Definition 8. *For a symmetric d-form f of V and a symmetric ℓ-form g of V, their product is defined to be a map $f \odot g$ from $V^{d+\ell}$ to $\Bbbk$ as:*

$$(f \odot g)(\mathbf{x}_1, ..., \mathbf{x}_{d+\ell}) := \sum_{\sigma} f(\mathbf{x}_{\sigma(1)}, ..., \mathbf{x}_{\sigma(d)}) \cdot g(\mathbf{x}_{\sigma(d+1)}, ..., \mathbf{x}_{\sigma(d+\ell)}),$$

where σ ranges from all permutations over the index set $[d + \ell]$ such that $\sigma(1) < \cdots < \sigma(d)$ and $\sigma(d + 1) < \cdots < \sigma(d + \ell)$.

It is routine to verify that the product $f \odot g$ is a symmetric $(d + \ell)$-form of V.

p-reduced symmetric algebra. Recall that the symmetric algebra of V is

$$\mathrm{Sym}(V) = \Bbbk \oplus V \oplus V^{\otimes 2} \oplus \cdots / C,$$

where C is the ideal generated by the set $\{\mathbf{x} \otimes \mathbf{y} - \mathbf{y} \otimes \mathbf{x} \mid \mathbf{x}, \mathbf{y} \in V\}$. What interests us most is a *special* quotient algebra, as the following definition specifies.

Definition 9. *The* p-reduced symmetric algebra *(or reduced symmetric algebra, for short) of* V*, is defined as the quotient algebra*

$$\overline{\mathrm{Sym}(V)} := \mathrm{Sym}(V)/I,$$

where I *is the (graded) ideal generated by the set* $\{\mathbf{x}^{\otimes p} \mid \mathbf{x} \in V\}$.

Remark 10. First, when $p = 0$, the p-reduced symmetric algebra coincides with the classical symmetric algebra. Moreover, the 2-reduced symmetric algebra is essentially the exterior algebra that plays an important role in Lars Ran's attack [20]. Finally, it is routine to verify that the p-reduced symmetric algebra admits the following direct decomposition

$$\overline{\mathrm{Sym}(V)} = \bigoplus_{d\geq 0} \overline{\mathrm{Sym}(V)}_d,$$

where $\overline{\mathrm{Sym}(V)}_d$ is the $\Bbbk$-vector space generated by $\{\mathbf{x}_1 \odot \mathbf{x}_2 \odot \cdots \odot \mathbf{x}_d \mid \mathbf{x}_1, ..., \mathbf{x}_d \in V\}$.

Lemma 11. *Let* $n = \dim_{\Bbbk} V$*. The* p*-reduced symmetric algebra of* V *is isomorphic to the quotient polynomial algebra* $\Bbbk[x_1, \ldots, x_n]/(x_1^p, \ldots, x_n^p)$*. Fix a basis* $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ *of* V*, the isomorphic is deduced by* $\mathbf{e}_i \mapsto x_i$ *for* $i = 1, \ldots, n$*.* □

Recall that Ding and Hodges [10] utilize the associated graded algebra $\mathbb{F}_q[x_1, \ldots, x_n]/(x_1^q, \ldots, x_n^q)$, whereas our algebra reveals the symmetry of polar form.

The set of all symmetric d-forms, $d \geq 0$, on a $\Bbbk$-vector space V naturally forms a graded algebra under the multiplication defined in Definition 8, and admits a canonical isomorphism to the p-reduced symmetric algebra. More precisely:

Theorem 12. *When* V *is finite-dimensional, there exists a graded algebra isomorphism:*

$$\bigoplus_{d\geq 0}\{\textit{symmetric } d\textit{-forms on } V\} \cong \overline{\mathrm{Sym}(V^*)} = \bigoplus_{d\geq 0} \overline{\mathrm{Sym}(V^*)}_d$$

Proof. Let n be the dimension of V over $\Bbbk$, and fix a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of V with its dual basis $\{\mathbf{e}_1^*, \ldots, \mathbf{e}_n^*\}$. The isomorphism is constructed as follows: for each degree $d \geq 0$, define a map Φ_d sending generators $\mathbf{e}_{i_1}^* \odot \cdots \odot \mathbf{e}_{i_d}^* \in \overline{\mathrm{Sym}(V^*)}_d$ to the symmetric d-form

$$(\mathbf{x}_1, \ldots, \mathbf{x}_d) \longmapsto \sum_{\sigma\in \mathrm{Perm}_d} \prod_{k=1}^{d} \mathbf{e}_{i_k}^*(\mathbf{x}_{\sigma(k)}),$$

which extends linearly to the full space. It is straightforward to verify that $\Phi_d(\mathbf{e}_{i_1}^* \odot \cdots \odot \mathbf{e}_{i_d}^*)$ satisfies all the conditions of a symmetric d-form and the map $\oplus_{d\geq 0}\Phi_d$ preserves the multiplication defined in Definition 8. The inverse map Ψ_d takes a symmetric d-form f to the element

$$\sum_{1\leq i_1\leq \cdots \leq i_d\leq n} \frac{f(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_d})}{m_1! \cdots m_k!} \mathbf{e}_{i_1}^* \odot \cdots \odot \mathbf{e}_{i_d}^*$$

where $\{m_1, \ldots, m_k\}$ are the repetition counts of distinct indices in $(i_1, \ldots, i_d)$, with $m_1 + \cdots + m_k = d$, when $\mathrm{char}(\Bbbk) = p > 0$, $1 \leq m_j \leq p - 1$ for all $1 \leq j \leq k$. □

Corollary 13. *Under the isomorphism in theorem 12, we interpret the polar form as a degree-2 element in the p-reduced symmetric algebra. For a polar form* $p'(\mathbf{x},\mathbf{y}) = \sum_{i,j} a_{ij}x_iy_j$ *with* $a_{ij} = a_{ji}$*, its image under* Ψ_2 *is given by:*

$$\begin{aligned}\Psi_2(p') &\overset{Thm12}{=} \sum_{1\le i<j\le n} a_{i,j}e_i^*\odot e_j^* + \sum_{i=1}^{n}\frac{a_{i,i}}{2!}e_i^*\odot e_i^* && \in \overline{\mathrm{Sym}(\mathbb{F}_q^{n*})}_2\\ &\overset{Lem11}{\leftrightarrow} \sum_{1\le i<j\le n} a_{i,j}x_ix_j + \sum_{i=1}^{n}\frac{a_{i,i}}{2!}x_i^2 && \in \mathbb{F}_q[x_1,\ldots,x_n]/(x_1^p,\ldots,x_n^p)\end{aligned}$$

where $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$ *is the standard basis of* $\mathbb{F}_q^n$*.*

3.2 Permanent minor

Recall that the determinant of a square matrix of order d is applied in in Lars Ran's attack [20], and this determinant is in essence an alternating multilinear d-form from V^d to $\Bbbk$. In this work, we propose its analogue in the reduced symmetric algebra setting, as the following definition shows.

Definition 14. *Let* $n = \dim_{\Bbbk} V$ *and* $(\mathbf{e}_1,\ldots,\mathbf{e}_n)$ *be an ordered* $\Bbbk$*-basis for* V*. Also, let* $i_1,i_2,...,i_d \in [n]$ *where* $d \ge 1$*. Then the* permanent minor *of* V *relative to the (ordered) basis* $(\mathbf{e}_1,\ldots,\mathbf{e}_n)$ *and the index sequence* $(i_1,\ldots,i_d)$ *is defined as the map* $\mathrm{Per}^{(\mathbf{e}_1,\ldots,\mathbf{e}_n)}_{(i_1,\ldots,i_d)} : V^d \to \Bbbk$ *as follows:*

$$\mathrm{Per}^{(\mathbf{e}_1,\ldots,\mathbf{e}_n)}_{(i_1,\ldots,i_d)}(\mathbf{x}_1,\mathbf{x}_2,\ldots,\mathbf{x}_d) := \sum_{\sigma}\mathbf{e}^*_{i_1}(\mathbf{x}_{\sigma(1)})\mathbf{e}^*_{i_2}(\mathbf{x}_{\sigma(2)})\cdots\mathbf{e}^*_{i_d}(\mathbf{x}_{\sigma(d)}),$$

where $\sigma \in \mathrm{Perm}_d$ *varies over all permutations over the index set* $[d]$*. Here,* d *is called the* order *of the permanant minor* $\mathrm{Per}^{(\mathbf{e}_1,\ldots,\mathbf{e}_n)}_{(i_1,\ldots,i_d)}$*.*

Some remarks about the permanent minor $\mathrm{Per}^{(\mathbf{e}_1,\ldots,\mathbf{e}_n)}_{(i_1,\ldots,i_d)}$ are in order. First, when the basis $(\mathbf{e}_1,\ldots,\mathbf{e}_n)$ for V is clear from the context, the superscript is usually omitted and no confusion arises. Moreover, it is routine to verify that $\mathrm{Per}_{(i_1,\ldots,i_d)}$ is a multilinear map; in fact, the permanent minor relative to the basis $(\mathbf{e}_1,\ldots,\mathbf{e}_n)$ and the index sequence $(i_1,\ldots,i_d)$ is actually the symmetric d-form $\mathbf{e}^*_{i_1}\odot\mathbf{e}^*_{i_2}\odot\cdots\odot\mathbf{e}^*_{i_d} \in \overline{\mathrm{Sym}(V^*)}$. Finally, the set of permanent minors of order d constitutes a $\Bbbk$-basis for $\overline{\mathrm{Sym}(V^*)}_d$.

In particular, when $d = n$ and $(i_1,i_2,...,i_n) = (1,2,...,n)$, this specific permanant minor is defined as

$$\mathrm{Per}_{(1,2,\ldots,n)}(\mathbf{x}_1,\ldots,\mathbf{x}_n) = \sum_{\sigma}\mathbf{e}^*_1(\mathbf{x}_{\sigma(1)})\mathbf{e}^*_2(\mathbf{x}_{\sigma(2)})\cdots\mathbf{e}^*_n(\mathbf{x}_{\sigma(n)}),$$

which is equivalent to the notion of the *permanent* of a square matrix [7]. What is more, this specific permanent minor is essentially the symmetric n-form $\mathbf{e}^*_1\odot\mathbf{e}^*_2\odot\cdots\odot\mathbf{e}^*_n \in \overline{\mathrm{Sym}(V^*)}$; when $p = 2$, it is equivalent to the notion of determinant.

3.3 Duality

For subsequent computation and analysis, this subsection devotes to properties of the d-space algebra $\overline{\mathrm{Sym}(V)}_d$ by presenting three propositions.

Proposition 15. *Let $p = \mathrm{char}(\Bbbk) > 0$. Also let $n = \dim_{\Bbbk} V$ with $\{\mathbf{e}_1, ..., \mathbf{e}_n\}$ being a $\Bbbk$-basis for V. Then the p-reduced symmetric algebra $\overline{\mathrm{Sym}(V)}$ is a finite-dimensional graded $\Bbbk$-algebra with the following properties:*

(1) Top degree component:
- *The algebra is supported in degrees 0 through $n(p-1)$.*
- *$\dim \overline{\mathrm{Sym}(V)}_{n(p-1)} = 1$, generated by the product $(\prod_{i=1}^{n} \mathbf{e}_i^{p-1})$.*

(2) Hilbert series:

$$H_{\overline{\mathrm{Sym}(V)}}(t) = \frac{(1-t^p)^n}{(1-t)^n} = (1 + t + \cdots + t^{p-1})^n$$

(3) Dimension formula: For each $d \geq 0$,

$$\dim \overline{\mathrm{Sym}(V)}_d = \sum_{j=0}^{\min(n, \lfloor d/p \rfloor)} (-1)^j \binom{n}{j} \binom{d - jp + n - 1}{n-1}$$

This formula counts degree d monomials where each variable has exponent $< p$.

Proof. By Lemma 11, we have the algebra isomorphism $\overline{\mathrm{Sym}(V)} \cong \Bbbk[x_1, \ldots, x_n]/(x_1^p, \ldots, x_n^p)$. Since the sequence $(x_1^p, \ldots, x_n^p)$ is regular, the Hilbert series of $\overline{\mathrm{Sym}(V)}$ is equal to $\frac{(1-t^p)^n}{(1-t)^n}$ Consequently, statements (1) and (3) follow directly from this Hilbert series computation combined with property (2). □

Theorem 16. *Let $n = \dim_{\Bbbk} V$. The p-reduced symmetric algebra $\overline{\mathrm{Sym}(V)}$ is a graded Frobenius algebra.*

Proof. By Proposition 15 we have $\overline{\mathrm{Sym}(V)} = \bigoplus_{i=0}^{u} \overline{\mathrm{Sym}(V)}_i$, where $u = n(p-1)$. Fix a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of V.

Define a homogeneous linear map $\varepsilon : \overline{\mathrm{Sym}(V)} \to \Bbbk$ of degree $-u$ by setting:

$$\varepsilon\left(k \cdot \mathbf{e}_1^{p-1} \odot \cdots \odot \mathbf{e}_n^{p-1}\right) = k \quad \text{and} \quad \varepsilon(x) = 0 \text{ for } \deg x < u.$$

This induces a bilinear form $\langle x, y \rangle := \varepsilon(x \odot y)$.

To verify non-degeneracy, take any non-zero $x \in \overline{\mathrm{Sym}(V)}$ and let $x_d = \sum_{\alpha} k_\alpha e_1^{\alpha_1} \odot \cdots \odot e_n^{\alpha_n}$ (where $|\alpha| = \sum \alpha_i = d$) be its non-zero homogeneous component. For each monomial term $k_\alpha e^\alpha$ in x_d, define the dual monomial:

$$y_\alpha := e_1^{p-1-\alpha_1} \odot \cdots \odot e_n^{p-1-\alpha_n} \in \overline{\mathrm{Sym}(V)}_{u-d}.$$

Then $\langle x, y_\alpha \rangle = k_\alpha \neq 0$ for at least one α, since $x_d \neq 0$. Thus $\overline{\mathrm{Sym}(V)}$ satisfies the condition of a graded Frobenius algebra. □

Proposition 17. *Let $n = \dim_{\Bbbk} V$. Then we have a canonical graded algebra isomorphism*

$$\overline{\mathrm{Sym}(V^*)} \cong \overline{\mathrm{Sym}(V)}^* \cong \bigoplus_{d\geq 0}^{n(p-1)} (\overline{\mathrm{Sym}(V)}_d)^*.$$

Proof. Fix a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of V with dual basis $\{\mathbf{e}_1^*, \ldots, \mathbf{e}_n^*\}$ of V^*. By Theorem 12, we give a graded algebra isomorphism $\oplus_{d\geq 0}\Phi_d$ from $\overline{\mathrm{Sym}(V^*)}$ to symmetric forms. $\Phi_d(e_{i_1}^* \odot e_{i_2}^* \odot \cdots \odot e_{i_d}^*)$ is a symmetric d-form. By the conditions of a symmetric d-form, it can well-define a $\Bbbk$-linear map from $\overline{\mathrm{Sym}(V)}_d$ to $\Bbbk$. □

4 Solving UOV Problem Using *p*-reduced Symmetric Algebra

We now utilize the reduced symmetric algebra introduced in the previous section to develop a corresponding XL algorithm for solving the UOV problem. Our approach builds upon the polar form-based UOV problem formulation presented in Section 2.2, which follows a framework similar to Lars Ran's attack.

4.1 Macaulay matrix on *p*-reduced symmetric algebra

The XL algorithm was designed to solve a system of multivariate polynomials with a unique solution over finite fields. It constructs the Macaulay matrix in a given degree and solves the resultant system using sparse matrix methods. The Macaulay matrix thus plays a central role in the algorithm, and its definition could refer to [8].

According to Definition 6 of symmetric forms, $p_1, p_2, \ldots, p_m$ are 2-forms. And with Definition 8, for every $(d-2)$-form f, $f \odot p_i$ is a d-form. To solve the reformulated UOV problem, we consider the Macaulay matrix of d-forms

$$\{\alpha_j \odot p_i : \alpha_j \text{ comes from basis of } \overline{\mathrm{Sym}(V)}_{d-2}, i \in [m]\}$$

and the basis of $\overline{\mathrm{Sym}(V)}_d$.

Here we present a toy example to show the Macaulay matrix on 3-form. Consider $\mathbb{F}_9$-space $V = \mathbb{F}_9^3$, take $d = 3$, $m = 2$. Let $\mathbf{e}_1 = (1,0,0)$, $\mathbf{e}_2 = (0,1,0)$ and $\mathbf{e}_3 = (0,0,1)$ be a standard basis of $\mathbb{F}_9^3$. For the homogeneous quadratic form $p_k(\mathbf{x}) = \sum_{i \le j} a_{i,j}^{(k)} x_i x_j$, its polar form can be rewritten as 2-form $\sum_{i \le j} a_{i,j}^{(k)} \mathbf{e}_i \odot \mathbf{e}_j$. Then a Macaulay matrix on the 3-form is

$$\begin{array}{c} \\ \mathbf{e}_1 \odot p_1 \\ \mathbf{e}_2 \odot p_1 \\ \mathbf{e}_3 \odot p_1 \\ \mathbf{e}_1 \odot p_2 \\ \mathbf{e}_2 \odot p_2 \\ \mathbf{e}_3 \odot p_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} \mathbf{e}_1\odot\mathbf{e}_1\odot\mathbf{e}_2 & \mathbf{e}_1\odot\mathbf{e}_1\odot\mathbf{e}_3 & \mathbf{e}_1\odot\mathbf{e}_2\odot\mathbf{e}_2 & \mathbf{e}_1\odot\mathbf{e}_2\odot\mathbf{e}_3 & \mathbf{e}_1\odot\mathbf{e}_3\odot\mathbf{e}_3 & \mathbf{e}_2\odot\mathbf{e}_2\odot\mathbf{e}_3 & \mathbf{e}_2\odot\mathbf{e}_3\odot\mathbf{e}_3 \end{array} \\ \begin{pmatrix} a_{1,2}^{(1)} & a_{1,3}^{(1)} & a_{2,2}^{(1)} & a_{2,3}^{(1)} & a_{3,3}^{(1)} & 0 & 0 \\ a_{1,1}^{(1)} & 0 & a_{1,2}^{(1)} & a_{1,3}^{(1)} & 0 & a_{2,3}^{(1)} & a_{3,3}^{(1)} \\ 0 & a_{1,1}^{(1)} & 0 & a_{1,2}^{(1)} & a_{1,3}^{(1)} & a_{2,2}^{(1)} & a_{2,3}^{(1)} \\ a_{1,2}^{(2)} & a_{1,3}^{(2)} & a_{2,2}^{(2)} & a_{2,3}^{(2)} & a_{3,3}^{(2)} & 0 & 0 \\ a_{1,1}^{(2)} & 0 & a_{1,2}^{(2)} & a_{1,3}^{(2)} & 0 & a_{2,3}^{(2)} & a_{3,3}^{(2)} \\ 0 & a_{1,1}^{(2)} & 0 & a_{1,2}^{(2)} & a_{1,3}^{(2)} & a_{2,2}^{(2)} & a_{2,3}^{(2)} \end{pmatrix} \end{array}$$

4.2 XL algorithm on *p*-reduced symmetric algebra

Now we give the XL algorithm on $\overline{\mathrm{Sym}(V)}$. Later in Section 4.3 we show how to find a parameter D such that the XL algorithm works.

Algorithm 1 XL algorithm on $\overline{\mathrm{Sym}(V)}$

Input: A sequence of 2-forms $\{f_i \in \overline{\mathrm{Sym}(\mathbb{F}_q^{n*})}_2 : i \in [m]\}$ with an isotropic subspace $O \subseteq \mathbb{F}_q^n$ of dimension o and a degree bound D, $2 \leq D \leq o(p-1)$.

Output: $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ such that $f_i(\mathbf{x}, \mathbf{y}) = 0$, for all $i \in [m]$.

1: Compute the set $\{\alpha_j \odot f_i : \alpha_j \text{ comes from basis of } \overline{\mathrm{Sym}(V)}_{D-2}, i \in [m]\}$ and construct its Macaulay matrix $\mathbf{M}_D$ using the basis of D-form.
2: Compute the reduced row echelon form of the Macaulay matrix.
3: Check if the dimension of the kernel equal to $\overline{\mathrm{Sym}(O)}_D$, if not, then fail.
4: Solve a permanent minors vector in the kernel space under some linear constraints.
5: From the vector, we will show it's easy get vector in O.

The vector we get from XL algorithm is a sequence of all the permanent minors of order d on some vectors in O. For isotropic subspace O, for any $o_1, \ldots, o_d \in O$, $p_i(o_1, o_2) = 0$. Then for every $f \in \overline{\mathrm{Sym}(\mathbb{F}_q^n)}_{d-2}$.

$$(f \odot p)(o_1, \ldots, o_d) = \sum_{\alpha=(\alpha_1,\ldots,\alpha_r)} k_\alpha e^\alpha(o_1, \ldots, o_d) = 0 \text{ with } \sum_i \alpha_i = d, \alpha_i < p-1.$$

The $(k_\alpha)_\alpha$ lies in a row of Macaulay matrix of dimension d, then the sequence of all the permanent minor on degree d, *i.e.*, $(e^\alpha(o_1, \ldots, o_d))_\alpha$ lies in the kernel of Macaulay matrix. Since $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}_d$ is the dual space of $\overline{\mathrm{Sym}(\mathbb{F}_q^{n*})}_d$ by proposition 17, $\overline{\mathrm{Sym}(O)}_d$ as a subspace of $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}_d$, every element μ can define a map uniquely, $\mu : \overline{\mathrm{Sym}(\mathbb{F}_q^{n*})}_d \to \mathbb{F}_q, e^\alpha \mapsto e^\alpha(\mu)$. Thus $\{(e^\alpha(\mu))_\alpha : \mu \in \overline{\mathrm{Sym}(O)}_d\} \cong \overline{\mathrm{Sym}(O)}_d$. Hence, if the dimension of $\overline{\mathrm{Sym}(O)}_d$ is equal to the dimension of $\mathrm{Ker}\mathbf{M}_d$, then the vector in kernel $\mathbf{M}_d$ is always lie in $\overline{\mathrm{Sym}(O)}_d$.

Let $o_1, \ldots, o_o \in \mathbb{F}_q^n$ be a basis of O with the lower $o \times o$ of the matrix $(o_1, \ldots, o_o)$ is the identity matrix. For $o_1^{\alpha_1} \odot o_2^{\alpha_2} \odot \cdots \odot o_o^{\alpha_o} \in \overline{\mathrm{Sym}(O)}_d$, when $n - o < i_1 \leq i_2 \cdots \leq i_d \leq n$, $\mathrm{Per}_{(i_1,\ldots,i_d)}(o_1^{\alpha_1}, o_2^{\alpha_2}, \cdots, o_o^{\alpha_o})$ is a constant number. when the repetition counts of indices $(n-o+1, \ldots, n)$ in $(i_1, \ldots, i_d)$ is $(\alpha_1, \ldots, \alpha_o)$, then $\mathrm{Per}_{(i_1,\ldots,i_d)}(o_1^{\alpha_1}, \ldots, o_o^{\alpha_o}) = \prod_i \alpha_i!$; otherwise, it is zero. By constraint those zero, we get a vector of all permanent minor of $(o_1^{\alpha_1}, \ldots, o_o^{\alpha_n})$ in $\mathrm{Ker}\mathbf{M}_d$.

A toy example for solving $o_i \in O$ using permanent minors. For $o_1 = (a_1, a_2, 1, 0)$, $o_2 = (b_1, b_2, 0, 1)$ is a basis of O and (o_1^2, o_2) is

$$\begin{pmatrix} a_1 & a_1 & b_1 \\ a_2 & a_2 & b_2 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we have $\mathrm{Per}_{(1,3,4)} = 2a_1$, $\mathrm{Per}_{(1,3,3)} = 2b_1$, $\mathrm{Per}_{(2,3,4)} = 2a_2$ and $\mathrm{Per}_{(2,3,3)} = 2b_2$, then we can compute o_1 and o_2.

4.3 Complexity analysis

In this subsection, we analyze the bit cost / complexity of our algorithm.

Parameter D. First we show how to choose a parameter D in XL algorithm on $\overline{\mathrm{Sym}(V)}$ as

$$D := \min\left\{2 \leq d \leq o(p-1) : \dim \mathrm{Ker}\mathbf{M}_d \leq \dim \overline{\mathrm{Sym}(O)}_d\right\}. \tag{1}$$

Recall that dimension of the d-space $\overline{\mathrm{Sym}(O)}_d$ is easy to obtain by the *dimension formula* stated in Proposition 15.

In the following, we estimate $\dim \mathrm{Ker}\mathbf{M}_d$. By definition of Macaulay matrix $\mathbf{M}_d$ of degree d, for $d \geq 0$, we have

$$\begin{aligned}\dim \mathrm{Ker}\mathbf{M}_d &= \dim_{\mathbb{F}_q} \overline{\mathrm{Sym}(\mathbb{F}_q^{n*})}_d - \dim_{\mathbb{F}_q}(f_1,\ldots,f_m)_d \\ &= \dim_{\mathbb{F}_q}\left(\overline{\mathrm{Sym}(\mathbb{F}_q^{n*})}/(f_1,\ldots,f_m)\right)_d \\ &= \dim_{\mathbb{F}_q}\left(\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^p,\ldots,x_n^p,f_1,\ldots,f_m)\right)_d\end{aligned}$$

To compute the dimension of the quotient algebra at an arbitrary degree d, we consider both the semi-regularity conjecture and the Hilbert series of semi-regular sequences in the p-reduced algebra. The definition of semi-regular sequences and the proof of their Hilbert series properties in the p-reduced symmetric algebra naturally generalize those for Boolean algebras; we present these results in the appendix A.

Theorem 18. *Quadratic forms sequence $(f_1,\ldots,f_m)$ is D-semi-regular in $\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^p,\ldots,x_n^p)$ if only if the Hilbert series of $\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^p,\ldots,x_n^p,f_1,\ldots,f_m)$ is given by:*

$$\left[\frac{(1+t+t^2+\cdots+t^{p-1})^n}{(1+t^2+\cdots+t^{2(p-1)})^m}\right]_D. \tag{2}$$

Conjecture 19. The polar forms sequence $(p'_1,\ldots,p'_m)$ of UOV instance (n,m,o,p) is a D-semi-regular sequence on p-reduced symmetric algebra $\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^p,\ldots,x_n^p)$ with very high probability, where D to be the first d for which

$$\dim_{\mathbb{F}_q}\left(\mathbb{F}_q[x_1,\ldots,x_n]/(x_1^p,\ldots,x_n^p,p'_1,\ldots,p'_m)\right)_d \leq \dim_{\mathbb{F}_q}\left(\mathbb{F}_q[x_1,\ldots,x_o]/(x_1^p,\ldots,x_o^p)\right)_d.$$

The conjecture is a Heuristic assumption, we don't have theoretical proof. We test it for some UOV parameters. The actual $\dim \mathrm{Ker}\mathbf{M}_d$ is equal to the coefficient of t^d of the truncated Hilbert series (2) when $d < D$ and the actual $\dim \mathrm{Ker}\mathbf{M}_D$ is equal to $\dim \overline{\mathrm{Sym}(O)}_D$.

(n, o, m, q, p)	d	actual $\dim(\ker \mathbf{M}_d)$	predicted $\dim(\ker \mathbf{M}_d)$	$\dim\left(\overline{\mathrm{Sym}(O)}_d\right)$
(6, 3, 6, 7, 7)	3	20	20	10
	4	15	15	15
(6, 3, 7, 7, 7)	3	14	14	10
	4	15	0	15
(8, 4, 8, 7, 7)	4	70	70	35
	5	56	56	56
(8, 4, 9, 7, 7)	4	42	42	35
	5	56	0	56
(8, 4, 10, 7, 7)	3	40	40	20
	4	35	15	35
(10, 5, 10, 7, 7)	5	252	252	126
	6	210	210	210
(10, 5, 11, 7, 7)	5	132	132	126
	6	210	0	210
(10, 5, 12, 7, 7)	4	121	121	70
	5	126	22	126

Table 1. Experimental results and our prediction of the dimension of $\mathrm{Ker}(\mathbf{M}_d)$ when $d < p = 7$. The values of d shown in boldface indicate when it reaches our target D as defined in Formula (1).

(n, o, m, q, p)	d	actual $\dim(\ker \mathbf{M}_d)$	predicted $\dim(\ker \mathbf{M}_d)$	$\dim\left(\overline{\mathrm{Sym}(O)}_d\right)$
(6, 3, 6, 9, 3)	3	14	14	7
	4	6	-21	6
(6, 3, 7, 9, 3)	3	8	8	7
	4	6	-36	6
(8, 4, 6, 9, 3)	4	65	65	19
	5	16	-48	16
(8, 4, 7, 9, 3)	4	35	35	19
	5	16	-112	16
(8, 4, 8, 9, 3)	3	48	48	16
	4	19	6	19
(10, 5, 7, 9, 3)	5	192	192	51
	6	45	-335	45
(10, 5, 8, 9, 3)	5	52	52	51
	6	45	-586	45
(10, 5, 9, 9, 3)	4	156	156	45
	5	51	-78	51

Table 2. Experimental results and our prediction of the dimension of $\mathrm{Ker}(\mathbf{M}_d)$ when $d \geq p = 3$. The values of d shown in boldface indicate when it reaches our target D as defined in Formula (1).

Cost estimate. By applying XL algorithm with Wiedemann algorithm, the cost of our attack is

$$\min_{1 \leq o' \leq o} 3(2r^2 + r)\binom{n'+1}{2}\left(\dim \overline{\mathrm{Sym}(\mathbb{F}_q^n)}_D - \dim \overline{\mathrm{Sym}(O')}_D + 1\right)^2$$

where $r = \log_2 q$. Notice that, in order to achieve a speed-up, during the cost estimation, we project a UOV instance (v, o, m, q) down to (v, o', m, q) with $o' < o$, and let O' denote the corresponding o'-dimensional totally isotropic space. In particular, by applying the dimension

formula, we obtain an explicit expression for the cost as:

$$\min_{1\le o'\le o} 3(2r^2+r)\binom{n'+1}{2}\Big(\sum_{j=0}^{\min\left(n,\left\lfloor\frac{D}{p}\right\rfloor\right)}(-1)^j\binom{n}{j}\binom{D-jp+n-1}{n-1} - \sum_{j=0}^{\min\left(o',\left\lfloor\frac{D}{p}\right\rfloor\right)}(-1)^j\binom{o'}{j}\binom{D-jp+o'-1}{o'-1}+1\Big)^2. \tag{3}$$

4.4 From duality view

In Theorem 16, we show $\overline{\mathrm{Sym}(\mathbb{F}_q^n)}$ is a graded Frobenius algebra, then by proposition 5, we have $\overset{d}{\odot}\mathbb{F}_q^n$ and $\overset{u-d}{\odot}\mathbb{F}_q^n$ are mutually dual spaces, where $u = n(p-1)$.

Then we can view the Macaulay matrix $\mathbf{M}_d$ on the d-form as the matrix corresponding with linear map for any d:

$$\begin{aligned}\mathcal{M}_d : \odot^{n(p-1)-d}\mathbb{F}_q^n &\to \left(\odot^{n(p-1)-(d-2)}\mathbb{F}_q^n\right)^m\\ \mu &\mapsto (\mu\odot p_1,\ldots,\mu\odot p_m)\end{aligned}$$

When set $d = o(p-1)$. For vinegar space $V = \langle \mathbf{v}_1,\ldots,\mathbf{v}_v\rangle$ and $\mathcal{V} = \mathbf{v}_1^{p-1}\odot\cdots\odot\mathbf{v}_v^{p-1} \in \overline{\mathrm{Sym}(V)}_{v(p-1)}$ its highest degree element. Same as [20], we have $\mathcal{V}\in \mathrm{Ker}\mathcal{M}_d$ because of $p_i \in \mathbb{F}_q^n \odot V$.

5 Performance

Recall that as a generalization of Lars Ran's XL attack [20], our Algorithm 1 can handle not only UOV instances with characteristic $p = 2$, but also those UOV instances with *odd* characteristic. For instance, in Section 5.1 we shall use our XL attack to analyze the concrete hardness of 12 recommended QR-UOV instances presented in [13]. And our XL attack means more than that.

Previous works in MPKC show that for a UOV instance, the order q of its underlying (finite) field $\Bbbk = \mathbb{F}_q$ is firmly connected to its concrete hardness, and a larger order usually results in a more secure UOV instance, *provided other parameters remain unchanged*; however, the characteristic $p = \mathrm{char}(\Bbbk)$ was usually not taken into the consideration of the concrete hardness analysis of UOV in the past. In contrast, in this section we show that our XL attack runs faster when the characteristic p of the underlying field $\Bbbk$ of UOV gets smaller. Conversely, this implies that choosing a larger characteristic p may help increase the (concrete) hardness of UOV; for instance, a UOV instance with $\Bbbk = \mathbb{F}_{79}$ is, in general, more secure than a similar UOV instance with $\Bbbk = \mathbb{F}_{81}$.

The reason our algorithm's efficiency is p-sensitive is that when p increases, it results in a significant increase in the dimension of the Macaulay matrix. Specifically, according to the dimension formula in Proposition 15, when p increases, the dimension of $\overline{\mathrm{Sym}(V)}_d$ increases exponentially for every degree d, which in turn leads to a growth in the dimension of the Macaulay matrix.

To empirically demonstrate the p-sensitivity of our attack, we present cost estimates for UOV instances in Table 3. For each group of parameters, we fix the number of variables n and equations m, and vary the field characteristic p as well as the field size $q = p^e$. Our results clearly demonstrate that the attack cost increases with p, even in cases where the field size q decreases. [3]

(n, o, m)	(p, e, q)	(D, o', n')	New
(112, 44, 44)	**(2, 8, 256)**	(18, 18, 86)	140
	(3, 5, 243)	(29, 15, 83)	193
	(5, 3, 125)	(51, 13, 81)	263
	(7, 2, 49)	(71, 12, 80)	310
(160, 64, 64)	**(2, 4, 16)**	(22, 22, 118)	175
	(3, 2, 9)	(37, 19, 115)	249
	(5, 1, 5)	(66, 17, 113)	347
(184, 72, 72)	**(2, 8, 256)**	(26, 26, 138)	206
	(3, 5, 243)	(44, 22, 134)	294
	(5, 3, 125)	(78, 20, 132)	409
	(7, 2, 49)	(108, 18, 130)	483
(244, 96, 96)	**(2, 8, 256)**	(32, 32, 180)	257
	(3, 5, 243)	(54, 27, 175)	367
	(5, 3, 125)	(96, 24, 172)	514
	(7, 2, 49)	(135, 23, 171)	616

Table 3. Bit-cost estimates of our new attack (New) against UOV. Here the parameter sets shown in boldface denotes the proposed parameter sets of UOV scheme [6]. We propose several new parameter sets for the UOV scheme and analyze their concrete hardness using Algorithm 1.

[3] Furthermore, as predicted by the cost estimation Formula (3), the influence of the extension degree e is negligible. In particular, when (n, m, p) are fixed, increasing q via a larger e leads to only a marginal increase in overall cost.

5.1 Attack on QR-UOV

Recall that for those four UOV-like schemes that advanced to the Round 2 of NIST's PQC additional signature algorithm competition, only QR-UOV [13] recommends parameter sets with *odd* characteristics. In this subsection, we shall apply our XL attack presented in Algorithm 1 to analyze the concrete hardness of 12 recommended instances of QR-UOV [13].

It is well-established that the reconciliation attack achieves optimal performance against UOV-like schemes when parameters satisfy $n - o \leq m$. Since all QR-UOV recommended parameters meet this condition, the reconciliation attack represents the most efficient known approach for these schemes. Therefore, we benchmark our algorithm's effectiveness by comparing its computational cost against the reconciliation attack.

S.L.	(n, o, m)	(p, e, q)	(D, o', n')	Our	Rec.
I	**(70, 18, 54)**	**(127, 3, 2048383)**	(28, 1, 53)	**164**	**164**
	(84, 10, 100)	(7, 10, 282475249)	(20, 4, 78)	159	148
	(75, 20, 60)	(31, 3, 29791)	(23, 1, 56)	**151**	**151**
	(67, 7, 70)	(31, 10, 819628286980801)	(21, 1, 61)	**152**	**152**
III	**(102, 26, 78)**	**(127, 3, 2048383)**	(40, 1, 77)	**231**	**231**
	(124, 14, 140)	(7, 10, 282475249)	(30, 5, 115)	230	219
	(111, 29, 87)	(31, 3, 29791)	(37, 2, 84)	229	221
	(99, 10, 100)	(31, 10, 819628286980801)	(32, 2, 91)	221	216
V	**(137, 35, 105)**	**(127, 3, 2048383)**	(49, 1, 103)	**291**	**291**
	(168, 19, 190)	(7, 10, 282475249)	(39, 7, 156)	299	277
	(146, 38, 114)	(31, 3, 29791)	(47, 2, 110)	291	283
	(124, 12, 120)	(31, 10, 819628286980801)	(45, 2, 114)	291	283

Table 4. Bit-cost estimates of our attack and reconciliation attack on corresponding UOV(n, o, m, q) instances against the proposed parameter sets in QR-UOV [13]. Here the parameter sets shown in boldface denotes the main proposed parameter sets. And the complexity of our attack and the reconciliation attack shown in boldface indicates the two complexity value collides.

QR-UOV remains secure against our attack because its characteristic is sufficiently large to render our approach ineffective. We observe that our algorithm achieves the same computational complexity as the reconciliation attack when $o' = 1$. This equivalence occurs because, when $o' = 1$, the Macaulay matrix $\mathbf{M}_d$ in our XL algorithm (operating in the p-reduced symmetric algebra) coincides with the Macaulay matrix used in the reconciliation attack for dimensions $d < p$. This alignment explains why the complexity of the XL algorithm in the p-reduced symmetric algebra matches that of the reconciliation attack for QR-UOV parameters with $o' = 1$ as illustrated in the table above.

As shown in Table 4, our attack does not outperform the reconciliation attack for standard QR-UOV parameters due to the large characteristic of QR-UOV. However, when we modify only the characteristic of QR-UOV's recommended parameters—setting it to 3 or 5—our attack demonstrates superior efficiency compared to the reconciliation attack, as illustrated in the table below.

(n, o, m)	(p, e, q)	(D, o', n')	Our	Rec.
(70, 18, 54)	(3, 3, 27)	(16, 8, 60)	122	145
	(5, 3, 125)	(23, 6, 58)	150	153
(102, 26, 78)	(3, 3, 27)	(21, 11, 87)	163	201
	(5, 3, 125)	(30, 8, 84)	201	215
(137, 35, 105)	(3, 3, 27)	(26, 13, 115)	204	255
	(5, 3, 125)	(38, 10, 112)	257	274

Table 5. Bit-cost estimates of our XL attack (Our) and reconciliation attack (Rec.) against QR-UOV [13]. Here, we choose several new parameter sets for the QR-UOV scheme and analyze their concrete hardness.

5.2 Parameter suggestions

In this subsection, we demonstrate the connection between the characteristic p and the concrete hardness of UOV instance with the MAYO scheme [5]. To be precise, we choose several parameter sets for MAYO, and analyze their concrete hardness using our new XL attack, as well as those attacks considered in [5] (*e.g.*, the direct attack, the Kipnis-Shamir attack, the reconciliation attack, the intersection attack and the collision attack).

Some remarks are in order. First, it can be seen from Table 6 that for certain MAYO instances (or more generally, for certain UOV instances), our XL attack presented in Algorithm 1 outperforms all other key-recovery attacks under consideration, or even all forgery attacks; this demonstrates the strength of our XL attack concretely. Moreover, our argument that a larger p usually results in a more secure instance can be confirmed in Table 6; for instance, the MAYO instance with $\Bbbk = \mathbb{F}_{79}$ turns out to be more secure than the MAYO instance with $\Bbbk = \mathbb{F}_{81}$, provided that the other parameters remain the same.

Notice that Our attack's performance depends heavily on the field characteristic p. This implies that when our XL attack dominate the concrete hardness result, the simplest way for achieving security upgrade is to increase p while keeping all other parameters unchanged. For example, switching MAYO_2 from $\mathbb{F}_{16}$ to $\mathbb{F}_{17}$ (or from $\mathbb{F}_{81}$ to $\mathbb{F}_{79}$) boosts security for obvious reasons.

(n, o, m)	(p, e, q)	(D, o', n')	New	Direct	KS	Rec.	Int.	Col.
(81, 64, 17)	(2, 4, 16)	(13, 13, 77)	**112**	155	211	167	228	141
	(17, 1, 17)	(46, 3, 67)	230	155	216	169	231	**145**
	(3, 4, 81)	(19, 10, 74)	**147**	177	323	190	302	217
	(79, 1, 79)	(110, 2, 66)	345	**176**	321	190	301	216
	(5, 4, 625)	(28, 7, 71)	**183**	192	462	205	394	312
	(7, 4, 2401)	(33, 6, 70)	199	**198**	554	211	455	374
	(31, 4, 923521)	(59, 2, 66)	263	**217**	959	232	723	649

Table 6. Bit-cost estimates of attacks including our new attack (New), direct attack (Direct), Kipnis-Shamir attack (KS), reconciliation attack (Rec.), intersection attack (Int.) as well as collision attack (Col.) against several MAYO instances. Here we use the cryptographic estimator introduced in [12] when $p > 2$. It should be noted those instances are not the recommended instances proposed in the MAYO submission [5].

6 Conclusion

In summary, this work presents a novel cryptanalytic approach against UOV-based multivariate cryptographic schemes using polar forms and p-reduced symmetric algebras. We develop a generalized framework that extends beyond the characteristic 2 case studied by Lars Ran, enabling attacks on odd characteristic scenarios through p-reduced algebraic structures. Our method leverages the symmetric properties of polar forms to construct an algebra isomorphic to symmetric algebras in characteristic 0 and to exterior algebras in characteristic 2. We propose an enhanced XL algorithm operating over p-reduced symmetric algebras that efficiently computes symmetric minors of oil variable matrices, leading to oil space recovery.

Furthermore, we establish that our XL-based approach constitutes a reconciliation attack under certain conditions. When applied to QR-UOV parameters, we show that the attack scenario falls within the reconciliation framework, thereby confirming the security of QR-UOV against polar form attacks. Our results provide new insights into the algebraic structure of multivariate schemes and contribute to the security analysis of NIST PQC candidates.

Our work not only advances the theoretical understanding of multivariate cryptography but also delivers concrete tools for evaluating and improving the security of post-quantum signature schemes. Future research directions include extending this framework to other multivariate schemes, optimizing the proposed algorithms, and exploring further applications of symmetric algebra in cryptography.

References

1. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.P., Verbel, J.: Improvements of algebraic attacks for solving the rank decoding and minrank problems. In: 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 26. pp. 507–536. Springer (2020)
2. Bettale, L., Faugere, J.C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology **3**(3), 177–197 (2009)
3. Beullens, W.: Improved cryptanalysis of UOV and rainbow. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12696, pp. 348–373. Springer (2021). https://doi.org/10.1007/978-3-030-77870-5_13, https://doi.org/10.1007/978-3-030-77870-5_13
4. Beullens, W.: Improved cryptanalysis of snova. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 277–293. Springer (2025)
5. Beullens, W., Campos, F., Celi, S., Hess, B., Kannwischer, M.J.: MAYO. Round 2 Additional Signatures, Post-Quantum Cryptography: Digital Signature Schemes (2025), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/mayo-spec-round2-web.pdf
6. Beullens, W., Chen, M.S., Ding, J., Gong, B., Kannwischer, M.J., Patarin, J., Peng, B.Y., Schmidt, D., Shih, C.J., Tao, C., Yang, B.Y.: UOV: Unbalanced Oil and Vinegar - Algorithm Specifications and Supporting Documentation Version 2.0. Round 2 Additional Signatures, Post-Quantum Cryptography: Digital Signature Schemes (2025), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/uov-spec-round2-web.pdf
7. Bhatia, R.: Matrix Analysis. Springer New York, NY (1997)
8. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 392–407. Springer (2000)
9. Ding, J., Gower, J.E., Schmidt, D.S.: Multivariate public key cryptosystems, vol. 25. Springer Science & Business Media (2006)
10. Ding, J., Hodges, T.: Inverting HFE Systems is Quasi-Polynomial for All Fields. In: Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference. Lecture Notes in Computer Science, vol. 6841, p. 721. Springer (2011)

11. Ding, J., Yang, B.Y., Chen, C.H.O., Chen, M.S., Cheng, C.M.: New differential-algebraic attacks and reparametrization of rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A., Yung, M. (eds.) Applied Cryptography and Network Security. pp. 242–257. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
12. Esser, A., Verbel, J.A., Zweydinger, F., Bellini, E.: SoK: CryptographicEstimators - a Software Library for Cryptographic Hardness Estimation. In: AsiaCCS. ACM (2024)
13. Furue, H., Ikematsu, Y., Hoshino, F., Takagi, T., Kosuge, H., Yamakoshi, K., Akiyama, R., Nakamura, S., Orihara, S., Kinjo, K.: QR-UOV. Round 2 Additional Signatures, Post-Quantum Cryptography: Digital Signature Schemes (2025), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/qruov-spec-round2-web.pdf
14. Kipnis, A., Shamir, A.: Cryptanalysis of the Oil and Vinegar signature scheme. In: Krawczyk, H. (ed.) Advances in Cryptology — CRYPTO '98. pp. 257–266. Springer Berlin Heidelberg, Berlin, Heidelberg (1998)
15. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Advances in Cryptology—EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques Davos, Switzerland, May 25–27, 1988 Proceedings 7. pp. 419–453. Springer (1988)
16. Call for additional digital signature schemes for the post-quantum cryptography standardization process (September 2022), available at https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf
17. Patarin, J.: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In: Coppersmith, D. (ed.) Advances in Cryptology — CRYPTO '95. pp. 248–261. Springer Berlin Heidelberg, Berlin, Heidelberg (1995)
18. Patarin, J.: The Oil and Vinegar signature scheme. In: Dagstuhl Workshop on Cryptography (September 1997)
19. Pébereau, P.: Singular points of UOV and VOX. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 294–323. Springer (2025)
20. Ran, L.: Wedges, oil, and vinegar: A new algorithm for UOV in characteristic 2. Rump Session Eurocrypt 2025 (2025), https://larsmath.github.io/assets/pdf/rumpsessioneurocrypt25.pdf
21. Scharlau, W.: Quadratic and hermitian forms. Springer-Verlag (1985)
22. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing **26**(5), 1484–1509 (1997)
23. Tao, C., Petzoldt, A., Ding, J.: Efficient key recovery for all HFE signature variants. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12825, pp. 70–93. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_4, https://doi.org/10.1007/978-3-030-84242-0_4
24. Team, T.R.: Modified parameters of rainbow in response to a refined analysis of the rainbow band separation attack by the nist team and the recent new minrank attacks (2020), http://precision.moscito. org/by-publ/recent/rainbow-pars.pdf
25. Wang, L.C., Chou, C.Y., Ding, J., Kuan, Y.L., Leegwater, J.A., Li, M.S., Tseng, B.S., Tseng, P.E., Wang, C.C.: SNOVA - Proposal for NISTPQC: Digital Signature Schemes Project. Round 2 Additional Signatures, Post-Quantum Cryptography: Digital Signature Schemes (2025), https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/snova-spec-round2-web.pdf
26. Yang, B.Y., Chen, J.M., Courtois, N.T.: On asymptotic security estimates in xl and gröbner bases-related algebraic cryptanalysis. In: Information and Communications Security: 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004. Proceedings 6. pp. 401–413. Springer (2004)
27. Yang, B.Y., Chen, O.C.H., Bernstein, D.J., Chen, J.M.: Analysis of QUAD. In: International Workshop on Fast Software Encryption. pp. 290–308. Springer (2007)

A Semi-regular Sequences over $\mathbb{F}_p$

In this section, we generalize the definition of semi-regular sequences from Boolean algebras $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2, \ldots, x_n^2)$ to p-reduced symmetric algebras. Let R denote the p-reduced symmetric algebra over $\mathbb{F}_q$:

$$R = \mathbb{F}_q[x_1, \ldots, x_n]/(x_1^p, \ldots, x_n^p),$$

where $p = \mathrm{char}(\mathbb{F}_q)$.

For any series $H = \sum_i H_i t^i \in \mathbb{Z}[[t]]$, we define the coefficient of t^i as H_i and its truncation up to degree d as $[\sum_i H_i t^i]_d = \sum_i^{d-1} H_i t^i$. For a $\mathbb{N}$-graded module M, M_d denotes its homogeneous component of degree d.

Definition 20. *Let $f_1, \ldots, f_m$ be a sequence of homogeneous element of R and D a positive integer. We say $f_1, \ldots, f_m$ is D-semi-regular in R if for all $i = 1, 2, \ldots, m$ and any homogeneous $u \in R$ satisfying:*

$$uf_i \in (f_1, \ldots, f_{i-1}) \text{ and } \deg(uf_i) < D,$$

then $u \in (f_1, \ldots, f_i^{p-1})$.

Lemma 21. *Let $f_1, \ldots, f_m$ be a D-semi-regular sequence in R. Then for all $i = 1, \ldots, m$, $k = 2, \ldots, p$, and any homogeneous element $u \in R$ satisfying:*

$$uf_i \in (f_1, \ldots, f_i^k) \text{ and } \deg(uf_i) < D,$$

it follows that $u \in (f_1, \ldots, f_i^{k-1})$.

Proof. Let $f = f_1$, and define $K_k = \operatorname{Ker}\left(R/f^{k-1}R \xrightarrow{\cdot f} R/f^kR : u \mapsto uf\right)$. For $k = 2, 3, \ldots, p-1$, we have the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & & & K_{k+1} & & K_k & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & f^{k-1}R/f^kR & \longrightarrow & R/f^kR & \longrightarrow & R/f^{k-1}R & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot f} & & \downarrow{\scriptstyle \cdot f} & & \downarrow{\scriptstyle \cdot f} & & \\
0 & \longrightarrow & f^kR/f^{k+1}R & \longrightarrow & R/f^{k+1}R & \longrightarrow & R/f^kR & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & R/fR & & R/fR & &
\end{array}$$

Applying the snake lemma yields the exact sequence:

$$0 \to \operatorname{Ker}\left(f^{k-1}R/f^kR \xrightarrow{\cdot f} f^kR/f^{k+1}R\right) \to K_k \to K_{k-1} \to 0.$$

This implies that if $K_{k,d} = 0$ for some degree $d \geq 0$, then $K_{k-1,d} = 0$. By the definition of D-semi-regularity, $K_{p-1,d} = 0$ for all $d < D - \deg(f)$. Consequently, $K_{k,d} = 0$ for $k = 2, \ldots, p-1$ and $d < D - \deg(f)$.

The result extends to f_i by considering $R = R/(f_1, \ldots, f_{i-1})$ and setting $f = f_i$, which preserves the commutative diagram structure. □

Theorem 22. *Let $f_1, \ldots, f_m$ be a D-semi-regular sequence of degree 2 in R. Then the Hilbert series of $R/(f_1, \ldots, f_m)$, truncated at D, is given by:*

$$[T]_D, \text{ where } T := \frac{(1 + t + \cdots + t^{p-1})^n}{(1 + t^2 + \cdots + t^{2(p-1)})^m}.$$

Otherwise, if $f_1, \ldots, f_m$ is D-semi-regular, but not $(D+1)$-semi-regular, then

$$\dim\left(R/(f_1, \ldots, f_m)\right)_D > T_D,$$

where T_D denotes the coefficient of t^D in T.

Proof. By the definition of D-semi-regularity and Lemma 21, taking $f = f_1$, we obtain that for each $k = 2, \ldots, p$, the following chain complex is exact in degrees less than D:

$$0 \longrightarrow R/(f^{k-1})[-2] \xrightarrow{\cdot f} R/(f^k) \longrightarrow R/(f) \longrightarrow 0. \tag{4}$$

This yields the identity for Hilbert series:

$$[H_{R/(f)}]_{D-2(p-k)} + [t^2 H_{R/(f^{k-1})}]_{D-2(p-k)} = [H_{R/(f^k)}]_{D-2(p-k)}, \quad k = 2, \ldots, p.$$

Multiplying by $t^{2(p-k)}$ gives:

$$[t^{2(p-k)} H_{R/(f)}]_D + [t^{2(p-k+1)} H_{R/(f^{k-1})}]_D = [t^{2(p-k)} H_{R/(f^k)}]_D. \quad k = 2, \ldots, p.$$

Summing these equations over $k = 2, \ldots, p$ produces:

$$[(1 + t^2 + \cdots + t^{2(p-1)}) H_{R/(f)}]_D = [H_R]_D.$$

Now let $R = R/(f_1, \ldots, f_{i-1})$:

$$[(1 + t^2 + \cdots + t^{2(p-1)}) H_{R/(f_1,\ldots,f_i)}]_D = [H_{R/(f_1,\ldots,f_{i-1})}]_D.$$

By induction:

$$\left[(1 + t^2 + \cdots + t^{2(p-1)})^m H_{R/(f_1,\ldots,f_m)}\right]_D = [H_R]_D.$$

Consequently:

$$[H_{R/(f_1,\ldots,f_m)}]_D = \left[\frac{H_R}{(1 + t^2 + \cdots + t^{2(p-1)})}\right]_D$$

For the second statement, let $i \in \{1, \ldots, m\}$ and $k \in \{2, \ldots, p\}$. Define

$$K_{ik} = \mathrm{Ker}\left(R/(f_1, \ldots, f_i^{k-1}) \xrightarrow{\cdot f_i} R/(f_1, \ldots, f_i^k)\right).$$

When $d < D-2$, we have $K_{ik,d} = 0$ for all i and k, while $K_{ip,D-2} \neq 0$ for some i. This implies the following equality of truncated Hilbert series:

$$\left[(1 + t^2 + \cdots + t^{2(p-1)}) H_{R/(f_1,\ldots,f_i)}\right]_{D+1} = \left[H_{R/(f_1,\ldots,f_{i-1})}\right]_{D+1} + t^D \dim K_{ip,D-2}, \quad (i = 1, \ldots, m).$$

Consequently, $H_{R/(f_1,\ldots,f_m),D} > T_D$. □