Strongly diagonal behavior in Vinogradov's mean value theorem

Kevin Ford[1] Trevor D. Wooley[2]

[1]University of Illinois

[2]University of Bristol

October, 2013

Vinogradov's mean value

Definition

$J_{s,k}(X)$ is the number of solutions of the system of Diophantine equations

$$\begin{aligned} x_1^k + \cdots + x_s^k &= y_1^k + \cdots + y_s^k \\ x_1^{k-1} + \cdots + x_s^{k-1} &= y_1^{k-1} + \cdots + y_s^{k-1} \\ &\vdots \\ x_1 + \cdots + x_s &= y_1 + \cdots + y_s \end{aligned}$$

where each variable is a positive integer $\leqslant X$.

Mean value form:

$$J_{s,k}(X) = \int_{[0,1]^k} \cdots \int \Big| \sum_{1 \leqslant n \leqslant X} e(\alpha_1 n + \cdots + \alpha_k n^k) \Big|^{2s} d\boldsymbol{\alpha}$$

Applications

Bounds on $J_{s,k}(X)$ have numerous applications:

- Bounds for exponential sums, e.g. Weyl sums
- Waring's problem
- the Prouhet-Tarry-Escott problem
- Diophantine inequalities
- Bounding the Riemann zeta function
- Additive combinatorics
- Short mixed character sums
- Equations over finite fields

From Weyl sums to Vinogradov's mean value

Let $f(\boldsymbol{\alpha}) = \sum_{1 \leqslant n \leqslant X} e(\alpha_1 n + \cdots + \alpha_k n^k)$.

If $f(\boldsymbol{\alpha})$ is large for some $\boldsymbol{\alpha}$, then

1. $f(\boldsymbol{\beta})$ is large when $\boldsymbol{\beta}$ is close to $\boldsymbol{\alpha}$;
2. For integer y,

$$\begin{aligned} f(\boldsymbol{\alpha}) &= \sum_{1+y \leqslant n \leqslant X+y} e(\alpha_1 n + \cdots + \alpha_k n^k) + O(y) \\ &= \sum_{1 \leqslant n \leqslant X} e(\alpha_1 (n+y) + \cdots + \alpha_k (n+y)^k) + O(y) \\ &= c(y) f(\boldsymbol{\beta}) + O(y), \end{aligned}$$

where $|c(y)| = 1$ and $\beta_j = \sum_{i \geqslant j} \alpha_i \binom{i}{j} y^{i-j}$.

Conclusion: if $f(\boldsymbol{\alpha})$ is large (say on a "minor arc"), then expect $J_{s,k}(X)$ to be large.

Lower bounds

I. The Diophantine system

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \qquad (1 \leqslant j \leqslant k)$$

has trivial (diagonal) solutions with $x_i = y_i$ for each i. Thus

$$J_{s,k}(X) \geqslant \lfloor X \rfloor^s.$$

II. If $|\alpha_j| \leqslant (6kX^j)^{-1}$ for every j, then $|\alpha_1 n + \cdots + \alpha_k n^k| \leqslant \frac{1}{6}$ for every $n \leqslant X$. Thus,

$$\begin{aligned} J_{s,k}(X) &\geqslant \int_{|\alpha_1| \leqslant (6kX)^{-1}} \cdots \int_{|\alpha_k| \leqslant (6kX^k)^{-1}} \left| \frac{1}{2} \lfloor X \rfloor \right|^{2s} d\boldsymbol{\alpha} \\ &\gg_{k,s} X^{2s - \frac{1}{2}k(k+1)}. \end{aligned}$$

Lower bounds, arithmetic proof

II. The second "trivial" lower bound can be proved by a counting argument: Let $J_{s,k}(X;\mathbf{h})$ be the number of solutions of the system of congruences

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = h_j \qquad (1 \leqslant j \leqslant k).$$

and let $r(\mathbf{m})$ be the number of solutions of the system

$$\sum_{i=1}^{s} x_i^j = m_j \qquad (1 \leqslant j \leqslant k).$$

By Cauchy's inequality,

$$J_{s,k}(X;\mathbf{h}) = \sum_{\mathbf{m}_1-\mathbf{m}_2=\mathbf{h}} r(\mathbf{m}_1)r(\mathbf{m}_2) \leqslant \sum_{\mathbf{m}} r(\mathbf{m})^2 = J_{s,k}(X;\mathbf{0}) = J_{s,k}(X).$$

Hence

$$\lfloor X \rfloor^{2s} = \sum_{\mathbf{h}} J_{s,k}(X;\mathbf{h}) \leqslant \sum_{\mathbf{h}} J_{s,k}(X) \ll X^{\frac{1}{2}k(k+1)} J_{s,k}(X).$$

Conjectured order

Easy lower bounds: $J_{s,k}(X) \gg_{k,s} \max\left(X^s, X^{2s-\frac{1}{2}k(k+1)}\right)$.

Main Conjecture: These bounds are sharp, i.e.

$$J_{s,k}(X) \ll_{k,s,\varepsilon} X^{\varepsilon} \max\left(X^s, X^{2s-\frac{1}{2}k(k+1)}\right)$$
$$= X^{\varepsilon} \cdot \begin{cases} X^s & s \leqslant \frac{k(k+1)}{2} \\ X^{2s-\frac{1}{2}k(k+1)} & s \geqslant \frac{k(k+1)}{2}. \end{cases}$$

Probabilistic heuristic: Choose $x_1, \dots, y_s$ at random from $[1, X]$. Then

$$E_j : x_1^j + \cdots + x_s^j - y_1^j - \cdots - y_s^j = 0$$

occurs with probability about X^{-j}. If all E_j are independent, then all E_j occur with probability about $X^{-\frac{1}{2}k(k+1)}$.

Estimates for $s \gtrsim k^2$ (Large s)

Definition

Let $\eta(s,k)$ be the infimum of numbers η so that

$$J_{s,k}(X) \ll X^{2s-\frac{1}{2}k(k+1)+\eta}$$

1. Karatsuba, Stechkin, 1975. We have $\eta(s,k) \lesssim \frac{1}{2}k^2 e^{-s/k^2}$ and

$$J_{s,k}(X) \sim C(s,k)X^{2s-\frac{1}{2}k(k+1)} \qquad \text{(A)}$$

for $s \gtrsim 3k^2 \log k$.

2. Wooley, 1992–96. We have (i) $\eta(s,k) \lesssim \frac{1}{2}k^2 e^{-2s/k^2}$;
(ii) (A) holds for $s \gtrsim k^2 \log k$.

3. Wooley, 2011, "Efficient congruencing".
(i) We have $\eta(s,k) = 0$ for $s \geqslant k^2 - 1$;
(ii) We have (A) for $s \geqslant k^2$.

Estimates for $s \lesssim \frac{1}{4}k^2$ (Small s)

Definition

Let $\delta(s,k)$ be the infimum of numbers δ so that

$$J_{s,k} \ll_{s,k} X^{s+\delta}.$$

Put $\lambda = s/k^2$. Then

- $\delta(k,s) \ll \lambda k^2$ (Stechkin, Karatsuba, 1975).
- $\delta(k,s) \ll \lambda^{3/2} k^2$ (Arkhipov-Karatsuba, 1978).
- $\delta(k,s) \ll \lambda^2 k^2$ (Tyrina, 1987).
- $\delta(k,s) = \lambda k^{5/2} \exp(-\frac{A}{k\lambda^2})$ (Wooley, 1995). Extremely good for $s \leqslant k^{3/2}(\log k)^{-1}$. Worse than trivial for $s \geqslant k^{3/2}$.
- $\delta(k,s) \leqslant 4\lambda = O(1)$ for $s \leqslant \frac{1}{4}k^2 + k$ (Wooley, 2012).
- $\delta(k,s) = 0$ for $s \leqslant \frac{1}{4}k^2 + \frac{1}{2}k$ (Ford-Wooley, 2013).

The main conjecture for smaller s

The Main Conjecture asserts that $J_{s,k}(X) \ll_{s,k,\varepsilon} X^{s+\varepsilon}$ when $s \leqslant \frac{1}{2}k(k+1)$. That is, the system

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \qquad (1 \leqslant j \leqslant k)$$

doesn't have "much more" than the trivial solutions.

I. True for $s \leqslant k$ trivially. Here $\mathbf{x}$ is a permutation of $\mathbf{y}$ by the Viéte-Girard-Newton formulas (A. Girard, 1629).

II. Known true for $s = k+1$ in the 1950s (L.-K. Hua). Before 2012, not known for any larger s.

Theorem (Ford-Wooley, 2013)

We have

$$J_{s,k}(X) \ll_{s,k,\varepsilon} X^{s+\varepsilon}$$

for $s \leqslant \frac{1}{4}(k+1)^2$.

Bounds for intermediate s, $\frac{1}{4}k^2 \lesssim s \lesssim k^2$

Central special case: $s = s_0 = \frac{1}{2}k(k+1)$.

- $\delta(k, s_0) \leqslant 0.303265\ldots k^2$ (Stechkin, Karatsuba, 1975).
- $\delta(k, s_0) \leqslant 0.256195\ldots k^2$ (Arkhipov-Karatsuba, 1978).
- $\delta(k, s_0) \leqslant 0.231960\ldots k^2$ (Tyrina, 1987).
- $\delta(k, s_0) \leqslant 0.238835\ldots k^2$ (Wooley, 1992).
- $\delta(k, s_0) \leqslant 0.202225\ldots k^2$ (A-K,Tyrina,Wooley hybrid).
- $\delta(k, s_0) \leqslant 0.125000\ldots k^2$ (Wooley, 2012).
- $\delta(k, s_0) \leqslant 0.085786\ldots k^2$ (Ford-Wooley, 2013).

Special case: $s = k^2 - tk$, where t is small.

- $\eta(k, s) \lesssim \frac{1}{2}t^2$ (Wooley, 2012).
- $\eta(k, s) \lesssim \frac{1}{4}t^2$ (Ford-Wooley, 2013).

Application: Waring's problem, I

Let $R_{s,k}(n) = \#\{(x_1, \dots, x_s) \in \mathbb{N}^s : n = x_1^k + \cdots + x_s^k\}$.
Hardy and Littlewood: asymptotic formula for $R_{s,k}(n)$ (large s).
Definition: $\widetilde{G}(k)$ is the smallest t such that the asymptotic formula holds for all $s \geqslant t$.

Well-known: It suffices that $t \geqslant 4k$ and for $\mathfrak{m}$ the minor arcs,

$$\int_{\mathfrak{m}} \left|g_k(\alpha; X)\right|^t d\alpha = o(X^{t-k}) \quad (X \to \infty), \quad g_k(\alpha; X) = \sum_{n \leqslant X} e(\alpha n^k).$$

Trivial bound: $\int_0^1 |g_k(\alpha; X)|^{2s}\, d\alpha \ll X^{2s-k+\eta(s,k)}$.

Tool 1 (Ford, 1995). For any integer m, $1 \leqslant m \leqslant k$,

$$\int_0^1 \left|g_k(\alpha; X)\right|^{2s} d\alpha \ll X^{2s-k+\frac{1}{m}\eta(s-\frac{1}{2}m(m-1),k)}.$$

Tool 2 (Wooley, 2012). One has

$$\int_{\mathfrak{m}} \left|g_k(\alpha; X)\right|^{2s} d\alpha \ll X^{2s-k-1+\eta(s,k)+\varepsilon}.$$

Application: Waring's problem, p. 2

Progression of bounds for $\widetilde{G}(k)$ for large k:

- $\widetilde{G}(k) \lesssim 4k^2 \log k$ (Hua, 1949).
- $\widetilde{G}(k) \lesssim 2k^2 \log k$ (Wooley, 1992).
- $\widetilde{G}(k) \lesssim k^2 \log k$ (Ford, 1995).
- $\widetilde{G}(k) \leqslant 2k^2 - k^{4/3} + O(k)$ (Wooley, 2011).
- $\widetilde{G}(k) \leqslant 2k^2 - 2^{2/3}k^{4/3} + O(k)$ (Ford-Wooley, 2013).

Some numerical improvements:

$$\widetilde{G}(12) \leqslant 253, \quad \widetilde{G}(13) \leqslant 299, \quad \widetilde{G}(14) \leqslant 349, \quad \widetilde{G}(15) \leqslant 403,$$

Vaughan's bounds $\widetilde{G}(k) \leqslant 2^k$ are still the best for $k = 3, 4, 5$.

Ideas for bounding $J_{s,k}(X)$

Perhaps the most important property of the system

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \qquad (1 \leqslant j \leqslant k) \tag{1}$$

is the invariance of the solution set under *translations* and *dilations*. That is, letting $x_i = Au_i + B$, $y_i = Av_i + B$ for each i, where $A, B \in \mathbb{N}$, the new system is easily seen, by the binomial theorem, to be equivalent to

$$\sum_{i=1}^{s}(u_i^j - v_i^j) = 0 \qquad (1 \leqslant j \leqslant k).$$

In particular, if $1 \leqslant a \leqslant q$, then the number of solutions of (1) with $1 \leqslant x_i, y_i \leqslant X$ and $x_i, y_i \equiv a \pmod q$ equals $J_{s,k}(\frac{X+q-a}{q})$.

Linnik's p-adic method, I

For $\psi(n;\boldsymbol{\alpha}) = \alpha_1 n + \cdots + \alpha_k n^k$, let

$$f(\boldsymbol{\alpha}) = \sum_{n\leqslant X} e\left(\psi(n;\boldsymbol{\alpha})\right), \quad f(\boldsymbol{\alpha};b,q) = \sum_{\substack{n\leqslant X\\ n\equiv b \pmod q}} e\left(\psi(n;\boldsymbol{\alpha})\right).$$

Fix a prime p. By Hölder's[1] inequality,

$$\begin{aligned} J_{s+k,k}(X) &= \int |f(\boldsymbol{\alpha})|^{2k} \Big| \sum_{\xi=1}^{p} f(\boldsymbol{\alpha};\xi,p)\Big|^{2s} d\boldsymbol{\alpha} \\ &\leqslant \int |f(\boldsymbol{\alpha})|^{2k} \Big(\sum_{\xi=1}^{p} 1\Big)^{2s-1} \sum_{\xi=1}^{p} |f(\boldsymbol{\alpha};\xi,p)|^{2s}\, d\boldsymbol{\alpha} \\ &\leqslant p^{2s} \max_{1\leqslant\xi\leqslant p} \int |f(\boldsymbol{\alpha})|^{2k} |f(\boldsymbol{\alpha};\xi,p)|^{2s}\, d\boldsymbol{\alpha}. \end{aligned}$$

[1] L. J. Rogers (1888)

Linnik's p-adic method, II

The integral

$$\int |f(\boldsymbol{\alpha})|^{2k} |f(\boldsymbol{\alpha}; \xi, p)|^{2s} \, d\boldsymbol{\alpha}$$

counts solutions of the Diophantine system

$$\sum_{i=1}^{s+k} (x_i^j - y_i^j) = 0 \qquad (1 \leqslant j \leqslant k)$$

with $x_{k+1}, \dots, x_{s+k}, y_{k+1}, \dots, y_{s+k} \equiv \xi \pmod{p}$.

Writing $x_i = pu_{i-k} + \xi$, $y_i = pv_{i-k} + \xi$ for $k+1 \leqslant i \leqslant s+k$, and using the binomial theorem, the system becomes

$$\sum_{i=1}^{k} (x_i - \xi)^j - (y_i - \xi)^j = p^j \sum_{i=1}^{s} (u_i^j - v_i^j) \qquad (1 \leqslant j \leqslant k).$$

Linnik's p-adic method, III

In particular,

$$\sum_{i=1}^{k}(x_i-\xi)^j-(y_i-\xi)^j\equiv 0 \pmod{p^j} \qquad (1\leqslant j\leqslant k).$$

Lifting solutions to a common modulus, the number of solutions $\mathbf{x},\mathbf{y}$ mod p^k of this system is $\leqslant p^{1+2+\cdots+(k-1)}$ times the number of solutions of the system

$$\sum_{i=1}^{k}(x_i-\xi)^j-(y_i-\xi)^j\equiv 0 \pmod{p^k} \qquad (1\leqslant j\leqslant k).$$

Assuming the x_i are distinct modulo p and similarly for the y_i, the Viète-Girard-Newton formulas imply $\mathbf{x}$ is a permutation of $\mathbf{y}$ modulo p^k. **Classical method:** count separately the x_i, y_i and the u_i, v_i. If $X^{1/k}\leqslant p\leqslant 2X^{1/k}$, then

$$J_{s+k,k}(X)\ll p^{2s+\frac{1}{2}k(k-1)}X^kJ_{s,k}(X/p+1).$$

Iteration gives $J_{hk,k}(X)\ll X^{2hk-\frac{1}{2}k(k+1)+\frac{1}{2}k^2(1-1/k)^h}$.

Efficient Congruencing (Wooley, 2011)

Take p much smaller than $X^{1/k}$. Since $\mathbf{x}$ is a permutation of $\mathbf{y}$ modulo p^k, one can "undo" the binomial theorem and get

$$J_{s+k,k}(X) \ll p^{2s+\frac{1}{2}k(k-1)} \max_{1\leqslant \xi \leqslant p} I(\xi),$$

where $I(\xi)$ counts solutions of the system

$$\sum_{i=1}^{k}(x_i^j - y_i^j) = \sum_{i=1}^{s}(w_i^j - z_i^j) \qquad (1 \leqslant j \leqslant k)$$

with $x_i \equiv y_i \pmod{p^k}$ and $w_i, z_i \equiv \xi \pmod{p}$. By Hölder,

$$\begin{aligned} I(b) &= \int \Big(\sum_{\eta=1}^{p^k} |f(\boldsymbol{\alpha}; \eta, p^k)|^2 \Big)^k |f(\boldsymbol{\alpha}; \xi, p)|^{2s}\, d\boldsymbol{\alpha} \\ &\leqslant p^{k^2} \max_{1\leqslant \eta \leqslant p^k} \int |f(\boldsymbol{\alpha}; \eta, p^k)|^{2k} |f(\boldsymbol{\alpha}; \xi, p)|^{2s}\, d\boldsymbol{\alpha}. \end{aligned}$$

Efficient congruencing, part 2

Applying Hölder again:

$$\int |f(\boldsymbol{\alpha};\eta,p^k)|^{2k}|f(\boldsymbol{\alpha};\xi,p)|^{2s}\,d\boldsymbol{\alpha} \leqslant \Big(\int |f(\boldsymbol{\alpha};\xi,p)|^{2s+2k}\,d\boldsymbol{\alpha}\Big)^{1-k/s} \times \Big(\int |f(\boldsymbol{\alpha};\eta,p^k)|^{2s}|f(\boldsymbol{\alpha};\xi,p)|^{2k}\,d\boldsymbol{\alpha}\Big)^{k/s}.$$

RHS: 1st integral is $J_{s+k,k}(X/p+1)$; 2nd counts solutions of

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = \sum_{i=1}^{k}(w_i^j - z_i^j) \qquad (1 \leqslant j \leqslant k)$$

with $x_i, y_i \equiv \eta \pmod{p^k}$ and $w_i, z_i \equiv \xi \pmod{p}$.

Efficient congruencing, part 3

By the binomial theorem again, the system is equivalent to

$$\sum_{i=1}^{k} \big((w_i - \eta)^j - (z_i - \eta)^j\big) \equiv 0 \pmod{p^{jk}} \qquad (1 \leqslant j \leqslant k).$$

After lifting the congruences all to modulus p^{k^2}, we again find that $\mathbf{w}$ is a permutation of $\mathbf{z}$ modulo p^{k^2} (*assuming the* w_i *are distinct modulo* p^2 *and similarly with the* z_i).

Continue this process, generating ever more efficient congruences modulo p^{k^3}, p^{k^4}. We stop when $p^{k^N} > X$. This bounds $J_{s+k,k}(X)$ in terms of $J_{s+k,k}(X/p)$, $J_{s+k,k}(X/p^k)$, etc.

The end result is $\eta(k^2 + k, k) = 0$.

Efficient congruencing variation 1

Arkhipov-Karatsuba, 1978. Let $1 \leqslant r \leqslant k$. Separate $2r$ variables $x_1, \dots, x_r, y_1, \dots, y_r$ instead of $2k$ variables. We get

$$\sum_{i=1}^{r} (x_i - \xi)^j - (y_i - \xi)^j \equiv 0 \pmod{p^j} \qquad (1 \leqslant j \leqslant k).$$

Lifting all congruences up to modulus p^k "costs" $p^{\frac{1}{2}k(k-1)}$.

Better: ignore the lower $k-r$ congruences (with $1 \leqslant j \leqslant k-r$) and lift the rest. The "cost" is now $p^{\frac{1}{2}r(r-1)}$, much less.
$\#$ variables $= \#$ congruences $\implies \mathbf{x} \equiv \mathbf{y} \pmod{p^k}$.

Now relate $J_{s+r,k}(X)$ to $J_{s,k}(X/p+1)$ in the classical setting. Often the optimal value of r is less than k.

Inserted into the Efficient Congruencing method, we relate $J_{s+r,k}(X)$ to $J_{s+r,k}(X/p)$, etc.

Efficient Congruencing variation 2

Tyrina, 1987. As with the Arkhipov-Karatsuba method, separate $2r$ variables and ignore the congruences for $1 \leqslant j \leqslant k-r$. However, we lift all the congruences only up to modulus p^t, where $1 \leqslant t \leqslant k$. For $t < k$, this has smaller "cost", namely

$$p^{\frac{1}{2}(t+r-k)(t+r-k-1)} \qquad (t+r \geqslant k).$$

Weaker conclusion: $\mathbf{x}$ is a permutation of $\mathbf{y}$ modulo p^t.

Tyrina (1987) takes $r = t \geqslant k/2$ in the classical setup.
We take arbitrary r, t; usually $r \approx t$ give the best bounds.

In the efficient congruencing iteration, we actually need to bound the number of solutions of the system

$$\sum_{i=1}^{r}(z_i-\eta)^j \equiv \sum_{i=1}^{r}(w_i-\eta)^j \pmod{p^{jb}} \qquad (1\leqslant j\leqslant k),$$

with $1\leqslant z_i, w_i \leqslant p^{tb}$, and all $w_i, z_i \equiv \xi \pmod{p^a}$, and $p\nmid(\eta-\xi)$.

The true "cost" of this system is

$$p^{\frac{b}{2}(t+r-k)(t+r-k-1)+\frac{a}{2}(t+r-k)(k+r-t-1)}.$$

Optimal cost: when $r+t=k$, above is p^0.

Our main theorem

Theorem

Suppose $1 \leqslant r, t \leqslant k$ *and* $r + t \geqslant k$. *For* $s = r(t+1)$,

$$J_{s,k}(X) \ll_\varepsilon X^{s+\frac{1}{2}(t+r-k)(t+r-k-1+\frac{2r-2}{t-1})+\varepsilon},$$

Example: If $r + t = k$, get $J_{s,k}(X) \ll X^{s+\varepsilon}$.
Max s at $r = t = k/2$ (k even), $r = \frac{k+1}{2}$, $t = \frac{k-1}{2}$ (k odd).

Example: $r = t = k - m$. Gives $\eta((k-m)^2 + (k-m), k) \leqslant m^2$.