Extracting decoupling estimates from number theory

Zane Li (North Carolina State University)

May 29, 2024

Vinogradov's Mean Value Theorem

Let $J_{s,k}(X)$ be the number of $2s$-tuples to the system

$$x_1 + x_2 + \cdots + x_s = y_1 + y_2 + \cdots + y_s$$
$$x_1^2 + x_2^2 + \cdots + x_s^2 = y_1^2 + y_2^2 + \cdots + y_s^2$$
$$\vdots$$
$$x_1^k + x_2^k + \cdots + x_s^k = y_1^k + y_2^k + \cdots + y_s^k$$

where $1 \leqslant x_i, y_i \leqslant X$. Lower bound: $\gtrsim_{s,k} X^s + X^{2s-k(k+1)/2}$

VMVT: $J_{s,k}(X) \lesssim_{s,k,\varepsilon} X^{\varepsilon}(X^s + X^{2s-k(k+1)/2})$.

Let $e(a) := e^{2\pi i a}$. Then

$$J_{s,k}(X) = \int_{[0,1]^k} \Big| \sum_{1 \leqslant n \leqslant X} e(\alpha_1 n + \alpha_2 n^2 + \cdots + \alpha_k n^k) \Big|^{2s} d\alpha.$$

For each k, from Hölder, if we know $s = k(k+1)/2$ then we know all $J_{s,k}(X)$ estimates for that particular k.

A brief history

Brief history (to be expanded upon later):

- $k = 2$ case is classical
- $k = 3$ case proven by Wooley in 2014 using efficient congruencing
- $k \geqslant 2$ case proven by Bourgain-Demeter-Guth in 2015 as a corollary of decoupling for the moment curve $\xi \mapsto (\xi, \xi^2, \ldots, \xi^k)$
- $k \geqslant 2$ case proven by Wooley in 2017 using efficient congruencing

Moment curve decoupling (Bourgain-Demeter-Guth): Partition $[0,1]$ into intervals I of length δ. Let f_I be defined such that $\widehat{f_I} := \widehat{f} 1_{I \times \mathbb{R}^{k-1}}$. Then for $p \geqslant 2$,

$$\|f\|_{L^p} \lesssim_\varepsilon \delta^{-\varepsilon}(1 + \delta^{-(\frac{1}{2} - \frac{k(k+1)}{2p})})(\sum_{I \subset [0,1] : |I| = \delta} \|f_I\|_{L^p}^2)^{1/2}$$

for all f with $\text{supp}(\widehat{f})$ contained in a δ^k neighborhood of $\{(\xi, \xi^2, \ldots, \xi^k) : \xi \in [0,1]\}$.

Numerology: p in decoupling is $2s$ in VMVT.

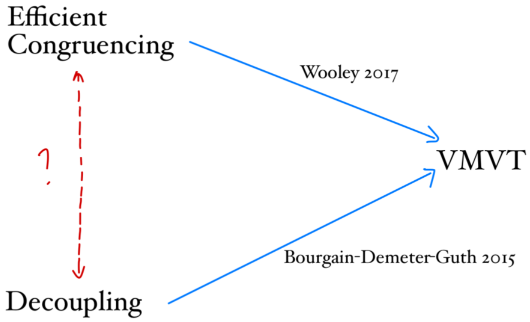
A more detailed VMVT history

Classical theory: $k = 2$ case and mid-1970s: $s \gtrsim k^2 \log k$ (Karatsuba, Stechkin)

Efficient congruencing:

- **Jan 2011, Wooley:** $s \geqslant k(k+1)$
- Dec 2011, Wooley: $s \geqslant k^2 - 1$
- **May 2012, Parsell-Prendiville-Wooley: generalization to analogue of VMVT for arbitrary TDI systems**
- Apr 2013, Ford-Wooley: $s \leqslant \frac{1}{4}(k+1)^2$
- Oct 2013, Wooley: $s \geqslant k^2 - k + 1$
- **Jan 2014, Wooley:** $s \leqslant \frac{1}{2}k(k+1) - \frac{1}{3}k + o(k)$ **and critical** $k = 3$
- Aug 2015, Wooley: efficient congruencing generalized to discrete restriction
- (Dec 2015, Bourgain-Demeter-Guth: VMVT proven using decoupling)
- **Aug 2017, Wooley: VMVT using nested efficient congruencing**

Motivation 1 for studying efficient congruencing



1. Reinterpreting Wooley's nested efficient congruencing led to a much shorter/technically simpler proof of moment curve decoupling (Guo-L.-Yung-Zorin-Kranich)

But nested efficient congruencing is somewhat the closest efficient congruencing argument to decoupling. Older arguments make use of much more number theory (solution counting).

Motivation 2

2. Prendiville-Parsell-Wooley: Consider a system of real homogeneous polynomials $(G_1, \ldots, G_s)$ depending on d variables $(\xi_1, \ldots, \xi_d)$. Define a set of polynomials

$$\mathscr{F} := \{\frac{\partial^{l_1+\cdots+l_d} G_j}{\partial \xi_1^{l_1} \ldots \partial \xi_d^{l_d}} : l_i \geqslant 0, 1 \leqslant i \leqslant d\}$$

Let $\mathscr{F}_0$ denote the subset of $\mathscr{F}$ consisting of all polynomials of positive degree. Let $\{F_1, \ldots, F_r\}$ be a maximal linearly independent subset of $\mathscr{F}_0$. Then the system $\mathbf{F} := (F_1, \ldots, F_r)$ is called a translation-dilation invariant (TDI) system. (Example: Take $G = \xi^k$, this gives VMVT.)

PPW proved the sharp multidimensional analogue of VMVT for $\mathbf{F}$ for s sufficiently large (depending on $\mathbf{F}$).

There is no decoupling estimate at the moment in the literature that would imply this result.

Today's goal

The argument in PPW is similar to the argument made by Wooley in 2011 which in turn is a much more refined version of the "classical argument". This interpretation is due to Cook-Hughes-L.-Mudgal-Robert-Yung.

Concentrate on a refinement of an argument by Karatsuba made in 1973. He proved that for $s \in k\mathbb{N}$, then

$$J_{s,k}(X) \lesssim_{s,k} X^{2s-k(k+1)/2+\frac{1}{2}\mathbf{k}^2(\mathbf{1}-\mathbf{1}/\mathbf{k})^{\mathbf{s}/\mathbf{k}}}.$$

Compare to

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

for $s \geqslant k(k+1)/2$.

With k fixed, think of as: "Vinogradov is true for large s"

We concentrate on the $k = 2$ case for simplicity. Let $J_s(X) := J_{s,2}(X)$.

What would decoupling look like if it was proven using 1970s VMVT technology?

Basic observations

Observation 1: The system

$$n_1 + n_2 + \cdots + n_s = m_1 + m_2 + \cdots + m_s$$
$$n_1^2 + n_2^2 + \cdots + n_s^2 = m_1^2 + m_2^2 + \cdots + m_s^2$$

is translation and dilation invariant.

Observation 2: Number of solutions with $1 \leqslant n_i, m_i \leqslant X$ with $n_i, m_i \equiv A \pmod{p^b}$ (and $p^b \leqslant X$) is $J_s(X/p^b)$.

Observation 3: The number of solutions to

$$n_1 + n_2 + \cdots + n_s = m_1 + m_2 + \cdots + m_s + H_1$$
$$n_1^2 + n_2^2 + \cdots + n_s^2 = m_1^2 + m_2^2 + \cdots + m_s^2 + H_2$$

with $1 \leqslant n_i, m_i \leqslant X$ is $\leqslant J_s(X)$. This is because it is equal to $\int_{[0,1]^2} |\sum_{n=1}^{X} e(nx + n^2 t)|^{2s} e(-H_1 x - H_2 t)\, dx\, dt$.

Observation 4: If I impose an additional constraint that $n_i, m_i \equiv A \pmod{p^b}$ then the number of solutions is $\leqslant J_s(X/p^b)$.

Reduction to the multilinear piece

Let p be a prime chosen so that $1 \ll p \ll X$. Choose $p = X^{1/2}$ later.

$$
\begin{aligned}
J_s(X) &= \int_{[0,1]^2} \Big|\sum_{n=1}^{X} e(nx + n^2 t)\Big|^{2s} \, dx\, dt \\
&= \int_{[0,1]^2} \Big|\sum_{n=1}^{X} e(\cdots)\Big|^4 \Big|\sum_{n=1}^{X} e(\cdots)\Big|^{2s-4} \\
&= \int_{[0,1]^2} \Big|\sum_{a_1, a_2 (p)} \sum_{\substack{n \equiv a_1 (p) \\ 1 \leqslant n \leqslant X}} e(\cdots) \sum_{\substack{n \equiv a_2 (p) \\ 1 \leqslant n \leqslant X}} e(\cdots)\Big|^2 \Big|\sum_{n=1}^{X} e(\cdots)\Big|^{2s-4}
\end{aligned}
$$

Two cases: $a_1 = a_2$ (narrow) and $a_1 \neq a_2$ (broad).

If the narrow contribution dominates, write $2 = (1/2)4$ and apply Hölder

$$
\int f^4 g^{2s-4} \leqslant \Big(\int f^{2s}\Big)^{\frac{4}{2s}} \Big(\int g^{2s}\Big)^{\frac{2s-4}{2s}}
$$

and then Minkowski to show that $J_s(X) \lesssim p^s J_s(X/p)$ (good).

Broad piece

If the broad piece dominates, the main term is:

$$\int_{[0,1]^2} \Big| \sum_{\substack{a_1,a_2(p)\\ \text{distinct}}} \sum_{\substack{n\equiv a_1(p)\\ 1\leqslant n\leqslant X}} e(nx+n^2t) \sum_{\substack{n\equiv a_2(p)\\ 1\leqslant n\leqslant X}} e(nx+n^2t)\Big|^2 \Big| \sum_{n=1}^{X} e(nx+n^2t)\Big|^{2s-4}$$

$$= \int_{[0,1]^2} \Big| \sum_{\substack{a_1,a_2(p)\\ \text{distinct}}} \sum_{\substack{n\equiv a_1(p)\\ 1\leqslant n\leqslant X}} e(\cdots) \sum_{\substack{n\equiv a_2(p)\\ 1\leqslant n\leqslant X}} e(\cdots)\Big|^2 \Big| \sum_{b(p)} \sum_{\substack{n=b(p)\\ 1\leqslant n\leqslant X}} e(\cdots)\Big|^{2s-4}$$

$$\leqslant p^{2s-4} \max_{b(p)} \int_{[0,1]^2} \Big| \sum_{\substack{a_1,a_2(p)\\ \text{distinct}}} \sum_{\substack{n\equiv a_1(p)\\ 1\leqslant n\leqslant X}} e(\cdots) \sum_{\substack{n\equiv a_2(p)\\ 1\leqslant n\leqslant X}} e(\cdots)\Big|^2 \Big| \sum_{\substack{n=b(p)\\ 1\leqslant n\leqslant X}} e(\cdots)\Big|^{2s-4}$$

For simplicity, assume the $0 \pmod p$ is where the max happens.

Solution counting

The integral counts the number of solutions to

$$n_1 + n_2 + n_3 + \cdots + n_s = m_1 + m_2 + m_3 + \cdots + m_s$$
$$n_1^2 + n_2^2 + n_3^2 + \cdots + n_s^2 = m_1^2 + m_2^2 + m_3^2 + \cdots + m_s^2$$

where $1 \leqslant n_i, m_i \leqslant X$, $n_3, \dots, n_s, m_3, \dots, m_s \equiv 0 \pmod{p}$ and n_1, n_2 are distinct mod p and m_1, m_2 are distinct mod p.

Count number of solutions to:

$$m_3 + \cdots + m_s = n_3 + \cdots + n_s + [n_1 + n_2 - m_1 - m_2]$$
$$m_3^2 + \cdots + m_s^2 = n_3^2 + \cdots + n_s^2 + [n_1^2 + n_2^2 - m_1^2 - m_2^2]$$

where $1 \leqslant n_i, m_i \leqslant X$. Since the other n_i, m_i are $\equiv 0 \pmod{p}$, for each valid $(n_1, \dots, m_2)$, there are $\leqslant J_{s-2}(X/p)$ many solutions $(n_3, \dots, m_s)$.

How many valid $(n_1, \ldots, m_2)$ are there? Any such valid 4-tuple must satisfy

$$n_1 + n_2 - m_1 - m_2 \equiv 0 \pmod{p}$$
$$n_1^2 + n_2^2 - m_1^2 - m_2^2 \equiv 0 \pmod{p^2}$$

where n_1, n_2 are distinct mod p and m_1, m_2 are distinct mod p and $1 \leqslant n_1, n_2, m_1, m_2 \leqslant X$. There are $\leqslant X^2$ choices for m_1 and m_2.

Given such a choice, what does this say about n_1, n_2?

We want to count the number of $n_1, n_2 \in [1, X]$ such that $n_1 \not\equiv n_2 \pmod{p}$ such that

$$n_1 + n_2 \equiv H_1 \pmod{p}$$
$$n_1^2 + n_2^2 \equiv H_2 \pmod{p^2}$$

for some (H_1, H_2). Since $p^2 = X$, instead of counting integers, we can count residue classes mod p^2. Paying a factor of p we may replace $H_1 \pmod{p}$ with $H_1' \pmod{p^2}$.

Solution counting, cont.

$$n_1 + n_2 \equiv H_1' \pmod{p^2}$$
$$n_1^2 + n_2^2 \equiv H_2 \pmod{p^2}$$

Suppose (A, B) mod p^2 is a solution and $A \not\equiv B \pmod{p}$. Suppose (C, D) mod p^2 is another such solution. Then

$$(X - C)(X - D) \equiv (X - A)(X - B) \pmod{p^2}.$$

Thus

$$(C - A)(C - B), (D - A)(D - B) \equiv 0 \pmod{p^2}.$$

Since $A \not\equiv B \pmod{p}$, we can't have both $p \mid C - A$ and $p \mid C - B$. Therefore either $A \equiv C \pmod{p^2}$ or $B \equiv C \pmod{p^2}$.

Similarly, we see $A \equiv D \pmod{p^2}$ or $B \equiv D \pmod{p^2}$. Therefore $\{A, B\}$ is a permutation of $\{C, D\}$.

The iteration

Therefore we see if broad dominates,

$$J_s(X) \lesssim p^{2s-4} \cdot J_{s-2}(X/p) \cdot X^2 \cdot p \cdot 1.$$

Is this ever sharp? Yes! As long as s is supercritical.

Heuristically $J_s(X) \approx X^{2s-3}$ if $s \geqslant 3$. If this is true, the RHS

$$= p^{2s-4} \cdot (X/p)^{2(s-2)-3} X^2 p = X^{2s-5} p^4 = X^{2s-3}$$

since $p = X^{1/2}$.

Karatsuba: For $s \in 2\mathbb{N}$, $J_s(X) \lesssim_s X^{2s-3+\frac{2}{2^{s/2}}}$.

The loss of $2/2^s$ comes from trying to get to supercritical $J_s(X)$ using only subcritical data.

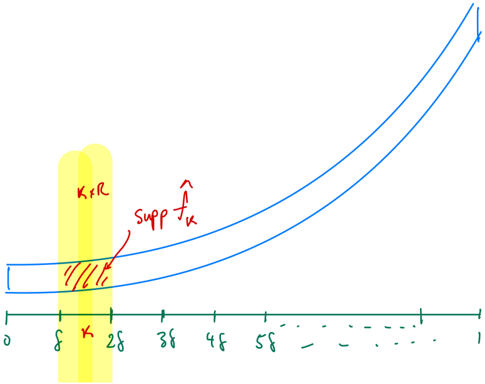
We incur a cost to get to the supercritical regime, but then once we're there, the cost lessens the farther we are from the critical number.

Parabola decoupling

Let P_δ be the partition of $[0,1]$ into intervals of length δ. Let f_I be defined so that $\widehat{f_I} := \widehat{f} 1_{I\times\mathbb{R}}$. Let $D_p(\delta)$ be the smallest constant such that

$$\|f\|_{L^p(\mathbb{R}^2)} = \|\sum_{K\in P_\delta([0,1])} f_K\|_{L^p(\mathbb{R}^2)} \leqslant D_p(\delta)(\sum_{I\in P_\delta([0,1])} \|f_K\|^2_{L^p(\mathbb{R}^2)})^{1/2}$$

for all f with Fourier transform supported in a δ^2 neighborhood of $\{(\xi,\xi^2) : \xi \in [0,1]\}$.



Parabola decoupling

Restriction of Bourgain-Demeter 2014/Bourgain-Demeter-Guth 2015 to the parabola case: For $p \geqslant 6$,

$$D_p(\delta) \lesssim_{\varepsilon,p} \delta^{-(\frac{1}{2}-\frac{3}{p})-\varepsilon}$$

If one believes the previous proof can prove a decoupling estimate:

What does solution counting correspond to?

We prove the following decoupling analogue: For $p \in 4\mathbb{N}$,

$$D_p(\delta) \lesssim_{\varepsilon,p} \delta^{-(\frac{1}{2}-\frac{3}{p})-\frac{1}{p}\cdot\frac{2}{2^{p/4}}-\varepsilon}$$

This implies the Karatsuba estimate (ignoring the ε) by taking $p = 2s$.

Decoupling: reduction to the broad case

Step 1: The first step was to show that the broad term dominates and so $J_s(X) \approx$

$$\int_{[0,1]^2} \Big| \sum_{\substack{a_1,a_2(p)\\ \text{distinct}}} \sum_{\substack{n\equiv a_1(p)\\ 1\leqslant n\leqslant X}} e(nx+n^2t) \sum_{\substack{n\equiv a_2(p)\\ 1\leqslant n\leqslant X}} e(nx+n^2t)\Big|^2 \Big|\sum_{n=1}^{X} e(nx+n^2t)\Big|^{2s-4}$$

We want to study the L^{2s} decoupling constant, so we want to start with $\int |f|^{2s} = \int |\sum_K f_K|^{2s}$ and see how much it costs to break up the sum.

We use a "broad-narrow" argument to show that

$$\int |f|^{2s} \approx \max_{\substack{I_1,I_2\in P_{O(1)}\\ d(I_1,I_2)\sim 1}} \int |f_{I_1} f_{I_2}|^2 |f|^{2s-4}.$$

The point is that we have inserted $O(1)$ separation into 2 terms of the multilinear expression corresponding to that the "$a_1 \neq a_2$".

Decoupling analogue of Step 2

We choose $\nu \sim \delta^{1/2}$ in analogy to how $p \sim X^{1/2}$.

We write

$$|f| = |\sum_{J \in P_\nu} f_J| \leqslant N \max_J |f_J|$$

where N is the number of J such that $f_J \neq 0$. Note $N \leqslant \nu^{-1}$. Then

$$\int |f|^{2s} \approx \max_{\substack{I_1, I_2 \in P_{O(1)} \\ d(I_1, I_2) \sim 1}} \int |f_{I_1} f_{I_2}|^2 |f|^{2s-4}$$

$$\leqslant N^{2s-4} \max_{J \in P_\nu} \max_{\substack{I_1, I_2 \in P_{O(1)} \\ d(I_1, I_2) \sim 1}} \int |f_{I_1} f_{I_2}|^2 |f_J|^{2s-4}$$

Now fix one of the I_1, I_2 and WLOG assume that max over J is attained at $J = [0, \nu]$ with $\nu \sim \delta^{1/2}$.

Step 3: Parabola geometry

We write $f_I = \sum_{K \in P_\delta(I)} f_K$ and so

$$\int |f_I f_{I'}|^2 |f_{[0,\nu]}|^{2s-4} = \int |\sum_{\substack{K \subset I \\ K' \subset I'}} f_K f_{K'}|^2 |f_{[0,\nu]}|^{2s-4}$$

where $d(I, I') \sim 1$. Since $\int f(x) = \widehat{f}(0)$, the above is

$$\sum_{\substack{K_1, K_2 \subset I \\ K_1', K_2' \subset I'}} [\widehat{f_{K_1}} * \widehat{f_{K_1'}} * \widehat{\overline{f_{K_2}}} * \widehat{\overline{f_{K_2'}}} * (\widehat{f_{[0,\nu]}} * \cdots * \widehat{\overline{f_{[0,\nu]}}})](0)$$

Since the K_i could be anywhere in $[0,1]$, $\widehat{f_{K_i}}$ is supported in a δ-box. Similarly for K_i'. Call these boxes τ_{K_i} and $\tau_{K_i'}$.

$\widehat{f_{[0,\nu]}}$ is essentially supported in $[0,\nu] \times [0,\nu^2]$. And therefore (essentially) so is $\widehat{f_{[0,\nu]}} * \cdots * \widehat{\overline{f_{[0,\nu]}}}$.

Parabola geometry

$$\sum_{\substack{K_1,K_2\subset I\\ K_1',K_2'\subset I'}} [\widehat{f_{K_1}} * \widehat{f_{K_1'}} * \overline{\widehat{f_{K_2}}} * \overline{\widehat{f_{K_2'}}} * (\widehat{f_{[0,\nu]}} * \cdots * \overline{\widehat{f_{[0,\nu]}}})](0)$$

Let $\square$ be the partition of $[0,\nu]\times[0,\nu^2]$ into $O(\nu^{-1})$ many squares of size $\nu^2=\delta$. So the above is

$$\sum_{\substack{K_2\subset I\\ K_2'\subset I'}} \sum_{\square} \sum_{\substack{K_1\subset I\\ K_1'\subset I'}} [\widehat{f_{K_1}} * \widehat{f_{K_1'}} * \overline{\widehat{f_{K_2}}} * \overline{\widehat{f_{K_2'}}} * (\widehat{f_{[0,\nu]}} * \cdots * \overline{\widehat{f_{[0,\nu]}}})1_{\square}](0)$$

Since $\nu^2=\delta$, every term in this expression is a δ-cube. For each fixed $K_2, K_2', \square$, I claim there are not very many (K_1, K_1') such that

$$0 \in \mathrm{supp}(\widehat{f_{K_1}} * \widehat{f_{K_1'}} * \overline{\widehat{f_{K_2}}} * \overline{\widehat{f_{K_2'}}} * (\widehat{f_{[0,\nu]}} * \cdots * \overline{\widehat{f_{[0,\nu]}}})1_{\square}).$$

$$= \tau_{K_1} + \tau_{K_1'} - \tau_{K_2} - \tau_{K_2'} + \square$$

Parabola geometry, cont.

For each $K_2, K_2', \square$, we claim that up to permutation the solution is unique. Suppose we had δ-intervals $(A, B) \subset I \times I'$ and $(C, D) \subset I \times I'$ such that

$$0 \in \tau_A + \tau_B - \tau_{K_2} - \tau_{K_2'} + \square$$
$$0 \in \tau_C + \tau_D - \tau_{K_2} - \tau_{K_2'} + \square.$$

This means there exists $\xi_A \in A$, $\xi_B \in B$, etc. such that

$$|\xi_A + \xi_B - \xi_C - \xi_D| \lesssim \delta, |\xi_A^2 + \xi_B^2 - \xi_C^2 - \xi_D^2| \lesssim \delta.$$

Since $A, C \subset I$, $B, D \subset I'$ and $d(I, I') \sim 1$.

$$d(A, B) \sim 1, d(C, D) \sim 1, d(A, D) \sim 1, d(B, C) \sim 1$$

and so $d(A, C) \lesssim \delta$ and $d(B, D) \lesssim \delta$. In other words the solutions up to permutation are essentially unique.

Putting things together

Using this geometric input (and lots of dyadic pigeonholing) we can eventually obtain that

$$D_{2s}(\delta)^{2s} \lessapprox \nu^{-s+1} D_{2s-4}(\delta/\nu)^{2s-4}$$

This iteration is sharp as long as p is supercritical. Since if p is supercritical, then $D_p(\delta)^p \approx \delta^{-(p/2-3)}$. Both sides are then:

$$LHS = \delta^{-s+3}, \quad RHS = \nu^{-s+1}(\delta/\nu)^{-(s-5)} = \delta^{-s+5}\nu^{-4} = \delta^{-s+3}$$

since $\nu = \delta^{1/2}$.

This iteration then gives that

$$D_{2s}(\delta)^{2s} \lessapprox \delta^{-(s-3)-\frac{2}{2^{s/2}}}$$

Moral:

$$D_{40}(\delta) \leftarrow D_{36}(\delta) \leftarrow \cdots D_8(\delta) \leftarrow D_4(\delta)$$

and since $D_4(\delta)$ can be proven directly, we eat the loss and then once we're supercritical, we iterate efficiently.

Could this estimate really have been proven in the 70s?

I would like to think yes.

The key geometric piece of information used is the same information used to prove the classical square function estimate:

$$\|f\|_{L^4(\mathbb{R}^2)} \lesssim \|(\sum_{K \in P_\delta} |f_K|^2)^{1/2}\|_{L^4(\mathbb{R}^2)}$$

for all f with Fourier transform supported in a δ^2 neighborhood of the parabola above $[0, 1]$.

The proceeds by expanding the L^4 and was essentially due to Fefferman in 1973.