NOTES AND EXERCISES ON F-SINGULARITIES (PRELIMINARY VERSION)

LINQUAN MA AND THOMAS POLSTRA

Contents

1. Introduction 2
2. Basics of Frobenius 3
2.1. The Frobenius endomorphism 3
2.2. F-finite rings 4
2.3. The rank of R^{1/p^e} 6
2.4. F-finite rings and excellence 8
3. F-pure rings and Fedder's criterion 10
3.1. Frobenius splittings and F-pure rings 10
3.2. Fedder's criterion for hypersurfaces 11
3.3. Frobenius powers of ideals 14
3.4. Fedder's criterion 14
4. Strongly F-regular rings 14
5. F-signature 19
5.1. Computational aspects of F-signature 21
5.2. The growth rate of R^{1/p^e} 27
5.3. Proof of Theorem 5.7 under the local hypothesis 29
5.4. Proof of Theorem 5.7 without the local hypothesis 29
5.5. F-signature exists 31
5.6. The splitting ideals 32
5.7. Positivity of F-signature and strongly F-regular rings 33
6. Hilbert-Kunz multiplicity 36
6.1. Hilbert-Kunz multiplicity of an $\mathfrak{m}$-primary ideal and connections with F-signature 38
References 40

Ma was supported in part by NSF Grant DMS #1600198 and NSF CAREER Grant DMS #1252860/1501102. Polstra was supported in part by NSF Postdoctoral Research Fellowship DMS #1703856.

Appendix A. Divisors and symbolic powers 42

(1) Fill in details on excellent and F-finite
(2) Maybe prove Radu-Andre characterizing geometrically regular maps
(3) F-finite rings are homomorphic image of regular rings
(4) Finite generation of anti-canonical: proof of splinter implies strong in dimension 2, survey Anurag's result, and Aberbach-Polstra
(5) Asymptotic stable of associated primes
(6) Frobenius action on local cohomology: F-rational and F-injective
(7) Finiteness of HSL numbers
(8) Finiteness of Frobenius text exponents (CM and gCM case)
(9) Deformation question: more details on Anurag's examples
(10) More general base change results on F-singularities
(11) F-signature one implies regular without using Hilbert–Kunz

1. Introduction

The action of Frobenius on a ring of positive characteristic has a long history of being used to characterize the singularities of the associated varieties. Work of Kunz shows that a Noetherian ring R of characteristic $p > 0$ is regular if and only if the Frobenius map on R is flat [Kun76]. The use of Frobenius was also applied to several important questions, for example the study of cohomological dimension [HS77] and the study of invariants rings under group actions [HR74] in positive characteristic.

With the development of tight closure theory [HH90] [HH94a] [HH94b] there was an explosion in the understanding of singularities via the Frobenius map, and a number of classes of singularities were formally introduced, which include F-regular, F-rational, F-pure and F-injective singularities. Quite surprisingly, via reduction mod p, these singularities have a correspondence to certain singularities in characteristic 0, whose definitions usually require resolution of singularities, for example see [HW02] [Smi97] [Har98] [HY03].

In this note we give an introduction and some recent development these "F-singularities", with a focus on the connection with Frobenius actions on local cohomology modules. We also introduce recent developments on an important invariant–F-signature, which measures how far a (strongly) F-regular singularity is from being a smooth point.

We leave a number of proofs of many (classical and modern) theorems as a series of exercises with hints. We encourage the interested readers to carry out these proofs on their own. From our perspective, after solving all exercises in the note, one should have enough knowledge and experience to start research in F-singularity theory.

Throughout this note, unless otherwise stated, all rings are assumed to be commutative, Noetherian, with 1.

2. Basics of Frobenius

2.1. **The Frobenius endomorphism.** Rings of prime characteristic $p > 0$ come equipped with a special endomorphism, namely the Frobenius endomorphism $F : R \to R$ defined by $F(r) = r^p$. The ring R is commutative and therefore F is multiplicative. Moreover, the map F is additive. Consider the binomial expansion of $F(r + s) = (r + s)^p = \sum_{i=0}^{p} \binom{p}{i} r^i s^{p-i}$ of two elements $r, s \in R$. Then all terms in the expansion have coefficient divisible by p, except the first and last term, and therefore $F(r + s) = r^p + s^p = F(r) + F(s)$, i.e., the map F is indeed a ring endomorphism. For each $e \in \mathbb{N}$ we can iterate the Frobenius endomorphism e times and obtain the eth Frobenius endomorphism $F^e : R \to R$ defined by $F^e(r) = r^{p^e}$ for each $e \in \mathbb{N}$.

Roughly speaking, the study of prime characteristic rings is often the study of algebraic and geometric properties of the Frobenius endomorphism. For example:

Exercise 1. Let R be a ring of prime characteristic $p > 0$. Show that R is reduced if and only if $F : R \to R$ is injective.

Exercise 2. Let R be a ring of prime characteristic $p > 0$ and $X = \operatorname{Spec}(R)$. Show that the Frobenius endomorphism $F : R \to R$ induces the identity map on the topological space X. That is, given $P \in X$ show that $F^{-1}(P) = P$.

There are several ways of studying the Frobenius endomorphism, but in these notes, we will be interested in the functors

$$F^e_* : \operatorname{Mod}(R) \to \operatorname{Mod}(R)$$

which are the functors obtained by restricting scalars along the Frobenius endomorphism.

That is given an R-module M we denote by F^e_*M (or M^{1/p^e}, but more on that later,) the R-module which as a set and as an Abelian group is M, but given an element $m \in M$, whose image in F^e_*M is denoted by F^e_*m, and element $r \in R$, multiplication is defined by $r \cdot F^e_*m = F^e_*r^{p^e}m$.

Exercise 3. Why is the functor $F^e_* : \operatorname{Mod}(R) \to \operatorname{Mod}(R)$ exact?

Suppose that R is a domain or even a reduced ring of prime characteristic $p > 0$ and let K be the total ring of fractions of R. If $\overline{K}$ is an algebraic closure of K then there are inclusions

$R \subseteq K \subseteq \overline{K}$ and we let

$$R^{1/p^e} = \{s \in \overline{K} \mid s^{p^e} \in R\}.$$

In other words, R^{1/p^e} is the collection of p^eth roots of elements of R.

Exercise 4. Suppose that R is a reduced ring of prime characteristic $p > 0$, let K be the total ring of fractions of R, and $\overline{K}$ an algebraic closure of K. Prove the following:

(1) $R \subseteq R^{1/p^e}$
(2) R^{1/p^e} is a ring of prime characteristic $p > 0$.
(3) R^{1/p^e} is unique up to non-unique isomorphism.
(4) $\varphi_e : R \to R^{1/p^e}$ defined by $\varphi_e(r) = r^{1/p^e}$ is an isomorphism of rings.

Exercise 5. Let R be a reduced ring of prime characteristic $p > 0$ and consider R^{1/p^e} as an R-module via the inclusion $R \subseteq R^{1/p^e}$. Show that the map $\psi_e : F^e_*R \to R^{1/p^e}$ defined by $\psi_e(F^e_*r) = r^{1/p^e}$ is an R-module isomorphism.

It is common practice for people to replace the use of F^e_*- and use the notation $(-)^{1/p^e}$. Specifically, if given an R-module M one denotes by M^{1/p^e} the module F^e_*M where the element m^{1/p^e} denotes the element F^e_*m. The advantage of using the notation M^{1/p^e} is that given $r \in R$ the element $rF^e_*m = F^e_*r^{p^e}m \in F^e_*M$ is identified as $rm^{1/p^e} \in M^{1/p^e}$, thus the multiplication may appear to be more natural. Nevertheless, it is advantageous to be comfortable with both sets of notation.

2.2. **F-finite rings.** A reduced ring R of prime characteristic $p > 0$ is said to be *F-finite* if for each $e \in \mathbb{N}$ the R-module R^{1/p^e} is finitely generated as an R-module.

Exercise 6. Show that a ring R of prime characteristic $p > 0$ is F-finite if and only if R^{1/p^e} is finitely generated for some $e \geq 1$.

The next set of exercises are standard, but show that F-finite rings are ubiquitous when one studies rings of prime characteristic.

Exercise 7. Let R be an F-finite ring of prime characteristic $p > 0$. prove the following:

(1) If $I \subseteq R$ an ideal then R/I is F-finite.
(2) If W a multiplicative subset of R then R_W is F-finite.
(3) If x an indeterminate then $R[x]$ and $R[[x]]$ are F-finite.
(4) Conclude that if $k = \mathbb{F}_p$, or if k is any other field such that $k^{1/p}$ is a finite dimensional k-vector space, then any ring R obtained by altering k by a combination of adjoining variables, adjoining analytic variables, localizing, and modding out by ideals produces an F-finite ring.

Exercise 8. Prove that a ring R of prime characteristic $p > 0$ is F-finite if and only if $R/\sqrt{0}$ is F-finite.

Exercise 9. If $(R, \mathfrak{m}, k)$ is a complete local ring of prime characteristic $p > 0$ then R is F-finite if and only if k is F-finite. (Hint: Cohen-Structure Theorem and Exercise 7.)

Exercise 10. Let R be an F-finite ring of prime characteristic $p > 0$ and M a finitely generated R-module. Show that M^{1/p^e} is a finitely generated R-module for each $e \in \mathbb{N}$. (Hint: Consider a surjective map $R^{\oplus N} \to M$ and use the fact that $(-)^{1/p^e} = F^e_* -$ is exact.)

Exercise 11. Let

$$S = \mathbb{F}_p[x_{1,1}, x_{2,1}, x_{2,2}, x_{3,1}, x_{3,2}, x_{3,3}, x_{4,1} \ldots],$$

W the multiplicative set

$$W = S - \Big((x_{1,1}) \cup (x_{2,1}, x_{2,2}) \cup (x_{3,1}, x_{3,2}, x_{3,3}) \cup \cdots\Big),$$

and let $R = S_W$. Nagata has shown R is a Noetherian domain of infinite Krull dimension, [Nag62]. Show that R is not F-finite.

As mentioned in the introduction, the singularities of a prime characteristic ring R are often studied via behavior of the Frobenius endomorphism. The most important theorem in this direction is Kunz's theorem:

Theorem 2.1 ([Kun69])**.** *Let R be a Noetherian ring of prime characteristic $p > 0$. Then R is regular if and only if R^{1/p^e} flat as an R-module for some, equivalently for all, $e \in \mathbb{N}$.*

We leave as an exercise the easier direction of Theorem 2.1.

Exercise 12. Let $(R, \mathfrak{m}, k)$ be an F-finite regular local ring. Show that R^{1/p^e} is free as an R-module. (Hint: Determine the depth of R^{1/p^e} as an R-module and apply the Auslander-Buchsbaum formula.)

By the Cohen-Structure Theorem a complete regular local ring $(R, \mathfrak{m}, k)$ of prime characteristic $p > 0$ and Krull dimension d is isomorphic to the power series ring $k[[x_1, \ldots, x_d]]$. If k is an F-finite field then R is F-finite by Exercise 7 and therefore R^{1/p^e} is free as an R-module by Exercise 12. Moreover, R^{1/p^e} will admit a "canonical" basis.

Exercise 13. Let R denote either $\mathbb{F}_p[[x_1, \ldots, x_n]]$ or $\mathbb{F}_p[x_1, \ldots, x_n]$. Prove that for each $e \in \mathbb{N}$ the set of elements $\{x_1^{i_1/p^e} \cdots x_n^{i_n/p^e} \mid 0 \leq i_j < p^e\}$ forms a basis of R^{1/p^e} as an R-module.

Exercise 14. Let k be an F-finite field and R denote either $k[[x_1, \ldots, x_n]]$ or $k[x_1, \ldots, x_n]$. Describe a basis of R^{1/p^e} as an R-module.

Exercise 15 (Very Difficult)**.** Find an example of a non-local F-finite regular domain R such that R^{1/p^e} is not free as an R-module for some $e \in \mathbb{N}$.

The next exercise gives a proof that localization functors and restricting scalars along an eth iterate of Frobenius commute.

Exercise 16. Let R be a ring of prime characteristic $p > 0$, M an R-module, and W a multiplicative set.

(1) Show that $\psi : (M^{1/p^e})_W \to (M_W)^{1/p^e}$ defined by $\psi(\frac{m^{1/p^e}}{s}) = (\frac{m}{s^{p^e}})^{1/p^e}$ is a map of R_W-modules.
(2) Show that $\varphi : (M_W)^{1/p^e} \to (M^{1/p^e})_W$ defined by $\varphi((\frac{m}{s})^{1/p^e}) = \frac{s^{(p^e-1)/p^e} m^{1/p^e}}{s}$ is a map of R_W-modules.
(3) Show that $\varphi \circ \psi$ is the identity map on $(M^{1/p^e})_W$.
(4) Show that $\psi \circ \varphi$ is the identity map on $(M_W)^{1/p^e}$.
(5) Conclude that $(M^{1/p^e})_W \cong (M_W)^{1/p^e}$ and therefore we may write M_W^{1/p^e} (or $F_*^e M_W$) to denote either of these isomorphic modules.

2.3. **The rank of R^{1/p^e}.** Suppose K is an F-finite field, i.e., $K^{1/p}$ is a finite dimensional vector space over K. Then $K \subseteq K^{1/p}$ is purely inseparable and therefore has a filtration of the form $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\gamma = K^{1/p}$ such that $K_i = K_{i-1}(\alpha)$, $\alpha^p \in K_i$, and α is the unique root of the irreducible polynomial $x^p - \alpha^p \in K_{i-1}[x]$. In particular, $\dim_K K^{1/p^e} = \operatorname{rank}_K K^{1/p^e} = p^{e\gamma}$ for all $e \in \mathbb{N}$.

Exercise 17. Let R be an F-finite domain of prime characteristic $p > 0$. Show that for each $P \in \operatorname{Spec}(R)$ that $\operatorname{rank}_{R_P} R_P^{1/p^e} = \operatorname{rank}_R R^{1/p^e}$. Conclude that there exists natural number $\gamma \in \mathbb{N}$ such that $\operatorname{rank}_R R^{1/p^e} = p^{e\gamma}$ for all $e \in \mathbb{N}$. (Hint: Use Exercise 16.)

Exercise 18. Let R be an F-finite ring of prime characteristic $p > 0$. Use the fact that R^{1/p^e} is finitely generated as an R-module to prove $R^{1/p^e} \otimes_R \widehat{R} \cong \widehat{R}^{1/p^e}$. Moreover, show that if $F : R \to R$ is the Frobenius endomorphism then the map $\widehat{F}$ obtained by applying $- \otimes_R \widehat{R}$ is the Frobenius endomorphism on $\widehat{R}$.

Exercise 19. Let $(R, \mathfrak{m}, k)$ be a reduced local F-finite ring of prime characteristic $p > 0$. Show that $\widehat{R}$ is reduced. (Hint: Use Exercise 1 and Exercise 18.)

Exercise 20. Let $(R, \mathfrak{m}, k)$ be an F-finite domain of prime characteristic $p > 0$ and let $\mathfrak{p}$ be a minimal prime ideal of $\widehat{R}$. (In particular $\widehat{R}_\mathfrak{p}$ is a field since $\widehat{R}$ is reduced.) Let K be the fraction field of R and let $L = \widehat{R}_\mathfrak{p}$. Verify the following:

(1) $L \otimes_K K^{1/p} \cong L \otimes_R R^{1/p}$ (Hint: $K^{1/p} \cong K \otimes_R R^{1/p}$ by Exercise 16.)

(2) $L \otimes_R R^{1/p} \cong L \otimes_{\widehat{R}} \widehat{R}^{1/p}$
(3) Conclude that $L^{1/p} \cong L \otimes_K K^{1/p}$ and therefore $\operatorname{rank}_L(L^{1/p}) = \operatorname{rank}_K(K^{1/p}) = \operatorname{rank}_R(R^{1/p})$.

Exercise 21. Let $(R, \mathfrak{m}, k)$ be a complete local F-finite domain of prime characteristic p. Let $x_1, \ldots, x_d$ be a system of parameters of R. Then the ring R is a finite extension of the regular local ring $A = k[[x_1, \ldots, x_d]]$ by the Cohen-Structure Theorem. Prove that $\operatorname{rank}_R(R^{1/p^e}) = \operatorname{rank}_A(A^{1/p^e})$.

Solution Outline. You should have computed the rank of A^{1/p^e} as an A-module in Exercise 14. In fact, you should have noticed $\operatorname{rank}_A(A^{1/p^e}) = \operatorname{rank}_k(k^{1/p^e})p^{ed}$. There is a commutative diagram:

$$\begin{array}{ccc} A & \longrightarrow & R \\ \downarrow & & \downarrow \\ A^{1/p^e} & \longrightarrow & R^{1/p^e} \end{array}$$

In particular, $\operatorname{rank}_A(R^{1/p^e}) = \operatorname{rank}_A(R)\operatorname{rank}_R(R^{1/p^e}) = \operatorname{rank}_A(A^{1/p^e})\operatorname{rank}_{A^{1/p^e}}(R^{1/p^e})$. It is now enough to show $\operatorname{rank}_A(R) = \operatorname{rank}_{A^{1/p^e}}(R^{1/p^e})$. □

Proposition 2.2. *If R is an F-finite ring, but not necessarily local, then R has finite Krull dimension.*

Proof. It is enough to check that each minimal prime $\mathfrak{p}$ of R that the quotient ring $R/\mathfrak{p}$ has finite Krull dimension. Therefore we may assume R is an F-finite domain. Exercise 16 implies for each $P \in \operatorname{Spec}(R)$ that $\operatorname{rank}_{R_P} R_P^{1/p^e} = \operatorname{rank}_R R^{1/p^e}$ and therefore there exists $\gamma \in \mathbb{N}$ such that $\operatorname{rank}_{R_P} R_P^{1/p^e} = p^{e\gamma}$ for each $P \in \operatorname{Spec}(R)$ and $e \in \mathbb{N}$. Therefore after replacing R by a localization at a prime $P \in \operatorname{Spec}(R)$ it is enough to show that if $(R, \mathfrak{m}, k)$ is a local F-finite domain of prime characteristic p then $\dim(R) \leq \gamma$ where γ is the unique integer so that $\operatorname{rank}_R R^{1/p^e} = p^{e\gamma}$ for all $e \in \mathbb{N}$.

Let $\widehat{R}$ be the completion of R. Then $\widehat{R}$ is reduced by Exercise 19 and if $\mathfrak{p}$ a minimal prime of $\widehat{R}$ then $L = \widehat{R}_{\mathfrak{p}}$ is a field and $\operatorname{rank}_L(L^{1/p}) = \operatorname{rank}_R R^{1/p}$ by Exercise 20. However, by Exercise 14 and Exercise 21 we have that $\operatorname{rank}_R(R^{1/p}) = \operatorname{rank}_{\widehat{R}/\mathfrak{p}}((\widehat{R}/\mathfrak{p})^{1/p}) = \operatorname{rank}_k(k^{1/p})p^{e\dim(\widehat{R}/\mathfrak{p})}$ (notice that $\operatorname{rank}_{\widehat{R}/\mathfrak{p}}((\widehat{R}/\mathfrak{p})^{1/p})$ did not depend on choice of minimal prime of $\widehat{R}$). In particular, since $\dim(\widehat{R}/\mathfrak{p}) = \dim(R)$ for some minimal prime of $\widehat{R}$ (and therefore for all minimal primes of $\widehat{R}$) we must have $\dim(R) \leq \gamma$. □

Exercise 22. Let R be an F-finite domain of prime characteristic $p > 0$. Let $P \subseteq Q$ be prime ideals of R and let $\kappa(P)$ and $\kappa(Q)$ denote the residue fields of R_P and R_Q respectively. Show that $\operatorname{ht}(P) + \log_p \operatorname{rank}_{\kappa(P)}(\kappa(P)^{1/p}) = \operatorname{ht}(Q) + \log_p \operatorname{rank}_{\kappa(Q)}(\kappa(Q)^{1/p})$.

2.4. **F-finite rings and excellence.** A Noetherian ring R is said to be *excellent* if R satisfies the following:

(1) The ring R is universally catenary.
(2) For each $P \in \operatorname{Spec}(R)$ the map $R_P \to \widehat{R_P}$ has geometrically regular fibers.
(3) If S is an R-algebra of finite type then the regular locus of S is an open subset of $\operatorname{Spec}(S)$.

We discuss below the definitions of the terms we just used. But first we state a theorem of Kunz concerning F-finite rings.

Theorem 2.3 ([Kun76]). *Every F-finite ring is excellent.*

The next set of exercises are meant to guide the reader through Kunz's proof of Theorem 2.3. Theorem 2.1 will be critical to the solution of several of the following exercises. First recall that a ring R is *catenary* if for each pair of prime ideals $P \subseteq Q$ any saturation of prime ideals from P to Q have the same length. A ring R is said to be *universally catenary* if every ring of finite type over R is catenary, i.e., every ring obtained from R by a combination of adjoining variables and modding out by ideals is catenary.

Exercise 23. Let R be an F-finite ring. Show that R is catenary. (Hint: First observe it is enough to show that if $(R, \mathfrak{m}, k)$ is a local F-finite domain then any saturated chain of prime ideals from 0 to $\mathfrak{m}$ have the same length. Consider an arbitrary saturation of 0 to $\mathfrak{m}$ by prime ideals and repeatedly use Exercise 22 to conclude the saturation must be of length $\dim(R)$.)

Exercise 24. Use Exercise 7 and Exercise 23 to conclude that F-finite rings are universally catenary.

We now guide the reader through a proof that the regular locus of an algebra of finite type over an F-finite ring is open. Let R be a Noetherian ring. Given ideal $I \subseteq R$ we let $V(I) = \{P \in \operatorname{Spec}(R) \mid I \subseteq P\}$ and given $s \in R$ we let $D(s) = \{P \in \operatorname{Spec}(R) \mid s \notin P\}$. Sets of the form $V(I)$ define all closed sets of $\operatorname{Spec}(R)$ and sets of the form $D(s)$ form a basis for the topology of $\operatorname{Spec}(R)$. Recall Nagata's criterion for openness:

Theorem 2.4 (Nagata's criterion for openness, [Mat89, pg. 187]). *Let R be a Noetherian ring and $U \subseteq \operatorname{Spec}(R)$ a subset of R. Then U is open in $\operatorname{Spec}(R)$ if and only if the following conditions are satisfied:*

(1) If $P, Q \in \operatorname{Spec}(R)$, $Q \subseteq P$, and $P \in U$ then $Q \in U$.
(2) If $P \in U$ then there exists $s \in R - P$ such that $V(P) \cap D(s) \subseteq U$.

Exercise 25. Let R be a Noetherian ring and M a finitely generated R-module. Let $U = \{P \in \operatorname{Spec}(R) \mid M_P \text{ is a free } R_P\text{-module}\}$. Show that U is an open subset of $\operatorname{Spec}(R)$.

Exercise 26. Let R be an F-finite ring and let $U = \{P \in \operatorname{Spec}(R) \mid R_P \text{ is regular}\}$. Show that U is open in $\operatorname{Spec}(R)$. Conclude that if S is an R-algebra of finite type then the regular locus of S is an open subset of $\operatorname{Spec}(S)$.

If $R \to S$ is a map of rings then $R \to S$ has *geometrically regular fibers* if for each $\mathfrak{p} \in \operatorname{Spec}(R)$ and purely inseparable finite field extension $\kappa(\mathfrak{p}) \subseteq L$ the ring $S \otimes_R \kappa(\mathfrak{p}) \otimes_{\kappa(\mathfrak{p})} L$ is regular. To prove Theorem 2.3 it remains to show that if R is F-finite and $P \in \operatorname{Spec}(R)$ then $R_P \to \widehat{R_P}$ has geometrically regular fibers. First observe since the property of being F-finite localizes we may replace R by R_P and show $R \to \widehat{R}$ has geometrically regular fibers.

Exercise 27. Let $(R, \mathfrak{m}, k)$ be local F-finite ring of prime characteristic p and let $\mathfrak{p} \in \operatorname{Spec}(R)$. Show that $\widehat{R} \otimes_R \kappa(\mathfrak{p})$ is a regular ring. (Hint: Observe first that we can replace R by $R/\mathfrak{p}$ so that $K = \kappa(\mathfrak{p})$ is the fraction field of R. To show $\widehat{R} \otimes_R K$ is regular first show that $\widehat{R} \otimes_R K$ is a 0-dimensional ring whose maximal ideals are in one to one correspondence with the minimal primes of $\widehat{R}$. Therefore to show $\widehat{R} \otimes_R K$ is regular it is enough to show $\widehat{R} \otimes_R K$ is reduced. Now use Exercise 1 and Exercise 18.)

Exercise 28. Let $(R, \mathfrak{m}, k)$ be an F-finite local domain of prime characteristic $p > 0$, K the fraction field of R, and $L = K[\alpha_1, \dots, \alpha_\ell]$ a purely inseparable finite field extension of K.

(1) Show that there exists an $e \in \mathbb{N}$ such that for each i the element $\alpha_i = \left(\frac{a_i}{b_i}\right)^{1/p^e}$ for some elements $a_i, b_i \in R$.
(2) Let $S = R[a_1^{1/p^e}, b_1^{1/p^e}, \dots, a_\ell^{1/p^e}, b_\ell^{1/p^e}]$. Show S is an F-finite domain which is module finite over R and has fraction field L.
(3) Show that S is a local ring with unique maximal ideal $\sqrt{\mathfrak{m}S}$.
(4) Let $\widehat{S}$ denote the completion of S with respect to its maximal ideal. Show $\widehat{R} \otimes_R L \cong \widehat{S} \otimes_S L$.

Exercise 29. Show that if R is an F-finite ring and $P \in \operatorname{Spec}(R)$ then $R_P \to \widehat{R_P}$ has geometrically regular fibers. (Hint: Reduce the problem to showing if $(R, \mathfrak{m}, k)$ is a local F-finite domain, K the fraction field of R, and L a purely inseparable finite extension of K then $\widehat{R} \otimes_R L$ is regular. Then use Exercise 27 and Exercise 28.)

In fact, we have the following stronger result relating F-finiteness and excellence.

Theorem 2.5 ([Kun69],[Kun76])**.** *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring of characteristic $p > 0$. Then R is F-finite if and only if R is excellent and k is F-finite.*

We already know that F-finite rings are excellent by Theorem 2.3, and if R is F-finite then so is $k = R/\mathfrak{m}$ and hence k is F-finite. We use the next set of exercises to guide the reader to the proof of the other direction of Theorem 2.5. We will need the following fact about excellent rings.

Theorem 2.6 ([sta16, Tag 032E]). *Let $(R, \mathfrak{m}, k)$ be an excellent domain with fraction field K. Then the integral closure of R in any finite extension L of K is module-finite over R.*

Exercise 30. Using the above theorem, show that if R is an excellent reduced ring such that the total quotient ring of R is F-finite, then R is F-finite.

Exercise 31. Use Cohen's structure theorem to prove that if $(R, \mathfrak{m}, k)$ is a Noetherian local ring such that k is F-finite, then $\widehat{R}$ is F-finite.

Exercise 32. Suppose $(R, \mathfrak{m}, k)$ is local and reduced, and $R \to \widehat{R}$ is geometrically regular. Prove that $\widehat{R}$ is also reduced (Hint: use the fact that reduceness is equivalent to R_0 and S_1). Let K be the total quotient ring of R. Show that the natural map $K^{1/p} \otimes_R \widehat{R} \to (K \otimes_R \widehat{R})^{1/p}$ is faithfully flat (Hint: The geometrically regular condition implies $L \otimes_R \widehat{R}$ is regular for every finite extension L over K. By Theorem 2.1, $L \otimes_R \widehat{R} \to (L \otimes_R \widehat{R})^{1/p}$ is faithfully flat. This implies $K^{1/p} \otimes_R \widehat{R} \to (K^{1/p} \otimes_R \widehat{R})^{1/p}$ is faithfully flat by taking direct limit, but this map factors through $(K \otimes_R \widehat{R})^{1/p}$).

Exercise 33. Prove the other direction of Theorem 2.5 as follows. First, it is enough to prove $R/\sqrt{0}$ is F-finite by Exercise 8 so we may assume that R and $\widehat{R}$ are both reduced (by Exercise 32). Use Exercise 31 to show that $\widehat{R}$ is F-finite. Then by Exercise 30, it is enough to prove the total quotient ring K of R is F-finite. Now use Exercise 32 to prove that $K^{1/p} \otimes_R \widehat{R}$ is finitely generated over $K \otimes_R \widehat{R}$. Conclude by proving that this implies that $K^{1/p}$ is finitely generated over K.

3. F-pure rings and Fedder's criterion

3.1. **Frobenius splittings and F-pure rings.** Let R be a ring and $M \to N$ a map of R-modules. We say that $M \to N$ *splits* if there is an R-linear map $N \to M$ such that $M \to N \to M$ is the identity map on M. Observe that if $M \to N$ splits then $N \cong M \oplus N/M$, i.e., M is a direct summand of N.

A *Frobenius splitting* is an onto R-linear map $R^{1/p^e} \to R$, i.e., a Frobenius splitting is a choice of an R-module decomposition $R^{1/p^e} \cong R \oplus M$. The information of a Frobenius splitting $R^{1/p^e} \to R$ is equivalent to knowing an R-linear map $R \to R^{1/p^e}$ (which isn't necessarily the natural inclusion) splits.

Exercise 34. Let S be either the regular local ring $\mathbb{F}_p[[x_1, \ldots, x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_1, \ldots, x_d]$.

(1) Show that S^{1/p^e} is a free S-module with basis $\{x_1^{i_1/p^e} \cdots x_d^{i_d/p^e} \mid 0 \leq i_j < p^e\}$.

(2) Show that for each tuple $(i_1, \ldots, i_d)$ with $0 \leq i_j < p^e$ there is a Frobenius splitting of $\varphi_{(i_1,\ldots,i_d)} : S^{1/p^e} \to S$ which is the S-linear map defined on basis elements as follows:

$$\varphi_{(i_1,\ldots,i_d)}(x_1^{j_1/p^e} \cdots x_n^{j_d/p^e}) = \begin{cases} 1 & (j_1, \ldots, j_d) = (i_1, \ldots, i_d) \\ 0 & (j_1, \ldots, j_d) \neq (i_1, \ldots, i_d) \end{cases}.$$

(3) Show that $\operatorname{Hom}_S(S^{1/p^e}, S)$ is a free S-module with with basis elements $\varphi_{(i_1,\ldots,i_n)}$ as described in part (2).

Exercise 35. Let k be an F-finite field which is not necessarily perfect. Let S be either the regular local ring $k[[x_1, \ldots, x_d]]$ or the standard graded polynomial ring $k[x_1, \ldots, x_d]$. How can the conclusions of Exercise 34 be extended to this scenario?

We say that an F-finite ring R is F*-pure* if for each $e \in \mathbb{N}$ there is a Frobenius splitting of $\varphi : R^{1/p^e} \to R$ such that $\varphi(1) = 1$, i.e., the Frobenius map $R \to R^{1/p^e}$ splits for each $e \in \mathbb{N}$.

Exercise 36. Let R be an F-finite ring. Show that R is F-pure if and only if $R \to R^{1/p^e}$ splits for some $e \in \mathbb{N}$.

Exercise 37. Let R be an F-finite ring and suppose R has a Frobenius splitting. Show that R is F-pure.

Exercise 38. Let R be an F-finite and F-pure ring. Show that R is reduced.

Exercise 39. Let R be an F-finite ring. Show that R is F-pure if and only if R_P is F-pure for each $P \in \operatorname{Spec}(R)$. (Hint: First prove that $R \to R^{1/p}$ splits if and only if the induced map $\operatorname{Hom}_R(R^{1/p}, R) \to \operatorname{Hom}_R(R, R)$ obtained by applying $\operatorname{Hom}_R(-, R)$ is surjective.)

Exercise 40. Let $(R, \mathfrak{m}, k)$ be an F-finite local ring of prime characteristic $p > 0$. Show that R is F-pure if and only if $\widehat{R}$ is F-pure.

3.2. **Fedder's criterion for hypersurfaces.** Our main goal is to outline a proof of Fedder's criterion, [Fed83], which gives an effective method of determining if the homomorphic image of a regular local (or regular graded) ring is F-pure. We begin our discussion of this criterion for hypersurfaces.

Let S be either the power series ring $\mathbb{F}_p[[x_1, \ldots, x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_1, \ldots, x_d]$ and $f \in S$. We would like to understand when the ring $S/(f)$ is F-pure, meaning that there exists $\varphi : (S/(f))^{1/p} \to S/(f)$ such that $\varphi(1^{1/p}) = 1$.

Our approach to determining whether $S/(f)$ is F-pure or not will require us to understand the set of homomorphisms $\mathrm{Hom}_{S/(f)}((S/(f))^{1/p}, S/(f))$.

Exercise 41. Let S be as above and $f \in S$. Denote by $(f)^{1/p}$ the ideal of $S^{1/p}$ generated by $f^{1/p}$.

(1) Show that if $\psi : S^{1/p} \to S$ is an S-linear map such that $\psi((f)^{1/p}) \subseteq (f)$ then there exists $\varphi : (S/(f))^{1/p} \to S/(f)$ which is $S/(f)$-linear and the following diagram commutes:

$$\begin{array}{ccc} (S/(f))^{1/p} & \xrightarrow{\varphi} & S/(f) \\ \uparrow & & \uparrow \\ S^{1/p} & \xrightarrow{\psi} & S. \end{array}$$

(2) Show that if $\varphi : (S/(f))^{1/p} \to S/(f)$ is an $S/(f)$-linear map then there exists S-linear map $\psi : S^{1/p} \to S$ such that $\psi((f)^{1/p}) \subseteq (f)$ and the following diagram commutes:

$$\begin{array}{ccc} (S/(f))^{1/p} & \xrightarrow{\varphi} & S/(f) \\ \uparrow & & \uparrow \\ S^{1/p} & \xrightarrow{\psi} & S. \end{array}$$

(3) Let $\mathcal{H}_f = \{\psi \in \mathrm{Hom}_S(S^{1/p}, S) \mid \psi((f)^{1/p}) \subseteq (f)\}$. Show that $\mathcal{H}_f$ is an S-module and use (1) and (2) above to conclude that there is a natural onto S-linear map

$$\mathcal{H}_f \xrightarrow{\Lambda_f} \mathrm{Hom}_{S/(f)}((S/(f))^{1/p}, S/(f)).$$

(4) Conclude that $S/(f)$ is F-pure if and only if there exists a Frobenius splitting of $S^{1/p}$ which is an element of $\mathcal{H}_f$.

Continue to let S and f be as above, $\mathcal{H}_f$ as in part (3) of Exercise 41, and $\mathcal{H} \xrightarrow{\Lambda_f} \mathrm{Hom}_{S/(f)}((S/(f))^{1/p}, S/(f))$ the natural onto S-linear map. To determine the structure of $\mathrm{Hom}_{S/(f)}((S/(f))^{1/p}, S/(f))$ and a criterion for $S/(f)$ to be F-pure it will be enough to better understand $\mathcal{H}_f$ and the kernel of Λ_f.

Exercise 42. Let $S \to T$ be a map of commutative rings and M an S-module. Show that $\mathrm{Hom}_S(T, M)$ has an T-module structure as follows: Given $\varphi \in \mathrm{Hom}_S(T, M)$ and $t \in T$ we let $t \cdot \varphi$ be the composition of maps

$$T \xrightarrow{t} T \xrightarrow{\varphi} M.$$

We will simply write $\varphi(t-)$ to denote this map and call $\varphi(t-)$ the map obtained from φ by premultiplication by t.

Exercise 43. Let S be either the regular local ring $\mathbb{F}_p[[x_1, \ldots, x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_1, \ldots, x_d]$. For each tuple $(i_1, \ldots, i_d)$ with $0 \le i_j < p$ let $\varphi_{(i_1,\ldots,i_d)}$ be as in Exercise 34 and let $\Phi = \varphi_{(p-1,\ldots,p-1)}$.

(1) Show that $\Psi : S^{1/p} \to \mathrm{Hom}_S(S^{1/p}, S)$ defined by $s^{1/p} \mapsto \Phi(s^{1/p}-)$ is an $S^{1/p}$-module isomorphism.
(2) Let $s \in S$. Show that $\Psi(s^{1/p}) \in \mathcal{H}_f$ if and only if $s^{1/p}f^{1/p} \in (f)S^{1/p}$ which happens if and only if $s^{1/p} \in (f)^{(p-1)/p}$.
(3) Use (2) to conclude that $\Psi : (f)^{(p-1)/p} \to \mathcal{H}_f$ is an isomorphism.
(4) Show that the kernel of the following composition

$$(f)^{(p-1)/p} \xrightarrow{\Psi} \mathcal{H}_f \xrightarrow{\Lambda_f} \mathrm{Hom}_{S/(f)}((S/(f))^{1/p}, S/(f))$$

is $(f)S^{1/p}$.
(5) Conclude that $\mathrm{Hom}_{S/(f)}((S/(f))^{1/p}, S) \cong \frac{(f)^{(p-1)/p}}{(f)S^{1/p}}$.

Exercise 44. Let S be either the regular local ring $\mathbb{F}_p[[x_1, \ldots, x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_1, \ldots, x_d]$ and let $\Psi : S^{1/p} \to \mathrm{Hom}_S(S^{1/p}, S)$ the isomorphism described in (1) of Exercise 43.

(1) Let $s \in S$. Show the following are equivalent:
   (a) There exists $\alpha^{1/p} \in S^{1/p}$ such that $\Psi(s^{1/p})(\alpha^{1/p}) = 1$.
   (b) $s^{1/p} \notin (x_1, \ldots, x_d)S^{1/p}$.
   (c) $s \notin (x_1^p, \ldots, x_d^p)S$.
(2) Conclude that if $f \in S$ then $S/(f)$ is F-pure if and only if $f^{p-1} \notin (x_1^p, \ldots, x_d^p)S$. (Hint: Use part (1) of this exercise in combination with (4) of Exercise 41 and (5) of Exercise 43.)

Exercise 45. Determine which of the following hypersurface rings are F-pure.

(1) $\mathbb{F}_2[x, y, z]/(x^3 + y^3 + z^3)$
(2) $\mathbb{F}_2[x, y, z]/(x^{11} + y^7 + xyz)$
(3) $\mathbb{F}_3[x, y, z]/(x^2 + y^2 + z^2)$
(4) $\mathbb{F}_7[x, y, z]/(x^3 + y^3 + z^3)$

Exercise 46. Let $S = \mathbb{Z}[x_1, \ldots, x_d]$ and $p_1, \ldots, p_\ell$ finitely many prime integers. Find $f \in S$ such that if p is a prime integer then $S/(f) \otimes_{\mathbb{Z}} \mathbb{F}_p$ is F-pure if and only if $p \in \{p_1, \ldots, p_\ell\}$.

Exercise 47. Let $S = \mathbb{Z}[x_1, \ldots, x_d]$ and $p_1, \ldots, p_\ell$ finitely many prime integers. Find $f \in S$ such that if p is a prime integer then $S/(f) \otimes_{\mathbb{Z}} \mathbb{F}_p$ is F-pure if and only if $p \notin \{p_1, \ldots, p_\ell\}$.

Exercise 48. Let S be either the regular local ring $\mathbb{F}_p[[x_1,\dots,x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_1,\dots,x_d]$ and let $f\in S$. Use the methods of previous exercises to show that for each $e\in\mathbb{N}$

$$\operatorname{Hom}_{S/(f)}((S/(f))^{1/p^e},S/(f))\cong\frac{(f)^{(p^e-1)/p^e}}{(f)S^{1/p^e}}.$$

3.3. **Frobenius powers of ideals.** Let R be a Noetherian ring of prime characteristic $p>0$. If $I\subseteq R$ is an ideal then the we define $I^{[p^e]}$ to be the ideal I expanded along Frobenius, i.e.,

$$I^{[p^e]}:=F^e(I)R.$$

Exercise 49. Let R be a ring of prime characteristic $p>0$ and $I=(x_1,\dots,x_\ell)$ an ideal of R. Show $I^{[p^e]}=(x_1^{p^e},\dots,x_\ell^{p^e})$.

Exercise 50. Let R be a Noetherian ring of prime characteristic $p>0$. Show there exists a $\ell\in\mathbb{N}$ such that

$$I^{\ell p^e}\subseteq I^{[p^e]}\subseteq I^{p^e}$$

for all $e\in\mathbb{N}$.

3.4. **Fedder's criterion.** Fedder's criterion for hypersurfaces can be extended to all homomorphic images of F-finite rings S for which $S^{1/p}$ is free as an S-module.

Theorem 3.1 (Fedder's Criterion, [Fed83])**.** *Let S be either the regular local ring $\mathbb{F}_p[[x_1,\dots,x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_1,\dots,x_d]$ and let $I\subseteq S$ be an ideal. Then S/I is F-pure if and only if $(I^{[p]}:_S I)\not\subseteq(x_1^p,\dots,x_d^p)$.*

Outline of proof. Let

$$\mathcal{H}_I=\{\varphi\in\operatorname{Hom}_S(S^{1/p},S)\mid\varphi(I^{1/p})\subseteq I\}.$$

Then $\mathcal{H}_I$ is an S-module and there is natural onto homomorphism $\mathcal{H}_I\xrightarrow{\Lambda_I}\operatorname{Hom}_{S/I}((S/I)^{1/p},S/I)$. In particular, S/I is F-pure if and only if there is a splitting φ of $S\subseteq S^{1/p}$ such that $\varphi((I)^{1/p})\subseteq I$. Let $\Psi:S^{1/p}\to\operatorname{Hom}_S(S^{1/p},S)$ be the isomorphism described in Exercise 43. Then $\Psi^{-1}(\mathcal{H}_I)=(IS^{1/p}:_{S^{1/p}}I^{1/p})$. Frobenius splittings of $S^{1/p}$ are in correspondence with elements not in $(x_1,\dots,x_d)S^{1/p}$ under the map $\Psi:S^{1/p}\to\operatorname{Hom}_S(S^{1/p},S)$. Hence there is a Frobenius splitting of $S^{1/p}$ in $\mathcal{H}_I$ if and only if $(IS^{1/p}:_{S^{1/p}}I^{1/p})\not\subseteq(x_1,\dots,x_d)S^{1/p}$ which is equivalent to $(I^{[p]}:_S I)\not\subseteq(x_1^p,\dots,x_d^p)$. ∎

4. Strongly F-regular rings

A Noetherian reduced F-finite ring R is called *strongly F-regular* if for every $c\in R$ that is not in any minimal prime of R, there exists $e\gg 0$ such that the map $R\to R^{1/p^e}$ sending 1 to c^{1/p^e} splits as a map of R-modules.

Exercise 51. Show that if R is strongly F-regular, then R is F-pure.

Exercise 52. Show that a reduced F-finite ring R is strongly F-regular if and only if R_P is strongly F-regular for every $P \in \operatorname{Spec} R$.

Perhaps the first example to keep in mind is the following.

Theorem 4.1. *An F-finite regular ring is strongly F-regular.*

Proof. Both properties localizes. So it enough to show that if $(R, \mathfrak{m}, k)$ is F-finite regular local, then R is strongly F-regular. By Exercise 12, R^{1/p^e} is a finite free R-module. For every $0 \neq c \in R$, there exists $e > 0$ such that $c^{1/p^e} \in R^{1/p^e}$ is part of a minimal basis of R^{1/p^e} over R: since otherwise $c^{1/p^e} \in \mathfrak{m}R^{1/p^e}$ for all e and thus $c \in \cap_e \mathfrak{m}^{[p^e]} = 0$ which is a contradiction. Since $c^{1/p^e} \in R^{1/p^e}$ is part of a minimal basis of R^{1/p^e} over R, the map $R \to R^{1/p^e}$ sending 1 to c^{1/p^e} splits. □

Exercise 53. Show that if R is a direct summand of S and S is strongly F-regular, then R is strongly F-regular. As a consequence, direct summand of regular rings are strongly F-regular.

We next prove some nice properties of strongly F-regular rings. We begin with a couple exercises.

Exercise 54. Show that an F-finite local ring R is strongly F-regular if and only if $\widehat{R}$ is strongly F-regular.

Exercise 55. Let $(R, \mathfrak{m}, k)$ be a strongly F-regular local ring. Show that R is a domain.

Theorem 4.2. *Let R be a strongly F-regular ring. Then $R \to S$ splits for any module-finite extension S of R.*

Proof. We may assume that R is local hence by Exercise 55, we may assume R is a domain. Killing a minimal prime of S, we may assume that S is also a domain. Now S is a torsion-free R-module, thus there exists an R-linear map $\theta\colon S \to R$ such that $\theta(1) = c \neq 0$. Since R is strongly F-regular, we can find e such that $R \to R^{1/p^e}$ sending 1 to c^{1/p^e} splits, call the splitting ϕ. Now consider the diagram with natural maps:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & S \arrow[d] \\ R^{1/p^e} \arrow[r] & S^{1/p^e} \end{tikzcd}$$

Now $\theta^{1/p^e}\colon S^{1/p^e} \to R^{1/p^e}$ sends 1 to c^{1/p^e}, thus $\phi \circ \theta^{1/p^e}$ sends $1 \in S^{1/p^e}$ to $1 \in R$. Therefore, $R \to S^{1/p^e}$ splits, this clearly implies $R \to S$ splits. □

A very big conjecture in tight closure and F-singularity theory is that whether the converse of the above theorem is true.

Conjecture 4.3. *Let R be an F-finite domain. If $R \to S$ splits for any module-finite extension S of R, then R is strongly F-regular.*

Some progress has been made towards a proof of Conjecture 4.3. The Conjecture is a theorem in the following scenarios:

(1) If R is Gorenstein by [HH94b].
(2) If R is $\mathbb{Q}$-Gorenstein by [Sin99].
(3) If the anti-canonical algebra of R is a Noetherian ring by [CEMS18].

For the reader not familiar with the terminology $\mathbb{Q}$-Gorenstein or anti-canonical algebra just know that there are implications (3) $\Rightarrow$ (2) $\Rightarrow$ (1) since every Gorenstein ring is $\mathbb{Q}$-Gorenstein and every $\mathbb{Q}$-Gorenstein ring has Noetherian anti-canonical algebra.

Exercise 56. Show that if R is strongly F-regular, then R is normal (Hint: consider $R \to R'$ where R' is the normalization of R and use Theorem 4.2). In particular, one-dimensional strongly F-regular rings are regular.

Our next goal is to show being strongly F-regular implies Cohen-Macaulay (this needs a little bit local cohomology theory).

Theorem 4.4. *Let R be an F-finite and strongly F-regular ring of prime characteristic $p > 0$. Then R is Cohen-Macaulay.*

Proof. All properties appearing in the statement of the theorem are local conditions. Thus we may assume R is local. We proceed by induction on the dimension of R. Recall that every strongly F-regular ring is a domain. If R is of dimension 0 then R is a field and every F-finite field is strongly F-regular.

Now suppose R has positive Krull dimension d. The properties of being F-finite, strongly F-regular, and Cohen-Macaulay are unaffected by completion. Thus we may further assume that R is complete. Moreover, the properties of being F-finite and strongly F-regular pass onto all localizations of R. Therefore, by induction, R_P is Cohen-Macaulay for all $P \in \operatorname{Spec}(R) - \{\mathfrak{m}\}$. The ring R admits a dualizing module ω_R. Therefore

$$H^i_{\mathfrak{m}}(R)^\vee \cong \operatorname{Ext}^{d-i}_R(\omega_R, R).$$

The module $\operatorname{Ext}^{d-i}_R(\omega_R, R)$ is Noetherian. Hence if $P \in \operatorname{Spec}(R) - \{\mathfrak{m}\}$ then $\operatorname{Ext}^{d-i}_R(\omega_R, R)_P \cong \operatorname{Ext}^{d-i}_{R_P}(\omega_{R_P}, R_P)$ which is 0 whenever $i < d$ (since ω_{R_P} is Cohen-Macaulay whenever R_P is Cohen-Macaulay). Hence $\operatorname{Ext}^{d-i}_R(\omega_R, R)$ is supported only at the maximal ideal whenever

$i < d$ and therefore has finite length. By Matlis duality, the local Cohomology module $H^i_{\mathfrak{m}}(R)$ has finite length whenever $i < \dim(R)$.

Let c be a nonzero element of R inside the maximal ideal and let $i < d$. For each $\eta \in H^i_{\mathfrak{m}}(R)$ there is a power of c, say c^N such that $c^N\eta = 0$. But $H^i_{\mathfrak{m}}(R)$ is a Noetherian R-module. Hence there exists N such that $c^N H^i_{\mathfrak{m}}(R) = 0$. Replacing c with c^N we may assume $cH^i_{\mathfrak{m}}(R) = 0$.

Observe $cH^i_{\mathfrak{m}}(R) = 0$ if and only if $c^{1/p^e} H^i_{\mathfrak{m}^{1/p^e}}(R^{1/p^e}) = 0$ for all $e \in \mathbb{N}$. Moreover,

$$H^i_{\mathfrak{m}^{1/p^e}}(R^{1/p^e}) = H^i_{\mathfrak{m}R^{1/p^e}}(R^{1/p^e}) = H^i_{\mathfrak{m}}(R^{1/p^e}).$$

We are assuming R is strongly F-regular. Hence there is an $e \in \mathbb{N}$ and R-linear map $R^{1/p^e} \to R$ such that the composition of the following maps is the identity map on R:

$$R \subseteq R^{1/p^e} \xrightarrow{\cdot c^{1/p^e}} R^{1/p^e} \to R.$$

Applying the i-th local cohomology functor $H^i_{\mathfrak{m}}(-)$ to the above composition of maps we see that the identity map on $H^i_{\mathfrak{m}}(R)$ factors through the 0-map on $H^i_{\mathfrak{m}}(R^{1/p^e})$ and therefore $H^i_{\mathfrak{m}}(R) = 0$ whenever $i < d$. $\square$

We next prove an extremely useful criterion for strong F-regularity.

Theorem 4.5. *Let R be a reduced and F-finite ring. Suppose there exists c not in any minimal prime of R such that R_c is strongly F-regular (e.g., R_c is regular). Then R is strongly F-regular if and only if there exists $e > 0$ such that the map $R \to R^{1/p^e}$ sending 1 to c^{1/p^e} splits as R-modules.*

Proof. Given any $d \in R$ that is not in any minimal prime of R, the image of d is not in any minimal prime of R_c. Therefore, since R_c is strongly F-regular, there exists $e_0 > 0$ and a map $\phi \in \mathrm{Hom}_{R_c}(R_c^{1/p^{e_0}}, R_c)$ such that $\phi(d^{1/p^{e_0}}) = 1$. Since we have $\mathrm{Hom}_{R_c}(R_c^{1/p^{e_0}}, R_c) \cong \mathrm{Hom}_R(R^{1/p^{e_0}}, R)_c$, $\phi = \varphi/c^n$ for some $n > 0$ and some $\varphi \in \mathrm{Hom}_R(R^{1/p^{e_0}}, R)$. It follows that $\varphi(d^{1/p^{e_0}}) = c^n$. Now we pick $e_1 > 0$ such that $n/p^{e_1} < 1/p^e$, since $R \to R^{1/p^e}$ sending 1 to c^{1/p^e} splits, it follows that $R \to R^{1/p^{e_1}}$ sending 1 to $c^{n/p^{e_1}}$ splits (check this!). We call such splitting θ. Finally we consider the map $\theta \circ \varphi^{1/p^{e_1}}\colon R^{1/p^{e_0 e_1}} \to R^{1/p^{e_1}} \to R$, it sends $d^{1/p^{e_0 e_1}} \to c^{n/p^{e_1}} \to 1$. $\square$

We also have the a Fedder type criterion for strongly F-regular rings.

Theorem 4.6. *Let S be either the regular local ring $\mathbb{F}_p[[x_1, \ldots, x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_1, \ldots, x_d]$ and let $I \subseteq S$ be a radical ideal. Then S/I is F-regular if and only if for every c not in any minimal prime of I, there exists $e > 0$ such that $c(I^{[p^e]} :_S I) \not\subseteq (x_1^{p^e}, \ldots, x_d^{p^e})$.*

We next give some examples of strongly F-regular rings.

Exercise 57. Let $R = k[x_0, \dots, x_d]/(x_0^n + x_1^n + \cdots x_d^n)$ where k is an F-finite field of characteristic $p > 0$. Then R is a hypersurface of dimension d and degree n. Prove that, if $n \leq d$ and $p \nmid n$, R is strongly F-regular.

Example 4.7. Let $R_d = K[x_1, \dots, x_{2d-1}]/(x_{2k-1}x_{2k} - x_{2k+1}^2 | 1 \leq k \leq d-1)$ where K is an F-finite field of characteristic $p > 0$ (e.g., the case $d = 2$ is the hypersurface $K[x, y, z]/xy - z^2$). We claim that R is a strongly F-regular complete intersection of dimension d.

Proof. We leave the reader to check that R_d is a complete intersection of dimension d (hint: $x_1, x_2, x_4, \dots, x_{2d-2}$ is a system of parameters). To show R_d is strongly F-regular, we use Theorem 4.5 and Theorem 4.6. First of all, $R_1 = K[x_1]$ is regular so strongly F-regular by Theorem 4.1. Suppose R_d is strongly F-regular, we show R_{d+1} is strongly F-regular. We consider

$$R_{d+1}[\frac{1}{x_1}] = \frac{K[x_3, \dots, x_{2d+1}]}{(x_{2k-1}x_{2k} - x_{2k+1}^2 | 2 \leq k \leq d-1)}[x_1, \frac{1}{x_1}] \cong R_d[x, \frac{1}{x}].$$

By induction hypothesis, R_d is strongly F-regular, so adjoining a new variable $R_d[x]$ is also strongly F-regular (for example one can use Theorem 4.6), and thus $R_{d+1}[\frac{1}{x_1}] \cong R_d[x, \frac{1}{x}]$ is strongly F-regular by Exercise 52. Therefore by Theorem 4.5, it is enough to prove that there exists $e > 0$ such that $R_{d+1} \to R_{d+1}^{1/p^e}$ sending 1 to x_1^{1/p^e} splits. This is equivalent to finding $e > 0$ such that

$$x_1 \prod_{k=1}^{d} (x_{2k-1}x_{2k} - x_{2k+1}^2)^{p^e-1} \notin (x_1^{p^e}, \dots, x_{2d+1}^{p^e})(\text{check this!}).$$

At this point, we note that, when $p^e > 2^{d-1} + 1$, there is one term on the left hand side

$$x_1 \binom{p^e-1}{1} (x_1x_2)^{p^e-2} x_3^2 \binom{p^e-1}{2} (x_3x_4)^{p^e-3} (x_5^2)^2 \cdots\cdots \binom{p^e-1}{2^{d-1}} (x_{2d-1}x_{2d})^{p^e-2^{d-1}-1} (x_{2d+1}^2)^{2^{d-1}}.$$

It is easy to check that the exponent of every x_i is $\leq p^e - 1$ (and there is no cancellation of this term), so it is not contained in $(x_1^{p^e}, \dots, x_{2d+1}^{p^e})$. $\square$

Exercise 58. Use the same method to check that $R = K[x_1, \dots, x_{2d-1}]/(x_{2k-1}x_{2k} - x_{2k+1}^{N_k} | 1 \leq k \leq d-1)$ where K is an F-finite field of characteristic $p > 0$ and $N_k \geq 2$ are arbitrary integers, is strongly F-regular.

In this example, $(R, \mathfrak{m}, K)$ is a standard graded complete intersection of dimension d and embedding dimension $2d - 1$, cut out by $d - 1$ degree 2 forms. In particular, the Hilbert-Samuel multiplicity of R at the homogenous maximal ideal $\mathfrak{m}$ is $e(\mathfrak{m}, R) = 2^{d-1}$. In fact, these data are in some sense “sharp”:

Exercise 59. Let $(R, \mathfrak{m}, k)$ be a strongly F-regular complete intersection of dimension d. Show that the embedding dimension of R is less than or equal to $2d - 1$.

Conjecture 4.8 (Watanabe)**.** *Let $(R, \mathfrak{m}, k)$ be a strongly F-regular complete intersection of dimension d. Then $e(\mathfrak{m}, R) \leq 2^{d-1}$.*

The interesting (and still open) case of the above conjecture is the case that R is not standard graded. In fact, we have

Exercise 60 (Hard)**.** Let $(R, \mathfrak{m}, k)$ be a strongly F-regular complete intersection of dimension d that is standard graded over k (where $\mathfrak{m}$ denote the unique homogeneous maximal ideal). Show that $e(\mathfrak{m}, R) \leq 2^{d-1}$.

5. F-signature

If R is a commutative ring and M a finitely generated R-module then the *free rank of M* is denoted $\operatorname{frk}_R M$, or simply $\operatorname{frk}(M)$ if R is understood, and is the largest rank of a free R-module F for which there exists a surjective R-linear map $M \to F$.

Exercise 61. Let R be a commutative ring and M a finitely generated R-module. Observe that $\operatorname{frk}(M)$ is equal to largest rank of a free module F which can be realized as a direct summand of M. In particular, $M \cong F \oplus N$ for some R-module N and N does not have a free summand.

Now suppose R is an F-finite domain of prime characteristic $p > 0$. The *eth Frobenius splitting number* of R is the free rank of R^{1/p^e} and is denoted by $a_e(R)$. Clearly, $a_e(R) \leq \operatorname{rank}(R^{1/p^e})$ for each $e \in \mathbb{N}$ and therefore the ratio $a_e(R)/\operatorname{rank}(R^{1/p^e}) \leq 1$ for each $e \in \mathbb{N}$. The F-signature of R is denoted by $s(R)$ and is defined to be the limit

$$s(R) = \lim_{e \to \infty} \frac{a_e(R)}{\operatorname{rank}(R^{1/p^e})}.$$

Convergence of the sequence $\frac{a_e(R)}{\operatorname{rank}(R^{1/p^e})}$ is not at all immediately obvious. In fact, convergence of the above sequence was an open problem of interest for quite sometime. Existence of F-signature under the local hypothesis was established in [Tuc12] and without the local hypothesis in [DPY16].

We guide the reader though an elementary proof of the existence of F-signature under the local hypothesis in Section 5.5. But first, observe that for e fixed the ratio $a_e(R)/\operatorname{rank}(R^{1/p^e}) = 1$ if and only if R^{1/p^e} is a free R-module.

Exercise 62. Let $(R, \mathfrak{m}, k)$ be an F-finite regular local ring of prime characteristic $p > 0$. Prove that $s(R) = 1$.

Amazingly enough, the converse of Exercise 62 holds!

Theorem 5.1. [HL02] *Let $(R, \mathfrak{m}, k)$ be an F-finite local ring of prime characteristic $p > 0$. If $s(R) = 1$ then R is a regular local ring.*

Exercise 62 brings up an interesting question, what is the growth rate of $a_e(R)$ when R is assumed to be a regular F-finite domain which is not assumed to be local? There do exist regular domains R for which R^{1/p^e} is not free as an R-module, see Exercise 15. However, a beautiful theorem of Serre allows us to effectively estimate the growth rate of $a_e(R)$ when R is assumed to be regular F-finite domain, but not necessarily local.

Theorem 5.2 (Serre's Theorem on Projective modules)**.** *Let R be a Noetherian domain of finite Krull dimension d and P a finitely generated projective R-module of rank at least $d+1$. Then P has a free summand.*

Use Theorem 5.2 to solve the following:

Exercise 63. Let R be an F-finite regular domain of prime characteristic $p > 0$. Let d be the Krull dimension of R. Show that for each $e \in \mathbb{N}$

$$\operatorname{rank}(R^{1/p^e}) - d \leq a_e(R) \leq \operatorname{rank}(R^{1/p^e}).$$

Conclude that the F-signature of R exists and is equal to 1.

We now focus our attention to the local scenario. When R is assumed to be local the free rank of a finitely generated R-module is "well-behaved." If the reader is interested in learning more about the F-signature of a non-local ring then we direct their attention to [DPY16].

Exercise 64. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring, not necessarily of prime characteristic, and let M be a finitely generated R-module.

(1) Suppose that $M \cong F \oplus \widetilde{M}$ where F is a free R-module and $\widetilde{M}$ is an R-module for which there does not exist an onto R-linear map $\widetilde{M} \to R$. Show that

$$\{\eta \in M \mid \varphi(\eta) \in \mathfrak{m}, \forall \varphi \in \operatorname{Hom}_R(M, R)\} \cong (\mathfrak{m}F) \oplus \widetilde{M}.$$

(2) Let $N = \{\eta \in M \mid \varphi(\eta) \in \mathfrak{m}, \forall \varphi \in \operatorname{Hom}_R(M, R)\}$. Observe that N is a submodule of M and $\operatorname{frk}(M) = \dim_k(M/N)$.

(3) If $M \cong G \oplus \overline{M}$ is another direct sum decomposition of M such that G is a free R-module and $\overline{M}$ is an R-module for which there does not exist an onto R-linear map $\overline{M} \to R$ then $\operatorname{rank}(F) = \operatorname{rank}(G)$.

(4) Conclude that if $(R, \mathfrak{m}, k)$ is an F-finite local ring of prime characteristic $p > 0$ and $R^{1/p^e} \cong F \oplus M$ where F is a free R-module and M does not have a free summand, then $\operatorname{rank}(F) = a_e(R)$.

Exercise 64 provides us a valuable tool for measuring the splitting numbers of R. Specifically, if $(R, \mathfrak{m}, k)$ is a local F-finite domain we set $I_e = \{r \in R \mid \varphi(r^{1/p^e}) \in \mathfrak{m}, \forall \varphi \in \operatorname{Hom}_R(R^{1/p^e}, R)\}$. Exercise 64 tells us $a_e(R) = \dim_k(R^{1/p^e}/I_e^{1/p^e})$ where I_e^{1/p^e} is the set of elements of R^{1/p^e} obtained by taking p^eth roots of elements of I_e.

Exercise 65. Let $(R, \mathfrak{m}, k)$ be an F-finite domain of prime characteristic $p > 0$ and Krull dimension d.

(1) Verify the claim that $a_e(R) = \dim_k(R^{1/p^e}/I_e^{1/p^e})$.
(2) Show I_e is an ideal of R containing $\mathfrak{m}^{[p^e]}$.
(3) Show that $\frac{a_e(R)}{\operatorname{rank}(R^{1/p^e})} = \frac{\ell(R/I_e)}{p^{ed}}$ where $\ell(R/I_e)$ denotes the length of R/I_e as an R-module. (Hint: Exactness of taking p^eth roots and Exercise 22 will be of use.)

5.1. **Computational aspects of F-signature.** Computing the F-signature of a local ring is quite challenging, even for hypersurfaces! However, we will describe a concrete method of computing the F-signature of an affine toric variety. But first, lets discuss the hypersurface case.

Let S be either the regular local ring $\mathbb{F}_p[[x_0, \ldots, x_d]]$ or the standard graded polynomial ring $\mathbb{F}_p[x_0, \ldots, x_d]$, $f \in S$ a nonzero element, and $R = S/(f)$.

Exercise 66. Let S, f, and R be as above. Show that $\operatorname{rank}(R^{1/p^e}) = p^{ed}$ for all $e \in \mathbb{N}$. (Hint: Use Exercise 22.)

Exercise 66 tells us that the F-signature of the d-dimensional hypersurface R is

$$s(R) = \lim_{e \to \infty} \frac{a_e(R)}{p^{ed}}.$$

Moreover, we did most of the work that is necessary to "compute" the values $a_e(R)$ in Section 3.2. Specifically, the numbers $a_e(R)$ equal to the $\mathbb{F}_p$-vector space dimension of $S^{1/p^e}/(\mathfrak{m}S^{1/p^e} :_{S^{1/p^e}} f^{(p^e-1)/p^e})$.

Exercise 67. Let S, f, and R be as above. Let $\mathfrak{m}$ be the ideal of S generated by the variables $(x_0, \ldots, x_d)$.

(1) Show that there is a short exact sequence of $\mathbb{F}_p$-vector spaces

$$0 \to \frac{S^{1/p^e}}{(\mathfrak{m}S^{1/p^e} :_{S^{1/p^e}} f^{(p^e-1)/p^e})} \to \frac{S^{1/p^e}}{\mathfrak{m}S^{1/p^e}} \to \frac{S^{1/p^e}}{(\mathfrak{m}, f^{(p^e-1)/p^e})S^{1/p^e}} \to 0.$$

(2) Show that $\dim_{\mathbb{F}_p}(S^{1/p^e}/\mathfrak{m}S^{1/p^e}) = p^{ed}$.
(3) Conclude that

$$a_e(R) = p^{ed} - \dim_{\mathbb{F}_p}\left(\frac{S^{1/p^e}}{(\mathfrak{m}, f^{(p^e-1)/p^e})S^{1/p^e}}\right)$$

and therefore

$$s(R) = 1 - \lim_{e\to\infty}\frac{1}{p^{ed}}\dim_{\mathbb{F}_p}\left(\frac{S^{1/p^e}}{(\mathfrak{m}, f^{(p^e-1)/p^e})S^{1/p^e}}\right).$$

Part (3) of the above exercise can give the illusion that computing the F-signature of a hypersurface is a reasonable task to accomplish. (Especially since S^{1/p^e} is a free S-module with an explicit basis!) However, maybe the following open conjecture, which has computational evidence of being true, will convince the reader that computing the F-signature of such rings can be quite difficult.

Conjecture 5.3 ([Mon08])**.** *Let $S = \mathbb{F}_2[[x, y, z, u, v]]$, $f = uv+x^3+y^3+xyz$, and $R = S/(f)$. Then*

$$s(R) = \frac{2}{3} - \frac{5}{14\sqrt{7}}.$$

We now turn our attention to a large class of rings for which the F-signature can be computed, coordinate rings of affine toric varieties. To do so, we recall the basics of constructing the coordinate ring of an affine toric variety from a rational polyhedral cone. We very crudely sketch the basic idea of this construction, for details, precise statements, and justifications we refer the reader to [Ful93] and [CLS11].

Let N be the lattice $\mathbb{Z}^n$ and M the dual lattice $M = \operatorname{Hom}_{\mathbb{Z}}(N, \mathbb{Z})$. (Observe that M is isomorphic to $\mathbb{Z}^n$.) We let $N_{\mathbb{R}}$ and $M_{\mathbb{R}}$ be the Euclidean n-spaces obtained from N and M by base changing to $\mathbb{R}$. Specifically, $N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^n$ and $M \otimes_{\mathbb{Z}} \mathbb{R} \cong \operatorname{Hom}_{\mathbb{R}}(N_{\mathbb{R}}, \mathbb{R})$.

Suppose $H \subseteq N$ is a subsemigroup of N. We always assume that our subsemigroup has the following property: If $\vec{y} \in N$ is such that $\vec{y}, -\vec{y} \in S$ then $\vec{y} = 0$, i.e., $H \cap -H = \{\vec{0}\}$. The *rational polyhedral cone* obtained from H is the subset $\sigma(H)$, or simply σ if H is understood, of $M_{\mathbb{R}}$ is defined by

$$\sigma = \{r_1\vec{s}_1 + \cdots + r_\ell\vec{s}_\ell \mid r_1, \cdots, r_\ell \geq 0, \vec{s}_1, \ldots, \vec{s}_\ell \in S\}.$$

Exercise 68. Let $N = \mathbb{Z}^2$. Describe the rational polyhedral cones associated with the following sub-semigroups of N.

(1) $H_1 = \operatorname{span}_{\mathbb{N}}\{\binom{1}{0}, \binom{0}{1}\}$.
(2) $H_2 = \operatorname{span}_{\mathbb{N}}\{\binom{1}{0}, \binom{1}{1}\}$.
(3) $H_3 = \operatorname{span}_{\mathbb{N}}\{\binom{1}{0}, \binom{1}{d}\}$ where $d \in \mathbb{N}$ where $d \in \mathbb{N}$.

(4) $H_4 = \mathrm{span}_{\mathbb{N}}\{\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}d\\-1\end{smallmatrix}\right)\}$ where $d \in \mathbb{N}$.

Let $\vec{e}_1, \ldots, \vec{e}_n$ denote the standard basis of $N_{\mathbb{R}} = \mathbb{R}^n$ and $\vec{e_1}^*, \ldots, \vec{e_n}^*$ the dual basis of $M_{\mathbb{R}}$. Suppose that $\vec{x} = x_1\vec{e}_1^* + \cdots x_n\vec{e}_n^* \in N_{\mathbb{R}}$ and $\vec{y} = y_1\vec{e}_1 + \cdots y_n\vec{e}_n \in M_{\mathbb{R}}$. Then we define $\langle \vec{x}, \vec{y} \rangle$ to be the real number

$$\langle \vec{x}, \vec{y} \rangle = x_1y_1 + \cdots + x_ny_n.$$

Suppose $H \subseteq N$ is a subsemigroup and σ the associated rational polyhedral cone. The *dual cone* of σ is the subset of $M_{\mathbb{R}}$ defined by

$$\sigma^\vee = \{\vec{x} \in M_{\mathbb{R}} \mid \langle \vec{x}, \vec{y} \rangle \geq 0, \forall \vec{y} \in \sigma\}.$$

Exercise 69. Let $N = \mathbb{Z}^2$. Describe the cones dual to the rational polyhedral cones associated with the following subsemigroups of N.

(1) $H_1 = \mathrm{span}_{\mathbb{N}}\{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$.
(2) $H_2 = \mathrm{span}_{\mathbb{N}}\{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)\}$.
(3) $H_3 = \mathrm{span}_{\mathbb{N}}\{\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \left(\begin{smallmatrix}1\\d\end{smallmatrix}\right)\}$ where $d \in \mathbb{N}$ where $d \in \mathbb{N}$.
(4) $H_4 = \mathrm{span}_{\mathbb{N}}\{\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}d\\-1\end{smallmatrix}\right)\}$ where $d \in \mathbb{N}$.

Let k be a field of prime characteristic. Given $H \subseteq N$ a subsemigroup, σ its rational polyhedral cone, and $\sigma^\vee$ its dual cone then *the coordinate ring of* σ is defined to be

$$k[S_\sigma] = k[x_1^{i_1} \cdots x_n^{i_n} \mid i_1\vec{e}_1^* + \cdots + i_n\vec{e}_n^* \in \sigma^\vee \cap M].$$

From this point forward we shall always assume the subsemigroup H is generated by *primitive generators*. Specifically, this means we can write $H = \mathrm{span}_{\mathbb{N}}\{\vec{y}_1, \ldots, \vec{y}_\ell\}$ and for each $1 \leq i \leq \ell$ there is no other integer vector $\vec{z} \in N$ such that $\vec{y}_i$ is the integer multiple of $\vec{z}$. For example, the subsemigroup $\mathrm{span}_{\mathbb{N}}\{\left(\begin{smallmatrix}2\\1\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$ is generated by primitive vectors but $\mathrm{span}_{\mathbb{N}}\{\left(\begin{smallmatrix}2\\2\end{smallmatrix}\right), \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\}$ is not generated by primitive vectors since $\left(\begin{smallmatrix}2\\2\end{smallmatrix}\right) = 2\left(\begin{smallmatrix}1\\1\end{smallmatrix}\right)$.

Let H be subsemigroup of $N = \mathbb{Z}^n$ generated by primimitve vectors. The ring $k[S_\sigma]$ will be a Noetherian domain. If the elements of S span $\mathbb{R}^n$ as a real vector space then we say that σ is full dimensional. In which case the Krull dimension of $k[S_\sigma]$ will be n, the ring $k[S_\sigma]$ will also be realized as the direct summand of a regular ring. In particular, under the assumption that the set S spans $\mathbb{R}^n$ as a real vector space we have that $k[S_\sigma]$ will be normal Cohen-Macaulay domain of prime characteristic $p > 0$. In fact, since we are assuming the characteristic of k is p the ring $k[S_\sigma]$ will be strongly F-regular.

Exercise 70. Let k be an F-finite field of prime characteristic $p > 0$ and H_1, H_2, H_3, H_4 be as in Exercise 68 and Exercise 69. Let $\sigma_i = \sigma(H_i)$ for $1 \leq i \leq 4$. Verify the following:

(1) $k[S_{\sigma_1}] = k[x_1, x_2]$.

(2) $k[S_{\sigma_2}] = k[x_1, x_1x_2]$.
(3) $k[S_{\sigma_3}] = k[x_1, x_2, x_1^d x_2^{-1}]$.
(4) $k[S_{\sigma_4}] = k[x_1, x_1x_2, x_1x_2^2, \dots, x_1x_2^d]$.

Theorem 5.4 ([WY04])**.** *Let σ be a full dimensional rational polyhedral cone obtained from a subsemigroup $H \subseteq N = \mathbb{Z}^n$ which is generated by primitive vectors. Suppose further that $\{\vec{y}_1, \dots, \vec{y}_\ell\}$ is a minimal set of primitive vectors spanning H over $\mathbb{N}$. Then the F-signature of $k[S_\sigma]$ is the Eucledian volume of the following set:*

$$\{\vec{x} \in M_{\mathbb{R}} \mid 0 \leq \langle \vec{x}, \vec{y_i} \rangle \leq 1, \forall 1 \leq i \leq \ell\}.$$

In particular, the F-signature of $k[S_\sigma]$ is a rational number which does not depend on the characteristic of k.

Exercise 71. Let k be an F-finite field of prime characteristic $p > 0$. Let $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ be as in Exercise 70. Verify the following:

(1) $s(k[S_{\sigma_1}]) = 1$.
(2) $s(k[S_{\sigma_2}]) = 1$.
(3) $s(k[S_{\sigma_3}]) = 1/d$.
(4) $s(k[S_{\sigma_4}]) = 1/d$.

Exercise 72. Let $N = \mathbb{Z}^2$, $H \subseteq N$ a subsemigroup, $\sigma = \sigma(H)$, and $\{\vec{y}_1, \dots, \vec{y}_\ell\}$ primitive generators of of H.

(1) Show that there exists $\vec{y}_i, \vec{y}_j \in \{\vec{y}_1, \dots, \vec{y}_\ell\}$ such that $\operatorname{span}_{\mathbb{R}_{\geq 0}}\{\vec{y}_1, \dots, \vec{y}_\ell\} = \operatorname{span}_{\mathbb{R}_{\geq 0}}\{\vec{y}_i, \vec{y}_j\}$.
(2) Rearrange the vectors $\{\vec{y}_1, \dots, \vec{y}_\ell\}$ so that $\vec{y}_1$ and $\vec{y}_2$ satisfy the conclusion of part (1) of the exercise. Show that

$$\{\vec{x} \in M_{\mathbb{R}} \mid 0 \leq \langle \vec{x}, \vec{y_i} \rangle \leq 1, \forall 1 \leq i \leq \ell\} = \{\vec{x} \in M_{\mathbb{R}} \mid 0 \leq \langle \vec{x}, \vec{y_1} \rangle \leq 1 \text{ and } \langle \vec{x}, \vec{y_2} \rangle \leq 1\}.$$

(3) Continue to let $\vec{y}_1$ and $\vec{y}_2$ satisfy the conclusion of (1). Suppose that $\vec{y}_1 = \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ and $\vec{y}_2 = \left(\begin{smallmatrix} c \\ d \end{smallmatrix}\right)$. Show that

$$s(k[S_\sigma]) = \frac{1}{|ad - bc|}.$$

The next exercise is meant to caution the reader. Exercise 72 tells us that the F-signature of a two-dimensional toric ring is always of the form $1/n$ for some natural number n. This phenomenon does not extend to higher dimensions.

Exercise 73. Let

$$H = \operatorname{span}_{\mathbb{N}} \left\{ \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ 1 \\ -1 \end{smallmatrix}\right) \right\},$$

$\sigma = \sigma(H)$, and k an F-finite field of prime characteristic $p > 0$. Show that $k[S_\sigma] \cong k[X, Y, Z, W]/(XY - ZW)$ and $s(k[S_\sigma]) = 2/3$.

Given a normal variety X we let $\operatorname{cl}(X)$ denote the divisor class group of X. We refer the reader to Appendix A for basics on the divisor class group. We wish to relate the F-signature of the coordinate ring of a normal affine toric variety with its divisor class group. Specifically, we outline a proof of the following:

Proposition 5.5. *Let R be the coordinate ring of a normal affine toric variety $X = \operatorname{Spec}(R)$ over an F-finite field k of prime characteristic $p > 0$ and suppose further that $|\operatorname{cl}(X)| < \infty$. Then*

$$s(R) = 1/|\operatorname{cl}(X)|.$$

Before proving Proposition 5.5 we first recall how to compute the divisor class group of a normal toric variety. Let $N = \mathbb{Z}^n$ and suppose $\vec{y}_1, \ldots, \vec{y}_\ell$ are primitive generators of a full dimensional subsemigroup S of N, $\sigma = \sigma(N)$ is the corresponding rational polyhedral cone, and $X = \operatorname{Spec}(k[S_\sigma])$. Let A_σ be the $\ell \times n$ matrix whose ℓ rows are the ℓ primitive generators of S. The matrix $\ell \times n$ matrix then represents a $\mathbb{Z}$-linear map from $\mathbb{Z}^n \to \mathbb{Z}^\ell$, which is injective since we are assuming S is full dimensional, and the divisor class group of X will then be isomorphic to the cokernel of this map.

For example, consider

$$S = S_\ell = \operatorname{span}_{\mathbb{N}} \left\{ \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} \ell \\ \ell \\ -1 \end{smallmatrix}\right) \right\}.$$

then A_σ is the 4×3 matrix

$$A_\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \ell & \ell & -1 \end{pmatrix}.$$

The cokernel of $\mathbb{Z}^3 \xrightarrow{A_\sigma} \mathbb{Z}^4$ is isomorphic to $\mathbb{Z}$ (check this) and thus the divisor class group of $\operatorname{Spec}(k[S_{\sigma_\ell}])$ is isomorphic to $\mathbb{Z}$.

Proof of Proposition 5.5. Let k, R, and X be as in the statement of the proposition. Suppose that $N = \mathbb{Z}^n$, S a full dimensional subsemigroup of N, and $\sigma = \sigma(S)$ is such that $k[S_\sigma] \cong R$. Suppose further that $\vec{y}_1, \ldots, \vec{y}_\ell$ are primitive generators of S and A_σ is the $\ell \times n$ matrix as described above which represents an injective map from $\mathbb{Z}^n \to \mathbb{Z}^\ell$. Then $\operatorname{cl}(X) \cong \operatorname{Coker}(A_\sigma)$. Thus the torsion-free rank of $\operatorname{cl}(X)$ is precisely $\ell - n$, hence $\operatorname{cl}(X)$ is finite if and only if $\ell - n = 0$, i.e., A_σ is a square matrix. Suppose that $\operatorname{cl}(X) = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_m}$ and $d_1 | d_2 | \cdots | d_m$.

Then A_σ has Smith Normal form

$$D_\sigma = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_m \end{pmatrix}.$$

In particular, $|\det(A_\sigma)| = |\det(D_\sigma)| = d_1 \cdots d_m = |\operatorname{cl}(X)|$.

We now show the F-signature of R is also $1/|\det(A_\sigma)|$. By Theorem 5.4 the F-signature of R is the Eucledian volume of

$$\{\vec{x} \in \mathbb{R}^n \mid 0 \le \langle \vec{y}_i, \vec{x}\rangle \le 1, \forall 1 \le i \le n\}.$$

If we set $\vec{y}_i = (a_{i,1}, \dots, a_{i,n})^T$ and $\vec{x} = (x_1, \dots, x_n)^T$ then $\langle \vec{y}_i, \vec{x}\rangle = a_{i,1}x_1 + \cdots + a_{i,n}x_n$. To compute the volume of the above set we apply the change of variables $u_i = a_{i,1}x_1 + \cdots + a_{i,n}x_n$ for each $1 \le i \le n$. Then the above set is transformed into the unit cube in the variables $u_1, \dots, u_n$. The reader should observe that the Jacobian matrix $\left(\frac{\partial u_i}{\partial x_j}\right)$ agrees with A_σ (well, at least upto transpose). We now leave it to the reader to apply the change of variables formula from Calculus to compute the volume of the above set as $1/\left|\left(\frac{\partial u_i}{\partial x_j}\right)\right|$. $\square$

Proposition 5.5 does not extend beyond the toric case. For example, there exist local unique factorization domains which are not regular. The divisor class group of such a ring is always the 0 group, which has one element, but the F-signature of such a ring must be strictly less than 1 by Theorem 5.1.

The methods of Proposition 5.5 provide a simple proof, in the toric case, a theorem of Carvajal-Rojas, Schwede, Tucker and Carvajal-Rojas. Let $(R, \mathfrak{m}, k)$ be a strongly F-regular local ring of prime characteristic $p > 0$ and let $X = \operatorname{Spec}(R)$. Suppose that $D \in \operatorname{cl}(X)$ is a torsion element and let $\operatorname{ord}(D)$ denote the order of D. In [CST16] the authors show that if p does not divide $\operatorname{ord}(D)$ then $\operatorname{ord}(D) \le 1/s(R)$. The same inequality was extended in [Car17] to the case that p does divide $\operatorname{ord}(D)$. Thus the inverse of F-signature provides a uniform upper bound to the order of a torsion element in the divisor class group of a strongly F-regular local ring.

Theorem 5.6 ([CST16, Car17]). *Let R be the coordinate ring of a normal affine toric variety $X = \operatorname{Spec}(R)$ over an F-finite field k of prime characteristic $p > 0$. Suppose $D \in \operatorname{cl}(X)$ is a torsion element. Then $\operatorname{ord}(D) \le 1/s(R)$.*

Outline of proof. We instruct the reader on how to prove the equivalent inequality $s(R) \le 1/\operatorname{ord}(D)$. Let $\vec{y}_1, \dots, \vec{y}_\ell$ be primitive generators of a subsemigroup of S of $N = \mathbb{Z}^n$ such that $k[S_\sigma] \cong R$. Let A_σ be the $\ell \times n$ matrix whose rows consist of the primitive generators of N.

By Theorem 5.4 the F-signature of R is the Euclidean volume of

$$\{\vec{x} \in M_{\mathbb{R}} \mid 0 \leq \langle \vec{x}, \vec{y_i} \rangle \leq 1, \forall 1 \leq i \leq \ell\}.$$

In particular, if $\vec{y}_{i_1}, \vec{y}_{i_2}, \ldots, \vec{y}_{i_n}$ are n distinct primitive generators of N then

$$s(R) \leq \mathrm{Vol}\{\vec{x} \in M_{\mathbb{R}} \mid 0 \leq \langle \vec{x}, \vec{y_{i_j}} \rangle \leq 1, \forall 1 \leq j \leq n\}.$$

As in the proof of Proposition 5.5 the volume of the set $\{\vec{x} \in M_{\mathbb{R}} \mid 0 \leq \langle \vec{x}, \vec{y_{i_j}} \rangle \leq 1, \forall 1 \leq j \leq n\}$ is simply $1/|\det(B)|$ where B is the square matrix whose rows consists of the primitive generators $\vec{y}_{i_1}, \ldots, \vec{y}_{i_n}$. We leave as an exercise for the reader to analyze the Smith-Normal form of the matrix A_σ, and especially how it is obtained via elementary row operations, to show that if there is an element of order m in the divisor class group, then there is an $n \times n$ submatrix of A_σ whose determinant, up to sign, is at least n. □

The next exercise is challenging, but methods similar to those used in the proof of Proposition 5.5 and Theorem 5.6 are of use.

Exercise 74 (Challenging)**.** Show that 0 is the only accumulation point of the collection of all F-signatures of affine toric varieties of a fixed dimension d. Specifically, show that if $\epsilon > 0$ then there are only finitely many numbers larger than ϵ which is realized as the F-signature of an affine toric variety of dimension d.

Interestingly enough, not many singular affine toric varieties have an F-signature larger than $1/2$. Jefferies showed in [**?**] that there are only two other values larger than $1/2$, but less than 1, that are realized as the F-signature of an affine toric variety. See Exercise 73 for an example where the F-signature of an affine toric ring is $2/3$. The other F-signature larger than $1/2$ achieved by a toric ring is $11/20$ and is achieved by the 5-dimensional ring

$$k[x_1, x_2, x_3, x_4, x_5, x_1x_2x_3x_4^{-1}x_5^{-1}].$$

It is an open problem to determine whether or not 0 is the only accumulation point of the collection of F-signatures achieved by all rings of a fixed dimension d. There is a related invariant, Hilbert-Kunz multiplicity, and it has been shown that the collection of Hilbert-Kunz multiplicities realized by all rings of a fixed dimension has nontrivial accumulation points.

Exercise 75 (Open Problem)**.** Let $d \geq 3$. Show that the collection of F-signatures realized by a d-dimensional ring has an accumulation point other than 0.

5.2. **The growth rate of R^{1/p^e}.** Let R be an F-finite ring of prime characteristic $p > 0$ and M a finitely generated R-module. Then we let $\mu_R(M)$, or simply $\mu(M)$ if R is understood, to be the minimal number of elements of M needed to generate M as an R-module. Suppose for simplicity that R is a domain. Recall that we let $\gamma(R)$ be the unique integer such that $\operatorname{rank}_R(R^{1/p^e}) = p^{e\gamma(R)}$ for all $e \in \mathbb{N}$, see Exercise 17.

Exercise 76. Let R be an F-finite domain of prime characteristic $p > 0$. Show that $p^{e\gamma(R)} \leq \mu_R(R^{1/p^e})$ for each $e \in \mathbb{N}$.

Amazingly enough, we will show that $p^{e\gamma(R)}$ will not be "too far" away from the true value of $\mu(R^{1/p^e})$. Specifically, we guide the reader through a two elementary proofs that there exists a constant $C \in \mathbb{R}$ such that $\mu(R^{1/p^e}) \leq Cp^{e\gamma(R)}$ for each $e \in \mathbb{N}$. We first extend the definition of $\gamma(R)$ to F-finite rings which are not assumed to be domains.

Let R be an F-finite ring and $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell\}$ be the minimal primes of R. Then for each $i \in \mathbb{N}$ the quotient ring $R/\mathfrak{p}_i$ is an F-finite domain and we let $\gamma(R/\mathfrak{p}_i)$ be the unique integer such that $\operatorname{rank}_{R/\mathfrak{p}_i}((R/\mathfrak{p}_i)^{1/p^e}) = p^{e\gamma(R/\mathfrak{p}_i)}$. We set $\gamma(R) = \max\{\gamma(R/\mathfrak{p}_1), \ldots, \gamma(R/\mathfrak{p}_\ell)\}$.

Our goal is to prove F-signature exists. Critical to showing F-signature exists is the following:

Theorem 5.7. *Let R be an F-finite ring and M a finitely generated R-module. Then there exists a constant $C \in \mathbb{R}$ such that for all $e \in \mathbb{N}$*

$$\mu_R(M^{1/p^e}) \leq Cp^{e\gamma(R)}.$$

Our first proof of Theorem 5.7 is only valid in the local scenario, since we will compare the growth rate of $\mu(M^{1/p^e})$ with the Hilbert function of an $\mathfrak{m}$-primary ideal, and the second proof, while arguably more elementary than the first, involves a basic Calculus trick. Both proofs rely on Exercise 22 in a critical way. Both proofs will also use the following two elementary exercises. The first exercise gives us a coarse and elementary way to estimate the number of generators of finitely generated R-module.

Exercise 77. Let R be a commutative ring, not necessarily of prime characteristic, and let $M_1 \to M_2 \to M_3 \to 0$ be a right exact sequence of finitely generated R-modules. Show that $\mu(M_2) \leq \mu(M_1) + \mu(M_3)$.

Observe that Exercise 77 provides us a method of reducing the proof of Theorem 5.7 to the case that R is an F-finite domain and $M = R$.

Exercise 78. Let R be an F-finite ring, M a finitely generated R-module, and $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_\ell = M$ a prime filtration of M. Suppose that $M_i/M_{i-1} \cong R/P_i$ where $P_i \in \operatorname{Spec}(R)$. Show that $\mu(M^{1/p^e}) \leq \sum_{i=1}^{\ell} \mu((R/P_i)^{1/p^e})$.

5.3. **Proof of Theorem 5.7 under the local hypothesis.** The next two exercises gives the "standard" method for proving Theorem 5.7 under the assumption that R is local. However, the reader can skip onto Section 5.4 for a proof of Theorem 5.7 which does not require the local hypothesis.

Exercise 79. Let $(R, \mathfrak{m}, k)$ be a local F-finite domain of prime characteristic $p > 0$ and Krull dimension d.

(1) Let $\mathfrak{m}^{[p^e]} = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = R$ be a prime filtration of $\mathfrak{m}^{[p^e]} \subseteq R$. Show that $M_i/M_{i-1} \cong k$ for each $1 \leq i \leq n$.
(2) Let $\mathfrak{m}^{[p^e]} = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = R$ be as in part (1). Show that $\mathfrak{m}R^{1/p^e} = M_0^{1/p^e} \subseteq M_1^{1/p^e} \subseteq \cdots \subseteq M_n^{1/p^e} = R^{1/p^e}$ is a filtration of $\mathfrak{m}R^{1/p^e} \subseteq R^{1/p^e}$ such that $M_i^{1/p^e}/M_{i-1}^{1/p^e}$ for each $1 \leq i \leq n$.
(3) Use Exercise 22 to conclude that if $\ell(R/\mathfrak{m}^{[p^e]})$ denotes the length of $R/\mathfrak{m}^{[p^e]}$ as an R-module then
$$\frac{\ell(R/\mathfrak{m}^{[p^e]})}{p^{ed}} = \frac{\ell(R^{1/p^e}/\mathfrak{m}R^{1/p^e})}{p^{e\gamma(R)}} = \frac{\mu(R^{1/p^e})}{p^{e\gamma(R)}}.$$

Exercise 80. Let $(R, \mathfrak{m}, k)$ be an F-finite local ring of prime characteristic $p > 0$ of Krull dimension d and let M be a finitely generated R-module. Show that there exists $C \in \mathbb{R}$ such that $\mu(M^{1/p^e}) \leq Cp^{e\gamma(R)}$ for all $e \in \mathbb{N}$. (Hint: Use Exercise 78 to reduce the exercise to the scenario that $M = R$ and R is a local F-finite domain. Then use (3) of Exercise 79 to observe that it is enough to show the existence of a constant C such that $\ell(R/\mathfrak{m}^{[p^e]}) \leq Cp^{ed}$ for all $e \in \mathbb{N}$. Exercise 50 should now be helpful.)

Exercise 80 gives Theorem 5.7 under the assumption that R is local, and this will be enough to prove the existence of the F-signature of a local ring of prime characteristic. We therefore invite the reader to skip onto Section 5.5 for a proof that the F-signature of a local ring exists and then comeback to work through the rest of this section.

5.4. **Proof of Theorem 5.7 without the local hypothesis.** In order to prove Theorem 5.7 without the local hypothesis we first observe that $\gamma(R)$ behaves "somewhat like" the Krull dimension of a local ring. More precisely:

Exercise 81. Let R be an F-finite domain and $I \subseteq R$ a nonzero ideal. Show that $\gamma(R/I) < \gamma(R)$. (Hint: Use Exercise 22.)

Our proof of Theorem 5.7 will also rely on an induction argument involving $\gamma(R)$.

Exercise 82. Let R be an F-finite ring of prime characteristic $p > 0$ and M a finitely R-module and suppose that $\gamma(R) = 0$. Show there exists $C \in \mathbb{R}$ such that $\mu(M^{1/p^e}) \leq C$ for all $e \in \mathbb{N}$. (Hint: Consider a prime filtration of M and use Exercise 22 to show that each prime factor is isomorphic to a perfect field of prime characteristic $p > 0$. Use Exercise 78 to conclude that $\mu(M^{1/p^e})$ is no more than the length of the prime filtration of $0 \subsetneq M$ for each $e \in \mathbb{N}$.)

We now give a proof of Theorem 5.7.

Proof of Theorem 5.7. Consider a prime filtration of M. Since taking p^eth roots is exact, i.e., restricting scalars is exact, we may assume $M = R$ and R is an F-finite domain. Let K be the fraction field of R. Then $R^{1/p} \otimes_R K \cong K^{1/p}$ is a K-vector space of dimension $p^{\gamma(R)}$. We can therefore choose elements $r_1 \dots, r_{\gamma(R)} \in R^{1/p}$ which is a basis of $K^{1/p}$ after applying $- \otimes_R K$. Moreover, $R^{1/p}$ is a torsion-free R-module and there is an injection $R^{\oplus p^{\gamma(R)}} \to R^{1/p}$ defined by mapping the ith basis element to r_i and this map is an isomorphism when localized at 0. In particular, there is a short exact sequence

$$0 \to R^{p^{\oplus \gamma(R)}} \to R^{1/p} \to C \to 0$$

such that C is a finitely generated and torsion R-module. By Exercise 81, $\gamma(R/\operatorname{Ann}_R C) \leq \gamma(R) - 1$ and we may therefore assume by induction that there exists a $C \in \mathbb{R}$ such that $\mu(M^{1/p^e}) \leq C p^{e(\gamma(R)-1)}$.

Taking p^{e-1}th roots is exact, hence there are short exact sequences

$$0 \to (R^{1/p^{e-1}})^{\oplus p^{\gamma(R)}} \to R^{1/p^e} \to C^{1/p^{e-1}} \to 0.$$

Thus $\mu(R^{1/p^e}) \leq p^{\gamma(R)} \mu(R^{1/p^{e-1}}) + \mu(M^{1/p^{e-1}})$. But applying the same argument to $R^{1/p^{e-1}}$ implies

$$\begin{aligned}
\mu(R^{1/p^e}) &\leq p^{\gamma(R)} \mu(R^{1/p^{e-1}}) + \mu(M^{1/p^{e-1}}) \\
&\leq p^{\gamma(R)}(p^{\gamma(R)} \mu(R^{1/p^{e-2}}) + \mu(M^{1/p^{e-2}})) + \mu(M^{1/p^{e-1}}) \\
&= p^{2\gamma(R)} \mu(R^{1/p^{e-2}}) + p^{\gamma(R)} \mu(M^{1/p^{e-2}}) + \mu(M^{1/p^{e-1}}).
\end{aligned}$$

Inductively

$$\mu(R^{1/p^e}) \leq p^{e\gamma(R)} + \sum_{i=0}^{e-1} p^{i\gamma(R)} \mu(M^{1/p^{e-1-i}}).$$

Therefore

$$\mu(R^{1/p^e}) \leq p^{e\gamma(R)} + \sum_{i=0}^{e-1} p^{i\gamma(R)} C p^{(e-1-i)(\gamma(R)-1)}.$$

We leave as an exercise to the reader that $\sum_{i=0}^{e-1} p^{i\gamma(R)} C p^{(e-1-i)(\gamma(R)-1)} \leq 2Cp^{e\gamma(R)}$.[1] Therefore

$$\mu(R^{1/p^e}) \leq (1+2C)p^{e\gamma(R)}$$

for each $e \in \mathbb{N}$. □

The above gives an elementary and novel way of proving a key proposition of [Pol18].

Exercise 83 (cf. [Pol18, Proposition 3.3])**.** Let R be an F-finite domain and M a finitely generated R-module. Show that there exists a constant $C \in \mathbb{R}$ such that $\mu(M_P^{1/p^e}) \leq Cp^{e\gamma(R_P)}$ for each $P \in \operatorname{Spec}(R)$. (Hint: Show $\gamma(R_P) = \gamma(R)$ for each $P \in \operatorname{Spec}(R)$ and then use Theorem 5.7).

5.5. **F-signature exists.** The next step towards proving F-signature exists is proving that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of finitely generated modules over a local ring, then $\operatorname{frk}(M) \leq \operatorname{frk}(M') + \mu(M'')$.

Exercise 84. Let $(R, \mathfrak{m}, k)$ be a local ring, not necessarily of prime characteristic, and let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be a short exact sequence of finitely generated R-modules.

(1) Suppose $M \cong R^{\oplus n} \oplus N$ and $M' \cong R^{\oplus n'} \oplus N'$ are direct sum decompositions of M and M' so that N and N' do not have a free R-summand. Show that $f(N) \subseteq (\mathfrak{m}R)^{\oplus n'} \oplus N'$. (Hint: Suppose for a contradiction that $f(N) \not\subseteq (\mathfrak{m}R)^{\oplus n'} \oplus N'$. Then show that N will have a free summand.)
(2) Use part (1) to show that there will be an induced map
$$(R^{\oplus n'} \oplus N)/N \cong R^{\oplus n'} \xrightarrow{\overline{f}} (R^{\oplus n} \oplus N)/(\mathfrak{m}R^{\oplus n} \oplus N) \cong k^{\oplus n}.$$
(3) Show that the cokernel of $\overline{f}$ is the homomorphic image of M''. Conclude that $\mu(\operatorname{Coker}(\overline{f})) \leq \mu(M'')$.
(4) Consider the right exact sequence $R^{\oplus n'} \xrightarrow{\overline{f}} k^{\oplus n} \to \operatorname{Coker}(\overline{f}) \to 0$ and use Exercise 77 to conclude that $n \leq n' + \mu(M'')$.

Our proof of existence of F-signature relies on the following basic calculus trick involving limits.

Exercise 85. Let p be a prime number, $\{s_e\}$ a sequence of real numbers, and C a constant such that
$$s_{e+1} \leq s_e + \frac{C}{p^e}$$
for each $e \in \mathbb{N}$.

[1]The key point to this inequality is that $(1 + \frac{1}{p} + \cdots \frac{1}{p^{e-1}}) \leq 2$ for all $e \in \mathbb{N}$.

(1) Show that for each $e' \in \mathbb{N}$ that
$$s_{e+e'} \leq s_e + \frac{2C}{p^e}.$$
(2) Use the inequality from (2) to show that
$$\limsup_{e\to\infty} s_e \leq \liminf_{e\to\infty} s_e$$
and conclude that $\lim_{e\to\infty} s_e$ exists.

We now guide the reader through a proof on the existence of F-signature.

Exercise 86. Let $(R, \mathfrak{m}, k)$ be an F-finite local domain of prime characteristic $p > 0$. Show that the sequence of numbers $a_e(R)/p^{e\gamma(R)}$ forms a Cauchy sequence as follows:

(1) Show that there exists a short exact sequence
$$0 \to R^{p^{\oplus\gamma(R)}} \to R^{1/p} \to C \to 0$$
such that C is a torsion R-module.

(2) Use exactness of $(-)^{1/p^e}$ and Exercise 84 to conclude that
$$a_{e+1}(R) \leq p^{\gamma(R)} a_e(R) + \mu(M^{1/p^e})$$
and therefore there exists $C \in \mathbb{R}$ such that
$$a_{e+1}(R) \leq p^{\gamma(R)} a_e(R) + Cp^{e(\gamma(R)-1)}$$
for all $e \in \mathbb{N}$.

(3) Divide the above inequality by $p^{e\gamma(R)}$ and use Exercise 85 to conclude that the F-signature of R exists.

5.6. **The splitting ideals.** Our next goal is to show that positivity of F-signature is equivalent to the property of being strongly F-regular. The technique discussed in these notes relies on understanding basic properties of the splitting ideals of a local ring.

Let $(R, \mathfrak{m}, k)$ be an F-finite local domain of prime characteristic $p > 0$. The *eth splitting ideal of* R is the set
$$I_e = \{r \in R \mid \varphi(r^{1/p^e}) \in \mathfrak{m}, \forall \varphi \in \operatorname{Hom}_R(R^{1/p^e}, R)\}.$$

Exercise 87. Let $(R, \mathfrak{m}, k)$ be an F-finite local domain of prime characteristic $p > 0$ and let I_e be the eth splitting ideal of R.

(1) Show that I_e is an ideal of R.

(2) Show that $\mathfrak{m}^{[p^e]} \subseteq I_e$.

(3) Show that R is strongly F-regular if and only if $\bigcap I_e = 0$.

(4) Show that if R is F-pure then $\{I_e\}$ is a descending set of ideals.

(5) Show that for each pair of integers $e, e_0 \in \mathbb{N}$ and $\varphi \in \operatorname{Hom}_R(R^{1/p^e}, R)$

$$\varphi(I_{e+e_0}^{1/p^e}) \subseteq I_{e_0}.$$

The next exercise demonstrates that the lengths of the cyclic modules R/I_e is an equivalent way to measure the F-signature of a local ring.

Exercise 88. Let $(R, \mathfrak{m}, k)$ be an F-finite local domain of prime characteristic $p > 0$ and let I_e be the eth splitting ideal of R.

(1) Show that if $R^{1/p^e} \cong R^{\oplus a_e(R)} \oplus M_e$ and M_e does not have a free R-summand then $I_e^{1/p^e} = (\mathfrak{m}R)^{\oplus a_e(R)} \oplus M_e$.

(2) Use Exercise 22 and exactness of taking p^eth roots to show that

$$\frac{a_e(R)}{\operatorname{rank}(R^{1/p^e})} = \frac{\ell(R/I_e)}{p^{e\dim(R)}}.$$

(3) Conclude that $s(R) = \lim_{e\to\infty} \ell(R/I_e)/p^{e\dim(R)}$.

5.7. **Positivity of F-signature and strongly F-regular rings.** Arguably, the most important theorem concerning F-signature is the following theorem of Aberbach and Leuschke:

Theorem 5.8 ([AL03])**.** *Let $(R, \mathfrak{m}, k)$ be an F-finite local ring of prime characteristic $p > 0$. Then the following are equivalent:*

(1) R is strongly F-regular;

(2) $s(R) > 0$.

The next exercise guides the reader through the easier implication of Theorem 5.8.

Exercise 89. Let $(R, \mathfrak{m}, k)$ be an F-finite local domain of prime characteristic $p > 0$ and suppose that R is not strongly F-regular. Thus there exists nonzero element $f \in R$ such that $\varphi(f^{1/p^e}) \in \mathfrak{m}$ for all $\varphi \in \operatorname{Hom}_R(R^{1/p^e}, R)$.

(1) Suppose $R^{1/p^e} \cong R^{\oplus a_e(R)} \oplus M_e$ is a choice of direct sum decomposition of R^{1/p^e} such that M_e does not have a free summand. Show that $f^{1/p^e} \in (\mathfrak{m}R)^{\oplus a_e(R)} \oplus M_e$ for each $e \in \mathbb{N}$.

(2) Show that for each $e \in \mathbb{N}$ there is an onto map

$$(R/(f))^{1/p^e} \to (R^{\oplus a_e(R)} \oplus M_e)/((\mathfrak{m}R)^{\oplus a_e(R)} \oplus M_e) \cong k^{\oplus a_e(R)}.$$

(3) Conclude that $a_e(R) \leq \mu((R/(f))^{1/p^e})$ for each $e \in \mathbb{N}$ and use Exercise 81 to conclude that $s(R) = 0$.

The "hard" direction of Theorem 5.8 reduces to the following:

Theorem 5.9 ([AL03])**.** *Let $(R, \mathfrak{m}, k)$ be an F-finite and strongly F-regular ring of prime characteristic p. For each $e \in \mathbb{N}$ let*

$$I_e = \{r \in R \mid \varphi(r^{1/p^e}) \in \mathfrak{m}, \forall \varphi \in \mathrm{Hom}_R(R^{1/p^e}, R)\}.$$

Then there exists an $e_0 \in \mathbb{N}$ such that $I_{e+e_0} \subseteq \mathfrak{m}^{[p^e]}$ for all $e \in \mathbb{N}$.

Recall that the ideals I_e are $\mathfrak{m}$-primary and $s(R) = \lim_{e\to\infty} \frac{a_e(R)}{\mathrm{rank}(R^{1/p^e})} = \lim_{e\to\infty} \frac{\ell(R/I_e)}{p^{e\dim(R)}}$. The next exercise allows the reader to see how Theorem 5.8 can be deduced from Theorem 5.9.

Exercise 90. Let $(R, \mathfrak{m}, k)$ be an F-finite domain of prime characteristic $p > 0$.

(1) Show that for all $e \in \mathbb{N}$
$$\frac{\ell(R/\mathfrak{m}^{[p^e]})}{p^{e\dim(R)}} = \frac{\dim_k\left(R^{1/p^e}/\mathfrak{m}R^{1/p^e}\right)}{\mathrm{rank}(R^{1/p^e})} \geq 1.$$
(2) Conclude that if we know that there exists $e_0 \in \mathbb{N}$ such that $I_{e+e_0} \subseteq \mathfrak{m}^{[p^e]}$ for all $e \in \mathbb{N}$ then
$$s(R) \geq \frac{1}{p^{e_0\dim(R)}} > 0.$$

The proof of Theorem 5.9 reduces to the case that R is complete. The following two exercises provides the necessary details to making this reduction.

Exercise 91. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring, not necessarily of prime characteristic, and let M be a finitely generated R-module.

(1) Show that there does not exist onto R-linear map $M \to R$ if and only if the map $\mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(M, k)$ is the 0-map where $\mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(M, k)$ is induced from applying $\mathrm{Hom}_R(M, -)$ to the natural surjection $R \to k$.
(2) Conclude that there does not exist onto R-linear map $M \to R$ if and only if there does not exist onto R-linear map $\widehat{M} \to \widehat{R}$.

Exercise 92. Let $(R, \mathfrak{m}, k)$ be a local F-finite domain of prime characteristic $p > 0$.

(1) Show that $a_e(R) = a_e(\widehat{R})$. (Hint: Use Exercise 91 and Exercise 64.)
(2) Suppose that
$$I_e = \{r \in R \mid \varphi(r^{1/p^e}) \in \mathfrak{m}, \forall \varphi \in \mathrm{Hom}_R(R^{1/p^e}, R)\}$$
and
$$J_e = \{s \in \widehat{R} \mid \varphi(s) \in \mathfrak{m}\widehat{R}, \forall \varphi \in \mathrm{Hom}_{\widehat{R}}(\widehat{R}^{1/p^e}, \widehat{R})\}.$$

Show that

$$I_e \otimes_R \widehat{R} \cong I_e \widehat{R} = J_e.$$

(3) Conclude that $I_{e+e_0} \subseteq \mathfrak{m}^{[p^e]}$ if and only if $J_{e+e_0} \subseteq \mathfrak{m}^{[p^e]}\widehat{R}$ and therefore Theorem 5.9 reduces to the case that R is complete.

We are now ready to present a proof of Theorem 5.9 which originally appeared in [PT18].

Proof of Theorem 5.9. By Exercise 92 we may assume $(R, \mathfrak{m}, k)$ is a complete local ring. Let $\underline{x} = x_1, \ldots, x_d$ be a system of parameters of R. Our first goal is to find a natural number $N \in \mathbb{N}$ with the following property: If $r \in R - \mathfrak{m}^{[p^e]}$ then there exists $\varphi \in \operatorname{Hom}_R(R^{1/p^e}, R)$ such that $\varphi(r^{1/p^e}) \notin (\underline{x})^N R$.

By the Cohen Structure Theorem R is module finite over the regular local ring $A = k[[x_1, \ldots, x_d]] \subseteq R$ where $k \subseteq R$ is a choice of coefficient field. For each $e \in \mathbb{N}$ we let $\operatorname{Hom}_A(R^{1/p^e}, A) \to \operatorname{Hom}_A(R, A)$ be the natural map induced from the inclusion $R \subseteq R^{1/p^e}$.

Observe that $\operatorname{Hom}_A(R, A)$ is a torsion-free R-module of rank 1 (prove this). Thus we can choose $\tau \in \operatorname{Hom}_A(R, A)$ and element $y \in R$ such that $y \cdot \operatorname{Hom}_A(R, A) \subseteq R \cdot \tau$. Moreover, since $A \subseteq R$ is module finite we may assume $y \in A$. Observe that the cyclic module $R \cdot \tau \cong R$ since $\operatorname{Hom}_A(R, A)$ is torsion-free. Denote by $\epsilon : \operatorname{Hom}_A(R, A) \to A$ the A-linear map which sends a map $\varphi \mapsto \varphi(1)$. Then for each $e \in \mathbb{N}$ we have the following commutative diagram:

$$\begin{tikzcd} \operatorname{Hom}_A(R^{1/p^e}, A) \arrow[r] & \operatorname{Hom}_A(R, A) \arrow[r, "\cdot y"] \arrow[d, "\epsilon"] & R \cdot \tau \cong R \arrow[d, "\epsilon"] \\ & A \arrow[r, "\cdot y"] & A. \end{tikzcd}$$

The reader should observe that the top row of the diagram consists of R-linear maps. Since $y \neq 0$ there exists integer N such that $y \notin (\underline{x})^N A$. We claim that for all $r \in R - \mathfrak{m}^{[p^e]}$ there exists $\varphi \in \operatorname{Hom}_R(R^{1/p^e}, R)$ such that $\varphi(r^{1/p^e}) \notin (\underline{x})^N R$.

Suppose that $r \in R - \mathfrak{m}^{[p^e]}$. Equivalently, $r \in R^{1/p^e} - \mathfrak{m}R^{1/p^e}$. Strongly F-regular rings are Cohen-Macaulay, see Theorem 4.4, and therefore by the Auslander-Buchsbaum formula R^{1/p^e} is a free A-module. In particular, r^{1/p^e} is a minimal generator a free A-module and there exists $\psi \in \operatorname{Hom}_A(R^{1/p^e}, A)$ such that $\psi(r^{1/p^e}) = 1$. Consider the R-linear map $R^{1/p^e} \xrightarrow{\Phi} \operatorname{Hom}_A(R^{1/p^e}, A)$ defined by $\Phi(x^{1/p^e}) = \varphi(r^{1/p^e} -)$ and consider the commutative diagram

$$\begin{tikzcd} R^{1/p^e} \arrow[r, "\Phi"] & \operatorname{Hom}_A(R^{1/p^e}, A) \arrow[r] & \operatorname{Hom}_A(R, A) \arrow[r, "\cdot y"] \arrow[d, "\epsilon"] & R \cdot \tau \cong R \arrow[d, "\epsilon"] \\ & & A \arrow[r, "\cdot y"] & A. \end{tikzcd}$$

Since the map ϵ is the evaluation at 1 map the reader should observe that the element r^{1/p^e} in the top left of the diagram is mapped to the element y in the bottom right of the diagram. Let $\varphi : R^{1/p^e} \to R$ be the R-linear map which is the composition of all maps in the top row of the above diagram. Then $\varphi(r^{1/p^e}) \notin (\underline{x})^N R$. Else, after applying the A-linear map ϵ we reach the contradiction that $y \in (\underline{x})^N A$.

We now recall Chevalley's lemma: Suppose $\{J_e\}$ is a descending chain of ideals in R whose intersection is 0. Given any $\mathfrak{m}$-primary ideal $\mathfrak{a}$ there exists an e_0 such that $J_{e_0} \subseteq \mathfrak{a}$.

The ideals $\{I_e\}$ are descending and $\cap I_e = 0$ by Exercise 87. Therefore there exists an $e_0 \in \mathbb{N}$ such that $I_{e_0} \subseteq (\underline{x})^N R$. We claim that $I_{e+e_0} \subseteq \mathfrak{m}^{[p^e]}$ for all $e \in \mathbb{N}$. Suppose for a contradiction that $I_{e+e_0} \not\subseteq \mathfrak{m}^{[p^e]}$ for some $e \in \mathbb{N}$. Suppose $r \in I_{e+e_0} - \mathfrak{m}^{[p^e]}$. By the above we can then find $\varphi \in \operatorname{Hom}_R(R^{1/p^e}, R)$ such that $\varphi(r^{1/p^e}) \notin (\underline{x})^N R$. However, this is not possible since $\varphi(I_{e+e_0}^{1/p^e}) \subseteq I_{e_0} \subseteq (\underline{x})^N R$ by Exercise 87. $\square$

6. Hilbert-Kunz multiplicity

An invariant attached to every F-finite ring of prime characteristic $p > 0$, which is related to F-signature, is Hilbert-Kunz multiplicity. In this appendix we guide the reader through a proof of existence of Hilbert-Kunz multiplicity. The reader will be able to establish the existence of Hilbert-Kunz multiplicity for all F-finite domains, not just the local ones. We then compare the proof of existence of Hilbert-Kunz multiplicity with the proof of existence of F-signature and invite the reader to find proofs of existence of F-signature without the local hypothesis.

Recall that if R is a commutative ring and M a finitely generated R-module, then we let $\mu_R(M)$, or simply $\mu(M)$, denote the minimal number of elements needed to generate M as an R-module. Also recall that if $(R, \mathfrak{m}, k)$ is local then $\mu(M) = \ell(M\mathfrak{m}M) = \dim_k(M/\mathfrak{m}M)$.

We now turn our attention to the numbers $\mu(R^{1/p^e})$ under the assumption that R is an F-finite domain of prime characteristic $p > 0$. The numbers $\mu(R^{1/p^e})$ are clearly bounded below by the rank of R^{1/p^e} as an R-module and equality is achieved whenever R^{1/p^e} is a free R-module. The *Hilbert-Kunz multiplicity of* R is defined to be the limit

$$\mathrm{e}_{\mathrm{HK}}(R) = \lim_{e\to\infty} \frac{\mu(R^{1/p^e})}{\operatorname{rank}(R^{1/p^e})}.$$

Existence of the above limit was first established by Monsky in [Mon83].

Exercise 93. Let $(R, \mathfrak{m}, k)$ be an F-finite domain of prime characteristic $p > 0$. Show that

$$\frac{\mu(R^{1/p^e})}{\operatorname{rank}(R^{1/p^e})} = \frac{\ell(R/\mathfrak{m}^{[p^e]})}{p^{e\dim(R)}}$$

for each $e \in \mathbb{N}$ and conclude that

$$\mathrm{e}_{\mathrm{HK}}(R) = \lim_{e\to\infty} \frac{\ell(R/\mathfrak{m}^{[p^e]})}{p^{e\dim(R)}}.$$

Exercise 94. Let $(R, \mathfrak{m}, k)$ be an F-finite regular local ring of prime characteristic $p > 0$. Prove that $\mathrm{e}_{\mathrm{HK}}(R) = 1$.

Exercise 95. (Challenging) Let R be a regular F-finite domain of prime characteristic $p > 0$. Show that the limit $\mathrm{e}_{\mathrm{HK}}(R)$ exists and is equal to 1. (Hint: Take a look at the Forester-Swan Theorem, [Mat89, Theorem 5.7].)

Amazingly enough, the converse of Exercise 94 holds under mild hypotheses.

Theorem 6.1 ([WY00])**.** *Let $(R, \mathfrak{m}, k)$ be an F-finite local ring such that $\widehat{R}$ is equidimensional. If $\mathrm{e}_{\mathrm{HK}}(R) = 1$ then R is a regular local ring.*

The reader who is interested in learning a proof of Theorem 6.1 are encouraged to read [HY02] as well as [WY00]. We remark the assumption that $\widehat{R}$ is equidimensional is a necessary assumption in Theorem 6.1.

Exercise 96. Let k be an F-finite field of prime characteristic $p > 0$ and let $R = k[[x, y, z]]/(xy, xz)$. Show that R is not a regular local ring, is not equidimensional, and $\mathrm{e}_{\mathrm{HK}}(R) = 1$.

Exercise 97. Let R be an F-finite domain. Show that the sequence of numbers $\mu(R^{1/p^e})/\operatorname{rank}(R^{1/p^e})$ forms a Cauchy sequence as follows:

(1) Show that there exists a short exact sequence

$$0 \to R^{p^{\gamma(R)}} \to R^{1/p} \to C \to 0$$

such that C is a torsion R-module.

(2) Use exactness of $(-)^{1/p^e}$ and Exercise 77 to conclude that

$$\mu(R^{1/p^{e+1}}) \leq p^{\gamma(R)}\mu(R^{1/p^e}) = \mu(C^{1/p^e}).$$

(3) Repeat the method of Exercise 86 to conclude that the limit $\mathrm{e}_{\mathrm{HK}}(R)$ exists.

The reader should observe at least one significant difference between the solutions of Exercise 86 and Exercise 97. Namely that the solution of Exercise 97 does not require the assumption that R is local. The assumption that R is local is used at one critical point in the solution of Exercise 86, and that is to conclude that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of finitely generated modules over a local ring then

$$\operatorname{frk}(M) \leq \operatorname{frk}(M') + \mu(M'').$$

Exercise 98. (Very challenging) Let R be a Noetherian ring, not necessarily of prime characteristic $p > 0$ nor local, and let

$$0 \to M' \to M \to M'' \to 0$$

a short exact sequence of finitely generated R-modules. Is it necessarily the case that

$$\operatorname{frk}(M') \leq \operatorname{frk}(M) + \mu(M'')?$$

If yes give a proof, if no give a counterexample.

The existence of F-signature without the local hypothesis has been established in [DPY16]. Their proof of existence needs the following:

Proposition 6.2. *Let R be a Noetherian ring of finite Krull dimension d and suppose that*

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of finitely generated R-modules. Then

$$\operatorname{frk}(M) \leq \operatorname{frk}(M') + \mu(M'') + d.$$

The proof of Proposition 6.2 given in [DPY16] relies on a deep theorem of Stafford which generalizes Theorem 5.2, see [Sta82] and [DSPY18]. We invite the reader to find a proof that the F-signature of a non-local F-finite domain exists without referencing Proposition 6.2.

Exercise 99. (Open problem) Let R be an F-finite domain of prime characteristic $p > 0$ and not necessarily local. Provide an "elementary proof" that the F-signature of R exists as a limit.

6.1. **Hilbert-Kunz multiplicity of an $\mathfrak{m}$-primary ideal and connections with F-signature.** Traditionally, the Hilbert-Kunz multiplicity of a local ring $(R, \mathfrak{m}, k)$ is not introduced as the limit $\lim_{e\to\infty} \mu(R^{1/p^e})/\operatorname{rank}(R^{1/p^e})$. Instead it is equivalently defined as $\lim_{e\to\infty} \ell(R/\mathfrak{m}^{[p^e]})/p^{e\dim(R)}$, see Exercise 93. We opted to use the definition involving $\mu(R^{1/p^e})$ since this is a definition that is well-defined for rings which are not assumed to be local. Nevertheless, the traditional way of defining Hilbert-Kunz multiplicity allows us to define the Hilbert-Kunz multiplicity of an $\mathfrak{m}$-primary ideal.

Suppose $(R, \mathfrak{m}, k)$ is a local F-finite domain of prime characteristic $p > 0$ and $I \subseteq R$ an $\mathfrak{m}$-primary ideal. The *Hilbert-Kunz multiplicity* of I is defined to be

$$\mathrm{e}_{\mathrm{HK}}(I) = \lim_{e\to\infty} \frac{\ell(R/I^{[p^e]})}{p^{ed}}.$$

The reader who has worked through Exercise 86 and Exercise 97 should be able to solve the following:

Exercise 100. Let $(R, \mathfrak{m}, k)$ be a local F-finite domain of prime characteristic $p > 0$ and $I \subseteq R$ an $\mathfrak{m}$-primary ideal. Show that $\ell(R/I^{[p^e]})/p^{e \dim(R)}$ is a Cauchy sequence and therefore the Hilbert-Kunz multiplicity of I exists.

There is an important connection between Hilbert-Kunz multiplicity and F-signature.

Theorem 6.3 ([PT18])**.** *Let $(R, \mathfrak{m}, k)$ be a local F-finite domain of prime characteristic $p > 0$. Then*

$$s(R) = \inf\{\mathrm{e}_{\mathrm{HK}}(I) - \mathrm{e}_{\mathrm{HK}}(J) \mid I \subsetneq J \textit{ are } \mathfrak{m}\textit{-primary ideals}\}.$$

An important open problem in prime characteristic commutative algebra, which would have a large impact on tight closure theory, is whether or not the F-signature of a local ring can always be realized as a relative Hilbert-Kunz multiplicity.

Conjecture 6.4. *Let $(R, \mathfrak{m}, k)$ be a local F-finite domain of prime characteristic $p > 0$. Then*

$$s(R) = \min\{\mathrm{e}_{\mathrm{HK}}(I) - \mathrm{e}_{\mathrm{HK}}(J) \mid I \subsetneq J \textit{ are } \mathfrak{m}\textit{-primary ideals}\}.$$

Large classes of rings are known to satisfy Conjecture 6.4. We guide the reader through Huneke's and Leuschke's proof that every Gorenstein local ring satisfies the conclusion of Conjecture 6.4.

Recall that if $(R, \mathfrak{m}, k)$ is a Gorenstein local ring and $\underline{x} = x_1, \ldots, x_d$ a system of parameters of R then there exists $u \in R - (\underline{x})$ such that the class of u generates $((\underline{x}) : \mathfrak{m})/(\underline{x})$. When this happens we say that the element u *generates the socle mod* $(\underline{x})$.

Exercise 101. Let $(R, \mathfrak{m}, k)$ be a local Gorenstein ring and

$$0 \to R \to M \to C \to 0$$

a short exact sequence of finitely generated R-modules. Suppose further that C is maximal Cohen-Macaulay module. Show that $M \cong R \oplus C$. (Hint: $\mathrm{Ext}^1_R(C, R) = 0$.)

The following is the main step towards proving Conjecture 6.4 for Gorenstein rings.

Exercise 102. Let $(R, \mathfrak{m}, k)$ be a Gorenstein local ring of dimension d and let M be a finitely generated maximal Cohen-Macaulay module which does not have a free summand. Let $\underline{x} = x_1, \ldots, x_d$ be a system of parameters of R and let u generate the socle mod $(\underline{x})$. We guide the reader through a proof that $uM \subseteq (\underline{x})M$. Let $m_1, \ldots, m_N \in M$ generate M as an R-module and consider the R-linear map $\varphi : R \to M^{\oplus N}$ defined by $1 \mapsto (m_1, \ldots, m_N)$.

(1) Let $I = \operatorname{Ann}_R M$. Show that there is a short exact sequence of the form

$$0 \to R/I \to M \to C \to 0$$

where C is the cokernel of φ.

(2) Assume that C is not maximal Cohen-Macaulay. Show that

$$R/(\underline{x}) \xrightarrow{\overline{\varphi}} M^{\oplus N}/(\underline{x}M^{\oplus N})$$

has nonzero kernel and therefore contains $((\underline{x}) : \mathfrak{m})/(\underline{x})$.

(3) Assume that C is maximal Cohen-Macaulay. Show that under this assumption that $I \not\subseteq (\underline{x})$. (Hint: $\underline{x}$ is regular on M and C and therefore regular on R/I and therefore if we assume $(\underline{x}) \subseteq I$ then $I = I \cap (\underline{x}) = I(\underline{x})$. Now use Nakayama's Lemma to conclude that $I = 0$ and then Exercise 101 to reach a contradiction.)

(4) Continue to assume C is maximal Cohen-Macaulay. By part (3) we know that $(\underline{x}) \not\subseteq I$. Using this fact, conclude that

$$R/(\underline{x}) \xrightarrow{\overline{\varphi}} M^{\oplus N}/(\underline{x})M^{\oplus N}$$

has nonzero kernel and therefore contains $((\underline{x}) : \mathfrak{m})/(\underline{x})$.

(5) Use parts (2) and (4) to conclude that $uM \subseteq (\underline{x})M$.

Exercise 103. Let $(R, \mathfrak{m}, k)$ be a local F-finite Gorenstein domain or prime characteristic $p > 0$. Suppose that $R^{1/p^e} \cong R^{\oplus a_e(R)} \oplus M_e$ and M_e does not have a direct summand. Suppose further that $\underline{x} = x_1, \ldots, x_d$ is a system of parameters of R and u generates the socle mod $(\underline{x})$.

(1) Use Exercise 102 to show that

$$\frac{\ell\left((\underline{x}, u)^{[p^e]} \big/ (\underline{x})^{[p^e]}\right)}{p^{e \dim(R)}} = \frac{a_e(R)}{\operatorname{rank}(R^{1/p^e})}.$$

(2) Conclude that $\mathrm{e}_{\mathrm{HK}}((\underline{x})) - \mathrm{e}_{\mathrm{HK}}((\underline{x}, u)) = s(R)$.

References

[AL03] Ian M. Aberbach and Graham J. Leuschke. The F-signature and strong F-regularity. *Math. Res. Lett.*, 10(1):51–56, 2003. 33, 34

[Car17] Javier Carvajal-Rojas. Finite torsors over strongly F-regular singularities. *ArXiv e-prints*, October 2017. 26

[CEMS18] Alberto Chiecchio, Florian Enescu, Lance Edward Miller, and Karl Schwede. Test ideals in rings with finitely generated anti-canonical algebras. *J. Inst. Math. Jussieu*, 17(1):171–206, 2018. 16

[CLS11] David A. Cox, John B. Little, and Henry K. Schenck. *Toric varieties*, volume 124 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011. 22

[CST16] Javier Carvajal-Rojas, Karl Schwede, and Kevin Tucker. Fundamental groups of F-regular singularities via F-signature. *ArXiv e-prints*, June 2016. 26

[DPY16] Alessandro De Stefani, Thomas Polstra, and Yongwei Yao. Globalizing F-invariants. *ArXiv e-prints*, August 2016. 19, 20, 38

[DSPY18] Alessandro De Stefani, Thomas Polstra, and Yongwei Yao. Generalizing Serre's splitting theorem and Bass's cancellation theorem via free-basic elements. *Proc. Amer. Math. Soc.*, 146(4):1417–1430, 2018. 38

[Fed83] Richard Fedder. F-purity and rational singularity. *Trans. Amer. Math. Soc.*, 278(2):461–480, 1983. 11, 14

[Ful93] William Fulton. *Introduction to toric varieties*, volume 131 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1993. The William H. Roever Lectures in Geometry. 22

[Har98] Nobuo Hara. A characterization of rational singularities in terms of injectivity of Frobenius maps. *Amer. J. Math.*, 120(5):981–996, 1998. 2

[HH90] Melvin Hochster and Craig Huneke. Tight closure, invariant theory, and the Briançon-Skoda theorem. *J. Amer. Math. Soc.*, 3(1):31–116, 1990. 2

[HH94a] Melvin Hochster and Craig Huneke. F-regularity, test elements, and smooth base change. *Trans. Amer. Math. Soc.*, 346(1):1–62, 1994. 2

[HH94b] Melvin Hochster and Craig Huneke. Tight closure of parameter ideals and splitting in module-finite extensions. *J. Algebraic Geom.*, 3(4):599–670, 1994. 2, 16

[HL02] Craig Huneke and Graham J. Leuschke. Two theorems about maximal Cohen-Macaulay modules. *Math. Ann.*, 324(2):391–404, 2002. 20

[HR74] Melvin Hochster and Joel L. Roberts. Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. *Advances in Math.*, 13:115–175, 1974. 2

[HS77] Robin Hartshorne and Robert Speiser. Local cohomological dimension in characteristic p. *Ann. of Math. (2)*, 105(1):45–79, 1977. 2

[HW02] Nobuo Hara and Kei-Ichi Watanabe. F-regular and F-pure rings vs. log terminal and log canonical singularities. *J. Algebraic Geom.*, 11(2):363–392, 2002. 2

[HY02] Craig Huneke and Yongwei Yao. Unmixed local rings with minimal Hilbert-Kunz multiplicity are regular. *Proc. Amer. Math. Soc.*, 130(3):661–665, 2002. 37

[HY03] Nobuo Hara and Ken-Ichi Yoshida. A generalization of tight closure and multiplier ideals. *Trans. Amer. Math. Soc.*, 355(8):3143–3174 (electronic), 2003. 2

[Kun69] Ernst Kunz. Characterizations of regular local rings for characteristic p. *Amer. J. Math.*, 91:772–784, 1969. 5, 9

[Kun76] Ernst Kunz. On Noetherian rings of characteristic p. *Amer. J. Math.*, 98(4):999–1013, 1976. 2, 8, 9

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid. 8, 37

[Mon83] P. Monsky. The Hilbert-Kunz function. *Math. Ann.*, 263(1):43–49, 1983. 36

[Mon08] Paul Monsky. Rationality of Hilbert-Kunz multiplicities: a likely counterexample. *Michigan Math. J.*, 57:605–613, 2008. Special volume in honor of Melvin Hochster. 22

[Nag62] Masayoshi Nagata. *Local rings*. Interscience Tracts in Pure and Applied Mathematics, No. 13. Interscience Publishers a division of John Wiley & Sons New York-London, 1962. 5

[Pol18] Thomas Polstra. Uniform bounds in F-finite rings and lower semi-continuity of the F-signature. *Trans. Amer. Math. Soc.*, 370(5):3147–3169, 2018. 31

[PT18] Thomas Polstra and Kevin Tucker. F-signature and Hilbert–Kunz multiplicity : a combined approach and comparison. *Algebra Number Theory*, 12(1):61–97, 2018. 35, 39

[Sin99] Anurag K. Singh. **Q**-Gorenstein splinter rings of characteristic p are F-regular. *Math. Proc. Cambridge Philos. Soc.*, 127(2):201–205, 1999. 16

[Smi97] Karen E. Smith. F-rational rings have rational singularities. *Amer. J. Math.*, 119(1):159–180, 1997. 2

[Sta82] J. T. Stafford. Generating modules efficiently over noncommutative rings. In *Paul Dubreil and Marie-Paule Malliavin Algebra Seminar, 34th Year (Paris, 1981)*, volume 924 of *Lecture Notes in Math.*, pages 72–88. Springer, Berlin-New York, 1982. 38

[sta16] The Stacks Project. 2016. 10

[Tuc12] Kevin Tucker. F-signature exists. *Invent. Math.*, 190(3):743–765, 2012. 19

[WY00] Kei-ichi Watanabe and Ken-ichi Yoshida. Hilbert-Kunz multiplicity and an inequality between multiplicity and colength. *J. Algebra*, 230(1):295–317, 2000. 37

[WY04] Kei-ichi Watanabe and Ken-ichi Yoshida. Minimal relative Hilbert-Kunz multiplicity. *Illinois J. Math.*, 48(1):273–294, 2004. 24

Appendix A. Divisors and symbolic powers

The purpose of this appendix is to guide reader through the basics of Weil divisors and connections with symbolic powers of height one ideals.

Let R be a Noetherian normal domain and K its field of fractions. Let $X = \operatorname{Spec}(R)$. A *Weil divisor* on X is a formal sum, over $\mathbb{Z}$, of codimension 1 irreducible subvarieties of X, i.e., a formal sum of height 1 primes of R, such that all but finitely many coefficients are 0. For example, if P_1, P_2 are height 1 primes of R then the following are examples of divisors:

(1) $D_1 = 2P_1 - 3P_3$
(2) $D_2 = P_1 + P_2 + P_3$
(3) $D_3 = 0$ (i.e., all coefficients are 0).

We let $\operatorname{Div}(X)$, and sometimes $\operatorname{Div}(R)$, be the free abelian group on all height 1 primes of R.

If $P \in \operatorname{Spec}(R)$ is a height 1 prime then R_P is a regular local ring of Krull dimension 1, and therefore is a principal ideal domain with fraction field K. Suppose that PR_P, the maximal ideal of R_P, is principally generated by $\pi_P \in R_P$. If $f \in K$ then f can be uniquely written as $u\pi_P^N$ for some unit $u \in R_P$ and $N \in \mathbb{Z}$. Thus for each height 1 prime P there is a valuation $\nu_P : K^\times \to \mathbb{Z}$ defined as follows:

$$\nu_P(f) = N$$

where N is the unique integer such that $f = u\pi_P^N$ and u is a unit of R_P.

Exercise 104. Let R be a normal domain, K its field of fractions, and $f \in K^\times$.

(1) Let P be a height 1 prime. Show that $f \in R_P$ if and only if $\nu_P(f) \geq 0$.
(2) Show that there exists only finitely many height 1 primes P such that $\nu_P(f) \neq 0$. (Hint: Write $f = \frac{f_1}{f_2}$ where f_1, f_2 are elements of R. Then for each prime P of height 1 we have $\nu_P(f) = \nu_P(f_1) - \nu_P(f_2)$. Therefore it is enough to solve the exercise for elements of R.)
(3) Conclude that for each $f \in K^\times$ there is a well-defined Weil divisor $\operatorname{div}(f)$ defined by

$$\sum_{\substack{P \in \operatorname{Spec}(R) \\ \operatorname{ht}(P)=1}} \nu_P(f)P.$$

(4) A divisor of the form $\operatorname{div}(f)$ is called a *principal divisor*. Show that the subset of $\operatorname{Div}(R)$ which consists of principal divisors forms a subgroup of $\operatorname{Div}(R)$.

Since the set of principal divisors form a subgroup of $\operatorname{Div}(R)$ there is an equivalence relation on $\operatorname{Div}(R)$ defined by $D_1 \sim D_2$ if $D_1 - D_2$ is a principal divisor. In fact, we say D_1 and D_2 are *linearly equivalent* if $D_1 \sim D_2$. The quotient group formed by modding out by all principal divisors is referred to as the *divisor class group of* R and is denoted by $\operatorname{cl}(R)$.

Exercise 105. Let R be a Noetherian normal domain. Show that R is a unique factorization domain if and only if $\operatorname{cl}(R) = 0$, i.e., every Weil divisor is principal. (Hint: Use the characterization that a R is a unique factorization domain if and only if every height 1 prime ideal is principal.)

Suppose D is a Weil divisor. We say that D is *effective* if all coefficients of D are non-negative. Similarly, we say that D is *anti-effective* if all coefficients of D are non-positive. If D is effective we write $D \geq 0$. More generally, if D_1, D_2 are Weil divisors we write $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$, i.e., all coefficients of D_1 are greater than or equal to the coefficients of D_2.

Exercise 106. Let R be a Noetherian normal domain and D a Weil divisor. Show that D is linearly equivalent to an effective divisor.

Exercise 107. Let R be a Noetherian normal domain and $f \in K^{\times}$. Show that $\operatorname{div}(f) \geq 0$ if and only if $f \in R$. (Hint: Recall that R being a normal domain implies that

$$R = \bigcap_{\substack{P \in \operatorname{Spec}(R) \\ \operatorname{ht}(P)=1}} R_P.)$$

If D is a divisor on a normal domain R then we let

$$R(D) := \{f \in K^{\times} \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

The following exercise guides the reader through a proof that each of the sets $R(D)$ are finitely generated R-module.

Exercise 108. Let R be a Noetherian normal domain and D, D_1, D_2 be Weil divisors.

(1) Show that $R(D)$ is an R-submodule of K.
(2) Show that $R(0) = R$.
(3) Show that $R(D_1) \subseteq R(D_2)$ if and only if $D_2 \geq D_1$. In particular, conclude that $R(D) \subseteq R$ if and only if D is anti-effective.
(4) Given $f \in K^{\times}$ show that there is an R-module isomorphism

$$R(D) \xrightarrow{\cdot f} R(-\operatorname{div}(f) + D).$$

(5) Show that $R(D)$ is a finitely generated R-module. (Hint: Find $f \in K^{\times}$ so that $-\operatorname{div}(f) + D$ is anti-effective and use part (3) and (4) of the exercise.)

The reader should now be able to make a connection with ideals of the form $R(D)$ and symbolic powers of ideals. Recall that if $P \subseteq R$ is a prime ideal then $P^{(n)} = P^n R_P \cap R$.

Exercise 109. Let $P_1, \ldots, P_\ell$ be finitely many height one primes of R and $n_1, \ldots, n_\ell$ non-negative integers. Show that

$$P_1^{(n_1)} \cap \cdots \cap P_1^{(n_\ell)} = R(-n_1 P_1 - \cdots - n_\ell P_\ell).$$

Department of Mathematics, University of Utah, Salt Lake City, UT 84102 USA
Email address: lquanma@math.utah.edu

Department of Mathematics, University of Utah, Salt Lake City, UT 84102 USA
Email address: polstra@math.utah.edu