18.118 DECOUPLING
LECTURE 17 NOTES

INSTRUCTOR: LARRY GUTH
TRANSCRIBED BY JONATHAN TIDOR

Recall the setup from last time. We're interested in the quantity

$$R_{s,k,A}(n) = \#\left\{(a_1, \ldots, a_s) \in [1, A] : a_1^k + \cdots + a_s^k = n\right\}.$$

The function $f \colon \mathbb{R}^k \to \mathbb{C}$ is defined by

$$f(x) = \sum_{a=1}^{A} e(a^k x_k + \cdots + a x_1).$$

We showed over the last two classes that to estimate the size of $R_{s,k,A}(n)$, one thing we'd like to do is to bound $|f(\mathbf{c})|$ where c_k is Diophantine. We proved that one could bound this by bounding

$$\int_{[0,1]^k} |f(x)|^p.$$

In particular we proved the following proposition.

Proposition 0.1. *If for some p,*

$$\int_{[0,1]^k} |f(x)|^p \lesssim A^\epsilon A^{p-\frac{k(k+1)}{2}},$$

then for c_k Diophantine

$$|f(\mathbf{c})| \lesssim A^{1-\frac{1}{p+1}+\epsilon}.$$

The hypothesis of this proposition is true for all $p \geq k(k+1)$, proved recently by both decoupling and another method of Trevor Wooley. In this (mostly self-contained) lecture we're going to prove the hypothesis for $p \gtrsim k^2 \log k$ following the method of Vinogradov.

Theorem 0.2 (Vinogradov)**.** *For $p \gtrsim k^2 \log k$ an even integer,*

$$\int_{[0,1]^k} |f(x)|^p \lesssim A^\epsilon A^{p-\frac{k(k+1)}{2}}.$$

By Proposition 0.1, this implies the following.

Corollary 0.3. *For c_k Diophantine,*

$$|f(\mathbf{c})| \lesssim A^{1-\sigma}$$

where $\sigma \gtrsim \frac{1}{k^2 \log k}$.

This was how Vinogradov proved his bounds on $R_{s,k}(n)$.

Definition 0.4.

$$J_{s,k}(A) = \#\{(a_1, \dots, a_s, b_1, \dots, b_s) \in [1, A]^{2s} : a_1^i + \cdots + a_s^i = b_1^i + \cdots + b_s^i \text{ for all } 1 \le i \le k\}.$$

$$J_{s,k}(A, \nu) = \#\{(a_1, \dots, a_s, b_1, \dots, b_s) \in [1, A]^{2s} : a_1^i + \cdots + a_s^i = b_1^i + \cdots + b_s^i + \nu_i \text{ for all } 1 \le i \le k\}.$$

We sometimes use the notation

$$\mathbf{V} = \left\{(a_1, \dots, a_s, b_1, \dots, b_s) \in \mathbb{N}^{2s} : a_1^i + \cdots + a_s^i = b_1^i + \cdots + b_s^i \text{ for all } 1 \le i \le k\right\}.$$

Recall from the very first lecture that for $p = 2s$ an even integer

$$\int_{[0,1]^k} |f(x)|^{2s} = J_{s,k}(A).$$

Thus our goal this lecture will be the following theorem of Vinogradov.

Theorem 0.5 (Vinogradov)**.**

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

where $\varepsilon(s,k) = e^{-s/k^2} k^2$.

Note that the above theorem does not restrict s, but is only interesting for $s \ge 10k^2 \log k$, say. The proof uses the following 3 tools. A good reference for this lecture is *Ten lectures on the interface between analytic number theory and harmonic analysis* by Hugh L. Montgomery.

1. Geometric methods

The geometric properties of this problem are most apparent when $s = k$. We'll work with $s = k$ here and deal with the rest of the variables later.

Define $\phi \colon \mathbb{R}^k \to \mathbb{R}^k$ by

$$\phi(a_1, \dots, a_k) = (a_1 + \cdots + a_k, a_1^2 + \cdots + a_k^2, \dots, a_1^k + \cdots + a_k^k).$$

Then it is easy to compute the Jacobian determinant of ϕ.

$$\det\left(\frac{\partial \phi_j}{\partial a_i}\right) = \det\left(j a_i^{j-1}\right) = k! \prod_{i<j} (a_i - a_j).$$

This is just a scaled version of the Vandermonde determinant.

This means that the Jacobian of ϕ is non-singular when the a_i are distinct and does not distort space too much when the a_i are not close to each other. This turns into a bound for "well-spaced" solutions to a certain Diophantine equation.

Definition 1.1. *$(\tilde{a}_1, \dots, \tilde{a}_k) \in [0,1]^k$ is γ-**well-spaced** if $|a_i - a_j| > \gamma$ for $i \neq j$. Similarly $(a_1, \dots, a_k) \in [1, A]^k$ is γ-**well-spaced** if $|a_i - a_j| > \gamma A$ for $i \neq j$.*

Lemma 1.2. *Let I_j be intervals such that $|I_j| \geq A^{j-1}$. The number of γ-well-spaced $(a_1, \dots, a_k) \in [1, A]^k$ such that $a_1^j + \cdots + a_k^j \in I_j$ for all $1 \leq j \leq k$ is*

$$\lesssim_\gamma \prod_{j=1}^{k} \left(\frac{|I_j|}{A^j} \right) A^k.$$

Proof sketch: First scale the problem as follows: $\tilde{a}_i = a_i/A$ and $\tilde{I}_j = I_j/A^j$. Note that $\tilde{a}_i \in [0,1]$ and $\tilde{a}_1^j + \cdots + \tilde{a}_k^j \in \tilde{I}_j$.

Now the Jacobian determinant of ϕ at $(\tilde{a}_1, \dots, \tilde{a}_k)$ is $\sim_\gamma 1$ since the point is γ-well-spaced. All the singular values of the Jacobian are $\lesssim 1$, which implies that they are bounded below $\gtrsim_\gamma 1$.

The scaled version of the lattice $[1, A]^k$ is a set of $\frac{1}{A}$-separated points in $[0,1]^k$. The γ-well-spaced points in this lattice turn into a $\sim_\gamma \frac{1}{A}$-separated set under ϕ.

This implies that at most $\prod_{j=1}^k |\tilde{I}_j| A^k$ points lie in $\tilde{I}_1 \times \cdots \times \tilde{I}_k$, as desired. (One way to see this is that the balls of radius $\frac{c(\gamma)}{2A}$ around the points are disjoint and all lie in $N_{\frac{c(\gamma)}{2A}}(\tilde{I}_1 \times \cdots \times \tilde{I}_k)$. Since $|\tilde{I}_j| \geq \frac{1}{A}$, taking this neighborhood does not increase the volume of the region by more than a constant factor.) $\square$

2. Hölderization

Given a combinatorial problem we can turn it into an integral using Fourier analysis, use Hölder's inequality, and then turn it back into a (different) combinatorial problem. It turns out that this is sometimes a useful thing to do.

Proposition 2.1. *Given positive integers r_i, sets $S_i \subset \mathbb{Z}^{r_i}$, and functions $P_i \colon \mathbb{Z}^{r_i} \to \mathbb{Z}^k$ for $1 \le i \le 2t$,*

$$\#\left\{(a_1, \ldots, a_{2t}) \in S_1 \times \cdots \times S_{2t} : \sum_{i=1}^{2t} P_i(a_i) = 0\right\} \le \prod_{i=1}^{2t}\left(\#\left\{a_{i_1}, \ldots, a_{i_t}, b_{i_1}, \ldots, b_{i_t} \in S_i : \sum_{j=1}^{t} P_i(a_{i_j}) = \sum_{j=1}^{t} P_i(b_{i_j})\right\}\right)^{\frac{1}{2t}}.$$

Proof.

$$\begin{aligned}
\#\left\{(a_1, \ldots, a_{2t}) \in S_1 \times \cdots \times S_{2t} : \sum_{i=1}^{2t} P_i(a_i) = 0\right\} \\
&= \int_{[0,1]^k} \prod_{i=1}^{2t}\left(\sum_{a_i \in S_i} e(P_i(a_i)x)\right) dx \\
&\le \prod_{i=1}^{2t}\left(\int_{[0,1]^k}\left|\sum_{a_i \in s_i} e(P_i(a_i)x)\right|^{2t}\right)^{\frac{1}{2t}} \\
&\le \prod_{i=1}^{2t}\left(\#\left\{a_{i_1}, \ldots, a_{i_t}, b_{i_1}, \ldots, b_{i_t} \in S_i : \sum_{j=1}^{t} P_i(a_{i_j}) = \sum_{j=1}^{t} P_i(b_{i_j})\right\}\right)^{\frac{1}{2t}}.
\end{aligned}$$

□

Here is a simpler version of the same idea, which is used in the proof of Theorem 0.5.

Proposition 2.2. *$J_{s,k}(A, \nu) \le J_{s,k}(A)$.*

Proof.

$$\begin{aligned}
J_{s,k}(A, \nu) &= \int_{[0,1]^k}\left|\sum_{a \in [1,A]} e(x_1 a + x_2 a^2 + \cdots + x_k a^k)\right|^{2s} e(\nu x)\, dx \\
&\le \int_{[0,1]^k}\left|\sum_{a \in [1,A]} e(x_1 a + x_2 a^2 + \cdots + x_k a^k)\right|^{2s} dx \\
&= J_{s,k}(A).
\end{aligned}$$

□

Remark 2.3. *Is there a proof of Proposition* 2.1 *without using this 'Fourier trick'? There is for Proposition* 2.2.

We'll use another version of this idea in the proof of Theorem 0.5.

3. Translation-dilation invariance

Proposition 3.1. $(a_1, \dots, a_s, b_1, \dots, b_s) \in \mathbf{V}$ *implies that* $(\lambda a_1 + t, \dots, \lambda a_s + t, \lambda b_1 + t, \dots, \lambda b_s + t) \in \mathbf{V}$ *for all* $\lambda, t \in \mathbb{N}$.

Proof. All the equations that define $\mathbf{V}$ are homogeneous, so dilation is obvious. Now suppose that $a_1^i + \dots + a_s^i = b_1^i + \dots + b_s^i$ for all $1 \le i \le k$. Then for $1 \le j \le k$, the equation

$$(a_1 + t)^j + \dots + (a_s + t)^j = (b_1 + t)^j + \dots + (b_s + t)^j$$

is a linear combination of the previous equations. □

4. Proof of Theorem 0.5

Lemma 4.1.

$$\# \Big\{ (a_1, \dots, a_k, \ \alpha_1, \dots, \alpha_{s-k}, b_1, \dots, b_k, \beta_1, \dots, \beta_{s-k}) \in \mathbf{V} \cap \left([1, A]^k \times [1, A^{\frac{k-1}{k}}]^{(s-k)} \right)^2, \\ (a_1, \dots, a_k), (b_1, \dots, b_k) \ \gamma\text{-well-spaced} \Big\} \lesssim_\gamma A^{\frac{k-1}{2}} A^k J_{s-k,k}(A^{\frac{k-1}{k}}).$$

Proof. There are fewer than A^k choices for b. After choosing b it is the case that $a_1^j + \dots + a_k^j \in b_1^j + \dots + b_k^j + [0, (s-k)A^{\frac{k-1}{k}j}]$, an interval of length $O(A^{j - \frac{j}{k}})$. By Lemma 1.2, there are at most $A^{\frac{k-1}{2}}$ choices for a well-spaced after b is chosen. Then the number of choices for (α, β) is given by $J_{s-k,k}(A^{\frac{k-1}{k}}, \nu(a, b))$ for $\nu_j(a, b) = a_1^j + \dots + a_k^j - b_1^j - \dots - b_k^j$. By Proposition 2.2, the desired inequality follows. □

Remark 4.2. *The above statement is true even without the assumption that* $(b_1, \dots, b_k)$ *is* γ*-well-spaced. Indeed, the proof does not make use of this assumption. However, the symmetry between* a *and* b *will be useful in the next lemma.*

Lemma 4.3.

$$\# \left\{ (a_1, \dots, a_s, b_1, \dots, b_s) \in \mathbf{V} \cap [1, A]^{2s}, \ (a_1, \dots, a_k), (b_1, \dots, b_k) \ \gamma\text{-well-spaced} \right\} \\ \lesssim_\gamma \left(A^{\frac{1}{k}} \right)^{2(s-k)} A^{\frac{k-1}{2}} A^k J_{s-k,k}(A^{\frac{k-1}{k}}).$$

Proof. Partition $[1, A] = \bigsqcup_{I \in \mathcal{I}} I$ where each $I \in \mathcal{I}$ is an interval of length $A^{\frac{k-1}{k}}$. Then the quantity we wish to compute is exactly

$$\sum_{I_i, J_j \in \mathcal{I}} \# \left\{ (a_1, \dots, a_k, \ \alpha_1, \dots, \alpha_{s-k}, b_1, \dots, b_k, \beta_1, \dots, \beta_{s-k}) \in \mathbf{V} \cap [1, A]^k \right. \\ \left. \times I_1 \times \dots \times I_{s-k} \times [1, A]^k \times J_1 \times \dots \times J_{s-k}, \ a, b \ \gamma\text{-well-spaced} \right\}.$$

Each term in the sum can be written as

$$\int_{[0,1]^k} \left| \sum_{\substack{a\in[1,A]^k \\ \gamma\text{-well-spaced}}} \prod_{i=1}^{k} e(\phi(a_i)x) \right|^2 \prod_{i=1}^{s-k} \left(\sum_{\alpha_i\in I_i, \beta_i\in J_i} e(\phi(\alpha_i)x)e(-\phi(\beta_i)x) \right) dx$$

$$\leq \prod_{i=1}^{s-k} \left(\int_{[0,1]^k} \left| \sum_{\substack{a\in[1,A]^k \\ \gamma\text{-well-spaced}}} \prod_{i=1}^{k} e(\phi(a_i)x) \right|^2 \left| \sum_{\alpha_i\in I_i} e(\phi(\alpha_i)x) \right|^{2(s-k)} dx \right)^{\frac{1}{2(s-k)}}$$

$$\cdot \prod_{i=1}^{s-k} \left(\int_{[0,1]^k} \left| \sum_{\substack{a\in[1,A]^k \\ \gamma\text{-well-spaced}}} \prod_{i=1}^{k} e(\phi(a_i)x) \right|^2 \left| \sum_{\beta_i\in J_i} e(\phi(\beta_i)x) \right|^{2(s-k)} dx \right)^{\frac{1}{2(s-k)}}$$

By Proposition 3.1, translation invariance, the right-hand side of the above equation is equal to the left-hand side of Lemma 4.1. There are $A^{\frac{1}{k}}$ intervals in $\mathcal{I}$ so there are $\left(A^{\frac{1}{k}}\right)^{2(s-k)}$ terms in the sum. This gives the desired bound in this lemma, which is $\left(A^{\frac{1}{k}}\right)^{2(s-k)}$ times the bound in Lemma 4.1. □

Now we wish to study

$$J_{s,k}(A) := \#\left\{(a_1, ..., , a_s, b_1, ..., b_s) \in V \cap [1, A]^{2s}\right\}.$$

The last lemma allows us to count the subset of these solutions where $(a_1, ..., a_k)$ and $(b_1, ..., b_k)$ are γ-well spaced. If a definite fraction of the solutions are well-spaced, then we get the inequality

$$J_{s,k}(A) \lesssim_\gamma \left(A^{\frac{1}{k}}\right)^{2(s-k)} A^{\frac{k-1}{2}} A^k J_{s-k,k}(A^{\frac{k-1}{k}}). \qquad (WS)$$

We label this equation (WS) for the well-spaced case. For $s - k \geq k(k+1)$, this estimate is actually sharp! In other words, define $\bar{J}_{s,k}(A)$ to be the conjectured upper bound for $J_{s,k}(A)$:

$$\bar{J}_{s,k}(A) = \max\left(A^s, A^{2s-\frac{k(k+1)}{2}}\right).$$

If $s-k \geq k(k+1)$, and if we replace $J_{s,k}$ by $\bar{J}_{s,k}$ in inequality (WS), we get an equality. Roughly speaking, if $s \geq k(k+1)$, then we conjecture that $J_{s,k}(A) \sim J_{s,k}(A,\nu)$ for all $\nu = (\nu_1, ..., \nu_k)$ with $|\nu_j| \leq A^j$. Assuming this kind of pseudorandomness, we would expect the arguments above to be tight. However, we do expect a loss when $s \geq k(k+1)$

but $s-k<k(k+1)$, because then $J_{s-k,k}(A)$ is much bigger than $J_{s-k,k}(A,\nu)$ for most ν.

Assuming for a moment that we are always in the well-spaced case, then we can iterate (WS) until s is close to k^2 and finally plug in a trivial estimate of the form $J_{s',k}(A')\le (A')^{2s'}$. Since $A'=A^{\left(\frac{k-1}{k}\right)^{s/k}}\sim A^{e^{-s/k^2}}$, we get the desired result.

If the solutions in $J_{s,k}(A)$ are usually not well-spaced, the Holderization trick leads to an even better iterative estimate:

$$J_{s,k}(A)\lesssim \gamma^{-2(k-1)}J_{s,k}(\gamma A) \qquad (NWS).$$

As long as γ is very small compared to the implicit constant, this is a very strong estimate for $J_{s,k}$. We sketch the proof of this estimate, which is a good exercise in the techniques introduced in the lecture. This reduction is also reminiscent of the broad/narrow trick that we have studied in restriction theory.

Let $W=W_\gamma\subset[1,A]^s$ be the set of $(a_1,...,a_s)\in[1,A]^s$ so that some k of the a_i are γ-well-spaced. We can write

$$J_{s,k}(A)=J_{s,k}(W,W)+2J_{s,k}(W,W^c)+J_{s,k}(W^c,W^c),$$

where, for instance,

$$J_{s,k}(W,W^c)=\#\left\{(a,b)\in W\times W^c,(a,b)\in V\right\}.$$

The first term, $J_{s,k}(W,W)$, counts the number of well-spaced solutions, and it is controlled by Lemma 4.3. By Holderization, the mixed term is controlled by the first and last terms. So if we are not in the well-spaced case, then

$$J_{s,k}(A)\lesssim J_{s,k}(W^c,W^c).$$

Now we cover $[1...A]$ with intervals I of length γA. We can write W^c as

$$W^c=\bigcup_{I_1,...I_s}W^c\cap(I_1\times...I_s).$$

A priori, there are γ^{-s} choices of $I_1,...I_s$. But W^c intersects $\lesssim\gamma^{-(k-1)}$ of these choices! Let N denote the set of all tuples $I_1,...,I_s$ so that $I_1\times...\times I_s$ intersects W^c. Now we can write

$$J_{s,k}(W^c,W^c)\le\sum_{(I_1,...I_s)\in N,(J_1,...,J_s)\in N}J_{s,k}(I_1,...,I_s,J_1,...,J_s),$$

where

$$J_{s,k}(I_1, ..., I_s, J_1, ...J_s) =$$

$$= \# \{(a_1, ..., a_s, , b_1, ..., b_s) \in I_1 \times ... \times I_s \times J_1 \times ... \times J_s, (a, b) \in V\} .$$

By Holderization and translation invariance, each $J_{s,k}(I_1, ...I_s, J_1, ...J_s) \leq J_{s,k}(\gamma A)$. Since the number of choices for the I_i and J_i is at most $|N|^2 \lesssim \gamma^{-2(k-1)}$, this shows (NWS).

In conclusion, we always have either (WS) or (NWS), and then a simple induction computation shows that Vinogradov's theorem holds. In this induction computation, the (WS) case is the worst case.