TOWARD AN EFFICIENT ALGORITHM FOR DECIDING THE VANISHING OF LOCAL COHOMOLOGY MODULES IN PRIME CHARACTERISTIC

YI ZHANG

Abstract. Let $R = k[x_1, \ldots, x_n]$ be a ring of polynomials over a field k of characteristic $p > 0$. There is an algorithm due to Lyubeznik for deciding the vanishing of local cohomology modules $H^i_I(R)$ where $I \subset R$ is an ideal. This algorithm has not been implemented because its complexity grows very rapidly with the growth of p which makes it impractical. In this paper we produce a modification of this algorithm that consumes a modest amount of memory.

Introduction

Since A. Grothendieck introduced local cohomology in 1961 [4], people have been interested in the structure of local cohomology modules. Let R be a commutative ring, let $I \subset R$ be an ideal and let M be an R-module. As a rule, local cohomology modules $H^t_I(M)$ are not finitely generated even if the module M is. So it is very difficult to tell whether these local cohomology modules vanish or not, and to this day, no algorithm has been found to decide their vanishing.

However, in the case that $R = k[x_1, \ldots, x_n]$ is the ring of polynomials in a finite number of variables over a field k and $M = R$, two completely different algorithms are known, one in characteristic 0 [12], the other in characteristic $p > 0$ [7, Remark 2.4]. The characteristic 0 algorithm uses ideas from the theory of D-modules, while the characteristic $p > 0$ algorithm uses ideas from the theory of F-modules. The characteristic 0 algorithm has been implemented and is part of the computer package "Dmodules" for Macaulay 2 [3]. The characteristic $p > 0$ algorithm has not been implemented since its complexity grows very rapidly with the growth of p which makes it impractical.

More precisely, let $R = \mathbb{Z}[x_1, \ldots, x_n]$, let $f_1, \ldots, f_s \in R$ be polynomials in variables $x_1, \ldots, x_n$ with integer coefficients, and let $I = (f_1, \ldots, f_s) \subset R$ be the ideal they generate. For a prime integer $p > 0$, let $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$, let $\bar{R} = \bar{\mathbb{Z}}[x_1, \ldots, x_n]$, let $\bar{f}_i \in \bar{R}$ be the polynomial obtained from f_i by reducing its coefficients modulo p, and let $\bar{I}$ be the ideal of $\bar{R}$ generated by $\bar{f}_1, \ldots, \bar{f}_s$. We keep this notation for the rest of the paper.

The algorithm from [7, Remark 2.4] for deciding the vanishing of the local cohomology module $H^t_{\bar{I}}(\bar{R})$ involves computations with the ideal $\bar{I}^{[p]}$ generated by the p-th powers of $\bar{f}_1, \ldots, \bar{f}_s$. The complexity of these computations grows very rapidly with the growth of p because the degrees of the polynomials $\bar{f}_i^p$ that generate the ideal $\bar{I}^{[p]}$ grow linearly and the amount of memory required to perform Gröbner bases calculations grows exponentially in the degrees of the generators [11].

2010 *Mathematics Subject Classification.* Primary 13A35; Secondary 13B22, 13H15, 14B05.

NSF support through grant DMS-0701127 is gratefully acknowledged.

In this paper, we present a modification of the algorithm from [7, Remark 2.4]. The amount of memory our modification consumes grows only linearly with the growth of p. Unfortunately, this is not enough to produce a fully practical algorithm since the number of operations still grows very rapidly with the growth of p, an extraordinary amount of time may be required to complete the calculation. Nevertheless, at least available memory is unlikely to be exhausted before the calculation is completed.

We view our result as an important step in a search for a fully practical algorithm. For our result shows that at least in terms of required memory, there is no obstacle to finding such an algorithm.

1. Preliminaries

Recall that $R = \mathbb{Z}[x_1, \ldots, x_n]$ is a ring of polynomials over the integers, $p \in \mathbb{Z}$ is a prime number and $\bar{R} = R/pR = (\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$. Local cohomology modules $H^i_I(R)$ have a structure of F-finite modules in the sense of [7]. In this section we review the algorithm from [7, Remark 2.4] for deciding the vanishing of F-finite modules and discuss some ingredients of our modification of this algorithm.

Given an integer ℓ, the ℓ-fold Frobenius homomorphism is $F^\ell : \bar{R}_s \xrightarrow{r \mapsto r^{p^\ell}} \bar{R}_t$, where $\bar{R}_s$ and $\bar{R}_t$ are copies of $\bar{R}$ (the subscripts stand for source and target). There are two associated functors, namely, the push-forward

$$F^\ell_* : \bar{R}_t\text{-mod} \to \bar{R}_s\text{-mod}$$

which is just the restriction of scalars functor (i.e. $F^\ell_*(M)$, for an $\bar{R}_t$-module M is M viewed as an $\bar{R}_s$-module via F^ℓ) and the pull-back

$$F^{*^\ell} : \bar{R}_s\text{-mod} \to \bar{R}_t\text{-mod}$$

such that $F^{*^\ell}(N) = \bar{R}_t \otimes_{\bar{R}_s} N$ and $F^{*^\ell}(N \xrightarrow{\lambda} N') = (\bar{R}_t \otimes_{\bar{R}_s} N \xrightarrow{\bar{R}_t \otimes_{\bar{R}_s} \lambda} \bar{R}_t \otimes_{\bar{R}_s} N')$. Normally one suppresses the subscripts and thinks of F^{*^ℓ} and F^ℓ_* as functors from $\bar{R}$-modules to $\bar{R}$-modules:

$$F^{*^\ell}, F^\ell_* : \bar{R}\text{-mod} \to \bar{R}\text{-mod}.$$

For every R-module M we set $\bar{M} = M/pM$; every $\bar{R}$-module is of the form $\bar{M}$ for some R-module M. Let an $\bar{R}$-module $\mathcal{M}$ be the limit of the inductive system

$$\bar{M} \xrightarrow{\beta} F^*(\bar{M}) \xrightarrow{F^*(\beta)} F^{*^2}(\bar{M}) \xrightarrow{F^{*^2}(\beta)} \ldots \tag{1.1}$$

where $\bar{M}$ is a finitely generated $\bar{R}$-module and $\beta : \bar{M} \to F^*(\bar{M})$ is an $\bar{R}$-module homomorphism. The module $\mathcal{M}$ is the underlying $\bar{R}$-module of an F-finite module which is defined as a pair $(\mathcal{M}, \theta)$ where $\theta : \mathcal{M} \to F^*(\mathcal{M})$ is an $\bar{R}$-module isomorphism [7, Definitions 1.1 and 1.9]. The isomorphism θ is not going to play any role in this paper because we are interested only in the vanishing of this F-finite module $(\mathcal{M}, \theta)$ which by definition means the vanishing of the underlying $\bar{R}$-module $\mathcal{M}$. For this reason we omit the definition of θ. By a slight abuse of terminology we call $\mathcal{M}$ itself the F-finite module generated by $\beta : \bar{M} \to F^*(\bar{M})$ (this map is called a generating morphism of $\mathcal{M}$).

The following proposition underlies the algorithm from [7, Remark 2.4] for deciding the vanishing of F-finite modules.

Proposition 1.1. [7, Proposition 2.3] *Suppose $\mathcal{M}$ is an F-finite module and let $\beta : \bar{M} \to F^*(\bar{M})$ be a generating morphism of $\mathcal{M}$ such that $\bar{M}$ is a finitely generated $\bar{R}$-module. Let $\beta_j : \bar{M} \to F^{*^j}(\bar{M})$ be the composition*

$$\bar{M} \xrightarrow{\beta} F^*(\bar{M}) \xrightarrow{F^*(\beta)} \cdots \xrightarrow{F^{*^{j-1}}(\beta)} F^{*^j}(\bar{M}).$$

Then:

(a) *The ascending chain* $\ker\beta_1 \subset \ker\beta_2 \subset \cdots$ *of submodules of $\bar{M}$ eventually stabilizes. Let $C \subset \bar{M}$ be the common value of* $\ker\beta_i$ *for sufficiently big i.*
(b) *If r is the first integer such that* $\ker\beta_r = \ker\beta_{r+1}$, *then* $\ker\beta_r = C$.
(c) *$\mathcal{M} = 0$ if and only if $\bar{M} = C$, i.e., β_r is the zero map.*

This leads to an algorithm for deciding whether the F-finite module $\mathcal{M}$ generated by $\beta : \bar{M} \to F^*(\bar{M})$ vanishes. We quote [7, Remark 2.4]:

[F]or each integer $j = 1, 2, 3, \ldots$ one should compute the kernel of β_j, and compare it with the kernel of β_{j-1}, until one finds r such that $\ker\beta_r = \ker\beta_{r-1}$. *One then should check whether* $\ker\beta_r$ *and $\bar{M}$ coincide. The F-finite module in question is zero if and only if they do coincide. If R is a polynomial ring in several variables over a field, these operations are implementable on a computer by means of standard software like Macaulay.*

However, a practical implementation of this algorithm faces difficulties. Namely, to compute $\ker\beta_j$ one has to be able to decide whether $\beta_j(m) \in F^{*^j}(\bar{M})$, for some $m \in \bar{M}$, vanishes. For example, if $\bar{M}$ is principal, i.e., $\bar{M} = R/\mathfrak{a}$, then $F^{*^j}(\bar{M}) = R/\mathfrak{a}^{[p^j]}$ where $\mathfrak{a}^{[p^j]}$ is the ideal generated by the p^j-th powers of the generators of $\mathfrak{a}$. Thinking of $\beta_j(m)$ as an element of R one has to decide whether $\beta_i(m) \in \mathfrak{a}^{[p^i]}$. If $\mathfrak{a}$ is generated by polynomials of degrees $d_1, \ldots, d_s$, then $\mathfrak{a}^{[p^j]}$ is generated by polynomials of degrees $d_1p^j, \ldots, d_sp^j$. These are huge, even for modest values of p and j. Deciding membership in an ideal generated by polynomials of huge degrees consumes a prohibitive amount of memory.

Recall that $f_1, \ldots, f_s \in R = \mathbb{Z}[x_1, \ldots, x_n]$ are polynomials with integer coefficients, $I = (f_1, \ldots, f_s) \subset R$ is the ideal they generate, $\bar{f}_j \in \bar{R} = R/pR$ is obtained from f_j by reducing its coefficients modulo p and $\bar{I} = (\bar{f}_1, \ldots, \bar{f}_s) \subset \bar{R}$ is the ideal generated by $\bar{f}_1, \ldots, \bar{f}_s \in \bar{R}$. Every local cohomology module $H^i_{\bar{I}}(\bar{R})$ acquires a structure of F-finite module as follows. Let $K^\bullet(\bar{R}; \bar{f}_1 \ldots, \bar{f}_s)$ be the Koszul cocomplex

$$0 \to K^0(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s) \xrightarrow{d^0} K^1(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s) \xrightarrow{d^1} \cdots \xrightarrow{d^{s-1}} K^s(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s) \to 0$$

where $K^t(\bar{R}; \bar{f}_1, \cdots, \bar{f}_s)$ is the direct sum of copies of $\bar{R}$ indexed by the cardinality t subsets of the set $\{1, \ldots, s\}$ and the differentials are defined by

$$d^{t-1}(\kappa)_{v_1,\ldots,v_t} = \sum_\ell (-1)^\ell \kappa_{v_1,\ldots,\hat{v_\ell},\ldots,v_t}$$

where $\kappa \in K^{t-1}(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ while $d^{t-1}(\kappa)_{v_1,\ldots,v_t} \in \bar{R}_{v_1,\ldots,v_t} \subseteq K^t(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ and $\kappa_{v_1,\ldots,\hat{v_\ell},\ldots,v_t} \in \bar{R}_{v_1,\ldots,\hat{v_\ell},\ldots,v_t} \subseteq K^{t-1}(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$.

Let $\bar{M}$ be the i-th cohomology module of $K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$. The i-th cohomology module of $K^\bullet(\bar{R}; \bar{f}_1^p, \ldots, \bar{f}_s^p)$ is $F^*(\bar{M})$ ([7, Remarks 1.0(e)]) and $H^i_I(R)$ is the F-finite module generated by the map $\beta : \bar{M} \to F^*(\bar{M})$ which is the map induced on cohomology by the chain map

$$K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s) \xrightarrow{\beta^\bullet} F^*(K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)) \cong K^\bullet(\bar{R}; \bar{f}_1^p, \ldots, \bar{f}_s^p)$$

which is defined as follows: the chain map $\beta^\bullet$ sends $\bar{R}_{v_1,\ldots,j_{\underline{i}}} \subseteq K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ to $\bar{R}_{v_1,\ldots,v_i} \subseteq K^i(\bar{R}; \bar{f}_1^p, \ldots, \bar{f}_s^p)$ via multiplication by $(\bar{f}_{v_1} \cdots \bar{f}_{v_i})^{p-1}$.

In this paper we produce a modification of the algorithm from [7, Remark 2.4] for deciding the vanishing of the F-finite module $H^i_{\bar{I}}(\bar{R})$. This modification avoids deciding membership in an ideal generated by polynomials of huge degrees and as a result it requires only a modest amount of memory. We explain the idea behind this modification after the following proposition.

Proposition 1.2. *Let M be the i-th cohomology module of the Koszul cocomplex $K^\bullet(R; f_1, \ldots, f_s)$. For all but finitely many prime integers p, the i-th cohomology module of the Koszul cocomplex $K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ is $\bar{M} = M/pM$.*

Proof. The cocomplex $K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ is just $\bar{\mathbb{Z}} \otimes_{\mathbb{Z}} K^\bullet(R; f_1, \ldots, f_s)$ where $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$. Since $K^j(R; f_1, \ldots, f_s)$ is a finitely generated R-module for all j, by the generic freeness lemma ([5, Lemma 8.1]) there is $\delta \in \mathbb{Z}$ such that upon inverting δ the images and the kernels of the differentials in the resulting cocomplex $K^\bullet(R_\delta; f_1, \ldots, f_s)$ as well as the cohomology modules of this cocomplex are free $\mathbb{Z}_\delta$-modules. Hence for every prime integer p that does not divide δ, the i-th cohomology module of $\bar{\mathbb{Z}} \otimes_{\mathbb{Z}} K^\bullet(R_\delta; f_1, \ldots, f_s) \cong \bar{\mathbb{Z}} \otimes_{\mathbb{Z}} K^\bullet(R; f_1, \ldots, f_s) = K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ is $\bar{M}$. $\square$

It is worth pointing out that the proof of the generic freeness lemma [5, Lemma 8.1] makes the integer δ algorithmically computable, given the polynomials $f_1, \ldots, f_s$. We are leaving the details to the interested reader.

Now we are ready to discuss the idea behind our modification of the algorithm from [7, Remark 2.4] for deciding the vanishing of $H^i_{\bar{I}}(\bar{R})$. Let M be the i-th cohomology module of the Koszul cocomplex $K^\bullet(R; f_1, \ldots, f_s)$. For every prime integer p such that the i-th cohomology module of the Koszul cocomplex $K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ is $\bar{M} = M/pM$, let $\beta : \bar{M} \to F^*(\bar{M})$ be a generating morphism of $H^i_{\bar{I}}(\bar{R})$ as above and let $\beta_j : \bar{M} \to F^{*^j}(\bar{M})$ be as in the statement of Proposition 1.1. According to Proposition 1.1 there exists an integer r such that $\ker \beta_r = \ker \beta_{r+1}$. In the next section, Section 2, we show that there is a computable upper bound u on the minimum such integer r; this upper bound u depends only on M and is independent of the particular prime integer p. And in Section 3 we produce an algorithm to decide whether β_j vanishes for fixed j and p. It is this algorithm that consumes a modest amount of memory. But it only decides the vanishing of β_j, not whether $\ker \beta_j = \ker \beta_{j-1}$. It is for this reason that we need a computable upper bound u (which just happens to be the same for all prime integers p, so u has to be computed just once). According to Proposition 1.1(b,c), the fact that $\ker \beta_r = \ker \beta_{r+1}$ for some $r \leq u$ implies that $H^i_{\bar{I}}(\bar{R}) = 0$ if and only if $\beta_u = 0$. So for every prime integer p, it's enough to decide whether $\beta_j = 0$ for just one specific value of j, namely $j = u$.

2. An upper bound on the number of steps involved in the algorithm

In this section, M is a finitely generated R-module where $R = \mathbb{Z}[x_1, \ldots, x_n]$. Recall that $\bar{R} = \bar{\mathbb{Z}}[x_1, \ldots, x_n]$ where $\bar{\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}$ and $\bar{M} = \bar{\mathbb{Z}} \otimes_{\mathbb{Z}} M = M/pM$. Let $\beta : \bar{M} \to F^*(\bar{M})$ be a generating morphism of an F-finite module $\mathcal{M}$. In the preceding section, we quoted an algorithm from [7, Remark 2.4] that decides whether $\mathcal{M} = 0$. By the number of steps involved in this algorithm we mean the first integer r such that $\ker\beta_r = \ker\beta_{r-1}$. The main result of this section is Corollary 2.6 which produces an upper bound on r that depends only on M (i.e. it is independent of p and β).

Lemma 2.1. *Notation being as above, if $\bar{M}$ has finite length in the category of $\bar{R}$-modules, then the first integer r such that $\ker\beta_r = \ker\beta_{r-1}$ satisfies the inequality $r \le u$, where u is the length of $\bar{M}$. In particular, $\mathcal{M} = 0$ if and only if $\ker\beta_u = \bar{M}$, i.e., $\beta_u = 0$.*

Proof. Since the length of $\bar{M}$ is finite, the number of strict containments in the ascending chain $\ker\beta_1 \subseteq \ker\beta_2 \subseteq \dots$ of submodules of $\bar{M}$ cannot be bigger than the length of $\bar{M}$. Since this ascending chain stabilizes at the first integer r such that $\ker\beta_r = \ker\beta_{r-1}$, this integer r must be less than or equal to the length of $\bar{M}$. $\square$

We define the *universal length* u of a finitely generated $\bar{R}$-module N as follows:

Definition 2.2. $u(N) = \max\{\text{length } \Gamma_{\mathfrak{p}}(N_{\mathfrak{p}}) \mid \mathfrak{p} \in \operatorname{Ass} N\}$, *where $\operatorname{Ass} N$ is the set of the associated primes of N, the torsion functor $\Gamma_{\mathfrak{p}}$ is the 0-th local cohomology functor $H^0_{\mathfrak{p}}(-)$, and the length is measured in the category of $R_{\mathfrak{p}}$-modules.*

Corollary 2.3. *Notation being as above, let $u = u(\bar{M})$. The first integer r such that $\ker\beta_r = \ker\beta_{r-1}$ satisfies the inequality $r \le u$. In particular, $\mathcal{M} = 0$ if and only if $\beta_u = 0$.*

Proof. By [7, Remark 2.13], we have $\operatorname{Ass}\mathcal{M} \subseteq \operatorname{Ass}\bar{M}$. Hence $\mathcal{M}$ vanishes if and only if $\Gamma_{\mathfrak{p}}(\mathcal{M}_{\mathfrak{p}})$ vanishes for all $\mathfrak{p} \in \operatorname{Ass}\bar{M}$. The module $\Gamma_{\mathfrak{p}}(\mathcal{M}_{\mathfrak{p}})$ is the limit of the system

$$\Gamma_{\mathfrak{p}}(\bar{M}_{\mathfrak{p}}) \to F^*(\Gamma_{\mathfrak{p}}(\bar{M}_{\mathfrak{p}})) \to F^{*^2}(\Gamma_{\mathfrak{p}}(\bar{M}_{\mathfrak{p}})) \to \dots$$

obtained by applying the functor $\Gamma_{\mathfrak{p}}(-_{\mathfrak{p}})$ to (1.1) and taking into account that the functors F^* and $\Gamma_{\mathfrak{p}}(-_{\mathfrak{p}})$ commute with each other. But the module $\Gamma_{\mathfrak{p}}(\bar{M}_{\mathfrak{p}})$ is of finite length over the local ring $R_{\mathfrak{p}}$ and its length is at most $u = u(\bar{M})$. So by Lemma 2.1, $\Gamma_{\mathfrak{p}}(\mathcal{M}_{\mathfrak{p}}) = 0$ if and only if the composition of the first u maps in the above system, i.e., the map

$$\Gamma_{\mathfrak{p}}(\beta_u)_{\mathfrak{p}} : \Gamma_{\mathfrak{p}}(\bar{M}_{\mathfrak{p}}) \to F^{*^{u+1}}(\Gamma_{\mathfrak{p}}(\bar{M}_{\mathfrak{p}}))$$

is zero. But the image of this map is nothing but $(\Gamma_{\mathfrak{p}}(\operatorname{im}\beta_u))_{\mathfrak{p}}$. Hence $\Gamma_{\mathfrak{p}}(\mathcal{M}_{\mathfrak{p}}) = 0$ if and only if $(\Gamma_{\mathfrak{p}}(\operatorname{im}\beta_u))_{\mathfrak{p}} = 0$.

It remains to show that $\operatorname{im}\beta_u = 0$ if and only if $(\Gamma_{\mathfrak{p}}(\operatorname{im}\beta_u))_{\mathfrak{p}} = 0$ for every $\mathfrak{p} \in \operatorname{Ass}\bar{M}$. This follows from the fact that $\operatorname{im}\beta_u$ is a submodule of $F^{*^{u+1}}(\bar{M})$ and therefore $\operatorname{Ass}(\operatorname{im}\beta_u) \subseteq \operatorname{Ass} F^{*^{u+1}}(\bar{M}) = \operatorname{Ass}\bar{M}$ by [6, Corollary 1.6]. $\square$

Lemma 2.4. *For all but finitely many prime integers p, the following hold.*

(a) The associated primes of $\bar{M}$ are minimal primes of ideals $(p, \mathfrak{p})$ as $\mathfrak{p}$ runs over the associated primes of M, and

(b) $\overline{\Gamma_{\mathfrak{p}}(M)} \stackrel{\text{def}}{=} \Gamma_{\mathfrak{p}}(M)/p\Gamma_{\mathfrak{p}}(M) \cong \Gamma_{(p,\mathfrak{p})}(\bar{M})$ for every associated prime $\mathfrak{p}$ of M.

It is worth pointing out that even if $\mathfrak{p}$ is an embedded associated prime of the module M, part (a) makes a claim only about minimal primes of the ideal $(p, \mathfrak{p})$, which would then be embedded associated primes of the module $\bar{M}$: no claim whatsoever is made in part (a) about embedded associated primes of the ideal $(p, \mathfrak{p})$.

Proof. (a) The set of the associated primes of M is finite and each associated prime of M contains at most one prime integer p. Hence all but finitely many prime integers p do not belong to any associated prime of M. Fix one such prime integer p.

Let $\mathfrak{q}$ be a prime ideal of R containing the integer p and associated to $\bar{M}$. This is the case if and only if $\bar{M}_{\mathfrak{q}} \neq 0$ and $\operatorname{depth} \bar{M}_{\mathfrak{q}} = 0$. Since $p \in \mathfrak{q}$ does not belong to any associated prime of M, the prime ideal $\mathfrak{q}$ is not associated to M, i.e., $\operatorname{depth} M_{\mathfrak{q}} > 0$. Since $\bar{M}_{\mathfrak{q}} = M_{\mathfrak{q}}/pM_{\mathfrak{q}}$, we conclude that $\{p\}$ is a maximal $M_{\mathfrak{q}}$-regular sequence of length 1, i.e., $\operatorname{depth} M_{\mathfrak{q}} = 1$.

Let $h = \dim R_{\mathfrak{q}} = \operatorname{height} \mathfrak{q}$, then the Auslander-Buchsbaum theorem ([10, Theorem 19.1]) implies that the projective dimension of $M_{\mathfrak{q}}$ in the category of $R_{\mathfrak{q}}$-modules is $h - \operatorname{depth} M_{\mathfrak{q}} = h - 1$. This in turn implies that $\operatorname{Ext}^{h-1}_{R_{\mathfrak{q}}}(M_{\mathfrak{q}}, R_{\mathfrak{q}}) \neq 0$. Since $\operatorname{Ext}^{h-1}_{R_{\mathfrak{q}}}(M_{\mathfrak{q}}, R_{\mathfrak{q}}) = \operatorname{Ext}^{h-1}_R(M, R)_{\mathfrak{q}}$, we conclude that the prime ideal $\mathfrak{q}$ is in the support of $\operatorname{Ext}^{h-1}_R(M, R)$.

If $\mathfrak{Q}$ is a prime ideal of height $< h - 1$, then $R_{\mathfrak{Q}}$ is regular and of dimension $< h - 1$, hence $\operatorname{Ext}^{h-1}_R(M, R)_{\mathfrak{Q}} = \operatorname{Ext}^{h-1}_{R_{\mathfrak{Q}}}(M_{\mathfrak{Q}}, R_{\mathfrak{Q}}) = 0$. Therefore every minimal prime of the R-module $\operatorname{Ext}^{h-1}_R(M, R)$ has height at least $h - 1$.

The height $h - 1$ minimal primes of $\operatorname{Ext}^{h-1}_R(M, R)$ are precisely the associated primes of M of height $h - 1$. Indeed, $\operatorname{Ext}^{h-1}_R(M, R)_{\mathfrak{p}} = \operatorname{Ext}^{h-1}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, R_{\mathfrak{p}}) \neq 0$ for a height $h-1$ prime ideal $\mathfrak{p}$ is equivalent by the Auslander-Buchsbaum theorem ([10, Theorem 19.1]) to $\operatorname{depth} M_{\mathfrak{p}} = 0$, i.e., $\mathfrak{p}$ being associated to M.

If $\mathfrak{q}$ contains a minimal prime $\mathfrak{p}$ of $\operatorname{Ext}^{h-1}_R(M, R)$ of height $h - 1$, then $\mathfrak{q}$, being of height h and containing $p \notin \mathfrak{p}$, is a minimal prime over the ideal $(p, \mathfrak{p})$.

If $\mathfrak{q}$ does not contain a minimal prime of $\operatorname{Ext}^{h-1}_R(M, R)$ of height $h - 1$, then $\mathfrak{q}$, being of height h and in the support of $\operatorname{Ext}^{h-1}_R(M, R)$, is itself a minimal prime of $\operatorname{Ext}^{h-1}_R(M, R)$ because every minimal prime of $\operatorname{Ext}^{h-1}_R(M, R)$ has height at least $h - 1$.

Thus if a prime integer p does not belong to any associated prime of M and does not belong to any associated prime of $\operatorname{Ext}^{h-1}_R(M, R)$ of height h, as h runs over all integers $\leq \dim R$, then every associated prime of $\bar{M}$ is a minimal prime over the ideal $(p, \mathfrak{p})$ where $\mathfrak{p}$ is an associated prime of M. Since the set of the associated primes of M and the set of the associated primes of $\operatorname{Ext}^{h-1}_R(M, R)$ of height h are finite, all but finitely many prime integers p have this property. This proves (a).

(b) The modules in the short exact sequence $0 \to \Gamma_{\mathfrak{p}}(M) \to M \to M/\Gamma_{\mathfrak{p}}(M) \to 0$ are finitely generated over R and R is a finitely generated $\mathbb{Z}$-algebra. Hence by the generic freeness lemma ([5, Lemma 8.1]) there is an integer $\gamma \in \mathbb{Z}$ such that $\Gamma_{\mathfrak{p}}(M)_\gamma, M_\gamma$ and $(M/\Gamma_{\mathfrak{p}}(M))_\gamma$ are free $\mathbb{Z}_\gamma$-modules. Since the induced sequence of free $\mathbb{Z}_\gamma$-modules $0 \to \Gamma_{\mathfrak{p}}(M)_\gamma \to M_\gamma \to (M/\Gamma_{\mathfrak{p}}(M))_\gamma \to 0$ is exact, tensoring over $\mathbb{Z}$ with $\mathbb{Z}/p\mathbb{Z}$ for a prime integer p which does not divide γ produces an exact sequence

$$0 \to \overline{\Gamma_{\mathfrak{p}}(M)} \to \bar{M} \to \overline{M/\Gamma_{\mathfrak{p}}(M)} \to 0$$

where $\overline{\Gamma_{\mathfrak{p}}(M)} = \Gamma_{\mathfrak{p}}(M)/p\Gamma_{\mathfrak{p}}(M)$ and $\overline{M/\Gamma_{\mathfrak{p}}(M)} = (M/\Gamma_{\mathfrak{p}}(M))/p(M/\Gamma_{\mathfrak{p}}(M))$.

Viewing $\overline{\Gamma_{\mathfrak{p}}(M)}$ as a submodule of $\bar{M}$ and considering that every element of $\overline{\Gamma_{\mathfrak{p}}(M)}$ is annihilated both by p and by some power of the ideal $\mathfrak{p}$, we conclude that

$\overline{\Gamma_{\mathfrak{p}}(M)} \subseteq \Gamma_{(p,\mathfrak{p})}(\bar{M})$. To prove (b) that this containment is actually an equality for all but finitely many p, it is enough to show that $\Gamma_{(p,\mathfrak{p})}(\bar{M}/\overline{\Gamma_{\mathfrak{p}}(M)}) = 0$, i.e., $\Gamma_{(p,\mathfrak{p})}(\overline{M/\Gamma_{\mathfrak{p}}(M)}) = 0$ for all but finitely many p (since $\bar{M}/\overline{\Gamma_{\mathfrak{p}}(M)} \cong \overline{M/\Gamma_{\mathfrak{p}}(M)}$). And to prove this vanishing, it is enough to show that for all but finitely many p, none of the minimal primes of the ideal $(p,\mathfrak{p})$ are associated to $\overline{M/\Gamma_{\mathfrak{p}}(M)}$.

Let h be the height of $\mathfrak{p}$ and let $\mathfrak{p}_1,\dots,\mathfrak{p}_s$ be the associated primes of $M/\Gamma_{\mathfrak{p}}(M)$ of height h. Since the heights of $\mathfrak{p}$ and $\mathfrak{p}_i$ are the same and $\mathfrak{p}$ is not associated to $M/\Gamma_{\mathfrak{p}}(M)$, i.e., $\mathfrak{p} \neq \mathfrak{p}_i$ for every i, the ideals $\mathfrak{p}+\mathfrak{p}_i$ are bigger than $\mathfrak{p}$ for every i. Hence the height of every prime ideal containing $\mathfrak{p}+\mathfrak{p}_i$ is at least $h+1$. This implies that there are only finitely many prime ideals $\mathfrak{Q}_1,\dots,\mathfrak{Q}_v$ of R of height $h+1$ that contain both $\mathfrak{p}$ and $\mathfrak{p}_i$ for some i.

Since only finitely many prime integers p are contained in one of these prime ideals $\mathfrak{Q}_1,\dots,\mathfrak{Q}_v$, and since the height of every minimal prime over the ideal $(p,\mathfrak{p})$ is $h+1$, we conclude that for all but finitely many prime integers p, no minimal prime over the ideal $(p,\mathfrak{p})$ coincides with one of the $\mathfrak{Q}_1,\dots,\mathfrak{Q}_v$. That is for all but finitely many prime integers p, no minimal prime over the ideal $(p,\mathfrak{p})$ contains one of the ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_s$.

But it follows from (a) that for all but finitely many prime integers p, every associated prime of $\overline{M/\Gamma_{\mathfrak{p}}(M)}$ of height $h+1$ contains an associated prime of $M/\Gamma_{\mathfrak{p}}(M)$ of height h, i.e., it contains one of the ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_s$. This finally shows that for all but finitely many prime integers p, no minimal prime over the ideal $(p,\mathfrak{p})$ is associated to $\overline{M/\Gamma_{\mathfrak{p}}(M)}$ and completes the proof of (b). ☐

Corollary 2.5. *The maximum of $u(\bar{M} = M/pM)$, as p runs through all the prime integers, is finite, where u is defined in Definition* 2.2.

Proof. If all associated primes of M contain prime integers, then for all prime integers p, except those finitely many contained in associated primes of M, the module $\bar{M} = M/pM$ is zero. Hence $u(\bar{M}) = 0$ for all but finitely many p.

Otherwise, let $\mathfrak{p}$ be an associated prime of M that does not contain any prime integer. Let h be the height of $\mathfrak{p}$. Let $y_1,\dots,y_{n-h} \in \tilde{R} = R \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[x_1 \dots, x_n]$ be linear combinations of variables $x_1,\dots,x_n$ with coefficients in $\mathbb{Q}$ such that $\tilde{R}/\mathfrak{p}\tilde{R}$ is finite over the ring $S = \mathbb{Q}[y_1,\dots,y_{n-h}]$. Since the field $\mathbb{Q}$ is infinite, generic linear combinations will do.

For each i, let $\bar{x}_i \in \tilde{R}/\mathfrak{p}\tilde{R}$ be the image of x_i under the natural map $\tilde{R} \to \tilde{R}/\mathfrak{p}\tilde{R}$ and let $\bar{x}_i^{t_i} + s_{i,1}\bar{x}_i^{t_i-1} + s_{i,2}\bar{x}_i^{t_i-2} + \dots = 0$, where $s_{i,j} \in S$, be an equation expressing integral dependence of $\bar{x}_i$ on S. The polynomials $s_{i,j} \in S$ have a finite number of coefficients in $\mathbb{Q}$ and $y_1,\dots,y_{n-h}$, as linear combinations of $x_1,\dots,x_n$, also have a finite number of coefficients in $\mathbb{Q}$. All these coefficients have a common denominator $\delta \in \mathbb{Z}$. Hence $y_1,\dots,y_{n-h} \in R_\delta = \mathbb{Z}_\delta[x_1,\dots,x_n]$ and $R_\delta/\mathfrak{p}R_\delta$ is a finite S_δ-module where $S_\delta = \mathbb{Z}_\delta[y_1,\dots,y_{n-h}]$.

Since S_δ is a subring of R_δ, the module M_δ has a natural structure of S_δ-module, hence so does $\Gamma_{\mathfrak{p}}(M_\delta)$. This is a finitely generated R_δ-submodule of M_δ supported at $\mathfrak{p}$ and therefore annihilated by some power of $\mathfrak{p}$. Hence $\Gamma_{\mathfrak{p}}(M_\delta)$ has a finite filtration with quotients finitely generated $R_\delta/\mathfrak{p}R_\delta$-modules. Since $R_\delta/\mathfrak{p}R_\delta$ is a finitely generated S_δ-module, $\Gamma_{\mathfrak{p}}(M)_\delta$ is a finitely generated S_δ-module.

Let p be a prime integer that does not divide δ, does not belong to any associated prime of M and does not belong to any height h minimal prime of the R-module

$\mathrm{Ext}_R^{h-1}(M,R)$ as h runs through all integers $\leq \dim R$. This includes all but finitely many prime integers p.

Since p does not belong to any associated prime of M, the module M has zero p-torsion. Let $S_{(p)}$ be the ring S localized at the principal prime ideal pS. Since the ring $S_{(p)}$ is a discrete valuation ring, since the module $\Gamma_{\mathfrak{p}}(M)$, being a submodule of M, has zero p-torsion and since $\Gamma_{\mathfrak{p}}(M)_\delta$ is a finitely generated S_δ-module, we conclude that $\Gamma_{\mathfrak{p}}(M)_{(p)} \stackrel{\text{def}}{=} S_{(p)} \otimes_S \Gamma_{\mathfrak{p}}(M)$ is a free $S_{(p)}$-module of finite rank $\rho = \dim_K(K \otimes_S \Gamma_{\mathfrak{p}}(M))$ where K is the fraction field of S. Hence the dimension of $\overline{\Gamma_{\mathfrak{p}}(M)_{(p)}} \stackrel{\text{def}}{=} \Gamma_{\mathfrak{p}}(M)_{(p)}/p\Gamma_{\mathfrak{p}}(M)_{(p)}$ over the residue field κ of $S_{(p)}$ also equals ρ. This implies that for every minimal prime $\mathfrak{q}$ over the ideal $(p,\mathfrak{p})$ the length of $\overline{\Gamma_{\mathfrak{p}}(M)}_{\mathfrak{q}}$ in the category of $R_{\mathfrak{q}}$-modules is at most ρ. Clearly the integer ρ is independent of the prime integer p.

It follows from Lemma 2.4(b) that $\overline{\Gamma_{\mathfrak{p}}(M)_{(p)}} \cong S_{(p)} \otimes_S \Gamma_{(p,\mathfrak{p})}(\bar{M})$ for all but finitely many prime integers p. Hence for every minimal prime $\mathfrak{q}$ over the ideal $(p,\mathfrak{p})$, the length of $\Gamma_{\mathfrak{q}}(\bar{M})_{\mathfrak{q}}$ in the category of $\bar{R}_{\mathfrak{q}}$-modules is at most ρ, which is independent of p. But according to Lemma 2.4(a), for all but finitely many p, every associated prime of $\bar{M}$ is minimal over $(p,\mathfrak{p})$ for some associated prime $\mathfrak{p}$ of M. □

Corollary 2.6. *Let $u = u(M)$ be the maximum of $u(\bar{M} = M/pM)$, as p runs through all the prime integers. Let p be any prime integer, let $\beta : \bar{M} \to F(\bar{M})$ be an $\bar{R}$-module homomorphism and let $\mathcal{M}$ be the F-finite module generated by β.*

(a) The first integer r such that $\ker\beta_r = \ker\beta_{r-1}$ satisfies the inequality $r \leq u$.

(b) $\mathcal{M} = 0$ if and only if $\beta_u = 0$.

Proof. This is a consequence of Corollaries 2.3 and 2.5. □

This corollary establishes an upper bound on the number of steps involved in the algorithm (i.e. on the first integer r such that $\ker\beta_r = \ker\beta_{r-1}$). This upper bound depends only on the R-module M and is independent of the prime integer p and even of the $\bar{R}$-module map $\beta : \bar{M} \to F^*(\bar{M})$.

The integer $u = u(M)$ plays an important role in our modification of the algorithm from [7, Remark 2.4]. Given the module M (say through generators and relations), it follows from the proofs of Lemma 2.4 and Corollary 2.5 that the integer $u = u(M)$ is algorithmically computable; we are leaving the details to the interested reader.

3. The Algorithm

In this section we complete the description of our modification of the algorithm from [7, Remark 2.4] for deciding the vanishing of local cohomology modules $H^i_{\bar{I}}(\bar{R})$. Recall that $R = \mathbb{Z}[x_1,\ldots,x_n]$ and $\bar{R} = R/pR = (\mathbb{Z}/p\mathbb{Z})[x_1,\ldots,x_n]$ where p is a prime integer. Let $f_1,\ldots,f_s \in R$ be polynomials and see Section 1 for the definition of the Koszul cocomplex $K^\bullet(R;f_1,\ldots,f_s)$. In this section, M denotes the i-th cohomology module of $K^\bullet(R;f_1,\ldots,f_s)$. Clearly M is a finitely generated R-module. We assume that the prime integer p has the property that the i-th cohomology module of the Koszul cocomplex $K^\bullet(\bar{R};\bar{f}_1,\ldots,\bar{f}_s)$ is $\bar{M} = M/pM$ where $\bar{f}_t \in \bar{R}$ is the polynomial obtained from f_t by reducing its coefficients modulo p. According to Proposition 1.2, all but finitely many prime integers p have this property. Let $I = (f_1,\ldots,f_s) \subset R$ (resp. $\bar{I} = (\bar{f}_1,\ldots,\bar{f}_s) \subset \bar{R}$) be the ideal generated by $f_1,\ldots,f_s$ (resp. $\bar{f}_1,\ldots,\bar{f}_s$).

As is pointed out in Section 1, the i-th cohomology module of $K^\bullet(\bar{R};\bar{f}_1^p,\dots,\bar{f}_s^p)$ is $F^*(\bar{M})$ and $H^i_I(\bar{R})$ is the F-finite module generated by the map $\beta:\bar{M}\to F^*(\bar{M})$, which is the map induced on cohomology by the chain map

$$\beta^\bullet : K^\bullet(\bar{R};\bar{f}_1,\dots,\bar{f}_s)\to F^*(K^\bullet(\bar{R};\bar{f}_1,\dots,\bar{f}_s))\cong K^\bullet(\bar{R};\bar{f}_1^p,\dots,\bar{f}_s^p),$$

which sends $\bar{R}_{v_1,\dots,v_i}\subseteq K^i(\bar{R};\bar{f}_1,\dots,\bar{f}_s)$ to $\bar{R}_{v_1,\dots,v_i}\subseteq K^i(\bar{R};\bar{f}_1^p,\dots,\bar{f}_s^p)$ via multiplication by $(\bar{f}_{v_1}\cdots\bar{f}_{v_i})^{p-1}$. Similarly, for every j, the i-th cohomology module of $K^\bullet(\bar{R};\bar{f}_1^{p^j},\dots,\bar{f}_s^{p^j})$ is $F^{*^j}(\bar{M})$ and the map $\beta_j:\bar{M}\to F^{*^j}(\bar{M})$ of Proposition 1.1 is the map induced on cohomology by the chain map

$$\beta_j^\bullet : K^\bullet(\bar{R};\bar{f}_1,\dots,\bar{f}_s)\to F^{*^j}(K^\bullet(\bar{R};\bar{f}_1,\dots,\bar{f}_s))\cong K^\bullet(\bar{R};\bar{f}_1^{p^j},\dots,\bar{f}_s^{p^j}),$$

which sends $\bar{R}_{v_1,\dots,v_i}\subseteq K^i(\bar{R};\bar{f}_1,\dots,\bar{f}_s)$ to $\bar{R}_{v_1,\dots,v_i}\subseteq K^i(\bar{R};\bar{f}_1^{p^j},\dots,\bar{f}_s^{p^j})$ via multiplication by $(\bar{f}_{j_1}\cdots\bar{f}_{j_i})^{p^j-1}$. This is because $\beta_j^\bullet=F^{*^{j-1}}(\beta^\bullet)\circ\cdots\circ F^*(\beta^\bullet)\circ\beta^\bullet$, where every $F^{*^t}(\beta^\bullet)$ sends $\bar{R}_{v_1,\dots,v_i}\subseteq K^i(\bar{R};\bar{f}_1,\dots,\bar{f}_s)$ to $\bar{R}_{v_1,\dots,v_i}\subseteq K^i(\bar{R};\bar{f}_1^{p^t},\dots,\bar{f}_s^{p^t})$ via multiplication by $(\bar{f}_{j_1}\cdots\bar{f}_{j_i})^{(p-1)p^t}$, and the equality $(p-1)+(p-1)p+(p-1)p^2+\cdots+(p-1)p^{j-1}=p^j-1$ holds.

The main result of this section is an algorithm to decide for a fixed j whether $\beta_j:\bar{M}\to F^{*j}(\bar{M})$ is the zero map, the point being that this algorithm avoids deciding membership in an ideal generated by polynomials whose degrees rapidly grow with the growth of p. As a result, the memory consumed by this algorithm grows slowly with the growth of p (more precisely, it grows linearly rather than exponentially). This algorithm plays a crucial role in our modification of the algorithm from [7, Remark 2.4].

Denote the multi-index $(i_1,\cdots,i_n)$ by $\bar{i}$. Let $F^\ell:\bar{R}_s\to\bar{R}_t$ be the ℓ-fold Frobenius homomorphism where, as in Section 1, R_s and R_t are copies of R. Since $\bar{\mathbb{Z}}$ is perfect, $\bar{R}_t$ is a free $\bar{R}_s$-module on the $p^{\ell n}$ monomials $e_{\bar{i}}=x_1^{i_1}\cdots x_n^{i_n}$ where $0\leqslant i_j<p^\ell$ for every j. Suppose N' is an $\bar{R}_s$-module. Then the pull-back $F^{*^\ell}(N')=\bar{R}_t\otimes_{\bar{R}_s}N'=\bigoplus_{\bar{i}}e_{\bar{i}}\otimes_{\bar{R}_s}N'$ is an $\bar{R}_t$-module, where $e_{\bar{i}}\otimes_{\bar{R}_s}N'(\cong N')$ will be called the $e_{\bar{i}}$-component of $F^*(N')$. Suppose N'' is an $\bar{R}_t$-module. For each $f\in\mathrm{Hom}_{\bar{R}_t}(N'',F^{*^\ell}(N'))$, define $f_{\bar{i}}=p_{\bar{i}}\circ f:F^\ell_*(N'')\to N'$, where

$$p_{\bar{i}}:F^{*^\ell}(N')(=\bigoplus_{\bar{i}}(e_{\bar{i}}\otimes_{\bar{R}_s}N'))\xrightarrow{y\mapsto e_{\bar{i}}\otimes p_{\bar{i}}(y)}e_{\bar{i}}\otimes_{\bar{R}_s}N'(\cong N')$$

is the natural projection onto the $e_{\bar{i}}$-component. We will need the following result from [9].

Theorem 3.1. *(Theorem 3.3 in [9]) We denote the multi-index $(p^\ell-1,\cdots,p^\ell-1)$ by $\overline{p^\ell-1}$. For every $\bar{R}_t$-module N'' and every $\bar{R}_s$-module N', there is an $\bar{R}_t$-linear isomorphism*

$$\begin{aligned}\mathrm{Hom}_{\bar{R}_s}(F^\ell_*(N''),N')&\cong\mathrm{Hom}_{\bar{R}_t}(N'',F^{*^\ell}(N'))\\ g_{\overline{p^\ell-1}}(-)&\leftarrow(g=\oplus_{\bar{i}}(e_{\bar{i}}\otimes_{\bar{R}_s}g_{\bar{i}}(-)))\\ h&\mapsto\oplus_{\bar{i}}(e_{\bar{i}}\otimes_{\bar{R}_s}h(e_{\overline{p^\ell-1}-\bar{i}}(-))).\end{aligned}$$

Definition 3.2. *Let $\beta_j:\bar{M}\to F^{*^j}(\bar{M})$ be the map from Proposition 1.1. Setting $N'=N''=\bar{M}$, we denote by $\alpha_j:F^j_*(\bar{M})\to\bar{M}$ the map associated to β_j by the isomorphism in Theorem 3.1, namely, $\alpha_j=(\beta_j)_{\overline{p^j-1}}$.*

Theorem 3.1 implies the following.

Corollary 3.3. *(a) In the above notation, $\beta_j = 0$ if and only if $\alpha_j = 0$.*

(b) Let $m_1, \ldots, m_v$ generate $\bar{M}$ as an R-module. The map $\beta_j = 0$ if and only if $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} m_t) = 0$ for every t and every $(i_1, \cdots, i_n)$ where $0 \leq i_q \leq p^j - 1$ for every q.

Proof. (a) is immediate from the fact that an isomorphism sends zero to zero while (b) follows from (a) and the fact that the set of elements $\{x_1^{i_1} \cdots x_n^{i_n} m_t\}$ generates $F_*^j(\bar{M})$ as an R_s-module, so $\alpha_j = 0$ if and only if α_j sends every generator of $F_*^j(\bar{M})$ to zero. □

Theorem 3.1 admits the following straightforward extension to complexes.

Corollary 3.4. *For every complex of $\bar{R}_t$-modules $\mathcal{N}''^{\bullet}$ and for every complex of $\bar{R}_s$-modules $\mathcal{N}'^{\bullet}$, there is an $\bar{R}_t$-linear isomorphism*

$$\begin{aligned} \mathrm{Hom}_{\bar{R}_s}(F_*^{\ell}(\mathcal{N}''^{\bullet}), \mathcal{N}'^{\bullet}) &\cong \mathrm{Hom}_{\bar{R}_t}(\mathcal{N}''^{\bullet}, F^{*^{\ell}}(\mathcal{N}'^{\bullet})) \\ g^{\bullet}_{\overline{p^{\ell}-1}}(-) &\leftarrow (g^{\bullet} = \oplus_{\bar{i}}(e_{\bar{i}} \otimes_{\bar{R}_s} g^{\bullet}_{\bar{i}}(-))) \\ h^{\bullet} &\mapsto \oplus_{\bar{i}}(e_{\bar{i}} \otimes_{\bar{R}_s} h^{\bullet}(e_{\overline{p^{\ell}-1-\bar{i}}}(-))), \end{aligned}$$

where Hom *denotes chain maps.*

A chain map $g^{\bullet} : \mathcal{N}''^{\bullet} \to F^{*^{\ell}}(\mathcal{N}'^{\bullet})$ induces a map

$$g^i : H^i(\mathcal{N}''^{\bullet}) \to H^i(F^{*^{\ell}}(\mathcal{N}'^{\bullet})) \cong F^{*^{\ell}}(H^i(\mathcal{N}'^{\bullet}))$$

on cohomology where the isomorphism follows from the fact that F^* is an exact functor. Let $h^{\bullet} : F_*^{\ell}(\mathcal{N}''^{\bullet}) \to \mathcal{N}'^{\bullet}$ be the chain map that corresponds to $g^{\bullet}$ under the isomorphism of Corollary 3.4. The chain map $h^{\bullet}$ induces a map

$$h^i : H^i(F_*^{\ell}(\mathcal{N}''^{\bullet})) \cong F_*^{\ell}(H^i(\mathcal{N}''^{\bullet})) \to H^i(\mathcal{N}'^{\bullet})$$

on cohomology where the isomorphism follows from the fact that F_* is an exact functor. It is straightforward from the definitions and the exactness of the functors F^* and F_* that h^i is the map associated to the map g^i by the isomorphism of Theorem 3.1 (upon setting $N'' = H^i(\mathcal{N}''^{\bullet})$ and $N' = H^i(\mathcal{N}'^{\bullet})$).

Let

$$\alpha_j^{\bullet} : F_*^j(K^{\bullet}(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)) \to K^{\bullet}(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$$

be the chain map associated to the above chain map $\beta_j^{\bullet}$ by the isomorphism of Corollary 3.4. It follows that the map $\alpha_j : F_*^j(\bar{M}) \to \bar{M}$ induced on cohomology by the chain map $\alpha_j^{\bullet}$ is precisely the map associated to $\beta_j : \bar{M} \to F^{*^j}(\bar{M})$ by the isomorphism of Theorem 3.1. Thus to compute $\alpha_j(m) \in \bar{M}$ for some $m \in F_*^j(\bar{M})$, one can take a cocycle $\tilde{m} \in F_*^j(K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s))$ that represents $m \in F_*^j(\bar{M})$, compute its image in $K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ via the chain map $\alpha_j^{\bullet}$ and take the class of this image in the i-th cohomology of $K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$, i.e., in $\bar{M}$. This class would be $\alpha_j(m)$.

Let $m_1, \ldots, m_v \in M$ generate M as an R-module. Let $\bar{m}_t \in \bar{M} = M/pM$ be the image of m_t under the natural map $M \to M/pM$. Clearly, $\bar{m}_1 \ldots, \bar{m}_v$ generate $\bar{M}$ as an $\bar{R}$-module. According to Corollary 3.3, the map β_j is the zero map if and only if $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) = 0$ for every $t \leq v$ and every $(i_1, \cdots, i_n)$ where $0 \leq i_q \leq p^j - 1$ for every q.

We are ready to describe our promised algorithm to decide, for a fixed j, whether $\beta_j : \bar{M} \to F^{*j}(\bar{M})$ is the zero map. As has just been explained, this is equivalent to deciding the vanishing of $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t)$ for all tuples $(i_1, \ldots, i_n, t)$. Our description consists of five steps. In Step 1 we explain that to decide the vanishing of $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t)$ for all tuples is equivalent to deciding the vanishing of $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t)$ for a fixed tuple in the sense that required memory differs by an amount that is independent of p. In Step 2 we explain that to decide the vanishing of $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t)$ for a fixed tuple reduces to first computing the cocycle $\alpha_j^\bullet(x_1^{i_1} \cdots x_n^{i_n} \overline{\tilde{m}_t}) \in K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ and then deciding whether this cocycle represents the zero element in the cohomology module (the element $\overline{\tilde{m}_t}$ is defined in Step 2). In Step 3 we explain that the computation of $\alpha_j^\bullet(x_1^{i_1} \cdots x_n^{i_n} \overline{\tilde{m}_t}) \in K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ reduces to the computation of $\alpha^\bullet_{j,v_1,\ldots,v_i}(x_1^{i_1} \cdots x_n^{i_n} \overline{\tilde{m}}_{t,v_1,\ldots,v_i})$ for every index $\{v_1, \ldots, v_i\}$ (the meaning of the index $\{v_1, \ldots, v_i\}$ is explained in Step 3). In Step 4 we describe the computation of $\alpha^\bullet_{j,v_1,\ldots,v_i}(x_1^{i_1} \cdots x_n^{i_n} \overline{\tilde{m}}_{t,v_1,\ldots,v_i})$ for a fixed index $\{v_1, \ldots, v_i\}$; this is the heart of our algorithm. Finally, in Step 5 we explain how to decide whether the cocycle $\alpha_j^\bullet(x_1^{i_1} \cdots x_n^{i_n} \overline{\tilde{m}_t})$ represents the zero element in the cohomology module.

Step 1. Pick a linear ordering of all the $(n+1)$-tuples $(i_1, \ldots, i_n, t)$ in such a way that every tuple determines the next tuple in the ordering (i.e. no additional information is required to determine the next tuple). For example, one can order all these tuples lexicographically. Our algorithm consists in deciding, for every tuple $(i_1, \ldots, i_n, t)$, whether or not $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) = 0$. If $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) \neq 0$ for some tuple, the algorithm stops and returns the answer that β_j does not vanish. If $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) = 0$, the algorithm moves to the next tuple in the ordering and all the information about the calculations for the preceding tuple is erased from memory (it is not used in the subsequent calculations). There are only finitely many tuples to consider, so the algorithm eventually stops. If a tuple $(i_1, \ldots, i_n, t)$ with $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) \neq 0$ is never encountered, the algorithm reports that $\beta_j = 0$. Thus the algorithm computes whether or not $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) = 0$ one tuple $(i_1, \ldots, i_n, t)$ at a time and the memory it consumes (modulo some finite amount that does not depend on the prime integer p and is required to store the generators $m_1, \ldots, m_v$ of M and the current tuple $(i_1, \ldots, i_n, t)$) is the memory required to decide whether or not $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) = 0$ for just one individual tuple $(i_1, \ldots, i_n, t)$. This concludes Step 1.

Step 2. The above considerations reduce deciding whether the map β_j vanishes to deciding for a fixed tuple $(i_1, \ldots, i_n, t)$ whether $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) = 0$. Let $\tilde{m}_t \in K^i(R; f_1, \ldots, f_s)$ be a cocycle that represents m_t in the i-th cohomology module of $K^\bullet(R; f_1, \ldots, f_s)$, i.e., in M. Let $\overline{\tilde{m}_t} \in K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ be the image of $\tilde{m}_t$ via the natural map $K^i(R; f_1, \ldots, f_s) \to K^i(R; f_1, \ldots, f_s)/pK^i(R; f_1, \ldots, f_s) \cong K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$. Clearly, $\overline{\tilde{m}_t} \in K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ is a cocycle that represents $\bar{m}_t$ in the i-th cohomology module of $K^\bullet(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$, i.e., in $\bar{M}$. As has been explained above, $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) \in \bar{M}$ is the element of $\bar{M}$, the i-th cohomology module of $K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$, represented by the cocycle $\alpha_j^\bullet(x_1^{i_1} \cdots x_n^{i_n} \overline{\tilde{m}_t}) \in K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$. Thus the problem of deciding whether $\alpha_j(x_1^{i_1} \cdots x_n^{i_n} \bar{m}_t) = 0$ reduces to first computing the cocycle $\alpha_j^\bullet(x_1^{i_1} \cdots x_n^{i_n} \overline{\tilde{m}_t}) \in K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ and then deciding whether this cocycle represents the zero element in the cohomology module, i.e., whether this cocycle is a coboundary. This concludes Step 2.

Step 3. The module $K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ is a direct sum of copies of the module $\bar{R}$ indexed by ordered tuples $\{v_1, \ldots, v_i\}$. The map $\alpha_j^\bullet$ is diagonal with respect to this direct sum decomposition, i.e., the image of $F_*^j(R_{v_1,\ldots,v_i}) \subseteq F_*^j(K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s))$ via this map is in $\bar{R}_{v_1,\ldots,v_i} \subseteq K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$. In other words, the i-th component of the chain map $\alpha_j^\bullet$ is the direct sum of maps $\alpha_{j,v_1,\ldots,v_i} : F_*^j(\bar{R}_{v_1,\ldots,v_i}) \to \bar{R}_{v_1,\ldots,v_i}$, one map for each tuple $\{v_1, \ldots, v_i\}$. Let $\widetilde{\overline{m}}_{t,v_1,\ldots,v_i} \in F_*^j(\bar{R}_{v_1,\ldots,v_i})$ be the component of $\overline{m_t}$ in $F_*^j(\bar{R}_{v_1,\ldots,v_i})$. The $\bar{R}_{v_1,\ldots,v_i}$-component of the element $\alpha_j^\bullet(x_1^{i_1} \cdots x_n^{i_n}\overline{m_t})$ of $K^i(\bar{R}; \bar{f}_1, \ldots, \bar{f}_s)$ is $\alpha_{j,v_1,\ldots,v_i}(x_1^{i_1} \cdots x_n^{i_n}\widetilde{\overline{m}}_{t,v_1,\ldots,v_i})$. Thus in order to compute $\alpha_j^\bullet(x_1^{i_1} \cdots x_n^{i_n}\overline{m_t})$, it is enough to compute $\alpha_{j,v_1,\ldots,v_i}^\bullet(x_1^{i_1} \cdots x_n^{i_n}\widetilde{\overline{m}}_{t,v_1,\ldots,v_i})$ for every tuple $\{v_1, \ldots, v_i\}$. The number of tuples $\{v_1, \ldots, v_i\}$ is finite and does not depend on p. In Step 4 we are going to describe, for a fixed tuple $\{v_1, \ldots, v_i\}$, an algorithm to compute $\alpha_{j,v_1,\ldots,v_i}^\bullet(x_1^{i_1} \cdots x_n^{i_n}\widetilde{\overline{m}}_{t,v_1,\ldots,v_i})$. This concludes Step 3.

Step 4. The map $\alpha_{j,v_1,\ldots,v_i}^\bullet : F_*^j(\bar{R}_{v_1,\ldots,v_i}) \to \bar{R}_{v_1,\ldots,v_i}$ is the map associated via Theorem 3.1 to the map $\beta_{j,v_1,\ldots,v_i}^\bullet : \bar{R} \cong \bar{R}_{v_1,\ldots,v_i} \to F^{*^j}(\bar{R}_{v_1,\ldots,v_i}) \cong \bar{R}$ which is nothing but the multiplication by $(f_{v_1} \cdots f_{v_i})^{p^j-1}$, as has been explained near the beginning of this section. Now for an element $y \in \bar{R}_{v_1,\ldots,v_i}$ write $\beta_{j,v_1,\ldots,v_i}^\bullet(y) = y(f_{v_1} \cdots f_{v_i})^{p^j-1}$ as $\bigoplus_{\bar{i}} e_{\bar{i}} g_{\bar{i}}^{p^j}$ where $g_{\bar{i}} \in \bar{R}_{v_1,\ldots,v_i}$ and $e_{\bar{i}} = x_1^{i_1} \cdots x_n^{i_n}$ with $0 \leqslant i_j < p^j$ for every j (every polynomial in $\bar{R}$ may be uniquely written in this way). By definition, $\alpha_{j,v_1,\ldots,v_i}^\bullet(y) = g_{\overline{p^j-1}}$. Setting $y = x_1^{i_1} \cdots x_n^{i_n}\widetilde{\overline{m}}_{t,v_1,\ldots,v_i}$ in this description, one gets $\alpha_{j,v_1,\ldots,v_i}^\bullet(x_1^{i_1} \cdots x_n^{i_n}\widetilde{\overline{m}}_{t,v_1,\ldots,v_i})$.

Both $(f_{v_1} \cdots f_{v_i})$ and $\widetilde{\overline{m}}_{t,v_1,\ldots,v_i}$ are polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Let $\mathfrak{m}_1, \ldots \mathfrak{m}_t$ and $\mu_1, \ldots, \mu_u$ be the monomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$ that appear in $(f_{v_1} \cdots f_{v_i})$ and in $\widetilde{\overline{m}}_{t,v_1,\ldots,v_i}$ respectively, that is $f_{v_1} \cdots f_{v_i} = \mathfrak{m}_1 + \cdots + \mathfrak{m}_t$ and $\widetilde{\overline{m}}_{t,v_1,\ldots,v_i} = \mu_1 + \cdots + \mu_u$. Every monomial $x_1^{i_1} \cdots x_n^{i_n}\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau$ may be written as a monomial in the variables, i.e., $\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau = cx_1^{\ell_1} \cdots x_n^{\ell_n}$ where $c \in \mathbb{Z}/p\mathbb{Z}$. Define the monomial $\gamma(\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau) = \gamma(cx_1^{\ell_1} \cdots x_n^{\ell_n})$ as follows: $\gamma(\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau) = 0$ if ℓ_s is not congruent to $p^j - 1$ modulo p^j for some s and $\gamma(\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau) = cx_1^{w_1} \cdots x_n^{w_n}$ where each $w_s = \frac{\ell_t - (p^j-1)}{p^j}$ otherwise. With this notation $\alpha_{j,v_1,\ldots,v_i}^\bullet(x_1^{i_1} \cdots x_n^{i_n}\widetilde{\overline{m}}_{t,v_1,\ldots,v_i})$ equals the summation of $\gamma(x_1^{i_1} \cdots x_n^{i_n}\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau)$ over all the monomials $\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau$ of total degree $q_1 + \cdots + q_t = p^j - 1$.

Our algorithm consists in going through all the monomials $\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau$ of total degree $q_1 + \cdots + q_t = p^j - 1$, computing $\gamma(m_1^{q_1} \cdots m_t^{q_t}\mu_j)$ for each of them and taking their sum. More precisely, pick a well-ordering of all the monomials $\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau$ of total degree $q_1 + \cdots + q_t = p^j - 1$ in such a way that every monomial determines the next monomial in the well-ordering (i.e. no additional information is required to determine the next monomial). For example one can order all these monomials lexicographically. Dedicate a section of the memory to record partial sums of the $\gamma(m_1^{q_1} \cdots m_t^{q_t}\mu_\tau)$s. Once another $\gamma(m_1^{q_1} \cdots m_t^{q_t}\mu_\tau)$ is computed, it is added to the old partial sum and stored in its place, while the old partial sum is erased. We perform this step for each monomial $\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau$ in the well-ordering. Once one step is completed, we move on to the next step by passing to the next monomial in the well-ordering. The computation is completed when all the monomials $\mathfrak{m}_1^{q_1} \cdots \mathfrak{m}_t^{q_t}\mu_\tau$ in the well-ordering are exhausted. This completes the description of the computation of $\alpha_{j,v_1,\ldots,v_i}^\bullet(x_1^{i_1} \cdots x_n^{i_n}\widetilde{\overline{m}}_{t,v_1,\ldots,v_i})$. This concludes Step 4.

Step 5. The next and final step in the algorithm is deciding whether the cocycle $\alpha_j^\bullet(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_t)$ represents the zero element in cohomology, i.e., whether this cocycle is a coboundary. Since

$$\alpha_j^\bullet(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_t)=\bigoplus_{v_1,\dots,v_i}\alpha_{j,v_1,\dots,v_i}^\bullet(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t,v_1,\dots,v_i})$$

and we have shown how to compute $\alpha_{j,v_1,\dots,v_i}^\bullet(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t,v_1,\dots,v_i})$ for all ordered tuples $\{v_1,\dots,v_i\}$, standard techniques can be used to accomplish this task. This completes Step 5.

Finally, the map α_j is the zero map if and only if the map β_j is the zero map by Corollary 3.3. This completes the description of the algorithm for deciding whether the map $\beta_j:\bar{M}\to F^{*^j}(\bar{M})$, for a fixed j, is the zero map.

The next proposition addresses he amount of memory required to perform this algorithm.

Proposition 3.5. *The amount of memory required to perform the just described algorithm grows linearly with respect to p.*

Proof. The computation of the cocycle

$$\alpha_j^\bullet(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_t)=\bigoplus_{v_1,\dots,v_i}\alpha_{j,v_1,\dots,v_i}^\bullet(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t,v_1,\dots,v_i})$$

and deciding whether this cocycle is a coboundary for a fixed element $x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_t$ are independent of such computations for all other elements $x_1^{i'_1}\cdots x_n^{i'_n}\overline{\tilde{m}}_{t'}$ and the only information from one such computation that could be needed for the continuation of the algorithm is the string $(i_1,\dots,i_n,t)$.

The computation of the element $\alpha_{j,v_1,\dots,v_i}^\bullet(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t,v_1,\dots,v_i})$ consists of a sequence of steps, one step for each monomial $\mathfrak{m}_1^{q_1}\cdots\mathfrak{m}_t^{q_t}\mu_\tau$ of total degree $q_1+\cdots+q_t=p^j-1$, as explained above. The arithmetic operations one has to perform are the same in every step and the information that has to be kept in memory after performing one step is the string $(q_1,\dots,q_t,\tau)$ and the partial sum of the $\gamma(x_1^{i_1}\cdots x_n^{i_n}\mathfrak{m}_1^{q_1}\cdots\mathfrak{m}_t^{q_t}\mu_\tau)$s. Each $\gamma(x_1^{i_1}\cdots x_n^{i_n}\mathfrak{m}_1^{q_1}\cdots\mathfrak{m}_t^{q_t}\mu_\tau)$, if non-zero, is a polynomial in $x_1,\dots,x_n$ of degree

$$\frac{\sum_s i_s+\sum_s q_s\deg\mathfrak{m}_s+\deg\mu_\tau-(p^j-1)n}{p^j}$$

Setting $D=\max\deg\mu_\tau$ and $d=\deg(f_{v_1}\cdots f_{v_i})$ and taking into account that $\sum_s i_s\le(p^j-1)n$ and $\sum_s q_s\deg\mathfrak{m}_s\le d(p^j-1)$, the above fraction is bounded above by

$$\frac{d(p^j-1)+D}{p^j}=d+\frac{D-d}{p^j}\le\max\{D,d\},$$

which is a constant independent of p and of the string $(i_1,\dots,i_n,q_1,\dots,q_t,\tau)$. Thus each $\gamma(x_1^{i_1}\cdots x_n^{i_n}\mathfrak{m}_1^{q_1}\cdots\mathfrak{m}_t^{q_t}\mu_\tau)$ and hence each partial sum of these is a polynomial whose degree is bounded above by a constant independent of p. Thus the amount of memory required to compute $\gamma(x_1^{i_1}\cdots x_n^{i_n}\mathfrak{m}_1^{q_1}\cdots\mathfrak{m}_t^{q_t}\mu_\tau)$ and memorize the resulting partial sum grows only inasmuch as one needs to store bigger and bigger coefficients of the polynomial which is the partial sum (the number of coefficients doesn't grow because the degree doesn't grow). These coefficients are elements of $\mathbb{Z}/p\mathbb{Z}$ and the amount of memory required to store those coefficients grows linearly with respect to p. Hence the amount of memory required to compute the element $\alpha^{\bullet}_{j,v_1,\ldots,v_i}(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t,v_1,\ldots,v_i})$ grows linearly with respect to p.

The cocycle

$$\alpha^{\bullet}_{j}(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t}) = \bigoplus_{v_1,\ldots,v_i} \alpha^{\bullet}_{j,v_1,\ldots,v_i}(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t,v_1,\ldots,v_i})$$

is an element of $K^i(\bar{R};\bar{f}_1,\ldots,\bar{f}_s)$ whose component in $\bar{R}_{v_1,\ldots,v_i}$ is a polynomial of degree bounded above by a constant independent of p and of the string $(i_1,\ldots,i_n)$. The modules $K^i(\bar{R};\bar{f}_1,\ldots,\bar{f}_s)$ are free $\bar{R}$-modules of finite rank and the entries of the matrices defining the differentials in $K^{\bullet}(\bar{R};\bar{f}_1,\ldots,\bar{f}_s)$ are polynomials of $\bar{R}$ whose degrees do not increase with p. Thus the number of arithmetic operations one has to perform in order to decide whether the cocycle $\alpha^{\bullet}_{j}(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t})$ is a coboundary does not increase with p. Hence the amount of memory required to decide whether the cocycle $\alpha^{\bullet}_{j}(x_1^{i_1}\cdots x_n^{i_n}\overline{\tilde{m}}_{t})$ is a coboundary grows only inasmuch as one needs to store bigger and bigger elements of the field $\mathbb{Z}/p\mathbb{Z}$ that appear in those arithmetic operations. The amount of memory required to store elements of $\mathbb{Z}/p\mathbb{Z}$ grows linearly with respect to p. This, finally, shows that the amount of memory required to decide whether the map $\beta_j : \bar{M} \to F^{*^j}(\bar{M})$ vanishes grows linearly with respect to p. $\square$

Needless to say, the above algorithm is far from being practical. Even though the required memory grows only linearly, the number of arithmetic operations one has to perform grows very rapidly. This is because the same arithmetic operations have to be performed for every monomial $x_1^{i_1}\cdots x_n^{i_n}$ with $i_t \leq p^j - 1$ and every monomial $\mathfrak{m}_1^{q_1}\cdots\mathfrak{m}_t^{q_t}$ with $\sum_t q_t = p^j - 1$. The number of these monomials grows very rapidly with p making the time required to complete the computation astronomical.

In conclusion we briefly summarize our modification of the algorithm from [7, Remark 2.4] for deciding the vanishing of the local cohomology module $H^i_{\bar{I}}(\bar{R})$ where $\bar{I} = (\bar{f}_1,\ldots,\bar{f}_s)$. First one computes the integer $u = u(M)$ (as defined in Corollary 2.6) where M is the i-th cohomology module of the Koszul complex $K^{\bullet}(R;f_1,\ldots,f_s)$. According to Corollary 2.6 the local cohomology module $H^i_{\bar{I}}(\bar{R})$ (which is the F-finite module generated by the map $\beta : \bar{M} \to F^*(\bar{M})$) vanishes if and only if the map $\beta_u : \bar{M} \to F^{*^u}(\bar{M})$ is the zero map. Thus all one has to do is apply our algorithm for deciding whether the map $\beta_j : \bar{M} \to F^{*^j}(\bar{M})$ vanishes for $j = u$.

Acknowledgment. *Part of this work is from the author's dissertation. The author gratefully thanks his advisor Professor Gennady Lyubeznik for his continued support and guidance.*

References

[1] M. F. Atiyah, I. G. Macdonald, Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[2] Bourbaki, Nicolas Algebra I. Chapters 13. Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. xxiv+709 pp.

[3] D. R. Grayson, M. E. Stillman, Macaulay2, a software system for research in algebraic geometry.
Available at *http://www.math.uiuc.edu/Macaulay2/.*
A. Leykin, H. Tsai, D-modules for Macaulay 2.
http://people.math.gatech.edu/∼aleykin3/Dmodules/index.html.

[4] A. Grothendieck, Local cohomology. Lecture Notes in Mathematics, No. 41 Springer-Verlag, Berlin-New York 1967.
[5] M. Hochster, J. L. Roberts, Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. Advances in Math. 13 (1974), 115175.
[6] C. L. Huneke, R. Y. Sharp, Bass numbers of local cohomology modules. Trans. Amer. Math. Soc. 339 (1993), no. 2, 765-779.
[7] G. Lyubeznik, F-modules: applications to local cohomology and D-modules in characteristic $p > 0$. J. Reine Angew. Math. 491 (1997), 65–130.
[8] G. Lyubeznik, On the vanishing of local cohomology in characteristic $p > 0$. *Compos. Math.* 142 (2006), no. 1, 207-221.
[9] G. Lyubeznik, W. Zhang, Y. Zhang, A property of the Frobenius map of a polynomial ring. Commutative algebra and its connections to geometry, 137-143, Contemporary Mathematics, 555, American Mathematical Society, Providence, RI, 2011.
[10] H. Matsumura, Commutative ring theory. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.
[11] E. W. Mayr, A. R. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals. Adv. in Math. 46 (1982), no. 3, 305-329.
[12] U. Walther, Algorithmic computation of local cohomology modules and the local cohomological dimension of algebraic varieties. J. Pure Appl. Algebra 139 (1999), no. 1-3, 303-321.

Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043
E-mail address: yizhang263@gmail.com