ACTA ARITHMETICA
XCIII.2 (2000)

The Fekete–Szegő theorem with splitting conditions: Part I

by

Robert Rumely (Athens, GA)

A classical theorem of Fekete and Szegő [4] says that if E is a compact set in the complex plane, stable under complex conjugation and having logarithmic capacity $\gamma(E) \geq 1$, then every neighborhood of E contains infinitely many conjugate sets of algebraic integers. Raphael Robinson [5] refined this, showing that if E is contained in the real line, then every neighborhood of E contains infinitely many conjugate sets of *totally real* algebraic integers.

In [2], David Cantor developed a theory of capacity for adelic sets in $\mathbb{P}^1$. One of his key results was a very strong theorem of Fekete–Szegő–Robinson type, which produced algebraic numbers whose conjugates lay in a specified neighborhood of an adelic set $\mathbb{E} = E_\infty \times \prod_p E_p$, and belonged to $\mathbb{P}^1(\mathbb{R})$, and $\mathbb{P}^1(\mathbb{Q}_p)$ for finitely many primes p ("splitting conditions"). Unfortunately there was a gap in the part of the proof concerning the splitting conditions.

Some time ago the author extended Cantor's theory, including the Fekete–Szegő theorem *without* splitting conditions, to arbitrary algebraic curves [6]. This paper represents a step towards establishing the theorem *with* splitting conditions. We prove the theorem in the special case where the ground field is $\mathbb{Q}$, the sets are $E_\infty = [-2r, 2r]$ and $E_p = \mathbb{Z}_p$ for primes p in a finite set T, and capacities are measured relative to the point ∞.

It will be apparent to anyone familiar with this kind of result that we have drawn ideas from earlier papers. The method of proof, called "patching", goes back to Fekete and Szegő [4]. The use of Chebyshev polynomials for the archimedean patching functions comes from Robinson [5], and the use of Stirling polynomials for the p-adic patching functions comes from Cantor [2]. However, we have introduced several new ideas: in particular, the method for preserving "well-distributed" sequences of roots of p-adic polynomials, and

2000 *Mathematics Subject Classification*: Primary 11R06, 31C15; Secondary 11R04, 14G40.

Key words and phrases: Fekete–Szegő theorem, capacity theory, splitting conditions.

Work supported in part by NSF grant DMS-9500842.

the step of moving the roots of the "partially patched" p-adic polynomials to keep them well-separated, are new.

1. Statement of the theorem

Notations. $\mathbb{Q}$ and $\mathbb{R}$ are the fields of rational and real numbers, $\mathbb{Q}_p$ is the field of p-adic numbers, $\mathbb{Z}_p$ is the ring of p-adic integers. The canonically normalized absolute value on $\mathbb{Q}_p$ will be written $|x|_p$, and its associated valuation, $\mathrm{ord}_p(x)$. For the archimedean prime $p = \infty$, we will write $\mathbb{Q}_\infty = \mathbb{R}$, and $|x|_\infty$ for the usual absolute value $|x|$ on $\mathbb{R}$. For finite primes p, if $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Q}_p^m$, let $\mathrm{ord}_p(\mathbf{x}) = \min(\mathrm{ord}_p(x_i))$. Given a set $E_p \subseteq \mathbb{Q}_p$, and a function $f : E_p \to \mathbb{Q}_p$, we write $\|f\|_{E_p}$ for the sup norm of f on E_p with respect to $|x|_p$. We will often measure the distance between p-adic numbers α, β in terms of $\mathrm{ord}_p(\alpha - \beta)$: if $\mathrm{ord}_p(\alpha - \beta) \le t$, then we say α and β are separated in ord value by at least t; and if $\mathrm{ord}_p(\alpha - \beta) \ge t$, then α and β are separated in ord value by at most t (note the reversal of comparatives). For a finite set T, $\#(T)$ will denote the cardinality of T. The natural logarithm of a real number t will be written $\ln(t)$, and the base p logarithm as $\log_p(t)$; when $p = \infty$ we set $\log_p(t) = \ln(t)$.

Our goal is to prove

THEOREM 1.1. *Let T be a finite set of prime numbers, and let $[-2r, 2r]$ be a real interval such that*

$$r \prod_{p \in T} p^{-1/(p-1)} > 1.$$

Then there exist infinitely many algebraic integers, all of whose conjugates in $\mathbb{C}$ are contained in the interval $[-2r, 2r]$, and all of whose conjugates in the p-adic complex numbers $\mathbb{C}_p$ (for $p \in T$) are contained in the set of p-adic integers $\mathbb{Z}_p$. (In particular, these numbers are totally real and "totally p-adic", for $p \in T$.)

Although we have stated Theorem 1.1 without reference to capacities, it is in fact capacity-theoretic. The quantity in the hypothesis is simply the capacity $\gamma(\mathbb{E}, \{\infty\})$ for $\mathbb{E} = E_\infty \times \prod_p E_p$, where $E_\infty = [-2r, 2r]$, $E_p = \mathbb{Z}_p$ for $p \in T$, and $E_p = \widetilde{O}_p$ for $p \notin T$, where $\widetilde{O}_p$ is the ring of integers of $\mathbb{C}_p$. The theorem is sharp in the sense that if $\gamma(\mathbb{E}, \{\infty\}) < 1$ then by Fekete's theorem (see [6], p. 414) the result is false. (We do not know whether or not the result holds if $\gamma(\mathbb{E}, \{\infty\}) = 1$ and $T \neq \emptyset$.)

The proof follows the classical method of Fekete and Szegő, which involves "patching" a carefully chosen polynomial with real coefficients—sequentially adjusting the coefficients from highest to lowest order so that they become integers—in such a way that control is maintained over the

locations of the roots. In our case, we simultaneously patch a real polynomial, and collection of polynomials with p-adic coefficients, to a common polynomial with integer coefficients. We actually prove

THEOREM 1.2. *Under the hypotheses above, there exist monic polynomials $u(x) \in \mathbb{Z}[x]$ with distinct roots, and arbitrarily high degree, whose roots in $\mathbb{C}$ all belong to the real interval $[-2r, 2r]$, and whose roots in $\mathbb{C}_p$ all belong to $\mathbb{Z}_p$, for each $p \in T$.*

2. Chebyshev polynomials and Stirling polynomials. Let $r > 0$ be a real number. The *Chebyshev polynomials* for the interval $[-2r, 2r]$ are defined by

$$T_{n,r}(2r\cos(\theta)) = 2r^n \cos(n\theta) \quad \text{for } n = 0, 1, 2, \dots \tag{2.1}$$

Clearly $\|T_{n,r}\|_{E_\infty} = 2r^n$ and $T_{n,r}(x)$ oscillates n times between $\pm 2r^n$ on $[-2r, 2r]$. Moreover, $T_{n,r}(x)$ has n simple roots in $[-2r, 2r]$, and $[-2r, 2r] = T_{n,r}^{-1}([-2r^n, 2r^n])$. It is easy to see that for $n \geq 1$, $T_{n,r}(x)$ is a monic polynomial of degree n. Writing

$$T_{n,r}(x) = z^n + \sum_{k=1}^{n} a_{k,r}(n) x^{n-k},$$

it is shown (in Robinson [5]) that the coefficients $a_{k,r}(n)$ are given by

$$a_{k,r}(n) = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ (-1)^m r^{2m} \dfrac{n}{m} \dbinom{n-m-1}{m-1} & \text{if } k = 2m \text{ is even,} \end{cases} \tag{2.2}$$

where $\binom{n-m-1}{m-1}$ is the binomial coefficient. In particular, for fixed k and r, $a_{k,r}(n)$ is itself a polynomial in n without constant term; and if $r = M/N$ is a rational number, then the coefficients of $a_{k,r}(n)$ are rational numbers with denominators dividing $N^k k!$. Thus, if r is rational, then for any fixed k_0 and any fixed integer $Q_0 \neq 0$, there is an integer N_0 (depending on r, k_0, and Q_0) such that if n is a multiple of N_0 then all the $a_{k,r}(n)$, for $1 \leq k \leq k_0$, are integers divisible by Q_0.

The *Stirling polynomial* of degree n is defined by

$$S_n(x) = \prod_{j=0}^{n-1} (x - j) = x^n + \sum_{k=1}^{n} b_k(n) x^k. \tag{2.3}$$

In particular $S_n(x)$ has n distinct roots in $\mathbb{Z}_p$, for each p. From the fact that

$$S_n(x) = n! \binom{x}{n}$$

follows

$$\|S_n\|_{\mathbb{Z}_p} = |n!|_p.$$

Again the coefficients $b_k(n)$ (for $k \geq 1$) are polynomials in n without constant term. Indeed, by a theorem of Schlömilch (see [3], p. 216)

$$b_k(n) = \sum_{0 \leq j < h \leq k} (-1)^{j+h} \binom{h}{j} \frac{(h-j)^{k+h}}{h!} \binom{n+h-1}{k+h} \binom{n+k}{k-h}. \tag{2.4}$$

Here each summand has an algebraic factor of $n(n-1)\dots(n-k)$. Since $b_k(n)$ has degree $2k$ and takes $\mathbb{N}$ to $\mathbb{Z}$, the coefficients in its expansion in powers of n have denominators that divide $(2k)!$.

It is well known that $\operatorname{ord}_p(n!) = (n - \sum a_i)/(p-1)$, where the a_i are the base p digits of n. From this we see that

$$\frac{n}{p-1} - \lceil \log_p(n) \rceil \leq \operatorname{ord}_p(n!) \leq \frac{n-1}{p-1}. \tag{2.5}$$

3. The basic ideas in patching. The purpose of this section is to describe the patching process in general terms, and to prove some estimates which guide how it is carried out. Formally, the patching process is as follows: for each $p \in T \cup \{\infty\}$, we begin with a polynomial $u_p^{(0)}(x) \in \mathbb{Q}_p[z]$ of degree n, where n is independent of p. The kth patching step, for $k = 1, \dots, n$, consists of choosing numbers $\Delta_p^{(k)} \in \mathbb{Q}_p$ and monic polynomials $w_p^{(k)}(x) \in \mathbb{Q}_p[x]$ of degree $n-k$, and setting

$$u_p^{(k)}(x) = u_p^{(k-1)}(x) + \Delta_p^{(k)} w_p^{(k)}(x) \quad \text{for each } p \in T \cup \{\infty\}. \tag{3.1}$$

Write

$$u_p^{(k)}(x) = x^n + \sum_{j=1}^{n} c_{p,j}^{(k)} x^{n-j}.$$

A step (3.1) has the effect of replacing the coefficient $c_{p,k}^{(k-1)}$ by $c_{p,k}^{(k)} = c_{p,k}^{(k-1)} + \Delta_p^{(k)}$, leaving higher order coefficients unchanged, and modifying lower order coefficients in ways that are not important to us. We will choose the multipliers $\Delta_p^{(k)} \in \mathbb{Q}_p$ so that $c_{p,k}^{(k)}$ is a rational integer c_k independent of p. Since the kth step only changes coefficients of terms of degree $n-k$ and lower, in the end the $u_p^{(n)}(x)$ are all equal to the same monic polynomial $u(x) \in \mathbb{Z}[x]$.

By hypothesis,

$$r > \prod_{p \in T} p^{1/(p-1)}. \tag{3.2}$$

After shrinking r, we can assume that $r = M/N$ is rational.

Set $E_\infty = [-2r, 2r]$ and $E_p = \mathbb{Z}_p$ for $p \in T$. The initial polynomials will be $u_\infty^{(0)}(x) = T_{n,r}(x)$ at the archimedean place, and $u_p^{(0)}(x) = S_n(x)$ for $p \in T$. These polynomials have all their roots in the sets E_p. The crucial

issue is to maintain this property at each step of the patching process. For this to be possible, n must be chosen large and appropriately divisible, and the patching polynomials $w_p^{(k)}(x)$ must be chosen with near-minimal sup norm on E_p.

In the case $p = \infty$, we will take

$$w_\infty^{(k)}(x) = T_{n-k,r}(x).$$

The idea is that since $u_\infty^{(0)}(x) = T_{n,r}(x)$ oscillates n times between $\pm 2r^n$, if the total magnitude of the patching terms is less than $2r^n$ then the final patched polynomial $u_\infty^{(n)}(x)$ will still have n roots in E_∞. To achieve this, let $h < r$ be such that $h \prod_{p\in T} p^{-1/(p-1)} > 1$ (cf. (3.2)). We will require that for an appropriate number L,

$$\begin{cases} \Delta_\infty^{(k)} = 0 & \text{for } k < L, \\ |\Delta_\infty^{(k)}| \le h^k & \text{for } k \ge L. \end{cases}$$

Then for each $x \in E_\infty$,

$$\Big|\sum_{k=1}^{n} \Delta_\infty^{(k)} w_\infty^{(k)}(x)\Big| \le \sum_{k=L}^{n} h^k \cdot 2r^{n-k} < \frac{1}{r^L(1-h/r)} \cdot 2r^n. \tag{3.3}$$

If L is sufficiently large, the right side will be less than $2r^n$; and then the patched polynomial will still have all its roots in $[-2r, 2r]$. Requiring $\Delta_\infty^{(k)} = 0$ for small k might appear to present problems in achieving integrality for the high-order coefficients, but our trump card is the rationality of r and the choice of n.

In the case of a finite prime $p \in T$, the patching polynomials $w_p^{(k)}(x)$ will be taken to be factors of the $u_p^{(k-1)}(x)$, chosen so that the cofactors $f^{(k)}(x) = u_p^{(k-1)}(x)/w_p^{(k)}(x)$ have their roots p-adically distributed like the roots of a Stirling polynomial. We isolate this concept as follows.

Definition 3.1. Let k be a positive integer. A *regular sequence* of length k in $\mathbb{Z}_p$ is a sequence $\alpha_0, \alpha_1, \ldots, \alpha_{k-1} \in \mathbb{Z}_p$ such that for each $j = 0, 1, \ldots, k-1$,

$$\operatorname{ord}_p(\alpha_j - j) \ge \log_p(k).$$

We simply speak of a "regular sequence" if k or $\mathbb{Z}_p$ is understood. Note that if $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ is a regular sequence of length k, then $\operatorname{ord}_p(\alpha_j - j) \ge \lceil \log_p(k) \rceil$ for all j, and $\operatorname{ord}_p(\alpha_i - \alpha_j) < \log_p(k)$ for distinct i, j.

The basis for patching on the p-adic side is given by

Lemma 3.1. *Let $f(x) = \prod_{j=0}^{k-1}(x - \alpha_j) \in \mathbb{Z}_p[x]$ be a polynomial whose roots form a regular sequence of length k in $\mathbb{Z}_p$. Suppose $b \ge 0$, and let*

$\Delta \in \mathbb{Z}_p$ satisfy

$$\mathrm{ord}_p(\Delta) \geq \frac{k}{p-1} + \log_p(k) + b.$$

Put $f^*(x) = f(x) + \Delta$. Then $f^*(x)$ factors completely over $\mathbb{Q}_p$, and its roots α_j^* again form a regular sequence of length k in $\mathbb{Z}_p$. Indeed, the α_j^* can uniquely be put in correspondence with the α_j in such a way that

$$\mathrm{ord}_p(\alpha_j^* - \alpha_j) \geq \lceil \log_p(k) + b \rceil \quad \textit{for all } j = 0, \ldots, k-1.$$

P r o o f. Fix one of the roots α_J of $f(x)$, and consider the Newton polygon of $f^*(x)$, expanded about the point α_J. (For the theory of Newton polygons, see [1], pp. 37–43.) Write

$$f^*(x) = \sum_{i=0}^{k} d_i (x - \alpha_J)^i.$$

By assumption $d_0 = \Delta$, and

$$d_1 = \pm \prod_{j \neq J} (\alpha_j - \alpha_J).$$

Since the α_j form a regular sequence, if $j \neq J$ the ultrametric inequality implies $\mathrm{ord}_p(\alpha_j - \alpha_J) = \mathrm{ord}_p(j - J)$. Therefore

$$\begin{aligned} \mathrm{ord}_p(d_1) &= \mathrm{ord}_p(J!) + \mathrm{ord}_p((k-1-J)!) \\ &= \mathrm{ord}_p((k-1)!) - \mathrm{ord}_p\left(\binom{k-1}{J}\right) \leq \frac{k-1}{p-1}. \end{aligned}$$

For $i \geq 2$,

$$d_i = \pm d_1 \sum_{\substack{j_1, \ldots, j_{i-1} \\ \text{distinct}, \neq J}} [(\alpha_{j_1} - \alpha_J) \ldots (\alpha_{j_{i-1}} - \alpha_J)]^{-1}$$

so that

$$\mathrm{ord}_p(d_i) \geq \mathrm{ord}_p(d_1) - (i-1)\log_p(k).$$

By the hypothesis on $\mathrm{ord}_p(\Delta)$, the Newton polygon of $f^*(x)$ has a break at the point $(1, \mathrm{ord}_p(d_1))$, and if its initial segment has slope m, then $-m \geq \log_p(k) + b$. Hence $f^*(x)$ has a unique root $\alpha_J^* \in \mathbb{Z}_p$ for which $\mathrm{ord}_p(\alpha_J^* - \alpha_J) \geq \lceil \log_p(k) + b \rceil$.

Since this holds for all J, the roots α_j^* form a regular sequence of length k in $\mathbb{Z}_p$.

We apply Lemma 3.1 as follows. After the $(k-1)$st step, write

$$u_p^{(k-1)}(x) = \prod_{j=0}^{n-1} (x - \alpha_{p,j}) = z^n + \sum_{j=1}^{n} c_{p,j} x^{n-j}.$$

Suppose that $\alpha_{p,0},\dots,\alpha_{p,k-1}$ form a regular sequence of length k. Then taking the patching polynomial to be

$$w_p^{(k)}(x)=\prod_{j=k}^{n-1}(x-\alpha_{p,j})$$

and choosing $\Delta_p^{(k)}\in\mathbb{Z}_p$ so that

$$\operatorname{ord}_p(\Delta_p^{(k)})\ge\frac{k}{p-1}+\log_p(k)+b\quad\text{ for some } b\ge 0,$$

we obtain

$$\begin{aligned}u_p^{(k)}(x)&=u_p^{(k-1)}(x)+\Delta_p^{(k)}w_p^{(k)}(x)\\&=\Big[\prod_{j=0}^{k-1}(x-\alpha_{p,j})+\Delta_p^{(k)}\Big]w_p^{(k)}(x)\\&=\prod_{j=0}^{k-1}(x-\alpha_{p,j}^*)\prod_{j=k}^{n-1}(x-\alpha_{p,j}).\end{aligned}$$

Of course, a similar result would have been obtained if any other regular sequence of roots, of length k, had been used.

Note that by the correspondence between the $\alpha_{p,j}$ and the $\alpha_{p,j}^*$ in Lemma 3.1, there is a natural labelling of the roots of each $u_p^{(k)}(x)$ in terms of $0,1,\dots,n-1$. Whenever we refer to an $\alpha_{p,j}$ it will be using this labelling.

If b is sufficiently large, then the $\alpha_{p,j}^*$ will not only form a regular sequence of length k, but they will be part of a longer regular sequence; this permits the patching process to continue. However, unless $b\ge\log_p(n)$, they need not be part of a regular sequence of length n; and for small k the interaction between the archimedean prime and the primes in T will force $b<\log_p(n)$. In consequence, some of the roots $\alpha_{p,j}^*$ moved in early steps may stray very near to other unpatched roots. These complications account for some of the difficulties in the proof below.

4. The proof of Theorem 1.2. As noted, our goal is to merge the local polynomials $u_p^{(0)}(x)$ into a single global polynomial $u(x)$. It is here that hypothesis (3.2) enters. Put

$$q=\prod_{p\in T}p^{1/(p-1)}.$$

Since we have chosen the parameter h so that $q<h<r$, there is a number k_0 such that for $k\ge k_0$,

$$\prod_{p\in T}p^{\lceil k/(p-1)+\log_p(k)\rceil}<h^k<r^k.$$

Thus, writing $c_{p,k}$ for the coefficient of z^{n-k} in $u_p^{(k-1)}(x)$, if $k \geq k_0$ there exists a number $c_k \in \mathbb{Z}$ satisfying

$$\begin{cases} |c_k - c_{\infty,k}| < h^k, \\ \mathrm{ord}_p(c_k - c_{p,k}) \geq k/(p-1) + \log_p(k) \quad \text{for } p \in T. \end{cases} \tag{4.1}$$

Therefore, if we put $\Delta_p^{(k)} = c_k - c_{p,k}$ for each p, the kth step of the patching process achieves an integral coefficient for x^{n-k}. For small k, (4.1) may not be satisfied: integrality for the high order coefficients must be arranged by other means.

We now proceed to the details of the proof. Once and for all, fix an h with $q < h < r$ and put

$$C = 1 + \frac{2 \cdot \#(T)}{\ln(h/q)}\ , \qquad Q = \prod_{p \in T} p.$$

We can assume T is not empty; when $T = \emptyset$, much of the argument below degenerates. In any case by [5] the result is already known in that situation.

There are five stages in the patching process:

I. Patching the coefficients c_k for $1 \leq k \leq L_1(n) := C \ln\ln(n)$, achieving integrality through the choice of n.

II. Patching the coefficients c_k for $L_1(n) < k \leq L_2(n) := C \ln(n)$, at which point h^k dominates q^k enough that further patching will move roots only within cosets $\{x \in \mathbb{Z}_p : \mathrm{ord}_p(x - \alpha_{p,j}) > \log_p(n)\}$, for each $p \in T$.

III. Moving the roots perturbed in stages I and II, so that for each $p \in T$ they are separated from other roots by at least $4C \log_p(n)$ in ord value.

IV. Patching the coefficients c_k for

$$L_2(n) < k \leq L_3(n) := \frac{13C \cdot \#(T)}{\ln(h/q)} \ln(n),$$

at which point h^k dominates q^k so much that even the roots moved in stages I–III can again be safely included in the patching process.

V. Patching the remaining coefficients c_k for $L_3(n) < k \leq n$.

The patching process can be carried through only for certain values of n. It is sufficient to have

(N1) $r^{L_1(n)}(1 - h/r) > 2$;
(N2) $\ln\ln(n) > (1 + 2 \cdot \#(T) \ln(C) + \ln(Q))/\ln(h/q)$;
(N3) $n > 3QL_2(n)$;
(N4) $n \geq e^e$;
(N5) $n > 3QL_3(n)$;
(N6) $L_2(n) > 1 + \max_{p \in T}(p^2)$;

(N7) n is divisible by

$$N^{\lceil L_1(n)\rceil}\lceil 2L_1(n)\rceil!\prod_{p\in T} p^{\lceil L_1(n)/(p-1)+\log_p(L_1(n))+\log_p(L_2(n))\rceil},$$

where N is the denominator of $r = M/N$.

The constraints (N1)–(N6) hold for all sufficiently large n. By Stirling's formula, the quantity in (N7) is easily seen to be $o(n)$, and hence (N7) holds for infinitely many n.

Stage I: *Patching for* $1 \le k < L_1(n) = C\ln\ln(n)$. The highest-order coefficients $a_k(n)$ of $u_\infty^{(0)}(x) = T_{n,r}(x)$ will be made integral through the choice of n, and, for $p \in T$, the coefficients $b_k(n)$ of the $u_p^{(0)}(x)$ will be adjusted to meet them. If n satisfies (N7), then for all $k \le L_1(n)$, and all $p \in T$, the $a_k(n)$ and $b_k(n)$ are rational integers satisfying

$$\operatorname{ord}_p(*) \ge L_1(n)/(p-1) + \log_p(L_1(n)) + \log_p(L_2(n)). \tag{4.2}$$

This is because the $a_k(n)$ and $b_k(n)$ are polynomials in n with rational coefficients and no constant term, and the denominators of the coefficients in both $a_k(n)$ and $b_k(n)$ divide $N^k(2k)!$.

To specify the kth patching step, it is enough to give the target coefficient $c_k \in \mathbb{Z}$ and the p-adic patching polynomials $w_p^{(k)}(x)$, since $\Delta_p^{(k)} = c_k - c_{p,k}$ and $w_\infty^{(k)}(x) = T_{n-k,r}(x)$. We will take $c_k = a_k(n)$ (so $\Delta_\infty^{(k)} = 0$), and

$$w_p^{(k)}(x) = \prod_{j=k}^{n-1}(x - \alpha_{p,j}).$$

On the p-adic side, using condition (4.2) and Lemma 3.1 one sees inductively that for each $k \le L_1(n)$:

(a) the patching coefficients $\Delta_p^{(k)}$ satisfy (4.2), for $p \in T$, and hence

(b) the $\lfloor L_1(n)\rfloor$ high-order coefficients of $u_p^{(k)}(x)$ also satisfy (4.2), for $p \in T$;

(c) the first $\lfloor L_2(n)\rfloor$ roots of $u_p^{(k)}(x)$ form a regular sequence of length $\lfloor L_2(n)\rfloor$ in $\mathbb{Z}_p$.

Stage II: *Patching for* $L_1(n) = C\ln\ln(n) < k \le L_2(n) = C\ln(n)$. Here both the archimedean and nonarchimedean $u_p^{(k)}(x)$ will be modified. The archimedean patching coefficients $\Delta_\infty^{(k)} = c_k - c_{\infty,k}$ can be chosen arbitrarily, subject to the condition $|\Delta_\infty^{(k)}| < h^k$, because under hypothesis (N1) the total archimedean patching error will be at most r^n (cf. (3.3)).

For $L_1(n) < k \le L_2(n)$, we claim that

$$h^k > \prod_{p\in T} p^{\lceil k/(p-1)+\log_p(k)+\log_p(L_2(n))\rceil}. \tag{4.3}$$

Indeed, (4.3) is implied by

$$\left(\frac{h}{q}\right)^k > Qk^{\#(T)}L_2(n)^{\#(T)}$$

which follows from the hypotheses on k, the definition of C, and (N2), via

$$\begin{aligned} k\ln(h/q) &> \left(1+\frac{2\cdot\#(T)}{\ln(h/q)}\right)\ln\ln(n)\ln(h/q) \\ &> \ln(Q)+2\cdot\#(T)\ln(C)+2\cdot\#(T)\ln\ln(n) \\ &> \ln(Q)+\#(T)\ln(k)+\#(T)\ln(L_2(n)). \end{aligned}$$

By (4.3), at the kth step we can find a target coefficient $c_k \in \mathbb{Z}$ such that

$$\begin{cases} |c_k - c_{\infty,k}| < h^k, \\ \mathrm{ord}_p(c_k - c_{p,k}) \geq k/(p-1) + \log_p(k) + \log_p(L_2(n)) \quad \text{for each } p \in T. \end{cases}$$

As in Stage I, the p-adic patching polynomials will be

$$w_p^{(k)}(x) = \prod_{j=k}^{n-1}(x-\alpha_{p,j}).$$

In Stage I we carefully preserved the property that the first $\lfloor L_2(n)\rfloor$ roots of $u_p^{(k)}(x)$ formed a regular sequence of length $\lfloor L_2(n)\rfloor$. By Lemma 3.1 and an inductive argument like that in Stage I, after each patching step, the first $\lfloor L_2(n)\rfloor$ roots of $u_p^{(k)}(x)$ continue to form a regular sequence of length $\lfloor L_2(n)\rfloor$.

Stage III. This stage only changes the p-adic polynomials. For notational convenience, set

$$m = \lfloor L_2(n)\rfloor$$

and write $u_p(x) = u_p^{(m)}(x)$.

In Stages I and II we have adjusted the highest m coefficients of the $u_p(x)$ to common integer values. However, in the process, we have perturbed the first m roots, and although these roots remain well-separated from each other, they may have drifted very near to other roots (they form a regular sequence of length m, but they may not be part of a regular sequence of length n). To enable the patching process to continue, we pause to move them away from any roots they may have strayed too near to, taking care that the m high-order coefficients of $u_p(x)$ remain unchanged. This is done by means of a p-adic implicit function theorem, and involves moving a second set of m roots in a way that compensates for the first.

Fix $p \in T$. The coefficients of $u_p(x)$ are elementary symmetric functions of the roots. Since the first m roots $\alpha_{p,0},\dots,\alpha_{p,m-1}$ form a regular sequence of length m (by the construction in Stages I and II), while the last $n-m$

roots are the same as those of $u_p^{(0)}(x)$ (and hence are contained in a regular sequence of length n), for each $j < m$ there is at most one root $\alpha_{p,\mu(j)} \neq \alpha_{p,j}$ such that

$$\operatorname{ord}_p(\alpha_{p,j} - \alpha_{p,\mu(j)}) \geq \log_p(n)$$

(necessarily, $\mu(j) \geq m$). On the other hand, since $n > 3 \cdot p^{\lceil \log_p(m) \rceil}$ by hypothesis (N3), it is possible to choose a second regular sequence of length m, consisting of roots $\alpha_{p,\tau(j)}$, $0 \leq j < m$, which avoids the "delicate" roots $\alpha_{p,j}$ and $\alpha_{p,\mu(j)}$, $0 \leq j < m$. By our choice of the $\alpha_{p,\tau(j)}$, for each $i \neq \tau(j)$, $0 \leq i < n$, we have

$$\operatorname{ord}_p(\alpha_{p,i} - \alpha_{p,\tau(j)}) < \log_p(n). \tag{4.4}$$

Given vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_p^m$ and $\mathbf{z} \in \mathbb{Z}_p^{n-2m}$, let $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbb{Z}_p^n$ (resp. $(\mathbf{y}, \mathbf{z}) \in \mathbb{Z}_p^{n-m}$) denote the concatenated vector, and if $\mathbf{x} = (x_1, \ldots, x_m)$, let $\widehat{\mathbf{x}}_i$ be $\mathbf{x}$ with its ith component omitted. Write $s_k(\mathbf{x}, \mathbf{y}, \mathbf{z})$ for the kth elementary symmetric function on the components of the concatenated vector. Note that for each i,

$$s_k(\mathbf{x}, \mathbf{y}, \mathbf{z}) = x_i s_{k-1}(\widehat{\mathbf{x}}_i, \mathbf{y}, \mathbf{z}) + s_k(\widehat{\mathbf{x}}_i, \mathbf{y}, \mathbf{z}). \tag{4.5}$$

In consequence, as a formal derivative,

$$\frac{\partial}{\partial x_i} s_k(\mathbf{x}, \mathbf{y}, \mathbf{z}) = s_{k-1}(\widehat{\mathbf{x}}_i, \mathbf{y}, \mathbf{z}).$$

Fixing $(\mathbf{y}, \mathbf{z}) \in \mathbb{Z}_p^{n-m}$, consider the map

$$S : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$$

defined by

$$S(\mathbf{x}) = S(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \begin{pmatrix} s_1(\mathbf{x}, \mathbf{y}, \mathbf{z}) \\ s_2(\mathbf{x}, \mathbf{y}, \mathbf{z}) \\ \vdots \\ s_m(\mathbf{x}, \mathbf{y}, \mathbf{z}) \end{pmatrix}.$$

Recall that for a vector ∇, we write $\operatorname{ord}_p(\nabla) = \min(\operatorname{ord}_p(\nabla_i))$.

LEMMA 4.1. *Suppose $m \geq p^2$. Let $\mathbf{x} \in \mathbb{Z}_p^m$ be a vector whose components form a regular sequence of length m, and let $\nabla \in \mathbb{Z}_p^m$ be a vector for which*

$$\operatorname{ord}_p(\nabla) \geq \frac{2m}{p-1} + b \quad \textit{for some } b \geq 0.$$

Then there is an $\mathbf{x}^* \in \mathbb{Z}_p^m$ satisfying $\operatorname{ord}_p(\mathbf{x}^* - \mathbf{x}) \geq m/(p-1) + b$ such that

$$S(\mathbf{x}^*, \mathbf{y}, \mathbf{z}) = S(\mathbf{x}, \mathbf{y}, \mathbf{z}) + \nabla.$$

P r o o f. We aim to apply Hensel's lemma in several variables. Consider the Jacobian matrix of $S(\mathbf{x})$, which by (4.5) is

$$J_S(\mathbf{x}) = \begin{pmatrix} 1 & \dots & 1 \\ s_1(\widehat{\mathbf{x}}_1, \mathbf{y}, \mathbf{z}) & & s_1(\widehat{\mathbf{x}}_m, \mathbf{y}, \mathbf{z}) \\ \vdots & & \vdots \\ s_{m-1}(\widehat{\mathbf{x}}_1, \mathbf{y}, \mathbf{z}) & \dots & s_{m-1}(\widehat{\mathbf{x}}_m, \mathbf{y}, \mathbf{z}) \end{pmatrix}.$$

The usual argument for computing Vandermonde determinants (equating variables, then examining the diagonal term), shows that

$$\det(J_S(\mathbf{x})) = \prod_{i<j}(x_i - x_j).$$

Similarly, if $\mathrm{cof}_{kl}(\mathbf{x})$ denotes the (k,l)-cofactor of $J_S(\mathbf{x})$ (obtained from $J_S(\mathbf{x})$ by deleting the kth row and lth column), then

$$\mathrm{cof}_{kl}(\mathbf{x}) = (-1)^{k+l} \prod_{\substack{i<j \\ i,j\neq l}} (x_i - x_j) P_{kl}(\mathbf{x}, \mathbf{y}, \mathbf{z})$$

where $P_{kl}(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is a polynomial with integer coefficients. Thus

$$[J_S(\mathbf{x})^{-1}]_{kl} = (-1)^{k+1} \frac{P_{lk}(\mathbf{x}, \mathbf{y}, \mathbf{z})}{\prod_{1\le i\le m,\, i\neq k}(x_i - x_k)}.$$

Since the components of $\mathbf{x}$ form a regular sequence of length m, for each $k = 1, \dots, m$,

$$\begin{aligned} \mathrm{ord}_p\Big(\prod_{\substack{1\le i\le m \\ i\neq k}} (x_i - x_k)\Big) &= \mathrm{ord}_p\Big(\prod_{\substack{1\le i\le m \\ i\neq k}} (i - k)\Big) \\ &= \mathrm{ord}_p((k-1)!(m-k)!) \le \frac{m-1}{p-1}. \end{aligned}$$

Consequently, each entry of $J_S(\mathbf{x})^{-1}$ has ord value $\ge -(m-1)/(p-1)$.

The usual proof of Hensel's lemma now shows that the sequence $\mathbf{x}^{(i)}$ defined by

$$\begin{cases} \mathbf{x}^{(0)} = \mathbf{x}, \\ \mathbf{x}^{(i+1)} = \mathbf{x}^{(i)} - J_S(\mathbf{x}^{(i)})^{-1}[S(\mathbf{x}^{(i)}) - S(\mathbf{x}) - \nabla] \end{cases}$$

converges to a vector $\mathbf{x}^* = \mathbf{x}^{(\infty)}$ with the desired properties. Here the components of each $\mathbf{x}^{(i)}$, and of $\mathbf{x}^*$, form a regular sequence of length m, because the hypothesis that $m \ge p^2$ implies that

$$\frac{m}{p-1} \ge \log_p(m).$$

Note that the condition $m \ge p^2$ holds for all $p \in T$, by (N6).

To move the roots $\alpha_{p,j}$ away from the $\alpha_{p,\mu(j)}$, we take

$$\mathbf{x} = (\alpha_{p,\tau(j)})_{0\le j\le m-1},$$
$$\mathbf{y} = (\alpha_{p,j})_{0\le j\le m-1}$$

and let $\mathbf{z}$ be the vector formed from the remaining roots of $u_p(x)$. Set $b = \log_p(n)$. Recalling that $\alpha_{p,\mu(j)}$ is the unique root distinct from $\alpha_{p,j}$ such that $\operatorname{ord}_p(\alpha_{p,j} - \alpha_{p,\mu(j)}) \ge \log_p(n)$ (if such a root exists), put

$$\alpha^*_{p,j} = \begin{cases} \alpha_{p,\mu(j)} + p^{\lceil 2m/(p-1)+b\rceil} & \text{if } \alpha_{p,\mu(j)} \text{ exists,} \\ \alpha_{p,j} & \text{otherwise} \end{cases}$$

and let

$$\mathbf{y}^* = (\alpha^*_{p,j})_{0\le j\le m-1}.$$

Evidently, for each $j < m$ for which an $\alpha_{p,\mu(j)}$ exists, we have

$$\operatorname{ord}_p(\alpha^*_{p,j} - \alpha_{p,\mu(j)}) \le \frac{2m}{p-1} + b + 1 < 4C\log_p(n) \tag{4.6}$$

(using the fact that $m \le C\ln(n)$ and $\ln(p)/(p-1) < 1$ for all primes p, and that $C\log_p(n) > 1$ by hypothesis (N6)). Since a priori all other roots are well-separated from $\alpha_{p,j}$ and $\alpha_{p,\mu(j)}$, we find that for each $j < m$, and all $i \ne j$,

$$\operatorname{ord}_p(\alpha_{p,i} - \alpha^*_{p,j}) < 4C\log_p(n). \tag{4.7}$$

Set

$$\nabla = S(\mathbf{x},\mathbf{y},\mathbf{z}) - S(\mathbf{x},\mathbf{y}^*,\mathbf{z}).$$

Then $\operatorname{ord}_p(\nabla) \ge 2m/(p-1)+b$, so Lemma 4.1, applied to $S(\mathbf{x},\mathbf{y}^*,\mathbf{z})$, shows there is an $\mathbf{x}^*$ with $\operatorname{ord}_p(\mathbf{x}^* - \mathbf{x}) \ge 2m/(p-1) + b + 1$ such that

$$S(\mathbf{x}^*,\mathbf{y}^*,\mathbf{z}) = S(\mathbf{x},\mathbf{y}^*,\mathbf{z}) + \nabla = S(\mathbf{x},\mathbf{y},\mathbf{z}).$$

If we put

$$\alpha^*_{p,\tau(j)} = \mathbf{x}^*_j,$$

then Lemma 4.1 assures us that

$$\operatorname{ord}_p(\alpha^*_{p,\tau(j)} - \alpha_{p,\tau(j)}) \ge \left\lceil \frac{m}{p-1} + b \right\rceil \ge \log_p(n).$$

Thus, replacing $\alpha_{p,\tau(j)}$ by $\alpha^*_{p,\tau(j)}$ only moves the root within a coset of size $\operatorname{ord}_p(x) \ge \log_p(n)$, and leaves its position in the regular sequence of length n (and hence its separation from the other roots) unchanged.

In consequence, the polynomial

$$u^*_p(x) = \prod_{j<m}(x - \alpha^*_{p,j}) \prod_{j<m}(x - \alpha^*_{p,\tau(j)}) \prod (x - w_j)$$

has the same m high-order coefficients as $u_p(x)$, but its roots are separated from each other by at least $4C\log_p(n)$ in ord value. We replace $u_p^{(m)}(x)$ by $u_p^*(x)$.

Stage IV: *Patching for* $L_2(n) < k \le L_3(n) := \frac{13C\cdot\#(T)}{\ln(h/q)}\ln(n)$. The purpose of this step is to patch until the dominance of h^k over q^k is so great that even the "delicate" roots $\alpha_{p,j}^*$ and $\alpha_{p,\mu(j)}$ with $j < \lfloor L_2(n)\rfloor$ can be safely moved. For $k > L_2(n) = C\ln(n)$, we have

$$h^k > \prod_{p\in T} p^{\lceil k/(p-1)+\log_p(k)+\log_p(n)\rceil}. \tag{4.8}$$

Indeed, (4.8) is implied by

$$\left(\frac{h}{q}\right)^k > Qk^{\#(T)}n^{\#(T)}$$

which follows from $n \ge k > C\ln(n)$ via

$$\begin{aligned} k\ln(h/q) &> \left(1+\frac{2\cdot\#(T)}{\ln(h/q)}\right)\ln(n)\ln(h/q) \\ &> \ln(n)\ln(h/q) + 2\cdot\#(T)\ln(n) \\ &> \ln(Q) + \#(T)\ln(k) + \#(T)\ln(n) \end{aligned}$$

using $\ln(n) > \ln\ln(n)$ and hypothesis (N2).

Put $l = \lfloor L_3(n)\rfloor$. We first choose a regular sequence of length l among the roots of $u_p(x)$ which avoids the delicate roots $\alpha_{p,j}$ and $\alpha_{p,\mu(j)}$ with $j < \lfloor L_2(n)\rfloor$. Since $n > 3\cdot p^{\lceil\log_p(l)\rceil}$ by hypothesis (N5), and at most two of the delicate roots are separated by less than $\log_p(n)$ in ord value from any of the other roots, such regular sequences exist. Let one be

$$\alpha_{p,\lambda(j)}, \qquad 0 \le j < l.$$

Let T_p be the complement of $\{\lambda(j) : 0 \le j < l\}$ in $\{j : 0 \le j < n\}$. By construction, the delicate roots are all contained in T_p.

For $L_2(n) < k \le L_3(n)$, choose the target coefficients $c_k \in \mathbb{Z}$ so that

$$\begin{cases} |c_k - c_{\infty,k}| < h^k, \\ \operatorname{ord}_p(c_k - c_{p,k}) > k/(p-1) + \log_p(k) + \log_p(n) \quad \text{for } p \in T, \end{cases}$$

and patch using the polynomials

$$w_p^{(k)}(x) = \prod_{j=k}^{l-1}(x-\alpha_{p,\lambda(j)}) \prod_{j\in T_p}(x-\alpha_{p,j}).$$

By Lemma 3.1, the roots $\alpha_{p,\lambda(j)}$, $0 \le j < k$, are moved by at most $\log_p(n)$ in ord value, so their position in the regular sequences (and their separation from other roots), remains unchanged.

Stage V: *Patching for* $L_3(n) < k \le n$. In this stage, patching is carried through to the end. By Lemma 4.2 below, the "delicate roots" from Stages I, II and III can be safely included in the patching process when

$$h^k > \prod_{p\in T} p^{\lceil k/(p-1)+3(4C\log_p(n))\rceil}. \tag{4.9}$$

A computation like the one that gave (4.8) (using (N3), (N4), and (N5)) shows that (4.9) holds if

$$k > L_3(n) = \frac{13C\cdot\#(T)}{\ln(h/q)}\ln(n).$$

Lemma 4.2. *Suppose* $f(z)=\prod_{j=0}^{m-1}(x-\alpha_{p,j})$ *is a polynomial which splits over* $\mathbb{Z}_p$, *and* $M \ge \lceil \log_p(m)\rceil$ *is such that*

(T1) *the* $\alpha_{p,j}$ *can be grouped into disjoint subsets* $T_1,\dots,T_l$ *so that each* T_i *is a subset of a regular sequence of length* $n_i \le m$ (*necessarily* $n_i \ge \#(T_i)$);

(T2) *the* $\alpha_{p,j}$ *can be labelled so that* $\mathrm{ord}_p(\alpha_{p,j}-j) \ge \log_p(n_i)$ *if* $\alpha_{p,j}\in T_i$;

(T3) $\mathrm{ord}_p(\alpha_{p,j}-\alpha_{p,k}) \le M$ *for all* $j\ne k$.

Put $f^*(x)=f(x)+\Delta$, *where* $\Delta\in\mathbb{Z}_p$ *satisfies*

$$\mathrm{ord}_p(\Delta) \ge \frac{m}{p-1} + (l+1)M.$$

Then $f^*(x)$ *splits completely over* $\mathbb{Z}_p$, *and its roots* $\alpha^*_{p,j}$ *can be uniquely set in one-to-one correspondence with the roots of* $f(x)$ *in such a way that for all* j,

$$\mathrm{ord}_p(\alpha^*_{p,j}-\alpha_{p,j}) > M.$$

Proof. Fix a root $\alpha_{p,J}$ of $f(x)$, and consider the Newton polygon of $f^*(x)$ expanded about $\alpha_{p,J}$: write

$$f^*(z)=\sum_{i=0}^{m} d_i(x-\alpha_{p,J})^i.$$

By assumption, $d_0=\Delta$ and

$$d_1 = \prod_{\substack{j=0\\ j\ne J}}^{m-1}(\alpha_{p,j}-\alpha_{p,J}). \tag{4.10}$$

We wish to estimate d_1. There is a unique integer J_0 in the range $0 \le J_0 < p^{\lceil\log_p(m)\rceil}$ for which

$$\mathrm{ord}_p(\alpha_{p,J}-J_0) \ge \log_p(m);$$

in particular, $\mathrm{ord}_p(\alpha_{p,J} - J_0) \geq \log_p(n_i)$ for each i. Furthermore, by hypothesis (T1), for each T_i there is at most one root $\alpha_{p,j_i} \in T_i$ such that

$$\mathrm{ord}_p(\alpha_{p,j_i} - J_0) \geq \log_p(n_i).$$

Let $\mathcal{E} = \{j_i : 1 \leq i \leq l\}$ be the set of indices of these exceptional roots; note that $J \in \mathcal{E}$.

If $\alpha_{p,j}$ is a root with $j \notin \mathcal{E}$, we claim that

$$\begin{aligned} \mathrm{ord}_p(\alpha_{p,j} - \alpha_{p,J}) &= \min(\mathrm{ord}_p(\alpha_{p,j} - j), \mathrm{ord}_p(j - J_0), \mathrm{ord}_p(\alpha_{p,J} - J_0)) \\ &= \mathrm{ord}_p(j - J_0). \end{aligned} \tag{4.11}$$

Indeed, if $\alpha_{p,j} \in T_i$, then $\mathrm{ord}_p(\alpha_{p,j} - j) \geq \log_p(n_i)$ by hypothesis (T2), while $\mathrm{ord}_p(\alpha_{p,j} - J_0) < \log_p(n_i)$ since j is not exceptional; and hence

$$\mathrm{ord}_p(j - J_0) < \mathrm{ord}_p(\alpha_{p,j} - j). \tag{4.12}$$

In particular, (4.12) implies that $j \neq J_0$. Consequently by the characterization of J_0 and the fact that $j < p^{\lceil \log_p(m) \rceil}$, we have $\mathrm{ord}_p(\alpha_{p,J} - J_0) \geq \log_p(m)$ but $\mathrm{ord}_p(\alpha_{p,J} - j) < \log_p(m)$, and so

$$\mathrm{ord}_p(j - J_0) < \mathrm{ord}_p(\alpha_{p,J} - J_0). \tag{4.13}$$

Now (4.12) and (4.13) yield (4.11). On the other hand for each root $\alpha_{p,j}$ with $j \in \mathcal{E}$, $j \neq J$, then in any case by hypothesis (T3),

$$\mathrm{ord}_p(\alpha_{p,j} - \alpha_{p,J}) \leq M. \tag{4.14}$$

Since $J \in \mathcal{E}$, we have $\#(\mathcal{E} \backslash \{J\}) \leq l - 1$. Hence by (4.10), (4.11), and (4.14),

$$\begin{aligned} \mathrm{ord}_p(d_1) &= \mathrm{ord}_p\Big(\prod_{\substack{j=0 \\ j \notin \mathcal{E}}}^{m-1} (j - J_0) \Big) + \mathrm{ord}_p\Big(\prod_{\substack{j \in \mathcal{E} \\ j \neq J}} (\alpha_{p,j} - \alpha_{p,J}) \Big) \\ &\leq \mathrm{ord}_p\Big(\prod_{\substack{j=0 \\ j \neq J_0}}^{m-1} (j - J_0) \Big) + (l-1)M. \end{aligned}$$

There are now two cases. If $J_0 < m$, then

$$\mathrm{ord}_p\Big(\prod_{\substack{j=0 \\ j \neq J_0}}^{m-1} (j - J_0) \Big) = \mathrm{ord}_p(J_0!) + \mathrm{ord}_p((m - J_0 - 1)!) \leq \frac{m-1}{p-1}.$$

However, if $J_0 \geq m$, then by the bound $J_0 - m < J_0 < p^{\lceil \log_p(m) \rceil}$ we have

$\lceil \log_p(J_0 - m) \rceil \le \lceil \log_p(m) \rceil$, and so by (2.5) it follows that

$$\begin{aligned} \operatorname{ord}_p\Big(\prod_{\substack{j=0 \\ j \ne J_0}}^{m-1} (j - J_0)\Big) &= \operatorname{ord}_p(J_0!) - \operatorname{ord}_p((J_0 - m)!) \\ &\le \frac{J_0 - 1}{p-1} - \left(\frac{J_0 - m}{p-1} - \lceil \log_p(J_0 - m) \rceil \right) \\ &= \frac{m-1}{p-1} + \lceil \log_p(m) \rceil. \end{aligned}$$

By assumption $M \ge \lceil \log_p(m) \rceil$. Thus, in either case,

$$\operatorname{ord}_p(d_1) \le \frac{m-1}{p-1} + lM. \tag{4.15}$$

For the coefficients d_i with $i \ge 2$, we have

$$d_i = \pm d_1 \sum_{\substack{k_1, \dots, k_{i-1} \\ \text{distinct}, \ne J}} [(\alpha_{p,k_1} - \alpha_{p,J}) \dots (\alpha_{p,k_{i-1}} - \alpha_{p,J})]^{-1}$$

so that

$$\operatorname{ord}_p(d_i) \ge \operatorname{ord}_p(d_1) - (i-1)M.$$

By our hypothesis on $\operatorname{ord}_p(\Delta)$, the Newton polygon of $f^*(x)$ has a break at the point $(1, \operatorname{ord}_p(d_1))$, and if its initial segment has slope m, then $-m > M$. Hence, $f^*(x)$ has a unique root α_J^* for which $\operatorname{ord}_p(\alpha_J^* - \alpha_J) > M$. By the uniqueness, this root belongs to $\mathbb{Q}_p$, and hence to $\mathbb{Z}_p$.

At the kth step of the patching process, we apply Lemma 4.2 with $m = k$, $l = 2$, $M = 4C \log_p(n)$ and

$$f(x) = \prod_{j=0}^{k-1} (x - \alpha_{p,j})$$

where the roots $\alpha_{p,j}$ are those of the current polynomial $u_p^{(k-1)}(x)$, given their natural labelling. Clearly $M \ge \lceil \log_p(m) \rceil$. We will take

$$\begin{aligned} T_1 &= \{\alpha_{p,j} : 0 \le j < \lfloor L_2(n) \rfloor\}, \\ T_2 &= \{\alpha_{p,j} : \lfloor L_2(n) \rfloor \le j < k\}, \end{aligned}$$

with $m_1 = \lfloor L_2(n) \rfloor$ and $m_2 = k$; thus T_1 consists of the roots moved in Stages I and II, and T_2 is an initial segment of the remaining roots. In Stages III, IV, and V, roots are moved only by quantities with ord value $\ge \log_p(n)$, preserving their position in the regular sequence of length n. Hence T_2 is a subset of a regular sequence of length n, but we only use that it is a subset of a regular sequence of length k. Hypothesis (T2) in Lemma 4.2 is satisfied for T_1, since T_1 is regular of length m_1 by the construction in Stages

I and II; and it is satisfied for T_2 since the original labelling of the roots was such that $\mathrm{ord}_p(\alpha_{p,j} - j) \geq \log_p(n)$ for roots in T_2, and this property was preserved thoughout the patching process.

As noted above, for $k > L_3(n) = \frac{13C \cdot \#(T)}{\ln(h/q)} \ln(n)$ we have

$$h^k > \prod_{p \in T} p^{\lceil k/(p-1) + 3(4C \log_p(n)) \rceil}.$$

We can thus find target coefficients $c_k \in \mathbb{Z}$ such that

$$\begin{cases} |c_k - c_{\infty,k}| < h^k, \\ \mathrm{ord}_p(c_k - c_{p,k}) > k/(p-1) + 3 \cdot 4C \log_p(n) \quad \text{for } p \in T. \end{cases}$$

The patching polynomials will simply be

$$w_p^{(k)}(x) = \prod_{j=k}^{n-1} (x - \alpha_{p,j}) \quad \text{for } k < n,$$

$$w_p^{(n)}(x) = 1.$$

It follows from Lemma 4.2 that at each step the roots are moved by quantities with ord value $> 4C \log_p(n)$. Hence they remain separated in ord value by at least $4C \log_p(n)$, and the hypotheses of Lemma 4.2 continue to hold; the patching process carries through to the end.

References

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, Science Publishers, New York, 1967.

[2] D. Cantor, *On an extension of the definition of transfinite diameter and some applications*, J. Reine Angew. Math. 316 (1980), 160–207.

[3] L. Comptet, *Advanced Combinatorics*, Reidel, Boston, 1979.

[4] M. Fekete and G. Szegő, *On algebraic equations with integral coefficients whose roots belong to a given set*, Math. Z. 63 (1955), 158–172.

[5] R. M. Robinson, *Conjugate algebraic integers in real point sets*, Math. Z. 84 (1964), 415–427.

[6] R. Rumely, *Capacity Theory on Algebraic Curves*, Lecture Notes in Math. 1378, Springer, New York, 1989.

Department of Mathematics
University of Georgia
Athens, GA 30602, U.S.A.
E-mail: rr@alpha.math.uga.edu

Received on 27.4.1998 (3369)