715: Lectures of October 17, 2002

Last time we discussed the behavior of ideals generated by monomials in permutable regular sequences, showing that intersections and colons of such ideals can be computed formally, just as though the elements were indeterminates. We want to prove that the same holds for elements that satisfy the weaker condition of each subset that is in a given prime is part of a system of parameters once we localize at that prime. However, if the ring is not locally equidimensional, then we need to assume that the elements are part of a system of parameters modulo every minimal prime. We shall assume that the ring is reduced, and that there is a completely stable test element. Later, if the ring is reduced and essentially of finite type over an excellent local ring, we shall not need to assume that there is such a test element, because we will prove the existence of test elements. For example, we shall prove that for any $c \in R^{\circ}$ such that R_c is regular, c has a power that is a completely stable test element. Of course, all of this discussion is in positive characteristic p.

We shall say that elements $x_1, \ldots, x_n$ of R are *permutable parameters* if in every homomorphic image R_Q/P of a local ring of R_Q of R, the image of each subsequence of the x's contained in Q in R_Q/P is part of a system of parameters for R_Q/P. If R_Q is equidimensional, this is equivalent to the assertion that the image of every subsequence of the x's contained in Q is part of a system of parameters for R_Q. If R is local, it is equivalent to the assertion that those x_j that are not units form part of a system of parameters modulo every minimal prime of R.

Example. Let $R = K[x, y, z]_{(x,y,z)}/\big((x, y) \cap (z)\big)$. There are two minimal primes, the image of (x, y), whose quotient is one-dimensional, and the image of (z), whose quotient is two-dimensional. Note that the ideal $(x, y) \cap (z) = (xz, yz)$. In this two-dimensional local ring the images of $x - z$ and $y - z$ form a system of parameters: once one kills these the ring becomes $k[z]_(z)/(z^2)$. But these are not permutable parameters in the sense describe in the paragraph just above, because they do not form a system of parameters modulo the minimal prime which is the image of (x, y).

Before proving the result that one may perform intersection and colon operations on monomial ideals in permutable parameters formally, up to taking tight closure, we need several preliminaries. We note the following fact from the structure theory of complete local rings.

Theorem. *Let (R, m) be a complete local ring containing a field. Then R contains a field, which we shall denote by K, that maps isomorphically onto is residue class field R/m. K is called a coefficient field for R. If K is a coefficient field for R and $x_1, \ldots, x_s \in m$, then there is a unique continuous K-algebra map θ from the formal power series ring $K[[X_1, \ldots, X_s]]$ to R sending X_i to x_i for all i. Moreover:*

(a) *If the x_i generate an m-primary ideal, then R is module-finite over the image of θ.*
(b) *If the x_i form a system of parameters, so that $s = \dim R$, then the map θ is injective, and one may think of R as module-finite over a regular subring that is the formal power series ring in the parameters.*
(c) *If the x_i generate m, then the map θ is surjective, and R is a homomorphic image of $K[[X_1, \dots, X_s]]$.*

Proof. The existence of a coefficient field is beyond the scope of these notes: proofs are given in M. Nagata's book *Local Rings*, H. Matsumura's book *Commutative Algebra*, and in many other sources. Once one has the existence of K, one gets a unique K-algebra map of the polynomial ring $K[X_1, \dots, X_s] \to R$ which has a unique continuous extension to the completion $K[[X_1, \dots, X_s]]$ of $K[X_1, \dots, X_s]$ at the ideal $(X_1, \dots, X_s)$. This map sends $\sum_{i=0}^{\infty} F_i$, where every F_i is a homogeneous polynomial of degree i in $X_1, \dots, X_s$, to $\sum_{i=0}^{\infty} F_i(x_1, \dots, x_n)$.

To prove parts (a) and (c), let $I = (x_1, \dots, x_s)R$, and choose elements $u_1, \dots, u_h$ in R such that their images in R/I are a K-vector space basis. In the case of part (c), we may take $h = 1$ and $u_1 = 1$. Thus, every element $r \in R$ can be written in the form $\sum_{i=1}^{h} c_i u_i + \epsilon_1$, where $\epsilon_1 = \sum_{j=1}^{s} x_j r_j$. Here, the $c_i \in K$ and the $r_j \in R$.

Each r_j can be expanded in the same way, as $\sum_{i=1}^{h} c_j^{(j)} u_i + \sum_{k=1}^{s} x_k r_k^{(j)}$: when we substitute in the formula for r and collect the coefficients on the u_i, we get that $r = \sum_{i=1}^{h} \big(c_i + \sum_{j=1}^{s} c_i^{(j)} x_j\big) u_i + \epsilon_2$, where $\epsilon_2 = \sum_{1 \le j_1 \le j_2 \le s} r_{j_1, j_2} x_{j_1} x_{j_2}$. We may then expand each r_{j_1, j_2} in the same way.

Recursively, one gets a sequence of expansions $r = \sum_{i=1}^{h} \alpha_i^{(k)} u_i + \epsilon_k$, where each $\alpha_i^{(k)}$ is a polynomial of degree at most $k-1$ in the x_t with coefficients in K, $\alpha_i^{(k+1)} - \alpha_i^{(k)}$ is homogeneous in the x_t of degree k with coefficients in K, and ϵ_k is an R-linear combination of monomials of degree k in $x_1, \dots, x_s$. Thus, for every i, the $\alpha_i^{(k)}$ form a Cauchy sequence that converges to an element in the image of θ, call it α_i, and because R is m-adically separated and complete and the I-adic and m-adic topologies are the same, we have that $r = \sum_{i=1}^{h} \alpha_i u_i$. Thus, the u_i span R over the image of θ. In the case of part (c), $h = 1$, and $u_1 = 1$ spans R over the image of θ. Since 1 is in the image of θ, it follows that θ is surjective.

For part (b), suppose not only that the x_i generate an m-primary ideal, but also that $s = \dim R$, so that the x_j are a system of parameters. If the map $K[[X_1, \dots, X_s]] \to R$ has a kernel, P, that is not zero, then $\dim K[[X_1, \dots, X_s]]/P < \dim K[[X_1, \dots, X_s]] = s$, and since R is a module-finite extension of $\dim K[[X_1, \dots, X_s]]/P$, it has the same dimension as $\dim K[[X_1, \dots, X_s]]/P$. This is a contradiction, since we have assumed that $\dim R = s$. Thus, in the situation of part (b), θ is injective. $\square$

We also need a lemma about the behavior of the intersection and colon operations under flat base change: we want to apply this to the powers of the Frobenius endomorphism of a regular ring.

Lemma. *Let $R \to S$ be a flat ring homomorphism and let I_1, I_2 be ideals of R.*
(a) $I_1 S \cap I_2 S = (I_1 \cap I_2)S$.

(b) *If I_2 is finitely generated (which is automatic if R is Noetherian), then $I_1S :_S I_2S = (I_1 :_R I_2)S$.*
(c) *If R is a regular ring of characteristic $p > 0$, then $I_1^{[q]} \cap I_2^{[q]} = (I_1 \cap I_2)^{[q]}$ and $I_1^{[q]} : I_2^{[q]} = (I_1 : I_2)^{[q]}$.*

Proof. By applying $\_ \otimes_R S$ to the exact sequence $0 \to I \to R$ we see that for all ideals I of R, we may identify $I \otimes_R S$ with IS.

For part (a), note that there is a short exact sequence

$$0 \to I_1 \cap I_2 \xrightarrow{\alpha} I_1 \oplus_R I_2 \xrightarrow{\beta} I_1 + I_2 \to 0,$$

where $\alpha(u) = u \oplus u$ and $\beta(i_1 \oplus i_2) = i_1 - i_2$. Exactness is preserved when we apply $\_\otimes S$, and after we make the identifications in the paragraph above, the result follows.

To prove (b), note that the case where I_2 is generated by one element r, so that we are considering $I_1 : (r)$, was consider earlier: one uses that the exact sequence

$$0 \to \big(I_1 :_R (r)\big)/I_1 \to R/I_1 \xrightarrow{r} R/I_1$$

remains exact after applying $\_ \otimes_R S$. In the general case, $I_2 = (r_1, \ldots, r_h)$, and

$$I_1S : I_2S = \bigcap_j I_1S :_S r_jS = \bigcap_j \big(I_1 :_R (r_j)\big)S,$$

by the case where I_2 is principal, and this is $\big(\bigcap(I_1 :_R (r_j)\big)S$ (by the result of part (a)) $= (I_1 :_R I_2)S$, as required.

Now (c) follows at once from (a) and (b) by taking $R \to S$ to be $R \xrightarrow{F^e} R$, since F^e is flat when R is regular, and the expansion of $I \subseteq R$ is $I^{[q]}$ in the right hand copy of R. $\square$

We also need:

Proposition. *Let $x_1, \ldots, x_n$ be permutable parameters in a locally excellent ring R. Then they are also permutable parameters in the completion of every local ring of R.*

Proof. The definition of permutable parameters is clearly phrased in such a way that it passes automatically to the local rings of R. Therefore, it suffices to show that if R is an excellent local ring and $x_1, \ldots, x_n$ are permutable parameters, then they are permutable parameters in $\widehat{R}$. Let Q be a minimal prime of $\widehat{R}$ lying over P in R. Then $R_P \to \widehat{R}_Q$ is faithfully flat, which shows that P is minimal in R. In studying the problem, we may therefore replace R by R/P and $\widehat{R}$ by $\widehat{R}/P\widehat{R}$, which is the completion of R/P. Therefore, we may assume that R is a local domain, in which the x_i form part of a system of parameters (we may drop from consideration any x_j that have become invertible: they will also be invertible in the completion). But then the x_i are part of a system of parameters for the completion, and the completion is equidimensional. $\square$

Theorem. *Let R be a reduced locally excellent Noetherian ring that has a completely stable test element. Let $x_1, \ldots, x_n$ be elements of R that are permutable parameters. Let $T = \Lambda[X_1, \ldots, X_n]$, where Λ is either $\mathbb{Z}$ or else a subfield of R. Extend the obvious map of Λ to R to all of T by sending every X_i to the corresponding x_i, and let $\mathcal{M}$ be the set of all monomials in the X_i. Then for any two ideals I_1, I_2 generated by elements of $\mathcal{M}$:*
(a) $(I_1R)^* :_R I_2R \subseteq \bigl((I_1 :_T I_2)R\bigr)^*$.
(b) $(I_1R)^* \cap (I_2R)^* \subseteq \bigl((I_1 \cap I_2)R\bigr)^*$.

Proof. Let c be a completely stable test element. Suppose that $u \in R$ is an element that is contained in the ideal on the right but not in the ideal on the left. Then we can choose q such that cu^q is not in $J^{[q]}$, where $J = (I_1 :_T I_2)R$ or $(I_1 \cap I_2)R$, as the case may be. We can localize at a maximal ideal of R while preserving this, and we may then complete. Thus, we may assume that R is a complete reduced local ring. All of our hypotheses are preserved, but some of the x_j may have become units. Replacing the x_j that have become units by 1 commutes with the formal calculation of colons and intersections of monomial ideals: we leave this as an exercise. Thus, we may assume that we have a counterexample in a complete local ring. Moreover, since u is not in the tight closure of J, we may kill a minimal prime of the ring while preserving this: u will still be in the ideal on the right.

Thus, we may assume that R is a complete local domain, and that the x's are part of a system of parameters. Then we may choose a coefficient field K for R, and we may include the x's in a full system of parameters for R. Thus, from now on, we assume that $x_1, \ldots, x_n$ is a full system of parameters for the complete local domain R. Let $A = K[[x_1, \ldots, x_n]]$. Then R is a module-finite extension domain of A. Because the x_j form a regular sequence in A, colon and intersection in A may be computed formally. Thus, in the present case, the content of parts (a) and (b) does not change if we replace T by A, and consider what happens when we expand monomial ideals from A to R. The result now follows from the lemma immediately following. $\square$

Lemma. *Let A be a regular domain and R a module-finite extension domain of A. Let I_1 and I_2 be ideals of A.*
(a) $(I_1R)^* \cap (I_2)R^* \subseteq \bigl((I_1 \cap I_2)R\bigr)^*$.
(b) $(I_1R)^* :_R (I_2)R \subseteq \bigl((I_1 :_A I_2)R\bigr)^*$.

Proof. Choose a maximal free submodule $A^{\oplus h} = G \subseteq R$, so that R/G is an A-torsion module, and choose $d \in A - \{0\}$ that kills it, so that $dR \subseteq G = A^{\oplus h}$.

If $u \in I_1R \cap I_2R$, then for all q, $u^q \in I_1^{[q]}R \cap I_2^{[q]}R$. Then $du^q \subseteq I_1^{[q]}(dR) \cap I_2^{[q]}(dR) \subseteq I_1^{[q]}G \cap I_2^{[q]}G = (I_1^{[q]})^{\oplus h} \cap (I_2^{[q]})^{\oplus h} = \bigl((I_1^{[q]} \cap I_2^{[q]})\bigr)^{\oplus h}$. Since A is regular and F^e is flat, $I_1^{[q]} \cap I_2^{[q]} = (I_1 \cap I_2)^{[q]}$. Thus, $du^q \in \bigl((I_1 \cap I_2)^{[q]}\bigr)^{\oplus h} = (I_1 \cap I_2)^{[q]}G \subseteq (I_1 \cap I_2)^{[q]}R = \bigl((I_1 \cap I_2)R\bigr)^{[q]}$ for all q, and so $u \in \bigl((I_1 \cap I_2)R\bigr)^*$, as required.

Now suppose that $u \in (I_1R)^* \cap (I_2R)^*$. Then for all q, $cu^q \in (I_1R)^{[q]} \cap (I_2R)^{[q]} = (I_1^{[q]})R \cap (I_2^{[q]})R \subseteq \bigl((I_1^{[q]} \cap I_2^{[q]})R\bigr)^*$, by the paragraph above, and this is $\bigl((I_1 \cap I_2)^{[q]}R\bigr)^*$, so that $c^2u^q \in (I_1 \cap I_2)^{[q]}R = \bigl((I_1 \cap I_2)R\bigr)^{[q]}$ for all q, and this yields that $u \in \bigl((I_1 \cap I_2)R\bigr)^*$, as required. This completes the proof of part (a).

For the second part, first note that with G and d as in the first paragraph, if $u \in (I_1R) :_R (I_2)R$ then $uI_2R \subseteq I_1R$, and, for all q, $u^qI_1^{[q]}R \subseteq I_2^{[q]}R$. Multiplying by d yields that $du^qI_1^{[q]}R \subseteq I_2^{[q]}G$ and so $du^q \subseteq I_2^{[q]}G :_G I_1^{[q]}$. Since G is A-free, this implies that

$$du^q \in (I_2^{[q]} :_A I_1^{[q]})G = \big((I_2 :_A I_1)^{[q]}\big)G \subseteq \big((I_2 :_A I_1)^{[q]}\big)R = \big((I_2 :_A I_1)R\big)^{[q]}.$$

This yields the required result.

Finally, suppose that $u \in (I_1R)^* :_R I_2$. Then $uI_2R \subseteq (I_1R)^*$, and so, for all q, $cu^q(I_2R)^q \subseteq (I_1R)^q$, yielding

$$cu^q \in (I_1R)^q :_R (I_2R)^q = (I_1^{[q]})R :_R (I_2^{[q]})R \subseteq \big((I_1^{[q]} :_A I_2^{[q]})R\big)^*$$

by the result of the paragraph above, and, multiplying by c, we get that

$$c^2u^q \in (I_1^{[q]} :_A I_2^{[q]})R = (I_1 :_A I_2)^{[q]}R = \big((I_1 :_A I_2)R\big)^{[q]},$$

as required. □

We next note the following:

Theorem. *Let R be a Gorenstein local ring and suppose that there exists $x_1, \dots, x_d$ one system of parameters $x_1, \dots, x_d$ such that $I = (x_1, \dots, x_d)$ is tightly closed. Then every ideal is tightly closed, i.e., R is weakly F-regular.*

Proof. In an approximately Gorenstein local ring R, we have already noted that for every ideal to be tightly closed, it suffices for the ideals in a sequence of m-primary irreducible ideals cofinal with the powers of m to be tightly closed. In this case we may take the sequence to be $\{I_t\}_t$, where $I_t = (x_1^t, \dots, x_d^t)R$. Let $u \in R - I$ generate the one-dimensional socle in R/I, and let $u_t = (x_1 \cdots x_d)^{t-1}u$, which we have already seen generates the one-dimensional socle in R/I_t. Thus, every ideal of R strictly larger than I_t contains u_t. To show that $I_t = I_t^*$ it suffices to show that $u_t \notin I_t^*$. Suppose otherwise. Then for some $c \in R^\circ$, we have that $cu_t^q \in I_t^{[q]}$ for all $q \gg 0$. This means that for some $c \in R^\circ$, $c((x_1 \cdots x_d)^{qt-q}u^q \in (x_1^{tq}, \dots, x_d^{tq})R$ for all $q \gg 0$, and so $cu^q \in (x_1^{tq}, \dots, x_d^{tq})R :_R (x_1 \cdots x_d)^{qt-q}R$ for all $q \gg 0$, and since R is Gorenstein, the x_j form a regular sequence, and this colon ideal may be computed formally, and turns out to be $(x_1^q, \dots, x_d^{[q]})R = I^{[q]}$. Thus, $cu^q \in I^{[q]}$ for all $q \gg 0$, and so $u \in I^*$. But we assumed that I is tightly closed, and so $u \in I$, contradicting our choice of u. □

Hilbert-Kunz functions

Let (R, m, K) be a local ring of positive prime characteristic p, let I be an m-primary ideal, and let M be a finitely generated R-module. We shall use the notation $\mathrm{HK}_{M,I}(e)$ for $\ell(M/I^{[q]}M)$. $\mathrm{HK}_{M,I}(e)$ is called the *Hilbert-Kunz function* of M with respect to I. If M is omitted it is understood that $M = R$. Recall that $\dim M = \dim(R/\mathrm{Ann}_RM)$. As usual, q is an abbreviation for p^e. If f and g are functions of e with g non-negative, we write $f(e) = \mathrm{O}(g(e))$ to mean that there exists a positive constant C, independent of e, such that $|f(e)| \le Cg(e)$ for all $e \gg 0$. Note that $q = p^e$ is a function of e and may be used in defining other functions of e.

Example. Let R be regular with a system of parameters $x_1, \dots, x_d$ that is *regular*, i.e., that generates the maximal ideal. Then $\mathrm{HK}_m(e) = \ell(R/x_1^q, \dots, x_d^q) = q^d$.

We are aiming to prove:

Theorem (Monsky). *If* $\dim M = d$, *then there is a positive real constant* $\gamma_{M,I} = \gamma$ *such that* $\mathrm{HK}_{M,I}(e) = \gamma q^d + \mathrm{O}(q^{d-1})$.

The constant $\gamma = \gamma_{M,I}$ is killed the *Hilbert-Kunz multiplicity* of M with respect to I. We shall write simply γ_I for $\gamma_{R,I}$. We shall take a while, first to prove this theorem, and then to make the connection with tight closure theory. The point is that in a complete local domain, if $I \subseteq J$ are m-primary ideals then $J \subseteq I^*$ if and only if $\gamma_I = \gamma_J$.

We focus now on Monsky's theorem. We want to make several reductions to prove this.

(1) Replacing R by $R/\mathrm{Ann}_R M$ (so that M becomes faithful) and I by its image in $R/\mathrm{Ann}_R M$ does not change any values of the Hilbert-Kunz function.

(2) Completing R, M, I does not change any of the values of the Hilbert-Kunz function. Therefore, we may assume that R is complete.

(3) Let R be complete with coefficient field K, and let $x_1, \dots, x_n$ be a system of parameters for R. Let A be the regular ring $K[[x_1, \dots, x_n]] \subseteq R$. Let $\overline{K}$ be an algebraic closure of K, and let $B = \overline{K}[[x_1, \dots, x_d]]$. Since $K[x_1, \dots, x_n] \subseteq \overline{K}[x_1, \dots, x_n]$ is flat (in fact free), this remains true when we localize the rings at the respective maximal ideals generated by $x_1, \dots, x_n$ and then complete. Thus, $A = K[[x_1, \dots, x_n]] \to \overline{K}[[x_1, \dots, x_n]] = B$ is flat. We may replace R, I, and M by $B \otimes_A R = S$, $B \otimes_A I \cong IS = J$, and $B \otimes_A M \cong S \otimes_R M = N$, without changing the values of the Hilbert-Kunz function or the dimension of the module. (Note that because R is module-finite over A, S is module-finite over B, and $(x_1, \dots, x_d)S$ is in every maximal ideal of S. When we kill this ideal we get $B/(x_1, \dots, x_d) \otimes_A R/(x_1, \dots, x_d) \cong \overline{K} \otimes KR/(x_1, \dots, x_d)$, and since m (the maximal ideal of R) has become nilpotent in the quotient, this ring is local with residue field $\overline{K}$. It follows that S is local with residue field $\overline{K}$. Also, $N/J^{[q]}N \cong S \otimes_R M/I^{[q]}M$, and the length of the former over S is the same as the length of the latter over R. In fact, for any finite length R-module W having a filtration with the factors s copies of K, since S is flat over R this gives a filtration of $S \otimes_R W$ with the factors s copies of $S \otimes_R K = S/mS = \overline{K}$.) To see that the dimension of M does not change, it suffices to see this when M is a cyclic R-module. But we are making a faithfully flat base change with 0-dimensional closed fiber.) Thus, Monsky's theorem reduces to the case of a complete local ring with an algebraically closed residue class field.