

Vinogradov's mean value theorem and its associated restriction theory via efficient congruencing.

Trevor D. Wooley

University of Bristol

Oxford, 29th September 2014

1. Introduction

Let $k \geq 2$ be an integer, and consider

$$g : \mathbb{T}^k \rightarrow \mathbb{C} \quad (\mathbb{T} = \mathbb{R}/\mathbb{Z} \simeq [0, 1)),$$

with an associated Fourier series

$$\tilde{g}(\alpha_1, \dots, \alpha_k) = \sum_{\mathbf{n} \in \mathbb{Z}^k} \hat{g}(n_1, \dots, n_k) e(n_1 \alpha_1 + \dots + n_k \alpha_k),$$

in which $\hat{g}(\mathbf{n}) \in \mathbb{C}$ and $e(z) = e^{2\pi iz}$.

1. Introduction

Let $k \geq 2$ be an integer, and consider

$$g : \mathbb{T}^k \rightarrow \mathbb{C} \quad (\mathbb{T} = \mathbb{R}/\mathbb{Z} \simeq [0, 1)),$$

with an associated Fourier series

$$\tilde{g}(\alpha_1, \dots, \alpha_k) = \sum_{\mathbf{n} \in \mathbb{Z}^k} \widehat{g}(n_1, \dots, n_k) e(n_1 \alpha_1 + \dots + n_k \alpha_k),$$

in which $\widehat{g}(\mathbf{n}) \in \mathbb{C}$ and $e(z) = e^{2\pi iz}$.

Restriction operator: (E. Stein, J. Bourgain, K. Hughes, et al.)

$$\mathcal{R}g := \sum_{\substack{\mathbf{n} \in \mathbb{Z}^k \\ \mathbf{n} = (n, n^2, \dots, n^k)}} \widehat{g}(\mathbf{n}) e(\mathbf{n} \cdot \boldsymbol{\alpha}).$$

[This is just one example of a restriction operator!]

1. Introduction

Let $k \geq 2$ be an integer, and consider

$$g : \mathbb{T}^k \rightarrow \mathbb{C} \quad (\mathbb{T} = \mathbb{R}/\mathbb{Z} \simeq [0, 1)),$$

with an associated Fourier series

$$\tilde{g}(\alpha_1, \dots, \alpha_k) = \sum_{\mathbf{n} \in \mathbb{Z}^k} \widehat{g}(n_1, \dots, n_k) e(n_1 \alpha_1 + \dots + n_k \alpha_k),$$

in which $\widehat{g}(\mathbf{n}) \in \mathbb{C}$ and $e(z) = e^{2\pi iz}$.

Restriction operator: (E. Stein, J. Bourgain, K. Hughes, et al.)

$$\mathcal{R}g := \sum_{\substack{\mathbf{n} \in \mathbb{Z}^k \\ \mathbf{n} = (n, n^2, \dots, n^k)}} \widehat{g}(\mathbf{n}) e(\mathbf{n} \cdot \boldsymbol{\alpha}).$$

[This is just one example of a restriction operator!]

We are interested in the norm of the operator $g \mapsto \mathcal{R}g$.

(Slightly) more concretely (for analytic number theorists):

Consider a sequence $(a_n)_{n=1}^{\infty}$ of complex numbers, not all zero, and define the exponential sum $f_{\mathbf{a}} = f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)$ by putting

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

(Slightly) more concretely (for analytic number theorists):

Consider a sequence $(a_n)_{n=1}^{\infty}$ of complex numbers, not all zero, and define the exponential sum $f_{\mathbf{a}} = f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)$ by putting

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

Aim: Obtain a bound for

$$\sup_{\mathbf{a}} (\|f_{\mathbf{a}}\|_{L^p} / \|\mathbf{a}\|_{\ell^2})$$

in terms of p , k and X .

(Slightly) more concretely (for analytic number theorists):

Consider a sequence $(a_n)_{n=1}^{\infty}$ of complex numbers, not all zero, and define the exponential sum $f_{\mathbf{a}} = f_{k,\mathbf{a}}(\alpha; X)$ by putting

$$f_{k,\mathbf{a}}(\alpha; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

Aim: Obtain a bound for

$$\sup_{\mathbf{a}} (\|f_{\mathbf{a}}\|_{L^p} / \|\mathbf{a}\|_{\ell^2})$$

in terms of p , k and X .

Conjecture (Main Restriction Conjecture)

For each $\varepsilon > 0$, one has

$$\frac{\|f_{\mathbf{a}}\|_{L^p}}{\|\mathbf{a}\|_{\ell^2}} \ll_{\varepsilon,p,k} \begin{cases} X^{\varepsilon}, & \text{when } 0 < p \leq k(k+1), \\ X^{\frac{1}{2} - \frac{k(k+1)}{2p}}, & \text{when } p > k(k+1). \end{cases}$$

(Even) more concretely (for analytic number theorists):

Consider a sequence $(a_n)_{n=1}^{\infty}$ of complex numbers, not all zero, and define the exponential sum $f_{\mathbf{a}} = f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)$ by putting

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

(Even) more concretely (for analytic number theorists):

Consider a sequence $(a_n)_{n=1}^{\infty}$ of complex numbers, not all zero, and define the exponential sum $f_{\mathbf{a}} = f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)$ by putting

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

Conjecture (Main Restriction Conjecture)

For each $\varepsilon > 0$, one has

$$\oint |f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll \begin{cases} X^\varepsilon \left(\sum_{n \leq X} |a_n|^2 \right)^s, & \text{when } s \leq \frac{1}{2}k(k+1), \\ X^{s - \frac{1}{2}k(k+1)} \left(\sum_{n \leq X} |a_n|^2 \right)^s, & \text{when } s > \frac{1}{2}k(k+1). \end{cases}$$

Here, we write \oint for $\int_{[0,1]^k}$.

Some observations, I:

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

Conjecture (Main Restriction Conjecture)

$$\int_{\mathbb{F}} |f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll \begin{cases} X^\varepsilon \left(\sum_{n \leq X} |a_n|^2 \right)^s, & \text{when } s \leq \frac{1}{2}k(k+1), \\ X^{s - \frac{1}{2}k(k+1)} \left(\sum_{n \leq X} |a_n|^2 \right)^s, & \text{when } s > \frac{1}{2}k(k+1). \end{cases}$$

Some observations, I:

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

Conjecture (Main Restriction Conjecture)

$$\oint |f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll \begin{cases} X^\varepsilon \left(\sum_{n \leq X} |a_n|^2 \right)^s, & \text{when } s \leq \frac{1}{2}k(k+1), \\ X^{s - \frac{1}{2}k(k+1)} \left(\sum_{n \leq X} |a_n|^2 \right)^s, & \text{when } s > \frac{1}{2}k(k+1). \end{cases}$$

Consider the sequence $(a_n) = 1$. Then MRC implies that

$$\oint |f_{k,1}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^\varepsilon (X^s + X^{2s - \frac{1}{2}k(k+1)}),$$

an assertion equivalent to the Main Conjecture in Vinogradov's Mean Value Theorem.

Some observations, II:

Consider the situation in which (a_n) is supported on a thin sequence, say

$$a_n = \text{card} \{ (x, y) \in \mathbb{Z}^2 : n = x^4 + y^4 \}.$$

Some observations, II:

Consider the situation in which (a_n) is supported on a thin sequence, say

$$a_n = \text{card} \{(x, y) \in \mathbb{Z}^2 : n = x^4 + y^4\}.$$

Then MRC implies that for $1 \leq s \leq \frac{1}{2}k(k+1)$, one should have

$$\begin{aligned} \int_{\phi} |f_{k,a}(\alpha; X)|^{2s} d\alpha &\ll X^\varepsilon \left(\sum_{n \leq X} |a_n|^2 \right)^s \\ &\ll X^\varepsilon \left(X^{1/2} \right)^s = X^{s/2+\varepsilon}. \end{aligned}$$

Some observations, II:

Consider the situation in which (a_n) is supported on a thin sequence, say

$$a_n = \text{card} \{(x, y) \in \mathbb{Z}^2 : n = x^4 + y^4\}.$$

Then MRC implies that for $1 \leq s \leq \frac{1}{2}k(k+1)$, one should have

$$\begin{aligned} \int |f_{k,a}(\alpha; X)|^{2s} d\alpha &\ll X^\varepsilon \left(\sum_{n \leq X} |a_n|^2 \right)^s \\ &\ll X^\varepsilon \left(X^{1/2} \right)^s = X^{s/2+\varepsilon}. \end{aligned}$$

But by orthogonality, when s is a positive integer, this integral counts the number of solutions of the system of equations

$$\sum_{i=1}^s ((u_i^4 + v_i^4)^j - (u_{s+i}^4 + v_{s+i}^4)^j) = 0 \quad (1 \leq j \leq k),$$

with $1 \leq u_i^4 + v_i^4 \leq X$ ($1 \leq i \leq 2s$).

Some observations, II:

So the number $N(X)$ of integral solutions of the system of equations

$$\sum_{i=1}^s ((u_i^4 + v_i^4)^j - (u_{s+i}^4 + v_{s+i}^4)^j) = 0 \quad (1 \leq j \leq k),$$

with $1 \leq u_i^4 + v_i^4 \leq X$ ($1 \leq i \leq 2s$), satisfies

$$N(X) \ll X^{s/2+\varepsilon}.$$

Some observations, II:

So the number $N(X)$ of integral solutions of the system of equations

$$\sum_{i=1}^s ((u_i^4 + v_i^4)^j - (u_{s+i}^4 + v_{s+i}^4)^j) = 0 \quad (1 \leq j \leq k),$$

with $1 \leq u_i^4 + v_i^4 \leq X$ ($1 \leq i \leq 2s$), satisfies

$$N(X) \ll X^{s/2+\varepsilon}.$$

But the number of diagonal solutions with $u_i = u_{s+i}$ and $v_i = v_{s+i}$, for all i , has order of growth $X^{s/2}$.

So this shows that “on average”, the solutions are diagonal. This is not a conclusion that follows from the Main Conjecture in Vinogradov’s mean value theorem (by any method known to me!).

2. Classical results (Bourgain, 1993)

The Main restriction Conjecture holds for $k = 2$, and in particular:

$$\int \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n\beta) \right|^{2s} d\alpha d\beta \ll \left(\sum_{n \leq X} |a_n|^2 \right)^s \quad (s < 3),$$

$$\int \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n\beta) \right|^6 d\alpha d\beta \ll X^\varepsilon \left(\sum_{n \leq X} |a_n|^2 \right)^3,$$

$$\int \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n\beta) \right|^{2s} d\alpha d\beta \ll X^{s-3} \left(\sum_{n \leq X} |a_n|^2 \right)^s \quad (s > 3).$$

Sketch proof for the case $k = 2$ and $s = 3$:

By orthogonality, the integral

$$\oint \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n \beta) \right|^6 d\alpha d\beta$$

counts the number of solutions of the simultaneous equations

$$\left. \begin{aligned} n_1^2 + n_2^2 + n_3^2 &= n_4^2 + n_5^2 + n_6^2 \\ n_1 + n_2 + n_3 &= n_4 + n_5 + n_6 \end{aligned} \right\},$$

with each solution counted with weight

$$a_{n_1} a_{n_2} a_{n_3} \bar{a}_{n_4} \bar{a}_{n_5} \bar{a}_{n_6}.$$

Sketch proof for the case $k = 2$ and $s = 3$:

By orthogonality, the integral

$$\oint \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n \beta) \right|^6 d\alpha d\beta$$

counts the number of solutions of the simultaneous equations

$$\left. \begin{aligned} n_1^2 + n_2^2 - n_3^2 &= n_4^2 + n_5^2 - n_6^2 \\ n_1 + n_2 - n_3 &= n_4 + n_5 - n_6 \end{aligned} \right\},$$

with each solution counted with weight

$$a_{n_1} a_{n_2} \bar{a}_{n_3} \bar{a}_{n_4} \bar{a}_{n_5} a_{n_6}.$$

Let $\mathcal{B}(\mathbf{h})$ denote the set of integral solutions of the equation

$$\left. \begin{aligned} n_1^2 + n_2^2 - n_3^2 &= h_2 \\ n_1 + n_2 - n_3 &= h_1 \end{aligned} \right\},$$

with $1 \leq n_i \leq X$.

Let $\mathcal{B}(\mathbf{h})$ denote the set of integral solutions of the equation

$$\left. \begin{aligned} n_1^2 + n_2^2 - n_3^2 &= h_2 \\ n_1 + n_2 - n_3 &= h_1 \end{aligned} \right\},$$

with $1 \leq n_i \leq X$.

Then by Cauchy's inequality,

$$\begin{aligned} \int \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n \beta) \right|^6 d\alpha d\beta &= \sum_{|h_i| \leq 2X^i (i=1,2)} \left(\sum_{(n_1, n_2, n_3) \in \mathcal{B}(\mathbf{h})} a_{n_1} a_{n_2} \bar{a}_{n_3} \right)^2 \\ &\leq \sum_{\mathbf{h}} \sum_{n_1, n_2, n_3} |\mathcal{B}(\mathbf{h})| |a_{n_1} a_{n_2} a_{n_3}|^2. \end{aligned}$$

Let $\mathcal{B}(\mathbf{h})$ denote the set of integral solutions of the equation

$$\left. \begin{aligned} n_1^2 + n_2^2 - n_3^2 &= h_2 \\ n_1 + n_2 - n_3 &= h_1 \end{aligned} \right\},$$

with $1 \leq n_i \leq X$.

Then by Cauchy's inequality,

$$\begin{aligned} \int \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n \beta) \right|^6 d\alpha d\beta &= \sum_{|h_i| \leq 2X^i (i=1,2)} \left(\sum_{(n_1, n_2, n_3) \in \mathcal{B}(\mathbf{h})} a_{n_1} a_{n_2} \bar{a}_{n_3} \right)^2 \\ &\leq \sum_{\mathbf{h}} \sum_{n_1, n_2, n_3} |\mathcal{B}(\mathbf{h})| |a_{n_1} a_{n_2} a_{n_3}|^2. \end{aligned}$$

But $|\mathcal{B}(\mathbf{h})|$ is bounded above by the number of solutions of

$$\begin{aligned} h_1^2 - h_2 &= (n_1 + n_2 - n_3)^2 - (n_1^2 + n_2^2 - n_3^2) \\ &= 2(n_1 - n_3)(n_2 - n_3), \end{aligned}$$

and this is $O(X^\epsilon)$ unless $n_1 = n_3$ or $n_2 = n_3$.

One should remove the special solutions with $n_1 = n_3$ or $n_2 = n_3$ in advance, and for the remaining solutions one finds that

$$\int \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n \beta) \right|^6 d\alpha d\beta \ll X^\varepsilon \sum_{n_1, n_2, n_3} |a_{n_1} a_{n_2} a_{n_3}|^2 \\ \ll X^\varepsilon \left(\sum_n |a_n|^2 \right)^3.$$

One should remove the special solutions with $n_1 = n_3$ or $n_2 = n_3$ in advance, and for the remaining solutions one finds that

$$\begin{aligned} \int \left| \sum_{1 \leq n \leq X} a_n e(n^2 \alpha + n \beta) \right|^6 d\alpha d\beta &\ll X^\varepsilon \sum_{n_1, n_2, n_3} |a_{n_1} a_{n_2} a_{n_3}|^2 \\ &\ll X^\varepsilon \left(\sum_n |a_n|^2 \right)^3. \end{aligned}$$

Key observation: With $\mathcal{B}(\mathbf{h})$ the set of integral solutions of the equation

$$\left. \begin{aligned} n_1^2 + n_2^2 - n_3^2 &= h_2 \\ n_1 + n_2 - n_3 &= h_1 \end{aligned} \right\},$$

with $1 \leq n_i \leq X$, one has $|\mathcal{B}(\mathbf{h})| \ll X^\varepsilon$ (Very strong control of the number of solutions of the associated Diophantine system).

Now let $\mathcal{B}_{s,k}(\mathbf{h})$ denote the set of integral solutions of the system

$$\sum_{i=1}^s x_i^j = h_j \quad (1 \leq j \leq k),$$

with $1 \leq x_i \leq X$. Then we have

$$|\mathcal{B}_{s,k}(\mathbf{h})| \ll 1 \quad (1 \leq s \leq k),$$

and (using estimates from Vinogradov's mean value theorem)

$$|\mathcal{B}_{s,k}(\mathbf{h})| \ll X^{s - \frac{1}{2}k(k+1)},$$

for $s > 2k(k-1)$ (uses W., 2014).

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

Theorem (Bourgain, 1993; K. Hughes, 2012)

For each $\varepsilon > 0$, one has MRC in the shape

$$\int |f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^\varepsilon (1 + X^{s - \frac{1}{2}k(k+1)}) \left(\sum_{n \leq X} |a_n|^2 \right)^s$$

whenever:

- (a) $k = 2$, or
- (b) $s \leq k + 1$, or
- (c) $s \geq 2k(k - 1)$.

Moreover, the factor X^ε may be removed when $s > 2k(k - 1)$.

$$f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X) = \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

Theorem (Bourgain, 1993; K. Hughes, 2012)

For each $\varepsilon > 0$, one has MRC in the shape

$$\oint |f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^\varepsilon (1 + X^{s - \frac{1}{2}k(k+1)}) \left(\sum_{n \leq X} |a_n|^2 \right)^s$$

whenever:

- (a) $k = 2$, or
- (b) $s \leq k + 1$, or
- (c) $s \geq 2k(k - 1)$.

Moreover, the factor X^ε may be removed when $s > 2k(k - 1)$.

The result (c) and its sequel depends on the latest “efficient congruencing” results in Vinogradov’s mean value theorem (W., 2014).

Theorem (Bourgain, 1993; K. Hughes, 2012)

For each $\varepsilon > 0$, one has MRC in the shape

$$\oint |f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^\varepsilon (1 + X^{s - \frac{1}{2}k(k+1)}) \left(\sum_{n \leq X} |a_n|^2 \right)^s$$

whenever:

- (a) $k = 2$, or
- (b) $s \leq k + 1$, or
- (c) $s \geq 2k(k - 1)$.

Moreover, the factor X^ε may be removed when $s > 2k(k - 1)$.

Theorem (Bourgain, 1993; K. Hughes, 2012)

For each $\varepsilon > 0$, one has MRC in the shape

$$\oint |f_{k,\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^\varepsilon (1 + X^{s - \frac{1}{2}k(k+1)}) \left(\sum_{n \leq X} |a_n|^2 \right)^s$$

whenever:

- (a) $k = 2$, or
- (b) $s \leq k + 1$, or
- (c) $s \geq 2k(k - 1)$.

Moreover, the factor X^ε may be removed when $s > 2k(k - 1)$.

Very recently: Bourgain and Demeter, 2014: The above (MRC) conclusion holds for $s \leq 2k - 1$ in place of $s \leq k + 1$.

3. Efficient congruencing

Recent techniques applied in the context of Vinogradov's mean value theorem allow one to establish:

Theorem (W. 2014)

For each $\varepsilon > 0$, one has MRC in the shape

$$\oint |f_{k,\mathbf{a}}(\alpha; X)|^{2s} d\alpha \ll X^\varepsilon (1 + X^{s - \frac{1}{2}k(k+1)}) \left(\sum_{n \leq X} |a_n|^2 \right)^s$$

whenever:

(a) $k = 2, 3$ (cf. classical $k = 2$), or

(b) $1 \leq s \leq D(k)$, where $D(4) = 8$, $D(5) = 10$, $D(6) = 17, \dots$, and $D(k) = \frac{1}{2}k(k+1) - \frac{1}{3}k + O(k^{2/3})$ (cf. classical $D(k) = k+1$), or

(c) $s \geq k(k-1)$ (cf. classical $s \geq 2k(k-1)$).

Moreover, the factor X^ε may be removed when $s > k(k-1)$.

We now aim to sketch the ideas underlying a slightly simpler result:

Theorem

For each $\varepsilon > 0$, one has MRC in the shape

$$\oint |f_{k,\mathbf{a}}(\alpha; X)|^{2s} d\alpha \ll X^\varepsilon (1 + X^{s - \frac{1}{2}k(k+1)}) \left(\sum_{n \leq X} |a_n|^2 \right)^s$$

whenever $s \geq k(k+1)$.

It is worth noting that we tackle the mean value directly, rather than using results about Vinogradov's mean value theorem (the special case $(a_n) = (1)$) indirectly.

Consider an auxiliary prime number p (for now, think of p as being a very small power of X).

Write

$$\rho_c(\xi) = \rho_c(\xi; \mathbf{a}) = \left(\sum_{\substack{1 \leq n \leq X \\ n \equiv \xi \pmod{p^c}}} |a_n|^2 \right)^{1/2},$$

and then define

$$\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X) = \rho_0(1)^{-1} \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

[Note: if $a_n = 0$ for all n , then define $\tilde{f}_{\mathbf{a}} = 0$.]

Consider an auxiliary prime number p (for now, think of p as being a very small power of X).

Write

$$\rho_c(\xi) = \rho_c(\xi; \mathbf{a}) = \left(\sum_{\substack{1 \leq n \leq X \\ n \equiv \xi \pmod{p^c}}} |a_n|^2 \right)^{1/2},$$

and then define

$$\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X) = \rho_0(1)^{-1} \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k).$$

[Note: if $a_n = 0$ for all n , then define $\tilde{f}_{\mathbf{a}} = 0$.]

We investigate

$$U_{s,k}(X; \mathbf{a}) = \oint |\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha}.$$

Observe that by Cauchy's inequality, one has

$$\begin{aligned} |f_{\mathbf{a}}(\boldsymbol{\alpha}; X)| &= \left| \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k) \right| \\ &\leq X^{1/2} \left(\sum_{n \leq X} |a_n|^2 \right)^{1/2}, \end{aligned}$$

whence

$$|\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X)| \leq X^{1/2}.$$

Observe that by Cauchy's inequality, one has

$$\begin{aligned} |f_{\mathbf{a}}(\boldsymbol{\alpha}; X)| &= \left| \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k) \right| \\ &\leq X^{1/2} \left(\sum_{n \leq X} |a_n|^2 \right)^{1/2}, \end{aligned}$$

whence

$$|\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X)| \leq X^{1/2}.$$

Thus

$$U_{s,k}(X; \mathbf{a}) = \int \phi |\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^s.$$

Observe that by Cauchy's inequality, one has

$$\begin{aligned} |f_{\mathbf{a}}(\boldsymbol{\alpha}; X)| &= \left| \sum_{1 \leq n \leq X} a_n e(n\alpha_1 + \dots + n^k \alpha_k) \right| \\ &\leq X^{1/2} \left(\sum_{n \leq X} |a_n|^2 \right)^{1/2}, \end{aligned}$$

whence

$$|\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X)| \leq X^{1/2}.$$

Thus

$$U_{s,k}(X; \mathbf{a}) = \oint |\tilde{f}_{\mathbf{a}}(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \ll X^s.$$

Moreover, one has that $U_{s,k}(X; \mathbf{a})$ is scale-invariant, by which we mean that it is invariant on scaling (a_n) to (γa_n) for any $\gamma > 0$.

Define

$$\lambda_s = \limsup_{X \rightarrow \infty} \sup_{\substack{(a_n) \in \mathbb{C}^{[X]} \\ |a_n| \leq 1}} \frac{\log U_{s,k}(X; \mathbf{a})}{\log X}.$$

Define

$$\lambda_s = \limsup_{X \rightarrow \infty} \sup_{\substack{(a_n) \in \mathbb{C}^{[X]} \\ |a_n| \leq 1}} \frac{\log U_{s,k}(X; \mathbf{a})}{\log X}.$$

Then there exists a sequence $(X_m)_{m=1}^{\infty}$ with $\lim_{m \rightarrow \infty} X_m = +\infty$ such that, for some sequence $(a_n) \in \mathbb{C}^{[X_m]}$ with $|a_n| \leq 1$, one has that for each $\varepsilon > 0$,

$$U_{s,k}(X_m; \mathbf{a}) \gg X^{\lambda_s - \varepsilon},$$

whilst whenever $1 \leq Y \leq X_m^{1/2}$, and for all sequences (a_n) , at the same time one has

$$U_{s,k}(Y; \mathbf{a}) \ll Y^{\lambda_s + \varepsilon}.$$

Define

$$\lambda_s = \limsup_{X \rightarrow \infty} \sup_{\substack{(a_n) \in \mathbb{C}^{[X]} \\ |a_n| \leq 1}} \frac{\log U_{s,k}(X; \mathbf{a})}{\log X}.$$

Then there exists a sequence $(X_m)_{m=1}^{\infty}$ with $\lim_{m \rightarrow \infty} X_m = +\infty$ such that, for some sequence $(a_n) \in \mathbb{C}^{[X_m]}$ with $|a_n| \leq 1$, one has that for each $\varepsilon > 0$,

$$U_{s,k}(X_m; \mathbf{a}) \gg X^{\lambda_s - \varepsilon},$$

whilst whenever $1 \leq Y \leq X_m^{1/2}$, and for all sequences (a_n) , at the same time one has

$$U_{s,k}(Y; \mathbf{a}) \ll Y^{\lambda_s + \varepsilon}.$$

We now fix such a value $X = X_m$ sufficiently large, and put

$$\Lambda = \lambda_{s+k} - \left(s + k - \frac{1}{2}k(k+1) \right).$$

Define

$$\lambda_s = \limsup_{X \rightarrow \infty} \sup_{\substack{(a_n) \in \mathbb{C}^{[X]} \\ |a_n| \leq 1}} \frac{\log U_{s,k}(X; \mathbf{a})}{\log X}.$$

Then there exists a sequence $(X_m)_{m=1}^{\infty}$ with $\lim_{m \rightarrow \infty} X_m = +\infty$ such that, for some sequence $(a_n) \in \mathbb{C}^{[X_m]}$ with $|a_n| \leq 1$, one has that for each $\varepsilon > 0$,

$$U_{s,k}(X_m; \mathbf{a}) \gg X^{\lambda_s - \varepsilon},$$

whilst whenever $1 \leq Y \leq X_m^{1/2}$, and for all sequences (a_n) , at the same time one has

$$U_{s,k}(Y; \mathbf{a}) \ll Y^{\lambda_s + \varepsilon}.$$

We now fix such a value $X = X_m$ sufficiently large, and put

$$\Lambda = \lambda_{s+k} - \left(s + k - \frac{1}{2}k(k+1) \right).$$

Aim: Prove that $\Lambda \leq 0$ for $s \geq k^2$.

Aim: Prove that $\Lambda \leq 0$ for $s \geq k^2$.

This implies that

$$U_{s+k}(X; \mathbf{a}) \ll X^{s+k-\frac{1}{2}k(k+1)+\varepsilon},$$

for $s+k \geq k(k+1)$, thereby confirming MRC under the same condition on s .

Approach this problem through an auxiliary mean value. Define

$$f_c(\boldsymbol{\alpha}; \xi) = \rho_c(\xi)^{-1} \sum_{\substack{1 \leq n \leq X \\ n \equiv \xi \pmod{p^c}}} a_n e(n\alpha_1 + \dots + n^k \alpha_k),$$

and then put

$$K_{a,b}(X) = \rho_0(1)^{-4} \sum_{\xi=1}^{p^a} \sum_{\eta=1}^{p^b} \rho_a(\xi)^2 \rho_b(\eta)^2 \oint |f_a(\boldsymbol{\alpha}; \xi)^{2k} f_b(\boldsymbol{\alpha}; \eta)^{2s}| d\boldsymbol{\alpha}.$$

$$K_{a,b}(X) = \rho_0(1)^{-4} \sum_{\xi=1}^{p^a} \sum_{\eta=1}^{p^b} \rho_a(\xi)^2 \rho_b(\eta)^2 \oint |f_a(\alpha; \xi)^{2k} f_b(\alpha; \eta)^{2s}| d\alpha.$$

One “expects” that

$$K_{a,b}(X) \ll X^\varepsilon (X/p^a)^{k-\frac{1}{2}k(k+1)} (X/p^b)^s,$$

and motivated by this observation, we define

$$[[K_{a,b}(X)]] = \frac{K_{a,b}(X)}{(X/p^a)^{k-\frac{1}{2}k(k+1)} (X/p^b)^s}.$$

$$[[K_{a,b}(X)]] = \frac{K_{a,b}(X)}{(X/p^a)^{k-\frac{1}{2}k(k+1)}(X/p^b)^s}.$$

$$[[K_{a,b}(X)]] = \frac{K_{a,b}(X)}{(X/p^a)^{k-\frac{1}{2}k(k+1)}(X/p^b)^s}.$$

Strategy:

(i) Show that if

$$U_{s+k,k}(X; \mathbf{a}) \gg X^{s+k-\frac{1}{2}k(k+1)+\Lambda},$$

then

$$[[K_{0,1}(X)]] \gg X^\Lambda.$$

(ii) Show that whenever

$$[[K_{a,b}(X)]] \gg X^\Lambda(p^\psi)^\Lambda,$$

then there is a small non-negative integer h with the property that

$$[[K_{a',b'}(X)]] \gg X^\Lambda(p^{\psi'})^\Lambda,$$

where

$$\psi' = (s/k)\psi + (s/k - 1)b, \quad a' = b, \quad b' = kb + h.$$

(ii) Show that whenever

$$[[K_{a,b}(X)]] \gg X^\Lambda (p^\psi)^\Lambda,$$

then there is a small non-negative integer h with the property that

$$[[K_{a',b'}(X)]] \gg X^\Lambda (p^{\psi'})^\Lambda,$$

where

$$\psi' = (s/k)\psi + (s/k - 1)b, \quad a' = b, \quad b' = kb + h.$$

By iterating this process, we obtain sequences $(a^{(n)})$, $(b^{(n)})$, $(\psi^{(n)})$ with

$$b^{(n)} \approx k^n \quad \text{and} \quad \psi^{(n)} \approx nk^n$$

for which

$$[[K_{a^{(n)},b^{(n)}}(X)]] \gg X^\Lambda (p^{\psi^{(n)}})^\Lambda.$$

Suppose that $\Lambda > 0$. Then the right hand side here increases so rapidly that, for large enough values of n , it is larger than the trivial estimate for the left hand side. This gives a contradiction, so that $\Lambda \leq 0$.

4. Translation invariance, and the congruencing idea

Observe that the system of equations

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

has a solution \mathbf{x}, \mathbf{y} if and only if, for any integral shift a , the system of equations

$$\sum_{i=1}^s ((x_i - a)^j - (y_i - a)^j) = 0 \quad (1 \leq j \leq k)$$

is also satisfied

4. Translation invariance, and the congruencing idea

Observe that the system of equations

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

has a solution \mathbf{x}, \mathbf{y} if and only if, for any integral shift a , the system of equations

$$\sum_{i=1}^s ((x_i - a)^j - (y_i - a)^j) = 0 \quad (1 \leq j \leq k)$$

is also satisfied

To see this, note that

$$\sum_{l=1}^j \binom{j}{l} a^{j-l} \sum_{i=1}^s ((x_i - a)^j - (y_i - a)^j) = \sum_{i=1}^s ((x_i - a + a)^j - (y_i - a + a)^j).$$

The mean value

$$\oint |f_a(\alpha; \xi)^{2k} f_b(\alpha; \eta)^{2s}| d\alpha$$

counts (with weights) the number of integral solutions of the system

$$\sum_{i=1}^k (x_i^j - y_i^j) = \sum_{l=1}^s ((p^b u_l + \eta)^j - (p^b v_l + \eta)^j) \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x}, \mathbf{y} \leq X$ and $(1 - \eta)/p^b \leq \mathbf{u}, \mathbf{v} \leq (X - \eta)/p^b$.

The mean value

$$\oint |f_a(\boldsymbol{\alpha}; \xi)^{2k} f_b(\boldsymbol{\alpha}; \eta)^{2s}| d\boldsymbol{\alpha}$$

counts (with weights) the number of integral solutions of the system

$$\sum_{i=1}^k (x_i^j - y_i^j) = \sum_{l=1}^s ((p^b u_l + \eta)^j - (p^b v_l + \eta)^j) \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x}, \mathbf{y} \leq X$ and $(1 - \eta)/p^b \leq \mathbf{u}, \mathbf{v} \leq (X - \eta)/p^b$.

By translation invariance (Binomial Theorem), this system is equivalent to

$$\sum_{i=1}^k ((x_i - \eta)^j - (y_i - \eta)^j) = p^{jb} \sum_{l=1}^s (u_l^j - v_l^j) \quad (1 \leq j \leq k),$$

The mean value

$$\oint |f_a(\alpha; \xi)^{2k} f_b(\alpha; \eta)^{2s}| d\alpha$$

counts (with weights) the number of integral solutions of the system

$$\sum_{i=1}^k (x_i^j - y_i^j) = \sum_{l=1}^s ((p^b u_l + \eta)^j - (p^b v_l + \eta)^j) \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x}, \mathbf{y} \leq X$ and $(1 - \eta)/p^b \leq \mathbf{u}, \mathbf{v} \leq (X - \eta)/p^b$.

By translation invariance (Binomial Theorem), this system is equivalent to

$$\sum_{i=1}^k ((x_i - \eta)^j - (y_i - \eta)^j) = p^{jb} \sum_{l=1}^s (u_l^j - v_l^j) \quad (1 \leq j \leq k),$$

whence

$$\sum_{i=1}^k (x_i - \eta)^j \equiv \sum_{i=1}^k (y_i - \eta)^j \pmod{p^{jb}} \quad (1 \leq j \leq k).$$

The mean value

$$\oint |f_a(\alpha; \xi)^{2k} f_b(\alpha; \eta)^{2s}| d\alpha$$

counts (with weights) the number of integral solutions of the system

$$\sum_{i=1}^k (x_i^j - y_i^j) = \sum_{l=1}^s ((p^b u_l + \eta)^j - (p^b v_l + \eta)^j) \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x}, \mathbf{y} \leq X$ and $(1 - \eta)/p^b \leq \mathbf{u}, \mathbf{v} \leq (X - \eta)/p^b$.

By translation invariance (Binomial Theorem), this system is equivalent to

$$\sum_{i=1}^k ((x_i - \eta)^j - (y_i - \eta)^j) = p^{jb} \sum_{l=1}^s (u_l^j - v_l^j) \quad (1 \leq j \leq k),$$

whence

$$\sum_{i=1}^k (x_i - \eta)^j \equiv \sum_{i=1}^k (y_i - \eta)^j \pmod{p^{jb}} \quad (1 \leq j \leq k).$$

In this way, we obtain a system of congruence conditions modulo p^{jb} for $1 \leq j \leq k$.

$$\sum_{i=1}^k (x_i - \eta)^j \equiv \sum_{i=1}^k (y_i - \eta)^j \pmod{p^{jb}} \quad (1 \leq j \leq k).$$

$$\sum_{i=1}^k (x_i - \eta)^j \equiv \sum_{i=1}^k (y_i - \eta)^j \pmod{p^{jb}} \quad (1 \leq j \leq k).$$

Suppose that \mathbf{x} is *well-conditioned*, by which we mean that x_1, \dots, x_k lie in distinct congruence classes modulo p . Then, given an integral k -tuple \mathbf{n} , the solutions of the system

$$\sum_{i=1}^k (x_i - \eta)^j \equiv n_j \pmod{p} \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x} \leq p$, may be lifted uniquely to solutions of the system

$$\sum_{i=1}^k (x_i - \eta)^j \equiv n_j \pmod{p^{kb}} \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x} \leq p^{kb}$.

$$\sum_{i=1}^k (x_i - \eta)^j \equiv \sum_{i=1}^k (y_i - \eta)^j \pmod{p^{jb}} \quad (1 \leq j \leq k).$$

Suppose that \mathbf{x} is *well-conditioned*, by which we mean that x_1, \dots, x_k lie in distinct congruence classes modulo p . Then, given an integral k -tuple \mathbf{n} , the solutions of the system

$$\sum_{i=1}^k (x_i - \eta)^j \equiv n_j \pmod{p} \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x} \leq p$, may be lifted uniquely to solutions of the system

$$\sum_{i=1}^k (x_i - \eta)^j \equiv n_j \pmod{p^{kb}} \quad (1 \leq j \leq k),$$

with $1 \leq \mathbf{x} \leq p^{kb}$.

In this way, the initial congruences essentially imply that

$$\mathbf{x} \equiv \mathbf{y} \pmod{p^{kb}},$$

provided that we inflate our estimates by $k!p^{\frac{1}{2}k(k-1)b}$

$$x \equiv y \pmod{p^{kb}}$$

$$\mathbf{x} \equiv \mathbf{y} \pmod{p^{kb}}$$

Now we are counting solutions with weights, so we reinsert this congruence information back into the mean value $K_{a,b}(X)$ to obtain the relation

$$K_{a,b}(X) \ll p^{\frac{1}{2}k(k-1)(a+b)} \rho_0(1)^{-4} \sum_{\xi=1}^{p^a} \sum_{\eta=1}^{p^b} \rho_a(\xi)^2 \rho_b(\eta)^2 \Xi,$$

where

$$\Xi = \oint \left(\sum_{\substack{1 \leq \xi' \leq p^{kb} \\ \xi' \equiv \xi \pmod{p^a}}} \frac{\rho_{kb}(\xi')^2}{\rho_a(\xi)^2} |f_{kb}(\alpha; \xi')|^2 \right)^k |f_b(\alpha; \eta)|^{2s} d\alpha.$$

$$\Xi = \int \left(\sum_{\substack{1 \leq \xi' \leq p^{kb} \\ \xi' \equiv \xi \pmod{p^a}}} \frac{\rho_{kb}(\xi')^2}{\rho_a(\xi)^2} |f_{kb}(\alpha; \xi')|^2 \right)^k |f_b(\alpha; \eta)|^{2s} d\alpha.$$

$$\Xi = \oint \left(\sum_{\substack{1 \leq \xi' \leq p^{kb} \\ \xi' \equiv \xi \pmod{p^a}}} \frac{\rho_{kb}(\xi')^2}{\rho_a(\xi)^2} |f_{kb}(\alpha; \xi')|^2 \right)^k |f_b(\alpha; \eta)|^{2s} d\alpha.$$

But by Hölder's inequality, the term here raised to power k is bounded above by

$$\begin{aligned} & \rho_a(\xi)^{-2k} \left(\sum_{\substack{1 \leq \xi' \leq p^{kb} \\ \xi' \equiv \xi \pmod{p^a}}} \rho_{kb}(\xi')^2 |f_{kb}(\alpha; \xi')|^{2s} \right)^{k/s} \left(\sum_{\substack{1 \leq \xi' \leq p^{kb} \\ \xi' \equiv \xi \pmod{p^a}}} \rho_{kb}(\xi')^2 \right)^{k-k/s} \\ & \ll \left(\rho_a(\xi)^{-2} \sum_{\substack{1 \leq \xi' \leq p^{kb} \\ \xi' \equiv \xi \pmod{p^a}}} \rho_{kb}(\xi')^2 |f_{kb}(\alpha; \xi')|^{2s} \right)^{k/s}. \end{aligned}$$

Then another application of Hölder's inequality yields

$$\begin{aligned} \Xi &\ll \int \left(\rho_a(\xi)^{-2} \sum_{\xi'} \rho_{kb}(\xi')^2 |f_{kb}(\alpha; \xi')|^{2s} \right)^{k/s} |f_b(\alpha; \eta)|^{2s} d\alpha \\ &\ll \Xi_1^{k/s} \Xi_2^{1-k/s}, \end{aligned}$$

where

$$\Xi_1 = \rho_a(\xi)^{-2} \sum_{\xi'} \rho_{kb}(\xi')^2 \int |f_b(\alpha; \eta)^{2k} f_{kb}(\alpha; \xi')^{2s}| d\alpha$$

and

$$\Xi_2 = \int |f_b(\alpha; \eta)|^{2s+2k} d\alpha.$$

Recall that

$$K_{a,b}(X) \ll p^{\frac{1}{2}k(k-1)(a+b)} \rho_0(1)^{-4} \sum_{\xi=1}^{p^a} \sum_{\eta=1}^{p^b} \rho_a(\xi)^2 \rho_b(\eta)^2 \Xi,$$

From here, yet another application of Hölder's inequality gives

$$K_{a,b}(X) \ll p^{\frac{1}{2}k(k-1)(a+b)} \Xi_3^{k/s} \Xi_4^{1-k/s},$$

where

$$\Xi_3 = \rho_0(1)^{-4} \sum_{\eta=1}^{p^b} \sum_{\xi'=1}^{p^{kb}} \rho_b(\eta)^2 \rho_{kb}(\xi')^2 \oint |f_b(\alpha; \eta)^{2k} f_{kb}(\alpha; \xi')^{2s}| d\alpha,$$

and

$$\begin{aligned} \Xi_4 &= \rho_0(1)^{-4} \sum_{\eta=1}^{p^b} \sum_{\xi=1}^{p^a} \rho_b(\eta)^2 \rho_a(\xi)^2 \oint |f_b(\alpha; \eta)|^{2s+2k} d\alpha \\ &\ll (X/M^b)^{s+k-\frac{1}{2}k(k+1)+\Lambda+\varepsilon}. \end{aligned}$$

Then one can check that

$$[[K_{a,b}(X)]] \lll [[K_{b,kb}(X)]]^{k/s} (X/M^b)^{(1-k/s)(\Lambda+\varepsilon)}.$$

Given the hypothesis that

$$[[K_{a,b}(X)]] \ggg X^\Lambda (p^\psi)^\Lambda,$$

this implies that

$$[[K_{b,kb}(X)]] \ggg X^\Lambda (p^{\psi'})^\Lambda,$$

where

$$\psi' = (s/k)\psi + (s/k - 1)b,$$

which is a little stronger than we had claimed earlier.

5. Further restriction ideas

Parsell, Prendiville and W., 2013 consider general translation invariant systems (cf. Arkhipov, Karatsuba and Chubarikov, 1980, 2000's). For example, consider the number $J(X)$ of solutions of the system

$$\sum_{i=1}^s x_i^j y_i^m = \sum_{i=s+1}^{2s} x_i^j y_i^m \quad (0 \leq j \leq 3, 0 \leq m \leq 2),$$

with $1 \leq \mathbf{x}, \mathbf{y} \leq X$.

The number of equations is $r = (3 + 1)(2 + 1) - 1 = 11$, the largest total degree is $k = 3 + 2 = 5$, the sum of degrees is

$$K = \frac{1}{2}3(3 + 1) \cdot \frac{1}{2}2(2 + 1) = 18,$$

and the number of variables in a block is 2.

(General) theorem shows that whenever $s > r(k + 1)$, then $J(X) \ll X^{2sd-K}$. Can develop a restriction variant of this work.

Most recent work: the “efficient congruencing” methods apply also to systems that are only approximately translation-invariant. Consider, for example, integers $1 \leq k_1 < k_2 < \dots < k_t$, and the number $T(X)$ of solutions of the system

$$\sum_{i=1}^s (x_i^{k_j} - y_i^{k_j}) = 0 \quad (1 \leq j \leq t),$$

with $1 \leq \mathbf{x}, \mathbf{y} \leq X$. Then (W. 2014) one has

$$T(X) \ll X^{s+\varepsilon},$$

whenever $1 \leq s \leq \frac{1}{2}t(t+1) - (\frac{1}{3} + o(1))t$ (t large).

Again, one can develop a restriction variant of these ideas.

(cf. classical $s \leq t+1$; and Bourgain and Bourgain-Demeter, 2014).