Proceedings of the 2nd IMT-GT Regional Conference on Mathematics, Statistics and Applications
Universiti Sains Malaysia

NEWTON POLYHEDRA AND ESTIMATION TO EXPONENTIAL SUMS

[1]Kamel Ariffin Mohd Atan and [2]J.H. Loxton

[1]Institute for Mathematical Research, Universiti Putra Malaysia, Malaysia
[2]School of Mathematics, Physics and Computing, Macquarie University, Australia

1. Introduction

The classical Newton polygon is a device for computing the fractional power series expansions of algebraic functions. Newton gave a number of examples of this process in his "Method of Fluxions" which amount to a general method. However, it was not till much later that Puiseux proved that every branch of a plane algebraic curve defined by a polynomial equation $f(x,y)=0$ has an expansion

$$y-y_0=\sum\nolimits_{j\geq 0} c_j\left(x-x_0\right)^{(a+bj)/q}$$

in a neighbourhood of a point (x_0,y_0) on the curve. In practice, the integers a,b and q can be read off from the Newton polygon and the coefficients c_j can be determined successively with ever-increasing labour. (See, for example, [18], pages $98-106$.) Much of this extends naturally to several variables. For example, let $z=(z_1,...,z_n)$ in C^{*n} be a complex n-vector with no component zero and for $\alpha=(\alpha_1,...,\alpha_n)$ in Z^n, write $z^\alpha=z_1^{\alpha_1}...z_n^{\alpha_n}$. Let $S_1,...,S_n$ be finite subsets of Z^n and let $N\left(S_1,...,S_n\right)$ denote the number of solutions in C^{*n} of the system of equations

$$\sum_{\alpha\ in\ S_i} c_{i,\alpha}z^\alpha=0(i=1,2,...n).$$

By analogy with the classical case, the Newton polyhedron of the equation

$$\sum_{\alpha\ in\ S} c_\alpha z^\alpha=0$$

is the convex hull $\hat{S}$ of the set S in R^n. Bernstein [7] has shown that for systems in general position, that is for all systems except for some agebraic submanifold in the space of coefficients,

$$N\left(S_1,...,S_n\right)=n!V\left(\hat{S}_1,...,\hat{S}_n\right)$$

where V is the Minkowski mixed volume of the n Newton polyhedra.(This is the symmetric multilinear function whose diagonal part $V\left(\hat{S},...\right)$ is just the n-dimensional Euclidean volume of $\hat{S}$). Moreover, the Newton polyhedra of the equations can be used to construct discriminant conditions which describe the special systems for which the formula breaks down. Another account of Bernstein's formula is given in [6]. We shall be concerned here with p-adic versions of these ideas. The motivation comes from the study of multiple exponential sum of the shape

$$S\left(f;q\right)=\sum_{\underset{\sim}{x}\ \mathrm{mod}\ q}\exp\left(2\pi i f\left(\underset{\sim}{x}\right)/q\right),$$

where f is a polynomial with integer coefficients and the summation is taken over a complete set of residues of each of the components of $\underset{\sim}{x}$ modulo q. Under suitable conditions of f, we can estimate $S(f;p)$ for a prime p using Deligne's work on the Weil conjuctures, then proceed to estimates for $S(f;p^\alpha)$ by induction, and use the multiplicativity of $S(f;q)$ in q to get the general case. This method is used in [15] to show that if f is a polynomial in $X_1,\ldots,X_n$ of degree d with integer coefficients, f considered modulo p is non-singular at infinity for each prime p dividing q, and the hypersurfaces $\frac{\partial f}{\partial X_i}=0$ meet transversely, then

$$\left|S\left(f;q\right)\right|\leq d^{n\omega(q)}q^{n/2}\left(\Delta^5,q\right)^{n/2},$$

where $\omega(q)$ denotes the number of distinct prime factors of q and Δ is the discriminant of grad f. (In fact, Δ is the least positive integer in the ideal in $Z\left[\underset{\sim}{X}\right]$ generated by the polynomials $\frac{\partial f}{\partial X_i}$ and the Hessian det $\left(\frac{\partial^2 f}{\partial X_i \partial X_j}\right)$). The simplest way to do the induction step in the estimation of $S(f;p^\alpha)$ is to reduce it to counting the solutions of a system of congruences. If we write $\underset{\sim}{x} = \underset{\sim}{u} + p^{[\alpha/2]}\underset{\sim}{v}$ in $S(f;p^\alpha)$, so that $\underset{\sim}{u}$ and $\underset{\sim}{v}$ run through complete sets of residues mod $p^{[\alpha/2]}$and mod $p^{\alpha-[\alpha/2]}$ respectively, we get

$$|S(f;p^\alpha)| \leq p^{n(\alpha-[\alpha/2])} \# \left\{ \underset{\sim}{u} \bmod p^{[\alpha/2]} : \operatorname{grad} f \equiv 0 \bmod p^{[\alpha/2]} \right\}.$$

In [15], the right-side of this inequality is estimated by some p-adic analysis invoking Hensel's lemma at a critical stage. This is responsible for the fairly poor dependence on the discriminant in the final result given above and the lack of any result at all when the discriminant vanishes. Complete exponential sums for polynomials in one variable can be treated much more satisfactorily. The key is to use the p-adic Newton polygon instead of Hensel's lemma [14], and to take the induction step in smaller stages [16]. This paper is the beginning of an attempt to make similar ideas work for multiple exponential sums. As usual, Q_p denotes the field of p-adic numbers with the p-adic valuation $|x|_p$ normalised by $|p|_p = p^{-1}$. We write $\operatorname{ord}_p x$ for the corresponding additive valuation, so that $|x|_p = p^{-\operatorname{ord}_p x}$. By convention $\operatorname{ord}_p 0 = \infty$. We will have occasion to use the algebraic closure of Q_p, denoted by $\overline{Q}_p$, and the completion of $\bar{Q}_p$ denoted by Ω_p. The p-adic valuation extends uniquely to $\bar{Q}_p$ and Ω_p. Let

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n$$

be a polynomial in $\Omega_p[X]$. The p-adic Newton polygon of f is the lower convex hull of the set of points $(i, \operatorname{ord}_p a_i)$ for $i = 0, 1 \ldots, n$. The slopes of the edges of the Newton polygon give the p-adic orders of the reciprocals of the roots of f, with their multiplicities. More precisely, if the Newton polygon has an edge joining $(i, \operatorname{ord}_p a_i)$ and $(i + r, \operatorname{ord}_p a_i + \lambda r)$, then f has exactly r roots with p-adic order -λ. Further if α is one of these roots and K is the field generated over Q_p by the coefficients of f, then $[K(\alpha) : K] \leq r$. (For all this, see [12], pages $89 - 91$. The last remark comes from the fact that all the conjugates of α over K have the same order).

In the subsequent sections, we set up a p-adic Newton polyhedron for polynomials in two variables and investigate its connection with the p-adic zeros of polynomials. This program is mentioned briefly by Krasner [13] and developed by Thaler [17] with an eye on applications in algebraic geometry. In effect, he works over the field Ω_p. Section 2 sharpens Thaler's ideas and gives very satisfactory information about the sizes of the zeros of a single polynomial, parallelling the results about Newton polygons stated above. One consequence is that if f is a polynomial in $Q_p[X, Y]$ and (α, β) is a given point, we can determine the distance from (α, β) to the nearest p-adic zero of f by using the Newton polyhedron. (See Theorem 3.1). This result could be used to sharpen a theorem of Birch and McCann [8] on the solubility of polynomial equation in p-adic integers, bypassing the use of Hensel's lemma. In the light of the application to exponential sums, a critical problem is to estimate the size of the common zeros of a pair of polynomials in $Q_p[X, Y]$. We discuss this subject in Section 4. Again, we can recover Hensel's lemma with a slight improvement, but we have not been able to prove everything that we believe to be true. Much of the work here extends readily to polynomials in n variables with $n > 2$. This extension and the application of the results to the estimation of exponential sums will be the subject of another paper.

2. The Newton polyhedron

Let

$$f(X, Y) = \sum a_{ij} X^i Y^j$$

be a polynomial with coefficients in Ω_p, the completion of the algebraic closure of the field Q_p of p-adic numbers. To each term $a_{ij}X^iY^j$ of the polynomial, associate the point $P_{ij} = (i, j, \operatorname{ord}_p a_{ij})$ in Euclidean space. Here, ord_p denotes the extension of the usual additive p-adic valuation from Q_p to Ω_p, with the convention that $\operatorname{ord}_p 0 = \infty$. The Newton polyhedron of f is defined to be the lower convex hull of the set of points P_{ij}. Kinematically, we obtain the Newton polyhedron by pushing up a horizontal plane until it bends around the points P_{ij}, eventually reaching 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 a number of semi-infinite vertical faces. We investigate first the connection between the Newton polyhedron and the sizes of the zeros of polynomials. In one direction, this is quite straightforward.

Theorem 2.1. *Let f be a polynomial in $\Omega_p[X,Y]$ and let (ξ,η) be a zero of f. Then the vector $(\operatorname{ord}_p\xi,\operatorname{ord}_p\eta,1)$ is normal to a line on the Newton polyhedron of f and lies between the normals to the faces of the Newton polyhedron adjacent to this line.*

Proof. Let

$$f(X,Y)=\sum a_{ij}X^iY^j$$

and let

$$T_{ij}=a_{ij}\xi^i\eta^j.$$

Since $f(\xi,\eta)=0$ the minimum of the numbers $\operatorname{ord}_p T_{ij}$ is attained by at least two of the terms, say

$$\operatorname{ord}_p T_{mn}=\operatorname{ord}_p T_{rs}=\min_{i,j}\operatorname{ord}_p T_{ij}=M.$$

The points P_{mn} and P_{rs} correspoding to these terms as in the definition at the beginning of this section lie on the plane

$$\Pi: X\operatorname{ord}_p\xi+Y\operatorname{ord}_p\eta+Z=M.$$

Each point P_{ij} lies on or above Π since $\operatorname{ord}_p T_{ij}\geq M$, so the line segment E joining P_{rs} to P_{mn} lies on the Newton polyhedron and lies in Π. Finally, the normal $(\operatorname{ord}_p\xi,\operatorname{ord}_p\eta,1)$ to Π is normal to E and lies between the upward-pointing normals to the faces of the Newton polyhedron adjacent to E because the Newton polyhedron is a convex surface lying above Π. □

We will prove the converse of this theorem. To this end, the following lemma is useful.

Lemma 2.1. *Let $f(x)=\sum a_iX^i$ and $g(X)=\sum b_iX^i$ be polynomials in $Q_p[X]$ with respective degrees m and n, and let $\lambda=r/s$ be a rational number (in lowest terms). Write*

$$\mu=\min_{0\leq i\leq m}(\operatorname{ord}_p a_i+\lambda i),\quad v=\min_{0\leq i\leq n}(\operatorname{ord}_p b_i+\lambda i).$$

Then there is a number ξ with degree at most

$$s(1+[\log(m+n+1)/\log p])$$

over Q_p such that

$$\operatorname{ord}_p\xi=\lambda,\quad \operatorname{ord}_p f(\xi)=\mu,\quad \operatorname{ord}_p g(\xi)=v.$$

Proof. Let K be a totally ramified extension of Q_p of degree s and let π be a prime element in K. We look for ξ in an unramified extension, L say, of K with $[L:K]=t$. Thus π is a prime element in L and the residue field of L has a set of representatives $\sum$ consisting of p^t elements of L. In L, we have the π -adic expansions

$$\xi=\pi^{\lambda s}\sum_{j\geq 0}x_j\pi^j,\quad a_i=\pi^{(\mu-\lambda i)s}\sum_{j\geq 0}a_{ij}\pi^j,\quad b_i=\pi^{(v-\lambda i)s}\sum_{j\geq 0}b_{ij}\pi^j$$

where the x_j,a_{ij} and b_{ij} are in $\sum$ and at least one a_{i0} and b_{i0} are non-zero. We obtain

$$f(\xi)=\pi^{\mu s}\sum_{i=0}^{n}a_{i0}x_0^i+0\left(\pi^{\mu s+1}\right),\quad g(\xi)=\pi^{vs}\sum_{i=0}^{n}b_{i0}x_0^i+0\left(\pi^{vs+1}\right).$$

If $\sum$ is sufficiently large, we can choose a non-zero x_0 in $\sum$ so that

$$\sum_{i=0}^{m}a_{i0}x_0^i\not\equiv 0,\quad \sum_{i=0}^{n}b_{i0}x_0^i\not\equiv 0\,(\operatorname{mod}\pi)$$

and then $\xi,f(\xi)$ and $g(\xi)$ have the prescribed orders. To find ξ, we avoid 0 and at most $m+n$ roots of the polynomial congruences. This is certainly possible if $p^t>m+n+1$, so we can take

$$t=1+[\log(m+n+1)/\log p].$$

□

Theorem 2.2. *Let f be a polynomial in $Q_p[X,Y]$ of degree at most d in X and Y. Let $n=(\lambda,\mu,\nu)$ be an integer vector with $\nu>0$. Suppose either $\underset{\sim}{n}$ is normal to a face F of the Newton polyhedron of f, or that $\underset{\sim}{n}$ is a normal to an edge E of the Newton polyhedron and lies between the upward pointing normals to the faces adjacent to E. Let ℓ denote the minimum of the lengths of the projections of F or E respectively on the x and y axes, but ignoring either projection if it has length zero. Then f has a zero (ξ,η) in $\bar{Q}_p$ with*

$$\operatorname{ord}_p\xi=\lambda/\nu,\ \operatorname{ord}_p\eta=\mu/\nu\quad\textit{and}\quad[Qp(\xi,\eta):Q_p]\le\nu\ell\left(1+\left[\log\left(2d+1\right)/\log p\right]\right).$$

Proof. Consider first the case in which $\underset{\sim}{n}$ is normal to an edge E of the Newton polyhedron. Write

$$f(X,Y)=\sum a_{ij}X^iY^j$$

and let P_{mn} and P_{rs} be the endpoints of E corresponding to the respective terms $a_{mn}X^mY^n$ and $a_{rs}X^rY^s$ as in the definition at the beginning of this section. Thus

$$\underset{\sim}{e}=(m-r,n-s,\operatorname{ord}_p(a_{mn}/a_{rs}))$$

is a vector along E. Choose ξ and η in $\bar{Q}_p$ with $\operatorname{ord}_p\xi=\lambda/\nu$ and $\operatorname{ord}_p\eta=\mu/\nu$. Since $\underset{\sim}{n}$ is orthogonal to $\underset{\sim}{e}$,

$$\nu\,\underset{\sim}{e}\cdot\underset{\sim}{n}=(m-r)\operatorname{ord}_p\xi+(n-s)\operatorname{ord}_p\eta+\operatorname{ord}_p(a_{mn}/a_{rs})=0,$$

that is

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

Next, let n_1 and n_2 be the normals to the faces F_1 and F_2 of the Newton polyhedron adjacent to E, normalised to have third component 1. Since $\underset{\sim}{n}$ lies in the plane of $\underset{\sim}{n_1}$ and $\underset{\sim}{n_2}$ and between them, we can write

$$\underset{\sim}{n}=\nu\left(\gamma\,\underset{\sim}{n_1}+(1-\gamma)\,\underset{\sim}{n_2}\right)$$

with $0\le\gamma\le1$. Let P_{ij} be any vertex on the Newton polyhedron. The vector, $\underset{\sim}{v}$ say, from P_{mn} to P_{ij} lies above the planes containing the faces F_1 and F_2, so

$$\underset{\sim}{v}\cdot\underset{\sim}{n}=\upsilon\left(\gamma\,\underset{\sim}{v}\cdot\underset{\sim}{n_1}+(1-\gamma)\,\underset{\sim}{v}\cdot\underset{\sim}{n_2}\right)\ge0,$$

giving

$$\operatorname{ord}_p a_{ij}\xi^i\eta^j\ge\operatorname{ord}_p a_{mn}\xi^m\eta^n.$$

Moreover, this is a strict inequality unless P_{ij} lies on E. Thus the two terms $a_{mn}\xi^m\eta^n$ and $a_{rs}\xi^r\eta^s$ dominate all other terms in $f(\xi,\eta)$. We can suppose $m>r$ and either $n=s$ or $m-r<|n-s|$: otherwise, the same argument can be made after relabelling the points and possibly interchanging x and y. Choose η in $\bar{Q}_p$ with $\operatorname{ord}_p\eta=\mu/\nu$ and write

$$g(x)=f(x,n)=\sum_i c_i(\eta)\,x^i,\quad c_i(\eta)=\sum_j a_{ij}\eta^j.$$

By the previous remarks,

$$\operatorname{ord}_p a_{mn}\eta^n=\min_j\operatorname{ord}_p a_{mj}\eta^j,\quad\operatorname{ord}_p a_{rs}\eta^s=\min_j\operatorname{ord}_p a_{rj}\eta^j.$$

By the lemma, we can choose η with $\operatorname{ord}_p\eta=\mu/\nu$ and

$$[Q_p(\eta):Q_p]\le\nu\left(1+\left[\log\left(2d+1\right)/\log p\right]\right)$$

so that

$$\operatorname{ord}_p c_m(\eta)=\operatorname{ord}_p a_{mn}\eta^n,\quad\operatorname{ord}_p c_r(\eta)=\operatorname{ord}_p a_{rs}\eta^s.$$

Consequently

$$\operatorname{ord}_p c_m(\eta)+\lambda m=\operatorname{ord}_p c_r(\eta)+\lambda r\le\operatorname{ord}_p c_i(\eta)+\lambda i$$

for each i and the inequality is strict for $i<r$ and $i>m$. The line segment of slope -λ, joining the points

$$(r,\operatorname{ord}_p c_r(\eta))\quad\text{and}\quad(m,\operatorname{ord}_p c_m(\eta))$$

is therefore an edge of the Newton polygon of $g(x)$. From the remarks in Section 1, $g(x)$ has a root ξ in $\bar{Q}_p$ with

$$\operatorname{ord}_p\xi=\lambda\quad\text{and}\quad[Q_p(\xi,\eta):Q_p(\eta)]\le m-r.$$

This choice of ξ and η satisfies the requirements of the theorem. Now suppose $\underset{\sim}{n}$ is a normal to a face F of the Newton polyhedron. Suppose the length of the projection of F onto the x-axis is less than or equal to that on the y-axis. Let E be the line segment joining two vertices of F which determine the extreme points of the projection on the x-axis. The preceding argument goes through with the choice of E exactly as before. □

3. The indicator diagram

The Newton polyhedron lacks one of the useful features of Newton polygon: it is rather hard to draw. The indicator diagram recaptures this essential feature for polynomials in two variables. The indicator diagram is the plane graph whose vertices and edges correspond to the faces and edges of the Newton polyhedron as follows. The vertex representing a face with normal (λ, μ, ν) is $(\lambda/\nu, \mu/\nu)$, and two vertices are joined by a straight edge when they represent faces which share a common edge on the Newton polyhedron. In this terminology, the theorems of section 2 assert that if (ξ, η) is a zero of f, then $(\operatorname{ord}_p \xi, \operatorname{ord}_p \eta)$ is a point on the indicator diagram and, conversely, every rational point of the indicator diagram gives the p-adic orders of the coordinates of a zero of f. For, suppose (λ, μ) is a point of the indicator diagram lying on the edge joining the vertices corresponding to the faces F_1 and F_2 of the Newton polyhedron. The vector $(\lambda, \mu, 1)$ is a linear combination of the normals to F_1 and F_2 and is normal to the common edge E say, of F_1 and F_2, and it lies between the upward-pointing normals to F_1 and F_2. So Theorem 2 gives a zero (ξ, η) with $\operatorname{ord}_p \xi = \lambda$ and $\operatorname{ord}_p \eta = \mu$ and the edgepoints of E determine the dominant terms of $f(\xi, \eta)$. If (λ, μ) lies on a second edge of the indicator diagram, we get further dominant terms of $f(\xi, \eta)$ and this means that $(\lambda, \mu, 1)$ is normal to a face of the Newton polyhedron and (λ, μ) is a vertex of the indicator diagram. Thus the edges of the indicator diagram do not cross each other. Let

$$f(X, Y) = \sum a_{ij} X^i Y^j$$

be a polynomial with coefficients in Ω_p. We single out for special attention the edges of the Newton polyhedron through the vertex $P_{00} = (0, 0, \operatorname{ord}_p a_{00})$. We call these edges and the corresponding edges of the indicator diagram the initial edges. Consider an initial edge, E say, of the Newton polyhedron from P_{00} to $P_{rs} = (r, s, \operatorname{ord}_p a_{rs})$. If (λ, μ) is a point of the corresponding initial edge E' of the indicator diagram, then $(\lambda, \mu, 1)$ is normal to E, so E' is a segment on the line

$$rx + sy = \operatorname{ord}_p (a_{00}/a_{rs}).$$

We shall use these ideas to estimate the smallest zero of f. To measure the size of a zero, we write

$$\operatorname{ord}_p (\xi, \eta) = \min \{\operatorname{ord}_p \xi, \operatorname{ord}_p \eta\}.$$

(This is just the additive form of the natural norm on Ω_p^2).

Theorem 3.1. *Let*

$$f(X, Y) = \sum a_{ij} X^i Y^j$$

be a polynomial in $Q_p[X, Y]$ of degree at most d in X and Y. Let

$$\delta = \max_{i,j} \frac{\operatorname{ord}_p (a_{00}/a_{ij})}{i + j} = \frac{\operatorname{ord}_p (a_{00}/a_{rs})}{r + s}$$

say, where the maximum is taken over all pairs $(i, j) \neq (0, 0)$ with $a_{ij} \neq 0$ and $r + s$ is chosen as large as possible if the maximum occurs more than once. Then f has a zero (ξ_0, η_0) in $\bar{Q}_p$ with

$$\operatorname{ord}_p (\xi_0, \eta_0) = \delta \quad \textit{and} \quad [Q_p (\xi_0, \eta_0) : Q_p] \leq (r + s)^2 (1 + [\log (2d + 1) / \log p]).$$

Moreover, every zero (ξ, η) of f satisfies $\operatorname{ord}_p (\xi, \eta) \leq \delta$.

Proof. Note first that the maximum defining δ occurs for a coefficient which determines an initial edge of the Newton polyhedron. Indeed, if the vertex

$$P_{mn} = (m, n, \operatorname{ord}_p a_{mn})$$

in the usual notation is not an initial edge, then there must be a vertex P_{ij} on an initial edge and lying on or below the plane

$$\frac{\operatorname{ord}_p (a_{00}/a_{mn})}{m + n} (x + y) + z = \operatorname{ord}_p a_{00}$$

which goes through P_{00} and P_{mn}, and this gives

$$\frac{\operatorname{ord}_p a_{00}/ai_j}{i+j} \geq \frac{\operatorname{ord}_p a_{00}/a_{mn}}{m+n}.$$

Label the initial edges of the Newton polyhedron in anticlockwise order about the vertical axis. Suppose the i-th one runs from P_{00} to $P_{r_i s_i}$. Let E_i denote the corresponding initial edge of the indicator diagram with equation

$$r_i x + s_i y = \operatorname{ord}_p a_{00}/a_{r_i s_i}.$$

The slope r_i/s_i are negative and increase with i, so the initial edges $E_1, E_2, ...$ form a convex polygonal arc in the plane running from the point at infinity corresponding to the first slope to that corresponding to the last. Moreover, the convexity of the Newton polyhedron means that the rest of the indicator diagram lies below the arc formed by the initial edges. Set

$$\delta_i = \frac{\operatorname{ord}_p a_{00}/a_{r_i s_i}}{r_i + s_i}.$$

The line $y = x$ intersects some initial edge, E_ℓ say, at the point δ_ℓ. Since the initial edges form a convex arc, the other initial edges intersect $y = x$ below this point, so we have $\delta_\ell = \max_i \delta_i = \delta$. Now by Theorem 2.2, there is a zero (ξ_0, η_0) of f with $\operatorname{ord}_p \xi_0 = \operatorname{ord}_p \eta_0$. If (δ, δ) is not a vertex of the indicator diagram, we apply Theorem 2.1, the edge E being the one joining P_{00} to P_{rs}. If (δ, δ) is a vertex, apply the theorem with F being the corresponding face of the Newton polyhedron and observe that the projection of F on the (x, y) plane is contained in the triangle bounded by

$$x = 0, y = 0 \quad \text{and} \quad x + y = r + s$$

and yields the required bound on $[Q_p(\xi_0, \eta_0) : Q_p]$. Finally, any point (λ, μ) on the indicator diagram satisfies $\min\{\lambda, \mu\} \leq \delta$ because it lies below the plane formed by the initial edges, so the last assertion follows theorem. □

A translation of coordinates gives the apparently more general statement discussed in section 1.

Corollary 3.1. *Let f be a polynomial in $Q_p[X, Y]$ and let α and β be in Q_p. Set*

$$\delta = \max_{(i,j)\neq(0,0)} \frac{1}{i+j}\left(\operatorname{ord}_p f(\alpha,\beta) - \operatorname{ord}_p \frac{1}{i!j!}\frac{\partial f^{i+j}}{\partial X^i \partial Y^j}(\alpha,\beta)\right).$$

Then f has a zero (ξ_0, η_0) in $\bar{Q}_p$ with

$$\operatorname{ord}_p(\xi_0 - \alpha, \eta_0 - \beta) = \delta$$

and every zero (ξ, η) of f satisfies

$$\operatorname{ord}_p(\xi - \alpha, \eta - \beta) \leq \delta.$$

Suppose, in particular, that α, β and the coefficients of the polynomial f are p-adic integers and that f is non-singular at (α, β). Let

$$\gamma = \operatorname{ord}_p(f_X(\alpha,\beta), f_Y(\alpha,\beta)).$$

Hensel's lemma applied as in [15], gives the following result: If $\operatorname{ord}_p f(\alpha, \beta) > 2\gamma$, then f has a zero (ξ, η) in Q_p with

$$\operatorname{ord}_p(\xi - \alpha, \eta - \beta) \geq \operatorname{ord}_p f(\alpha,\beta) - \gamma.$$

Corollary 3.2 gives a sharper result of this kind.

Corollary 3.2. *Let f be a polynomial in $Q_p[X, Y]$ with degree at most d in X and Y and let α and β be in Q_p. Set*

$$\gamma = \operatorname{ord}_p(f_X(\alpha,\beta), f_Y(\alpha,\beta))$$

and suppose that

$$\operatorname{ord}_p f(\alpha,\beta) > \gamma + \max_{i+j>1} \frac{1}{i+j-1}\left\{\gamma - \operatorname{ord}_p \frac{\partial f^{i+j}}{\partial X^i \partial Y^i}(\alpha,\beta)\right\}$$

Then f has a zero (ξ, η) in $\bar{Q}p$ with

$$\operatorname{ord}_p(\xi - \alpha, \eta - \beta) \geq \operatorname{ord}_p f(\alpha,\beta) - \gamma,$$

and

$$[Q_p(\xi,\eta) : Qp] \leq 1 + \left[\log(2d+1)/\log_p\right].$$

Proof. Write

$$f(X+\alpha, Y+\beta) = \sum a_{ij} X^i Y^i$$

and suppose that $\operatorname{ord}_p a_{10} \leq \operatorname{ord}_p a_{01}$. The hypotheses give

$$\operatorname{ord}_p a_{00}/a_{10} > \frac{\operatorname{ord}_p a_{00}/a_{ij}}{i+j}$$

whenever $i+j>1$, so we can take

$$\delta = \operatorname{ord}_p a_{00} - \gamma \quad \text{and} \quad r=1, s=0$$

in Theorem 3.1. □

At least for $p > 2d+1$, the last corollary guarantees a zero in Q_p. We cannot expect any such result when f is singular at (α, β). For example, the polynomial $f(X) = X^2 + p^a$ has no zeros in Q_p when a is odd but $\operatorname{ord}_p f(0)$ can be made arbitrarily large.

4. Common zeros

Let f and g be two polynomials in $Q_p[X, Y]$. We wish to use the information contained in their Newton polyhedra to study the common zeros of f and g. The first remark is immediate, after the construction of Section 3. If (ξ, η) is a common zero, then the point $(\operatorname{ord}_p \xi, \operatorname{ord}_p \eta)$ lies on the indicator diagrams of both f and g. It will probably be difficult to find a completely satisfactory result in the opposite direction. Nevertheless, calculations with polynomials of low degree lead us to the following suggestion.

Conjecture 4.1. *Let f and g be polynomials in $Q_p[X, Y]$ and let (λ, μ) be a point on the indicator diagrams of both f and g. Assume that there are no edges of the indicator diagrams through (λ, μ) which coincide. Then f and g have a common zero (ξ, η) in Ω_p with*

$$\operatorname{ord}_p \xi = \lambda \quad \textit{and} \quad \operatorname{ord}_p \eta = \mu.$$

We will prove a special case of this conjecture, with an extra hypothesis to ensure that the geometry of the indicator diagrams is simple.

Theorem 4.1. *Let f and g be polynomials in $Q_p[X, Y]$ with degrees at most d_f and d_g respectively, and suppose that $p > 2d_f d_g$. Let (λ, μ) be a point on the indicator diagrams of both f and g, but not a vertex on either diagram, and suppose that the edges through (λ, μ) do not coincide. Then f and g have a common zero (ξ, η) in Ω_p with*

$$\operatorname{ord}_p \xi = \lambda \quad \textit{and} \quad \operatorname{ord}_p \eta = \mu.$$

Proof. Since (λ, μ) is not a vertex on the indicator diagram of f, there are exactly two terms of f which dominate the other terms at any point (x, y) in Ω_p^2 with $\operatorname{ord}_p x = \lambda$ and $\operatorname{ord}_p y = \mu$. We write $f = s_1 + s_2 + f_1$, where s_1 and s_2 are the two dominant terms of f, that is $\operatorname{ord}_p s_1 = \operatorname{ord}_p s_2$ and this order is less than that of the remaining terms in f_1 whenever $\operatorname{ord}_p x = \lambda$ and $\operatorname{ord}_p y = \mu$. Similarly, we write $g = t_1 + t_2 + g_1$, where t_1 and t_2 are dominant terms of g. After replacing x by $p^\lambda x$ and y by $p^\mu y$, we can suppose $\lambda = \mu = 0$. Also, after multiplying f and g by suitable constants, we can suppose $\operatorname{ord}_p s_i = \operatorname{ord}_p t_i = 0$ for $i = 1$ and 2, whenever $\operatorname{ord}_p x = \operatorname{ord}_p y = 0$. Now all the coefficients of f_1 and g_1 have positive orders. We write

$$s_1 s_2^{-1} = -a^{-1} x^\alpha y^\beta \quad \textit{and} \quad t_1 t_2^{-1} = -b^{-1} x^\gamma y^\delta,$$

so that the equations $f = g = 0$ become

$$x^\alpha y^\beta = a(1 + f_1/s_2), x^\gamma y^\delta = b(1 + g_1/t_2).$$

The edges of the indicator diagrams of f and g passing through the point $(0, 0)$ have the respective slopes $-\alpha/\beta$ and $-\gamma/\delta$. By hypothesis, these slopes are distinct, so that $d = \alpha\delta - \beta\gamma$ is non-zero. We can therefore "solve" the equations by

$$x = h_1(x, y) = a^{\delta/d} b^{-\beta/d} (1 + f_1/s_2)^{\delta/d} (1 + g_1/t_2)^{-\beta/d}$$

$$y = h_2(x, y) = a^{-\gamma/d} b^{\alpha/d} (1 + f_1/s_2)^{-\gamma/d} (1 + g_1/t_2)^{\alpha/d}.$$

If $\operatorname{ord}_p x = \operatorname{ord}_p y = 0$, the d-th roots of the functions on the right can be defined by their binomial expansions.These converge p-adically because $p > d$ and $\operatorname{ord}_p f_1/s_2$ and $\operatorname{ord}_p g_1/t_2$ are positive. Let

$$S = \left\{(X, Y) \text{ in } \Omega_p^2 : \operatorname{ord}_p x = \operatorname{ord}_p y = 0\right\}$$

and define $h : S \to S$ by the rule

$$h(x, y) = (h_1(x, y), h_2(x, y)).$$

We assert that h is a contraction mapping on S. In fact, by the earlier remarks, $h_1(x, y)$ has an absolutely convergent expansion on S, say

$$h_1(x, y) = c_0 + \sum_{(i,j)\neq(0,0)} c_{ij} x^i y^j,$$

where the coefficients c_{ij} satisfy $|c_{ij}|_p \leq M < 1$ for all i and j, and

$$|c_{ij}|_p \to 0 \; as \; |i| + |j| \to \infty.$$

For (x_1, y_1) and (x_2, y_2) in S,

$$\left|x_1^i y_1^j - x_2^i y_2^j\right|_p = \left|\left(x_1^i - x_2^i\right) y_1^j + x_2^i \left(y_1^j - y_2^j\right)\right|_p \leq \max\left\{|x_1 - x_2|_p, |y_1 - y_2|_p\right\}$$

and consequently

$$|h_1(x_1, y_1) - h_1(x_2, y_2)|_p \leq M \max\left\{|x_1 - x_2|_p, |y_1 - y_2|_p\right\}.$$

The same inequality holds for h_2. The norm $\|(x, y)\| = \max\left\{|x|_p, |y|_p\right\}$ makes it into a complete metric space and S is closed subset, so has unique fixed point (ξ, η) in S. By the previous construction, (ξ, η) is common zero of f and g and its component have the required p-adic order. As in [15], Hensel's lemma can be used to construct common zeros of f and g in case the curves $f = 0$ and $g = 0$ intersect transversely. We can recover this result and even a little more from Theorem 4. □

The above discussion and results are adapted from our paper in [5].

5. An explicit estimate of exponential sums associated with a cubic polynomial

Let $x = (x_1, ..., x_n)$ denote a vector in the space Z^n where Z denotes as usual the ring of integers. Let q be a positive integer and f a polynomial in $Z[x]$. The exponential sum associated with this polynomial is defined as

$$S(f; q) = \sum e^{\frac{2\pi i f(x)}{q}}$$

where the sum is over a complete set of residues x modulo q. As a result of his proof of the Weil conjectures, Deligne [10] showed that if p is a prime, then

$$|S(f; p)| \underline{\leq} (m-1)^n p^{n/2}$$

where m denotes the total degree of the associated polynomial f, under the condition that the homogeneous part of f having the highest degree is non-singular modulo p. Deligne's work opens the way to estimates of the sum associated with any positive integer q. Loxton and Vaughan [6] for example found very precise estimate for the sum in terms of invariants associated with a one-variable polynomial f. However, the genera results for polynomials of several variables are less complete. It can be shown that $S(f; q)$ has a multiplicative property with respect to q (see for example Loxton and Smith [15]). That is if q_1,q_2 have no common factors then there exist integers m_1 and m_2 such that

$$S(f; q_1 q_2) = S(m_2 f, q_1) S(m_1 f, q_2).$$

Consequently it suffices to examine exponential sums of the form $S(f; p^\alpha)$. In this paper we give an estimate for such an exponential sums with f a cubic polynomial with coefficients in the ring Z. The ensuing discussion is adapted from our paper in [1].

5.1. Some preliminary results. In the following discussion we will denote $e^{2\pi it/p^\alpha}$ by $e_{p^\alpha}(t)$ for any integer t. Let $f(x,y)$ be a polynomial with integer coefficients. Atan [2] adapted the results of Loxton and Smith [15], to show that the estimate for $S(f;p^\alpha)$ is dependent on $N(f;p^\alpha)$, the number of common solutions to the congruences

$$f_x(x,y) \equiv 0, f_y(x,y) \equiv 0 \bmod p^\alpha.$$

Here f_x and f_y denote the usual partial derivatives of f with respect to the variables x and y respectively. We rewrite Atan's assertion as follows.

Theorem 5.1. *Let p be a prime and $f(x,y)$ be a polynomial in $Z(x,y)$. For $\alpha > 1$, let*

$$S(f;p^\alpha) = \sum_{x,y \bmod p^\alpha} e_{p^\alpha}(f(x,y)) \quad \textit{and} \quad \Theta = [\alpha/2].$$

Then

$$|S(f;p^\alpha)| \leqq p^{2(\alpha-\Theta)} N\left(f;p^\Theta\right).$$

Proof. Define $\gamma = \alpha - \Theta$ so that $2\gamma \geqq \alpha$ and $\gamma \geqq \Theta \geqq 1$. Let z denote the pair (z,z') in Z^2 and $x = u + p^\gamma v$, so that x runs through the residue classes modulo p^α as u runs through the residue classes modulo p^γ and v runs through the residue classes modulo p^Θ. By using the Taylor expansion of $f(x) = f(u + p^\gamma v)$ we can rewrite $S(f;p^\alpha)$ as follows:

$$S(f;p^\alpha) = \sum_{u \bmod p^\gamma} e_{p^\alpha}(f(u)) \sum_{v \bmod p^\Theta} e_{p^\alpha}(p^\gamma \operatorname{grad} f(u) \cdot v)$$

The inner sum clearly vanishes unless both $f_x(u)$ and $f_y(u)$ are congruent to 0 modulo p^α. Under this condition each term in the inner sum is equal to 1. It follows then that the inner sum is equal to $p^{2\Theta}$, and hence

$$S(f;p^\alpha) = p^{2\Theta} \sum e_{p^\alpha}(f(u)),$$

where the sum is taken over all x modulo p^α such that

$$\operatorname{grad}\ f(u) \equiv 0 \bmod p^\Theta.$$

Since there are $p^{2(\gamma-\Theta)}$ points u modulo p^γ corresponding to each solution of the above congruences modulo p^Θ, we have

$$|S(f;p^\alpha)| \leqq p^{2\Theta+2(\gamma-\Theta)} N\left(f;p^\Theta\right)$$

as required. □

If α is odd a slightly sharper estimate than the one in Theorem 5.1 can be obtained. Towards this end we define the set

$$K_f(u) = \{v = (v,v') \bmod p : vJ_f(u) \equiv 0 \bmod p\}$$

where $u = (u,u')$ and J_f is the Jacobian matrix

$$J_f(u) = \begin{bmatrix} f_{xx}(u) & f_{xy}(u) \\ f_{xy}(u) & f_{yy}(u) \end{bmatrix}.$$

Our result for this category of α is as follows.

Theorem 5.2. *Let p be a prime and $f(x,y)$ be a polynomial in $Z(x,y)$. Let*

$$\alpha = 2\Theta + 1 \quad \textit{with} \quad \Theta \geqq 1.$$

Then

$$|S(f;p^\alpha)| \leqq p^\alpha \sum |K_f(u)|^{1/2}$$

where the sum is taken over all $u = (u,u')$ modulo p^Θ such that $\operatorname{grad} f(u) \equiv 0 \bmod p^\Theta$ *and, in addition, when p is odd* $\operatorname{grad} f(u) \cdot v \equiv 0 \bmod p^{\Theta+1}$ *for all v in $K_f(u)$.*

Proof. From the proof of Theorem 5.1, $S(f;p^\alpha) = p^{2\Theta} \sum e_{p^\alpha}(f(x))$, where the sum is taken over all $x = (x,x')$ modulo p^γ at which $f_x(x)$ and $f_y(x)$ vanish modulo p^Θ and $\gamma = \Theta + 1$.

Let

$$x = u + p^\Theta v$$

so that x, u and v run through the residue classes modulo p^{γ}, p^{Θ} and p respectively. By a Taylor expansion

$$f(x) = f(u) + p^{\Theta} \text{ grad } f(u) \cdot v + \frac{1}{2} p^{2\Theta} v J_f(u) v^t \left(\text{mod} p^{\alpha}\right)$$

we obtain

$$S(f; p^{\alpha}) = p^{2\Theta} \sum e_{p^{\alpha}}(f(u)) G_f(u),$$

where the sum is taken over all u modulo p^{Θ} such that grad $f(u) \equiv 0 \bmod p^{\Theta}$ and $G_f(u)$ denotes the Gaussian sum

$$G_f(u) = \sum_{v \bmod p} e_p\left(\frac{1}{2} v J_f(u) v^t + p^{-\Theta} \text{grad } f(u) \cdot v\right).$$

Now consider

$$|G_f(u)|^2 = \sum_{v,w} e_p\left(\frac{1}{2} v J_f(u) v^t - w J_f(u) w^t + p^{-\Theta} \text{grad } f \cdot (v - w)\right).$$

Write $v = w + z$ and carry out the summation over w. This gives

$$|G_f(u)|^2 = p^2 \sum_{z J_f(u) = 0 \bmod p} e_p\left(\frac{1}{2} z J_f(u) z^t + p^{-\Theta} \text{grad } f(u) \cdot z\right).$$

If we replace here z by $z + v$ where v is any point in $K_f(u)$, we get

$$|G_f(u)|^2 = e_p\left(\frac{1}{2} v J_f(u) v^t + p^{-\Theta} \text{grad } f(u) \cdot v\right) |G_f(u)|^2.$$

Hence, $G_f(u)$ is 0 unless

$$\frac{1}{2} v J_f(u) v^t + p^{-\Theta} \text{grad } f(u) \cdot v \equiv 0 \left(\text{mod} p\right)$$

for all v in $K_f(u)$. If p is odd, this condition is equivalent to

$$p^{-\Theta} \text{grad } f(u) \cdot v \equiv 0 \left(\text{mod} p\right)$$

for all v in $K_f(u)$ and we have

$$|G_f(u)|^2 = p^2 |K_f(u)|.$$

From this, we get the estimate in the theorem. If $p = 2$, the condition for $G_f(u)$ to be non-zero does not simplify, but we still have the

$$|G_f(u)|^2 \leqq p^2 |K_f(u)|$$

and the required estimate follows. From the above it is seen that the estimate for $S(f; p^{\alpha})$ is dependent on the estimates of $N\left(f; p^{\Theta}\right)$ and $K_f(u)$. In the following section we will examine these two quantities. In the ensuing discussion p will always denote a prime and for a rational number x, $\text{ord}_p x$ will indicate the highest power of p dividing x. We will set $\text{ord}_p x = \infty$ if $x = 0$. □

5.2. Estimation of $N(f; p^{\alpha})$. Let p be a prime and $f = (f_1, ..., f_n)$ be an n-tuple of polynomials in $x = (x_1, ..., x_n)$ with coefficients in Z. Let $N(f; p^{\alpha})$ denote the cardinality of the set

$$V(f; p^{\alpha}) = \{u \bmod p^{\alpha} : f(u) \equiv 0 \bmod p^{\alpha}\}$$

where $\alpha > 0$ and each component of u runs through a complete set of residues modulo p^{α}. The estimation of $N(f; p^{\alpha})$ has been the topic of research of many authors. For example Loxton and Smith [15] showed that for $\alpha > 0$ and a one-variable polynomial $f(x)$ in $Z[x]$,

$$N(f; p^{\alpha}) \leqq m p^{\alpha - (\alpha - \delta)/e}$$

if $\alpha > \delta$, where m is the number of distinct zeros ξ_i of f that generate its associated algebraic number field K, and δ is the highest power of p such that $D(f) \equiv 0 \left(\text{mod} p^{\delta}\right)$ where $D(f)$ represents the intersections of the fractional ideals of K generated by the numbers

$$\frac{f^{(e_i)}(\xi_i)}{e_i!}, i \geqq 1$$

and $e = \max_j e_j$ with e_j denoting the multiplicity of ξ_j. A similar result was obtained by Chalk and Smith [9] by employing Hensel's Lemma. In their work Loxton and Smith [15] showed that for

$$f = (f_1, ..., f_n),$$

$$N(f; p^\alpha) \leqq \begin{cases} p^{n\alpha} & \text{if } \alpha \leqq n\delta \\ (\text{ Deg } f)\, p^{n\delta} & \text{if } \alpha > n\delta \end{cases}$$

where δ is the highest power of p dividing the discriminant of f. Atan [3] considered linear polynomials $f = (f_1, ..., f_n)$ in $(x_1, ..., x_n)$ with coefficients in the p-adic ring Z_p. He showed that

$$N(f; p^\alpha) \leqq \min\left\{p^{n\alpha}, p^{(n-r)\alpha + r\delta}\right\}$$

where δ is the minimum of the p-adic orders of $r \times r$ non-singular submatrices of the reduced coefficient matrix of f. Let $f = (f_1, ..., f_n)$ be an n-tuple of polynomials in $Z_p[x]$ where $x = (x_1, ..., x_n), \xi_i$ common zeros of f and

$$H_i(\alpha) = \left\{x \in \Omega_p^n : \text{ord}_p(x - \xi_i) = \max_j \text{ord}_p(x - \xi_j) \text{ and } \text{ord}_p f(x) \geqq \alpha\right\}$$

where Ω_p is a complete and algebraically closed p-adic field. Following the method of Loxton and Smith [15] we show below that the cardinality $N(f; p^\alpha)$ of the set

$$V(f; p^\alpha) = \{x \bmod p^\alpha : f(x) \equiv 0 \bmod p^\alpha\}$$

is dependent on the p-adic distance between common zeros ξ_i of f and elements x in $H_i(\alpha)$.

Lemma 5.1. *Let p be a prime, and f an n-tuple of polynomials in $x = (x_1, ..., x_n)$ with coefficients in Z_p. Let ξ_i be a common zero of f. Then*

$$N(f; p^\alpha) \leqq \sum_i p^{n(\alpha - \gamma_i(\alpha))}$$

where

$$\gamma_i(\alpha) = \inf_{x \in H_i(\alpha)} ord(x - \xi_i).$$

Proof. Consider the set $V_i(f; p^\alpha)$ of points in $V(f; p^\alpha)$ that are close p-adically to a common zero ξ_i of f. That is

$$V_i(f; p^\alpha) = \left\{x \in V(f; p^\alpha) : \text{ord}_p(x - \xi_i) = \max_j \text{ord}_p(x - \xi_j)\right\}.$$

Then

$$N(f; p^\alpha) \leqq \sum_i \text{card } V_i(f; p^\alpha). \tag{1}$$

Consider the set

$$H_i(\alpha) = \left\{x \in \Omega_p^n : \text{ord}_p(x - \xi_i) = \max_j \text{ord}_p(x - \xi_j) \text{ and } \text{ord}_p f(x) \geqq \alpha\right\}.$$

Let

$$\gamma_i(\alpha) = \inf_{x \in H_i(\alpha)} \text{ord}_p(x - \xi_i) \tag{2}$$

for all i. Now, every $\alpha \geqq 1, V_i(f; p^\alpha) \subseteq H_i(\alpha)$ for all i. Hence,

$$\text{card } V_i(f; p^\alpha) \leqq \text{card } \left\{x \bmod p^\alpha : \text{ord}_p(x - \xi_i) \geqq \gamma_i(\alpha)\right\}.$$

That is,

$$\text{card } V_i(f; p^\alpha) \leqq p^{n\alpha - n\gamma_i(\alpha)} \tag{3}$$

with $\alpha \geqq \gamma_i$ for all i. Our assertion then follows from (1), (2), and (3). □

The determination of the size of $\gamma_i(\alpha)$ in the estimate above has been the subject of scrutiny of several researchers (see for example Loxton and Smith [13]). Using the method described in Section 4 as our tool we arrive at the estimate $\gamma_i(\alpha)$ associated with the two-variable polynomial

$$f(x, y) = \alpha x^3 + bx^2 y + cxy^2 + dy^3 + ex + my + n(0)$$

with coefficients in the ring of p-adic integers Z_p, with the property that

$$c^2 - 3bd, bc - 9ad \quad \text{and} \quad b^2 - 3ac$$

are non-zero, in the following lemma.

Lemma 5.2. *Let p be a prime and (0) a polynomial in $Z_p[x,y]$ with non-vanishing coefficients in the homogeneous part of degree 3. Let*

$$\delta = \max\left\{\operatorname{ord}_p 3a, \operatorname{ord}_p b, \operatorname{ord}_p c, ord\ _p 3d\right\}.$$

Suppose (x_0, y_0) is in Ω_p^2 with

$$\operatorname{ord}_p f_x(x_0,y_0), \quad \operatorname{ord}_p f_y(x_0,y_0) \geqq \alpha.$$

If $\alpha > \delta$, then there is a zero (ξ,η) of f_x and f_y in Ω_p^2 such that

$$\operatorname{ord}_p(\xi - x_0), \quad \operatorname{ord}_p(\eta - y_0) \geq \frac{1}{2}(\alpha - \delta)$$

Proof. Let $X = x - x_0$, $Y = y - y_0$, and $h = f_x$, $g = f_y$. Then

$$h(X,Y) = 3aX^2 + 2bXY + cY^2 + h_x X + h_y Y + h_0,$$
$$g(X,Y) = bX^2 + 2cXY + 3dY^2 + g_x X + g_y Y + g_0$$

where l_z denotes the partial derivatives of the polynomial l with respect to z defined at

$$(x_0,y_0) \quad and \quad l_0 = l(x_0,y_0).$$

Let α,β be the roots of the quadratic polynomial

$$u(x) = \left(c^2 - 3bd\right)x^2 + (bc - 9ad)x + b^2 - 3ac.$$

If $\alpha \neq \beta$, then it can be shown that the polynomials

$$H(U,V) = (3a + b\alpha)(h + \alpha g), G(U,V) = (3a + b\beta)(h + \beta g)$$

with

$$U = (3a + b\alpha)X + (b + c\alpha)Y, V = (3a + b\beta)X + (b + c\beta)Y$$

will have a simple intersection in the indicator diagrams associated with their respective Newton polyhedrons. By Theorem 4.1 and resubstitution of variables there is a common zero (ξ,η) of h and g with

$$\operatorname{ord}_p(\xi - x_0), \quad \operatorname{ord}_p(\eta - y_0) \geqq \frac{1}{2}(\alpha - \delta_0)$$

where

$$\delta_0 = \max\left\{\operatorname{ord}_p 3a, \operatorname{ord}_p b\right\}.$$

We obtain the required estimate from our hypothesis since clearly $\delta_0 \leqq \delta$. □

The following theorem gives the estimate for $\mathrm{N}(f_x, f_y; p^\alpha)$ where f is as in the above lemma. The proof follows from the results of Lemmas 5.1 and 5.2, and the fact that by a theorem of Bezout (see for example [11]) f_x and f_y have at most 4 common zeros.

Theorem 5.3. *Let p be a prime and (0) a polynomial in $Z_n[x,y]$ with non-vanishing terms in its homogeneous part of degree 3. Let*

$$\alpha > 0 \quad and \quad \delta = \max\left\{\operatorname{ord}_p 3a,\ \operatorname{ord}_p b,\ \operatorname{ord}_p c,\ ord\ _p 3d\right\}.$$

Then

$$N(f_x, f_y; p^\alpha) \leqq \min\left\{p^{2\alpha}, 4p^{\alpha+\delta}\right\}.$$

5.3. Estimation of $S(f;p^\alpha)$. Let f be a two-variable polynomial with integer coefficients of total degree m and p a prime. From the work of Deligne on Weyl's conjecture it can be shown that

$$|S(f;p^\alpha)| \leqq (m-1)^2 p$$

under suitable conditions on f. Let p be an odd prime and $\alpha > 1$. If

$$f(x,y) = ax^3 + bx^2y + cx + dy + e$$

is a polynomial in $Z[x,y]$, and

$$\delta = \max\left\{\operatorname{ord}_p 3a, \frac{3}{2}\operatorname{ord}_p b\right\},$$

Atan [8] showed that for this cubic polynomial

$$|S(f;p^\alpha)| \leqq \min\left\{p^{2\alpha}, 4p^{\frac{3\alpha}{2}+\delta}\right\}.$$

In the following theorem we will consider a more general polynomial than the one above of the form (0) with coefficients in Z and we will show that δ is in fact dependent on the coefficients of the dominant terms of f, provided that each term in this homogeneous portion of highest degree of f is non-zero. The assertion generalizes and improves the result as stated immediately above especially in the determination of the value of δ.

Theorem 5.4. *Let p be an odd prime and $\alpha > 1$. Let (0) be a polynomial in $Z[x, y]$, with non-zero coefficients in its cubic segment. Let*

$$\delta = \max\left\{\operatorname{ord}_p 3a, \operatorname{ord}_p b, \operatorname{ord}_p c, \operatorname{ord}_p 3d\right\}.$$

Then

$$|S(f; p^\alpha)| \leqq \min\left\{p^{2\alpha}, 4p^{\frac{3\alpha}{2}+\delta}\right\}.$$

Proof. In Theorem 5.3 it is shown that

$$N(f_x, f_y; p^\alpha) \leqq \min\left\{p^{2\Theta}, 4p^{\Theta+\delta}\right\}$$

where $\Theta = [\alpha/2]$. If $\alpha = 2\Theta$, it follows from Theorem 5.1 that

$$|S(f; p^\alpha)| \leqq p^{2(\alpha-\Theta)} \min\left\{p^{2\Theta}, bp^{\Theta+\delta}\right\}$$

which lead us to the required estimate. Suppose now that $\alpha = 2\Theta + 1$ with $\Theta \geqq 1$. We will apply the result of Theorem 5.2 in this case. If

$$D = (bm - ce)^2 - (3am - be)(cm - 3de)$$

is not divisible by p, then the congruences

$$f_x = 3ax^2 + 2bxy + cy^2 + e, f_y = bx^2 + 2cxy + 3dy^2 + m$$

and

$$|J_f| = \left(12ac - 4b^2\right)x^2 + (36ad - 4bc)xy + \left(12bd - 4c^2\right)y^2 \equiv 0 \pmod{p}$$

do not have a common solution. Thus, in this case each term in the sum $\sum |K_f(u)|^{1/2}$ is 1. Consequently,

$$|S(f; p^\alpha)| \leqq p^\alpha N\left(f; p^\Theta\right)$$

and the required estimate follows. If D is divisible by p then there are two possibilities in $\sum |K_f(u)|^{1/2}$. If $|K_f(u)| \leqq 1$ then the term corresponding to u is counted with weight at most $p^{\alpha+1/2}$. If $|K_f(u)| = 2$ then the term corresponding to u must satisfy the stronger congruence grad $f(u) \equiv 0 \left(\mathrm{mod} p^{\Theta+1}\right)$ and hence must be counted with weight at most p^α. As a result we would have

$$|S(f; p^\alpha)| \leqq p^{\alpha+1/2} N\left(f; p^\Theta\right) \leqq p^{\alpha+1/2} \min\left\{p^{2\Theta}, 4p^{\Theta+\delta}\right\}$$

and the estimate as required follows. □

6. Conclusion

In this paper we obtained explicit estimate for $S(f; p^\alpha)$ for more general cubic polynomial f than one considered in an earlier work through the application of the Newton polyhedron method developed. The result generalizes and improves that in the previous work and give some indications on how the general case should be examined especially in the search for the most suitable discriminant analogous to the one-variable case.

References

[1] K. A. M. Atan, An explicit estimate of exponential sums associated with a cubic polynomial, *Acta Math. Hungar.* **69**(1-2)(1995), 83–93.

[2] K.A. M. Atan, An estimate for multiple exponential sums in two variable, *Sains Malaysia,* **18** (1989), 129–135.

[3] K. A. M. Atan, A method for determining the cardinality of the set of solutions to congruence equations, *Pertanika* **11** (1988), 125–131.

[4] K.A. M. Atan and I.B. Abdullah, On the estimate to solutions of congruence equations associated with a cubic form, *Pertanika J. Sci. & Technol.* **1** (1993), 1–10.

[5] K. A. Atan and J. H. Loxton, Newton polyhedra and solutions of congruences, in *Diophantine analysis (Kensington, 1985)*, 67–82, Cambridge Univ. Press, Cambridge.

[6] M.F. Atiyah, Angular momentum, convex polyhedra and algebraic geometry, *Proc. Edin. Math. Soc.* **26** (1983).

[7] D.N. Bernstein, The number of rots of a system of equations, Funkt, Anal, Appl, 9, part 3 (1974), 1–4.

[8] B.J. Birch and K. McCann, A criterion for the p-adic solubility of diophantine equations, *Quart. J. Math. Oxford (2)* **18** (1967), 59–63.

[9] J.H. Chalk and R.A. Smith, Sandor's Theorem on Polynomial Congruences and Hensel's Lemma, *C.R. Math. Rep. Sci. Canada* **4** (1982), 49–54.

[10] P. Deligne, La Conjecture de Weil, *Publ. Math. IHES* **43** (1974), 273–307.

[11] R. Hartshorne, *Algebraic Geometry*, Springer Verlag, New York, Berlin, 1977, pp. 53–54.

[12] N. Koblitz, *p-Adic Numbers, p-Adic Analysis and Zeta Functions*, Springer Verlag, New York, Berlin, 197.
[13] M. Krasner, Theorie des fonctions, *C.R. Acad. Sci. Paris* **222** (1946), 582.
[14] J.H. Loxton and R.A. Smith, On Hua's estimate for exponential sums, *J. London Math. Soc. (2)* **26** (1982), 15–20.
[15] J.H. Loxton and R.A. Smith, Estimates for multiple exponential sums, *J. Austral. Math. Soc.* **33**(1982), 125–134.
[16] J.H. Loxton and R.C. Vaughan, Estimates for complete exponential sums, *Canad. Bull. Math.* **28** (1985), 440–454.
[17] A.J. Thaler, On the Newton polytope, *Proc. Amer. Math. Soc.* (1964), 944–950.
[18] R.J. Walker, *Algebraic Curves*, Springer, 1978.