Nested efficient congruencing and (non) translation-dilation invariance

Trevor D. Wooley

ERC Advanced Grant No. 695223, University of Bristol

MSRI Workshop, 2017/05

1. TDI: translation-(dilation)-invariance

TDI systems: What is a *translation-dilation-invariant system*?

1. TDI: translation-(dilation)-invariance

TDI systems: What is a *translation-dilation-invariant system*?

A system of polynomial equations

$$\Phi_i(\mathbf{x}) = 0 \quad (1 \leq i \leq t)$$

with the property that

$$\mathbf{x} \text{ is a solution}$$

if and only if

$$\text{for all } q \in \mathbb{N} \text{ and } a \in \mathbb{Z}, \text{ the tuple } q\mathbf{x} + a \text{ is a solution}$$

1. TDI: translation-(dilation)-invariance

TDI systems: What is a *translation-dilation-invariant system*?

A system of polynomial equations

$$\Phi_i(\mathbf{x}) = 0 \quad (1 \leq i \leq t)$$

with the property that

$$\mathbf{x} \text{ is a solution}$$

if and only if

$$\text{for all } q \in \mathbb{N} \text{ and } a \in \mathbb{Z}, \text{ the tuple } q\mathbf{x} + a \text{ is a solution}$$

For example, the equation

$$x - 2y + z = 0.$$

1. TDI: translation-(dilation)-invariance

TDI systems: What is a *translation-dilation-invariant system*?

A system of polynomial equations

$$\Phi_i(\mathbf{x}) = 0 \quad (1 \leq i \leq t)$$

with the property that

$$\mathbf{x} \text{ is a solution}$$

if and only if

$$\text{for all } q \in \mathbb{N} \text{ and } a \in \mathbb{Z}, \text{ the tuple } q\mathbf{x} + a \text{ is a solution}$$

For example, the equation

$$x - 2y + z = 0.$$

(Need not work over $\mathbb{Z}$, or work with polynomials, or could work with inequalities or congruences instead of equations, or ... or ...).

Another TDI example: the *Vinogradov system of equations*

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

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

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

is also satisfied. This is translation invariance – homogeneity implies dilation invariance.

Another TDI example: the *Vinogradov system of equations*

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

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

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

is also satisfied. This is translation invariance – homogeneity implies dilation invariance.

To see this, note that

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

[Earliest use of TDI in (1) might be Mordell, 1932?]

One can also consider *approximate TDI* systems φ of the shape

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

where $\varphi_j(t)$ is p-adically "close" to t^j, say (or in the world of inequalities over $\mathbb{R}$, "close" in the reals),

One can also consider *approximate TDI* systems φ of the shape

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

where $\varphi_j(t)$ is p-adically "close" to t^j, say (or in the world of inequalities over $\mathbb{R}$, "close" in the reals),

or *TDI families* consisting of sets Φ of systems of polynomials φ with the property that when $\varphi \in \Phi$, then the mapping $\mathbf{x} \mapsto q\mathbf{x} + a$ sends φ to another element of Φ.

[Of course, one can trivially generate TDI families this way, but the idea is useful nonetheless]

2. Vinogradov's mean value theorem $\sim$ 1935

Aim to bound

$$f_k(\boldsymbol{\alpha}; X) = \sum_{1 \le x \le X} e(\alpha_1 x + \ldots + \alpha_k x^k)$$

via estimates for the mean value

$$\begin{aligned} J_{s,k}(X) &= \int_{[0,1)^k} |f_k(\boldsymbol{\alpha}; X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \\ &= \oint f_k(\boldsymbol{\alpha}; X)^s f_k(-\boldsymbol{\alpha}; X)^s \, \mathrm{d}\boldsymbol{\alpha} \\ &= \# \left\{ 1 \le \mathbf{x}, \mathbf{y} \le X \, : \, \sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \quad (1 \le j \le k) \right\}. \end{aligned}$$

This counts the number of integral solutions of a TDI system.

2. Vinogradov's mean value theorem $\sim$ 1935

Aim to bound

$$f_k(\boldsymbol{\alpha}; X) = \sum_{1 \le x \le X} e(\alpha_1 x + \ldots + \alpha_k x^k)$$

via estimates for the mean value

$$\begin{aligned} J_{s,k}(X) &= \int_{[0,1)^k} |f_k(\boldsymbol{\alpha}; X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha} \\ &= \oint f_k(\boldsymbol{\alpha}; X)^s f_k(-\boldsymbol{\alpha}; X)^s \, \mathrm{d}\boldsymbol{\alpha} \\ &= \# \left\{ 1 \le \mathbf{x}, \mathbf{y} \le X \, : \, \sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \quad (1 \le j \le k) \right\}. \end{aligned}$$

This counts the number of integral solutions of a TDI system.

Estimates for $J_{s,k}(X)$ go by the name

"Vinogradov's mean value theorem" (VMVT).

$$J_{s,k}(X) = \int_{[0,1)^k} |f_k(\boldsymbol{\alpha}; X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha}$$
$$= \#\left\{ 1 \le \mathbf{x}, \mathbf{y} \le X \, : \, \sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \quad (1 \le j \le k) \right\}.$$

Have $J_{s,k}(X) \gg X^s + X^{2s - \frac{1}{2}k(k+1)}$.

Conjecture (Main Conjecture in VMVT)

For each $s, k \in \mathbb{N}$ and $\varepsilon > 0$, have $J_{s,k}(X) \ll X^{s+\varepsilon} + X^{2s - \frac{1}{2}k(k+1)}$.

$$J_{s,k}(X) = \int_{[0,1)^k} |f_k(\boldsymbol{\alpha}; X)|^{2s} \, \mathrm{d}\boldsymbol{\alpha}$$
$$= \#\left\{ 1 \le \mathbf{x}, \mathbf{y} \le X \, : \, \sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \quad (1 \le j \le k) \right\}.$$

Have $J_{s,k}(X) \gg X^s + X^{2s - \frac{1}{2}k(k+1)}$.

Conjecture (Main Conjecture in VMVT)

For each $s, k \in \mathbb{N}$ and $\varepsilon > 0$, have $J_{s,k}(X) \ll X^{s+\varepsilon} + X^{2s - \frac{1}{2}k(k+1)}$.

Easy to show: If MC holds for $s = k(k+1)/2$, then it holds for all s.

Conjecture (Strong MC in VMVT)

Suppose $s, k \in \mathbb{N}$ with $k \ge 3$. Then $J_{s,k}(X) \ll X^s + X^{2s - \frac{1}{2}k(k+1)}$.

Conjectures take a different shape in the multidimensional setting.

Theorem (Vinogradov, 1935; Hua, 1949; Karatsuba, 1973)

Suppose that $s, k \in \mathbb{N}$ *and* $s \geq k$. *Then*

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

where $\eta_{s,k} = \frac{1}{2}k^2(1-1/k)^{[s/k]} \leq k^2 e^{-s/k^2}$.

Theorem (Vinogradov, 1935; Hua, 1949; Karatsuba, 1973)

Suppose that $s, k \in \mathbb{N}$ *and* $s \geq k$. *Then*

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

where $\eta_{s,k} = \frac{1}{2}k^2(1-1/k)^{[s/k]} \leq k^2 e^{-s/k^2}$.

- Known in full for $k = 1$ (trivial) and $k = 2$

$$J_{3,2}(X) \sim \frac{18}{\pi^2} X^3 \log X \quad \text{(Rogovskaya, 1986; Blomer and Brüdern, 2010)}$$

- Known for $k \geq 2$ and $1 \leq s \leq k+1$ (Hua, 1947)

$$J_{k+1,k}(X) = (k+1)!X^{k+1} + o(X^{k+1}) \quad \text{(Vaughan and W., 1997)}$$

- Known for $s \geq H(k)$, where $H(3) = 8$, $H(4) = 23$, $H(5) = 55$, ..., and $H(k) = k^2(\log k + 2\log\log k + O(1))$ (Hua, 1947; W. 1992, 1996).

3. Applications

• Waring's problem, especially the asymptotic formula (W., 2012-2016; Bourgain, 2016)

• discrete restriction theory (Bourgain, Demeter, Guth, 2016; W. 2015)

• sum-product theorem (Croot and Hart, 2010)

• Hilbert-Kamke problem (Mit'kin, Arkhipov 1980's)

• counting integral solutions, Hasse Principle, Weak approximation for simultaneous diagonal equations (numerous, including W. 2014)

• solutions of congruences in short intervals (M.-C. Chang, Shparlinski, Zumalacárregui)

• zero-free region for Riemann zeta function (Vinogradov, Korobov, 1958; Ford, 2002)

• geometry of spaces of morphisms from $\mathbb{P}^r(\mathbb{C})$ to a diagonal hypersurface in $\mathbb{P}^s(\mathbb{C})$ (Ellenberg-Venkatesh, Liu and W., 2010's).

4. Efficient congruencing and l^2-decoupling

W., 2010+, Efficient congruencing (EC), a congruence (=p-adic short interval) based method (cf. Linnik, 1942);
Bourgain, Demeter and Guth, 2016, l^2-decoupling, a real short-interval based method (cf. Vinogradov, 1935).

Theorem (MC in VMVT is true)

For each $\varepsilon > 0$,

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

4. Efficient congruencing and l^2-decoupling

W., 2010+, Efficient congruencing (EC), a congruence (=p-adic short interval) based method (cf. Linnik, 1942);
Bourgain, Demeter and Guth, 2016, l^2-decoupling, a real short-interval based method (cf. Vinogradov, 1935).

Theorem (MC in VMVT is true)

For each $\varepsilon > 0$,

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

- Classical for $k = 1, 2$ (classical), due to W. (2014/2016) for $k = 3$ and BDG (2015/2016) for $k \geq 4$.
- (W., 2014/2017) for $1 \leq s \leq \frac{1}{2}k(k+1) - \frac{1}{3}k + O(k^{2/3})$ and for $s \geq k(k-1)$.
- Conjecturally, one should be able to take $\varepsilon = 0$ for $k \geq 3$.

There are numerous generalisations and extensions. For example, let $\varphi_1, \dots, \varphi_k \in \mathbb{Z}[t]$ be polynomials with non-vanishing Wronskian

$$\det \left(\varphi_j^{(i)}(t) \right)_{1 \le i,j \le k},$$

in which $\varphi^{(i)}$ denotes the i-th derivative of φ.

Theorem (Nested EC)

For each $\varepsilon > 0$, whenever $1 \le s \le k(k+1)/2$, one has

$$\int_{[0,1]^k} \Big| \sum_{1 \le x \le X} e(\alpha_1 \varphi_1(x) + \dots + \alpha_k \varphi_k(x)) \Big|^{2s} \mathrm{d}\alpha \ll X^{s+\varepsilon}.$$

Corollary (MC in MVMT)

One has $J_{s,k}(X) \ll X^{s+\varepsilon} + X^{2s-k(k+1)/2}$.

Just take $\varphi_j(t) = t^j$ $(1 \le j \le k)$.
[Note: there is an analogous result with $\phi_j = f(t)/g(t) \in \mathbb{Q}(t)$.]

Nested EC may be applied as a p-adic method for any prime p, including $p = \infty$ (when it runs as a short real interval method). It is no surprise that it therefore applies in the setting of completions of fields more generally:

Example 1 Let K be an algebraic extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$, and let $\mathfrak{O}_K$ denote the ring of integers of K. Also, let $\{\omega_1, \dots, \omega_n\}$ denote an integral coordinate basis of $\mathfrak{O}_K$ over $\mathbb{Z}$.

Define

$$\mathfrak{B}(X) = \{x = a_1\omega_1 + \dots + a_n\omega_n \in \mathfrak{O}_K : a_i \in \mathbb{Z} \cap [-X, X]\}.$$

Finally, let $J_{s,k}(X; K)$ denote the number of $\mathfrak{O}_K$-integral solutions, with $\mathbf{x}, \mathbf{y} \in \mathfrak{B}(X)^s$, of the system

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

Theorem (W., 2017)

One has $J_{s,k}(X; K) \ll (X^n)^{s+\varepsilon} + (X^n)^{2s-k(k+1)/2}$.

Theorem (W., 2017)

One has $J_{s,k}(X;K) \ll (X^n)^{s+\varepsilon} + (X^n)^{2s-k(k+1)/2}$.

Consequence 1: asymptotic formulae for the number of solutions of diagonal equations of the shape

$$a_1 x_1^k + \ldots + a_s x_s^k = 0,$$

with fixed $a_1, \ldots, a_s \in \mathfrak{O}_K$, and $x_i \in \mathfrak{B}(X)$, provided that $s \geq k^2 + k + 1$ (probably even when $s \geq k^2 - k + 3\sqrt{k}$). [cf. Birch, 1962: $s \geq 2^k + 1$]

Consequence 2: main conjecture for infinitely many multidimensional systems given by Weil restriction (just expand relative to the integral coordinate basis). For example, the cubic system built from monomials

$$x^3 - 3xy^2,\ 3x^2y - y^3,\ x^2 - y^2,\ xy,\ x,\ y.$$

Example 2: (Function Fields) Let p be prime and $q = p^l$. When $\mathrm{ch}(\mathbb{F}_q) < k$, the polynomials

$$x_1^j + \cdots + x_s^j \quad (1 \le j \le k)$$

are not all independent, and so the system of equations

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

is not a proper intersection over $\overline{\mathbb{F}_q(t)}$.

Example 2: (Function Fields) Let p be prime and $q = p^l$. When $\mathrm{ch}(\mathbb{F}_q) < k$, the polynomials

$$x_1^j + \cdots + x_s^j \quad (1 \le j \le k)$$

are not all independent, and so the system of equations

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

is not a proper intersection over $\overline{\mathbb{F}_q(t)}$.

Example

When $\mathrm{ch}(\mathbb{F}_q) = 2$, one has

$$x_1^{2\ell} + \cdots + x_s^{2\ell} = (x_1^{\ell} + \cdots + x_s^{\ell})^2,$$

and hence all equations of even degree may be deleted from the Vinogradov system above without altering the solution set.

Example 2: (Function Fields) Let p be prime and $q = p^l$. When $\mathrm{ch}(\mathbb{F}_q) < k$, the polynomials

$$x_1^j + \cdots + x_s^j \quad (1 \le j \le k)$$

are not all independent, and so the system of equations

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

is not a proper intersection over $\overline{\mathbb{F}_q(t)}$.

Example

When $\mathrm{ch}(\mathbb{F}_q) = 2$, one has

$$x_1^{2\ell} + \cdots + x_s^{2\ell} = (x_1^{\ell} + \cdots + x_s^{\ell})^2,$$

and hence all equations of even degree may be deleted from the Vinogradov system above without altering the solution set.

This turns out not to be an obstruction, but in fact assists in obtaining sharper bounds!

Let the base p expansion of k be

$$k = a_0 + a_1 p + \cdots + a_n p^n,$$

with $a_i \in \{0, 1, \ldots, p-1\}$ $(1 \leq i \leq n)$.

Let the base p expansion of k be

$$k = a_0 + a_1 p + \cdots + a_n p^n,$$

with $a_i \in \{0, 1, \ldots, p-1\}$ $(1 \leq i \leq n)$.

Observation

In the binomial expansion of $(x+a)^k$ in a ring of characteristic p, the only terms x^ℓ that appear are those with base p expansion

$$\ell = b_0 + b_1 p + \cdots + b_n p^n,$$

in which $0 \leq b_i \leq a_i$ $(0 \leq i \leq n)$.
[This is a consequence of Lucas' criterion].

Let the base p expansion of k be

$$k = a_0 + a_1 p + \cdots + a_n p^n,$$

with $a_i \in \{0, 1, \ldots, p-1\}$ $(1 \le i \le n)$.

Observation

In the binomial expansion of $(x+a)^k$ in a ring of characteristic p, the only terms x^ℓ that appear are those with base p expansion

$$\ell = b_0 + b_1 p + \cdots + b_n p^n,$$

in which $0 \le b_i \le a_i$ $(0 \le i \le n)$.
[This is a consequence of Lucas' criterion].

So if $1 \le k_u < k_{u-1} < \cdots < k_1 = k$ is the list of such ℓ, then a translation-dilation invariant system is given by

$$\sum_{i=1}^{s} (x_i^{k_j} - y_i^{k_j}) = 0 \quad (1 \le j \le u).$$

Observation

If $p^{\tau_j} \| k_j$, *then on writing*

$$\widetilde{k}_j = k_j p^{-\tau_j} \quad (1 \le j \le u),$$

we have

$$x_1^{k_j} + \cdots + x_s^{k_j} = (x_1^{\widetilde{k}_j} + \cdots + x_s^{\widetilde{k}_j})^{p^{\tau_j}} \quad (1 \le j \le u).$$

Observation

If $p^{\tau_j} \| k_j$, *then on writing*

$$\widetilde{k}_j = k_j p^{-\tau_j} \quad (1 \le j \le u),$$

we have

$$x_1^{k_j} + \cdots + x_s^{k_j} = (x_1^{\widetilde{k}_j} + \cdots + x_s^{\widetilde{k}_j})^{p^{\tau_j}} \quad (1 \le j \le u).$$

Our invariant system, analogous to the classical system

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

now becomes

$$\sum_{i=1}^{s} (x_i^{\widetilde{k}_j} - y_i^{\widetilde{k}_j}) = 0 \quad (1 \le j \le \widetilde{u}).$$

Example

Consider the situation in which $k = 13$ over $\mathbb{F}_8[t]$. Then the characteristic is 2, and one has $k = 2^3 + 2^2 + 1$.

Example

Consider the situation in which $k = 13$ over $\mathbb{F}_8[t]$. Then the characteristic is 2, and one has $k = 2^3 + 2^2 + 1$.

One obtains

$$\{k_1, \dots, k_u\} = \{2^3 + 2^2 + 1, 2^3 + 2^2, 2^3 + 1, 2^3, 2^2 + 1, 2^2, 1\},$$

and hence $\{\widetilde{k}_1, \dots, \widetilde{k}_{\widetilde{u}}\} = \{13, 9, 5, 3, 1\}$.

Example

Consider the situation in which $k = 13$ over $\mathbb{F}_8[t]$. Then the characteristic is 2, and one has $k = 2^3 + 2^2 + 1$.

One obtains

$$\{k_1, \dots, k_u\} = \{2^3 + 2^2 + 1, 2^3 + 2^2, 2^3 + 1, 2^3, 2^2 + 1, 2^2, 1\},$$

and hence $\{\widetilde{k}_1, \dots, \widetilde{k}_{\widetilde{u}}\} = \{13, 9, 5, 3, 1\}$.

Theorem (Yu-Ru Liu and W., 2004-2017)

The number of solutions $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q[t]$ of degree at most d to the system

$$\sum_{i=1}^{s} (x_i^{\widetilde{k}_j} - y_i^{\widetilde{k}_j}) = 0 \quad (1 \le j \le \widetilde{u}),$$

is $\ll (q^{d+1})^{s+\varepsilon} + (q^{d+1})^{2s-\widetilde{k}_1-\dots-\widetilde{k}_{\widetilde{u}}}$.

5. The strategy of basic EC

Write

$$f(\boldsymbol{\alpha}; X) = \sum_{1 \le n \le X} e(n\alpha_1 + \ldots + n^k \alpha_k).$$

We seek to estimate

$$J_{t,k}(X) = \oint |f(\boldsymbol{\alpha}; X)|^{2t} \, \mathrm{d}\boldsymbol{\alpha}.$$

5. The strategy of basic EC

Write

$$f(\boldsymbol{\alpha}; X) = \sum_{1 \le n \le X} e(n\alpha_1 + \ldots + n^k \alpha_k).$$

We seek to estimate

$$J_{t,k}(X) = \oint |f(\boldsymbol{\alpha}; X)|^{2t} \, \mathrm{d}\boldsymbol{\alpha}.$$

Define

$$\lambda_t = \limsup_{X \to \infty} \frac{\log J_{t,k}(X)}{\log X}.$$

5. The strategy of basic EC

Write

$$f(\boldsymbol{\alpha}; X) = \sum_{1 \le n \le X} e(n\alpha_1 + \ldots + n^k \alpha_k).$$

We seek to estimate

$$J_{t,k}(X) = \oint |f(\boldsymbol{\alpha}; X)|^{2t} \, \mathrm{d}\boldsymbol{\alpha}.$$

Define

$$\lambda_t = \limsup_{X \to \infty} \frac{\log J_{t,k}(X)}{\log X}.$$

Then there exists a sequence $(X_m)_{m=1}^{\infty}$ with $\lim_{m \to \infty} X_m = +\infty$ such that for each $\varepsilon > 0$,

$$J_{t,k}(X_m) \gg X^{\lambda_t - \varepsilon},$$

whilst whenever $Y \ge \log X_m$, at the same time one has

$$J_{t,k}(Y) \ll Y^{\lambda_t + \varepsilon}.$$

For this sketch we focus on $t \ge k(k+1)$, and put $s = t - k$.

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

$$\Lambda = \lambda_t - (2t - \tfrac{1}{2}k(k+1)).$$

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

$$\Lambda = \lambda_t - (2t - \tfrac{1}{2}k(k+1)).$$

Idea A: Assume $\Lambda > 0$ and derive a contradiction

This is a testable hypothesis, the contradiction of which proves that $\Lambda \le 0$ for $s \ge k^2$. This implies that

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

for $t = s + k \ge k(k+1)$, thereby confirming MC for $t \ge k(k+1)$.

Approach this problem through an auxiliary mean value. Define

$$\mathfrak{f}_c(\boldsymbol{\alpha}; \xi) = \sum_{\substack{1 \le n \le X \\ n \equiv \xi \ (\mathrm{mod}\ p^c)}} e(n\alpha_1 + \ldots + n^k \alpha_k),$$

and then put

$$K_{a,b}(X) = \max_{\xi,\eta} \oint |\mathfrak{f}_a(\boldsymbol{\alpha}; \xi)^{2k} \mathfrak{f}_b(\boldsymbol{\alpha}; \eta)^{2s}| \, \mathrm{d}\boldsymbol{\alpha}.$$

Here p is an auxiliary prime – think of $p \asymp X^\theta$ with $\theta > 0$ sufficiently small in terms of s and k. But $\varepsilon > 0$ will be still smaller.

One "expects" that

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

and motivated by this observation, we define

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

Strategy:

(i) Show that if $J_{s+k,k}(X) \gg X^{2s+2k-\frac{1}{2}k(k+1)+\Lambda}$, 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 $\psi' = (s/k)\psi + (s/k-1)b, \quad a' = b, \quad b' = kb + h.$

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

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

If $\Lambda > 0$, 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 $\Lambda \leq 0$, as we sought to show.

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

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

If $\Lambda > 0$, 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 $\Lambda \leq 0$, as we sought to show.

One can apply this strategy for different primes p, and also for $p = \infty$ (in which setting congruence classes are otherwise known as real short intervals).

6. Basic EC – some more details

The mean value

$$K_{a,b}(X) = \oint |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2k}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s}|\,\mathrm{d}\boldsymbol{\alpha}$$

counts the number of integral solutions of the system

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

with $1 \le \mathbf{x}, \mathbf{y} \le X$ and $(1-\eta)/p^b \le \mathbf{u}, \mathbf{v} \le (X-\eta)/p^b$ subject to $\mathbf{x} \equiv \mathbf{y} \equiv \xi \pmod{p^a}$.

6. Basic EC – some more details

The mean value

$$K_{a,b}(X) = \oint |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2k}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s}|\,\mathrm{d}\boldsymbol{\alpha}$$

counts the number of integral solutions of the system

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

with $1 \le \mathbf{x}, \mathbf{y} \le X$ and $(1-\eta)/p^b \le \mathbf{u}, \mathbf{v} \le (X-\eta)/p^b$ subject to $\mathbf{x} \equiv \mathbf{y} \equiv \xi \pmod{p^a}$. By TDI, this system is equivalent to

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

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

Thus, we obtain a system of congruence conditions mod p^{jb} $(1 \le j \le k)$.

Suppose that $\mathbf{x}$ is *well-conditioned*, by which we mean that $x_1, \ldots, x_k$ lie in distinct congruence classes modulo p^a. Then, for each fixed choice of $y_1, \ldots, y_k$, there are at most $k! p^{\frac{1}{2}k(k-1)(b+a)}$ solutions of this system of congruences modulo p^{kb} (Hensel's Lemma).

Suppose that $\mathbf{x}$ is *well-conditioned*, by which we mean that $x_1, \dots, x_k$ lie in distinct congruence classes modulo p^a. Then, for each fixed choice of $y_1, \dots, y_k$, there are at most $k! p^{\frac{1}{2}k(k-1)(b+a)}$ solutions of this system of congruences modulo p^{kb} (Hensel's Lemma).
In this way, the initial congruences essentially imply that

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

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

Suppose that $\mathbf{x}$ is *well-conditioned*, by which we mean that $x_1, \dots, x_k$ lie in distinct congruence classes modulo p^a. Then, for each fixed choice of $y_1, \dots, y_k$, there are at most $k! p^{\frac{1}{2}k(k-1)(b+a)}$ solutions of this system of congruences modulo p^{kb} (Hensel's Lemma).
In this way, the initial congruences essentially imply that

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

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

Now reinsert into $K_{a,b}(X)$ to obtain

$$K_{a,b}(X) \ll p^{\frac{1}{2}k(k-1)(a+b)} \max_{\xi,\eta} \Xi,$$

where

$$\Xi = \oint \Bigg(\sum_{\substack{1 \le \xi' \le p^{kb} \\ \xi' \equiv \xi \pmod{p^a}}} |\mathfrak{f}_{kb}(\boldsymbol{\alpha}; \xi')|^2 \Bigg)^k |\mathfrak{f}_b(\boldsymbol{\alpha}; \eta)|^{2s} \, \mathrm{d}\boldsymbol{\alpha}$$

$$\ll (p^{kb-a})^k \max_{\xi'} \oint |\mathfrak{f}_{kb}(\boldsymbol{\alpha}; \xi')^{2k} \mathfrak{f}_b(\boldsymbol{\alpha}; \eta)^{2s}| \, \mathrm{d}\boldsymbol{\alpha}.$$

Idea B: Now apply Hölder's inequality to reverse roles:

$$K_{a,b}(X) \ll p^{\frac{1}{2}k(k-1)(a+b)+k(kb-a)} \Xi_1^{k/s} \Xi_2^{1-k/s},$$

where

$$\Xi_1 = \max_{\xi,\eta} \oint |\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2k} \mathfrak{f}_{kb}(\boldsymbol{\alpha};\xi')^{2s}| \, \mathrm{d}\boldsymbol{\alpha} = K_{b,kb}(X),$$

and (by TDI)

$$\Xi_2 = \oint |\mathfrak{f}_b(\boldsymbol{\alpha};\eta)|^{2s+2k} \, \mathrm{d}\boldsymbol{\alpha} \ll J_{s+k,k}(X/p^b) \ll (X/p^b)^{2s+2k-\frac{1}{2}k(k+1)+\Lambda+\varepsilon}.$$

Idea B: Now apply Hölder's inequality to reverse roles:

$$K_{a,b}(X) \ll p^{\frac{1}{2}k(k-1)(a+b)+k(kb-a)} \Xi_1^{k/s} \Xi_2^{1-k/s},$$

where

$$\Xi_1 = \max_{\xi,\eta} \oint |\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2k} \mathfrak{f}_{kb}(\boldsymbol{\alpha};\xi')^{2s}| \, \mathrm{d}\boldsymbol{\alpha} = K_{b,kb}(X),$$

and (by TDI)

$$\Xi_2 = \oint |\mathfrak{f}_b(\boldsymbol{\alpha};\eta)|^{2s+2k} \, \mathrm{d}\boldsymbol{\alpha} \ll J_{s+k,k}(X/p^b) \ll (X/p^b)^{2s+2k-\frac{1}{2}k(k+1)+\Lambda+\varepsilon}.$$

Then one can check that

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

Idea B: Now apply Hölder's inequality to reverse roles:

$$K_{a,b}(X) \ll p^{\frac{1}{2}k(k-1)(a+b)+k(kb-a)} \Xi_1^{k/s} \Xi_2^{1-k/s},$$

where

$$\Xi_1 = \max_{\xi,\eta} \oint |\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2k} \mathfrak{f}_{kb}(\boldsymbol{\alpha};\xi')^{2s}| \, \mathrm{d}\boldsymbol{\alpha} = K_{b,kb}(X),$$

and (by TDI)

$$\Xi_2 = \oint |\mathfrak{f}_b(\boldsymbol{\alpha};\eta)|^{2s+2k} \, \mathrm{d}\boldsymbol{\alpha} \ll J_{s+k,k}(X/p^b) \ll (X/p^b)^{2s+2k-\frac{1}{2}k(k+1)+\Lambda+\varepsilon}.$$

Then one can check that

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

So

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

where

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

which is a little stronger than we had claimed earlier.

7. Multigrade EC

Consider r with $1 \le r \le \kappa < k$. The mean value

$$K_{a,b}^{r}(X) = \oint |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2r}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s}|\,\mathrm{d}\boldsymbol{\alpha},$$

with $s = t - r$, counts the number of integral solutions of the system

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

with $1 \le \mathbf{x}, \mathbf{y} \le X$ and $(1-\eta)/p^b \le \mathbf{u}, \mathbf{v} \le (X-\eta)/p^b$ satisfying $\mathbf{x} \equiv \mathbf{y} \equiv \xi \pmod{p^a}$.

7. Multigrade EC

Consider r with $1 \le r \le \kappa < k$. The mean value

$$K_{a,b}^{r}(X) = \oint |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{2r}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{2s}|\,\mathrm{d}\boldsymbol{\alpha},$$

with $s = t - r$, counts the number of integral solutions of the system

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

with $1 \le \mathbf{x}, \mathbf{y} \le X$ and $(1-\eta)/p^b \le \mathbf{u}, \mathbf{v} \le (X-\eta)/p^b$ satisfying $\mathbf{x} \equiv \mathbf{y} \equiv \xi \pmod{p^a}$.

By TDI, we obtain

$$\sum_{i=1}^{r}((x_i - \eta)^j - (y_i - \eta)^j) \equiv 0 \pmod{p^{jb}} \quad (k - r + 1 \le j \le k),$$

whence with $m = k - r + 1$ we have

$$\sum_{i=1}^{r}((x_i - \eta)^j - (y_i - \eta)^j) \equiv 0 \pmod{p^{mb}} \quad (k - r + 1 \le j \le k).$$

Put $x_i = p^a w_i + \xi$ and $y_i = p^a z_i + \xi$. Then by linear algebra, we obtain

$$\sum_{i=1}^{r} (p^a w_i)^j + O_{\mathbf{w}}(p^{(r+1)a}) \equiv \sum_{i=1}^{r} (p^a z_i)^j + O_{\mathbf{z}}(p^{(r+1)a}) \pmod{p^{mb}} \quad (1 \le j \le r)$$

Put $x_i = p^a w_i + \xi$ and $y_i = p^a z_i + \xi$. Then by linear algebra, we obtain

$$\sum_{i=1}^{r} (p^a w_i)^j + O_{\mathbf{w}}(p^{(r+1)a}) \equiv \sum_{i=1}^{r} (p^a z_i)^j + O_{\mathbf{z}}(p^{(r+1)a}) \pmod{p^{mb}} \quad (1 \le j \le r)$$

Suppose that $\mathbf{x}$ is *well-conditioned*, by which we mean that $x_1, \dots, x_r$ lie in distinct congruence classes modulo p^{a+1}. Then, for each fixed choice of $\mathbf{z}$, there are $O(1)$ possible solutions $\mathbf{w}$ modulo p^{mb-ra}.

Put $x_i = p^a w_i + \xi$ and $y_i = p^a z_i + \xi$. Then by linear algebra, we obtain

$$\sum_{i=1}^{r} (p^a w_i)^j + O_{\mathbf{w}}(p^{(r+1)a}) \equiv \sum_{i=1}^{r} (p^a z_i)^j + O_{\mathbf{z}}(p^{(r+1)a}) \pmod{p^{mb}} \quad (1 \le j \le r)$$

Suppose that $\mathbf{x}$ is *well-conditioned*, by which we mean that $x_1, \dots, x_r$ lie in distinct congruence classes modulo p^{a+1}. Then, for each fixed choice of $\mathbf{z}$, there are $O(1)$ possible solutions $\mathbf{w}$ modulo p^{mb-ra}.

This implies that we may impose the condition

$$\mathbf{x} \equiv \mathbf{y} \pmod{p^{(k-r+1)b-(r-1)a}}$$

within the mean value at essentially no cost.

Put $x_i = p^a w_i + \xi$ and $y_i = p^a z_i + \xi$. Then by linear algebra, we obtain

$$\sum_{i=1}^{r} (p^a w_i)^j + O_{\mathbf{w}}(p^{(r+1)a}) \equiv \sum_{i=1}^{r} (p^a z_i)^j + O_{\mathbf{z}}(p^{(r+1)a}) \pmod{p^{mb}} \quad (1 \le j \le r)$$

Suppose that $\mathbf{x}$ is *well-conditioned*, by which we mean that $x_1, \dots, x_r$ lie in distinct congruence classes modulo p^{a+1}. Then, for each fixed choice of $\mathbf{z}$, there are $O(1)$ possible solutions $\mathbf{w}$ modulo p^{mb-ra}.

This implies that we may impose the condition

$$\mathbf{x} \equiv \mathbf{y} \pmod{p^{(k-r+1)b-(r-1)a}}$$

within the mean value at essentially no cost. Inserting this congruence information back into $K^r_{a,b}(X)$, we obtain

$$K^r_{a,b}(X) \ll \oint \Bigg(\sum_{\substack{1 \le \xi' \le p^{(k-r+1)b-(r-1)a} \\ \xi' \equiv \xi \pmod{p^a}}} |\mathfrak{f}_{(k-r+1)b-(r-1)a}(\boldsymbol{\alpha}; \xi')|^2 \Bigg)^r |\mathfrak{f}_b(\boldsymbol{\alpha}; \eta)|^{2s} \, \mathrm{d}\boldsymbol{\alpha}$$

$$\ll (p^{(k-r+1)b-ra})^k \max_{\xi'} \oint |\mathfrak{f}_{(k-r+1)b-(r-1)a}(\boldsymbol{\alpha}; \xi')^{2r} \mathfrak{f}_b(\boldsymbol{\alpha}; \eta)^{2s}| \, \mathrm{d}\boldsymbol{\alpha}$$

Idea B: Now apply Hölder's inequality to reverse roles:

$$[[K^r_{a,b}(X)]] \ll [[K^{r-1}_{a,b}(X)]]^{\frac{\kappa-r-2}{\kappa-r-1}} [[K^{\kappa}_{b,(k-r+1)b-(r-1)a}(X)]]^{\frac{1}{\kappa-r-1}}.$$

Idea B: Now apply Hölder's inequality to reverse roles:

$$[[K^r_{a,b}(X)]] \ll [[K^{r-1}_{a,b}(X)]]^{\frac{\kappa-r-2}{\kappa-r-1}} [[K^{\kappa}_{b,(k-r+1)b-(r-1)a}(X)]]^{\frac{1}{\kappa-r-1}}.$$

Note: We need $(k-r+1)b-(r-1)a > 0$ for this to be valid, so this limits how large we may take r to be, without cunning schemes to circumvent this restriction.

Idea B: Now apply Hölder's inequality to reverse roles:

$$[[K^r_{a,b}(X)]] \ll [[K^{r-1}_{a,b}(X)]]^{\frac{\kappa-r-2}{\kappa-r-1}} [[K^{\kappa}_{b,(k-r+1)b-(r-1)a}(X)]]^{\frac{1}{\kappa-r-1}}.$$

Note: We need $(k-r+1)b-(r-1)a > 0$ for this to be valid, so this limits how large we may take r to be, without cunning schemes to circumvent this restriction.

In general, obtain

$$[[K^r_{a,b}]] \ll (X/p^b)^{\Lambda(1-r/s)} \prod_{m=0}^{r-1} [[K^r_{b,(k-m)b-ma}]]^{\frac{s-r}{(s-m)(s-m-1)}},$$

and one has to figure out how much, "on average", the parameter b increases relative to the average exponent r/s. For example, when $k=3$ we obtain an equation relating these averages

$$B_{n+1} = \frac{1}{3}(2B_n - A_n) + \frac{1}{6}(3B_n) \quad \text{and} \quad A_{n+1} = \left(\frac{1}{3}+\frac{1}{6}\right) A_n,$$

with characteristic roots 1 and $\frac{1}{6}$. It is crucial here that one of these roots is at least 1.

8. Nested EC and MC in VMVT

The MEC method establishes the MC in VMVT for $J_{s,k}(X)$ when $k = 3$ and when $k \geq 4$ and $1 \leq s \leq k(k+1)/2 - k/3 + o(k)$. Drawing inspiration from an idea in l^2-decoupling, one can cover the gap of $k/3$ to recover the main conjecture.

8. Nested EC and MC in VMVT

The MEC method establishes the MC in VMVT for $J_{s,k}(X)$ when $k = 3$ and when $k \geq 4$ and $1 \leq s \leq k(k+1)/2 - k/3 + o(k)$. Drawing inspiration from an idea in l^2-decoupling, one can cover the gap of $k/3$ to recover the main conjecture.

The main idea is to observe that the p-adic concentration argument works just as well when the equations previously considered are replaced by congruences modulo p^B, with B large.

8. Nested EC and MC in VMVT

The MEC method establishes the MC in VMVT for $J_{s,k}(X)$ when $k = 3$ and when $k \geq 4$ and $1 \leq s \leq k(k+1)/2 - k/3 + o(k)$. Drawing inspiration from an idea in l^2-decoupling, one can cover the gap of $k/3$ to recover the main conjecture.

The main idea is to observe that the p-adic concentration argument works just as well when the equations previously considered are replaced by congruences modulo p^B, with B large.

Consider $\phi_1, \ldots, \phi_k \in \mathbb{Z}[t]$, complex numbers $\mathfrak{a}_n$ not all zero, and for large N define

$$f_{\mathfrak{a}}(\boldsymbol{\alpha}; N) = N^{-1/2} \sum_{1 \leq x \leq N} \mathfrak{a}_n e(\psi(n; \boldsymbol{\alpha})),$$

where $\psi(n; \boldsymbol{\alpha}) = \alpha_1 \phi_1(n) + \ldots + \alpha_k \phi_k(n)$.

The mean value

$$U_s^B(N;\mathfrak{a}) = \oint_{p^B} |f_{\mathfrak{a}}(\boldsymbol{\alpha};N)|^{2s}\,\mathrm{d}\boldsymbol{\alpha} = p^{-kB}\sum_{u_1=1}^{p^B}\cdots\sum_{u_k=1}^{P^B}|f_{\mathfrak{a}}(\mathbf{u}p^{-B};N)|^{2s}$$

counts solutions of the system of congruences

$$\sum_{i=1}^{s}(\phi_j(x_i)-\phi_j(y_i)) \equiv 0 \pmod{p^B},$$

with $1 \le \mathbf{x},\mathbf{y} \le N$, with each solution being counted with weight

$$N^{-s}\prod_{i=1}^{s}\mathfrak{a}_{x_i}\overline{\mathfrak{a}}_{y_i}.$$

We are interested in arithmetic progressions modulo p^h, say, so define

$$\mathfrak{f}_h(\boldsymbol{\alpha};\xi) = (N/p^h)^{-1/2} \sum_{\substack{1\le n\le N\\ n\equiv\xi \pmod{p^h}}} \mathfrak{a}_n e(\psi(n;\boldsymbol{\alpha}))$$

and

$$U_s^{B,h}(N;\xi) = \oint_{p^B} |\mathfrak{f}_h(\boldsymbol{\alpha};\xi)|^{2s}\,\mathrm{d}\boldsymbol{\alpha},$$

$$U_s^{B,h}(N) = p^{-h} \sum_{1\le\xi\le p^h} U_s^{B,h}(N;\xi).$$

We are interested in arithmetic progressions modulo p^h, say, so define

$$\mathfrak{f}_h(\boldsymbol{\alpha};\xi) = (N/p^h)^{-1/2} \sum_{\substack{1\le n\le N\\ n\equiv\xi \pmod{p^h}}} \mathfrak{a}_n e(\psi(n;\boldsymbol{\alpha}))$$

and

$$U_s^{B,h}(N;\xi) = \oint_{p^B} |\mathfrak{f}_h(\boldsymbol{\alpha};\xi)|^{2s}\,\mathrm{d}\boldsymbol{\alpha},$$

$$U_s^{B,h}(N) = p^{-h} \sum_{1\le\xi\le p^h} U_s^{B,h}(N;\xi).$$

Definition: We say that ϕ is a p^c-spaced system of polynomials when $\phi_j(t) \equiv t^j \pmod{p^c}$ $(1 \le j \le k)$ as polynomials.

This is easy to arrange for systems of polynomials with non-vanishing Wronskian (i.e. sufficiently independent).

Big definition – when $\theta \geq 1$, put $H = \lceil B/\theta \rceil$ and define

$$\lambda_s(\theta) = \limsup_{\tau \to 0} \limsup_{B \to \infty} \limsup_{N \to \infty} \sup_{\phi \in \Phi_\tau(B)} \sup_{\mathfrak{a}_n} \frac{\log(U_s^B(N)/U_s^{B,H}(N))}{\log(p^H)},$$

in which $\Phi_\tau(B)$ denotes the set of p^c-spaced polynomials with $c \geq \tau B$.

Big definition – when $\theta \geq 1$, put $H = \lceil B/\theta \rceil$ and define

$$\lambda_s(\theta) = \limsup_{\tau \to 0} \limsup_{B \to \infty} \limsup_{N \to \infty} \sup_{\phi \in \Phi_\tau(B)} \sup_{\mathfrak{a}_n} \frac{\log(U_s^B(N)/U_s^{B,H}(N))}{\log(p^H)},$$

in which $\Phi_\tau(B)$ denotes the set of p^c-spaced polynomials with $c \geq \tau B$.

Note that Hölder's inequality yields

$$|f_{\mathfrak{a}}(\boldsymbol{\alpha}; N)|^{2s} \leq p^{(s-1)H} \sum_{1 \leq \xi \leq p^H} |\mathfrak{f}_H(\boldsymbol{\alpha}; \xi)|^{2s}$$

whence

$$U_s^B(N) \leq p^{sH} U_s^{B,H}(N),$$

from which we see that $\lambda_s(\theta) \leq s$.

Theorem

Let $k \in \mathbb{N}$ and suppose that p is a prime number with $p > k$. Then whenever $k(k-1)/2 < s \leq k(k+1)/2$, one has $\lambda_s(k) = 0$.

Theorem

Let $k \in \mathbb{N}$ and suppose that p is a prime number with $p > k$. Then whenever $k(k-1)/2 < s \leq k(k+1)/2$, one has $\lambda_s(k) = 0$.

Corollary

Suppose that B is sufficiently large in terms of s, k, τ, ε. Then for every p^c-spaced k-tuple of polynomials ϕ with $c \geq \tau B$, and every $(\mathfrak{a}_n)$, one has

$$U_s^{B,H}(N) \ll p^{B\varepsilon} U_s^{B,H}(N) \quad \text{with} \quad H = \lceil B/k \rceil.$$

A corollary of this statement is the main conjecture in VMVT (just take B large enough that $p^{B/k} > N$).

Effectively, what this statement says is that these systems of congruences modulo p^B are equipped almost for free with the property that solutions are pushed towards the diagonal modulo $p^{B/k}$ whenever $s \leq k(k+1)/2$ — a weak version of Hensel's lemma, but spread over many variables.

A sketch of ideas underlying nested EC

Proceed inductively, assuming that the main theorem has been proved for smaller systems. Define

$$K^r_{a,b}(N;\xi,\eta) = \oint_{p^B} |\mathfrak{f}_a(\boldsymbol{\alpha};\xi)^{r(r+1)}\mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{k(k+1)-r(r+1)}|\,\mathrm{d}\boldsymbol{\alpha}$$

and

$$K^r_{a,b} = p^{-a}\sum_{1\le\xi\le p^a} p^{-b} \sum_{\substack{1\le\eta\le p^b\\ \eta\not\equiv\xi \pmod p}} K^r_{a,b}(N,\xi,\eta).$$

Also, define

$$[[K^r_{a,b}]] = \left(K^r_{a,b}/U_s^{B,H}(N)\right)^{\frac{k-1}{r(k-r)}}.$$

Using TDI, the mean value $K^r_{a,b}(N;\xi,\eta)$ is essentially equivalent to $K^r_{a,b}(N;\xi-\eta,0)$, and this implies a congruence condition on the first $r(r+1)$ variables:

$$\sum_{i=1}^{r(r+1)/2} (x_i^j - y_i^j) + O(p^c) \equiv 0 \pmod{(p^{jb}, p^B)} \quad (1 \le j \le k).$$

Using TDI, the mean value $K^r_{a,b}(N;\xi,\eta)$ is essentially equivalent to $K^r_{a,b}(N;\xi-\eta,0)$, and this implies a congruence condition on the first $r(r+1)$ variables:

$$\sum_{i=1}^{r(r+1)/2} (x_i^j - y_i^j) + O(p^c) \equiv 0 \pmod{(p^{jb}, p^B)} \quad (1 \le j \le k).$$

Restricting to $k-r+1 \le j \le k$, as in MEC, we may use the inductive hypothesis for systems of r equations in $r(r+1)/2$ pairs of variables to see that the congruence condition modulo $p^{(k-r+1)b}$ on the system forces variables to be in a common congruence class ζ modulo $p^{b'}$ (in an average sense), where

$$b' = (k-r+1)b/r.$$

Using TDI, the mean value $K^r_{a,b}(N;\xi,\eta)$ is essentially equivalent to $K^r_{a,b}(N;\xi-\eta,0)$, and this implies a congruence condition on the first $r(r+1)$ variables:

$$\sum_{i=1}^{r(r+1)/2} (x_i^j - y_i^j) + O(p^c) \equiv 0 \pmod{(p^{jb}, p^B)} \quad (1 \le j \le k).$$

Restricting to $k-r+1 \le j \le k$, as in MEC, we may use the inductive hypothesis for systems of r equations in $r(r+1)/2$ pairs of variables to see that the congruence condition modulo $p^{(k-r+1)b}$ on the system forces variables to be in a common congruence class ζ modulo $p^{b'}$ (in an average sense), where

$$b' = (k-r+1)b/r.$$

Thus

$$K^r_{a,b} \ll p^{b\varepsilon} \oint_{p^B} |\mathfrak{f}_{b'}(\boldsymbol{\alpha};\zeta)^{r(r+1)} \mathfrak{f}_b(\boldsymbol{\alpha};\eta)^{k(k+1)-r(r+1)}| \, \mathrm{d}\boldsymbol{\alpha}.$$

Now apply Hölder's inequality to reverse the roles of the variables. Normalising, we obtain

$$[[K_{a,b}^r]] \ll p^{b\varepsilon}[[K_{b',b}^{r-1}(N)]]^{1-1/r}\left([[K_{b,b'}^{k-r}]]^{r/(k-r+1)}\right)^{1/r},$$

with $b' = \lceil (k-r+1)b/r \rceil$ and in particular

$$(b'/b)(r/(k-r+1)) \geq 1.$$

Now apply Hölder's inequality to reverse the roles of the variables. Normalising, we obtain

$$[[K_{a,b}^r]] \ll p^{b\varepsilon}[[K_{b',b}^{r-1}(N)]]^{1-1/r}\left([[K_{b,b'}^{k-r}]]^{r/(k-r+1)}\right)^{1/r},$$

with $b' = \lceil (k-r+1)b/r \rceil$ and in particular

$$(b'/b)(r/(k-r+1)) \geq 1.$$

These relations can be glued together in much the same way as in MEC, and the last inequality ensures that we obtain an explosive p-adic concentration argument.
In brief, we assume that

$$U_s^B(N) > (p^H)^\Lambda U_s^{B,H}(N),$$

with $H = \lceil B/k \rceil$ and $\Lambda > 0$, and we derive a contradiction to show that $\Lambda \leq 0$.

This contradiction arises by showing that if

$$[[K_{a,b}^{r}]] \gg (p^{\psi})^{\wedge}(p^{H})^{\wedge},$$

for some $\psi > 0$, then there are a', b', r', ψ' with

$$[[K_{a',b'}^{r'}]] \gg (p^{\psi'})^{\wedge}(p^{H})^{\wedge},$$

with ψ' growing rather more rapidly than b' (in fact $\psi' \geq nb'$ after n steps). By iterating as before, we derive a contradiction against a trivial estimate.

9. Beyond EC/decoupling?

What about the Big TOE (Big Theory Of Everything)? Given a system of t equations

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

with $W(\varphi) \neq 0$, can one establish diagonal behaviour with s beyond the EC/decoupling limit $t(t+1)/2$?

9. Beyond EC/decoupling?

What about the Big TOE (Big Theory Of Everything)? Given a system of t equations

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

with $W(\varphi) \neq 0$, can one establish diagonal behaviour with s beyond the EC/decoupling limit $t(t+1)/2$?

Theorem (Salberger and W., 2010)

Let $k_1, \dots, k_t$ be integers with $1 \le k_1 < k_2 < \dots < k_t$, and denote by $S_s(X; \mathbf{k})$ the number of integral solutions of the system

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

with $1 \le \mathbf{x}, \mathbf{y} \le X$. Then provided that $k_1 \dots k_t \ge (2s-t)^{4s-2t}$, one has

$$S_s(X; \mathbf{k}) \sim s! X^s.$$

Let $L_{s,k}(X)$ denote the number of integral solutions of the system of equations

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \quad (2 \le j \le k),$$

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

Theorem (Brandes und W., 2017)

Suppose that $1 \le s \le (k^2-1)/2$. *Then*

$$L_{s,k}(X) \ll X^{s+\varepsilon}.$$

Note that $(k^2-1)/2$ is roughly half way between the EC/decoupling limit $k(k-1)/2$ and the bound indicated by the Main Conjecture for this problem of $(k^2+k-2)/2$.

Let $L_{s,k}(X)$ denote the number of integral solutions of the system of equations

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \quad (2 \le j \le k),$$

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

Theorem (Brandes und W., 2017)

Suppose that $1 \le s \le (k^2-1)/2$. *Then*

$$L_{s,k}(X) \ll X^{s+\varepsilon}.$$

Note that $(k^2-1)/2$ is roughly half way between the EC/decoupling limit $k(k-1)/2$ and the bound indicated by the Main Conjecture for this problem of $(k^2+k-2)/2$.

FIN!