HOMOLOGICAL CHARACTERIZATION OF BOUNDED $\mathbb{F}_2$-REGULARITY

TIMOTHY J. HODGES AND SERGIO D. MOLINA

Abstract. Semi-regular sequences over $\mathbb{F}_2$ are sequences of homogeneous elements of the algebra $B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$, which have as few relations between them as possible. It is believed that most such systems are $\mathbb{F}_2$-semi-regular and this property has important consequences for understanding the complexity of Gröbner basis algorithms such as **F4** and **F5** for solving such systems. In fact even in one of the simplest and most important cases, that of quadratic sequences of length n in n variables, the question of the existence of semi-regular sequences for all n remains open. In this paper we present a new framework for the concept of $\mathbb{F}_2$-semi-regularity which we hope will allow the use of ideas and machinery from homological algebra to be applied to this interesting and important open question. First we introduce an analog of the Koszul complex and show that $\mathbb{F}_2$-semi-regularity can be characterized by the exactness of this complex. We show how the well known formula for the Hilbert series of a $\mathbb{F}_2$-semi-regular sequence can be deduced from the Koszul complex. Finally we show that the concept of first fall degree also has a natural description in terms of the Koszul complex.

1. Introduction

The concept of $\mathbb{F}_2$-*semi-regularity* was introduced in [1, 2, 3] in order to assess the complexity of certain Gröbner basis algorithms applied to solving systems of equations over the Galois field $\mathbb{F}_2$. For $\mathbb{F}_2$-semi-regular systems one can determine explicitly the highest degree of polynomials that will arise in the application of these Gröbner basis algorithms and this information enables one to predict with some accuracy the length of time taken by such an algorithm to solve a semi-regular system of equations in any given implementation. Systems of polynomial equations over $\mathbb{F}_2$ arise naturally in many diverse settings but in particular they have arisen recently in cryptography with respect to the analysis of the Hidden Field Equations cryptosystems and to the solution of the discrete logarithm problem. Classical regular

Key words and phrases. Semi-regularity, finite field, Koszul complex.

Corresponding author: Timothy Hodges, Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221-0025, USA, email:timothy.hodges@uc.edu.

The first author was partially supported by a grant from the Charles P. Taft Research Center.

The second author was partially supported by a scholarship from COLFUTURO/Foundation for the Future of Colombia and by the Maita Levine Fellowship, University of Cininnati, USA.

sequences can be characterized by the exactness of the associated Koszul complex. In this article we introduce an analog of the Koszul complex and show that $\mathbb{F}_2$-semi-regularity can be characterized by the exactness of this complex.

Consider a system of polynomial equations over $\mathbb{F}_2$

$$\begin{aligned} p_1(X_1,\ldots,X_n) &= 0 \\ p_2(X_1,\ldots,X_n) &= 0 \\ \vdots \qquad & \vdots \\ p_m(X_1,\ldots,X_n) &= 0 \end{aligned}$$

where $p_i(X_1,\ldots,X_n) \in \mathbb{F}_2[X_1,\ldots,X_n]$. Since as functions $X_i^2 = X_i$, we may effectively view the polynomials p_i as being elements of the algebra of functions from $\mathbb{F}_2^n \to \mathbb{F}_2$ which is the ring $A = \mathbb{F}_2[X_1,\ldots,X_n]/(X_1^2 + X_1,\ldots,X_n^2 + X_n)$. Denote the image of X_i in this ring by x_i. We can then reduce this system to one of the form $p_i(x_1,\ldots,x_n) = 0$ where the p_i are written in terms of the standard basis of monomials $x_{i_1}\cdots x_{i_t}$. A Gröbner basis algorithm with respect to a degree-ordering requires the finding of non-trivial combinations of the p_i which are of smaller degree. Thus, heuristically, the worst case scenario is when such non-trivial combinations do not occur until the highest degree possible. Since we only need to consider the highest degree terms to observe such behavior it suffices to work in the associated graded ring $\mathbb{F}_2[X_1,\ldots,X_n]/(X_1^2,\ldots,X_n^2)$.

In slightly more generality, we will work in the framework of the graded ring

$$R = \mathbb{K}[X_1,\ldots,X_n]/(X_1^2,\ldots,X_n^2)$$

where $\mathbb{K}$ is a field of characteristic two. We actually study the more general concept of bounded $\mathbb{F}_2$-regularity. If M is a graded R-module, then for any $d \in \mathbb{Z}$, we define the degree-shifted module $M(d)$ to be the graded R-module M with grading $M(d)_i := M_{i+d}$. For $D \in \mathbb{Z}$ we set $M_{\le D} := \bigoplus_{j\le D} M_j$. We say a homogeneous element λ of degree $d > 0$ is *$\mathbb{F}_2$-regular up to degree D on M* if for all $i \le D$ the graded map

$$(M/\lambda M)(-d)_i \xrightarrow{\lambda} M_i$$

given by multiplication by λ is injective. Notice that this map is well-defined since $\lambda^2 = 0$. We say a sequence $\lambda_1,\ldots,\lambda_m$ of homogeneous elements is $\mathbb{F}_2$-regular up to degree D on M if for all $i = 1,\ldots,m$, λ_i is $\mathbb{F}_2$-regular up to degree D on $M/(\lambda_1,\ldots,\lambda_{i-1})M$.

In the case $M = R$ the definition can be restated saying that a sequence $\lambda_1,\ldots,\lambda_m$ of homogeneous elements of R of positive degrees is $\mathbb{F}_2$-regular up to degree D if for all $i = 1,2,\ldots,m$, if μ is homogeneous and

$$\mu\lambda_i \in (\lambda_1,\ldots,\lambda_{i-1}) \quad \text{and} \quad \deg(\mu) + \deg(\lambda_i) \le D$$

then $\mu \in (\lambda_1,\ldots,\lambda_{i-1},\lambda_i)$. This is the form in which the concept of $\mathbb{F}_2$-semi-regularity was originally given in [2].

This notion is a characteristic 2 analog of the notion of bounded regularity studied by Diem in [4]. In [4], Diem gave a characterization of bounded regularity in terms of the vanishing of the first cohomology of the associated Koszul complex. In this article we give an analogous characterization of bounded $\mathbb{F}_2$-regularity in terms of the first cohomology of an appropriate analog of the Koszul complex.

Let $\lambda \in R$ be a homogeneous element of positive degree. Since $\lambda^2 = 0$ we have a well-defined complex $\mathcal{K}(\lambda)$ given by

$$\mathcal{K}(\lambda) : 0 \longrightarrow R/(\lambda) \xrightarrow{\lambda} R \longrightarrow 0.$$

For a sequence $\lambda_1, \dots, \lambda_m$ of homogeneous elements of R of positive degree, we set

$$\mathcal{K}(\lambda_1, \dots, \lambda_m) = \mathcal{K}(\lambda_1) \otimes \cdots \otimes \mathcal{K}(\lambda_m)$$

where $\mathcal{K}(\lambda_1) \otimes \cdots \otimes \mathcal{K}(\lambda_m)$ is the tensor product of complexes as defined in [10]. We prove that the following are equivalent:

(1) $\lambda_1, \dots, \lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M
(2) $H_1(M \otimes \mathcal{K}(\lambda_1, \dots, \lambda_m))_{\leq D} = 0$
(3) $H_i(M \otimes \mathcal{K}(\lambda_1, \dots, \lambda_m))_{\leq D} = 0$ for all $i \geq 1$.

As we noted above this is an analog of a result proved by Diem for bounded regularity in the polynomial ring $S = \mathbb{F}[X_1, \dots, X_n]$ over an arbitrary field $\mathbb{F}$. In this case the corresponding complex is the usual Koszul complex $\mathcal{K}'(\lambda_1, \dots, \lambda_m) = \mathcal{K}'(\lambda_1) \otimes \cdots \otimes \mathcal{K}'(\lambda_m)$ where $\mathcal{K}'(\lambda)$ is the complex $0 \longrightarrow S \xrightarrow{\lambda} S \longrightarrow 0$. In [4], Diem proves the following equivalent characterization of bounded regularity. Let $f_1, \dots, f_m \in S$ be a sequence of homogeneous elements of positive degrees. Then the following are equivalent.

(1) $f_1, \dots, f_m$ is regular up to degree D on M
(2) $H_1(M \otimes \mathcal{K}'(f_1, \dots, f_m))_{\leq D} = 0$

In section 3 we look at some consequences of our result. We give a characterization of $\mathbb{F}_2$-semi-regularity in terms of the exactness of the Koszul complex. We show how the well known formula for the Hilbert series of a $\mathbb{F}_2$-semi-regular sequence can be deduced from the Koszul complex. Finally we show that the concept of first fall degree also has a natural description in terms of the Koszul complex.

2. Bounded Regularity and Exactness of the Koszul Complex

In the ring $R = \mathbb{K}[X_1, \dots, X_n]/(X_1^2, \dots, X_n^2)$, all homogeneous elements of positive degree satisfy $\lambda^2 = 0$ so obviously regularity in the usual sense is impossible. The natural replacement for this notion is that the kernel of the multiplication map should be as small as possible, namely (λ). However this is also an unnatural condition since clearly if $\deg \lambda + \deg \mu > n$, then $\mu\lambda = 0$. The appropriate analogs of regularity turn out to be bounded $\mathbb{F}_2$-regularity, where the kernel of the multiplication map is precisely (λ) up to a certain degree; and $\mathbb{F}_2$-semi-regularity, where λ is $\mathbb{F}_2$-regular up to the maximum degree possible. The precise definitions are as follows.

Definition 2.1. Let M be a graded R-module. Let $\lambda \in R$ be a homogeneous element of degree $d > 0$ and let D be an integer. Then λ is *$\mathbb{F}_2$-regular up to degree D on M* if for all $i \leq D$ the graded map

$$(M/\lambda M)(-d)_i \xrightarrow{\lambda} M_i$$

given by multiplication by λ is injective. Notice that this map is well-defined since $\lambda^2 = 0$. More generally, let $\lambda_1, \dots, \lambda_m$ be a sequence of homogeneous elements of positive degrees $d_1, \dots, d_m$ and $D \in \mathbb{Z}$. Then the sequence is *$\mathbb{F}_2$-regular up to degree D on M* if for all $i = 1, \dots, m$, λ_i is $\mathbb{F}_2$-regular up to degree D on $M/(\lambda_1, \dots, \lambda_{i-1})M$.

Definition 2.2. For an ideal $I \subset R$ we define

$$\operatorname{Ind}(I) = \min\{d \geq 0 \mid I \cap R_d = R_d\}$$

A sequence $\lambda_1, \dots, \lambda_m$ of homogeneous elements of positive degree is said to be *$\mathbb{F}_2$-semi-regular* if it is regular up to degree $\operatorname{Ind}((\lambda_1, \dots, \lambda_m)) - 1$ on R.

Our goal in this section is to show that $\mathbb{F}_2$-regularity up to degree D is equivalent to the exactness of a certain analog of the Koszul complex up to degree D. We begin by recalling the definition of the tensor product of two chain complexes [10, 2.7.1].

Definition 2.3. Let S be a commutative ring. Let

$$X_\bullet : \cdots \longrightarrow X_n \xrightarrow{\partial_n^X} X_{n-1} \longrightarrow \cdots$$

and

$$Y_\bullet : \cdots \longrightarrow Y_n \xrightarrow{\partial_n^Y} Y_{n-1} \longrightarrow \cdots$$

be two complexes of S-modules. Then we form the complex $X_\bullet \otimes_S Y_\bullet$ by setting

$$(X_\bullet \otimes_S Y_\bullet)_i = \bigoplus_{p+q=i} X_p \otimes_S Y_q$$

and defining the differential to be $\partial_i^{X\otimes Y} : (X_\bullet \otimes_S Y_\bullet)_i \longrightarrow (X_\bullet \otimes_S Y_\bullet)_{i-1}$ given by

$$\partial_i^{X\otimes Y}(x_p \otimes y_q) = \partial_p^X(x_p) \otimes y_q + (-1)^p x_p \otimes \partial_q^Y(y_q).$$

We can now define our analog of the Koszul complex.

Definition 2.4. Let $\lambda \in R = \mathbb{K}[X_1, \dots, X_n]/(X_1^2, \dots, X_n^2)$, be a homogeneous element of positive degree $d > 0$. We denote by $\mathcal{K}(\lambda)$ the complex

$$\mathcal{K}(\lambda) : 0 \longrightarrow R/(\lambda) \xrightarrow{\lambda} R \longrightarrow 0.$$

For a sequence $\lambda_1, \dots, \lambda_m$ of homogeneous elements of R of positive degree, we set

$$\mathcal{K}(\lambda_1, \dots, \lambda_m) = \mathcal{K}(\lambda_1) \otimes \cdots \otimes \mathcal{K}(\lambda_m).$$

For example, if $\deg \lambda_i = d_i$, then $\mathcal{K}(\lambda_1, \lambda_2)$ is the complex

$$0 \to \frac{R}{(\lambda_1)}(-d_1 - d_2) \otimes \frac{R}{(\lambda_2)}(-d_1 - d_2) \to \frac{R}{(\lambda_1)}(-d_1) \oplus \frac{R}{(\lambda_2)}(-d_2) \to R \to 0$$

where the differential is defined by: if $(\overline{x}, \overline{y}) \in R/(\lambda_1)(-d_1) \oplus R/(\lambda_2)(-d_2)$ then $\partial(\overline{x}, \overline{y}) = \lambda_1 x + \lambda_2 y$; and if $\overline{x} \otimes \overline{y} \in R/(\lambda_1)(-d_1 - d_2) \otimes R/(\lambda_2)(-d_1 - d_2)$ then $\partial(\overline{x} \otimes \overline{y}) = (\lambda_2 \overline{xy}, \lambda_1 \overline{xy})$. Also, if we define $e_{12} = 1$ in $R/(\lambda_1, \lambda_2)$, $e_1 = 1$ in $R/(\lambda_1)$, and $e_2 = 1$ in $R/(\lambda_2)$, then $\partial(e_{12}) = \lambda_2 e_1 + \lambda_1 e_2$, $\partial(e_1) = \lambda_1$, $\partial(e_2) = \lambda_2$.

By induction we can check that $\mathcal{K}(\lambda_1, \dots, \lambda_m)$ has the form

$$\begin{gathered} 0 \to \cdots \to \bigoplus_{1 \le i_1 < \cdots < i_r \le m} \tfrac{R}{(\lambda_{i_1}, \dots, \lambda_{i_r})}(-d_{i_1} - \cdots - d_{i_r}) \to \cdots \\ \cdots \to \bigoplus_{1 \le i < j \le m} \tfrac{R}{(\lambda_i, \lambda_j)}(-d_i - d_j) \to \bigoplus_{1 \le i \le m} \tfrac{R}{(\lambda_i)}(-d_i) \to R \to 0, \end{gathered}$$

where if $e_{i_1, \dots, i_r}$ is the unity of $R/(\lambda_{i_1}, \dots, \lambda_{i_r})$ then

$$\partial(e_{i_1, \dots, i_r}) = \sum_{l=1}^{r} \lambda_{i_l} e_{i_1, \dots, \widehat{i_l}, \dots, i_r}$$

Notice that $H_0(\mathcal{K}(\lambda_1, \dots, \lambda_m)) = R/(\lambda_1, \dots, \lambda_m)$. More generally, the complex $M \otimes \mathcal{K}(\lambda_1, \dots, \lambda_m)$ has the form

$$\begin{gathered} 0 \to \cdots \to \bigoplus_{1 \le i_1 < \cdots < i_r \le m} \tfrac{M}{(\lambda_{i_1}, \dots, \lambda_{i_r})M}(-d_{i_1} - \cdots - d_{i_r}) \to \cdots \\ \cdots \to \bigoplus_{1 \le i < j \le m} \tfrac{M}{(\lambda_i, \lambda_j)M}(-d_i - d_j) \to \bigoplus_{1 \le i \le m} \tfrac{M}{(\lambda_i)M}(-d_i) \to M \to 0, \end{gathered}$$

where for $[m]_{i_1, \dots, i_r} \in (M/(\lambda_{i_1}, \dots, \lambda_{i_r})M)(-d_{i_1} - \cdots - d_{i_r})$ ($[m]_{i_1, \dots, i_r}$ meaning the class of $m \in M(-d_{i_1} - \cdots - d_{i_r})$ module $(\lambda_{i_1}, \dots, \lambda_{i_r})M$) we have that

$$\partial([m]_{i_1, \dots, i_r}) = \sum_{l=1}^{r} [\lambda_{i_l} m]_{i_1, \dots, \widehat{i_l}, \dots, i_r}.$$

Proposition 2.5. *Let $\lambda \in R$ be a homogeneous element of positive degree. Let $\mathcal{C} : \cdots \longrightarrow C_n \xrightarrow{\partial_n^C} C_{n-1} \longrightarrow \cdots$ be a complex of R-modules. We have an exact sequence of complexes*

$$0 \to \mathcal{C} \to \mathcal{C} \otimes \mathcal{K}(\lambda) \to \mathcal{C}' \to 0$$

where $\mathcal{C}'$ is the complex such that $(\mathcal{C}')_n = C_{n-1}/\lambda C_{n-1}$ and the differential is given by

$$\partial_n^{\mathcal{C}'}(\overline{a}) = \overline{\partial_{n-1}^{\mathcal{C}}(a)}$$

The homology exact sequence has the form

$$\begin{gathered} \cdots \longrightarrow H_n(\mathcal{C}) \longrightarrow H_n(\mathcal{C} \otimes \mathcal{K}(\lambda)) \longrightarrow H_n(\mathcal{C}') \xrightarrow{\lambda} H_{n-1}(\mathcal{C}) \\ \longrightarrow H_{n-1}(\mathcal{C} \otimes \mathcal{K}(\lambda)) \longrightarrow H_{n-1}(\mathcal{C}') \longrightarrow \cdots \end{gathered}$$

where the connecting map is given by multiplication by λ.

Proof. Notice that $(\mathcal{C}\otimes\mathcal{K}(\lambda))_n = (C_n\otimes R)\oplus(C_{n-1}\otimes R/(\lambda))$, which under the canonical identifications is $C_n \oplus (C_{n-1}/\lambda C_{n-1})$. Thus the complex $\mathcal{C}\otimes\mathcal{K}(\lambda)$ is given by

$$\cdots \longrightarrow C_n \oplus (C_{n-1}/\lambda C_{n-1}) \longrightarrow C_{n-1} \oplus (C_{n-2}/\lambda C_{n-2}) \longrightarrow \cdots$$
$$\cdots \longrightarrow C_1 \oplus (C_0/\lambda C_0) \longrightarrow C_0 \longrightarrow 0$$

Let us see that the boundary map is given by

$$\begin{aligned}\partial_n^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(\varepsilon,\overline{\eta}) &= (\partial_n^{\mathcal{C}}(\varepsilon) + (-1)^{n-1}\lambda\eta, \overline{\partial_{n-1}^{\mathcal{C}}(\eta)}) \\ &= (\partial_n^{\mathcal{C}}(\varepsilon) + \lambda\eta, \overline{\partial_{n-1}^{\mathcal{C}}(\eta)}).\end{aligned}$$

Consider $(\varepsilon\otimes r') \in C_n\otimes R$. Then $\partial_n^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(\varepsilon\otimes r') = \partial_n^{\mathcal{C}}(\varepsilon)\otimes r' \in C_{n-1}\otimes R$, since $\mathcal{K}(\lambda)$ has no module in degree -1. Now, consider $(\eta\otimes\overline{r}) \in C_{n-1}\otimes R/(\lambda)$, then $\partial_{n-1}^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(\eta,\overline{r}) = \partial_{n-1}^{\mathcal{C}}(\eta)\otimes\overline{r} + (-1)^{n-1}\eta\otimes\lambda r$. Notice that $\partial_{n-1}^{\mathcal{C}}(\eta)\otimes\overline{r} \in C_{n-2}\otimes R/(\lambda)$ and $(-1)^{n-1}\eta\otimes\lambda r \in C_{n-1}\otimes R$. Thus, under the canonical identifications $C_i\otimes R$ with C_i and $C_j\otimes R/(\lambda)$ with $C_j/\lambda C_j$ it follows that the boundary map in $\mathcal{C}\otimes\mathcal{K}(\lambda)$ takes the required form.

The maps in sequence $0\to\mathcal{C}\to\mathcal{C}\otimes\mathcal{K}(\lambda)\to\mathcal{C}'\to 0$ are the natural maps $\varepsilon\mapsto(\varepsilon,0)$ and $(\varepsilon,\eta)\mapsto\eta$. One verifies easily given the above description of $\partial_n^{\mathcal{C}\otimes\mathcal{K}(\lambda)}$ that these maps are indeeed morphisms of complexes. The exactness is clear from the definition of the maps.

By [10, Theorem 1.3.1] we have a long homology exact sequence. Let us see that the connecting homomorphism in the long exact sequence on homology is multiplication by λ. Let $\overline{\eta} \in C_{n-1}/\lambda C_{n-1}$ such that $\overline{\eta} \in \operatorname{Ker}(\partial_n^{\mathcal{C}'}) = \operatorname{Ker}(\overline{\partial_{n-1}^{\mathcal{C}}})$. Thus, $\partial_n^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(0,\overline{\eta}) = (0+\lambda\eta, 0) \in C_{n-1}\oplus(C_{n-2}/\lambda C_{n-2})$ and a preimage of this element under the map

$$C_{n-1} \to C_{n-1}\oplus(C_{n-2}/\lambda C_{n-2})$$

is $\lambda\eta$, as required. □

Let $\mathcal{C} : \cdots \longrightarrow C_n \xrightarrow{\partial_n^C} C_{n-1} \longrightarrow \cdots$ be a complex of $\mathbb{Z}$-graded R-modules. For $d\in\mathbb{Z}$, we denote by $\mathcal{C}(d)$ the complex obtained from $\mathcal{C}$ by degree shift; i.e., $(\mathcal{C}(d))_i = C_i(d)$.

Lemma 2.6. *Let M be a graded R-module. Let $\lambda_1,\dots,\lambda_k$ be a sequence of homogeneous elements of positive degrees $d_1,\dots,d_k$, let D be a natural number. If $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k))_{\leq D} = 0$ then for all $1\leq i<k$ we have that $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_i))_{\leq D} = 0$.*

Proof. Clearly it is sufficient to prove the result for $i = k-1$. Consider the exact sequence of complexes in Proposition 2.5 where $\mathcal{C} = M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{k-1})$ and denote the differentials $\partial^{\mathcal{C}\otimes\mathcal{K}(\lambda_k)}$ and $\partial^{\mathcal{C}'}$ by σ and $\overline{\delta}$ respectively. From the long exact sequence in Proposition 2.5 we have that the sequence

$$H_2(\mathcal{C}'(-d_k)) \xrightarrow{\lambda_k} H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{k-1})) \to H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k))$$

is exact. Thus it is sufficient to prove that

$$H_2(\mathcal{C}'(-d_k))_{\leq D} = 0. \tag{1}$$

Using standard identifications, the key portion of the complex $\mathcal{C}'$ is

$$\bigoplus_{1\leq i<j\leq k-1} \frac{M}{(\lambda_i,\lambda_j,\lambda_k)M}(-d_i-d_j) \xrightarrow{\overline{\delta}_2} \bigoplus_{1\leq i\leq k-1} \frac{M}{(\lambda_i,\lambda_k)M}(-d_i) \xrightarrow{\overline{\delta}_1} M/\lambda_k M$$

Let l be an integer with $l \leq D$ and consider

$$([m_i]_{ik}) \in \left(\bigoplus_{1\leq i\leq k-1} \frac{M}{(\lambda_i,\lambda_k)M}(-d_i-d_k)\right)_l$$

such that $([m_i]_{ik}) \in \operatorname{Ker}(\overline{\delta}_1)$. Then

$$[\lambda_1 m_1]_k + \cdots + [\lambda_{k-1}m_{k-1}]_k = 0 \in (M/\lambda_k M)(-d_k)_l.$$

Thus, there exits $m \in M(-2d_k)_l$ such that

$$\lambda_1 m_1 + \cdots + \lambda_{k-1}m_{k-1} + \lambda_k m = 0 \in M(-d_k)_l. \tag{2}$$

Consider the element

$$([m_1]_1,\ldots,[m_{k-1}]_{k-1},[m]_k) \in \left(\bigoplus_{1\leq i\leq k} \frac{M}{(\lambda_i)M}(-d_i)\right)_{l-d_k}$$

By (2) we have that $\sigma_1([m_1]_1,\ldots,[m_{k-1}]_{k-1},[m]_k) = 0$. Since $H_1(M \otimes \mathcal{K}(\lambda_1,\ldots,\lambda_k))_{\leq D} = 0$, then at level $l-d_k \leq D$, we have that $\operatorname{Ker}(\sigma_1) = \operatorname{Im}(\sigma_2)$. Therefore there exists

$$([a_{ij}]_{ij}) \in \left(\bigoplus_{1\leq i<j\leq k} \frac{M}{(\lambda_i,\lambda_j)M}(-d_i-d_j)\right)_{l-d_k}$$

such that

$$\sigma_2\left([a_{ij}]_{ij}\right) = ([m_1]_1,\ldots,[m_{k-1}]_{k-1},[m]_k).$$

So for all $1 \leq i \leq k-1$ we have

$$[m_i]_i = \sum_{\substack{1\leq p\leq k\\ p\neq i}} [\lambda_p a_{ip}]_i = \sum_{\substack{1\leq p\leq k-1\\ p\neq i}} [\lambda_p a_{ip}]_i + \ [\lambda_k a_{ik}]_i.$$

Consider

$$([a_{ij}]_{ijk}) \in \left(\bigoplus_{1\leq i<j\leq k-1} \frac{M}{(\lambda_i,\lambda_j,\lambda_k)M}(-d_i-d_j-d_k)\right)_l.$$

Notice that

$$\overline{\delta}_2\left([a_{ij}]_{ijk}\right) = ([y_1]_{1k},\ldots,[y_{k-1}]_{(k-1)k}),$$

where

$$[y_i]_{ik} = \sum_{\substack{1\leq p\leq k-1\\ p\neq i}} [\lambda_p a_{ip}]_{ik} = [m_i]_{ik} \in (M/(\lambda_i,\lambda_k)M)(-d_i-d_k))_l \,.$$

Therefore, $([m_i]_{ik}) = \overline{\delta}_2([a_{ij}]_{ijk}) \in \operatorname{Im}(\overline{\delta}_2)$. Thus we have shown that $\operatorname{Ker}(\overline{\delta}_1) = \operatorname{Im}(\overline{\delta}_2)$ at level $l-d_k$. Hence $H_2(\mathcal{C}'(-d_k))_l = 0$, as required. □

The following theorem gives a homological characterization of $\mathbb{F}_2$-regularity up to degree D on a module M.

Theorem 2.7. *Let M be a graded R-module. Let $\lambda_1,\dots,\lambda_m$ be a sequence of homogeneous elements of positive degrees $d_1,\dots,d_m$, and let D be a natural number. Then, $\lambda_1,\dots,\lambda_m$ is is $\mathbb{F}_2$-regular up to degree D on M if and only if $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m))_{\leq D}=0$.*

Proof. Let us suppose that $\lambda_1,\dots,\lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M. Let us prove that $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m))_{\leq D}=0$ by induction on m. Consider first the case when $m=1$. Suppose that λ_1 is $\mathbb{F}_2$-regular up to degree D on M. Then, by definition we have that the sequence

$$0\to(M/\lambda_1M)(-d_1)_i \xrightarrow{\lambda_1} M_i\to 0$$

is exact for all $i\leq D$. Notice that the complex $M\otimes\mathcal{K}(\lambda_1)$ is given by

$$0\to(M/\lambda_1M)(-d_1) \xrightarrow{\lambda_1} M\to 0.$$

Thus, $H_1(M\otimes\mathcal{K}(\lambda_1))_{\leq D}=0$.

Now suppose that $m>1$. Since $\lambda_1,\dots,\lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M then by definition the sequence $\lambda_1,\dots,\lambda_{m-1}$ is $\mathbb{F}_2$-regular up to degree D on M. Consider the complexes $\mathcal{C}=M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{m-1})$, $\mathcal{C}\otimes\mathcal{K}(\lambda_m)=M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m)$, and $\mathcal{C}'$ as in Proposition 2.5. From that proposition we have that the following sequence is exact

$$\begin{aligned}&H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{m-1}))\to H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m))\\ &\to H_1(\mathcal{C}'(-d_m))\xrightarrow{\lambda_m} H_0(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{m-1})).\end{aligned}$$

Notice that $H_0(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{m-1})) = M/(\lambda_1,\dots,\lambda_{m-1})M$. Now, the complex $\mathcal{C}'$ is given by

$$\mathcal{C}' : 0\to\cdots\to \bigoplus_{1\leq i\leq m-1}\frac{M}{(\lambda_i,\lambda_m)M}(-d_i)\xrightarrow{\overline{\delta_1}} M/\lambda_mM\to 0\to 0$$

And by the definition of the differentials of this complex we have that $H_1(\mathcal{C}') = M/(\lambda_1,\dots,\lambda_m)M$. Therefore,

$$H_1(\mathcal{C}'(-d_m)) = (M/(\lambda_1,\dots,\lambda_m)M)(-d_m)$$

Thus, we have the exact sequence

$$\begin{aligned}&H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{m-1}))\to H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m))\\ &\to (M/(\lambda_1,\dots,\lambda_m)M)(-d_m)\xrightarrow{\lambda_m} M/(\lambda_1,\dots,\lambda_{m-1})M.\end{aligned}$$

By inductive hypothesis we have $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{m-1}))_{\leq D}=0$. Moreover, since $\lambda_1,\dots,\lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M, then

$$((M/(\lambda_1,\dots,\lambda_m)M)(-d_m))_{\leq D}\xrightarrow{\lambda_m}(M/(\lambda_1,\dots,\lambda_{m-1})M)_{\leq D}$$

has trivial kernel. We conclude that $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m))_{\leq D}=0$.

Conversely, let $\lambda_1,\dots,\lambda_m$ be a sequence of homogeneous elements of positive degrees. Suppose that $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m))_{\leq D}=0$. By Lemma 2.6 we have that $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k))_{\leq D}=0$, for all $k=1,\dots,m$. As above, we have that the sequence

$$H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k))\to(M/(\lambda_1,\dots,\lambda_k)M)(-d_k)\xrightarrow{\lambda_k}M/(\lambda_1,\dots,\lambda_{k-1})M$$

is exact for all $k=1,\dots,m$. Since $H_1(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k))_{\leq D}=0$, for all $k=1,\dots,m$, then the kernel of the map

$$((M/(\lambda_1,\dots,\lambda_k)M)(-d_k))_{\leq D}\xrightarrow{\lambda_k}(M/(\lambda_1,\dots,\lambda_{k-1})M)_{\leq D}$$

is trivial for all $k=1,\dots,m$. Therefore $\lambda_1,\dots,\lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M. □

Corollary 2.8. *Let M be a graded R-module. Let $\lambda_1,\dots,\lambda_m\in R$ be a sequence of homogeneous elements of positive degrees $d_1,\dots,d_m$, and let D be a natural number. Then, $\lambda_1,\dots,\lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M if and only if $\lambda_{\sigma(1)},\dots,\lambda_{\sigma(m)}$ is $\mathbb{F}_2$-regular up to degree D on M for any permutation σ.*

Theorem 2.9. *Let M be a graded R-module. Let $\lambda_1,\dots,\lambda_m$ be a sequence of homogeneous elements of positive degrees $d_1,\dots,d_m$, and let D be a natural number. Then, $\lambda_1,\dots,\lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M if and only if $H_i(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_m))_{\leq D}=0$ for all $i>0$.*

Proof. The "if" part of the assertion follows *a fortiori* from Theorem 2.7. Suppose that the sequence $\lambda_1,\dots,\lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M. We prove by induction on k that $H_i(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k))_{\leq D}=0$ for all $i>0$ and for all $1\leq k\leq m$. Note that the case $i=1$ was already proved in Theorem 2.7 so we only need to prove the the assertion for $i>1$.

Consider first the case $k=1$. By definition, λ_1 is $\mathbb{F}_2$-regular up to degree D. The complex $M\otimes\mathcal{K}(\lambda_1)$ is just

$$0\to(M/\lambda_1M)(-d_1)\xrightarrow{\lambda_1}M\to 0.$$

so it is trivial that $H_i(M\otimes\mathcal{K}(\lambda_1))_{\leq D}=0$ for all $i>1$.

Now suppose $k>1$. Certainly $\lambda_1,\dots,\lambda_k$ is $\mathbb{F}_2$-regular up to degree D on M. Consider the complexes $\mathcal{C}=M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{k-1})$, $\mathcal{C}\otimes\mathcal{K}(\lambda_k)=M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k)$, and $\mathcal{C}'$ as in Proposition 2.5. From that proposition we have that the following sequence is exact

$$H_i(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{k-1}))\to H_i(M\otimes\mathcal{K}(\lambda_1,\dots,\lambda_k))\to H_i(\mathcal{C}'(-d_k))$$

Notice that $H_i(\mathcal{C}')=H_{i-1}(M'\otimes\mathcal{K}(\lambda_1,\dots,\lambda_{k-1}))$ where $M'=(M/\lambda_kM)$. By Corollary 2.8 and the definition of $\mathbb{F}_2$-regularity up to degree D we have that the sequence $\lambda_1, \ldots, \lambda_{k-1}$ is $\mathbb{F}_2$-regular up to degree D on M'. Thus, by inductive hypothesis $H_i(\mathcal{C}')_{\leq D} = 0$ and so $H_i(\mathcal{C}'(-d_k))_{\leq D} = 0$ also. By induction we also have that $H_i(M \otimes \mathcal{K}(\lambda_1, \ldots, \lambda_{k-1}))_{\leq D} = 0$ for all $i > 1$. Therefore, $H_i(M \otimes \mathcal{K}(\lambda_1, \ldots, \lambda_k))_{\leq D} = 0$ for all $i > 1$. □

We can summarize these results in the following theorem.

Theorem 2.10. *Let M be a non-trivial finitely generated graded R-module. Let $\lambda_1, \ldots, \lambda_m$ be a sequence of homogeneous elements of positive degrees $d_1, \ldots, d_m$, and let D be a natural number. Then the following are equivalent.*

(1) $\lambda_1, \ldots, \lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M
(2) $H_1(M \otimes \mathcal{K}(\lambda_1, \ldots, \lambda_m))_{\leq D} = 0$
(3) $H_i(M \otimes \mathcal{K}(\lambda_1, \ldots, \lambda_m))_{\leq D} = 0$ for all $i > 0$.

Example 1. Let $R = \mathbb{F}_2[X_1, \ldots, X_4]/(X_1^2, \ldots, X_4^2)$ and let $I = (\lambda_1, \lambda_2)$ be the ideal generated by the homogeneous elements $\lambda_1 = x_1x_2$ and $\lambda_2 = x_1x_3$. Thus, $\mathcal{K}(\lambda_1, \lambda_2)$ is the complex

$$0 \to \frac{R}{(\lambda_1, \lambda_2)}(-4) \xrightarrow{\partial_2} \frac{R}{(\lambda_1)}(-2) \oplus \frac{R}{(\lambda_2)}(-2) \xrightarrow{\partial_1} R \to 0$$

where

$$\partial_2 = \begin{bmatrix} \lambda_1 \\ \lambda_2 \end{bmatrix}, \quad \partial_1 = \begin{bmatrix} \lambda_1 & \lambda_2 \end{bmatrix}$$

Notice that $R = \bigoplus_{k=0}^4 R_k$, where

$$\dim R_0 = 1, \quad \dim R_1 = 4, \quad \dim R_2 = 6, \quad \dim R_3 = 4, \quad \dim R_4 = 1.$$

Also, we have that $\mathrm{Ind}(I) = 4$. Clearly, for $i \leq 3$ we have that

$$\left(\frac{R}{(\lambda_1, \lambda_2)}(-4) \right)_i = 0$$

Therefore, for $i \leq 3$ we have the sequence

$$0 \xrightarrow{\partial_2} \left(\frac{R}{(\lambda_1)}(-2) \oplus \frac{R}{(\lambda_2)}(-2) \right)_i \xrightarrow{\partial_1} R_i \to 0$$

Since λ_1, $\lambda_2 \in R_2$ are linearly independent then $H_1(\mathcal{K}(\lambda_1, \lambda_2))_{\leq 2} = 0$, and by Theorem 2.10 the sequence λ_1, λ_2 is $\mathbb{F}_2$-regular up to degree 2 on R. However, for the case $i = 3$, we have that $\partial(\overline{x_3}, \overline{x_2}) = \lambda_1 x_3 + \lambda_2 x_2 = x_1x_2x_3 + x_1x_2x_3 = 0$. Thus $H_1(\mathcal{K}(\lambda_1, \lambda_2))_3 \neq 0$. By Definition 2.2 and Theorem 2.10 the sequence λ_1, λ_2 is not $\mathbb{F}_2$-*semi-regular* .

Now, let $J = (\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ be the ideal generated by the homogeneous elements $\lambda_1 = x_1x_2$, $\lambda_2 = x_1x_3$, $\lambda_3 = x_1x_4$ and $\lambda_4 = x_2x_3$ in R. Thus, $\mathcal{K}(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ is the complex

$$0 \to \cdots\cdots \to \bigoplus_{1 \leq i < j \leq 4} \tfrac{R}{(\lambda_i, \lambda_j)}(-4) \xrightarrow{\partial_2} \bigoplus_{1 \leq i \leq 4} \tfrac{R}{(\lambda_i)}(-2) \xrightarrow{\partial_1} R \to 0$$

where

$$\partial_2 = \begin{bmatrix} \lambda_2 & \lambda_3 & \lambda_4 & 0 & 0 & 0 \\ \lambda_1 & 0 & 0 & \lambda_3 & \lambda_4 & 0 \\ 0 & \lambda_1 & 0 & \lambda_2 & 0 & \lambda_4 \\ 0 & 0 & \lambda_1 & 0 & \lambda_2 & \lambda_3 \end{bmatrix}, \quad \partial_1 = \begin{bmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \end{bmatrix}$$

Notice that $\mathrm{Ind}(J) = 3$. Clearly, for $i \le 2$ we have that

$$\left(\bigoplus_{1 \le i < j \le 4} \frac{R}{(\lambda_i, \lambda_j)}(-4) \right)_i = 0$$

Therefore, for $i \le 2$ we have the sequence

$$0 \xrightarrow{\partial_2} \left(\bigoplus_{1 \le i \le 4} \frac{R}{(\lambda_i)}(-2) \right)_i \xrightarrow{\partial_1} R_i \to 0$$

Since λ_1, λ_2, λ_3, $\lambda_4 \in R_2$ are linearly independent then $H_1(\mathcal{K}(\lambda_1, \ldots, \lambda_4))_{\le 2} = 0$, and by Theorem 2.10 and Definition 2.2 the sequence λ_1, λ_2, λ_3, λ_4 is $\mathbb{F}_2$-*semi-regular* .

3. Consequences

3.1. **Semi-regularity.** Theorem 2.9 states that a sequence $\lambda_1, \ldots, \lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M if and only if the complex $M \otimes \mathcal{K}(\lambda_1, \ldots, \lambda_m)_j$ is a "resolution" of the j-th degree component of M for all $0 \le j \le D$. Using this result we can give an interesting alternative characterization of $\mathbb{F}_2$-semi-regularity.

Definition 3.1. Let M be a non-trivial finitely generated graded R-module. We define the index of M to be the smallest t such that $M_j = 0$ for all $j \ge t$. A sequence of homogeneous elements $\lambda_1, \ldots, \lambda_m$ of positive degrees is said to be $\mathbb{F}_2$-semi-regular on M if it is regular up to degree $\mathrm{Ind}(M/(\lambda_1, \ldots, \lambda_m)M) - 1$ on M.

Theorem 3.2. *Let M be a non-trivial finitely generated graded R-module. Let $\lambda_1, \ldots, \lambda_m$ be a sequence of homogeneous elements of positive degree. Then $\lambda_1, \ldots, \lambda_m$ is $\mathbb{F}_2$-semi-regular on M if and only if*

$$H_0(M \otimes \mathcal{K}(\lambda_1, \ldots, \lambda_m))_j \neq 0 \implies H_i(M \otimes \mathcal{K}(\lambda_1, \ldots, \lambda_m))_j = 0 \textit{ for all } i > 0$$

In other words the sequence is $\mathbb{F}_2$-semi-regular on M if our analog of the Koszul sequence in degree j is a "resolution" of $(M/(\lambda_1, \ldots, \lambda_m)M)_j = H_0(\mathcal{K}(\lambda_1, \ldots, \lambda_m)_j$ whenever the latter is non-zero.

3.2. **Hilbert Series.** Regularity of a sequence $\lambda_1, \ldots, \lambda_m$ up to degree D on a finitely generated graded module M can be characterized using the Hilbert series of $M/(\lambda_1, \ldots, \lambda_m)M$ up to degree D. Recall that the Hilbert series of a graded module M is the formal series $HS_M(z) = \sum_{i=-\infty}^{\infty} (\dim M_j) z^j$ and that for a finitely generated module this will be a Laurent polynomial. For a formal Laurent series $a(z) = \sum_s^\infty a_i z^i$, we denote its truncation at degree D by

$$[a(z)]_D = \sum_s^D a_i z^i$$

It is known [2, 8] that the sequence $\lambda_1, \dots, \lambda_m$ is $\mathbb{F}_2$-regular up to degree D on M if and only if

$$\left[HS_{M/(\lambda_1,\dots,\lambda_m)M}(z)\right]_D = \left[\frac{HS_M(z)}{\prod_{i=1}^m (1+z^{d_i})}\right]_D$$

Now it is clear that if

$$0 \to L_m \to \cdots \to L_0 \to 0$$

is a sequence of finitely generated graded modules that is exact up to degree D, then

$$[HS_{L_0}(z)]_D = \sum_{i=1}^m (-1)^i [HS_{L_i}(z)]_D$$

So one would expect the above formula to be deducible directly from the Koszul complex. We now show this follows from the following identity and an easy induction.

Lemma 3.3. *Let $d_1, \dots, d_k$ be positive integers and let $d = d_1 + \cdots + d_k$. Then*

$$\prod_{i=1}^k \frac{1}{1+z^{d_i}} = \frac{\sum_{s=0}^{k-1} \sum_{i_1<\cdots<i_s} (-1)^s \prod_{j=1}^s \left(\frac{z^{d_{i_j}}}{1+z^{d_{i_j}}}\right)}{(1-(-1)^k z^d)}$$

Proof.

$$\begin{aligned}
\prod_{i=1}^k \frac{1}{1+z^{d_i}} &= \prod_{i=1}^k \left(1 - \frac{z^{d_i}}{1+z^{d_i}}\right) \\
&= \sum_{s=0}^k \sum_{i_1<\cdots<i_s} (-1)^s \prod_{j=1}^s \left(\frac{z^{d_{i_j}}}{1+z^{d_{i_j}}}\right) \\
&= \sum_{s=0}^{k-1} \sum_{i_1<\cdots<i_s} (-1)^s \prod_{j=1}^s \left(\frac{z^{d_{i_j}}}{1+z^{d_{i_j}}}\right) + (-1)^k \prod_{j=1}^k \frac{z^{d_j}}{1+z^{d_j}}
\end{aligned}$$

So

$$(1-(-1)^k z^d) \prod_{i=1}^k \frac{1}{1+z^{d_i}} = \sum_{s=0}^{k-1} \sum_{i_1<\cdots<i_s} (-1)^s \prod_{j=1}^s \left(\frac{z^{d_{i_j}}}{1+z^{d_{i_j}}}\right)$$

and the result follows. □

Theorem 3.4. *Suppose that M is a finitely generated graded module with Hilbert series $p(z)$ and suppose that $\lambda_1, \dots, \lambda_k$ is $\mathbb{F}_2$-regular up to degree D on M. Then*

$$\left[HS_{M/(\lambda_1,\dots,\lambda_k)M}(z)\right]_D = \left[\frac{p(z)}{\prod_{i=1}^k (1+z^{d_i})}\right]_D$$

Proof. We use induction with the base case being $k = 0$ (the "empty sequence") for which the result is trivially true. Since $\lambda_1, \dots, \lambda_k$ is $\mathbb{F}_2$-regular up to degree D on M, the corresponding Koszul complex $M \otimes \mathcal{K}(\lambda_1, \dots, \lambda_k)$ is exact in degree less than or equal to D. Explicitly this complex is

$$\begin{aligned}
0 \to \frac{M}{(\lambda_1,\dots,\lambda_k)M}(-d_1 - \dots - d_k) \to \dots \\
\dots \to \bigoplus_{i_1<\dots<i_s} \frac{M}{(\lambda_{i_1},\dots,\lambda_{i_s})M}(-d_{i_1} - \dots - d_{i_s}) \to \dots \\
\dots \to \bigoplus_{1\le i\le k} \frac{M}{(\lambda_i)M}(-d_i) \to M \to \frac{M}{(\lambda_1,\dots,\lambda_k)M} \to 0
\end{aligned}$$

By Corollary 2.8 any subsequence $\lambda_{i_1}, \dots, \lambda_{i_s}$ is again $\mathbb{F}_2$-regular up to degree D on M, so by induction the result holds for all but the first and last term of the complex. In particular,

$$[HS_{M/(\lambda_{i_1},\dots,\lambda_{i_s})M(-d_{i_1}-\dots-d_{i_s})}(z)]_D = \left[\frac{p(z)}{\prod_{j=1}^s (1+z^{d_{i_j}})} z^{d_{i_1}+\dots+d_{i_s}}\right]_D$$

Set $H(z) = HS_{M/(\lambda_1,\dots,\lambda_k)M}(z)$. Then from the exact sequence we have that

$$[H(z)]_D - (-1)^k[z^d H(z)]_D = \left[\sum_{s=1}^{k-1} (-1)^s \sum_{i_1<\dots<i_s} p(z) \left(\prod_{j=1}^s \frac{z^{d_{i_j}}}{1+z^{d_{i_j}}}\right)\right]_D$$

So

$$\begin{aligned}
[H(z)]_D &= \left[p(z) \sum_{i=1}^{k-1} (-1)^s \sum_{i_1<\dots<i_s} \prod_{j=1}^s \left(\frac{z^{d_{i_j}}}{1+z^{d_{i_j}}}\right) \Big/ (1-(-1)^k z^d)\right]_D \\
&= \left[\frac{p(z)}{\prod_{i=1}^k (1+z^{d_i})}\right]_D
\end{aligned}$$

by Lemma 3.3. □

3.3. **First Fall Degree.** The concept of first fall degree was introduced by Dubois and Gama in [6] (under the name of degree of regularity) in their study of the complexity of Gröbner basis attacks on the Hidden Field Equation crytposystems. Since that time it has continued to play a significant role in cryptography [5, 7, 9]. In [6] the first fall degree of functions $f_1, \dots, f_m \in \mathbb{K}[X_1, \dots, X_n]/(X_1^2 - X_1, \dots X_n^2 - X_n)$ is the first degree at which there exist non-trivial combinations which produce functions of lower degree. Since this is essentially a question about the highest degree terms of the f_i, the concept can be recast in the associated graded ring R. In [7] the first fall degree of homogeneous elements $\lambda_1, \dots, \lambda_m \in R$ is defined to be the first degree at which non-trivial relations between the λ_i exist. We show below that $H_1(M \otimes \mathcal{K}(\lambda_1, \dots, \lambda_m))$ can be naturally interpreted as the space of non-trivial relations of $\lambda_1, \dots, \lambda_m$ on M. This allows us to include the concept of first fall degree naturally into the framework of our Koszul complexes. It also allows us to re-express Theorem 2.7 in terms of the first fall degree.

Let $\lambda_1, \dots, \lambda_m \in R$ be a sequence of homogeneous elements of positive degrees $d_1, \dots, d_m$. Let V be an m-dimensional vector space with basis $\{e_1, \dots, e_m\}$, graded by setting $\deg e_i = d_i$. Let $\mathcal{R}(\lambda_1, \dots, \lambda_m)$ be the kernel of the natural map $R \otimes_{\mathbb{K}} V \longrightarrow R$ given by $\sum_i b_i \otimes e_i \mapsto \sum_i b_i \lambda_i$. Then we have an exact sequence in degree d

$$0 \longrightarrow \mathcal{R}_d(\lambda_1, \dots, \lambda_m) \longrightarrow \sum_i R_{d-d_i} \otimes e_i \longrightarrow \sum_i R_{d-d_i} \lambda_i \longrightarrow 0$$

Inside $\mathcal{R}_d(\lambda_1, \dots, \lambda_m)$ there is a subspace of "trivial relations" of degree d $\mathcal{T}_d(\lambda_1, \dots, \lambda_m)$ spanned by elements of the form

(1) $b\lambda_i \otimes e_j - b\lambda_j \otimes e_i$ where $b \in R_{d-d_i-d_j}$;
(2) $b\lambda_i \otimes e_i$ where $b \in R_{d-2d_i}$.

We define the *first fall degree* of $\lambda_1, \dots, \lambda_m$ to be the first degree at which non-trivial relations occur; that is,

$$\mathrm{D_{ff}}(\lambda_1, \dots, \lambda_m) = \min\{d \mid \mathcal{R}_d(\lambda_1, \dots, \lambda_m)/\mathcal{T}_d(\lambda_1, \dots, \lambda_m) \neq 0\}$$

Lemma 3.5. *Let $\lambda_1, \dots, \lambda_m$ be a sequence of homogeneous elements of positive degree. Then $\mathcal{R}_d(\lambda_1, \dots, \lambda_m)/\mathcal{T}_d(\lambda_1, \dots, \lambda_m) \cong H_1(\mathcal{K}(\lambda_1, \dots, \lambda_m))_d$. Hence*

$$\mathrm{D_{ff}}(\lambda_1, \dots, \lambda_m) = \min_d\{H_1(\mathcal{K}(\lambda_1, \dots, \lambda_m))_d \neq 0\}$$

Proof. It suffices to verify that the map $\phi : R \otimes V \to \bigoplus_i R/(\lambda_i)$ given by $\phi\left(\sum b_i \otimes e_i\right) = \sum_i [b_i]_i$ induces an isomorphism from $\mathcal{R}_d(\lambda_1, \dots, \lambda_m)/\mathcal{T}_d(\lambda_1, \dots, \lambda_m)$ to $H_1(\mathcal{K}(\lambda_1, \dots, \lambda_m))_d$. This verification is routine and we omit the details. □

This result allows us to generalize the concept of first fall degree as follows.

Definition 3.6. Let M be a non-trivial finitely generated R-module and let $\lambda_1, \dots, \lambda_m$ be a sequence of homogeneous elements of positive degree. We define the first fall degree of $\lambda_1, \dots, \lambda_m$ on M to be

$$\mathrm{D^{M}_{ff}}(\lambda_1, \dots, \lambda_m) = \min_d\{H_1(M \otimes \mathcal{K}(\lambda_1, \dots, \lambda_m))_d \neq 0\}$$

Example 2. Let $R = \mathbb{F}_2[X_1, \dots, X_4]/(X_1^2, \dots, X_4^2)$ and let $I = (\lambda_1, \lambda_2)$ be the ideal generated by the homogeneous elements $\lambda_1 = x_1x_2$ and $\lambda_2 = x_1x_3$. From Example 1 we have that

$$\mathrm{D}^{\mathrm{R}}_{\mathrm{ff}}(\lambda_1, \lambda_2) = 3$$

Finally we can reinterpret Theorem 2.7 in terms of the first fall degree.

Theorem 3.7. *Let M be a graded R-module. Let $\lambda_1, \dots, \lambda_m$ be a sequence of homogeneous elements of positive degree, and let D be a natural number. Then, $\lambda_1, \dots, \lambda_m$ is is $\mathbb{F}_2$-regular up to degree D on M if and only if $D < \mathrm{D}^{\mathrm{M}}_{\mathrm{ff}}(\lambda_1, \dots, \lambda_m)$.*

4. Conclusion

Consider again a system of polynomial equations over $\mathbb{F}_2$

$$\begin{aligned} p_1(X_1, \dots, X_n) &= 0 \\ p_2(X_1, \dots, X_n) &= 0 \\ \vdots \quad & \quad \vdots \\ p_m(X_1, \dots, X_n) &= 0 \end{aligned}$$

where $p_i(X_1, \dots, X_n) \in \mathbb{F}_2[X_1, \dots, X_n]$. Recall that this system is said to be $\mathbb{F}_2$-semi-regular if the sequence of highest total degree terms $p_1^{top}, \dots, p_m^{top}$ is semi-regular. It is believed that most such systems are $\mathbb{F}_2$-semi-regular and this property has important consequences for understanding the complexity of Gröbner basis algorithms for solving such systems. Experimental evidence suggest that this is so but so far there has been little theoretical progress on this issue. At this stage it is still an open question, even when $m = n$ and the p_i are quadratic, whether there exist $\mathbb{F}_2$-semi-regular sequences for all n. In this paper we presented a new framework for the concept of $\mathbb{F}_2$-semi-regularity which we hope will allow the use of ideas and machinery from homological algebra to be applied to this interesting and important open question.

References

[1] M. Bardet, *Étude des systèmes algébriques surdéterminés. Applications aux codes correctuers et la cryptographie.* PhD thesis, Université Paris VI, Décembre 2004.

[2] M. Bardet, J-C. Faugère, B. Salvy, *Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over $\mathbb{F}_2$ with solutions in* $\mathbb{F}_2$, in: INRIA Research Report 5049, 2003.

[3] M. Bardet, J.-C. Faugère, B. Salvy and B.-Y. Yang, *Asymptotic Expansion of the Degree of Regularity for Semi-Regular Systems of Equations*, MEGA 2005, Sardinia, Italy

[4] C. Diem, *Bounded Regularity*, Journal of Algebra 423 (2015): 1143-1160.

[5] J. Ding, T. J. Hodges, *Inverting the HFE systems is quasipolynomial for all fields.* In: Advances in Cryptology - Crypto 2011, Lecture Notes in Computer Science 6841, pp 724-742, Springer, Berlin 2011.

[6] V. Dubois, N. Gama, *The degree of regularity of HFE systems.* In: Abe, M. (ed.) Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security. LNCS, vol. 6477, pp. 557-576. Springer, Berlin (2010)

[7] T. J. Hodges, C. Petit and J. Schlather, *First Fall Degree and Weil Descent*, Finite Fields and Their Applications 30 (2014), 155-177.

[8] T. J. Hodges, S. D. Molina and J. Schlather, *On the existence of homogeneous semi-regular sequences in.*, Journal of Algebra 476 (2017): 519-547.

[9] Christophe Petit and Jean-Jacques Quisquater, *On Polynomial Systems Arising from a Weil Descent*, in X. Wang and K. Sako (Eds.): ASIACRYPT 2012, LNCS 7658, pp. 451–466, 2012.

[10] C. Weibel, *An introduction to homological algebra*, Cambridge, 1994.

Email address, Timothy Hodges: `timothy.hodges@uc.edu`

University of Cincinnati, Cincinnati, OH 45221-0025, USA

Email address, Sergio Molina: `molinasd@ucmail.uc.edu`

University of Cincinnati, Cincinnati, OH 45221-0025, USA