CONSTRUCTING TOTALLY $p$-ADIC NUMBERS OF SMALL HEIGHT

S. CHECCOLI AND A. FEHM

Abstract. Bombieri and Zannier gave an effective construction of algebraic numbers of small height inside the maximal Galois extension of the rationals which is totally split at a given finite set of prime numbers. They proved, in particular, an explicit upper bound for the lim inf of the height of elements in such fields. We generalize their result in an effective way to maximal Galois extensions of number fields with given local behaviour at finitely many places.

1. Introduction

Let $h$ denote the absolute logarithmic Weil height on the field $\overline{\mathbb{Q}}$ of algebraic numbers. We are interested in explicit height bounds for elements of $\overline{\mathbb{Q}}$ with special local behaviour at a finite set of primes. The first result in this context is due to Schinzel [Sch73] who proved a height lower bound for elements in the field of totally real algebraic numbers $\mathbb{Q}^{tr}$, the maximal Galois extension of $\mathbb{Q}$ in which the infinite prime splits totally. More precisely, he showed that every $\alpha \in \mathbb{Q}^{tr}$ has either $h(\alpha) = 0$ or

$$h(\alpha) \geq \frac{1}{2} \log \left( \frac{1 + \sqrt{5}}{2} \right).$$

Explicit upper and lower bounds for the limit infimum of the height of algebraic integers in $\mathbb{Q}^{tr}$ are given in [Smy80, Smy81, Fla96].

In [BZ01] Bombieri and Zannier investigate the analogous problem for the $p$-adic numbers. More precisely, in [BZ01, Theorem 2] they prove the following:

Theorem 1.1 (Bombieri–Zannier). Let $p_1, \ldots, p_n$ be distinct prime numbers, for each $i$ let $E_i$ be a finite Galois extension of $\mathbb{Q}_{p_i}$, and $L$ the maximal Galois extension of $\mathbb{Q}$ contained in all $E_i$. Denote by $e_i$ and $f_i$ the ramification index and inertia degree of $E_i/\mathbb{Q}_{p_i}$. Then

$$\liminf_{\alpha \in L} h(\alpha) \geq \frac{1}{2} \sum_{i=1}^{n} \frac{\log(p_i)}{e_i(p_i^{f_i} + 1)}.$$

In the special case $E_i = \mathbb{Q}_{p_i}$, Bombieri and Zannier in [BZ01, Example 2] show that the lower bound in Theorem 1.1 is almost optimal. More precisely:

Theorem 1.2 (Bombieri–Zannier). Let $p_1, \ldots, p_n$ be prime numbers and let $L$ be the maximal Galois extension of $\mathbb{Q}$ contained in all $\mathbb{Q}_{p_i}$. Then

$$\liminf_{\alpha \in L} h(\alpha) \leq \sum_{i=1}^{n} \frac{\log(p_i)}{p_i - 1}.$$

Other proofs, refinements and generalizations were given in [Fil14, Pot15, FP15, FP19, PS19]. See also [Smy07] for a general survey on the height of algebraic numbers. In Remark 1.4 we will discuss in detail the contribution [Fil14] and how it compares to our work.
The goal of this note is to generalize in an effective way the upper bound Theorem 1.2 to general $E_i$, and to further replace the base field $\mathbb{Q}$ by an arbitrary number field. Our main result is the following:

**Theorem 1.3.** Let $K$ be a number field and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct primes ideals of the ring of integers $\mathcal{O}_K$ of $K$. For each $i$, let $E_i$ be a finite Galois extension of the completion $F_i$ of $K$ at $\mathfrak{p}_i$. Denote by $e_i$ and $f_i$ the ramification index and the relative inertia degree of $E_i/F_i$ and write $q_i = [\mathcal{O}_K/\mathfrak{p}_i] = p_i^{f_i(p_i^{1/f_i})}$. Then for the maximal Galois extension $L$ of $K$ contained in all $E_i$,

$$\liminf_{\alpha \in L} h(\alpha) \leq \sum_{i=1}^n \frac{f(p_i|p_i)}{[K : \mathbb{Q}]} \frac{\log(p_i)}{e_i(q_i^{f_i} - 1)}.$$

More precisely, let

$$C = \max \left\{ [K : \mathbb{Q}], \Delta_K, \max_i (e_if_i), \max_i q_i^{f_i} \right\},$$

where $\Delta_K$ is the absolute discriminant of $K$. Then for every $0 < \epsilon < 1$ there exist infinitely many $\alpha \in \mathcal{O}_L$ of height

$$(1.1) \quad h(\alpha) \leq \sum_{i=1}^n \frac{f(p_i|p_i)}{[K : \mathbb{Q}]} \frac{\log(p_i)}{e_i(q_i^{f_i} - 1)} + 13nC^{2n+2} \frac{\log ([K(\alpha) : K])}{[K(\alpha) : K]} + \left\{ \begin{array}{ll}
0, & n = 1 \\
n\epsilon, & n > 1. \end{array} \right.$$ $\forall\epsilon$

Namely, for every $\rho \geq 3C^n$ there exists such $\alpha$ of degree

$$(1.2) \quad \rho \leq [K(\alpha) : K] \leq \begin{cases}
C\rho, & n = 1 \\
\frac{(4 \log C)^{n+1}}{n^{\log^2(1+\epsilon)}}, & n > 1.
\end{cases}$$

Note that in the special case $K = \mathbb{Q}$ and $E_i = \mathbb{Q}_{p_i}$ we reobtain Theorem 1.2 except that Theorem 1.3 appears stronger in that the result is effective and the limit can be taken over algebraic integers. However, an inspection of the proof of Bombieri and Zannier shows that it is effective as well and does in fact produce algebraic integers.

**Remark 1.4.** Theorem 1.3 provides an effective version of a result of Fili [Fil14, Theorem 1.2]. The bound in that result seems to differ from ours by the factor $e(p_i|p_i)$, and [Fil14, Theorem 1.1] (and similarly [FP15, Theorem 9]) also states a variant of Theorem 1.1 which contradicts our Theorem 1.3 but according to Paul Fili (personal communication) this is merely an error in normalization in [Fil14] and [FP15] that became apparent when comparing to our result, and the $e_i$ in the denominator of Theorems 1.1, 1.2, and Conjecture 1 of [Fil14] (and similarly in the statements of [FP15]) should have been the absolute instead of the relative ramification index. When this correction is made, the lower bound of [Fil14, Theorem 1.1] agrees with the one in [FP19, Theorem 13], and the upper bound of [Fil14, Theorem 1.2] agrees with the one in Theorem 1.3.

In any case, Fili’s proof of [Fil14, Theorem 1.2] uses capacity theory on analytic Berkovich spaces and does not provide explicit bounds on the degree and the height of a sequence of integral elements in the lim inf. Instead, our effective proof is more elementary and is inspired by Bombieri and Zannier’s effective proof of Theorem 1.2. To the best of our knowledge, Theorem 1.3 is the only result currently available that gives a bound on the height in terms of the degree of such a sequence of $\alpha$, except for the case

where $K = \mathbb{Q}$ and $E_i = \mathbb{Q}_{p_i}$ for all $i$, where such a bound can be deduced from [BZ01].

We also remark that our use of [Fil14, Theorem 1.2] in [CF21] is limited to the cases where [Fil14, Theorem 1.2] agrees with Theorem 1.3.
The paper is organised as follows. In Section 2 we collect all the preliminary results needed to prove Theorem 1.3, namely: a consequence of Dirichlet’s theorem on simultaneous approximation (Proposition 2.1), a bound for the size of representatives in quotient rings of rings of integers (Proposition 2.2), a variant of Hensel’s lemma (Proposition 2.3), a bound for the height of a root of a polynomial defined over a number field in terms of its coefficients (Proposition 2.4), and a construction of special Galois invariant sets of representatives of residue rings of local fields (Proposition 2.5).

The proof of Theorem 1.3 is carried out in Section 3. We briefly sketch it here for clarity. Following Bombieri and Zannier’s strategy, given \( \rho \geq 3C^n \) we construct a monic irreducible polynomial \( g \in \mathcal{O}_K[X] \) such that

(i) its degree is upper and lower bounded in terms of \( \rho \) as the degree of \( \alpha \) in Theorem 1.3,

(ii) the complex absolute value of all conjugates of its coefficients is sufficiently small, and

(iii) all its roots are contained in all \( E_i \).

In Bombieri and Zannier’s proof of Theorem 1.2, (i) and (ii) were achieved by using the Chinese Remainder Theorem to deform the polynomial \( \prod_{i=1}^{\rho} (X - i) \) into an irreducible polynomial of the same degree with coefficients small enough to give the desired bound for the height of the roots. Then a variant of Hensel’s lemma was applied to show that the roots of the constructed polynomial are still in \( \mathbb{Q}_p \) for each \( i \).

In our generalisation, the degree of the polynomial is carefully chosen to obtain (i) in Section 3.1 via Proposition 2.1 (necessary only if \( n > 1 \), which leads to the better bounds in the case \( n = 1 \)). The polynomial \( g \) satisfying (ii) is then constructed in Section 3.2. We start with polynomials \( \prod_{\alpha \in A_i} (X - \alpha) \), where now \( A_i \subseteq \mathcal{O}_{E_i} \) is a set constructed using Proposition 2.5. These polynomials are then merged into an irreducible polynomial \( g \) by applying the Chinese Remainder Theorem and Proposition 2.2 to bound the size of its coefficients. Property (iii) is verified in Section 3.3 using Proposition 2.3. Finally, Proposition 2.4 is applied to show that \( g \) has a root \( \alpha \) of height bounded from above as desired.

2. Notation and preliminaries

We fix some notation. If \( K \) is a number field or a non-archimedean local field we let \( \mathcal{O}_K \) denote the ring of integers of \( K \). For an ideal \( \mathfrak{a} \) of \( \mathcal{O}_K \) we denote by \( N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}| \) its norm. For a nonzero prime ideal \( \mathfrak{p} \) of \( \mathcal{O}_K \), we denote by \( v_\mathfrak{p} \) the discrete valuation on \( K \) with valuation ring \( (\mathcal{O}_K)_\mathfrak{p} \) normalized such that \( v_\mathfrak{p}(K^\times) = \mathbb{Z} \). If \( L/K \) is an extension of number fields and \( \mathfrak{P} \) is a prime ideal of \( \mathcal{O}_L \) lying above a prime ideal \( \mathfrak{p} \) of \( \mathcal{O}_K \) we denote by \( e(\mathfrak{P} | \mathfrak{p}) \) and \( f(\mathfrak{P} | \mathfrak{p}) \) the ramification index and the inertia degree. For an extension \( E/F \) of non-archimedean local fields we denote the ramification index and the inertia degree also by \( e(E/F) \) and \( f(E/F) \).

2.1. Auxiliary results. In this section we collect the preliminary results we need to prove Theorem 1.3. These results are not related to each other and we list them in this section following their order of appearance in the proof of Theorem 1.3.

Proposition 2.1. Let \( x_1, \ldots, x_n \) be integers greater than 1. For every \( \rho \geq 3 \) and \( 0 < \epsilon < 1 \) there exist positive integers \( r, k_1, \ldots, k_n \) such that \( r \geq \rho \) and, for all \( i \), \( r \leq x_i^{k_i} \leq (1+\epsilon)r \) and

\[
k_i \leq \frac{2^{2n+1} \log^n \left( \max_j x_j \right) \log(\rho)}{\log(x_i) \log^n (1+\epsilon)}.
\]
Proposition 2.2. Let $K$ be a number field of degree $m = [K : \mathbb{Q}]$. Given a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, there exists a set of representatives $A$ of $\mathcal{O}_K/\mathfrak{a}$ such that, for every $a \in A$ and every $\sigma \in \text{Hom}(K, \mathbb{C})$, one has

$$|\sigma(a)| \leq \delta_K N(a)^{1/m}$$

where $\delta_K = m^{3/2} (m(m-1))^{1/4} \sqrt{\Delta_K}$.

Proof. This is an immediate consequence of well-known results on lattice reduction. For instance, [BFH17, Proposition 15] gives for every $\alpha \in \mathcal{O}_K$, an element $a \in \mathcal{O}_K$ with $\alpha - a \in \mathfrak{a}$ such that

$$\sqrt{\sum_{\sigma} |\sigma(a)|^2} \leq \frac{1}{\ell} m^2 \frac{m(m-1)}{2} \sqrt{\Delta_K} N(a)^{1/m}$$

where $\ell$ depends on certain parameters $\eta \in (1/2, 1)$, $\delta \in (\eta^2, 1)$ and $\theta > 0$ coming from applying a variant of the LLL-reduction algorithm as in [CSV12, Theorem 5.4] and [NSV11, Theorem 7] (see also [BFH17, §4, p.595]) to a $\mathbb{Z}$-basis of $\mathfrak{a}$. In particular, choosing $\eta = 2/3$, $\delta = 7/9$ and $\theta = (\sqrt{19} - 4)/3$, we have $\ell = 2$, which gives the claimed upper bound for $|\sigma(a)|$. \hfill $\Box$

The following proposition is a variant of Hensel’s lemma.

Proposition 2.3. Let $E$ be a finite extension of $\mathbb{Q}_p$, $\mathfrak{P}$ the maximal ideal of $\mathcal{O}_E$ and $v = v_{\mathfrak{P}}$. Let $f \in E[X]$ and $x_0 \in E$. Assume there exist $a, b \in \mathbb{Z}$ such that

(i) $v(f(x_0)) > a + b$,

(ii) $v(f(x_0)) \leq a$,

(iii) $v(f(x_0)) \geq a - (\nu - 1)b$ for every $\nu \geq 2$.

Then there exists $x \in E$ with $f(x) = 0$ and $v(x - x_0) > b$.

Proof. This can be proved precisely as the special case $E = \mathbb{Q}_p$ in [BZ01, Lemma 1]. Alternatively, one can reduce this to one of the standard forms of Hensel’s lemma as follows. Let $\beta \in E$ with $v(\beta) = b$ and $g(X) := (\beta f(x_0))^{-1} f(\beta X + x_0)$ is in $\mathcal{O}_E[X]$ by (i)-(iii) and has a simple zero $X = 0$ modulo $\mathfrak{P}$ by (i) and (ii), hence by Hensel’s lemma $g$ has a zero $x' \in \mathfrak{P}$, and $x = \beta x' + x_0$ is then the desired zero of $f$. \hfill $\Box$

The final proposition in this subsection gives a bound for the height of the roots of a polynomial with small algebraic coefficients.

Proposition 2.4. Let $K$ be a number field and let $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0 \in \mathcal{O}_K[X]$. If $B \geq 1$ with $|\sigma(a_i)| < B$ for every $i$ and every $\sigma \in \text{Hom}(K, \mathbb{C})$, then $f$ has a root $\alpha$ with

$$h(\alpha) \leq \frac{\log(B\sqrt{m+1})}{4m}.$$
Proof. Let \( M_K = M_K^0 \cup M_K^\infty \) be the set of (finite and infinite) places of \( K \) and let \( d = [K : \mathbb{Q}] \). For a place \( v \in M_K \), denote by \( d_v = [K_v : \mathbb{Q}_v] \) the local degree. Let

\[
\hat{h}(f) = \log \left( \prod_{v \in M_K} M_v(f)^{d_v/d} \right)
\]

where if \( v \) is non-archimedean \( M_v(f) = \max_i |a_i|_v \), while if \( v \) is archimedean and corresponds to the embedding \( \sigma \in \text{Hom}(K, \mathbb{C}) \), \( M_v(f) \) is the Mahler measure \( M(\sigma(f)) \) of the polynomial \( \sigma(f) \).

By [Zan09, Appendix A, section A.2, pag. 210] we have that, if \( \alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}} \) are the roots of \( f \) (with multiplicities), then \( \hat{h}(f) = \sum_{i=1}^m h(\alpha_i) \) where \( h \) denotes the usual logarithmic Weil height. Thus, if \( \alpha \) is a root of \( f \) of minimal height, then

\[
(2.1) \quad h(\alpha) \leq \frac{\hat{h}(f)}{m}.
\]

Let \( \sigma_1, \ldots, \sigma_r \) and \( \tau_1, \tau_1, \ldots, \tau_s, \tau_s \) be, respectively, the real and pairwise conjugate complex embeddings of \( K \) in \( \mathbb{C} \), so that \( d = r + 2s \). As \( f \) has coefficients in \( \mathcal{O}_K \), \( M_v(f) \leq 1 \) if \( v \) is non-archimedean and we have that

\[
\hat{h}(f) \leq \log \left( \prod_{v \in M_K^\infty} M_v(f)^{d_v/d} \right) = \log \left( \prod_{i=1}^r M(\sigma_i(f))^{1/d} \cdot \prod_{j=1}^s M(\tau_j(f))^{2/d} \right) = \log \left( \prod_{\sigma \in \text{Hom}(K, \mathbb{C})} M(\sigma(f))^{1/d} \right).
\]

By [Zan09, Section 3.2.2, formula (3.7)] and by our hypothesis on \( B \), we have that \( M(\sigma(f)) \leq B \sqrt{m+1} \) for all \( \sigma \in \text{Hom}(K, \mathbb{C}) \), thus \( \hat{h}(f) \leq \log(B \sqrt{m+1}) \) and, plugging this bound into (2.1), we conclude. \( \square \)

2.2. Representatives of residue rings of local fields. This subsection contains the technical key result needed to construct the local polynomials in the proof of Theorem 1.2.3. Let \( E/F \) be a Galois extension of non-archimedean local fields with Galois group \( G \). Let \( \mathfrak{p} \) be the maximal ideal of \( \mathcal{O}_F \), \( \mathfrak{p} \) be the maximal ideal of \( \mathcal{O}_E \) and for \( k \in \mathbb{N} \) denote by \( \pi_k : \mathcal{O}_E \to \mathcal{O}_E/\mathfrak{p}^k \) the residue map.

It is known that one can always find a \( G \)-invariant set of representatives of the residue field \( \mathcal{O}_E/\mathfrak{p} \), e.g. the Teichmüller representatives. As long as the ramification of \( E/F \) is tame, one can also find \( G \)-invariant sets of representatives of each residue ring \( \mathcal{O}_E/\mathfrak{p}^k \), but if the ramification is wild, this is not necessarily so. We will therefore work with the following substitute for such a \( G \)-invariant set of representatives:

Proposition 2.5. Let \( E/F \) be a Galois extension of non-archimedean local fields and define \( G, \mathfrak{p}, \mathfrak{p}, \pi_k \) as above. Let \( d \) be a multiple of \( |G| \). There exists a constant \( c \) such that for every \( k \) there is \( A \subseteq \mathcal{O}_E \) such that

1. \( A \) is \( G \)-invariant,
2. all orbits of \( A \) have length \( |G| \),
3. \( \pi_k|A : A \to \mathcal{O}_E/\mathfrak{p}^k \) is \( d \)-to-1 and onto, and
4. \( \pi_k+1|A \) is injective.

Moreover, if \( F \) is a \( p \)-adic field, one can choose

\[
c \leq e(\mathfrak{p}|\mathfrak{p}) \left( d + |G| + \frac{e(\mathfrak{p}|\mathfrak{p})}{p-1} + 1 \right).
\]
Proof. Note that $G$ naturally acts on $O_E$ and on $O_E/P^k$, and that $π_k$ is $G$-equivariant. Fix some primitive element $α ∈ O_E$ of $E/F$ and a uniformizer $θ ∈ O_F$ of $v_p$, and let

$$
eq e(\mathfrak{P}|p),$$

$$c_0 = \max_{\mathfrak{P} \neq \mathfrak{O}G} v_\mathfrak{P}(α - σα), \text{ (with } c_0 = 0 \text{ if } G = 1),$$

$$c_1 = \lceil |G| + c_0/e \rceil, \text{ and}$$

$$c = e(d + c_1).$$

Let $k ∈ \mathbb{N}$ be given. The desired set $A$ is obtained by applying the following Claim in the case $X = O_E/P^k$:

**Claim.** For every $G$-invariant subset $X ⊆ O_E/P^k$ there exists a $G$-invariant subset $A ⊆ O_E$ with all orbits of length $|G|$ such that $π_{k+c}|A$ is injective and $π_k|A$ is $d$-to-1 onto $X$.

We prove the Claim by induction on $|X|$: If $X = \emptyset$, $A = \emptyset$ satisfies the claim. If $X ≠ \emptyset$ take $x ∈ X$ and let $X' = X \setminus Gx$, where $Gx$ denotes the orbit of $x$ under $G$. By the induction hypothesis there exists $A' ⊆ O_E$ satisfying the claim for $X'$. Choose $a ∈ π_k^{-1}(x)$ and let $k_0 = \lceil \frac{k}{e} \rceil$. Then

$$n_0 := \min\{ n ≥ 0 : v_\mathfrak{P}(a - σa) ≠ e(k_0 + n) + v_\mathfrak{P}(α - σα) \forall 1 ≠ σ ∈ G \} < |G|,$$

as $v_\mathfrak{P}(α - σa) - v_\mathfrak{P}(α - σα)$ attains less than $|G|$ many distinct values. Thus for $1 ≠ σ ∈ G$,

$$v_\mathfrak{P}((a + \theta_0^{k_0}α) - σ(a + \theta_0^{k_0}α)) = \min\{v_\mathfrak{P}(a - σa), e(n_0 + k_0) + v_\mathfrak{P}(α - σα)\} ≤ e(n_0 + k_0) + c_0 < k + ec_1,$$

so if we replace $a$ by $a + \theta_0^{k_0}α$, we can assume without loss of generality that $π_{k+c_1}$ is injective on $Ga$ and that $|Ga| = |G|$. If we now let

$$A = A' ∪ \{ σ(a) + \theta_0^{k_0+c_1+j} : σ ∈ G, 0 ≤ j < d/|Gx| \}$$

where $Gx$ is the stabilizer of $x$, then $π_k|A$ is $d$-to-1 onto $X = X' ∪ Gx$ and $A$ is $G$-invariant with all orbits of length $|G|$. As

$$k + ec_1 ≤ e(k_0 + c_1 + j) < k + c,$$

we have that $π_{k+c}|A$ is injective.

Now, if $F$ is a $p$-adic field and if we chose $α ∈ O_E$ to be also a generator of $O_E$ as a $O_F$-algebra, by [Ser80] Chap.IV, Ex. 3(c)], one has the explicit bound $c_0 ≤ e(\mathfrak{P}/p)/(p - 1)$ which implies the stated bound for $c$. □

**Remark 2.6.** Note that if (4) holds for some $c, k, A$, then also for $c', k, A$ for any $c' ≥ c$.

3. **Proof of Theorem 1.3**

Using the notation of Theorem 1.3 for every $1 ≤ i ≤ n$, let $\mathfrak{P}_i$ be the maximal ideal of $O_E_i$, $v_i$ the extension of $v_{\mathfrak{P}_i}$ to an algebraic closure of $E_i$, $G_i = \text{Gal}(E_i/F_i)$ and $d = \prod_{i=1}^{n} |G_i|$. Let $C$ be the constant from Theorem 1.3, note that $C ≥ 2$, and let $c = 4C^{n+1}$. Fix an integer $ρ ≥ 3C^n$ and note that $ρ/d ≥ 3$ since $d ≤ C^n$. If $n = 0$ let $ε = 0$, otherwise fix $0 < ε < 1$. 


3.1. Choosing the right degree. If \( n > 1 \) we apply Proposition 2.1 to \( x_i = q_i^{f_i} \) to obtain positive integers \( r > \rho/d \) and \( k_1, \ldots, k_n \) such that for every \( i \),

(i) \( r \leq q_i^{f_i k_i} \leq (1+\varepsilon)r \)

(ii) \( k_i \leq 2^{2(n+1)}(\log C)^n \frac{\log(\rho/d)}{\log(1+\varepsilon)} \),

where we used that, for every \( i \), \( \log 2 \leq \log(x_i) = \log(q_i^{f_i}) \leq \log(C) \). It follows that

\[
\log(\rho/d) \leq \log(r) \leq (4 \log C)^{n+1} \frac{\log(\rho/d)}{\log^\varepsilon(1+\varepsilon)}.
\]

If \( n = 1 \) we instead set \( r = q_1^{f_1 k_1} \), where \( k_1 = \lceil \log(\rho/d)/\log(q_1^{f_1}) \rceil \), so that (i) holds with \( \varepsilon = 0 \), and

\[
\log(\rho/d) \leq \log(r) \leq \log(\rho/d) + \log(q_1^{f_1}).
\]

Using that \((4 \log C)^{n+1} \geq \log^n(1+\varepsilon)\), we conclude

\[
\rho \leq dr \leq \begin{cases} C \rho, & n = 1 \\ \rho^{(4 \log C)^{n+1}}, & n > 1 \end{cases}
\]

3.2. Construction of the polynomial \( g \). We first want to prove the following:

Claim. For every \( i \), there exists a polynomial \( g_i \in \mathcal{O}_K[X] \) of degree \( dr \) whose set of roots \( A_i \) satisfies

(a) \( A_i \subseteq E_i \),

(b) \( v_i(\alpha - \beta) < k_i + c \) for all \( \alpha, \beta \in A_i \) with \( \alpha \neq \beta \), and

(c) \( v(g_i'() \alpha) \leq d \left( \frac{q_i^{f_i k_i - 1}}{q_i^{f_i - 1}} + c \right) \) for every \( \alpha \in A_i \).

Proof of the claim. As \( e(\mathfrak{P}_i) = (d + |G_i| + \frac{a_i |p_i|}{p_i - 1} + 1) \leq C(C^m + C + 1) \leq 4C^{m+1} = c \), by Proposition 2.5 there is a \( G_i \)-invariant set \( A_i' \subseteq \mathcal{O}_{E_i} \) with all orbits of length \( |G_i| \) such that \( A_i' \to \mathcal{O}_{E_i}/\mathfrak{P}_i^{k_i} \) is \( d \)-to-1 and \( A_i' \to \mathcal{O}_{E_i}/\mathfrak{P}_i^{k_i+c} \) is injective. As \( |A_i'| = dq_i^{f_i k_i} \), \( |G_i| \) divides \( d \), and \( r \leq q_i^{f_i k_i} \), there exists a \( G_i \)-invariant subset \( A_i \subseteq A_i' \) with \( |A_i| = dr \). Let

\[
\tilde{g}_i = \prod_{\alpha \in A_i} (X - \alpha) \in \mathcal{O}_{F_i}[X].
\]

We first prove that conditions (a)-(c) hold for \( \tilde{g}_i \) and the set \( \tilde{A}_i \), instead of \( g_i \) and \( A_i \). Note that \( \tilde{g}_i \in \mathcal{O}_{F_i}[X] \) is monic of degree \( dr \) and that condition (a) holds for \( \tilde{A}_i \) by construction. Moreover, as the map \( A_i \to \mathcal{O}_{E_i}/\mathfrak{P}_i^{k_i+c} \) is injective, we have that condition (b) is also satisfied for \( A_i \). As for condition (c), note that the valuation \( v_{\mathfrak{P}_i} \), on \( \mathcal{O}_{E_i} \), induces a map \( \tilde{v} : (\mathcal{O}_{E_i}/\mathfrak{P}_i^{k_i}) \setminus \{0\} \to \{0, \ldots, k_i - 1\} \) such that \( v_{\mathfrak{P}_i}(\gamma) = \tilde{v}(\pi_{E_i}(\gamma)) \) for all \( \gamma \in \mathcal{O}_{E_i} \setminus \mathfrak{P}_i^{k_i} \),
where \( \pi_k \) denotes the residue map \( \mathcal{O}_{E_i} \rightarrow \mathcal{O}_{E_i}/p_i^{k_i} \). Now
\[
v_{\psi_i}(\tilde{g}_i'(\alpha)) = \sum_{\alpha \neq \beta \in A_i} v_{\psi_i}(\alpha - \beta)
\]
\[
\leq \sum_{\alpha \neq \beta \in A_i'} v_{\psi_i}(\alpha - \beta)
\]
\[
\pi_{k_i}(\alpha) = \pi_{k_i}(\beta)
\]
\[
< (d - 1) \cdot (k_i + c) + d \cdot \sum_{0 \neq a \in \mathcal{O}_{E_i}/p_i^{k_i}} \bar{v}(a)
\]
and
\[
\sum_{0 \neq a \in \mathcal{O}_{E_i}/p_i^{k_i}} \bar{v}(a) = \sum_{j=0}^{k_i-1} |\{a : \bar{v}(a) = j\}| \cdot j = \sum_{l=1}^{k_i-1} \sum_{j=0}^{k_i-1} |\{a : \bar{v}(a) = j\}|
\]
\[
= \sum_{l=1}^{k_i-1} (q_{l}^{f_i(k_i-l)} - 1) = \sum_{l=0}^{k_i-1} q_{l}^{f_i-l} - k_i = \frac{1 - q_{l}^{f_i} k_i}{1 - q_{l}^{f_i}} - k_i
\]
and plugging this into the previous inequality gives condition \( (\text{c}) \) for \( \tilde{g}_i \).

As \( \mathcal{O}_K \) is dense in \( \mathcal{O}_{E_i} \) with respect to \( v_i \), we obtain a monic polynomial \( g_i \in \mathcal{O}_K[X] \) of degree \( dr \) arbitrarily close to \( \tilde{g}_i \). Let \( A_i \) be the set of roots of \( g_i \). By the continuity of roots [EP05, Theorem 2.4.7] we can achieve that the roots of \( g_i \) are arbitrarily close to the roots of \( \tilde{g}_i \), in particular that conditions \( (\text{b}) \) and \( (\text{c}) \) are satisfied by \( g_i \) and \( A_i \). Moreover, by Krasner’s lemma [Lan94, Ch.II, §2, Proposition 4], we can in addition achieve condition \( (\text{a}) \), completing the proof of the claim. \( \square \)

Now, let \( p_0 \) be the smallest prime number not in the set \( \{p_1, \ldots, p_n\} \) and let \( p_0 \) be a prime ideal of \( \mathcal{O}_K \) above \( p_0 \). Fix a monic polynomial \( g_0 \in \mathcal{O}_K[X] \) of degree \( dr \) whose reduction modulo \( p_0 \) is irreducible. Let
\[
m_i = \frac{d}{e_i} \left( \frac{q_{l}^{f_i k_i} - 1}{q_{l}^{f_i} - 1} + k_i + 2c \right)
\]
and
\[
a = p_0 p_1^{m_1} \cdots p_n^{m_n}.
\]
By the Chinese Remainder Theorem and Proposition 2.2, there exists a monic polynomial \( g \in \mathcal{O}_K[X] \) such that
\begin{enumerate}
\item \( \deg g = dr \),
\item \( g \equiv g_0 \mod p_0[X] \),
\item \( g \equiv g_i \mod p_i^{m_i}[X] \) for \( i = 1, \ldots, n \), and
\item \( |\sigma(a)| \leq \delta_K N(a)^{1/K-2} \sqrt{|\Delta_K|} \) for every coefficient \( a \) of \( g \) and every \( \sigma \in \text{Hom}(K, \mathbb{C}) \),
\end{enumerate}
where \( \delta_K = [K : \mathbb{Q}]^2 \frac{|K - \mathbb{Q}|}{|K - \mathbb{R}|} \sqrt{|\Delta_K|} \).
Note that \( (4) \) implies that \( g \) is irreducible. In particular, we get from \( (1) \) and \( (3.1) \) that every root \( \alpha \) of \( g \) satisfies the degree bound \( 1.2 \) of Theorem 1.3.
3.3. The roots of \( g \) are in \( E_i \) for every \( i \). We claim that the conditions of Proposition 2.3 hold for the field \( E_i \), the polynomial \( g \) and \( x_0 = \alpha \in A_i \) (which lies in \( E_i \) by condition (iii)) by setting \( a = v_i(g_i(\alpha)) \) and \( b = k_i + c - 1 \). Indeed, by (ii)

\[
(3.3) \quad a = v_i(g_i(\alpha)) \leq d \cdot \frac{q_i^{f_i k_i} - 1}{q_i^{f_i} - 1} + dc < e_i m_i - b,
\]

and, writing \( g - g_i = t_i \) with \( t_i \in p_i^{m_i}[]X \) by (ii) of Section 3.2 we have \( g(\alpha) = t_i(\alpha) \) and therefore \( v_i(g(\alpha)) \geq e_i m_i + a + b \), so condition (ii) holds. Similarly for condition (iii), we have \( g'(\alpha) = t'_i(\alpha) + g'_i(\alpha) \) and since

\[
v_i(t'_i(\alpha)) \geq e_i m_i > v_i(g'_i(\alpha)),
\]

we conclude that \( v_i(g'(\alpha)) = v_i(g'_i(\alpha)) = a \). Now for \( \nu \geq 2 \) write

\[
g_i(\nu)(\alpha) = \nu! g_i(\alpha) \sum_{B \subseteq A_i} \prod_{\beta \in B, \alpha \in B} (\alpha - \beta)^{-1}.
\]

Thus

\[
v_i(g_i(\nu)(\alpha)/\nu !) \geq a - (\nu - 1) \max_{\beta \neq \alpha} v_i(\alpha - \beta) \geq a - (\nu - 1)b
\]

where the last inequality holds by (ii). Moreover, using (3.3), we get

\[
v_i(t'_i(\nu)(\alpha)/\nu !) \geq e_i m_i - v_i(\nu!) \geq a + b - \frac{e(\mathfrak{p}_i | p_i) \nu}{p_i - 1} \geq a - (\nu - 1)b
\]

where the last inequality holds since \( b \geq c \geq \frac{e(\mathfrak{p}_i | p_i)}{p_i - 1} \). Thus

\[
v_i(g_i(\nu)(\alpha)/\nu !) \geq \min \left\{ v_i(g_i(\nu)(\alpha)/\nu !), v_i(t'_i(\nu)(\alpha)/\nu !) \right\} \geq a - (\nu - 1)b
\]

fulfilling condition (iii).

So Proposition 2.3 gives \( \alpha' \in E_i \) with \( g(\alpha') = 0 \) and \( v_i(\alpha' - \alpha) > b \). As \( v_i(\alpha - \beta) \leq b \) for all \( \beta \in A_i \setminus \{ \alpha \} \) by (ii), we conclude that \( \alpha' \neq \beta' \) for all \( \alpha \neq \beta \). Hence \( g \) has precisely \( |A_i| = dr \) many roots in \( E_i \). As this holds for every \( i \) and \( g \) totally splits in the maximal Galois extension \( L \) of \( K \) that is contained in all \( E_i \). Moreover, as \( g \in \mathcal{O}_K[X] \), all roots of \( g \) are actually in \( \mathcal{O}_L \).

3.4. Bounding the height of the roots of \( g \). From condition (iv) of Section 3.2 for every coefficient \( a \) of \( g \) and every \( \sigma \in \text{Hom}(K, \mathbb{C}) \), we have

\[
|\sigma(a)| \leq B := \delta_K N(p_0)^{1/[K:Q]} \cdot \prod_{i=1}^n N(p_i)^{m_i/[K:Q]}.
\]

By Proposition 2.4 \( g \) has a root \( \alpha \in \mathcal{O}_L \) with \( h(\alpha) \) bounded by

\[
\frac{\log(B \sqrt{\deg g + 1})}{\deg g} \leq \frac{\log(\delta_K N(p_0)^{1/[K:Q]} \sqrt{\deg g + 1})}{\deg g} + \sum_{i=1}^n \frac{m_i}{\deg g} \cdot \frac{\log(q_i)}{[K:Q]}
\]

By the definition of \( m_i \) in (3.2) and recalling \( \deg g = dr \) from (i), we have

\[
\frac{m_i}{\deg g} = \frac{1}{e_i} \cdot \frac{1}{q_i^{f_i k_i} - 1} \cdot \frac{q_i^{f_i k_i} - 1}{r} + \frac{k_i}{e_i r} + \frac{2c}{e_i r}.
\]

Condition (ii) of Section 3.2 implies that

\[
\frac{q_i^{f_i k_i} - 1}{r} \leq 1 + \epsilon.
\]
Moreover,
\[
\frac{k_i}{e_i r_f} = \frac{\log(q_i^{f_i} )}{e_i r_f \log(q_i)} \leq \frac{2d}{e_i r_f \log(q_i)} \cdot \frac{\log(\deg g)}{\deg g} \leq 3C n \frac{\log(\deg g)}{\deg g}
\]

Finally,
\[
\frac{2c}{e_i r_f} \leq \frac{8d C^{n+1}}{e_i \deg g} \leq \frac{8C^{2n+1}}{\deg g}.
\]

Therefore, substituting in (3.5), and recalling that \( C \geq 2 \) and \( \rho \geq 3 \), we have
\[
\frac{m_i}{\deg g} \leq \frac{1}{e_i (q_i^{f_i} - 1)} + \frac{\epsilon}{e_i (q_i^{f_i} - 1)} + 11C^{2n+1} \frac{\log(\deg g)}{\deg g}.
\]

Thus the second summand in (3.4) can be bounded as
\[
\sum_{i=1}^{n} \frac{m_i}{\deg g} \frac{\log(q_i)}{[K : Q]} \leq \sum_{i=1}^{n} \frac{f(p_i | p_i)}{[K : Q]} \cdot \frac{\log(p_i)}{e_i (q_i^{f_i} - 1)} + n \epsilon + 11nC^{2n+2} \frac{\log(\deg g)}{\deg g}.
\]

As for the first summand in (3.4), note that \( N(p_0)^{1/[K : Q]} \leq p_0 \) where \( p_0 \) is the smallest prime number not in the set \( \{ p_1, \ldots, p_n \} \), which, by Bertrand’s postulate, can be bounded by \( p_0 < 2 \max_i p_i \leq 2C \). Moreover,
\[
\delta_K = \lceil K : Q \rceil^{\frac{1}{2}} \sqrt{|\Delta_K|} \leq C^2 \cdot 2^{\frac{C_1 - 1}{2}}
\]

and thus, as \( C \geq 2 \),
\[
\frac{\log(\delta_K N(p_0)^{1/[K : Q]} \sqrt{\deg g + 1})}{\deg g} \leq \frac{\log(C^3 2^{\frac{C^2 + 2}{4} \sqrt{\deg g + 1}})}{\deg g} \leq 2nC^{2n+1} \frac{\log(\deg g)}{\deg g}.
\]

Therefore, from (3.4) we get
\[
h(\alpha) \leq \sum_{i=1}^{n} \frac{f(p_i | p_i)}{[K : Q]} \cdot \frac{\log(p_i)}{e_i (q_i^{f_i} - 1)} + n \epsilon + 13nC^{2n+2} \frac{\log(\deg g)}{\deg g},
\]

so \( \alpha \) satisfies the height bound (1.1) of Theorem 1.3 (recalling that \( \epsilon = 0 \) if \( n = 1 \)).

ACKNOWLEDGMENTS

The authors thank Lukas Pottmeyer for pointing out the results in [Fil14, EP15, FP19], Paul Fili for the exchange regarding [Fil14], and Philip Dittmann for helpful discussions on \( p \)-adic fields as well as for suggesting the short proof of Proposition 2.3. The first author’s work has been funded by the ANR project Gardio 14-CE25-0015.

REFERENCES

[BFH17] J. Biasse, C. Fieker and T. Hofmann. On the computation of the HNF of a module over the ring of integers of a number field. J. Symb. Comp. 80(3):581–615, 2017.
[BZ01] E. Bombieri and U. Zannier. A note on heights in certain infinite extensions of \( \mathbb{Q} \). Rend. Mat. Acc. Lincei 12:5–15, 2001.
[CSV12] X.-W. Chang, D. Stehlé and G. Villard. Perturbation analysis of the QR factor \( R \) in the context of LLL lattice basis reduction. Math. Comput. 81(279):1487–1511, 2012.
[CF21] S. Checcoli and A. Fehm. On the Northcott property and local degrees. To appear in Proc. Amer. Math. Soc., 2021.
[EP05] A. J. Engler and A. Prestel. Valued Fields. Springer, 2005.
[Fil14] P. Fili. On the heights of totally \( p \)-adic numbers. J. Théor. Nombres Bordeaux 26(1):103–109, 2014.
[FP15] P. Fili and C. Petsche. Energy Integrals Over Local Fields and Global Height Bounds. International Mathematics Research Notices 2015(5):1278–1294, 2015.
