MATEMATIKA, 1990, Jilid 6,no.1, hlm 37-48

SATU KAEDAH MENGANGGAR HASIL TAMBAH EKSPONEN BERGANDA

Kamel Ariffin bin Mohd Atan
Jabatan Matematik
Universiti Pertanian Malaysia.

Abstrak

Penganggaran hasiltambah eksponen berganda $S(f;q) = \sum_{\tilde{x}} e^{2\pi i f(x)/q}$ yang dinilaikan di atas set reja modulo q yang lengkap menjadi tajuk kajian ramai penyelidik. Di dalam makalah ini anggaran kepada hasil tambah ini untuk $q = p^{\alpha}$, p nombor perdana dan $\alpha > 0$ didapatkan melalui kaedah polihedron Newton yang telah dihasilkan terlebih dahulu. Didapati hasil tambah ini bersandar kepada anggaran kekardinalan set penyelesaian sistem persamaan kongruen tertentu modulo $p^{\left[\frac{\alpha}{2}\right]}$, dan juga kepada hasil tambah Gaussan tertentu bergantung kepada pariti α. Anggaran yang diperolehi adalah terbaik mungkin dengan kaedah polihedron Newton terutama apabila α genap.

1. Pendahuluan

Katakan Z menandakan gelanggang integer. Untuk $n \geq 1$, katakan f polinomial dalam $\underset{\sim}{x} = (x_1,\ldots,x_n)$ di dalam Z^n dengan jumlah darjah $m > 1$. Bagi setiap integer positif q dan setiap polinomial seperti f, kita takrifkan hasil tambah eksponen

$$S(f;q) = \Sigma\, e_q(f(\underset{\sim}{x}))$$

dengan hasil tambah ini diambil di atas set reja x modulo q yang lengkap dan $e_q(t) = e^{2\pi i t/q}$. Pentingnya hasil tambah seperti ini dalam bidang teori nombor analisis memang diketahui ramai (lihat contohnya Chowla dan Davenport [1]). Sebagai akibat langsung dari kajian yang dilakukan oleh Deligne [2] mengenai Konjektur Weil beliau telah dapat menunjukkan bahawa bagi sebarang nombor perdana p,

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

dengan syarat bahagian homogen f yang berdarjah tertinggi adalah tak singular modulo p. Kajiannya memberikan petunjuk kepada jalan mencari anggaran S(f;q) untuk sebarang q. Loxton dan Vaughn [4] umpamanya memberikan anggaran yang tepat bagi S(f;q) untuk polinomial satu pembolehubah dalam sebutan beberapa ciri tak berubah polinomial tersebut. Keputusan-keputusan yang lebih umum untuk polinomial beberapa pembolehubah tidaklah begitu lengkap. Kamel Ariffin [6] telah memperolehi anggaran yang lebih eksplisit untuk $S(f;p^\alpha)$ bagi polinomial tertentu f dalam dua pembolehubah berdarjah 2 dan 3, dalam sebutan peringkat p-adik pekali-pekalinya.

Seperti yang diketahui S(f;q) mempunyai sifat berdaya darab terhadap q. Yakni, jika q_1 dan q_2 integer-integer yang perdana relatif, maka ada integer-integer m_1 dan m_2 demikian hingga

$$S(f;q_1q_2) = S(m_2f;q_1)S(m_1f;q_2).$$

Dengan demikian adalah memadai kita meneliti hasiltambah-hasiltambah eksponen $S(f;p^{\alpha})$ yang bermodulo kuasa nombor perdana. Di sepanjang perbincangan kita p akan menandakan nombor perdana dan bagi x di dalam medan nombor nisbah Q, $\text{per}_p\, x$ pula akan menandakan kuasa tertinggi p yang membahagi x, dengan mengambil $\text{per}_p\, 0 = \infty$.

Dalam makalah ini suatu batas atas bagi $|S(f;p^{\alpha})|$ dengan f polinomial dalam $\underset{\sim}{x} = (x_1,..,x_n)$, $n > 2$, berpekali integer dan berdarjah $m > 1$ akan *diberikan bagi nombor* perdana p dan $\alpha > 1$. Anggaran bagi batas ini diperolehi dengan menggunakan keputusan-keputusan yang telah diperolehi oleh pengarang melalui kaedah polihedron Newton di dalam sebuah terbitan terdahulu.

2. Suatu batas atas bagi $S(f(\underset{\sim}{x}),p^{\alpha})$

Bagi $n \geq 2$, katakan $f(\underset{\sim}{x})$ polinomial di dalam $Z[\underset{\sim}{x}]$ dengan $\underset{\sim}{x} = (x_1,...,x_n)$. Kita tandakan dengan ∇f matrik $[f_{\underset{\sim}{x}}] = [f_{x_1},f_{x_2},..,f_{x_n}]$ dengan f_{x_i} menandakan terbitan separa biasa f terhadap x_i, $i = 1,2,...,n$. Biarkan $N(f;p^{\gamma})$ *menandakan kekardinalan set* $\{\underset{\sim}{u} \bmod p^{\gamma} : \nabla f(\underset{\sim}{u}) \equiv \underset{\sim}{0} \bmod p^{\gamma}\}$.

Teorem yang berikut ini memberikan suatu batas atas bagi $|S(f;p^{\theta})|$ dengan $\theta = [\frac{\alpha}{2}]$. Pembuktiannya merupakan pengitlakan kepada pembuktian Teorem 2.1 oleh Kamel Ariffin [6].

Teorem 2.1

Katakan p nombor perdana dan $f(\underset{\sim}{x})$ polinomial di dalam $Z[\underset{\sim}{x}]$ dengan $\underset{\sim}{x} = (x_1,...,x_n)$. Untuk $\alpha > 1$, biarkan

$$S(f;p^{\alpha}) = \sum_{\underset{\sim}{x} \bmod p^{\alpha}} e_{p^{\alpha}}(f(\underset{\sim}{x}))$$

dan $\theta = \left[\frac{\alpha}{2}\right]$. Maka

$$\left|S(f;p^{\alpha})\right| \leq p^{n(\alpha-\theta)} N(f;p^{\theta}).$$

Bukti. Takrifkan $\gamma = \alpha - \theta$ supaya $2\gamma \geq \alpha$ dan $\gamma \geq \theta \geq 1$. Kita ungkapkan semula $f(\underset{\sim}{x})$ seperti berikut. Biarkan

$$\underset{\sim}{x} = \underset{\sim}{u} + p^{\gamma}\underset{\sim}{v}$$

supaya $\underset{\sim}{x}$ mengambil nilai di dalam kelas-kelas reja modulo p^{α} apabila $\underset{\sim}{u}$ mengambil nilai di dalam kelas-kelas reja modulo p^{γ} dan $\underset{\sim}{v}$ pula mengambil nilai di dalam kelas-kelas reja modulo p^{θ}.

Dengan mengembangkan $f(\underset{\sim}{x})$ dengan menggunakan Teorem Taylor kita perolehi,

$$f(\underset{\sim}{x}) = f(\underset{\sim}{u}) + p^{\gamma} \nabla f(\underset{\sim}{u}).\underset{\sim}{v} \pmod{p^{\alpha}}.$$

Oleh itu,

$$S(f;p^{\alpha}) = \sum_{\underset{\sim}{u} \bmod p^{\gamma}} e_{p^{\alpha}}(f(\underset{\sim}{u})) \sum_{\underset{\sim}{v} \bmod p^{\theta}} e_{p^{\alpha}}(p^{\gamma} \nabla f(\underset{\sim}{u}).\underset{\sim}{v}).$$

Hasil tambah yang terkedalam jelas terhapus kecuali jika kesemua $f_{\underset{\sim}{x}}(\underset{\sim}{u})$ kongruen dengan 0 modulo p^{θ}. Jika syarat ini dipenuhi maka hasil tambah terkedalam ini adalah sama dengan $p^{n\theta}$ oleh sebab tiap-tiap sebutannya adalah 1. Dengan demikian

$$S(f;p^{\alpha}) = p^{n\theta} \sum e_{p^{\alpha}}(f(\underset{\sim}{u}))$$

dengan hasil tambahnya dinilaikan di atas semua $\underset{\sim}{u}$ modulo p^{γ} sedemikian hingga

$$\nabla f(\underset{\sim}{u}) \equiv 0 \bmod p^{\theta}.$$

Oleh sebab terdapat $p^{n(\gamma-\theta)}$ titik $\underset{\sim}{u}$ modulo p^{γ} untuk setiap selesaian persamaan-persamaan kongruen modulo p^{θ} di atas, maka

$$|S(f;p^{\alpha})| \leq p^{n\theta + n(\gamma-\theta)} N(f;p^{\theta})$$

seperti yang ditegaskan oleh teorem ini. □

Jika α genap maka berikutan dari teorem di atas $|S(f;p^{\alpha})| \leq p^{\frac{n\alpha}{2}} N(f;p^{\alpha/2})$. Katalah sekarang α ganjil. Teorem yang berikut ini menunjukkan bahawa anggaran $|S(f;p^{\alpha})|$ adalah bersandar kepada hasil tambah Gaussan bentuk kuadratik yang ditakrifkan oleh Jakobian bagi $f_{\underset{\sim}{x}}$ pada titik tertentu. Di dalam teorem ini $J_{\nabla f}$ menandakan matrik Jakobian bagi ∇f.

Teorem 2.2

Katakan $f(\underset{\sim}{x})$ polinomial di dalam $Z[\underset{\sim}{x}]$ dengan $\underset{\sim}{x} = (x_1,\ldots,x_n)$. Jika $\alpha = 2\beta + 1$ dengan $\beta \geq 1$ maka

$$|S(f;p^{\alpha})| \leq p^{n\beta} \sum_{\underset{\sim}{u} \bmod p^{\beta}} |G(\underset{\sim}{u})|$$

dengan

$$G(\underset{\sim}{u}) = \Sigma\, e_p(p^{-\beta}\, \nabla f(\underset{\sim}{u})\underset{\sim}{v}^t + \frac{1}{2}\underset{\sim}{v}\, J_{\nabla f}(\underset{\sim}{u})\underset{\sim}{v}^t)$$

dan hasil tambah ini dinilaikan di atas set $\underset{\sim}{u}$ dengan $\nabla f(\underset{\sim}{u}) \equiv 0 \bmod p^{\beta}$.

Bukti. Katakan $\theta = \left[\frac{\alpha}{2}\right]$, $\gamma = \alpha - \theta$ dan $\underset{\sim}{x} = (x_1,\ldots,x_n)$. Maka dengan bukti kepada Teorem 2.1 kita perolehi

$$S(f;p^{\alpha}) = p^{n\theta} \sum_{0\le t_i<p^{\gamma}} e_{p^{\alpha}}(f(\underset{\sim}{t})) \qquad (1)$$

dengan hasil tambah ini dinilaikan di atas t_i, $0 \le t_i < p^{\gamma}$, $1 \le i \le n$ demikian hingga $f_{\underset{\sim}{x}}(\underset{\sim}{t}) \equiv 0 \bmod p^{\theta}$. Oleh sebab $\alpha = 2\beta + 1$ dengan $\beta \ge 1$, maka jelaslah $\gamma = \beta + 1$.

Untuk setiap i, $1 \le i \le n$, biarkan

$$t_i = u_i + p^{\beta} v_i$$

dengan $0 \le t_i < p^{\beta+1}$, $0 \le u_i < p^{\beta}$ dan $0 \le v_i < p$. Melalui Teorem Taylor, pengembangan $f(\underset{\sim}{t})$ modulo p^{α} di sekitar $\underset{\sim}{u} = (u_1,\ldots,u_n)$ ialah

$$f(\underset{\sim}{t}) = f(\underset{\sim}{u}) + p^{\beta}\nabla f(\underset{\sim}{u})\underset{\sim}{v}^t + \frac{1}{2}p^{2\beta}\underset{\sim}{v}\, J_{\nabla f}(\underset{\sim}{u})\underset{\sim}{v}^t \bmod p^{\alpha} \qquad (2)$$

dengan $\underset{\sim}{v} = (v_1,\ldots,v_n)$, $\nabla f(\underset{\sim}{u}) = [f_{x_1}(\underset{\sim}{u})\ldots f_{x_n}(\underset{\sim}{u})]$, $J_{\nabla f}(\underset{\sim}{u})$ matrik Jakobian bagi ∇f pada $\underset{\sim}{u}$ and $\underset{\sim}{v}^t$ menandakan transposisi $\underset{\sim}{v}$. Sekarang, biarkan

$$S = \sum e_{p^{\alpha}}(f(\underset{\sim}{t})) \qquad (3)$$

dengan hasil tambah ini dinilaikan di atas t_i, $0 \le t_i < p^{\beta+1}$, $1 \le i \le n$ dengan $\nabla f(\underset{\sim}{t}) \equiv 0 \bmod p^{\beta}$. Maka dari (2) and (3)

$$S = \sum e_{p^{\alpha}}(f(\underset{\sim}{u})).G(\underset{\sim}{u})$$

di atas u_i, $0 \le u_i < p^{\beta}$, $1 \le i \le n$ demikian hingga $\nabla f(\underset{\sim}{u}) \equiv 0 \bmod p^{\beta}$. Oleh itu,

$$|S| \leq \sum_{0 \leq u_i < p^{\beta}} |G(\underset{\sim}{u})|$$

$1 \leq i \leq n$ dengan $\nabla \underset{\sim}{f}(\underset{\sim}{u}) \equiv \underset{\sim}{0} \bmod p^{\beta}$. Maka, oleh sebab $\theta = \beta$,

$$|S(f;p^{\alpha})| \leq p^{n\beta} \sum_{\underset{\sim}{u} \bmod p^{\beta}} |G(\underset{\sim}{u})|$$

di atas $\underset{\sim}{u}$ demikian hingga $\nabla \underset{\sim}{f}(\underset{\sim}{u}) \equiv 0 \pmod{p^{\beta}}$ seperti yang ditegaskan. □

Adalah jelas dari Teorem 2.1 dan 2.2 bahawa anggaran kepada $S(f;p^{\alpha})$ adalah bersandar kepada anggaran $N(f;p^{\theta})$ dan $|G(\underset{\sim}{u})|$. Dalam bahagian berikut kita berikan penganggaran kepada $N(f;p^{\theta})$. Untuk anggaran $|G(\underset{\sim}{u})|$ pula kita gunakan anggaran yang telah diberikan oleh Loxton dan Smith [3] untuk tujuan kita.

3. Penganggaran $N(f;p^{\alpha})$

Sekarang kita berikan suatu batas atas $N(\underset{\sim}{f},p^{\alpha})$ dengan $\underset{\sim}{f}$ suatu n-rangkap polinomial di dalam $Z[\underset{\sim}{x}]$. Terlebih dahulu kita berikan takrif yang berikut.

Takrif 3.1

Katakan $\underset{\sim}{f} = (f_1,\ldots,f_n)$ n-rangkap polinomial di dalam $Z[\underset{\sim}{x}]$ dengan $\underset{\sim}{x} = (x_1,\ldots,x_n)$ dan $g_i(\underset{\sim}{x})$ polinomial di dalam $Z[\underset{\sim}{x}]$ yang diperolehi dari $f_i(\underset{\sim}{x})$, $1 \leq i \leq n$, dengan menetapkan nilai sebarang $(n-1)$ rangkap di dalam $\underset{\sim}{x}$. Katakan ξ_j pensifar g_i dengan kegandaan e_j. Kita takrifkan $\delta_i(\underset{\sim}{f})$ dan $e_i(\underset{\sim}{f})$ masing-masing dengan

$$\delta_i(\underset{\sim}{f}) = \max_j \operatorname{per}_p g_i^{(e_j)}(\xi_j)/e_j!$$

dan

$$e_i(\underset{\sim}{f}) = \max_j e_j \quad , \quad 1 \le i \le n.$$

Teorem 3.1

Katakan p nombor perdana dan $\underset{\sim}{f} = (f_1,..,f_n)$ n-rangkap polinomial berdarjah m di dalam $Z[\underset{\sim}{x}]$ dengan $\underset{\sim}{x} = (x_1,...,x_n)$, $n > 1$. Katakan $\delta = \max_{1 \le i \le n} \delta_i(\underset{\sim}{f})$ dan $e = \max_{1 \le i \le n} e_i(\underset{\sim}{f})$. Maka

$$N(f;p^{\alpha}) \le \begin{cases} p^{n\alpha} & \text{jika } \alpha \le \delta \\ mp^{n\alpha - \frac{(\alpha-\delta)}{e}} & \text{jika } \alpha > \delta \end{cases}$$

Bukti

Penegasan teorem adalah remeh jika $\alpha \le \delta$. Andaikan sekarang $\alpha > \delta$. Pertimbangkan set

$$V_{\underset{\sim}{f}}(p^{\alpha}) = \left\{ \underset{\sim}{x} \bmod p^{\alpha} : \underset{\sim}{f}(\underset{\sim}{x}) \equiv \underset{\sim}{0} \bmod p^{\alpha} \right\}.$$

Oleh sebab $f_1(\underset{\sim}{x}) \equiv 0 \bmod p^{\alpha}$ salah satu persamaan kongruen di dalam $V_{\underset{\sim}{f}}(p^{\alpha})$ maka jelaslah

$$N_{\underset{\sim}{f}}(p^{\alpha}) \le N_{f_1}(p^{\alpha}) \qquad (1)$$

dengan $N_g(p^{\alpha})$ menandakan kekardinalan set $V_g(p^{\alpha})$.

Kita boleh mengandaikan nilai-nilai tetap bagi $x_1,...,x_{n-1}$ dalam $\underset{\sim}{x} \bmod p^{\alpha}$ oleh kerana kaedah pembuktiannya sama bagi sebarang (n - 1) rangkap $\underset{\sim}{x}$. Katakan $x = x_n$ dan pertimbangkan polinomial $g_1(x)$ di dalam Z[x]. Katalah

$$g_i(x) = a_o x^k + a_1 x^{k-1} + \ldots + a_k = a_o \prod_j (x - \xi_j)^{e_j}$$

dengan pekali di dalam medan adik-p Ω_p yang lengkap, tertutup secara aljabar dan dengan $k \leq m$ dan ξ_j pensifar-pensifar g_i yang berlainan dengan kegandaan e_j, $j > 0$. Dengan menggunakan kaedah polihedron Newton, Kamel Ariffin [5] memperoleh satu keputusan yang mengimplikasikan bahawa bagi setiap penyelesaian adik-p ξ_j,

$$N_{g_i}(p^\alpha) \leq mp^{\alpha - \frac{\alpha - \delta_i}{e_i}} \qquad (2)$$

dengan $\delta_i = \delta_i(f) = \max_j \operatorname{per}_p g_i^{(e_j)}(\xi_j)/e_j!$ dan $e_j = e_i(f) = \max_j e_j$.

Sekarang, terdapat $p^{(n-1)\alpha}$ pilihan bagi $x_1,..,x_{n-1}$ mod p^α. Maka jelaslah

$$N_{f_i}(p^\alpha) \leq p^{(n-1)\alpha} N_{g_i}(p^\alpha). \qquad (3)$$

Dengan demikian penegasan teorem kita perolehi daripada (1), (2) dan (3) dengan membiarkan $\delta = \max_i \delta_i$ dan $e = \max_i e_i$. □

4. Anggaran bagi $S(f;p^\alpha)$

Teorem berikut ini memberikan suatu anggaran bagi $S(f;p^\alpha)$ dengan f suatu polinomial berdarjah $m \geq 2$ di dalam $Z[\underset{\sim}{x}]$, $\underset{\sim}{x} = (x_1,\ldots,x_n)$, $n > 1$, $\nabla\underset{\sim}{f}$ dan $\delta_i(\underset{\sim}{f})$ pula seperti yang telah ditakrifkan di atas.

Teorem 4.1

Katakan p nombor perdana dan $f(\underset{\sim}{x})$ polinomial berdarjah m + 1 di dalam $Z[\underset{\sim}{x}]$ dengan $\underset{\sim}{x} = (x_1,\ldots,x_n)$. Katakan $\delta = \underset{1 \le i \le n}{\text{maks}}\ \delta_i(\nabla f)$ dan $e = \underset{1 \le i \le n}{\text{maks}}\ e_i(\nabla f)$. Jika $\alpha > 1$, maka

$$|S(f;p^{\alpha})| \le mp^{\min(n\alpha,\ n\alpha - (\alpha-2\delta-1)/2e)}.$$

Bukti

Melalui Teorem 2.1, kita dapati

$$|S(f;p^{\alpha})| \le p^{n(\alpha-\theta)}\, N(f;p^{\theta}) \qquad (1)$$

dengan $\theta = \left[\frac{\alpha}{2}\right]$. Adalah jelas ∇f polinomial-polinomial yang berdarjah selebih-lebihnya m. Jika α genap maka oleh Teorem 3.1,

$$N(f;p^{\theta}) \le mp^{\min(n\alpha,\ n\theta - (\theta-\delta)/e)}.$$

Keputusan teorem ini kita perolehi daripada (1) dan dengan membiarkan $\theta = \alpha/2$.

Katalah sekarang α ganjil. Katakan $\alpha = 2\beta + 1$ dengan $\beta \ge 1$. Oleh Teorem 2.2

$$|S(f;p^{\alpha})| \le p^{n\beta} \sum_{\underset{\sim}{u} \bmod p^{\beta}} |G(\underset{\sim}{u})| \qquad (2)$$

dengan hasil tambah ini dinilaikan di atas semua $\underset{\sim}{u}$ demikian hingga $\nabla f(\underset{\sim}{u}) \equiv 0 \bmod p^{\beta}$ dan $G(\underset{\sim}{u})$ adalah hasil tambah Gaussan

$$G(\underset{\sim}{u}) = \Sigma\, e_p\left(p^{-\beta}\, \nabla f(\underset{\sim}{u})\underset{\sim}{v}^t + \frac{1}{2}\, \underset{\sim}{v}\, J_{\nabla f}(\underset{\sim}{u})\, \underset{\sim}{v}^t\right)$$

dengan $\underset{\sim}{u} = (u_1,..,u_n)$, $\underset{\sim}{v} = (v_1,..,v_n)$, $0 \le u_i < p^{\beta}$, $0 \le v_i < p$, $1 \le i \le n$ dan $J_{\nabla \underset{\sim}{f}}$ matrik Jakobian bagi $\nabla \underset{\sim}{f}$. Oleh Teorem 4 Loxton dan Smith (1982), kita dapati

$$|G(\underset{\sim}{u})| = p^{n/2} \, |\mathrm{Ker}_p \, J_{\nabla \underset{\sim}{f}}|^{1/2}$$

dengan $\mathrm{Ker}_p A$ menandakan bilangan unsur di dalam set $\{\underset{\sim}{x} \bmod p : \underset{\sim}{x} A \equiv 0 \bmod p\}$ dan A pula matrik integer bersaiz n x n. Adalah jelas $|\mathrm{Ker}_p \, J_{\nabla \underset{\sim}{f}}| \le p^n$. Maka oleh (2),

$$|S(f,p^{\alpha})| \le p^{n\beta+n} \, N(f;p^{\beta}).$$

Dengan demikian berikutan dari Teorem 2.1, kita perolehi

$$|S(f;p^{\alpha})| \le mp^{n\beta+n+\min(n\beta,\ n\beta - (\beta-\delta)/e)}. \qquad (3)$$

Penegasan teorem ini diperolehi dengan membiarkan $\beta = \dfrac{\alpha - 1}{2}$ dalam ungkapan (3).

Penutup

Anggaran yang diperolehi bagi $S(f;p^{\alpha})$ apabila α genap adalah yang terbaik mungkin dengan kaedah polihedron Newton. Walau bagaimanapun anggaran $S(f;p^{\theta})$ apabila α ganjil dijangkakan boleh diperbaiki lagi dengan menganalisis dengan lebih teliti hasil tambah Gaussan yang terlibat.

Rujukan

1. S. Chowla and Davenport, "On Weyl's inequality and Waring's problem for cubes". Acta Arithmetica VI (1961) 505-521.

2. P. Deligne, "La Conjecture de Weil" I. Inst. Haute Etudes Sci. Publ. Math. 43 (1974), 273-307.

3. Loxton and Smith, "Estimates for multiple exponential sums", J. Aust. Math. Soc. 33 (1982), 125-134.

4. Loxton and Vaughn, "The estimation of complete exponential sums. Canad. Math. Bull. (4) 28 (1985) 440 - 454.

5. Kamel Ariffin, "A method for determining the cardinality of the set of solutions to congruence equations", Pertanika 11 (1) (1988) 125-131.

6. Kamel Ariffin, "An estimate for multiple exponential sums in two variables", Sains Malaysiana 18 (4) (1989) 129-135.