Revisiting the Wedge Attack on the UOV Problem

Jintai Ding[1], Peigen Li[2⋆], and Siyong Tao[3]

[1] Xian Jiaotong-Liverpool University
jintai.ding@gmail.com
[2] Beijing Institute of Mathematical Sciences and Applications
lpg22@bimsa.cn
[3] Department of Mathematical Sciences, Tsinghua University
taosy22@mails.tsinghua.edu.cn

Abstract. In this article, we first reformulate the wedge attack within a cleaner algebraic-geometric framework and then extend it to multi-homogeneous systems over fields of arbitrary characteristic. Building on these tools, we apply the resulting multi-homogeneous wedge attack to the security analysis of SNOVA.

Keywords: UOV problem · Wedge attack · Multi-homogeneous polynomial systems · SNOVA

1 Introduction

Multivariate public key cryptosystems (MPKCs) constitute one of the major families of post-quantum cryptographic schemes, offering attractive features such as efficient signing, compact signatures, and low computational overhead. In an MPKC, the public key is typically given by a system of multivariate quadratic polynomials over a finite field, while the secret key specifies a hidden algebraic structure that enables efficient cryptographic operations. The security of MPKCs relies on the presumed difficulty of solving multivariate quadratic systems, known as the multivariate quadratic (MQ) problem. Although the MQ problem is NP-complete in the general case [9], its average-case complexity and the existence of exploitable algebraic structures remain central issues in the design and analysis of multivariate cryptographic schemes.

The Unbalanced Oil and Vinegar (UOV) scheme [17, 12] is among the most extensively studied MPKC families. The core idea of UOV is to construct a public quadratic map that hides a special decomposition of variables into oil and vinegar components. Consequently, the security of UOV relies on the difficulty of recovering this hidden oil–vinegar structure from the public key, which is commonly referred to as the UOV problem.

⋆ Corresponding author.

Definition 1.1 (UOV problem). *Let $v > o$ and m be positive integers, and set $n = v + o$. Given a homogeneous quadratic map $(p_1, \ldots, p_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ that vanishes on an o-dimensional subspace $\mathcal{O} \subset \mathbb{F}_q^n$, called the oil space, the UOV problem is to recover $\mathcal{O}$.*

Since its introduction, UOV has undergone extensive cryptanalytic investigation, and the underlying oil–vinegar framework has become a fundamental paradigm in multivariate cryptography.

The flexibility of the UOV framework has further led to a number of important variants and extensions. For example, QR-UOV, MAYO, and SNOVA introduce additional algebraic structures, lifting techniques, or compact representations to improve the trade-offs between security, public-key size, and signature size. Together with the original UOV scheme, these four constructions have recently been selected as third-round candidates in the National Institute of Standards and Technology (NIST) additional post-quantum digital signature competition, demonstrating the continued practical importance of UOV-based approaches.

The security of UOV-based constructions has been studied from a variety of cryptanalytic perspectives. Classical key recovery attacks include the Kipnis–Shamir (KS) attack [12], which exploits linear-algebraic properties of the hidden oil space, as well as subsequent reconciliation [6], intersection [3], and rectangular MinRank attacks [3] that recover partial information about the secret structure or reduce the complexity of the associated MQ systems. These developments have significantly influenced the selection of secure parameters and the design of more sophisticated UOV-based schemes.

More recently, a new class of structural attacks has emerged that challenges the security analysis of UOV-based constructions from a different perspective. Ran [19] introduced the *wedge attack*, which exploits specific algebraic dependencies arising from the hidden structure of the UOV problem. Subsequently, Jin et al. [11] and Furue et al. [7] generalized this approach and demonstrated that wedge-type phenomena may extend beyond the original UOV setting to a broader class of multivariate schemes. Furthermore, the authors of [4] and [20] independently applied wedge attacks to the security analysis of SNOVA.

These recent results highlight the need for a systematic understanding of the algebraic mechanisms underlying wedge attacks. In particular, it remains important to clarify how such attacks interact with the additional algebraic structures introduced in modern UOV-based constructions and whether these structures provide genuine protection or introduce new vulnerabilities. This motivates a deeper investigation of wedge-type attacks from an algebraic and complexity-theoretic viewpoint.

Our contributions The main contributions of this paper are summarized as follows.

1. We reformulate the wedge attack as a right-kernel recovery problem for Macaulay matrices. In both truncated polynomial rings and exterior algebras, the hidden oil space is encoded by a quotient map whose dual lies in

the Macaulay kernel. When the natural dimension bound is sharp, an identity block in this dual map gives a normalized kernel basis from which the defining linear polynomials can be read explicitly; see §4.1.
2. We extend this recovery mechanism to multi-homogeneous systems in multi-truncated polynomial rings and multi-exterior algebras. The resulting criteria recover all component oil spaces from a multi-graded Macaulay kernel whenever the corresponding graded quotient dimensions agree. We then specialize both formulations to the reconciliation- and lifting-intersection systems arising from SNOVA; see §4.2 and §5.
3. We clarify the role of Hilbert-series estimates in selecting an attack degree. Such estimates can suggest useful total degrees or multidegrees, but they do not by themselves certify the dimension equality required by the recovery theorems. We illustrate this limitation with explicit experiments; see §4.3.

Outline The remainder of the paper is organized as follows. §2 fixes the notations and semi-regular sequences. §3 recalls the wedge attack and the kernel-recovery viewpoint used in this work. §4 develops the reformulation first in the total-degree setting and then in the multi-homogeneous setting, for both truncated polynomial rings and exterior algebras; it also discusses the limitations of Hilbert-series-based degree selection. Finally, §5 applies the multi-graded recovery criteria to SNOVA through its reconciliation and lifting-intersection formulations.

2 Preliminaries

2.1 Notation and algebraic sets

Throughout the paper, $q = p^e$ is a prime power, $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$, and $\mathbb{F}_{q^s}$ denotes the degree-s extension of $\mathbb{F}_q$. For a positive integer c, we write $[c]$ for the set $\{1, \ldots, c\}$.

Let I be an ideal of $\mathbb{F}_q[x_1, \ldots, x_n]$. Its zero set over $\overline{\mathbb{F}}_q$ is

$$V(I) := \{\mathbf{v} \in \overline{\mathbb{F}}_q^n : \ f(\mathbf{v}) = 0 \text{ for all } f \in I\}$$

and its set of $\mathbb{F}_{q^s}$-rational points is

$$V_{\mathbb{F}_{q^s}}(I) := \{\mathbf{v} \in \mathbb{F}_{q^s}^n : \ f(\mathbf{v}) = 0 \text{ for all } f \in I\}.$$

2.2 Semi-regular sequences in truncated polynomial rings

Suppose that

$$F(\mathbf{t}) = \sum_{\mathbf{d} \in \mathbb{N}^c} a_{\mathbf{d}} \mathbf{t}^{\mathbf{d}} \in \mathbb{Z}[[t_1, \cdots, t_c]].$$

Define

$$\mathrm{Supp}_+(F) := \{\mathbf{d} \in \mathbb{N}^c : \ \forall \mathbf{r} \leq \mathbf{d}, \ a_{\mathbf{r}} \geq 0\}$$

and

$$[F(\mathbf{t})]_+ := \sum_{\mathbf{d}\in \mathrm{Supp}_+(F)} a_{\mathbf{d}}\mathbf{t}^{\mathbf{d}}.$$

For an integer $\ell \geq 1$, we define the p^ℓ-truncated polynomial ring

$$R := \mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^{p^\ell}, \ldots, x_n^{p^\ell}\rangle$$

and write R_d for its degree-d component. Then the Hilbert series of R is

$$H(t) = \sum_{d\in\mathbb{N}} \dim(R_d)t^d = h(t)^n, \quad h(t) = 1 + t + \cdots + t^{p^\ell - 1}.$$

Definition 2.1 (Semi-regular sequence). *Let $p_1, \ldots, p_m \in R$ be homogeneous polynomials of degrees $d_1, \ldots, d_m$. We say that $p_1, \ldots, p_m$ is a semi-regular sequence over R if the Hilbert series of the quotient by $I = \langle p_1, \ldots, p_m\rangle \subset R$ is given by*

$$H_{R/I}(t) := \sum_{d\in\mathbb{N}} \dim(R_d/I_d)t^d = \Big[\frac{h(t)^n}{\prod_{i=1}^m h(t^{d_i})}\Big]_+, \quad I_d = R_d \cap I \tag{2.1}$$

Remark 2.2. The notion of semi-regularity was introduced by Bardet in [2, Chapitre 3] in two settings: the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$ and the Boolean truncated polynomial ring

$$\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2\rangle.$$

Bardet's original definition is formulated in terms of the injectivity of the multiplication maps induced by the polynomials $p_1, \ldots, p_m$ in the relevant graded components. The prescribed Hilbert series of $\langle p_1, \ldots, p_m\rangle$ is an equivalent characterization of this injectivity property; see [2, Proposition 3.2.5]. By contrast, Baena et al. [1, Definition 4] recently gave a precise definition of semi-regularity in the q-truncated polynomial ring

$$\mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^q, \cdots, x_n^q\rangle$$

for any prime power q.

We next record the multi-graded version. For an integer $\ell \geq 1$, we define the ℓ-truncated multi-graded polynomial ring

$$\mathcal{R} := \mathbb{F}_q[\mathbf{x}_1, \ldots, \mathbf{x}_c]/\langle x_{ij}^{p^\ell} : 1 \leq i \leq c,\ 1 \leq j \leq n_i\rangle, \qquad \mathbf{x}_i = (x_{i1}, \ldots, x_{in_i}).$$

We give $\mathcal{R}$ the $\mathbb{Z}^c$-grading determined by $\deg(x_{ij}) = \mathbf{e}_i$, where $\mathbf{e}_i$ is the i-th standard basis vector of $\mathbb{Z}^c$. A polynomial is *multi-homogeneous* of multidegree $\mathbf{d} = (d_1, \ldots, d_c)$ if each of its monomials has multidegree $\mathbf{d}$; the corresponding homogeneous component is denoted by $\mathcal{R}_{\mathbf{d}}$. The Hilbert series of $\mathcal{R}$ is then

$$H(\mathbf{t}) = \sum_{\mathbf{d}\in\mathbb{N}^c} \dim(\mathcal{R}_{\mathbf{d}})\mathbf{t}^{\mathbf{d}} = \prod_{i=1}^{c}(1 + t_i + \cdots + t_i^{p^\ell - 1})^{n_i}.$$

Definition 2.3 (Multi-graded semi-regular sequence). *Let $p_1, \ldots, p_m \in \mathcal{R}$ be multi-homogeneous polynomials of degrees $\mathbf{d}_1, \ldots, \mathbf{d}_m$. We say that $p_1, \ldots, p_m$ is a semi-regular sequence over $\mathcal{R}$ if the Hilbert series of the quotient by $\mathcal{I} = \langle p_1, \ldots, p_m \rangle$ is given by*

$$H_{\mathcal{R}/\mathcal{I}}(\mathbf{t}) := \sum_{\mathbf{d} \in \mathbb{N}^c} \dim(\mathcal{R}_{\mathbf{d}}/\mathcal{I}_{\mathbf{d}})\mathbf{t}^{\mathbf{d}} = \left[\frac{\prod_{i=1}^{c} h(t_i)^{n_i}}{\prod_{i=1}^{m} h(\mathbf{t}^{\mathbf{d}_i})}\right]_+, \quad \mathcal{I}_{\mathbf{d}} = \mathcal{I} \cap \mathcal{R}_{\mathbf{d}}.$$

Remark 2.4.

1. To the best of our knowledge, the existing literature does not provide a rigorous definition of semi-regularity for ideals in a truncated polynomial ring in terms of their Hilbert series. By contrast, Hilbert series of ideals in a multi-graded polynomial ring $\mathcal{R}$ have already appeared in cryptanalytic works; see, for example, [18, 3, 15, 16], including two attacks on SNOVA in [5, 8]. Truncated multi-homogeneous polynomial systems were studied in [20, §5.3]; however, that work does not give a rigorous definition of semi-regularity for an ideal generated by a multi-homogeneous system.
2. Although semi-regularity for a multigraded system can also be characterized in terms of the injectivity of the corresponding multiplication maps, introducing this characterization would reduce the readability of the article. Moreover, the only property we need is that the Hilbert series allows us to compute the dimension of the kernel of the corresponding Macaulay matrix. We therefore choose to define semi-regularity directly in terms of the Hilbert series.

2.3 Semi-regular sequences in exterior algebras

We also need a notion of semi-regularity for the exterior-algebra systems used in §4. Since an exterior algebra is finite-dimensional and contains zero divisors in every positive degree, the usual definition of a regular sequence in a polynomial ring does not apply verbatim. Moreover, the expected Hilbert series is characteristic-dependent. We therefore follow the Hilbert-series convention used throughout this paper and make the following definition.

Let V be an n-dimensional vector space over $\mathbb{F}_q$ with basis $e_1, \ldots, e_n$, and let

$$W := \bigwedge V = \bigoplus_{d=0}^{n} W_d,$$

$$W_d := \bigwedge^{d} V = \mathrm{span}_{\mathbb{F}_q}\{e_{i_1} \wedge \cdots \wedge e_{i_k} : 1 \le i_1 < \cdots < i_k \le n\}.$$

Thus

$$H_W(t) = \sum_{d=0}^{n} \dim(W_d) t^d = (1+t)^n.$$

Definition 2.5 (Exterior semi-regular sequence). *Let $q_1, \ldots, q_m \in W_2$ and let $\mathfrak{a} = \langle q_1, \ldots, q_m \rangle_W$ be the homogeneous two-sided ideal they generate. We call $q_1, \ldots, q_m$ an* exterior semi-regular sequence *if*

$$H_{W/\mathfrak{a}}(t) := \sum_{d=0}^{n} \dim(W_d/\mathfrak{a}_d)t^d = \begin{cases} \left[\dfrac{(1+t)^n}{(1+t^2)^m}\right]_+, & \mathrm{char}(\mathbb{F}_q) = 2, \\ \left[(1+t)^n(1-t^2)^m\right]_+, & \mathrm{char}(\mathbb{F}_q) \neq 2, \end{cases} \tag{2.2}$$

where $\mathfrak{a}_d = \mathfrak{a} \cap W_d$.

The two cases in Eq. (2.2) reflect different algebra structures. In characteristic two, after choosing a basis, W is isomorphic to the commutative square-zero algebra

$$\mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle,$$

and a quadratic generator contributes the factor $(1+t^2)^{-1}$. In odd characteristic, W is graded-commutative and a degree-two generator is even; the expected maximal-rank contribution is instead $1-t^2$. Thus the phrase "semi-regular in the exterior algebra" always refers to Definition 2.5, rather than to the truncated-polynomial definition in Eq. (2.1).

We next record the multi-graded version. Let V_i have dimension n_i and set

$$\mathcal{W} := \bigwedge V_1 \otimes \cdots \otimes \bigwedge V_c, \qquad \mathcal{W}_{\mathbf{d}} := \bigwedge^{d_1} V_1 \otimes \cdots \otimes \bigwedge^{d_c} V_c.$$

Its multi-graded Hilbert series is

$$H_{\mathcal{W}}(\mathbf{t}) = \prod_{i=1}^{c} (1+t_i)^{n_i}.$$

Definition 2.6 (Multi-graded exterior semi-regularity). *Let $q_1, \ldots, q_m \in \mathcal{W}$ be multi-homogeneous elements of multidegrees $\boldsymbol{\delta}_r \in \mathbb{N}^c$ ($r \in [m]$), with $|\boldsymbol{\delta}_r| = 2$ for every r, and put $\mathfrak{A} = \langle q_1, \ldots, q_m \rangle_{\mathcal{W}}$. We call the sequence* multi-graded exterior semi-regular *if*

$$\begin{aligned} H_{\mathcal{W}/\mathfrak{A}}(\mathbf{t}) &:= \sum_{\mathbf{d}} \dim(\mathcal{W}_{\mathbf{d}}/\mathfrak{A}_{\mathbf{d}})\mathbf{t}^{\mathbf{d}} \\ &= \begin{cases} \left[\dfrac{\prod_{i=1}^{c}(1+t_i)^{n_i}}{\prod_{r=1}^{m}(1+\mathbf{t}^{\boldsymbol{\delta}_r})}\right]_+, & \mathrm{char}(\mathbb{F}_q) = 2, \\ \left[\prod_{i=1}^{c}(1+t_i)^{n_i} \prod_{r=1}^{m}(1-\mathbf{t}^{\boldsymbol{\delta}_r})\right]_+, & \mathrm{char}(\mathbb{F}_q) \neq 2. \end{cases} \end{aligned} \tag{2.3}$$

where $\mathfrak{A}_{\mathbf{d}} = \mathfrak{A} \cap \mathcal{W}_{\mathbf{d}}$.

Remark 2.7. Definitions 2.5 and 2.6 are Hilbert-series definitions. In the applications below they are used as degree-selection heuristics: the predicted coefficient is compared with the dimension of the quotient by the hidden linear ideal. As in the commutative truncated setting, equality with the predicted Hilbert series is an assumption and need not hold for structured UOV or SNOVA instances.

3 Wedge attack

In this section, we first review the wedge attack proposed by Ran [19]. Let $V = \mathbb{F}_q^n$ and $E = V^*$, where $\mathrm{char}(\mathbb{F}_q) = 2$, and let $p_1, \ldots, p_m$ be the homogeneous quadratic polynomials from Definition 1.1. Define their polar forms by

$$q_i(\mathbf{x}, \mathbf{y}) := p_i(\mathbf{x}+\mathbf{y}) - p_i(\mathbf{x}) - p_i(\mathbf{y}), \qquad 1 \le i \le m.$$

The defining UOV property in Definition 1.1 gives

$$q_i(\mathbf{o}, \mathbf{o}') = 0 \qquad \text{for all } \mathbf{o}, \mathbf{o}' \in \mathcal{O} \text{ and } 1 \le i \le m. \tag{3.1}$$

In characteristic two, each q_i is alternating and therefore corresponds to a 2-form in $\bigwedge^2 E$.

Let $\dim(\mathcal{O}) = o$, and $v = n - o$. Ran showed that Eq. (3.1) implies the following decomposition:

$$q_j = \sum_{k=1}^{v} \mathbf{v}_k \wedge \mathbf{x}_{j,k}, \quad \mathbf{v}_k, \mathbf{x}_{j,k} \in \bigwedge^1 E.$$

This observation leads to the following linear map:

$$\mathcal{M} : \bigwedge^v E \longrightarrow \left(\bigwedge^{v+2} E\right)^m, \qquad \omega \longmapsto (q_1 \wedge \omega, \ldots, q_m \wedge \omega). \tag{3.2}$$

Its kernel contains the vector $\mathcal{V} := \mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_v$, which encodes the hidden oil space.

The map $\mathcal{M}$ is represented by a matrix. Hence its kernel can be computed by linear algebra. If $\ker(\mathcal{M}) = \mathrm{span}\{\mathcal{V}\}$, equivalently,

$$\dim \ker(\mathcal{M}) = 1,$$

then the hidden oil space can be recovered from $\ker(\mathcal{M})$.

A key point in the wedge attack is how to estimate the dimension of $\ker(\mathcal{M})$. Ran [19, Proposition 2] proved that

$$\dim \ker(\mathcal{M}) = \dim \ker(\mathcal{M}_{\mathcal{F}}^o),$$

where $\mathcal{M}_{\mathcal{F}}^o$ is the degree-o Macaulay matrix of the polynomials $p_1, \cdots, p_m$ over the truncated polynomial ring

$$\mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^2, \cdots, x_n^2 \rangle.$$

Therefore, the dimension of the kernel of $\mathcal{M}$ can be estimated from the Hilbert series of the ideal generated by the polynomials $p_1, \cdots, p_m$ in the truncated polynomial ring $\mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^2, \cdots, x_n^2 \rangle$. Under the assumption that $p_1, \cdots, p_m$ form a semi-regular sequence, the Hilbert series is given by

$$H(t) = \left[\frac{(1+t)^n}{(1+t^2)^m}\right]_+. \tag{3.3}$$

More recently, Jin et al. [11] generalized the wedge attack to odd characteristic fields. The key idea is to consider the symmetric algebra instead of exterior algebra. Based on the results in [11], Furue et al. [7] generalized the wedge attack to p^ℓ-truncated polynomial rings

$$\mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^{p^\ell}, \cdots, x_n^{p^\ell}\rangle$$

over any finite field $\mathbb{F}_q$.

It is worth noting that Le et al. had already made an initial attempt to apply the wedge attack to SNOVA in [13], although their analysis did not yield precise results. More recently, essentially the same group of authors presented a substantially refined and more conclusive analysis in [4]. At nearly the same time, Tseng et al. independently obtained similar results in [20].

4 Algebraic-Geometric Reformulation of the Wedge Attack

In this section, we first reformulate the wedge attack in a cleaner algebraic-geometric framework. Then we extend this framework to multi-homogeneous systems.

4.1 Total-degree setting

We begin with the algebraic idea underlying our reformulation. In the UOV setting, let $I = \langle p_1, \cdots, p_m\rangle$, and let $J = \langle L_1, \cdots, L_v\rangle$ be the ideal defining the oil space $\mathcal{O}$, where $L_1, \cdots, L_v$ are linear polynomials. Since every p_i vanishes on the oil space, we have $I \subseteq J$. In the UOV setting, L_i can be written as

$$L_i = x_i + \ell_i(x_{v+1}, \ldots, x_n), \qquad \ell_i = \sum_{j=v+1}^{n} a_{ij}x_j, \qquad i \in [v]. \tag{4.1}$$

Our goal is to recover J from the known ideal I.

We translate Ran's wedge-attack strategy into the following graded-algebraic problem. We seek a degree d for which

$$I_d = J_d \neq 0.$$

Once such a degree is found, the degree-d component I_d contains enough information to recover the linear generators of J. Because $I_d \subseteq J_d$, the condition $I_d = J_d$ can be detected through equality of the corresponding quotient dimensions.

To search for a suitable degree and carry out the recovery, we realize I and J in two families of graded algebras. The first consists of the p^ℓ-truncated polynomial rings

$$R = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{p^\ell}, \ldots, x_n^{p^\ell}\rangle,$$

and the second consists of the exterior algebras

$$W = \bigwedge (\mathbb{F}_q^n)^*,$$

where $(\mathbb{F}_q^n)^* = \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^n, \mathbb{F}_q)$ is the dual space. The next two subsections develop the same recovery principle in these two algebras.

Truncated polynomial rings Fix a positive integer ℓ and set

$$R = \mathbb{F}_q[x_1, \cdots, x_n]/\langle x_1^{p^\ell}, \cdots, x_n^{p^\ell} \rangle.$$

In the UOV setting, we again denote the images of $p_1, \ldots, p_m$ and $L_1, \ldots, L_v$ in R by the same symbols. Let $I = \langle p_1, \ldots, p_m \rangle \subseteq R$ and $J = \langle L_1, \ldots, L_v \rangle \subseteq R$ be the corresponding ideals. In particular, $I \subseteq J$.

For each $d \in \mathbb{N}$, we consider the linear map

$$\mathcal{M}_d : \bigoplus_{i=1}^{m} R_{d-2} \to R_d, \quad (a_i)_{i=1}^m \mapsto \sum_{i=1}^{m} a_i p_i.$$

Its image is I_d and its dual map is

$$\mathcal{M}_d^\vee : \mathrm{Hom}_{\mathbb{F}_q}(R_d, \mathbb{F}_q) \to \mathrm{Hom}_{\mathbb{F}_q}\left(\bigoplus_{i=1}^{m} R_{d-2}, \mathbb{F}_q \right).$$

The degree-d Macaulay matrix M_d is the matrix representing $\mathcal{M}_d^\vee$. Its columns are indexed by monomials x^a in R_d, and its rows are indexed by the products $x^b p_i$, where $i \in [m]$ and $x^b \in R_{d-2}$. The $(x^b p_i, x^a)$-entry of M_d is the coefficient of x^a in $x^b p_i$.

Note that $\mathcal{M}_d^\vee$ can be represented by the degree-d Macaulay matrix M_d of the public polynomials $p_1, \cdots, p_m$ over R. In particular, the right kernel of M_d is $\ker \mathcal{M}_d^\vee$.

We set $R_d = 0$ if $d \leq 0$. Hence

$$\dim \ker \mathcal{M}_d^\vee = \dim \mathrm{coker} \mathcal{M}_d = \dim R_d/I_d \geq \dim R_d/J_d. \tag{4.2}$$

The authors of [7] proved that when equality holds in Eq. (4.2), one can recover the vector space $\mathcal{O}$ from $\ker \mathcal{M}_d^\vee$. In what follows, we provide an alternative algebraic-geometric proof of this result.

Theorem 4.1. *If, for some integer $d > 0$,*

$$\dim R_d/I_d = \dim R_d/J_d > 0, \tag{4.3}$$

then we can recover the linear polynomials L_i from the right kernel of the degree-d Macaulay matrix M_d.

Proof. Let S be the graded algebra $\mathbb{F}_q[x_{v+1},\dots,x_n]/\langle x_{v+1}^{p^\ell},\dots,x_n^{p^\ell}\rangle$ and regard S as a subalgebra of R with an $\mathbb{N}$-grading inherited from R. We define the graded algebra homomorphism

$$\varphi : R \to S, \quad \varphi(x_i) = \begin{cases} -\ell_i & i \le v \\ x_i & i > v. \end{cases}$$

φ is surjective, $\ker\varphi = J$. Hence it induces an isomorphism

$$R_d/J_d \xrightarrow{\sim} S_d. \tag{4.4}$$

We next describe the dual of this quotient map explicitly. For every degree-d monomial $x^{\boldsymbol{\alpha}} \in S_d$, define

$$F_{\boldsymbol{\alpha}} : R_d \longrightarrow \mathbb{F}_q, \qquad F_{\boldsymbol{\alpha}}(f) := [x^{\boldsymbol{\alpha}}]\varphi(f),$$

where $[x^{\boldsymbol{\alpha}}]\varphi(f)$ denotes the coefficient of $x^{\boldsymbol{\alpha}}$ in $\varphi(f)$. Because φ is the identity on S, these functionals satisfy

$$F_{\boldsymbol{\alpha}}(x^{\boldsymbol{\beta}}) = \begin{cases} 1, & \boldsymbol{\alpha} = \boldsymbol{\beta}, \\ 0, & \boldsymbol{\alpha} \ne \boldsymbol{\beta}, \end{cases} \qquad x^{\boldsymbol{\alpha}}, x^{\boldsymbol{\beta}} \in S_d.$$

Thus the $F_{\boldsymbol{\alpha}}$ are linearly independent. Moreover, $I_d \subseteq J_d = \ker(\varphi|_{R_d})$, so every $F_{\boldsymbol{\alpha}}$ vanishes on I_d. Hence

$$\operatorname{Span}_{\mathbb{F}_q}\{F_{\boldsymbol{\alpha}} : x^{\boldsymbol{\alpha}} \in S_d\} \subseteq \{F \in \operatorname{Hom}_{\mathbb{F}_q}(R_d, \mathbb{F}_q) : F(I_d) = 0\} = \ker \mathcal{M}_d^\vee. \tag{4.5}$$

The containment is an equality, because

$$\dim S_d = \dim R_d/J_d = \dim R_d/I_d = \dim \ker \mathcal{M}_d^\vee.$$

It remains to explain why this equality allows us to recover the individual functionals $F_{\boldsymbol{\alpha}}$, rather than only their span. Let $r = \dim R_d$ and $s = \dim S_d$, enumerate the degree-d monomials in S_d as

$$x^{\boldsymbol{\alpha}_1}, \dots, x^{\boldsymbol{\alpha}_s},$$

and enumerate the remaining degree-d monomials of R_d as $x^{\boldsymbol{\beta}_1}, \dots, x^{\boldsymbol{\beta}_{r-s}}$. We use the ordered monomial basis

$$\left(x^{\boldsymbol{\beta}_1}, \dots, x^{\boldsymbol{\beta}_{r-s}}, x^{\boldsymbol{\alpha}_1}, \dots, x^{\boldsymbol{\alpha}_s}\right)$$

of R_d; the order within either group may be chosen arbitrarily. Define $A_d \in \mathbb{F}_q^{r\times s}$ by taking its j-th column to be the coordinate vector of $F_{\boldsymbol{\alpha}_j} \in R_d^*$ with respect to the dual of this ordered basis. Equivalently, the entry in the row indexed by a degree-d monomial $x^{\boldsymbol{\beta}}$ and the column indexed by $\boldsymbol{\alpha}_j$ is

$$(A_d)_{\boldsymbol{\beta},j} = F_{\boldsymbol{\alpha}_j}(x^{\boldsymbol{\beta}}).$$

For the last s rows, the Kronecker-delta identity above gives $F_{\boldsymbol{\alpha}_j}(x^{\boldsymbol{\alpha}_k}) = \delta_{jk}$. Consequently,

$$A_d = \begin{pmatrix} B_d \\ I_s \end{pmatrix},$$

where $(B_d)_{ij} = F_{\boldsymbol{\alpha}_j}(x^{\boldsymbol{\beta}_i})$ records the evaluations on the monomials outside S_d. In particular, the projection of $\ker \mathcal{M}_d^\vee = \mathrm{Im}(A_d)$ onto the last $\dim S_d$ coordinates is an isomorphism. Starting from any basis of $\ker \mathcal{M}_d^\vee$, we may therefore perform Gaussian elimination on these last coordinates and obtain the unique normalized basis whose lower block is the identity. This normalized basis is precisely the collection of columns of A_d, and hence determines every $F_{\boldsymbol{\alpha}}$.

Finally, fix $i \in [v]$ and $j \in \{v+1, \ldots, n\}$. Since $\dim S_d > 0$, we have $1 \leq d \leq (n-v)(p^\ell - 1)$. We can therefore choose a degree-d monomial

$$x^{\boldsymbol{\alpha}} = x_{v+1}^{\alpha_{v+1}} \cdots x_n^{\alpha_n} \in S_d \qquad \text{with } \alpha_j \geq 1.$$

Set $g = x_i x^{\boldsymbol{\alpha}} / x_j$. Using $\varphi(x_i) = -\sum_{k=v+1}^n a_{ik} x_k$, we obtain

$$\varphi(g) = -\sum_{k=v+1}^{n} a_{ik} x_k \frac{x^{\boldsymbol{\alpha}}}{x_j}.$$

The coefficient of $x^{\boldsymbol{\alpha}}$ in this expression is exactly $-a_{ij}$; no term with $k \neq j$ contributes to that monomial. Hence

$$F_{\boldsymbol{\alpha}}\left(x_i \frac{x^{\boldsymbol{\alpha}}}{x_j}\right) = -a_{ij}.$$

All the coefficients a_{ij} can thus be read from the normalized basis of $\ker M_d$. This recovers every L_i, and therefore the oil space $\mathcal{O} = V(L_1, \ldots, L_v)$. □

Exterior algebras Let

$$W = \bigwedge (\mathbb{F}_q^n)^* = \bigoplus_{d=0}^{n} W_d, \qquad W_d = \bigwedge^d (\mathbb{F}_q^n)^*,$$

and let $e^1, \ldots, e^n$ be the basis dual to the standard basis of $\mathbb{F}_q^n$. Thus W_d has basis $e^{i_1} \wedge \cdots \wedge e^{i_d}$, where $1 \leq i_1 < \cdots < i_d \leq n$.

Let $\omega_1, \ldots, \omega_m \in W_2$ be the alternating forms arising from the polar forms of $p_1, \cdots, p_m$. Set

$$\eta_i = e^i + \sum_{j=v+1}^{n} a_{ij} e^j, \qquad \mathfrak{a} = \langle \omega_1, \ldots, \omega_m \rangle, \qquad \mathfrak{b} = \langle \eta_1, \ldots, \eta_v \rangle,$$

where the coefficients a_{ij} are as in Eq. (4.1). The isotropy of $\mathcal{O}$ gives $\mathfrak{a} \subseteq \mathfrak{b}$; In analogy with the truncated-polynomial case, consider

$$\mathcal{M}_{d,\Omega} : \bigoplus_{r=1}^{m} W_{d-2} \longrightarrow W_d, \qquad (b_r)_{r=1}^m \longmapsto \sum_{r=1}^{m} b_r \wedge \omega_r.$$

Its image is $\mathfrak{a}_d$, and hence

$$\dim \ker \mathcal{M}_{d,\Omega}^{\vee} = \dim W_d/\mathfrak{a}_d \geq \dim W_d/\mathfrak{b}_d = \binom{n-v}{d}, \tag{4.6}$$

where $\mathcal{M}_{d,\Omega}^{\vee}$ is the dual map of $\mathcal{M}_{d,\Omega}$. Similarly, let $M_{d,\Omega}$ denote the degree-d Macaulay matrix associated with $\omega_1, \ldots, \omega_m$, defined analogously to M_d.

Theorem 4.2. *For some $d > 0$, if*

$$\dim W_d/\mathfrak{a}_d = \dim W_d/\mathfrak{b}_d > 0, \tag{4.7}$$

then the linear polynomials $L_1, \ldots, L_v$, and hence $\mathcal{O}$, can be recovered from the right kernel of the degree-d Macaulay matrix $M_{d,\Omega}$.

Proof. Put $V = \bigwedge\langle e^{v+1}, \ldots, e^n\rangle$ and define

$$\psi : W \longrightarrow V, \qquad \psi(e^i) = -\sum_{j=v+1}^{n} a_{ij}e^j \ (i \leq v), \qquad \psi(e^j) = e^j \ (j > v).$$

Then $\ker \psi = \mathfrak{b}$, so $W_d/\mathfrak{b}_d \cong V_d$. For each $\tau = \{i_1 < \cdots < i_d\} \subseteq \{v+1, \ldots, n\}$, let

$$F_\tau(f) = [e^{i_1} \wedge \cdots \wedge e^{i_d}]\psi(f), \qquad f \in W_d.$$

Since $\mathfrak{a}_d \subseteq \mathfrak{b}_d$, every F_τ belongs to $\ker \mathcal{M}_{d,\Omega}^{\vee}$. Moreover, the restrictions of the F_τ to V_d form its dual basis. The dimension equality in Eq. (4.7) therefore yields

$$\ker \mathcal{M}_{d,\Omega}^{\vee} = \mathrm{Span}_{\mathbb{F}_q}\{F_\tau : |\tau| = d\}.$$

Order the basis of W_d so that the basis of V_d occurs last. The coordinate matrix of the F_τ then has the form $\left(B_d^{\mathsf{T}}, I\right)^{\mathsf{T}}$. Thus Gaussian elimination on the last coordinates of any right-kernel basis recovers every individual F_τ.

Finally, fix $i \leq v$ and $j > v$. Because $1 \leq d \leq n-v$, choose $\tau = \{i_1 < \cdots < i_d\}$ containing $j = i_k$. Directly from the definition of ψ,

$$F_\tau\left(e^i \wedge e^{i_1} \wedge \cdots \wedge \widehat{e^{i_k}} \wedge \cdots \wedge e^{i_d}\right) = (-1)^k a_{ij}.$$

Hence the normalized right-kernel basis determines every a_{ij} and therefore all the L_i and the oil space $\mathcal{O}$. □

Remark 4.3. 1. For $\ell = 1$ and $\mathrm{char}\,\mathbb{F}_q = 2$, the truncated polynomial ring R and the exterior algebra W are isomorphic, which is the original idea of [19]. When $\mathrm{char}\,\mathbb{F}_q \neq 2$ and the public UOV maps are represented by symmetric matrices, the corresponding alternating forms $\omega_1, \ldots, \omega_m$ are zero. However, if one can find nonzero alternating forms $\omega_1, \ldots, \omega_m$ that vanish on the oil space, then one can apply the wedge attack to the exterior algebra $\bigwedge(\mathbb{F}_q^n)^*$, as in SNOVA.

2. In Theorems 4.1 and 4.2, the conditions $\dim R_d/I_d = \dim R_d/J_d > 0$ and $\dim W_d/\mathfrak{a}_d = \dim W_d/\mathfrak{b}_d > 0$ can be checked by computing the Hilbert series of I (resp. $\mathfrak{a}$) and J (resp. $\mathfrak{b}$), under the assumption that the UOV systems are semi-regular in the respective settings. In [19], the author considers only the case $d = o$. More generally, one can consider the wedge map

$$\mathcal{M} : \bigwedge^{n-d} E \longrightarrow \left(\bigwedge^{n-d+2} E \right)^m, \qquad \omega \longmapsto (q_1 \wedge \omega, \ldots, q_m \wedge \omega). \tag{4.8}$$

   Then the condition $\dim W_d/\mathfrak{a}_d = \dim W_d/\mathfrak{b}_d$ is equivalent to the statement that the kernel of $\mathcal{M}$ is generated by $\mathcal{V} = \mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_v$. Thus, it is not necessary to require $\dim \ker \mathcal{M} = 1$. Furthermore, one can replace the p^ℓ-truncated polynomial ring R by a k-truncated polynomial ring for any positive integer k. Unfortunately, we find that, for standard UOV parameters, the condition $\dim R_d/I_d = \dim R_d/J_d > 0$ is not satisfied for any d unless $k = p^\ell$ for some ℓ.
3. The complexity of the wedge attack is dominated by the complexity of computing the right kernel of the Macaulay matrix M_d (resp. $M_{d,\Omega}$).

4.2 Multi-homogeneous setting

The polynomial systems arising from the SNOVA signature scheme [21] possess a natural multi-homogeneous structure; see also [14, 5, 8]. This motivates us to extend the preceding framework to multi-homogeneous polynomial systems and to formulate the corresponding Multi-UOV problem. In [20, §5], building on the proof of [19, Proposition 2], the authors formulate the Multi-UOV problem in a similar manner and develop a wedge attack against SNOVA. From our perspective, this attack can be reformulated in terms of the Macaulay matrix associated with the underlying multi-homogeneous system.

Definition 4.4 (Multi-UOV problem). *Let c, m be positive integers. For each $i \in [c]$, let $n_i = v_i + o_i$. Given a multi-homogeneous quadratic polynomial map*

$$(p_1, \ldots, p_m) : \mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_c} \longrightarrow \mathbb{F}_q^m$$

such that there exist subspaces $\mathcal{O}_i \subseteq \mathbb{F}_q^{n_i}$ with $\dim \mathcal{O}_i = o_i$ satisfying

$$\mathcal{O}_1 \times \cdots \times \mathcal{O}_c \subseteq V(p_1, \ldots, p_m),$$

the Multi-UOV problem is to recover the subspaces $\mathcal{O}_1, \ldots, \mathcal{O}_c$.

In the Multi-UOV setting above, we assume that

$$p_1, \ldots, p_m \in \mathbb{F}_q[\mathbf{x}_1, \ldots, \mathbf{x}_c], \qquad \mathbf{x}_i = (x_{i1}, \ldots, x_{in_i}), \quad i \in [c],$$

where each hidden subspace $\mathcal{O}_i \subseteq \mathbb{F}_q^{n_i}$ has dimension

$$\dim \mathcal{O}_i = o_i = n_i - v_i,$$

and is defined by the linear polynomials

$$L_{i,j} = x_{ij} + \ell_{i,j}(x_{i,v_i+1}, \ldots, x_{i,n_i}), \qquad i \in [c], \quad j \in [v_i].$$

Equivalently, $\mathcal{O}_i = V(L_{i,1}, \ldots, L_{i,v_i})$. Thus,

$$\mathcal{I} := \langle p_1, \ldots, p_m \rangle \subseteq \mathcal{J} := \langle L_{i,j} : i \in [c],\ j \in [v_i] \rangle.$$

Our goal is to recover the linear polynomials $L_{i,j}$ from the known ideal $\mathcal{I}$.

We mainly work with two families of $\mathbb{Z}^c$-graded algebras. The first family consists of the multi-truncated polynomial rings

$$\mathcal{R} := \mathbb{F}_q[\mathbf{x}_1, \ldots, \mathbf{x}_c] \big/ \big\langle x_{ij}^{p^\ell} : i \in [c],\ j \in [n_i] \big\rangle, \quad \mathbf{x}_i = (x_{i1}, \ldots, x_{in_i}).$$

Give each variable x_{ij} multidegree $\mathbf{e}^i \in \mathbb{Z}^c$, and write $\mathcal{R}_{\mathbf{d}}$ for the component of multidegree $\mathbf{d}$. The second family consists of the multi-exterior algebras

$$\mathcal{W} := \bigwedge \Big(\bigoplus_{i=1}^{c} V_i \Big) \cong \bigwedge V_1 \otimes \cdots \otimes \bigwedge V_c,$$

where V_i is a vector space over $\mathbb{F}_q$ of dimension $n_i = v_i + o_i$. Its homogeneous component of multidegree $\mathbf{d} = (d_1, \ldots, d_c)$ is

$$\mathcal{W}_{\mathbf{d}} = \bigwedge^{d_1} V_1 \otimes \cdots \otimes \bigwedge^{d_c} V_c, \qquad \dim \mathcal{W}_{\mathbf{d}} = \prod_{i=1}^{c} \binom{n_i}{d_i}.$$

Multi-truncated polynomial rings In the Multi-UOV setting, we again denote the images of the polynomials and linear polynomials in $\mathcal{R}$ by $p_1, \ldots, p_m$ and $L_{1,1}, \ldots, L_{c,v_c}$, respectively. Then

$$\mathcal{I} = \langle p_1, \ldots, p_m \rangle \subset \mathcal{J} = \langle L_{i,j} : i \in [c],\ j \in [v_i] \rangle \subset \mathcal{R}.$$

Suppose that the p_r are multi-homogeneous of multidegree $\boldsymbol{\delta}_r$. For $\mathbf{d} \in \mathbb{N}^c$, consider the multi-graded Macaulay map

$$\mathcal{M}_{\mathbf{d}} : \bigoplus_{r=1}^{m} \mathcal{R}_{\mathbf{d}-\boldsymbol{\delta}_r} \longrightarrow \mathcal{R}_{\mathbf{d}}, \qquad (g_r)_{r=1}^m \longmapsto \sum_{r=1}^{m} g_r p_r,$$

where $\mathcal{R}_{\mathbf{a}} = 0$ if some coordinate of $\mathbf{a}$ is negative. Its image is $\mathcal{I}_{\mathbf{d}}$, and therefore

$$\dim \ker \mathcal{M}_{\mathbf{d}}^{\vee} = \dim \mathcal{R}_{\mathbf{d}} / \mathcal{I}_{\mathbf{d}} \geq \dim \mathcal{R}_{\mathbf{d}} / \mathcal{J}_{\mathbf{d}}, \tag{4.9}$$

where $\mathcal{M}_{\mathbf{d}}^{\vee}$ is the dual map of $\mathcal{M}_{\mathbf{d}}$. Similarly, let $M_{\mathbf{d}}$ denote the multidegree-$\mathbf{d}$ Macaulay matrix associated with $p_1, \ldots, p_m$, defined analogously to M_d.

Define

$$\mathcal{S} := \mathbb{F}_q[x_{ij} : i \in [c],\ v_i < j \leq n_i] \big/ \langle x_{ij}^{p^\ell} : i \in [c],\ v_i < j \leq n_i \rangle,$$

Then $\mathcal{R}/\mathcal{J} \cong \mathcal{S}$.

Theorem 4.5. *Let* $\mathbf{d} \geq \mathbf{1}$. *If*

$$\dim \mathcal{R}_{\mathbf{d}}/\mathcal{I}_{\mathbf{d}} = \dim \mathcal{R}_{\mathbf{d}}/\mathcal{J}_{\mathbf{d}} > 0,$$

then all the linear polynomials $L_{i,j}$, *and hence the spaces* $\mathcal{O}_1, \ldots, \mathcal{O}_c$, *can be recovered from the right kernel of the multidegree-*$\mathbf{d}$ *Macaulay matrix* $M_{\mathbf{d}}$.

Proof. Apply the proof of Theorem 4.1 to the multi-graded quotient map $\mathcal{R} \to \mathcal{S}$: the equality of dimensions identifies the right kernel with the image of its dual, while the identity block indexed by the monomials of $\mathcal{S}_{\mathbf{d}}$ normalizes a kernel basis and reveals the coefficients of every $\ell_{i,j}$. □

Remark 4.6. A Multi-UOV problem can be regarded as a UOV problem by forgetting the multigrading on $\mathcal{R}$. In that case, we search for an integer $d > 1$ satisfying

$$\dim \mathcal{R}_d/\mathcal{I}_d = \dim \mathcal{R}_d/\mathcal{J}_d > 0, \tag{4.10}$$

where $\mathcal{R}_d = \oplus_{\mathbf{d}\in\mathbb{N}^c, |\mathbf{d}|=d}\mathcal{R}_{\mathbf{d}}, \mathcal{I}_d = \mathcal{I} \cap \mathcal{R}_d$, and similarly for $\mathcal{J}_d$. Since $\mathcal{I}_{\mathbf{d}} \subseteq \mathcal{J}_{\mathbf{d}}$, if Eq. (4.10) holds for some $d > 0$, then each $\mathbf{d} \in \mathbb{N}^c$ with $|\mathbf{d}| = d$ and $\mathbf{d} \leq (p^\ell - 1)\mathbf{1}$ satisfies the condition of Theorem 4.5. In fact,

$$\ker \mathcal{M}_d^\vee = \bigoplus_{\mathbf{d}\in\mathbb{N}^c:|\mathbf{d}|=d} \ker \mathcal{M}_{\mathbf{d}}^\vee.$$

Although the oil space can be recovered from $\ker \mathcal{M}_d^\vee$, it is enough to use a suitable $\ker \mathcal{M}_{\mathbf{d}}^\vee$. Computing the latter is more efficient because the multidegree-$\mathbf{d}$ Macaulay matrix $M_{\mathbf{d}}$ is usually much smaller than the total-degree matrix M_d.

Multi-exterior algebras Choose bases $e^{i,1}, \ldots, e^{i,n_i}$ of V_i. Suppose that the hidden subspace in the i-th block is defined by

$$\eta^{i,j} = e^{i,j} + \sum_{k=v_i+1}^{n_i} a_{i,j,k} e^{i,k}, \qquad i \in [c], \quad j \in [v_i].$$

Let $\omega_1, \ldots, \omega_m \in \mathcal{W}$ be multi-homogeneous 2-forms induced by $p_1, \ldots, p_m$, with $\deg(\omega_r) = \boldsymbol{\delta}_r$ and $|\boldsymbol{\delta}_r| = 2$, that vanish on the product of the hidden spaces, and set

$$\mathfrak{A} = \langle \omega_1, \ldots, \omega_m \rangle, \qquad \mathfrak{B} = \langle \eta_{i,j} : i \in [c],\ j \in [v_i] \rangle.$$

Then $\mathfrak{A} \subseteq \mathfrak{B}$. For $\mathbf{d} \in \mathbb{N}^c$, define

$$\mathcal{M}_{\mathbf{d},\boldsymbol{\Omega}} : \bigoplus_{r=1}^{m} \mathcal{W}_{\mathbf{d}-\boldsymbol{\delta}_r} \longrightarrow \mathcal{W}_{\mathbf{d}}, \qquad (b_r)_{r=1}^m \longmapsto \sum_{r=1}^{m} b_r \wedge \omega_r,$$

where $\boldsymbol{\Omega} = (\omega_1, \ldots, \omega_m)$ and $\mathcal{W}_{\mathbf{a}} = 0$ if some coordinate of $\mathbf{a}$ is negative. Its image is $\mathfrak{A}_{\mathbf{d}}$, so

$$\dim \ker \mathcal{M}_{\mathbf{d},\boldsymbol{\Omega}}^\vee = \dim \mathcal{W}_{\mathbf{d}}/\mathfrak{A}_{\mathbf{d}} \geq \dim \mathcal{W}_{\mathbf{d}}/\mathfrak{B}_{\mathbf{d}} = \prod_{i=1}^{c} \binom{o_i}{d_i}, \tag{4.11}$$

where $\mathcal{M}^{\vee}_{\mathbf{d},\boldsymbol{\Omega}}$ is the dual map of $\mathcal{M}_{\mathbf{d},\boldsymbol{\Omega}}$. Similarly, let $M_{\mathbf{d},\boldsymbol{\Omega}}$ denote the multidegree-$\mathbf{d}$ Macaulay matrix associated with $\omega_1, \ldots, \omega_m$, defined analogously to M_d.

Theorem 4.7. *Let* $\mathbf{1} \leq \mathbf{d} \leq \mathbf{o}$*, where* $\mathbf{o} = (o_1, \ldots, o_c)$*. If*

$$\dim \mathcal{W}_{\mathbf{d}}/\mathfrak{A}_{\mathbf{d}} = \dim \mathcal{W}_{\mathbf{d}}/\mathfrak{B}_{\mathbf{d}},$$

then all the forms $\eta_{i,j}$*, and hence the hidden spaces, can be recovered from the right kernel of the multidegree-*$\mathbf{d}$ *Macaulay matrix* $M_{\mathbf{d},\boldsymbol{\Omega}}$*.*

Proof. Apply Theorem 4.2 to the multi-graded quotient map that sends each $e^{i,j}$ with $j \leq v_i$ to $-\sum_{k>v_i} a_{i,j,k} e^{i,k}$ and fixes the remaining basis vectors: the identity block normalizes the right-kernel basis, from which all $a_{i,j,k}$ are read block by block. □

Remark 4.8.

1. In [19, §7], the wedge attack is extended to UOV systems over fields of odd characteristic by passing from the symmetric algebra to an exterior algebra on two copies of the underlying vector space. More precisely, let $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be homogeneous quadratic polynomials with oil space $\mathcal{O} \subseteq \mathbb{F}_q^n$. For each i, define an alternating bilinear form on $\mathbb{F}_q^n \oplus \mathbb{F}_q^n$ by

$$\omega_i\big((\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{d})\big) = p_i(\mathbf{b}+\mathbf{c}) - p_i(\mathbf{a}+\mathbf{d}) - p_i(\mathbf{b}) - p_i(\mathbf{c}) + p_i(\mathbf{a}) + p_i(\mathbf{d}).$$

   With respect to the decomposition $\mathbb{F}_q^n \oplus \mathbb{F}_q^n$, the form ω_i has bidegree $(1,1)$; hence $\omega_i \in \mathcal{W}_{1,1}$ for $\mathcal{W} = \bigwedge((\mathbb{F}_q^n \oplus \mathbb{F}_q^n)^*)$. Moreover, ω_i vanishes on $\mathcal{O} \oplus \mathcal{O}$. Thus the resulting system is a Multi-UOV instance, and the multi-wedge attack described above can be applied to recover $\mathcal{O} \oplus \mathcal{O}$, and hence $\mathcal{O}$.
2. Under the assumption that the multi-homogeneous polynomial system is semi-regular, the Hilbert series of the ideal $\mathcal{I}$ (resp. $\mathfrak{A}$) can be computed by the formula in §2. The conditions in Theorems 4.5 and 4.7 can be checked by computing the Hilbert series of $\mathcal{I}$ (resp. $\mathfrak{A}$) and $\mathcal{J}$ (resp. $\mathfrak{B}$).
3. The complexity of the wedge attack is dominated by the complexity of computing the right kernel of the multidegree Macaulay matrix $M_{\mathbf{d}}$ (resp. $M_{\mathbf{d},\boldsymbol{\Omega}}$).

4.3 Limitations of Hilbert Series-Based Degree Estimation

In this subsection, we discuss the limitations of using Hilbert series to estimate a degree at which the wedge attack succeeds. The estimates derived from the semi-regularity definitions in §2 assume that the public polynomials are semi-regular in the relevant truncated algebra. This assumption may fail for structured UOV systems. We focus below on the total-degree phenomenon observed in our experiments; the multidegree case is analogous.

Compared with a random system, the polynomial system $p_1, \cdots, p_m$ arising from a UOV instance has additional algebraic structure, which may cause semi-regularity to fail. This phenomenon in the total-degree setting was also observed in [10].

By Theorem 4.1, the wedge attack succeeds when equality holds in Eq. (4.2). A Hilbert-series estimate instead uses the condition

$$[H_{R/I}(t)]_d \le [H_{R/J}(t)]_d, \tag{4.12}$$

to estimate a degree d at which the wedge attack may become effective, where $[\cdot]_d$ denotes the degree-d coefficient of a power series.

In practice, the condition in Eq. (4.12) is not necessary for a successful attack, because $[H(t)]_d$ need not equal the actual dimension $\dim(R_d/I_d)$. Nevertheless, when

$$[H_{R/I}(t)]_d < [H_{R/J}(t)]_d,$$

we observe that

$$\dim R_d/I_d = [H_{R/J}(t)]_d$$

with high probability in our experiments. In this case, Theorem 4.1 recovers $\mathcal{O}$ from $\ker \mathcal{M}_d^{\vee}$.

Moreover, we found examples in which Eq. (4.12) is satisfied but $\dim R_d/I_d$ still exceeds $[H_{R/J}(t)]_d$, causing the wedge attack to fail; see Appendix A. Fortunately, in our experiments on practical small-parameter UOV instances, this situation occurs only rarely. However, for larger parameters, our understanding remains limited by computational resource constraints. Determining the parameter ranges for which the Hilbert series of a UOV system can be computed exactly remains an open problem in both the truncated-polynomial-ring and exterior-algebra settings.

In Table 1, we report experimental results on the effectiveness of the wedge attack for UOV(n, o, m, q) instances across different parameter sets. The results show that, for most small-parameter UOV instances, the wedge attack remains effective even when the underlying system is not semi-regular.

Table 1: Experimental effectiveness of the wedge attack. Here D is the smallest degree with $T_1(D) \le T_o(D)$, where $T_1(D)$ is the coefficient of t^D in Eq. (2.1), $T_o(D) = [H_{R/J}]_D$, and $T_{\text{uov}}(D) = \dim(R_D/I_D)$. The last column reports the number of failures among 1000 trials.

(n, o, m, q, ℓ)	D	$T_{\text{uov}}(D)$	$T_1(D)$	$T_o(D)$	Failures
(6,4,3,2,1)	3	4	0	4	792/1000
(6,4,4,2,1)	3	4	0	4	335/1000
(6,4,5,2,1)	3	4	0	4	94/1000
(6,4,6,3,1)	3	16	14	16	251/1000
(8,3,5,3,1)	6	1	0	1	1/1000
(8,3,6,3,1)	5	3	0	3	2/1000
(8,3,7,3,1)	5	3	0	3	0/1000
(10,4,6,2,1)	4	1	0	1	10/1000
(10,4,8,2,1)	4	1	0	1	0/1000

Remark 4.9. Note that in Table 1, the Hilbert-series-based estimate of the degree D fails to predict the success of the wedge attack only in particularly unfavorable cases, such as $(n, o, m, q, \ell) = (6, 4, 3, 2, 1)$. In most other cases, this estimate of D is effective.

At the same time, comparing $T_{\text{uov}}(D)$ with $T_1(D)$ shows that UOV instances are generally not semi-regular. Nevertheless, when $T_1(D) < T_o(D)$, we typically observe that $T_{\text{uov}}(D) = T_o(D)$, which indicates that the wedge attack remains effective in these cases.

5 Applications

In this section, we apply the multi-wedge attack to SNOVA [21]. The wedge attack has also been independently applied to SNOVA in [4, 20], but those approaches are restricted to fields of even characteristic. Our approach also applies in odd characteristic and may be viewed as a generalization of the framework in [19, 11, 7].

We refer the reader to [21] for the full description of SNOVA. We first derive the relevant multi-homogeneous systems and then apply the truncated and exterior-algebra recovery criteria of Theorems 4.5 and 4.7, respectively.

5.1 Common reduction to multi-homogeneous systems

We begin by reformulating the recovery problem as the S-stable UOV problem. Two related systems are then obtained through reconciliation and lifting-intersection techniques, respectively.

Definition 5.1 (S-stable UOV problem). *Let $n, v, o, \ell \in \mathbb{N}$ with $v > o$ and $n = v + o$. Let $S \in \mathbb{F}_q^{\ell \times \ell}$ be a symmetric matrix with an irreducible characteristic polynomial. For $0 \le i \le \ell - 1$, define*

$$\Lambda_{S^i} := I_n \otimes S^i \in \mathbb{F}_q^{n\ell \times n\ell}.$$

Given a homogeneous quadratic map

$$(p_1, \ldots, p_m) : \mathbb{F}_q^{n\ell} \to \mathbb{F}_q^m$$

that vanishes on an $o\ell$-dimensional subspace $\mathcal{O} \subset \mathbb{F}_q^{n\ell}$ satisfying

$$\Lambda_{S^i}\mathbf{x} \in \mathcal{O}, \qquad \forall\, \mathbf{x} \in \mathcal{O}, \quad 0 \le i \le \ell - 1, \tag{5.1}$$

find the subspace $\mathcal{O}$.

The quadratic polynomials $p_1, \ldots, p_m$ admit the matrix representation given in [21]:

$$p_i(\mathbf{x}) = \mathbf{x}^\top P_i\, \mathbf{x}, \quad i = 1, \ldots, m, \tag{5.2}$$

where $P_i \in \mathbb{F}_q^{n\ell \times n\ell}$. Thus, the S-stable UOV problem amounts to finding an $o\ell$-dimensional subspace $\mathcal{O} \subset \mathbb{F}_q^{n\ell}$ such that

$$\mathbf{x}^\top \cdot \Lambda_{S^a} \cdot P_i \cdot \Lambda_{S^b} \cdot \mathbf{y} = 0 \tag{5.3}$$

for all $\mathbf{x}, \mathbf{y} \in \mathcal{O}$, $1 \le i \le m$, and $0 \le a, b \le \ell - 1$.

Remark 5.2. In general, Eq. (5.3) does not follow directly from Eq. (5.1) and Eq. (5.2). In SNOVA, however, the matrices $P_1, \ldots, P_m$ are constructed so that

$$\mathbf{x}^\top \cdot P_i \cdot \mathbf{y} = 0, \quad \forall\, \mathbf{x}, \mathbf{y} \in \mathcal{O}, \quad i = 1, \cdots, m, \tag{5.4}$$

which yields the required reformulation.

Let $\lambda \in \mathbb{F}_{q^\ell}$ be an eigenvalue of S, and let $\xi \in \mathbb{F}_{q^\ell}^\ell$ be a corresponding eigenvector. Let $\tau : \mathbb{F}_{q^\ell} \to \mathbb{F}_{q^\ell}$ denote the Frobenius map $z \mapsto z^q$. Since the characteristic polynomial of S is irreducible, every $\mathbf{x} \in \mathbb{F}_q^{n\ell}$ has a unique decomposition

$$\mathbf{x} = \sum_{i=1}^{\ell} \mathbf{x}_i \otimes \tau^{i-1}(\xi), \quad \mathbf{x}_i \in \mathbb{F}_{q^\ell}^n\,. \tag{5.5}$$

Moreover, $\mathbf{x}_i = \tau^{i-1}(\mathbf{x}_1)$.

We define $p_{i,a,b}(\mathbf{x}) = \mathbf{x}^\top \Lambda_{S^a} P_i \Lambda_{S^b}\, \mathbf{x}$. Expanding $\mathbf{x}$ in the eigenbasis gives

$$\begin{aligned} p_{i,a,b}(\mathbf{x}) &= \Big(\sum_{r=1}^{\ell} \mathbf{x}_r \otimes \tau^{r-1}(\xi)\Big)^\top \cdot \Lambda_{S^a} \cdot P_i \cdot \Lambda_{S^b} \cdot \Big(\sum_{s=1}^{\ell} \mathbf{x}_s \otimes \tau^{s-1}(\xi)\Big) \\ &= \sum_{r=1}^{\ell}\sum_{s=1}^{\ell} \tau^{r-1}(\lambda^a)\tau^{s-1}(\lambda^b) \cdot \Big(\mathbf{x}_r \otimes \tau^{r-1}(\xi)\Big)^\top \cdot P_i \cdot \Big(\mathbf{x}_s \otimes \tau^{s-1}(\xi)\Big) \end{aligned} \tag{5.6}$$

For $1 \le r, s \le \ell$, define

$$\begin{aligned} \bar{p}_{i,r,s}(\mathbf{x}_1, \cdots, \mathbf{x}_\ell) :&= \Big(\mathbf{x}_r \otimes \tau^{r-1}(\xi)\Big)^\top \cdot P_i \cdot \Big(\mathbf{x}_s \otimes \tau^{s-1}(\xi)\Big) \\ &= \mathbf{x}_r^\top \cdot \bar{P}_{i,(r,s)} \cdot \mathbf{x}_s, \quad 1 \le r, s \le \ell, \end{aligned} \tag{5.7}$$

where $\bar{P}_{i,(r,s)} \in \mathbb{F}_{q^\ell}^{n\times n}$ is defined by

$$\bar{P}_{i,(r,s)} := \Big(\tau^{r-1}(\xi) \otimes I_n\Big)^\top \cdot P_i \cdot \Big(\tau^{s-1}(\xi) \otimes I_n\Big).$$

Multi-homogeneous polynomial formulation The following result was established in [14, 5, 8].

Proposition 5.3. *Assume that $\mathcal{O} \subseteq \mathbb{F}_q^{n\ell}$ is an $o\ell$-dimensional subspace satisfying Eq. (5.1) and Eq. (5.3). Then the following statements hold.*

(i) *There exist $\mathbb{F}_{q^\ell}$-linear subspaces*

$$\mathcal{O}_1, \ldots, \mathcal{O}_\ell \subseteq \mathbb{F}_{q^\ell}^n, \qquad \dim(\mathcal{O}_r) = o \quad (1 \le r \le \ell),$$

such that

$$\mathcal{O}_1 \times \cdots \times \mathcal{O}_\ell \subseteq V_{\mathbb{F}_{q^\ell}}\big(\bar{p}_{i,r,s} : 1 \le i \le m,\ 1 \le r, s \le \ell\big). \tag{5.8}$$

Moreover, $\mathcal{O}_r = \tau^{r-1}(\mathcal{O}_1)$ for every $1 \le r \le \ell$.

(ii) *Let W_1 and W_2 be invertible linear combinations of $\bar{P}_{1,(1,1)}, \ldots, \bar{P}_{o,(1,1)}$. For $a \in \{1,2\}$, set*

$$L_{a,r} := \left(\tau^{r-1}(W_a)\right)^{-1},$$

and define the componentwise lifting intersections by

$$\mathcal{I}_r := \tau^{r-1}(W_1)\mathcal{O}_r \cap \tau^{r-1}(W_2)\mathcal{O}_r.$$

Then

$$\mathcal{I}_1 \times \cdots \times \mathcal{I}_\ell \subseteq V_{\mathbb{F}_{q^\ell}}\left(\bar{p}_{i,r,s}^{(a,b)}(\mathbf{x}_1, \ldots, \mathbf{x}_\ell) : {}^{1\le i\le m,\ 1\le r,s\le \ell,}_{a,b\in\{1,2\}}\right), \tag{5.9}$$

where

$$\bar{p}_{i,r,s}^{(a,b)}(\mathbf{x}_1, \ldots, \mathbf{x}_\ell) := \mathbf{x}_r^\top L_{a,r}^\top \bar{P}_{i,(r,s)} L_{b,s} \mathbf{x}_s.$$

Moreover, $\mathcal{I}_r = \tau^{r-1}(\mathcal{I}_1)$ for every $1 \le r \le \ell$.

Alternating-form formulation For $1 \le r, s \le \ell$, define

$$\bar{q}_{i,r,s}(\mathbf{x}_1, \ldots, \mathbf{x}_\ell) := \bar{p}_{i,r,s}(\mathbf{x}_1, \ldots, \mathbf{x}_\ell) - \bar{p}_{i,s,r}(\mathbf{x}_1, \ldots, \mathbf{x}_\ell). \tag{5.10}$$

Similarly, for $a, b \in \{1,2\}$, define

$$\bar{q}_{i,r,s}^{(a,b)} := \bar{p}_{i,r,s}^{(a,b)} - \bar{p}_{i,s,r}^{(b,a)}.$$

The polar forms associated with $\bar{q}_{i,r,s}$ and $\bar{q}_{i,r,s}^{(a,b)}$ are alternating 2-forms, denoted by $\omega_{i,r,s}$ and $\omega_{i,r,s}^{(a,b)}$, respectively. Proposition 5.3 implies that $\omega_{i,r,s}$ vanishes on $\mathcal{O}_1 \times \cdots \times \mathcal{O}_\ell$, whereas $\omega_{i,r,s}^{(a,b)}$ vanishes on $\mathcal{I}_1 \times \cdots \times \mathcal{I}_\ell$.

5.2 Application of the multi-wedge attack to SNOVA

Fix $\nu > 0$ and $1 \le \ell' \le \ell$, and work over

$$\mathcal{R}^{(p^\nu)} = \mathbb{F}_{q^\ell}[\mathbf{x}_1, \ldots, \mathbf{x}_{\ell'}]/\langle x_{rj}^{p^\nu} : r \in [\ell'],\ j \in [n]\rangle, \qquad \deg(x_{rj}) = \mathbf{e}_r.$$

The reconciliation and lifting-intersection systems are, respectively,

$$\mathcal{P}_{\mathrm{rec}} = \{\bar{p}_{i,r,s} : i \in [m],\ r, s \in [\ell']\}, \qquad \mathcal{P}_{\mathrm{int}} = \{\bar{p}_{i,r,s}^{(a,b)} : i \in [m],\ r, s \in [\ell'],\ a, b \in [2]\}.$$

Every polynomial indexed by (r, s) has multidegree $\mathbf{e}_r + \mathbf{e}_s$. For $\star \in \{\mathrm{rec}, \mathrm{int}\}$, let $\mathcal{A}_\star$ be the ideal generated by $\mathcal{P}_\star$, and let $\mathcal{B}_\star$ be the linear ideal defining the corresponding product of hidden spaces: the $\mathcal{O}_r$ for $\star = \mathrm{rec}$ and the $\mathcal{I}_r$ for $\star = \mathrm{int}$. Proposition 5.3 gives $\mathcal{A}_\star \subseteq \mathcal{B}_\star$. Hence, by Theorem 4.5, the right kernel of the multidegree $\mathbf{d}$ Macaulay matrix recovers all component hidden spaces whenever

$$\dim \mathcal{R}_{\mathbf{d}}^{(p^\nu)}/(\mathcal{A}_\star)_{\mathbf{d}} = \dim \mathcal{R}_{\mathbf{d}}^{(p^\nu)}/(\mathcal{B}_\star)_{\mathbf{d}} > 0, \qquad \mathbf{d} \ge \mathbf{1}. \tag{5.11}$$

The same systems admit an exterior-algebra formulation. Put $E_r = (\mathbb{F}_{q^\ell}^n)^*$ and $\mathcal{W} = \bigotimes_{r=1}^{\ell'} \bigwedge E_r$. Let $\boldsymbol{\Omega}_\star$ be the nonzero alternating forms obtained from $\mathcal{P}_\star$, let $\mathfrak{a}_\star = \langle \boldsymbol{\Omega}_\star \rangle$, and let $\mathfrak{b}_\star$ be the ideal generated by the linear polynomials defining the corresponding component hidden spaces. Their vanishing gives $\mathfrak{a}_\star \subseteq \mathfrak{b}_\star$. The exterior Macaulay map is

$$\mathcal{M}_{\mathbf{d},\boldsymbol{\Omega}_\star} : \bigoplus_{\omega \in \boldsymbol{\Omega}_\star} \mathcal{W}_{\mathbf{d}-\deg\omega} \longrightarrow \mathcal{W}_{\mathbf{d}}, \qquad (b_\omega)_\omega \longmapsto \sum_\omega b_\omega \wedge \omega.$$

If h_r denotes the dimension of the hidden space in block r, then Theorem 4.7 recovers all component spaces from the right kernel of this map whenever $\mathbf{1} \le \mathbf{d} \le (h_1, \ldots, h_{\ell'})$ and

$$\dim \mathcal{W}_{\mathbf{d}}/(\mathfrak{a}_\star)_{\mathbf{d}} = \dim \mathcal{W}_{\mathbf{d}}/(\mathfrak{b}_\star)_{\mathbf{d}} = \prod_{r=1}^{\ell'} \binom{h_r}{d_r}. \tag{5.12}$$

Finally, $\mathcal{O}_r = \tau^{r-1}(\mathcal{O}_1)$ in the reconciliation case, so one recovered component determines the original S-stable oil space $\mathcal{O}$. Both formulations may be restricted to the first ℓ' blocks and combined with the unbalanced-down technique of [4], thereby extending the methods in [7, 4, 20].

A Counterexample to the Wedge Attack

We provide the following counterexample to the wedge attack in [19].

Consider parameters $p = 2$, $\ell = 1$, $q = 2(= 2^1)$, $n = 10$, $o = 4$, and $m = 6$. Then $v = n - o = 6$. Note that

$$\min\{\frac{o-1}{2}, 2\} \cdot m = 9 > v = 6 > o = 4$$

and

$$\sum_{i=0}^{\lfloor \frac{o}{2} \rfloor} (-1)^i \binom{m+i-1}{i} \binom{v+o}{v+2i} = \binom{10}{6} - 6 \cdot \binom{10}{8} + \binom{7}{2} \cdot \binom{10}{10} = -39 \le 1.$$

Hence the tuple $(v = 6, o = 4, m = 6)$ is admissible in the sense of [19].

Consider the following UOV($v = 6, o = 4, m = 6, q = 2$) system:

$$\begin{aligned}
f_1 &= x_1x_1 + x_1x_4 + x_1x_5 + x_1x_7 + x_1x_9 + x_2x_2 + x_2x_3 + x_2x_6 + x_2x_7 + x_2x_9 + x_2x_{10} \\
&\quad + x_3x_3 + x_3x_4 + x_3x_5 + x_3x_6 + x_3x_8 + x_3x_9 + x_4x_5 + x_4x_8 + x_4x_9 + x_5x_5 + x_5x_6 \\
&\quad + x_5x_7 + x_5x_8 + x_6x_6 + x_6x_8 + x_6x_9, \\
f_2 &= x_1x_1 + x_1x_4 + x_1x_7 + x_1x_9 + x_2x_3 + x_2x_4 + x_2x_5 + x_2x_7 + x_2x_{10} + x_3x_3 + x_3x_5 \\
&\quad + x_3x_8 + x_3x_9 + x_4x_5 + x_4x_7 + x_5x_6 + x_5x_7 + x_6x_8 + x_6x_9, \\
f_3 &= x_1x_1 + x_1x_4 + x_1x_5 + x_1x_8 + x_1x_9 + x_2x_2 + x_2x_4 + x_2x_7 + x_2x_{10} + x_3x_6 + x_3x_7 \\
&\quad + x_3x_9 + x_4x_4 + x_4x_7 + x_5x_6 + x_5x_8 + x_6x_6, \\
f_4 &= x_1x_2 + x_1x_5 + x_1x_8 + x_1x_9 + x_1x_{10} + x_2x_2 + x_2x_5 + x_2x_6 + x_2x_8 + x_2x_{10} + x_3x_4 \\
&\quad + x_3x_7 + x_3x_9 + x_3x_{10} + x_4x_5 + x_4x_7 + x_4x_8 + x_5x_5 + x_5x_6 + x_5x_7 + x_5x_9 + x_6x_7, \\
f_5 &= x_1x_1 + x_1x_3 + x_1x_6 + x_1x_{10} + x_2x_4 + x_2x_5 + x_2x_9 + x_3x_7 + x_3x_8 + x_3x_{10} + x_4x_6 \\
&\quad + x_4x_9 + x_5x_6 + x_5x_8, \\
f_6 &= x_1x_2 + x_1x_3 + x_1x_4 + x_1x_7 + x_1x_8 + x_1x_9 + x_1x_{10} + x_2x_4 + x_2x_5 + x_2x_6 + x_2x_{10} \\
&\quad + x_3x_3 + x_3x_6 + x_3x_9 + x_3x_{10} + x_4x_5 + x_4x_6 + x_4x_7 + x_4x_8 + x_4x_{10} + x_5x_6 + x_5x_7 \\
&\quad + x_5x_8 + x_5x_9 + x_6x_9 + x_6x_{10}.
\end{aligned} \tag{A.1}$$

In

$$A_2 := \mathbb{F}_2[x_1, \ldots, x_{10}]/\langle x_1^2, \ldots, x_{10}^2\rangle,$$

we consider the Macaulay matrix $\mathcal{M}_d^{(2)}$ for each d. Define

$$T_1(d) = \text{the coefficient of } z^d \text{ in } \Big[\frac{(1 + z + \cdots + z^{p^\ell - 1})^n}{(1 + z^2 + \cdots + z^{2(p^\ell - 1)})^m}\Big]_+, \tag{A.2}$$

$$T_o(d) = \text{the coefficient of } z^d \text{ in } (1 + z + \cdots + z^{p^\ell - 1})^o. \tag{A.3}$$

For $(p, \ell, n, o, m) = (2, 1, 10, 4, 6)$, we have

$$\begin{aligned}
\frac{(1+z)^{10}}{(1+z^2)^6} &= 1 + 10z + 39z^2 + 60z^3 - 39z^4 + \cdots, \\
(1+z)^4 &= 1 + 4z + 6z^2 + 4z^3 + z^4.
\end{aligned}$$

We obtain the following table:

Table 2: The dimensions of the Macaulay matrices $\mathcal{M}_d^{(2)}$ in A_2, together with $T_1(d)$ and $T_o(d)$, for UOV($v = 6, o = 4, m = 6, q = 2$). Here d is the degree; "rows" and "cols" denote the numbers of rows and columns of $\mathcal{M}_d^{(2)}$, respectively; "rank" is the rank over $\mathbb{F}_2$; $\dim\ker \mathcal{M}_d^{(2)} = \text{cols} - \text{rank}$; and $T_1(d)$ and $T_o(d)$ are the coefficient values defined above.

d	rows	cols	rank	$\dim\ker \mathcal{M}_d^{(2)}$	$T_1(d)$	$T_o(d)$
0	0	1	0	1	1	1
1	0	10	0	10	10	4
2	6	45	6	39	39	6
3	60	120	60	60	60	4
4	270	210	208	2	0	1
5	720	252	252	0	0	0

Bibliography

[1] Baena, J., Cabarcas, D., Tiwari, S.K., Verbel, J., Villota, L.: Admissible parameters for the crossbred algorithm and semi-regular sequences over finite fields. Designs, Codes and Cryptography **93**(7), 2561–2589 (2025)

[2] 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)

[3] Beullens, W.: Improved cryptanalysis of uov and rainbow. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 348–373. Springer (2021)

[4] Bros, M., Le, T.H., Lichtinger, J., Minaud, B., Perlner, R., Smith-Tone, D., Valenzuela, C.: Exploiting SNOVA's structure in the wedge product attack. Cryptology ePrint Archive (2026)

[5] Cabarcas, D., Li, P., Verbel, J., Villanueva-Polanco, R.: Improved attacks for SNOVA by exploiting stability under a group action. In: Annual International Cryptology Conference. pp. 358–389. Springer (2025)

[6] Ding, J., Yang, B.Y., Chen, C.H.O., Chen, M.S., Cheng, C.M.: New differential-algebraic attacks and reparametrization of Rainbow. In: Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings 6. pp. 242–257. Springer (2008)

[7] Furue, H., Ikematsu, Y.: Key recovery attacks on uov using p^l-truncated polynomial rings. Cryptology ePrint Archive (2026)

[8] Furue, H., Ikematsu, Y., Nakamura, S., Akiyama, R.: Improved cryptanalysis of snova by solving multi-homogeneous systems via matrix transformations. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 405–435. Springer (2025)

[9] Garey, M.R., Johnson, D.S.: Computers and intractability, vol. 174. freeman San Francisco (1979)

[10] Ikematsu, Y., Saito, T.: Hilbert series for systems of uov polynomials. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **107**(3), 275–282 (2024)

[11] Jin, Y., Pan, Y., He, X., Gong, B., Ding, J.: Security analysis on uov families with odd characteristics: Using symmetric algebra. In: IACR International Conference on Public-Key Cryptography. pp. 428–454. Springer (2026)

[12] Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: Annual international cryptology conference. pp. 257–266. Springer (1998)

[13] Le, H., Bros, M., Lichtinger, J., Minaud, B., Perlner, R., Smith-Tone, D., Valenzuela, C.: Exploiting snova's structure in the wedge product attack. In: NIST 6th PQC Standardization Conference (2025)

[14] Li, P., Ding, J.: Cryptanalysis of the SNOVA signature scheme. In: International Conference on Post-Quantum Cryptography. pp. 79–91. Springer (2024)
[15] Nakamura, S., Ikematsu, Y., Wang, Y., Ding, J., Takagi, T.: New complexity estimation on the Rainbow-Band-Separation attack. Theoretical Computer Science **896**, 1–18 (2021)
[16] Nakamura, S., Wang, Y., Ikematsu, Y.: A new analysis of the Kipnis-Shamir method solving the minrank problem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E106.A**(3), 203–211 (2023)
[17] Patarin, J.: The oil and vinegar algorithm for signatures. In: Dagstuhl Workshop on Cryptography, 1997 (1997)
[18] Perlner, R., Smith-Tone, D.: Rainbow band separation is better than we thought. Cryptology ePrint Archive, Paper 2020/702 (2020)
[19] Ran, L.: Wedges, oil, and vinegar: An analysis of uov in the exterior algebra. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 363–388. Springer (2026)
[20] Tseng, P.E., Wang, L.C., Li, P., Kuan, Y.L.: Investigating the wedge map on SNOVA. Cryptology ePrint Archive (2026)
[21] Wang, L.C., Tseng, P.E., Kuan, Y.L., Chou, C.Y.: A simple noncommutative UOV scheme. Cryptology ePrint Archive (2022)