Math 711: Lecture of September 10, 2007

In order to give our next characterization of tight closure, we need to discuss a theory of multiplicities suggested by work of Kunz and developed much further by P. Monsky. We use $\ell(M)$ for the length of a finite length module M.

Hilbert-Kunz multiplicities

Let (R, m, K) be a local ring, $\mathfrak{A}$ an m-primary ideal and M a finitely generated nonzero R-module. The standard theory of multiplicities studies $\ell(M/\mathfrak{A}^n M)$ as a function of n, especially for large n. This function, the *Hilbert function of M with respect to* $\mathfrak{A}$, is known to coincide, for all sufficiently large n, with a polynomial in n whose degree d is the Krull dimension of M. This polynomial is called the *Hilbert polynomial* of M with respect to $\mathfrak{A}$. The leading term of this polynomial has the form $\dfrac{e}{d!}\,n^d$, where e is a positive integer.

In prime characteristic $p > 0$ one can define another sort of multiplicity by using Frobenius powers instead of ordinary powers.

Theorem (P. Monsky). *Let (R, m, K) be a local ring of prime characteristic $p > 0$ and let $M \neq 0$ be a finitely generated R-module of Krull dimension d. Let $\mathfrak{A}$ be an m-primary ideal of R. Then there exist a positive real number γ and a positive real constant C such that*

$$|\ell(M/\mathfrak{A}^{[q]}M) - \gamma q^d| \leq C q^{d-1}$$

for all $q = p^e$.

One may also paraphrase the conclusion by writing

$$\ell(M/\mathfrak{A}^{[q]}M) = \gamma q^d + O(q^{d-1})$$

where the vague notation $O(q^{d-1})$ is used for a function of q bounded in absolute value by some fixed positive real number times q^{d-1}. The function $e \mapsto \ell(M/\mathfrak{A}^{[q]}M)$ is called the *Hilbert-Kunz* function of M with respect to $\mathfrak{A}$. The real number γ is called the *Hilbert-Kunz multiplicity* of M with respect to $\mathfrak{A}$. In particular, one can conclude that

$$\gamma = \lim_{q\to\infty} \frac{\ell(M/\mathfrak{A}^{[q]}M)}{q^d}.$$

Note that this is the behavior one would have if $\ell(M/\mathfrak{A}^{[q]}M)$ were eventually a polynomial of degree d in q with leading term γq^d: *but this is not true.* One often gets functions that are not polynomial.

When $M = R$, we shall write $\gamma_{\mathfrak{A}}$ for the Hilbert-Kunz multiplicity of R with respect to $\mathfrak{A}$.

Monsky's proof (cf. [P. Monsky, *The Hilbert-Kunz function*, Math. Ann. **263** (1983) 43–49]) of the existence of the limit γ is, in a sense, not constructive. He achieves this by proving that $\{\frac{\ell(M/\mathfrak{A}^{[q]}M)}{q^d}\}_q$ is a Cauchy sequence. The limit is only known to be a real number, not a rational number.

Example. Here is one instance of the non-polynomial behavior of Hilbert-Kunz functions. Let

$$R = (\mathbb{Z}/5\mathbb{Z})[[W,\, X,\, Y,\, Z]]/(W^4 + X^4 + Y^4 + Z^4),$$

with maximal ideal m. Then

$$\ell(R/m^{[5^e]}) = \frac{168}{61}(5^e)^3 - \frac{107}{61}(3^e).$$

See [C. Han and P. Monsky, *Some surprising Hilbert-Kunz functions*, Math Z. **214** (1983) 119–135.]

Hilbert-Kunz multiplicities give a characterization of tight closure in certain complete local rings:

Theorem. *Let $(R,\, m,\, K)$ be a complete local ring of prime characteristic $p > 0$ that is reduced and equidimensional. Let $\mathfrak{A}$ and $\mathfrak{B}$ be m-primary ideals such that $\mathfrak{A} \subseteq \mathfrak{B}$. Then $\mathfrak{B} \subseteq \mathfrak{A}^*$ if and only if $\gamma_{\mathfrak{A}} = \gamma_{\mathfrak{B}}$.*

This has two immediate corollaries. Suppose that $(R,\, m,\, K)$ and $\mathfrak{A}$ are as in the statement of the Theorem. Then, first, $\mathfrak{A}^*$ is the largest ideal $\mathfrak{B}$ between $\mathfrak{A}$ and m such that $\gamma_{\mathfrak{B}} = \gamma_{\mathfrak{A}}$. Second, if $u \in m$, then $u \in \mathfrak{A}^*$ if and only if $\gamma_{\mathfrak{A}+Ru} = \gamma_{\mathfrak{A}}$. Therefore, the behavior of Hilbert-Kunz multiplicities determines what tight closure is in the case of a complete local ring, since one can first reduce to the case of a complete local domain, and then to the case of an m-primary ideal. This in turn determines the behavior of tight closure in all algebras essentially of finite type over an excellent local (or semilocal) ring.

We shall spend some effort in these lectures on understanding the behavior of the rings R^+. One of the early motivations for doing so is the following result from [M. Hochster and C. Huneke, *Infinite integral extensions and big Cohen-Macaulay algebras*, Annals of Math. bf 135 (1992) 53–89].

Theorem. *Let $(R,\, m,\, K)$ be a complete (excellent also suffices) local domain of prime characteristic $p > 0$. Then R^+ is a big Cohen-Macaulay algebra over R.*

Although this result has been stated in terms of the very large ring R^+, it can also be thought of as a theorem entirely about Noetherian rings. Here is another statement, which is readily seen to be equivalent.

Theorem. *Let $(R,\, m,\, K)$ be a complete local domain of prime characteristic $p > 0$. Let $x_1,\, \dots\,, x_{k+1}$ be part of a system of parameters for R. Suppose that we have a relation $r_{k+1}x_{k+1} = r_1x_1 + \cdots + r_kx_k$. Then there is a module-finite extension domain S of R such that $r_{k+1} \in (x_1,\, \dots\,, x_k)S$.*

The point here is that R^+ is the directed union of all module-finite extension domains S of R.

We should note that this Theorem is not at all true in equal characteristic 0. In fact, if one has a relation

$$(*) \quad r_{k+1}x_{k+1} = r_1x_1 + \cdots + r_kx_k$$

on part of a system of parameters in a normal local ring $(R,\, m,\, K)$ that contains the rational numbers $\mathbb{Q}$ and $r_{k+1} \notin (x_1,\, \dots\,, x_k)R$, then there does not exist any module-finite extension S of R such that $r_{k+1} \in (x_1,\, \dots\,, x_k)S$. In dimension 3 or more there are always complete normal local domains that are not Cohen-Macaulay. One such example is given at the bottom of p. 12 and top of p. 13 of the Lecture Notes of September 5. In such a ring one has relations such as $(*)$ on a system of parameters with $r_{k+1} \notin (x_1,\, \dots\,, x_k)R$, and one can never "get rid of" these relations in a module-finite extension domain. Thus, these relations persist even in R^+.

One key point is the following:

Theorem. *Let R be a normal domain. Let S be a module-finite extension domain of R such that the fraction field $\mathcal{L}$ of S has degree d over the fraction field $\mathcal{K}$ of R. Suppose that $\dfrac{1}{d} \in R$, which is automatic if $\mathbb{Q} \subseteq R$. Then*

$$\frac{1}{d}\,\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}$$

gives an R-module retraction of S to R. In particular, for every ideal I of R, $IS \cap R = I$.

The last statement follows from part (a) of the Proposition on p. 11 of the Lecture Notes of September 5.

Here is an explanation of why trace gives such a retraction. First off, recall that $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}$ is defined as follows: if $\lambda \in \mathcal{L}$, multiplication by λ defines a $\mathcal{K}$-linear map $\mathcal{L} \to \mathcal{L}$. The value of $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}(\lambda)$ is simply the trace of this $\mathcal{K}$-linear endomorphism of $\mathcal{L}$ to itself. It may be computed by choosing any basis $v_1,\, \dots\,, v_d$ for $\mathcal{L}$ as a vector space over $\mathcal{K}$. If M is the matrix of the $\mathcal{K}$-linear map given by multiplication by λ, this trace is simply the sum of the entries on the main diagonal of this matrix. Its value is independent of the choice of basis, since a different basis will yield a similar matrix, and the similar matrix will have the same trace. It is then easy to verify that this gives a $\mathcal{K}$-linear map from $\mathcal{L} \to \mathcal{K}$.

Now suppose that $s \in S$. We want to verify that its trace is in R. There are several ways to argue. We shall give an argument in which we descend to the case where R is the integral closure of Noetherian domain, and we shall then be able to reduce to the case where R is a DVR, i.e., a Noetherian valuation domain, which is very easy.

Note that $\mathcal{K}\otimes_R S$ is a localization of S, hence, a domain, and that it is module-finite over $\mathcal{K}$, so that it is zero-dimensional. Hence, it is a field, and it follows that $\mathcal{K}\otimes_R S = \mathcal{L}$. Hence, every element of $\mathcal{L}$ has a multiple by a nonzero element of R that is in S. In particular, we can choose a basis $s_1, \ldots, s_d$ for $\mathcal{L}$ over $\mathcal{K}$ consisting of elements of S. Extend it to a set of generators $s_1, \ldots, s_n$ for S as an R-module. Without loss of generality we may assume that $s = s_n$ is among them. We shall now construct a new counter-example in which R is replaced by the integral closure R_0 of a Noetherian subdomain and S by

$$R_0 s_1 + \cdots + R_0 s_n.$$

To construct R_0, note that every $s_i s_j$ is an R-linear combination of $s_1, \ldots, s_n$. Hence, for all $1 \le i,\ j \le n$ we have equations

$$(*) \quad s_i s_j = \sum_{k=1}^{n} r_{ijk} s_k$$

with all of the r_{ijk} in R. For $j > d$, each s_j is a $\mathcal{K}$-linear combination of $s_1, \ldots, s_d$. By clearing denominators we obtain equations

$$(**) \quad r_j s_j = \sum_{k=1}^{d} r_{jk} s_j$$

for $d < j \le n$ such that every $r_j \in R - \{0\}$ and every $r_{jk} \in R$.

Let R_1 denote the ring generated over the prime ring (either $\mathbb{Z}$ or some finite field $\mathbb{Z}/p\mathbb{Z}$) by all the r_{ijk}, rjk, and r_j. Of course, R_1 is a Noetherian ring. Let R_0 be the integral closure of R_1 in its fraction field. (It is possible to show that R_0 is Noetherian, but we don't need this fact.) Now let $S_0 = R_0 s_1 + \cdots + R_0 s_n$, which is evidently generated as an R_0-module by $s_1, \ldots, s_n$. The equations $(*)$ hold over R_0, and so S_0 is a subring of S. It is module-finite over R_0. The equations $(**)$ hold over R_0, and $s_{d+1}, \ldots,\ s_n$ are linearly dependent on $s_1, \ldots, s_d$ over the fraction field $\mathcal{K}_0$ of R_0. Finally, $s_1, \ldots, s_d$ are linearly independent over $\mathcal{K}_0$, since this is true even over $\mathcal{K}$. Hence, $s_1, \ldots, s_d$ is a vector space basis for $\mathcal{L}_0$ over $\mathcal{K}_0$.

The matrix of multiplication by $s = s_n$ with respect to the basis $s_1, \ldots, s_d$ is the same as in the calculation of the trace of s from $\mathcal{L}$ to $\mathcal{K}$. This trace is not in R_0, since it is not in R. We therefore have a new counterexample in which R_0 is the integral closure of the Noetherian ring R_1. By the Theorem near the bottom of the first page of the Lecture Notes of September 13 from Math 711, Fall 2006, R_0 is an intersection of Noetherian valuation domains that lie between R_0 and $\mathcal{K}_0$. Hence, we can choose such a valuation domain V that does not contain the trace of s. We replace R_0 by V and S_0 by

$$T = Vs_1 + \cdots + Vs_n,$$

which gives a new counter-example in which the smaller ring is a DVR. The proof that T is a ring module-finite over V with module generators $s_1, \ldots, s_n$ such that a basis for the field extension is $s_1, \ldots, s_d$ is the same as in the earlier argument when we replaced R by R_0. Likewise, the trace of s with respect to the two new fraction fields is not affected. In fact, we can use any integrally closed ring in between R_0 and R.

Consequently, we may assume without loss of generality that $R = V$ is a DVR. Since S is a finitely generated torsion-free R-module and R is a principal ideal domain, S is free as R-module. Therefore, we may choose $s_1, \ldots, s_d \in S$ to be a free basis for S over R, and it will also be a basis for $\mathcal{L}$ over $\mathcal{K}$. The matrix for multiplication by s then has entries in R. It follows that its trace is in R, as required. $\square$

Corollary. *Let R be a normal domain containing the rational numbers $\mathbb{Q}$. Let S be an extension ring of R, not necessarily a domain.*

(a) *If S is module-finite over R, then R is a direct summand of S.*

(b) *If S is integral over R, then for every ideal I of R, $IS \cap R = I$.*

Proof. For part (a), we may choose a minimal prime P of S disjoint from the multiplicative system $R - \{0\} \subseteq S$. Then $R \to S \to S/P$ is module-finite over R, and since $P \cap R = \{0\}$, $\iota : R \hookrightarrow S/P$ is injective. By the result just proved, R is a direct summand of S/P: let $\theta : S/P \to R$ be a splitting, so that $\theta \circ \iota$ is the identity on R. Then the composite $S \to S/P \xrightarrow{\theta} R$ splits the map $R \to S$.

For the second part, suppose that $r \in R$ and $r \in IS$. Then there exist $f_1, \ldots, f_h \in I$ and $s_1, \ldots, s_h \in S$ such that

$$r = f_1 s_1 + \cdots + f_h s_h.$$

Let $S_1 = R[s_1, \ldots, s_h]$. Then S_1 is module-finite over R, and so by part (a), R is a direct summand of S_1. But we still have that $r \in IS_1 \cap R$, and so by part (a) of the Proposition on p. 11 of the Lecture Notes of September 5, we have that $r \in I$. $\square$

The fact that ideals of normal rings containing $\mathbb{Q}$ are contracted from integral extensions may seem to be an advantage. But the failure of this property in characteristic $p > 0$, which, in fact, enables one to use module-finite extensions to get rid of relations on systems of parameters, is perhaps an even bigger advantage of working in positive characteristic.

Note that the result on homomorphisms of plus closures of rings given in the Proposition at the top of p. 10 of the Lecture Notes of September 7 then yields:

Theorem. *Let $R \to S$ be a local homomorphism of complete local domains of prime characteristic $p > 0$. Then there is a commutative diagram:*

$$\begin{array}{ccc} B & \longrightarrow & C \\ \uparrow & & \uparrow \\ R & \longrightarrow & S \end{array}$$

such that B is a big Cohen-Macaulay algebra over R and C is a big Cohen-Macaulay algebra over S.

The point is that one can take $B = R^+$ and $C = S^+$, and then one has the required map $B \to C$ by the Proposition cited just before the statement of the Theorem. The same result can be proved in equal characteristic 0, but the proof depends on reduction to characteristic $p > 0$. When we discussed the existence of "sufficiently many big Cohen-Macaulay algebras" in mixed characteristic, it is this sort of result that we had in mind.

The following result of Karen Smith [K. E. Smith, *Tight Closure of Parameter Ideals,* Inventiones Math. **115** (1994) 41–60] (which also contains a form of the result when the ring is not necessarily local) may be viewed as providing another connection between big Cohen-Macaulay algebras and tight closure.

Theorem. *Let R be a complete (or excellent) local domain and let I be an ideal generated by part of a system of parameters for R. Then $I^* = IR^+ \cap R$.*

Property (3) stated on p. 7 of the Lecture Notes of September 7 implies that $IR^+ \cap R \subseteq I^*$, since R^+ is a directed union of module-finite extension domains S. The converse for parameter ideals is a difficult theorem.

This result suggests defining a closure operation on ideals of any domain R as follows: the *plus closure* of I is $IR^+ \cap R$. This plus closure is denoted I^+. Thus, plus closure coincides with tight closure for parameters ideals in excellent local domains of characteristic $p > 0$. Note that plus closure is not very interesting in equal characteristic 0, for if I is an ideal of a normal ring R that contains the rationals, $I^+ = I$.

It is very easy to show that plus closure commutes with localization. Thus, if it were true in general that plus closure agrees with tight closure, it would follow that tight closure commutes with localization. However, recent work of H. Brenner and others suggests that tight closure does not commute with localization in general, and that tight closure is not the same as plus closure in general. This is not yet proved, however.

Recently, the Theorem that R^+ is a big Cohen-Macaulay algebra when (R, m, K) is an excellent local domain of prime characteristic $p > 0$ has been strengthened by C. Huneke and G. Lyubeznik. See [C. Huneke and G. Lyubeznik, *Absolute integral closure in positive characteristic,* Advances in Math. **210** (2007) 498–504]. Roughly speaking, the original version provides a module-finite extension domain S of R that trivializes *one* given relation on parameters. The Huneke-Lyubeznik result provides a module-finite extension S that simultaneously trivializes *all* relations on all systems of parameters in the original ring. Their hypothesis is somewhat different. R need not be excellent: instead, it is assumed that R is a homomorphic image of a Gorenstein ring. Note, however, that the new ring S need not be Cohen-Macaulay: new relations on parameters may have been introduced.

The arguments of Huneke and Lyubeznik give a global result. The ring need not be assumed local. Under mild hypotheses, in characteristic p, the Noetherian domain R has a module finite extension S such that for every local ring R_P of R, all of the relations on all systems of parameters in R_P become trivial in S_P. In order to prove this result, we need to develop some local cohomology theory.

Finally, we want to mention the following result of Ray Heitmann, referred to earlier.

Theorem (R. Heitmann). *Let R be a complete local domain of mixed characteristic p. Let x, y, z be a system of parameters for R. Suppose that $rz \in (x, y)R$. Then for every $N \in \mathbb{N}$, $p^{1/N}r \in (x, y)R^+$.*

See [R. C. Heitmann, *The direct summand conjecture in dimension three*, Annals of Math. **156** (2002) 695–712].

The condition satisfied by r in this Theorem bears a striking resemblance to one of our characterizations of tight closure: see condition (#) near the bottom of p. 6 of the Lecture Notes of September 6. In a way, it is very different: in tight closure theory, the element c is anything but p, which is 0. Heitmann later proved (cf. [R. C. Heitmann, *Extended plus closure and colon-capturing*, J. Algebra **293** (2005) 407–426]) that in the Theorem above, one can use any element of R^+, not just p. The entire maximal ideal of R^+ multiplies r into $(x, y)R^+$.

Heitmann's result stated in the Theorem above already suffices to prove the existence of big Cohen-Macaulay algebras in dimension 3 in mixed characteristic: see [M. Hochster, *Big Cohen-Macaulay algebras in dimension three via Heitmann's theorem*, J. Algebra **254** (2002) 395–408].

It is possible that, for a complete local domain R of dimension 3 and mixed characteristic, R^+ is a big Cohen-Macaulay algebra. This is an open question.

It is also an open question whether an analogue of Heitmann's theorem holds in complete local domains of mixed characteristic in higher dimension. We shall further discuss these issues later.