AN ELEMENTARY COMPUTATION OF THE F-PURE THRESHOLD OF AN ELLIPTIC CURVE

GILAD PAGI

Abstract. We compute the $F$-pure threshold of a degree three homogeneous polynomial in three variables with an isolated singularity. The computation uses elementary methods to prove a known result of Bhatt and Singh (from [2]).

1. Introduction

In this note, 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 $\mathbb{P}^2$. Let $K$ denote a field of prime characteristic $p$ and let $R = K[x_1, ..., x_t]$. Fix any polynomial $f \in R$. By $F$-pure threshold we mean:

\begin{equation}
FT(f) := \sup \left\{ \frac{N}{p^e} \mid N, e \in \mathbb{Z}_{>0}, f^N \notin (x_1^{p^e}, ..., x_t^{p^e})R \right\},
\end{equation}

a definition that first appeared in [3], although the first formulation using tight closure theory is stated in [10].

The $F$-pure threshold is a numerical measurement of the singularity of $f$ at the origin. If $f$ is smooth there, $FT(f) = 1$. Smaller values of $FT(f)$ mean “worse singularities” of $f$ at the origin. The $F$-pure threshold is a characteristic $p$ analog of the log canonical threshold of a complex singularity (see [18]). When $f$ is defined over $\mathbb{C}$, one can reduce to the characteristic $p$ case, compute $FT(f)$ and compare the values in different $p$’s to the log canonical threshold. The limit of $FT(f)$ when $p \to \infty$ approaches the log canonical threshold of $f$ ([24, Theorems 3.3,3.4]). This fact is the culmination of a series of papers, going back to [15], [26], [8], [11], [27], [9], [28]. See the survey [1] for a gentle 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 $E \overset{F}{\rightarrow} E$ induces a map $H^1(E, O_E) \overset{F^*}{\rightarrow} H^1(E, O_E)$. 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 2.1. See also [12, IV.4] and [25, V.3,V.4].

In the upcoming sections we present an elementary proof of the following result of Bhatt and Singh:

**Theorem 1.1 (Main Theorem).** Let $K$ denote a field of prime characteristic $p > 2$. 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 a couple of proofs in [2] using a translation into local cohomology; Generalizations can be found in [14]. In contrast, our approach involves directly investigating the form of $f$ raised to integer powers using a generalized formula of the well known polynomial $H_p(\lambda) = \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i$ with $m = (p-1)/2$, used to compute the Hasse invariant. See also [22], [23].

Going back to the characteristic 0 case, for infinitely many $p$’s, the reduction of an elliptic curve mod $p$ is ordinary (e.g. over $\mathbb{Q}$ see [22, Excercise 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. For a general polynomial, this remains an open question (see some progress [13]).

The author acknowledges the financial support of NSF grant DMS-0943832.
Acknowledgments. This article is part of my Ph.D. thesis, which is being written under the direction of Karen Smith of University of Michigan. I would like to thank Prof. Smith for many useful 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.

2. Discussion

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 change of coordinates. So without loss of generality we assume $K$ is algebraically closed and change coordinates so $f$ is in its Legendre form:

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

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 [12, IV, Corollary 4.22].

**Proposition 2.1.** 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 $K$:

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

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

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

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

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

It turns out that when investigating integer powers of $f_a$, one gets coefficients similar to the form of $H_p(a)$, as we prove later in the Main Technical Lemma. This motivates the following definition:

**Definition 2.2.** 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 [21], we call it the Deuring Polynomial of degree $n$. When the indeterminant $\lambda$ 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 $p$. For an odd prime $p$, the polynomial $H\{\frac{p-1}{2}\}$ is $H_p(\lambda)$ and plays an important role in number theory, as we saw in Proposition 2.1. We shall dedicate the next section to investigate the connection of $H\{n\}$ to our problem and prove interesting properties of it.

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

$$(2.2.1) \quad n_e = \frac{N_e}{2} = \frac{p^e - 1}{2}$$

Specifically, when $e = 1$ we have:

$$n_1 = \frac{p - 1}{2}.$$
Theorem 2.3 (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.

The next section is dedicated to develop the required machinery. Afterwards we prove Main Theorem V2 directly.

Remark 2.4. The Deuring polynomials $H\{m\}$ 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 [19]. Indeed, if $P_m(x)$ denotes the $m$th Legendre polynomial then:

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

as follows by a simple substitution and a known “textbook” formula for the Legendre polynomials ([17, Exercise 2.12]); this is pointed out in [5] and [4]. In section 3, 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 our paper self-contained and, we hope, more straightforward than relying on the vast literature on Legendre polynomials.

3. Deuring Polynomials and Machinery

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

Theorem 3.1 (Lucas’s Theorem). [See [20] and [7]] Let $k = (k_1, ..., k_n) \in \mathbb{N}^n$ 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 $k_i$ in its 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 $\binom{N}{k}$ satisfy:

$$\binom{N}{k} = \frac{N!}{k_1! \cdots k_n!} = \binom{0}{a_{10} a_{20} \cdots a_{n0}} \binom{1}{a_{11} a_{21} \cdots a_{n1}} \cdots \binom{e}{a_{1e} a_{2e} \cdots a_{ne}} \pmod{p},$$

with the convention that if $a_{ij} + ... + a_{nj} > b_j$ then $\binom{b_j}{a_{ij} a_{2j} \cdots a_{nj}} = 0$. Specifically, $\binom{N}{k} \not\equiv 0 \pmod{p}$ 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 $j$th digits of the $k_i$’s.

The next lemma shows that understanding the Deuring polynomial $H\{n\}$ of Definition 2.2 is crucial for the discussion.

Lemma 3.2 (Main Technical Lemma). Let $f_\lambda = y^2z - x(x-z)(x-\lambda z)$ and let $N = n + m$ be an 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.
Corollary 3.3. Let \( f \) both Apply the Proof.

Let \( f \) be a prime. Then \( H\{p-1\} \in \mathbb{F}_p[\lambda] = (\lambda - 1)^{p-1} \).

Proof. The coefficients of \( H\{p-1\}\) 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 \(p^{\text{th}}\) row starts and ends with 1, while the rest of the entries are zero. Ergo, the \((p - 1)^{\text{th}}\) row consists of \( \pm 1 \)'s due to the identity:

\[
\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}.
\]

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

\[
p - 1 : 1 \quad -1 \quad 1 \quad -1 \quad \ldots \quad -1 \quad 1 \quad -1 \quad 1
\]

\[
p : 1 \quad 0 \quad 0 \quad 0 \quad \ldots \quad \ldots \quad 0 \quad 0 \quad 0 \quad 1
\]

So using the geometric series formula we get:

\[
H\{p-1\} = 1 + \lambda + \ldots + \lambda^{p-1} = \frac{\lambda^p - 1}{\lambda - 1} = (\lambda - 1)^{p-1}
\]

Lemma 3.5. Fix a prime \( p \). Let \( H\{n\} \in \mathbb{F}_p[\lambda] \). Write the \( p \)-expansion of \( n \):

\[
n = b_0 p^0 + b_1 p^1 + \ldots + b_c p^c.
\]

Then

\[
H\{n\} = H\{b_0\}^1 H\{b_1\}^p H\{b_2\}^{p^2} \cdots H\{b_c\}^{p^c}
\]

Proof. Denote \( f = H\{n\} \) and \( g = H\{b_0\}^1 H\{b_1\}^p \cdots H\{b_c\}^{p^c} \). First notice that \( f \) and \( g \) are of the same degree as \( \text{deg } f = n \) and \( \text{deg } g = b_0 + b_1p + b_2p^2 + \ldots + b_c p^c = n \). Fix \( \lambda^i \) and let us compare its coefficient in both \( f \) and \( g \). For \( i = 0 \), the coefficient of \( \lambda^0 \) 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:

\[
i = a_0 p^0 + a_1 p^1 + \ldots + a_c p^c,
\]

so

\[
\lambda^i = \lambda^{a_0 p^0} \lambda^{a_1 p^1} \cdots \lambda^{a_c p^c}.
\]

Note that the largest power \( c \), as appears in the expansion of \( n \), is sufficient as \( i \leq n \). Notice that the powers of \( \lambda \) in \( H\{b_j\}^{p^j} \) can only be \( \{0p^i, 1p^i, 2p^i, \ldots, b_j p^i\} \). So if \( j_1 \neq j_2 \) then the set of powers in \( H\{j_1\}^{p^{j_1}} \)
and in $H\{j_2\}^{p^{j_2}}$ 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 $\lambda^i = \lambda^{a_0p^0}\lambda^{a_1p^1} \cdots \lambda^{a_ep^e}$.

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

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

$$\lambda^i = \lambda^{a_0p^0} \lambda^{a_1p^1} \cdots \lambda^{a_ep^e}$$

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

$$\left(\frac{b_0}{a_0}\right)^2 \left(\frac{b_1}{a_1}\right)^{2p} \cdots \left(\frac{b_e}{a_e}\right)^{2p^e}.$$ 

By Fermat’s little theorem, the expression is:

$$\left(\frac{b_0}{a_0}\right)^2 \left(\frac{b_1}{a_1}\right)^{2} \cdots \left(\frac{b_e}{a_e}\right)^{2},$$

which is precisely the coefficient of $\lambda^i$ in $f$ due to Lucas’s Theorem. Otherwise, if for some $j$, $a_j > b_j$, then $\lambda^i$ 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 3.6.** 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 3.5](#) after writing $\frac{p^e-1}{2}$ in its $p$-expansion and using geometric series formula:

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

Recall that we denote $n_\epsilon = (p^\epsilon - 1)/2$ and then $n_1 = (p-1)/2$. We can rewrite [Corollary 3.6](#) as

$$H\{n_\epsilon\} = (H\{n_1\})^{1+p+\ldots+p^{\epsilon-1}}$$

Note that $H\{n_1\}$ is the polynomial appearing in [Proposition 2.1](#) so it has an important role in the context of our [Main Theorem](#).

In our proof of the [Main Theorem V2](#) we will encounter another polynomial: $H\{n_1 - 1\}$. We shall now investigate it.

**Lemma 3.7.** Fix an integer $n$. Let $F(\lambda) \in \mathbb{Q}[\lambda]$ 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 $p > n$. 

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

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

Now, observe:

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

Shift the index of the middle sum to get:
\[ (3.7.1) \quad = \sum_{i=0}^{n-1} \binom{n-1}{i}^2 \lambda^i - \sum_{i=1}^{n} \binom{n-1}{i-1}^2 \lambda^i + \sum_{i=1}^{n} 2 \binom{n-1}{i-1} \frac{n}{i} \lambda^i. \]

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:
\[
2 \binom{n-1}{i-1} \frac{n}{i} = 2 \binom{n-1}{i-1} \frac{n-i+i}{i} = 2 \binom{n-1}{i-1} \left( \frac{n-i}{i} + 1 \right) = 2 \binom{n-1}{i-1} \binom{n-1}{i} + 2 \binom{n-1}{i-1}^2.
\]

So when \( i \) is fixed, the coefficient of \( \lambda^i \) in \( (3.7.1) \) is
\[
\binom{n-1}{i}^2 - \binom{n-1}{i-1}^2 + 2 \binom{n-1}{i-1} \binom{n-1}{i} + 2 \binom{n-1}{i-1}^2 \]
which further simplifies as:
\[
\left( \binom{n-1}{i} \right)^2 = \left( \binom{n-1}{i-1} + \binom{n-1}{i} \right)^2 = \binom{n}{i}^2,
\]
using the known identity \( (3.4.1) \). So we conclude:
\[
(1 - \lambda)H\{n-1\} + 2nF = H\{n\}.
\]

\[ \square \]

**Lemma 3.8.** Fix a prime \( p > 2 \). Recall \( n_1 = (p-1)/2 \). Then the following holds over any field \( K \) in characteristic \( p \):

1. \( H\{n_1\} \in K[\lambda] \) has no repeated roots. Further, \( \lambda = 0, 1 \) are not roots of \( H\{n_1\} \).
2. Let \( F(\lambda) \in K[\lambda] \) be the formal antiderivative of the polynomial \( H\{n_1-1\}(\lambda) \) with constant coefficient 0. Then \( F \) has no repeated roots.

**Proof.**

1. This is proved in [10] (see also [25, Theorem 4.1]) but we provide a sketch. Let \( D_{PF} \) be the following differential operator (which is called the Picard-Fuchs operator):
\[
D_{PF} = 4\lambda(1-\lambda) \frac{d^2}{d\lambda^2} + 4(1-2\lambda) \frac{d}{d\lambda} - 1
\]

One can check that \( D_{PF}H\{n_1\}(\lambda) = 0 \). Moreover, since \( H\{n_1\}(0) \neq 0 \) and \( H\{n_1\}(1) \) (can be computed directly), \( H\{n_1\}(\lambda) \) has no repeated roots in over \( K \).

2. We follow similar steps as in the proof of (1), however we need a different differential equation. We will show that over \( K \):
\[
(3.8.1) \quad 4\lambda(\lambda-1)F'' + 8\lambda F' + F = 0
\]

Where \( F', F'' \) are the first and second derivatives with respect to \( \lambda \), respectively. Once we prove \( (3.8.1) \) we see that the only possible repeated roots of \( F \) can be 0 or 1 by the following argument: Suppose \( \alpha \) is a root of \( F \) of multiplicity \( r \geq 2 \). Since \( \deg F = n_1 = (p-1)/2 \), then \( r < p \). So write
\[
F = g_1(\lambda) \cdot (\lambda - \alpha)^r \quad \text{where} \quad g_1(\alpha) \neq 0,
\]
\[
F' = g_2(\lambda) \cdot (\lambda - \alpha)^{r-1} \quad \text{where} \quad g_2(\alpha) \neq 0,
\]
\[
F'' = g_3(\lambda) \cdot (\lambda - \alpha)^{r-2} \quad \text{where} \quad g_3(\alpha) \neq 0.
\]

Plug the above expression in \( (3.8.1) \) and divide by \( (\lambda - \alpha)^{r-2} \) to get
\[
4\lambda(\lambda-1)g_3 + 8\lambda(\lambda - \alpha)g_2 + (\lambda - \alpha)^2 g_1 = 0.
\]

Plugging in \( \lambda = \alpha \) gives:
\[
4\alpha(\alpha-1)g_3(\alpha) = 0
\]
Since $p \neq 2$, $4$ is a unit. We get:

$$\alpha(\alpha - 1) \equiv 0 \pmod{p} \Rightarrow \alpha = 0, 1$$

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

While $0$ is a root of $F$, it is simple since $F'(0) = H\{n_1 - 1\}(0) = 1$. In addition, $\lambda = 1$ is not a root of $F'(\lambda)$ as the following combinatorial identity (which holds over $\mathbb{Z}$) shows:

$$F'(1) = H\{n_1 - 1\}(1) = \sum_{0}^{n_1 - 1} \binom{n_1 - 1}{i}^2 = \binom{2n_1 - 2}{n_1 - 1} = \binom{p - 3}{n_1 - 1},$$

which is not zero in $K$ by Lucas's Theorem.

All that is left to do is to show that the differential equation (3.8.1) holds. This can be done by checking the coefficient of $\lambda^i$ in the different summands. Note that we are working over $\mathbb{F}_p$ so $2n_1 = p - 1 = -1$. Also recall that we are using the convention that if $k < 0$ then $\binom{n}{k} = 0$:

- coefficient in $F$:
  $$\binom{n_1 - 1}{i}^2$$

- coefficient in $F'$:
  $$\binom{n_1 - 1}{i}^2$$

- coefficient in $8F'$:
  $$\binom{n_1 - 1}{i}^2$$

- coefficient in $4\lambda F''$:
  $$4\binom{n_1 - 1}{i}^2(i) = \binom{n_1 - 1}{i}^2 \frac{4(n_1 - 1 - (i - 1))^2(i)}{(i)^2} = \binom{n_1 - 1}{i}^2 \frac{2(n_1 - 2i)^2(i)}{(i)^2} = \binom{n_1 - 1}{i}^2 \frac{(-1 - 2i)^2}{(i)^2}$$

Notice that for $i = 0$, we have $i - 1 < 0$ so all the coefficients are 0. Now compute the coefficient of $\lambda^i$ with $i > 0$ in

$$4\lambda^2 F'' - 4\lambda F' + 8\lambda F' + F.$$ 

We get:

$$\binom{n_1 - 1}{i}^2 \frac{4(4i - 1)(4i^2 - 4i - 1 - 4i - 4i^2 + 8i + 1)}{i} = 0$$

\[\square\]

**Remark 3.9.** Fix any integer $n > 1$ and let $F \in \mathbb{Q}[\lambda]$ be the antiderivative of $H\{n\}$ constant coefficient 0. We can compute a differential equation similar to (3.8.1) that $F$ satisfies and deduces properties of $F$'s roots. However, this is beyond the scope of this article.

**Corollary 3.10.** Fix an integer $n \geq 1$ and a prime $p > \max\{2, n\}$. Let $K$ be a field of characteristic $p$. Let $F$ be the formal antiderivative of $H\{n - 1\}$ with constant coefficient 0. Then $H\{n\}$ and $H\{n - 1\}$ share no roots if and only if $F$ has no repeated roots. In particular, $H\{n_1\}$, $H\{n_1 - 1\}$ share no roots in characteristic $p$.

**Proof.** Consider the ideal $I = (H\{n\}, H\{n - 1\})$ in $K[\lambda]$. From Lemma 3.7 we have:

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

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. From Lemma 3.8(2) we see that for $n = n_1$, indeed $F$ has no repeated roots, thus for any $p$, $H\{n_1\}, H\{n_1 - 1\}$ share no roots in characteristic $p$. \[\square\]

We end this section with 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 $K$. Denote the monomial $\lambda^{\mu_1} \cdots \lambda^{\mu_s}$ by $x^\mu$ where $\mu$ is the multieponent $[\mu_1, ..., \mu_t]$. Similarly, for $s$ scalars in $K$, $b_1, ..., b_s$, we denote $\mathbf{b} = [b_1, ..., b_s]$. Now, let $x^{\mu_1}, ..., x^{\mu_s}$ be the monomials of $f$. Using the usual meaning of dot product we have:

$$f = \mathbf{b} \cdot [x^{\mu_1}, ..., x^{\mu_s}] = b_1 x^{\mu_1} + ... + b_s x^{\mu_s}.$$ 

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

$$\max \mathbf{k} = \max \{k_1, ..., k_t\} = \max_{1 \leq i \leq t} k_i.$$
Using this notation, we have the following straightforward way to produce upper and lower bounds for $FT(f)$:

**Lemma 3.11.** 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:

\[(3.11.1) \quad f^N = \sum_{\text{distinct multi-exponents } k} c_k x^k.\]

Note that all but finitely many $c_k$’s are 0. Fix $e \in \mathbb{Z}_{\geq 0}$ and consider $\frac{N}{p^e}$. Then:

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

**Proof.** This is immediate from the definition (1.0.1) and from [1, 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 3.12.** Let $f$ be a homogeneous polynomial of degree $d$ in $t$ variables. Let $x^k$ be a monomial in $f^N$ with a non-zero coefficient. Denote $k = [k_1, ..., k_t]$. Then $k_1 + ... + k_t = dN$. Moreover, $\max k \geq Nd/t$ and if $\max k = Nd/t$ then $k = [Nd/t, Nd/t, ..., Nd/t]$.

**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 $k$ are less than $Nd/t$. Lastly, if $\max k = Nd/t$ but another power is less, then $k_1 + ... + k_t$ is less than $Nd$.

\[\square\]

4. PROOF OF THE MAIN THEOREM

Now we are ready to prove the [Main Theorem V2]

**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

\[N_e = p^e - 1, \quad n_e = N_e/2 = (p^e - 1)/2.\]

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 3.3] and [Lemma 3.12] we get:

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

where $m = (x, y, z)$ and $m^{[p^e]} = (x^{p^e}, y^{p^e}, z^{p^e}) K[x, y, z]$. By [Lemma 3.11] if we show that $\binom{2n_e}{n_e} H\{n_e\}(a) \neq 0$ (mod $p$) for any $e$, then we get a lower bound of $N_e/p^e = \frac{p^e - 1}{p^e}$ for $FT(f_a)$. By taking $e \to \infty$ we get that:

\[\lim_{e \to \infty} \frac{p^e - 1}{p^e} \leq FT(f_a) \leq 1 \Rightarrow 1 = FT(f_a)\]

So suffices to show that $\binom{2n_e}{n_e} H\{n_e\}(a) \neq 0$ (mod $p$).

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

\[2n_e = p^e - 1 = (p - 1)p^{e-1} + (p - 1)p^{e-2} + ... + (p - 1)p^0 + 1\]

\[n_e = \frac{p^e - 1}{2}p^{e-1} + \frac{p^e - 1}{2}p^{e-2} + ... + \frac{p^e - 1}{2}p^0\]

Since the digits of $n_e$ and $n_e$ are added without carrying to the digits of $2n_e$, by Lucas’s Theorem $\binom{2n_e}{n_e} \neq 0$ (mod $p$).

Next, due to [Corollary 3.6]

\[H\{n_e\}(a) = (H\{n_e\}(a))^{1 + p + ... + p^{e-1}}\]
We conclude that $H\{n_e\}(a) \neq 0 \pmod{p}$ since the polynomial is ordinary, which means that $H\{n_1\}(a) \neq 0 \pmod{p}$. 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 3.12 all other monomials $x^k$ satisfy $\max k \geq N + 1 = p$. So apply Lemma 3.11 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 $p^e - p^{e-1} - 1$ 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 $f_a^N \notin m[p^e]$. Notice that:

$$N = p^e - p^{e-1} - 1 = p^e - 2p^{e-1} + p^{e-1} - 1 = (p-1)(p^{e-1}) + (n_1 - 1)(p^{e-1}) + p^{e-1} - 1.$$

We set

$$n = (n_1)(p^{e-1}),$$
$$$$

$$m = (n_1 - 1)(p^{e-1}) + p^{e-1} - 1.$$ 

Notice that $m + 1 = n$.

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

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

From the Main Technical Lemma we get the coefficient of a critical term in $f_a^N$ is:

$$(m + n \ \ n \ H\{m\}(a))$$

We wish to prove that the coefficient $[4.0.1]$ is non-zero mod $p$. We shall break it to two parts, the multinomial $(m+n)$, 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:

$$n = (0)^p + (0)^{p^1} + ... + (0)^{p^{e-2}} + n_1 p^{e-1},$$
$$m = (p-1)^p + (p-1)^{p^1} + ... + (p-1)^{p^{e-2}} + (n_1 - 1) p^{e-1}.$$ 

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

We complete the proof that the coefficient $[4.0.1]$ 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 $m$:

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

Use Lemma 3.5 to deduce

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

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 3.4 Only $\lambda = 1$ is a root of $H\{p-1\}$ but $H\{n_1\}(1)$ is not zero due to Lemma 3.8 1).

It remains to compare the roots of $H\{n_1\}$ and $H\{n_1 - 1\}$. From Corollary 3.10 we conclude that they share no roots, as required. This concludes the proof.

\[ \Box \]

Discussion 4.1. 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 $\text{char}(K) = 2$. From Lemma 3.5 we deduce that over $K$ and for any integer $m > 0$, $H\{m\} = H\{1\}^m = (1 + \lambda)^m$. Since $a \neq 1$, $a$ does not satisfy any Deuring polynomial over $K$. To prove that $1/2$ is
an upper bound, just observer that $f_0^e$ is already in $(x^2, y^2, z^2)$ making $1/2$ an upper bound. Now, we would like to show that $(2^e-1)/2^e$ is a lower bound for all $e$, which would result in an lower bound of $1/2$. So let

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

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

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

By construction, and due to 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.

References

[1] Angélica Benito, Eleonore Faber, and Karen E. Smith. Measuring singularities with Frobenius: the basics. In Commutative algebra, pages 57–97. Springer, New York, 2013.
[2] Bhargav Bhatt and Anurag K. Singh. The $F$-pure threshold of a Calabi-Yau hypersurface. Math. Ann., 362(1-2):551–567, 2015.
[3] Manuel Blickle, Mircea Mustaţa, and Karen E. Smith. F-thresholds of hypersurfaces. Trans. Amer. Math. Soc., 361(2):6549–6565, 2009.
[4] John Brillhart and Patrick Morton. Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the super-singular polynomial. J. Number Theory, 106(1):79–111, 2004.
[5] John Cullinan and Farshid Hajir. On the Galois groups of Legendre polynomials. Indag. Math. (N.S.), 25(3):534–552, 2014.
[6] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ., 14:197–272, 1941.
[7] L.E. Dickson. Theorems on the residues of multinomial coefficients with respect to a prime modulus. Quarterly Journal of Pure and Applied Mathematics, 33:378–384, 1902.
[8] Nobuo Hara. Geometric interpretation of tight closure and test ideals. Trans. Amer. Math. Soc., 353(5):1885–1906, 2001.
[9] Nobuo Hara. Geometric interpretation of tight closure and test ideals. Nagoya Math. J., 175:59–74, 2004.
[10] Nobuo Hara and Kei-ichi Watanabe. F-regular and F-pure rings vs. log terminal and log canonical singularities. J. Algebraic Geom., 11(2):363–392, 2002.
[11] Nobuo Hara and Ken-ichi Yoshida. A generalization of tight closure and multiplier ideals. Trans. Amer. Math. Soc., 355(8):3143–3174, 2003.
[12] R. Hartshorne. Algebraic Geometry. Springer, NY, 1977.
[13] Daniel J. Hernández. F-purity versus log canonicity for polynomials. Nagoya Math. J., 224(1):10–36, 2016.
[14] Daniel J. Hernández, Luis Núñez Betancourt, Emily E. Witt, and Wenliang Zhang. F-pure thresholds of homogeneous polynomials. Michigan Math. J., 65(1):57–87, 2016.
[15] Melvyn Hochster and Craig Huneke. Tight closure, invariant theory, and the Briançon-Skoda theorem. J. Amer. Math. Soc., 3(1):31–116, 1990.
[16] Jun-ichi Igusa. Class number of a definite quaternion with prime discriminant. Proc. Nat. Acad. Sci. U.S.A., 44:312–314, 1958.
[17] Wolfram Koepf. Hypergeometric summation. Universitext. Springer, London, second edition, 2014. An algorithmic approach to summation and special function identities.
[18] János Kollár. Singularités de pairs. In Algebraic geometry—Santa Cruz 1995, volume 62 of Proc. Sympos. Pure Math., pages 221–287. Amer. Math. Soc., Providence, RI, 1997.
[19] Adrien Marie Legendre. Recherches sur l’attraction des sphéroides homogènes. Mémoires de Mathematiques et de Physique, X:411–435, 1785. Présentés à l’Académie Royale des Sciences, par divers savans, et lus dans ses Assemblées.
[20] Edouard Lucas. Théorie des Fonctions Numéiques Simplement Periodiques. [Continued]. Amer. J. Math., 1(3):197–240, 1878.
[21] Patrick Morton. Explicit identities for invariants of elliptic curves. J. Number Theory, 120(2):234–271, 2006.
[22] Susanne Müller. The $F$-pure threshold of quasi-homogeneous polynomials. 2016. preprint, https://arxiv.org/abs/1601.08086
[23] Susanne Müller. The $F$-pure threshold of quasi-homogeneous polynomials. 2017. preprint, https://arxiv.org/abs/1702.07553
[24] Mircea Mustaţă, Shunsuke Takagi, and Kei-ichi Watanabe. F-thresholds and Bernstein-Sato polynomials. In European Congress of Mathematics, pages 341–364. Eur. Math. Soc., Zürich, 2005.
[25] Joseph H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.
[26] Karen E. Smith. The multiplier ideal is a universal test ideal. Comm. Algebra, 28(12):5915–5929, 2000. Special issue in honor of Robin Hartshorne.
[27] Shunsuke Takagi. An interpretation of multiplier ideals via tight closure. J. Algebraic Geom., 13(2):393–415, 2004.
[28] Shunsuke Takagi and Kei-ichi Watanabe. On $F$-pure thresholds. J. Algebra, 282(1):278–297, 2004.