4-9-2004

Two Theorems about Maximal Cohen--Macaulay Modules

Craig Huneke
University of Kansas

Graham J. Leuschke
Syracuse University

Mathematische Annalen manuscript No.
(will be inserted by the editor)

Two theorems about maximal Cohen–Macaulay modules

Craig Huneke · Graham J. Leuschke ⋆

February 1, 2008 – © Springer-Verlag 2008

Abstract. This paper contains two theorems concerning the theory of maximal Cohen–Macaulay modules. The first theorem proves that certain Ext groups between maximal Cohen–Macaulay modules M and N must have finite length, provided only finitely many isomorphism classes of maximal Cohen–Macaulay modules exist having ranks up to the sum of the ranks of M and N. This has several corollaries. In particular it proves that a Cohen–Macaulay local ring of finite Cohen–Macaulay type has an isolated singularity. A well-known theorem of Auslander gives the same conclusion but requires that the ring be Henselian. Other corollaries of our result include statements concerning when a ring is Gorenstein or a complete intersection on the punctured spectrum, and the recent theorem of Leuschke and Wiegand that the completion of an excellent Cohen–Macaulay local ring of finite Cohen–Macaulay type is again of finite Cohen–Macaulay type. The second theorem proves that a complete local Gorenstein domain of positive characteristic p and dimension d is F-rational if and only if the number of copies of R splitting out of R^{1/p^e} divided by p^{de} has a positive limit. This result generalizes work of Smith and Van den Bergh. We call this limit the F-signature of the ring and give some of its properties.

Key words. maximal Cohen–Macaulay modules, F-rationality, Hilbert–Kunz multiplicity

Mathematics Subject Classification (2000): (2000 MSC): 13C14, 13H10, 13D07, 13A35, 13D40

Throughout this paper we will work with a Noetherian local ring $(R, \mathfrak{m})$. Recall that a finitely generated R-module M is *maximal Cohen–Macaulay (MCM)* if $\operatorname{depth} M = \dim R$. We say that R has *finite Cohen–Macaulay type* (or *finite CM type*) provided there are only finitely many isomorphism classes of indecomposable MCM R-modules. There is a large body of work devoted to the classification of Cohen–Macaulay local rings of finite CM type, for example see the book [22]. One of the first and most famous results is that of M. Auslander [1]: if R is complete Cohen–Macaulay and has finite Cohen–Macaulay type, then R has an isolated singularity, i.e. for all primes $\mathfrak{p} \neq \mathfrak{m}$, $R_\mathfrak{p}$ is a regular local ring. (Yoshino [22] points out that R need only be Henselian and have a canonical module.) A key point in Auslander's proof is to prove that the modules $\operatorname{Ext}^1_R(M, N)$ are of finite length for arbitrary MCM modules M and N, and he accomplishes this by using the theory of almost split sequences. The first result in this paper gives a proof of the finite length

Department of Mathematics
University of Kansas
Lawrence, KS 66045
e-mail: huneke@math.ukans.edu
gleuschke@math.ukans.edu

⋆ Both authors were partially supported by the National Science Foundation. The second author was also partially supported by the Clay Mathematics Institute.

of the Ext modules but with several notable improvements: we do not need to assume the base ring is Henselian (nor has a canonical module), and furthermore we can give an explicit bound on the power of the maximal ideal annihilating $\operatorname{Ext}^1_R(M,N)$ in terms of the number of isomorphism classes of MCM modules of multiplicity at most the sum of the multiplicities of M and N (without assuming there are only finitely many isomorphism classes of MCMs). This result has several corollaries of interest. By applying the theorem to special modules M we are able to give several results which have the flavor that the ring must be either Gorenstein, a complete intersection, or regular on the punctured spectrum provided there are only finitely many isomorphism classes of MCM modules up to some number depending upon the number of generators of the special module (e.g., when the module M is the canonical module, we conclude the ring is Gorenstein on the punctured spectrum). We are able to give a direct proof of a recent theorem of Leuschke and Wiegand that a Cohen–Macaulay local ring R has finite Cohen–Macaulay type if and only the completion of R has finite Cohen–Macaulay type.

In the second theorem we discuss a more general class of rings introduced in a paper of K.E. Smith and M. Van den Bergh [17]. We consider reduced Cohen–Macaulay local rings of prime characteristic p, and let $q = p^e$ be a varying power of p. We say that R is *F-finite* if the Frobenius map $F : R \to R$ sending r to r^p is a finite map. A reduced local F-finite Cohen–Macaulay ring R is said to have finite F-representation type (or FFRT for short) if only finitely many isomorphism classes of indecomposable MCM modules occur as direct summands of $R^{1/q}$ as q ranges over all powers of p. Among other results, Smith and Van den Bergh proved that if we denote by a_q the number of copies of R splitting out of $R^{1/q}$, then provided R is strongly F-regular (a tight closure notion — see [9]), and has FFRT, the limit of $a_q/q^{\dim R}$ exists and is positive. We show (without the assumption of FFRT) that if the limit is positive, then R is weakly F-regular, that is, all ideals of R are tightly closed. When R is Gorenstein, we are able to prove the limit always exists, and moreover prove that this limit is positive if and only if R is F-rational (which is equivalent to strongly F-regular in the F-finite Gorenstein case). When the limit exists, we call it the *F-signature* of R and denote it by $s(R)$. Several examples at the end of this paper show that $s(R)$ is a delicate invariant of the ring which gives considerable information about the type of the singularity of R. For example, when R is the hypersurface $x^2 + y^3 + z^5 = 0$ (the famous E_8 singularity), then the F-signature is 1/120. (This ring is the ring of invariants of a group of order 120 acting on $k[x, y, z]$.) We also prove that $0 \le s(R) \le 1$, and $s(R) = 1$ if and only if the ring is regular.

1. Finite type

Theorem 1. *Let $(R,\mathfrak{m})$ be a local ring and let M and N be two finitely generated MCM modules over R, having multiplicities m and n respectively. Assume that there are only finitely many isomorphism classes of MCM modules of multiplicity $m+n$. If h is the number of such isomorphism classes, then $\mathfrak{m}^h$ annihilates $\operatorname{Ext}^1_R(M,N)$. In particular, $\operatorname{Ext}^1_R(M,N)$ has finite length.*

Proof. We claim that for any $\chi \in \operatorname{Ext}^1_R(M,N)$ and any $r_1, ..., r_h \in \mathfrak{m}$, $r_1 \cdots r_h\chi = 0$. Let

$$\chi : 0 \longrightarrow N \longrightarrow K \longrightarrow M \longrightarrow 0$$

be given, and consider

$$r_1 \cdots r_k \chi : 0 \longrightarrow N \longrightarrow K_k \longrightarrow M \longrightarrow 0$$

as k runs through all positive integers, and each $r_i \in \mathfrak{m}$. Since each K_k is a MCM module and the multiplicity of K_k is equal to the sum of the multiplicities of M and N, by assumption there must be repetitions among the K_k. That is, there exist integers a and b, with $a < b$ and $a \leq h$, such that $K_a \cong K_b$. Replace χ by $r_1 \cdots r_a \chi$ and set $r = r_{a+1} \cdots r_b$ to assume that we have

$$\chi : 0 \longrightarrow N \longrightarrow K \longrightarrow M \longrightarrow 0$$

and

$$r\chi : 0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$$

and that $L \cong K$. We will show that $\chi = 0$.

Recall that $r\chi$ is constructed from χ by the following pushout diagram

$$\begin{array}{ccccccccc}
\chi : 0 & \longrightarrow & N & \xrightarrow{i} & K & \longrightarrow & M & \longrightarrow & 0 \\
 & & {\scriptstyle r}\downarrow & & \downarrow & & \| & & \\
r\chi : 0 & \longrightarrow & N & \longrightarrow & L & \longrightarrow & M & \longrightarrow & 0.
\end{array}$$

In particular, $L \cong N \oplus K / \langle (rn, i(n)) : n \in N \rangle$. This gives another exact sequence

$$\zeta : 0 \longrightarrow N \xrightarrow{\left[\begin{smallmatrix} r \\ i \end{smallmatrix}\right]} N \oplus K \longrightarrow L \longrightarrow 0.$$

Since $L \cong K$, ζ is "apparently split", and Miyata's theorem [4, A3.29] implies that ζ splits. The map $\zeta^* : \mathrm{Ext}^1_R(M, N) \longrightarrow \mathrm{Ext}^1_R(M, N \oplus K)$ obtained by applying $\mathrm{Hom}_R(M, -)$ to ζ is thus a split injection. We claim that χ goes to zero in the second component $\mathrm{Ext}^1_R(M, K)$. Applying $\mathrm{Hom}_R(M, -)$ to χ gives the exact sequence

$$\mathrm{Hom}_R(M, M) \longrightarrow \mathrm{Ext}^1_R(M, N) \longrightarrow \mathrm{Ext}^1_R(M, K).$$

The identity endomorphism of M maps to $\chi \in \mathrm{Ext}^1_R(M, N)$, so χ goes to zero in $\mathrm{Ext}^1_R(M, K)$, and it is easy to check that this map coincides with the second component of ζ^*. This proves the claim, that is, $\zeta^*(\chi) = (r\chi, 0)$ in $\mathrm{Ext}^1_R(M, N) \oplus \mathrm{Ext}^1_R(M, K)$. Letting f be a left splitting for ζ^*, we see that $\chi = f(r\chi, 0) = rf(\chi, 0)$. Iterating shows that χ is infinitely divisible by r, so $\chi = 0$, as desired. Since $r_1, ..., r_a$ are arbitrary elements in $\mathfrak{m}$, this proves that $\mathfrak{m}^a$ annihilates $\mathrm{Ext}^1_R(M, N)$. □

Our first application is to local rings of finite Cohen–Macaulay type.

Corollary 2. *Let $(R, \mathfrak{m})$ be a Cohen–Macaulay local ring of finite CM type. Then R is an isolated singularity.*

Proof. Set $d = \dim(R)$. It suffices to prove that $\mathrm{Ext}^1_R(M,N)$ has finite length for all MCM modules M and N. For suppose this is true, and let $\mathfrak{p} \in \operatorname{Spec} R$ be different from $\mathfrak{m}$. Consider syzygies of $R/\mathfrak{p}$:

$$0 \longrightarrow \mathrm{syz}^R_{d+1}(R/\mathfrak{p}) \longrightarrow F_d \longrightarrow \mathrm{syz}^R_d(R/\mathfrak{p}) \longrightarrow 0. \tag{1}$$

Since R is Cohen–Macaulay, $M := \mathrm{syz}^R_d(R/\mathfrak{p})$ and $N := \mathrm{syz}^R_{d+1}(R/\mathfrak{p})$ are MCM R-modules. By hypothesis, localizing (1) at $\mathfrak{p}$ gives a split exact sequence, so $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are both free $R_\mathfrak{p}$-modules. But this implies that the residue field of $R_\mathfrak{p}$ has a finite free resolution, and so $R_\mathfrak{p}$ is a regular local ring.

Since R has finite CM type, the assumptions of Theorem 1 are satisfied for all such M and N, giving the desired conclusion. □

Remark. Corollary 2 is a generalization of a celebrated theorem of Auslander [1], which has the same conclusion but requires that R be complete. In fact, Auslander obtained this theorem as a corollary of a more general result, which we can also recover. Specifically, Auslander considers the following situation: Let T be a complete regular local ring and let Λ be a possibly non-commutative T-algebra which is a finitely generated free T-module. Say that Λ is *nonsingular* if $\operatorname{gl.dim.} \Lambda = \dim T$, and that Λ has *finite representation type* if there are only finitely many isomorphism classes of indecomposable finitely generated Λ-modules that are free as T-modules. If Λ has finite representation type, then $\Lambda_\mathfrak{p}$ is nonsingular for all nonmaximal primes $\mathfrak{p}$ of T [1, Theorem 10]. We are primarily interested in the commutative case, so we leave to the interested reader the extension of Corollary 2 to Auslander's context.

We are grateful to the anonymous referee for pointing out this generalization, as well as a small change in the proof of Theorem 1 that makes the extension possible.

An almost immediate consequence of the Theorem 1 is a rather powerful one:

Theorem 3. *Let $(R,\mathfrak{m})$ be a Cohen–Macaulay local ring and let M be a finitely generated maximal Cohen–Macaulay R-module. Set $e = e(R)$, the multiplicity of R, and $n = \mu(M)$, the minimal number of generators of M. If R has only finitely many indecomposable nonisomorphic MCM modules of multiplicity at most $n \cdot e$, then $M_\mathfrak{p}$ is free for all primes $\mathfrak{p} \neq \mathfrak{m}$.*

Proof. Consider the exact sequence

$$0 \to N \to R^n \to M \to 0.$$

This is an element of $\mathrm{Ext}^1_R(M,N)$. Since the sum of the multiplicities of M and N is $n \cdot e$, Theorem 1 gives us that $\mathrm{Ext}^1_R(M,N)$ has finite length. Hence after localizing the short exact sequence at an arbitrary prime $\mathfrak{p} \neq \mathfrak{m}$ the sequence splits and $M_\mathfrak{p}$ is then free. □

Using this we can give stronger results concerning when a given local ring is regular, or Gorenstein, or a complete intersection on the punctured spectrum in terms of the ring having only finitely many indecomposable MCM modules up to a certain multiplicity.

Corollary 4. *Let $(R, \mathfrak{m})$ be either a localization of a finitely generated algebra over a field k of characteristic 0, or a quotient of a power series ring over a field k of characteristic 0. In the first case, let Ω be the module of Kähler differentials of R over k, and in the second case let Ω be the universally finite module of differentials of R over k. Assume that Ω is a maximal Cohen–Macaulay module. Set $e = e(R)$ and let n be the embedding dimension of R, that is, $n = \mu(\mathfrak{m}/\mathfrak{m}^2)$. If R has only finitely many indecomposable nonisomorphic MCM modules of multiplicity at most $n \cdot e$, then $R_{\mathfrak{p}}$ is regular for all primes $\mathfrak{p} \neq \mathfrak{m}$.*

Proof. In either case there is an exact sequence,

$$0 \to N \to R^n \to \Omega \to 0.$$

(The number of generators of Ω is at most the embedding dimension of R by Theorem 25.2 of [14] or Theorem 11.10 of [12].) Applying Theorem 3 then shows that $\Omega_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ module for all primes $\mathfrak{p} \neq \mathfrak{m}$. Applying Theorem 7.2 of [12] in the first case and Theorem 14.1 of [12] in the second case, we see that $R_{\mathfrak{p}}$ is regular. □

Although the assumption that the module of differentials is Cohen–Macaulay is quite strong, it can occur even if the ring is not regular: Let $B = k[X_{ij}]$, where $X = (X_{ij})$ is an $m \times n$ matrix of indeterminates, and let $r < \min(m, n)$ be an integer. Let $R = B/I_{r+1}(X)$. If $I_{r+1}(X)$ has grade at most two, then the module of Kähler differentials Ω is a MCM R-module ([2, Prop. 14.7]).

Corollary 5. *Let $(R, \mathfrak{m})$ be a Cohen–Macaulay local ring with canonical module ω. Assume that R has only finitely many indecomposable nonisomorphic MCM modules of multiplicity at most* $\operatorname{type}(R) \cdot e(R)$*. Then R is Gorenstein on the punctured spectrum.*

Proof. Applying Theorem 3 to the extension

$$\chi : 0 \longrightarrow \operatorname{syz}_1^R(\omega) \longrightarrow R^t \longrightarrow \omega \longrightarrow 0,$$

where $t = \operatorname{type}(R)$, shows that $\chi_{\mathfrak{p}}$ is split for every nonmaximal prime $\mathfrak{p}$. It follows that $\omega_{\mathfrak{p}}$ is free for all nonmaximal primes $\mathfrak{p}$, which implies that $R_{\mathfrak{p}}$ is Gorenstein for all such primes. □

Corollary 6. *Let $R = A/I$, where A is a regular local ring. Assume that R is Cohen–Macaulay and that I/I^2 is a MCM R-module. If R has only finitely many indecomposable nonisomorphic MCM modules of rank at most $\mu_A(I)$, then $R_{\mathfrak{p}}$ is a complete intersection for all nonmaximal primes $\mathfrak{p}$ of R.*

Proof. This follows from Theorem 3 as well, together with the fact that I/I^2 is a free R-module if and only if I is generated by an A-regular sequence ([14, 19.9]). □

This raises the question of when I/I^2 is a MCM R-module. Herzog [6] showed that this is the case when I is a codimension three prime ideal in a regular local ring A such that $R = A/I$ is Gorenstein, and this was generalized in [10] to the case in which I is licci and generically a complete intersection in a regular local ring A such that A/I is Gorenstein. Since the height of the defining ideal of the non-complete intersection locus of a Gorenstein licci ideal is known to be bounded, the above Corollary shows that Gorenstein licci algebras in general can never have finite CM type, nor even have only finitely many isomorphism classes of MCMs of rank at most the embedding codimension of the algebra. This observation can be extended to the case in which R is licci but not Gorenstein by using the module $I/I^2 \otimes \omega$, which is known to be MCM over R [3].

In a similar vein we can prove:

Corollary 7. *Let $R = A/I$, where A is a regular local ring. Assume that R is Cohen–Macaulay and normal, and that $I/I^{(2)}$ is a MCM R-module. If R has only finitely many indecomposable nonisomorphic MCM modules of rank at most $\mu_A(I)$, then $R_\mathfrak{p}$ is a complete intersection for all nonmaximal primes $\mathfrak{p}$ of R.*

Proof. As in the proofs above, the assumptions together with Theorem 3 show that $(I/I^{(2)})_\mathfrak{p}$ is $R_\mathfrak{p}$-free for all $\mathfrak{p} \neq \mathfrak{m}$. Since R is normal, R satisfies Serre's condition S_2, is reduced and I_Q is generated by a regular sequence for all primes $Q \supseteq I$ such that the height of Q/I is at most 1. From the main theorem of [16] it follows that $I_\mathfrak{p}$ is generated by a regular sequence for all $\mathfrak{p} \neq \mathfrak{m}$. □

We also are able to recover a recent result of Leuschke and Wiegand, [13]:

Corollary 8. *Let $(R, \mathfrak{m})$ be an excellent local Cohen–Macaulay ring having finite CM type. Then the completion $\widehat{R}$ also has finite CM type.*

Proof. In [20] it was shown that if R is a Cohen–Macaulay local ring which is of finite CM type and such that the completion $\widehat{R}$ is an isolated singularity, then $\widehat{R}$ has finite CM type. Since R is excellent and has an isolated singularity by Corollary 2, $\widehat{R}$ also has an isolated singularity, and the conclusion follows. □

2. The F-signature

In this section, let $(R, \mathfrak{m})$ be a Cohen–Macaulay local ring of dimension d containing a field of characteristic $p > 0$ and such that R is F-finite. As usual, q will denote a varying power of p. We will consider the direct-sum decomposition

$$R^{1/q} = R^{a_{1q}} \oplus M_2^{a_{2q}} \oplus \cdots \oplus M_{n_q}^{a_{n_q q}} \tag{*}$$

of $R^{1/q}$ into indecomposable MCM R-modules. We refer the reader to [9] for basic definitions concerning the theory of tight closure.

Definition 9. *The F-*signature *of R is $s(R) = \lim\limits_{q\to\infty} \frac{a_{1q}}{q^d}$, provided the limit exists.*

Smith and Van den Bergh [17] show that if R is strongly F-regular and the set of indecomposable modules M_i appearing in the decomposition (*) is finite (as q ranges over all powers of p), then $\lim\limits_{q\to\infty} \frac{a_{iq}}{q^d}$ exists and is positive for each i. For further results in this direction, see [21]. We will show that $s(R)$ always exists for Gorenstein local rings R, and is positive if and only if R is F-rational.

Recall that a local Noetherian ring of positive characteristic R is said to be *F-rational* if ideals generated by parameters are tightly closed. In the case that R is Gorenstein this is equivalent to every ideal being tightly closed. In case R is not necessarily Gorenstein, we can easily prove that if $\limsup \frac{a_{1q}}{q^d} > 0$, then R is weakly F-regular.

For the proofs we use a characterization of tight closure in terms of Hilbert–Kunz functions. Let $(R, \mathfrak{m})$ be a local Noetherian ring of prime characteristic p, and let I be an $\mathfrak{m}$-primary ideal. The *Hilbert–Kunz function* of I is the function taking an integer n to the length of $R/I^{[p^n]}$, where $I^{[p^n]}$ is the ideal generated by all the p^nth powers of elements of I. The Hilbert–Kunz multiplicity of I, denoted $e_{HK}(I)$ or $e_{HK}(I, R)$, is $\lim_{q=p^n \to \infty} \frac{\lambda(R/I^{[q]})}{q^d}$, where $\lambda(M)$ is the length of M. This limit always exists (see, for example, Chapter 6 of [9]).

We need the following special case of Theorem 8.17 of [7]:

Theorem 10. *Let $(R, \mathfrak{m})$ be a reduced, equidimensional complete local ring of prime characteristic p. Let $I \subseteq J$ be two $\mathfrak{m}$-primary ideals. Then $I^* = J^*$ if and only if $e_{HK}(I) = e_{HK}(J)$. (Here I^* denotes the tight closure of I.)*

We note that the assumption concerning test elements in [7, Theorem 8.17] is automatic in this case since the ring is excellent, reduced, and local. See [8, Theorem 6.1].

Theorem 11. *Assume that $(R, \mathfrak{m})$ is a complete reduced F-finite Cohen–Macaulay local ring containing a field of prime characteristic p and let $d = \dim R$. We adopt the notation from the beginning of this section. Then*
(1) If $\limsup \frac{a_{1q}}{q^d} > 0$, then R is weakly F-regular;
(2) If in addition R is Gorenstein, then $s(R)$ exists, and is positive if and only if R is F-rational.

Proof. Assume that R is not weakly F-regular, that is, not all ideals of R are tightly closed. By [8, Theorem 6.1] R has a test element, and then [7, Proposition 6.1] shows that the tight closure of an arbitary ideal in R is the intersection of $\mathfrak{m}$-primary tightly closed ideals. Since R is not weakly F-regular, there exists an $\mathfrak{m}$-primary ideal I with $I \neq I^*$. Choose an element Δ of $I : \mathfrak{m}$ which is not in I^*. Decompose $R^{1/q}$ into indecomposable MCM R-modules as in (*). Then

$$\begin{aligned}
\lambda(R/I^{[q]}) - \lambda(R/(I, \Delta)^{[q]}) &= \lambda(R^{1/q}/IR^{1/q}) - \lambda(R^{1/q}/(I, \Delta)R^{1/q}) \\
&= a_{1q}\lambda(R/I) + a_{2q}\lambda(M_2/IM_2) + \cdots \\
&\qquad - [a_{1q}\lambda(R/(I, \Delta)) + a_{2q}\lambda(M_2/(I, \Delta)M_2) + \cdots] \\
&\geq a_{1q}\lambda(R/I) - a_{1q}\lambda(R/(I, \Delta)) \\
&= a_{1q}.
\end{aligned}$$

Dividing by q^d and taking the limit gives on the left-hand side a difference of Hilbert-Kunz multiplicities,

$$e_{HK}(I, R) - e_{HK}((I, \Delta), R).$$

But by Theorem 10, this difference is zero, showing that $\limsup \frac{a_{1q}}{q^d} = 0$.

Assume now that R is Gorenstein. To prove (2), it suffices to take $I = (\underline{x})$ generated by a system of parameters and show that the difference $\lambda(M_i/\underline{x}M_i) - \lambda(M_i/(\underline{x}, \Delta)M_i)$ is zero for all indecomposable nonfree MCM modules M_i. We state this as a separate lemma.

Lemma 12. *Let $(R, \mathfrak{m})$ be a Gorenstein local ring and let M be an indecomposable nonfree MCM R-module. Let $\underline{x}$ be a system of parameters for R, and let $\Delta \in R$ be a representative for the socle of $R/(\underline{x})$. Then $\Delta M \subseteq \underline{x}M$.*

Proof. Choose generators $\{m_1, \dots, m_n\}$ for M and define a homomorphism $R \longrightarrow M^n$ by $1 \mapsto (m_1, \dots, m_n)$. Let N be the cokernel and set $I = \operatorname{Ann}(M)$, so that we have an exact sequence

$$0 \longrightarrow R/I \longrightarrow M^n \longrightarrow N \longrightarrow 0.$$

First assume that N is MCM. Then $\underline{x}$ is regular on N and on R/I. If $I \subseteq (\underline{x})$, then $I = I \cap (\underline{x}) = I\underline{x}$, so $I = (0)$ by NAK. This gives the exact sequence $0 \longrightarrow R \longrightarrow M^n \longrightarrow N \longrightarrow 0$. Since R is Gorenstein and N is MCM, this sequence must split, contradicting the fact that M^n has no free summands. So $I \not\subseteq (\underline{x})$. When we kill $\underline{x}$, therefore, the map $\overline{R} \longrightarrow \overline{M}^n$ has nonzero kernel, which must contain Δ. Since the elements $m_1, \dots, m_n$ generate M, this says precisely that $\Delta M \subseteq \underline{x}M$.

Finally assume that N is not MCM. Then when we kill $\underline{x}$, there is a nonzero Tor:

$$0 \longrightarrow \operatorname{Tor}_1^R(N, R/(\underline{x})) \longrightarrow \overline{R} \longrightarrow \overline{M}^n \longrightarrow \overline{N} \longrightarrow 0.$$

Again, the map $\overline{R} \longrightarrow \overline{M}^n$ has nonzero kernel, so $\Delta \mapsto 0$. □

Returning to the proof of (2), we have

$$\lambda(R/(\underline{x})^{[q]}) - \lambda(R/(\underline{x}, \Delta)^{[q]}) = a_{1q}$$

and

$$e_{HK}(\underline{x}, R) - e_{HK}((\underline{x}, \Delta), R) = s(R).$$

This shows that the limit exists, and is positive if and only if $\underline{x}$ can be chosen to generate a tightly closed ideal, if and only if R is F-rational. □

We now derive some basic properties of the F-signature.

Proposition 13. *Let R be a reduced F-finite local ring of prime characteristic p, and assume that the F-signature $s(R)$ exists. Then*
(1) $s(R_\mathfrak{p}) \geq s(R)$ for every prime ideal $\mathfrak{p}$ of R;
(2) $s(R) = s(\widehat{R})$, where $\widehat{R}$ is the completion of R.

Proof. The proposition is clear from the facts that $(R_\mathfrak{p})^{1/q} \cong (R^{1/q})_\mathfrak{p}$ and $(\widehat{R})^{1/q} \cong \widehat{R^{1/q}}$. □

Proposition 14. *Let $(R, \mathfrak{m})$ be a reduced F-finite Cohen–Macaulay local ring with infinite residue field, such that the F-signature $s = s(R)$ exists. Then*

$$(e-1)(1-s) \geq e_{HK}(R) - 1,$$

where $e = e(R)$ and $e_{HK}(R)$ are the Hilbert–Samuel and Hilbert–Kunz multiplicities, respectively.

Proof. Let $\underline{x}$ be a system of parameters generating a minimal reduction of $\mathfrak{m}$, and take a composition series

$$(\underline{x}) = I_{e-1} \subset I_{e-2} \subset \cdots \subset I_1 = \mathfrak{m}$$

with successive quotients isomorphic to $R/\mathfrak{m}$. Then the proof of Theorem 11 shows that

$$\lambda(R/I_{j+1}^{[q]}) - \lambda(R/I_j^{[q]}) \geq a_{1q}$$

for each $j = 1, \ldots, e-2$. Dividing both sides by q^d, taking the limit, and adding the inequalities, we obtain

$$e_{HK}((\underline{x}), R) - e_{HK}(\mathfrak{m}, R) \geq (e-1)s.$$

Since $(\underline{x})$ is a minimal reduction for $\mathfrak{m}$ and R is Cohen-Macaulay, $e_{HK}((\underline{x}), R) = e((\underline{x}), R) = e$. This gives the desired inequality. □

Proposition 15. *Let $(R, \mathfrak{m})$ be a reduced F-finite Cohen–Macaulay local ring such that the F-signature $s = s(R)$ exists. Then*

$$s(R) \leq \frac{e_{HK}(I) - e_{HK}(J)}{\lambda(J/I)}$$

for every pair of $\mathfrak{m}$-primary ideals $I \subseteq J$. If R is Gorenstein and has infinite residue field, then equality is attained for I a minimal reduction of $\mathfrak{m}$ and $J = (I, \Delta)$, where Δ represents a generator of the socle of R/I.

Proof. For arbitrary $q = p^e$, decompose $R^{1/q} \cong R^{a_q} \oplus M_q$, where M_q has no nonzero free direct summands. Then

$$\begin{aligned}
\lambda(R/I^{[q]}) - \lambda(R/J^{[q]}) &= \lambda(R^{1/q}/IR^{1/q}) - \lambda(R^{1/q}/JR^{1/q}) \\
&= \lambda((R^{a_q} \oplus M_q)/I(R^{a_q} \oplus M_q)) - \lambda((R^{a_q} \oplus M_q)/J(R^{a_q} \oplus M_q)) \\
&\geq a_q\lambda(R/I) - a_q\lambda(R/J) \\
&= a_q\lambda(J/I).
\end{aligned}$$

Rearranging, dividing by $q^{\dim R}$, and taking the limit give the result. The statement about equality is just a rewording of the last sentence of Theorem 11. □

Corollary 16. *Let $(R, \mathfrak{m})$ be a reduced F-finite Cohen–Macaulay local ring such that the F-signature $s = s(R)$ exists. Then $s(R) = 1$ if and only if R is regular.*

Proof. If R is regular, then for all $q = p^e$, $R^{1/q}$ is a free R-module whose rank is q^d. It follows that $s(R) = 1$. Conversely suppose that $s(R) = 1$. Then Proposition 14 proves that $e_{HK}(R) = 1$. Since Cohen–Macaulay rings are automatically unmixed, we obtain from [18] that R is regular. (See also [11] for an alternate approach.) □

We next compute the F-signature for several examples. It is evident from these examples that the F-signature gives very delicate information concerning the nature of the singularity.

Example 17. Let $R = k[[x^n, x^{n-1}y, \dots, y^n]]$, the n^{th} Veronese subring of $k[[x,y]]$, where k is a perfect field of positive characteristic p. Assume that $n \geq 2$ and $p \nmid n$. Then Herzog [5] has shown that R has finite CM type. Specifically, the indecomposable nonfree MCM R-modules are the fractional ideals $I_1 = (x,y)$, $I_2 = (x^2, xy, y^2)$, $\dots$, $I_{n-1} = (x^{n-1}, x^{n-2}y, \dots, y^{n-1})$. For consistency, denote R also by I_0.

We have the following decompositions of R, I_1, $\dots$, I_{n-1} as modules over the ring R^p of p^{th} powers. All congruences are modulo n. This decomposition was done by Seibert [15].

$$R = \bigoplus_{\substack{a+b\equiv 0\\ 0\le a,b<p}} R^p x^a y^b \oplus \bigoplus_{\substack{a+b\equiv -1\\ 0\le a,b<p}} I_1^{[p]} x^a y^b \oplus \cdots \oplus \bigoplus_{\substack{a+b\equiv 1\\ 0\le a,b<p}} I_{n-1}^{[p]} x^a y^b$$

$$I_1 = \bigoplus_{\substack{a+b\equiv 1\\ 0\le a,b<p}} R^p x^a y^b \oplus \bigoplus_{\substack{a+b\equiv 0\\ 0\le a,b<p}} I_1^{[p]} x^a y^b \oplus \cdots \oplus \bigoplus_{\substack{a+b\equiv 2\\ 0\le a,b<p}} I_{n-1}^{[p]} x^a y^b$$

$$\vdots$$

$$I_k = \bigoplus_{\substack{a+b\equiv k\\ 0\le a,b<p}} R^p x^a y^b \oplus \bigoplus_{\substack{a+b\equiv k-1\\ 0\le a,b<p}} I_1^{[p]} x^a y^b \oplus \cdots \oplus \bigoplus_{\substack{a+b\equiv n-1-k\\ 0\le a,b<p}} I_{n-1}^{[p]} x^a y^b$$

$$\vdots$$

$$I_{n-1} = \bigoplus_{\substack{a+b\equiv -1\\ 0\le a,b<p}} R^p x^a y^b \oplus \bigoplus_{\substack{a+b\equiv -2\\ 0\le a,b<p}} I_1^{[p]} x^a y^b \oplus \cdots \oplus \bigoplus_{\substack{a+b\equiv 0\\ 0\le a,b<p}} I_{n-1}^{[p]} x^a y^b$$

For any given pair (p,n) and $k < n$, it is easy to compute the number of pairs (a,b) with $0 \le a,b < p$ and $a+b \equiv k$. For a general estimate, let m_k be this number. Since we have $|m_k - m_{k-1}| \le 1$ (even when the indices are taken modulo n) and $\sum_k m_k = p^2$, we obtain

$$\left\lfloor \frac{p^2}{n} \right\rfloor \le m_k \le \left\lfloor \frac{p^2}{n} \right\rfloor + r,$$

where r is the remainder upon writing $p^2 = Ln + r$, $0 \le r < n$.

This implies that if the data from the decompositions is arranged in a matrix $A = (a_{ij})$, where a_{ij} is the number of direct summands isomorphic to $I_j^{[p]}$ occurring in the decomposition of I_i, then each entry of A is of the form $(1/n)(p^2 \pm c)$. For any $s \ge 1$, the entries of A^s are again $(1/n)$ times a polynomial in p^2, of degree $2s$. This gives $s(R) = 1/n$.

For a concrete example, take $p = 5$ and $n = 3$. Then the matrix A is

$$\begin{bmatrix} 8 & 8 & 9 \\ 9 & 8 & 8 \\ 8 & 9 & 8 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 5^2-1 & 5^2-1 & 5^2+2 \\ 5^2+2 & 5^2-1 & 5^2-1 \\ 5^2-1 & 5^2+2 & 5^2-1 \end{bmatrix}.$$

The entries of A^s for $s \ge 1$ are polynomials in $p^2 = 25$ of the form $\frac{1}{3}p^{2s}$ + lower order terms. Thus we see that $\lim_{s\longrightarrow\infty} \dfrac{a_{1q}}{p^{2s}} = \dfrac{1}{3}$.

Example 18. (See [18, Thm. 5.4].) Let $(R,\mathfrak{m})$ be a two-dimensional Gorenstein complete local ring of characteristic p. Assume that R is F-finite and F-rational. Then R is a double point and is isomorphic to $k[[x,y,z]]/(f)$, where f is one of the following:

type	equation	char R	$s(R)$	
(A_n)	$f = xy + z^{n+1}$	$p \geq 2$	$1/(n+1)$	$(n \geq 1)$
(D_n)	$f = x^2 + yz^2 + y^{n-1}$	$p \geq 3$	$1/4(n-2)$	$(n \geq 4)$
(E_6)	$f = x^2 + y^3 + z^4$	$p \geq 5$	$1/24$	
(E_7)	$f = x^2 + y^3 + yz^3$	$p \geq 5$	$1/48$	
(E_8)	$f = x^2 + y^3 + z^5$	$p \geq 7$	$1/120$	

We compute the F-signature in each of these examples as follows: In each example a minimal reduction J of the maximal ideal $\mathfrak{m}$ has the property that $\mathfrak{m}/J$ is a vector space of dimension 1. Hence $e_{HK}(J) - e_{HK}(R) = s(R)$ as in the proof of Theorem 11. Since J is generated by a regular sequence and is a reduction of $\mathfrak{m}$, $e_{HK}(J) = e(J) = e(\mathfrak{m}) = 2$. On the other hand, [18, Thm. 5.4] gives the Hilbert-Kunz multiplicity for each of these examples, giving our statement (see also [19]).

Given that each of the examples above is an invariant ring of a polynomial ring S under a finite group G, and in each case $s(R) = |G|^{-1}$, one may ask if this is true in general. The simple example $R = k[x_1, x_2, x_3]^{S_3}$, where S_3 acts naturally by permuting the variables, shows that something more is needed; R is regular, so $s(R) = 1$. When R is Gorenstein, we can completely analyze the F-signature in terms of the R-module structure of S.

Proposition 19. *Let $(R,\mathfrak{m}) \subseteq (S,\mathfrak{n})$ be a module-finite extension of CM local rings of characteristic p with R Gorenstein. Assume that R is a direct summand of S (as an R-module), that $R/\mathfrak{m} = S/\mathfrak{n}$ is infinite, and that $s(R)$ and $s(S)$ both exist. Let $r = \operatorname{rank}_R S$ and let f be the number of R-free direct summands in S. Then*

$$s(R) \geq f\frac{s(S)}{r}.$$

If in addition S is regular, then equality holds.

Proof. Let I be a minimal reduction of $\mathfrak{m}$, and let $J = (I, \Delta)$ where Δ represents the generator of the socle of R/I. Then by Proposition 15, $s(R) = e_{HK}(I,R) - e_{HK}(J,R)$. By [18, 2.7], $e_{HK}(I,R) = e_{HK}(IS,S)/r$ and similarly for J. Proposition 14 then shows that $s(R) \geq [s(S)\lambda(JS/IS)]/r$. Finally, write $S \cong R^f \oplus M$, where M is a MCM R-module with no free summands. Then Lemma 12 and the definitions of I and J show that $\lambda(JS/IS) = \lambda(JR^f/IR^f) + \lambda(JM/IM) = f$, as desired.

If S is regular, then we may bypass the use of Proposition 14 by observing that ([18, 1.4]) $e_{HK}(IS,S) = \lambda(S/IS)$ and similarly for JS, so $s(R) = f\frac{s(S)}{r}$. □

Together with Proposition 14, Proposition 19 gives the following interesting application to quotient singularities, a relationship between order of the group G such that R can be represented as S^G and the number of free summands of S as an R-module.

Corollary 20. *Let S be an F-finite regular local ring of characteristic p, with infinite residue field, and let G be a finite group acting on S with $p \nmid |G|$. Set $R = S^G$ and assume that R is Gorenstein. Write $S = R^f \oplus M$, where M has no nonzero free direct summands. Then*

$$|G| = \frac{f}{s(R)} \geq f \frac{e(R) - 1}{e(R) - e_{HK}(R)}.$$

References

1. M. Auslander, *Isolated singularities and the existence of almost split sequences*, Proc. ICRA IV, Lecture Notes in Mathematics, vol. 1178, Springer-Verlag, New York-Berlin, 1986, pp. 194–241.
2. W. Bruns and U. Vetter, *Determinantal Rings*, Springer-Verlag, Berlin, 1988.
3. R.O. Buchweitz, *Contributions à la théorie des singularités*, Thesis, University of Paris VII, 1981.
4. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.
5. J. Herzog, *Ringe mit nur endlich vielen Isomorphieklassen von maximalen unzerlegbaren Cohen–Macaulay Moduln*, Math. Ann. **233**, (1978), 21–34.
6. ———, *Ein Cohen–Macaulay-Kriterium mit Anwendungen auf den Konormalenmodul und den Differentialmodul*, Math. Z. **163** (1978), 149–162.
7. M. Hochster and C. Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math. Soc. **3** (1990), 31–116.
8. ———, *F-regularity and smooth base change*, Trans. Amer. Math. Soc. **346** (1994), 1–60.
9. C. Huneke, *Tight Closure and its Applications*, CBMS Lecture notes in Mathematics, vol. 88, American Math. Soc., 1996.
10. C. Huneke and B. Ulrich, *Powers of licci ideals*, Commutative algebra (Berkeley, CA, 1987) (M. Hochster, C. Huneke, and J. Sally, eds.), Math. Sci. Res. Inst. Publ., vol. 15, Springer, 1989, pp. 339–346.
11. C. Huneke and Y. Yao, *Unmixed local rings of minimal Hilbert-Kunz multiplicity are regular*, to appear, Proc. Amer. Math. Soc.
12. E. Kunz, *Kähler Differentials*, Vieweg Advanced Lectures in Mathematics, Vieweg, 1986.
13. G. Leuschke and R. Wiegand, *Ascent of finite Cohen–Macaulay type*, J. Algebra **228** (2000), 674–681.
14. H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Math., vol. 8, Cambridge University Press, Cambridge, 1986.
15. G. Seibert, *The Hilbert-Kunz function of rings of finite Cohen-Macaulay type*, Arch. Math. **69** (1997), no. 4, 286–296.
16. D. Smith, *A variation on a theme of Vasconcelos*, J. Algebra **225** (2000), no. 1, 381–390.
17. K. E. Smith and M. Van den Bergh, *Simplicity of rings of differential operators in prime characteristic*, Proc. London Math. Soc. (3) **75** (1997), no. 1, 32–62.
18. K.I. Watanabe and K.I. Yoshida, *Hilbert-Kunz multiplicity and and inequality between multiplicity and colength*, J. Alg. **230** (2000), 295–317.
19. K.I. Watanabe and K.I. Yoshida, *Hilbert-Kunz multiplicity of two-dimensional local rings* preprint.
20. R. Wiegand, *Local rings of finite Cohen–Macaulay type*, J. Algebra **203** (1998), 156–168.
21. Y. Yao, Developing thesis, University of Kansas.
22. Y. Yoshino, *Cohen–Macaulay modules over Cohen–Macaulay rings*, London Math. Soc. Lect. Notes Ser., vol. 146, Cambridge University Press, 1990.