An Estimation of *p*-adic Sizes of Common Zeros of Partial Derivative Polynomials Associated with a Seventh Degree Form with Complete Dominant Terms

[1] Siti Hasana Sapar & [2] Kamel Ariffin Mohd Atan

[1, 2] Laboratory of Theoretical Studies
Institute for Mathematical Research
Universiti Putra Malaysia

[1, 2] Department of Mathematics
Faculty of Science
Universiti Putra Malaysia

[1]sitihas@putra.upm.edu.my

Abstract

It is known that the value of the exponential sum $S(f;p^{\alpha})$ depends on the estimate of the cardinality $|V|$, the number of elements contained in the set

$$V=\{\underline{x} \bmod p^{\alpha} \mid f_{\underline{x}} \equiv \underline{0} \bmod p^{\alpha}\}$$

where $f_{\underline{x}}$ is *the partial derivatives of f with* respect to $\underline{x}$. The cardinality of V in turn depends on the p-adic sizes of common zeros of the partial derivatives $f_{\underline{x}}$.

This paper presents a method of determining the *p*-adic sizes of the components of (ξ,η) a common root of partial derivative polynomials of $f(x,y)$ in $Z_p[x,y]$ of degree seven based on the p-adic Newton polyhedron technique associated with the polynomial. The polynomial is of the form

$$f(x,y)=ax^7+bx^6y+cx^5y^2+dx^4y^3+ex^3y^4+ mx^2y^5+nxy^6+ry^7+sx+ty+k$$

The estimate obtained is in terms of the p-adic sizes of the coefficients of the dominant terms in *f*.

Introduction

Let $V=\{\underline{x} \bmod q \mid f_{\underline{x}} \equiv \underline{0} \bmod q\}$ where $f_{\underline{x}}$ are the partial derivatives of *f* with respect to $\underline{x}$. The estimation of the cardinality of *V* has been the subject of much research in number theory one application of which is in the quest to find the best possible estimates for multiple exponential sums of the form $S(f;q)=\sum_{\underline{x} \bmod q} \exp\left(\frac{2\pi i f}{q}\right)$ where $f(\underline{x})$ is a polynomial in $Z[\underline{x}]$ and the sum taken over a complete set of residues *x* modulo a *positive integer q*.

Loxton and Vaughn [3] are among the researchers who investigate $S(f;q)$ where *f* is a non-linear polynomial in $Z[\underline{x}]$. They showed that the estimation of $S(f;q)$ depend on the number of common zeros of the partial derivative polynomials of *f* with respect to $\underline{x}$ modulo *q*.

Through the works of Loxton and Vaughn [3] it is found that the cardinality of *V* can be estimated from the *p*-adic sizes of common zeros to partial derivative polynomials associated with *f* in the neighbourhood of points in the product space Ω_p^n, *n*>0.

The estimations of exponential sums are also found by other workers such as Mohd Atan K.A [4], Chan and Mohd Atan [1], Heng and Mohd Atan [2] for lower degree two-variable polynomials. The approach is by using *p*-adic Newton polyhedron technique associated with this polynomial.

Koblitz [7] discusses the Newton polygon to determine the *p*-adic sizes of common zeros of the one-variable polynomial and power series in $\Omega_p[x]$ with Ω_p is the completion of the algebraic closure of Q_p the field of rational p-adic numbers. Mohd Atan and Loxton [5] extend the Newton polygon idea in the p-adic case to polynomials in two-variable and call it Newton polyhedron method. This method involves reduction of the partial derivatives of the polynomial f. That is f_x and f_y are reduced to one-variable polynomials by employment of suitable parameters. The Newton polyhedron associated with the polynomial so obtained are then considered and combination of their indicator diagrams examined.

There exist common zeros of the single-variable polynomials whose p-adic orders correspond to the intersection points in the combination of the indicator diagrams associated with the respective Newton polyhedron of the polynomials. The p-adic sizes of these zeros are then determined, and this leads to sizes of common zeros of the partial derivatives of f.

p-adic Orders of Zeros of A Polynomial

Mohd Atan and Loxton [5] conjectured that to every point of intersection of the combination of the indicator diagrams associated with the Newton polyhedra of a pair of polynomials in $Z_p[x,y]$ there exist common zeros of both polynomials whose p-adic orders correspond to this point.

A special case of this conjecture was proved by Mohd Atan and Loxton [5]. Sapar and Mohd Atan [6] improved this result and is written as follows:

Theorem 1
Let p be a prime. Suppose f and g are polynomials in $Z_p[x, y]$. Let (μ,λ) be the points of intersection of the indicator diagrams associated wih f and g at the vertices or simple points of intersections. Then there are ξ and η in Ω_p satisfying $f(\xi,\eta)=g(\xi,\eta)=0$ and $ord_p\xi=\mu,\quad ord_p\eta=\lambda$.

In **Theorem 2** we give the estimates of the p-adic sizes of common zeros of partial derivative of the polynomial $f(x,y)=ax^7+bx^6y+cx^5y^2+dx^4y^3+ex^3y^4+mx^2y^5+nxy^6+ry^7+sx+ty+k$ in the neighbourhood of (0,0) in $\Omega_p^{\ 2}$

First we have the assertion as in **Lemma 1**. In this lemma and the theorem that follows: $\alpha_1=\dfrac{6b+2\lambda_1c}{6(7a+\lambda_1b)}, \alpha_2=\dfrac{6b+2\lambda_2c}{6(7a+\lambda_2b)}$ with λ_1, λ_2 zeros of $k(\lambda)=(21rd-3en)\lambda^2+(35cr-em)\lambda+5cn-dm$. It is clear that $\alpha_1\neq\alpha_2$ since $\lambda_1\neq\lambda_2$.

Lemma 1
Let U,V be in $\Omega_p^{\ 2}$ with $U=x+\alpha_1y$ and $V=x+\alpha_2y$. Let $p>7$ be a prime, a, b, c, d, e, m, n and r in Z_p, $ord_pb^2>ord_pac$, $\delta=\max\{ord_pa,ord_pb,ord_pc,ord_pd,ord_pe,ord_pm,ord_pn,ord_pr\}$ and $ord_ps,ord_pt\geq\alpha>\delta$.
If $ord_pU=\frac{1}{6}ord_p\dfrac{s+\lambda_1t}{7a+\lambda_1b}$, $ord_pV=\frac{1}{6}ord_p\dfrac{s+\lambda_2t}{7a+\lambda_2b}$ and $ord_p(35cr-em)^2>ord_p(21rd-3en)(5cn-dm)$ then $ord_px\geq\frac{1}{6}(\alpha-\delta)$ and $ord_py\geq\frac{1}{6}(\alpha-\delta)$.

Proof:

Let $x = \dfrac{\alpha_2 U - \alpha_1 V}{\alpha_2 - \alpha_1}$ and $y = \dfrac{U - V}{\alpha_1 - \alpha_2}$

with $ord_p U = \dfrac{1}{6} ord_p \dfrac{s + \lambda_1 t}{7a + \lambda_1 b}$, $ord_p V = \dfrac{1}{6} ord_p \dfrac{s + \lambda_2 t}{7a + \lambda_2 b}$.

Then,

$$ord_p x = ord_p(\alpha_1 V - \alpha_2 U) - ord_p(\alpha_1 - \alpha_2) \qquad (1)$$

and

$$ord_p y = ord_p(U - V) - ord_p(\alpha_1 - \alpha_2) \qquad (2)$$

with $ord_p(\alpha_1 - \alpha_2) = ord_p \dfrac{(6b^2 - 14ac)(\lambda_1 - \lambda_2)}{6(7a + \lambda_1 b)(7a + \lambda_2 b)}$ (3)

and $\lambda_1 - \lambda_2 = \dfrac{\sqrt{(35cr - em)^2 - 4(21rd - 3en)(5cn - dm)}}{(21rd - 3en)}$.

Since $ord_p(35cr - em)^2 > ord_p(21rd - 3en)(5cn - dm)$, we have

$$ord_p(\lambda_2 - \lambda_1) = \frac{1}{2} ord_p \frac{5cn - dm}{3(7rd - en)}.$$

Therefore by (1),

$$ord_p x = ord_p(\alpha_2 U - \alpha_1 V) - ord_p \frac{(6b^2 - 14ac)(\lambda_1 - \lambda_2)}{6(7a + \lambda_1 b)(7a + \lambda_2 b)}.$$

Suppose $\min\{ord_p \alpha_2 U, ord_p \alpha_1 V\} = ord_p \alpha_2 U$. Then we have

$$ord_p x \geq ord_p U + ord_p \frac{6b + 2\lambda_2 c}{6(7a + \lambda_2 b)} - ord_p \frac{(6b^2 - 14ac)(\lambda_1 - \lambda_2)}{6(7a + \lambda_1 b)(7a + \lambda_2 b)}.$$

Then,

$$\begin{aligned} ord_p x &\geq ord_p U + ord_p(6b + 2\lambda_2 c) - ord_p(6b^2 - 14ac) - ord_p(\lambda_2 - \lambda_1) + ord_p(7a + \lambda_1 b) \\ &= \frac{1}{6} ord_p \frac{s + \lambda_1 t}{7a + \lambda_1 b} + ord_p(6b + 2\lambda_2 c) - ord_p(6b^2 - 14ac) \\ &\quad - \frac{1}{2} ord_p \frac{5cn - dm}{3(7rd - en)} + ord_p(7a + \lambda_1 b). \end{aligned}$$

Suppose $\min\{ ord_p 6b, ord_p 2\lambda_2 c \} = ord_p 6b$. Since $p>7$ and $ord_p b^2 > ord_p ac$, we obtain

$$ord_p x \geq \frac{1}{6} ord_p \frac{s + \lambda_1 t}{7a + \lambda_1 b} + ord_p b - ord_p ac - \frac{1}{2} ord_p \frac{5cn - dm}{3(7rd - en)} + ord_p(7a + \lambda_1 b).$$

Suppose $\min\{ ord_p 7a, ord_p \lambda_1 b \} = ord_p \lambda_1 b$. Since $ord_p b^2 > ord_p ac$, we have

$$ord_p x \geq \frac{1}{6} ord_p \frac{s+\lambda_1 t}{7a+\lambda_1 b} + ord_p b - ord_p b^2 - \frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)} + ord_p (7a+\lambda_1 b) .$$

Since $ord_p (35cr-em)^2 > ord_p (21rd-3en)(5cn-dm)$, we have

$$ord_p x \geq \frac{1}{6} ord_p \frac{s+\lambda_1 t}{7a+\lambda_1 b} - \frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)} + \frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)}$$

$$= \frac{1}{6} ord_p \frac{s+\lambda_1 t}{7a+\lambda_1 b} .$$

Suppose $\min\{ ord_p s, ord_p \lambda_1 t \} = ord_p s$ and $\min\{ ord_p 7a, ord_p \lambda_1 b \} = ord_p \lambda_1 b$, we obtain

$$ord_p x \geq \frac{1}{6}\left(ord_p s - ord_p \lambda_1 b \right) \geq \frac{1}{6}\left(ord_p s - ord_p a \right) .$$

Then, by hypothesis,

$$ord_p x \geq \frac{1}{6}\left(\alpha - \delta \right) .$$

Now, from (2) and (3), we have

$$ord_p y = ord_p (U-V) - ord_p \frac{(6b^2-14ac)(\lambda_1-\lambda_2)}{6(7a+\lambda_1 b)(7a+\lambda_2 b)} .$$

Suppose $\min\{ ord_p U, ord_p V \} = ord_p U$. Since $ord_p (7a+\lambda_1 b) = ord_p (7a+\lambda_2 b)$, we have

$$ord_p y \geq ord_p U - ord_p (6b^2-14ac) - ord_p (\lambda_2-\lambda_1) + 2 ord_p (7a+\lambda_1 b)$$

$$= \frac{1}{6} ord_p (s+\lambda_1 t) - ord_p ac - \frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)} + \frac{11}{6} ord_p (7a+\lambda_1 b) .$$

Suppose $\min\{ ord_p 7a, ord_p \lambda_1 b \} = ord_p \lambda_1 b$. since $ord_p b^2 > ord_p ac$, we have

$$ord_p y \geq \frac{1}{6} ord_p (s+\lambda_1 t) - ord_p b^2 - \frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)} + \frac{11}{6} ord_p b + \frac{11}{6}\left(\frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)} \right)$$

$$\geq \frac{1}{6}\left(ord_p (s+\lambda_1 t) - ord_p b \right) - \frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)} + \frac{1}{2} ord_p \frac{5cn-dm}{3(7rd-en)} .$$

That is, $ord_p y \geq \frac{1}{6}\left(ord_p (s+\lambda_1 t) - ord_p b \right)$. Then, by hypothesis, $ord_p y \geq \frac{1}{6}(\alpha-\delta)$.

We will get the same result if $\min\{ ord_p 6b, ord_p 2\lambda_2 c \} = ord_p 2\lambda_2 c$, $\min\{ ord_p 7a, ord_p \lambda_1 b \} = ord_p 7a$ and $\min\{ ord_p s, ord_p \lambda_1 t \} = ord_p \lambda_1 t$ $\min\{ ord_p U, ord_p V \} = ord_p V$. Therefore, we have $ord_p x \geq \frac{1}{6}(\alpha-\delta)$ and $ord_p y \geq \frac{1}{6}(\alpha-\delta)$ as asserted.

Theorem 2

Let $f(x,y) = ax^7 + bx^6 y + cx^5 y^2 + dx^4 y^3 + ex^3 y^4 + mx^2 y^5 + nxy^6 + ry^7 + sx + ty + k$ be a polynomial in $Z_p[x,y]$ with $p>7$. Let $\alpha > 0$, $ord_p b^2 > ord_p ac$, $\delta = \max\{ord_p a, ord_p b, ord_p c, ord_p d, ord_p e, ord_p m, ord_p n, ord_p r\}$, and $ord_p (35cr-em)^2 > ord_p (21rd-3en)(5cn-dm)$. If $ord_p f_x(0,0), ord_p f_y(0,0) \geq \alpha > \delta$ then there exists (ξ,η) such that $f_x(\xi,\eta)=0, f_y(\xi,\eta)=0$ and $ord_p \xi \geq \frac{1}{6}(\alpha-\delta)$, $ord_p \eta \geq \frac{1}{6}(\alpha-\delta)$.

Proof:

Let $g = f_x$ and $h = f_y$ and λ constant. Then,

$$(g+\lambda h)(x,y) = (7a+\lambda b)x^6 + (6b+2\lambda c)x^5 y + (5c+3\lambda d)x^4 y^2 + (4d+4\lambda e)x^3 y^3$$
$$+ (3e+5\lambda m)x^2 y^4 + (2m+6\lambda n)xy^5 + (n+7\lambda r)y^6 + s + \lambda t$$

and

$$\frac{(g+\lambda h)(x,y)}{7a+\lambda b} = x^6 + \left(\frac{6b+2\lambda c}{7a+\lambda b}\right)x^5 y + \left(\frac{5c+3\lambda d}{7a+\lambda b}\right)x^4 y^2 + \left(\frac{4d+4\lambda e}{7a+\lambda b}\right)x^3 y^3$$
$$+\left(\frac{3e+5\lambda m}{7a+\lambda b}\right)x^2 y^4 + \left(\frac{2m+6\lambda n}{7a+\lambda b}\right)xy^5 + \left(\frac{n+7\lambda r}{7a+\lambda b}\right)y^6 + \frac{s+\lambda t}{7a+\lambda b}. \qquad (4)$$

Let α_{ij} denote the coefficients of $x^i y^j$ in (4) with $i+j=6$. By completing the sextic equation (4) and by solving simultaneously equations $\alpha_{ij}(\lambda)=0$, $i \neq 0$, $j \neq 0$ and $i+j=6$, we obtain

$$\frac{(g+\lambda h)(x,y)}{7a+\lambda b} = \left(x + \frac{6b+2\lambda c}{6(7a+\lambda b)}y\right)^6 + \frac{s+\lambda t}{7a+\lambda b}, \qquad (5)$$

where,

$$\frac{n+7\lambda r}{7a+\lambda b} - \frac{1}{8}\left(\frac{2m+6\lambda n}{7a+\lambda b}\right)\left(\frac{4d+4\lambda e}{5c+3\lambda d}\right) = 0.$$

That is,

$$(21rd-3en)\lambda^2 + (35cr-em)\lambda + 5cn - dm = 0. \qquad (6)$$

By (6), we have two values of λ, say λ_1, λ_2 where

$$\lambda_1 = \frac{-(35cr-em)+\sqrt{(35cr-em)^2 - 4(21rd-3en)(5cn-dm)}}{2(21rd-3en)}$$

and $\lambda_2 = \dfrac{-(35cr-em)-\sqrt{(35cr-em)^2 - 4(21rd-3en)(5cn-dm)}}{2(21rd-3en)}$.

$\lambda_1 \neq \lambda_2$ since $ord_p(35cr-em)^2 > ord_p(21rd-3en)(5cn-dm)$.

Now, let

$$U = x + \frac{6b+2\lambda_1 c}{6(7a+\lambda_1 b)}y \qquad (7)$$

$$V = x + \frac{6b+2\lambda_2 c}{6(7a+\lambda_2 b)}y \qquad (8)$$

$$F(U,V) = (g+\lambda_1 h)(x,y) \qquad (9)$$

and $\quad G(U,V) = (g+\lambda_2 h)(x,y)$. $\qquad (10)$

By substituting U and V in (5), we obtain a polynomial in (U,V) as follows

$$F(U,V)=(7a+\lambda_1 b)U^6+s+\lambda_1 t \tag{11}$$

$$G(U,V)=(7a+\lambda_2 b)V^6+s+\lambda_2 t \tag{12}$$

The combination of the indicator diagrams associated with Newton polyhedra of (11) and (12) is as shown below:

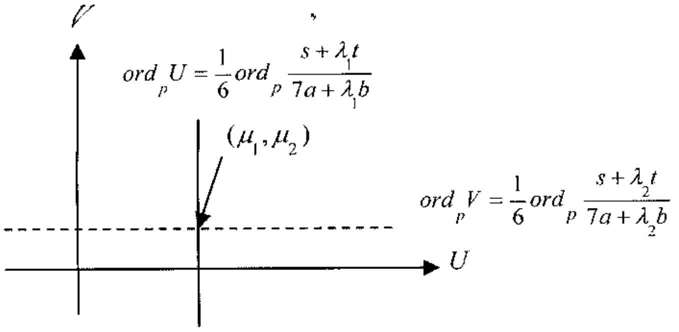
V
$ord_p U=\frac{1}{6}ord_p\frac{s+\lambda_1 t}{7a+\lambda_1 b}$
(μ_1,μ_2)
$ord_p V=\frac{1}{6}ord_p\frac{s+\lambda_2 t}{7a+\lambda_2 b}$
U

Figure 1: The indicator diagrams of $F(U,V)=(7a+\lambda_1 b)U^6+s+\lambda_1 t$ and $G(U,V)=(7a+\lambda_2 b)V^6+s+\lambda_2 t$.

From **Figure 1** and **Theorem 1** there exists $(\hat{U},\hat{V})$ in Ω_p^2 such that $F(\hat{U},\hat{V})=0$, $G(\hat{U},\hat{V})=0$ and $ord_p\hat{U}=\mu_1$, $ord_p\hat{V}=\mu_2$ with $\mu_1=\frac{1}{6}ord_p\frac{s+\lambda_1 t}{7a+\lambda_1 b}$ and $\mu_2=\frac{1}{6}ord_p\frac{s+\lambda_2 t}{7a+\lambda_2 b}$.

Let $U=\hat{U}$ and $V=\hat{V}$ in (7) and (8). There exists (x_0 , y_0) such that

$$x_0=\frac{\alpha_2\hat{U}-\alpha_1\hat{V}}{\alpha_2-\alpha_1} \text{ and } y_0=\frac{\hat{U}-\hat{V}}{\alpha_1-\alpha_2}.$$

Then, $ord_p x_0=ord_p(\alpha_1\hat{V}-\alpha_2\hat{U})-ord_p(\alpha_1-\alpha_2)$

and $ord_p y_0=ord_p(\hat{U}-\hat{V})-ord_p(\alpha_1-\alpha_2)$.

By **Lemma 1**, we have

$$ord_p x_0\geq\frac{1}{6}(\alpha-\delta) \text{ and } ord_p y_0\geq\frac{1}{6}(\alpha-\delta).$$

Let $\xi=x_0$ and $\eta=y_0$. By back substitution in (9) and (10) and since $\lambda_1\neq\lambda_2$ we have $g(\xi,\eta)=f_x(\xi,\eta)=0$ and $h(\xi,\eta)=f_y(\xi,\eta)=0$

Thus, $ord_p\xi=ord_p x_0\geq\frac{1}{6}(\alpha-\delta)$ and $ord_p\eta=ord_p y_0\geq\frac{1}{6}(\alpha-\delta)$ with (ξ,η) a common zero of g and h.

Conclusion

This work demonstrates that common zeros of certain p-adic orders of partial derivatives of a two-variable polynomial with coefficients in Z_p can be obtained through applications of the Newton polyheron technique. We have also shown that the p-adic orders of the zeros can be determined explicitly in terms of the p-adic orders of the coefficients of the dominant terms of the two-variable polynomial. This work extends future direction in finding explicit estimates of exponential sums associated with much higher degree of two-variable polynomials, which will in turn pave the way to finding better estimates of the sum associated with polynomials in several variables.

References:

[1] Chan, K.L. and Mohd Atan, K.A. 1997. On the Estimate to Solutions of Congruence Equations Associated with a Quartic Form. *Journal of Physical Science* **8**:21-34.

[2] Heng, S.H. and Mohd Atan, K.A. 1999. "An Estimation of Exponential Sums Associated With A Cubic Form". *Journal of Physical Science* **10**:1-21.

[3] Loxton, J.H. and Vaughn R.C. 1985. The Estimate of Complete Exponential Sums. *Canad. Mth Bull.* **28**(4):440-454 .

[4] Mohd. Atan, K.A. 1986. Newton Polyhedral Method of Determining p-adic Orders of Zeros Common to Two Polynomials in $Q_p[x,y]$. *Pertanika* **9**(3):375-380. Universiti Pertanian Malaysia.

[5] Mohd. Atan, K.A. and Loxton, J.H. 1986. Newton Polyhedra and Solutions of Congruences. *In Loxton, J.H. and Van der Poorten, A.(ed). Diophantine Analysis. Cambridge* : Cambridge University Press.

[6] Sapar, S.H. and Mohd Atan, K.A. 2002. Estimate for the Cardinality of the Set of Solution to Congruence Equations (Malay), *Journal of Technology* No.**36**(C):13-40.

[7] Koblitz, N. 1977. *p-adic Numbers, p-adic analysis and zeta Function.* New York:Springer-Verlag.