Optimality of Root Spacing and Complexity Bounds for Trinomials over $p$-adic Fields

Elliott Fairchild

July 2021

Abstract

For a univariate trinomial $f(x) = c_1 + c_2x^{a_2} + c_3x^{a_3}$, we review a method to lift degenerate roots of $f$ over $\mathbb{Z}/(p)$ to roots of $f$ over $\mathbb{Q}_p$. We use this technique to show partial optimality of the logarithmic root closeness bound of $-O(p \log^2(a_3H) \log_p(a_3))$ recently proven by Rojas and Zhu, and give full optimality of a bound on the efficiency of this technique.

1 Introduction

Let $f(x) = c_1 + c_2x^{a_2} + c_3x^{a_3} \in \mathbb{Z}[x]$, $0 < a_2 < a_3$, be a univariate trinomial. Computing bounds on the distances between roots of $f$ over $\mathbb{Q}_p$ induces faster solving $f$, which in turn encodes fast solving over $\mathbb{Z}/(p^k)$, a problem with applications in number theory and coding theory (see, e.g., [3, 6, 1]). Recent work of Rojas and Zhu [5] has shown that for $\zeta_1, \zeta_2$ roots of $f$, $\log|\zeta_1 - \zeta_2|_p \geq -O(p \log^2(a_3H) \log_p(a_3))$. We examine the optimality of this bound.

**Theorem 1.1.** Let $f, p, H$ be as above, $\zeta_1, \zeta_2$ roots of $f$. Then $\log|\zeta_1 - \zeta_2|_p = -\Omega(\log \max\{a_3, H\})$

Our result shows at least a linear dependence on $a_3, H$. We are currently unaware of any examples with $\log|\zeta_1 - \zeta_2|_p = -\Omega(p^\epsilon)$ for some $\epsilon > 0$.

We now give the tools and definitions relevant to our result. First, we recall the classical Hensel’s lemma:

**Lemma 1.2.** (See, e.g., [2, Thm. 4.1 & Inequality (5.7)].) Let $f(x) \in \mathbb{Z}[x]$ and suppose $a \in \mathbb{Z}_p$ satisfies

$$f(a) = 0 \mod p, \quad f'(a) \neq 0 \mod p.$$  

Then there is a unique $\alpha \in \mathbb{Z}_p$ such that $f'(\alpha) = 0$ in $\mathbb{Z}_p$ and $\alpha = a \mod p$.

We next define a structure first introduced in [4] to extend Hensel’s lemma to degenerate roots. We let $\text{ord}_p : \mathbb{C}_p \to \mathbb{Q}$ be the standard $p$-adic valuation on $\mathbb{C}_p$.  


Definition 1.3. [4] Let $f \in \mathbb{Z}[x]$ and let $\bar{f}$ be its reduction mod $p$. For a degenerate root $\zeta \in \mathbb{F}_p$ of $\bar{f}$, define $s(f, \zeta) := \min_{i \geq 0} \{ i + \text{ord}_p f(i)(\zeta) \}$. For $k \in \mathbb{N}, i \geq 1$, define inductively a set $T_{p,k}(f)$ of pairs $(f_{i-1,\mu}, k_{i-1}) \in \mathbb{Z}[x] \times \mathbb{N}$ as follows: Set $(f_{0,0}, 0) := (f, k)$, then for $i \geq 1$ with $(f_{i-1,\mu}, k_{i-1}) \in T_{p,k}(f)$, and any degenerate root $\zeta_{i-1} \in \mathbb{F}_p$ with $s_{i-1} := s(f_{i-1,\mu}, \zeta_{i-1})$, let $\zeta := \mu + \zeta_{i-1}p^{-i}, k_i, \zeta := k_{i-1, \mu} - s_{i-1}, f_i, \zeta(x) := p^{-s(f_{i-1,\mu}, \zeta_{i-1})} f_{i-1,\mu}(\zeta_{i-1} + px) \mod p^{k_i},$ and include $(f_i, \mu, k_i, \zeta)$ in $T_{p,k}(f)$.

The pairs $(f_i, \mu, k_i, \zeta)$ form the nodes of a tree structure, which we now define.

Definition 1.4. [4] Define $T_{p,k}(f)$ inductively as follows:
(i) Set $f_{0,0} = f, k_{0,0} = k$, and let $(f_{0,0}, k_{0,0})$ be the label of the root node of $T_{p,k}(f)$.
(ii) The non-root nodes of $T_{p,k}(f)$ are labeled uniquely by the $(f_{i,\zeta}, k_i, \zeta) \in T_{p,k}(f)$ for $i \geq 1$.
(iii) There is an edge from node $(f_{i,\zeta}, k_i, \zeta)$ to node $(f_{j,\zeta}, k_j, \zeta)$ iff there is a degenerate root $\zeta_{i-1} \in \mathbb{F}_p$ of $f_{i,\zeta}$ with $s(f_{i,\zeta}, \zeta_{i-1}) \in \{2, \ldots, k_{i-1,\mu} - 1\}$ and $\zeta = \mu + \zeta_{i-1}p^{-i}$.

Example 1.5. Consider the binomial $f_{0,0} = f(x) = x^9 - 1$ over $\mathbb{Z}_3$, and let $k_{0,0} \geq 4$. Then 1 is the degenerate root of $f$ mod 3. We find $s(f, 1) = 3$, and $f_{1,1} = 3^{-3}((1 + 3x)^9 = x \mod 3$. As the root 0 of $f_{1,1}$ is non-degenerate, the root $1 + 0 \cdot 3 + \ldots$ lifts by Hensel’s Lemma. Further, this is the only root of $f$ in $\mathbb{Z}_3$.

The nodes of $T_{p,k}(f)$ indeed encode the base-p digits of roots $f$ over $\mathbb{Z}_p$.

Lemma 1.6. [4, Lem. 2.2 \& 6] Suppose $f \in \mathbb{Z}[x] \setminus p\mathbb{Z}[x]$ has degree $d, f_{0,0} := f, i \geq 1, \mu := \zeta_0 + \cdots + p^{-i-2}\zeta_{i-2}$ is a root of the mod $p^{-i}$ reduction of $f$, $\zeta' := \mu + p^{-i}\zeta_{i-1}$, the pairs $(f_{i-1,\mu}, k_{i-1})$ and $(f_{i-1,\zeta'}, k_{i-1})$ both lie in $T_{p,k}(f)$, and $\zeta_{i-1}$ has multiplicity $m$ as a root of $f_{i-1,\mu}$ in $\mathbb{F}_p$. Then $T_{p,k}(f)$ has depth $\lfloor (k - 1)/2 \rfloor$ and at most $\lceil d/2 \rceil$ nodes at depth $i \geq 1$. Also, deg $f_{i,\zeta'} \leq s(f_{i-1,\mu}, \zeta_{i-1}) \leq \min \{ k_{i-1,\mu}, m \}$, and $f_{i,\zeta}p^{-s} f(\zeta_0 + \zeta_1 p + \cdots + \zeta_{i-1} p^{i-1}) \geq 2i$. In particular, $f(\zeta_0 + \zeta_1 p + \cdots + \zeta_{i-1} p^{i-1}) = 0 \mod p^i$.

The first statement of the lemma above implies that $k$ must be sufficiently large for the depth of $T_{p,k}(f)$ to be large enough to detect non-degenerate roots of $f$ (if they exist). For any binomial $f = c_0 + c_1 x^d$ with $c_0 c_1 \neq 0 \mod p$, it is known that $T_{p,k}(f)$ has depth at most 1, and that $k > s(f_{0,0}, \zeta_0)$ is large enough for $T_{p,k}(f)$ to achieve its maximal depth. For trinomials, such a sufficiently large $k$ is determined in [5].

Proposition 1.7. [5, Coroll. 6.6] Suppose $f(x) = c_1 + c_2 x^{a_2} + c_3 x^{a_3} \in \mathbb{Z}[x]$ has degree $d, 0 < a_2 < a_3, p \mid c_1 c_2 c_3$. Let $S_0$ be the maximum of $s(f, \zeta_0)$ for any degenerate root of $f$ over $\mathbb{Z}/p$, and define $D$ to be the maximum of $\text{ord}_p(\zeta_1 - \zeta_2)$ over all distinct non-degenerate roots $\zeta_1, \zeta_2$ of $f$ over $\mathbb{Z}_p$, or 0 if
there are fewer than two distinct non-degenerate roots of \( f \). Finally, define \( M_p \) to be 4, 3, 2, according to \( p = 2, p = 3, p \geq 5 \). Then

\[
    k \geq 1 + S_0 \min\{1, D\} + M_p \max\{D - 1, 0\}
\]
guarantees \( T_{p,k}(f) \) has depth \( \geq D \).

As the complexity of solving algorithms is dependent on \( k \) [5], our goal is to determine the smallest \( k \) so that \( T_{p,k}(f) \) has depth \( D \) as above. It turns out that the \( k \) given above is optimal:

**Theorem 1.8.** For \( p \geq 5 \), there exist trinomials \( f = c_1 + c_2 x^{a_2} + c_3 x^{a_3} \) such that \( T_{p,k}(f) \) has depth \( \geq D \implies k \geq 1 + S_0 \min\{1, D\} + M_p \max\{D - 1, 0\} \).

## 2 Proofs

We prove Theorems 1 and 2 by examining the trees of two families of examples.

**Example 2.1.** Consider the family \( g_p(x) = x^2 - (2 + p')x + 1 + p' \). Constructing \( T_{p,k}(g_p) \) with \( f_{0,0} = g_p \), we see that \( f_{0,0} = x^2 - 2x + 1 \), so that 1 is the unique degenerate root of \( f_{0,0} \). We obtain \( s(f_{0,0}, 1) = 2 \), and compute \( k_{1,1} = k_{0,0} - 2 \) and \( f_{1,1} = p^{-2}((1 + px)^2 - (2 + p')x + 1 + p') = p^{-2}(p^2x^2 - p'x) = x^2 - p^{-1}x \mod p^{k_{1,1}} \). Proceeding, we find \( s(f_{1,1}, 0) = 2 \), \( k_{1,1} = k_{1-1,1} - 2 \), and \( f_{i,1} = x^2 - p^{i-1}x \mod p^{k_{1,1}} \) for all \( i > 1 \). At \( i = j \), \( f_{j,1+\ldots+0} = x^2 - x \), so that we obtain non-degenerate roots 1 and \( 1 + p' \) that lift uniquely by Hensel’s Lemma. Clearly, it is necessary that \( k \geq 1 + 2j = 1 + 2(2j - 1) = 1 + 2 + 2(j - 1) = 1 + S_0 + 2D \) for the roots to be discovered, and that \( |\log((1 + p') - 1)|_p = O(\log(H - 2)) \).

**Example 2.2.** Consider now the family \( h_p(x) = x^{2+p'} - 2x + 1 \). We again set \( f_{0,0} = h_p \) and have that 1 is a degenerate root of \( f_{0,0} \), and compute \( s(f_{0,0}, 1) = 2 \), \( k_{1,1} = k_{0,0} - 2 \), \( f_{1,1} = p^{-2}((1 + px)^2 + p' - 2(1 + px)) = p^{-2}(p^{j+1}x + (p^j + 2)(p^j + 1)p^j x^2 + \text{higher order terms}) = p^{-j-1}x^2 + x^2 \mod p^{k_{1,1}} \). We note that the "higher order terms" in the binomial expansion of \( f_{1,1} \) are killed off in its reduction mod-\( p \). We then have \( s(f_{1,1}, 1) = 2 \), \( k_{2,1} = k_{1,1} - 2 \) and see that all higher order terms of \( f_{1,1} \) increase in powers of \( p \) in \( p^{-2}f_{1,1}(px) \), so that more terms disappear mod \( p^{k_{2,1}} \). Proceeding, we see that for \( i > 1 \), \( s(f_{i,1-1}, 0) = 2 \), \( k_{i,1} = k_{i-1,1} - 2 \), and \( f_{i,1} = p^{i-1}x + x^2 \). At \( i = j \), we obtain non-degenerate roots 1 and \( 1 + (p - 1)p' \) that lift uniquely by Hensel’s Lemma, yielding a necessary \( k \geq 1 + 2j = 1 + 2 + 2(j - 1) = 1 + 2 + 2(j - 1) = 1 + S_0 + 2D, \) and \( |\log((1 + (p - 1)p') - 1)|_p = O(\log(a_3 - 2)) \).

## 3 Future directions

It is not a priori clear if the phenomena described in either of the theorems occur generically, or if there is a particular relation between the coefficients and degrees of monomial terms of \( f \) that governs this extremal behavior. One immediate
direction to pursue is numerical testing of random $f$ - namely, one implements the root solving algorithms described in [5] and determines for which $f$ root spacing and $k$ are extremal. As we are currently unaware of any trinomials with attaining the full $O(p \log^2(a_3H) \log_p(a_3))$ bound, numerical experiments could serve to find examples with even more tightly packed roots.

It is unclear what the relationship between the necessary $k$ for depth $D$ and the closeness of roots is; while both families of examples provided achieve both extremes simultaneously, it is not obvious that the relationship holds for all extremal $f$. Heuristically, it makes sense that that large $k$ and close roots are related - both come from a tree with high depth. Making more precise this relationship would provide information on when either of the phenomena occur.

4 Acknowledgements

I would like to thank Professor Maurice Rojas for his constant support and patience in answering my many questions throughout this project. I would also like to thank Josh Goldstein in helping me through my technical difficulties throughout the REU. I am grateful for Texas A&M University and NSF NSF REU grant DMS-1757872 for providing me with and supporting me through this opportunity.

References


