UNIVERSITI PUTRA MALAYSIA

SATU PENDEKATAN KOMPUTER TERHADAP PENGANGGARAN HASIL TAMBAH EKSPONEN BERGANDA

ISMAIL BIN ABDULLAH

FSAS 1993 1

SATU PENDEKATAN KOMPUTER TERHADAP PENGANGGARAN HASIL TAMBAH EKSPONEN BERGANDA

Oleh

ISMAIL BIN ABDULLAH

Disertasi Yang Dikemukakan Sebagai Memenuhi Syarat Untuk Mendapatkan Ijazah Doktor Falsafah di Fakulti Sains dan Pengajian Alam Sekitar

Universiti Pertanian Malaysia

Oktober 1993

Buat kedua-dua ibubapaku
Abdullah dan Halimah
yang sudah tiada.
Semoga ALlah s.w.t mengampunkan
segala dosa mereka. Amin!

Hadiah kasih buat

Umi Purwati Sunoto
Lathifah Ulfa
Rina Fadhilah
Irfan Satria
Mohd Mujahid
Abdul Jabbar
Nurul Khairiyyah

PENGHARGAAN

Pertama sekali jutaan terima kasih diucapkan kepada Pengerusi Jawatankuasa Penyeliaan iaitu Professor Madya Dr. Kamel Ariffin bin Mohd Atan atas segala kesabaran, bantuan, sokongan, dorongan dan bimbingan beliau beberapa tahun yang sungguh bermakna.

Ribuan terima kasih juga disampaikan kepada Professor Dr. Mohamed bin Suleiman, Professor Madya Dr. Harun bin Budin dan Professor Madya Dr. Bachok bin Taib kerana dorongan yang telah mereka curahkan.

Juga ucapan terima kasih yang senada ditujukan kepada Universiti Pertanian Malaysia dan Jabatan Perkhidmatan Awam Malaysia kerana telah meluangkan masa dan menyediakan peruntukan kewangan sehingga penulisan tesis ini menjadi suatu kenyataan.

Sumbangan yang sungguh bererti datang dari seluruh keluarga yang dengan segala kelucuan dan kesabaran mereka telah melahirkan aspirasi dan dorongan padu sehingga penulisan tesis ini dapat disempurnakan.

KANDUNGAN

SENARAI JADUAL

Jadual **Mukasurat**

SENARAI RAJAH

Rajah **Mukasurat**

SENARAI SIMBOL DAN SINGKATAN

p	Nombor Perdana
α	Eksponen Nombor Perdana
Z	Gelanggang Integer
Q	Medan Nombor Nisbah
R	Medan Nombor Nyata
C	Medan Nombor Kompleks
Z_p	Gelanggang Integer p-adic
Q_p	Medan Nombor Nisbah p-adic
$[a]$	Integer Terbesar yang Kecil atau Sama Dengan a
(a,b)	Pembahagi sepunya terbesar bagi a dan b
$\underline{x}$	n-rangkap pembolehubah $(x_1, \ldots, x_n)$
F	Gelanggang atau Medan
$F[\underline{x}]$	Gelanggang polinomial dengan pekali dalam F.
$\underline{f}$	m-rangkap polinomial $(f_1, \ldots, f_m), m > 1$.
$\mathrm{drjh}\, \underline{f}$	Darjah bagi polinomial $\underline{f}$
$J_{\underline{f}}$	Matriks Jacobian bagi $\underline{f}$
$Ord_p a$	Kuasa tertinggi bagi p yang membahagi a.
$\overline{Q}_p$	Tutupan Aljabar bagi Q_p
$S(f;q)$	Hasil Tambah Eksponen
$\nabla \underline{f}$	Kecerunan bagi $\underline{f}$
$D(\underline{f})$	Pembezalayan bagi $\underline{f}$
TTF	Teorem Terakhir Fermat
CAD	Computer Aided Design
CAM	Computer Aided Manufacturing
CAR	Computer Aided Research
CGAR	Computer Graphics Aided Research
(x_e, y_e, z_e)	Koordinat Mata (eyes)
(x_s, y_s, z_s)	Koordinat Layar (screen)
RAM	Random Acces Memory
MB	Mega Bytes
N_f	Polihedron Newton

V	Bucu pada N_f
E	Sisi pada N_f
L	Unjuran sisi pada N_f
δ	Pembeza layan.
$V(\underline{f};p^{\alpha})$	Set $\{\underline{x} \bmod p^{\alpha} : \underline{f} \equiv 0 \bmod p^{\alpha}\}$
$N(\underline{f};p^{\alpha})$	Kekardinalan bagi set $V(\underline{f};p^{\alpha})$
$G_f(u)$	Hasil Tambah Gaussian.
maks	Maksimum
mini	Minimum
mod	Modulo
eksp	Eksponen
$e_k(t)$	$e^{2\pi i t/k}$
$\vert\ \vert_p$	Penilaian terhadap p
$\prod$	Hasil darab
$\sum$	Hasil tambah
Δ	Pembeza layan Separa
$d_m(q)$	Bilangan perwakilan bagi q sebagai hasil darab m integer positif
pen A	Penentu A
inf	infimum
sup	supremum

Abstrak disertasi yang dikemukakan kepada Senat Universiti Pertanian Malaysia sebagai memenuhi syarat bagi Ijazah Doktor Falsafah

SATU PENDEKATAN KOMPUTER TERHADAP PENGANGGARAN HASIL TAMBAH EKSPONEN BERGANDA

OLEH

ISMAIL BIN ABDULLAH

OKTOBER 1993

Pengerusi : Professor Madya Dr. Kamel Ariffin bin Mohd Atan

Fakulti : Fakulti Sains dan Pengajian Alam Sekitar,

Dengan $n > 0, \underline{x} = (x_1, \cdots, x_n)$ dan $f(\underline{x})$ suatu polinomial dalam $Z[\underline{x}]$, Hasil tambah eksponen berganda ditakrifkan sebagai

$$S(f;q) = \sum_{\underline{x} \bmod q} \exp(2\pi i f(\underline{x})/q)$$

dengan hasil tambah diambil ke atas set lengkap reja modulo $q > 0$.

Penyelidikan hasil tambah eksponen bagi polinomial dua pembolehubah dengan pekali dalam medan p-adic dikaji dengan menggunakan teknik polihedron Newton. Gambar rajah penunjuk telah dikemukakan bagi menolong dalam kajian selanjutnya, tetapi kesukaran timbul dalam kes di mana kombinasi gambar rajah penunjuk bertindih pada bucu dan tembereng tertentu. Dalam kes itu teknik polihedron Newton hingga kini belum dapat memberikan maklumat tepat mengenai saiz punca sepunya p-adic yang sangat diperlukan dalam proses penganggaran hasil tambah eksponen.

Masalah pertindihan gambar rajah penunjuk pada bucu dan tembereng diteliti secara lebih mendalam. Kombinasi gambar rajah penunjuk menghasilkan persilangan dalam pelbagai bentuk. Salah satu kombinasi yang dihasilkan ialah persi-

langan tepat atau persilangan mudah. Telah dibincangkan dan dibuktikan bahawa persilangan yang demikian akan menghasilkan pensifar sepunya. Satu pengitlakan telah dibuat sebagai berikut:

Katakan f dan g dua buah polinomial dalam $Z_p[x, y]$ mempunyai pensifar sepunya dalam Ω_p. Biarkan (μ, λ) menjadi sebarang titik sepunya pada kedua-dua gambar rajah penunjuk yang disekutukan dengan f dan g. Maka terdapat ξ, η, M dan N sedemikian hingga $\mathrm{ord}_p \xi = \mu + \mathrm{ord}_p M$ dan $\mathrm{ord}_p \eta = \lambda + \mathrm{ord}_p N$ dan $f(\xi, \eta) = g(\xi, \eta) = 0$. Nilai M dan N dapat ditentukan setelah nilai bagi (μ, λ) diketahui melalui persilangan pada gambar rajah penunjuk.

Melalui beberapa contoh yang dikemukakan dan diselesaikan melalui bantuan komputer, didapati bahawa wujud penyelesaian bagi persilangan gambar rajah penunjuk yang bertindih baik di bucu atau tembereng.

Katakan f dan g dua buah polinomial dalam $Z_p[x, y]$. Jika (ξ, η) ialah pensifar sepunya bagi f dan g maka terdapat titik sepunya (μ, λ) berada pada kedua-dua gambar rajah penunjuk yang dikaitkan dengan f dan g sedemikian hingga $\mathrm{ord}_p \xi = \mu$ dan $\mathrm{ord}_p \eta = \lambda$.

Anggaran bagi *S(f;p)* boleh dibuat melalui proses induksi dan cara termudah ialah dengan mengira penyelesaian bagi sistem persamaan kongruen. Polinomial berikut yang berbentuk kubik telah dikaji

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + kx + my + n$$

dan pembeza layan δ yang bersesuaian dengannya didapati sebagai

$$\delta = \text{maks}\{\text{ord}_p 3a, \text{ord}_p b, \text{ord}_p c, \text{ord}_p 3d\}$$

Melalui pembeza layan tersebut anggaran yang lebih baik dapat dihasilkan bagi $S(f; p^{\alpha})$ untuk polinomial berkenaan. Proses penjelmaan telah digunakan bagi menjadikan polinomial di atas polinomial satu pembolehubah dan dengan menggunakan kaedah polihedron Newton kewujudan penyelesaian mereka dapat dibuktikan. Kekardinalan bagi set $V(f_x, f_y; p^{\alpha})$ untuk suatu polinomial $f(x,y)$ dapat ditentukan dan anggaran $S(f; p^{\alpha})$ diperolehi.

Abstract of dissertattion submitted to the Senate of Universiti Pertanian Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A COMPUTER APPROACH TO THE ESTIMATION OF MULTIPLE EXPONENTIAL SUMS

BY

ISMAIL BIN ABDULLAH

OCTOBER, 1993

Chairman : Assoc. Professor Dr. Kamel Ariffin bin Mohd Atan

Faculty : Faculty of Science and Environmental Studies,

With $n > 0$, $\underline{x} = (x_1, \cdots, x_n)$ and $f(\underline{x})$ is a polynomial in $Z[\underline{x}]$, the multiple exponential sum is defined to be

$$S(f;q) = \sum_{\underline{x} \bmod q} \exp(2\pi i f(\underline{x})/q)$$

where the sum is taken over a complete set of residues modulo $q > 0$.

Investigations on the sums when f is a two-variable polynomial with coefficients in the p-adic field is studied using the Newton polyhedron technique. The concept of Indicator diagrams is introduced to help further investigation, but ambiguities, however, arise in cases where the combinations overlap in certain segments of the indicator diagrams. In such cases the present Newton polyhedron technique does not give exact information on the p-adic sizes of common zeros which are vital in the estimations of the sums.

The problem of overlapping of indicator diagrams at the vertices and segments are looked into in depth. The combinations of indicator diagrams results in various

forms of intersections. One of the combinations is the simple intersection. It has been discussed and proved that such intersection gives common zeros. A generalization has been made as follows:

Let f and g be two polynomial in $Z_p[x, y]$ having common zeros in Ω_p. Let (μ, λ) be any common point on both indicator diagrams associated with f and g. Then, there exists ξ, η, M and N such that $\mathrm{ord}_p \xi = \mu + \mathrm{ord}_p M$ and $\mathrm{ord}_p \eta = \lambda + \mathrm{ord}_p N$ and $f(\xi, \eta) = g(\xi, \eta) = 0$. Values of M and N can be determined after the values of (μ, λ) are known as a result of the intersection of the indicator diagrams.

Through several examples that are considered and solved using the computers, it is found that the solution exists in cases of overlapping vertices and segments of the indicator diagrams associated with certain polynomials.

Let f and g be two polynomials in $Z_p[x, y]$. If (ξ, η) is the common zeros of f and g, then there exists common point (μ, λ) on both indicator diagrams associated with f and g such that $\mathrm{ord}_p \xi = \mu$ and $\mathrm{ord}_p \eta = \lambda$.

The estimate of *S(f;p)* can be obtained through the induction process and the easiest method to do that is by counting the solutions of systems of congruence equations. The following polynomial in a cubic form has been studied

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + kx + my + n$$

and the appropriate discriminant δ has been found as

$$\delta = \max\{\mathrm{ord}_p 3a, \mathrm{ord}_p b, \mathrm{ord}_p c, \mathrm{ord}_p 3d\}$$

With the discriminant a better estimate of $S(f;p^{\alpha})$ for the polynomial is obtained. Transformation process is applied to transform the polynomial to a polynomial of one variable and by using the Newton Polyhedron technique the existence of the solution is proved. The cardinality of the set $V(f_x, f_y; p^{\alpha})$ for polynomial *f(x,y)* can be determined and the estimate of $S(f;p^{\alpha})$ obtained.

BAB I

PENDAHULUAN

Tatatanda dan Takrifan

Z, Q, R dan *C* masing-masing menandakan gelanggang integer, medan nombor nisbah, medan nombor nyata dan medan nombor kompleks. Dengan *p* senantiasa menandakan nombor perdana, Q_p pula mewakili medan nombor *p*-adic dan Z_p gelanggang integer *p*-adic, sementara Ω_p ialah suatu perluasan medan aljabar bagi Q_p.

Huruf kecil Roman mewakili unsur-unsur dalam *Z* atau Z_p. Huruf Greek α adalah senantiasa eksponen bagi suatu nombor perdana *p*. Simbol [ ] menandakan fungsi integer terbesar. Jika $a \in R$, maka $[a]$ akan bermakna integer terbesar yang lebih kecil atau sama dengan *a*. Tatatanda *(a,b)* menandakan pembahagi sepunya terbesar bagi *a* dan *b*, kecuali pada masa-masa tertentu yang penggunaannya jelas merujuk kepada pasangan tertib.

Tatatanda $\underline{x}$ menyatakan pembolehubah-pembolehubah rangkap-*n* $(x_1, \ldots, x_n)$, $n \geq 1$ dan *F* mewakili gelanggang atau medan, $F[\underline{x}]$ bermakna gelanggang polinomial dengan pekali dalam *F*. Bagi kegunaan kita *F* akan merujuk sama ada kepada *Z* atau Q_p atau perluasan medan bagi Q_p.

Andaikan $f = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ suatu polinomial dalam $F[\underline{x}]$. Kita nyatakan darjah f dengan drjh f dan mentakrifkannya sebagai $\text{drjh} f = \underset{i_1 \ldots i_n}{\text{maks}} (i_1 + \ldots + i_n)$.

Simbol $\underline{f}$ membawa makna suatu polinomial rangkap-*n* $(f_1, \ldots, f_m), m > 1$ dalam $F[\underline{x}]$ dan $J_{\underline{f}}$ ialah matriks Jacobian $\left[\frac{\partial f_i}{\partial x_j}\right]$, $1 \leq i \leq m$, $1 \leq j \leq n$ bagi polinomial $\underline{f}$.

Andaikan $\underline{f} = (f_1, \ldots, f_m)$ ialah rangkap-*m* bagi polinomial linear dalam $F[\underline{x}]$. Jika $f_i = \sum a_{ij} x_j$, $1 \leq i \leq m$, $1 \leq j \leq n$, kita sebut matriks *m* x *n*, a_{ij} dengan julat yang sama bagi *i* dan *j*, sebagai matriks mewakili $\underline{f}$.

Simbol eksponen seperti biasa ditakrifkan sebagai $\exp(y) = e^y$ dan bagi suatu integer *k* positif, $e_k(t) = \exp(2\pi i t/k)$, bagi sebarang $t \in Z$.

Misalkan *p* sebarang nombor perdana. Bagi sebarang integer tak sifar *a*, $\text{ord}_p a$ menyatakan kuasa tertinggi bagi *p* yang membahagi *a*, iaitu *m* yang terbesar sedemikian hingga $a \equiv 0 (\text{mod}\, p^m)$.

Jika $x = a/b$ sebarang nombor nisbah, maka kita mentakrifkan $\text{ord}_p x$ sebagai $\text{ord}_p a - \text{ord}_p b$

Kita mentakrifkan suatu pemetaan yang ditandakan dengan $| \, |_p$ pada *Q* sebagai berikut:

$$|x|_p = \begin{cases} \dfrac{1}{p^{\text{ord}_p x}} & \text{jika, } x \neq 0 \\ 0 & \text{jika, } x = 0 \end{cases}$$

Boleh diperlihatkan bahawa pemetaan $| \, |_p$ seperti yang ditakrifkan di atas adalah penilaian tak-arkhimedes pada Q.

Suatu jujukan $\{a_i\}$ yang terdiri dari nombor nisbah disebut sebagai jujukan Cauchy jika untuk suatu nombor $\epsilon > 0$ terdapat suatu N sedemikian hingga $|a_i - a_{i'}|_p < \epsilon$, apabila kedua-dua $i, i' > N$. Kita sebut dua jujukan Cauchy $\{a_i\}$ dan $\{b_i\}$ setara jika $\operatorname{had}_{i \to \infty} |a_i - b_i|_p = 0$.

Kita takrifkan medan Q_p sebagai set kelas kesetaraan jujukan Cauchy dalam Q, iaitu Q_p ialah pelengkap bagi Q terhadap penilaian $| \, |_p$.

Kita tandakan dengan $\overline{Q}_p$ tutupan aljabar bagi Q_p dan dengan Ω_p pelengkap bagi $\overline{Q}_p$ terhadap penilaian $| \, |_p$. Kita perhatikan bahawa penilaian $| \, |_p$ boleh diperluas secara unik dari $\overline{Q}_p$ ke Q_p dan Ω_p, dengan Ω_p lengkap dan tertutup secara aljabar.

Dengan takrifan di atas kita nyatakan takrifan berikut bagi poligon Newton bagi polinomial dengan pekali dalam medan *p*-adic seperti yang diberikan oleh Koblitz (1977).

Takrifan 1

Jika,

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

suatu polinomial di dalam $\Omega_p[x]$, maka poligon Newton bagi f ialah hull cembung bawah bagi set titik-titik $(i, \operatorname{ord}_p a)$. Jika $a_j = 0$ bagi j tertentu, maka kita ambil $\operatorname{ord}_p a_j = \infty$. Ini bermakna poligon Newton bagi f adalah garis poligonal yang terhasil melalui pemutaran garis mencancang melalui $(0, \mathrm{ord}_p a_0)$ mengikut lawan arah putaran jarum jam sehingga garis itu membengkok di sekeliling titik-titik $(i, \mathrm{ord}_p a_i)$ dan akhirnya mencapai titik $(n, \mathrm{ord}_p a_n)$.

Latar Belakang

Hasil tambah eksponen ditakrifkan sebagai

$$S(f;q) = \sum_{\underline{x} \bmod q} e_q(f(\underline{x})) \qquad [1]$$

bagi setiap $f \in Z[\underline{x}]$ dengan q ialah suatu integer positif berdarjah lebih besar daripada 1. Hasil tambah diambil bagi set lengkap reja x modulo q. Setiap komponen bagi $x \in Z$ mempunyai nilai yang sepadan dalam set lengkap reja modulo q. Pernyataan $\underline{x}$ mod q merujuk kepada set semua $\underline{x}$ yang apabila dibahagi dengan q meninggalkan baki salah satu unsur dari set $\{0,1,2,\ldots,q\text{-}1\}$. Davenport (1959), Igusa (1978) dan Schmidt (1982) memperihalkan peranan penting hasil tambah eksponen dalam teori nombor analisis.

Perhatikan polinomial

$$f(x) = \sum_{i=0}^{m} a_i x^i$$

di dalam *Z[x]* berdarjah $m > 1$. Kajian yang sistematik mengenai [1] bagi n yang lebih besar dan dalam kes satu pembolehubah telah dibuat oleh Hardy dan Littlewood (1919) yang ada kaitan dengan masalah Waring. Mereka membuat kesimpulan, jika $(a_n, q) = 1$ maka untuk sebarang $\epsilon > 0$

$$|S(f;q)| \leq c q^{1-2^{1-m}+\epsilon} .$$

dengan c suatu pemalar yang tak bersandar pada q. Kamke (1923/24) juga memperolehi keputusan yang sama apabila beliau menyelidiki masalah taburan bahagian pecahan polinomial dan masalah Waring bagi polinomial. Mordell (1932) membuktikan bahawa

$$|S(f;q)| \leq cp^{1-\left(\frac{1}{m}\right)}$$

dengan c suatu pemalar, yang tak bersandar pada p. Dengan menggunakan keputusan ini, Hua (1940) mendapati bahawa untuk sebarang $\epsilon > 0$.

$$|S(f;q)| \leq cp^{1-\left(\frac{1}{m}\right)+\epsilon} \qquad [2]$$

dengan c suatu pemalar yang bersandar pada m dan ϵ sahaja. Keputusan Hua telah diperbaiki oleh Jing-Run Chen (1977) yang menunjukkan bahawa jika kandungan bagi f-$f(0)$ perdana relatif terhadap q, maka

$$|S(f;q)| \leq e^{7(n+1)} q^{1-\frac{1}{(n+1)}}$$

Berdasarkan kajiannya ke atas hipotesis Riemann, Weil (1948) mendapatkan anggaran

$$|S(f;q)| \leq (m-1)p^{\left(\frac{1}{2}\right)}$$

untuk $2 \leq m < p$. Menggunakan anggaran ini, Necaev (1953) membuktikan bahawa

$$|S(f;q)| \leq cq^{1-\frac{1}{m}}$$

dengan c suatu pemalar bersandar pada m sahaja. Anggaran Hua [2] telah digunakan oleh Stechkin (1980) bagi menunjukkan bahawa

$$|S(f;q)| \leq c^m q^{1-\frac{1}{m}} (c(f), q)^{\frac{1}{m}}$$

untuk pemalar mutlak positif c tertentu, dengan $c(f)$ menandakan kandungan bagi f-$f(0)$. Perhatikan h suatu polinomial dalam $R[\underline{x}]$ dengan pemfaktoran

$$h = c \prod_{i=1}^{m} (x - \alpha_i)$$

di dalam tutupan aljabar K medan pembahagi bagi R. Takrifkan pembeza layan h dengan

$$D(h) = c^{2(m-1)} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

Melalui takrifan pembeza layan ini Smith (1980) telah membuktikan bahawa jika pembeza layan $D(f')$ bagi f' terbitan bagi f dalam $Z[\underline{x}]$ bukan sifar maka

$$|S(f;q)| \leq q^{\frac{1}{2}} (D(f'), q) d_{m-1}(q)$$

untuk semua $q \geq 1$, dengan $d_j(q)$ menyatakan bilangan perwakilan bagi q sebagai hasildarab j nombor positif, dan $(D(f'), q)$ menandakan pembahagi sepunya terbesar bagi kedua-dua sebutan berkenaan.

Andaikan $f(x) = \sum a_i x^{m-1} = a_o \prod (x - \zeta_i)^{e_i}$ dengan $\zeta_i \cdots \zeta_k$ adalah nombor aljabar yang berbeza dan e_i gandaan bagi ζ_i, $1 \leq i \leq k$. Chudnovsky (1974) memperkenalkan pembeza layan separa bagi f dengan mentakrifkannya sebagai