The complexity of solving Weil restriction systems

THE COMPLEXITY OF SOLVING WEIL RESTRICTION SYSTEMS

ALESSIO CAMINATA, MICHELA CERIA, AND ELISA GORLA

Abstract. The solving degree of a system of multivariate polynomial equations provides an upper bound for the complexity of computing the solutions of the system via Gröbner basis methods. In this paper, we consider polynomial systems that are obtained via Weil restriction of scalars. The latter is an arithmetic construction which, given a finite Galois field extension $k \hookrightarrow K$, associates to a system $\mathcal{F}$ defined over K a system Weil($\mathcal{F}$) defined over k, in such a way that the solutions of $\mathcal{F}$ over K and those of Weil($\mathcal{F}$) over k are in natural bijection. In this paper, we find upper bounds for the complexity of solving a polynomial system Weil($\mathcal{F}$) obtained via Weil restriction in terms of algebraic invariants of the system $\mathcal{F}$.

1. Introduction

The Weil restriction of scalars is a construction which is of interest mostly within arithmetic geometry and number theory. Given a finite Galois field extension $k \hookrightarrow K$, it allows one to associate an object defined over k to one defined over K, with the properties that their rational points are in natural bijection. This object can be for example a quasi-projective variety, or an affine or projective scheme. In the case when we start with an affine or projective scheme defined by a system of polynomial equations $\mathcal{F}$ defined over K, then the Weil restriction of scalars associates to $\mathcal{F}$ a system Weil($\mathcal{F}$) defined over k: the defining equations of the Weil restriction of the original scheme. As we already mentioned, the solutions of $\mathcal{F}$ over K and those of Weil($\mathcal{F}$) over k are in natural bijection.

In this situation, the Weil restriction of scalars is of interest also within cryptography. This construction has found applications within elliptic and hyperelliptic curve cryptography, where it is used to compute discrete logarithms, see e.g. [Gau09]. The Discrete Logarithm Problem is a computational problem of central important in public-key cryptography, as several cryptographic primitives rely on its hardness for their security. The Weil restriction is also used in multivariate cryptography, one of the current proposals for building post-quantum resistant cryptographic primitives. In this context, the Weil restriction of scalars is useful in order to construct polynomial systems in such a way that their algebraic structure is disguised, so that the designer of the system is the only one who has at their disposal an efficient algorithm to compute its solutions, see e.g.[Pat96].

Mathematics Subject Classification (2020): 13P10, 13P15, 13P25.

Keywords and phrases: Weil restriction, solving degree, degree of regularity, Gröbner basis

The first author is supported by the Italian PRIN2020, Grant number 2020355B8Y "Squarefree Gröbner degenerations, special varieties and related topics" and by the European Union within the program NextGenerationEU.

The Weil restriction of scalars is also used, although never explicitly mentioned, in coding theory. For example, one can regard spread codes as the rational points of the Weil restriction of scalars of a Grassmannian of lines with respect to an extension of finite fields, see [MGR08]. The algebraic structure of spread codes makes their decoding particularly efficient, see [GMR12].

We are interested in estimating the complexity of solving a system of polynomial equations obtained via Weil restriction of scalars by using Gröbner basis methods. It is well-known that computing the reduced lexicographic Gröbner basis of a system of polynomial equations allows one to compute the solutions of the system, assuming that they are finitely many and that one can efficiently compute the roots of univariate polynomials. This is the case, e.g., over finite fields. Currently, some of the most efficient families of algorithms for computing a Gröbner basis are those based on linear algebra, including [Fau99, CKPS00, Fau02]. Their complexity is bounded from above by a known function of an invariant of the system, called the solving degree. In this paper we give upper bounds for the solving degree of the Weil restriction of a system of polynomial equations in terms of algebraic invariants of the original system. This gives an upper bound on the complexity of solving the Weil restriction system.

The paper is organized as follows. In Section 2 we define the solving degree of a polynomial system and recall the definition and some facts on the Weil restriction of scalars. The main result of Section 3 is Theorem 3.3, where we compute some algebraic invariants of $\mathrm{Weil}(\mathcal{F})$ in terms of those of $\mathcal{F}$. As a consequence, in Corollary 3.4 we derive an upper bound for the solving degree of a homogeneous Weil restriction system. In Section 4 we derive the desired upper bounds for the solving degree of a (not necessarily homogeneous) Weil restriction system. In particular, in Theorem 4.7 we give an upper bound for the solving degree of $\mathrm{Weil}(\mathcal{F})$ in terms of the Castelnuovo-Mumford regularity of the system obtained from $\mathcal{F}$ by homogenizing its equations. In Corollary 4.12 we do the same for a system to which we have added the field equations and in Proposition 4.13 we relate the degree of regularity of a Weil restriction system to that of the original system.

2. Preliminaries

In this section we present the definitions and preliminary results that we rely on in the rest of the paper. In § 2.1, we briefly recall the definitions of solving degree and degree of regularity. We limit ourselves to the basic notions necessary to define these two invariants and we refer to [CG21] for a more detailed exposition. In § 2.2, we recall the construction of Weil restriction and we present an algebraic proof of Weil's Theorem in the affine case.

2.1. **Solving degree and degree of regularity.** Let K be a field and let $R = K[x_1, \dots, x_m]$ be a polynomial ring in m variables over K, equipped with the degree reverse lexicographic term order. We consider a (not necessarily homogeneous) polynomial system $\mathcal{F} = \{f_1, \dots, f_r\}$ in R . The *linear algebra based algorithms* for solving the system $\mathcal{F}$ transform the problem of computing a Gröbner basis of the ideal generated by $\mathcal{F}$ into one or more instances of Gaussian elimination of Macaulay matrices. These are constructed as follows. For any degree $d \in \mathbb{Z}_+$ the *Macaulay matrix* $M_{\leq d}$ of $\mathcal{F}$ has columns indexed by the terms of R of degree $\leq d$, sorted in decreasing order from left to right. The rows of $M_{\leq d}$ are indexed

by the polynomials $m_{i,j}f_j$, where $m_{i,j}$ is a term in R such that $\deg(m_{i,j}f_j) \leq d$. The entry (i,j) of $M_{\leq d}$ is the coefficient of the term of column j in the polynomial corresponding to the i-th row.

The size of the Macaulay matrices $M_{\leq d}$, hence the computational complexity of computing their reduced row echelon forms, depends on the degree d. Therefore, it is important to estimate the largest d of the Macaulay matrices involved in the computation of the Gröbner basis. For this reason, Ding and Schmidt [DS13] introduced the concept of solving degree.

Definition 2.1 (Solving degree)**.** Let $\mathcal{F}$ be a polynomial system in R. The *solving degree* of $\mathcal{F}$ (with respect to the degree reverse lexicographic term order) is the least degree d such that Gaussian elimination on the Macaulay matrix $M_{\leq d}$ produces a Gröbner basis of $\mathcal{F}$. We denote it by $\mathrm{sd}(\mathcal{F})$.

Remarks 2.2. 1) One can define and consider the solving degree with respect to any term order. However, it turns out that in practice computations with respect to the degree reverse lexicographic term order are often faster than with respect to any other term order. For this reason, in this paper we will only consider the solving degree with respect to the degree reverse lexicographic term order.

2) Some variants of the algorithms perform Gaussian elimination on $M_{\leq d}$ and then add to the Macaulay matrix $M_{\leq d}$ the rows corresponding to polynomials $h \cdot f$, where h is a term and f is a polynomial such that $\deg(f) < d$ and the leading term of f was not the leading term of any row of $M_{\leq d}$ before performing Gaussian elimination. Throughout the paper, we consider the situation when *no extra rows are inserted*. Notice that the solving degree is still an upper bound on the degree in which the algorithms adopting this variation terminate. See also [CG21, Remark 6] for a more detailed discussion.

The definition of solving degree has an algorithmic nature and it is usually difficult to estimate the solving degree of a polynomial system without solving it. So many authors use the *degree of regularity* introduced by Bardet, Faugère, and Salvy [Bar04, BFS04] as a proxy for the solving degree.

Let I be a homogeneous ideal of R, and let $A = R/I$. For an integer $d \geq 0$, we denote by A_d the homogeneous part of degree d of A. The function $\mathrm{HF}_A(-) : \mathbb{N} \to \mathbb{N}$, $\mathrm{HF}_A(d) = \dim_k A_d$ is called *Hilbert function* of A. The *Hilbert series* of A is defined as $\mathrm{HS}_A(z) = \sum_{j\in\mathbb{N}} \mathrm{HF}_A(j)z^j$. It is well known that for large d, the Hilbert function of A is a polynomial in d called *Hilbert polynomial* and denoted by $\mathrm{HP}_A(d)$.

Definition 2.3 (Degree of regularity)**.** Let $\mathcal{F} = \{f_1, \ldots, f_r\} \subseteq R$ be a system of equations and let $(\mathcal{F}^{\mathrm{top}}) = (f_1^{\mathrm{top}}, \ldots, f_r^{\mathrm{top}})$ be the ideal of R generated by the homogeneous part of highest degree of $\mathcal{F}$. Assume that $(\mathcal{F}^{\mathrm{top}})_d = R_d$ for $d \gg 0$. The *degree of regularity* of $\mathcal{F}$ is

$$d_{\mathrm{reg}}(\mathcal{F}) = \min\{d \geq 0 \mid (\mathcal{F}^{\mathrm{top}})_d = R_d\} = \min\{d \geq 0 \mid \mathrm{HF}_{R/(\mathcal{F}^{\mathrm{top}})}(d) = 0\}.$$

For examples and a discussion on the relation between the solving degree and the degree of regularity of a polynomial system we refer the reader to [CG21, §4.1], [BDDGMT20, §4.1], [T19, Corollary 3.67], [ST21, Theorem 2.1], and [CG23].

In this paper, we use results from [CG21] to produce upper bounds for the solving degree. Some of these results require the assumption that the system is in generic coordinates according to [BS87, Definition 1.5]. We recall the definition for the convenience of the reader. See also [CG22, Remark 5] for a discussion about the generic coordinates assumption over finite fields.

Definition 2.4. Let $I \subseteq R$ be a homogeneous ideal with $\dim(R/I) = d \geq 0$. We say that I is *in generic coordinates over* $\overline{K}$ if x_i is non-zerodivisor mod $(I + (x_m, \ldots, x_{i+1}))^{\text{sat}}$ for all $i = m, m-1, \ldots, m-d+1$, where $(I+(x_m, \ldots, x_{i+1}))^{\text{sat}}$ is the saturation of $I+(x_m, \ldots, x_{i+1})$ with respect to the irrelevant maximal ideal of R.

Remark 2.5. Let $J \subseteq R$ be a homogeneous ideal with $\dim(R/J) = d \geq 0$. Following the terminology of [BS87], denote by $U_d(J)$ the set of d-tuples of homogeneous linear forms $(h_m, \ldots, h_{m-d+1}) \in R_1^d$ such that h_i is non-zerodivisor mod $(J + (h_m, \ldots, h_{i+1}))^{\text{sat}}$ for $i = m, m-1, \ldots, m-d+1$. The terminology that we use in Definition 2.4 is motivated by the observation that, for any given J, there is an open set of coordinate changes

$$U(J) = \{g \in \mathrm{GL}_n(K) \mid (x_m, \ldots, x_{m-d+1}) \in U_d(gJ)\}.$$

Notice that, depending on J and K, $U(J)$ may be the empty set. Definition 2.4 states that $I \subseteq R$ is in generic coordinates over $\overline{K}$ if and only if $\mathrm{Id} \in U(I \otimes_K \overline{K})$. In particular, $U(I \otimes_K \overline{K}) \subseteq \mathrm{GL}_n(\overline{K})$ is a dense open subset of $\mathrm{GL}_n(\overline{K})$.

2.2. **Weil restriction.** Let $k \hookrightarrow K$ be a finite Galois field extension of degree n with Galois group $G = \mathrm{Gal}(K/k)$ and let $\{\alpha_1, \ldots, \alpha_n\}$ be a k-vector space basis of K. We consider two polynomial rings: the polynomial ring $R = K[x_1, \ldots, x_m]$ in m variables over K and the polynomial ring $S = k[x_{i,j}]_{i=1,\ldots,m, j=1,\ldots,n}$ in nm variables over k. We define a K-algebra homomorphism $\psi : R \to S \otimes_k K$ via

$$\psi(x_i) = x_{i,1}\alpha_1 + \cdots + x_{i,n}\alpha_n \quad \forall i = 1, \ldots, m. \tag{1}$$

Definition 2.6. Let $f \in R$ be a polynomial. The *Weil restriction* of f is the set of polynomials $\mathrm{Weil}(f) = \{f_1, \ldots, f_n\} \subseteq S$ defined by

$$f_1\alpha_1 + \cdots + f_n\alpha_n = f(\psi(x_1), \ldots, \psi(x_n)) \in S \otimes_k K,$$

where the right hand side is the image of f under the map $\psi : R \to S \otimes_k K$ defined in (1). If $\mathcal{F} = \{g_1, \ldots, g_r\} \subseteq R$ is a polynomial system, then its Weil restriction is the system $\mathrm{Weil}(\mathcal{F}) = \mathrm{Weil}(g_1) \cup \cdots \cup \mathrm{Weil}(g_r) \subseteq S$. If $I = (g_1, \ldots, g_r)$ is an ideal of R, the Weil restriction of I is the ideal $\mathrm{Weil}(I)$ of S generated by the Weil restrictions of $g_1, \ldots, g_r$. If $V = \mathrm{Spec}(R/I)$ is an affine scheme over K, then the Weil restriction of V is the affine scheme $\mathrm{Weil}(V) = \mathrm{Spec}\,(S/\mathrm{Weil}(I))$ over k.

The definition of Weil restriction of an ideal and of an affine scheme does not depend on the choice of the generators. In fact, the Weil restriction has a more general functorial interpretation.

Remark 2.7. Given a quasi-projective scheme V over K, one can consider the following contravariant functor

$$\begin{aligned}\mathcal{R}_{K|k}(V) : \mathrm{Sch}/k &\to \mathrm{Sets} \\ T &\mapsto \mathrm{Hom}_K(T \times_k K, V).\end{aligned}$$

This functor is representable, i.e., there exists a unique scheme W over k such that $\mathcal{R}_{K|k}(V) \cong \mathrm{Hom}_k(-, W)$. The scheme W is called the Weil restriction of V with respect to the extension $k \subseteq K$. If $V = \mathrm{Spec}(K[x_1, \ldots, x_n]/I)$ is an affine scheme, then its Weil restriction W as defined here coincides with the affine scheme $\mathrm{Weil}(V)$ as defined in Definition 2.6 (see [Nau99, §3, Proposition 2]).

A well-known result by Weil [Weil82] states that for any quasi-projective scheme V over K with Weil restriction $W = \mathrm{Weil}(V)$ there is an isomorphism

$$W \times_k K \cong \prod_{\sigma \in G} V^\sigma,$$

where V^σ denotes the conjugate of V via $\sigma \in G$. We give an algebraic proof of this fact in the affine case. The methods introduced in this proof will be useful throughout the paper.

Theorem 2.8 (Weil)**.** *Let $k \hookrightarrow K$ be a finite Galois field extension of degree n with Galois group G, and let $I \subseteq K[x_1, \ldots, x_m]$ be an ideal. Let $S = k[x_{i,j}]_{i=1,\ldots,m, j=1,\ldots,n}$. Then, there is a K-algebra isomorphism*

$$\Psi : \bigotimes_{\sigma \in G} (K[x_1, \ldots, x_m]/I)^\sigma \longrightarrow (S/\,\mathrm{Weil}(I)) \otimes_k K.$$

Proof. First of all, since the tensor product of polynomial rings is again a polynomial ring, we can fix an isomorphism

$$\bigotimes_{\sigma \in G} K[x_1, \ldots, x_m]^\sigma \cong K[x_{i,\sigma}]_{i=1,\ldots,m,\ \sigma \in G},$$

where the variables $x_{i,\sigma}$ keep track of the action of the Galois group as follows: $\tau \circ x_{i,\sigma} = x_{i,\tau\sigma}$. Similarly, given a polynomial F with coefficients in K, we define an action of $\sigma \in G$ on F by $\sigma(F) = F^\sigma$, where the polynomial F^σ is the same as F, but with all coefficients changed by the action of σ. Notice that this can be applied to polynomials in $K[x_1, \ldots, x_m]$ and $K[x_{i,j}]_{i=1,\ldots,m,j=1,\ldots,n}$. Under the isomorphism above, the product over G of the ideal $I = (F_1, \ldots, F_r)$ corresponds to an ideal generated by polynomials $f_{\sigma,t} = F_t^\sigma(x_{1,\sigma}, \ldots, x_{m,\sigma})$ for $\sigma \in G$ and $t = 1, \ldots, r$.

We define the K-algebra isomorphism

$$\begin{aligned}\Psi : K[x_{i,\sigma}]_{i=1,\ldots,m,\ \sigma \in G} &\longrightarrow K[x_{i,j}]_{i=1,\ldots,m,j=1,\ldots,n} \\ x_{i,\sigma} &\mapsto \sigma(\alpha_1)x_{i,1} + \cdots + \sigma(\alpha_n)x_{i,n}.\end{aligned}$$

The map Ψ is K-linear and its invertibility follows from [Coh03, Proposition 7.6.6], since the associated matrix is block diagonal, with each diagonal block of size $n \times n$ and of the form:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{n-1}(\alpha_1) & \sigma_{n-1}(\alpha_2) & \cdots & \sigma_{n-1}(\alpha_n) \end{pmatrix}^T,$$

where $G = \{\sigma_0 = \mathrm{Id}, \sigma_1, \ldots, \sigma_{n-1}\}$.

We assume for simplicity that $I = (F)$ is principal, with corresponding Weil restriction $\mathrm{Weil}(I) = (f_1, \ldots, f_n)$. To conclude the proof we have to show that $\Psi((f_{\sigma_0}, ..., f_{\sigma_{n-1}})) = (f_1, ..., f_n)$, where the equality is intended as ideals.
We know that $f_\sigma = F^\sigma(x_{1,\sigma}, ..., x_{m,\sigma})$. On the other hand,

$$F\left(\sum_{j=1}^n \alpha_j x_{1,j}, ..., \sum_{j=1}^n \alpha_j x_{m,j}\right) = \alpha_1 f_1(x_{i,j}) + ... + \alpha_n f_n(x_{i,j})$$

by definition of Weil restriction. By letting $\sigma \in G$ act on both sides of the previous equality we obtain

$$F^\sigma\left(\sum_{j=1}^n \sigma(\alpha_j) x_{1,j}, ..., \sum_{j=1}^n \sigma(\alpha_j) x_{m,j}\right) = \sigma(\alpha_1) f_1(x_{i,j}) + ... + \sigma(\alpha_n) f_n(x_{i,j}).$$

On the other hand, $F^\sigma(\sum_{j=1}^n \sigma(\alpha_j) x_{1,j}, ..., \sum_{j=1}^n \sigma(\alpha_j) x_{m,j}) = \Psi(f_\sigma)$. This proves that $\Psi(f_\sigma) = \sigma(\alpha_1) f_1(x_{i,j}) + ... + \sigma(\alpha_n) f_n(x_{i,j})$, which yields $\Psi((f_{\sigma_0}, ..., f_{\sigma_{n-1}})) = (f_1, ..., f_n)$.

If I is not principal, then it suffices to fix a system of generators for I and repeat the same reasoning for each generator. □

3. A commutative algebra approach to Weil restriction

In this section, we study some commutative algebra properties of the Weil restriction of an ideal in a polynomial ring. We begin with two preliminary lemmas.

Lemma 3.1. *Let $A = k[x_1, \ldots, x_m]$ and $B = k[y_1, \ldots, y_t]$ be two polynomial rings over a field k, and let $I \subseteq A$ and $J \subseteq B$ be two homogeneous ideals with corresponding minimal graded free resolutions $\mathbb{F}_\bullet \to A/I \to 0$ and $\mathbb{G}_\bullet \to B/J \to 0$. Then the product complex $(\mathbb{F} \otimes \mathbb{G})_\bullet$ is a minimal graded free resolution of $A/I \otimes_k B/J \cong k[x_1, \ldots, x_m, y_1, \ldots, y_t]/(I + J)$.*

Proof. If we denote by $\mathbb{F}_\bullet = (F_i, d_i)$ and $\mathbb{G}_\bullet = (G_j, \delta_j)$ the two complexes, then the tensor product complex is given by $(\mathbb{F} \otimes \mathbb{G})_h = \bigoplus_{i+j=h} (F_i \otimes_k G_j)$ with differential maps $\partial_h(f \otimes g) = d_i(f) \otimes g + (-1)^i f \otimes \delta_j(g)$ for $f \in F_i$, $g \in G_j$. From this, we see immediately that if $\mathbb{F}_\bullet$ and $\mathbb{G}_\bullet$ are minimal, i.e. $d_i(F_i) \subseteq (x_1, \ldots, x_m)F_{i-1}$ and $\delta_j(G_j) \subseteq (y_1, \ldots, y_t)G_{j-1}$, then $(\mathbb{F} \otimes \mathbb{G})_\bullet$ is also minimal. Then from the Künneth formula [Rot09, Corollary 10.84] we obtain $H_0(\mathbb{F} \otimes \mathbb{G}) = H_0(\mathbb{F}) \otimes_k H_0(\mathbb{G}) = A/I \otimes_k B/J$ and $H_n(\mathbb{F} \otimes \mathbb{G}) = \bigoplus_{i+j=n} (H_i(\mathbb{F}) \otimes_k H_j(\mathbb{G})) = 0$ for any $n > 0$. So $(\mathbb{F} \otimes \mathbb{G})_\bullet$ is exact and resolves $A/I \otimes_k B/J$. □

Lemma 3.2. *Let A and B be two finitely generated $\mathbb{N}$-graded algebras over a field k. Then*

$$\mathrm{HS}_{A\otimes_k B}(z) = \mathrm{HS}_A(z) \cdot \mathrm{HS}_B(z)$$

Proof. We observe that $(A \otimes_k B)_h = \bigoplus_{i+j=h} A_i \otimes_k B_j$. Therefore we have

$$\begin{aligned}
\mathrm{HS}_A(z) \cdot \mathrm{HS}_B(z) &= \sum_h \sum_{i+j=h} (\dim_k A_i \cdot \dim_k B_j)\, z^h \\
&= \sum_h \left(\sum_{i+j=h} \dim_k (A_i \otimes_k B_j) \right) z^h \\
&= \sum_h \dim_k \left(\bigoplus_{i+j=h} (A_i \otimes_k B_j) \right) z^h \\
&= \sum_h \dim_k (A \otimes_k B)_h \, z^h \\
&= \mathrm{HS}_{A\otimes_k B}(z).
\end{aligned}$$

□

Theorem 3.3. *Let $k \hookrightarrow K$ be a finite Galois field extension of degree n. Let $I \subseteq R = K[x_1, \ldots, x_m]$ be a homogeneous ideal, and let $\mathrm{Weil}(I) \subseteq S = k[x_{i,j}]_{i=1,\ldots,m, j=1,\ldots,n}$ be its Weil restriction. Then*

(i) $\dim(S/\mathrm{Weil}(I)) = n \cdot \dim(R/I)$.
(ii) $\mathrm{proj.dim}\,(S/\mathrm{Weil}(I)) = n \cdot \mathrm{proj.dim}(R/I)$.
(iii) If R/I is Cohen-Macaulay, then $S/\mathrm{Weil}(I)$ is Cohen-Macaulay.
(iv) If R/I is a complete intersection, then $S/\mathrm{Weil}(I)$ is a complete intersection.
(v) $\mathrm{reg}\,(\mathrm{Weil}(I)) = n \cdot \mathrm{reg}(I) - n + 1$.
(vi) $\mathrm{HS}_{S/\mathrm{Weil}(I)}(z) = \big(\mathrm{HS}_{R/I}(z)\big)^n$.
(vii) $e\,(S/\mathrm{Weil}(I)) = e\,(R/I)^n$, *where $e(-)$ denotes the Hilbert-Samuel multiplicity.*

Proof. Since the above properties are invariant under field extension, we will replace $S/\mathrm{Weil}(I)$ by $S/\mathrm{Weil}(I) \otimes_k K \cong S'/\mathrm{Weil}(I)$ where $S' = S \otimes_k K = K[x_{i,j}]_{i=1,\ldots,m,j=1,\ldots,n}$. By Theorem 2.8, we have a degree-preserving K-algebra isomorphism

$$S'/\mathrm{Weil}(I) \cong \bigotimes_{\sigma\in G} (R/I)^\sigma, \tag{2}$$

where $G = \mathrm{Gal}(K/k)$. This yields *(i)*.

Now, let $\mathbb{F}_\bullet \to R/I \to 0$ be a minimal graded free resolution of R/I with $\mathbb{F} = (F_i, d_i)$. For any $\sigma \in G$, a minimal graded free resolution of $(R/I)^\sigma$ is given by $\mathbb{F}_\bullet^\sigma \to (R/I)^\sigma \to 0$, where the free modules of $\mathbb{F}_\bullet^\sigma$ are the same as those of $\mathbb{F}_\bullet$ and the differential maps are twisted by the action of σ on the coefficients. Therefore, by Lemma 3.1 we have the following minimal graded free resolution:

$$\bigotimes_{\sigma\in G} \mathbb{F}_\bullet^\sigma \to \bigotimes_{\sigma\in G} (R/I)^\sigma \to 0.$$

We can use this fact to prove the desired properties. First, we observe that if $\mathbb{F}_\bullet$ has length $p = \text{proj.dim}(R/I)$, then the length of $\bigotimes \mathbb{F}_\bullet^\sigma$ will be np with the last non-zero module being $F_p \otimes \cdots \otimes F_p$. This proves *(ii)*.

To prove *(iii)* we recall that, by the Auslander-Buchsbaum formula, a quotient T/J of a polynomial ring T by an ideal J is Cohen-Macaulay if and only if $\text{proj.dim}(T/J) = \text{ht}(J)$. From *(ii)* and assuming R/I Cohen-Macaulay, we get

$$\text{proj.dim}\left(S'/\operatorname{Weil}(I)\right) = n \cdot \text{proj.dim}(R/I) = n \cdot \text{ht}(I).$$

On the other hand, we have

$$\begin{aligned}\text{ht}\left(\operatorname{Weil}(I)\right) &= \dim(S') - \dim\left(S'/\operatorname{Weil}(I)\right)\\ &= n \cdot \dim(R) - n \cdot \dim(R/I)\\ &= n \cdot \text{ht}(I),\end{aligned}$$

where the equality $\dim(S'/\operatorname{Weil}(I)) = n \cdot \dim(R/I)$ follows from *(i)*.

To prove *(v)*, recall that for any homogeneous ideal $I \subseteq R$ one has $\text{reg}(I) = \text{reg}(R/I) + 1$ and $\text{reg}(R/I) = \max\{a_i - i\}$, where $a_i = \max\{j : R(-j) \text{ is a direct summand of } F_i\}$. We assume that $\text{reg}(R/I)$ is achieved in the resolution $\mathbb{F}_\bullet$ in homological position i, that is, $\text{reg}(R/I) = j - i$ with $F_i = R(-j) \oplus F_i'$, and F_i' is a free R-module. The free module $F_i \otimes \cdots \otimes F_i$ is a direct summand of $\left(\bigotimes \mathbb{F}^\sigma\right)_{ni}$, and contains the R-module $R(-j) \otimes \cdots \otimes R(-j) \cong R(-nj)$ as direct summand. This yields

$$\text{reg}(S'/\operatorname{Weil}(I)) = \text{reg}\left(\bigotimes_{\sigma \in G} (R/I)^\sigma\right) \geq nj - ni = n(j-i) = n \cdot \text{reg}(R/I).$$

To prove the reverse inequality, fix $h \leq \text{proj.dim}(S'/\operatorname{Weil}(I))$, and consider

$$\left(\bigotimes \mathbb{F}^\sigma\right)_h = \bigoplus_{i_1 + \cdots + i_n = h} F_{i_1} \otimes \cdots \otimes F_{i_n}.$$

The maximum shift in each direct summand $F_{i_1} \otimes \cdots \otimes F_{i_n}$ above is $a_{i_1} + \cdots + a_{i_n}$. Thus, we obtain

$$a_{i_1} + \cdots + a_{i_n} - h = (a_{i_1} - i_1) + \cdots + (a_{i_n} - i_n) \leq n \cdot \text{reg}(R/I).$$

Since the regularity of $S'/\operatorname{Weil}(I)$ is the maximum of all the above expressions of the form $a_{i_1} + \cdots + a_{i_n} - h$ for $i_1 + \cdots + i_n = h$ and $h \leq \text{proj.dim}(S'/\operatorname{Weil}(I))$, we obtain

$$\text{reg}(S'/\operatorname{Weil}(I)) \leq n \cdot \text{reg}(R/I),$$

which gives the desired equality.

Property *(vi)* follows directly from (2) and Lemma 3.2.

Finally, property *(vii)* follows from *(vi)* and the fact that the Hilbert-Samuel multiplicity of R/I is the evaluation in 1 of the numerator of the simplified Hilbert series of R/I, see e.g. [Val98, Section 1]. □

From Theorem 3.3 we immediately obtain bounds on the solving degree and degree of regularity of the Weil restriction of homogeneous systems of polynomials. In the next section we will extend these results to the non-homogeneous case.

Corollary 3.4. *Let $k \hookrightarrow K$ be a finite Galois field extension of degree n. Let $\mathcal{F} \subseteq R = K[x_1, \dots, x_m]$ be a system of homogeneous polynomials with Weil restriction* $\mathrm{Weil}(\mathcal{F}) \subseteq S = k[x_{i,j}]_{i=1,\dots,m,j=1,\dots,n}$.

(1) If $\mathrm{Weil}(\mathcal{F})$ *is in generic coordinates over $\overline{k}$, then*

$$\mathrm{sd}(\mathrm{Weil}(\mathcal{F})) \leq n \cdot \mathrm{reg}(\mathcal{F}) - n + 1.$$

(2) Assume that $(\mathcal{F})_d = R_d$ for $d \gg 0$. Then

$$d_{\mathrm{reg}}(\mathrm{Weil}(\mathcal{F})) = n \cdot d_{\mathrm{reg}}(\mathcal{F}) - n + 1.$$

Proof. (1) From [CG21, Theorem 9] we have that

$$\mathrm{sd}(\mathrm{Weil}(\mathcal{F})) \leq \mathrm{reg}(\mathrm{Weil}(\mathcal{F})).$$

Now, by Theorem 3.3 we get

$$\mathrm{reg}(\mathrm{Weil}(\mathcal{F})) = n \cdot \mathrm{reg}(\mathcal{F}) - n + 1$$

as required.

(2) Since the system $\mathcal{F}$ is homogeneous and $(\mathcal{F})_d = R_d$ for $d \gg 0$, then $d_{\mathrm{reg}}(\mathcal{F}) = \mathrm{reg}(\mathcal{F})$. Then the claim follows from Theorem 3.3. □

4. Solving degree and degree of regularity of Weil restriction systems

We now consider the situation when the system $\mathcal{F}$ is not necessarily homogeneous. In this case, the Weil restriction system $\mathrm{Weil}(\mathcal{F})$ is not necessarily homogeneous and we cannot bound its solving degree with the Castelnuovo-Mumford regularity of the corresponding ideal, but we should rather look at the ideal generated by the homogenized system $\mathrm{Weil}(\mathcal{F})^h$. However, we could also swap the two operations. Namely, first homogenize the system $\mathcal{F}$ and then apply Weil restriction to get a new system $\mathrm{Weil}(\mathcal{F}^h)$. Clearly, the systems $\mathrm{Weil}(\mathcal{F}^h)$ and $\mathrm{Weil}(\mathcal{F})^h$ are not the same. In fact, they even live in different polynomial rings. However, there is a strict relation between these two systems that we are going to explore in this section. Before that, let us fix the notation.

Notation 4.1. Let $k \hookrightarrow K$ be a finite Galois field extension of degree n with a fixed basis $\{\alpha_1 = 1, \alpha_2, \dots, \alpha_n\}$ of K over k. Let $R = K[x_1, \dots, x_m]$ be a polynomial ring, and let $S = k[x_{i,j}]_{i=1,\dots,m,j=1,\dots,n}$ be the polynomial ring in nm variables over k. We consider a system of polynomials $\mathcal{F} = \{f_1, \dots, f_r\} \subseteq R$ not all homogeneous and the corresponding homogenized system $\mathcal{F}^h \subseteq R[t]$ obtained by homogenization with respect to a new variable t. We have two polynomial systems:

- $\mathrm{Weil}(\mathcal{F}^h) \subseteq S[t_1, \dots, t_n]$, obtained by Weil restriction of $\mathcal{F}^h$, where $t_1, \dots, t_n$ are the variables obtained by Weil restriction from t, i.e., $\sum \alpha_i t_i = t$.
- $\mathrm{Weil}(\mathcal{F})^h \subseteq S[t]$, obtained by homogenization of $\mathrm{Weil}(\mathcal{F})$ with respect to a new variable t.

Lemma 4.2. *Let $\mathcal{F} \subseteq R$ be a system of polynomials as in Notation 4.1. Then the equations of* $\mathrm{Weil}(\mathcal{F})^h$ *are obtained from those of* $\mathrm{Weil}(\mathcal{F}^h)$ *by setting $t_1 = t$ and $t_2 = \cdots = t_n = 0$.*

Proof. Let $f \in \mathcal{F}$, let $d = \deg f$ and write $f = \sum_{a=0}^{d} f_a$, where f_a is homogeneous of degree a. Then $f^h = \sum_{a=0}^{d} f_a t^{d-a}$. The polynomials $g_1, \ldots, g_n$ of the Weil restriction $\mathrm{Weil}(f^h)$ of f^h are obtained from the relation

$$\begin{aligned} g_1\alpha_1 + \cdots + g_n\alpha_n &= f^h\left(\sum_{j=1}^{n} x_{i,j}\alpha_j, \sum_{j=1}^{n} t_j\alpha_j : \ i = 1, \ldots, m\right) \\ &= \sum_{a=0}^{d} f_a\left(\sum_{j=1}^{n} x_{i,j}\alpha_j : \ i = 1, \ldots, m\right)\left(\sum_{j=1}^{n} t_j\alpha_j\right)^{d-a}. \end{aligned} \tag{3}$$

On the other hand, the polynomials $h_1, \ldots, h_n$ of the system $\mathrm{Weil}(f)^h$ are obtained from the identity

$$h_1\alpha_1 + \cdots + h_n\alpha_n = \sum_{a=0}^{d} f_a\left(\sum_{j=1}^{n} x_{i,j}\alpha_j : \ i = 1, \ldots, m\right) t^{d-a},$$

since the homogenization with respect to t and substituting $\sum_{j=1}^{n} x_{i,j}\alpha_j$ for x_i are commuting operations. Setting $t_1 = t$ and $t_2 = \cdots = t_n = 0$ into (3) yields

$$\begin{aligned} g_1(x_{i,j}, t, 0, \ldots, 0)\alpha_1 + \cdots + g_n(x_{i,j}, t, 0, \ldots, 0)\alpha_n &= \sum_{a=0}^{d} f_a\left(\sum_{j=1}^{n} x_{i,j}\alpha_j : \ i = 1, \ldots, m\right) t^{d-a} \\ &= h_1\alpha_1 + \cdots + h_n\alpha_n. \end{aligned}$$

Since $g_1, \ldots, g_n, h_1, \ldots, h_n$ have coefficients in k and $\alpha_1, \ldots, \alpha_n$ are k-linearly independent, one has $g_\ell(x_{i,j}, t, 0, \ldots, 0) = h_\ell$ for $\ell = 1, \ldots, n$. □

Example 4.3. Let $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ with $\alpha^3 = \alpha + 1$ and we fix the basis $\{1, \alpha, \alpha^2\}$ of $\mathbb{F}_8$ over $\mathbb{F}_2$. We consider the system $\mathcal{F} = \{f\}$ where $f = y^2 + xy + \alpha x + \alpha^2 \in \mathbb{F}_8[x, y]$. Then we have $f^h = y^2 + xy + \alpha xt + \alpha^2 t^2$ and its Weil restriction is the system $\mathrm{Weil}(f^h) = \{g_1, g_2, g_3\}$ where

$$\begin{aligned} g_1 &= y_1^2 + x_1y_1 + x_2y_3 + x_3y_2 + x_1t_3 + x_2t_2 + x_3t_1 + x_3t_3 + t_3^2, \\ g_2 &= y_3^2 + x_1y_2 + x_2y_1 + x_2y_3 + x_3y_2 + x_3y_3 + x_1t_1 + x_1t_3 + x_2t_2 + x_2t_3 + x_3t_1 + x_3t_2 + x_3t_3 + t_2^2, \\ g_3 &= y_2^2 + y_3^2 + x_1y_3 + x_2y_2 + x_3y_1 + x_3y_3 + x_1t_2 + x_2t_1 + x_2t_3 + x_3t_2 + x_3t_3 + t_1^2 + t_2^2 + t_3^2. \end{aligned}$$

Here we used the substitution $x = x_1 + \alpha x_2 + \alpha^2 x_3$ and similarly for y and t. On the other hand, the polynomials h_1, h_2, h_3 of the system $\mathrm{Weil}(f)^h$ are

$$\begin{aligned} h_1 &= y_1^2 + x_1y_1 + x_2y_3 + x_3y_2 + x_3t, \\ h_2 &= y_3^2 + x_1y_2 + x_2y_1 + x_2y_3 + x_3y_2 + x_3y_3 + x_1t + x_3t, \\ h_3 &= y_2^2 + y_3^2 + x_1y_3 + x_2y_2 + x_3y_1 + x_3y_3 + x_2t + t^2. \end{aligned}$$

It is easy to check that h_1, h_2, h_3 are obtained from g_1, g_2, g_3 by setting $t_1 = t$ and $t_2 = t_3 = 0$.

Lemma 4.4. *Let $\mathcal{F} \subseteq R$ be a system of polynomials as in Notation 4.1. Then t is non zerodivisor in $R[t]/(\mathcal{F}^h)$ if and only if $t_1, \ldots, t_n$ are a regular sequence in $S[t_1, \ldots, t_n]/(\mathrm{Weil}(\mathcal{F}^h))$.*

Proof. First, we recall the following fact on Hilbert series, shown in [Par10, Proposition 1]. Given a finitely generated $\mathbb{N}$-graded algebra A over a field and elements $y_1, \dots, y_r \in A_1$, then $\mathrm{HS}_{A/(y_1,\dots,y_r)}(z) = (1-z)^r \mathrm{HS}_A(z)$ if and only if $y_1, \dots, y_r$ is a regular sequence in A. Hence t is non zerodivisor modulo $(\mathcal{F}^h)$ if and only if

$$\mathrm{HS}_{R/(\mathcal{F}^h \cup \{t\})}(z) = (1-z) \cdot \mathrm{HS}_{R/(\mathcal{F}^h)}(z).$$

Moreover, $t_1, \dots, t_n$ are a regular sequence in $S[t_1, \dots, t_n]/(\mathrm{Weil}(\mathcal{F}^h))$ if and only if

$$\mathrm{HS}_{S[t_1,\dots,t_n]/((\mathrm{Weil}(\mathcal{F}^h))+(t_1,\dots,t_n))}(z) = (1-z)^n \cdot \mathrm{HS}_{S[t_1,\dots,t_n]/(\mathrm{Weil}(\mathcal{F}^h))}(z).$$

One also has

$$\mathrm{HS}_{S[t_1,\dots,t_n]/((\mathrm{Weil}(\mathcal{F}^h))+(t_1,\dots,t_n))}(z) = \mathrm{HS}_{S[t]/(\mathrm{Weil}(\mathcal{F}^h \cup \{t\}))}(z) = \left(\mathrm{HS}_{R[t]/(\mathcal{F}^h \cup \{t\})}(z)\right)^n$$

where we used Theorem 3.3 for the second equality, and the fact that $\mathrm{Weil}(\mathcal{F}^h \cup \{t\}) = \mathrm{Weil}(\mathcal{F}^h) \cup \{t_1, \dots, t_n\}$ for the first equality. Moreover

$$\mathrm{HS}_{S[t_1,\dots,t_n]/(\mathrm{Weil}(\mathcal{F}^h))}(z) = \left(\mathrm{HS}_{R[t]/(\mathcal{F}^h)}(z)\right)^n.$$

again by Theorem 3.3. It follows that t is non zerodivisor modulo $(\mathcal{F}^h)$ if and only if $t_1, \dots, t_n$ are a regular sequence in $S[t_1, \dots, t_n]/(\mathrm{Weil}(\mathcal{F}^h))$. □

Theorem 4.5. *Let $\mathcal{F} \subseteq R$ be a system of polynomials as in Notation 4.1 and assume that t is non zerodivisor in $R[t]/(\mathcal{F}^h)$. Then*

$$\mathrm{reg}(\mathrm{Weil}(\mathcal{F})^h) = n \cdot \mathrm{reg}(\mathcal{F}^h) - n + 1.$$

Proof. First, we observe that, by Lemma 4.4, $t_1, \dots, t_n$ are a regular sequence in $S/(\mathrm{Weil}(\mathcal{F}^h))$, so in particular $t_2, \dots, t_n$ are. We recall also that by [Eis05, Corollary 4.13] if M is a finitely generated module and x is a linear form that is a non zerodivisor on M then $\mathrm{reg}\, M = \mathrm{reg}\, M/xM$. Now, we can compute

$$\begin{aligned}
\mathrm{reg}\left(\mathrm{Weil}(\mathcal{F})^h\right) &= \mathrm{reg}\left(S[t]/(\mathrm{Weil}(\mathcal{F})^h)\right) + 1 \\
&= \mathrm{reg}\left(S[t_1, \dots, t_n]/((\mathrm{Weil}(\mathcal{F}^h)) + (t_2, \dots, t_n))\right) + 1 \\
&= \mathrm{reg}\left(S[t_1, \dots, t_n]/\,\mathrm{Weil}(\mathcal{F}^h)\right) + 1 \\
&= n \cdot \mathrm{reg}\left(R[t]/(\mathcal{F}^h)\right) + 1 \\
&= n\,\mathrm{reg}(\mathcal{F}^h) - n + 1.
\end{aligned}$$

where the second equality follows from Lemma 4.2, the third one from the observation above since $t_2, \dots, t_n$ are a regular sequence modulo $\mathrm{Weil}(\mathcal{F}^h)$, and the fourth equality follows from Theorem 3.3. □

For a system $\mathcal{H}$ we denote by $\mathrm{max.\,GB.\,deg}(\mathcal{H})$ the largest degree of an element in a reduced degree-reverse-lexicographic Gröbner basis of $\mathcal{H}$. We recall that by [CG21, Remark 7] we have

$$\mathrm{max.\,GB.\,deg}(\mathcal{H}) = \mathrm{sd}(\mathcal{H})$$

for any homogeneous system $\mathcal{H}$.

Lemma 4.6. *Let $\mathcal{F} \subseteq R$ be a system of polynomials as in Notation 4.1. Assume that $t \nmid 0$ in $R[t]/(\mathcal{F}^h)$. Then*

$$\operatorname{sd}(\operatorname{Weil}(\mathcal{F}^h)) = \operatorname{sd}(\operatorname{Weil}(\mathcal{F})^h).$$

Proof. Consider the degree reverse lexicographic order with $t_2, \dots, t_n$ the last variables. By Lemma 4.4, $t_2, \dots, t_n$ is a regular sequence modulo $\operatorname{Weil}(\mathcal{F}^h)$. Therefore, $t_2, \dots, t_n$ is a regular sequence modulo $\operatorname{in}(\operatorname{Weil}(\mathcal{F}^h))$. In other words, the variables $t_2, \dots, t_n$ do not appear in the monomial minimal generators of $\operatorname{in}(\operatorname{Weil}(\mathcal{F}^h))$. It follows that, if $\mathcal{G}$ is a minimal Gröbner basis of $\operatorname{Weil}(\mathcal{F}^h)$, then $\mathcal{G} \cup \{t_2, \dots, t_n\}$ is a minimal Gröbner basis of $\operatorname{Weil}(\mathcal{F}^h) \cup \{t_2, \dots, t_n\}$. Since the system $\operatorname{Weil}(\mathcal{F})^h$ does not involve $t_2, \dots, t_n$ and by [CG21, Theorem 7] and Lemma 4.2 we have

$$\begin{aligned}\operatorname{sd}(\operatorname{Weil}(\mathcal{F})^h) &= \text{max. GB. deg}(\operatorname{Weil}(\mathcal{F})^h) = \text{max. GB. deg}(\operatorname{Weil}(\mathcal{F})^h \cup \{t_2, \dots, t_n\}) \\ &= \text{max. GB. deg}(\operatorname{Weil}(\mathcal{F}^h) \cup \{t_2, \dots, t_n\}) = \text{max. GB. deg}(\operatorname{Weil}(\mathcal{F}^h)) \\ &= \operatorname{sd}(\operatorname{Weil}(\mathcal{F}^h)).\end{aligned}$$

□

Theorem 4.7. *Let $\mathcal{F} \subseteq R$ be a system of polynomials as in Notation 4.1. Assume that $t \nmid 0$ in $R[t]/(\mathcal{F}^h)$ and that $\mathcal{F}^h$ has finitely many projective solutions. Then*

$$\operatorname{sd}(\operatorname{Weil}(\mathcal{F})) \leq n \cdot \operatorname{reg}(\mathcal{F}^h) - n + 1.$$

Proof. Since $\mathcal{F}^h$ has finitely many projective solutions and $t \nmid 0$ in $R[t]/(\mathcal{F}^h)$, then $R[t]/(\mathcal{F}^h)$ is Cohen-Macaulay of Krull dimension one. Therefore, $S[t_1, \dots, t_n]/(\operatorname{Weil}(\mathcal{F}^h))$ is Cohen-Macaulay of Krull dimension n by Theorem 3.3. Since $t \nmid 0$ modulo $\mathcal{F}^h$, then $t_n, \dots, t_1$ is a regular sequence modulo $\operatorname{Weil}(\mathcal{F}^h)$ by Lemma 4.4. Therefore $t_n, \dots, t_1 \in U_n(\operatorname{Weil}(\mathcal{F}^h))$, where we follow the notation of Remark 2.5 (see also [BS87, Definition 1.5]). Hence

$$\operatorname{reg}(\operatorname{Weil}(\mathcal{F}^h)) = \operatorname{reg}(\operatorname{in}(\operatorname{Weil}(\mathcal{F}^h))) \geq \text{max. GB. deg}(\operatorname{Weil}(\mathcal{F}^h)) = \operatorname{sd}(\operatorname{Weil}(\mathcal{F}^h)),$$

where the first equality follows from [BS87, Theorem 2.4] and the second equality from [CG21, Remark 7]. Moreover

$$\operatorname{sd}(\operatorname{Weil}(\mathcal{F})) \leq \operatorname{sd}\left(\operatorname{Weil}(\mathcal{F})^h\right) = \operatorname{sd}\left(\operatorname{Weil}(\mathcal{F}^h)\right),$$

where the inequality follows from [CG21, Theorem 7] and the equality from Lemma 4.6. Summarizing

$$\operatorname{sd}(\operatorname{Weil}(\mathcal{F})) \leq \operatorname{sd}\left(\operatorname{Weil}(\mathcal{F}^h)\right) \leq \operatorname{reg}\left(\operatorname{Weil}(\mathcal{F}^h)\right) = n \cdot \operatorname{reg}(\mathcal{F}^h) - n + 1,$$

where the last equality follows from Theorem 4.5. □

In particular, we obtain the following result for a system defined over a finite field and which contains the field equations.

Definition 4.8. Let $\mathbb{F}_q$ be a finite field of cardinality q. The equations $x_1^q - x_1, \dots, x_m^q - x_m \in \mathbb{F}_q[x_1, \dots, x_m]$ are called the *field equations* of $\mathbb{F}_q$.

Corollary 4.9. *Let $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ be an extension of finite fields. Let $\mathcal{F} \subseteq \mathbb{F}_{q^n}[x_1, \dots, x_m]$ and assume that $\mathcal{F}$ contains the field equations of $\mathbb{F}_{q^n}$. Assume also that $t \nmid 0$ in $R[t]/(\mathcal{F}^h)$. Then*

$$\mathrm{sd}\left(\mathrm{Weil}(\mathcal{F})\right) \leq n \cdot \mathrm{reg}(\mathcal{F}^h) - n + 1.$$

Theorem 4.7 allows us to extends the Macaulay bound to the Weil restriction of a complete intersection.

Corollary 4.10. *Let $\mathcal{F} \subseteq R$ be a system of polynomials as in Notation 4.1. Suppose that $(\mathcal{F}^h) \subseteq R[t]$ is a complete intersection of degrees $d_1, \dots, d_r$ in generic coordinates over $\overline{K}$, then $\mathrm{Weil}(\mathcal{F})^h$ is a complete intersection in generic coordinates over $\overline{k}$. In this case*

$$\mathrm{sd}\left(\mathrm{Weil}(\mathcal{F})\right) \leq n \cdot \mathrm{reg}(\mathcal{F}^h) - n + 1 = n(d_1 + \ldots + d_r) - nr + 1.$$

Proof. If $(\mathcal{F}^h) \subseteq R[t]$ is a complete intersection in generic coordinates over $\overline{K}$, then $t, x_m, \dots, x_{r+1}$ are a regular sequence modulo $(\mathcal{F}^h)$. By Lemma 4.4, $t_n, \dots, t_1, x_{m,n}, \dots, x_{r+1,1}$ are a regular sequence modulo $\mathrm{Weil}(\mathcal{F}^h)$. Moreover, $\mathrm{Weil}(\mathcal{F}^h)$ is a complete intersection of codimension nr by Theorem 3.3 and it is in generic coordinates over $\overline{k}$. By Lemma 4.4 the same holds for $\mathrm{Weil}(\mathcal{F})^h$. □

Suppose now that $\mathcal{F}$ contains the fields equations of $\mathbb{F}_{q^n}$. It is easy to check that $\mathrm{Weil}(\mathcal{F})$ also contains the field equations of $\mathbb{F}_{q^n}$. In practice, in order to solve the system $\mathrm{Weil}(\mathcal{F})$ over $\mathbb{F}_q$, it makes sense to add the field equations of $\mathbb{F}_q$ to it. The next proposition allows us to bound the solving degree of the system that we obtain in this way. The explicit bound is given in Corollary 4.12.

Proposition 4.11. *Let $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ be an extension of finite fields. Let $\mathcal{F} \subseteq \mathbb{F}_q[x_1, \dots, x_m]$ be a system of polynomials which contains the field equations of $\mathbb{F}_{q^n}$. Then*

$$\mathrm{sd}\left(\mathcal{F} \cup \{x_i^q - x_i \mid i = 1, \dots, m\}\right) \leq \mathrm{sd}(\mathcal{F}^h).$$

Proof. The homogenized system $\mathcal{F}^h$ contains the homogenizations of the field equations of $\mathbb{F}_{q^n}$, namely $x_i^{q^n} - x_i t^{q^n - 1}$ for all $i = 1, \dots, m$. Since $x_i^q - x_i t^{q-1} \mid x_i^{q^n} - x_i t^{q^n-1}$, then

$$\max.\,\mathrm{GB.}\,\deg(\mathcal{F}^h \cup \{x_i^q - x_i t^{q-1}\}) \leq \max.\,\mathrm{GB.}\,\deg(\mathcal{F}^h).$$

Since for a homogeneous system $\mathcal{H}$ we know that $\max.\,\mathrm{GB.}\,\deg(\mathcal{H}) = \mathrm{sd}(\mathcal{H})$ by [CG21, Remark 7], we obtain that

$$\mathrm{sd}(\mathcal{F}^h \cup \{x_i^q - x_i t^{q-1} \mid i = 1, \dots, m\}) \leq \mathrm{sd}(\mathcal{F}^h),$$

which concludes the proof. □

Corollary 4.12. *Let $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^n}$ be an extension of finite fields. Let $\mathcal{F} \subseteq \mathbb{F}_{q^n}[x_1, \dots, x_m]$ be a system of polynomials which contains the field equations of $\mathbb{F}_{q^n}$. Assume that $t \nmid 0$ modulo $\mathcal{F}^h$. Then*

$$\mathrm{sd}\left(\mathrm{Weil}(\mathcal{F}) \cup \{x_{i,j}^q - x_{i,j}\}\right) \leq n \cdot \mathrm{reg}(\mathcal{F}^h) - n + 1.$$

Proof. Combining Proposition 4.11, Lemma 4.6, Corollary 3.4, and [CG21, Theorem 11] we obtain

$$\begin{aligned}\operatorname{sd}\left(\operatorname{Weil}(\mathcal{F}) \cup \{x_{i,j}^q - x_{i,j}\}\right) &\leq \operatorname{sd}\left(\operatorname{Weil}(\mathcal{F})^h\right) \\ &= \operatorname{sd}\left(\operatorname{Weil}(\mathcal{F}^h)\right) \\ &\leq n \cdot \operatorname{reg}(\mathcal{F}^h) - n + 1.\end{aligned}$$

□

Similarly to the solving degree, one can relate the degree of regularity of a system to that of its Weil restriction.

Proposition 4.13. *Let $\mathcal{F} \subseteq R$ be a system of polynomials. Then*

$$\operatorname{Weil}(\mathcal{F}^{\mathrm{top}}) = \operatorname{Weil}(\mathcal{F})^{\mathrm{top}}.$$

Moreover, if $(\mathcal{F}^{\mathrm{top}})_d = R_d$ for $d \gg 0$, then

$$d_{\mathrm{reg}}\left(\operatorname{Weil}(\mathcal{F})\right) = n \cdot d_{\mathrm{reg}}(\mathcal{F}) - n + 1.$$

Proof. The equality $\operatorname{Weil}(\mathcal{F}^{\mathrm{top}}) = \operatorname{Weil}(\mathcal{F})^{\mathrm{top}}$ follows from observing that substituting the homogeneous linear forms (1) commutes with taking the top degree part of the polynomial. Since $(\mathcal{F}^{\mathrm{top}})_d = R_d$ for $d \gg 0$, then $\operatorname{Weil}(\mathcal{F}^{\mathrm{top}})_d = \operatorname{Weil}(\mathcal{F})^{\mathrm{top}} = S_d$ for $d \gg 0$ by Theorem 3.3. Now the relation between the degree of regularity of $\mathcal{F}$ and that of its Weil restriction follows from Corollary 3.4. □

References

[Bar04] Magali Bardet, *Étude des systémes algébriques surdéterminés. Applications aux codes correcteurs et á la cryptographie*, Ph.D. thesis, Université Paris 6 (2004).

[BDDGMT20] Mina Bigdeli, Emanuela De Negri, Manuela M. Dizdarevic, Elisa Gorla, Romy Minko, Sulamithe Tsakou, *Semi-regular sequences and other random systems of equations*, Women in Numbers Europe III – Research Directions in Number Theory, A. Cojocaru, S. Ionica and E. Lorenzo Garcia Eds., Association for Women in Mathematics Series 24, pp. 75–114, Springer (2022).

[BFS04] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, *On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations*, ICPPSS International Conference on Polynomial System Solving (2004).

[BH98] Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay rings. Revised edition*, Cambridge Studies in Advanced Mathematics 39, Cambridge University Press (1998).

[BS87] David Bayer, Michael Stillman, *A criterion for detecting m-regularity*, Invent. Math. 87 (1987), no. 1, pp. 1–11.

[CG21] Alessio Caminata, Elisa Gorla, *Solving multivariate polynomial systems and an invariant from commutative algebra*, Arithmetic of Finite Fields – WAIFI 2020, Bajard J.C., Topuzoğlu A. Eds., Lecture Notes in Computer Science 12542, pp. 3–36, Springer (2021).

[CG22] Alessio Caminata, Elisa Gorla, *The complexity of MinRank*, Women in Numbers Europe III – Research Directions in Number Theory, A. Cojocaru, S. Ionica and E. Lorenzo Garcia Eds., Association for Women in Mathematics Series 24, pp. 163–169, Springer (2022).

[CG23] Alessio Caminata, Elisa Gorla, *Solving degree, last fall degree, and related invariants*, J. Symb. Comput. 114 (2023), pp. 322–335.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, Adi Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, Proceedings of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT), Lecture Notes in Computer Science 1807, pp. 392–407, Springer (2000).

[Coh03] Paul Moritz Cohn, *Basic algebra. Groups, rings and fields*, Springer-Verlag London, London (2003).

[DBMMW08] Jintai Ding, Johannes Buchmann, Mohamed S.E. Mohamed, Wael S.A.E. Moahmed, Ralf-Philipp Weinmann, *MutantXL*, Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08), Beijing, China, LMIB, pp. 16–22 (2008).

[DS13] Jintai Ding, Dieter Schmidt, *Solving degree and degree of regularity for polynomial systems over finite fields*, Number theory and cryptography, Lecture Notes in Computer Science 8260, pp. 34–49, Springer (2013).

[Eis05] David Eisenbud, *The Geometry of Syzygies. A Second Course in Commutative Algebra and Algebraic Geometry*, Springer (2005).

[Fau99] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases (F4)*, J. Pure Appl. Algebra 139 (1999), pp. 61–88.

[Fau02] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ISSAC'02, pp. 75–83, New York, NY, USA (2002).

[Gau09] Pierrick Gaudry, Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem, J. Symb. Comput. 44 (2009), no. 12, pp. 1690–1702.

[GMR12] Elisa Gorla, Felice Manganiello, Joachim Rosenthal, *An algebraic approach for decoding spread codes*, Advances in Mathematics of Communications 6, no. 4 (2012), 443–466.

[MGR08] Felice Manganiello, Elisa Gorla, Joachim Rosenthal, *Spread codes and spread decoding in network codes*, Proceedings of the IEEE International Symposium on Information Theory 2008 – ISIT 2008, pp. 881–885 (2008).

[Nau99] Niko Naumann, *Weil-Restriktion abelscher Varietäten*, Diplomarbeit at Universität GHS Essen (1999).

[CGP15] Brian Conrad, Ofer Gabber, Gopal Prasad, *Pseudo-reductive groups*, Second edition. New Mathematical Monographs, 26. Cambridge University Press (2015).

[Par10] Keith Pardue, *Generic sequences of polynomials*, J. Algebra 324 (2010), pp. 579–590.

[Pat96] Jacques Patarin, *Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms*, International Conference on the Theory and Applications of Cryptographic Techniques, pp. 33–48, Springer (1996).

[Rot09] Joseph J. Rotman, *An introduction to homological algebra*, Second edition, Springer (2009).

[ST21] Igor Semaev, Andrea Tenti, *Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases*, J. Algebra **565** (2021), 651–674.

[T19] Andrea Tenti, *Sufficiently overdetermined random polynomial systems behave like semiregular ones*, PhD Thesis, University of Bergen (2019), available at `https://hdl.handle.net/1956/21158`.

[Val98] Giuseppe Valla, *Problems and results on Hilbert functions of graded algebras*, Six Lectures on Commutative Algebra, J. Elias, J.M. Giral, R.M. Miró-Roig, S. Zarzuela Eds., Modern Birkhäuser Classics, Birkhäuser (1998).

[Weil82] André Weil, *Adeles and Algebraic Groups*, Progress in Math. 23, Birkhäuser (1982).

Alessio Caminata, Dipartimento di Matematica, Università di Genova, via Dodecaneso 35, 16146, Genova, Italy
Email address: caminata@dima.unige.it

Michela Ceria, Dipartimento di Meccanica, Matematica e Management, Politecnico di Bari, via Orabona 4, 70125, Bari, Italy
Email address: michela.ceria@gmail.com

Elisa Gorla, Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, CH-2000 Neuchâtel, Switzerland
Email address: elisa.gorla@unine.ch