Special Conditions on Maximal Cohen-Macaulay Modules, and Applications to the Theory of Multiplicities

by

Douglas Hanes

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
1999

Doctoral Committee:

Professor Melvin Hochster, Chair
Professor Andreas Blass
Associate Professor Karen E. Smith
Professor J.Tobias Stafford
Assistant Professor Jamie Tappenden

ACKNOWLEDGEMENTS

I wish above all to thank Professor Melvin Hochster, who has inspired much of the work presented in this thesis. Through numerous classes and more than three years of almost weekly meetings, he has had an inestimable influence upon my study and research. I also wish to recognize the influence of Professor Craig Huneke, who introduced me to the study of commutative algebra, and who has consistently encouraged me in my academic endeavors over the last eight years.

Thanks also to my committee members for their help in preparing this dissertation, as well as for the knowledge I have gained from their courses while at the University of Michigan.

TABLE OF CONTENTS

CHAPTER I

Introduction

The general theme of this dissertation will be to prove certain statements about local or positively graded Noetherian rings by passing to a suitably chosen module over the ring, which may in some way have nicer properties than the ring itself. The problem may then in general be broken into two parts. The first, which is to determine what sorts of modules can be shown to exist over a certain class of rings, will be the subject of chapters 2 and 3. The results presented there are of interest in their own right, and provide some partial answers to questions in the literature. But the existence of such modules also has implications for questions regarding the structure of the ring and its algebra extensions. The second part of our endeavour, which is to explore these implications, is taken up in the latter part of the dissertation.

A commutative ring R is *Noetherian* if every ideal I of R is finitely generated, which is to say that every element of I can be written as an R-linear combination of finitely many elements $f_1, \dots, f_n$ in I. This property holds for the integers $\mathbb{Z}$ and for any field K. Moreover, if R is Noetherian, then so are polynomial rings $R[X_1, \dots, X_m]$ over R and homomorphic images R/I, where I is an ideal of R. This already provides a wealth of examples, including the coordinate rings of affine varieties or the homogeneous coordinate rings of projective varieties over a field K, which take the form

$$R = \frac{K[X_1, \dots, X_m]}{(f_1, \dots, f_n)},$$

where $f_1, \dots, f_n$ are elements of the polynomial ring $K[X_1, \dots, X_m]$.

If R is the homogeneous coordinate ring of a projective variety, then the polynomials f_i may be assumed to be homogeneous, which is to say that each f_i is a K-linear combination of monomials of the same degree. Such rings serve as the prototype for the more general notion of an $\mathbb{N}$-graded ring, a ring R with a decomposition

$$R = \oplus_{i \in \mathbb{N}} R_i$$

into additive groups, and with the property that if $x \in R_s$ and $y \in R_t$, then $xy \in R_{s+t}$. It follows from these conditions that R_0 must itself be a ring, that $R^+ = \oplus_{i>0} R_i$ is an ideal of R, and that any maximal ideal of R generated by homogeneous elements must contain R^+. In fact, we will always assume that R_0 is a local ring (see below), so that R has a unique homogeneous maximal ideal.

We will also wish to consider local rings, and even complete local rings. A local ring, which possesses a unique maximal ideal, may be obtained from any Noetherian commutative ring by inverting all elements outside of some prime ideal. If R is the coordinate ring of an affine variety, then the local ring R_m obtained by localizing at a maximal ideal m is just the ring of rational functions defined at the point corresponding to m. The completion of R_m with respect to its maximal ideal is then the R_m-algebra containing all formal power series in the generators of m. Localizations and completions of Noetherian rings retain the Noetherian property. In fact, if R is any complete local ring which contains a field, then one may express R as a homomorphic image of a power series ring:

$$R = \frac{K[[X_1, \dots, X_m]]}{(f_1, \dots, f_n)},$$

where K is a field and one of course needs to kill only finitely many power series f_i.

An open question which has inspired much of the research contained in this dissertation is the following conjecture, which first appeared in [12].

Conjecture 1.0.1 (Lech). *Let $(R, m) \subseteq (S, n)$ be a flat local extension of Noetherian local rings. Then the multiplicity of S is greater than or equal to the multiplicity of R.*

The multiplicity e_R of R is defined as follows: let (R, m) be a local ring of Krull dimension d. Associated to R is the Hilbert function $H_R : \mathbb{N} \to \mathbb{N}$ given by $H(t) = \dim_K(m^t/m^{t+1})$, where $K = R/m$ is the residue class field of R. For all sufficiently large t, $H_R(t)$ is given by a polynomial in t of dimension $d-1$ (provided $d \geq 1$), and the multiplicity e_R of R is defined to be $(d-1)!$ times the leading coefficient of this polynomial (when $d = 0$, $H(t)$ is eventually 0, and we define e_R to be the length of the ring R). So the multiplicity gives, in a certain sense, an asymptotic measure of the rate of growth of the ring R.

The simplest example of the multiplicity is given by the so-called "fat" points of the affine line: if one considers the algebraic subset of the complex line (which has ring of functions $\mathbb{C}[X]$) defined by the equation $X^n = 0$, the subset so defined is the point $\{0\}$ for every $n > 0$. But one wishes to keep track of the fact that the defining function vanishes to degee n at this point, and that the coordinate ring $R = \mathbb{C}[X]/(X^n)$ varies with n. In this simple case, n is precisely the multiplicity of the ring.

If the extension ring S in Lech's conjecture is actually a finitely-generated R-module, then requiring the extension to be flat is equivalent to saying that S is a free R-module. When we say that the extension is local, we mean that the maximal ideal m of R embeds into the maximal ideal n of S. So in the case of a module-finite extension, Lech's conjecture is equivalent to the following statement: let S be a finitely generated free R-module, and suppose that S is given a local ring structure compatible with that of the submodule R (think of the ring R as being the first free summand of S). Then the rate of growth of the ring S, with respect to its maximal ideal n, is at least as great as the rate of growth of R. Stated in this way, the conjecture seems very natural and plausible.

Lech's conjecture has now stood for almost forty years, and remains open in almost all cases, with the best partial results still those proved in Lech's original two papers [12] and [13]. There he proved the conjecture in the case that the rings have dimension 2, in the case that the fibre S/mS is a complete intersection, and also in the case that the embedding dimension of S does not exceed that of R by more than one.

The conjecture remains open in dimensions 3 and higher, even in the case that R and S are graded, and S is a module-finite (free) extension of R. However, the method of passing to modules with special properties has shown promise in attacking this problem. In particular, it is highly advantageous to consider R-modules which are *maximal Cohen-Macaulay* (abbreviated MCM).

If R is a complete local ring containing a field or a finitely generated graded algebra over a field K, then R can be realized as a module-finite extension of a power series ring $A = K[[x_1, \dots, x_d]]$ (in the complete local case) or of a polynomial ring $A = K[x_1, \dots, x_d]$ (in the graded case). Any finitely generated (graded) R-module M is then also an A-module by restriction of scalars, and in this case M is MCM if and only if it is a free A-module (a general definition is given in section 1.5). In particular, the ring R is Cohen-Macaulay if and only if it is a flat extension of the subring A. Hochster proved the existence of *big* (i.e. not finitely generated)

MCM modules for local rings containing a field, and used the existence of such modules in order to prove many important homological conjectures (see [8, 7]). But his conjecture that a complete local ring must possess a finitely generated (or small) MCM module remains open for rings of dimension greater than 2 (see Theorem 1.5.3 and section 6.2 for some partial results).

We may extend the notion of the multiplicity to any finitely generated module M over a local or graded ring R (for example, this may be done with the same sort of Hilbert function as for the ring). Then, if M is MCM, and if the subring $A = K[[x_1, \dots, x_d]]$ (or $K[x_1, \dots, x_d]$) is chosen appropriately, the multiplicity of M is simply the vector-space dimension of the module

$$\frac{M}{(x_1, \dots, x_d)M},$$

which is also equal to the free rank of M as an A-module.

This makes the multiplicity of a MCM module relatively easy to compute, or at least approximate. And, as we will see, the multiplicity of the ring can often be recovered from that of the module. But we will need to simplify the process of computing multiplicities even further. For this, let m be the maximal ideal of the ring R. Since the multiplicity of M is just the vector-space dimension of $M/(x_1, \dots, x_d)M$, we can make the calculation easier by assuming that m^t multiplies M into $(x_1, \dots, x_d)M$ for some small value of t. As an extreme example, we might even hope that $mM = (x_1, \dots, x_d)M$, in which case the multiplicity of M is equal its minimal number of generators as an R-module. This condition will reappear in the definition of a *linear* maximal Cohen-Macaulay module (see section 1.1).

Over a Cohen-Macaulay ring R of prime characteristic $p > 0$, we show the existence of MCM modules which satisfy strong conditions of this kind. This has allowed approximations of multiplicities which have allowed proofs of certain cases of Lech's conjecture. In what follows, we will denote the embedding dimension of the ring R by $\mathrm{edim}(R)$. If R is the local ring at the origin of an affine variety X over a field K, then the embedding dimension is, quite appropriately, equal to the minimum dimension of an affine space $\mathbb{A}^n_K$ into which a neighborhood of the origin in X can be embedded.

Theorem 1.0.2. *Let R be a positively graded algebra, generated by its 1-forms, over a perfect field K of characteristic $p > 0$; let m denote the homogeneous maximal ideal of R. Suppose that R possesses a graded MCM module M, with all generators in the same degree, and that the dimension of R does not exceed 4. Then Lech's conjecture holds for any flat local extension $(R, m) \subseteq (S, n)$. If $dim(R) = 5$, then the conjecture holds provided that once we reduce to the case $dim(S) = 5$, we have either $m \hookrightarrow n^2$ or $edim(S) \geq edim(R) + 6$.*

Note that if R is graded rather than local, we call the extension $(R, m) \subseteq (S, n)$ flat local if $m \hookrightarrow n$ and $R_m \to S_n$ is flat local.

This is already a significant improvement over the previously known results, and solves the problem for a large class of graded Cohen-Macaulay rings of low dimensions. In fact, if R is a positively graded K-algebra of dimension 3, where K is a perfect field of characteristic p, then a graded MCM module is known to exist (see Theorem 1.5.3), and so the conjecture holds even without any Cohen-Macaulayness assumption.

In the case that the base ring R is local rather than graded, the methods do not yield quite as much. Nevertheless, I have made significant progress in the case that the base ring has Krull dimension 3.

Proposition 1.0.3. *Let (R, m) be a 3-dimensional local ring of positive prime char-*

acteristic p, with perfect residue field, and assume that R has a MCM module of positive rank. If $(R, m) \subseteq (S, n)$ is a flat local extension of 3-dimensional local rings, and if either $edim(S) \geq edim(R) + 3$ or if $m \hookrightarrow n^2$, then $e_R \leq e_S$.

It is a theorem of Lech that, in the situation above, edim(S) is at least as great as edim(R) (see [13]); moreover, Lech has proved the conjecture in the case that the difference in embedding dimensions is 0 or 1.

The proofs of these statements rely upon prime characteristic p methods in order to produce interesting MCM modules which would not otherwise be readily available. Nonetheless, suppose we are presented instead with the coordinate ring

$$R = \frac{K[X_1, \ldots, X_n]}{(f_1, \ldots, f_t)}$$

of a variety defined by the polynomials $f_1, \ldots, f_t$, where K is a field of characteristic 0. If it turns out that the coefficients of the f_i are integers (which would no doubt be the case in any example which the reader might casually write down), then one may view the variety X as the set of solutions to certain polynomials over $\mathbb{Z}$ in the field K. In fact, points of X correspond precisely to homomorphisms from the ring

$$R_0 = \frac{\mathbb{Z}[X_1, \ldots, X_n]}{(f_1, \ldots, f_t)}$$

into K.

But a great deal of insight into the solutions of polynomials over $\mathbb{Z}$ may be gained by looking at the solutions in the finite fields $\mathbb{Z}/p\mathbb{Z}$, where p is any prime number. And these solutions are described by the rings

$$R = \frac{(\mathbb{Z}/p\mathbb{Z})[X_1, \ldots, X_n]}{(f_1, \ldots, f_t)},$$

which have positive prime characteristic p. This indicates that the case of rings of positive prime characteristic is more central than might at first be apparent. In fact, it is often possible to deduce statements about rings containing a field of characteristic 0 from the corresponding statements about rings of prime characteristic. This process of *reduction to characteristic* p can be quite technical, depending upon the statement in question, but the above discussion gives a good idea of the motivation behind the technique. In section 4.4, we outline a reduction to characteristic p argument for Theorem 1.0.2 and Proposition 1.0.3.

Some related issues will be considered in the course of the dissertation. Although some of the results are independent of the main line of argument, all revolve around the two major themes of special conditions on maximal Cohen-Macaulay modules and conjectures on the multiplicities of local or graded Noetherian rings.

1.1 Maximal Cohen-Macaulay modules with special properties

In chapter 2 we define and characterize certain properties of a maximal Cohen-Macaulay module M over a local or positively graded ring R. All of the conditions which are considered are generalizations of the condition of *linearity*, introduced by B. Ulrich in [20]. We may define a linear maximal Cohen-Macaulay module (abbreviated lin MCM) as follows:

Definition 1.1.1. Let (R, m) be a Noetherian local ring with a finitely generated maximal Cohen-Macaulay module M. Then M is said to be a linear maximal Cohen-Macaulay module (or lin MCM) if $e_R(M) = \nu(M)$, where $e_R(M)$ is the multiplicity of the module M, and $\nu(M)$ is the minimum number of generators of M as an R-module.

Perhaps the greatest interest in linear MCM modules has stemmed from the fact that the associated graded module $\mathrm{gr}_m(M)$ of a lin MCM M remains MCM (see e.g.

[1]). This provides important information, as the associated graded ring $\mathrm{gr}_m R$ often falls far short of Cohen-Macaulayness, even when R is Cohen-Macaulay. However, it turns out that the existence of linear MCM modules is far easier to characterize in the graded case, and most of the existence results are for graded rings. What will concern us more here is the numerical properties of such a module.

Seen from this point of view, the linearity condition expresses a best-possible characteristic of the module M. For if we assume that the residue field R/m of R is infinite, then we may choose a minimal reduction $I = (x_1, \ldots, x_d)$ of m, and the definition implies that M is linear if and only if $mM = IM$ (see section 1.5 for theory of reduction ideals). This makes the Hilbert function, as well as the multiplicity, of a linear MCM module especially easy to compute.

Given this characterization of linearity, we may quite naturally introduce the following generalization: we say that the *reduction degree* of a finitely generated MCM module M is the least integer n such that $m^n M \subseteq (x_1, \ldots, x_d)M$ for some minimal reduction $(x_1, \ldots, x_d)$ of m. M is of course linear if and only if its reduction degree is one.

The existence of modules with low reduction degree will be shown to imply some new cases of Lech's conjecture. In fact, it turns out that a sequence of modules asymptotically approaching a certain reduction degree condition usually provides just as much information as a single module actually satisfying the condition. The point is that even though a module has reduction degree t, it may be the case, for some $s < t$, that the length of $(m^s + I)M/IM$ is insignificant in comparison with $l(M/IM) = e(M)$. Then we may treat M as if its reduction degree were s. Our most general definition is:

Definition 1.1.2. A sequence of MCM R-modules $\{M_i\}_{i \geq 0}$ is said to have reduction degrees approaching t if for some minimal reduction I of m,

$$\frac{l((m^t + I)M_i/IM_i)}{l(M_i/IM_i)} \to 0$$

as $i \to \infty$.

It is not surprising that the existence of linear maximal Cohen-Macaulay modules has proved very difficult to establish, considering the strength of the linearity condition. Such modules are known to exist for one-dimensional rings, two-dimensional graded Cohen-Macaulay domains, rings of minimal multiplicity, strict complete intersections, and certain rings of determinantal varieties (see [2] and [1]). We will show in chapter 3 that Segre products of graded rings with lin MCMs possess lin MCMs; and that in dimension 3, any Veronese subring of a ring possessing a graded lin MCM still admits a lin MCM.

The difficulty involved in showing the existence of linear MCM modules for even the Veronese subrings of a polynomial ring of dimension 3 is surprising, if lin MCMs are to exist in any generality. But just as surprising is the fact that the algorithm for producing these modules, with delicate modification, produces sequences of MCMs approaching linearity over a much broader class of rings of dimension 3. In particular, we achieve the following:

Proposition 1.1.3. *Suppose that R is a 3-dimensional positively graded K-algebra, generated by its 1-forms, where K is a perfect field of characteristic $p > 0$. Suppose moreover that R is a Cohen-Macaulay domain. Then R possesses a sequence of MCM modules M_i with the property that $e(M_i)/\nu(M_i) \to 1$ as $i \to \infty$.*

In other words, such a ring R possesses a sequence of MCM modules which "approach" linearity in the numerical sense. In fact, by setting aside the more stringent condition of linearity, and considering instead the more general definitions of chapter 2, we may prove the following much richer existence result:

Theorem 1.1.4. *Suppose that R is a positively graded K-algebra of dimension $d \geq 3$, generated by its 1-forms, where K is a perfect field of characteristic $p > 0$. Suppose moreover that R is a Cohen-Macaulay domain. Then R possesses a sequence of MCM modules M_i with reduction degrees approaching $d - 2$.*

As indicated earlier, this result will be extremely useful in the approximation of multiplicities. In the local (non-graded) case, one cannot achieve quite as much with the same methods, but we can still prove a much stronger result in positive prime characteristic than is available in characteristic 0. By utilizing the Frobenius endomorphism, we are able to show (Proposition 2.3.4) that any Cohen-Macaulay local ring R of characteristic p possesses a sequence of MCM modules with reduction degrees approaching the dimension of R.

1.2 Applications to multiplicities

In chapter 4 we will show how the existence of maximal Cohen-Macaulay modules of low reduction degree can be used in order to prove certain cases of Lech's conjecture. One result which has been known for some time, and which was first shown to me by M. Hochster, is that the existence of a sequence of MCMs approaching linearity over the base ring R implies Lech's conjecture for any flat local extension $(R, m) \subseteq (S, n)$. Combining this with Proposition 1.1.3 suffices to prove the conjecture in the case that the base ring R is graded of dimension 3 over a perfect field K of characteristic $p > 0$ (Proposition 4.1.5).

In order to apply the existence of MCMs with higher reduction degrees, we will require the following generalization of another theorem of Lech, which states that the embedding dimension of a flat local extension of R, of the same dimension, is always greater than or equal to that of R (see [13]). The result presented here allows us to replace R by a finitely generated module M in the conclusion.

Proposition 1.2.1. *Let $(R,m) \subseteq (S,n)$ be a flat local extension of rings of the same dimension, M a finitely generated R-module, and set $M' = S \otimes_R M$. Then*

$$\nu_S(nM') \geq \nu_R(mM) + (\nu(n) - \nu(m)) \cdot \nu(M).$$

Here $\nu_R(N)$ represents the minimal number of generators of any R-module N; in particular, $\nu(m)$, the minimal number of generators of the maximal ideal, is the embedding dimension of the ring R. This inequality on the 'embedding dimensions' of the modules M and M' allows a corresponding inequality $e_R(M) \leq e_S(M')$ on the multiplicities, provided that M is chosen to be a MCM module with sufficiently small reduction degree. This yields our first major result on Lech's conjecture (section 4.3).

Theorem 1.2.2. *Let (R,m) be a local or $\mathbb{N}$-graded domain, and let (S,n) be a flat local extension of R of the same dimension. Suppose that R possesses a MCM module M with $red(M) = 3$, or even a sequence of MCM modules $\{M_i\}$ with reduction degrees approaching 3. If $m \hookrightarrow n^2$, or if $edim(S) - edim(R) + depth(gr_m M_i) \geq dim(R) + 1$ for each M_i, then $e_R \leq e_S$.*

Combining this with existence results of chapter 3 then allows a proof of Theorem 1.0.2.

In the remainder of section 4.3 , we attempt to prove similar results for rings of equal characteristic 0 (i.e. local or graded rings which contain a field K of characteristic 0). In particular, we note that since Theorem 1.2.2 requires no hypothesis on the characteristic, we may apply this theorem in any cases in which suitable MCM modules can be shown to exist. The most general technique of applying the Frobenius is not available, but we note certain cases in which MCMs of low reduction degree can nonetheless be shown to exist.

1.3 Hilbert-Kunz multiplicities and ordinary multiplicities

If a commutative ring R has positive prime characteristic p, then one has the equality $(x+y)^p = x^p + y^p$ for any elements x and y of R. It follows that the map $F : R \to R$ which sends each element z to z^p is actually a ring endomorphism, called the *Frobenius* endomorphism. By composition, one then obtains, for any $e > 0$, the endomorphism $F^e : R \to R$ which takes each element to its p^e power. Similarly, for any ideal $I = (x_1, \ldots, x_t) \subseteq R$ and any power $q = p^e$, the ideal $I^{[q]}$ generated by all q^{th} powers of elements of I is given by

$$I^{[q]} = (x_1^q, \ldots, x_t^q).$$

Given an m-primary ideal I, this allows us to define a new Hilbert-type function associated to R by setting

$$HK_I(t) = l(R/I^{[p^t]}).$$

Monsky has shown [16] that this function is asymptotic in $q = p^t$ to $c_I q^d$ for some positive real number c_I (see section 1.3), and we may naturally regard c_I as a new multiplicity on the ring R (called the *Hilbert-Kunz* multiplicity with respect to I). Remarkably, it is not known whether c_I must be rational.

In particular, we denote c_m by c_R, and in section 5.1 we show how a direct appeal to this invariant yields partial results for Lech's conjecture in all dimensions. For the ordinary and Hilbert-Kunz multiplicities are strongly related: in general, one has the inequalities $e_R \geq c_R \geq e_R/d!$, where d is the Krull dimension of the ring R.

Since we can use the Frobenius endomorphism in order to produce modules whose minimal number of generators of is asymptotic to $c_R q^d$, our methods allow us to make estimates of e_S in terms of c_R, where $(R, m) \subseteq (S, n)$ is a flat local extension. Although the following propositions do not give a complete proof of the conjecture in any dimension, notice that they place some significant bounds upon the class of possible counterexamples:

Proposition 1.3.1. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of Cohen-Macaulay rings of positive prime characteristic p and dimension d, with R/m perfect, and let J be a minimal reduction of n. If $l(S/(mS + J)) \geq d!$, then $e_R \leq e_S$. In particular, if* $\mathrm{edim}(S) - \mathrm{edim}(R) \geq d! + d - 1$, *then $e_R \leq e_S$.*

Proposition 1.3.2. *If $(R, m) \subseteq (S, n)$ is a flat local extension of Cohen-Macaulay rings of prime characteristic $p > 0$ and dimension d, with R/m perfect, and if m embeds into $n^{d!}$, then $e_R \leq e_S$.*

In section 5.2, we consider the Hilbert-Kunz multiplicity explicitly. We are able to show that the whole enterprise of proving inequalities on multiplicities under flat local extensions and localizations can be successfully carried out if one considers the Hilbert-Kunz multiplicity instead of the ordinary Hilbert-Samuel multiplicity. In fact, the results are not even restricted to inequalities on the Hilbert-Kunz multiplicities, but actually give strong inequalities on the corresponding Hilbert-Kunz functions. The main results are the following:

Theorem 1.3.3. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of rings of positive prime characteristic. Then $c_R \leq c_S$; moreover, for any $q = p^e$, it is in fact the case that $q^t \cdot l(R/m^{[q]}) \leq l(S/n^{[q]})$, where $t = dim(S) - dim(R)$.*

Theorem 1.3.4. *Let (R, m) be a Noetherian local ring of characteristic $p > 0$, and* *let P be a prime ideal of R such that height$(P)+$dim$(P) =$ dim(S). Then $c_{R_P} \leq c_R$. In fact, if $t =$ dim(R/P), then $l(R/m^{[q]}) \geq q^t \cdot l(R_P/P^{[q]}R_P)$ for every $q = p^e$.*

The Hilbert-Kunz multiplicity is still very poorly understood in comparison with the ordinary multiplicity; in particular, it has been computed for only a very small class of rings. But the results above may contribute towards a better understanding of the Hilbert-Kunz functions, as well as providing further motivation for their study.

1.4 Specialized MCMs via splitting results

In the final chapter, we will show how to to use splitting results and the Frobenius endomorphism in order to prove the existence of MCM modules with other special properties over certain graded rings of positive prime characteristic p. We recall the notion of the a-invariant for graded rings and modules, which was first introduced by Goto and Watanabe in [6]. This notion is closely related to that of the reduction degree, but gives somewhat better information in the case that the homogeneous maximal ideal is not generated by one-forms. Again, our object will be to produce MCM modules whose a-invariant is sufficiently bounded. What we prove is the following:

Theorem 1.4.1. *Let R be a finitely generated positively graded equidimensional K-algebra, with K a perfect field of characteristic $p > 0$. Suppose R has a graded module M, of the same dimension, which is Cohen-Macaulay except possibly at the origin. Then R has a MCM module M with a-invariant $a(M) < 0$.*

This result is applied in section 6.2, where we solve the problem of existence of small Cohen-Macaulay modules for certain Segre products of $\mathbb{N}$-graded algebras over a field. Our most general result is the following:

Theorem 1.4.2. *Let $R = R_1 \otimes_{seg} R_2 \cdots \otimes_{seg} R_n$ be a Segre product of positively graded rings R_i over a field K, and assume that each of the rings R_i has dimension at least 2. If, for each i, R_i has a graded MCM-module M_i with $a(M_i) < 0$, then R possesses a (small) graded MCM module.*

The MCM module over the Segre product ring is just the Segre product of the modules M_i. A similar result on the Cohen-Macaulayness of Segre product rings was proved by Goto and Watanabe in [6], and the above theorem follows quite directly from their work.

Combining the theorem with the results of section 5.1 then implies the following corollary, which gives a partial result to the conjecture on existence of finitely generated MCM modules.

Corollary 1.4.3. *Let $R_1, \ldots, R_n$ be finitely generated $\mathbb{N}$-graded algebras over a perfect field K of characteristic $p > 0$, with $(R_i)_0 = K$ for each i. If each ring R_i has a finitely generated graded maximal Cohen-Macaulay module, then the Segre product $R_1 \otimes_{seg} R_2 \otimes_{seg} \ldots \otimes_{seg} R_n$ also has a finitely generated graded maximal Cohen-Macaulay module.*

In the final part of chapter 6 we attempt some similar results without the assumptions that the ring in question be graded or have positive prime characteristic. In particular, in the characteristic 0 graded case we exploit Theorem 1.4.2, which contains no reference to the characteristic of the field.

1.5 Background for the dissertation

For the general theory of local rings, the reader is referred to the text [15] of H. Matsumura. Material more specific to this thesis is presented in the book [3] of W.

Bruns and J. Herzog. Nevertheless, I will attempt here to summarize those facts which are to be used repeatedly throughout the dissertation.

If (R, m) is a local or positively graded ring of Krull dimension d, then one can always choose a *system of parameters*, a sequence of d elements $x_1, \dots, x_d$ in R with the property that the unique maximal (or homogeneous maximal) ideal m is a minimal prime of the ideal $I = (x_1, \dots, x_d)$. This is equivalent to saying that the homomorphic image R/I is an Artinian ring. Moreover, if the ring is graded, these elements may be chosen to be homogeneous. One defines a *regular sequence* on an R-module M to be a sequence of elements $z_1, \dots, z_s$ in R with the property that the image of z_{i+1} in $R/(z_1, \dots, z_i)$ is a nonzerodivisor on $M/(z_1, \dots, z_i)M$ for $0 \leq i \leq s-1$ (in other words, if $z_{i+1}u \in (z_1, \dots, z_i)M$ for some $u \in M$, we require that $u \in (z_1, \dots, z_i)M$). This gives an invariant of the module M as follows:

Definition 1.5.1. The *depth* of the module M is the maximum integer s such that R contains a regular sequence on M of length s. M is called a Cohen-Macaulay module if $\text{depth}(M) = \dim(M)$, and is called a maximal Cohen-Macaulay module (abbreviated MCM) if $\text{depth}(M) = \dim(R)$.

It is easy to show that the depth of a module M must always be less than or equal to its dimension, and that a regular sequence on a module M must form part of a system of parameters for the ring R. In fact, one can show that M is maximal Cohen-Macaulay if and only if every system of parameters of R is a regular sequence on M.

We will need to keep track of various invariants of a finitely generated (graded) module M over the local (or graded) ring (R, m). The *minimal number of generators* $\nu(M)$ is equal to $\dim_K(M/mM)$, and is the least n for which there exists a surjection $R^{(n)} \to M \to 0$. If R is an integral domain with fraction field L, then we define the *torsion-free rank* (or just the rank) of M to be the L-dimension of $L \otimes_R M$. The rank of M is also equal to the largest s for which there exists an injection $R^{(s)} \hookrightarrow M$. If R is not a domain, then we will say that M has well-defined rank s if $M_P \cong R_P^{(s)}$ for every associated prime ideal P of R. This condition is equivalent to the existence of a short exact sequence

$$O \to R^{(s)} \to M \to C \to 0,$$

where $zC = 0$ for some element z which is a nonzerodivisor in R.

An extension $I \subseteq J$ of ideals of R is *integral* if there exists some positive integer k such that $J^{n+k} = I^n \cdot J^k$ for all $n \geq 0$. In this case, we also say that I is a *reduction* of J. If $K = R/m$ is infinite and J is an ideal primary to the maximal ideal m of R, it is a theorem of Northcott and Rees (see [17]) that J has a *minimal* reduction J' (i.e. J' is minimal with respect to inclusion among the reductions of J), and that J' must be generated by a system of parameters.

The *Hilbert function* $H_M : \mathbb{Z} \to \mathbb{N}$ of a finitely generated graded module M over a Noetherian positively graded ring (R, m) with R_0 Artinian is defined by $H_M(t) = l_R(M_t)$, the length of a composition series for M_t. It is an important fact that if R is generated over R_0 by forms of degree one, then for all t sufficiently large, one has $H_M(t) = P_M(t)$, where $P_M(t)$ is a polynomial in t of degree $d - 1 = \dim(M) - 1$. We define the *multiplicity* of M to be $(d-1)!$ times the leading coefficient of $P_M(t)$. If (R, m) is local (or graded) with m-primary ideal I (i.e. $m^t \subseteq I$ for some $t \geq 0$), and M is a finitely generated R-module, then we define the multiplicity $e(I; M)$ of M with respect to I to be the multiplicity of the associated graded module $\mathrm{gr}_I M$.

There are two facts about multiplicities which we will use repeatedly throughout the thesis. First, if $I \subseteq J$ is an integral extension of m-primary ideals, then $e(I; M) = e(J; M)$ for any finitely generated R-module M (see [17]). Secondly, if

M is a maximal Cohen-Macaulay module, and if I is generated by a system of parameters, it follows from the results of Serre (see [19]) that $e(I;M) = l(M/IM)$. Putting these statements together, we see that if M is a MCM module over a local ring (R,m), and I is a minimal reduction of m, then $e_R(M) = e(m;M) = l(M/IM)$.

Finally, we need to develop some notation for modules over local rings (R,m) of positive prime characteristic p. If M is any module over the ring R, and $e > 0$, then we obtain a new module ${}^eM$ over R via restriction of scalars for F^e. In other words, ${}^eM = M$ as a group, but has a new R-module structure given by $r \circ m = r^q m$, where $r \in R$, $m \in M$, and $q = p^e$. In order to know that the modules ${}^eM$ associated to a finitely generated module M remain finitely generated, it is necessary to assume that R is *F-finite*; i.e. that $F : R \to R$ gives R as a module-finite ring extension of itself. If R is a complete local ring with residue field K, or if R is a finitely generated algebra over the field K, then R will be F-finite so long as K is assumed to be perfect (this ensures that $F : K \to K$ is an isomorphism). In particular, since we assume that all rings are Noetherian, an $\mathbb{N}$-graded ring R with $R_0 = K$ a perfect field will be finitely generated over K, hence F-finite. In this case, one can show that for any $e \geq 0$ and $q = p^e$, one has $e_R({}^eM) = q^d e_R(M)$; if M has well-defined rank, one also obtains $\operatorname{rank}_R({}^eM) = q^d \cdot \operatorname{rank}_R(M)$. Notice that if I is any ideal of R, then $I({}^eM) = I^{[q]}M$, where $I^{[q]}$ is the ideal of R generated by all q^{th} powers of elements of I.

We will also be interested in knowing the minimal numbers of generators of the modules ${}^eM$. Although this cannot usually be calculated precisely, much information is provided by the following theorem of [16]:

Theorem 1.5.2 (Monsky). *Let (R,m) be a local ring of positive prime characteristic p, let M be a finitely generated R-module of dimension d, and let I be any*

m-primary ideal. Then the function $HK_{I,M} : \mathbb{N} \to \mathbb{N}$ defined by $HK_{I,M}(e) = l(M/I^{[p^e]}M)$ is asymptotic in $q = p^e$ to $c_{I,M}q^d$ for large e, where $c_{I,M}$ is some positive real number.

The real number $c_{I,M}$ is called the *Hilbert-Kunz multiplicity* of M with respect to I, and the function $HK_{I,M}$ is called the Hilbert-Kunz function of M with respect to I. Since we will usually be interested in the case that $I = m$, we denote $c_{m,M}$ by c_M and simply refer to this as the Hilbert-Kunz multiplicity of M. Notice that, since

$$\nu({}^eM) = l({}^eM/m \cdot {}^eM) = l(M/m^{[q]}M)$$

in the case that R is F-finite and R/m is perfect, this gives us at least an asymptotic approximation of the numbers of generators of the modules ${}^eM$. We remark that if M has well-defined positive rank over R, then $c_M = \mathrm{rank}_R(M) \cdot c_R$.

We define the *local cohomology* of a finitely generated module as follows: for any $n \geq 0$, the natural surjection $R/m^{n+1} \to R/m^n$ induces maps

$$\mathrm{Ext}^i_R(R/m^n, M) \to \mathrm{Ext}^i_R(R/m^{n+1}, M)$$

for all $i \geq 0$. We define the local cohomology modules of M by

$$H^i_m(M) = \varinjlim \mathrm{Ext}^i_R(R/m^n, M).$$

The local cohomology modules are Artinian, but are not finitely generated in general. They are related to the depth of an R-module in the following way: if M is an R-module of depth t and dimension d, then $H^d_m(M) \neq 0$, $H^t_m(M) \neq 0$, and $H^i_m(M) = 0$ for any $i < t$ or $i > d$. Thus, we see that

$$\mathrm{depth}(M) = \min\{i : H^i_m(M) \neq 0\}.$$

If (R, m) local or positively graded (with R_0 Artinian) is Cohen-Macaulay of dimension d, then the *canonical module* ω_R of R is the unique (up to non-unique isomorphism) R-module satisfying

$$\omega_R^\vee = \mathrm{Hom}(\omega, E_R(K)) \cong H_m^d(R),$$

where $E_R(K)$ is then injective hull of the residue field K over R. The local duality theorem then implies that for any $i \geq 0$,

$$H_m^i(M)^\vee = \mathrm{Hom}(H_m^i(M), E_R(K)) \cong \mathrm{Ext}_R^{d-i}(M, \omega_R)$$

for any finitely generated R-module M, and hence $\mathrm{Ext}_R^i(M, \omega_R) = 0$ if and only if $i > \dim(R) - \mathrm{depth}(M)$. If R is module-finite over a regular ring A (e.g. if R is positively graded with $R_0 = K$ a field, or if R is complete local), then $\omega_R \cong \mathrm{Hom}_A(R, A)$ (actually $\mathrm{Hom}_A(R, A(-\dim(A)))$ in the graded case). If the local ring R is a homomorphic image of a regular ring S with $\dim(S) - \dim(R) = t$, then $\omega_R \cong \mathrm{Ext}_S^t(R, S)$.

If ω_R is a canonical module for R, then $M^* = \mathrm{Hom}(M, \omega_R)$ gives a dualizing functor on on the class of MCM R-modules. In particular, M^* is MCM and $(M^*)^* \cong M$ for any MCM module M. Moreover, if

$$O \to M_1 \to M_2 \to M_3 \to 0$$

is a short exact sequence of MCM modules, then

$$O \to M_3^* \to M_2^* \to M_1^* \to 0$$

is also a short exact sequence of MCM modules. In fact, if R is module-finite over a regular ring A, or a homomorphic image of a regular ring S (but not necessarily Cohen-Macaulay), then one may still obtain a dualizing functor with the same properties on the set of MCM modules by setting $M^* = \mathrm{Hom}_A(M, A)$ or $M^* = \mathrm{Ext}^t_S(M, S)$, where $t = \dim(S) - \dim(R)$, as appropriate. One can show that any of these definitions give the same operation $(-)^*$ in the case that more than one of them is defined. Finally, if N is a module over (R, m), we define the *socle* of N by $\mathrm{Soc}(N) = \mathrm{Ann}_N m$, the largest submodule of N which is killed by m. Then, if M is a MCM R-module and I is a parameter ideal of R, we define the *type* $r(M)$ of M by

$$r(M) = \dim_K \mathrm{Soc}(M/IM).$$

It can be shown that the type is independent of the choice of the parameter ideal I. Moreover, if we have a dualizing operation $(-)^*$ on MCM modules, then $r(M) = \nu(M^*)$ for any MCM module M. This fact will be used repeatedly in the arguments of chapter 4.

I end the introduction with a theorem which will be used repeatedly throughout the dissertation, and whose proof will serve as something of a paradigm for much of the work which follows. The theorem was proved independently by Hartshorne and by Peskine and Szpiro [18], but remained unpublished until it was rediscovered by Hochster, who gave a proof in [7]. It implies the existence of finitely generated MCM modules for a 3-dimensional graded ring over a perfect field of positive prime characteristic, the only significant case in which the question of existence of small MCM modules has been answered in dimension 3. Its proof uses the general fact that if M is a graded module over a positively graded ring R of characteristic $p > 0$, then ${}^eM$ naturally splits into $q = p^e$ summands as an R-module. One gets such splitting for the simple reason that qth powers of elements of R raise degrees by a multiple of q when applied to M. Thus, the action of R on ${}^eM$ preserves the submodules ${}^eM(i)$ generated by forms of M of degree i mod q, which are therefore direct summands. (Some of the summands may be 0, but for any $D > 0$, at least D summands will be nonzero for all e sufficiently large.)

Theorem 1.5.3 (Hartshorne-Peskine-Szpiro). *Let R be a finitely generated $\mathbb{N}$-graded equidimensional K-algebra with $R_0 = K$ a perfect field of characteristic $p > 0$, and let m be the homogeneous maximal ideal. Suppose R has a finitely generated graded equidimensional module M with $dim(M) = dim(R)$, and that M_P is maximal Cohen-Macaulay over R_P for any prime $P \neq m$. Then R has a finitely generated MCM-module.*

Proof: Since K is perfect, ${}^eM$ is a finitely generated module for each e. Moreover, ${}^eM = \oplus_{0 \leq j < p^e} {}^eM(i)$, where ${}^eM(i) = \oplus_{j \equiv i \bmod p^e} M_j$. We will show that, for sufficiently large e, at least one of the summands ${}^eM(i)$ is MCM.

By hypothesis, the local cohomology modules $H^j_m({}^eM)$ are finite-length for $j < \dim(R)$. Moreover, it follows from the definition that $H^j_m({}^eM) \cong {}^e(H^j_m(M))$ for all j and any $e \geq 0$. Hence, we may conclude that for all e greater than or equal to some fixed e_0, each $H^j_m({}^eM)$, $j < \dim(R)$, is a K-vector space of fixed dimension γ_j, and that the Frobenius map induces an isomorphism $H^j_m({}^eM) \cong H^j_m({}^{e+1}M)$.

Thus, if we choose e large enough so that M has at least $\sum \gamma_j$ nonzero direct summands, then since $\oplus_{j<\dim(R)} H^j_m({}^eM)$ has dimension $\sum \gamma_j$, we must have $\oplus_{j<\dim(R)} H^j_m({}^eM(i)) = 0$ for some some nonzero summand ${}^eM(i)$. It follows that ${}^eM(i)$ is a finitely generated maximal Cohen-Macaulay module for R. $\square$

CHAPTER II

Maximal Cohen-Macaulay modules satisfying special conditions

2.1 Definitions and background

The following definition was first introduced by Ulrich in [20]. In that paper, Ulrich was able to give a simple characterization of the Gorenstein property for a Cohen-Macaulay local ring in the presence of a MCM module which is sufficiently close to being *linear*, as defined below. Ulrich's theorem, and some further developments along the same lines, will be presented in section 4.

Definition 2.1.1. Let (R, m) be a Noetherian local ring with a finitely generated maximal Cohen-Macaulay module M. Then M is said to be linear (or a maximally generated maximal Cohen-Macaulay module) if $e(M) = \nu(M)$.

The first existence results for linear MCMs were set out by J. Brennan, J. Herzog, and B. Ulrich in [2]. There they showed the existence of lin MCMs for one-dimensional rings, two-dimensional graded Cohen-Macaulay domains, rings of minimal multiplicity, and certain rings of determinantal varieties. The most significant existence result to appear subsequently is that of Backelin, Herzog, and Ulrich in [1]. There the existence of lin MCMs was proved for local rings which are *strict* complete intersections (i.e. both the ring and its associated graded ring are complete intersections).

A question posed in Ulrich's original paper [20] was whether every local Cohen-Macaulay ring posesses a linear MCM module. There is as yet no known counterexample, although the condition is so strong as to make a positive answer seem unlikely in general. Moreover, the existence of lin MCMs in any particular case has very strong consequences, as will be seen below. In this chapter and the next, we will give a positive answer to the question for some new classes of rings, as well as many existence results for related but somewhat less restrictive notions.

If we assume that the residue field of R is infinite, then we may choose a minimal reduction $I = (x_1, \ldots, x_d)$ of m. Now we know that $e(M) = l(M/IM)$ and $\nu(M) = l(M/mM)$. It is then obvious that $e(M) \geq \nu(M)$ (the general case of this inequality can be deduced by extending the residue field) and that M is linear if and only if $mM = IM$. It is this characterization of linearity which is to be stressed in much of the work presented here.

A further approach to formulating the question of existence of lin MCMs is as follows: assume that R either is complete local and contains an infinite field, or else is positively graded over an infinite field K. Then we may choose a minimal reduction $(x_1, ..., x_d)$ of the maximal ideal m and express R as a module-finite extension of the power series ring $A = K[[x_1, \ldots, x_d]]$ (or of the polynomial ring $A = K[x_1, \ldots, x_d]$). Now a MCM module M over R must also be MCM, hence free, over the regular ring A. Thus, a MCM module over R is simply a free A-module with the added structure of an R-module.

Question 2.1.2. Let R be a complete local ring containing an infinite field, and let $(x_1, ..., x_d)$ be a minimal reduction of the maximal ideal m. Set $A = K[[x_1 ... x_d]] \subseteq R$. Can you define, for some n, an A-algebra homomorphism $R \to M_n(A)$? Given such a homomorphism, can you define another one (for possibly greater value of n), such that all elements of m map to matrices with all entries in the maximal ideal $(x_1, ..., x_d)$?

Of course, giving an A-algebra map $R \to M_n(A)$ is equivalent to defining an R-module structure on $A^{(n)}$ which extends the usual A-module structure. If the module M defined in this way is linear, then we know that $mM = (\underline{x})M$, which is to say that elements of m act upon A^n by matrices with entries in $(\underline{x})$.

Both of the above correspond to solving polynomial equations with coefficients in A in some matrix ring $M_n(A)$; namely, the same equations satisfied by the generators of R as an A-algebra. They may also be considered as solving in A certain polynomial equations on the entries of the matrices, simply by considering a matrix equation as a system of n^2 equations on the entries of the matrices.

In the graded case, the problem of mapping to a matrix ring over a regular subring can be translated into even more familiar terms:

Lemma 2.1.3. *If R is a positively graded K-algebra, generated by its 1-forms, and if R possesses a lin MCM (i.e. there is a map $R \to M_n(A)$, as above, with no entries with nonzero constant coefficient), then there is a solution in which the entries of the matrices are linear forms in the elements $x_1, \ldots, x_d$ of $A = K[x_1, \ldots, x_d]$.*

Proof: As noted above, constructing such a mapping is equivalent to finding solutions $\{Z_i = F_i \in A\}$ of finitely many polynomial equations

$$G_j(x_1, \ldots, x_d, Z_1, \ldots, Z_r) \in A[Z_1, \ldots, Z_r],$$

where the Z_i correspond to the entries of matrices in $M_n(A)$ to which the generators of R are to be mapped. Since R is graded, the G_j are homogeneous elements of the ideal $(x_1, \ldots, x_d, Z_1, \ldots, Z_r)$.

Thus, since the polynomials F_i have zero constant term, it is easy to see that the lowest degree (potentially nonzero) component of $G_j(x_1, \ldots, x_d, F_1, \ldots, F_r)$ in A is given by $G_j(x_1, \ldots, x_d, f_1, \ldots, f_r)$, where f_i is the linear term of F_i; whence $\{Z_i = f_i\}$ must also give a solution. $\square$

Thus, finding a lin MCM M over R which has free rank n over A is equivalent to solving the polynomial equations $G_j(x_1, \ldots, x_d, f_1, \ldots, f_r)$ with linear forms $f_i = a_1x_1 + \ldots + a_nx_d$. But these identities hold if and only if the coefficients of all the monomials in the expansion are 0, and these coefficients are given by polynomials in the coefficients $\underline{a}$ over K. So the existence of such a module M is equivalent to the statement that a certain affine variety contained in $\mathbb{A}_K^{drn^2}$ is nonempty. Note that it is not at all clear that one can give a similar characterization of the existence of a (not necessarily linear) MCM module, since there is no way of bounding the degrees of the polynomials which occur as entries in a potential matrix solution. What we have really used above is a version of the following result on linear MCM modules (see [2]):

Proposition 2.1.4 (Brennan, Herzog, and Ulrich). *If M is a linear MCM module over a local ring (R, m), then the the associated graded module $gr_m(M)$ is MCM over $gr_m(R)$.*

This result is interesting in light of the fact that no such statement can be made with regard to a general MCM module over R.

The following definitions give weakenings of the linearity property which will be of use in later sections. Note that given a Cohen-Macaulay local (or positively graded) ring (R, m) and a minimal reduction I of m, there certainly exists some $n > 0$ such that $m^n \subseteq I$. So another approach to the problem of lin MCMs is to consider the question: what is the minimum integer n such that for some MCM R-module M, $m^n M \subseteq IM$? And, in particular, is $n = 1$? This leads one to the following generalization:

Definition 2.1.5. Let M be a finitely generated MCM-module over a local ring (R, m). Then we define the *reduction degree* of the module M (denoted $\text{red}(M)$) to be the least integer n such that $m^n M \subseteq (x_1, \ldots, x_d)M$ for some minimal reduction $(x_1, \ldots, x_d)$ of m.

Of course, reduction degree one is just linearity. And if $M = R$, then the reduction degree corresponds to the reduction number of the maximal ideal m.

In future sections it will also be necessary to allow the following somewhat less rigid definition. Although more complex, this notion will prove just as worthwhile in applications to Lech's conjecture, and it allows for far stronger existence results.

Definition 2.1.6. A sequence of MCM R-modules $\{M_i\}_{i \geq 0}$ is said to have *reduction degrees approaching* t if for some minimal reduction I of m,

$$\frac{l((m^t + I)M_i/IM_i)}{l(M_i/IM_i)} \to 0$$

as $i \to \infty$.

2.2 Properties

In this section we will show how the modules defined in section 1 behave with respect to certain standard operations on maximal Cohen-Macaulay modules. First, suppose that (R, m) is a Cohen-Macaulay local ring with canonical module ω_R (for a treatment of canonical modules see [3]). It is known that the class of MCM R-modules is preserved under the operation of dualizing into ω_R (see section 1.5). The following theorem shows that the class of linear MCM modules is also preserved under this operation. Moreover, if the dual module is linear, its structure can be given somewhat more specifically.

Theorem 2.2.1. *Let (R, m) be a Cohen-Macaulay local ring with infinite residue field K, and suppose R has canonical module ω_R. Let M be a MCM R-module. Then M is linear if and only if the module $M^* = \mathrm{Hom}_R(M, \omega_R)$ is linear. Moreover, in this case one has $\nu(M) = \nu(M^*)$.*

Proof: Since $M \cong \mathrm{Hom}_R(M^*, \omega_R)$, it suffices to prove the *only if* implication.

It is a well-known fact that if M is MCM, then so is M^* (see e.g. [3], Theorem 3.3.10). So suppose that M is linear; i.e. that $mM = IM$ for some parameter ideal $I = (x_1, \dots, x_d)$. To see that M^* is also linear, it suffices to show that M^*/IM^* is killed by the maximal ideal m. Note that

$$M^*/IM^* = \mathrm{Hom}_R(M, \omega_R) \otimes_R R/I \cong \mathrm{Hom}_{R/I}(M/IM, \omega_R/I\omega_R)$$

(see [3]). Since M is linear, M/IM is a K-vector space of dimension $\nu(M)$, and is killed by m; and since I is a parameter ideal in the Cohen-Macaulay ring R, it follows that $\omega_R/I\omega_R \cong \omega_{R/I} = E_{R/I}(K)$, the injective hull of the residue field. Finally, since $\mathrm{Hom}_{R/I}(K, E_{R/I}(K)) \cong K$, it follows that M^*/IM^* is isomorphic to a K-vector space of dimension $\nu(M)$, which shows that M^* is linear with $\nu(M)$ generators. □

So now suppose that (R, m) is Cohen-Macaulay with canonical module ω_R, and has a non-free linear MCM module M. Then we may write down a presentation

$$O \to U \to R^n \to M \to 0$$

where $n = \nu(M)$ and U is (necessarily) MCM. Applying the operation $\mathrm{Hom}_R(-, \omega_R)$, we get a new exact sequence of MCM modules

$$O \to M^* \to \omega_R^n \to U^* \to 0$$

where M^* is linear and $\nu(M^*) = \nu(M) = n$. Hence, if I is a parameter ideal such that $mM = IM$, we get an injection $K^n \cong M/IM \hookrightarrow \omega^n/I\omega^n$, the image of which must equal to the n-dimensional socle of $\omega^n/I\omega^n$. These considerations immediately yield the following:

Corollary 2.2.2. *Let (R, m) be a Cohen-Macaulay local ring with canonical module ω_R, and let I be a minimal reduction of the maximal ideal m. Let α represent a lifting to ω of a generator of the socle of $\omega/I\omega$. Then R has a linear MCM module if and only if there exist, for some $n > 0$, elements u_{ij} of $I\omega_R$ such that the submodule N of ω_R^n spanned by the n elements*

$$(\alpha + u_{11}, u_{12}, \dots, u_{1n}),\ (u_{21}, \alpha + u_{22}, u_{23}, \dots, u_{2n}), \dots, (u_{n1}, \dots, u_{n\,n-1}, \alpha + u_{nn})$$

has the property that ω_R^n/N is MCM.

We will need to know later on that the more general properties of reduction degree are also preserved by this sort of dualizing. Since it is not necessary to assume that the ring R is Cohen-Macaulay, I do not wish to assume the existence of a canonical module over R. Nevertheless, one may often define a functor $(-)^*$ with many of the same properties, as was seen in section 1.5.

Proposition 2.2.3. *Let R be a local or positively graded algebra containing a field, and assume that R admits a dualizing functor $(-)^*$ on MCM modules (of the kind defined in section 1.5). Then for any MCM module M over R, one has $red(M) = red(M^*)$. Likewise, if $\{M_i\}$ is a sequence of MCMs over R, then this sequence has reduction degrees approaching t if and only if the same is true of the sequence $\{M_i^*\}$.*

Proof: We first note that completion at the maximal ideal commutes with dualizing; i.e. that $(\hat{M})^* \cong (M^*)^\wedge$ for any R-module M. This follows from the flatness of $R \to \hat{R}$ and from the fact that the maximal ideal of R extends to that of $\hat{R}$ (see [3], section 3.3). Moreover, since the definitions of reduction degree and sequences approaching a certain reduction degree refer only to finite length quotients of modules over R, these properties are preserved under the operation of completion at the maximal ideal. Similarly, if R is a complete local ring with coefficient field K, all of the relevant properties and operations are preserved when we extend K to a larger field L.

It follows that we may reduce to the case that R is a complete local ring with infinite coefficient field K. If $I = (x_1, \dots, x_d)$ is a minimal reduction of m_R, let $A = K[[x_1, \dots, x_d]] \subseteq R$. We may now assume that the operation $(-)^*$ on MCM R-modules is defined by $M^* = \mathrm{Hom}_A(M, A)$ (see section 1.5).

First note that $M^*/IM^* \cong \mathrm{Hom}_K(M/IM, K)$. It immediately follows that if m^t kills the module M/IM, then it also kills the module M^*/IM^*. This shows that $\mathrm{red}(M^*) \leq \mathrm{red}(M)$, and since $M \cong (M^*)^*$, we see that $\mathrm{red}(M) = \mathrm{red}(M^*)$.

Secondly, note that for any M, we have $l(M/IM) = l(M^*/IM^*)$. Thus, to prove the second statement, it suffices to give a uniform bound for

$$\alpha = l\left(\frac{(m^t + I)M^*}{IM^*}\right)$$

in terms of

$$\beta = l\left(\frac{(m^t + I)M}{IM}\right).$$

But since $M^*/IM^* = (M/IM)^\vee = \mathrm{Hom}_K(M/IM, K)$, we have from the following lemma that $\alpha \leq \nu(m^t) \cdot \beta$, where of course $\nu(m^t)$ is a constant independent of the module M. Thus, if the modules $\{M_i\}$ have reduction degrees approaching t, the same must be true of their duals $\{M_i^*\}$. $\square$

Lemma 2.2.4. *Let M be a finitely generated module over an Artinian K-algebra A, and let J be an ideal of A. Then $l(JM^\vee) \leq \nu(J) \cdot l(JM)$.*

Proof: Since $M^{\vee\vee} = M$, it is equivalent to show that for any M, $l(JM) \leq \nu(J) \cdot l(JM^\vee)$. First, we wish to see that

$$l(JM^\vee) = l(M) - l(\mathrm{Ann}_M J) = l(M/\mathrm{Ann}_M J).$$

For this, set $J = (x_1, \dots, x_n)$, and consider the exact sequence

$$0 \to \mathrm{Ann}_M J \to M \to M^{(n)},$$

where the last map is given by the $n \times 1$-column matrix with the x's as its entries. Since applying the functor $^\vee$ is exact, this induces the short exact sequence

$$O \to JM^\vee \to M^\vee \to (\mathrm{Ann}_M J)^\vee \to 0,$$

from which the conclusion follows (note that $\dim_K M^\vee = \dim_K M$ for any finitely generated module M).

But now we need only note that the vector space JM is spanned by elements of the form xm, where x is a generator of J and $m \in M \setminus \mathrm{Ann}_M J$. Thus

$$l(JM) \leq \nu(J) \cdot l(M/\mathrm{Ann}_M J) = \nu(J) \cdot l(JM^\vee),$$

as required. $\square$

Finally, if (R, m) is a local ring of dimension d which admits a minimal reduction $I = (x_1, \dots, x_d)$, then the condition of linearity on a MCM module M, namely $mM = IM$, corresponds to the regularity condition in the case that $M = R$ is the ring itself. It is known that regularity is maintained under the operation of localization. Moreover, if M is MCM over R, and P is a prime ideal, then the localized module $M_P = M \otimes R_P$ remains MCM over R_P. So a natural question is whether the localization M_P at a prime ideal of a linear MCM module over R is still linear. Unfortunately, the answer is negative:

Example 2.2.5. There exist linear MCM modules which do not remain linear upon localizing. In particular, if R is a homogeneous 2-dimensional Cohen-Macaulay domain with infinite residue field, and R is not normal, then R has a lin MCM M and a height one prime P such that M_P is not linear.

Proof: If R is a homogeneous 2-dimensional Cohen-Macaulay domain with infinite residue class field, then R admits a linear MCM module M and an exact sequence

$$O \to N \to M \to I \to 0,$$

where N is MCM and I is an height 2 homogeneous ideal of R (this was proved by Brennan, Herzog, and Ulrich in [2]).

Thus, if P is a prime ideal of R of height one, we see that

$$O \to N_P \to M_P \to R_P \to 0$$

remains exact, from which it follows that if M_P is linear, then R_P is also linear, i.e. regular. Thus M_P cannot be linear for any non-regular height one prime P of R. $\Box$

2.3 Existence of MCMs with low reduction degree

For a Cohen-Macaulay local ring R, one can always find a MCM module with reduction degree less than that of the ring itself, or a module whose ratio of multiplicity to number of generators is smaller than that of the ring.

Proposition 2.3.1. *Let (R,m) be a local Cohen-Macaulay ring with reduction number n (i.e. $m^n = Im^{n-1}$ for some minimal reduction I of m), and assume that R is not regular. Then:*

1. *R has a MCM-module M with reduction degree less than n.*

2. *R has a MCM-module M with $e(M) \leq \frac{e_R}{2} \cdot \nu(M)$.*

Proof: Let U_i be the *ith* syzygy module of $K = R/m$. Then for sufficiently large d, U_d and U_{d+1} are MCM. Moreover if $(x_1, \ldots, x_n)$ is a minimal reduction of m, then the exact sequence

$$O \to U_{d+1} \to R^s \to U_d \to 0$$

of MCM modules with U_{d+1} mapping into mR^s yeilds the exact sequence

$$O \to U_{d+1}/(\underline{x})U_{d+1} \to R^s/(\underline{x})R^s \to U_d/(\underline{x})U_d \to 0$$

Now, it is clear that the image of $m^{n-1}U_{d+1}$ after going mod $(\underline{x})$ maps to

$$m^n(R^s/(\underline{x})R^s) = 0$$

in the second exact sequence; and hence $m^{n-1}U_{d+1} \subseteq (\underline{x})U_{d+1}$. Thus, the MCM module U_{d+1} has reduction degree less than or equal to $n-1$.

Moreover, since the projective dimension of K is infinite, we must be able to choose d as above so that U_d and U_{d+1} are MCM, and $\nu(U_{d+1}) \geq s = \nu(U_d)$. Since multiplicities are additive on short exact sequences, we know that $e(U_d) + e(U_{d+1}) = s \cdot e_R$. It follows that for at least one of U_d and U_{d+1}, one must have

$$e(U_i) \leq (s/2) \cdot e_R \leq \frac{e_R}{2} \cdot \nu(U_i). \ \square$$

Of course, one would like to generalize the above argument in order to show how to proceed from a MCM module M with reduction degree n to one with reduction degree $(n-1)$. But it is not clear that we can construct short exact sequences in the same way as above for a general M. Nevertheless, it is worthwhile to pose the question in its strongest form:

Question 2.3.2. Let M be a MCM-module over (R, m) which is not linear. Then is there a short exact sequence of MCM-modules

$$0 \to U \to M^s \to N \to 0$$

such that U maps into mM^s? (Equivalently, does there exist some $s > 0$ and some submodule $U \subseteq mM^s$ such that M/U is a MCM R-module?). A positive answer would imply, by an inductive argument, not only the existence of lin MCMs, but also that the Grothendieck group of MCM modules over R is generated by the linear MCM modules.

Since the maximal ideal of a local ring (R, m) of fixed dimension d may have arbitrarily high reduction number, the above results are still not very satisfying. But, at least for rings of prime characteristic $p > 0$, one can give an existence result dependent only upon the dimension of the ring. In the case that the reduction number t of m_R is high, these results are much better than those achieved above.

Lemma 2.3.3. *Let (R, m) be any d-dimensional local ring of characteristic $p > 0$. If $I = (x_1, \ldots, x_d)$ is a minimal reduction of m, then for sufficiently large $q = p^e$, $(m^{d+1})^{[q]} \subseteq I^{[q]}$.*

Proof: There exists $t > 0$ such that $m^n = I^{n-t}m^t$ for all $n \geq t$. But then, as long as $q \geq t$, it is clear that

$$(m^{d+1})^{[q]} \subseteq m^{dq+q} \subseteq I^{dq+q-t} \subseteq I^{dq} \subseteq I^{[q]}. \square$$

Proposition 2.3.4. *Let (R, m) be a d-dimensional F-finite ring of characteristic $p > 0$, with perfect residue field K. If R possesses a MCM module M, then the modules ${}^eM$ are MCM modules of reduction degree less than or equal to $d+1$ for sufficiently large e. Moreover, the sequence of modules $\{{}^eM\}_{e \geq 0}$ has reduction degrees approaching d.*

Proof: The first statement immediately follows from the lemma, since

$$m^{d+1} \cdot ({}^eM) = (m^{d+1})^{[q]}M.$$

For the second note that, by the same argument as above, we have

$$m^t(m^d)^{[q]} \subseteq m^{dq+t} \subseteq I^{dq} \subseteq I^{[q]}$$

for all sufficiently large q. Thus, for $e >> 0$, the module

$$\frac{(m^d + I)({}^eM)}{I({}^eM)}$$

is killed by m^t (via the usual module structure). Since such a module, seen as an R-module via the usual module structure, clearly needs at most $\nu(m^d) \cdot \nu(M)$ generators, we thus see that

$$l\left(\frac{(m^d + I)({}^eM)}{I({}^eM)}\right) \leq l(R/m^t) \cdot \nu(m^d) \cdot \nu(M),$$

independently of e.

Since the ranks and multiplicities of the modules ${}^eM$ approach infinity (except in the case $d = 0$, which is trivial), this shows that their reduction degrees must approach d. □

Proposition 2.3.5 (Graded case). *If (R, m) is a finitely generated positively graded algebra over a perfect field K of characteristic $p > 0$, with $R_0 = K$, and if R is Cohen-Macaulay except at the origin (i.e. R_P is Cohen-Macaulay for any prime P not equal* *to the irrelevant ideal m), then R has a MCM-module M with $m^d M \subseteq IM$. If R is generated over K by one-forms, then one also obtains a sequence of MCMs with reduction degrees approaching $d-1$.*

Proof: As before, if $m^n = I^{n-t}m^t$ for all $n > t$, then it is clear that, for sufficiently large q, $(m^d)^{[q]}I^t \subseteq I^{dq-t+t} \subseteq I^{[q]}$. Thus, the length of $m^d({}^eR)/I({}^eR)$ is bounded by $\nu(m^d)$ times the length of R/I^t for all large e.

By theorem 1.5.3, we know that for some $t \geq 0$ and all sufficiently large e, the module ${}^eR$ will have at least $\nu(m^d) \cdot l(R/I^t) + 1$ (nonzero) MCM direct summands. It follows that at least one such summand must be MCM with reduction degree less than or equal to d.

For the second part, note that there exists some $a \geq 0$ such that for $q >> 0$, there exists $q - a \leq b < q$ such that $M_{b,q}$ (the summand of ${}^eR$ generated by forms of degree b mod q) is MCM. But then $m^{t+a}(m^{d-1})^{[q]}$ multiplies the summand $M_{b,q}$ into $I^{[q]}$, and we may argue as above to show that there is a sequence of MCM summands of the modules ${}^eR$ which have reduction degrees approaching $d-1$. $\square$

2.4 A theorem of Ulrich in characteristic $p > 0$

In this section I wish to give an application of the prime-characteristic techniques to a theorem of Ulrich which appeared in the original paper [20]. We start by showing the existence of linear MCM modules for a certain class of local rings of positive prime characteristic p. The conditions placed upon these rings are rather restrictive, as their maximal ideal m is already required to be very close to equaling a parameter ideal I, in the sense that $m = I^F$, the *Frobenius closure* of I. However, we can show that any local Cohen-Macaulay ring of characteristic p has a multitude of *nice* extension algebras which have this property.

Definition 2.4.1. Let R be a ring of positive prime characteristic p, and let I be an ideal of R. Then the Frobenius closure I^F of I in R is the set of elements $z \in R$ such that for some $e \geq 0$ (equivalently, for every $e >> 0$), $z^{p^e} \in I^{[p^e]}$. The tight closure I^* of I is the set of elements $z \in R$ with the property that $cz^{p^e} \in I^{[p^e]}$ for all $e \geq 0$, where c is some nonzerodivisor in R.

Both I^F and I^* are ideals, and it is not difficult to show that both are contained in the integral closure of I.

Lemma 2.4.2. *Let (R,m) be an F-finite Cohen-Macaulay local ring of characteristic $p > 0$. If $m = I^F$ for some parameter ideal $I = (x_1, \ldots, x_d)$, then R has a linear MCM module.*

Proof: Since m is finitely generated, we may choose $e > 0$ such that $m^{[q]} = I^{[q]}$, where $q = p^e$. Now, if we just let ${}^eR$ stand for R viewed as a module over itself via the eth power of the Frobenius endomorphism, it is easy to see that $m({}^eR) = m^{[q]}R = I^{[q]}R = I({}^eR)$. Moreover, as R is Cohen-Macaulay, $x_1^q, \ldots, x_d^q$ is a regular sequence on R; whence $x_1, \ldots, x_d$ is a regular sequence on ${}^eR$. Thus ${}^eR$ is a linear MCM module for R. □

Proposition 2.4.3. *Let (R,m) be an F-finite Cohen-Macaulay local ring of characteristic $p > 0$. Then there exists a flat local module-finite extension of R which possesses a linear MCM module. In fact, for any system of parameters $x_1, \ldots, x_d$ of R, and for any sufficiently large $q = p^e$ (dependent upon the system of parameters $(\underline{x})$), the free extension*

$$S = \frac{R[z_1, \ldots, z_d]}{(z_1^q - x_1, \ldots, z_d^q - x_d)}$$

has a linear MCM module.

Proof: Let $I = (\underline{x})$ be an ideal generated by a system of parameters of R. Then clearly, for sufficiently large $q = p^e$, we have $m^{[q]} \subseteq I$. But the elements $z_1, \dots, z_d$ obviously form a system of parameters of

$$S = \frac{R[z_1, \dots, z_d]}{(z_1^q - x_1, \dots, z_d^q - x_d)}$$

and since the maximal ideal n of S is generated by m and the z's, we see that $n^{[q]} = m^{[q]}S + (\underline{z}^q)S = (\underline{z}^q)S$. Hence n is the Frobenius closure of a parameter ideal, and the result now follows from the preceding lemma. $\square$

Note that this shows that any property which is preserved by contraction from a faithfully flat extension, and which is implied by the existence of a linear MCM module, will hold for all Cohen-Macaulay local rings with positive prime characteristic p and perfect residue field. In particular, it raises the question of whether the existence of a linear MCM is such a property.

Question 2.4.4. If $R \subseteq S$ is a flat local extension of local Cohen-Macaulay rings of the same dimension, and if S has a linear MCM module, must R have one?

Finally we may deduce the following consequence from the existence of linear MCM modules over the free extensions described above. According to Lemma 2.4.2, ${}^eS$ is a linear MCM module for the extension ring S in Proposition 2.4.3. But note that $F^e(S) \subseteq R \subseteq S$, and the same reasoning as before shows that this makes R a linear MCM module over S, since $m^{[q]}R + (\underline{z}^q)R = (\underline{z}^q)R$.

The following theorem was proved by Ulrich in [20].

Theorem 2.4.5 (Ulrich). *Let R be a local Cohen-Macaulay ring, and suppose M is a finitely generated MCM R-module of positive rank such that*

1. $2\nu(M) > e_R \cdot \operatorname{rank}(M)$.

2. $\operatorname{Ext}^i_R(M, R) = 0$ *for* $1 \leq i \leq \dim(R)$.

Then R is Gorenstein.

In general, R is Gorenstein if and only if the second condition holds for every MCM module M. The theorem says that if a certain module M has sufficiently nice numerical properties, then it suffices to check condition 2 for this particular module. In particular, if M is a linear MCM module of positive rank for R, the theorem implies that R is Gorenstein if and only if $\operatorname{Ext}^i_R(M, R) = 0$ for $1 \leq i \leq \dim(R)$ (the *only if* direction follows from the fact that R is its own canonical module). Moreover, if R is a local ring of characteristic $p > 0$, and S is the free extension of R defined above, then it is clear that:

1. S is Cohen-Macaulay if and only if R is, by faithful flatness.

2. $S/(\underline{z}) \cong R/(\underline{x})$, whence these residues also must have isomorphic socles.

Hence R is Gorenstein if and only if S is; and if R is Cohen-Macaulay and F-finite, S may be chosen so that it has R as a linear MCM module, when viewed as an S-module via a suitable power of the Frobenius endomorphism. From this we obtain the following:

Corollary 2.4.6. *Let (R, m) be an F-finite Cohen-Macaulay local domain of characteristic $p > 0$, and let $q = p^e$ be chosen so that*

$$S = \frac{R[z_1, \ldots, z_d]}{(z_1^q - x_1, \ldots, z_d^q - x_d)}$$

has R (viewed as an S-module via $F^e(S) \subseteq R$) as a linear MCM module. Then R is Gorenstein if and only if $\operatorname{Ext}^i_S(R, S) = 0$ *for all* $i \geq 1$.

Proof: The corollary of course follows from the theorem and subsequent discussion, provided we show that the MCM-module used in the corollary has positive rank. If the extension ring S is a domain, then this is necessarily the case. And it is easy to see that if R is a domain, then the nilpotent ideal of S is prime: for if ab is nilpotent for elements a and b of S, then $a^q b^q$ is also nilpotent, where a^q and b^q are nonzero elements of R, which implies that either $a^q = 0$ or $b^q = 0$. Hence S will be a domain if and only if it is reduced.

So assume that $s = \sum_i r_i \underline{z}^{\underline{a}}$ is a nilpotent element of S, where the sum is taken over monomials in z with $0 \leq a_j < q$ for each $1 \leq j \leq d$, and $r_i \in R$ for all i. Taking qth powers, we get that $s^q = \sum r_i^q \underline{x}^{\underline{a}} = 0$, since it is at least a nilpotent element of R. This says that the monomials $\{x_1^{a_1} \cdots x_d^{a_d} : 1 \leq a_i < q\}$ have a nontrivial relation over $R^{[q]}$. Such a relation would continue to hold in the completion $\hat{R}$, which is module finite over the power series ring $A = K[[x_1, \ldots, x_d]]$. But this is contradicted by the fact that there is no such relation over $A^{[q]}$ and the fact that $R^{[q]} \cong R$ is Cohen-Macaulay, hence flat over $A^{[q]}$. $\square$

CHAPTER III

Existence results for specialized maximal Cohen-Macaulay modules

3.1 Linear MCM modules over monomial rings

In trying to find some new classes of Cohen-Macaulay rings for which linear MCM modules can be shown to exist, a good place to look is among the classes of monomial rings and determinantal rings, where combinatorial arguments may allow actual computations of such numerical invariants as the multiplicity. At least one result in this direction has already been attained, and appears in the article [2]:

Proposition 3.1.1 (Brennan, Herzog, Ulrich). *Let $s \geq r \geq 0$ be positive integers, $A = K[x_1, \ldots, x_n]$ a polynomial ring over the field K, and C an $r \times s$ matrix whose entries are linear forms in A. Assume, moreover, that* $\mathrm{grade}(I_r(C)) = \mathrm{height}(I_r(C))$*, where $I_r(C)$ is the ideal of A generated by the $r \times r$ minors of C. Then $R = A/I_r(C)$ admits a linear MCM module M.*

I will not reproduce the proof, except to say that the result stated here may be deduced from the case of the ring of generic $r \times r$ minors, where $n = r \cdot s$ and C is just the matrix which has the variables as its entries. The generic ring is known to be Cohen-Macaulay by a result of Eagon and Northcott (see [5]). In the statement above the condition on the grade of $I_r(C)$ is necessary in order to ensure that R is

Cohen-Macaulay.

This result of course invites the following more general:

Question 3.1.2. Let $A = K[x_{ij} : 1 \leq i \leq m,\ 1 \leq j \leq n]$ be a polynomial ring over the field K, where we assume that $m \leq n$. Let X be the $m \times n$ matrix whose ij entry is x_{ij}, and set $R_r(X) = A/I_r(X)$ for $1 \leq r \leq m$. For which choices of m, n, and r does $R_r(X)$ admit a linear MCM module?

The results of Eagon and Hochster in [4] show that all of the rings $R_r(X)$ are Cohen-Macaulay. The proposition stated above gives a positive answer to the question in the case that r is maximal; namely $r = m$. Here I will give a proof in the case that r is minimal (excepting the trivial case $r = 1$): namely $r = 2$.

Proposition 3.1.3. *For any m and n, and any field K, the ring of generic 2×2 minors $R_2(X)$ admits a linear MCM module.*

Proof: The first thing we need to note is that $R_2(X)$ is isomorphic to the K-subalgebra R of the polynomial ring $K[X_1, \ldots, X_m, Y_1, \ldots, Y_n]$ generated by the monomials

$$X_1^{a_1} \cdots X_m^{a_m} Y_1^{b_1} \cdots Y_n^{b_n}$$

with $\sum a_i = \sum b_j$ (i.e. R is the Segre product of the polynomial rings $K[X_1, \ldots, X_m]$ and $K[Y_1, \ldots, Y_n]$). Indeed, it is clear that we may map $R_2(X)$ onto R by sending x_{ij} to X_iY_j, since the relations on the x_{ij} in $R_2(X)$ are generated by those of the form $x_{ij}x_{kl} - x_{il}x_{kj}$. Since both rings are known to be domains of the same dimension $m + n - 1$ (see e.g. [3]), this map must be an isomorphism.

We will henceforward work with the ring R. Note that, for any integer $t > 0$, there exists a ring homomorphism $f_t : R \to R$ which is the identity on K and sends X_iY_j to $X_i^tY_j^t$ for all i and j. Moreover, R viewed as an R-module in this way splits into direct summands $M_t(c_1, \dots, c_m, d_1, \dots, d_n)$ generated over K by the monomials

$$X_1^{a_1} \cdots X_m^{a_m} Y_1^{b_1} \cdots Y_n^{b_n}$$

with $a_i \equiv c_i$ and $b_i \equiv d_i \bmod t$, and $\sum a_i = \sum b_j$.

Since R is Cohen-Macaulay, R viewed as an R module via f_t will be a MCM module, and hence any summand must also be MCM. I claim that, for any $t > m$, the module

$$W = M_t(-1, -1, \dots, -1, 0, 0, \dots, 0, -m)$$

is linear (here the first m entries are -1).

First we wish to show that the rank of W as an R-module is 1. But this is clear from the fact that we may obtain any monomial in W from the element $X_1^{t-1} \cdots X_m^{t-1} Y_n^{tm-m} \in W$ by successively multiplying by elements of the form

$$X_i^t Y_n^t \quad \text{or} \quad \frac{Y_i^t}{Y_n^t} = \frac{X_1^t Y_i^t}{X_1^t Y_n^t},$$

all of which are t^{th} powers of elements of the fraction field of R.

Thus $e(W) = e(R)$, which can be calculated as follows. Since the d^{th} power of the maximal ideal of R is generated by all products of monomials of degree d in a polynomial ring of dimension m with monomials of degree d in a polynomial ring of dimension n, the leading term of the Hilbert polynomial for R must be:

$$\frac{d^{m-1}}{(m-1)!} \cdot \frac{d^{n-1}}{(n-1)!}.$$

It follows that

$$\dim(R) = m + n - 1 \quad \text{and} \quad e(R) = \frac{(m+n-2)!}{(m-1)!(n-1)!} = \binom{m+n-2}{m-1}.$$

All that remains to show is that W needs at least $e(R)$ generators as an R-module. But since R acts on W by t^{th} powers, this follows if we can find $e(R)$

distinct monomials in W in which the exponents of the X's are all less than t. This requirement is easily seen to be satisfied by the monomials:

$$X_1^{t-1}\cdots X_m^{t-1}Y_1^{i_1t}\cdots Y_{n-1}^{i_{n-1}t}Y_n^{i_nt+t-m},\ \text{where}\ \sum_{j=1}^{n} i_j = m-1,$$

since the number of such elements is equal to the number of monomials of degree $m-1$ in n variables, namely $\binom{m+n-2}{m-1}$. Thus $\nu(W) \geq e(R)$, which completes the proof that W is a linear MCM module over R. $\square$

Note 3.1.4. Many other choices for the residues of the exponents and for the degree of the map from R to itself will yield linear MCM modules. In particular, the same proof as the one given above shows that

$$M_t(-j_1,\dots,-j_m,0,\dots,0,-\sum_{k=1}^{m} j_k)$$

is linear as long as $t > \sum_{k=1}^{m} j_k$.

The problem of existence of linear MCM modules for generic rings of minors has thus been solved in the cases of 2×2 minors and maximal minors. So it is reasonable to hope that one can give a positive answer for all of the rings $R_r(X)$ of generic $r\times r$ minors. For future reference, we record the following (see [11]): for any $m,n,r>0$, if we set $A = K[X_{ij}]_{1\leq i\leq m, 1\leq j\leq n}$, then we have $\dim(A/I_{r+1}(X)) = (m+n-r)\cdot r$ and

$$e(A/I_{r+1}(X)) = \det\left[\binom{m+n-i-j}{m-i}\right]_{i,j=1,\dots,r} = \prod_{i=0}^{n-r-1}\frac{(m+i)!\,i!}{(r+i)!\,(m-r+i)!}$$

Although we started out studying determinantal rings, the proof of the proposition used the structure of the ring as a toric subring of a polynomial ring, i.e. as a normal subring generated by monomials. This leads us to ask whether the same methods might allow us to show the existence of linear MCM modules for all toric rings. In particular, for such a ring R, one always has maps $f_t : R \to R$ as above, and

R viewed as a module in this way splits into MCM direct summands $M_t(i_1, \dots, i_N)$, as before. One may ask whether some such module is always linear. The following example shows that this is not always the case.

Example 3.1.5. Let S be the monomial subring of

$$K[X_1, \dots, X_r, Y_1, \dots, Y_s, Z_1, \dots, Z_t]$$

generated by all monomials which have the same total degree in each of the three sets of variables $\underline{X}$, $\underline{Y}$, and $\underline{Z}$ (where we assume that $r, s, t > 1$). Let $f_q : S \to S$ be the map defined by multiplying all exponents of monomials by q, as above. Then for no choice of residues $0 \leq a_i, b_i, c_i < q$ is the module

$$M_q(a_1, \dots, a_r, b_1, \dots, b_s, c_1, \dots, c_t)$$

(nonzero and) linear MCM.

Proof: As in the preceding proposition, one can see that the modules $M_q(\underline{i})$ have rank 1, and that the multiplicity of the ring S is

$$\frac{(r+s+t-3)!}{(r-1)!(s-1)!(t-1)!} = \binom{r+s+t-3}{r-1} \cdot \binom{s+t-2}{s-1}.$$

So suppose we have chosen the residues, and assume, without loss of generality, that

$$\sum_1^r a_i \leq \sum_1^s b_i \leq \sum_1^t c_i.$$

The module $W = M_q(\underline{a}, \underline{b}, \underline{c})$ will then be generated as an S-module by those monomials in S whose exponents have the appropriate residues mod q, and which have the property that all the exponents occuring in at least one of the three sets of variables are less than q. Because of the way we ordered the sums of the residues, this implies that W is generated by monomials in which all the exponents on the Z's are less than q; i.e. by monomials

$$X_1^{a_1+i_1q}X_2^{a_2+i_2q}\cdots X_r^{a_r+i_rq}Y_1^{b_1+j_1q}Y_2^{b_2+j_2q}\cdots Y_s^{b_s+j_sq}Z_1^{c_1}\cdots Z_t^{c_t}$$

with $\sum_1^r i_k = (1/q)(\sum_1^t c_l - \sum_1^r a_i) < t$ and $\sum_1^s j_k = (1/q)(\sum_1^t c_l - \sum_1^s b_s) < t$. As before, it follows that the number of such monomials is less than or equal to

$$\binom{r+t-2}{t-1}\cdot\binom{s+t-2}{t-1} = \binom{r+t-2}{r-1}\cdot\binom{s+t-2}{s-1}.$$

And this number is clearly less than the multiplicity of S. $\square$

3.2 Segre products of rings with lin MCMs

In this section I wish to prove a very general theorem on the existence of linear MCM modules over Segre product rings. Embedded within the proof can be found an alternative argument for Proposition 3.1.3. But the theorem also implies the existence of lin MCMs for the rings considered in Example 3.1.5, as well as for many others. A central idea of the proof, which will appear again later on, is to use the fact that the Hilbert function of a lin MCM is equal to the Hilbert function of a free module over a polynomial ring. This often allows one to generalize constructions for polynomial rings to any graded ring which possesses a lin MCM M, by working with the module M instead of the ring.

First we give the formal definition of the Segre product ring, then our result on linear MCM modules.

Definition 3.2.1. Let R and S be positively graded algebras over a a field K, with $R_0 = S_0 = K$. Then the Segre product ring $R \otimes_{seg} S$ is the positively graded K-subalgebra of $R \otimes_K S$ with graded pieces $(R \otimes_K S)_t = R_t \otimes_K S_t$ for all $t \geq 0$.

Proposition 3.2.2. *Let (R, m) and (S, n) be positively graded K-algebras generated by their 1-forms, where K is an infinite field and m and n represent irrelevant ideals; and suppose that R and S are integral domains. If R and S each possess a linear MCM module, then their Segre product ring $R \otimes_{seg} S$ also possesses a linear MCM module.*

Proof: If R and S have linear MCM modules M and N, respectively, then the associated graded modules $\mathrm{gr}_m(M)$ and $\mathrm{gr}_n(N)$ are linear MCMs with all generators in degree 0 (see Proposition 2.1.4). From here on we assume that M and N have these properties.

We may use graded Noether normalization to choose 1-forms $X_1, \ldots, X_r$ in R and $Y_1, \ldots, Y_s$ in S such that R and S are graded module-finite extensions of the polynomial rings $A = K[X_1, \ldots, X_r]$ and $B = K[Y_1, \ldots, Y_s]$, respectively. Since M is a graded lin MCM over R, we know that M is free of rank $c = e_R(M)$ as an A-module; moreover, $mM = (\underline{X})M$, which is to say that every 1-form of R acts on $M \cong_A A^c$ by a matrix of linear forms in the X's. Similarly, $N \cong_B B^d$, where $d = e_S(N)$, and 1-forms of S act on N via matrices of linear forms in the Y's.

Note that we have a module-finite extension $A \otimes_{seg} B \subseteq R \otimes_{seg} S$, and that $A \otimes_{seg} B$ is isomorphic to the subring of the polynomial ring $K[X_1, \ldots, X_r, Y_1, \ldots, Y_s]$ generated over K by all monomials which have the same total degree in the X's as in the Y's. The polynomial ring $K[\underline{X}, \underline{Y}]$ then splits over $A \otimes_{seg} B$ into submodules U_α generated by all monomials μ with the property that $\deg_X \mu - \deg_Y \mu = \alpha$, and it follows from a result of Goto and Watanabe that U_α is MCM over $A \otimes_{seg} B$ for $s > \alpha > -r$ (see [6]).

Although the polynomial ring $K[X_1, \ldots, X_r, Y_1, \ldots, Y_s]$ is generally not a module over $R \otimes_{seg} S$, the free $K[X_1, \ldots, X_r, Y_1, \ldots, Y_s]$ - module $M \otimes_K N$ of rank cd is an $R \otimes_{seg} S$ - module with induced module structure. Moreover, since 1-forms of R (respectively S) act on $M \cong A^c$ (respectively $N \cong B^d$) by matrices of 1-forms of $K[\underline{X}]$ (resp. $K[\underline{Y}]$), we see that $M \otimes_K N$ still splits as an $R \otimes_{seg} S$ - module into the direct summands $(M \otimes_K N)_\alpha = (K[\underline{X}, \underline{Y}]^{(cd)})_\alpha =$ the submodule of $M \otimes_K N$ generated by the vectors

$$\{(v_1, \dots, v_{cd}) : \text{each } v_i \in U_\alpha\}$$

Let us denote $(M \otimes_K N)_0$ by $M \otimes_{seg} N$ and $(M \otimes_K N)_{s-1}$ by W. It follows from Goto and Watanabe's result that both $M \otimes_{seg} N$ and W are MCM modules over $A \otimes_{seg} B$; hence they are also MCM over $R \otimes_{seg} S$. Moreover, if we denote the irrelevant ideals of $A \otimes_{seg} B$ and $R \otimes_{seg} S$ by I and J, respectively, then we know that $I(M \otimes_{seg} N) = J(M \otimes_{seg} N)$ and $IW = JW$.

It follows, in the first place, that

$$e(J; M \otimes_{seg} N) = e(I; M \otimes_{seg} N) = cd \cdot \binom{r+s-2}{s-1},$$

since $M \otimes_{seg} N$ is free of rank cd over $A \otimes_{seg} B$, which has multiplicity equal to $\binom{r+s-2}{s-1}$. Likewise,

$$\nu_{R \otimes_{seg} S}(W) = \nu_{A \otimes_{seg} B}(W) = cd \cdot \nu_{A \otimes_{seg} B}(U_{s-1}).$$

And since U_{s-1} is minimally generated over $A \otimes_{seg} B$ by monomials in the X's of degree $s-1$, we have $\nu_{A \otimes_{seg} B}(U_{s-1}) = \binom{r+s-2}{s-1}$. Thus, we have shown that the minimal number of generators of W over $R \otimes_{seg} S$ is equal to the multiplicity of of the module $M \otimes_{seg} N$.

Now, since $R \otimes_{seg} S$ is a domain, it will follow that W is a linear MCM for $R \otimes_{seg} S$, provided that we can show that W and $M \otimes_{seg} N$ have the same rank as $R \otimes_{seg} S$-modules. Note that there is certainly an inclusion

$$M \otimes_{seg} N \hookrightarrow W$$

given by multiplication by X_1^{s-1} (we could of course also use any other form of degree $s-1$ in the X's). Moreover, a typical element of W has the form

$$w = (\sum_i f_{1i}(\underline{X})\beta_{1i}, \dots, \sum_i f_{cd,i}(\underline{X})\beta_{cd,i}) \in (K[\underline{X}, \underline{Y}])^{(cd)},$$

with each $\beta_{ji} \in A \otimes_{seg} B$ and each f a form of degree $s-1$. Rewriting, we see that

$$w = \sum_{ji} f_{ji}(\underline{X})\mu_{ji}, \text{ where } \mu_{ji} = \beta_{ji} \cdot e_j \in M \otimes_{seg} N.$$

Thus, it suffices to notice that for any form f of degree $s-1$ in $K[\underline{X}]$, and for any $\mu \in M \otimes_{seg} N$, one has

$$f(\underline{X}) \cdot \mu = \frac{f(\underline{X})Y_1^{s-1}}{X_1^{s-1}Y_1^{s-1}} \cdot X_1^{s-1}\mu = \alpha \cdot X_1^{s-1}\mu,$$

where α is in the fraction field L of $R \otimes_{seg} S$. This implies that the injection of $M \otimes_{seg} N$ into W given above induces an isomorphism

$$L \otimes (M \otimes_{seg} N) \xrightarrow{\sim} L \otimes W$$

of L- vector spaces; and we have shown that $\mathrm{rank}(M \otimes_{seg} N) = \mathrm{rank}(W)$, as required. $\square$

3.3 Linear MCM modules over Veronese rings

Another class of monomial rings for which we might naturally hope to answer the question of the existence of linear MCMs is the class of Veronese subrings of polynomial rings. In dimensions 2 and 3, the question of existence of lin MCMs is positively answered for these rings. Moreover, in the same way as for Segre products, the proofs can be adapted to the case of Veronese subrings of a ring R which possesses a linear MCM. Finally, the proofs of existence entail a classification of graded MCMs over Veronese subrings which may be of interest in its own right.

The methods for constructing linear MCMs over Veronese rings of dimension 3 turn out to yield far-reaching generalizations, as we will see in subsequent sections. Results to be presented there should indicate that the class of Veronese subrings of regular rings is more representative of the class of graded K-algebras than might at first be apparent.

We first need to introduce some notation. If S is any Noetherian $\mathbb{Z}$-graded ring with graded pieces S_i, and t is any positive integer, then the t^{th} Veronese subring of S is the subring

$$S^{(t)} = \oplus_{i \in \mathbb{Z}} S_{it}.$$

Note that S is a finitely generated graded $S^{(t)}$-module, and that S splits into a direct sum

$$S = \oplus_{i=0}^{t-1} S_{i,t},$$

of $S^{(t)}$-modules, where $S_{i,t} = \oplus_{a \in \mathbb{Z}} S_{i+at}$.

Likewise, if M is a graded S-module, then M becomes an $S^{(t)}$-module via restriction of scalars, and one has an $S^{(t)}$-module splitting

$$M = \oplus_{i=0}^{t-1} M_{i,t},$$

where the modules $M_{i,t}$ are defined in the analogous way.

Note that if M is MCM over S, then the module-finiteness of S over $S^{(t)}$ implies that M is MCM over $S^{(t)}$. It follows that all of the direct summands $M_{i,t}$ must be MCM, as well. In particular, this shows that all Veronese subrings of a Cohen-Macaulay ring are Cohen-Macaulay. Finally, it is easy to see that if S is a domain generated by 1-forms over a field K, then the torsion-free rank over $S^{(t)}$ of any of the modules $S_{i,t}$ is one, whence the torsion-free rank of S over $S^{(t)}$ is t.

Although the existence of lin MCMs over Veronese rings of dimension 2 is known (see [2]), the method used here gives a very satisfactory answer in this case:

Proposition 3.3.1. *Let $R = S^{(t)}$, the t^{th} Veronese subring of the polynomial ring $S = K[X,Y]$ in 2 variables over the field K. Then any MCM module over R is isomorphic to a direct sum of modules of the form $S_{i,t}$.*

Proof: If M is a graded MCM module over R, let $Q = (S \otimes_R M)^{\vee\vee}$, the reflexivization of the expanded module. Then Q is Cohen-Macaulay (see [3]), hence free over S. But we may also note that, since M is already reflexive over R, we have $M = Q_{0,t}$. The conclusion is now apparent. □

Let $S = K[X,Y]$, as above. Since the multiplicity of the Veronese subring $R = S^{(t)}$ is t, it follows that the multiplicity of each of the R-modules $S_{i,t}$ is also t. But for each $0 \leq i < t$ the module $S_{i,t}$ is generated by the $i+1$ monomials of degree i in X and Y. We thus obtain:

Corollary 3.3.2. *If $S = K[X,Y]$, then $S_{-1,t}$ is the unique indecomposable linear MCM module over $S^{(t)}$ for every t.*

The situation becomes more interesting in dimension 3, where we actually obtain new results. I will first give the classification of MCMs over the Veronese subrings, then the results on lin MCMs. As above, $S = K[X,Y,Z]$ will be a polynomial ring in 3 variables over a field. Note that the graded canonical module of S is $S(-3)$, whence the canonical module of $S^{(t)}$ is $S_{3,t}$ (see [6]).

Proposition 3.3.3. *Let R be the t^{th} Veronese subring of $S = K[X,Y,Z]$. Then every finitely generated graded MCM module over R is equal to $W_{0,t}$, where W is a* *second syzygy over S of a finitely generated graded module N with the property that $N_{it} = 0$ for any integer i (in particular, N is killed by $\mathfrak{m}_S^t$).*

Proof: As before, let M be a graded MCM module over R, and let $M^* = \mathrm{Hom}(M, \omega_R)$. Now let $Q = (S \otimes_R M^*)^{**}$; since Q has depth at least 2 over S, $\mathrm{pd}_S Q \leq 1$. That is, we have an exact sequence:

$$O \to S^a \to S^b \to Q \to 0.$$

Applying the functor $\mathrm{Hom}(-, S(-3))$ to this sequence, we get a new exact sequence:

$$0 \to Q^* \to S^b \to S^a \to N \to 0$$

where $N = \mathrm{Ext}^1_S(Q, \omega_S)$.

Now there are just two things to note. First of all, we know since M is reflexive that $Q_{0,t} = M^*$, and it can then easily be seen that $Q^*_{0,t} = M$. Q^* is obviously a second syzygy of N, so the second thing is to show that N has the required properties. It follows from general results on the Hom and Ext functors that N is graded. Moreover, since $N_{0,t} = \mathrm{Ext}^1_R(M^*, \omega_R)$ and M^* is MCM, it follows that $N_{0,t} = 0$. $\square$

Note that the conclusion of the proposition does include the case of the modules S_i, since free S-modules are of course second syzygies of the zero module.

In the special case where $R = S^{(2)}$ this leaves us with only R, $S_{1,2}$, and $W = (\mathrm{Syz}^2(K))_{0,2}$ as indecomposable MCM modules. In dimension 3, the first two are easily seen not to be linear; but it turns out that the last is. In a similar fashion, one may show the existence of lin MCMs over all Veronese subrings in dimension 3:

Proposition 3.3.4. *Let $R = S^{(t)}$ be the t^{th} Veronese subring of the polynomial ring $S = K[X, Y, Z]$ of dimension 3. Then R has a linear MCM module of rank 2.*

Proof: Let N be the kernel of the free S-module map

$$S(-1)^{t+1} \xrightarrow{A} S^{t-1}$$

defined by the matrix

$$A = \begin{bmatrix} X & Y & Z & 0 & \cdots & 0 & 0 & 0 \\ 0 & X & Y & Z & \cdots & 0 & 0 & 0 \\ & & & \cdots & & & & \\ 0 & 0 & 0 & \cdots & X & Y & Z & 0 \\ 0 & 0 & 0 & \cdots & 0 & X & Y & Z \end{bmatrix}$$

Now set $M = N_{-1,t}$. We will show that M is a lin MCM over R.

The first thing we need is a

Lemma 3.3.5. *$(X, Y, Z)^{t-1}S^{t-1}$ is contained in the image of A.*

Proof: It is easy to see that $I_{t-1}(A)$, the ideal of S generated by the $(t-1)$-sized minors of A, is equal to $(X, Y, Z)^{t-1}$. The lemma now follows from quite general results on matrices. □

Back to proof of Proposition: It follows from the lemma that

$$0 \to M \to S^{(t+1)}_{-2,t} \xrightarrow{A} S^{(t-1)}_{-1,t} \to 0 \tag{3.1}$$

is a short exact sequence of R-modules, from which it follows that M is MCM. Moreover, since $\text{rank}_R S_{i,t} = 1$ for any i, we know that $\text{rank}_R M = 2$, and hence the multiplicity of M is $2e_R = 2t^2$.

Finally, we know that, for any l,

$$\dim_K S_l = \binom{l+2}{l} = \frac{(l+1)(l+2)}{2}.$$

Thus, we have that

$$\dim_K(M_0 = N_{t-1}) = (t+1)\binom{t}{2} - (t-1)\binom{t+1}{2} = 0.$$

There are now two ways of seeing that M is linear. In the first place, we may note that, by the preceding remark, M is generated by forms of degree at least $2t-2$ in S. So $m_R M = m^t M$ is generated by forms of degree at least $3t-2$, all of which must be contained in $(X^t, Y^t, Z^t)S^{(t+1)}_{-2,t}$ (by a simple application of the pigeon-hole principle). But since (3.1) is a short exact sequence of MCM modules, and X^t, Y^t, Z^t is a system of parameters of R, it follows that $m_R M = (X^t, Y^t, Z^t)M$. M is thus seen to be linear.

Alternatively, one may simply calculate that

$$\dim_K M_1 = \dim_K(N_{2t-1}) = (t+1)\cdot\binom{2t}{2} - (t-1)\cdot\binom{2t+1}{2} = 2t^2,$$

whence $\nu(M) \geq e(M)$, and M is linear. $\square$

As in the case of Segre products, the above proof can be adapted to rings which are not themselves regular, but do possess lin MCMs, which have Hilbert functions equal to those of free modules over a regular ring. The proof is essentially the same, so I will omit the details.

Theorem 3.3.6. *Let (S, n) be a 3-dimensional $\mathbb{N}$-graded domain over a field K, generated as a K-algebra by its 1-forms. If S possesses a linear maximal Cohen-Macaulay module M, then any Veronese subring of S also possesses a lin MCM.*

Proof: First, we may replace M by $\mathrm{gr}_n M$, which is a graded lin MCM over S, with all generators in degree 0. Now proceed as before, replacing the ring by M: if $R = S^{(t)}$ define N by the short exact sequence

$$0 \to N \to M^{(t+1)}_{-2,t} \xrightarrow{A} M^{(t-1)}_{-1,t} \to 0,$$

where A is the matrix defined in the proposition (but here X, Y, Z represent a system of parameters of 1-forms in S).

As before, we can calculate that $\mathrm{rank}_R N = 2{\cdot}\mathrm{rank}_S M$, whence $e_R(N) = 2t^2 e_S(M)$. Moreover, as before, N vanishes in degree 0, whereas

$$\dim_K(N_1) = \nu_S(M) \cdot \left[(t+1)\binom{2t}{2} - (t-1)\binom{2t+1}{2}\right] = 2t^2 \cdot \nu_S(M).$$

(By choice of M, one has $\dim_K M_l = \nu(M) \cdot \binom{l+2}{2}$). The Cohen-Macaulayness and linearity of N over R now obviously follow from the same properties of M over S. □

The kind of classification we have been carrying out for graded MCMs over Veronese rings might theoretically be extended to all dimensions, but it quickly becomes complicated and unrevealing. Thus, I will just make a few observations about the case of dimension 4.

As before, if R is the t^{th} Veronese subring of $S = K[W, X, Y, Z]$, and M is a graded MCM over R, we let $Q = (S \otimes_R M^*)^{**}$. Q then has projective dimension at most 2 over S, so we get exact sequences:

$$O \to W \to S^c \to Q \to 0 \tag{3.2}$$

$$O \to S^a \to S^b \to W \to 0 \tag{3.3}$$

Applying the functor $\mathrm{Hom}(-, S(-4))$, this gives new exact sequences:

$$O \to Q^* \to S^c \to W^* \to N_1 \to 0 \tag{3.4}$$

$$O \to W^* \to S^b \to S^a \to N_2 \to 0 \tag{3.5}$$

where $N_1 = \mathrm{Ext}^1(Q, \omega_S)$ and $N_2 = \mathrm{Ext}^1(W, \omega_S) = \mathrm{Ext}^2(Q, \omega_S)$ must vanish in degrees divisible by t, since $Q_{0,t} = M^*$ is MCM. These facts, along with $M = Q^*_{0,t}$, characterize the graded MCMs over R.

The situation is a little more transparent in the special case that $t = 2$. In that case, both N_1 and N_2 must just be finite K-vector spaces killed by the maximal ideal (W, X, Y, Z). It follows from (3.5) that $W^* = S^{(m)} \oplus (\mathrm{Syz}^2 K)^{(n)}$ for some m and n. Then (3.4) implies that Q^* is a first module of syzygies of U for some module $m_S W^* \subseteq U \subseteq W^*$. The following lemma characterizes the submodules U of W with this property.

Lemma 3.3.7. *Let (R, m, K) be a local (or $\mathbb{N}$-graded) ring containing K, and M a finitely generated (graded) R-module. Suppose that one has an R-module U and $n \geq 0$ such that*

$$(mR)^{(n)} \oplus mM \subseteq U \subseteq R^{(n)} \oplus M.$$

Then $U \cong R^{(k)} \oplus (mR)^{(n-k)} \oplus M'$ for some $k \leq n$ and some submodule M' of M with $mM \subseteq M'$.

Proof: Let $M' = M \cap U$. Since $mM \subseteq M'$, we know that $U/(mR^{(n)} + M')$ is a K-vector space of dimension $k \leq n$. Moreover, by applying a K-linear automorphism of $R^{(n)}$, we may assume that a basis of $U/(mR^{(n)} + M')$ is given by the images of elements $\{e_i + w_i : 1 \leq i \leq k\}$ in U, where we think of $R^{(n)}$ as $Re_1 + \cdots + Re_n$, and where $w_i \in M$ for each i. If we let V be the submodule of U generated by $\{e_i + w_i : 1 \leq i \leq k\}$, then it is apparent that V is free of rank n. What we wish to show is that

$$U = V \oplus m(Re_{k+1} + \cdots + Re_n) \oplus M'.$$

First we note that the sum on the right is direct. For a relation would take the form $(v_1 + u_1) + v_2 + u_2 = 0$, where $v_1 \in Re_1 + \ldots Re_k$, $v_2 \in Re_{k+1} + \ldots Re_n$, $u_1, u_2 \in M$, and $u_1 \neq 0$ only if $v_1 \neq 0$. It is then apparent that the relation must be trivial.

Denote the module on the right hand side by U'. Clearly $U' \subseteq U$. Note that $mM \subseteq M' \subseteq U'$; and thus for $i \leq k$, we have $m \cdot Re_i \subseteq U' + m \cdot w_i = U'$. Hence $m(R^{(n)} \oplus M) \subseteq U'$. Finally, it follows from the choices of M' and V that $U/m(R^{(n)} + M) = U'/m(R^{(n)} + M)$. Thus $U = U'$, which proves the lemma. $\square$

Combining the lemma with the preceding discussion gives the following classification of MCM modules over the second Veronese subring of a polynomial ring of dimension four.

Corollary 3.3.8. *Let M be a graded MCM over $R = S^{(2)}$, where $S = K[W, X, Y, Z]$. Then $M \cong Q_{0,2}$ for some S-module*

$$Q \cong S^{(m_1)} \oplus (\mathrm{Syz}_S^2 K)^{(m_2)} \oplus \mathrm{Syz}_S^1(U'),$$

where m_1, m_2, and n are nonnegative integers, and $m_S \cdot (\mathrm{Syz}^2 K)^{(n)} \subseteq U' \subseteq (\mathrm{Syz}^2 K)^{(n)}$.

To a large extent, we already know about the "even" parts of S and $\mathrm{Syz}_S^2 K$, and it is a computation to show that in dimension 4 none of these modules are linear. Thus, in looking for a lin MCM, we might as well restrict our attention to the "new" modules which are the even-degree parts of $\mathrm{Syz}^1(U')$ for $(\mathrm{Syz}^2 K)^{(n)} \subseteq U' \subseteq (\mathrm{Syz}^2 K)^{(n)}$, where the latter is a proper inclusion. As the following proposition shows, it is possible to construct a lin MCM over $R = (K[X, Y, Z, W])^{(2)}$ in this way:

Proposition 3.3.9. *$R = S^{(2)}$ has a linear MCM module, where $S = K[X, Y, Z, W]$ is the polynomial ring in four variables over a field K.*

Proof: We know that $N = \mathrm{Syz}^2_S K$ is generated as an S-module by the six vectors

$$\begin{bmatrix} Y \\ -X \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} Z \\ 0 \\ -X \\ 0 \end{bmatrix}, \begin{bmatrix} W \\ 0 \\ 0 \\ -X \end{bmatrix}, \begin{bmatrix} 0 \\ Z \\ -Y \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ W \\ 0 \\ -Y \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ W \\ -Z \end{bmatrix}$$

in $S^{(4)}$ (which we will denote by $e_1, e_2, \ldots, e_6$, ordered as above). Let U be the submodule generated by $e_1,\ e_2,\ e_3 + e_4,\ e_5,\ e_6$. Since

$$Xe_4 = -Ze_1 + Ye_2, \quad We_4 = Ze_5 - Ye_6$$

$$Ye_3 = We_1 + Xe_5, \text{ and } \ Ze_3 = We_2 + Xe_6,$$

we see that $m_S N \subseteq U$.

Now, if $Q = \mathrm{Syz}^1 U$, we get a short exact sequence:

$$O \to Q \to S(-3)^{(5)} \to U \to 0.$$

I am thinking of generators of N as being in degree 3, since I assume that N is the second module of syzygies of a copy of K in degree 1. The important thing is that the generators of N lie in odd degree.

If $M = Q_{0,2}$, we then see that, since $U_{0,2} = N_{0,2}$ and $\mathrm{rank}(N) = 3$, we have $\mathrm{rank}_R M = 5 - 3 = 2$. Hence $e(M) = 2 \cdot e_R = 16$. Moreover, we know that

$$\dim_K Q_4 = 5 \cdot \nu(m_S) - \nu(m_S N) = 0$$

$$\dim_K Q_6 = 5 \cdot \nu(m^3) - \nu(m^3 N) = 100 - 84 = 16.$$

(The Hilbert function of N can be directly calculated from the exact sequence

$$0 \to N \to S(-2)^{(4)} \to S(-1) \to K \to 0$$

and the Hilbert function of S.) It follows that M needs at least 16 generators, and so M must be linear. $\square$

In the usual spirit of things, I am able to generalize the above result in the following manner:

Proposition 3.3.10. *Let R be a 4-dimensional graded K-algebra generated by 1-forms, and assume that R possesses a linear MCM module M. Then the second Veronese subring of R also has a lin MCM.*

Proof: As usual, we may replace M by $\mathrm{gr}_n M$, and assume that M is graded with all generators in degree 0. We then mimic the proof given above. Assume that M is generated in degree 0, and let W, X, Y, Z be a system of parameters of 1-forms for R. Define the R-module U by the short exact sequence:

$$0 \to U \to M(-1)^{(4)} \overset{[W,X,Y,Z]}{\to} m_R M \to 0.$$

Since M is linear MCM over R, we see that U_{odd}, the $R^{(2)}$-summand of U generated in odd degrees, is MCM over $R^{(2)}$, and that in fact U is none other than the module $\mathrm{Syz}_2^A K \otimes_A M$, where $A = K[W, X, Y, Z]$.

Now just let $U' = V \otimes_A M$, where $V \subseteq \mathrm{Syz}_2^A K$ is the 5-generator submodule used in the proof of Proposition 3.3.9. Since $m_R M = m_A M$, we again have that $m_R U \subseteq U'$, whence $U'_{odd} = U_{odd}$ is MCM over $R^{(2)}$. Now define an R-module Q by the exact sequence:

$$O \to Q \to M^{(5)} \to U' \to 0$$

where the surjection of $M^{(5)}$ onto U' is the obvious one.

Since U'_{odd} is MCM over $R^{(2)}$, we see that Q_{odd} is also MCM over $R^{(2)}$. But, as before, Q_{odd} is generated by forms in $M^{(5)}$ of degree at least 3; and we know, since M is linear, that $m_R^5 M = m_A^5 M \subseteq (W^2, X^2, Y^2, Z^2)M$. Hence $m_R^2 Q_{odd} \subseteq (W^2, X^2, Y^2, Z^2)Q_{odd}$, and we see that Q_{odd} is a lin MCM over $R^{(2)}$ (note that (W^2, X^2, Y^2, Z^2) is a system of parameters for $R^{(2)}$). □

Corollary 3.3.11. *Let $S = K[W, X, Y, Z]$, the polynomial ring in four variables over a field. Then $S^{(2^n)}$ has a lin MCM for any $n \geq 0$.*

3.4 Approximation results for graded rings

So far, I have been unable to resolve the question of existence of linear maximal Cohen-Macaulay modules over Veronese rings in any further cases. But the methods used to prove the existence of linear MCMs over Veronese rings of dimension 3 can be adapted in order to produce vastly more general results. Below we give the most general theorem for graded rings. Although the proof is quite technical, the main ideas may be shortly summarized.

First, by employing a matrix similar to that used in dimension 3, one may show that any Veronese subring of a polynomial ring of dimension d possesses a graded MCM of reduction degree $d - 2$ (I omit the proof, since it is easy to derive from the proof of the 3-dimensional case and the arguments of this section). Secondly, by using a system of parameters of 1-forms, one may produce similar modules over the Veronese subrings of any graded K-algebra R. Little can be said about the actual reduction degrees of these modules, but their behaviour should in some sense approach that of the modules constructed when R is regular. Finally, by employing the Frobenius endomorphism, one may view modules over certain Veronese subrings of R as R-modules via restriction of scalars.

Applications of the theorem will be given in the chapter on Lech's Conjecture.

But the argument is also quite interesting in itself, in that it provides a compelling example of how a property of Veronese subrings of regular rings may be generalized in order to prove the existence of an "approximate" property over a much broader class of positively graded rings.

Theorem 3.4.1. *Suppose that (R, m) is a positively graded K-algebra of dimension $d \geq 3$, generated by its 1-forms, where K is a perfect field of characteristic $p > 0$. Suppose moreover that R possesses a finitely generated graded MCM module M, with generators all in the same degree. Then R possesses a sequence $\{M_i\}$ of MCM modules with reduction degrees approaching $d - 2$.*

Proof: Without loss of generality, we may assume that M is generated in degree 0. We begin by fixing some notation: first, let the Hilbert polynomial of M be given by

$$P_M(t) = (e/(d-1)!)t^{d-1} + kt^{d-2} + \ldots = \dim_K(M_t),$$

where the latter equality holds for t sufficiently large, and $e = e_R(M)$. Next we fix a minimal reduction I of m genterated by a system of parameters of 1-forms, and a positive integer c such that $m^{n+c} = I^n \cdot m^c$ for all $n \geq 0$.

For each $q = p^i$ great enough so that $q > c$ and $H_M(t) = P_M(t)$ for $t \geq q - 2$, we define the module W_i as follows: let

$$N_i = \mathrm{Ker}(M(-1)^{q-c+d-2} \xrightarrow{A} M^{q-c-1}),$$

where $I = (X_1, \ldots, X_d)$ and A is the $(q - c - 1) \times (q - c + d - 2)$ sized matrix:

$$\begin{bmatrix} X_1 & X_2 & \cdots & X_d & 0 & \cdots & 0 & 0 & 0 \\ 0 & X_1 & \cdots & X_{d-1} & X_d & \cdots & 0 & 0 & 0 \\ & & & & \cdots & & & & \\ & & & & \cdots & & & & \\ 0 & 0 & 0 & \cdots & X_1 & X_2 & \cdots & X_d & 0 \\ 0 & 0 & 0 & \cdots & 0 & X_1 & \cdots & X_{d-1} & X_d \end{bmatrix}$$

Now set $W_i = (N_i)_{-1,q}$.

The $R^{(q)}$-module W_i becomes an R-module via F^i, the i^{th} power of the Frobenius endomorphism. Moreover, since $I^{q-c-1}M^{q-c-1}$ is in the image of A, and since $m^{q-1} = I^{q-c-1}m^c$, we see that there is an exact sequence:

$$O \to W_i \to M_{-2,q}^{(q-c+d-2)} \to M_{-1,q}^{(q-c-1)} \to 0$$

induced by A (recall that q must be sufficiently large). In particular, since the latter two modules are MCM over R via F^i, we know that the module W_i is a MCM R-module.

It remains to show that the modules W_i satisfy the stipulated numerical condition. First, since $e_R(M_{f,q}) = q^{d-1}e$ for any q and any $0 \leq f < q$, we see from the short exact sequence above that $e_R(W_i) = e(d-1)q^{d-1}$.

Now, if $W_{i,0} = (N_i)_{q-1}$ is the first (potentially) nonzero graded piece of W_i (and

i is sufficiently large), we may use the short exact sequence to compute:

$$\begin{aligned}\dim_K(W_{i,0}) &= (q-c+d-2)\cdot P_M(q-2)-(q-c-1)\cdot P_M(q-1)\\ &= (q-c+d-2)[(e/(d-1)!)(q-2)^{d-1}+k(q-2)^{d-2}+\dots]\\ &\quad -(q-c-1)[(e/(d-1)!)(q-1)^{d-1}+k(q-1)^{d-2}+\dots]\\ &= q^{d-1}[(e/(d-1)!)(-c+d-2)+(d-1)(e/(d-1)!)(-2)+k\\ &\quad -(e/(d-1)!)(-c-1)-(d-1)(e/(d-1)!)(-1)-k]+\dots.\end{aligned}$$

This shows that $\dim_K(W_{i,0})$ is given by a polynomial $P_0(q)$ in $q = p^i$ of degree no greater than $d-2$. It is easy to see from the above calculation that the degree d term vanishes. Moreover, all contributions to the degree $d-1$ term come from the terms of P_M which are explicitly shown, and it is a simple calculation to show that the the resulting coefficient in degree $d-1$ is equal to 0.

Also, one should note that, for any q sufficiently large, we have

$$(m^{d-1})^q\cdot m^{q-2}\cdot m^c = m^{dq+c-2}\subseteq I^{dq-2}\subseteq I^{[q]}.$$

Thus, $(m^{d-1})^{[q]}\cdot m^{q-2}\cdot M\subseteq I^{[q]}M :_M m^c$. Moreover, note that for any $q=p^i$,

$$l\left(\frac{I^{[q]}M :_M m^c}{I^{[q]}M}\right)\leq r(M)\cdot l(R/m^c),$$

where $r(M)$ is the type of the module M.

We may conclude that the length of $m^{d-1}\cdot(M_{-2,q}^{(q-c+d-2)}/IM_{-2,q}^{(q-c+d-2)})$ is bounded by $\beta\cdot(q-c+d-2)$ for all q, where $\beta = r(M)\cdot l(R/m^c)$ is constant. Note that a similar, but easier, argument shows that $m^d\cdot M_{-2,q}\subseteq IM_{-2,q}$ for $q\geq c$.

Hence, considering the short exact sequence

$$O\to W_i/IW_i\to M_{-2,q}^{(q-c+d-2)}/IM_{-2,q}^{(q-c+d-2)}\to M_{-1,q}^{(q-c+-1)}/IM_{-1,q}^{(q-c-1)}\to 0,$$

we see that

$$l\left(\frac{(m^{d-2}+I)W_i}{IW_i}\right) \leq \nu(m^{d-2}) \cdot \dim_K(W_{i,0}) + \beta \cdot (q-c+d-2),$$

a polynomial in q of degree at most $d-2$. Since the multiplicity of M_i is given by a polynomial of degree $d-1$ in q, this clearly gives the desired result. $\square$

I believe it is worth stating the result in the case $\dim(R) = 3$ separately, in that reduction degree one is equivalent to linearity, and we began with the search for linear MCMs.

Corollary 3.4.2. *Suppose that (R, m) is a 3-dimensional positively graded K-algebra, generated by its 1-forms, where K is a perfect field of characteristic $p > 0$. Then R possesses a sequence of MCM modules M_i with the property that as $i \to \infty$,*

$$\frac{e(M_i)}{\nu(M_i)} \to 1.$$

Proof: If P is a homogeneous minimal prime of R with $\dim(R/P) = 3$, then it clearly suffices to produce such a sequence of modules over R/P. But the theorem 1.5.3 of Hartshorne-Peskine-Szpiro implies that R/P possesses a graded MCM of positive rank. We may now simply apply the theorem with $d = 3$. $\square$

Note 3.4.3. Although the modules W_i constructed in the proof of Theorem 3.4.1 possess a natural grading over the ring (R, m), it is not generally the case that $W_i \cong \mathrm{gr}_m W_i$. However, we may use the exact sequence

$$O \to W_i \to M_{-2,q}^{(q-c+d-2)} \to M_{-1,q}^{(q-c-1)} \to 0$$

in order to calculate the dimension of the second graded piece of W_i, as follows:

$$\begin{aligned}
\dim_K(W_{i,1}) &= (q-c+d-2)\cdot P_M(2q-2)-(q-c-1)\cdot P_M(2q-1) \\
&= (q-c+d-2)[(e/(d-1)!)(2q-2)^{d-1}+k(2q-2)^{d-2}+\ldots] \\
&\quad -(q-c-1)[(e/(d-1)!)(2q-1)^{d-1}+k(2q-1)^{d-2}+\ldots] \\
&= q^{d-1}\cdot 2^{d-2}\cdot(e/(d-2)!)+\ldots
\end{aligned}$$

(i.e. $\dim_K(W_{i,1})$ is polynomial in $q=p^i$ of degree $d-1$, with leading coefficient $2^{d-2}\cdot(e/(d-2)!)$). Note that the degree d term of the polynomial is easily seen to vanish, and that the terms shown are the only ones involved in the calculation of the degree $d-1$ coefficient. The actual value of this coefficient is now given by a simple calculation.

If I is a system of parameters of one-forms for R, then the length of

$$(I+m^2)W_i/m^2W_i$$

must be asymptotic in $q=p^i$ to at least d times this dimension (though not necessarily as great as $d\cdot\nu(W_i)$). This fact will be used in chapter 4.

CHAPTER IV

Lech's Conjecture

4.1 Linear MCM modules and Lech's conjecture

In his paper [12], Christer Lech made the following conjecture on flat extensions of local rings. We say that the homomorphism $(R, m) \hookrightarrow (S, n)$ is flat if S is a flat R-module, and local if the image of m is contained in n.

Conjecture 4.1.1 (Lech). *Let $(R, m) \subseteq (S, n)$ be a flat local extension of Noetherian local rings. Then the multiplicity of S is greater than or equal to the multiplicity of R.*

The proof of the conjecture may be reduced to the case that R and S are complete. Note that, if we then localize S at a prime Q lying over m, we get a new flat local extension $(R, m) \subseteq (S_Q, QS_Q)$, where the rings R and S_Q have the same dimension. The following version of a theorem of [13] then allows us to reduce the original conjecture to the case that R and S have the same dimension. The condition of excellence is quite technical, but holds for most of the rings which we consider. In particular, complete local rings are excellent.

Theorem 4.1.2 (Lech). *Let (R, m) be an excellent local Noetherian ring, and let P be a prime ideal with the property that $height(P) + dim(R/P) = dim(R)$. Then $e(R_P) \leq e(R)$.*

In fact, if (R, m) is a d-dimensional local ring, and if we can show that Lech's conjecture holds for any flat local extension $(R, m) \subseteq (S, n)$ with $\dim(S) = d$, then we can show Lech's conjecture for all flat local extensions $(R, m) \subseteq (S, n)$. For future refererence, we state this formally as:

Lemma 4.1.3. *Let (R, m) be a d-dimensional local ring, and suppose that $e_R \leq e_S$ for any flat local extension $(R, m) \subseteq (S, n)$ with dim$(S) = d$. Then $e_R \leq e_S$ for any flat local extension $(R, m) \subseteq (S, n)$, regardless of the dimension of S.*

Proof: Let $(R, m) \subseteq (S, n)$ be a flat local extension. The completion $\hat{S}$ of S has the same multiplicity as S, and is still a flat extension of R. Thus, we may assume that S is complete (and therefore excellent). Since $\dim(S) = \dim(R) + \dim(S/mS)$ (see e.g. [15], section 15), we may choose a minimal prime P of mS with height$(P) + \dim(S/P) = \dim(S)$. Now $(R, m) \subseteq (S_P, PS_P)$ is a flat local extension of rings of the same dimension d, and we know by Theorem 4.1.2 that $e_{S_P} \leq e_S$. This completes the proof of the lemma. $\square$

As mentioned in the introduction, the most significant cases of the conjecture which have been proved are those in which the base ring R has dimension 2 or when the fibre S/mS is isomorphic to a complete intersection [12, 13].

What we will show in this chapter is that the existence of specialized MCM modules of positive rank for the base ring R sometimes allows a proof of Lech's Conjecture. In particular, the existence of a lin MCM of positive rank over R always proves the conjecture. For if M is a linear MCM module of positive rank for R (in fact, one may reduce to the case that R and S are domains, and then any module has finite rank), we know that

$$e(R) = e_R(M)/\mathrm{rank}_R(M) = \nu_R(M)/\mathrm{rank}_R(M).$$

Likewise,

$$e(S) = e_S(S \otimes M)/\mathrm{rank}_S(S \otimes M) \geq \nu_S(S \otimes M)/\mathrm{rank}_S(S \otimes M)$$

(see the section on background in the introduction). Thus, since minimal numbers of generators and ranks of modules do not change upon tensoring with a flat local extension, we see that $e(S) \geq e(R)$.

Note 4.1.4. For example, the result of Backelin, Herzog, and Ulrich in [1] thus implies that Lech's conjecture holds for any flat local extension $R \subseteq S$ in which the base ring R is a strict complete intersection. (A local ring (R, m) is a strict complete intersection if both R and $\mathrm{gr}_m R$ are complete intersections.)

Of course, even in the case that M is not linear, the above argument shows that

$$e(S) \geq \nu(M)/\mathrm{rank}(M) = e(R) \cdot \frac{\nu(M)}{e_R(M)}.$$

So to prove Lech's Conjecture, it suffices to find a MCM module M such that the ratio of $\nu(M)$ to $e(M)$ is sufficiently close to 1. Combining this with Corollary 3.4.2 immediately yields the following result.

Proposition 4.1.5. *Let (R, m) be a positively graded 3-dimensional algebra over a perfect field K of characteristic $p > 0$, generated by 1-forms. Then $e_R \leq e_S$ for any flat local extension $(R, m) \subseteq (S, n)$.*

Note 4.1.6. If (R, m) is graded with homogeneous maximal ideal m (and (S, n) is either graded or local), we call the extension flat local if $m \hookrightarrow n$ and $R_m \hookrightarrow S_n$ is flat.

In fact, since e_R and e_S are both integers, the conjecture is equivalent to $e_S > e_R - 1$. This is of course completely trivial, but notice that it allows us to put a weaker requirement on the module M. The above formula shows that $e_S > e_R - 1$ if there exists an MCM M of positive rank with

$$\frac{\nu(M)}{e(M)} > 1 - \frac{1}{e_R}.$$

In particular, if (R, m) is a d-dimensional F-finite local Cohen-Macaulay domain of characteristic $p > 0$, with perfect residue field K, then we may consider the MCMs ${}^eR$ for $e > 0$. Denote the Hilbert-Kunz multiplicity of R by c_R. Then $e({}^eR) = e_R q^d$ for all $e > 0$, while $\nu({}^eR)$ is asymptotic in q to $c_R q^d$. Hence,

$$\frac{\nu({}^eR)}{e({}^eR)} \to \frac{c_R}{e_R}$$

as $e \to \infty$. Comparing this with the previous paragraph, we get the following:

Corollary 4.1.7. *Let (R, m) be a d-dimensional F-finite local Cohen-Macaulay domain of characteristic $p > 0$, with perfect residue field K. If $c_R > e_R - 1$, then Lech's conjecture holds for any flat local extension $(R, m) \subseteq (S, n)$.*

Unfortunately, very little is known about Hilbert-Kunz multiplicities in general. The only case in which the above obviously holds is if $e_R = 2$ (it is a theorem that $c_R = 1$ if and only if R is regular; see [16]). So let us record the following:

Question 4.1.8. For which Cohen-Macaulay rings of characteristic $p > 0$ is $c_R > e(R) - 1$, where c_R is the Hilbert-Kunz multiplicity of R?

4.2 On 'embedding dimensions' of modules

The following results were proved by Lech in his paper [13]. Although interesting in its own right, the theorem may also be seen as a first step towards proving the various Lech-Hironaka type inequalities, since the embedding dimension of a ring R is equal to $H_R^{(0)}(1)$, the second value taken by the Hilbert function of R. The main purpose of this section is to generalize the theorem to modules. Although the proof is straightforward, the result given here is a key element in the arguments of the next section, where certain new cases of Lech's conjecture are established.

Theorem 4.2.1 (Lech). *Let (Q,m) be a local ring with m-primary ideal q. Suppose Q/q is equicharacteristic, and that q/q^2 is a free Q/q module. Then the minimum number of generators of q is no greater than the minimum number of generators of m.*

Corollary 4.2.2 (Lech). *Let $(R,m) \subseteq (S,n)$ be a flat couple of d-dimensional local rings. Then $edim(R) \leq edim(S)$.*

Proof: Since S is flat over R, the ideal mS of S requires the same number of generators as m; thus we may consider m as an ideal of S. But, since m/m^2 is a free R/m-module, it follows from the flatness of $R \to S$ that mS/m^2S is free over S/mS. Finally, mS is n-primary, and since $R/m \hookrightarrow S/mS$, S/mS must be equicharacteristic. Thus applying the theorem to S and mS proves the corollary. $\square$

We now wish to prove a similar result, but with R replaced by any finitely generated R-module M and S replaced by $S \otimes_R M$. For now, this will yield a result on linear MCM modules (corollary 4.2.4) and also allow us to deduce some cases of Lech's Conjecture from the existence of MCMs of reduction degree 2 (corollary 4.2.5).

Proposition 4.2.3. *Let $(R,m) \subseteq (S,n)$ be a flat local extension of rings of the same dimension, let M be a finitely generated R-module, and set $M' = S \otimes_R M$.*

Then $\nu(nM') \geq \nu(mM) + (\nu(n) - \nu(m)) \cdot \nu(M)$.

Proof: This is obviously true for $M = R^n$ free, given Lech's result that $\nu(n) \geq \nu(m)$; so it suffices, proceeding inductively, to prove the statement for $N = M/Ry$, $y \in mM$, assuming that it is true for M.

By flatness, $N' = S \otimes_R N = M'/Sy$, where the image of y in M' is in $mM' \subseteq nM'$. If $y \in m^2M$, then $\nu(mN) = \nu(mM)$, and since the image of y is in $m^2M' \subseteq n^2M'$, we also have $\nu(nM') = \nu(nN')$. Hence the proposition holds for N (of course $\nu(M) = \nu(N)$ so the last term in the inequality does not change).

If $y \in mM \setminus m^2M$, then $\nu(mN) = \nu(mM) - 1$, and since the image of y is in $mM' \subseteq nM'$, $\nu(nN') \geq \nu(nM') - 1$. Since $\nu(N) = \nu(M)$, the remaining term does not change, and we see that the inequality continues to hold for N. $\square$

Corollary 4.2.4. *Let* $(R, m) \subseteq (S, n)$ *be a flat local extension of d-dimensional local rings, and let* M *be a finitely generated R-module with the property that* $gr_m M$ *is MCM. If* $S \otimes_R M$ *is a linear MCM-module, then* M *is also a lin MCM, and* $edim(R) = edim(S)$.

Proof: Suppose $M' = S \otimes M$ is linear MCM. By a result of [2], it follows that $\mathrm{gr}_n(M')$ is MCM. Moreover, since minimal numbers of generators and multiplicities are not changed by extending the residue field, we may assume, without loss of generality, that R and S have infinite residue fields.

Now, if M' is linear, we have $nM' = (\underline{y})M'$ for some system of parameters $y_1, \ldots, y_d$ of S, and we see that $\nu(nM') \leq d\nu(M') = d\nu(M)$ (in fact, since $\mathrm{gr}_n(M')$ is MCM, we must have equality). So by Proposition 4.2.3, $\nu(mM) \leq d\nu(M)$, where the inequality is strict unless $\nu(m) = \nu(n)$.

But since $\mathrm{gr}_m M$ is MCM, $\nu(mM) \geq d \cdot \nu(M)$ (if $(x_1, \ldots, x_d)$ is a minimal reduction of m, then the $x_i \in m\backslash m^2$, and their leading forms have only the Koszul relations on M). Thus $\nu(mM) = d\nu(M)$ and $mM = (\underline{x})M$. We conclude that M is linear, and also that $\mathrm{edim}(R) = \mathrm{edim}(S)$. □

Corollary 4.2.5. *Let $(R, m) \subseteq (S, n)$ be a flat couple of local rings. Suppose R has a MCM module M of positive rank, with reduction degree 2 with respect to a minimal reduction $I = (x_1, \ldots, x_d)$ of the maximal ideal. Moreover, assume that $gr_m(M)$ has depth at least $d-2$. Then $e_R \leq e_S$.*

Proof: By Lemma 4.1.3, we may reduce to the case in which R and S have the same dimension, and then $M' = S \otimes M$ is MCM. Since $e_R = e(M)/\mathrm{rank}_R M$ and $e_S = e(M')/\mathrm{rank}_S M'$, and since $\mathrm{rank}_R M = \mathrm{rank}_S M'$, it suffices to show that $e_R(M) \leq e_S(M')$. But because of the assumptions on M, we have:

$$e(M) = l\left(\frac{M}{IM}\right) \leq \nu(M) + \nu(mM) - (d-2)\nu(M),$$

where $d = \dim(R)$ (we may choose the minimal reduction $I = (x_1, \ldots, x_d)$ in such a way that the leading forms of $x_1, \ldots, x_{d-2}$ form a regular sequence on $\mathrm{gr}_m M$). Similarly,

$$e(M') \geq \nu(M') + \nu(nM') - d\nu(M').$$

Since the result is already known in the case that $\nu(n) \leq \nu(m) + 1$ (see [12, 13]), we may assume that the difference of embedding dimesions is at least 2. Then we may apply the proposition to see that

$$e(M') \geq \nu(M) + \nu(mM) - (d-2)\nu(M),$$

and the result now follows from a comparison of the two inequalities. □

Of course, having shown that the embedding dimension of (R, m) must be less than or equal to that of (S, n), one would like to proceed to show that the square of the maximal ideal of R needs no more generators than the square of the maximal ideal of S; or at least that $\nu(m)+\nu(m^2) \leq \nu(n)+\nu(n^2)$. In proving such an assertion, one may as well assume that $m^3 = 0$. Then it suffices to provide a positive answer to one of the following questions, as before.

Question 4.2.6. Let J be an ideal of a local ring (S, m) with $J^3 = 0$, and J/J^2 and J^2 both free S/J-modules. Also assume S/J to be equicharacteristic. Then can you show that $\nu(J^2) \leq \nu(m^2)$, or at least that $\nu(J) + \nu(J^2) \leq \nu(m) + \nu(m^2)$?

4.3 Applications to Lech's conjecture

In this section we will see how the above results can be combined with the existence results of the previous chapter in order to prove some cases of Lech's conjecture. We already know that if R has MCM-modules approaching linearity, then Lech's conjecture holds for any flat extension with base ring R, and that existence of a MCM module with reduction degree 2 also often implies the conjecture. Here we wish to extend these results, obtaining more substantial new results on the conjecture. The main result is the following:

Theorem 4.3.1. *Let (R, m) be a local or $\mathbb{N}$-graded domain, with infinite residue field, and let (S, n) be a flat local extension of R of the same dimension. Suppose that R possesses a MCM module M with $red(M) = 3$, or even a sequence of MCM modules $\{M_i\}$ with reduction degrees approaching 3. If $m \hookrightarrow n^2$, or if $edim(S) - edim(R) + depth(gr_m M_i) \geq dim(R) + 1$ for each M_i, then $e_R \leq e_S$.*

Proof: Let I and J be minimal reductions of m and n, respectively. In the case that R is local, we may reduce to the case that R and S are complete.

For now, just assume that M is a MCM module with reduction degree 3. Recall that, if we let $M^* = \mathrm{Hom}(M, A)$, where A is a regular subring of R over which R is module-finite, then M^* is MCM if and only if M is, and has the same reduction degree as M. Moreover, we know that $\nu(M) = r(M^*)$ and $\nu(M^*) = r(M)$. In particular, by replacing M by M^*, if necessary, we may assume that the minimal number of generators of M is at least as great as its type.

We know that $m^3M \subseteq IM$, whence $m^2M \subseteq IM :_M m$. Thus $l((m^2+I)M/IM) \leq r(M) \leq \nu(M)$. Moreover, if we set $b = \mathrm{depth}(\mathrm{gr}_m M)$, then it follows from the genericity of minimal reductions that we may choose $I = (x_1, \ldots, x_d)$ in such a way that the initial forms of $x_1, \ldots, x_b$ form a regular sequence on $\mathrm{gr}_m M$. Thus

$$l(mM/(I + m^2)M) \leq \nu(mM) - b \cdot \nu(M),$$

and it follows that

$$e_R(M) = l(M/IM) \leq 2\nu(M) + \nu(mM) - (\mathrm{depth}(\mathrm{gr}_m M)) \cdot \nu(M).$$

On the other hand, we have by Proposition 4.2.3 that if $M' = S \otimes_R M$, then $\nu(nM') \geq \nu(mM) + (\nu(n) - \nu(m))\nu(M)$. Hence, just looking at the first two pieces of $\mathrm{gr}_n M'$, we already get the estimate:

$$e_S(M') \geq (1 - d)\nu(M) + \nu(nM') \geq (1 - d + \nu(n) - \nu(m))\nu(M) + \nu(mM).$$

But it follows from our assumptions that

$$\nu(n) - \nu(m) + 1 - d \geq 2 - \mathrm{depth}(\mathrm{gr}_m(M)).$$

Thus, a comparison of the two estimates shows that $e_R(M) \leq e_S(M')$.

Finally, if $m \hookrightarrow n^2$, note that M'/n^2M' is free over S/n^2S, whence

$$e_S(M') = l(M'/JM') \geq (1 + \nu(n) - d) \cdot \nu(M),$$

whereas we have as above that

$$e_R(M) \leq 2\nu(M) + l(mM/(m^2 + I)M) \leq (2 + \nu(m) - d)\nu(M).$$

Since we are free to assume that $\nu(n) - \nu(m) \geq 1$, this again shows that $e_R(M) \leq e_S(M')$; and since $\mathrm{rank}_R M = \mathrm{rank}_S M'$, we may divide by the rank in any of the cases in order to see that $e_R \leq e_S$, as claimed.

Now suppose instead that we have only a sequence of MCMs $\{M_i\}$ with reduction degrees approaching 3. By Proposition 2.2.3, the sequence of modules $\{M_i^*\}$ also has reduction degrees approaching 3. And since M_i has the same rank and multiplicity as M_i^*, it follows that any sequence $\{N_i\}$, where each N_i is either M_i or M_i^*, will have reduction degrees approaching 3. Hence, we are free to replace each M_i by its dual, if necessary, so as to obtain a new sequence of MCMs approaching reduction degree 3, but with the further property that $\nu(M_i) \geq r(M_i)$ for each i. We shall henceforward assume that the original sequence $\{M_i\}$ has this property.

We may again assume that $\nu(n) - \nu(m) \geq 2$, and then the same argument as given above shows that for each i,

$$l\left(\frac{M_i}{(m^2 + I)M_i}\right) + r(M_i) \leq e_S(M_i').$$

Because the M_i have reduction degrees approaching 3, we know that

$$\epsilon_i = l(m^3 \cdot (M_i/IM_i))$$

becomes insignificant compared to the rank of M_i as i increases.

Finally, from the exact sequence

$$0 \to \mathrm{Soc}(M_i/IM_i) \to M_i/IM_i \to (M_i/IM_i)^{(\nu(m))},$$

where the map on the right is given by a vector whose entries are the generators of the maximal ideal, we see that

$$l(m^2 \cdot (M_i/IM_i)) \leq r(M_i) + \nu(m) \cdot \epsilon_i.$$

Thus $e_R(M_i) = l(M_i/IM_i) \leq e_S(M_i') + \nu(m) \cdot \epsilon_i$. Dividing through by $\mathrm{rank}(M_i)$ and taking the limit then shows that $e_R \leq e_S$, as above. $\square$

Note that if (R, m) is an $\mathbb{N}$-graded algebra over a field K, and if the MCM modules M_i are actually graded by powers of m (i.e. $M_i \cong \mathrm{gr}_m M_i$), then we may dispense with the extra hypothesis on embedding dimensions or on the embedding of m into the square of the maximal ideal of S (since Lech has proved the conjecture in the case that $\nu(n) - \nu(m) \leq 1$, we are free to assume that the difference of embedding dimensions is at least 2). Moreover, it is then reasonable to state the conclusion for all flat local extensions of R, since we may use Lemma 4.1.3 in order to reduce to the case of a flat local extension of rings of the same dimension. This gives the following:

Corollary 4.3.2. *Let (R, m) be an $\mathbb{N}$-graded domain, and let (S, n) be a flat local extension of R. Suppose R possesses a MCM module M with $red(M) = 3$, or even a sequence of MCM modules $\{M_i\}$ with reduction degrees approaching 3, and that all of the modules M_i are graded by powers of m. Then $e_R \leq e_S$.*

Moreover, using the existence results of chapter 3, we may obtain substantial new results concerning Lech's conjecture in the case that R is positively graded of characteristic p.

Corollary 4.3.3. *Let R be a positively graded algebra, generated by its 1-forms, over a perfect field K of characteristic $p > 0$. Suppose that R possesses a graded MCM module M of positive rank, with all generators in the same degree, and that* *the dimension of R does not exceed 4. Then Lech's conjecture holds for any flat local extension $(R, m) \subseteq (S, n)$. If the dimension of R is 5, and if we have reduced to the case that dim$(S) = 5$ (as in Lemma 4.1.3), then we still obtain $e_R \leq e_S$, provided that either $m \hookrightarrow n^2$ or edim(S) − edim$(R) \geq 6$.*

Proof: By Theorem 3.4.1, R has, at worst, a sequence of MCMs with reduction degrees approaching $\dim(R) - 2$. Moreover, it follows from Lemma 4.1.3 that we may reduce to the case in which $\dim(S) = \dim(R)$. The conclusion is the same as that of Proposition 4.1.5 in the case that $\dim(R) = 3$, and follows from Theorem 4.3.1 in the case that $\dim(R) = 5$.

If the dimension of R is 4, we can do somewhat better than is indicated by Theorem 4.3.1. For this, note that the modules $\{W_i\}$ constructed in the proof of Theorem 3.4.1 have reduction degrees approaching 2. Moreover, it follows from Note 3.4.3 that $l(I + m^2)W_i/m^2W_i$ is asymptotic in $q = p^i$ to at least

$$4 \cdot (1/2)e_R(W_i) \cdot q^4 \geq 2\nu(W_i) \cdot q^4.$$

Thus, $e_R(W_i) \leq \nu(mW_i) - \nu(W_i)$ (asymptotically in q). Since we may assume $\nu(n) - \nu(m) \geq 2$, we get

$$e_S(W_i') \geq \nu(mW_i) - \nu(W_i),$$

for each i, as in the proof of Theorem 4.3.1. This completes the proof of the corollary. □

In the case that R and S are 3-dimensional rings of prime characteristic p, we may still often obtain MCM modules with reduction degrees approaching 3. An argument similar to that of Theorem 4.3.1 provides some new results on Lech's conjecture in this case, as well (although we obtain slightly better results). Recall that the conjecture was proved by Lech in the case that $\mathrm{edim}(S) - \mathrm{edim}(R) \leq 1$.

Proposition 4.3.4. *Let (R, m) be a local ring of dimension 3 and prime characteristic $p > 0$, with perfect residue field, and suppose that R possesses a finitely generated MCM module N of positive rank. If $(R, m) \subseteq (S, n)$ is a flat local extension of rings of dimension 3, and if either $edim(S) \geq edim(R) + 3$ or else $m \hookrightarrow n^2$, then $e_R \leq e_S$.*

Proof: We may first reduce to the case in which both R and S are complete. In particular, this implies that R is F-finite.

Since $\dim(R) = 3$, we know that the MCM modules ${}^eR$ have reduction degrees approaching 3 (Proposition 2.3.4). As before, one may replace this sequence by one in which the number of generators is always as great as the type.

If $\nu(n) \geq \nu(m) + 3$, then we know by the result of the previous section that for any MCM module M over R, and $M' = S \otimes_R M$, that

$$e_S(M') \geq \nu(M) + \nu(mM).$$

Note that if $M = {}^eN$, then

$$\nu(M) + \nu(mM) = l(N/(m^2)^{[q]}N) \geq l(N/m^{2q}N),$$

and the latter is asyptotic in q to $(4/3)e_R(N) \cdot q^3$. On the other hand, $e_R(M)$ is asymptotic to $e_R(N) \cdot q^3$. We have thus shown that, in fact, $e_S \geq (4/3) \cdot e_R$.

In the case that $m \hookrightarrow n^2$, note that for any MCM module M over R, we have

$$M'/n^2M' \cong (S/n^2)^{\nu(M)}.$$

It follows that

$$e_S(M') \geq (1 + \nu(n) - 3) \cdot \nu(M),$$

whereas

$$l(mM/(I + m^2)M) \leq (\nu(m) - 3) \cdot \nu(M).$$

But by the same argument as for the graded case, it suffices to show that

$$e_S(M') \geq 2\nu(M) + l(mM/(I+m^2)M$$

for any such M. This clearly follows from the two given estimates, provided that $\nu(n) - \nu(m) \geq 1$, and the remaining case was proved by Lech. □

4.4 The reduction to characteristic $p > 0$

In this section I would merely like to note that the results of section 4.3 should be amenable to the process of reduction to characteristic p. Such arguments are generally quite detailed, and the proofs remain to be given. Nevertheless, it appears that the process can be carried out, resulting in the following more general results:

Conjecture 4.4.1. *Let R be a positively graded algebra, generated by its 1-forms over a field K (of any characteristic). Suppose that R possesses a graded MCM module M of positive rank, and that the dimension of R does not exceed 5. Then Lech's conjecture holds for any flat local extension $(R, m) \subseteq (S, n)$.*

Conjecture 4.4.2. *Let (R, m) be a an equicharacteristic local ring of dimension 3, and suppose that R possesses a finitely generated MCM module N of positive rank. If $(R, m) \subseteq (S, n)$ is a flat local extension, and if either* $\mathrm{edim}(S) \geq \mathrm{edim}(R) + 3$ *or else $m \hookrightarrow n^2$, then $e_R \leq e_S$.*

These results are to be proved by showing that if there were a counterexample in which the rings had equal characteristic 0, then a counterexample could be constructed over a field of characteristic $p > 0$.

In the case that $(R, m) \subseteq (S, n)$ is a flat local extension of finitely generated graded algebras over a field K of characteristic 0, the reduction should not present great difficulties. We should be able to replace the field K by a finitely generated $\mathbb{Z}$-algebra $A \subseteq K$, and R, S, and a MCM R-module M by finitely generated A-algebras R_A and S_A and a finitely generated R_A-module M_A in such a way that:

- R_A, M_A, and S_A are all A-free; and $K \otimes_A R_A \cong R$, $K \otimes_A S_A \cong S$, and $K \otimes_A M_A \cong M$.
- S_A is free over R_A, and M_A is free over $A[x_1, \ldots, x_d]$, where $x_1, \ldots, x_d$ is a homogeneous system of parameters of R with coefficients in A.
- For any residue field κ of A, $M_\kappa = \kappa \otimes_A M_A$ has the same rank over $R_\kappa = \kappa \otimes_A R$ as M has over R.
- For any such κ, R_κ and S_κ have the same multiplicities as R and S, respectively.

Given a counterexample to conjecture 1, this would produce a new counterexample in which the field K is finite, hence perfect of positive characteristic. Since we have already proved the theorem in this case, we would thus have a proof in characteristic 0, as well.

In the case that either or both of the rings R and S fails to be affine over K, it will be necessary to first apply the theory of approximation rings in order to reduce to the case of affine algebras. We may reduce to the case that R and S are complete, and then R is module-finite over a power series ring T. Expressing all of the relevant properties by equations over T, we may hope to descend the counterexample to one in which the rings R and S are module-finite over a regular affine subring of T. Then we may proceed as above to produce a counterexample over a field of positive characteristic p.

CHAPTER V

Hilbert-Kunz multiplicities and Lech's Conjecture

5.1 Basic Applications of the Hilbert-Kunz multiplicity

In the paper [12], Christer Lech proved the following result, which gives an approximation to his conjecture on the multiplicities of rings under a flat local homomorphism.

Proposition 5.1.1. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of rings of dimension d. Then $e_R \leq d! \cdot e_S$, where e_R and e_S stand for the ordinary multiplicities of the respective rings.*

What I would like to note is that if the rings have prime characteristic $p > 0$, and if we adopt some more recent terminology, then the proof may essentially be broken into two pieces. First, what Lech shows is that $e_S \geq c_R$, the Hilbert-Kunz multiplicity of R. Secondly, it is easy to show that for any R, we have $c_R \leq e_R \leq d! \cdot c_R$. It then follows that $e_R \leq d! \cdot e_S$.

Now, if R is an F-finite Cohen-Macaulay local domain with perfect residue field, we may give a short proof of the inequality $e_S \geq c_R$. To do this, simply consider the MCM modules ${}^eR$ over R, which for large e have rank equal to q^d, and whose numbers of generators is asymptotic in q to $c_R q^d$ (where $q = p^e$). Clearly now

$$e_S q^d = e(S \otimes {}^eR) \geq \nu({}^eR) \approx c_R q^d,$$

and dividing through by the rank gives the result.

Before moving on to prove some results on Hilbert-Kunz multiplicities in the next section, I would like to give a further application of this line of reasoning. First we need to formally state the following:

Lemma 5.1.2. *Let $(R, m) \subseteq (S, n)$ be a flat couple of local rings of the same dimension. Let J be a parameter ideal of S, let M be a MCM module over R, and set $M' = S \otimes_R M$. Then $e(J; M') \geq l(S/(mS + J)) \cdot \nu(M)$. In particular, if J is a minimal reduction of n, then we have $e(M') \geq l(S/(mS + J)) \cdot \nu(M)$.*

Proof: Clearly $e(J; M') = l(M'/JM') \geq l(M'/(m + J)M')$. But since M' is tensored up from R, we know that $M'/mM' \cong (S/mS)^{(\nu(M))}$. Thus $l(M'/(m+J)M') = l(S/(mS + J)) \cdot \nu(M)$, and the lemma is proved. □

In particular, suppose that (R, m) is a d-dimensional F-finite ring of positive prime characteristic p, with perfect residue field. If M is a MCM module of positive rank, then we may apply the lemma to the modules ${}^eM$, which have $\mathrm{rank}_R({}^eM) = q^d \cdot \mathrm{rank}_R(M)$ and $\nu({}^eM) \approx c_R q^d \cdot \mathrm{rank}(M)$. This gives the stronger result that $e_S \geq l(S/(mS + J)) \cdot c_R$ for any flat local extension S of dimension d, which implies that

$$e_S \geq \frac{l(S/(mS + J))}{d!} \cdot e_R.$$

This obviously gives some new cases of Lech's conjecture:

Proposition 5.1.3. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of local rings of positive prime characteristic p and Krull dimension d, with R/m perfect, and assume that R possesses a MCM module M of positive rank. If $l(S/(mS+J)) \geq d!$ for some minimal reduction J of n, then $e_S \geq e_R$. In particular, if $edim(S) - edim(R) \geq$*

$d! + d - 1$, then $e_S \geq e_R$.

The proof follows immediately from Lemma 5.1.2 and a reduction to the case that R is complete and has perfect residue field. Of course, it is trivial that, given the ring R, there exists some number a such that any flat local extension S with $l(S/(mS+J)) \geq a$ will have multiplicity greater than or equal to that of R (for example, one might just choose $a = e_R$). What is interesting about the proposition is that it gives a uniform constant for all rings of a given dimension.

In a similar vein, we would like to say that if the maximal ideal of R embeds into a high power of the maximal ideal of S, then the multiplicity of S must be greater than or equal to that of R. Some such statement is made possible by the following:

Lemma 5.1.4. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of Cohen-Macaulay rings, and assume that R is not regular. Then mS is not contained in any parameter ideal of S.*

Proof: Let J be a parameter ideal of S, and choose a non-free MCM module M over R of positive rank (a sufficiently high syzygy module of the residue field will do). Since S is Cohen-Macaulay and flat over R, we know that $M' = S \otimes_R M$ is MCM of positive rank (see e.g. [15], section 23), and is not free over S. As above, we see that M'/mM' is free of rank $\nu(M)$ over S/mS. Hence $e(J; M') \geq l(S/(mS+J)) \cdot \nu(M)$.

Now, because M is not free, we know that $e(J; M') < e(J; S) \cdot \nu(M)$. Thus, if it were the case that $mS \subseteq J$, we would have

$$e(J; M') \geq l(S/JS) \cdot \nu(M) > e(J; M'),$$

a contradiction. $\square$

In the case that R is Cohen-Macaulay, the lemma is yet another generalization of the statement that R is regular if any flat local extension is regular. Moreover, we now have the sort of result we were looking for with regard to Lech's conjecture (although the estimate is very rough), namely:

Proposition 5.1.5. *If $(R, m) \subseteq (S, n)$ is a flat couple of d-dimensional Cohen-Macaulay local rings of prime characteristic $p > 0$, with R/m perfect, and if m embeds into $n^{d!}$, then $e_R \leq e_S$.*

Proof: By Proposition 5.1.3, we need only show that $l(S/(mS+J)) \geq d!$, where J is a minimal reduction of n. But by Lemma 5.1.4, we have that mS is not contained in J (we may certainly concentrate on the case where R is not regular), which implies that $n^{d!}$ is not contained in J. Thus $l(S/(mS+J)) \geq d!$ (a very crude estimate indeed!), and we see that

$$e_S \geq d! \cdot c_R \geq e_R. \ \square$$

5.2 Inequalities on Hilbert-Kunz multiplicities

We now know, for a flat local extension $R \subseteq S$ of rings of characteristic $p > 0$, that $e_S \geq c_S$, $e_R \geq c_R$, and $e_S \geq c_R$. Moreover, it is conjectured that $e_S \geq e_R$. So the only question left to ask about the ordering of the four invariants is whether $c_S \geq c_R$. In other words, can we prove the Lech-type conjecture with ordinary multiplicity replaced by Hilbert-Kunz multiplicity?

The answer turns out to be positive; in fact, one may more or less follow Lech's program for proving the same results about ordinary multiplicities, developed in [12] and [13]. The step which proved intractable before was to prove the inequality on multiplicities for a flat local extension of rings of the same dimension. But if we work with Hilbert-Kunz multiplicities instead, this statement may be proved as follows.

Proposition 5.2.1. *Let $(R, m) \subseteq (S, n)$ be a flat local extension of rings of the same dimension d, and assume that the rings have prime characteristic $p > 0$. Then $c_R \leq c_S$. In fact, for any $q = p^e$, we have $l(R/m^{[q]}) \leq l(S/n^{[q]})$.*

Proof: Set $a = l_S(S/mS)$, which is finite since R and S have the same dimension. For any ideal I of R, we then know that $l(S/IS) = a \cdot l(R/I)$; in particular, $l(S/m^{[q]}S) = a \cdot l(R/m^{[q]})$ for any $q = p^e$.

Now consider a composition series

$$mS = I_0 \subseteq I_1 \subseteq \ldots \subseteq I_{a-1} = n \subseteq I_a = S$$

(where $I_{j+1}/I_j \cong S/n$ for each j). When we apply the Frobenius functor to this series, we get the new series

$$m^{[q]}S = I_0^{[q]} \subseteq I_1^{[q]} \subseteq \ldots \subseteq I_{a-1}^{[q]} = n^{[q]} \subseteq S.$$

All we now need to note is that each quotient $I_{j+1}^{[q]}/I_j^{[q]}$ still needs only one generator as an S-module, and is killed by $n^{[q]}$. Thus $l(S/m^{[q]}S) \leq a \cdot l(S/n^{[q]})$.

Putting together the conclusions of the previous two paragraphs, we see that

$$l(R/m^{[q]}) \leq l(S/n^{[q]})$$

for any $q = p^e$, as claimed. $\square$

Now suppose that the flat extension ring S has dimension greater than that of R. If we choose a prime P of S which is minimal over mS, then we get a new flat extension $(R, m) \subseteq (S_P, PS_P)$ of rings of the same dimension, and we may conclude that $c_R \leq c_{S_P}$. Moreover, we may choose P in such a way that height$(P)+$ dim$(R/P) = $ dim(S) (see e.g. [15], section 15). So in order to prove that $c_R \leq c_S$, it would suffice to prove that for a prime P of S with height$(P)+$dim$(R/P) = $ dim(S), we have $c_{S_P} \leq c_S$. Lech was able to prove the corresponding theorem for ordinary multiplicities, with only mild restrictions on the ring, and we may deduce the result for Hilbert-Kunz multiplicities by a similar sequence of arguments (but in our case we achieve full generality!).

Theorem 5.2.2. *Let (R, m) be a Noetherian local ring of characteristic $p > 0$, and let P be a prime ideal of R such that height(P) + dim(R/P) = dim(R). Then $c_{R_P} \leq c_R$. In fact, if $t =$ dim(R/P), then $l(R/m^{[q]}) \geq q^t \cdot l(R_P/P^{[q]}R_P)$ for every $q = p^e$.*

It is clear that the theorem follows by induction, if we prove it in the case where height(P) = dim$(R) - 1$, so from now on we will assume this to be the case. In following Lech's program, we will begin with the following simple, but fundamental case. In fact, this is where the proof of the theorem on localization most differs from the one given for ordinary multiplicities.

Lemma 5.2.3. *Let R and P be as in the theorem, and assume in addition that $m = P + (f)$ for some $f \in R$. Then $c_{R_P} \leq c_R$. In fact, for any $q = p^e$, we have $l(R/m^{[q]}) \geq q \cdot l(R_P/P^{[q]}R_P)$.*

Proof: To begin with, let us set $P^{\{q\}} = P^{[q]}R_P \cap R$. Since $m^{[q]} = P^{[q]} + (f^q)$, and since $P^{[q]} \subseteq P^{\{q\}}$, we have $l(R/m^{[q]}) \geq l(R/(P^{\{q\}} + f^q))$. Moreover, since f is a nonzerodivisor mod $P^{\{q\}}$, it is clear that $l(R/(P^{\{q\}}+f^q)) = q \cdot l(R/(P^{\{q\}}+f))$. Thus it is sufficient to show that $l(R/(P^{\{q\}} + f)) \geq l(R_P/P^{[q]}R_P)$.

In showing this, we may without loss of generatlity pass to the ring $S = R/P^{\{q\}}$.

Now the claim is that $l(S/fS) \geq l(S_P)$. But since f is a nonzerodivisor in S, and since P is the unique minimal prime of S, we have that

$$l(S/fS) \geq e_S = e(S/PS) \cdot l(S_P)$$

by the additivity formula for multiplicities. All that remains is to note that, by hypothesis, $S/P = R/P$ is a DVR, and so $e(S/PS) = 1$. This completes the proof of the lemma. $\square$

The condition that R/P be a DVR is equivalent to the condition that R/P is normal. This is not true in general, but we will adapt Lech's reduction to this case by using the module-finiteness of the integral closure $(R/P)'$ over R/P. The difference here is that, since we already have the proposition on flat local extensions of the same dimension, this need not be stated as an assumption.

Lemma 5.2.4. *The proof of the theorem may be reduced to the case in which the integral closure $(R/P)'$ of R/P is module-finite over R/P.*

Proof: Let $\hat{R}$ denote the completion of R, and let P^* be a minimal prime of $P\hat{R}$ with $\dim(\hat{R}/P^*) = \dim(\hat{R}/P\hat{R})$. It is clear that R and $\hat{R}$ have the same Hilbert-Kunz functions; and since $R_P \subseteq \hat{R}_{P^*}$ is a flat local extension of rings of the same dimension, we have by the proposition that

$$l(\hat{R}_{P^*}/(P^*)^{[q]}) \geq l(R_P/P^{[q]}R_P)$$

for every $q = p^e$. Thus it suffices to prove the theorem for $\hat{R}$ and P^*, and we may assume the R is complete local.

But then it is a well-known fact that any homomorphic image domain of R has integral closure which is finitely generated as a module. Hence we may reduce to this case. □

As in the proof for ordinary multiplicities, we also need the following preliminary lemma:

Lemma 5.2.5. *Let R be a Noetherian ring of characteristic p, and let M and m be prime ideals of the polynomial extension $R[z]$ and R, respectively, such that $M \cap R = m$. Then for any $q = p^e$, we have*

$$l\left(\frac{R[z]_M}{M^{[q]}R[z]_M}\right) = l\left(\frac{R_m}{m^{[q]}R_m}\right)$$

if $M = mR[z]$; and otherwise

$$l\left(\frac{R[z]_M}{M^{[q]}R[z]_M}\right) = q \cdot l\left(\frac{R_m}{m^{[q]}R_m}\right).$$

Proof: We may as well assume from the beginning that (R, m) is local; let us also set $(S, n) = (R[z]_M, MR[z]_M)$. In the case that $M = mR[z]$, $R \subseteq S$ is a flat local extension with $n = mS$. Hence, for any q, we have

$$l(S/n^{[q]}) = l(S/m^{[q]}S) = l(S/mS) \cdot l(R/m^{[q]}) = l(R/m^{[q]}).$$

So now assume $M \neq mR[z]$. Then we must have $M = mR[z] + (f)$ for some monic polynomial $f \in R[z]$.

Now, $R[f]$ is also isomorphic to a polynomial ring over R, and the length of $(m+f)^{[q]}$ in $R[f]$ is $q \cdot l(R/m^{[q]})$. Moreover, $R[z]$ is still flat over $R[f]$, and $M = (m+f)R[z]$; so it follows as in the first case that

$$l\left(\frac{S}{n^{[q]}}\right) = l\left(\frac{R[f]}{(m+f)^{[q]}}\right) = q \cdot l\left(\frac{R}{m^{[q]}}\right),$$

as desired. □

Proof of Theorem 5.2.2:

Recall that we are now assuming $\dim(R/P) = 1$, and that the normalization $(R/P)'$ of R/P is module-finite over R/P. Set $(R/P)' = (R/P)[c_1, \ldots, c_j]$, and consider the composition of surjective homomorphisms

$$R[z_1, \ldots, z_j] \to (R/P)[z_1, \ldots, z_j] \to (R/P)'.$$

If we let P^* and M^* denote the inverse images in $R[z_1, \ldots, z_j]$ of the (0) ideal and an arbitrary maximal ideal M in $(R/P)'$, then we immediately see that $M^* \cap R = m$, $P^* \cap R = P$, and $R[z_1, \ldots, z_j]_{M^*}/P^* R[z_1, \ldots, z_j]_{M^*}$ is a DVR.

Now we know the result for P^*, M^*, and $R[z_1, \ldots, z_j]$; and by Lemma 5.2.5, we have that $c_R = c(R[z_1, \ldots, z_j]_{M^*})$ and $c_{R_P} = c(R[z_1, \ldots, z_j]_{P^*})$. Thus we have completed the proof that $c_{R_P} \leq c_R$.

In fact, applying the lemma inductively shows that there exist positive integers s and t such that for any $q = p^e$,

$$q^s \cdot l(R/m^{[q]}) = l(R[\underline{z}]/(M^*)^{[q]}) \geq q \cdot l(R[\underline{z}]_{P^*}/(P^*)^{[q]}) = q^{t+1} \cdot l(R_P/P^{[q]}R_P),$$

where s and t are each at most j. A consideration of the dimensions of the rings involved implies that $s \geq t$, so to complete the proof it suffices to show that $t = j$.

But note that, for every $1 \leq i \leq j$, there are nonzero elements a_i and b_i in R/P such that $a_i c_i = b_i$. Hence, there exist elements x_i and y_i in R, with x_i not in P, such that $x_i z_i - y_i \in P^*$. It follows that $P^* \cap R[z_1, \ldots, z_i]$ is for no i generated by $P^* \cap R[z_1, \ldots, z_{i-1}]$. Thus, it follows from Lemma 5.2.5 that $t = j$, and we may divide by q^j above to see that

$$l(S/m^{[q]}) \geq q \cdot l(R_P/P^{[q]}R_P)$$

for every q. $\square$

Of course, this completes the proof of the theorem on flat extensions, as well. We may now record the theorem in its full generality:

Theorem 5.2.6. *Let* $(R, m) \subseteq (S, n)$ *be a flat local extension of rings of positive prime characteristic, where* $\dim(S) - \dim(R) = t$*. Then* $c_R \leq c_S$*; moreover, for any* $q = p^e$*, it is in fact the case that* $q^t \cdot l(R/m^{[q]}) \leq l(S/n^{[q]})$.

This result is not only more easily proved than Lech's conjecture, but also has a significantly stronger conclusion. It should serve as a poignant example of the power of characteristic p techniques.

CHAPTER VI

Splitting Results and existence of small Cohen-Macaulay modules

6.1 More special conditions on MCM modules in characteristic $p > 0$

In this section we will show how to use splitting arguments over a ring of positive prime characteristic p in order to generate MCM modules with certain special properties. The proofs given here do rely heavily upon characteristic p methods, but some consideration will be given at the end of the chapter to what can be done in equal characteristic 0, or in the non-graded case.

Recall the theorem 1.5.3 Hartshorne-Peskine-Szpiro, which produced MCM modules over certain graded rings of characteristic $p > 0$. The crux of the argument was that lower local cohomology modules $H^i_m({}^eM)$ had bounded lengths for all e. Hence, for large enough e, one of the direct summands of ${}^eM$ must have vanishing i^{th} local cohomology. The same sort of argument will be applied here in order to produce modules with other nice properties.

First, even for a finitely generated graded maximal Cohen-Macaulay module M over R, it is not true that $H^d_m(M)$ has finite length for $d = \dim(R)$. But it is true, since the module $H^d_m(M)$ is Artinian, that the part of this module in nonnegative degrees must have finite length. Thus, we may introduce the concept of the *a-invariant* of a finitely generated graded R-module M. The definition given here generalizes the notion of the a-invariant of the ring R.

Note 6.1.1. Let R be a finitely generated positively graded K-algebra, where $R_0 = K$ and $\dim(R) = d$. Recall that the a-invariant of R is given by $a(R) = \sup\{a : [H^d_m(R)]_a \neq 0\}$ (see [6]). Also, if R is Cohen-Macaulay, $x_1, \ldots, x_n$ is a homogeneous system of parameters, and $I = (x_1, \ldots, x_n)$; then $a(R) = deg(G) - \sum deg(x_i)$, where G is a form of largest degree in $R \setminus IR$ (see e.g. [9]).

Definition 6.1.2. For R as above, and M a finitely generated graded R-module, the a-invariant of M is given by $a(M) = \sup\{a : [H^d_m(M)]_a \neq 0\} - \beta(M)$, where $\beta(M) = \min\{b : M(b) \neq 0\}$.

As for the ring R, one can show that if M is maximal Cohen-Macaulay and $I = (x_1, \ldots, x_d)$ is a parameter ideal, then $a(M) + \beta(M) = \deg(G) - \sum \deg(x_i)$, where G is a homogeneous element of $M \setminus IM$ of largest degree. Also note that if we replace M by a twist so that its generator of least degree is in degree 0, then the a-invariant of M is just the maximal degree in which $H^d_m(M)$ fails to vanish.

If the ring R is generated over a field by 1-forms, and the module M is MCM with all its generators in the same degree, then the above notion is really no different from that of the reduction degree of the module M. In fact, one has $a(M)+d+1 = \mathrm{red}(M)$, where d is the dimension of the ring. To see this, note that neither side of the equality is changed by replacing M by a twist which is generated in degree 0. Then if $I \subseteq R$ is generated by a system of parameters of 1-forms, and if G is a homogeneous element of $M \setminus IM$ of maximal degree, we have

$$a(M) + d = \deg(G) = red(M) - 1.$$

In particular, M is linear if and only if $a(M) = -d$. Moreover, in this case, the following theorem has already been proved in chapter 1, since $\mathrm{red}(M) \leq d$ if and only if $a(M) < 0$. Nevertheless, for the present section, the notion of a-invariant will still be the better one with which to work.

Theorem 6.1.3. *Let (R, m) be a finitely generated positively graded equidimensional K-algebra, with K a perfect field of characteristic $p > 0$. Suppose R has a graded module M, of the same dimension, which is Cohen-Macaulay except possibly at the origin (i.e. M_P is MCM over R_P for any prime $P \neq m$). Then R has a MCM module M with a-invariant $a(M) < 0$.*

Proof: By Theorem 1.5.3, R possesses a finitely generated graded MCM module N. Without loss of generality, we may replace N by a suitable twist and assume that $N_t = 0$ for $t < 0$.

We know that $H^d_m({}^eN) \cong {}^eH^d_m(N)$ for any $e \geq 0$, and it is easy to see that the grading on $H^d_m({}^eN)$ is obtained from that on $H^d_m(N)$ by dividing all degrees by q.

Thus, we must also have equality of the nonnegative part of the highest local cohomology for all e, i.e. $[H^d_m({}^eN)]_{t\geq 0} = [{}^e(H^d_m(N))]_{t\geq 0}$. If follows that the nonnegative part of the dth local cohomology of ${}^eM$ has fixed finite K-dimension $\gamma = \dim_K[H^d_m(N)]_{t\geq 0}$ for all e. For e large enough, ${}^eN$ will split into more than γ direct summands. Since the operation $[H^d_m(\_)]_{t\geq 0}$ commutes with direct summands, we will therefore be able to find a MCM summand N' of ${}^eN$ with $[H^d_m(N')]_{t\geq 0} = 0$. Since ${}^eN$ is still 0 in negative degrees, the same will be true of N', and thus $a(N') < 0$.

□

The above theorem will be applied in section 6.2 to prove a new case of the conjecture on the existence of small Cohen-Macaulay modules. It turns out that the condition $a(M) < 0$ is precisely what is needed in order to ensure that the Segre product of two MCM modules remains Cohen-Macaulay.

But first I wish to note that the same argument can be used in some cases to produce MCMs upon which the action of an ideal becomes indistinguishable from that of its tight closure. Recall that, in the case that an F-finite Cohen-Macaulay local (or positively graded) ring (R, m) has its maximal ideal equal to the Frobenius closure of a parameter ideal, the modules ${}^eR$ are in fact lin MCMs for $e >> 0$ (Lemma 2.4.2). Moreover, the same proof shows that for such a ring R and for any ideal I, one can find a MCM module M for R such that $IM = I^F M$. In the graded case, if we assume a sufficient abundance of *test elements*, we may obtain similar results with regard to tight closures of ideals.

Proposition 6.1.4. *Let (R, m) be an F-finite positively graded Cohen-Macaulay K-algebra, where K is a perfect field of characteristic $p > 0$. Suppose that R has an m-primary ideal of test elements I (in particular, this is the case if R has isolated non-Gorenstein and non-F-regular locus). Then for any finite set of ideals $\{J_i\}$ of R, there exists a MCM-module M over R such that $J_i^* M = J_i M$ for each i.*

Proof: Given an ideal J, set $s = \nu(J^*)$, the minimal number of generators of the tight closure ideal J^*. For any $c \in I$, we know that $c(J^*)^{[q]} \subseteq J^{[q]}$ for all $q = p^e$. Thus $I(J^*)^{[q]} \subseteq J^{[q]}$ for any $q = p^e$ and any ideal J.

Thus, for any $e \geq 0$, $J^*({}^eR)/J({}^eR) \cong (J^*)^{[q]}/J^{[q]}$ has length less than or equal to $l(R/I) \cdot s = b$, since this module is killed by I and needs at most as many generators as J^*. Now, if $q = p^e$ is chosen large enough so that ${}^eR$ splits into more than b direct summands, then at least one summand will be a MCM module M such that $J^*M = JM$.

Clearly the same method can be used to get a MCM module on which finitely many ideals become equal to their tight closures: we just need to take e large enough so that the number of direct summands of ${}^eR$ is larger than a sum of finitely many constants b_i. The details are omitted. □

Corollary 6.1.5. *If R satisfies the hypotheses of the proposition, and if the homogeneous maximal ideal m is equal to the tight closure I^* of some parameter ideal I, then R has a linear MCM module.*

Finally, we would like to show how a weaker requirement on the ideal of test elements suffices for rings with multi-gradings. The point is that if I is an ideal of test elements with $\dim(R/I) = r$, then for large q, the modules $(J^*)^{[q]}/J^{[q]}$ are killed by I, and hence can be thought of as R/I-modules. It follows that their lengths should eventually be bounded by a poynomial function of degree r in q. But if R has a nontrivial s-multigrading, then the modules ${}^eR$ will split into roughly q^s direct summands. As long as $s > r$, we should be able to get the same conclusion as in the proposition above. We do need to be careful about the hypotheses.

Proposition 6.1.6. *Let R be an F-finite Cohen-Macaulay K-algebra, where K is a perfect field of characteristic $p > 0$, and suppose that R has a nondegenerate multigrading by s copies of the natural numbers. Moreover, suppose that R has an ideal of test elements I with $\dim(R/I) = r < s$. Then for any finite set $\{J_i\}$ of ideals of R with the property that $J_i + I$ is primary to the homogeneous maximal ideal m for each i, there exists a MCM-module M for R such that $J_i^*M = J_iM$ for each i.*

Proof: One can use the multe-grading to see that for large e, the module ${}^eR$ will split into at least aq^s nonzero MCM direct summands, where a is some positive constant. All that really concerns us is that, for any polynomial function F of degree less than s in q, ${}^eR$ will have more than $F(q)$ direct summands for large enough e.

Now let J be an ideal of R such that $I + J$ is m-primary, and let $h = \nu(J^*)$. Then for any e, the module $W_e = J^*({}^eR)/J({}^eR) \cong (J^*)^{[q]}/J^{[q]}$ is killed by $I + J^{[q]}$

and needs at most h generators. Since $\dim(R/I) = r$ and $(J + I)/I$ is m-primary in R/I, it follows from general results on Hilbert-Kunz functions that for e sufficiently large the length of W_e is bounded by a polynomial function of degree r in $q = p^e$.

Thus, ${}^eR$ eventually has a MCM summand M such that $J^*M = JM$, and it is clear how to modify the argument in order to handle a finite set of ideals $\{J_i\}$. $\square$

6.2 Small MCM modules over Segre product rings

As alluded to in the introduction to this chapter, the existence of MCMs with negative a-invariant will allow us to prove the existence of small Cohen-Macaulay modules over certain Segre products of graded rings. The Segre product is defined as follows:

Definition 6.2.1. Let R and S be positively graded algebras over a a field K, with $R_0 = S_0 = K$. Then the Segre product ring $R \otimes_{seg} S$ is the positively graded K-subalgebra of $R \otimes_K S$ with graded pieces $(R \otimes_K S)_t = R_t \otimes_K S_t$ for all $t \geq 0$.

If R and S are the homogeneous coordinate rings of projective varieties X and Y over K, then $R \otimes_{seg} S$ is the homogeneous coordinate ring of the Segre embedding of the product variety $X \times Y$. It is well-known that the product of Cohen-Macaulay projective varieties remains Cohen-Macaulay; but even if the corresponding coordinate rings are Cohen-Macaulay, the Segre product may not be. Nevertheless, if $R_1, \ldots, R_n$ are positively graded rings which possess small (graded) MCM modules, or are themselves Cohen-Macaulay, we may ask whether the Segre product $R_1 \otimes_{seg} \cdots \otimes_{seg} R_n$ possesses a small MCM module.

A partial answer to this question was given by Frank Ma in [14]. His result is:

Proposition 6.2.2 (Ma). *Let R be the coordinate ring of $C_1 \times C_2 \times \cdots \times C_n$, where* *each C_i is a smooth projective curve over an algebraically closed field k. Then R has a finitely generated maximal Cohen-Macaulay module.*

Given finitely generated graded modules M_i over the coordinate rings R_i, one may form the Segre product $M_1 \otimes_{seg} \cdots \otimes_{seg} M_n$ in the analogous way, and it is easy to see that this is a finitely generated graded module over the Segre product ring $R_1 \otimes_{seg} \cdots \otimes_{seg} R_n$. What Ma shows is that if the M_i are chosen to be suitably nice MCM modules, then the Segre product module is MCM over the Segre product ring. In the language of this paper, the relevant property of the M_i turns out to be that they have a-invariant less than 0. The following result can then be easily derived from the work [6], and much of Ma's proof is incorporated into the proof given here.

Theorem 6.2.3. *Let $R = R_1 \otimes_{seg} R_2 \cdots \otimes_{seg} R_n$ be a Segre product of finitely generated positively graded rings R_i over a field K, and assume that each of the rings R_i has dimension at least 2. If, for each i, R_i has a graded MCM-module M_i with $a(M_i) < 0$, then R possesses a (small) graded MCM module.*

Proof: Let m_i be the homogeneous maximal ideal of the corresponding ring R_i for each i. Note that, by suitably twisting M_i, we may assume that $[M_i]_{t<0} = 0$, and that $[H^d_{m_i}(M_i)]_t = 0$ for $t \geq 0$. Now just let $M = M_1 \otimes_{seg} \cdots \otimes_{seg} M_n$ be the Segre product of the modules M_i. We will show that M is a MCM module for R.

For each i, let $X_i = \mathrm{Proj}(R_i)$, and let $\tilde{M}_i$ be the sheaf associated to M_i on X_i. Since M_i is MCM of depth at least 2 over R_i, we know that $M_i \cong \oplus_{t\in\mathbb{Z}} H^0(X_i, \tilde{M}_i(t))$; and that for $j \geq 1$, $H^{j+1}_{m_i}(M_i) = \oplus_{t\in\mathbb{Z}} H^j(X_i, \tilde{M}_i(t))$. Now set $d = \dim(R) = (\sum \dim(R_i) - 1) + 1$, and let m represent the homogeneous maximal ideal of R. What we need to show is that $H^i_m(M) = 0$ for $i < d$. In order to do this, we will apply the Kunneth formula (which holds for any i and t):

$$H^i(X_1 \times X_2 \times \ldots \times X_n, \tilde{M}(t)) = \bigoplus_{j_1+j_2+\ldots j_n=i} \otimes_{r=1}^n H^{j_r}(X_r, \tilde{M}_r(t))$$

To begin with, we may apply the formula with $i = 0$ to see that

$$H^0(X_1 \times X_2 \times \ldots \times X_n, \tilde{M}(t)) = \otimes_r H^0(X_r, \tilde{M}_r(t)) = \otimes_{r=1}^n [M_r]_t = M_t.$$

Thus, the Serre map $s : M \to \oplus_{t\in\mathbb{Z}} H^0(X, \tilde{M}(t))$ is an isomorphism, and we have $H^i_m(M) = 0$ for $i = 0, 1$.

For $0 < j < d-1$ we have that $H^{j+1}_m(M) = \oplus_{t\in\mathbb{Z}} H^j(X, \tilde{M}(t))$.; so we need to show that $H^j(X, \tilde{M}(t)) = 0$ for any integer t, where $X = X_1 \times X_2 \times \ldots \times X_n$. But because of the way that the M_i were originally chosen, we see that each term of the sum on the right hand side of the relevant Kunneth formula is 0 unless either (1) $j_r = 0$ for all r, and $t \geq 0$; or else (2) $j_r = \dim(X_r)$ for all r, and $t < 0$. It follows that $H^j(X, \tilde{M}(t)) = 0$ for any $0 < j < d-1$, which completes the proof that M is a MCM module over R. □

Of course, this theorem has been proved with the results of the previous section in mind, which tell us that if the product is taken over a perfect field of characteristic $p > 0$, any reasonable hypotheses on the rings R_i will allow us to produce MCM modules over these rings with a-invariant less than 0. Putting the two results together yields the following very general result in characteristic p:

Corollary 6.2.4. *Let $R_1, \ldots, R_n$ be finitely generated positively graded algebras over a perfect field of characteristic $p > 0$, with $(R_i)_0 = K$. If each ring R_i has a graded maximal Cohen-Macaulay module, then the Segre product $R_1 \otimes_{seg} R_2 \otimes_{seg} \ldots \otimes_{seg} R_n$ also has a small (graded) maximal Cohen-Macaulay module.*

Note 6.2.5. The corollary of course follows immediately from theorems 6.1.3 and 6.2.3. But if the MCM modules over the rings R_i are denoted by M_i, then the Kunneth formulas used in the proof above show that the Segre product module $M = M_1 \otimes_{seg} \cdots \otimes_{seg} M_n$ has lower local cohomology modules of finite length over the Segre product ring $R_1 \otimes_{seg} R_2 \otimes_{seg} \cdots \otimes_{seg} R_n$, which is still a finitely generated graded algebra over a perfect field. Thus, the existence of a MCM module over the Segre product ring also follows from Theorem 1.5.3.

The methods used for showing the existence of MCM modules with a-invariant less than 0 are in general not applicable for rings of characteristic 0. Nevertheless, Theorem 6.2.3 is independent of the characteristic, so whenever it is possible to show the existence of such modules, partial results to the Segre product problem in characteristic 0 may be obtained. A few cases are treated below.

1. If R is a positively graded Cohen-Macaulay ring, it may be the case that R itself has a-invariant less than 0. This is true, for example, in the the case that R is a monomial subring of a polynomial ring over a field.

2. In fact, it is even sufficient for $a(R) = 0$. For one may consider an exact sequence of graded MCM modules:

$$O \to M \to R^n \to N \to 0,$$

where M embeds into mR^n. The exact sequence

$$O \to H^d_m(M) \to H^d_m(R^n) \to H^d_m(N) \to 0,$$

where the map on the left still has entries of positive degree, then clearly implies that $a(M) < 0$.

3. If (R, m) is a positively graded K-algebra, and M is a graded linear MCM R-module, then $M' = \mathrm{gr}_m M$ is a lin MCM over R which has generators all in the same degree, and it is easy to see that $a(M') < 0$. Thus it is a consequence of [1] that homogeneous complete intersections have MCMs with a-invariant less than 0.

4. In fact, upon closer inspection of the proof given in [1], one sees that the following more general conclusion may just as easily be reached:

   Note 6.2.6. If R is a positively graded ring which possesses a graded MCM module M with $a(M) = s$, and if x is a homogeneous form in R which is a non-zerodivisor on M, then the ring R/xR possesses a graded MCM module M' with $a(M') \leq s + 1$.

   In particular, if R is Cohen-Macaulay with $a(R) = s$, and if $x_1, \ldots, x_d$ is part of a homogeneous system of parameters for R, then $R/(x_1, \ldots, x_d)R$ has a graded MCM with $a(M) \leq s + d$.

   This will of course provide more rings possessing MCMs of negative a-invariant. For example, if R possesses a graded MCM M with $a(M) \leq 2$, then any hypersurface R/f, with f homogeneous, possesses a graded MCM with a-invariant less than 0.

5. Let R be a Cohen-Macaulay ring which admits, for an infinite sequence of positive integers t, ring homomorphisms $f_t : R \to R$ such that the image of f_t is contained in $R^{(t)}$, R is module-finite over the image of f_t, and the image of f_t contains a minimal reduction of m^t. Given such maps, one may proceed as in the case of characteristic $p > 0$: R splits into t direct summands over the

image of f_t, and for large enough t, one of these summands will necessarily have a-invariant less than 0.

Thus, any Segre product over a field K of rings of one of the above types will possess a MCM module, regardless of the characteristic of K.

6.3 Further approaches to characteristic 0 or non-graded rings

Many of the results of the preceding sections are obtained by methods only available in the characteristic $p > 0$ or $\mathbb{N}$-graded cases. But as in the study of Segre products, we wish to determine the extent to which similar results may be obtained without these hypotheses. In particular, we might ask whether the problem of existence of a certain kind of module for a local ring R is amenable to the methods of reduction to characteristic p.

Question 6.3.1. Can the existence of small Cohen-Macaulay modules (or linear MCM modules, or graded MCM modules with negative a-invariant) be reduced to the case of characteristic $p > 0$?

If the modules which occur when one passes to various prime characteristics are not bounded in some way, then this method has little hope of success. There is no apparent way in which one may express the condition of not having such a module in terms of finitely many equations. But this would be possible if, for example, one could bound the ranks of the free modules occuring in presentations of the desired modules in characteristic p.

Another approach to the characteristic 0 case is to just try to mimic the methods applied in characteristic p:

Proposition 6.3.2. *Let R be a positively graded, equidimensional ring (which is a homomorphic image of a regular ring), with $R_0 = K$ a field; and suppose R has isolated non-Cohen-Macaulay singularity. Then for suitably large n, the Veronese subring $R^{(n)}$ has a MCM-module (with a-invariant less than 0).*

Proof: For any $D > 0$, there exists some n_0 such that R splits into at least D direct summands over $R^{(n)}$ for every $n \geq n_0$. As $R^{(n)}$ contains a system of parameters for R, we know that $H^i_{m_{R^{(n)}}}(R)$ is isomorphic to, and hence has the same finite length as, $H^i_m(R)$ for all $i < \dim(R)$. Likewise, the length of the positive degree part of $H^d_m(R)$ is preserved. Thus, for sufficiently large n, one of the summands of R as an $R^{(n)}$-module must be a MCM-module for $R^{(n)}$ with a-invariant less than 0. $\square$

The reason that this method falls short in characteristic 0 is that there is in general no natural homomorphism from R to $R^{(n)}$ (such endomorphisms do exist for monomial subrings of polynomial rings, but in this case the polynomial ring itself will be a finitely generated MCM with a-invariant less than 0).

Even if we restrict ourselves to the case of rings of characteristic $p > 0$, we may hope to get similar results to the ones above for rings which are local instead of positively graded. In particular, we can recover similar splitting results in the case that R has Krull dimension 1, as proved by Hochster in [7].

Proposition 6.3.3 (Hochster). *If R is a complete local domain of dimension 1 and characteristic $p > 0$, with perfect residue field K, and if M is any torsion-free R-module, then ${}^eM$ splits for $e >> 0$.*

If we could produce such splitting results in higher dimensions, we would obtain new results on the existence of small MCM modules for many non-graded rings.

Finally, we note the following proposition, which was essentially proved in [10] by M. Hochster and J. Roberts. The only difference is that Hochster and Roberts assumed the ring to be graded, whereas the argument given here shows this condition to be unnecessary.

Definition 6.3.4. A ring homomorphism $R \to S$ is called *pure* if $M \hookrightarrow S \otimes_R M$ for every R-module M. A ring R of prime characteristic $p > 0$ is called F-pure if the Frobenius endomorphism $R \xrightarrow{F} R$ is pure.

Proposition 6.3.5. *Let R be an F-finite local ring of characteristic $p > 0$, with perfect residue field K. Suppose R has isolated non-C-M singularity, and that R is F-pure. Then for all $e' > e$, the module $M = Coker(F^{e'-e} : {}^{e}R \to {}^{e'}R)$ is a MCM-module for R.*

Proof: See [10] for the details on local cohomology.

Since R is F-pure, the map induced by F on the local cohomology modules $H^i_m({}^eR)$ is injective. This implies, in the first place, that for a given $i < \dim(R)$ all of the modules $H^i_m({}^eR)$ are isomorphic K -vector spaces; and it follows that the maps on the local cohomology modules induced by F must be isomorphisms for all $i < \dim(R)$. Now it is apparent from the long exact sequence on local cohomology induced by the short exact sequence

$$0 \to {}^{e}R \xrightarrow{F^{e'-e}} {}^{e'}R \to M \to 0$$

that $H^i_m(M) = 0$ for all $i < \dim(R)$. $\square$

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] J. Backelin, J. Herzog, and B.Ulrich. Linear maximal Cohen-Macaulay modules over strict complete intersections. *Journal of Pure and Applied Algebra*, 71:187–202, 1991.

[2] J. Brennan, J. Herzog, and B. Ulrich. Maximally generated Cohen-Macaulay modules. *Mathematica Scandinavica*, 61:181–203, 1987.

[3] W. Bruns and J. Herzog. *Cohen-Macaulay Rings*. Cambridge University Press, Cambridge, 1990.

[4] J. Eagon and M. Hochster. Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *American Journal of Mathematics*, 93:1020–1058, 1971.

[5] J. Eagon and D.G. Northcott. Generically acyclic complexes and generically perfect ideals. *Proceedings of the Royal Society, Series A*, 299:147–172, 1967.

[6] S. Goto and K. Watanabe. On graded rings, I. *Journal of the Mathematical Society of Japan*, 30:179–213, 1978.

[7] M. Hochster. Big Cohen-Macaulay modules and algebras and embeddability in rings of Witt vectors. *Queen's Papers on Pure and Applied Mathematics*, 42:106–195.

[8] M. Hochster. *Topics in the homological theory of modules over commutative rings*, volume 24 of *CBMS Regional Conference Series in Mathematics*. American Mathematical Society, Providence, RI, 1975.

[9] M. Hochster and C. Huneke. Tight closure of parameter ideals and splitting in module-finite extensions. *Journal of Algebraic Geometry*, 3:599–670, 1994.

[10] M. Hochster and J. Roberts. The purity of the Frobenius and local cohomology. *Advances in Mathematics*, 21:117–172, 1976.

[11] C. Huneke and M. Miller. A note on the multiplicity of Cohen-Macaulay algebras with pure resolutions. *Canadian Journal of Mathematics*, 37:1149–1162, 1985.

[12] C. Lech. Note on multiplicities of ideals. *Arkiv for Mathematik*, 4:63–86, 1960.

[13] C. Lech. Inequalities related to certain couples of local rings. *Acta Mathematica*, 112:69–89, 1964.

[14] F. Ma. Splitting in integral extensions, Cohen-Macaulay modules and algebras. *Journal of Algebra*, 116:176–195, 1988.

[15] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, Cambridge, 1986.

[16] P. Monsky. The Hilbert-Kunz funtion. *Mathematische Annalen*, 263:43–49, 1983.

[17] D.G. Northcott and D. Rees. Reductions of ideals in local rings. *Proceedings of the Cambridge Philosophical Society*, 50:145–158, 1954.

[18] C. Peskine and L. Szpiro. Notes sur un air de H. Bass. Unpublished preprint, Brandeis University.

[19] J.-P. Serre. *Algèbre locale. Multiplicités*, volume 11 of *Lecture Notes in Mathematics.* Springer, 1965.

[20] B. Ulrich. Gorenstein rings and modules with high numbers of generators. *Mathematische Zeitschrift*, 188:23–32, 1984.

ABSTRACT

Special Conditions on Maximal Cohen-Macaulay Modules, and Applications to the Theory of Multiplicities

by

Douglas Hanes

Chair: Melvin Hochster

The dissertation explores the existence of maximal Cohen-Macaulay modules satisfying certain special conditions which are generalizations of the linearity property. In particular, the existence of linear maximal Cohen-Macaulay modules is proved for certain classes of graded rings.

The existence of such modules is then exploited in order to prove some new cases of Lech's conjecture on multiplicities under flat local extensions. The conjecture is proved in many cases in which the base ring R has prime characteristic p; and is either 3-dimensional, or else graded by 1-forms over a field and of dimension less than or equal to 5.

Lech-type theorems on flat extensions and localization are proved for the Hilbert-Kunz multiplicity. Moreover, the existence of small maximal Cohen-Macaulay modules is shown for certain Segre product rings.