Enhanced Algorithms For F-Pure Threshold Computation

by

Gilad Pagi

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2018

Doctoral Committee:

Professor Karen E. Smith, Chair
Associate Professor Bhargav B. Bhatt
Professor Sergey Fomin
Professor Melvin Hochster
Professor Mircea I. Mustaţă
Associate Professor James P. Tappenden

Gilad Pagi

gpagi@umich.edu

ORCID-iD: 0000-0003-4393-6055

To my beautiful family, thanks for the *support* in crossing this *threshold*.

ACKNOWLEDGEMENTS

This dissertation is being written under the direction of Karen Smith of University of Michigan. I would like to thank Prof. Smith for many enlightening discussions. Many thanks to Prof. Daniel Hernández for his remarks on the earlier draft and to Prof. Michael Zieve, Prof. Sergey Fomin and Prof. Bhargav Bhatt for fruitful conversations.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

ABSTRACT

In this dissertation, we explore different computational techniques for the F-pure threshold invariant of monomial ideals and of polynomials. For the former, we introduce a novel algorithm to reduce the number of generators of the ideal and the number of variables involved in the remaining generators, thus effectively creating a new "simpler" ideal with the same value of the F-pure threshold. Then, the value is the sum of entries of the inverse to the new ideal's splitting matrix. This algorithm can be further improved by using the integral closure of the ideal.

For polynomials, we introduce a direct computational technique involving properties of roots of Deuring polynomials, which are closely related to Legendre polynomials. This technique is then applied to two different families of polynomials: polynomials defining Elliptic Curves, and bivariate homogeneous polynomials with up to four distinct roots in projective space of dimension 1. The invariance of the F-pure threshold under changing variables is then used to prove properties of prime characteristic roots of Legendre polynomials.

We end the dissertations with generalizing the Deuring polynomial techniques used thus far, and introducing a way to explicitly stratify the coefficient space of polynomials supported by a fixed set of monomials, by identifying regions representing polynomials with the same F-pure threshold. We give an explicit description of the different strata as subschemes of a projective space.

CHAPTER I

Introduction, Motivation, and Results

1.1 Background and Motivation

Consider the polynomial ring $R = K[x_1, ..., x_t]$, where K is a field of prime characteristic p. In this thesis we are mainly concerned with direct computational methods for the *F-pure threshold* of either a polynomial f, denoted $FT(f)$, or an monomial ideal I, denoted $FT(I)$. The F-pure threshold is a numerical invariant, measuring the singularity of the hypersurface $\mathbb{V}(f)$ or the subscheme $\mathbb{V}(I)$ at a point, which, without loss of generality, we assume to be the origin of K^t. For example, if f is smooth at the origin, then $FT(f) = 1$. Smaller values of $FT(f)$ mean "worse singularities" of f at that point.

The F-pure threshold can be viewed as a characteristic p analog of the *log canonical threshold*, an invariant of singularities in characteristic 0. The log canonical threshold of a complex polynomial f (at the origin), denoted $\operatorname{lct}(f)$, is the supremum over all non-negative real numbers λ such that $|f|^{-2\lambda}$ is locally integrable at the origin of $\mathbb{C}^t$. The log canonical threshold plays a crucial role in birational geometry and, specifically, in the *Minimal Model Program* in characteristic 0. There is optimism that the F-pure threshold can play a similar role in finally settling the Minimal Model Program in characteristic p. See surveys [KM98], [ST12], [Kol13].

Our work concentrates on the computation of the F-pure threshold in the case of

polynomials and monomial ideals in polynomial rings, although the F-pure threshold can be defined for any ideal in any regular ring and even more generally. While the definition arose in the theory of tight closure and F-purity of pairs ([HR76],[HH90], [HY03]), we approach the subject using an alternative definition and the reader needs nothing more in order to appreciate the computational techniques presented in later chapters.

Definition I.1 (see [MTW05], [BMS08])**.** Fix a field K of characteristic $p > 0$, let $I \subset K[x_1, ..., x_t]$ be an ideal. Denote $R = K[x_1, ..., x_t]$. The F-pure threshold of I (at the origin) is:

$$FT(I) := \sup \left\{ \frac{N}{p^e} \;\middle|\; N, e \in \mathbb{Z}_{>0}, I^N \not\subset (x_1^{p^e}, ..., x_t^{p^e})R \right\}. \tag{I.1.1}$$

Specifically, when I is principle, say $I = (f)$ for some polynomial $f \in K[x_1, ..., x_t]$, we have:

$$FT(f) := \sup \left\{ \frac{N}{p^e} \;\middle|\; N, e \in \mathbb{Z}_{>0}, f^N \not\in (x_1^{p^e}, ..., x_t^{p^e})R \right\}. \tag{I.1.2}$$

Notice that p is absent from the notation and should be understood from the context.

Suppose $f \in \mathbb{Z}[x_1, ..., x_t]$ has integer coefficients. For each prime p, f has a natural image in $\mathbb{F}_p[x_1, ..., x_t]$, denoted f_p. Now we can compute $FT(f_p)$, for each p, and compare it to $\mathrm{lct}\,(f)$. A well known feature of the F-pure threshold is that the limit of $FT(f_p)$, when $p \to \infty$, approaches the log canonical threshold of f. This fact is the culmination of a series of papers, going back to [HH90], [Smi00], [Har01], [HW02], [HY03], [Tak04], [HT04], [TW04], until finally articulated in [MTW05, Theorem 3.4]. Based on experimental evidence, even more is expected, as the following decades-old open question suggests:

Question I.2. Let $f \in \mathbb{Z}[x_1, .., x_t]$, such that $f \in (x_1, ..., x_t)$. For any prime p, denote by f_p the natural image in $\mathbb{F}_p[x_1, ..., x_t]$. Let $\mathcal{P}$ be the set of all primes p such that $FT(f_p) = \text{lct}\,(f)$. Is it true that $\mathcal{P}$ is of infinite cardinality?

For a general $f \in \mathbb{C}[x_1, .., x_t]$ the same question can be asked, only the *reduction to positive characteristic* step is a bit more technical. However, the conjecture is still open and worth researching even when f has integer coefficients. This question, as stated, appears in [MTW05, Conjenture 3.6], but it roots date back to the work of the Japanese school of tight closure (see [HW02]). Surveys and other formulation can be found in [Smi97],[BFS13] and [EM06].

The open question itself motivates us to improve our methods of computing the F-pure threshold and the log canonical threshold of a polynomial f. In [Her16], Hernandez identifies scenarios where the answer for **Question I.2** is positive based on properties of the monomial ideal generated by the monomials supporting f. This fact drives us to investigate the computational aspects of $FT(I)$ when I is a monomial ideal. Note that for a monomial ideal in $K[x_1, ..., x_t]$, one can compute $FT(I)$ if K is of characteristic p or $\text{lct}\,(I)$ if K has characteristic 0, and observe that these numbers are identical (see [HY03, Theorem 6.10]). As a matter of fact, it is apparent that the underlying field K, and, in particular, its characteristic, play no role in the actual computation of $FT(I)$ when I is a monomial ideal.

1.2 Outline

In Chapter II, we describe some known methods of computing $FT(I)$ for a monomial ideal I, including how to describe I by its *splitting matrix* $M \in \mathbb{Z}_{\geq 0}^{t \times s}$, containing in each column the multiexponents of the generating monomials of I. Then we develop an algorithm to simplify the ideal I by identifying a "simpler" monomial ideal

J with the same value of the F-pure threshold, possibly containing fewer monomials and involving fewer variables:

Theorem I.3. *Let I be a monomial ideal in $K[x_1, ..., x_d, x_{d+1}, .., x_t]$. Then there exists a monomial ideal J with the following properties:*

1. *$FT(I) = FT(J)$,*
2. *J is generated by d monomials involving only d variables,*
3. *The splitting matrix of J, M, is a $d \times d$ invertible matrix,*
4. *$FT(I)$ is the sum of entries of M^{-1}.*

Note that the last statement shows directly that $FT(I) \in \mathbb{Q}$, a well known fact as the log canonical threshold of I is rational ([Kol97, Proposition 8.5]) had we considered I to be an ideal over $\mathbb{C}$, and this number is identical to the F-pure threshold, $FT(I)$, for all p ([HY03, Theorem 6.10]).

The algorithm we develop is of polynomial time complexity. The algorithm involves a linear programming sub-procedure. Solving the general case linear programming problem in polynomial time is "Problem 9" in the list of Smale's open problems (see [Sma98]). However, our setup involves only rational numbers and there are algorithms to solve linear programming in polynomial time in this specific case, like the "interior point method"([Kar84]); we refer again to [Sma98, Problem 9] and its references for more details. In **Appendix A** we include a MATLAB code implementing a version of our algorithm.

We end this chapter by improving our algorithm as we apply it on the integral closure of I, $\overline{I}$, instead of I. This approach is justified as $FT(I) = FT(\overline{I})$ (see **Corollary II.37**).

In the next chapters we aim to compute the F-pure threshold of specific fami-

lies of polynomials. We start in Chapter III by developing the required machinery for the F-pure threshold computation of polynomials in general. Then we investigate the *Deuring polynomials*, which are closely related to the 250-year-old *Legendre polynomials*. We define the Deuring polynomial of degree n over $\mathbb{Z}[\lambda]$ or $\mathbb{F}_p[\lambda]$ as:

$$H\{n\}(\lambda) = \sum_{i=0}^{n} \binom{n}{i}^2 \lambda^i$$

The properties of their roots turn out to have crucial implications on the F-pure threshold computations in the following chapters. For example, consider the polynomial $f = (x+y)(x+\lambda y)$. When we raise f to integer powers, f^N, we get that the coefficient of $x^N y^N$ is exactly $H\{N\}(\lambda)$. Even though $FT(f)$ is easy to compute for this specific f, this Deuring polynomial has a critical impact on the computation of $FT(hf)$ or $FT(h+f)$, when h is another polynomial. See **Lemma IV.5**. The most important tools of this chapter are the following, and we will heavily use them in F-pure threshold computations later.

Lemma I.4. [**Schur's Congruence**] Fix a prime p. Let $H\{n\} \in \mathbb{F}_p[\lambda]$. Write the base p-expansion of n:

$$n = b_0 p^0 + b_1 p^1 + ... + b_e p^e,$$

where $b_0, ..., b_e$ are integers between 0 and $p-1$. Then

$$H\{n\} = H\{b_0\}^1 H\{b_1\}^{p^1} H\{b_2\}^{p^2} \cdots H\{b_e\}^{p^e}$$

Theorem I.5. *Fix an integer $n \geq 1$ and a prime p such that $n < p/2$. Let K be a field of characteristic p. Then $H\{n\}$ and $H\{n-1\}$ share no roots.*

Although our proofs of these facts are independent from existing literature, one can prove them using known results of Legendre polynomials. The relationship

between the Deuring polynomials and the Legendre polynomials is explained in **section 3.5**.

In Chapter IV we put these Deuring polynomial results to use in providing a direct computation of the F-pure threshold of the family of the defining polynomials of Elliptic curves. In [BS15] it is proven:

Theorem I.6. *Let K denote a field of prime characteristic $p > 3$. Let $f \in K[x, y, z]$ be a homogeneous polynomial of degree three defining an elliptic curve E in $\mathbb{P}^2_K$. Then:*

$$FT(f) = \begin{cases} 1 & \text{if } E \text{ is ordinary} \\ 1 - \frac{1}{p} & \text{if } E \text{ is supersingular} \end{cases}$$

Bhatt and Singh provide two proofs in [BS15] using a translation into local cohomology; In contrast, our approach involves directly investigating the form of f raised to integer powers. Once we do that, we get critical coefficients of the form of the Deuring polynomials, and we apply the machinery developed in the previous chapter. We manage to reprove the theorem for $p > 2$ using this approach. For completeness, we include a direct proof for the case of $p = 2$, so the theorem can be stated for *all primes characteristics*.

In Chapter V we investigate polynomials defining subschemes of $\mathbb{P}^1$ supported at four points. We notice that when these four points are distinct, we can transform such polynomials to a more "canonical" form, which share critical features with the defining polynomials of an elliptic curves from the previous chapter. We then compute their F-pure threshold directly using the Deuring polynomials.

Theorem I.7. *Let K be a field of prime characteristic p. Let $c, b \in \mathbb{Z}_{>0}$ with $p \equiv 1 \pmod{b+c}$. Let $f \in K[x, y]$ be a homogeneous polynomial of degree $2b + 2c$ with exactly four distinct roots over $\mathbb{P}^1_{\overline{K}}$, where the multiplicities are b, b, c, c after fixing*

an order. Let a be the their cross-ratio. Denote $n = \frac{c}{c+b}(p-1)$. Then

$$FT(f) = \begin{cases} \frac{1}{b+c} & \text{if } H\{n\}(a) \neq 0 \\ \frac{1}{b+c}\left(1 - \frac{1}{p}\right) & \text{if } H\{n\}(a) = 0 \end{cases}$$

In particular, if f is a degree four polynomial with four distinct roots in $\mathbb{P}^1$, i.e. $b = c = 1$, we get:

Theorem I.8. *Let K be a field of prime characteristic p. Consider a degree four homogeneous polynomial $f \in K[x, y]$, with distinct roots over $\mathbb{P}^1_{\overline{K}}$. After fixing an order of the roots, let $a \in \overline{K}$ be their cross-ratio. Denote $n_1 = \frac{p-1}{2}$. Then*

$$FT(f) = \begin{cases} \frac{1}{2} & \text{if } p = 2 \text{ or if both } p > 2 \text{ and } H\{n_1\}(a) \neq 0 \\ \frac{1}{2}\left(1 - \frac{1}{p}\right) & \text{if } p > 2 \text{ and } H\{n_1\}(a) = 0 \end{cases}$$

It is surprising that the value of the F-pure threshold is determined by the cross-ratio, specifically whether or not the cross-ratio is a root of a certain Deuring polynomials. In addition to computing the F-pure threshold, this theorem gives us insight on the roots of Deuring polynomials and Legendre polynomials in positive characteristic, which is of independent interest; we introduce a new proof of the following known property (see the equivalent result for Deuring polynomials in [BM04]):

Corollary I.9. Fix a prime $p > 2$, a field K of characteristic p and let $n = \frac{p-1}{2}$. If $b \in K - \{\pm 1\}$ is a root of the Legendre polynomial of degree n, $P_n(x) \in K[x]$, then these are roots as well:

$$\pm b, \pm\frac{3+b}{-1+b}, \pm\frac{3-b}{1+b}.$$

We dedicate the last chapter to generalizing the computational technique we used so far, specifically, we are generalizing the elegant **Schur's Congruence**(**Lemma I.4**). Such generalization is possible under some assumptions (**Conjecture VI.21**). Fix

a set of monomials, $\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}$. Let $b_1, ..., b_s$ be indeterminates. We are interested in computing the F-pure threshold of a generic polynomial:

$$f = b_1\boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + b_s\boldsymbol{x}^{\boldsymbol{\mu}_s}.$$

Then, we wish to find out how $FT(f)$ changes when we plug in scalars from K instead of the b's and get a "specialized" polynomial in $K[x_1, ..., x_t]$. Put differently, we are interested in investigating the function:

$$FT : \mathbb{P}^{s-1} \to \mathbb{Q},$$

defined by

$$FT(c_1, ..., c_s) = FT(f), \text{ where } f = c_1\boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + c_s\boldsymbol{x}^{\boldsymbol{\mu}_s}.$$

In [BMS08] it is proven that FT obtains only finitely many values. By assuming **Conjecture VI.21**, we are able to offer a constructive proof of that fact and show explicitly which regions of $\mathbb{P}^{s-1}$ obtain the same value under FT. These regions are complements of vanishing sets of a finite number of coefficients that we compute from the monomials $\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}$. These coefficients plays a similar role to the Deuring polynomials we encountered in previous chapters.

CHAPTER II

F-Pure Threshold of Monomial Ideals

In this chapter, we shall define and investigate the F-pure threshold of a monomial ideal I. We describe some known methods of computing $FT(I)$, including the *Newton polygon* and the *Splitting polytope*. By applying both methods simultaneously, we develop the **Monomial Ideal Reduction Algorithm** to simplify the ideal I by identifying a "simpler" monomial ideal J with the same value of the F-pure threshold, possibly containing fewer monomials and involving fewer variables. We end the chapter with an improvement of the algorithm using I's integral closure.

2.1 Definitions

The following is another interpretation of the definition of the F-pure threshold.

Definition II.1 (see [MTW05])**.** Let $I \subset K[x_1, ..., x_t]$ be a non-zero ideal, where K is a field of prime characteristic p. Denote $\mathfrak{m} = (x_1, ..., x_t)$ and assume $I \subset \mathfrak{m}$. For a positive integer e, let:

$$\nu_I(p^e) := \max\{w \mid I^w \not\subset \mathfrak{m}^{[p^e]}\}.$$

Then the F-pure threshold of I at the origin is

$$FT(I) := \lim_{e\to\infty} p^{-e}\nu_I(p^e)$$

Note that p is absent from the notation and should be understood from the context.

Discussion II.2. The above is well defined: If I is generated by s elements, then $I^{s(p^e-1)+1}$ has to be in $\mathfrak{m}^{[p^e]}$ by the pigeon hold principle, which gives an upper bound for $\nu_I(p^e)$. Further, if $I^n \subset \mathfrak{m}^{[p^{e+1}]}$ then $I^n \subset \mathfrak{m}^{[p^e]}$, which tells us that every upper bound of $\nu_I(p^{e+1})$ is also an upper bound of $\nu_I(p^e)$, thus the sequence $\{\nu_I(p^e)\}_e$, is non-decreasing. We can say something stronger. Due to the faithful flatness of the Frobenius map on a regular ring we get that:

$$I^{\nu_I(p^e)} \not\subset \mathfrak{m}^{[p^e]} \Rightarrow \left(I^{\nu_I(p^e)}\right)^{[p]} \not\subset \mathfrak{m}^{[p^{e+1}]} \Rightarrow I^{p\nu_I(p^e)} \not\subset \mathfrak{m}^{[p^{e+1}]}$$

So $p\nu_I(p^e) \leq \nu_I(p^{e+1})$, which implies that the sequence $\{p^{-e}\nu_I(p^e)\}_e$ is non-decreasing. Since it is bounded above by the sequence $\{p^{-e}(s(p^e-1)+1)\}_e$, the limit $FT(I)$ exists and bounded above by s, the number of generators of I. It is bounded below by 0 since for large values of e, I is not in $\mathfrak{m}^{[p^e]}$ and the sequence $\{p^{-e}\nu_I(p^e)\}_e$ is not constant zero.

Discussion II.3. To summarize, let $I \subset K[x_1, ..., x_t]$ be a non-zero ideal, generated by s elements, where K is a field of prime characteristic p, Denote $\mathfrak{m} = (x_1, ..., x_t)$ and assume $I \subset \mathfrak{m}$. Then $FT(I) \in (0, s]$.

Example II.4. When $I = (x_1, ..., x_t) = \mathfrak{m}$, $\nu_I(p^e) = s \cdot (p^e - 1)$ by the pigeonhole principle. So it is easy to see that $FT(I) = t$, where t is the number of generators.

The F-pure threshold of any ideal is actually a rational number (see [BMS09]); we shall later provide a proof for the monomial case using the computational techniques we develop.

Example II.5. Consider $I = (x, y^2)$ in $\mathbb{F}_3[x, y]$. Let us show that $FT(I) = 3/2$. Fix $e > 0$. We claim that for $w = 3^e - 1 + \frac{3^e-1}{2}$, I^w is not in (x^{3^e}, y^{3^e}): just observe the

element $x^{3^e-1}y^{2\frac{3^e-1}{2}}$ in I^w and not in (x^{3^e}, y^{3^e}). By taking e to infinity we see that $3/2 \leq FT(I)$. On the other hand, all the elements of I^{w+1} are in (x^{3^e}, y^{3^e}), so by definition $w = \nu_I(p^e)$ and thus $3/2$ is indeed $FT(I)$.

We would like to concentrate on the case where $I \subset K[x_1, ..., x_t]$ is a monomial ideal. In [Her16], Hernández introduces a method of computing $FT(I)$ using its "Splitting Matrix". Specifically, [Her16, Proposition 36] reproves that the F-pure threshold of a monomial ideal is not only independent of the characteristic, it is identical to the *log canonical threshold* of I at the origin, $\mathrm{lct}\,(I)$, where we replace K by $\mathbb{C}$. The log canonical threshold of I can be computed by I's "Newton polygon" ([How01, Example 5])[1] thus can be used to compute the same number. We shall present both methods now. Then we will create an algorithm that utilizes both methods simultaneously in order to find a "simpler" ideal in a "simpler" polynomial ring with the same F-pure threshold, for which the computation is easier.

2.1.1 Newton Polygon

Fix a ring $R = K[x_1, ..., x_t]$ where K is any field. We adopt a multiexponent notation and denote $x_1^{\mu_1}x_2^{\mu_2}\cdots x_t^{\mu_t}$ as $\boldsymbol{x}^{\boldsymbol{\mu}}$. Consider the monomial ideal $I = (\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s})$, $\boldsymbol{\mu}_j = (\mu_{1j}, ..., \mu_{tj}) \in \mathbb{Z}^t_{\geq 0}$, $j = 1, ..., s$, in $K[x_1, ..., x_t]$. The *Newton Polygon* of I, N, is defined in the following way. Let L be the set of points representing all the monomials in I, where $\boldsymbol{x}^{\boldsymbol{\mu}} = \boldsymbol{x}^{(\mu_{1j},...,\mu_{tj})}$ is interpreted as a point in $(\mu_{1j}, ..., \mu_{tj}) \in \mathbb{R}^t$; then N is a the convex hull of L in $\mathbb{R}^t$. Note that N is independent of the set of generators of I.

Combine [How01, Example 5] with [Her16, Proposition 36] to conclude[2]:

[1] We follow [How01] and refer to this object as a "polygon" rather than "polytope" even though it is not necessarily two dimensional

[2] Originally, $FT(I) = \mathrm{lct}\,(I)$ is proven in [HY03]

Theorem II.6. *Let I be a monomial ideal in $K[x_1, .., x_t]$, where K is a field. Let N be I's Newton Polygon. Denote $\mathbf{1}_t = (1, ..., 1) \in \mathbb{R}^t$. Then*

$$\text{lct}\,(I) = \max\{\lambda \neq 0 \mid \tfrac{1}{\lambda}\mathbf{1} \in N\} \quad \textit{when } \text{char}K = 0$$

$$FT(I) = \max\{\lambda \neq 0 \mid \tfrac{1}{\lambda}\mathbf{1} \in N\} \quad \textit{when } \text{char}K > 0.$$

I.e, the F-pure threshold (or the log canonical threshold) is the reciprocal of any coordinate of the point where the ray directed (1,...,1) punctures N.

Note that in order to identify the puncture point, suffices to compute the boundary of the polygon, which is part of the convex hall of any set of generators. Also note that by using the natural $\mathbb{N}^t$-grading on the ring, we can identify any monomial ideal I with a minimal set of generators and consider the convex hull of them. As a matter of fact, the Newton polygon is actually a property of the *integral closure* of I. We expand on this point of view later in **subsection 2.2.1**.

Example II.7. Let us repeat the computation in **Example II.5**. The Newton polygon of I is generated by $(1, 0)$ and $(0, 2)$. The boundary can be represented by the equation $y = 2 - 2x$. Requiring $x = y$ yields to $x = 2/3$. The reciprocal is $FT(I) = 3/2$ as expected.

Discussion II.8. Theorem II.6 reveals a rather geometric description of $FT(I)$, it is set by the distance along which the ray $\mathbf{1}_s$ punctures the boundary of the Newton polygon. This polygon can be complicated; however we will show that we can change I and thus change the polygon, without affecting the coordinates of the puncture point.

Example II.9. Let $I = (x^{20}y^{10}z^{14}, x^{10}y^{20}z^{15}) \subset K[x, y, z]$. A part of the boundary of I's Newton polygon and the puncture point can be seen in **Figure 2.2**. A computation reveals that the coordinates of the points are (15,15,15). Ergo, we would

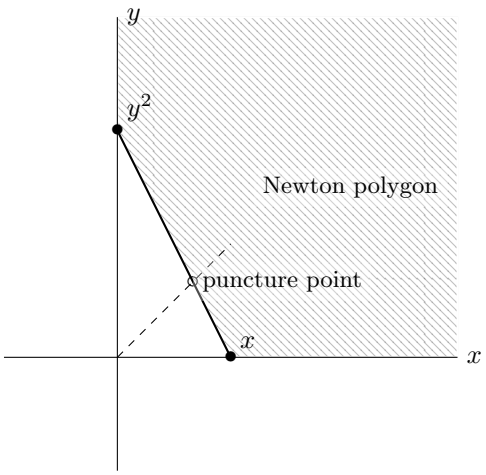

Figure 2.1: Newton polygon of (x, y^2)

have gotten the same result, if we had projected the problem to the x, y plane. Algebraically, this is equivalent to computing $FT(I')$ of $I' = (x^{20}y^{10}, x^{10}y^{20}) \subset K[x, y]$, as seen in **Figure 2.3**. We later formulate how to do these reductions systematically.

2.1.2 Hernandez's Splitting Matrix and Splitting Polytope

Recall our multiexponent notation: we denote $x_1^{\mu_1} x_2^{\mu_2} \cdots x_t^{\mu_t}$ as $\boldsymbol{x}^{\boldsymbol{\mu}}$. Consider the monomial ideal $I = (\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s})$, $\boldsymbol{\mu}_j = (\mu_{1j}, ..., \mu_{tj}) \in \mathbb{Z}^t_{\geq 0}$, $j = 1, ..., s$, in $K[x_1, ..., x_t]$ where K can be any field. The *Splitting Matrix* of I is $M = \{\mu_{ij}\}$. It is a matrix with non-negative integer entries of size $t \times s$; every column represents a monomial in the generating set and every row corresponds to a variable.

Unless defined otherwise, for a vector $\mathbf{k} = (k_1, ..., k_s) \in \mathbb{Z}^s_{\geq 0}$, we denote by $|\mathbf{k}|$ the sum of its entries (not to be confused with its norm), and $\max \mathbf{k}$ as its maximal entry.

$$|\boldsymbol{k}| = k_1 + k_2 + ... + k_s \tag{II.9.1}$$

$$\max \boldsymbol{k} = \max_{1 \leq j \leq s} k_j \tag{II.9.2}$$

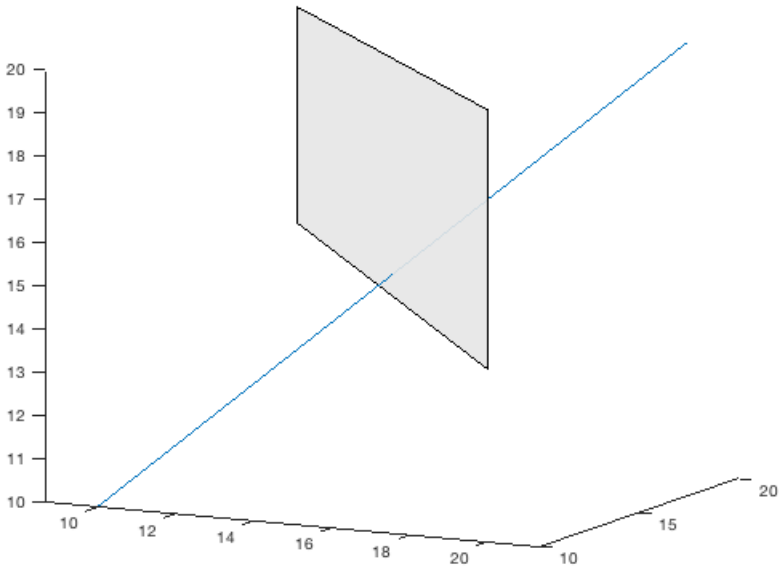

Figure 2.2: Newton polygon of $(x^{20}y^{10}z^{14}, x^{10}y^{20}z^{15})$

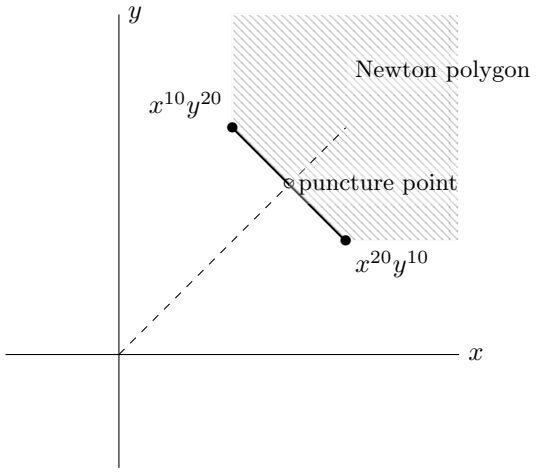

Figure 2.3: Newton polygon of $(x^{20}y^{10}, x^{10}y^{20})$

Also, we use $\preceq$ to denote component-wise inequality between vectors, i.e.

$$\boldsymbol{k} \preceq \boldsymbol{k}' \iff k_j \leq k'_j, \ \forall 1 \leq j \leq s$$

Finally, we denote $\mathbf{1}_t = (1, ..., 1) \in \mathbb{Z}^t$.

Now we are ready to compute $FT(I)$ using the splitting matrix M, as proven in [Her16, Proposition 36]:

Theorem II.10. *Consider the monomial ideal $I = (\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}) \subset K[x_1, ..., x_t]$, where K is any field. Let M be I's splitting matrix. Then*

$$FT(I) = \max\{|\boldsymbol{k}| \mid \boldsymbol{k} \in \mathbb{R}^s, \ M\boldsymbol{k} \preceq \mathbf{1}_t\}$$

Discussion II.11. From **Theorem II.10** we can see again that $FT(I)$ is independent from the underlying field. In fact it is a property of the matrix M and we can denote it as $FT(M)$. This invariant can be computed for any matrix with non-negative integer entries that does not have a row or a column of zeros.

Definition II.12 (**The Splitting Polytope**)**.** Consider the monomial ideal $I = (\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}) \subset K[x_1, ..., x_t]$, where K is any field. Let M be I's splitting matrix. The set

$$\{\boldsymbol{k} \in \mathbb{R}^s_{\geq 0} \mid M\boldsymbol{k} \preceq \mathbf{1}_t\}$$

is called the *Splitting Polytope* of M.

The splitting polytope of M is different from the Newton polygon; the former lives in $\mathbb{R}^s$, where s is the number of monomials generating I, while the latter lives in $\mathbb{R}^t$, where t is the number of variables.

To obtain the value $FT(I)$, one takes the hyperplane in $\mathbb{R}^s$ defined by $L_c := \mathbb{V}(k_1 + ... + k_s - c)$ with $c = 0$, and slides it along the direction $\mathbf{1}_s$, i.e. increasing c. We identify the largest value c such that for any $\epsilon > 0$, the hyperplane $L_{c+\epsilon}$ is no

longer intersecting the splitting polytope, while L_c does. This value of c is $FT(I)$. Put differently, if $\mathcal{S}(I)$ denotes the splitting polytope of I, then:

$$FT(I) = \sup\{c \mid \mathbb{V}(k_1 + ... + k_s - c) \cap \mathcal{S}(I) \neq \emptyset\},$$

and we can replace the supremum with maximum since $\mathcal{S}(I)$ is compact.

With that geometrical interpretation in mind, we later present a systematic procedure of eliminating monomials to get a new ideal I' and thus simplifying the splitting polytope while preserving the value $FT(I) = FT(I')$.

Example II.13. Let

$$M = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & 6 \end{bmatrix}.$$

M represents the ideal $I = (\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \boldsymbol{\mu}_3) = (xy^2, x^2y, y^6)$. In **Figure 2.4** we can see M's splitting polytope. Sliding the hypersurface $|\boldsymbol{k}| = c$ until it leaves the polytope reveals that $FT(I) = 2/3$. Note that the point of intersection happens on the $\boldsymbol{\mu}_1\boldsymbol{\mu}_2$-plane, so we would get the same F-pure threshold value if we take $I' = (\boldsymbol{\mu}_1, \boldsymbol{\mu}_2) = (xy^2, x^2y)$. That is, eliminating the last column of M.

2.2 Simplifying Splitting Matrices

Recall from the previous section that the value of the F-pure threshold of a monomial ideal can be regarded as an invariant of a splitting matrix, which can be any matrix of non-negative integer values where no row or columns is all zeros. In this section, we will show a procedure of systematically simplifying a splitting matrix while preserving the value $FT(M)$.

Definition II.14. The *unit simplex*, denoted as $\mathcal{C} = \mathcal{C}(S)$ is a set in $\mathbb{R}^s$ defined by:

$$\mathcal{C}(s) := \{\mathbf{k} \in \mathbb{R}^s \mid 0 \leq k_j \leq 1 \text{ for all } 1 \leq j \leq s \text{ and } |\boldsymbol{k}| = 1\}$$

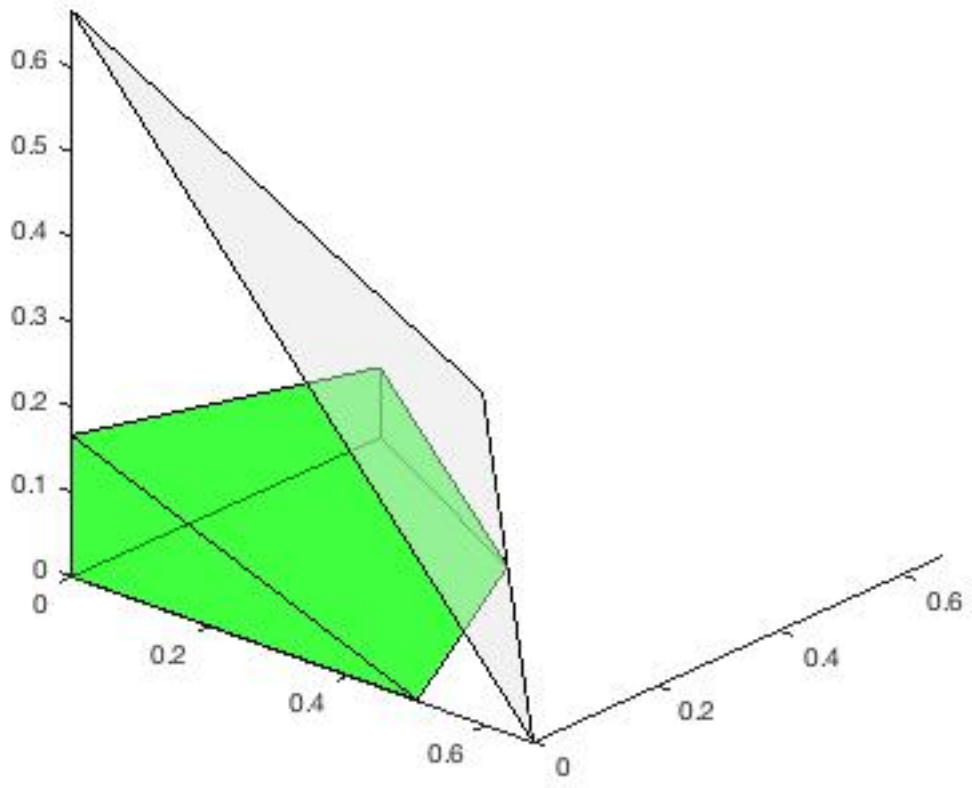

Figure 2.4: The splitting polytope of M and the hypersurface $|\boldsymbol{k}| = 2/3$

When the dimension s is understood from the context, we might just write $\mathcal{C}$.

Notice that $\mathcal{C}$ is the intersection of the unit cube $\mathcal{I}^s$ with the hyperplane $|\boldsymbol{k}| = k_1 + ... + k_s = 1$, thus compact. Also note that that $\mathcal{C}$ is convex: If $\mathbf{k}, \mathbf{k}' \in \mathcal{C}$, then for any $\lambda \in [0,1]$, the line of vectors $\boldsymbol{\ell}(\lambda) = (1-\lambda)\mathbf{k} + \lambda\mathbf{k}'$ is in $\mathcal{C}$ as the entries are all between 0 and 1, and their sum is still 1.

Definition II.15. Let $M \in \mathbb{Z}^{t\times s}$ be a splitting matrix. Let $\mathcal{C} = \mathcal{C}(s)$ be the unit simplex. Then we define:

$$\beta(M) = \min_{\mathcal{C}} \{\max M\mathbf{k}\}.$$

Let us show that the usage of min instead of inf is justified:

Proposition II.16. Let $M \in \mathbb{Z}^{t\times s}$ be a splitting matrix (so without a column with only zero entries). Denote $\mathcal{C} = \mathcal{C}(s)$. Then there exists a vector $\mathbf{k} \in \mathcal{C}$ that exhibits $\inf_{\mathcal{C}} \max M\mathbf{k}$. Moreover, $0 < \beta(M)$.

Proof. Denote $\beta = \inf_{\mathcal{C}} \max M\mathbf{k}$. The function $\max M\mathbf{k} : \mathbb{R}^s \to \mathbb{R}$ is continuous, thus obtains its extrema values on the compact set $\mathcal{C}$. Let $\mathbf{k} \in \mathcal{C}$ a vector that obtains β. Then $0 < \beta$ since the entries of M are non-negative integers, and the entries of that $\mathbf{k}$ are non-negative, while one of the k_j's must be non-zero and any column in M must contain a non-zero entry. □

The next proposition reveals the relation between $\beta(M)$ and $FT(M)$.

Proposition II.17. Let $M \in \mathbb{Z}^{t\times s}$ be a splitting matrix. Denote $\mathcal{C} = \mathcal{C}(s)$. Then $\beta(M) = 1/FT(M)$.

Proof. Suppose that $\boldsymbol{k} \in \mathcal{C}$ achieves $\beta = \beta(M)$. Define $\boldsymbol{k}' = \frac{1}{\beta}\boldsymbol{k}$. Observe that $M\boldsymbol{k}' \preceq \mathbf{1}_t$, thus $\boldsymbol{k}'$ is in the splitting polytope, and its sum of entries is $\frac{1}{\beta}$ by **Theorem II.10**

we conclude:

$$\frac{1}{\beta} \leq FT(M) \Rightarrow \frac{1}{FT(M)} \leq \beta$$

On the other hand, consider a vector $\boldsymbol{k}$ achieving $FT(M)$, that is: $M\boldsymbol{k} \preceq \mathbf{1}_t$ and $|\boldsymbol{k}| = FT(M)$. Define $\boldsymbol{k'} = \frac{1}{FT(M)}\boldsymbol{k}$. Notice that $\boldsymbol{k'} \in \mathcal{C}$, and $maxM\boldsymbol{k'} \leq \frac{1}{FT(M)}$. By definition: $\beta \leq \max M\boldsymbol{k'} \leq \frac{1}{FT(M)}$ so we conclude:

$$\beta(M) = 1/FT(I)$$

□

Discussion II.18. The characterization in **Definition II.15** leads to an important insight regarding the invariant $\beta(M)$. Working with $\boldsymbol{k} \in \mathcal{C}$ can be interpreted as minimizing a "convex" linear combination in the columns space of M while we are maximizing the entries of $M\boldsymbol{k}$. So, in some sense, we are minimizing over the columns while maximizing over the rows. Let us formulate that idea:

Proposition II.19. Let $M = \{\mu_{ij}\} \in \mathbb{Z}_{\geq 0}^{t\times s}$ be a splitting matrix. Denote the i^{th} row as $\boldsymbol{\mu}^i$ and the j^{th} column as $\boldsymbol{\mu}_j$.

1. Let M' be the matrix obtained by deleting the i^{th} row from M. Then $FT(M) \leq FT(M')$.
2. Suppose the $\boldsymbol{\mu}^i \preceq \boldsymbol{\mu}^{i'}$, and let M' be the matrix obtained from M after deleting the i^{th} row (the "smaller" row). Then $FT(M) = FT(M')$.
3. Let M' be the matrix obtained by deleting the j^{th} column from M. Then $FT(M') \leq FT(M)$.
4. Suppose the $\boldsymbol{\mu}_{j'} \preceq \boldsymbol{\mu}_j$, and let M' be the matrix obtained from M after deleting the j^{th} column (the "bigger" column). Then $FT(M) = FT(M')$.

Proof. We shall use **Definition II.15** and prove the proposition for $\beta(M)$, which is sufficient due to **Proposition II.17**.

1. Let $\boldsymbol{k}$ obtain $\beta(M)$, i.e. $\max M\boldsymbol{k} = \beta(M)$. So $\max M'\boldsymbol{k} \leq \beta(M)$ since we are deleting an entry from $M\boldsymbol{k}$. Ergo, $\beta(M') \leq \beta(M)$.

2. Let $\boldsymbol{k}'$ obtain $\beta(M')$, i.e. $\max M'\boldsymbol{k}' = \beta(M')$. Consider $M\boldsymbol{k}'$. By the given, the i^{th} entry of $M\boldsymbol{k}'$ is smaller than the entry in the i' spot, thus smaller than the maximal entry. So $\max M'\boldsymbol{k} = \beta(M')$ and thus $\beta(M) \leq \beta(M')$. Considering the previous statement, we are done.

3. Every vector $\boldsymbol{k}' \in \mathcal{C}(s-1)$ give rise to a vector $\boldsymbol{k} \in \mathcal{C}(s)$ with $M\boldsymbol{k} = M'\boldsymbol{k}'$; just add 0 entry in the j^{th} spot to $\boldsymbol{k}$. Suppose $\boldsymbol{k}'$ obtain $\beta(M')$ and let $\boldsymbol{k}'$ give rise to $\boldsymbol{k}$ as above. So $\beta(M') = \max M\boldsymbol{k}$ is a candidate to be $\beta(M)$. Ergo $\beta(M) \leq \beta(M')$.

4. Let $\boldsymbol{k} = (k_1, ..., k_j, ..., k_s)$ obtain $\beta(M)$, so $\max M\boldsymbol{k} = \beta(M)$. Define a new vector $\boldsymbol{h} = (h_1, ..., h_s)$ with $h_j = 0, h_{j'} = k'_j + k_j$ and all the rest of the entries are identical to $\boldsymbol{k}$'s entries. We have that $\boldsymbol{h} \in \mathcal{C}(s)$ while $M\boldsymbol{h} \preceq M\boldsymbol{k}$. Eliminate the j^{th} entry to get $\boldsymbol{h}'$ with $M'\boldsymbol{h}' = M\boldsymbol{h}$. Thus:

$$\beta(M') \leq \max M'\boldsymbol{h}' = \max M\boldsymbol{h} \leq \max M\boldsymbol{k} = \beta(M).$$

   Considering the previous statement, we are done.

□

The row and column elimination describe in **Proposition II.19** can be done repeatedly. We can even say more:

Proposition II.20. Let $M = \{\mu_{ij}\} \in \mathbb{Z}_{\geq 0}^{t \times s}$ be a splitting matrix. Denote the i^{th} row as $\boldsymbol{\mu}^i$ and the j^{th} column as $\boldsymbol{\mu}_j$.

1. Suppose that $\boldsymbol{k}$ achieves $\beta(M)$, i.e. $\max M\boldsymbol{k} = \beta(M)$, while the i^{th} entry of $M\boldsymbol{k}$ is strictly less than $\beta(M)$ (we shall refer it as a sub-β entry.) Let M' be obtained from M be deleting the i^{th} row. Then $FT(M) = FT(M')$.
2. Suppose that $\boldsymbol{k}$ achieves $\beta(M)$, while the j^{th} entry of $\boldsymbol{k}$ is 0. Let M' be obtained from M be deleting the j^{th} column. Then $FT(M) = FT(M')$.

Proof.

1. Without loss of generality, we can assume that we are deleting the last row since we can rearrange the rows of M. From **Proposition II.19** we already have $\beta(M') \leq \beta(M)$. For the sake of contradiction, suppose $\beta(M') < \beta(M)$. So we have some vector $\mathbf{k}'$ such that $M'\mathbf{k}'$ has entries of $\beta(M')$ or less. Adding back the last row we get that $M\mathbf{k}'$ has the same entries as $M\mathbf{k}$ except the last entry, which must be $\beta(M)$ or more due the minimality of $\beta(M)$. Now consider a line of vectors in $\mathcal{C} = \mathcal{C}(s)$: $\boldsymbol{\ell}(\lambda) = (1-\lambda)\mathbf{k} + \lambda\mathbf{k}'$ for $\lambda \in [0,1]$. Notice that $\boldsymbol{\ell}(0) = \mathbf{k}$, $\boldsymbol{\ell}(1) = \mathbf{k}'$ and $|\boldsymbol{\ell}(\lambda)| = 1$. Each entry of $M\boldsymbol{\ell}(\lambda)$ is a linear function in λ, starting from the entry in $M\mathbf{k}$ and ending in the relevant entry in $M\mathbf{k}'$. Except the last row, all the entries start from the values $\beta(M)$ or less, and end in a value $\beta(M')$ or less. The last entry starts from a sub-$\beta(M)$ value and ends in an entry of $\beta(M)$ or more. Observe **Figure 2.5**. Looking at the maximal point of intersection of the graph of the last entry with all other graphs, one see how $\max M\boldsymbol{\ell}(\lambda) < \beta(M)$ for some $\lambda \in (0,1)$ contradicting the minimality of $\beta(M)$.
2. The proof is very similar to the last statement in **Proposition II.19**. Let $\boldsymbol{k} = (k_1, ..., k_j, ..., k_s)$ obtain $\beta(M)$, i.e. $\max M\boldsymbol{k} = \beta(M)$. Eliminate the j^{th}

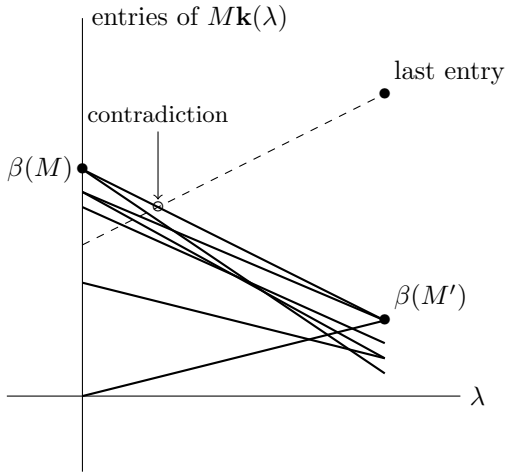

Figure 2.5: Contradiction to the minimality of $\beta(M)$

entry to get $\boldsymbol{k}'$ with $M'\boldsymbol{k}' = M\boldsymbol{k}$. Thus:

$$\beta(M') \leq \max M'\boldsymbol{k}' = \max M\boldsymbol{k} = \beta(M).$$

Together with **Proposition II.19**, we are done.

□

Discussion II.21. Let us discuss the interpretation of eliminating rows and columns while preserving $FT(M)$, as seen in **Proposition II.20**. For computational purposes we are working with a matrix M, while the underlying algebraic structure is a monomial ideal $I \subset K[x_1, ..., x_t]$. When we are eliminating the i^{th} row, we are eliminating the variable x_i, or setting $x_i = 1$ if you will. This changes the ideal and the ambient ring without changing the F-pure threshold. Geometrically, we are projecting the Newton polygon onto the hypersurface corresponding to $\mu_i = 0$, while preserving the coordinates of the puncture point.

When we are eliminating the j^{th} column, we are eliminating a generating monomial of I, and getting a different ideal with the same F-pure threshold. Geometrically, we are projecting the splitting polytope onto the hypersurface $\boldsymbol{\mu}_j = 0$, while

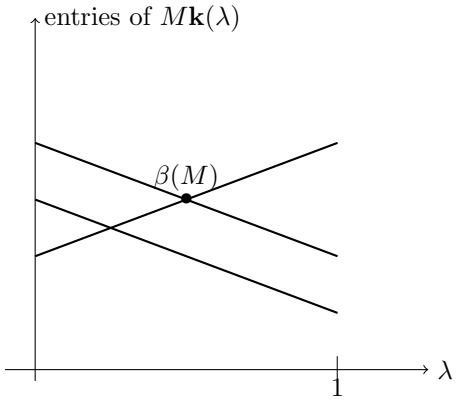

Figure 2.6: Computation of $\beta(M)$

preserving the value representing $FT(I)$, as described in **Discussion II.11**.

Example II.22. Recall **Example II.9** and observe the splitting matrix

$$M = \begin{bmatrix} 20 & 10 \\ 10 & 20 \\ 14 & 15 \end{bmatrix}.$$

Set $\mathbf{k} = [a, 1-a]^{Tr} \in \mathcal{C}(2)$ (We use Tr since technically, we need $\mathbf{k}$ to be a column vector). Then $M\mathbf{k} = [10a+10, -10a+20, -a+15]^{Tr}$. A simple sketch(**Figure 2.6**) shows that $a = 0.5$ yields the vector $[15, 15, 14.5]$ and $\beta(M) = 15$, as it is the minimal maximal entry. The third row corresponds to a sub-β entry, thus could have been disregarded, and the computation could have been executed on

$$M = \begin{bmatrix} 20 & 10 \\ 10 & 20 \end{bmatrix}.$$

Corollary II.23. Let $M \in \mathbb{Z}^{s\times t}$ be a splitting matrix, representing a monomial ideal $I \subset K[x_1, ..., x_t]$. Then there exists a sub-matrix $M' \in \mathbb{Z}^{s'\times t'}$, which is obtained by deleting rows and columns, with the following properties:

1. $FT(M) = FT(M')$ (i.e. the F-pure threshold of I is the same of the F-pure threshold of some other ideal J, which is obtained by removing generators and eliminating variables from I.)
2. For all $\boldsymbol{k} \in \mathcal{C}(s')$ with $\max M'\boldsymbol{k} = 1/FT(M)$ we have $M'\boldsymbol{k} = 1/FT(M)\mathbf{1}_{t'}$ and all the entries of $\boldsymbol{k}$ are non-zero.
3. The kernel of M', as a linear map $\mathbb{R}^{s'} \to \mathbb{R}^{t'}$, is of dimension 0.
4. M' is a invertible square matrix.
5. $$FT(M) = \mathbf{1}_{t'}^{Tr} M'^{-1} \mathbf{1}_{t'},$$
   i.e. the sum of entries of the inverse matrix.
6. $FT(M) \in \mathbb{Q}$

Proof. The first two statements are a result of **Proposition II.20** applied repeatedly, until no further elimination can be done.

The third statement follows from the previous one: If the kernel of M' has dimension 2 or more, we can find a vector in the kernel $\boldsymbol{v}$ where $|\boldsymbol{v}| = 0$. Now take $\boldsymbol{k} \in \mathcal{C}(s')$ such that $M'\boldsymbol{k} = (1/FT(M))\mathbf{1}_{t'}$, i.e. achieves $\beta(M)$. The line $\boldsymbol{\ell}(\lambda) = \boldsymbol{k} + \lambda\boldsymbol{v}$ contains vectors that satisfy $M'\ell(\lambda) = (1/FT(M))\mathbf{1}_{t'}$ and $|\boldsymbol{\ell}(\lambda)| = 1$. Moreover, the line $\ell(\lambda)$ intersects the unit simplex $\mathcal{C} = \mathcal{C}(s')$ as $\boldsymbol{k} \in \boldsymbol{\ell}(\lambda) \cap \mathcal{C}$ and $\boldsymbol{k}$ is not on the boundary of $\mathcal{C}$ as all of its entries are positive. By convexity of the unit simplex, we have a line segment in $\mathcal{C}$ achieving $\beta(M)$, thus we must have a vector on the boundary achieving $\beta(M)$, and this is a contradiction. The only other option aside from a trivial kernel,

is that the kernel is one dimensional, and spanned by a vector $\boldsymbol{w}$ with, without loss of generality, $|\boldsymbol{w}| > 0$. For a small $\epsilon > 0$ consider the following equation, which is true for all ϵ:

$$M'\boldsymbol{\ell}(\epsilon) = \mathbf{1}_t \text{ where } \boldsymbol{\ell}(\epsilon) = FT(M)\boldsymbol{k} + \epsilon\boldsymbol{w}$$

For a small enough epsilon we get that the entries of $\ell(\epsilon)$ are all positive and $|\ell(\epsilon)| > FT(M)$. This contradicts **Theorem II.10**. As the the forth statement, since M' is injective, $s' \leq t'$. So just pick a basis for the row space, and get a new matrix M'. We claim that $\beta(M') = \beta(M)$ and suffices to prove that eliminating one row that is a linear combination of the rest of the rows does not change the value of the F-pure threshold. So, without loss of generality, assume that $M \in \mathbb{Z}^{t\times s}$ is an injective matrix satisfying the first 3 statements and let M' be a matrix obtained by eliminating the last row that happens to be linearly dependent of the others:

$$\boldsymbol{\mu}^t = \alpha_1\boldsymbol{\mu}^1 + ... + \alpha_{t'-1}\boldsymbol{\mu}^{t-1}.$$

Denote $\beta = \beta(M)$ and $\beta' = \beta(M')$. Notice that since $M\boldsymbol{k} = \beta\mathbf{1}_t$, we have:

$$\alpha_1 + ... + \alpha_{t-1} = 1$$

By **Proposition II.19** one can see that $\beta' \leq \beta$. For the sake of contradiction, assume that $\beta' < \beta$ and we have some $\boldsymbol{k}'$ such that $\max M'\boldsymbol{k}' \leq \beta'$. By observing at $M\boldsymbol{k}'$ we have to conclude that the first $t-1$ entries must be β' or less while the last entry must be more than β. Notice that:

$$\beta' = \beta'\alpha_1 + ... + \beta'\alpha_{t-1} \leq (M\boldsymbol{k}')_1\alpha_1 + ...(M\boldsymbol{k}')_{t-1}\alpha_{t-1} = (M\boldsymbol{k}')_t > \beta,$$

which is a contradiction.

Lastly, $FT(M)$ is the sum of entries of $\boldsymbol{k}$ such that $M'\boldsymbol{k} = \mathbf{1}_{t'}$ so it is in fact:

$$\mathbf{1}_{t'}^{Tr}M'^{-1}\mathbf{1}_{t'}.$$

Since M has integer entries, M'^{-1} has rational entries, so $\mathbf{1}_{t'}^{Tr} M'^{-1} \mathbf{1}_{t'} \in \mathbb{Q}$ $\square$

Remark II.24. Note that for a given splitting matrix M, one can find $FT(M)$ using Linear Programming:

$$FT(M) = \max_{\boldsymbol{k}} \mathbf{1}_s \cdot \boldsymbol{k} \text{ under } M\boldsymbol{k} \preceq \mathbf{1}_t,\ 0 \preceq \boldsymbol{k}.$$

Thus there are efficient algorithms of Finding $FT(M)$. Once we have that value, we can follow the algorithm presented next (in **Discussion II.25**) to find the invertible sub-matrix as in **Corollary II.23**.

Discussion II.25 (**Monomial Ideal Reduction Algorithm**)**.** Given M, follow this algorithm to find an invertible sub-matrix as in **Discussion II.25**.

1. If there are any dominating row and/or columns, eliminate them and repeat from the top.
2. Find $FM(T)$ using Linear Programming (**Remark II.24**). The output includes a vector $\boldsymbol{k}$ such that :
$$|\boldsymbol{k}| = FT(M),\ M\boldsymbol{k} \preceq \mathbf{1}_t$$
3. Let $\boldsymbol{v} := M\boldsymbol{k}$. Mark all rows corresponding to entries of $\boldsymbol{v}$ that are strictly less than 1. They will be eliminated shortly.
4. If the entries of $\boldsymbol{k}$ are all positive and M has a kernel vector $\boldsymbol{w} \neq 0$ with $|\boldsymbol{w}| = 0$, follow the next procedure:
   (a) For any $1 \leq i \leq s$, let $\lambda_i := -k_i/w_i$ where if $w_i = 0$ let $\lambda_i = -\infty$.
   (b) Let $\lambda := \max_{1 \leq i \leq s} \lambda_i$. Since $\boldsymbol{w} \neq 0$, λ is finite. Let i' be the index such that $\lambda = \lambda_{i'}$.
   (c) Let $\boldsymbol{k}' := \boldsymbol{k} + \lambda \boldsymbol{w}$. Note that for any i:
$$k'_i = k_i + \lambda w_i \geq k_i + (\lambda_i) w_i = k_i,$$

while at least one of the entries, the i' one, is 0.

(d) Note that $M\boldsymbol{k} = M\boldsymbol{k}$ and $|\boldsymbol{k}| = |\boldsymbol{k}'|$. Redefine $\boldsymbol{k} := \boldsymbol{k}'$.

5. Mark all columns corresponding to a 0 entry in $\boldsymbol{k}$. They will be eliminated shortly.

6. Let M' be the sub-matrix obtained by eliminating all rows and columns we previously marked.

7. If $M' \neq M$, Go back to to the top and repeat the process for M'. Note that it is guaranteed that $FT(M) = FT(M')$.

8. Otherwise, M' must be injective (see **Corollary II.23**). If M is not invertible, choose a basis for the row space and eliminate all rows not in it. Then repeat the algorithm from the top. Otherwise the process is done.

Remark II.26. Note that the algorithm is not fully deterministic as one can choose $\boldsymbol{w} \in \ker M$ in many ways, for example replace $\boldsymbol{w}$ by $-\boldsymbol{w}$. Also, a basis for the row space is not unique. Indeed the invertible sub-matrix of M is not unique in general. Furthermore, the $\boldsymbol{k}$ we get from the Linear Programming algorithm is not unique in general. Please refer to **Appendix A** for a MATLAB implementation example.

Remark II.27. Let us analyze the time complexity of this algorithm, from a computer science standpoint. For simplicity, let $n = \max\{s, t\}$. The outer loop is done, in the worst case, $s + t \leq 2n$ times: once for every row and every column being eliminated. In the loop there are a sequence of sub-procedures: find dominating rows and columns, linear programing, solving linear system of equations, finding rank and finding row space. Each of them can be done in a polynomial time; finding dominating rows and columns is easily seen to be cubic, while the Gauss elimination is cubic as well (this is an easy computations, although it can be even more improved as seen

in [Str69]), which facilitates all the sub-procedures except for the linear programming. In a sense, the linear programming is the bottle neck of this algorithm. For the most general case, finding a polynomial time algorithm is one of Smale's open problems, however an $O(n^{3.5})$ algorithm is known when the problem is posed over $\mathbb{Q}$, like the "interior point methods" (see [Kar84] and [Sma98, Problem 9]). Moreover, the linear programming need to be executed only once, to find the value of $FT(M)$ and of the very first $\boldsymbol{k}$. In later iterations, the value of $FT(M)$ is proven to stay the same, while the same $\boldsymbol{k}$ can also be used between iterations, after eliminating the 0 entries. We conclude that the algorithm can runs in $O(n^4)$ time.

Example II.28. We shall demonstrate the algorithm using the ideal:

$$I = (y^2z, x^3, x^2z, xz^2).$$

Note that this is the support of the Legendre form of the defining polynomial of an elliptic curve over an algebraically closed filed with characteristic not equal to 2, as in equation (IV.2.1). The matrix is:

$$M = \begin{bmatrix} 0 & 3 & 2 & 1 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \end{bmatrix}.$$

There are no dominating rows or columns. After applying linear programming, one can see that $FT(M) = 1$ and that we can take:

$$\boldsymbol{k} = \begin{bmatrix} 1/2 \\ 1/6 \\ 1/6 \\ 1/6 \end{bmatrix}, \; M\boldsymbol{k} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}.$$

We cannot mark any row for elimination, but we can find a kernel vector:

$$\boldsymbol{w} = \begin{bmatrix} 0 \\ -1 \\ 2 \\ -1 \end{bmatrix}, |\boldsymbol{w}| = 0$$

Using $\boldsymbol{k}' = \boldsymbol{k} - \frac{1}{12}\boldsymbol{w} = [1/2, 1/4, 0, 1/4]^{Tr}$, one can mark the third column for elimination and get:

$$M' =: \begin{bmatrix} 0 & 3 & 1 \\ 2 & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix}.$$

One can check that M' is invertible and the process actually ends here.

However, if we work with $\boldsymbol{k}' = \boldsymbol{k} + \frac{1}{6}\boldsymbol{w} = [1/2, 0, 1/2, 0]$ we can eliminate the second and the fourth column and get:

$$M' = \begin{bmatrix} 0 & 2 \\ 2 & 0 \\ 1 & 1 \end{bmatrix}.$$

One can see that $M'[1/2, 1/2]^{Tr} = [1, 1]^{Tr}$ and that M' is injective. So we can choose an arbitrary basis for the row space. Once choice would be:

$$M'' = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}.$$

Another choice would let us to eliminate further by using dominating columns and rows:

$$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 \end{bmatrix}.$$

Or

$$\begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 \end{bmatrix}.$$

Translating back to ideals, we get that all of the following monomial ideals, in their respective rings or in the original ring, have a the same F-pure threshold of 1 we (add arrows to illustrate how the algorithm produced the different ideals from the original one):

$$\begin{array}{ccc} (y^2z, x^3, x^2z, xz^2) & \longrightarrow & (y^2z, x^3, xz^2) \\ \downarrow & & \\ (y^2z, x^3, xz^2) & \longrightarrow & (y^2, x^2) \\ \downarrow & & \\ (z) & & \end{array}$$

Example II.29. When invoking the **Monomial Ideal Reduction Algorithm**, it is important to follow all steps. We emphasize that the algorithm terminates only when we are executing an iteration that incurs no further reductions. For example, if one is given an invertible matrix M it is not true that the sum of the entries of the inverse matrix is $FT(M)$, as more reductions may be done. Here is a concrete example:

$$M = \begin{bmatrix} 5 & 1 & 2 \\ 1 & 4 & 3 \\ 2 & 3 & 0 \end{bmatrix}.$$

When we executes the algorithm, we get that $FT(M) = 5/13$ and the matrix is reduced to:

$$M' = \begin{bmatrix} 5 & 2 \\ 1 & 3 \end{bmatrix},$$

while the sum of entries of M^{-1} is $18/49$.

Remark II.30. Given a monomial ideal, I, it gives rise to a splitting matrix M. We apply the algorithm above to obtain one or more invertible sub-matrices with the same F-pure threshold, each represents a monomial ideal J in a possibly different ring, with the same F-pure threshold. We can even put J back in the original ring by re-inserting the eliminated variables. Then these J's may or may not contain I as they are obtained by eliminating certain generators, but also by eliminating certain variables from other generators.

Question II.31. Is there a relations between these J ideals and the minimal primes of I or the primary decomposition of I?

Going back to **Example II.28**, we start with:

$$I = (y^2z, x^3, x^2z, xz^2),$$

apply the algorithm and get:

$$(y^2z, x^3, xz^2), (y^2, x^2), (z)$$

One can compute that $I \subset K[x, y, z]$ has two minimal primes and one embedded prime,

$$P_1 = (x, y), P_2 = (x, z), P_3 = (x, y, z),$$

respectively. Also, one can compute a primary decomposition of I. The primary ideals that must appear in the decomposition are:

$$J_1 = (x, y^2), J_2 = (x^3, z), \text{ where } Rad(J_i) = P_i$$

For the embedded prime we can take, for example, $J_3 = (x^2, y^2, z^2)$, so:

$$I = (x, y^2) \cap (x^3, z) \cap (x^2, y^2, z^2)$$

Example II.32. Fix integers $b, c \geq 1$. Take the ideal:

$$I = (x^{2c+b}y^b, x^{2c+b-1}, y^{b+11}, ..., x^{b+1}y^{2c+b-1}, x^b y^{2c+b}) \subset K[x, y]$$

The splitting matrix is

$$M = \begin{bmatrix} 2c+b & 2c+b-1 & \dots & b+1 & b \\ b & b+1 & \dots & 2c+b-1 & 2c+b \end{bmatrix}.$$

Using Newton Polygon method (see **Theorem II.6**), we get a that the boundary of the polygon is determined by a single line segment containing integer points (α, β) such that $0 \leq \alpha \leq 2c+b$ and $\alpha + \beta = 2c + 2b$. The "puncture point" is $(b+c, b+c)$, so $FT(M) = 1/(b+c)$. Notice that taking $\boldsymbol{k} = [1/2, 0, ..., 0, 1/2]^{Tr}$ gives $M\boldsymbol{k} = [(b+c), (b+c)]^{Tr}]$, allowing us to eliminate almost all the columns of the matrix and get:

$$M' = \begin{bmatrix} 2c+b & b \\ b & 2c+b \end{bmatrix},$$

which is invertible and has the same F-pure threshold.

Question II.33. If we begin with an $\mathfrak{m}$-primary monomial ideal I, can we improve the algorithm?

Say I is generated by $x_1^{a_1}, x_2^{a_2}, ..., x_t^{a^t}$, call them singletons, and some extra monomials not of the form $x_i^{a_i}$, call them mixed. We can find examples where the $FT(I)$ is set only by singletons, only by the mixed, or a combination of them:

For

$$I = (x^3, y^3, xy),\ M = \begin{bmatrix} 3 & 0 & 1 \\ 0 & 3 & 1 \end{bmatrix},$$

an invocation of the algorithm shows that $FT(M) = 1$ and since $M[001]^{tr} = 1$, we can eliminate the first two columns and just use the last mixed monomial. That is,

we can reduce the ideal to (xy). Further use the algorithm to reduce to (x) or (y), i.e. generated by the mixed monomial.

For

$$I = (x^3, y^2, z^3, x^2z^2),\ M = \begin{bmatrix} 3 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 2 \end{bmatrix},$$

we compute $FT(M) = 7/6$ and the reduced ideal is (x^3, y^2, z^3), i.e. generated only by the singletons.

Finally, for

$$I = (x^6, y^2, z^6, x^2z^2),\ M = \begin{bmatrix} 6 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 2 \end{bmatrix},$$

we compute $FT(M) = 1$ and the reduced ideal is (y^2, x^2z^2), (which then turns to (y^2, x^2)), i.e. we have to use a combination of singletons and mixed monomials.

2.2.1 Improvements Using The Integral Closure

Discussion II.34. Recall the algorithm from **Discussion II.25**. Suppose we are interested in computing $FT(I)$ for a monomial ideal I, with a corresponding splitting matrix M. Now, let f be an element in the ring that is not in I, but the F-pure threshold of the ideal $J = I + (f)$ is the same as $FT(I)$. What are the implications of computing $FT(I)$ by actually invoking the algorithm on $J = I + (f)$? One can see that we might get more options for $\boldsymbol{k}$ in step 2 of the **Monomial Ideal Reduction Algorithm**. Ergo, we enlarge the matrix and take a computational performance hit with the prospect of maybe ending up with a smaller matrix and a simpler ideal when the algorithm terminates. A systematic way to do this enhancement is by adding elements of the *integral closure* of I, an approach we explore in this subsection.

We are working with the following standard definition (see [HS06, Definition 1.1.1]):

Definition II.35 (**Integral Closure**)**.** Let I be an ideal in a ring R. An element $r \in R$ is said to be integral over I if there exist an integer n and elements $a_i \in I^i$, $i = 1, ..., n$, such that:

$$r^n + a_1 r^{n-1} + ... + a_{n-1} r + a_n = 0$$

The *integral closure* of I in R, denoted $\overline{I}$, consisting of all $r \in R$ that are integral over I.

It is well known that $\overline{I}$ is an ideal itself, and when I is a monomial ideal, $\overline{I}$ is a monomial ideal as well. One can refer to the first chapter of [HS06] for more details. The following shows the the Newton polygon of I and $\overline{I}$ is the same:

Theorem II.36. *Let I be a monomial ideal in $K[x_1, ..., x_t]$, where K is a field. Let $\boldsymbol{\mu} = (\mu_1, ..., \mu_t) \in \mathbb{Z}^t_{\geq 0}$ be a point in $\mathbb{R}^t$. Then $\boldsymbol{\mu}$ is in the Newton polygon of I if and only if $\boldsymbol{x}^{\boldsymbol{\mu}} \in \overline{I}$*

Proof. See [HS06, Proposition 1.4.6][Eis08, Exercise 4.23]. □

We deduce the well known fact about the F-pure threshold, which is actually true for any ideal:

Corollary II.37. Let I be a monomial ideal in $K[x_1, ..., x_t]$, where K is a field. Then the F-pure threshold of I and of the integral closure of I is the same.

Proof. Since the F-pure threshold can be described as an invariant of the Newton polygon of I, the statement is immediate from **Theorem II.36**. □

Using these results, we have a systematic way to execute the enhancement described in **Discussion II.34**: create a new ideal by adding monomials in the Newton

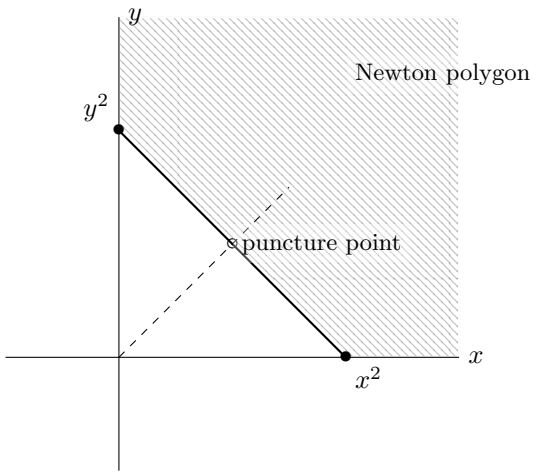

Figure 2.7: Newton polygon of (x^2, y^2)

polygon that are close to, in the Euclidean sense, the "puncture point" described in **Theorem II.6**. In the lack of such information, one can just invoke the algorithm on $\overline{I}$ altogether.

Example II.38. Consider $I = (x^2, y^2) \subset K[x, y]$. One can draw the Newton polygon and observe that $FT(I) = 1$ as the puncture point is $(1, 1)$ (see **Figure 2.7**). An execution of the **Monomial Ideal Reduction Algorithm** terminates immediately as we cannot eliminate a generator or a variable. However, if we use the theorems above, we conclude that xy is in the integral closure of I, since (1,1) is part of the Newton polygon. Indeed, $r = xy$ satisfies $r^2 - x^2y^2 = 0$. So let us invoke the algorithm on (x^2, xy, y^2) with a splitting matrix of:

$$M = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \end{bmatrix}.$$

Since $FT(I) = 1$, we can choose to work with $\boldsymbol{k} = [0, 1, 0]^{Tr}$, and eliminate the left and the right columns. Then we can eliminate one dominated row and end up with $M' = [1]$ which corresponds to either (x) or (y).

Corollary II.39. Let $I \subset K[x_1, ..., x_t]$ be a monomial ideal, where K is a field.

Suppose that $FT(I) = \frac{1}{a}$ for some integer $a > 0$. Then $\overline{I}$ contains the element $x_1^a \cdots x_t^a$ and the **Monomial Ideal Reduction Algorithm** invoked on $\overline{I}$ or on $I + (x_1^a \cdots x_t^a)$ can output a principle ideal (x_1^a).

Proof. If $FT(I) = \frac{1}{a}$, the "puncture point" is $(a, a, ..., a)$. Ergo, by **Theorem II.36**, $x_1^a \cdots x_t^a \in \overline{I}$. When invoking the algorithm in either $\overline{I}$ or $I + (x_1^a \cdots x_t^a)$, the splitting matrix consist of a column of $[a, a, ..., a]^{Tr}$. Thus, step 2 of the algorithm can produce $\boldsymbol{k}$ with all zero entries, except an entry of $1/a$ corresponding to said column. So we eliminate all other columns, and the next step is to eliminate all dominated rows. Finally we end up with a splitting matrix of $M' = [a]$ as required. □

Discussion II.40. Suppose that we have all the monomials generating an integrally closed ideal I in $K[x_1, ..., x_t]$. Observe at the Newton polygon in $\mathbb{R}^t$. The puncture point is on a facet of the boundary of that polygon, which is defined by t' monomials, where $1 \leq t' \leq t$. It is easy to see that the monomials defining this facet have to be linearly independent. Ergo, we can eliminate all other monomials and immediately be left with an injective splitting matrix. We now complete the algorithm by taking a basis for the row space. We conclude that enough information on the integral closure of the ideal can make the algorithm terminate almost immediately.

Discussion II.41. The takeaway of this subsection is that the **Monomial Ideal Reduction Algorithm**(**Discussion II.25**) works best, in terms of obtaining a simpler output, when invoked on integrally closed ideals. However, note that these ideals have more generators in general, so the time complexity of the algorithm is hurt. For example, if we have s generators for I, the algorithm runs in $O(s^4)$ (see **Remark II.27**); adding s' number of generators results in running time of $O((s + s')^4) = O(s^4) + O(s'^4)$. So we pay $O(s'^4)$ of time in order to get a possibly

simpler ideal when the algorithm terminates.

We can give a more accurate bound of the time complexity if we are given a concrete algorithm and if we notice that s becomes $s + s'$ but t stays the same. One can look at the algorithm in **Appendix A** and see that finding dominating columns is an $O(ts^2)$ task, and the outer loop is done $s+t$ times. Ergo, the $O(n^4)$ bound, with $n = \max(s, t)$, can be written as $O(ts^3)$. This makes the additional time complexity be $O(ts'^3)$ instead of $O(s'^4)$ when introducing s' more generators.

CHAPTER III

F-Pure Threshold of Polynomials and Deuring Polynomials

We dedicate this chapter to develop useful machinery for the computation of the F-pure threshold of polynomials. We start by observing the direct computation consisting of raising polynomials to integer powers and then we deduce on how to compute bounds by looking at the coefficients of "critical" monomials (**Lemma III.2**). In the cases presented in later chapters, one critical coefficient that keeps showing up is a polynomial expression which we call the *Deuring Polynomial* (see later **Lemma IV.5**). These polynomials are closely related to the Legendre Polynomials, which have been investigated for almost 250 years. For the F-pure threshold computation, is beneficial to analyze the Deuring polynomials, and specifically their roots mod p. This is the goal of this chapter.

3.1 F-pure Threshold of Polynomials

Definition II.1 is used to define the F-pure threshold of the ideal generated by a polynomial f, or just the F-pure threshold of the polynomial f. In this case, the characteristic of the underlying field is important. Recall our definition for the F-pure threshold of a polynomial (I.1.2):

Definition III.1. Let K denote a field of prime characteristic p and let $R = K[x_1, ..., x_t]$. Fix any polynomial $f \in R$. The F-pure threshold of f (at the ori-

gin) is:

$$FT(f) := \sup\left\{ \frac{N}{p^e} \;\middle|\; N, e \in \mathbb{Z}_{>0}, f^N \notin (x_1^{p^e}, ..., x_t^{p^e})R \right\}. \tag{III.1.1}$$

Let us present two useful observations for computing $FT(f)$. Let K be a field. A polynomial $f \in K[x_1, ..., x_t]$ is a linear combination of monomials over K and recall our multiexponent notaion; denote the monomial $x_1^{\mu_1} \cdots x_t^{\mu_t}$ by $\mathbf{x}^{\boldsymbol{\mu}}$ where $\boldsymbol{\mu}$ is the multiexponent $[\mu_1, ..., \mu_t]$. Similarly, for s scalars in K, $b_1, ..., b_s$, we denote $\mathbf{b} = [b_1, ..., b_s]$. Now, let $\mathbf{x}^{\boldsymbol{\mu}_1}, ..., \mathbf{x}^{\boldsymbol{\mu}_s}$ be the monomials of f. Using the usual meaning of dot product we have:

$$f = \mathbf{b} \cdot [\mathbf{x}^{\boldsymbol{\mu}_1}, ..., \mathbf{x}^{\boldsymbol{\mu}_s}] = b_1\mathbf{x}^{\boldsymbol{\mu}_1} + ... + b_s\mathbf{x}^{\boldsymbol{\mu}_s}.$$

For a multiexponent $\mathbf{k} = [k_1, ..., k_t]$ we denote $\max \mathbf{k}$ as the maximal power in the multiexponent $\mathbf{k}$, i.e.

$$\max \mathbf{k} = \max[k_1, ..., k_t] = \max_{1 \le i \le t} k_i.$$

Using this notation, we have the following straightforward way to produce upper and lower bounds for $FT(f)$:

Lemma III.2. Let $R = K[x_1, ..., x_t]$ where K is a field of prime characteristics p, and let $f \in R$. Let N be a positive integer. Raise f to the power of N and collect all monomials, so that:

$$f^N = \sum_{\text{distinct multi-exponents } \mathbf{k}} c_{\mathbf{k}}\mathbf{x}^{\mathbf{k}}. \tag{III.2.1}$$

Note that all but finitely many $c_{\mathbf{k}}$'s are 0. Fix $e \in \mathbb{Z}_{\ge 0}$ and consider $\frac{N}{p^e}$. Then:

1. $\frac{N}{p^e} < FT(f) \iff \exists \mathbf{k}$ such that $c_{\mathbf{k}} \neq 0$ and $\max \mathbf{k} < p^e$.
2. $FT(f) \le \frac{N}{p^e} \iff \forall \mathbf{k}$, either $c_{\mathbf{k}} = 0$ or $\max \mathbf{k} \ge p^e$.

Proof. This is immediate from the definition (III.1.1) and from [BFS13, Prop 3.26] which implies that for any $\frac{N}{p^e} \in [0,1]$,

$$f^N \notin (x_1^{p^e}, ..., x_t^{p^e})R \iff \frac{N}{p^e} < FT(f).$$

□

Lemma III.3. Let f be a homogeneous polynomial of degree d in t variables. Let $\mathbf{x^k}$ be a monomial in f^N with a non-zero coefficient. Denote $\mathbf{k} = [k_1, ..., k_t]$. Then $k_1 + ... + k_t = dN$. Moreover, $\max \mathbf{k} \geq Nd/t$ and if $\max \mathbf{k} = Nd/t$ then $\mathbf{k} = [Nd/t, Nd/t, ..., Nd/t]$.

Proof. The first statement is immediate since any monomial of f^N is of degree dN. Ergo, we cannot have that all t entries of $\mathbf{k}$ are less than Nd/t. Lastly, if $\max \mathbf{k} = Nd/t$ but another power is less, then $k_1 + ... + k_t$ is less than Nd. □

Discussion III.4. Let us present a few well known facts about $FT(f)$. Unlike the monomial ideal case, for different p's, we might get different $FT(f)$'s, as the coefficients in (III.2.1) can be zero in one characteristic and non-zero in another. For example, $FT(x^2 + y^3)$ is $5/6$ if $p \equiv 1 \pmod 6$ and $5/6(1 - 1/5p)$ if $p \equiv 5 \pmod 6$ (see [BFS13, Example 3.11]).

If we enlarge the underlying field, that is performing base change, nothing in the above computation changes and the value $FT(f)$ is preserved. A common practice is to move to the algebraic closure of the field. It is also an easy exercise to see that $FT(f)$ is preserved under a linear change of variables.

Every polynomial f is supported by a set of monmials, which generates a monomial ideal denoted $\text{Supp}(f)$. It is natural to explore the connection between $FT(f)$ and $FT(\text{Supp}(f))$. Since $f \in \text{Supp}(f)$, it is immediate from **Definition II.1** and

from the bounds in **Discussion II.3** that:

$$FT(f) \leq \min\{1, FT(\mathrm{Supp}(f))\}$$

3.2 Definition of Deuring Polynomials

Definition III.5. Let $n \in \mathbb{Z}_{\geq 0}$. Define the following polynomial in $\mathbb{Z}[\lambda]$:

$$H\{n\}(\lambda) := \sum_{i=0}^{n} \binom{n}{i}^2 \lambda^i$$

Following [Mor06], we call it the *Deuring Polynomial*[1] of degree n. When the indeterminant λ is understood from the context we omit it and write $H\{n\}$. We often abuse notation and write $H\{n\} \in \mathbb{F}_p[\lambda]$ for the natural image mod p.

Remark III.6. The Deuring polynomials $H\{n\}$ are closely related to the Legendre polynomials arising as solutions to the Legendre differential equation. Legendre polynomials are of importance to many physical problems, including finding the gravitational potential of a point mass, as in Legendre's original work [Leg85]. Indeed, if $P_n(x)$ denotes the n^{th} Legendre polynomial then:

$$H\{n\}(\lambda) = (1-\lambda)^n P_n\left(\frac{1+\lambda}{1-\lambda}\right),$$

as follows by a simple substitution and a known "textbook" formula for the Legendre polynomials ([Koe14, Exercise 2.12]); this is pointed out in [BM04] and [CH14]. In the next sections, we establish several properties of Deuring polynomials, which can also be deduced from analogous facts about Legendre polynomials. We include direct algebraic proofs not relying on typical analytic techniques such as orthogonality in function spaces. In this way, we keep this chapter self-contained and, we hope, more straightforward than relying on the vast literature on Legendre polynomials. In **section 3.5** we show how the main results on Deuring polynomials can be deduced from known theorems on Legendre Polynomials.

[1] Arguably it first appeared in [Deu41]

3.3 Basic Properties

We first recall some well known techniques for working in characteristics p. Fix a prime p. Every integer N can be written *uniquely* in its base p-expansion (or simply its p-expansion) as follows: fix a power e such that $N < p^{e+1}$. Then there exist unique integers $0 \leq a_0, ..., a_e \leq p-1$ such that

$$N = a_0 p^0 + a_1 p^1 + ... + a_e p^e$$

We can also say that $N = \sum_{e=0}^{\infty} a_e p^e$ while all but finitely many a_e's are zero.

We recall how to compute binomial and multinomial coefficients mod p.

Theorem III.7 (**Lucas's Theorem**). *[See [Luc78] and [Dic02]] Let $\boldsymbol{k} = (k_1, ..., k_n) \in \mathbb{N}^n$ and set $N = k_1 + ... + k_n$. Fix a prime p. Let e be an integer such that $N < p^{e+1}$. Write each of the k_i's in their base p-expansion:*

$$k_i = a_{i0} p^0 + a_{i1} p^1 + ... + a_{ie} p^e$$

(some a_{ij}'s may be 0). Also write N in its base p-expansion:

$$N = b_0 p^0 + b_1 p^1 + ... + b_e p^e$$

Then the multinomial coefficient $\binom{N}{\boldsymbol{k}}$ satisfy:

$$\binom{N}{\boldsymbol{k}} = \frac{N!}{k_1! \cdots k_n!} \equiv \binom{b_0}{a_{10}\, a_{20}\, ...\, a_{n0}} \binom{b_1}{a_{11}\, a_{21}\, ...\, a_{n1}} \cdots \binom{b_e}{a_{1e}\, a_{2e}\, ...\, a_{ne}} \pmod{p},$$

with the convention that if $a_{1j} + ... + a_{nj} > b_j$ then $\binom{b_j}{a_{1j}\, a_{2j}\, ...\, a_{nj}} = 0$. Specifically, $\binom{N}{\boldsymbol{k}} \not\equiv 0 \pmod{p}$ if and only if the digits of the p-expansion of the k_i's are not carrying when added.

Due to **Lucas's Theorem**, a multinomial coefficient is 0 if and only if for some j, the j^{th} digit of N is not the sum of the of the j^{th} digits of the k_i's.

Lemma III.8. Let p be a prime. Then $H\{p-1\} \in \mathbb{F}_p[\lambda]$ is $(\lambda-1)^{p-1}$.

Proof. The coefficients of $H\{p-1\}(\lambda)$ are the squares of the numbers appearing on the $(p-1)^{\text{th}}$ row in Pascal's Triangle mod p. Due to **Lucas's Theorem**, the p^{th} row starts and ends with 1, while the rest of the entries are zero. Ergo, the $(p-1)^{\text{th}}$ row consists of ± 1's due to the identity:

$$\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}. \tag{III.8.1}$$

For illustration, here are the $(p-1)^{\text{th}}$ and the p^{th} rows of Pascal's Triangle:

$p-1:$	1	-1	1	-1	...	-1	1	-1	1	
$p:$	1	0	0	0	...	...	0	0	0	1

So using the geometric series formula we get:

$$H\{p-1\} = 1 + \lambda + ... + \lambda^{p-1} = \frac{\lambda^p - 1}{\lambda - 1} = (\lambda-1)^{p-1}$$

□

Lemma III.9 (**Schur's Congruence**). [2] Fix a prime p. Let $H\{n\} \in \mathbb{F}_p[\lambda]$. Write the p-expansion of n:

$$n = b_0 p^0 + b_1 p^1 + ... + b_e p^e.$$

Then

$$H\{n\} = H\{b_0\}^1 H\{b_1\}^{p^1} H\{b_2\}^{p^2} \cdots H\{b_e\}^{p^e}$$

Proof. Denote $f = H\{n\}$ and $g = H\{b_0\}^1 H\{b_1\}^{p^1} \cdots H\{b_e\}^{p^e}$. First notice that f and g are of the same degree as $\deg f = n$ and $\deg g = b_0 + b_1 p + b_2 p^2 + ... + b_e p^e = n$. Fix λ^i and let us compare its coefficient in both f and g. For $i = 0$, the coefficient

[2] This lemma was formulated by Schur in the context of Legendre polynomials. However, the first published proof is due to Wahab([Wah52]) half a decade later.

of λ^0 is 1 in any Deuring polynomial, and so in f and in g. Now fix $0 < i \leq n$. In f, the coefficient is

$$\binom{n}{i}^2.$$

To compute the coefficient in g, write i in its base p-expansion:

$$i = a_0 p^0 + a_1 p^1 + ... + a_e p^e,$$

so

$$\lambda^i = \lambda^{a_0 p^0} \lambda^{a_1 p^1} \cdots \lambda^{a_e p^e}.$$

Note that the largest power e, as appears in the expansion of n, is sufficient as $i \leq n$. Notice that the powers of λ in $H\{b_j\}^{p^j}$ can only be $\{0p^j, 1p^j, 2p^j, ..., b_j p^j\}$. So if $j_1 \neq j_2$ then the set of powers in $H\{b_{j_1}\}^{p^{j_1}}$ and in $H\{b_{j_2}\}^{p^{j_2}}$ are disjoint except for 0. Moreover, picking one monomial in each of factors of g and multiplying them together yields a unique monomial of g and due to uniqueness of the p-expansion of i, there is only one possible combination of terms in the different $H\{b_j\}(\lambda)^{p^j}$'s that can yield the monomial

$$\lambda^i = \lambda^{a_0 p^0} \lambda^{a_1 p^1} \cdots \lambda^{a_e p^e}.$$

Namely, we need to follow its p-expansion and choose λ^{a_0} from $H\{b_0\}(\lambda)^{p^0}$, $\lambda^{a_1 p}$ from $H\{b_1\}(\lambda)^{p^1}$ and so on.

$$\begin{array}{rccccc} g = & H\{b_0\}^1 & H\{b_1\}^{p^1} & H\{b_2\}^{p^2} & \cdots & H\{b_e\}^{p^e} \\ \lambda^i = & \lambda^{a_0 p^0} & \lambda^{a_1 p^1} & \lambda^{a_2 p^2} & \cdots & \lambda^{a_e p^e} \end{array}$$

Ergo, if $a_j \leq b_j$ for all $1 \leq j \leq e$, then λ^i appears in g with a coefficient of:

$$\binom{b_0}{a_0}^2 \binom{b_1}{a_1}^{2p} \cdots \binom{b_e}{a_e}^{2p^e}.$$

By Fermat's little theorem, the expression is:

$$\binom{b_0}{a_0}^2 \binom{b_1}{a_1}^2 \cdots \binom{b_e}{a_e}^2,$$

which is precisely the coefficient of λ^i in f due to **Lucas's Theorem**. Otherwise, if for some j, $a_j > b_j$, then λ^i is not in g, and its coefficient in f is 0 as well since i and $n-i$ are carrying in the j^{th} digit when added and thus $\binom{n}{i} = 0$. □

Corollary III.10. In characteristic p:

$$H\left\{\frac{p^e-1}{2}\right\} = H\left\{\frac{p-1}{2}\right\}^{1+p+\ldots+p^{e-1}}$$

Proof. We apply **Lemma III.9** after writing $\frac{p^e-1}{2}$ in its p-expansion and using geometric series formula:

$$\frac{p^e-1}{2} = \frac{p-1}{2}(1+p+\ldots+p^{e-1}) = \frac{p-1}{2} + \frac{p-1}{2}p + \ldots + \frac{p-1}{2}p^{e-1}$$

□

It is useful to denote

$$n_e = (p^e-1)/2,$$

and then

$$n_1 = (p-1)/2.$$

So, we can rewrite **Corollary III.10** as

$$H\{n_e\} = (H\{n_1\})^{1+p+\ldots+p^{e-1}}$$

Note that $H\{n_1\}$ is the polynomial appearing later in **Proposition IV.3**, **Theorem IV.4** and **Theorem V.1**, so it has an important role in our computations. In the proofs of these theorems we will encounter another polynomial: $H\{n_1-1\}$. We shall now investigate it, and for that we need the following definition:

Definition III.11. Fix an integer $n \geq 0$. We define

$$F\{n\}(\lambda) \in \mathbb{Q}[\lambda]$$

to be the formal antiderivative of the polynomial $H\{n-1\}(\lambda)$ with constant coefficient 0.

Lemma III.12. Fix an integer $n \geq 0$. Let $F = F\{n-1\}(\lambda) \in \mathbb{Q}[\lambda]$, which is the formal antiderivative of the polynomial $H\{n-1\}(\lambda)$ with constant coefficient 0. We denote $H\{n-1\} = F'$. Then

$$(1-\lambda)F' + 2nF = H\{n\}.$$

Note that this equality holds characteristic 0 and thus in all positive characteristics p such that $n < p$.

Proof. Let us give a specific formula for $F(\lambda)$:

$$F(\lambda) = \sum_{i=0}^{n-1} \binom{n-1}{i}^2 (i+1)^{-1}\lambda^{i+1} = \sum_{i=1}^{n} \binom{n-1}{i-1}^2 (i)^{-1}\lambda^i.$$

Now, observe:

$$(1-\lambda)H\{n-1\}+2nF = \sum_{i=0}^{n-1} \binom{n-1}{i}^2 \lambda^i - \sum_{i=0}^{n-1} \binom{n-1}{i}^2 \lambda^{i+1} + 2n \sum_{i=1}^{n} \binom{n-1}{i-1}^2 (i)^{-1}\lambda^i.$$

Shift the index of the middle sum to get:

$$= \sum_{i=0}^{n-1} \binom{n-1}{i}^2 \lambda^i - \sum_{i=1}^{n} \binom{n-1}{i-1}^2 \lambda^i + \sum_{i=1}^{n} 2\binom{n-1}{i-1}^2 \frac{n}{i}\lambda^i. \tag{III.12.1}$$

For $i = 0$, we get that only the leftmost sum contributes a constant coefficient, which is 1 as required. Now consider the case where $1 \leq i \leq n$. We need the following identity to simplify the rightmost sum:

$$\begin{aligned} 2\tbinom{n-1}{i-1}^2 \tfrac{n}{i} &= 2\tbinom{n-1}{i-1}^2 \tfrac{n-i+i}{i} = 2\tbinom{n-1}{i-1}^2 \left(\tfrac{n-i}{i} + 1\right) = \\ &= 2\tbinom{n-1}{i-1}\tbinom{n-1}{i} + 2\tbinom{n-1}{i-1}^2. \end{aligned}$$

So when i is fixed, the coefficient of λ^i in (III.12.1) is

$$\binom{n-1}{i}^2 - \binom{n-1}{i-1}^2 + 2\binom{n-1}{i-1}\binom{n-1}{i} + 2\binom{n-1}{i-1}^2$$

Combining like terms simplifies as:

$$\binom{n-1}{i-1}^2 + 2\binom{n-1}{i-1}\binom{n-1}{i} + \binom{n-1}{i}^2,$$

which further simplifies as:

$$= \left(\binom{n-1}{i-1} + \binom{n-1}{i}\right)^2 = \binom{n}{i}^2$$

using the known identity (III.8.1). So we conclude:

$$(1-\lambda)H\{n-1\} + 2nF = H\{n\}.$$

□

We next develop differential equations for $H\{n\}$ and $F\{n\}$ that will help us to investigate their roots.

Lemma III.13. Let $n \geq 0$ be an integer and denote $H = H\{n\} \in \mathbb{Z}[\lambda]$. Then H satisfied the following differential equation:

(III.13.1) $$\lambda(\lambda-1)H'' + (\lambda(1-2n)-1)H' + n^2H = 0.$$

Proof. We demonstrate how to constructively find differential operators for $H\{n\}$ with a general n, working over $\mathbb{Z}$. This method is easily generalized for polynomials with similar form, as seen later in **Lemma III.18**.

Fix $n \in \mathbb{Z}_{>0}$ and denote $H = H\{n\}(\lambda)$. Let us write down the coefficients of λ^i in the polynomials $H, H', \lambda H', H'', \lambda H''$ and $\lambda^2 H''$:

$$\begin{aligned}
&\text{coefficient in } H: && \binom{n}{i}^2 \\
&\text{coefficient in } H': && (i+1)\binom{n}{i+1}^2 \\
&\text{coefficient in } \lambda H': && (i)\binom{n}{i}^2 \\
&\text{coefficient in } H'': && (i+1)(i+2)\binom{n}{i+2}^2 \\
&\text{coefficient in } \lambda H'': && (i)(i+1)\binom{n}{i+1}^2 \\
&\text{coefficient in } \lambda^2 H'': && (i-1)(i)\binom{n}{i}^2
\end{aligned}$$

We can multiply and divide the coefficients by the same non-zero factor without affecting the relations between them. So divide by $\binom{n}{i}^2$ to get:

$$\begin{aligned}
&\text{coefficient in } H: && 1 \\
&\text{coefficient in } H': && (i+1)\left(\frac{n-i}{i+1}\right)^2 \\
&\text{coefficient in } \lambda H': && i \\
&\text{coefficient in } H'': && (i+1)(i+2)\left(\frac{n-i}{i+1}\right)^2\left(\frac{n-i-1}{i+2}\right)^2 \\
&\text{coefficient in } \lambda H'': && (i)(i+1)\left(\frac{n-i}{i+1}\right)^2 \\
&\text{coefficient in } \lambda^2 H'': && (i-1)(i)
\end{aligned}$$

Now, multiply by $(i+1)(i+2)$ to clear denominators:

$$\begin{aligned}
&\text{coefficient in } H: && (i+1)(i+2)\\
&\text{coefficient in } H': && (i+2)\,(n-i)^2\\
&\text{coefficient in } \lambda H': && i(i+1)(i+2)\\
&\text{coefficient in } H'': && (n-i)^2\,(n-i-1)^2\\
&\text{coefficient in } \lambda H'': && (i)(i+2)\,(n-i)^2\\
&\text{coefficient in } \lambda^2 H'': && (i-1)(i)(i+1)(i+2)
\end{aligned}$$

Expand terms and write them as polynomials in i:

$$\begin{aligned}
&\text{coefficient in } H: && 2+3i+i^2\\
&\text{coefficient in } H': && 2n^2+(n^2-4n)i+(2-2n)i^2+i^3\\
&\text{coefficient in } \lambda H': && 2i+3i^2+i^3\\
&\text{coefficient in } H'': && n^2(n-1)^2-2n(2n^2-3n+1)i+(6n^2+6n+1)i^2+i^4\\
&\text{coefficient in } \lambda H'': && (2n^2)i+n(n-4)i^2+2(1-n)i^3+i^4\\
&\text{coefficient in } \lambda^2 H'': && -2i-i^2-2i^3+i^4
\end{aligned}$$

Since we would like to find a relation between these expression for any i, we write the coefficients of i in each expression as columns of a matrix and then investigate its kernel over $\mathbb{Z}$:

$$\begin{bmatrix}
2 & 2n^2 & 0 & n^2(n-1)^2 & 0 & 0\\
3 & n(n-4) & 2 & -2n(2n^2-3n+1) & 2n^2 & -2\\
1 & 2(1-n) & 3 & 6n^2-6n+1 & n(n-4) & -1\\
0 & 1 & 1 & 2-4n & 2(1-n) & 2\\
0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix}.$$

We started with 6 expressions that resulted, after manipulations, in 6 polynomials in i of degree 4 or less, i.e. defined by 5 coefficients. Consequently, the above matrix has 5 rows and 6 columns, which guarantees a non-trivial kernel. In our case, a direct computation shows that the kernel is spanned by:

$$M = \begin{bmatrix} n^2 \\ -1 \\ 1-2n \\ 0 \\ -1 \\ 1 \end{bmatrix},$$

as the matrix is of rank 5. We conclude that $H = H\{n\}$ satisfy the following differential equation over $\mathbb{Z}$:

$$\lambda(\lambda-1)H'' + (\lambda(1-2n)-1)H' + n^2 H = 0 \tag{III.13.2}$$

Note that this proof is constructive. One can also verify directly the last equation without motivating the origin of that equation. □

Remark III.14. For example, set $n = \frac{p-1}{2}$ for an odd prime p, and multiply by 4 in order to clear denominators. We get:

$$4\lambda(\lambda-1)H'' + 4(\lambda(2-p)-1)H' + (p-1)^2 H = 0$$

Over $\mathbb{F}_p$, this equations becomes:

$$4\lambda(\lambda-1)H'' + 4(2\lambda-1)H' + H = 0,$$

which is identical to the *Picard-Fuchs* operator (see [Sil09, Remark 4.2]). In many cases n is a polynomial in p with rational coefficients, say $n = g(p)$. So when working

in $\mathbb{F}_p$, one can replace n by $g(p)$, clear denominators and get a differential operator over $\mathbb{F}_p$ which does not depend on n.

Lemma III.15. Let K be a field of prime characteristic p. let $F \in K[\lambda]$ be any polynomial of degree $d < p$ (not necessarily Deuring polynomial or its formal antiderivative) and denote F', F'' as its first and second derivative, respectively. Suppose that F satisfies a differential equation of the form

$$\lambda(\lambda-1)F'' + a\lambda F' + bF' + cF = 0,\ a, b, c \in K. \tag{III.15.1}$$

Then the only possible repeating roots of F are $\lambda = 0$ and $\lambda = 1$.

Proof. Suppose α is a root of F of multiplicity $r \geq 2$. Since $\deg F = d < p$, then $r < p$. So write

$$\begin{aligned} F &= g_1(\lambda)\cdot(\lambda-\alpha)^r \quad \text{where} \quad g_1(\alpha) \neq 0, \\ F' &= g_2(\lambda)\cdot(\lambda-\alpha)^{r-1} \quad \text{where} \quad g_2(\alpha) \neq 0, \\ F'' &= g_3(\lambda)\cdot(\lambda-\alpha)^{r-2} \quad \text{where} \quad g_3(\alpha) \neq 0. \end{aligned}$$

Plug the above expression in (III.15.1) and divide by $(\lambda-\alpha)^{r-2}$ to get

$$\lambda(\lambda-1)g_3 + (a\lambda+b)(\lambda-\alpha)g_2 + c(\lambda-\alpha)g_1 = 0.$$

Plugging in $\lambda = \alpha$ gives:

$$\alpha(\alpha-1)g_3(\alpha) = 0$$

We get:

$$\alpha(\alpha-1) = 0 \Rightarrow \alpha = 0, 1$$

i.e. the only possible repeated roots of F are $\alpha = 0$ or $\alpha = 1$. □

We pause for a moment to mention a known combinatorial identity. We include a proof for completeness.

Proposition III.16. Let $n \in \mathbb{Z}_{\geq 0}$. Then

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$$

Proof. The right hand side is the number of ways to choose n objects in from a set of $2n$ objects. The left hand side can be written as:

$$\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}$$

So we interpret it as the following combinatorial process of choosing n objects out of $2n$: Color the objects in the set of $2n$ using 2 colors, red and green, so that we have n object of each. Now, in order to choose n objects, we can choose 0 red objects and n green objects. The total number of ways to do it is the first summand:

$$\binom{n}{0}\binom{n}{n}$$

Alternatively, we can choose 1 red object and $n-1$ green ones. The total number of ways to do it is the second summand:

$$\binom{n}{1}\binom{n}{n-1}$$

And so on. Note that the choice of n objects in each step is disjoint from the choice in the other step, so by adding the summands together we have to get the right hand side. □

Now we conclude an important property of $H\{n\}$:

Corollary III.17. Fix a prime p, and an integer $0 \leq n < p/2$. Let K be a field of characteristic p. Then $H\{n\} \in K[\lambda]$ has no repeated roots. Further, $\lambda = 0, 1$ are not roots of $H\{n\}$.

Proof. Let $H = H\{n\}$. Combining **Lemma III.13** and **Lemma III.15** shows that the only possible repeating roots of H are 0 and 1. However, $H(0) = 1$. Moreover, **Proposition III.16** shows:

$$H\{n\}(1) = \sum_{0}^{n} \binom{n}{i}^2 = \binom{2n}{n}.$$

This is non-zero mod p because $2n < p$, thus $\lambda = 1$ is not a root of H as well. □

Now let us prove a similar property for $F\{n\}$:

Lemma III.18. Fix $n \geq 0$. Let $F = F\{n\} \in \mathbb{Q}[\lambda]$ be the formal antiderivative of $H\{n\} \in \mathbb{Z}[\lambda]$ with constant coefficient 0. Then F satisfies:

$$\lambda(\lambda - 1)F'' - (1 + 2n)\lambda F' + (n + 1)^2 F = 0 \tag{III.18.1}$$

Further, if K is a field of prime characteristic p and $0 \leq n < p/2$, then $F\{n\}$ has a natural image in $K[\lambda]$ and has simple roots over K.

Proof. Similar to **Lemma III.13**, we enumerate the coefficients of λ^i in the different terms, construct a matrix and compute the kernel:

$$\begin{aligned}
&\text{coefficient in } F: && \binom{n}{i-1}\frac{1}{i} \\
&\text{coefficient in } F': && \binom{n}{i} \\
&\text{coefficient in } \lambda F': && \binom{n}{i-1} \\
&\text{coefficient in } F'': && (i+1)\binom{n}{i+1} \\
&\text{coefficient in } \lambda F'': && (i)\binom{n}{i} \\
&\text{coefficient in } \lambda^2 F'': && (i-1)\binom{n}{i-1}
\end{aligned}$$

If we pull $\frac{1}{i^2(i+1)}\binom{n}{i-1}$ outside from each coefficient, we get:

$$\begin{aligned}
&\text{coefficient in } F: && \frac{1}{i^2(i+1)}\binom{n}{i-1}\left(i(i+1)\right)\\
&\text{coefficient in } F': && \frac{1}{i^2(i+1)}\binom{n}{i-1}\left((n-i+1)^2(i+1)\right)\\
&\text{coefficient in } \lambda F': && \frac{1}{i^2(i+1)}\binom{n}{i-1}\left(i^2(i+1)\right)\\
&\text{coefficient in } F'': && \frac{1}{i^2(i+1)}\binom{n}{i-1}\left((n-i+1)^2(n-i)^2\right)\\
&\text{coefficient in } \lambda F'': && \frac{1}{i^2(i+1)}\binom{n}{i-1}\left((n-i+1)^2 i(i+1)\right)\\
&\text{coefficient in } \lambda^2 F'': && \frac{1}{i^2(i+1)}\binom{n}{i-1}\left(i^2(i+1)(i-1)\right)
\end{aligned}$$

The coefficient of λ^0 in (III.18.1) is 0 in all the terms. For $0 < i \leq n+1$, we can divide by $\frac{1}{i^2(i+1)}\binom{n}{i-1}$, expands each coefficient to a polynomial in i, and find a linear relation by writing the coefficients of i^0, i^1, i^2, i^3, i^4 in columns of matrix: write the coefficients of powers of i in F in the first column, in F' in the second column and so on.

$$M = \begin{bmatrix}
0 & (n+1)^2 & 0 & n^2(n+1)^2 & 0 & 0\\
1 & (n+1)^2 - 2n - 2 & 0 & -n^2(2n+2) - 2n(n+1)^2 & (n+1)^2 & 0\\
1 & -2n-1 & 1 & (n+1)^2 + n^2 + 2n(2n+2) & (n+1)^2 - 2n - 2 & -1\\
0 & 1 & 1 & -4n-2 & -2n-1 & 0\\
0 & 0 & 0 & 1 & 1 & 1
\end{bmatrix}$$

A direct computation shows that the rank of the matrix is 5 and the kernel space is

spanned by:

$$\begin{bmatrix} (n+1)^2 \\ 0 \\ -2\,n-1 \\ 0 \\ -1 \\ 1 \end{bmatrix}.$$

Ergo, F satisfies the differential equation (III.18.1) in characteristic 0 and thus in every characteristics in which F can be defined. A sufficient condition is $n+1 < p$ since in this case we can invert all the power of $H\{n\}$. Let K be field of prime characteristic p with $0 \leq n < p/2$. Since for all primes $p/2 \leq p-1$, the condition $n < p/2$ guarantees that we can define F in $K[\lambda]$. Using **Lemma III.15**, the above differential equation shows that the only possible repeating roots of F is 0 and 1. However, they are not roots of $H\{n\} = F'$ as can be seen in **Corollary III.17**. □

Remark III.19. Note that the differential equation from **Lemma III.13** can be deduced from **Lemma III.18** by simply taking a derivative.

Now we conclude that adjacent Deuring polynomials share no roots. This is the most important fact for the F-pure threshold computations done in the next chapters.

Theorem III.20. *Fix an integer $n \geq 1$ and a prime p such that $n < p/2$. Let K be a field of characteristic p. Then $H\{n\}$ and $H\{n-1\}$ share no roots.*

Proof. Let F be the formal antiderivative of $H\{n-1\}$ with constant coefficient 0 Consider the ideal $I = (H\{n\}, H\{n-1\})$ in $K[\lambda]$. From **Lemma III.12** we have:

$$I = (H\{n\}, H\{n-1\}) = ((1-\lambda)F' + 2nF, F') = (2nF, F') = (F, F'),$$

where the last inequality holds since $2n$ is a unit in $\mathbb{F}_p$ and thus in K. Therefore, I is the unit ideal if and only if F is has simple roots, which is the result in **Lemma III.18**. □

These are all the results we need in order to proceed with the computations of the F-pure threshold of the families of polynomials presented in the next chapters. However, it is interesting to further investigate the Deuring polynomials as algebraic objects.

3.4 More On Deuring Polynomials

Lemma III.9 motivates us to define the following:

Definition III.21. Let K be a filed of characteristic p. Define

$$H\{N,r\}(\lambda) := \sum_{i=0}^{N} \binom{N}{i}^r \lambda^i$$

Now we can generalize **Schur's Congruence**:

Proposition III.22. Fix a prime p and two positive integers n, r. Let $H\{n,r\} \in \mathbb{F}_p[\lambda]$. Write the p-expansion of n:

$$n = b_0 p^0 + b_1 p^1 + ... + b_e p^e.$$

Then

$$H\{n\} = H\{b_0\}^1 H\{b_1\}^{p^1} H\{b_2\}^{p^2} \cdots H\{b_e\}^{p^e}$$

Proof. Literally the same proof as in **Lemma III.9**. □

The computations we present later, rely heavily on **Schur's Congruence**. Ergo, if one finds families of polynomials where $H\{n,r\}$ shows up as coefficients in their

integer powers, one can use the same techniques to easily find bounds of the the F-pure threshold. For a general discussion about implications of Schur's Congruence, see **Chapter VI**.

The next proposition help us to investigate the roots of $H\{n\}$. Due to **Schur's Congruence**, in characteristic p, suffices to look at $H\{n\}$ with $n = 0, 1, ..., p-1$.

Proposition III.23. Fix $n \in \mathbb{Z}_{>0}$ and $H = H\{n\}$. Then:

(1) In characteristic 0, $H\{n\}$ has simple roots and 1 is not a root.

(2) In characteristic p, $H\{n\}(1) \equiv 0 \mod p$ if and only if $\binom{2n}{n} \equiv 0 \mod p$.

(3) In characteristic p with $n \leq p-1$, $H\{n\}$ has simple roots, except maybe for $\lambda = 1$ which may repeat.

(4) In characteristic p, if $2n < p$ then $H\{n\}$ has simple roots.

Proof. We use the differential operator III.13.1 and the argument in **Lemma III.15** to show that the only possible repeated roots of $H\{n\}$ in characteristic 0 are 0 and 1. Further, over any field $H\{n\}(0) = 1$ and $H\{n\}(1) = \binom{2n}{n}$, where the latter is a known combinatorial identity (see **Proposition III.16**). This proves (1) and (2).

For (3) simply apply the argument of **Lemma III.15** for the roots which are not 1. (4) is true since $2n < p$ guarantees that $\binom{2n}{n}$ is not 0 in $\mathbb{F}_p$.

□

Fix $p > 0$. We know that $H\{0\}, ..., H\{n_1\}$ are all simple, and we would like to investigate the repeating roots of $H\{n_1 + 1\}, ..., H\{p-1\}$.

Proposition III.24. Fix a prime p and an integer $0 \leq m \leq n_1$. Then the multiplicity of the root $\lambda = 1$ in $H\{n_1 + m\} \in \mathbb{F}_p[\lambda]$ is $2m$.

Proof. From **Proposition III.23** we conclude that $\lambda = 1$ is not a root of $H\{n_1\}$ while it is for $H\{n_1 + m\}$ with $1 \leq m \leq p-1$. So the case of $m = 0$ is covered.

From **Lemma III.8** we have that $H\{p-1\} = H\{n_1+n_1\} = (\lambda-1)^{p-1}$ so the multiplicity of 1 is $p-1 = 2n_1$ as required. Now fix some $1 \leq m \leq n_1$. Assume that s is the multiplicity of $\lambda - 1$ in $H\{n_1+m\}$ while r is the multiplicity of $\lambda-1$ in $H\{n_1+m-1\}$. We use induction on m, to show that $1 \leq s-r \leq 2$. Note that both r, s are less than p since the degree of the polynomials are less than p. We would like to use **Lemma III.12**. We can then write:

$$H'\{n_1+m\} = (\lambda-1)^{s-1}h(\lambda),\ h(1) \not\equiv 0 \pmod{p}$$

Recall that r is the multiplicity of $(\lambda-1)$ in $H\{n_1+m-1\}$. So we can write:

$$\begin{aligned} &H\{n_1+m-1\} = (\lambda-1)^r g(\lambda), \\ &H'\{n_1+m-1\} = r(\lambda-1)^{r-1}g + (\lambda-1)^r g', \\ &g(1) \not\equiv 0 \pmod{p}. \end{aligned}$$

Now plug in **Lemma III.12** with $n = n_1+m$, take one derivative, and combine like terms (note that $2n_1 = p-1 = -1$ in $\mathbb{F}_P$):

$$(\lambda-1)^r((-r+2m-2)g + (1-\lambda)g') = (\lambda-1)^{s-1}h \tag{III.24.1}$$

First notice that $r \leq s-1$. If $r < s-1$ then we can divide by $(\lambda-1)^r$ and plug in $\lambda = 1$. All the terms vanish except for $(-r+2m-2)g(1)$. In such case we conclude that $r = 2m-2$. Plugging that in, we get:

$$(\lambda-1)^{2m-2}((1-\lambda)g') = (\lambda-1)^{s-1}h.$$

The left hand side is divisible by $(\lambda-1)^{2m-1}$ which makes $s = 2m$. In particular, $s-r = 2$.

Now, denote r_m to be the multiplicity of $(\lambda-1)$ in $H\{n_1+m\}$. Observe the sequence $r_0, ..., r_{n_1}$. We know that $r_0 = 0$ and $r_{n_1} = 2n_1$, while $r_i - r_{i-1}$ is either 1

or 2. But observe:

$$2n_1 = r_{n_1} - r_0 = \sum_{i=1}^{n_1}(r_i - r_{i-1}) \geq n_1 \min_i(r_i - r_{i-1}).$$

This proves that the increase in the multiplicity must be 2 in each step, which shows that $r_m = 2m$ as required.

□

Corollary III.25. Fix a prime p and an integer $0 \leq m < n_1$. Then the multiplicity of the root $\lambda = 1$ in $F\{n_1 + m\} \in \mathbb{F}_p[\lambda]$ is $2m + 1$.

Proof. Use **Lemma III.12** with $n = n_1 + m + 1$ and plug in $\lambda = 1$. It is apparent that $F(1) = 0$. **Proposition III.24** shows that the multiplicity of 1 as a root of $F' = H\{n_1+m\}$ is $2m$, thus the multiplicity of 1 as a root of F is $2m$ as required. □

Lemma III.26. Fix a prime p and an integer $0 < n < p$. Then $H = H\{n\}$ is the only monic polynomial of degree n or less solving the differential equation **Equation III.13.1** in characteristic p and 0.

Proof. Suffices to prove the claim in characteristic p. Let $H = a_0 + a_1\lambda + ... + a_n\lambda^n$. Consider the set of polynomials in $\mathbb{F}_p$ with degree n or less as a vector space over $\mathbb{F}_p$ of dimension $n + 1$. Fix a basis $1, \lambda, \lambda^2, ..., \lambda^n$ and thus we represent H by a column vectors composed of its coefficients:

$$h = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

Denote the differential operator in (III.13.1) as $\mathcal{D}$. Notice that $\mathcal{D}$ cannot increase the degree of the polynomial it is acting on since multiplication by λ and λ^2 is applies

on H' and H'' accordingly. Thus the matrix representing the differential operator is upper triangular. We compute the entries on the diagonal: when $\mathcal{D}$ acting on λ^i, we get,

$$n^2\lambda^i + (1-2n)i\lambda^i + i(i-1)\lambda^i + \text{lower order terms},$$

making the appropriate diagonal entry

$$n^2 + (1-2n)i + i(i-1) = n^2 - 2ni + i^2 = (n-i)^2.$$

Since $0 \leq i \leq n$, then only non-zero entry is the last one. Ergo, the rank of $\mathcal{D}$ is n, making its kernel one dimensional. So up to multiplication of a scalar, only one polynomial solves the differential equation.

□

Lemma III.27. Fix a prime p and an integer $0 \leq m \leq n_1$. Then over $\mathbb{F}_p$:

$$H\{n_1 + m\} = (\lambda - 1)^{2m} H\{n_1 - m\}$$

Proof. From **Proposition III.24** we have a factorization:

$$H\{n_1 + m\} = (\lambda - 1)^{2m} g_m$$

where g_m is a polynomial. For $m = 0$ there is nothing to prove. For $m = n_1$, we have from **Lemma III.8** that $H\{2n_1\} = H\{p-1\} = (\lambda-1)^{p-1}$ while $H\{n_1 - n_1\} = H\{0\} = 1$. It is left to observe the cases where $1 \leq m \leq n_1 - 1$. We shall observe that g_m satisfy the same differential equation (III.13.1) as $H\{n_1 - m\}$ over $\mathbb{F}_p$, which is sufficient due to **Lemma III.26**. Observe:

$$H\{n_1 + m\} = (\lambda - 1)^{2m} g_m$$
$$H\{n_1 + m\}' = 2m(\lambda - 1)^{2m-1} g_m + (\lambda - 1)^{2m} g_m'$$
$$H\{n_1 + m\}'' = 2m(2m-1)(\lambda - 1)^{2m-2} g_m + 4m(\lambda - 1)^{2m-1} g_m' + (\lambda - 1)^{2m} g_m''$$

Now plug everything in the differential equation (III.13.1) for n_1+m, which is satisfied by $H\{n_1+m\}$. We shall do it by parts. Notice that $2(n_1+m)$ in characteristic p is $2m-1$:

$$\begin{aligned}
\lambda(1-\lambda)H\{n_1+m\}'' = &\quad (\lambda-1)^{2m-1}[2m(2m-1)\lambda g_m + 4m(\lambda-1)\lambda g'_m + +\lambda(\lambda-1)^2 g''_m] \\
(\lambda(2-2m)-1)H\{n_1+m\}' = &\quad (\lambda-1)^{2m-1}[(\lambda(2-2m)-1)2m g_m + (\lambda(2-2m)-1)(\lambda-1)g'_m] \\
(n_1+m)^2 H\{n_1+m\} = &\quad \tfrac{(2(n_1+m))^2}{4}(\lambda-1)^{2m} g_m = \tfrac{(2m-1)^2}{4}(\lambda-1)^{2m} g_m
\end{aligned}$$

Now collect the coefficients of g_m, g'_m and g''_m separately:

$$\begin{aligned}
g_m: &\quad (\lambda-1)^{2m-1}\left[2m\lambda(2m-1) + 2m\lambda(2-2m) - 2m + (\lambda-1)\tfrac{4m^2-4m+1}{4}\right] \\
g'_m: &\quad (\lambda-1)^{2m-1}\left[+4m(\lambda-1)\lambda + (2\lambda(1-m)-1)(\lambda-1)\right] \\
g''_m: &\quad (\lambda-1)^{2m-1}(\lambda-1)\left[\lambda(\lambda-1)\right]
\end{aligned}$$

Simplify the square bracket for g_m:

$$2m\lambda(2m-1) + 2m\lambda(2-2m) - 2m + (\lambda-1)\frac{4m^2-4m+1}{4} =$$

$$= 2m\lambda(1) - 2m + (\lambda-1)\frac{4m^2-4m+1}{4} = (\lambda-1)(2m + \frac{4m^2-4m+1}{4}) =$$

$$= (\lambda-1)\frac{4m^2+4m+1}{4} = (\lambda-1)\frac{2m+1}{4} = (\lambda-1)(n_1-m)^2,$$

since $(2(n_1-m))^2 = (-1-2m)^2 = (1+2m)^2$. So the coefficient of g_m is

$$(\lambda-1)^{2m}(n_1-m)^2$$

Simplify the square bracket for g'_m:

$$+4m(\lambda-1)\lambda + (2\lambda(1-m)-1)(\lambda-1) = (\lambda-1)(4m\lambda - 2m\lambda + 2\lambda - 1) =$$

$$= (\lambda-1)(2\lambda(1+m)-1) = (\lambda-1)(\lambda(1-2(n_1-m))-1).$$

So the coefficient of g'_m is

$$(\lambda-1)^{2m}(\lambda(1-2(n_1-m))-1)$$

The coefficient of g_m'' is simply:

$$(\lambda-1)^{2m}(\lambda(\lambda-1))$$

We conclude that g_m satisfy the following differential equation:

$$(\lambda-1)^{2m}\left[\lambda(\lambda-1)g_m''+(\lambda(1-2(n_1-m))-1)g_m'+(n_1-m)^2g_m\right]=0$$

The expression in the square bracket is a polynomial. So the equation can be satisfied only if

$$\lambda(\lambda-1)g_m''+(\lambda(1-2(n_1-m))-1)g_m'+(n_1-m)^2g_m=0$$

over $\mathbb{F}_p$, which is the same differential equation satisfied by $H\{n_1-m\}$ as required.

□

Remark III.28. It is tempting to claim that once p is fixed, then $H\{0\},...,H\{(p-1)/2\}$ have distinct roots. This claim is false, and examples can be easily found computationally. E.g. when $p=23$, then $\lambda=10$ is a root of both $H\{10\}$ and $H\{7\}$. When $p=17$, $H\{8\},H\{4\}$ share the factor $\lambda^2+16\lambda+1$.

Corollary III.29. Consider the polynomials $H\{n\},H\{n+1\}$ and a prime $p>2$. Then:

1. In characteristic 0, $H\{n\},H\{n+1\}$ have no common roots.
2. In characteristic p, with $n\leq n_1$, $H\{n\},H\{n+1\}$ have no common roots.
3. In characteristic p, with $n_1<n\leq p-1$, the only possible common factor of $H\{n\},H\{n+1\}$ is $(\lambda-1)$. If we denote $n=n_1+m$ then $(H\{n\},H\{n+1\})=(\lambda-1)^{2m}$.

Proof. Denote $F=F\{n\}$. From **Lemma III.12** and **Theorem III.20** we have that over any field

$$(H\{n\},H\{n+1\})=(F,F')$$

1. From **Lemma III.18** we deduce that F has simple roots thus $(H\{n\}, H\{n+1\})$ is the unit ideal in $\mathbb{Q}[\lambda]$.
2. Over $\mathbb{F}_p$, 0 is never a root of $F' = H\{n\}$, but 1 might be a root of F' if and only if $n > n_1$ (see **Proposition III.23** and **Lemma III.27**). Thus for $n \leq n_1$, 1 is not a root of $F' = H\{n\}$, rendering F to have simple roots. Thus $(H\{n\}, H\{n+1\}) = (1)$ over $\mathbb{F}_p$.
3. When $n_1 < n = n_1 + m$, from **Lemma III.27** and (2) we have:

$$(H\{n\}, H\{n+1\}) = (H\{n_1+m\}, H\{n_1+m+1\}) =$$

$$= (1-\lambda)^{2m}(H\{n_1-m\}, (1-\lambda)^2 H\{n_1-m-1\}) = (1-\lambda)^{2m}(1) = (1-\lambda)^{2m}$$

□

3.5 Legendre Polynomials

The Legendre Polynomials are well known and their properties can be found in many textbooks (for example, see [OMS09] and [AO09]. They can be defined in many ways and we mention two; for a positive integer n, the Legendre polynomial of degree n, $P_n(x)$, is a solution of the *Legendre's Differential Equation*:

$$\frac{d}{dx}\left[(1-x^2)\frac{d}{dx}P_n(x)\right] + n(n+1)P_n(x) = 0 \tag{III.29.1}$$

I.e. $P_n(x)$ is an eigenvector corresponding to the eigenvalue $\mu = n(n+1)$ in the Sturm-Liouville problem:

$$\frac{d}{dx}\left[(1-x^2)\frac{d}{dx}P(x)\right] = -\mu P(x)$$

Equivalently, we can get the different P_n's by performing Gram-Schmidt process on the real linear space spanned L by $\{1, x, x^2, ...\}$ with an inner product:

$$\langle f(x), g(x)\rangle = \int_{-1}^{1} f(x)g(x)\,dx.$$

So $P_n(x)$ are a orthogonal basis of L:

$$\int_{-1}^{1} P_n(x)P_m(x)\,dx = \frac{2}{2n+1}\delta_{nm},$$

where δ_{mn} is the Kronecker delta.

The relation between $P_n(x)$ and $H\{n\}(\lambda)$ is well known (see [CH14]):

$$H\{n\}(\lambda) = (1-\lambda)^n P_n\left(\frac{1+\lambda}{1-\lambda}\right) \tag{III.29.2}$$

The most crucial properties of $H\{n\}$ for the sake of F-pure threshold computation are **Theorem III.20** and **Lemma III.9**. Analytical techniques can be used to prove these through properties of $P_n(x)$: using the orthogonality, one can show that all the roots of $P_n(x)$ are between -1 and 1, and that all are simple. Moreover, we have a recursive relation:

$$P_n(x) = \frac{2n-1}{n}xP_{n-1}(x) - \frac{n-1}{n}P_{n-2}(x),\ n > 1$$

So it follows easily that $P_n(x), P_{n-1}(x)$ cannot have a common root in $\mathbb{R}$, since otherwise, it is a root of P_{n-2} as well, and so on. When reducing mod p, same argument holds as long as $1 \leq n < p$. This fact matches the result in **Theorem III.20** and **Corollary III.29**. **Lemma III.27** can be shown by another well-known characteristic p congruence ([Lan88, Lemma 2.2]): for $0 \leq n < p$:

$$P_n \equiv P_{p-1-n} \pmod{p}$$

Lemma III.9 is attributed to Schur but the first published proof is in [Wah52], which is slightly different than ours. Properties about repeated roots of $P_n(x)$ mod p can be found in [Lan88].

CHAPTER IV

F-Pure Threshold of Elliptic Curves

In this chapter, we provide an alternative and elementary proof for a known result about the F-pure threshold of a homogeneous polynomial of degree three in three variables with an isolated singularity. Such a polynomial defines an elliptic curve in $\mathbb{P}^2$. We show that once we transform the defining polynomial to the Legendre form, we get a polynomial f such that Deuring polynomials show up as coefficients in different integer powers of f. Then we apply the machinery from the previous chapter and describe an explicit computation of the F-pure threshold.

4.1 Introduction

The F-pure threshold of the defining equation of an elliptic curve in $\mathbb{P}^2$ is closely related to supersingularity. Recall the definition of supersingularity of an elliptic curve E in characteristic $p > 2$. The Frobenius morphism $E \xrightarrow{F} E$ induces a map $H^1(E, \mathcal{O}_E) \xrightarrow{F^*} H^1(E, \mathcal{O}_E)$. Then E is defined to be supersingular if F^* is the zero map. Otherwise, E is ordinary.

For our purpose, we adopt a more concrete characterization of supersingularity, in terms of the Hasse invariant of the defining polynomial f of E in $\mathbb{P}^2$. We review and develop this point of view in **Proposition IV.3**. See also [Har77, IV.4] and [Sil09, V.3,V.4].

In the upcoming sections we present an elementary proof of the following result, originally proven by Bhatt and Singh for $p > 3$:

Theorem IV.1 (**Main Theorem**). *Let K denote a field of prime characteristic $p > 0$. Let $f \in K[x, y, z]$ be a homogeneous polynomial of degree three defining an elliptic curve E in $\mathbb{P}^2_K$. Then:*

$$FT(f) = \begin{cases} 1 & \text{if } E \text{ is ordinary} \\ 1 - \frac{1}{p} & \text{if } E \text{ is supersingular} \end{cases}$$

Bhatt and Singh provide two proofs in [BS15] using a translation into local cohomology; Generalizations can be found in [HNnBWZ16]. In contrast, our approach involves directly investigating the form of f raised to integer powers using the Deuring polynomial $H\{m\}(\lambda) = \sum_{i=0}^{n} \binom{m}{i}^2 \lambda^i$ with $m = (p-1)/2$ (this polynomial is used to compute the Hasse invariant and sometimes is denoted H_p in the literature in this context). We manage to prove the theorem for $p > 2$ using this approach. For completeness, we later include a direct proof for the case of $p = 2$, so the theorem holds as stated for *all prime characteristics*.

Discussion IV.2. Going back to the characteristic 0 case, for an elliptic curve defined over $\mathbb{Q}$ there are infinitely many p's for which the reduction mod p is ordinary (see [Sil09, Execise V.5.11]). So we see that not only the F-pure threshold approaches the log canonical threshold, but it actually equals the log canonical threshold for infinitely many primes. This fact proves **Question I.2** for the family of elliptic curves defined over $\mathbb{Q}$, but for a general polynomial, the question remains open.

4.2 Preliminaries

Let K denote a field of prime characteristic $p > 2$. Let $f \in K[x, y, z]$ be homogeneous polynomial of degree three with an isolated singularity. Let $E \subset \mathbb{P}^2$ be

the elliptic curve defined by f. Note that the supersingularity of E and the value of $FT(f)$ are invariant under passing to the algebraic closure $\overline{K}$ and under a linear change of coordinates. So without loss of generality we assume K is algebraically closed and change coordinates so f is in its Legendre form:

$$f_a(x,y,z) = y^2z - x(x-z)(x-az), \;\; a \in K - \{0,1\} \tag{IV.2.1}$$

By letting a range over $K - \{0,1\}$ we are addressing all possible elliptic curves in $\mathbb{P}^2$ up to isomorphism. Thus, it suffices to prove the **Main Theorem** for this one-parameter family of polynomials.

Working with f_a allows us to assert supersingularity by a simple computation on a. We are going to work with the following, as proven in [Har77, IV, Corollary 4.22].

Proposition IV.3. Let K be a field of prime characteristics $p > 2$. Let $f_a(x,y,z) = y^2z - x(x-z)(x-az) \in K[x,y,z]$, with $a \in K - \{0,1\}$. Let $E \subset \mathbb{P}^2$ be the elliptic curve defined by f_a. Then E is supersingular if and only if over K:

$$\sum_{i=0}^{m} \binom{m}{i}^2 a^i = 0, \text{ with } m = (p-1)/2,$$

that is if and only if a is a root of the polynomial

$$H_p(\lambda) = \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i, \text{ with } m = (p-1)/2$$

in $K[\lambda]$. Otherwise, E is ordinary.

In particular, if a is transcendental over $\overline{\mathbb{F}_p}$, the polynomial $f_a \in K[x,y,z]$ always defines an ordinary elliptic curve.

Note that $H_p(\lambda)$ as noted in [Har77] is the Deuring polynomial $H\left\{\frac{p-1}{2}\right\}$, as we denoted in **Definition III.5**. It turns out that when investigating integer powers

of f_a, one gets coefficients that are Deuring polynomials of different degrees, as we prove later in the **Main Technical Lemma**. (Also note that $H\left\{\frac{p-1}{2}\right\}$ plays an important role in number theory, as **Proposition IV.3** implies.)

To make notation more compact, for a fixed p and a non negative integer e we define:

$$\begin{aligned} N_e &= p^e - 1 \\ n_e = N_e/2 &= \tfrac{p^e-1}{2}, \end{aligned} \tag{IV.3.1}$$

Specifically, when $e = 1$ we have:

$$n_1 = \frac{p-1}{2}.$$

Using **Proposition IV.3** we can rewrite the **Main Theorem** in a more computationally-friendly version, for the $p > 2$ case:

Theorem IV.4 (**Main Theorem V2**)**.** *Let K denote a field of prime characteristic $p > 2$. Let $f_a(x, y, z) = y^2z - x(x - z)(x - az) \in K[x, y, z]$, with $a \in K - \{0, 1\}$. Let $n_1 = (p - 1)/2$. Then:*

$$FT(f_a) = \begin{cases} 1 & \text{if } H\{n_1\}(a) \not\equiv 0 \pmod p \\ 1 - \frac{1}{p} & \text{if } H\{n_1\}(a) \equiv 0 \pmod p \end{cases}$$

When $H\{n_1\}(a) \not\equiv 0 \pmod p$, we say that f_a is ordinary. Otherwise we say that f_a is supersingular.

4.3 Proof of The Main Theorem

Lemma IV.5 (**Main Technical Lemma**)**.**

1. Let $f_\lambda = y^2z - x(x - z)(x - \lambda z)$ and let $N = n + m$ be a positive integer. Then the coefficient of $x^{2m}y^{2n}z^{n+m}$ in f^N is $\binom{n+m}{n}H\{m\}(\lambda)$ up to sign.

2. Let $f_\lambda = (x+y)(x+\lambda y)$ and let N be a positive integer. Then the coefficient of $x^N y^N$ in f_λ^N is $H\{N\}(\lambda)$.

Proof.

1. Observe $(y^2 z - x(x-z)(x-\lambda z))^{n+m}$. Since y is only in the left term, we need to raise it to the power of n. This gives the binomial coefficient $\binom{n+m}{n}$. So it is left to identify the coefficient of $x^{2m}z^m$ in $(-x(x-z)(x-\lambda z))^m = (-1)^m x^m (x-z)^m (x-\lambda z)^m$. This allows us to just compute the coefficient of $x^m z^m$ in $(x-z)^m(x-\lambda z)^m$. Notice:

$$(x-z)^m(x-\lambda z)^m = \left(\sum_{i=0}^{m} \binom{m}{i} (-1)^{m-i} x^i z^{m-i}\right)\left(\sum_{j=0}^{m} \binom{m}{j} (-\lambda)^j x^{m-j} z^j\right).$$

   For the coefficient of $x^m z^m$ we need to set $i = j$, so we end up with:

$$(-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i = (-1)^m H\{m\}.$$

   Together, up to sign, we get $\binom{n+m}{n} H\{m\}$.

2. This is very similar to the first statement and the proof is almost identical. Notice:

$$f_\lambda^N = (x+y)^N (x+\lambda y)^N = \left(\sum_{i=0}^{N} \binom{N}{i} x^i y^{N-i}\right)\left(\sum_{j=0}^{N} \binom{N}{j} (\lambda)^j x^{N-j} y^j\right).$$

   For the coefficient of $x^N y^N$ we need to set $i = j$, so we end up with:

$$\sum_{i=0}^{N} \binom{N}{i}^2 \lambda^i = H\{N\}.$$

   As required.

□

Corollary IV.6. Let $f_\lambda = y^2 z - x(x-z)(x-\lambda z)$ and let $N = 2n$. So the coefficient of $x^{2n} y^{2n} z^{2n}$ in f^N is $\binom{2n}{n} H\{n\}(\lambda)$ up to sign.

Proof. Apply the **Main Technical Lemma** with $m = n$. □

we now prove the **Main Theorem V2**, and we shall recall different properties of Deuring polynomials as needed.

Proof. Fix $p > 2$. We first show that if f_a is ordinary then $FT(f_a)$ is 1. Recall the notations: for an integer $e \geq 1$ we denote

$$N_e = p^e - 1$$

$$n_e = N_e/2 = (p^e - 1)/2.$$

In particular,

$$n_1 = \frac{p-1}{2}.$$

Let us raise f_a to the power of $N_e = p^e - 1$. Due to **Corollary IV.6** and **Lemma III.3** we get:

$$f^N = \pm \binom{2n_e}{n_e} H\{n_e\}(a) x^{N_e} y^{N_e} z^{N_e} + \text{terms already in } \mathfrak{m}^{[p^e]},$$

where $\mathfrak{m} = (x, y, z)$ and $\mathfrak{m}^{[p^e]} = (x^{p^e}, y^{p^e}, z^{p^e})K[x, y, z]$. By **Lemma III.2**, if we show that $\binom{2n_e}{n_e} H\{n_e\}(a) \not\equiv 0 \pmod{p}$ for any e, then we get a lower bound of $N_e/p^e = \frac{p^e-1}{p^e}$ for $FT(f_\lambda)$. By taking $e \to \infty$ we get that:

$$\lim_{e\to\infty} \frac{p^e - 1}{p^e} \leq FT(f_\lambda) \leq 1 \Rightarrow 1 = FT(f_\lambda)$$

So suffices to show that $\binom{2n_e}{n_e} H\{n_e\}(a) \not\equiv 0 \pmod{p}$.

First we deal with $\binom{2n_e}{n_e}$. We shall write both $2n_e$ and n_e in their base p-expansion:

$$\begin{aligned} 2n_e = p^e - 1 = &\quad (p-1)p^1 &+ &\quad (p-1)p^2 &+ &\quad \ldots &+ &\quad (p-1)p^{e-1} \\ n_e = &\quad \tfrac{p-1}{2}p^1 &+ &\quad \tfrac{p-1}{2}p^2 &+ &\quad \ldots &+ &\quad \tfrac{p-1}{2}p^{e-1} \end{aligned}$$

Since the digits of n_e and n_e are added without carrying to the digits of $2n_e$, by **Lucas's Theorem** $\binom{2n_e}{n_e} \not\equiv 0 \pmod{p}$.

Next, due to **Corollary III.10**:

$$H\{n_e\}(a) = (H\{n_1\}(a))^{1+p+\ldots+p^{e-1}}$$

We conclude that $H\{n_e\}(a) \not\equiv 0 \pmod{p}$ since the polynomial is ordinary, which means that $H\{n_1\}(a) \not\equiv 0 \pmod{p}$. This concludes the case where f_a is ordinary.

Now, we deal with the supersingular case. So fix $p > 2$ and assume that f_a is supersingular, i.e. that a is a root of $H\{n_1\}$. We first establish $1 - 1/p$ as an upper bound. Let $N = p - 1$. Consider f_a^N. Because f_a is supersingular, the coefficient of $x^N y^N z^N$ is 0 since it involves $H\{n_1\}(a)$. From **Lemma III.3**, all other monomials $\mathbf{x^k}$ satisfy $\max \mathbf{k} \geq N + 1 = p$. So apply **Lemma III.2** to get an upper bound of

$$\frac{N}{p} = \frac{p-1}{p} = 1 - \frac{1}{p}$$

As for the lower bound, fix $e \geq 1$. We will show that $\frac{p^e - p^{e-1} - 1}{p^e}$ is a lower bound for all e, which yields a lower bound of $1 - 1/p$ by taking $e \to \infty$. Once we show that, the proof is complete. We fix e and $N = p^e - p^{e-1} - 1$, and we shall prove that $f^N \notin \mathfrak{m}^{[p^e]}$. Notice that:

$$\begin{aligned} N = p^e - p^{e-1} - 1 \quad &= p^e - 2p^{e-1} + p^{e-1} - 1 = \\ &= (p-2)(p^{e-1}) + p^{e-1} - 1 = \\ &= (n_1)(p^{e-1}) + (n_1 - 1)(p^{e-1}) + p^{e-1} - 1. \end{aligned}$$

We set

$$\begin{aligned} n = \quad & (n_1)(p^{e-1}) \\ m = \quad & (n_1 - 1)(p^{e-1}) + p^{e-1} - 1. \end{aligned}$$

Notice that $m + 1 = n$.

In order to show the lower bound, it suffices to compute the coefficient of $\mathbf{x}^{2m,2n,n+m}$ in f_a^N and show that it is non-zero, because:

$$\max(2n, 2m, m+n) = 2n = (2n_1)(p^{e-1}) = (p-1)(p^{e-1}) < p^e.$$

From the **Main Technical Lemma** we get the coefficient of $\mathbf{x}^{2m,2n,n+m}$ in f^N is:

$$\binom{m+n}{n} H\{m\}(a) \tag{IV.6.1}$$

We wish to prove that the coefficient (IV.6.1) is non-zero mod p. We shall break it to two parts, the multinomial $\binom{m+n}{n}$, and the polynomials expression $H\{m\}(a)$. Let us start with the multinomial. We write m, n in their p-expansion while taking advantage of the geometric series formula:

$$\begin{array}{rccccccccc} n = & (0)p^0 & + & (0)p^1 & + & \ldots & + & (0)p^{e-2} & + & n_1 p^{e-1} \\ m = & (p-1)p^0 & + & (p-1)p^1 & + & \ldots & + & (p-1)p^{e-2} & + & (n_1-1)p^{e-1} \end{array}$$

So when adding m and n, the digits are not carrying, which implies that the multinomial coefficient $\binom{m+n}{n}$ is non-zero.

We complete the proof that the coefficient (IV.6.1) is not zero by showing that $H\{m\}(a)$ is not zero mod p. Recall that by our supersingularity hypothesis $H\{n_1\}(a) \equiv 0 \pmod{p}$. So suffices to show that the polynomials $H\{n_1\}$ and $H\{m\}$ share no roots in characteristic p. Observe again the p-expansion of m:

$$m = (p-1) + (p-1)p + (p-1)p^2 + \ldots + (p-1)p^{e-2} + (n_1-1)p^{e-1}$$

Use **Lemma III.9** to deduce

$$H\{m\} = H\{p-1\}^{1+p+\ldots+p^{e-2}} H\{n_1-1\}^{p^{e-1}}$$

So the problem is reduced to verifying that the irreducible factors of the polynomial $H\{n_1\}(\lambda) \in \mathbb{F}_p[\lambda]$ are neither factors of $H\{p-1\}(\lambda) \in \mathbb{F}_p[\lambda]$ nor of $H\{n_1-1\}(\lambda) \in \mathbb{F}_p[\lambda]$. The problem does not depend on e.

Let us start with $H\{p-1\}$. Recall **Lemma III.8**. Only $\lambda = 1$ is a root of $H\{p-1\}$ but $H\{n_1\}(1)$ is not zero due to **Corollary III.17**.

It remains to compare the roots of $H\{n_1\}$ and $H\{n_1-1\}$. From **Theorem III.20** we conclude that they share no roots, as required. This concludes the proof.

□

Discussion IV.7. For completeness, let us compute that $FT(f_a) = 1/2$ for

$$f_a = y^2z + x(x+z)(x+az),\ a \in K - \{0,1\}$$

where $\mathrm{char}(K) = 2$. From **Lemma III.9** we deduce that over K and for any integer $m > 0$, $H\{m\} = H\{1\}^m = (1+\lambda)^m$ (this is also because for any $c \in \mathbb{F}_2, c^2 = c$). Since $a \neq 1$, a does not satisfy any Deuring polynomial over K. To prove that $1/2$ is an upper bound, just observe that f_a^1 is already in (x^2, y^2, z^2) making $1/2$ an upper bound. Now, we would like to show that $(2^{e-1}-1)/2^e$ is a lower bound for all e, which would result in an lower bound of $1/2$. So let

$$N = 2^{e-1} - 1 = 1 + 2 + 2^2 + ... + 2^{e-3} + 2^{e-2}$$

To avoid carrying, choose $N = n + m$ with

$$n = 2^{e-2}, m = 2^{e-2} - 1 = n - 1 = 1 + 2 + ... + 2^{e-3}.$$

By construction, and due to **Main Technical Lemma**, the coefficient of $x^{2m}y^{2n}z^{n+m}$ does not vanish, while $\max\{2n, 2m, m+n\} = 2n = 2^{e-1} < 2^e$. Thus we get an lower bound of $N/2^e = (2^{e-1}-1)/2^e$ as required.

4.4 Elliptic Curves in Characteristic 2

To complete the $p = 2$ case of **Theorem IV.1**, we shall compute the F-pure threshold of polynomials defining elliptic curves in characteristic 2. Up to a change of variables, a defining polynomial can be of these two forms:

$$f = zy^2 + xyz + x^3 + a_2x^2z + a_6z^3$$

or

$$f = zy^2 + a_3z^2y + x^3 + a_4xz^2 + a_6z^3,$$

as the following proposition shows:

Proposition IV.8. Let E be an elliptic curve over a field K of characteristic 2 for which the Weierstrass equation is (see [Sil09, Chapter III.1]):

$$y^2z + a_1xyz + a_3yz^2 + x^3 + a_2x^2z + a_4xz^2 + a_6z^3 = 0,\ a_1, a_2, a_3, a_4, a_6 \in K$$

If $a_1 \neq 0$ then we can perform linear change variables and get the form:

$$y^2z + xyz + x^3 + a_2'x^2z + a_6'z^3 = 0,\ a_2', a_6' \in K$$

Alternatively, if $a_1 = 0$, we can perform linear change variables and get the form:

$$y^2z + a_3z^2y + x^3 + a_4'xz^2 + a_6'z^3 = 0,\ \ a_3, a_4', a_6' \in K$$

Proof. [Was08, Section 2.8] □

We deduce that in characteristic 2, Elliptic Curves adopt two forms as above. The first case corresponds to ordinary curves where the second case corresponds to supersingular curves (see [Was08, Section 3.1]). Let us discuss the ordinary case:

Proposition IV.9. Let $f = zy^2 + xyz + x^3 + a_2x^2z + a_6z^3$ where $a_2, a_6 \in K$ where $\mathrm{char}K = 2$. Then $FT(f) = 1$.

Proof. Consider the splitting matrix of f:

$$M = \begin{pmatrix} 0 & 1 & 3 & 2 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 3 \end{pmatrix}$$

It is easy to see that M is of rank 3, thus the full solution of $M\mathbf{k} = [N, N, N]^{Tr}$ is:

$$\mathbf{k} = \begin{pmatrix} 0 \\ N \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha \begin{pmatrix} 1 \\ -2 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 3 \\ -6 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

Ergo, the coefficient of $x^N y^N z^N$ in f^N can be computed by summing all possible pairs α, β such that $\mathbf{k} \in \mathbb{Z}^5_{\geq 0}$:

$$\sum_{\alpha,\beta | \mathbf{k} \in \mathbb{Z}^5_{\geq 0}} \binom{N}{\alpha + 3\beta, N - 2\alpha - 6\beta, 2\beta, \alpha, \beta} a_2^{\alpha} a_6^{\beta} \tag{IV.9.1}$$

We claim that the only non zero summand in (IV.9.1) is when $\alpha = \beta = 0$. We shall prove that any other choice would make the the base 2 digits of $\alpha + 3\beta, N - 2\alpha - 6\beta, 2\beta, \alpha, \beta$ to carry when added. Indeed add the last three to get $\alpha + 3\beta$, which is identical to the first one. In characteristic 2, the base-2 expansion consist of only 0 and 1 digits while $1 + 1 = 0$; ergo, the only why to add two identical numbers without carrying is when both are 0. So, to avoid carrying, $\alpha + 3\beta = 0$. Since both non-negative, $\alpha = \beta = 0$.

We conclude that in f^N, the monomial $x^N y^N z^N$ appears with coefficient 1. So let $N = 2^e - 1 = 1 + 2 + ... + 2^{e-1}$ and observe that $f^N \notin (x, y, z)^{[2^e]}$ thus $N/p^e < FT(f)$ for all e. So $1 = FT(f)$ simply by talking the limit. □

Let us discuss the supersingular case:

Proposition IV.10. Let $f = zy^2 + a_3 z^2 y + x^3 + a_4 x z^2 + a_6 z^3$ where $a_3, a_4, a_6 \in K$ where char$K = 2$. Then $FT(f) = 1/2$.

Proof. First notice that already $f^1 \in (x, y, z)^{[2]}$ making $1/2$ an upper bound. To see that $1/2$ is a lower bound, raise f to the power of $N = 2^{e-1} - 1$. Look at the

monomial $y^{2N}z^N$ in f^N. Since 2 is the maximal power of y in f and appears only in the monomial zy^2, we must get $y^{2N}z^N$ in

$$f^N = \underbrace{f \cdot f \cdot \ldots \cdot f}_{N \text{ times}}$$

by choosing y^2z in all N factors, making $y^{2N}z^N$'s coefficient 1. Now observe $2N = 2^e - 2 < 2^e$, thus $N/2^e = 1/2 - 1/2^e$ is a lower bound for all e. Ergo, $1/2$ is indeed a lower bound for $FT(f)$. The proof is now complete. $\square$

CHAPTER V

The F-Pure Threshold of Schemes Supported at Four Points in $\mathbb{P}^1$, and The Cross-Ratio

In this chapter, we provide an elementary computation of the F-pure threshold of the homogeneous defining equation of a certain type of subschemes of $\mathbb{P}^1$ supported at four points. For the case where the four points are distinct, we transform the defining polynomials to a form that share critical features with the defining polynomials of Elliptic Curves from the previous chapter. We explicitly deduce a formula for the F-pure threshold using the same machinery. The formula depends on whether the cross-ratio of these four points satisfies a certain *Deuring* Polynomial. We shall see that the results in this chapter reduces **Question I.2**, for a certain family of bivariate forms, to understanding roots of Legendre polynomials over $\mathbb{F}_p$.

5.1 Introduction

The first goal is to compute the F-pure threshold of a bivariate homogeneous polynomial of degree four. Consider the four roots in $\mathbb{P}^1$. Because the case of multiple roots is easy (see **Discussion V.10**), our main result treats the case where the roots are all distinct:

Theorem V.1. *Let K be a field of prime characteristic p. Consider a degree four homogeneous polynomial $f \in K[x,y]$, with distinct roots over $\mathbb{P}^1_{\overline{K}}$. After fixing*

an order of the roots, let $a \in \overline{K}$ *be their cross-ratio. Denote* $n_1 = \frac{p-1}{2}$*, and let* $H\{n_1\}(\lambda) \in K[\lambda]$ *be the Deuring polynomial (defined in* ***Definition III.5****) of degree* n_1*. Then*

$$FT(f) = \begin{cases} \frac{1}{2} & \text{if } p = 2 \text{ or if both } p > 2 \text{ and } H\{n_1\}(a) \neq 0 \\ \frac{1}{2}\left(1 - \frac{1}{p}\right) & \text{if } p > 2 \text{ and } H\{n_1\}(a) = 0. \end{cases}$$

It is intriguing that the value of the F-pure threshold depends on whether the cross-ratio satisfies some (Möbius transformation of) Legendre polynomial. The technique we use in the proof relies on the properties of the Deuring Polynomials as presented in **section 3.3**.

We generalize **Theorem V.1** to certain higher degree polynomials:

Theorem V.2. *Let* K *be a field of prime characteristic* p*. Let* $c, b \in \mathbb{Z}_{>0}$ *with* $p \equiv 1 \pmod{b+c}$*. Let* $f \in K[x, y]$ *be a homogeneous polynomial of degree* $2b + 2c$ *with exactly four distinct roots over* $\mathbb{P}^1_{\overline{K}}$*, where the multiplicities are* b, b, c, c *after fixing an order. Let* a *be the their cross-ratio. Denote* $n = \frac{c}{c+b}(p-1)$*. Then*

$$FT(f) = \begin{cases} \frac{1}{b+c} & \text{if } H\{n\}(a) \neq 0 \\ \frac{1}{b+c}\left(1 - \frac{1}{p}\right) & \text{if } H\{n\}(a) = 0 \end{cases}$$

Discussion V.3. We now point out how the open question in **Question I.2** relates to Legendre polynomials for the case of the family of polynomials in **Theorem V.2**. Let f be a polynomial as in the theorem and assume that f has integer coefficients. One can compute that $\operatorname{lct}(f) = \frac{1}{b+c}$. In order to verify the conjecture for this specific family of polynomials, one should prove that there are infinitely many p's such that the cross ratio of the image of f in $\mathbb{F}_p$, f_p, is not a root of $H\left\{\frac{c}{b+c}(p-1)\right\}$ over $\overline{F_p}$. For example, here is a precise formulation of our statement is the simplest case.

Question V.4. Suppose $f = x^b y^b (x+y)^c (x+ay)^c \in \mathbb{Z}[x,y]$. Denote

$$\mathcal{P} = \left\{ \text{all primes } p \;\middle|\; p \equiv 1 \pmod{b+c} \text{ and } H\left\{\frac{c}{b+c}(p-1)\right\}(a) \not\equiv 0 \pmod{p} \right\}.$$

Is it true that the cardinality of $\mathcal{P}$ is infinite?

This may be very difficult, and is related to deep theorems in number theory. For example, the case where $b = c = 1$ is already known as it is equivalent to the fact that there are infinitely many p's such that an elliptic curve is ordinary (see **Discussion IV.2** and [Pag17]). Further evidence that the conjecture is connected to ordinarity is explored in [MS11].

In addition, the F-pure threshold computation in **Theorem V.1** provides a new proof for an immediate corollary regarding properties of the roots of Legendre polynomials mod p:

Corollary V.5. Fix a prime $p > 2$, a field K of characteristic p and let $n = \frac{p-1}{2}$. If $b \in K - \{\pm 1\}$ is a root of the Legendre polynomial of degree n, $P_n(x) \in K[x]$, then these are roots as well:

$$\pm b, \pm\frac{3+b}{-1+b}, \pm\frac{3-b}{1+b}.$$

See **section 5.3**.

5.2 Computation of the F-pure threshold

Let f be a bivariate degree four homogeneous polynomial. We would like to reduce the problem of computing $FT(f)$ of this quite general polynomial to a problem of computing the F-pure Threshold of a more "canonical" polynomial.

Proposition V.6. Let $f \in K[x,y]$ be a degree four homogeneous polynomial over a field K of characteristic p. Then $FT(f)$ is identical to the F-pure threshold of one

of the following polynomials:

$$x^4, x^3y, x^2y^2, x^2y(x+y), xy(x+y)(x+ay) \text{ with } a \in \overline{K} - \{0,1\}. \tag{V.6.1}$$

Proof. $FT(f)$ is preserved under base change, scalar multiplication and linear change of variables. Thus, without loss of generality, let K is algebraically closed, over which f factors as a product linear terms. Now change variables to obtains one of the five forms in (V.6.1), and suffices to compute $FT(f)$ for each of these cases. □

We are interested in the last form, since the F-pure threshold can be computed easily in the rest of the cases. For completeness, we comment about them in **Discussion V.10**.

Recall **Lemma IV.5**. This lemma shows that understanding the Deuring polynomial $H\{n\}$ is crucial for the discussion. Since the F-pure threshold is invariant under base change and linear change of variables, we can assume $K = \overline{K}$ and that our polynomials adopts the last form in **Proposition V.6**. Thus, we can reduce **Theorem V.1** and **Theorem V.2** to a more computationally friendly theorem (it is easy to see that a is the cross-ratio of the roots once we fix an order and that a cannot be $0, 1$ or ∞ since the roots are all distinct. We include a detailed computation later in the proof of **Corollary V.11**):

Theorem V.7. *Let K be a field of prime characteristic p. Let $c, b \in \mathbb{Z}_{>0}$ with $p \equiv 1 \pmod{b+c}$. Fix $f \in K[x,y]$ of the form:*

$$f_a = x^b y^b (x+y)^c (x+ay)^c,\ a \in K - \{0,1\}, \tag{V.7.1}$$

Denote $n = \frac{c}{c+b}(p-1)$ and let $H\{n\}(\lambda) \in K[\lambda]$ be the Deuring polynomial of degree n. Then

$$FT(f_a) = \begin{cases} \frac{1}{b+c} & \text{if } H\{n\}(a) \neq 0 \\ \frac{1}{b+c}\left(1 - \frac{1}{p}\right) & \text{if } H\{n\}(a) = 0 \end{cases}$$

As long as $p \neq 2$, **Theorem V.1** is a special case of **Theorem V.7** in which $b = c = 1$. Note also that the $p \neq 2, b = c = 1$ scenario is also provable by applying [HNnBWZ16, Theorem 3.5] with $a = L = 1, b = 2$ per their notation; however the computation is not direct. The proof of the general **Theorem V.7** follows next where the $p = 2$ special case is proven right after.

We start with a small lemma:

Lemma V.8. Let c be an integer bigger than 1. Let p be a prime such that $c < p$. Then, there exist a power of p, r, such that $p^r \equiv 1 \pmod{c}$.

Proof. Look at the sequence $p, p^2, p^3, ...$ in the ring $R = \mathbb{Z}/(c)$. Record the first pair of powers that reduce to the same element in R, say p^s, p^t with $s < t$. So

$$p^t - p^s = \alpha c$$

For some integer α. Since $c < p$, divide by p^s to get:

$$c \mid p^{t-s} - 1$$

which proved the result. □

Now, for the proof of **Theorem V.7**:

Proof. The key observation is that for a positive integer N, we use **Lemma IV.5** and **Lemma III.3** to deduce:

$$\begin{aligned} f_a^N &= x^{bN} y^{bN} ((x+y)(x+ay))^{cN} = \\ &= x^{(b+c)N} y^{(b+c)N} H\{cN\}(a) + \text{ an element in } (x^{(b+c)N+1}, y^{(b+c)N+1}) \end{aligned} \tag{V.8.1}$$

Let us prove that $1/(b+c)$ is an upper bound. Fix an integer $e > 0$ and set $N = \frac{1}{b+c}(p^e - 1 + p - 1)$. From (V.8.1), combined with **Lemma III.2**, we get the $N/p^e = \frac{1}{b+c}\frac{p^e+p-2}{p^e}$ is an upper bound. Taking $e \to \infty$, we get that $FT(f_a) \leq \frac{1}{b+c}$ as required.

In the case that $H\{n\}(a) \neq 0$, we wish to show that $\frac{1}{b+c}$ is also a lower bound. With $e > 0$ and $N = \frac{1}{b+c}(p^e - 1)$, the coefficient of $x^{(b+c)N}y^{(b+c)N}$ in f_a^N is $H\{cN\}(a)$. Since $(b+c)N = p^e - 1 < p^e$, showing that $H\{cN\}(a) \neq 0$ would establish $N/p^e = \frac{1}{b+c}\frac{p^e-1}{p^e}$ as a lower bound for any $e > 0$, and thus $\frac{1}{b+c} \leq FT(f_a)$. Let us compute the p-expansion of cN:

$$cN = \frac{c}{b+c}(p^e - 1) = \frac{c(p-1)}{b+c} + \frac{c(p-1)}{b+c}p + ... + \frac{c(p-1)}{b+c}p^{e-1}$$

Note that $n = \frac{c(p-1)}{b+c}$ is an integer between 0 and $p-1$. Ergo, by **Lemma III.9**

$$H\{cN\}(a) = H\left\{\frac{c}{b+c}(p^e - 1)\right\}(a) = (H\{n\}(a))^{\text{some power}} \neq 0 \tag{V.8.2}$$

In the case that $H\{n\}(a) = 0$, we would like to show that $FT(f_a) = \frac{1}{b+c}\left(1 - \frac{1}{p}\right)$. To establish that value as an upper bound, consider again $N = \frac{1}{b+c}(p^e - 1)$. From (V.8.1) and (V.8.2) we see that $H\{cN\}(a) = 0$ and thus $f_a^N \in (x,y)^{[p^e]}$, making N/p^e an upper bound. Plug in $e = 1$ to see that $\frac{1}{b+c}\left(1 - \frac{1}{p}\right)$ is indeed an upper bound.

As for a lower bound, we recall **Theorem III.20** and note that since $H\{n\}(a) = 0$, $H\{n-1\}(a) \neq 0$. Since $c < p$ (p is at least $b+c+1$), and p is a prime, there is a power of p that is congruent to 1 mod c (see **Lemma V.8**). Denote it as p^d. For any positive integer m, $p^{md} \equiv 1 \pmod{c}$ and thus we define:

$$\ell(m) := (p-n)p^{md-1} \equiv 1 \pmod{c},$$

because c divide n.

Now, consider the integer

$$N' = (p-1)p^0 + (p-1)p^1 + ... + (p-1)p^{e-2} + (n-1)p^{e-1} = p^{e-1} - 1 + (n-1)p^{e-1} = np^{e-1} - 1$$

for $e \gg 1$. The digits of the p expansion are $(p-1)$ and $(n-1)$. We cannot just yet use N' as cN since it is not necessarily divisible by c. In fact, since n is divisible

by c, it is congruent to $c-1$ mod c. By subtracting $\ell(1)$ from N' we are making the p^{d-1} digit become $(n-1)$ instead of $(p-1)$, and then $N'-\ell(1)$ is congruent to $c-2$ mod c. So we shall do the same for the p^{2d-1} digit, the p^{3d-1} digit and so on, through the $p^{(c-1)d-1}$ digit. Now we get an integer divisible by c and we can define N:

$$cN = N' - \ell(1) - ... - \ell(c-1) = np^{e-1} - 1 - \ell(1) - ... - \ell(c-1),$$

$$N = \frac{1}{b+c}(p-1)p^{e-1} - L,$$

were L is some integer constant, not dependent on e. We are about to show that N/p^e is a lower bound for arbitrary large e, which complete the proof. Notice that $(b+c)N = (p-1)p^{e-1} - (b+c)L < p^e$, while the coefficient of $x^{(b+c)N}y^{(b+c)N}$ in f^N is $H\{cN\}$. We carefully crafted cN to have a p expansion containing only digits of $(p-1)$ or $(n-1)$. Using **Lemma III.9**, we have:

$$H\{cN\} = H\{p-1\}^{\text{some power}} H\{n-1\}^{\text{some power}}.$$

Indeed $H\{cN\}(a)$ is non-zero since $H\{n-1\}(a) \neq 0$ and since $H\{p-1\} = (\lambda-1)^{p-1}$ (**Lemma III.8**) while $a = 1$ is not a root of $H\{n\}$ (**Corollary III.17**). This completes the proof. □

As promised, we deal with the $p = 2$ case:

Proposition V.9. Let K be a field of prime characteristic $p = 2$. Fix a polynomial:

$$f_a = xy(x+y)(x+ay),\ a \in K - \{0,1\}$$

Then $FT(f_a) = \frac{1}{2}$

Proof. Note that (V.8.1) holds, with $b = c = 1$, but we cannot replicate the same proof as in **Theorem V.7** as, for example, $N = (1/2)(p^e \pm 1)$ is not an integer. We

need to use different N's. For the upper bound, use $N = \frac{1}{2}p^e$ (we intentionally do not plug in $p = 2$ for clarity). Then f_a^N is in $(x, y)^{[p^e]}$ thus $N/p^e = 1/2$ is an upper bound.

As for the lower bound, use $N = \frac{1}{2}(p^e - 2)$. Then f_a^N has a monomial $x^{2N}y^{2N}$ with $2N = p^e - 2 < p^e$. As long as a is not a root of $H\{N\}$, $N/p^e = (1/2)(1 - 2/p^e)$ is a lower bound, which approaches to $1/2$ as $e \to \infty$. Notice that:

$$N = \frac{1}{2}(p^e - 2) = p^{e-1} - 1 = 1 + p + ... + p^{e-2}.$$

So due to **Lemma III.9**

$$H\{N\} = H\{1\}^{\text{some power}} = (1 + \lambda)^{\text{some power}}.$$

Since $a \neq 1$, $H\{N\}(a) \neq 0$ and we are done. □

Discussion V.10. For completeness, let us present all possible values of the F-pure threshold of a bivariate degree four homogeneous polynomial with four roots, not necessarily distinct. Consider again these five forms:

$$x^4, x^3y, x^2y^2, x^2y(x + y), xy(x + y)(x + \lambda y) \text{ with } \lambda \in K - \{0, 1\},$$

Indeed suffices to compute $FT(f)$ for each of these cases. The monomial cases are straightforward; it is easy to show that $FT(x_1^{a_1}x_2^{a_2} \cdots x_t^{a_t})$ is $(\max(a_1, ..., a_t))^{-1}$ ([BFS13, Example 3.10]). The $f = x^2y(x + y)$ case is treated in [Her14] as it is a binomial, and it is easy to see that the F-pure threshold in this case is $\frac{1}{2}$. The last case is the subject of **Theorem V.1**.

5.3 Conclusions for Legendre Polynomials

An immediate consequence of **Theorem V.1** is the following conclusion (which is a known property as presented in [BM04]).

Corollary V.11.

1. Fix a prime $p > 2$, and let $n = \frac{p-1}{2}$. If $a \in \overline{\mathbb{F}_p} - \{0, 1\}$ is a root of $H\{n\}$, then so are:

$$(a)^{\pm 1}, (1-a)^{\pm 1}, \left(\frac{a}{a-1}\right)^{\pm 1}. \tag{V.11.1}$$

2. Fix a prime $p > 2$, a field K of characteristic p, and let $n = \frac{p-1}{2}$. If $b \in K - \{\pm 1\}$ is a root of the Legendre polynomial of degree n, $P_n(x) \in K[x]$, then also:

$$\pm b, \pm\frac{3+b}{-1+b}, \pm\frac{3-b}{1+b}.$$

Theorem V.2 give rise to another corollary (which is similar to **Lemma III.27**); the statement is known in the context of Legendre polynomials.

Corollary V.12. Fix a prime $p > 2$. Let $b, c \in \mathbb{Z}_{>0}$ such that $p \equiv 1 \pmod{(b+c)}$. Let $a \in \overline{\mathbb{F}_p} - \{0, 1\}$, then:

$$H\left\{\frac{b}{b+c}(p-1)\right\}(a) = 0 \iff H\left\{\frac{c}{b+c}(p-1)\right\}(a) = 0.$$

The following discussion illustrate how the F-pure threshold computation provide a new proof for both corollaries. Let $K = \overline{K}$ and consider a degree four homogeneous polynomial $f \in K[x, y]$ with distinct roots (z_1, z_2, z_3, z_4) over $\mathbb{P}^1_K$. The linear change of variables needed to get the form

$$f_a = xy(x+y)(x+ay) \text{ with } a \in K - \{0, 1\} \tag{V.12.1}$$

sends:

$$(z_1, z_2, z_3, z_4) \mapsto (0, \infty, -1, -a),$$

and a quick computation reveals that a is the cross-ratio:

$$a = \frac{z_4 - z_1}{z_4 - z_2}\frac{z_3 - z_2}{z_3 - z_1}$$

Since the roots are all distinct, a is not $0, 1$ or ∞. Notice that a depends on the order we had chosen for the roots. Considering all possible orders, we can get the same form (V.12.1) only with one of the following: $a, 1/a, 1-a, 1/(1-a), a/(a-1), (a-1)/a$. This can be done using a linear change of variables, thus the value of the F-pure threshold is preserved. With the notation from (V.12.1), we conclude that:

$$FT\left(f_a\right) = FT\left(f_{1/a}\right) = FT\left(f_{1-a}\right) = FT\left(f_{1/(1-a)}\right) = FT\left(f_{a/(a-1)}\right) = FT\left(f_{(a-1)/a}\right),$$

However, the conclusion of **Theorem V.1** is independent of the implicit order we had chosen for the roots. This geometrical insight reveals the interesting property of the roots of $H\left\{\frac{p-1}{2}\right\}$ over $\overline{\mathbb{F}_p}$ mentioned in the first statement of **Corollary V.11**. Note that $H\{n\}(a) = 0 \iff H\{n\}(1/a) = 0$ is expected due to the symmetry in **Definition III.5**:

$$H\{n\}(\lambda) = \lambda^n H\{n\}(1/\lambda), \tag{V.12.2}$$

but the inference on the rest of the roots in (V.11.1) is not at all trivial. The second statement of **Corollary V.11** is obtained by rewriting the first statement using (III.29.2) and we include the computation here for completeness: Let T be the matrix

$$T = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}.$$

T represents the Möbius transformation $\frac{\lambda+1}{-\lambda+1}$. Thus, if a is a root of $H\{n\}$, then multiply $T[1,\, 0]^{Tr}$ to see that $\frac{a+1}{-a+1}$ is a root of P_n (as **Equation III.29.2** shows).

Note that the inverse of T is:

$$T^{-1} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix},$$

however we can ignore the scalar multiplier as it does not affect the underlying Möbius transformation. So, if b is a root of P_n, then $\frac{a-1}{a+1}$ is a root of $H\{n\}$. Now denote:

$$T_1 = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix},$$

$$T_2 = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix},$$

$$T_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Notice that T_1, T_2, T_3 represents transformations which map roots of $H\{n\}$ to roots of $H\{n\}$. Ergo, TT_iT^{-1}, for $i = 1, 2, 3$, gives us transformations which map roots of P_n to roots of P_n. These matrices give the roots as described in the second statement of **Corollary V.11**.

A similar analysis, performed in the case of **Theorem V.2**, gives us **Corollary V.12**: Consider a homogeneous polynomial over $K[x, y]$, $K = \overline{K}$, with 4 distinct (ordered) roots (z_1, z_2, z_3, z_4) over $\mathbb{P}^1_K$ of multiplicities b, b, c, c respectively. After a linear change of variables the polynomial adopts the form:

(V.12.3) $$f_a = x^b y^b (x + y)^c (x + ay)^c,\ a \in K - \{0, 1\}.$$

In order to do so, one maps

$$(z_1, z_2, z_3, z_4) \mapsto (0, \infty, -1, -a),$$

which yields the same cross-ratio:

$$a = \frac{z_4 - z_1}{z_4 - z_2}\frac{z_3 - z_2}{z_3 - z_1}$$

Considering the result in **Theorem V.2**, it is crucial to notice the value of $FT(f_a)$ is symmetric in b, c but we cannot arbitrarily reorder the roots — 0 and ∞ has to have the same multiplicity to obtain the form (V.12.3), possibly with b and c interchanged. A computation shows that we can get the same form with $1/a$ instead of a, while the other values of the cross-ratio are not allowed when $b \neq c$. However, since we can interchange b and c we get that:

$$H\left\{\frac{b}{b+c}(p-1)\right\}(a) = 0 \iff H\left\{\frac{c}{b+c}(p-1)\right\}(a) = 0.$$

This proves **Corollary V.12**. The argument presents a new proof of **Lemma III.27**.

CHAPTER VI

Schur Compliance, Stratification of Parameter paces by $FT(f)$

In this chapter we generalize the techniques used in the previous chapters. Specifically, we are generalizing the elegant **Schur's Congruence**(**Lemma III.9**). Such generalization is possible under some assumptions (**Conjecture VI.21**). This allows us to compute the F-pure threshold values for the family of all polynomials supported by the same monomials. As a result, an explicit stratification of the coefficient space by algebraic subvarieties arises, each represent a set of polynomials sharing the same F-pure threshold value.

6.1 Introduction

Throughout this chapter we will follow the same setup.

Discussion VI.1 (**Setup**)**.** Fix a prime integer p. Fix an algebraically closed field K of prime characteristic p and let $R = K[x_1, ..., x_t]$ be a polynomial ring over K. Fix a set of monomials, $\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}$ and let $M \in \mathbb{Z}_{\geq 0}^{t \times s}$ be the resulting splitting matrix (see **subsection 2.1.2**). Let $b_1, ..., b_s$ be indeterminates. We are interested in computing the F-pure threshold of a generic polynomial:

$$f = b_1\boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + b_s\boldsymbol{x}^{\boldsymbol{\mu}_s}.$$

Then, we wish to find out how $FT(f)$ changes when we plug in scalars from K instead of the b's and get a "specialized" polynomial in $K[x_1, ..., x_t]$. Put differently, we are interested in investigating the function:

$$FT : \mathbb{P}^{s-1} \to \mathbb{Q},$$

defined by

$$FT(c_1, ..., c_s) = FT(f), \text{ where } f = c_1\boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + c_s\boldsymbol{x}^{\boldsymbol{\mu}_s}.$$

Note that the coefficient space is taken to be $\mathbb{P}^{s-1}$ rather than K^s because the F-pure threshold is invariant under scalar multiplication, i.e. under scaling of the b_i's, and because we avoid defining the F-pure threshold on the zero polynomial.

Specifically, we would like to see which regions in $\mathbb{P}^{s-1}$ obtain the same value under FT and how FT can be used to stratify $\mathbb{P}^{s-1}$. By adopting this approach we are, in fact, computing the F-pure threshold of all polynomials $f \in K[x_1, ..., x_t]$ supported by any subset of the monomials $\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}$ since we are allowing some of the c_i's to be 0. Nevertheless, it might be simpler to separate the case where we specialize one of the b's to be 0 and just analyze a different matrix, i.e. with one less column.

Semicontinuity ([MY09, Theorem 5.1]) is used to show that the image FT cannot contain a strictly decreasing sequence of values. Further, [BMS08, Proposition 3.8] proves that the image of FT contains only finitely many numbers. However, our goal is to give an *explicit* description of the regions of $\mathbb{P}^{s-1}$ sharing the same value under FT, as well as a constructive procedure to find them. This goal is achieved in **Theorem VI.22** and **Remark VI.23**, after assuming certain technical conditions we describe next (the actual assumption is **Conjecture VI.21**).

6.2 Computing $FT(f)$ Using Sequences

Let f be a polynomial as in the **Setup**, with indeterminate coefficients. Let N be a positive integer, and let $\boldsymbol{x}^{\boldsymbol{v}}$ be a monomial, where $\boldsymbol{v} \in \mathbb{Z}^t_{\geq 0}$ is the multiexponent. We denote by

$$C\{N, \boldsymbol{x}^{\boldsymbol{v}}\}$$

the coefficient of the monomial $\boldsymbol{x}^{\boldsymbol{v}}$ in f^N. For a generic polynomial, $C\{N, \boldsymbol{x}^{\boldsymbol{v}}\}$ is a polynomial in the b's. Note that $C\{N, \boldsymbol{x}^{\boldsymbol{v}}\}$ is 0 if $\boldsymbol{x}^{\boldsymbol{v}}$ is absent from f^N. When we specialize f or even just plug in some $c \in K$ instead of some b_i, the value of the new coefficient $C\{N, \boldsymbol{x}^{\boldsymbol{v}}\}$ is the value we get form specializing the generic coefficient in the same way. Recall from **Lemma III.2** (with the notation (II.9.2)) that if $C\{N, \boldsymbol{x}^{\boldsymbol{v}}\}$ is non-zero and $\max \boldsymbol{v} < p^e$ for some e, then we get that N/p^e is a lower bound of $FT(f)$, i.e. $N/p^e < FT(f)$.

Definition VI.2 (**Monomial Sequence**)**.** Let f be as in the **Setup**, possibly after specializing. Consider a sequence of integer powers and monomials:

$$\mathcal{T} := (N_1, \boldsymbol{x}^{\boldsymbol{v}_1}), (N_2, \boldsymbol{x}^{\boldsymbol{v}_2}), ..., (N_i, \boldsymbol{x}^{\boldsymbol{v}_i}), ... \tag{VI.2.1}$$

Let e_i be the minimal power of p such that

$$\max \boldsymbol{v}_i < p^{e_i}, \text{ (i.e. if the coefficient of } \boldsymbol{v}_i \text{ in } f^{N_i} \text{ is non-zero, then } f^{N_i} \notin \mathfrak{m}^{[p^{e_i}]})$$

We say that $\mathcal{T}$ is a *monomial sequence* if the integers are strictly increasing, $N_1 < N_2 < ... < N_i < ...$, and if the following rational numbers form a non-decreasing sequence:

$$\frac{N_1}{p^{e_1}} \leq \frac{N_2}{p^{e_2}} \leq ... \leq \frac{N_i}{p^{e_i}} \leq ...$$

Note that a monomial sequence $\mathcal{T}$ gives rise to a sequence of coefficients:

$$C\{\mathcal{T}\} = C\{N_1, \boldsymbol{x}^{\boldsymbol{v}_1}\}, C\{N_2, \boldsymbol{x}^{\boldsymbol{v}_2}\}, ..., C\{N_i, \boldsymbol{x}^{\boldsymbol{v}_i}\}, ...$$

In addition, it give rise to a non-decreasing sequence of possible lower bounds for $FT(f)$:

$$B\{\mathcal{T}\} = \frac{N_1}{p^{e_1}}, \frac{N_2}{p^{e_2}}, ..., \frac{N_i}{p^{e_i}}, ...$$

where $\frac{N_i}{p^{e_i}}$ is a lower bound if the relevant coefficient $C\{N_i, \boldsymbol{x}^{\boldsymbol{v}_i}\}$ is non-zero. Let us denote:

$$\overline{\mathcal{T}} := \sup B\{\mathcal{T}\}$$

Definition VI.3 (**Lower Approximating Sequence**)**.** Let f be as in the **Setup**, possibly after specializing. Consider a monomial sequence:

$$\mathcal{T} = (N_1, \boldsymbol{x}^{\boldsymbol{v}_1}), (N_2, \boldsymbol{x}^{\boldsymbol{v}_2}), ..., (N_i, \boldsymbol{x}^{\boldsymbol{v}_i}), ... \tag{VI.3.1}$$

The sequence $\mathcal{T}$ gives rise to a sequence of coefficients:

$$C\{\mathcal{T}\} = C\{N_1, \boldsymbol{x}^{\boldsymbol{v}_1}\}, C\{N_2, \boldsymbol{x}^{\boldsymbol{v}_2}\}, ..., C\{N_i, \boldsymbol{x}^{\boldsymbol{v}_i}\}, ...$$

and to a non-decreasing sequence rational numbers:

$$B\{\mathcal{T}\} = \frac{N_1}{p^{e_1}}, \frac{N_2}{p^{e_2}}, ..., \frac{N_i}{p^{e_i}}, ...$$

We say that $\mathcal{T}$ is a *lower approximating sequence* if $C\{\mathcal{T}\}$ is not eventually zero (i.e. for any $L \in \mathbb{N}$ there exists $l > L$ such that $C\{N_l, \boldsymbol{x}^{\boldsymbol{v}_l}\} \neq 0$). Note that in such case,

$$\overline{\mathcal{T}} \leq FT(f)$$

Remark VI.4. Consider again the **Setup**, without specializing. Let $\mathcal{T}$ be a lower approximating sequence for $FT(f)$. Notice that $C\{\mathcal{T}\}$ is a sequence of polynomials in the b's. If we specialize f, we specialize accordingly $C\{\mathcal{T}\}$, which now may or may not be eventually zero. That is, after specialization, $\mathcal{T}$ may not be a lower approximation sequence anymore. The reverse direction is impossible: if $\mathcal{T}$ is not a lower approximating sequence for f, it cannot become one after specializing.

Proposition VI.5. Let f be as in the **Setup**, possibly after specializing. Then there exists a lower approximating sequence $\mathcal{T}$ such that $\overline{\mathcal{T}} = FT(f)$.

Proof. Recall **Definition II.1** and its notation. For a positive integer e, let $N_e := \nu_{(f)}(p^e) = \max\{N \mid f^N \notin \mathfrak{m}^{[p^e]}\}$. That is, if we raise f to the power of N_e, we can find a monomial $\boldsymbol{x}^{\boldsymbol{v}_e}$ with a non-zero coefficient such that $\max \boldsymbol{v}_e < p^e$. So Let

$$\mathcal{T} = (N_1, \boldsymbol{x}^{\boldsymbol{v}_1}), (N_2, \boldsymbol{x}^{\boldsymbol{v}_2}), ..., (N_i, \boldsymbol{x}^{\boldsymbol{v}_i}), ...$$

The sequence $C\{\mathcal{T}\}$ contains only non-zero elements and due to **Discussion II.2**, $B\{\mathcal{T}\}$ is non-decreasing. So $\mathcal{T}$ is a lower approximating sequence. By definition $\overline{\mathcal{T}} = FT(f)$. □

We call a lower approximating sequence with $\overline{\mathcal{T}} = FT(f)$, an *approximating sequence*. We get the following immediate corollary:

Corollary VI.6. Let f be as in the **Setup**, possibly after specializing. Then $\sup \overline{\mathcal{T}}$ over all lower approximating sequences $\mathcal{T}$ is exactly $FT(f)$. Moreover, it is achieved by some approximating sequence $\mathcal{T}$, i.e. for this sequence $\overline{\mathcal{T}} = FT(f)$.

Discussion VI.7. Given a polynomial, it is not hard to find a monomial sequence of $(N_i, \boldsymbol{x}^{\boldsymbol{v}_i})$, you can even do it somewhat arbitrarily. The hard part is first, to make sure it is a lower approximating one — that the coefficients are non-zero eventually; second, that it is an *approximating* one — how can you tell that you have the best lower bound possible? Enter Schur Compliance.

6.3 Schur Compliance

Definition VI.8 (**Schur Compliance**)**.** Let f be as in the **Setup**, possibly after specializing. Let $\boldsymbol{v}$ be the multiexponent corresponding to $\mathbf{x}^{\boldsymbol{v}}$ in f^N. Let $U_N \subset \mathbb{Z}^s_{\geq 0}$ be the set of vectors $\mathbf{k}$ such that $M\mathbf{k} = \boldsymbol{v}$ and with $|\mathbf{k}| = N$ while $\binom{N}{\mathbf{k}} \neq 0$. For any

vector $\mathbf{k}$ of non-negative integers, we denote $\{\mathbf{k}_e\}_{e=0}^{\infty}$ the p-expansion of its entries. Note that all but finitely many are the zero vectors. We say that the triple $(M, \boldsymbol{v}, N)$ is *Schur Compliant* if

$$\text{for all } \mathbf{k}, \mathbf{k}' \in U_N \text{ and for all } e \in \mathbb{Z}_{\geq 0},\ M\mathbf{k}_e = M\mathbf{k}'_e$$

Remark VI.9. Note that **Definition VI.8** does not depend on the coefficients of f. It is a property of the triple $(M, \boldsymbol{v}, N)$ thus can be tested on the supporting monomials of f. Any specialization will not affect this property.

We are now ready to generalize the elegant and useful **Schur's Congruence** we encountered in the context of Deuring polynomials:

Proposition VI.10 (**Generalized Schur's Congruence**)**.** Let f be as in the **Setup**, possibly after specializing. Fix a positive integer N. Let $\boldsymbol{v}$ be the multiexponent corresponding to $\mathbf{x}^{\boldsymbol{v}}$ in f^N and assume that $(M, \boldsymbol{v}, N)$ is Schur Compliant. Let $U = U_N \subset \mathbb{Z}_{\geq 0}$ be the set of vectors $\mathbf{k}$ such that $M\mathbf{k} = \boldsymbol{v}$ and with $|\mathbf{k}| = N$ while $\binom{N}{\mathbf{k}} \neq 0$. Fix one vector $\mathbf{k} \in U$ with p-expansion $\mathbf{k}_0 + \mathbf{k}_1 p + ... + \mathbf{k}_e p^e$. Denote $M\mathbf{k}_i = \boldsymbol{v}_i$ and $N = n_0 + n_1 p + ... + n_e p^e$. Denote the coefficient of the monomial $\mathbf{x}^{\boldsymbol{v}}$ in f^N as $C\{N, \mathbf{x}^{\boldsymbol{v}}\}$. Then:

$$C\{N, \mathbf{x}^{\boldsymbol{v}}\} = C\{n_0, \mathbf{x}^{\boldsymbol{v}_0}\} \cdot C\{n_1, \mathbf{x}^{\boldsymbol{v}_1}\}^p \cdots C\{n_e, \mathbf{x}^{\boldsymbol{v}_e}\}^{p^e}$$

Proof. Due to Schur compliance, $\forall \mathbf{k} \in U$, $M\mathbf{k}_i = \boldsymbol{v}_i$. Therefore the right hand side is independent of the $\mathbf{k} \in U$ we pick to compute the $\boldsymbol{v}_i$'s. Write the monomials of f as $\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}$. Replace the coefficients of f by indeterminants $b_1, .., b_s$ and get a new polynomial:

$$f = b_1 \boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + b_s \boldsymbol{x}^{\boldsymbol{\mu}_s}$$

We shall prove the statement for this generic polynomial and the statement will be true once we specialize, i.e. plug in the actual coefficient of the original f. So, the

left hand side is the following polynomial in $b_1, ..., b_s$:

$$\sum_{\mathbf{k}\in\mathbb{Z}^s_{\geq 0}, M\mathbf{k}=\boldsymbol{v}, |\mathbf{k}|=N} \binom{N}{\mathbf{k}} \mathbf{b}^{\mathbf{k}}$$

The right hand side is the following polynomial in $b_1, ..., b_s$:

$$\left(\sum_{\mathbf{k}\in\mathbb{Z}^s_{\geq 0}, M\mathbf{k}=\boldsymbol{v}_0, |\mathbf{k}|=n_0} \binom{n_0}{\mathbf{k}} \mathbf{b}^{\mathbf{k}}\right) \left(\sum_{\mathbf{k}\in\mathbb{Z}^s_{\geq 0}, M\mathbf{k}=\boldsymbol{v}_1, |\mathbf{k}|=n_1} \binom{n_1}{\mathbf{k}} \mathbf{b}^{\mathbf{k}}\right)^p \cdots \left(\sum_{\mathbf{k}\in\mathbb{Z}^s_{\geq 0}, M\mathbf{k}=\boldsymbol{v}_e, |\mathbf{k}|=n_e} \binom{n_e}{\mathbf{k}} \mathbf{b}^{\mathbf{k}}\right)^{p^e}$$

We want to observe that these two polynomials (in the b's) are the same and we shall do it by comparing the integer coefficient of each monomial of the form $\mathbf{b}^{\mathbf{k}}$. Fix one monomial $\mathbf{b}^{\mathbf{k}}$ from the left hand side with a non-zero coefficient. Write the p expansion of $\mathbf{k}$ as $\mathbf{k}_0 + \mathbf{k}_1 p + ... + \mathbf{k}_e p^e$. Since $\binom{N}{\mathbf{k}} \neq 0$, we have that $|\mathbf{k}_i| = n_i$, and by **Schur Compliance**, $M\mathbf{k}_i = \boldsymbol{v}_i$. So we get $\mathbf{b}^{\mathbf{k}}$ in the right hand side as well, and the integer coefficient is the same due to **Lucas's Theorem**(**Theorem III.7**). For the reverse direction we do not need Schur compliance: Fix $\mathbf{k}_0$ for the first parenthesis, $\mathbf{k}_1$ from the next parenthesis, and so on until we fix $\mathbf{k}_e$. Then $\mathbf{k} = \mathbf{k}_0 + \mathbf{k}_1 p + ... + \mathbf{k}_e p^e$ must show up in the left hand side due to linearity:

$$M\mathbf{k} = M(\mathbf{k}_0 + \mathbf{k}_1 p + ... + \mathbf{k}_e p^e) = M\mathbf{k}_0 + M\mathbf{k}_1 p + ... + M\mathbf{k}_e p^e = \boldsymbol{v}_0 + \boldsymbol{v}_1 p + ... + \boldsymbol{v}_e p^e = \boldsymbol{v}$$

Note that since $0 \leq n_0, n_1, ..., n_e \leq p-1$, then the entries of each $\mathbf{k}_i$ must be between 0 and $p-1$, otherwise the sum of entries exceeds n_i. This shows that $\mathbf{k}_0 + \mathbf{k}_1 p + ... + \mathbf{k}_e p^e$ is indeed the p-expansion of $\mathbf{k}$. The integer coefficient is the same due to **Lucas's Theorem**(**Theorem III.7**). □

Remark VI.11. Note that if M is injective, every vector $\boldsymbol{v}$ is easily seen to be Schur compliant. In this case, the coefficients are of the form $c \cdot \boldsymbol{b}^{\boldsymbol{v}}$ where c is some multinomial coefficient.

Discussion VI.12 (**Lower Schur Sequences, Basic Coefficients**)**.** If we are lucky to identify that **Generalized Schur's Congruence** applies on enough triples $(M, \boldsymbol{x}^{\boldsymbol{v}}, N)$, we can compute the F-pure threshold of a polynomial more easily by identifying lower approximating sequences. Specifically, suppose we are given a sequence $\mathcal{T}$ as in (VI.3.1). Suppose that $B\{\mathcal{T}\}$ is non-decreasing and we would like to test if $\mathcal{T}$ is indeed a lower approximating sequence. In order to do that, we need to verify that $C\{\mathcal{T}\}$ is not eventually zero so, in general, we need to check infinitely many coefficients. This is not the case if $\mathcal{T}$ is composed of monomials and corresponding powers of f which are Schur Compliant (in which case, we call $\mathcal{T}$ a *lower Schur sequence*). If so, we can use **Generalized Schur's Congruence** and realize that all the coefficients are simply products of coefficients of the form $C\{n_i, \boldsymbol{x}^{\boldsymbol{v}_i}\}$, with $0 \leq n_i \leq p-1$ and $\boldsymbol{v}_i$ are all multiexponents occurring in f^{n_i}. So identify the set of:

$$\mathcal{C} = \{C\{n, \boldsymbol{x}^{\boldsymbol{v}}\} \neq 0 \mid 0 \leq n \leq p-1\} \subset K[b_1, ..., b_s]$$

We call them the *Basic Coefficients*, and we have finitely many of them. We denote them by

$$\pi_1, ..., \pi_m \in K[b_1, ..., b_s]$$

Note that the basic coefficients are homogeneous polynomials in $b_1, ..., b_s$.

Definition VI.13. [**M-Basic Closed Set**] Let f be as in the **Setup** without specializing. Recall that M denotes the splitting matrix. Denote $\pi_1, ..., \pi_m \in K[b_1, ..., b_s]$ as the basic coefficients. For some $\alpha \in \{0, 1\}^m$, We call $\boldsymbol{\pi}^{\boldsymbol{\alpha}}$ a *squarefree monomial* in the π's. We say that the closed projective subvariety $X \subset \mathbb{P}^{s-1}$ is an *M-basic closed set* if X can be defined as a vanishing set of an ideal generated by squarefree monomials in the basic coefficients. Note that we define $\mathbb{P}^{s-1} = \mathbb{V}(0)$ and $\emptyset = \mathbb{V}(1)$ to be M-basic closed sets as well.

Remark VI.14. Since we have a finite number of basic coefficients, we have a finite number of squarefree monomials in the basic coefficients and thus, a finite number of M-basic closed sets. Moreover, this collection is easily seen to be closed under unions and intersections.

Remark VI.15. Let f be as in the **Setup** and let $\pi_1, ..., \pi_m$ be the basic coefficients. Then the number of M-basic closed sets is exactly the number of ideals generated by squarefree monomials in the π's, excluding the monomial ideal $(1) = (\boldsymbol{\pi}^{\mathbf{0}})$ (corresponding to the empty set). If there are no algebraic relations among the π's (i.e. $K[\pi_1, ..., \pi_m]$ is a polynomial ring) then the number of squarefree monomial ideals is easily seen to be equal to the number of *antichains* in the partially ordered set of the squarefree monomials (e.g. use primary decomposition). The number of antichains is the m^{th} Dedekind number (this is a standard enumeration of the squarefree ideals, see [Slo73], [Com74, §7.2] for details.) The first numbers, starting from $m = 1$, are[1]:

$$3, 6, 20, 168, 7581, 7828354, 2414682040998, 56130437228687557907788$$

Asymptotic bounds can be found in [Kor81]. We conclude that the number of M-basic closed sets is bounded by the relevant Dedekind number (minus 1, if we want to be accurate). Note that this bound can be far from optimal as there might be algebraic relations among the basic coefficient. (See also **Remark VI.24** later). For a quick computation, one can use the following bound: given m basic coefficients, the number of distinct squarefree monomials, excluding $1 = \boldsymbol{\pi}^{\mathbf{0}}$, is $2^m - 1$; so the number of possible sets of generators is 2^{2^m-1}, giving an upper bound for the number of squarefree monomial ideals. This bound is far from optimal since we are counting multiple sets of generators for the same ideals but it is easy to compute.

[1] See sequence A000372 in https://oeis.org/

Proposition VI.16. Let f be as in the **Setup** without specializing. Let $\mathcal{T}$ be a lower Schur sequence. Then there exists an M-basic closed set X_T with the following property: $\mathcal{T}$ is a lower Schur sequence under the specialization $(c_1, ..., c_s) \in \mathbb{P}^{s-1}$, if and only if $(c_1, ..., c_s) \in \mathbb{P}^{s-1} - X_T$.

Proof. Scan the coefficients in $C\{\mathcal{T}\}$ (it is not eventually zero since it is given that $\mathcal{T}$ is a lower approximating sequence when f is not specialized). Let $X_i \subset \mathbb{P}^{s-1}$ denote the vanishing set of the i^{th} coefficient in $C\{\mathcal{T}\}$. Apply **Generalized Schur's Congruence**(**Proposition VI.10**) and conclude that X_i is an M-basic closed set. $C\{\mathcal{T}\}$ is eventually zero exactly when we specialize at the set:

$$X_T := \bigcup_{j=1}^{\infty} \bigcap_{i=j}^{\infty} X_i,$$

which is an M-basic closed set as seen in **Remark VI.14**. □

Remark VI.17. For any lower approximating sequence $\mathcal{T}$, we can define $X_{\mathcal{T}} \subset \mathbb{P}^{s-1}$ as in the above proposition: $\mathcal{T}$ is a lower approximating sequence under the specialization $(c_1, ..., c_s) \in \mathbb{P}^{s-1}$, if and only if $(c_1, ..., c_s) \in \mathbb{P}^{s-1} - X_T$. However if $\mathcal{T}$ is not a lower Schur sequence, $X_{\mathcal{T}}$ may or may not be an M-basic closed set.

Example VI.18. We demonstrate the concept of **Schur Compliance**(**Definition VI.8**) by addressing the family of polynomials in **Theorem V.7** with $b = c = 1$. So consider the polynomial

$$f = b_1x^3y + b_2x^2y^2 + b_3xy^3 \in K(b_1, b_2, b_3)[x, y],$$

where b_1, b_2, b_3 are indeterminants and K is a field of chracteristic $p > 2$. We are in fact addressing a bigger family of polynomials, since in **Theorem V.7** we are specializing $b_1 = 1, b_2 = (1 + b_3)$. First, let us show that $(M, \boldsymbol{x}^{[2N,2N]})$ is Schur

compliant, where:

$$M = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix}.$$

Solving $M\mathbf{k} = [2N, 2N]^{Tr}$ yields:

$$\mathbf{k} = \begin{bmatrix} 0 \\ N \\ 0 \end{bmatrix} + r \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix}$$

Note the r must be an integer between 0 and $N/2$. Let us write the p-expansion of N, r and $\mathbf{k}$, where the middle entry in the expansion of $\boldsymbol{k}$ will be computed shortly:

$$\begin{aligned} N = \;& n_0 + && n_1 p + && \ldots + && n_e p^e \\ r = \;& r_0 + && r_1 p + && \ldots + && r_e p^e \\ \mathbf{k} = \;& \begin{bmatrix} r_0 \\ ? \\ r_0 \end{bmatrix} + && \begin{bmatrix} r_1 \\ ? \\ r_1 \end{bmatrix} p + && \ldots && \begin{bmatrix} r_e \\ ? \\ r_e \end{bmatrix} p^e \end{aligned}$$

Since $|\mathbf{k}_i| = n_i$ and the digits must not carry, we must have:

$$\begin{aligned} N = \;& n_0 + && n_1 p + && \ldots + && n_e p^e \\ r = \;& r_0 + && r_1 p + && \ldots + && r_e p^e \\ \mathbf{k} = \;& \begin{bmatrix} r_0 \\ n_0 - 2r_0 \\ r_0 \end{bmatrix} + && \begin{bmatrix} r_1 \\ n_1 - 2r_1 \\ r_1 \end{bmatrix} p + && \ldots && \begin{bmatrix} r_e \\ n_e - 2r_e \\ r_e \end{bmatrix} p^e. \end{aligned}$$

Ergo,

$$\mathbf{k}_i = \begin{bmatrix} 0 \\ n_i \\ 0 \end{bmatrix} + r_i \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix},$$

so

$$M\mathbf{k}_i = M\begin{bmatrix} 0 \\ n_i \\ 0 \end{bmatrix} + r_i \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} = M\begin{bmatrix} 0 \\ n_i \\ 0 \end{bmatrix} = \begin{bmatrix} 2n_i \\ 2n_i \end{bmatrix} = \boldsymbol{v}_i.$$

The last computation is valid for any choice of r, as Schur compliance requires.

Now, that Schur compliance has been established for vectors of the form $[2N, 2N]^{Tr}$, let us suggest the following sequence. Denote:

$$N_e = \frac{p^e - 1}{2},\ 2N_e < p^e,$$

and create a sequence

$$\mathcal{T} = \{(N_e, \boldsymbol{x}^{(2N_e, 2N_e)})\}_e.$$

We compute that:

$$B\{\mathcal{T}\} = \left\{\frac{1}{2}\frac{p^e - 1}{p^e}\right\}_e,\ \text{thus } \overline{\mathcal{T}} = \frac{1}{2}$$

Now, observe that:

$$C\{\mathcal{T}\} = C\left\{\frac{p^e - 1}{2}, \boldsymbol{x}^{(2N_e, 2N_e)}\right\}_e.$$

Apply **Generalized Schur's Congruence** and observe that all of these coefficients are products of the same basic coefficient:

$$\pi = C\left\{\frac{p-1}{2}, \boldsymbol{x}^{(2N_1, 2N_1)}\right\},$$

and thus

$$X_T = \mathbb{V}(\pi)$$

Therefore, for any specialization, as long as π is non-zero, we have a lower bound of $\frac{1}{2}$ for $FT(f)$. In the specific case of **Theorem V.7**, $\pi = H\left\{\frac{p-1}{2}\right\}$. However this example is more general, and π is a polynomials in b_1, b_2, b_3, with the property of described in **Generalized Schur's Congruence**. For example, for $p = 5$ one gets:

$$\pi = b_2^2 + 2b_1b_3$$

Example VI.19. Let us give an example for a triple $(M, \boldsymbol{x}^{\boldsymbol{v}}, N)$ that is *not* Schur compliant over K with char$K = 5$. Take the same matrix:

$$M = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix}.$$

Let $N = 17$, and let:

$$\boldsymbol{v} = \begin{bmatrix} 36 \\ 32 \end{bmatrix}.$$

Among the preimages of $\boldsymbol{v}$ we can find:

$$\mathbf{k} = \begin{bmatrix} 7 \\ 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} + 5 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix},$$

and

$$\mathbf{k} = \begin{bmatrix} 6 \\ 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix} + 5 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}.$$

However,

$$M \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ 2 \end{bmatrix} \neq \begin{bmatrix} 11 \\ 17 \end{bmatrix} = M \begin{bmatrix} 1 \\ 2 \\ 4 \end{bmatrix},$$

and also

$$M \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 6 \\ 6 \end{bmatrix} \neq \begin{bmatrix} 5 \\ 3 \end{bmatrix} = M \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}.$$

6.4 Stratification

We need the following technical lemma to deduce that $FT : \mathbb{P}^{s-1} \to \mathbb{Q}$ obtains a maximal value on M-basic closed sets.

Lemma VI.20. Let $K = \overline{K}$ be an algebraically closed field of prime characteristic $p > 0$. Let $b_1, .., b_s$ be indeterminates. Fix q homogeneous polynomials, $\pi_1, ..., \pi_q \in K[b_1, .., b_s]$, defining a non empty subset:

$$X = \mathbb{V}(\pi_1, ..., \pi_q) \subset \mathbb{P}^{s-1}.$$

Set $R = K[b_1, ..., b_s]/\mathrm{Rad}(\pi_1, ..., \pi_q)$ with the convention that when $q = 0$, $R = K[b_1, .., b_s]$. Fix s monomials $\boldsymbol{x}^{\boldsymbol{\mu}_1}, ..., \boldsymbol{x}^{\boldsymbol{\mu}_s}$, and let

$$f = b_1\boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + b_s\boldsymbol{x}^{\boldsymbol{\mu}_s} \in R[x_1, .., x_t].$$

For a point $(c_1, .., c_s) \in X$, we denote:

$$g = c_1\boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + c_s\boldsymbol{x}^{\boldsymbol{\mu}_s} \in K[x_1, ..., x_t],$$

that is, the polynomial we get from f after specializing at $(c_1, .., c_s)$. Then the following are satisfied:

1. An approximating sequence of g, $\mathcal{T}$, exists and gives rise to a lower approximating sequence of f, $\mathcal{T}'$, with $\overline{\mathcal{T}} = \overline{\mathcal{T}'}$.
2. $FT(g) \leq FT(f)$.
3. There exists a polynomial

   $$h = d_1\boldsymbol{x}^{\boldsymbol{\mu}_1} + ... + d_s\boldsymbol{x}^{\boldsymbol{\mu}_s} \in K[x_1, ..., x_t], \text{ where } (d_1, ..., d_s) \in X,$$

   such that $FT(f) = FT(h)$.
4. The function $FT : \mathbb{P}^{s-1} \to \mathbb{Q}$, as defined in the **Setup**(**Discussion VI.1**), obtains a maximum on X, i.e. there exists $(d_1, ..., d_s) \in X$ such that $FT(d_1, ..., d_s)$ is the maximum value the function FT obtains on X.
5. For each M-basic closed set, the function FT obtains a maximum, where M is the splitting matrix of the support of f.

Proof. Note that the computation of $FT(f)$ is done over $R[x_1, ..., x_t]$ where the computation of $FT(g)$ is done over $K[x_1, .., x_t]$.

1. Apply **Proposition VI.5** to find an approximating sequence of g, call it $\mathcal{T}$. Use the same underlying monomial sequence to construct a monomial sequence for f, call it $\mathcal{T}'$. With the notation from **Proposition VI.5**, observe that the sequence of powers N_i, the monomials $\boldsymbol{x}^{\boldsymbol{v}_i}$ and bounds $B\{\mathcal{T}\} = B\{\mathcal{T}'\}$ do not change. The only difference is that $C\{\mathcal{T}'\}$ is a sequence of coefficient taken from R, while $C\{\mathcal{T}\}$ is a sequence of coefficients taken from K. Note that $C\{\mathcal{T}\}$ is obtained from $C\{\mathcal{T}'\}$ by specializing in $(c_1, ..., c_s)$. Because $\mathcal{T}$ is an approximating sequence for g, $C\{\mathcal{T}\}$ is not eventually 0, and therefore $C\{\mathcal{T}'\}$ is not eventually 0 as well, making $\mathcal{T}'$ a *lower* approximating sequence for f.

2. Use $\mathcal{T}'$ from above and notice that:

$$FT(g) = \overline{\mathcal{T}} = \overline{\mathcal{T}'} \leq FT(f)$$

3. Apply **Proposition VI.5** on f to find an approximating sequence $\mathcal{Q}$ of f, i.e. the sequence of coeffiennt $C\{\mathcal{Q}\}$ is not eventually 0 in R and $\overline{\mathcal{Q}} = FT(f)$. Let $X_{\mathcal{Q}} \subset X \subset \mathbb{P}^{s-1}$ be the set of s-tuples of coefficients that make $C\{\mathcal{Q}\}$ eventually zero once specialized there. If we can prove that $X_{\mathcal{Q}} \subsetneq X$ we are done: we can choose $(d_1, ..., d_s) \in X - X_{\mathcal{Q}}$, specialize there to get a polynomial h and a lower approximating sequence $\mathcal{T}$ with $FT(f) = \overline{T} \leq FT(h)$, which must be $FT(h)$ by (2.). For the sake of contradiction, assume $X = X_{\mathcal{Q}}$. In this case, at every point $(c_1, .., c_s) \in X$, the sequence of coefficients $C\{\mathcal{Q}\}$ is eventually zero after specializing. However, $C\{\mathcal{Q}\}$ consists of homogeneous regular functions on X and therefore $C\{\mathcal{Q}\}$ is eventually zero in R, prior to any specialization, a contradiction.

4. From the previous statement we get a polynomial h, with coefficients in X, that obtains the maximal possible F-pure threshold value, $FT(f)$.
5. Recall from **Definition VI.13** that any M-basic closed set is defined by a squarefree monomial ideal in the basic coefficient, so simply apply (4.) on that ideal.

□

Our main result is proven later under the following conjecture:

Conjecture VI.21. Let f be as in the **Setup**,where the b's are taken from any field (so can indeterminates or have algebraic relations between them). Then there exists a lower Schur sequence $\mathcal{T}$ with $\overline{\mathcal{T}} = FT(f)$. We simply call such $\mathcal{T}$ a *Schur sequence*.

This conjecture is true for any f where the support gives rise to an injective splitting matrix (see **Remark VI.11**). It is also evidently true for the families of polynomials we encountered in previous chapters (after partial specializing): the elliptic curve case, where the supporting monomials are $y^2z, x^3, x^2z, xz^2 \in K[x,y,z]$, and the four $\mathbb{P}^1$ roots case, where the supporting monomials are $x^3y, x^2y^2, xy^3 \in K[x,y]$.

The next theorem is known in general due to [BMS08, Proposition 3.8] and [MY09, Theorem 5.1], but we offer a constructive proof when assuming **Conjecture VI.21**:

Theorem VI.22. *Recall the* ***Setup****. Recall the function* $FT : \mathbb{P}^{s-1} \to \mathbb{Q}$ *where* $FT(c_1, ..., c_s)$ *is the* F*-pure threshold of the polynomial* f *after specializing* $(b_1, ..., b_s) = (c_1, ..., c_s)$*. Assume* ***Conjecture VI.21*** *is true. Then:*

1. *FT obtains finitely many distinct values,* $r_1 > r_2 > ... > r_m \in \mathbb{Q}$.
2. $FT^{-1}(r_1)$ *is an open dense set of* $\mathbb{P}^{s-1}$*. For* $i = 2, ..., m$, $FT^{-1}(r_i)$ *is a Zariski open set of an* M*-basic closed set* $\{FT < r_{i-1}\}$.

3. *If we have a total of q basic coefficients, then the number of values obtained by FT is bounded by q^{th} Dedekind number.*

Proof. Start with f as in the **Setup**. Collect all lower Schur sequences $T = \{\mathcal{T}_i\}_I$. This collection includes all the lower Schur sequences for any specialization, as explained in **Remark VI.4**. Due the **Lemma VI.20**, the collection T contains sequences that obtains the the maximal value the function FT obtains on $\mathbb{P}^{s-1}$, a value which we denote as r_1. Denote them as

$$T_1 = \{\mathcal{T} \in T \mid \overline{\mathcal{T}} = r_1\}.$$

For each $\mathcal{T} \in T_1$, observe at $X_{\mathcal{T}}$ (as denoted in **Proposition VI.16**), an M-basic closed set. Let X_1 be their intersection, which is another M-basic closed set. Note that away from X_1, we have at least one Schur sequence $\mathcal{T}$, i.e. such that $C\{\mathcal{T}\}$ is not eventually 0, whereas in X_1 all sequences are no longer lower approximating ones. Ergo, away from X_1, the value of $FT(f)$ after specializing $(b_1, ..., b_s) = (c_1, ..., c_s) \in \mathbb{P}^{s-1} - X_1$, is r_1. Notice that

$$X_1 = \{FT < r_1\}$$

If X_1 is not empty, we can repeat the above procedure. Due to the **Conjecture VI.21** and **Lemma VI.20**, we keep looking at the collection of all lower Schur sequences $T - T_1$, and identify the ones with the maximal $\overline{\mathcal{T}}$, and denote that maximal value as r_2. We then define

$$T_2 = \{\mathcal{T} \in T - T_1 \mid \overline{\mathcal{T}} = r_2\}.$$

We use the same considerations to find an M-basic closed set X_2' defined as the intersection of all $X_{\mathcal{T}}$ for $\mathcal{T} \in T_2$; observe that away from X_2' (inside X_1), we get the next biggest possible value of $FT(f)$, r_2. We then repeat the analysis for

$$X_2 = X_1 \cap X_2' = \{FT < r_2\},$$

and so on. In each step we get that the next biggest possible value of $FT(f)$ is achieved on the a Zariski dense open set of the an M-basic closed set $X_i \subset \mathbb{P}^{s-1}$, and we turn to analyze the complement. As each X_i is a distinct M-basic closed set, their number is bounded by the q^{th} Dedekind (see **Remark VI.15**). □

Remark VI.23. The proof above reveals a constructive way to identify the different regions of $\mathbb{P}^{s-1}$ sharing the same value under FT. First we identify all the basic coefficients, that is, the coefficients $C_i \neq 0$ in f^n with $1 \leq n \leq p-1$. Next, identify all the vanishing sets that can be described as unions and intersections of $\mathbb{V}(C_i)$. Then, it suffices to compute the F-pure threshold of one polynomial from each said vanishing sets. Finally, we can bundle up together all the regions with the same value under FT. This procedure can be easily programmed and terminates since we have only finitely many specialized polynomials to consider. (One can use the previously computed values of multinomial coefficients in the next steps of the process in order to speed up the computation; this technique is called "memoization").

Remark VI.24. The fact that the image of FT is finite can be derived from [BMS08, Proposition 3.8]. The reference suggests a bound that is dependent on p and on the degree of the polynomial f. Our bound is the q^{th} Dedekind number, where q is the number of basic coefficients. However, if we know exactly which of the basic coefficient should be considered in the computation of FT, we can take their number as q and then the bound is reduced. In the family of elliptic curves and in the family of bivariate polynomials with four distinct roots in $\mathbb{P}^1$, we demonstrated that we just need to consider one basic coefficient, $\pi = H\left\{\frac{p-1}{2}\right\}$. Thus we take $q = 1$ and then we have 2 different values of FT, where the first Dedekind number is 3.

Remark VI.25. In [BMS09, Conjecture 4.4], it is conjectured that the set of all

possible values of $FT(f)$ for $f \in K[x_1, ..., x_n]$ has the Ascending Chain Condition (ACC). Our **Conjecture VI.21** leads to an explicit way to compute the values of $FT(f)$ once we *fix the set of supporting monomials*. Can this explicit description be further used to shed more light on the ACC conjecture? Are the two conjectures related? See [Sat17] for recent development on the ACC for the F-pure threshold.

Example VI.26. As we mentioned before, when M is injective, all the lower approximating sequences are lower Schur sequences and therefore **Conjecture VI.21** applies, as well as **Theorem VI.22**. Since the basic coefficient are of the form of a scalar times a monomial in $b_1, ..., b_s$, we can explicitly compute all possible M-basic closed sets. There are simply determined by which of the b's are specialized to be 0 or not. For example, if we take $b_1x^2 + b_2x^3$, we get that the maximal F-pure threshold (either $5/6$ or $5/6(1 - 1/5p)$) is obtained away from $\mathbb{V}(b_1b_2)$, $1/2$ is obtain on $\mathbb{V}(b_1b_2) - \mathbb{V}(b_1)$ and that $1/3$ is obtained on $\mathbb{V}(b_1) - \mathbb{V}(b_2)$.

CHAPTER VII

Open Questions

We end this thesis by restating some questions that had arisen in our analysis.

1. In **Chapter II** we introduced **Monomial Ideal Reduction Algorithm** an the to "simplify" a monomial ideal while preserving its F-pure threshold. There are several "simplified" such ideals. How can we relate them to the original ideal?

2. Can the **Monomial Ideal Reduction Algorithm** be carried out without using linear programming to find $FT(M)$? Can its time complexity be improved?

3. Recall **Question I.2**: Let $f \in \mathbb{Z}[x_1, .., x_t]$, such that $f \in (x_1, ..., x_t)$. For any prime p, denote by f_p the natural image in $\mathbb{F}_p[x_1, ..., x_t]$. Let $\mathcal{P}$ be the set of all primes p such that $FT(f_p) = \text{lct}\,(f)$. Is it true that $\mathcal{P}$ is of infinite cardinality?

   This question is still open for many families of polynomials. For the family in **Chapter V**, this is reduced to **Question V.4**: Suppose $f = x^b y^b (x+y)^c (x+ay)^c \in \mathbb{Z}[x, y]$. Denote

   $$\mathcal{P} = \left\{ \text{all primes } p \;\middle|\; p \equiv 1 \pmod{b+c} \text{ and } H\left\{ \frac{c}{b+c}(p-1) \right\}(a) \not\equiv 0 \pmod{p} \right\}.$$

   Is it true that the cardinality of $\mathcal{P}$ is infinite?

   Can we answer this question more easily?

4. Let $P_n(x)$ be the Legendre polynomial of degree n. Denote

$$L_n(x) = \begin{cases} P_n(x), & \text{if } n \text{ is even;} \\ P_n(x)/x, & \text{if } n \text{ is odd} \end{cases}$$

Stieltjes conjectured in 1890 that L_n is irreducible over $\mathbb{Q}$ but only a few cases are known to be true (see [CH14]). This has implication on the behavior of roots of $H\{n\}$. To be more precise we conjecture the following over $\mathbb{C}$:

   (a) The only common factor of $H\{n\}, H\{m\}$, $n \neq m$, is $\lambda - 1$, which happens if and only if both m, n are odd.

   (b) If n is even, $H\{n\}$ is irreducible over $\mathbb{Q}$. If n is odd, $H\{n\}/(\lambda - 1)$ is irreducible over $\mathbb{Q}$.

5. In **Chapter V**, we concluded **Corollary V.5**, a property of the roots of Legendre polynomials over $\mathbb{F}_p$. Is it a new property or is there a reference to this statement in the vast literature on Legendre polynomials?

6. In the last chapter we proved how **Conjecture VI.21** helped to identify the stratification of the parameter space by the FT function. We identified a number of scenarios where the conjecture applies; does it always apply? Moreover, the M-basic closed sets in the coefficient space give rise to a very coarse topology of the coefficient space. It is interesting to further investigate the topological properties. Lastly, is there a connection between the ACC conjecture and our conjecture? See **Remark VI.25**.

APPENDIX

APPENDIX A

MATLAB Code for Monomial Ideal Algorithm

Here is the MATLAB code implementing the algorithm in **Discussion II.25**. Note that there are numerical considerations when equating two floating point numbers so the code is not guaranteed to be accurate and the result should be verified using theoretical considerations.

```
function M = invSubMatAlgo(M)
eps = 1E-5;
r2=0;
c2=0;
[r,c] = size(M);}
while and((r2+c2) < (r+c), (r+c) >2)
    M = eliminateDomination(M);
    [r,c] = size(M);
    [k, FTM, v, error] = betaFinder(M);
    if error
        disp('error in linprog')
        return
    end
```

```
    delrows = find(v<(1-eps)*ones(r,1));
    %%  adding ones as a rows ensures that the sum of entries is 0
    kernel = null([M;ones(1,c)],'r');
    [~,kerSize] = size(kernel);
    if kerSize > 0
        %% can use any linear combination of kernel vectors.
        k = boundaryVector(k,kernel(:,1));
    end
    delcols = find(k<eps*ones(c,1));
    M( delrows',:) = [];
    M( :,delcols') = []];
    [r2,c2] = size(M);
    if and(r+c == r2+c2, r2 ~= c2)
        M = eliminateDependentRows(M);
        [r2,c2] = size(M);
    end
end

function M = eliminateDependentRows(M)
isEliminateion = true;
while isEliminateion
    [M,isEliminateion] = eliminateDependentRow(M);
end

function [M,isEliminate] = eliminateDependentRow(M)
```

```
[r,~]=size(M);
rnk = rank(M);
isEliminate = false;
for rowCandidate = 1:r
    M2 = M;
    M2(rowCandidate,:)=[];
    rnk2 = rank(M2);
    if rnk2 == rnk
        M=M2;
        isEliminate = true;
        return
    end
end

function M2 = eliminateDomination(M)
M2 = eliminateDominatedRows(M);
M2 = eliminateDominatingdCols(M2);
[r,c] = size(M);
[r2,c2] = size(M2);
while r2+c2<r+c
    M = M2;
    M2 = eliminateDominatedRows(M);
    M2 = eliminateDominatingdCols(M2);
    [r,c] = size(M);
    [r2,c2] = size(M2);
```

```
end


function M2 = eliminateDominatingdCols(M)
[r,c]=size(M);
M2 = M;
for candidate = 1:c
    for i= 1:c
        if i == candidate
            continue
        else
            if sum(M(:,candidate) >= M(:,i)) == r
                M2(:,candidate) = [];
                return
            end
        end
    end
end


function M2 = eliminateDominatedRows(M)
[r,c]=size(M);
M2 = M;
for rowCandidate = 1:r
    for i= 1:r
        if i == rowCandidate
            continue
```

```
        else
            if sum(M(rowCandidate,:) <= M(i,:)) == c
                M2(rowCandidate,:) = [];
                return
            end
        end
    end
end


function  x = boundaryVector(k,kerVec)
if sum(kerVec)<0
    v = -kerVec;
else
    v = kerVec;
end
maxindex = -1;
maxVal = [];
startFlag = true;
[s, ~] = size(k);
for i = 1:s
    if v(i) ~= 0
        if startFlag
            startFlag = false;
            maxVal = -k(i)/v(i) - 1;
        end
```

```
        if maxVal < -k(i)/v(i)
            maxindex = i;
            maxVal = -k(i)/v(i);
        end
    end
end
x=(k+maxVal.*v);



function [x, FTM, betaVector, error] = betaFinder(M)
[r,c] = size(M);
[x,mFTM,exit,~] = linprog(-ones(1,c),M,ones(r,1),[],[],zeros(c,1),[]);
error = (exit < 1);
FTM = -mFTM;
betaVector = M*x;
```

BIBLIOGRAPHY

BIBLIOGRAPHY

[AO09] Ravi P. Agarwal and Donal O'Regan, *Ordinary and partial differential equations*, Universitext, Springer, New York, 2009, With special functions, Fourier series, and boundary value problems. MR 2467288

[BFS13] Angélica Benito, Eleonore Faber, and Karen E. Smith, *Measuring singularities with Frobenius: the basics*, Commutative algebra, Springer, New York, 2013, pp. 57–97.

[BM04] John Brillhart and Patrick Morton, *Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial*, J. Number Theory **106** (2004), no. 1, 79–111. MR 2049594

[BMS08] Manuel Blickle, Mircea Mustaţă, and Karen E. Smith, *Discreteness and rationality of F-thresholds*, Michigan Math. J. **57** (2008), 43–61, Special volume in honor of Melvin Hochster. MR 2492440

[BMS09] ———, *F-thresholds of hypersurfaces*, Trans. Amer. Math. Soc. **361** (2009), no. 12, 6549–6565.

[BS15] Bhargav Bhatt and Anurag K. Singh, *The F-pure threshold of a Calabi-Yau hypersurface*, Math. Ann. **362** (2015), no. 1-2, 551–567.

[CH14] John Cullinan and Farshid Hajir, *On the Galois groups of Legendre polynomials*, Indag. Math. (N.S.) **25** (2014), no. 3, 534–552. MR 3188847

[Com74] Louis Comtet, *Advanced combinatorics*, enlarged ed., D. Reidel Publishing Co., Dordrecht, 1974, The art of finite and infinite expansions. MR 0460128

[Deu41] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[Dic02] L.E. Dickson, *Theorems on the residues of multinomial coefficients with respect to a prime modulus*, Quarterly Journal of Pure and Applied Mathematics **33** (1902), 378–384.

[Eis08] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, NY, 2008.

[EM06] Lawrence Ein and Mircea Mustaţă, *Invariants of singularities of pairs*, International Congress of Mathematicians. Vol. II, Eur. Math. Soc., Zürich, 2006, pp. 583–602. MR 2275611

[Har77] R. Hartshorne, *Algebraic geometry*, Springer, NY, 1977.

[Har01] Nobuo Hara, *Geometric interpretation of tight closure and test ideals*, Trans. Amer. Math. Soc. **353** (2001), no. 5, 1885–1906.

[Her14] Daniel J. Hernández, *F-pure thresholds of binomial hypersurfaces*, Proc. Amer. Math. Soc. **142** (2014), no. 7, 2227–2242.

[Her16] ———, *F-purity versus log canonicity for polynomials*, Nagoya Math. J. **224** (2016), no. 1, 10–36.

[HH90] Melvin Hochster and Craig Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math. Soc. **3** (1990), no. 1, 31–116.

[HNnBWZ16] Daniel J. Hernández, Luis Núñez Betancourt, Emily E. Witt, and Wenliang Zhang, *F-pure thresholds of homogeneous polynomials*, Michigan Math. J. **65** (2016), no. 1, 57–87.

[How01] J. A. Howald, *Multiplier ideals of monomial ideals*, Trans. Amer. Math. Soc. **353** (2001), no. 7, 2665–2671. MR 1828466

[HR76] Melvin Hochster and Joel L. Roberts, *The purity of the Frobenius and local cohomology*, Advances in Math. **21** (1976), no. 2, 117–172. MR 0417172

[HS06] Craig Huneke and Irena Swanson, *Integral closure of ideals, rings, and modules*, London Mathematical Society Lecture Note Series, vol. 336, Cambridge University Press, Cambridge, 2006. MR 2266432

[HT04] Nobuo Hara and Shunsuke Takagi, *On a generalization of test ideals*, Nagoya Math. J. **175** (2004), 59–74.

[HW02] Nobuo Hara and Kei-ichi Watanabe, *F-regular and F-pure rings vs. log terminal and log canonical singularities*, J. Algebraic Geom. **11** (2002), no. 2, 363–392.

[HY03] Nobuo Hara and Ken-ichi Yoshida, *A generalization of tight closure and multiplier ideals*, Trans. Amer. Math. Soc. **355** (2003), no. 8, 3143–3174.

[Kar84] N. Karmarkar, *A new polynomial-time algorithm for linear programming*, Combinatorica **4** (1984), no. 4, 373–395. MR 779900

[KM98] János Kollár and Shigefumi Mori, *Birational geometry of algebraic varieties*, Cambridge Tracts in Mathematics, vol. 134, Cambridge University Press, Cambridge, 1998, With the collaboration of C. H. Clemens and A. Corti, Translated from the 1998 Japanese original. MR 1658959

[Koe14] Wolfram Koepf, *Hypergeometric summation*, second ed., Universitext, Springer, London, 2014, An algorithmic approach to summation and special function identities. MR 3289086

[Kol97] János Kollár, *Singularities of pairs*, Algebraic geometry—Santa Cruz 1995, Proc. Sympos. Pure Math., vol. 62, Amer. Math. Soc., Providence, RI, 1997, pp. 221–287.

[Kol13] ———, *Singularities of the minimal model program*, Cambridge Tracts in Mathematics, vol. 200, Cambridge University Press, Cambridge, 2013, With a collaboration of Sándor Kovács. MR 3057950

[Kor81] A. D. Korshunov, *The number of monotone Boolean functions*, Problemy Kibernet. (1981), no. 38, 5–108, 272. MR 640855

[Lan88] Peter S. Landweber, *Supersingular elliptic curves and congruences for Legendre polynomials*, Elliptic curves and modular forms in algebraic topology (Princeton, NJ, 1986), Lecture Notes in Math., vol. 1326, Springer, Berlin, 1988, pp. 69–93. MR 970282

[Leg85] Adrien Marie Legendre, *Recherches sur l'attraction dès spheroïdes homogènes*, Mémoires de Mathematiques et de Physique **X** (1785), 411–435, Prèsentès a l'Academie Royale des Sciences, par divers savans, et lus dans ses Assemblèes.

[Luc78] Edouard Lucas, *Theorie des Fonctions Numeriques Simplement Periodiques. [Continued]*, Amer. J. Math. **1** (1878), no. 3, 197–240.

[Mor06] Patrick Morton, *Explicit identities for invariants of elliptic curves*, J. Number Theory **120** (2006), no. 2, 234–271.

[MS11] Mircea Mustaţă and Vasudevan Srinivas, *Ordinary varieties and the comparison between multiplier ideals and test ideals*, Nagoya Math. J. **204** (2011), 125–157. MR 2863367

[MTW05] Mircea Mustaţă, Shunsuke Takagi, and Kei-ichi Watanabe, *F-thresholds and Bernstein-Sato polynomials*, European Congress of Mathematics, Eur. Math. Soc., Zürich, 2005, pp. 341–364.

[MY09] Mircea Mustaţă and Ken-Ichi Yoshida, *Test ideals vs. multiplier ideals*, Nagoya Math. J. **193** (2009), 111–128. MR 2502910

[OMS09] Keith Oldham, Jan Myland, and Jerome Spanier, *An atlas of functions*, second ed., Springer, New York, 2009, With Equator, the atlas function calculator, With 1 CD-ROM (Windows). MR 2466333

[Pag17] Gilad Pagi, *An elementary computation of the F-pure threshold of an elliptic curve*, preprint, `https://arxiv.org/abs/1706.07309`.

[Sat17] Kenta Sato, *Ascending chain condition for F-pure thresholds on a fixed strongly F-regular germ*, preprint, `https://arxiv.org/abs/1710.05331`.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Slo73] N. J. A. Sloane, *A handbook of integer sequences*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973. MR 0357292

[Sma98] Steve Smale, *Mathematical problems for the next century*, Math. Intelligencer **20** (1998), no. 2, 7–15. MR 1631413

[Smi97] Karen E. Smith, *Vanishing, singularities and effective bounds via prime characteristic local algebra*, Algebraic geometry—Santa Cruz 1995, Proc. Sympos. Pure Math., vol. 62, Amer. Math. Soc., Providence, RI, 1997, pp. 289–325. MR 1492526

[Smi00] ———, *The multiplier ideal is a universal test ideal*, Comm. Algebra **28** (2000), no. 12, 5915–5929, Special issue in honor of Robin Hartshorne.

[ST12] Karl Schwede and Kevin Tucker, *A survey of test ideals*, Progress in commutative algebra 2, Walter de Gruyter, Berlin, 2012, pp. 39–99. MR 2932591

[Str69] Volker Strassen, *Gaussian elimination is not optimal*, V. Numer. Math. **13** (1969), 354–356.

[Tak04] Shunsuke Takagi, *An interpretation of multiplier ideals via tight closure*, J. Algebraic Geom. **13** (2004), no. 2, 393–415.

[TW04] Shunsuke Takagi and Kei-ichi Watanabe, *On F-pure thresholds*, J. Algebra **282** (2004), no. 1, 278–297.

[Wah52] J. H. Wahab, *New cases of irreducibility for Legendre polynomials*, Duke Math. J. **19** (1952), 165–176. MR 0045864

[Was08] Lawrence C. Washington, *Elliptic curves*, second ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008, Number theory and cryptography. MR 2404461