Pertanika 9(1), 51 – 56 (1986)

Newton Polyhedra and p-Adic Estimates of Zeros of Polynomials in $\Omega_p[x, y]$

KAMEL ARIFFIN MOHD ATAN
Mathematics Department,
Faculty of Science and Environmental Studies,
Universiti Pertanian Malaysia,
43400 Serdang, Selangor, Malaysia.

Key words: p-adic estimates, zeros of polynomials, indicator diagrams.

ABSTRAK

Polihedron Newton yang disekutukan dengan suatu polinomial dalam $\Omega_p[x, y]$ diperkenalkan. Dibuktikan bahawa wujud hubungan antara polihedron Newton dengan pensifar-pensifar polinomial yang disekutukan dengannya itu. Hubungan ini digunakan untuk mendapatkan anggaran p-adic pensifar-pensifar tersebut. Suatu batas atas bagi peringkat p-adic pensifar-pensifar ini diperolehi dengan menggunakan kaedah polihedron Newton.

ABSTRACT

Newton polyhedron associated with a polynomial in $\Omega_p[x, y]$ is introduced. Existence of a relationship between a Newton polyhedron and zeros of its associated polynomial is proved. This relationship is used to arrive at the p-adic estimates of the zeros. An upper bound to the p-adic orders of these zeros is found using the Newton polyhedron method.

1. INTRODUCTION

The role of the Newton polygon in obtaining properties of zeros of polynomials in one variable is quite well-known. For example, the Newton polygon can be usefully applied in proving Puiseux's theorem (Walker, 1962; Lefschetz, 1953). A Sathaye (1983) also considered generalised Newton-Puiseux expansion.

In the p-adic case Koblitz (1977) discusses the Newton polygon method for polynomials and power series in $\Omega_p[x]$ where Ω_p denotes the completion of the algebraic closure of the field of p-adic numbers Q_p. Here estimates concerning zeros of polynomials are derived from the properties of the associated Newton polygon. Loxton and Smith (1982) investigated the application of the Newton polygon technique although a different method was eventually used to arrive at their result.

In this paper we consider extending the Newton polygon idea in the p-adic case to polynomials in two variables and call it the Newton polyhedron method. We will derive p-adic properties of zeros of such polynomials from their associated Newton polyhedrons, as asserted in Theorem 2.1 and Theorem 2.2.

With p denoting a prime, we define the valuation $\| _p$ on Q_p as usual. That is

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

where $\mathrm{ord}_p\, x$ denotes the highest power of p dividing x and $\mathrm{ord}_p\, x = \infty$ if $x = 0$. This valuation extends uniquely from Q_p to $\bar{Q}_p$ the algebraic closure of Q_p and to Ω_p, and Ω_p is complete and algebraically closed.

Birch and Mc Cann (1967) showed that if $f(x_1, \ldots, x_n)$ is a polynomial with integral coefficients and $\mathrm{ord}_p(f(a_1, \ldots, a_n)) > \mathrm{ord}_p D_n(f)$ where $D_n(f)$ is the discriminant of f for some integers $a_1, \ldots, a_n$, then there are p-adic integers $\alpha_1, \ldots, \alpha_n$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$ and $\mathrm{ord}_p(a_i - \alpha_i) > 0$ for $i = 1, \ldots, n$.

From the properties of p-adic zeros established for polynomials in two variables from the associated Newton polyhedron, we give an estimate for the p-adic order of zeros of polynomials in two variables with coefficients in $\bar{Q}_p$. Our assertion is as follows.

Theorem 1.1

Let f be a polynomial in $\bar{Q}_p[x, y]$. Let

$$\delta = \max_{r,s} \frac{1}{r+s}\left\{\mathrm{ord}_p f(\alpha, \beta) - \mathrm{ord}_p \frac{f^{(r+s)}(\alpha, \beta)}{r!s!}\right\}$$

for some α, β in $\bar{Q}_p$ where the maximum is taken over all pairs of non-negative integers (r, s). Then f has a zero (ξ_o, η_o) in $\bar{Q}_p^2$ with $\mathrm{ord}_p(\xi_o - \alpha, \eta_o - \beta) = \delta$ and every zero (ξ, η) of f satisfies $\mathrm{ord}_p(\xi - \alpha, \eta - \beta) \leq \delta$.

2. NEWTON POLYHEDRON AND ZEROS OF A POLYNOMIAL IN $\Omega_p[x, y]$

Definition 2.1

Let $f(x, y) = \Sigma a_{ij}x^iy^j$ be a polynomial of degree n in $\Omega_p[x, y]$. We map the terms $T_{ij} = a_{ij}x^iy^j$ of f to the points $P_{ij} = (i, j, \mathrm{ord}_p a_{ij})$ in the Euclidean space. The Newton polyhedron of f is defined to be the lower convex hull of the set S of points P_{ij}, $0 \leq i, j \leq n$. It is the highest convex connected surface which passes through or below the points in S. If $a_{ij} = 0$ for some (i, j) then we take $\mathrm{ord}_p a_{ij} = \infty$.

By the above definition the Newton polyhedron of a polynomial f in $\Omega_p[x, y]$ which we will denote by N_f will consist of polyhydral faces possessing edges and vertices on and above which lie all the points P_{ij} corresponding to each term T_{ij} in f. It is the highest polyhedral surface obtained by raising the horizontal plane until it bends around various points P_{ij} and eventually reaches the outermost points P_{ij} which correspond to the points (i, j) on the classical Newton polygon of f. Around these points the plane bends up to form several vertical faces perpendicular to the 1 – 2 plane passing through the terminal edges determined by the outermost points P_{ij}.

Theorem 2.1

Let p be a prime and f be a polynomial in $\Omega_p[x, y]$. If (ξ, η) is a zero of f then $(\mathrm{ord}_p \xi, \mathrm{ord}_p \eta, 1)$ is normal to an edge in N_f and falls between the upward-pointing normals to the faces of N_f adjacent to this edge.

Proof: Let $f(x, y) = \sum_{i,j=0}^{n} a_{ij}x^iy^j$ where the a_{ij} are in Ω_p. Let $T_{ij} = a_{ij}\xi^i\eta^j$. Since (ξ, η) is a zero of f(x, y) it follows that there are at least two terms T_{rs}, T_{mn} say of $f(\xi, \eta)$ which attain the minimum ord_p, that is $\mathrm{ord}_p T_{rs} = \mathrm{ord}_p T_{mn} = \min_{i,j} \mathrm{ord}_p T_{ij}$. Thus, the corresponding points P_{rs} and P_{mn} to T_{rs} and T_{mn} respectively satisfy the equation:

$$x\,\mathrm{ord}_p \xi + y\,\mathrm{ord}_p \eta + z = M \quad (1)$$

where $M = \min_{i,j} \mathrm{ord}_p T_{ij}$. That is P_{rs} and P_{mn} lie on the plane Z say whose equation is given in (1).

Since $M \leq \mathrm{ord}_p T_{ij}$ for every $0 \leq i, j \leq n$, it follows that every point P_{ij} in S lies on or above the plane Z, and the line segment E joining P_{rs} to P_{mn} is either an edge or lies on a face F of N_f. In either case E lies in the plane Z. The normal $\underset{\sim}{u} = (\mathrm{ord}_p \xi, \mathrm{ord}_p \eta, 1)$ to Z is normal to F containing E. Clearly $\underset{\sim}{u}$ is normal to at least one of the edges of F. Further, since N_f lies above Z, $\underset{\sim}{u}$ must lie between the upward-pointing normals to the faces of N_f adjacent to the edges of F.

We will prove the converse to the above theorem. First we have the following lemma.

Lemma 2.1: Let L be a finite extension of Q_p. Let $f(x) = \sum_{i=0}^{m} a_i x^i$ and $g(x) = \sum_{i=0}^{n} b_i x^i$ be polynomials in L[X]. Let λ be in Q and let $\mu_o = \min_i (\text{ord}_p a_i + i\lambda)$, $\mu_1 = \min_i (\text{ord}_p b_i + i\lambda)$. Then there is a ξ in $\overline{Q}_p$ with $\text{ord}_p \xi = \lambda$ and $\text{ord}_p f(\xi) = \mu_o$ and $\text{ord}_p g(\xi) = \mu_1$.

Proof: Let K be a finite unramified extension of L with prime element π chosen so that the residue field is sufficiently large as required below. Let Σ be a set of representatives in K for the residue field. Write

$$a_i = \pi^{\mu_o - i\lambda + \epsilon_i} \sum_{\ell \geq 0} a_i^{(\ell)} \pi^{\ell} \quad (0 \leq i \leq m)$$

where $\epsilon_i \geq 0$ and the $a_i^{(\ell)}$ are in Σ and $a_i^{(0)} \neq 0$. Consider

$$\xi = \pi^{\lambda} \sum_{\ell \geq 0} C_\ell \pi^{\ell}$$

where the C_ℓ are in Σ and $C_o \neq 0$. Then

$$f(\xi) = \pi^{\mu_o} \sum_{\epsilon_j = 0} a_i^{(0)} C_o^i + 0(\pi^{\mu_o + 1}).$$

If the residue field is sufficiently large, we can find C_o in Σ so that

$$\sum_{\epsilon_i = 0} a_i^{(0)} C_o^i \not\equiv 0 \pmod{\pi}$$

and this gives the required ξ in $\overline{Q}_p$ for the polynomial f.

Similarly, by letting

$$b_i = \pi^{\mu_1 - i\lambda + \epsilon_i} \sum_{\ell \geq 0} b_i^{(\ell)} \pi^{\ell} \quad (0 \leq i \leq n)$$

where $\epsilon_i \geq 0$, the $b_i^{(\ell)}$ are in Σ and $b_i^{(0)} \neq 0$ and considering

$$\xi = \pi^{\lambda} \sum_{\ell \geq 0} C_\ell \pi^{\ell}$$

as above, we see that ξ can also be chosen to be the required element in $\overline{Q}_p$ for the polynomial g.

Theorem 2.2

Let f be a polynomial in $\overline{Q}_p[x, y]$. Let E be a non-vertical edge of N_f common to two adjacent faces F_1 and F_2. Suppose $\underset{\sim}{n} = (\lambda, \mu, 1)$ is normal to E and lies between the upward-pointing normals to F_1 and F_2. Then there are ξ and η in $\overline{Q}_p$ such that $\text{ord}_p \xi = \lambda$, $\text{ord}_p \eta = \mu$ and $f(\xi, \eta) = 0$.

Proof: Let $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$ and let V_{rs} and V_{mn} be the end-points of the edge E on N_f. Then

$\underset{\sim}{e} = (m - r, n - s, \text{ord}_p a_{mn} - \text{ord}_p a_{rs})$ is a vector from V_{rs} to V_{mn}.

Choose ξ, η in $\overline{Q}_p$ with $\text{ord}_p \xi = \lambda$, $\text{ord}_p \eta = \mu$. We show first that the terms corresponding to V_{rs} and V_{mn} dominate in $f(\xi, \eta)$. Since $\underset{\sim}{n}$ is orthogonal to $\underset{\sim}{e}$, we have

$(m - r)\,\text{ord}_p \xi + (n - s)\,\text{ord}_p \eta + \text{ord}_p a_{mn} - \text{ord}_p a_{rs} = 0$, that is

$\text{ord}_p a_{rs} \xi^r \eta^s = \text{ord}_p a_{mn} \xi^m \eta^n$.

Let $\underset{\sim}{n}_1$ and $\underset{\sim}{n}_2$ be the upward-pointing normals to the faces F_1 and F_2 respectively, normalised to have third component equal to 1.

Since $\underset{\sim}{n}$ is in the plane of $\underset{\sim}{n}_1$ and $\underset{\sim}{n}_2$ and lies between them, we can write

$$\underset{\sim}{n} = \gamma \underset{\sim}{n}_1 + (1 - \gamma)\underset{\sim}{n}_2$$

with $0 \leq \gamma \leq 1$.

Let V_{ij} be any point in N_f and let $\underset{\sim}{v}$ be the vector from V_{rs} to V_{ij}. From the definition of N_f, the line segment from V_{rs} to V_{ij} lies on or above the planes determined by F_1 and F_2. So, we have

$$\underset{\sim}{v} \cdot \underset{\sim}{n} = \gamma\, \underset{\sim}{v} \cdot \underset{\sim}{n}_1 + (1 - \gamma)\, \underset{\sim}{v} \cdot \underset{\sim}{n}_2 \geq 0 ,$$

that is

$$\mathrm{ord}_p a_{ij}\, \xi^i \eta^j \geq \mathrm{ord}_p a_{rs}\, \xi^r \eta^s .$$

Hence, as asserted

$$\mathrm{ord}_p a_{rs}\, \xi^r \eta^s = \mathrm{ord}_p a_{mn}\, \xi^m \eta^n$$

$$= \min_{i,j} \mathrm{ord}_p a_{ij}\, \xi^i \eta^j .$$

(2) We can suppose $r \neq m$. Otherwise the same argument applies after interchanging x and y. Choose η in $\overline{Q}_p$ with $\mathrm{ord}_p\, \eta = \mu$ as specified below, and write

$$g(x) = f(x, \eta) = \sum_k c_k(\eta)x^k$$

where

$$c_k(\eta) = \sum_j a_{kj}\, \eta^j$$

By part (1), $\mathrm{ord}_p a_{rs} \eta^s = \min_j \mathrm{ord}_p a_{rj} \eta^j$ and $\mathrm{ord}_p a_{mn} \eta^n = \min_j \mathrm{ord}_p a_{mj} \eta^j$. By Lemma (2.1) we can choose η in $\overline{Q}_p$ with $\mathrm{ord}_p\, \eta = \mu$ so that $\mathrm{ord}_p c_r(\eta) = \mathrm{ord}_p a_{rs} \eta^s$ and $\mathrm{ord}_p c_m(\eta) = \mathrm{ord}_p a_{mn} \eta^n$. Using (1) again, we have

$\mathrm{ord}_p c_r(\eta) + \lambda r = \mathrm{ord}_p c_m(\eta) + \lambda m \leq \mathrm{ord}_p c_k(\eta) + \lambda k$, for each k. Thus the line segment joining the points $(r, \mathrm{ord}_p c_r(\eta))$ and $(m, \mathrm{ord}_p c_m(\eta))$ having slope $-\lambda$, is part of the Newton polygon of g(x). By a standard theorem (see Koblitz (1977) lemma 4, page 90), therefore, there is a ξ in $\overline{Q}_p$ with $\mathrm{ord}_p\, \xi = \lambda$ and $g(\xi) = 0$. This choice of ξ and η satisfies the requirements of the theorem.

3. p-adic ESTIMATE OF ZEROS OF A POLYNOMIAL IN $\Omega_p [x, y]$

Definition 3.1

Let $(\mu_i, \lambda_i, 1)$ be the normalised upward-pointing normals to the faces F_i of N_f, of a polynomial f(x, y) in $\Omega_p[x, y]$. We map $(\mu_i, \lambda_i, 1)$ to the point (μ_i, λ_i) in the x – y plane. If F_r and F_s are adjacent faces in N_f, sharing a common edge, we construct the straight line joining (μ_r, λ_r) and (μ_s, λ_s). If F_r shares a common edge with a vertical face F say $\alpha x + \beta y = \gamma$ in N_f we construct the straight line segment joining (μ_r, λ_r) and the appropriate point at infinity that corresponds to the normal of F, that is the segment along a line with slope $-\alpha / \beta$. We call the set of lines so obtained the Indicator diagram associated with N_f.

Hence by the above definition if (μ, λ) is a point lying on the straight line segment joining (μ_1, λ_1) and (μ_2, λ_2) say in the Indicator diagram of an N_f then $(\mu, \lambda, 1)$ is normal to the common edge of the faces to which $(\mu_1, \lambda_1, 1)$ and $(\mu_2, \lambda_2, 1)$ are normal. It follows by Theorem 2.2 that the point (μ, λ) gives the p-adic order of a zero (ξ, η) of the associated polynomial f.

Definition 3.2

We call the segment in an Indicator diagram of an N_f that corresponds to the initial edges passing through the vertical axis in R^3, the initial segments of the Indicator diagram.

Let $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$ be a polynomial in $\Omega_p [x, y]$ of degree n, and let $\alpha_{ij} = \mathrm{ord}_p a_{oo} - \mathrm{ord}_p a_{ij}$. Then the equation of an initial segment of the Indicator diagram associated with N_f is of the form $rx + sy = \alpha_{rs}$ obtained by considering the relationships of normals (x, y, 1) to the edges ${}_{oo}E_{rs}$ of N_f which join the points V_{oo}: (0, 0, $\mathrm{ord}_p a_{oo}$) and V_{rs}: (r, s, $\mathrm{ord}_p a_{rs}$).

By making use of the Newton polyhedron method we give the following theorem.

Theorem 3.1

Let $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$ be a polynomial in $\overline{Q}_p[x, y]$ and let

$$\delta = \max_{r,s} \frac{1}{(r+s)} (\text{ord}_p\, a_{oo} - \text{ord}_p\, a_{rs})$$

where the maximum is taken over all pairs (r, s). Then f has a zero (ξ_o, η_o) in $\overline{Q}_p^2$ with $\text{ord}_p(\xi_o, \eta_o) = \delta$ and every zero (ξ, η) satisfies $\text{ord}_p(\xi, \eta) \leq \delta$.

Proof: We note first that the maximum defining δ occurs for an initial edge in N_f. Let ${}_{oo}E_{r_j s_j}$ and ${}_{oo}E_{r_{j+1} s_{j+1}}$ denote a pair of initial edges common to an initial face F_j in N_f such that by the convexity of N_f and the consecutive ordering of the initial edges,

$$\frac{r_j}{s_j} > \frac{r_{j+1}}{s_{j+1}}.$$

Let ℓ_i denote the segments in the Indicator diagram corresponding to the edges ${}_{oo}E_{r_i s_i}$ in N_f. Thus ℓ_j and ℓ_{j+1} in the Indicator diagram associated with N_f are adjacent segments sharing a common vertex. Now the equation of ℓ_i is given by

$$r_i x + s_i y = \alpha_{r_i s_i}$$

where $\alpha_{r_i s_i} = \text{ord}_p\, a_{oo} - \text{ord}_p\, a_{r_i s_i}$. Since $\frac{r_j}{s_j} > \frac{r_{j+1}}{s_{j+1}}$, ℓ_j is steeper than ℓ_{j+1}. As this is true for every j, $1 \leq j \leq k$ say, the set of initial segments in the Indicator diagram associated with N_f has a convex shape. The line y = x intersects some initial segment ℓ_m say, at a point (μ_m, μ_m). Also, for every j, $j \neq m$ the line y = x intersects lines ℓ_j produced at some points (μ_j, μ_j). Since $\frac{r_{m+t}}{s_{m+t}} < \frac{r_m}{s_m} < \frac{r_{m-t}}{s_{m-t}}$ it follows that $\mu_m > \mu_{m-t}, \mu_{m+t}$ for every t, $0 < t < m$, $m + t \leq k$. Hence

$$\mu_m \geq \mu_j \quad (1)$$

for every j, $1 \leq j \leq k$. By considering the equation of ℓ_j, there are r_j, s_j such that

$$\mu_j = \frac{1}{r_j + s_j} \text{ord}_p \frac{a_{oo}}{a_{r_j s_j}}$$

Then, clearly by (1),

$$\mu_m = \max_j \frac{1}{r_j + s_j} \text{ord}_p \frac{a_{oo}}{a_{r_j s_j}} \quad (2)$$

By the convexity of the set of initial segments in the Indicator diagram associated with N_f, for every point (μ_j, λ_j) in the initial segments ℓ_j, we have

$$\mu_m > \min_j (\mu_j, \lambda_j) \quad (3)$$

for every j, $j \neq m$. By Theorem 2.2 and Definition 3.1 there exist ξ_o, η_o in $\overline{Q}_p$ such that $\text{ord}_p\, \xi_o = \mu_m$, $\text{ord}_p\, \eta_o = \mu_m$ and $f(\xi_o, \eta_o) = 0$, and there are ξ_j, η_j in $\overline{Q}_p$ with $\text{ord}_p\, \xi_j = \mu_j$, $\text{ord}_p\, \eta_j = \lambda_j$ and $f(\xi_j, \lambda_j) = 0$. Our assertion then follows from (2), (3) and letting $\delta = \mu_m$.

The above theorem is a special case of Theorem 1.1 whose proof is as follows.

Proof of Theorem 1.1. Let g(X, Y) be the resulting polynomial on expanding $f(X + \alpha, Y + \beta)$ using Taylor's theorem. That is,

$$g(X, Y) = f(\alpha, \beta) + \sum_{\substack{r,s \geq 0 \\ (r,s) \neq (0,0)}} \frac{f^{(r+s)}(\alpha, \beta) X^r Y^s}{r!s!}$$

By Theorem 3.1 there are γ_1, γ_2 in $\overline{Q}_p$ such that $f(\gamma_1, \gamma_2) = 0$ and $\text{ord}_p(\gamma_1, \gamma_2) = \delta$ and every zero (X', Y') of g satisfies $\text{ord}_p(X', Y') \leq \delta$.

Set $\xi_o = \gamma_1 + \alpha$, $\eta_o = \gamma_2 + \beta$ and $\xi = X' + \alpha$, $\eta = Y' + \beta$. Then (ξ_o, η_o) and (ξ, η) are zeroes of f satisfying the requirements of the theorem.

CONCLUSION

Theorems 2.1 and 2.2 assert the existence of relationships between zeros of polynomials in $\Omega_p[x, y]$ and their associated Newton polyhedra. This relationship is already well-known for one-variable polynomials with coefficients in Ω_p. Newton polyhedra associated with polynomials in two variables with coefficients in Ω_p is treated in more detail in Mohd Atan (1984). The result of Theorem 1.1 gives an improvement to a result by Birch and McCann (1967) for polynomials in two variables.

ACKNOWLEDGEMENTS

The author would like to express his gratitude to Assoc. Prof. J. Loxton of the University of New South Wales for suggesting the problem and for discussions leading to the result.

REFERENCES

WALKER, R.J. (1962): 'Fractional power series', Algebraic Curves, Dover Publ. Inc., pp. 97 – 106.

LEFSCHETZ, S. (1953): 'Puiseux's Theorem', Algebraic Geometry, Princeton, Univ. Press. pp. 99 – 104.

SATHAYE, A. (1983): 'Generalised Newton-Puiseux Expansion and Abhyyankar-Moh semigroup Theorem', *Inventiones Math.* 74: 149 – 157.

KOBLITZ, N. (1977): 'p-adic power series', p-adic Analysis, and Zeta-Functions, Springer Verlag, New York, Berlin 1977.

LOXTON, J.H. and SMITH, R.A. (1982): 'On Hua's estimate for exponential sums' *J. London Math. Soc.* 26(2): 15 – 20.

BIRCH, B.J. and McCANN, K. (1967): 'A Criteria for the p-adic solubility of diophantine equations', *Quart. J. Math. Oxford* 18(2): 59 – 63.

MOHD ATAN K.A. (1984). Newton polyhedra and estimates for exponential sums. Ph.D. Thesis, University of New South Wales, Kensington, Australia.

(Received 16 July, 1985)