LEGENDRE POLYNOMIALS ROOTS AND THE $F$-PURE THRESHOLD OF BIVARIATE FORMS

GILAD PAGI

ABSTRACT. We provide a direct computation of the $F$-pure threshold of degree four homogeneous polynomials in two variables and, more generally, of certain homogeneous polynomials with four distinct roots. The computation depends on whether the cross ratio of the roots satisfies a specific Möbius transformation of a Legendre polynomial. We then make a connection between a long lasting open question, involving the relationship between the $F$-pure and the log canonical threshold, and roots of Legendre polynomials over $\mathbb{F}_p$.

1. Introduction. In this note, we provide an elementary computation of the $F$-pure threshold of the homogeneous defining equation of a family of subschemes of $\mathbb{P}^1$ supported at four points. Our formula depends on whether the cross-ratio of these four points satisfies a certain Deuring polynomial: a Deuring polynomial is a Möbius transformation of a Legendre polynomial of the same degree (See Definition 2.1).

Let $K$ denote a field of prime characteristic $p$ and let $R = K[x_1, ..., x_t]$. Fix any polynomial $f \in R$. By the $F$-pure threshold (at the origin) we mean:

\[
FT(f) := \sup \left\{ \frac{N}{p^e} \mid N, e \in \mathbb{Z}_{>0}, f^N \not\in (x_1^{p^e}, ..., x_t^{p^e})R \right\}.
\]

This definition appeared in [BMS09] (the original tight-closure formulation is stated in [TW04]). The $F$-pure threshold is a characteristic $p$ analog of the log canonical threshold of a complex singularity (as defined in [Kol97]). A famous open conjecture, stated in Discussion 1.3 relates these two thresholds; interestingly, our work reduces this conjecture, for a certain family of bivariate forms, to understanding roots of Legendre polynomials over $\mathbb{F}_p$.

Our first goal is to compute the $F$-pure threshold of a bivariate homogeneous polynomial of degree four. Because the case of multiple roots is easy (see Discussion 3.7), our main result treats the case where the roots are all distinct:

Theorem 1.1. Let $K$ be a field of prime characteristic $p$. Consider a degree four homogeneous polynomial $f \in K[x, y]$, with distinct roots over $\mathbb{P}^1_K$. After fixing an order of the roots, let $a \in K$ 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 2.1) of degree $n_1$. Then

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

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 [Pag18a]. While some of these properties can be deduced from known facts about Legendre polynomials, we include straightforward algebraic proofs (or cite some from [Pag18a]) in order to be self-contained.

We generalize [Theorem 1.1] to certain higher degree polynomials:

Theorem 1.2. 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 $\mathbb{P}^1_K$, where

\[
1991 \text{ AMS Mathematics subject classification.} \quad 14H20.
\]

Keywords and phrases. F pure threshold, Deuring polynomial, Legendre Polynomial.

The author acknowledges the partial financial support of NSF grant DMS-0943832.

Received by the editors July-09-2020.

1
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 1.3.** Our theorem connects a well known open question regarding the relationship between $F$-pure and log canonical threshold to a seemingly unrelated question of roots of Legendre polynomials over $\mathbb{F}_p$. Recall the open question. Consider a polynomial $f$ with integer coefficients. On the one hand, we can consider $f$ as a complex polynomial, and compute the log canonical threshold of $f$, denoted $\text{lct}(f)$. On the other hand we can compute $FT(F_p)$ repeatedly for each $p$, where $F_p$ is the natural image of $f$ over $\mathbb{Z}_p$. Let $\mathcal{P}$ be the set of all primes $p$ such that $FT(F_p) = \text{lct}(f)$. A decades old open conjecture predicts that $\mathcal{P}$ is of infinite cardinality. It is well known that $\lim_{p \to \infty} FT(F_p) = \text{lct}(f)$. We now point out how this open question relates to Legendre polynomials for the case of the family of polynomials in Theorem 1.2. Let $f$ be a polynomial as in the theorem. One can compute that $\text{lct}(f) = \frac{1}{b+c}$. 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 $f_p$ is not a root of $H\left\{\frac{c}{b+c}(p-1)\right\}$ over $\mathbb{F}_p$. For example, here is a precise formulation of our statement is the simplest case.

**Question 1.4.** Suppose $f = x^b y^b (x+y)^c(x+ay)^c \in \mathbb{Z}[x,y]$. Denote

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

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 [Pag18a]). Further evidence that the conjecture is connected to ordinarity is explored in [MS11].

In addition, the $F$-pure threshold computation in Theorem 1.1 provides an immediate alternative proof for the known corollary regarding properties of the roots of Legendre polynomials mod $p$.

**Corollary 1.5.** 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 4.

**Acknowledgments.** This article is part of my Ph.D. thesis ([Pag18b]), which was written under the direction of Karen Smith of University of Michigan. I would like to thank Prof. Smith for many useful discussions.
2. Roots of Deuring Polynomials In Prime Characteristic. A crucial part of computing $FT(f)$ is identifying when coefficients of monomials of $f^N$ vanish. We later observe \textbf{[Lemma 3.4]} that one of these coefficient is no other than the Deuring polynomial \textbf{[Definition 2.1]} evaluated at the cross-ratio. Therefore, we turn to investigate roots of Deuring polynomials in prime characteristic.

\textbf{Definition 2.1.} For an integer $n > 0$, define the following polynomial in $\mathbb{Z}[\lambda]$: 

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

Following \textbf{[Mor06]}, we call $H\{n\}(\lambda)$ the \textit{Deuring Polynomial} of degree $n$; it can be equivalently defined using the Legendre polynomial of degree $n$, $P_n(x)$:

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

(see \textbf{[Pag18a]} for more details.) When the indeterminate $\lambda$ 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 of this integer polynomial mod $p$.

We shall investigate the roots of $H\{n\}$ in characteristics $p$. The following two lemmas are proven in \textbf{[Pag18a]}:

\textbf{Lemma 2.2.} Let $p$ be a prime. Then $H\{p - 1\} \in \mathbb{F}_p[\lambda]$ is $(\lambda - 1)^{p-1}$.

\textbf{Lemma 2.3 (Schur’s Congruence).} Fix a prime $p$. Let $H\{n\} \in \mathbb{F}_p[\lambda]$. Write the $p$-expansion of $n$:

$$n = b_0p^0 + b_1p^1 + ... + b_e p^e.$$ 

Then 

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

\textbf{Example 2.4.} In characteristic $p$, where $p$ is an odd prime:

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

For the computation of our main theorems, we need the following properties of the roots of $H\{n\}$ in characteristic $p$:

\textbf{Lemma 2.5.} 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 $H\{n\}$. Moreover, if $0 < n < p/2$ then $H\{n\}$ and $H\{n - 1\}$ share no roots.

The above lemma follows from the orthogonality of Legendre polynomials and the recursive relation between them (see the author’s Ph.D. thesis for more details). If the reader would like to avoid analytic techniques, we provide a purely algebraic proof of \textbf{Lemma 2.5} which reveals interesting properties of Deuring polynomials. The rest of this section is dedicated for that goal. Alternatively, the reader may skip directly to the computation of \textbf{Theorem 3.5} in the next section.

\textbf{In [Pag18a], we prove:}

\textsuperscript{4}Arguably it first appeared in \textbf{[Deu41]}. 

Lemma 2.6. Fix an integer \( n \geq 0 \). Let \( F = F(\lambda) \in \mathbb{Q}[\lambda] \) be 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 \( n < p \).

We next develop differential equations for \( H\{n\} \) it formal antiderivative that will help us to investigate their roots. Once we do that, we can use the following lemma to deduce properties of their roots:

Lemma 2.7. Let \( K \) be a field of prime characteristic \( p \). Let \( F \in K[\lambda] \) of degree \( d < p \) and denote \( F', F'' \) as its first and second derivative, respectively. Suppose that \( F \) satisfies a differential equation of the form
\[
(\lambda \lambda'') + a\lambda F' + bF' + cF = 0, \quad a, b, c \in K.
\]
Then the only possible repeating roots of \( F \) are \( \lambda = 0 \) and \( \lambda = 1 \).

**Proof.** Suppose \( \alpha \) is a root of \( F \) of multiplicity \( r \geq 2 \). Since \( \deg F = d < p \), 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 \((2.7.1)\) and divide by \((\lambda - \alpha)^{r-2}\) to get
\[
\lambda(\lambda - 1)g_1 + (a\lambda + b)(\lambda - \alpha)g_2 + c(\lambda - \alpha)^2g_1 = 0.
\]
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 \( \alpha = 1 \). \( \square \)

Proposition 2.8. Fix \( n \geq 0 \). Let \( F = F(\lambda) \in \mathbb{Q}[\lambda] \) be the formal antiderivative of \( H\{n\} \in \mathbb{Z}[\lambda] \) with constant coefficient 0. Then \( F \) satisfies:
\[
(\lambda(\lambda - 1)F'' - (1 + 2n)\lambda F' + (n + 1)^2F = 0
\]
Further, if \( K \) is a field of prime characteristic \( p \) and \( 0 \leq n < p/2 \), then \( F \) has a natural image in \( K[\lambda] \) and it only has simple roots over \( K \).

**Proof.** There is a constructive proof for the validity of \((2.8.1)\) in [Pag18b, Lemma III.18]. One can also simply plug in:
\[
F(\lambda) = \sum_{i=0}^{n} \binom{n}{i} \frac{1}{i+1} \lambda^{i+1}
\]
and observe that \( F \) satisfies the differential equation \((2.8.1)\) 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 2.7] 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 proven independently later in Corollary 2.11 \( \square \)

Lemma 2.9. Let \( n \geq 0 \) be an integer and denote \( H = H\{n\} \in \mathbb{Z}[\lambda] \). Then \( H \) satisfies the following differential equation:
\[
(2.9.1) \quad \lambda(\lambda - 1)H'' + (\lambda(1 - 2n) - 1)H' + n^2H = 0.
\]
Proof. Simply take the derivative of (2.8.1). □

Remark 2.10. For example, set $n = \frac{p-1}{2}$ for an odd prime $p$, and multiply by 4 in order to clear denominators. We get:

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

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 $n$.

Now we conclude the first part of Lemma 2.5

Corollary 2.11. 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 2.9 and Lemma 2.7 shows that the only possible repeating roots of $H$ are 0 and 1. However, $H(0) = 1$. Moreover, the following combinatorial identity (which holds over $\mathbb{Z}$) shows:

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

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

Now we conclude the last part of Lemma 2.5

Corollary 2.12. 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 2.6 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 $F$ only has simple roots, which is the result in Proposition 2.8. □

3. Computation of the $F$-pure threshold. We start this section with two useful observations for computing $FT(f)$. Let $K$ be a field. A polynomial $f \in K[x_1, \ldots, x_t]$ is a linear combination of monomials over $K$. Denote the monomial $x_1^{i_1} \cdots x_t^{i_t}$ by $x^{\mu}$ where $\mu$ is the multiexponent $[\mu_1, \ldots, \mu_t]$. Similarly, for $s$ scalars in $K$, $b_1, \ldots, b_s$, we denote $b = [b_1, \ldots, b_s]$. Now, let $x^{\mu_1}, \ldots, x^{\mu_s}$ be the monomials of $f$. Using the usual meaning of dot product we have:

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

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

$$\max k = \max_{1 \leq i \leq t} k_i.$$ 

Using this notation, we have the following straightforward way to produce upper and lower bounds for $FT(f)$:
Lemma 3.1. 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:

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

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

Proof. This is immediate from the definition, specifically (1.0.1), and from [BFS13, Prop 3.26] which implies that for any \( \frac{N}{p^e} \in [0, 1] \),

\[
f^N \not\in (x_1^{p^e}, ..., x_t^{p^e})R \iff \frac{N}{p^e} < FT(f).
\]

Lemma 3.2. 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 \( Nd \).

We can now focus on the polynomials appearing in our main theorems. 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 3.3. 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:

\[
(3.3.1) \quad x^4, x^3y, x^2y^2, x^2y(x+y), xy(x+y)(x+ay) \text{ with } a \in K - \{0, 1\}.
\]

Proof. \( FT(f) \) is preserved under base change, scalar multiplication and linear change of variables. Thus, without loss of generality, let \( K \) be algebraically closed, over which \( f \) factors as a product linear terms. Now change variables to obtains one of the five forms in (3.3.1), 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 3.7].

The next lemma shows that understanding the Deuring polynomial \( H\{n\} \) is crucial for the discussion.

Lemma 3.4 (Main Technical Lemma). Let \( f_\lambda = (x+y)(x+\lambda y) \) and let \( N \) be a positive integer. Then the coefficient of \( x^N y^N \) in \( f_\lambda^N \) is \( H\{N\}\{\lambda\} \).

Proof. Notice:

\[
f_\lambda^N = (x+y)^N(x+\lambda y)^N = \left( \sum_{i=0}^{N} \binom{N}{i} x^i y^{N-i} \right)^2 \left( \sum_{j=0}^{N} \binom{N}{j} (\lambda)^j x^{N-j} y^j \right).
\]
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. \hfill \Box

Consider the statements in **Theorem 1.1** and **Theorem 1.2** and let us reduce them to a more computationally friendly theorem. Since the $F$-pure threshold is invariant under base change and linear change of variables, we can assume $K = \overline{K}$. In light of **Proposition 3.3**, the polynomials in these statements can be fixed to have the form $x y (x + y)(x + ay)$ or $x y^p(x + y)^p(x + ay)^p$ respectively, as 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 $\infty$ since the roots are all distinct. The equivalent statement we get is:

**Theorem 3.5.** 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:

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

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 1.1** is a special case of **Theorem 3.5** 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 $a = L = 1, b = 2$; however the computation is not direct. The proof of the general **Theorem 3.5** follows next where the $p = 2$ special case is proven right after.

**Proof.** The key observation is that for a positive integer $N$, we use **Lemma 3.4** and **Lemma 3.2** to deduce:

$$
(3.5.2) \quad f_a^N = x^{bN} y^{cN}((x + y)(x + ay))^{cN} = x^{(b+c)N} y^{(b+c)N} H\{cN\}(a) + I
$$

where $I$ is an element in the ideal $(x^{(b+c)N+1}, y^{(b+c)N+1})$. 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 (3.5.2), combined with **Lemma 3.1** we get the $N/p^e = \frac{1}{b+c} \frac{p^e - 1}{p^e}$ 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 $cN$:

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

Note that $n = \frac{c(p-1)}{b+c}$ is between 0 and $p - 1$. Ergo, by **Lemma 2.3**

$$
H\{cN\}(a) = H\{(\frac{c}{b+c}(p^e - 1))(a)\} = (H\{n\}(a))^g \neq 0
$$

where $g$ is the resulting positive integer exponent (its exact value is not important). 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 (3.5.2) and (3.5.3) we see that $H\{cN\}(a) = 0$ and thus $f_a^N \in (x^{p^e}, y^{p^e})$, 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, first apply an appropriate change of coordinates, if needed, to ensure that $b \geq c$. Now, recall Lemma 2.5. Note that $n < p/2$ and $H\{n\}(a) = 0$, thus $H\{n-1\}(a) \neq 0$. Since $c < p$, and $p$ is a prime, there is a power of $p$ that is congruent to 1 mod $c$. Denote it as $p^d$. For an integer $m$, $p^{md} \equiv 1 \pmod{c}$ and thus we define:

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

because $c$ divides $n$.

Now, consider the integer

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

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 $c$. By subtracting $\ell(1)$ from $N'$ we are making the $p^{d-1}$ digit become $(n - 1)$ instead of $(p - 1)$. Then 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 $N$:

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

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

were $L$ is some integer constant, not dependent on $e$. We are about to show that $N/p^e$ is a lower bound for an arbitrary large $e$, which will 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 2.3 we have:

$$H\{cN\} = H\{p - 1\}^{\text{some power}} H\{n - 1\}^{\text{some power}}.$$
However, the conclusion of Theorem 1.1 then:

This geometrical insight reveals the interesting property of the roots of $H$. (4.2.1) sends:

$$f(a)^{±1}, (1-a)^{±1}, \left(\frac{a}{a-1}\right)^{±1}.$$ 

Corollary 4.1.

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

$$a^{±1}, (1-a)^{±1}, \left(\frac{a}{a-1}\right)^{±1}.$$ 

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

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

Theorem 1.2 gives rise to another corollary; (this statement is also known in the context of Legendre polynomials).

Corollary 4.2. Fix a prime $p > 2$. Let choose $b, c \in \mathbb{Z}_{>0}$ such that $p \equiv 1 \pmod{(b+c))}$. Let $a \in \mathbb{F}_p - \{0,1\}$, 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 provides new proofs to 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 $\mathbb{P}_K^1$. The linear change of variables needed to get the form

$$f_a = xy(x+y)(x+ay)$$

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:

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

Since the roots are all distinct, $a$ is not 0, 1 or $\infty$. Notice that $a$ depends on the order we had chosen for the roots. Considering all possible orders, we can get the same form (4.2.1) 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 (4.2.1), we conclude that:

$$FT(f_a) = FT(f_{1/a}) = FT(f_{1-a}) = FT(f_{1/(1-a)}) = FT(f_{a/(a-1)}) = FT(f_{(a-1)/a}).$$

However, the conclusion of Theorem 1.1 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 $\mathbb{F}_p$ mentioned in the first statement of Corollary 4.1. Note that $H\{n\}(a) = 0 \iff H\{n\}(1/a) = 0$ is expected due to the symmetry in Definition 2.1.

(4.2.2)

$$H\{n\}(\lambda) = \lambda^n H\{n\}(1/\lambda),$$

but the inferring on the rest of the roots in (4.1.1) is not at all trivial. The second statement of Corollary 4.1 is obtained by rewriting the first statement using (4.2.1).
A similar analysis, performed in the case of Theorem 1.2 gives us Corollary 4.2. Consider a homogeneous polynomial over $K[x, y]$, $K = K$, with 4 distinct (ordered) roots $(z_1, z_2, z_3, z_4)$ over $K$ of multiplicities $b, b, c, c$ respectively. After a linear change of variables the polynomial adopts the form:

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

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:

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

Considering the result in Theorem 1.2 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 $\infty$ has to have the same multiplicity to obtain the form (4.2.3), 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 4.2. The argument presents a new proof of a known fact in the context of Legendre polynomials.

REFERENCES


Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109-1043, USA

Email address: gpagi@umich.edu