DISCRETE ANALOGUES IN HARMONIC ANALYSIS POLAND LECTURES – NOVEMBER 2013

JAMES WRIGHT

Abstract. The basic aim of the lectures is to describe two well-developed lines of investigation, both looking at various discrete analogues of euclidean harmonic analysis problems, and to introduce a third perspective which is a hybrid of the two.

Overview of three perspectives

We begin by introducing two perspectives focussed on discrete analogues in harmonic analysis, both perspectives started in the early 1990's and have been developed to the current day. In both cases these points of views have bared much fruit although they have very different goals and aims. In one case, the goal is to gain a better understanding of the core problems in euclidean harmonic analysis which have remained unsolved for many years; problems which go by the names of Kakeya, Restriction, Bochner-Riesz, etc... The idea is to find model problems for these central problems in a simple setting which highlights certain features of the problem. This was initiated by Tom Wolff who proposed a model for the Kakeya problem in the setting of finite fields [58]. This proved to be the perfect setting which highlighted basic geometric combinatorial issues in incidence geometry. After Wolff, G. Mockenhaupt and T. Tao [44] proposed a model problem for the Fourier Restriction Problem in the setting of finite fields. They developed this perspective, emphasising the need for these model problems to attract mathematicians outside the area to these key problems in harmonic analysis, with hopes that their input would introduce new techniques and ideas which are needed to solve the outstanding conjectures.

Since Wolff, Mockenhaupt and Tao, many people (for instance A. Carbery,J. Ellenberg, A. Hart, A. Iosevich, Koh, R. Oberlin, B. Stones, etc...) have developed this point of view, further studying these problems and introducing model problems for other euclidean problems in the finite field setting. We will examine in more detail these problems in finite fields, emphasising differences with their euclidean cousins in order to see how well these problems are serving as models.

In the late 1980's J. Bourgain [6], [7], [8], [9] generalised the famous pointwise ergodic result of Birkhoff; instead of averaging a function along the entire orbit generated by the iterates of a measure-preserving transformation T (that is,

$\{T^n\}_{n\geq 1}$), Bourgain considered what happens along a sparse subsequence of iterates; for example, along the squares $\{T^{n^2}\}_{n\geq 1}$. In so doing he needed to examine discrete analogues over the integers $\mathbb{Z}$ of singular maximal functions from euclidean harmonic analysis. In some cases the maximal functions in the euclidean setting, known generally as maximal Radon transforms, have only been been understood (relatively) recently. Nevertheless when one passes to the integers the problems become significantly more difficult and often number-theoretic issues, as well as harmonic analysis issues, arise. Since Bourgain's work, starting in the early 90's, many people have pursued this line of looking at modern euclidean harmonic analysis problems over the integers for other types of operators (singular integrals, fractional integrals, etc...); most notably E.M. Stein, S. Wainger, D. Oberlin, A. Magyar and A. Ionescu. The main motivation for doing so has continued to come from problems in ergodic theory.

We introduce a third perspective, a kind of hybrid of the two perspectives described above. Instead of looking at these euclidean harmonic analysis problems in the setting of a finite field, say the field of integers modulo a prime integer p, $\mathbb{Z}/p\mathbb{Z}$, or in the setting of the ring of integers $\mathbb{Z}$, we propose to look at these problems in the setting of the ring of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$, for general n (or in more general rings of integers where one finds lots of divisors). We will develop this middle road perspective in the last few lectures and there we will see that the euclidean problems are modelled much more closely in rings with lots of divisors than in finite fields.

A difference one finds when working in finite fields is the lack of scales at ones' disposal. This can have the effect of simplifying technicalities but it can also produce very different outcomes. Divisors on the other hand will play the role of various scales (note that in the finite field $\mathbb{Z}/p\mathbb{Z}$ the prime number p does not have too many divisors!) and in settings where there are many divisors, we will see that certain euclidean scaling arguments will work and consequently the outcome in $\mathbb{Z}/n\mathbb{Z}$ for general n, say, will be the same as in the corresponding euclidean case.

Similar to the second perspective of examining euclidean harmonic analysis problems over the integers $\mathbb{Z}$, there will also be number-theoretic issues which arise in looking at these problems over $\mathbb{Z}/n\mathbb{Z}$ but the number theory is more elementary in nature. Nevertheless, the new twist is that the number-theoretic estimates need to be very sharp in contrast to problems over $\mathbb{Z}$ where often any nontrivial, ϵ gain is sufficient. We will find that there is a very close interplay between results and estimates in the euclidean setting and the corresponding result and estimate in elementary number theory. The interplay goes both ways and in these lectures we will demonstrate how a harmonic analysts point of view can be used for basic problems in number theory.

1. Central problems in euclidean harmonic analysis

A basic object in euclidean harmonic analysis is the fourier transform, defined for integrable functions $f \in L^1(\mathbb{R}^n)$ as

$$\mathcal{F}f(\xi) \;=\; \int_{\mathbb{R}^n} f(x) e^{-2\pi i x\cdot\xi}\, dx.$$

It is a simple consequence of the Lebesgue dominated convergence theorem that $\mathcal{F}f(\xi)$ is a continuous function and little more effort shows that as an operator, $\mathcal{F}$ is a bounded linear operator from $L^1(\mathbb{R}^n)$ to $C_0(\mathbb{R}^n)$, the space of continuous functions which vanish at infinity. When we want to emphasis the transform aspect over the operator aspect, we will write $\mathcal{F}f(\xi) = \widehat{f}(\xi)$.

In particular, we see that for a general integrable function f, the fourier transform $\widehat{f}$ is a nice continuous bounded function and so no serious singularities are produced when we compute the fourier transform of an L^1 function. Although it is not obvious from the definition, it is possible (and important for many problems in harmonic analysis) to define the fourier transform for a general $L^p(\mathbb{R}^n)$ function when $1 \le p \le 2$. We first begin with the observation that

$$\int_{\mathbb{R}^n} |\mathcal{F}f(\xi)|^2\, d\xi \;=\; \int_{\mathbb{R}^n} |f(x)|^2\, dx \qquad \text{whenever} \quad f \in L^1(\mathbb{R}^n) \cap L^2(\mathbb{R}^n)$$

which says that the fourier transform preserves the L^2 norm. From this it is relatively straightforward to see that the fourier transform $\mathcal{F}$ extends uniquely to a unitary operator on the Hilbert space $L^2(\mathbb{R}^n)$. We can then use the method of interpolation to define $\mathcal{F}$ on each $L^p(\mathbb{R}^n)$ for each $1 \le p \le 2$, and obtain a bounded linear operator $\mathcal{F} : L^p(\mathbb{R}^n) \to L^{p'}(\mathbb{R}^n)$ where $p' = p/(p-1)$, the so-called Hausdorff-Young inequality (or more concretely, one simply splits any $f \in L^p(\mathbb{R}^n)$ into a sum $f = f_1 + f_2$ where $f_1 \in L^1(\mathbb{R}^n)$ and $f_2 \in L^2(\mathbb{R}^n)$, define $\widehat{f} := \widehat{f_1} + \widehat{f_2}$, and check that the definition does not depend on how we split f).

Hence $\mathcal{F}f$ is at best an arbitrary L^2 function when we compute the fourier transform of L^2 functions (being a unitary operator, $\mathcal{F}$ maps L^2 *onto* L^2) and hence $\mathcal{F}f$ is only well defined up to sets of measure zero. Therefore for general L^2 functions f, $\widehat{f}$ can have severe singularities on any set of measure zero (it could be identically infinite). It turns out that the fourier transform $\mathcal{F}$ does not map L^p onto $L^{p'}$ when $1 \le p < 2$ and hence $\mathcal{F}f$ is not an arbitrary $L^{p'}$ function as f varies over L^p. As we already observed, $\mathcal{F}f$ is not an arbitrary L^∞ function when $f \in L^1$ since it is also continuous and so in this case, $\mathcal{F}f$ is not singular on any set of measure zero (the restriction of $\mathcal{F}f$ to a set of measure zero remains continuous with respect to the induced topology).

It is a remarkable observation of E.M. Stein from the mid 1960s that if p is sufficiently close to 1, then the fourier transform $\widehat{f}$ of any $f \in L^p(\mathbb{R}^n)$ cannot be too singular on spheres! In particular, Stein proved that for p sufficiently close to 1, one can restrict the fourier transform of an arbitrary $L^p(\mathbb{R}^n)$ function to the unit sphere $\mathbb{S}^{n-1} = \{x \in \mathbb{R}^n : x \cdot x = 1\}$ and make sense of $\mathcal{R}f := \widehat{f}\big|_{\mathbb{S}^{n-1}}$ as an L^2

density of the sphere. More precisely he showed that the *a priori* inequality

$$\|\mathcal{R}f\|_{L^2(\mathbb{S}^{n-1})} \;\leq\; C\,\|f\|_{L^p(\mathbb{R}^n)} \tag{1}$$

holds for p close to 1. This lies in sharp contrast to what can happen on hyperplanes – for any hyperplane H, one can easily show that (1) cannot hold for any $p > 1$ simply by constructing an $f \in L^p$ so that $\widehat{f}$ is concentrated and large near a compact piece of H (see the Exercises). Hence the fact that spheres have nonvanishing curvature plays a key role in Stein's fundamental observation.

Much later, the exact range of p for which (1) holds was determined by P. Tomas [55] and Stein [49] himself[1]; the above inequality holds in the range $1 \leq p \leq (2n+2)/(n+3)$ and fails outside this range. The complete $L^p \to L^q$ mapping properties of the restriction operator $\mathcal{R}$ of the fourier transform to the sphere remains an open problem. It is conjectured that

$$\|\mathcal{R}f\|_{L^q(\mathbb{S}^{n-1})} \;\leq\; C\,\|f\|_{L^p(\mathbb{R}^n)} \tag{2}$$

holds exactly in the range $q \leq [(n-1)/(n+1)]p'$ whenever $1 \leq p < 2n/(n+1)$ and despite the efforts of many people establishing partial results, notably from three Fields' medalists, this problem remains open in all dimensions[2] $n \geq 3$. This is known as the Fourier Restriction Problem and gives a precise formulation of what kinds of singularities can occur on spheres when one computes the fourier transform of L^p functions.

It is also conjectured that (2) holds if spheres are replaced by any compact piece of a hypersurface with nonvanishing gaussian curvature; furthermore, it is known that some nontrivial fourier restriction phenomena occurs whenever the curvature of the underlying hypersurface does not vanish to infinite order at any point. Since Stein's observation, restriction estimates similar to those in (1) or (2) have become an indispensable tool in the study of many PDEs and analogues have been discovered in a multitude of settings, including the study of primes!

The Fourier Restriction Problem has been studied for varieties S in $\mathbb{R}^n$ which are not hypersurfaces and here we mention the case of curves where the problem has been completely resolved remarkably in the nondegenerate case for all $n \geq 2$. In 1985, S.W. Drury [21] showed that the operator $\mathcal{R}$ restricting the fourier transform to a compact piece of the curve $t \to (t, t^2, \ldots, t^n)$ satisfies the bounds in (2) whenever $p' \geq qn(n+1)/2$ and $p' > 0.5n(n+1)+1$. The relationship $p' \geq qn(n+1)/2$ between the exponents p and q is easily seen to be necessary from a simple scaling argument (we'll come back to this point later). However the condition $p' > 0.5n(n+1)+1$ on the p exponent is not easily seen to be necessary and in fact, it was unknown to Drury and harmonic analysts in general until recently. However it was known to number theorists since 1979, see [2], as there is an interesting connection with an old number theory problem called Tarry's problem. We'll discuss this connection later (see the Exercise 1.7, for example).

---

[1]Tomas established the restriction result in the open range $1 \leq p < (2n+2)/(n+3)$ and Stein established the endpoint estimate

[2]The conjecture was solved in 1970 in two dimensions by C. Fefferman and Stein [26], see also [64].

Closely connected to the Fourier Restriction Problem is the the problem of Bôchner-Riesz summability which is concerned with inverting the fourier transform: when does

$$f(x) \;=\; \int_{\mathbb{R}^n} \widehat{f}(\xi)\, e^{2\pi i x\cdot\xi}\, d\xi \tag{3}$$

hold? It is known to hold for Schwartz functions f and it is known to hold for *a.e.* $x \in \mathbb{R}^n$ whenever $f, \widehat{f} \in L^1$. However the question here is in what sense does (3) hold for $f \in L^p(\mathbb{R}^n)$ when $1 < p \leq 2$. When $p = 2$ it is known (and not hard to prove) that

$$\int_{|\xi|\leq R} \widehat{f}(\xi)\, e^{2\pi i x\cdot\xi}\, d\xi \;\to\; f(x) \quad \text{when} \;\; R \to \infty \tag{4}$$

converges in the $L^2(\mathbb{R}^n)$ sense. Here $|\xi|$ denotes the euclidean norm of ξ and when $n = 1$, it is well known that (4) converges in $L^p(\mathbb{R})$ norm for $1 < p < \infty$ (not too hard and due to M. Riesz from the 1930s). A much deeper result is that (4) also also holds in the almost everywhere pointwise sense, again for $n = 1$ and for $f \in L^p(\mathbb{R}), 1 < p < \infty$; this is due to Carleson [11] ($p = 2$) and Hunt [36] ($1 < p < \infty$) from the mid to late 1960s.

In higher dimensions, many mathematicians tried to show that (4) still holds for $2n/(n+1) \leq p \leq 2n/(n-1)$ (it can be easily shown that outside this range, (4) fails in L^p norm). A shocking result of C. Fefferman [27] showed that when $n \geq 2$, (4) does **not** hold in the L^p sense for any $p \neq 2$! This result used the existence of Kakeya sets (compact subsets of $\mathbb{R}^n$ which contain a unit line segment in every direction) which have measure zero in a decisive way.

It is natural to consider slightly smoothed out versions of the integral in (4); instead of cutting off the integration where $|\xi| \leq R$, we insert the factor $(1 - |\xi|^2/R)^\delta$ and ask for which exponents p does

$$\int_{|\xi|\leq R} \big(1 - |\xi|^2/R\big)^\delta \widehat{f}(\xi)\, e^{2\pi i x\cdot\xi}\, d\xi \;\to\; f(x) \quad \text{when} \;\; R \to \infty \tag{5}$$

converge in $L^p(\mathbb{R}^n)$ norm. This is the Bôchner-Riesz Problem and it is conjectured that when[3] $0 < \delta \leq (n-1)/2$, (5) holds precisely in the range $2n/(n+1+2\delta) < p < 2n/(n-1-2\delta)$. As in the case of the Fourier Restriction Problem, the Bôchner-Riesz Problem is known to hold when $n = 2$ (Carleson and Sjölin [12] established this in 1972) but remains unsolved in higher dimensions $n \geq 3$. Furthermore it is known that the Bôchner-Riesz Conjecture implies the Fourier Restriction Conjecture [54] and that there is a partial implication in the opposition direction.

Yet another core problem in euclidean harmonic analysis which is intimately connected to the Bôchner-Riesz Problem and the Fourier Restriction Problem is the so-called Kakeya Problem. Strangely and somewhat non-intuitively, as we already mentioned, Kakeya sets can have measure zero but it is suspected that these sets have full dimension; it is conjectured that Kakeya sets in $\mathbb{R}^n$ must have dimension n. This is the Kakeya Problem and although there are many different notions of dimension from geometric measure theory (Hausdorff, Minkowski, box, packing,

[3] when $\delta > (n-1)/2$, it is easy to see that (5) holds for all $1 \leq p \leq \infty$

etc ...), it would be a major advance to establish the conjecture for any notion of dimension. In these lectures we will refer to any of these notions of dimension as a *geometric dimension*. Again the Kakeya conjecture is known when $n = 2$ [19] but remains open in higher dimensions $n \geq 3$ and we know that the Fourier Restriction Conjecture (and hence the Bôcher-Riesz Conjecture) implies the Kakeya Conjecture.

An intuitive simple notion of dimension is the upper Minkowski dimension $\overline{\dim}$ defined for compact sets $E \subset \mathbb{R}^n$ as $\overline{\dim}(E) = n - \limsup_{\delta \to 0} \log |E_\delta| / \log(\delta)$ where E_δ denotes the δ neighborhood of E and $|E_\delta|$ denotes the Lebesgue measure of E_δ; hence if E is a unit line segment, E_δ is a $1 \times \delta \times \cdots \times \delta$ tube (or δ-tube for short) with measure about δ^{n-1} and so $\overline{\dim}(E) = 1$. More generally if E is a compact piece of a smooth k surface, then $|E_\delta| \sim \delta^{n-k}$ implying $\overline{\dim}(E) = k$ as expected. When considering a δ neighborhood of a Kakeya set E, it suffices to assume $E_\delta = \cup_j T_\delta^{\omega_j}(x_j)$ where $\{\omega_j\}_{j=1}^N \subset \mathbb{S}^{n-1}$ is a maximal (hence $N \sim \delta^{-(n-1)}$) δ-separated collection of directions by which we mean the angle $\angle \omega_j, \omega_k$ between directions is at least δ. Here $T_\delta^\omega(x)$ denotes the δ-tube centred at x and oriented in the direction ω. The Kakeya conjecture (for Minkowski dimension) is equivalent to showing that for every $\epsilon > 0$, there is a constant C_ϵ such that

$$|\bigcup T_\delta^{\omega_j}(x_j)| \ \geq \ C_\epsilon \, \delta^\epsilon \tag{6}$$

holds for any maximal δ-separated collection of δ-tubes. Since $\sum_j |T_\delta^{\omega_j}(x_j)| \sim 1$, the conjecture (6) says that any maximal δ-separated collection of δ-tubes is essentially disjoint.

Although a very deep problem, there is an even more difficult, quantitative version of the geometric measure theoretic formulation of the Kakeya problem (for example, (6)) which is of more interest to harmonic analysts, the so-called Maximal Kakeya Problem: for every $\epsilon > 0$, there is a constant C_ϵ such that

$$\| \sum_j \chi_{T_j} \|_{L^{n/(n-1)}(\mathbb{R}^n)} \ \leq \ C_\epsilon \, \delta^{-\epsilon} \tag{7}$$

holds for any maximal δ-separated collection of δ-tubes $\{T_j\}$ (here χ_A denotes the indicator function of a set A, equal to 1 for $x \in A$ and zero otherwise). Note that since $\sum_j \int \chi_{T_j}(x) dx \sim 1$, we have

$$1 \ \sim \ \int_{\cup_k T_k} \sum_j \chi_{T_j}(x) dx \ \leq \ \| \sum_j \chi_{T_j} \|_{L^{n/(n-1)}} \, |\cup_k T_k|^{1/n} \ \leq \ C_\epsilon \, \delta^{-\epsilon} |\cup_k T_k|^{1/n}$$

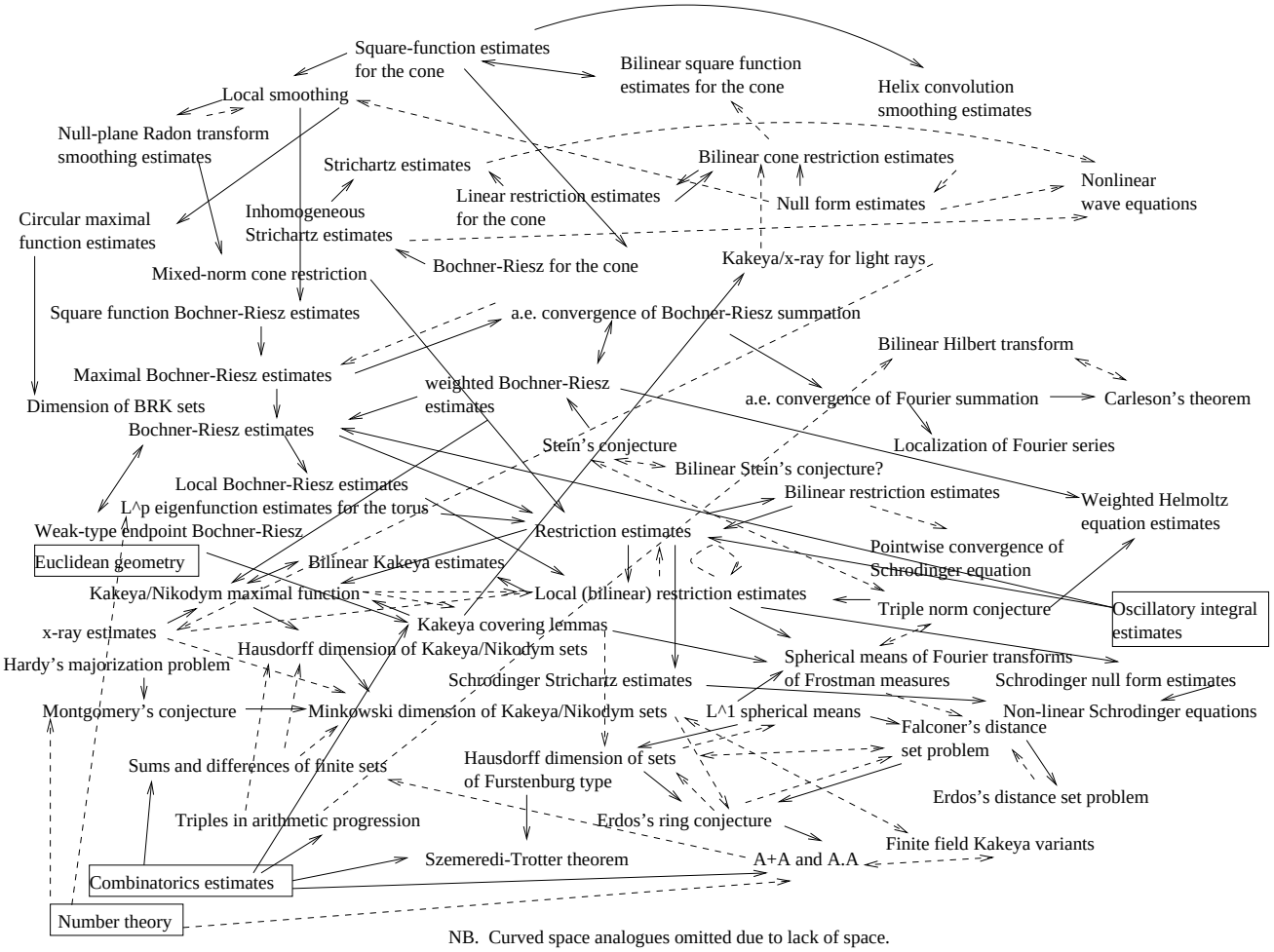
by Hölder's inequality and so the Kakeya Conjecture (6) is implied by the Maximal Kakeya Conjecture (7). It turns out that the Maximal Kakeya Conjecture is equivalent to (it is the dual formulation of) certain L^p boundedness properties of

$$f^*(\omega) \ := \ \sup_{T \parallel \omega} \frac{1}{|T|} \int_T |f(x)| \, dx$$

where the supremum is taken over all δ-tubes oriented in the direction ω. This maximal function is a variant of the classical Hardy-Littlewood maximal function and is the reason why we give the name Maximal Kakeya Problem to this quantitative version of the Kakeya problem. The following are established implications:

Bôchner-Riesz Conjecture ⇒ Fourier Restriction Conjecture ⇒ Maximal Kakeya Conjecture ⇒ Kakeya Conjecture

BUT THIS IS ONLY A PARTIAL LIST AND THERE ARE MANY MANY CONNECTIONS BETWEEN THE CORE PROBLEMS IN EUCLIDEAN HARMONIC ANALYSIS



NB. Curved space analogues omitted due to lack of space.

Exercises

1.1 Show that $\widehat{f} \in C_0\mathbb{R}^n)$ whenever $f \in L^1(\mathbb{R}^n)$. Hint: to show the vanishing at infinity, do it first for simple functions and then pass to a general L^1 function by a density argument.

1.2 Show any $f \in L^p(\mathbb{R}^n), 1 \leq p \leq 2$ can be split as $f = f_1 + f_2$ where $f_1 \in L^1$ and $f_2 \in L^2$. Furthermore, for such a splitting, show that defining the fourier transform for $f \in L^p, 1 \leq p \leq 2$ by $\widehat{f} = \widehat{f_1} + \widehat{f_2}$ does not depend on how we split f.

1.3 Let $f(x) = e^{-\pi x^2}$ be a guassian function on $\mathbb{R}^1$ and define

$$F(\xi) \ := \ \int_{\mathbb{R}} f(x) e^{-2\pi i x \xi} dx.$$

Show that $F'(\xi) = -2\pi\xi F(\xi)$ and hence deduce that $F(\xi) = e^{-\pi\xi^2}$ implying $\widehat{f}(\xi) = e^{-\pi\xi^2}$. Hint: $F(0) = 1$.

1.4 Let $f(x) = e^{-\pi|x|^2}$ be a gaussion on $\mathbb{R}^n$. Here $|x| = x \cdot x = x_1^1 + \cdots + x_n^2$ where $x = (x_1, \ldots, x_n)$. Show that $\widehat{f}(\xi) = e^{-\pi|\xi|^2}$.

1.5 Let $H = \{x = (x_1, \ldots, x_n) : |x| \leq 1, x_n = 0\}$. Consider the possible Fourier restriction inequalities

$$\|\widehat{f}|_H\|_{L^q(H)} \ \leq \ C_{p,q}\|f\|_{L^p(\mathbb{R}^n)}.$$

Show that necessarily $p = 1$ and hence there is no *restriction phenomenon* for H. Hint: for large $\lambda > 0$, consider

$$f(x) = f(x_1, \ldots, x_n) \ := \ \psi(x_1, \ldots, x_{n-1}, x_n/\lambda)$$

where $\psi(x) = e^{-2\pi|x|^2}$ is the gaussian considered in the previous exericse.

1.6 Show the equivalent dual formulation of Restriction Problem (2) is

$$\|(bd\sigma)^\vee\|_{L^{p'}(\mathbb{R}^n)} \ \leq C_{p,q}\|b\|_{L^{q'}(\mathbb{S}^{n-1}, d\sigma)}$$

where $(bd\sigma)^\vee(x) = \int_{\mathbb{S}^{n-1}} b(\omega) e^{2\pi i x\cdot\omega} d\sigma(\omega)$.

From well-known asymptotics for $(d\sigma)^\vee(x)$ (in particular $|(d\sigma)^\vee(x)| \leq C_n|x|^{-(n-1)/2}$), one can see that $(d\sigma)^\vee \in L^{p'}$ if and only if $p'(n-1)/2 > n$ or $p' > 2n/(n-1)$ which implies the conjectured L^p range $1 \leq p < 2n/(n+1)$ for the fourier restriction phenomenon to hold.

1.7 In a similar way as the previous exercise, show the $L^p \to L^q$ mapping property of the restricition operator $Rf = \widehat{f}|_\Gamma$ to the compact piece of the curve $\Gamma : [0,1] \to \mathbb{R}^n$ parameterising the moment curve $\Gamma(t) = (t, t^2, \ldots, t^n)$ is equivalent to $\|Eb\|_{p'} \leq C\|b\|_{q'}$ where

$$Eb(x) \ := \ \int_0^1 b(t)\, e^{2\pi i x\cdot\Gamma(t)}\, dt.$$

Hence determining those exponents p for which $E1 \in L^{p'}(\mathbb{R}^n)$ gives a necessary range on p for which the fourier restriction phenomenon is possible for the moment curve Γ. This turns out to be nontrivial and it was eventually sorted by number theorists. In [2], it was shown that $E1 \in L^{p'}(\mathbb{R}^n)$ exactly when $p' > 0.5n(n+1)+1$. It turns out that $\|E1\|_{p'}$ appears as a constant in the main term of an asymptotic formula for the number of solutions to a system of Diophantine equations, known as Tarry's Problem. Hence knowing when $\|E1\|_{p'}$ is finite has significance for harmonic analysts and number-theorists for different reasons!

2. Harmonic analysis problems in finite fields

In these lectures we replace the real field $\mathbb{R}$ which underpins the core problems in euclidean harmonic analysis with a finite field $\mathbb{F}$ and seek model problems in the setting of $\mathbb{F}^n$. We begin with T. Wolff's finite field Kakeya problem and illustrate how certain well-known arguments, namely Bourgain's bush argument and Wolff's hairbrush argument, simplify in this setting while highlighting some of the key combinatorial features of the euclidean argument. We then go on to give Z. Dvir's [23] complete resolution of the Kakeya problem in finite fields and discuss it's implications for euclidean problems. Finally we will examine the Fourier Restriction Problem in the setting of finite fields, concentrating on the differences with their euclidean cousin.

Finite field Kakeya. In the setting of finite fields, it still makes sense to talk about Kakeya sets; that is, sets $E \subset \mathbb{F}^n$ which contain a line in every direction. A direction in $\mathbb{F}^n$ is represented by a nonzero vector $\vec{b} \in \mathbb{F}^n \setminus \{0\}$ and two nonzero vectors $\vec{b}, \vec{b}'$ represent the same direction if $\vec{b} = t\vec{b}'$ for some $t \in \mathbb{F}$. The number of directions is then $(q^n-1)/(q-1) \sim q^{n-1}$ where $q = \#\mathbb{F}$ is the number of elements in the finite field. A line $\ell_{\vec{a},\vec{b}} = \{\vec{a} + t\vec{b} : t \in \mathbb{F}\}$ is determined by a direction $\vec{b}$ and a point $\vec{a}$ lying on it. Note that $\ell_{\vec{a},\vec{b}} = \ell_{\vec{a},\vec{b}'}$ if $\vec{b}$ and $\vec{b}'$ represent the same direction.

When working in the setting of finite fields, one quickly observes the lack of scales and this is a big difference when passing from euclidean problems where there is a continuum of scales (parameterised by $\mathbb{R}^+$ for instance) to problems over a finite field where there are just one or two scales. In particular there is no difference between a δ-tube and a line in the finite field setting. Furthermore in this finite setting, the natural measure is counting measure and so it does not make sense to talk about sets of measure zero.

Nevertheless it was with great insight that T. Wolff (from the early 1990s), realising that the geometric Kakeya problem in $\mathbb{R}^n$ essentially says that any maximal δ-separated collection of δ-tubes is disjoint, proposed the following interesting finite

field model of the Kakeya problem, see [58]: there exists a universal constant C such that

$$\#E \ \geq \ C\, q^n \quad \text{for every Kakeya set } E \subset \mathbb{F}^n. \tag{8}$$

Hence a Kakeya set E nearly fills out all of $\mathbb{F}^n$ and since $\#\ell = q$ for every line $\ell \subset \mathbb{F}^n$, (8) says that the roughly q^{n-1} lines in E pointing in distinct directions must be essentially pairwise disjoint. Formally, we have the relation $\delta \leftrightarrow q^{-1}$ between the euclidean and finite field setting and a bound $\#E \geq Cq^d$ for all Kakeya sets corresponds to the statement *Kakeya sets have dimension at least d*. T. Wolff's finite field Kakeya problem is a basic question in incidence geometry and it is surprising that it had not been proposed earlier. Several known methods from euclidean harmonic analysis have a particularly simple manifestation in the finite field world.

Bourgain's bush argument [5]**.** In the finite field setting, this argument is the following. Given a set E of q^{n-1} lines $\{\ell\}$ with distinct directions and a multiplicity parameter μ, define a point $x \in \mathbb{F}^n$ to be of *high μ-multiplicity* if there are at least μ lines $\ell_j \in \{\ell\}$ with $x \in \ell_j$. Consider two cases: 1) there is a point x (a bush) of high μ-multiplicity and 2) there is no point in $\mathbb{F}^n$ with μ-multiplicity. In the first case, any μ lines $\{\ell_j\}_{j=1}^{\mu}$ in E with $x \in \ell_j$ are pairwise disjoint (except for the point x where they intersect) and so $\#E \geq \#\cup_{j=1}^{\mu} \ell_j = \mu(q-1)+1 \sim \mu q$. In the second case,

$$q\, q^{n-1} \ = \ \sum_{x \in E} \sum_{\ell \subset E} \chi_\ell(x) \ \leq \ \mu\ \#E$$

implying that $\#E \geq q^n/\mu$. Choosing $\mu = q^{(n-1)/2}$ shows that $\#E \geq Cq^{(n+1)/2}$ and hence *Kakeya sets have dimension at least* $(n+1)/2$. This corresponds to a result of Drury [22] (for the Kakeya Problem) of M. Christ, J. Duoandikoetxea, and J.L. Rubio de Francia [15] (for the Maximal Kakeya Problem) in the euclidean setting, the first nontrivial bound (now called *the trivial bound*) for Kakeya sets in all dimensions. Bourgain [5] used the bush argument as a wedge to bootstrap beyond the trivial bound showing the existence of an $\epsilon_n > 0$ such that the dimension of any Kakeya set is at least $(n+1)/2 + \epsilon_n$.

Cordóba's argument [18]**.** This gives an alternative proof of the Kakeya conjecture in two dimensions (first established by P.O. Davies [19]) and can be upgraded to solve the Maximal Kakeya Problem when $n = 2$. The argument is the following: suppose that $E \subset \mathbb{F}^2$ contains $q/2$ points on a line in each of m different directions, say $\{\ell_j\}_{j=1}^m$ are these lines. Since $\#(\ell_j \cap \ell_k) = 1$ if $j \neq k$ (if $j = k$, we have $\#(\ell_j \cap E) \geq q/2$) and $m \leq q+1$,

$$\sum_{x \in \mathbb{F}^2} \big(\sum_{j=1}^m \chi_{\ell_j}(x)\big)^2 \ = \ \sum_{j=1}^m \sum_{k=1}^m \#(\ell_j \cap \ell_k) \ = \ m(m-1+q) \ \leq \ 2mq$$

and so by the Cauchy-Schwarz inequality,

$$m\, q/2 \ \leq \ \sum_{x \in E} \sum_{j=1}^m \chi_{\ell_j}(x) \ \leq \ (\#E)^{1/2} \big(\sum_{x \in \mathbb{F}^2} \sum_{j=1}^m \chi_{\ell_j}(x)\big)^{1/2} \ \leq \ C\sqrt{(\#E)qm}$$

implying that for such sets E, there is a universal constant C' so that

$$\#E \ \geq \ C'\, m\, q. \tag{9}$$

Since Kakeya sets have the above property with $m = q + 1$, the Kakeya conjecture (8) follows when $n = 2$.

Wolff's hairbrush argument [59]**.** This argument replaces incidences with high multiplicity at a single point (a bush) with incidences with high multiplicity on a line (a hairbrush) and utilises Cordóba's 2-d argument.

Given a set E of q^{n-1} lines $\{\ell_j\}$ with distinct directions and a multiplicity parameter μ, we now define a *line* (instead of a point) $\ell \in \{\ell_j\}$ to be of *high μ-multiplicity* if for at least $q/2$ points $x \in \ell$, the cardinality of $\{j : x \in \ell_j\}$ is a least $\mu+1$. Consider two cases: 1) there is a line ℓ (a hairbrush) of high μ-multiplicity and 2) there are no lines with high μ-multiplicity.

In case 1), let ℓ_k be a line with high μ-multiplicity and let $\{\Pi_i\}$ be an enumeration of the 2-planes containing ℓ_k. Then there are at least $\mu q/2$ lines ℓ_j with $j \neq k$ which intersect ℓ_k. Each such line belongs to a unique 2-plane Π_i and contains $q - 1$ points of Π_i which do not belong to ℓ_k. If $\mathcal{L}_i$ denotes the collection of lines ℓ_j which are contained in Π_i, then by (9) we have

$$\#(E \cap \Pi_i \cap (\mathbb{F}^n \setminus \ell_k) \ \geq \ Cq\, \#\mathcal{L}_i$$

which in turn implies

$$\#E \ \geq \ Cq \sum_i \#\mathcal{L}_i \ \geq \ C\mu q^2 \tag{10}$$

by summing in i and noting that the collections of lines $\mathcal{L}_i$ are pairwise disjoint.

In case 2), set $\tilde{E} := \{x \in E : x \text{ belongs to at most } \mu\ \ell_j' s\}$ and note that $\#\tilde{E} \cap \ell_j \geq q/2$ for every line ℓ_j since there are no lines with high μ-multiplicity. Hence

$$\#E \ \geq \ \#\tilde{E} \ \geq \ \mu^{-1} \sum_{x \in \tilde{E}} \sum_j \chi_{\tilde{E} \cap \ell_j}(x) \ \geq \ \mu^{-1} \sum_j \#(\tilde{E} \cap \ell_j) \ \geq \ \mu^{-1}\, q^{n-1} q/2$$

since each point of $\tilde{E}$ belongs to at most μ of the lines ℓ_j. This bound, together with (10), implies that $\#E \geq Cq^{(n+2)/2}$ by choosing $\mu = q^{(n-2)/2}$.

Wolff's argument in the euclidean setting (which is more involved) shows that all Kakeya sets have dimension at least $(n+2)/2$ and when Wolff announced this result in [59], it was considered a major advance on the conjecture.

Dvir's resolution of finite field Kakeya [23]**.** . Although many established euclidean techniques and partial results for the Kakeya problem have simplified finite field versions, the hope was to go beyond what we know in the euclidean setting, perhaps by attracting people and techniques from other subject areas. Before Dvir came along, little was accomplished in this regard and the only truly finite field result at the time which still does not have a euclidean analogue is due to

Terry Tao who introduced some ideas from algebraic geometry to go beyond what we know about the Kakeya problem in four dimensions.

Z. Dvir shocked the harmonic analysis community and proved the finite field Kakeya conjecture in all dimensions by a simple application of the so-called *polynomial method*, a well-known method employed for instance by K. Roth in his famous (Fields' medal winning) result that any algebraic number cannot be approximated by rationals to any order greater than two (see the Exercise). Here's Dvir's proof:

We begin by recalling that any polynomial $p(x) \in F[X]$ with coefficients in some field F can have at most d roots lying in F where d is the degree of p. Furthermore if $E \subset F$ has cardinality strictly less than d, there is nonzero polynomial $p(x) \in F[X]$ with degree at most d which vanishes on E; that is, $p(x) = 0$ for all $x \in E$. The higher dimensional analogue is the following: if $E \subset F^n$ has cardinality strictly less than $\binom{n+d}{n}$ then there is a nonzero polynomial $p \in F[X_1, \ldots, X_n]$ of degree at most d which vanishes on the set E. The proof only uses elementary linear algebra. First note that $\binom{n+d}{n}$ is the dimension of the vector space V of polynomials in $F[X_1, \ldots, X_n]$ of degree at most d and $\#E$ is the dimension of vector space W of functions $f : E \to F$. Since $\#E < \binom{n+d}{n}$, we see that the linear evaluation map $p \to \{p(x)\}_{x \in E}$ from V to W is non-injective and hence there is a nonzero polynomial p of degree at most d which vanishes on E. Dvir's argument combines this observation with the following proposition.

Proposition 2.1. *Suppose $\mathbb{F}$ is a finite field with q elements and suppose that $p \in \mathbb{F}[X_1, \ldots, X_n]$ is a polynomial of degree at most $q-1$ vanishing on some Kakeya set $E \subset \mathbb{F}^n$. Then p must be the zero polynomial.*

Hence every Kakeya set $E \subset \mathbb{F}^n$ has cardinality at least $\binom{q-1+n}{n}$ and since $\binom{q-1+n}{n} = (1/n!)q^n + O_n(q^{n-1})$ as $q \to \infty$, we arrive a proof of the Kakeya conjecture in finite fields!

Proof. Write $p(x) = \sum_{i=0}^{d} P_i(x)$ where d is the degree of p and for each $0 \leq i \leq d$, P_i denotes the ith homogeneous component. Note that P_d is nonzero if p is nonzero. Also d cannot be zero since p vanishes on E.

Now for any direction $\vec{b} \in \mathbb{F}^n \setminus \{0\}$ there is an $\vec{a} \in \mathbb{F}^n$ such that $\ell_{\vec{a},\vec{b}} \subset E$ since E is a Kakeya set and hence $f(t) := p(\vec{a} + t\vec{b})$ vanishes identically on $\mathbb{F}$ implying that $f \in \mathbb{F}[X]$ is the zero polynomial since the degree d of f is at most $q-1$. The coefficient of t^d in $f(t)$ is $P_d(\vec{b})$ and so is zero. Since $d \geq 1$ and P_d is homogeneous of degree d, we see that P_d must therefore vanish at every point in $\mathbb{F}^n$. For every $(x_2, \ldots, x_n) \in \mathbb{F}^{n-1}$ the polynomial $t \to P_d(t, x_2, \ldots, x_n)$ vanishes on $\mathbb{F}$ and has degree at most $q-1$; hence it is the zero polynomial. Writing $P_d(t, x_2, \ldots, x_n) = \sum_{j=0}^{d} Q_j(x_2, \ldots, x_n)t^j$, we see that each polynomial Q_j of $n-1$ variables vanishes on $\mathbb{F}^{n-1}$ and since the degrees of these polynomials is still at most $q-1$, we can iterate the above observation to conclude that each Q_j and hence P_d is the zero polynomial. This is a contradiction if we suppose that p is nonzero. □

Unfortunately, the polynomial method is extremely dependent on the algebraic nature of the finite field setting and does not seem to extend directly to the euclidean case (though there has been some spectacular success to extend the method to certain problems in discrete combinatorial incidence geometry; most notably the recent resolution of the Erdös distance problem by L. Guth and N. Katz [30] and the joints problem of M. Sharir by Guth, Katz in dimension 3 [31] and H. Kaplan, M. Sharir and E. Shustin [41], independently by R. Quilodrán [45], in all dimensions). On the other hand, this result lends significant indirect support to the euclidean Kakeya conjecture; in particular, the result morally rules out any algebraic counterexample to the euclidean conjecture, since a highly algebraic example to this conjecture would likely be adaptable to the finite field setting. (The examples of zero measure Kakeya sets in the euclidean setting have no finite field analogue, but they are non-algebraic in nature, and in particular take advantage of the multiple scales available in euclidean space.)

Finite Field Maximal Kakeya Conjecture. . Recall from (7) that the euclidean Kakeya Maximal Conjecture is equivalent to the bound

$$\int (\sum_j \chi_{T_j}(x))^{n/(n-1)}\, dx \;\leq\; C_\epsilon \delta^{-\epsilon}$$

holding for every $\epsilon > 0$ and for every maximal δ-separated collection of δ-tubes $\{T_j\}$. Since there is no difference between δ-tubes and lines in the finite field setting due to the lack of scales, the finite field version of the Maximal Kakeya Conjecture states that for every maximal collection $\{\ell_j\}$ of lines in distinct directions (so there are roughly q^{n-1} such lines)

$$q^{-n} \sum_{x \in \mathbb{F}^n} (\sum_j \chi_{\ell_j}(x))^{n/(n-1)} \;\leq\; C \tag{11}$$

and in exactly the same way that (7) implies (6), we see that (11) implies (8); in (11), we are using normalised counting measure to define L^p norms on $\mathbb{F}^n$ in order to model local L^p norms on $\mathbb{R}^n$ defined over some compact set, say. Cordóba's argument described above establishes (11) in two dimensions and the polynomial method used by Dvir has been adapted by J. Eilenberg, R. Oberlin and T. Tao in [24] to establish (11) in all dimensions.

Finite Field Fourier Restriction. In [44], G. Mockenhaupt and T. Tao proposed a finite field model problem for the Fourier Restriction Problem. Although the problem will still ask for $L^p - L^q$ mapping properties of the restriction of the fourier transform, the question needs to be formulated correctly since the space of all complex-valued functions on the finite space $\mathbb{F}^n$ is finite dimensional and all norms (and in particular L^p norms) are equivalent on a finite dimensional vector space!

We fix a non-principal character e on $\mathbb{F}$; that is, a nontrivial additive homomorphism $e : \mathbb{F} \to \mathbb{T}$ into the group $\mathbb{T}$ of complex numbers of modulus 1. For instance if $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ is the finite field of integers modulo p for some prime p, we could set $e(x) := exp(2\pi ix/p)$. Once we find one non-principal character e, we can form others from elements $y \in \mathbb{F}$ by setting $e_y(x) = e(xy)$ (note that $e_1 = e$ and $e_0 \equiv 1$ is the principal character). In fact all characters of $\mathbb{F}$ arise in this way. The exact choice of e will not matter.

The normalisations for Haar measure we choose on the vector space $\mathbb{F}^n$ is counting measure and on the dual space $\mathbb{F}_*^n$ is normalised counting measure so that integrals are defined as

$$\int_{\mathbb{F}^n} f(x)\,dx \;:=\; \sum_{x\in\mathbb{F}^n} f(x) \quad \text{and} \quad \int_{\mathbb{F}_*^n} g(\xi)\,d\xi \;:=\; \frac{1}{q^n}\sum_{\xi\in\mathbb{F}_*^n} g(\xi)$$

which in turn define L^p norms $\|f\|_{L^p(\mathbb{F}^n)}$ and $\|g\|_{L^p(\mathbb{F}_*^n)}$ on $\mathbb{F}^n$ and $\mathbb{F}_*^n$, respectively. We will often abbreviate L^p norms by $\|f\|_p$ if the context is clear.

We define the fourier transform of a complex-valued function on $\mathbb{F}^n$ by

$$\widehat{f}(\xi) \;=\; \int_{\mathbb{F}^n} f(x)\,e(-x\cdot\xi)\,dx$$

where $x\cdot\xi := x_1\xi_1 + \cdots + x_n\xi_n$. Similarly we define the inverse fourier transform

$$g^\vee(x) \;=\; \int_{\mathbb{F}_*^n} g(\xi)\,e(\xi\cdot x)\,d\xi$$

for functions on $\mathbb{F}_*^n$ and one can check that $(\widehat{f})^\vee(x) = f(x)$ as well as $\|f\|_{L^2(\mathbb{F}^n)} = \|\widehat{f}\|_{L^2(\mathbb{F}_*^n)}$, both identities follow by a simple calculation using the key orthogonality property

$$\sum_{x\in\mathbb{F}} e(xy) \;=\; \begin{cases} 0 & \text{if } y \neq 0, \\ q & \text{if } y = 0 \end{cases} \tag{12}$$

which holds for any non-principal character e on $\mathbb{F}$.

For any nonempty $S \subset \mathbb{F}_*^n$ set of frequencies, we endow S with *surface measure* σ which we define by

$$\int_S g(\omega)d\sigma(\omega) \;:=\; \frac{1}{\#S}\sum_{\xi\in S} g(\xi)$$

which in turn allows us to define L^p norms $\|g\|_{L^p(S,d\sigma)}$ for functions g defined on S and also allows us to define the inverse fourier transform of σ by

$$\sigma^\vee(x) \;=\; \int_S e(\xi\cdot x)d\sigma(\xi) \;=\; \frac{1}{\#S}\sum_{\xi\in S} e(\xi\cdot x).$$

The *Finite Field Fourier Restriction Problem* with respect to S is to determine those exponents p and r such that there is a constant $C = C_{p,r,n}$ where

$$\|\widehat{f}|_S\|_{L^r(S,d\sigma)} \leq C\,\|f\|_{L^p(\mathbb{F}^n)} \tag{13}$$

holds; most importantly the constant C, which may depend on p, r and n, should be independent of the cardinality of $\mathbb{F}$ (as well as f of course). We will restrict ourselves to exponents $p, r \geq 1$ and observe that for any S, (13) holds for $p = 1$ and any $r \geq 1$. These are the *trivial* bounds and we say that *the fourier restriction phenomenon occurs* for a set S if (13) holds for some $p > 1$

The dual formulation of the finite field fourier restriction problem is

$$\|(gd\sigma)^\vee\|_{L^{p'}(\mathbb{F}^n)} \leq C\,\|g\|_{L^{r'}(S,d\sigma)} \tag{14}$$

and one can (and should) check that (13) holds if and only if (14) holds with the came constant C.

Consider the example $S = \{\xi = (\xi_1, \ldots, \xi_n) \in \mathbb{F}_*^n : \xi_n = 0\}$ of the ξ_n coordinate hyperplane in $\mathbb{F}_*^n$. For each $x = (x_1, \ldots, x_n) \in \mathbb{F}^n$, set $x' = (x_1, \ldots, x_{n-1})$ so that $x = (x', x_n)$. Let $S^* = \{x \in \mathbb{F}^n : x' = 0\}$ and define $f(x) := (1/q)\chi_{S^*}(x)$ so that $\widehat{f}(\xi) = \chi_S(\xi)$. Therefore $\|\widehat{f}|_S\|_{L^r(S,d\sigma)} = 1$ for every r. On the other hand, $\|f\|_{L^p(\mathbb{F}^n)} = q^{(1/p)-1}$ and therefore with respect to this S, (13) only holds for $p = 1$. so that there is no fourier restriction phenomenon for S and similarly for any affine subspace of $\mathbb{F}_*^n$.

On the other hand, let us consider any example of frequencies S with the property that the fourier transform of its surface measure σ has some *decay*; that is, there is a $\delta > 0$ such that $|\sigma^\vee(x)| \leq Cq^{-\delta}$ holds for all $x \neq 0$ and for some constant C dependent of x and $q = \#\mathbb{F}$ (no such decay estimate holds for surface measure on an affine subspace – see the Exercises). Since

$$\int_S \widehat{f}(\xi)\overline{\widehat{f}(\xi)}d\sigma(\xi) = \frac{1}{\#S}\iint_{\mathbb{F}^n\times\mathbb{F}^n} f(x)\overline{f(y)}\sum_{\xi\in S} e(-\xi\cdot(x-y))dxdy,$$

we have

$$\|\widehat{f}|_S\|_{L^2(S,d\sigma)}^2 \leq \int_{\mathbb{F}^n} |f(x)f * \sigma^\vee(x)|dx \leq \|f\|_{L^p(\mathbb{F}^n)}\|f * \sigma^\vee\|_{L^{p'}(\mathbb{F}^n)} \tag{15}$$

and hence to establish an $L^p \to L^2$ restriction bound (that is, to prove (13) with $r = 2$), it suffices to study the $L^p \to L^{p'}$ mapping properties of $f \to f * \sigma^\vee$.

We can bound $f * \sigma^\vee$ by Young's convolution inequality to obtain

$$\|f * \sigma^\vee\|_{L^{p'}(\mathbb{F}^n)} \leq \|\sigma^\vee\|_{L^s(\mathbb{F}^n)}\,\|f\|_{L^p(\mathbb{F}^n)}$$

where $s = p'/2$. The decay bound $|\sigma^\vee(\xi)| \leq Cq^{-\delta}$ for $\xi \neq 0$ implies that $\|\sigma^\vee\|_{L^s(\mathbb{F}^n)} \leq 2$ whenever $s \geq n/\delta$ and therefore we see that (13) holds for $r = 2$ whenever

$1 \leq p \leq 2n/(2n-\delta)$ implying that the fourier restriction phenomenon holds whenever the fourier transform of surface measure of S has some nontrivial decay.[4] In the euclidean setting, a smooth variety S in $\mathbb{R}^n$ has the property that the fourier transform of its surface measure σ possesses some nontrivial decay $|\sigma^\vee(\xi)| \leq C|\xi|^{-\delta}$ (for some $\delta > 0$) exactly when some curvature of the variety does not vanish to infinite order.

Necessary conditions. In the euclidean setting, for a given variety $S \subset \mathbb{R}^n_*$, there are typically two types of arguments giving necessary condtions for the analogue of (13) to hold. First there is a scaling type argument using homogeneity considerings to test (13) with a scaled family f_δ so that $\widehat{f_\delta}$ is supported near S for all $\delta > 0$. These are sometimes referred to as Knapp-type examples and gives a necessary relationship between the exponents p, r. Due to the lack of scales in finite fields, this type of example reduces to testing (13) with an f such that $\widehat{f} = \delta_\eta$ where δ_η is the dirac mass at some $\eta \in S$ (it is this lack of scaling argument in finite field setting where we begin to see the difference with the euclidean problem). In this case, $f(x) = e(x \cdot \eta)/q^n$ so that $\|f\|_p = q^{-n/p'}$. On the other hand, $\|\widehat{f}|_S\|_r = [\#S]^{-1/q}$ leading to the necessary relation $p' \geq rn/d$ where $\#S \sim q^d$, say.

The other argument uses the dual formulation (14) to give a necessary L^p range for the fourier restriction phenomenon to happen. Here we take $g \equiv 1$ so that the $L^{r'}(S, d\sigma)$ norm of g is equal to 1 and therefore a uniform in q bound for the $L^{p'}(\mathbb{F}^n)$ norm for $\sigma^\vee$ gives a necessary condition on the p exponents for there to be any possible restriction estimate. Unlike the euclidean case, it is often the case the best possible uniform decay estimate for $\sigma^\vee$ gives the best possible p' range for uniform bounds of the $L^{p'}(\mathbb{F}^n)$ norm for $\sigma^\vee$. Again this is due in part to the lack of scales in finite fields.

From above we see that if $|\sigma^\vee(x)| \leq Cq^{-d'/2}$ for $x \neq 0$, then $\|\sigma^\vee\|_{L^{p'}(\mathbb{F}^n)} \leq 2$ whenever $p' \geq 2n/d'$ and therefore we arrive at the general necessary conditions

$$p' \geq rn/d \quad \text{and} \quad p' \geq 2n/d' \tag{16}$$

for any variety S having the follwing two properties: (1) $\#S \sim q^d$ and (2) there is a constant C indepedent of q such that $|\sigma^\vee(x)| \leq Cq^{-d'/2}$ holds for all nonzero $x \in \mathbb{F}^n$.

In this discrete setting, the exponent d in $\#S \sim q^d$ can be interpreted as the*geometric dimension* of the variety S and the exponent d' in the best possible decay bound for $\sigma^\vee$ can be interpreted as the *fourier dimension* of S. Both dimensions have precise formulations in the euclidean setting where it is always the case that $d' \leq d$ although strict inequality holds more often than not. In the finite field setting, it is still the case that $d' \leq d$ (simply note that $\|\sigma^\vee\|_2 \sim q^{(n-d)/2}$ if $\#S \sim q^d$) however as long as S does not contain an affine subspace or similar obstructions, we tend to have $d = d'$ which follows from work of Weil, Deligne and others on the Riemann hypothesis in finite fields.

[4]This is the finite field version of Stein's original argument from the mid 1960s illustrating the fourier restriction phenomenon for the sphere

Basic examples. A standard example is the *finite field paraboloid* $S = \{\xi = (\xi', \xi_n) \in \mathbb{F}_*^n : \xi_n = \xi' \cdot \xi'\}$. It is not difficult to compute

$$\sigma^\vee(x) = \int_S e(\xi \cdot x) d\sigma(\xi) = \frac{1}{q^{n-1}} \sum_{\xi' \in \mathbb{F}_*^{n-1}} e(x' \cdot \xi' + x_n \xi' \cdot \xi') = \prod_{j=1}^{n-1} G(x_n, x_j)$$

which splits into an $(n-1)$-fold product of Gauss sums $G(a,b) = \int_{\mathbb{F}_*} e(ay^2 + by) dy$. Easier yet is to compute $|G(a,b)|$; in fact if $2a \neq 0$,

$$|qG(a,b)|^2 = \sum_{y \in \mathbb{F}_*} \sum_{z \in \mathbb{F}_*} e(a(y-z)(y+z) + b(y-z)) = \sum_{u \in \mathbb{F}_*} e(au^2 + bu) \big[\sum_{z \in \mathbb{F}_*} e(2auz) \big] = q$$

since the last z sum is equal to 0 for $u \neq 0$. If $a = 0$, then $G(0,b) = 0$ if $b \neq 0$ and $G(0,0) = 1$ which provided the charateristic of $\mathbb{F}$ is not equal to 2 gives $|G(a,b)| = q^{-1/2}$ when $a \neq 0$ and $G(0,b) = 0$ or 1 depending whether $b \neq 0$ or $b = 0$, respectively. If the characteristic of $\mathbb{F}$ is 2, then $G(a,b) = 1$ for all choices of $a, b \in \mathbb{F}$.

Hence if the charateristic of $\mathbb{F}$ is not equal to 2, then $|\sigma^\vee(x)| \leq q^{-(n-1)/2}$ for all $x \neq 0$ and so in this case, $d = d' = n-1$ since $\#S = q^{n-1}$.

Another example of interest is the moment curve $S = \{(y, y^2, \dots, y^n) \in \mathbb{F}_*^n : y \in \mathbb{F}_*\}$. Here

$$\sigma^\vee(x) \;=\; \int_S e(\xi \cdot x) d\sigma(\xi) \;=\; \frac{1}{q} \sum_{y \in \mathbb{F}_*} e(x_1 y + x_2 y^2 + \cdots + x_n y^n)$$

is an exponential sum over a finite field and it is a nontrivial fact that $|\sigma^\vee(x)| \leq C_n q^{-1/2}$ for all $x \neq 0$ provided that the charateristic of $\mathbb{F}$ exceeds n; this is due to A. Weil [57] and follows as a consequence from his solution of the Riemann hypothesis for curves in finite fields. Since $\#S = q$ for this example, we have $d = d' = 1$ if the characteristic of $\mathbb{F}$ is larger than n.

Here we begin to see differences with the euclidean problem. For the paraboloid, the lack of scales in fnite fields imposes a weaker necessary relation between the exponents $p' \geq nr/(n-1)$ compared to the stronger (more restrictive) relation $p' \geq (n+1)r/(n-1)$ in the euclidean case. The same is true for the moment curve, the necessary condition $p' \geq rn$ in the finite field setting is more restrictive than the condition $p' \geq rn(n+1)/2$ for the euclidean problem.

On the other hand, the necessary range $p' \geq 2n/(n-1)$ of p exponents for there to be a restriction phenomenon for the paraboloid is the same more or less (up to an endpoint) in both settings. However for the moment curve, the necessary p range $p' \geq 2n$ in the finite field setting is again less restrictive than the necessary range $p' > 0.5n(n+1)+1$ in the euclidean setting.

Stein-Tomas argument. Recall the sharp L^2 (where we fix $r = 2$) fourier restriction esitmate for spheres obtained by Stein and Tomas showing that (1) holds precisely in the range $p' \geq (2n+2)/(n-1)$. The argument uses only two ingredients about spheres; namely that the geometric dimension is $n-1$ and that the fourier dimension is also $n-1$. The same estimate holds for any hypersurface with nonvanishing gaussian curvature and in fact it gives one the same bound in any setting where the two dimensions are $n-1$. In particular we will illustrate the argument here in the finite field setting but we will return to this argument later and show how it works in a very general setting incorporating both the finite field and euclidean settings as particular instances.

Proposition 2.2. *Let $S \subset \mathbb{F}_*^n$ be a variety with the following two properties; 1) $\#S = q^d$ and 2) for some constant C, we have the uniform bound $|\sigma^\vee(x)| \leq Cq^{-d'/2}$ for all $x \neq 0$. Then (13) holds for for $p' \geq 2(2n+d'-2d)/d'$.*

Applying Proposition 2.2 to the paraboloid S where $d = d' = n-1$ shows that (13) with $r = 2$ holds for $p' \geq 2(n+1)/(n-1)$ which matches what one gets in the euclidean setting but in the finite field setting, this is (presumably) a suboptimal estimate.

Proof. We start as in (15) to reduce matters to bounding the operator $Tf := f * \sigma^\vee$ from L^p to $L^{p'}$ but instead of using Young's inequality we will now bound the operator T more efficiently. We decompose $\sigma^\vee(x) = \sigma^\vee(x)\chi_{x\neq 0}(x) + \delta_0(x) := K(x) + \delta_0$ where δ_0 is the dirac mass at the origin; $\delta_0(x) = 1$ if $x = 0$ and 0 otherwise. This leads to a decomposition of $T = T_1 + T_2$ where $T_2 = Id$ is the identity operator.

This decomposition is the finite field version of a Littlewood-Paley decomposition where in the euclidean setting, we would decompose $\sigma = \sum_k \sigma_k$ into dyadic annuli in frequency/fourier space. Recall that there is a lack of scales in finite fields and this is reflected in the fact the appropriate Littlewood-Paley decomposition in this setting is to decompose the fourier transform into just two pieces (as opposed to countably many dyadic pieces), one at the origin 0 and one away from the origin.

For $p \leq 2$, we have $\|T_2 f\|_{p'} \leq \|f\|_p$ and to estimate T_1, we use the bounds $\|K\|_\infty \leq Cq^{-d'/2}$ which is simply 2), the hypothesised uniform decay bound for $\sigma^\vee$, and $\|\widehat{K}\|_\infty \leq q^n/\#S = q^{n-d}$ which follows from 1), $\#S = q^d$. Therefore $\|Tf\|_2 \leq Cq^{n-d}\|f\|_2$ and $\|Tf\|_\infty \leq Cq^{-d'/2}\|f\|_\infty$ which implies (by interpolation)

$$\|Tf\|_{p'} \;\leq\; C_p q^{2(n-d)/p'} q^{-d'(1/2-1/p')}\|f\|_p \;\leq\; C_p\|f\|_p$$

if $p' \geq 2(2n+d'-2d)/d'$. □

Fefferman-Sjölin-Zygmund argument. We now show how an argument which dates back to C. Fefferman [28], Sjölin [48] and Zygmund [64] plays out in the finite field setting. It is particularly effective when the variety S is *m-dimensional*, $\#S \sim q^m$, and when there is a k so that we have a good bound on the number of representations of any $\eta \in \mathbb{F}_*^n$ by a k-fold sum of elements from S; that is, we have a good bound on the number of ways we can write $\eta = \xi_1 + \cdots + \xi_k$ where each $\xi_j \in S$.

Proposition 2.3. *Let $S \subset \mathbb{F}_*^n$ be a variety which can be parametrised by the graph of a map $\Phi : \mathbb{F}_*^m \to \mathbb{F}_*^{n-m}$ so that $S = \{\Psi(t) := (t, \Phi(t)) : t \in \mathbb{F}_*^k\}$. Suppose that for every $\eta \in \mathbb{F}_*^n$, the number of ways we can represent η as a sum of k elements in S is at most A; that is we suppose that,*

$$\#\{(t_1, \dots, t_k) \in (\mathbb{F}_*^m)^k : \eta = \Psi(t_1) + \Psi(t_2) + \cdots + \Psi(t_k)\} \ \leq \ A \tag{17}$$

holds for some A. Then (14) holds for $p' \geq kr$ and $p' \geq 2k$ with a constant $C = q^{n/kr} q^{-m/r} A^{1/kr}$. Hence we obtain a uniform $L^p \to L^r$ fourier restriction bound (13) if $p' \geq rk, 2k$ and $A \leq C q^{k-n}$.

Proof. With S parametrised as a graph, we see that the surface measure σ of S has the property

$$gd\sigma(\phi) \ = \int_{\mathbb{F}_*^m} \phi(\Psi(t)) g(t) dt \ = \ \frac{1}{q^m} \sum_{t \in \mathbb{F}_*^m} \phi(\Psi(t)) g(t)$$

for any density function g; here we identify density functions with functions defined on the parameter space $\mathbb{F}_*^m$.

It suffices to prove (14) for $p' = kr \geq 2k$. Hence by the Hausdorff-Young inequality,

$$\|(gd\sigma)^\vee\|_{p'}^k \ = \ \|[(gd\sigma)^\vee]^k\|_{p'/k} \ = \ \|(gd\sigma * \cdots * gd\sigma)^\vee\|_r \ \leq \ \|gd\sigma * \cdots * gd\sigma\|_{r'}$$

where the $* \cdots *$ denotes a k-fold convolution. Writing $\vec{t} = (t_1, \dots, t_k) \in (\mathbb{F}_*^m)^k$, $\Gamma(\vec{t}) = \Psi(t_1) + \cdots + \Psi(t_k)$ and $G(\vec{t}) = g(t_1) \cdots g(t_k)$, we have

$$gd\sigma * \cdots * gd\sigma(\phi) \ = \int_{(\mathbb{F}_*^m)^k} \phi(\Gamma(\vec{t}) G(\vec{t}) d\vec{t} \ = \ \frac{1}{q^{mk}} \sum_{\vec{t} \in (\mathbb{F}_*^m)^k} G(\vec{t}) \sum_{\eta \in \mathbb{F}_*^n : \eta = \Gamma(\vec{t})} \phi(\eta)$$

$$= \ \frac{1}{q^{mk}} \sum_{\eta \in \mathbb{F}_*^n} \phi(\eta) \sum_{\vec{t} \in (\mathbb{F}_*^m)^k} G(\vec{t}) \ \chi_{T_\eta}(\vec{t}) \ = \ \int_{\mathbb{F}_*^n} \phi(\eta) D(\eta) d\eta$$

where $T_\eta = \{\vec{t} \in (\mathbb{F}_*^m)^k : \Gamma(\vec{t}) = \eta\}$ and

$$D(\eta) \ := \ q^{n-mk} \sum_{\vec{t} \in (\mathbb{F}_*^m)^k} G(\vec{t}) \ \chi_{N_\eta}(\vec{t})$$

is the density of the measure $gd\sigma * \cdots * gd\sigma$. Hence $\|gd\sigma * \cdots * gd\sigma\|_{r'} = \|D\|_{r'}$ and so

$$\|gd\sigma * \cdots * gd\sigma\|_s^s \ = \ \frac{q^{(n-mk)r'}}{q^n} \sum_{\eta \in \mathbb{F}_*^n} \Big| \sum_{\vec{t} : \Phi(\vec{t}) = \eta} G(\vec{t}) \Big|^{r'}.$$

We set $T_\eta := \{\vec{t} \in (\mathbb{F}_*^m)^k : \Gamma(\vec{t}) = \eta\}$ and write the above $L^{r'}$ norm as

$$\|gd\sigma * \cdots * gd\sigma\|_{r'}^{r'} \;=\; \frac{q^{(n-mk)r'}}{q^n} \sum_{\vec{s}\in(\mathbb{F}_*^m)^k} \frac{1}{\#T_{\Gamma(\vec{s})}} \Big| \sum_{\vec{t}:\Gamma(\vec{t})=\Gamma(\vec{s})} G(\vec{t}) \Big|^{r'}$$

which can be estimated above, via Hölder's inequality in the $\vec{t}$ sum, showing

$$\|gd\sigma * \cdots * gd\sigma\|_{r'}^{r'} \;\le\; \frac{q^{(n-mk)r'}}{q^n} \sum_{\vec{t}\in(\mathbb{F}_*^m)^k} |G(\vec{t})|^{r'} \, [\#T_{\Gamma(\vec{t})}]^{r'-1}. \tag{18}$$

Since $\#T_{\Gamma(\vec{t})} \le A$ uniformly in $\vec{t}$ by (17), we have

$$\|(gd\sigma^\vee\|_{p'} \le \|gd\sigma * \cdots * gd\sigma\|_{r'}^{1/k} \;\le\; q^{n/kr} q^{-m/r} A^{1/kr} \|g\|_{L^{r'}(\mathbb{F}_*^m)}.$$

□

We now apply Proposition 2.3 to the moment curve $S = \{(t, t^2, \dots, t^n) : t \in \mathbb{F}\}$ with $k = n$ when $\mathrm{char}(\mathbb{F}) > n$. Here $m = 1$, $\Psi(t) = (t, t^2, \dots, t^n)$ and $\Gamma(\vec{t}) = \Psi(t_1) + \cdots + \Psi(t_n)$. We claim that $\#T_\eta \le n!$ so that we can take $A = n!$ and hence we have the following corollary, proved in [44].

Corollary 2.4. *For the moment curve S, the restriction estimates* (13) *and/or* (14) *holds with a uniform constant C if and only if $p' \ge rn$ and $p' \ge 2n$.*

Proof. As we have already seen that it suffices to show that for any given $\eta \in \mathbb{F}_*^n$, the number of $\vec{t} = (t_1, \dots, t_n) \in \mathbb{F}_*^n$ of n-tuples of elements from $\mathbb{F}$ which satisfy $\Gamma(\vec{t}) = \eta$ is at most $n!$ if $\mathrm{char}(\mathbb{F}) > n$. Consider two solutions $\vec{t}, \vec{s}$ so that $\Gamma(\vec{t}) = \Gamma(\vec{s})$ and consider the two monic polynomials

$$T(x) = \prod_{j=1}^n (x - t_j) = \sum_{j=0}^n (-1)^j e_{n-j}(\vec{t}) x^j \quad \text{and} \quad S(x) = \prod_{j=1}^n (x - s_j) = \sum_{j=0}^n (-1)^j e_{n-j}(\vec{s}) x^j$$

whose roots are given by $\vec{t}$ and $\vec{s}$, respectively. Here $e_0 = 1$ and for $1 \le j \le n$,

$$e_j(\vec{t}) \;=\; \sum_{1 \le k_1 < \cdots < k_j \le n} t_{k_1} \cdots t_{k_n}$$

define the elementary symmetric polynomials in n variables and these can be expressed in terms of the symmetric power functions $p_j(\vec{t}) = t_1^j + \cdots + t_n^j$ for $1 \le j \le n$ via the Newton-Girard formulae; $k e_k = \sum_{i=1}^k (-1)^{i-1} e_{k-i} p_i$. Since $p_i(\vec{t}) = \eta_i = p_i(\vec{s})$ for each $1 \le i \le n$, we have $k e_k(\vec{t}) = k e_k(\vec{s})$ for each $1 \le k \le n$. If $\mathrm{char}(\mathbb{F}) > n$, then we see that the polynomials S and T above define the same polynomial from which we deduce that the two ordered sets of roots $\vec{t} = (t_1, \dots, t_n)$ and $\vec{s} = (s_1, \dots, s_n)$ must differ by a permutation. This shows that there are at most $n!$ solutions to $\Gamma(\vec{t}) = \eta$. □

We highlight that the argument above, bounding the number of solutions $\vec{t}$ to $\Gamma(\vec{t}) = \eta$, is valid in many rings with characteristic larger than n. However the fact used above that a monic polynomial with coefficients

in a ring R is uniquely determined by its roots does not hold in general. This is the case for rings with no zero divisors, but it is not true in general and is closely related to the 'fact' that in integral domains, the number of roots of a polynomial does not exceed its degree. Consider for example the polynomial $p(x) = x^2 - 5x$ with coefficients in the ring $R = \mathbb{Z}/6\mathbb{Z}$, it has roots $x = 0, 2, 3$ and 5 in the ring R and in particular $p(x) = x(x-5) = (x-2)(x-3)$.

Exercises

2.1 Suppose $\mathbb{F}$ has q elements. Show that the number of directions in $\mathbb{F}^n$ is $(q^n - 1)/(q-1)$.

2.2 Fix n and consider $q \to \infty$. Show that $\binom{q-1+n}{n} = (1/n!)q^n + O(q^{n-1})$.

2.3 Show that two lines $\ell_{\vec{a},\vec{b}}$ and $\ell_{\vec{a},\vec{c}}$ are the same line in $\mathbb{F}^n$ if and only if $\vec{b}$ and $\vec{c}$ represent the same direction.

2.4 Use Cordóba's argument to establish the finite field Maximal Kakeya Conjecture in two dimensions.

2.5 Show that (11) implies (8).

2.6 Let V be the vector space of all polynomials $p \in \mathbb{F}[X_1, \ldots, X_n]$ of degree at most d. Show that $\dim V = \binom{n+d}{n}$.

2.7 Let α be an algebraic number of degree $d \geq 2$ and prove Liouville's theorem that there is a constant $c = c(\alpha)$ such that

$$|\alpha - p/q| \;\geq\; c/q^d \quad \text{for every rational} \;\; p/q \tag{19}$$

by completing the following steps: 1) let $f \in \mathbb{Z}[X]$ have degree d such that $f(\alpha) = 0$ and note for any rational p/q with $f(p/q) \neq 0$, we have $1/q^d \leq |f(p/q)|$, and 2) on the other hand, $|f(p/q)| \leq M|\alpha - p/q|$ follows by expanding f around $x = \alpha$.

Now try to improve Liouville's result by finding a polynomial $g \in \mathbb{Z}$ of small degree r on the one hand, and having α as a root with high multiplicity m on the other hand. The above argument then shows that (19) holds with d replaced by r/m. (You should fail by realising that necessarily $r/m \geq d$).

Thue however used this idea, but now looking for polynomials $g \in \mathbb{Z}[X,Y]$ of two variables and he was able to improve Liouville's result, replacing d with $d/2$. Thus began the *polynoimial method* and eventually Roth succeeded, using polynomials of many variables to show every algebraic number α is not approximable by rationals to any order greater than 2! He won a Field's medal for this.

2.8 Let $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ be the field of integers modulo a prime p. Show that if $E : \mathbb{F} \to \mathbb{T}$ is a character of $\mathbb{F}$, then there is a $y \in \mathbb{F}$ such that $E(x) = e^{2\pi i xy/p}$.

2.9 Prove the orthogonality relations (12) for any non-principal character e on a finite field $\mathbb{F}$. And then go on to establish the claimed identities $\widehat{f}^{\vee}(x) = f(x)$ and $\|\widehat{f}\|_{L^2(\mathbb{F}_*^n)} = \|f\|_{L^2(\mathbb{F}^n)}$.

2.10 Show that two formulation of the finite field fourier restriction problem (13) and (14) are equivalent.

2.11 Let $H = \{\xi = (\xi_1, \dots, \xi_n) \in \mathbb{F}_*^n : \xi_n = 0\}$ be the ξ_n coordinate hyperplane in $\mathbb{F}_*^n$. Show that the surface measure σ of H satisfies $(d\sigma)^{\vee}(x) = 1$ for all $x' = (x_1, \dots, x_{n-1}) \neq 0$. Hence $(d\sigma)^{\vee}(x)$ has no uniform decay bound away from $x = 0$.

2.12 Suppose that the field $\mathbb{F}$ has characteristic equal to 2. For a given pair of elements $a, b \in \mathbb{F}$, examine the number of solutions $(x, y) \in \mathbb{F}^2$ to the system of equations $x + y = a$ and $x^2 + y^2 = b$. Does the number depend on the choice of a, b?

2.13 Let R be a ring whose charcteristic is either 0 or if positive, is larger than n. Consider the system of equations

$$x_1 + \cdots + x_n = a_1,\ x_1^2 + \cdots + x_n^2 = a_2,\ \dots,\ x_1^n + \cdots + x_n^n = a_n$$

for a fixed n-tuple $(a_1, \dots, a_n) \in R^n$. Show that if R has no zero divisors (that is, R is an integral domain), then the above system has at mosts $n!$ solutions $(x_1, \dots, x_n)$ in R^n.

2.14 Consider the ring $R = \mathbb{Z}/N\mathbb{Z}$ of integers modulo N with $N = p^L$ a power of a prime p. For $u, v \in R$, let

$$T_{u,v} \ := \ \{(x, y) \in R^2 : x + y = u + v, \text{ and } x^2 + y^2 = u^2 + v^2\}$$

be the collection of solutions to a pair of diophantine equations in R. Show that $\#T_{u,v} \leq 2\, gcd(u - v, p^L)$. Generalise this to an arbitrary integer N but now we have $\#T_{u,v} \ll gcd(u - v, N)$. Finally, show by example that this is no universal constant C such that $\#T_{u,v} \leq C gcd(u - v, N)$.

3. Harmonic analysis problems over the integers $\mathbb{Z}$

We begin by giving a brief survey of some results in ergodic theory due to Bourgain and connections with work of Stein and Wainger on singular integral variants. These problems are discrete analogues of euclidean harmonic analysis problems where the underlying real field $\mathbb{R}$ is replaced by the ring of integers $\mathbb{Z}$. In this discrete setting the objects which correspond to oscillatory integrals in the euclidean setting are exponential sums. There are many techniques and methods which have been developed over the years to understand exponential sums but one of the more powerful ones is the so-called circle method from analytic number theory. We plan to give a crash course on this famous Hardy-Littlewood-Ramanujan circle method in the context of the work of Stein and Wainger, illustrating how it can be used to understand exponential sums which arise as Fourier multipliers.

Pointwise ergodic problems. The setting of much of ergodic theory is a *dynamical system* which is a probability space $(X, \mathcal{B}, \mu)$, together with an invertible measure-preserving transformation $T : X \to X$; that is, X is a set with a σ-algebra of subsets $\mathcal{B}$ called the *measurable* sets, and $\mu : \mathcal{B} \to [0, 1]$ is a probability measure on $(X, \mathcal{B})$ so that $\mu(X) = 1$ and $\mu(\emptyset) = 0$. Furthermore, for every $E \in \mathcal{B}$, we have $T^{-1}(E) \in \mathcal{B}$ and $\mu(T^{-1}(E)) = \mu(E)$. We often supress mentioning the σ-algebra $\mathcal{B}$ explicitly although it is understood to be there in the background.

The dynamics of such a system is then given by the iterates of $T, T^2 = T \circ T, T^3 = T \circ T \circ T$, etc... however the dynamics can be given more generally by a semi-group (or even a group) of measure-preserving transformations; for example, it could be described by a *flow* $\{T_t\}_{t \geq 0}$ such that $T_0 = \text{Identity}$ and $T_{s+t} = T_s \circ T_t$.

A famous theorem of Birkhoff states the following: if (X, μ, T) is a dynamical system, then for every $f \in L^1(X, \mu)$, the *time* averages

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} f(T^n x) \tag{20}$$

exists for μ *almost every* $x \in X$. Furthermore if T is *ergodic* (that is whenever $T^{-1}(E) = E$ for some measurable E, either $\mu(E) = 0$ or $\mu(E) = 1$), then the limit in (20) is constant and equals to $\int_X f d\mu$. In other words, the time avarages equals the space average.

Bourgain was interested in generalising this result by considering time averages along a sparse sequence of the orbit $\{T^n x\}$; for example, he asked what happens when one averages along the squares of the interates $\{T^{n^2} x\}$. In [7], [8] and [9], Bourgain proved the following:

Proposition 3.1. *Let (X, μ, T) be a dynamical system. For any $f \in L^p(X, \mu)$ with $p > 1$, the averages $1/N \sum_{n=1}^{N} f(T^{n^2} x)$ converge as $N \to \infty$ for μ almost every $x \in X$.*

In [8] and [9], Bourgain extended this result, replacing the squares $\{n^2\}$ with any polynomial sequence $\{p(n)\}$ where p is an general polynomial with integer coefficients.

One approach to these *pointwise ergodic theorems* is to control the corresponding maximal function. In the case of Birkhoff's original result, we want to bound $f^*(x) := \sup_N 1/N|\sum_{n=1}^N f(T^n x)|$ and in the case of Bourgain's result Proposition 3.1, we want to control

$$f^*_{sq}(x) \ := \ \frac{1}{N}\Big|\sum_{n=1}^N f(T^{n^2}x)\Big|.$$

It is a straightforward exercise to show that if we knew the maximal function was bounded on some L^p space AND we knew that the the pointwise convergence result (for example, (20) in the case of the classical time averages) held for a dense class of functions f in L^p, then we could deduce that the pointwise convergence result held for all $f \in L^p$.

In general it is not straightforward to verify the pointwise convergence result for some dense class of functions, especially in the setting of a general dynamical system, and so obtaining L^p bounds for the associated maximal function should only be considered as a step (albeit a major step in many cases) in the proof of a pointwise ergodic theorem.

A transference principle. Many a priori estimates for ergodic averages can be established from *transferring* the corresponding estimate on the simple system $(\mathbb{Z}, S)$ where $S(n) = n + 1$ is the shift transformation $S : \mathbb{Z} \to \mathbb{Z}$. The shift S is measure preserving if we take counting measure m as our measure on $\mathbb{Z}$. We illustrate here how L^p bounds for the maximal function f^* above follow from the corresponding $\ell^p = L^p(\mathbb{Z}, m)$ bounds for the classical Hardy-Littlewood maximal function

$$Mf(j) \ := \ \sup_N \frac{1}{N}\Big|\sum_{n=1}^N \phi(S^n j)\Big| \ = \ \sup_N \frac{1}{N}\Big|\sum_{n=1}^N \phi(j+n)\Big|$$

on the integers $\mathbb{Z}$. It suffices to consider $f^*_0(x) := \sup_{N\le N_0} 1/N|\sum_{n=1}^N f(T^n x)|$ and obtain L^p bounds independent of N_0. Fix $J \gg N_0$ and $x \in X$ and define a function ϕ on $\mathbb{Z}$ by $\phi(j) := f(T^j x)$ for $1 \le j \le J$ and zero otherwise. Note that

$$\frac{1}{N}\sum_{n=1}^N \phi(j+n) \ = \ \frac{1}{N}\sum_{n=1}^N f(T^n(T^j x)) \quad \text{for } \ 1 \le j \le J - N_0$$

so that

$$M_0\phi(j) \ := \ \sup_{N\le N_0} \frac{1}{N}\Big|\sum_{n=1}^n \phi(j+n)\Big| \ = \ \sup_{N\le N_0} \frac{1}{N}\Big|\sum_{n=1}^N f(T^n T^j x)\Big| \ = \ f^*_0(T^j x)$$

for $1 \le j \le J - N_0$. The inequality $\|M_0\phi\|_{\ell^p} \le \|M\phi\|_{\ell^p} \le C_p\|\phi\|_{\ell^p}$ implies

$$\sum_{j\le J-N_0} |f^*_0(T^j x)|^p \ \le \ C_p^p \sum_{j\le J} |f(T^j x)|^p.$$

Integrating in x over X and using the invariance of the transformation T with respect to μ shows

$$(J - N_0) \int_X |f_0^*(x)|^p d\mu(x) \ \leq \ C_p^p \, J \int_X |f(x)|^p d\mu(x)$$

which implies $\|f_0^*\|_p \leq C_p \|f\|_p$ by taking $J \to \infty$.

The same argument works for many other maximal functions including Bourgain's maximal function f_{sq}^* along the squares, reducing its L^p boundedness properties to the associated maximal function

$$M_{sq}\phi(j) \ = \ \sup_{N \geq 1} \frac{1}{N} \Big| \sum_{n=1}^{N} \phi(j + n^2) \Big|$$

along the squares in $\mathbb{Z}$. Furthermore weak-type bounds (for example, $\mu(x \in X : f^*(x) \geq \lambda) \leq C\lambda^{-1}\|f\|_1$) can be deduced in a similar way from the corresponding weak-type bound on the integers $\mathbb{Z}$. The above transference arugment is is an instance of what is commonly known as Calderón's Transference Principle.

It is well-known that the Hardy-Littlewood maximal function M satisfies a weak-type bound on ℓ^1 as described above (via a covering lemma argument for instance) and so by an interpolation argument, one obtains ℓ^p bounds for M for all $1 < p \leq \infty$. Hence by the Calderón Transference Principle introduced above, we see that the maximal function f^* of classical ergodic/time averages also satisfies weak-type bounds on $L^1(X, \mu)$ as well as $L^p(X, \mu), 1 < p \leq \infty$ bounds.

From $\mathbb{R}$ to $\mathbb{Z}$ and back again. We pause here to examine the relationship between the classical Hardy-Littlewood maximal function Mf on $\mathbb{Z}$ and the corresponding Hardy-Littlewood maximal function

$$\mathcal{M}f(x) \ := \ \sup_{h>0} \frac{1}{h} \int_0^h |f(x + t)| dt$$

on the real line $\mathbb{R}$ as well as the relationship between Bourgain's maximal fucntion M_{sq} and its cousin on the reals. Interestingly in Hardy and Littlewood's original paper [32] studying the basic mapping properties of $\mathcal{M}$, they discretized the problem, reducing matters to the maximal function M on the integers $\mathbb{Z}$ which allowed them to introduce their famous rearrangement argument reducing matters further to combinational issues. Nowadays though people usually analyse M or $\mathcal{M}$ via covering lemma arguments introduced by N. Weiner.

Let us now proceed in the opposite direction of Hardy and Littlewood's original approach and see how one can pass from M to $\mathcal{M}$. We start with a nonnegative function ϕ on the integers $\mathbb{Z}$ and construct a nonnegative function f on $\mathbb{R}$ by setting

$f(x) = \phi(j)$ if $x \in (j-1, j]$. We observe that for $j - 1 < x \leq j$,

$$\frac{1}{N}\sum_{n=1}^{N} \phi(j+n) \;=\; \frac{1}{N}\int_{j-x}^{j-x+N} f(x+t)dt \;\leq\; 2\frac{1}{N+1}\int_{0}^{N+1} f(x+t)dt$$

and therefore we have the pointwise bound $M\phi(j) \leq 2\mathcal{M}f(x)$. Therefore

$$\sum_{j\in\mathbb{Z}} |M\phi(j)|^p \;\leq\; 2\int_{\mathbb{R}} \mathcal{M}f(x)^p dx$$

and this, together with the fact that $\|\phi\|_{\ell^p} = \|f\|_{L^p(\mathbb{R})}$ shows how we can deduce ℓ^p bounds for M from $L^p(\mathbb{R})$ bounds for $\mathcal{M}$. A similar argument shows how we can deduce weak-type bounds for M from the corresponding bounds for $\mathcal{M}$.

The continuous analogue for Bourgain's maximal function M_{sq} is

$$\mathcal{M}_{sq}f(x) \;:=\; \sup_{h>0}\Big|\frac{1}{h}\int_0^h f(x+t^2)dt\Big| \;=\; \sup_{h>0}\Big|\frac{1}{2h}\int_0^{h^2} f(x+s)\frac{ds}{\sqrt{s}}\Big|$$

and from the bound (for $f \geq 0$)

$$\frac{1}{2h}\int_0^{h^2} f(x+s)\frac{ds}{\sqrt{s}} = \sum_{k\geq 0}\frac{1}{2h}\int_{h^2/2^{k+1}}^{h^2/2^k} f(x+s)\frac{ds}{\sqrt{s}} \leq \sum_{k\geq 0} 2^{-k/2}\frac{2^k}{h^2}\int_0^{h^2/2^k} f(x+s)ds,$$

we see that $\mathcal{M}_{sq}f(x) \leq 2\mathcal{M}f(x)$. Hence L^p bounds as well as a weak-type bound on L^1 for $\mathcal{M}_{sq}$ follows from those for $\mathcal{M}$.

There is no analagous estimate between M_{sq} and M and furthermore, the passage from $\mathcal{M}$ to M we saw above completely fails for $\mathcal{M}_{sq}$ and M_{sq}. In fact, it was recently shown that M_{sq} fails to satisfy a weak-type bound on ℓ^1, see [10]. Hence standard covering lemma arguments fail for M_{sq} and an alternative approach is needed to prove ℓ^p (or say ℓ^2) bounds directly without using any estimate on ℓ^1.

Singular and Maximal Radon Transforms. In [7] and [8], Bourgain used fourier transform techniques as well as number-theoretic considerations to prove that M_{sq} (and hence the more general f^*_{sq}) is bounded on ℓ^p for all $p > 1$. The approach Bourgain introduced to examine the maximal function M_{sq} and others is similar to the approach Stein and his collaborators introduced to analyse singular and maximal Radon tranforms.

Two prototypical examples from this theory are the Maximal and Hilbert transform along a parabola

$$\mathcal{M}_{par}f(x,y) := \sup_{h>0}\int_0^h |f(x-t, y-t^2)|dt, \text{ and } \mathcal{H}_{par}f(x,y) := p.v.\int_{\mathbb{R}} f(x-t,y-t^2)\frac{dt}{t}.$$

In both cases these are homogeneous operators with repect to parabolic dilations of critical degree but since the underlying kernel is supported along a lower dimensional variety (a parabola in this case), it lacks the smoothness required for standard Calderón-Zygmund theory to apply. In fact these were the first operators in the general family of Maximal and Singular Randon Transforms whose $L^p, 1 < p < \infty$ boundedness were established although it is still a (major) open problem whether

either $\mathcal{M}_{par}$ or $\mathcal{H}_{par}$ satisfy weak-type bounds on L^1. Like M_{sq}, covering lemma arguments dramatically fail for $\mathcal{M}_{par}$ and $\mathcal{H}_{par}$.

Bourgain's argument for M_{sq} has been extended by Ionescu, Magyar, Stein and Wainger in [40] to treat the 2-dimensional discrete operator

$$M_{par}f(n_1,n_2) \;:=\; \sup_N \frac{1}{N}\Big|\sum_{n=1}^{N} f(n_1-m,n_2-m^2)\Big|$$

and Stein and Wainger [52] introduced the singular integral variant

$$H_{par}f(n_1,n_2) \;:=\; \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{f(n_1-m,n_2-m^2)}{n}.$$

There is an intimate interplay between singular and maximal operators although the natural space to treat maximal operators is L^∞ (and L^1 if it is expected there is a weak-type bound on L^1) whereas the natural space to treat the singular integral operators is L^2 since as convolution operators $\mathcal{H}_{par}f = f*\mathcal{K}_{par}$, $H_{par}f = f*K_{par}$, L^2 boundedness is equivalent to showing that the mulipliers

$$\mathfrak{m}_{par}(\xi,\eta) := \int_{\mathbb{R}} e^{2\pi i(\eta t^2+\xi t)}\,\frac{dt}{t} \quad\text{and}\quad m_{par}(\psi,\theta) := \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{e^{2\pi i(\theta n^2+\psi n)}}{n}$$

are bounded functions; here $\mathfrak{m}_{par} = \widehat{\mathcal{K}_{par}}(\xi,\eta)$ and $m_{par} = \widehat{K_{par}}$ where the fourier transform used for $\mathfrak{m}_{par}$ is defined on $L^2(\mathbb{R}^2)$ and produces a function defined on the dual group $\mathbb{R}^2_* \simeq \mathbb{R}^2$. The fourier transform used for m_{par} is defined on $L^2(\mathbb{Z}^2)$ and produces a function on the dual group $\mathbb{Z}^2_* \simeq \mathbb{T}^2$.

Since no one has been able to treat $\mathcal{M}_{par}$ on L^1 and we now know that M_{sq} and M_{par} do not satisfy a weak-type bound on ℓ^1, we need a way to treat these operators on ℓ^p for $p>1$ more directly. In the early 1970s, Stein introduced powerful fourier transform techniques to deal with ultra-singular integral operators (of which $\mathcal{M}_{par}$ and $\mathcal{H}_{par}$ are examples). These methods are more transparent for singular convolution operators like $\mathcal{H}_{par}$ and H_{par} where L^2 bounds are reduced to showing that the corresponding multiplier is a bounded function.

The first proof showing that the oscillatory integral $\mathfrak{m}_{par}(\xi,\eta)$ is a bounded function in (ξ,η) is due to E. Fabes [25] and used the method of steepest decent; however the argument does not generalise to other situations or to L^p bounds. Stein and Wainger [50] used a more flexible method based on what harmonic analysts call van der Corput's lemma:

Lemma 3.2. *For any $k\geq 2$, there is a constant C_k such that for any real-valued $\phi\in C^k[a,b]$ satisfying $|\phi^{(k)}(x)|\geq 1$ for $x\in[a,b]$, the estimate*

$$\Big|\int_a^b e^{2\pi i\lambda\phi(x)}dx\Big| \;\leq\; C_k\,\lambda^{-1/k} \tag{21}$$

holds uniformly for all $\lambda \geq 1$. Furthermore the estimate (21) *holds when $k = 1$ if in addition, ϕ' is monotone.*

For a proof of Lemma 3.2, see [49] or [63].

Their method generalised to bound oscillatory integrals defined with respect to a general polynomial phase; that is, one can replace $\eta t^2 + \xi t$ defining $\mathfrak{m}_{par}$ with a general polynomial phase $\eta t^d + \cdots + \xi t$. Stein and Wainger refined their method in [51] which allowed them to extend L^2 bounds for $\mathcal{H}_{par}$ to $L^p, 1 < p < \infty$ bounds for both $\mathcal{H}_{par}$ and $\mathcal{M}_{par}$.

Here are the rudiments of their argument: first of all it is natural to resolve the singularity $1/t$ in $\mathcal{H}_{par}$ or $\mathfrak{m}_{par}$ dyadically by decomposing $\mathcal{H}_{par} = \sum_k \mathcal{H}_k$ or $\mathfrak{m}_{par} = \sum_k \mathfrak{m}_k$ where

$$\mathcal{H}_k f(x,y) = \int_{2^k \leq |t| < 2^{k+1}} f(x-t, y-t^2) \frac{dt}{t} \quad \text{and} \quad \mathfrak{m}_k(\xi,\eta) = \int_{2^k \leq |t| < 2^{k+1}} e^{2\pi i(\eta t^2 + \xi t)} \frac{dt}{t}.$$

One reason why it is natural to start with such a dyadic decomposition is that the individual pieces $\{\mathcal{H}_k\}$ act independently – we will see this explicitly in just a moment. Making the change of variables $s = 2^{-k}t$ shows that $\mathfrak{m}_k(\xi,\eta) = \mathfrak{m}_0(2^k\xi, 2^{2k}\eta)$ and an application of van der Corput's Lemma 3.2 shows that

$$|\mathfrak{m}_k(\zeta)| \;\leq\; C \min(|\delta_{2^k}\zeta|^{-1/2}, |\delta_{2^k}\zeta|) \;\leq\; C \min([2^k\rho(\zeta)]^{-1/2}, [2^k\rho(\zeta)]^{1/2}) \tag{22}$$

where $\zeta = (\xi,\eta)$, $\delta_u\zeta = (u\xi, u^2\eta)$ and $\rho(\zeta) = (|\xi|^2 + |\eta|)^{1/2}$ so that $\rho(\delta_u\zeta) = u\rho(\zeta)$ for $u > 0$.

For a fixed ζ, we split the sum $\sum_k \mathfrak{m}_k(\zeta)$ into two parts; for k such that $2^k \geq \rho(\zeta)^{-1}$, using the bound $[2^k\rho(\zeta)]^{-1/2}$ for $\mathfrak{m}_k$, and for k such that $2^k \leq \rho(\zeta)^{-1}$, using the bound $[2^k\rho(\zeta)]^{1/2}$ for $\mathfrak{m}_k$, we see that $\mathfrak{m}_{par}(\zeta)$ is uniformly bounded in ζ. Furthermore the bound (22) shows that the L^2 operator norms of $\mathcal{H}_k\mathcal{H}_j^*$ and $\mathcal{H}_k^*\mathcal{H}_j$ satisfy

$$\|\mathcal{H}_k\mathcal{H}_j^*\|_{op},\ \|\mathcal{H}_k^*\mathcal{H}_j\|_{op} \;\leq C\, 2^{-\epsilon|j-k|} \quad \text{for some } \epsilon > 0. \tag{23}$$

Although the dyadic pieces $\{\mathcal{H}_k\}$ are not exactly orthogonal, $\mathcal{H}_k\mathcal{H}_j^* = 0 = \mathcal{H}_k^*\mathcal{H}_j$, the inequalities in (23) show that the $\mathcal{H}_k$ are *almost orthogonal* and it is a general result, known as the Cotlar-Knapp-Stein Lemma, see [49], that such bounds imply that the pieces $\{\mathcal{H}_k\}$ act independently enough so that the sum $\sum_k \mathcal{H}_k$ is bounded on L^2. The Cotlar-Knapp-Stein result is valid in any Hilbert space but does not necessarily extend to $L^p, p \neq 2$ bounds; however it is possible to show that the bounds in (22) imply L^p bounds for all $1 < p < \infty$ by using Littlewood-Paley theory with respect to dyadic parabolic annuli $A_k = \{\zeta : \rho(\zeta) \sim 2^k\}$. See the Exercises.

Stein and Wainger introduced a square function argument in [51] to examine the associated maximal function $\mathcal{M}_{par}$ associated to $\mathcal{H}_{par}$. First it is a simple matter to see that the pointwise bound $\mathcal{M}_{par}f(x,y) \leq C \sup_k |\mathcal{M}_k f(x,y)|$ holds where M_k

is the dyadic averaging operator

$$\mathcal{M}_k f(x,y) \ := \ 2^{-k} \int_{2^k}^{2^{k+1}} f(x-t, y-t^2) dt$$

Let ϕ be such that $\widehat{\phi} \in C_0^\infty(\mathbb{R}^2)$ satisfies $\widehat{\phi} \equiv 1$ in a neighborhood of $(0,0)$. Set $\phi_k(x,y) = 2^{3k}\phi(2^k x, 2^{2k} y)$ and note that

$$(24) \ \ \mathcal{M}_{par} f(x,y) \ \leq \ C\Big[\Big(\sum_{k\in\mathbb{Z}} |\mathcal{M}_k f(x,y) - \phi_k * f(x,y)|^2\Big)^{1/2} \ + \ \sup_{k\in\mathbb{Z}} |\phi_k * f(x,y)|\Big].$$

The maximal function $\sup_k |\phi_k * f(x,y)|$ is pointwise bounded by the strong maximal function and so is bounded on all $L^p(\mathbb{R}^2), 1 < p \leq \infty$ (see the Exercises). Let's denote by $Sf(x,y)$ the square function in (24) and so the study of $\mathcal{M}_{par}$ is redued to examining Sf.

To show that S is bounded on L^2, it suffices by Plancherel's theorem to prove that the associated "multiplier"

$$\mathfrak{n}(\zeta) \ = \ \Big(\sum_{k\in\mathbb{Z}} |\mathfrak{n}_k(\zeta) - \widehat{\phi}_k(\zeta)|^2\Big)^{1/2}$$

is a bounded function of ζ. Here $\mathfrak{n}_k(\zeta) = \mathfrak{n}_0(2^k\xi, 2^{2k}\eta)$ where $\mathfrak{n}_0(\zeta) = \int_1^2 e^{2\pi i(\eta t^2 + \xi t)} dt$ is similar to $\mathfrak{m}_k$, satisfying the same decay bound $|\mathfrak{n}_k(\zeta)| \leq C[2^k \rho(\zeta)]^{-1/2}$ but the behaviour for small ζ is different although in this case, we can compare $\mathfrak{n}_k$ to $\widehat{\phi}_k$ so that we have the same bounds for $\mathfrak{n}_k - \widehat{\phi}_k$ as we do for $\mathfrak{m}_k$;

$$(25) \qquad |\mathfrak{n}_k(\zeta) - \widehat{\phi}_k(\zeta)| \ \leq \ C \ \min([2^k\rho(\zeta)]^{-1/2}, [2^k\rho(\zeta)]^{1/2}).$$

Hence L^2 bounds for S follow in the same way as for $\mathcal{H}_{par}$ as well as L^p bounds via Littlewood-Paley theory.

The discrete operators H_{par} and M_{par}. As in the continuous case, we concentrate on the ℓ^2 theory for the singular integral operator H_{par} which as we have seen is a multiplier operator whose multiplier is given by the exponential sum m_{par}. However our analysis will follow the harmonic analysis given above for $\mathcal{H}_{par}$ and $\mathcal{M}_{par}$ (with number-theoretic refinements which we implement via the circle method) and so can be further refined to treat the ℓ^p theory for both H_{par} and M_{par}.

Interestingly there is an similar history bounding m_{par} as there is for $\mathfrak{m}_{par}$. Arkhipov and Oskolkov [3] first proved that $m_{par}(\psi,\theta)$ is a bounded function of (ψ,θ) for entirely different reasons (they were interested in spectra for uniform convergence) using bounds of Vinogradov for exponential sums; furthermore, their method is strong enough to obtain the same result for analagous exponential sums where the quadratic phase $\theta n^2 + \psi n$ is replaced by a general polynomial phase $p(n)$ with real coefficients. However their methods are not suitable to show that m_{par} is an L^p multiplier with $p \neq 2$. In [52], Stein and Wainger developed an altervative approach and showed that H_{par} is bounded on $L^p(\mathbb{Z}^2)$ for $3/2 < p < 3$ and then later these L^p estimates were extended to the full range $1 < p < \infty$ by Ionescu and Wainger in [39].

We begin as with $\mathcal{H}_{par}$ and divide $H_{par}f = \sum_{k\geq 1} H_k f$ dyadically where the multiplier m_k associated to H_k is given by

$$m_k(\psi,\theta) \;=\; \sum_{2^k\leq |n|<2^{k+1}} \frac{e^{2\pi i(\theta n^2+\psi n)}}{n}.$$

Although the bound $|m_k(\psi,\theta)| \leq C[2^k\rho(\psi,\theta)]^{1/2}$ still holds, the corresponding decay bound utterly fails for m_k. In the continuous case, it is only the *size* of the fourier variables $\zeta = (\xi,\eta)$ as measured by $\rho(\zeta)$ which determines when the oscillatory integral $\mathfrak{m}_k$ is small – we see this explicitly in the bounds (22). However when we pass to the discrete exponential sum $m_k(\psi,\theta)$, it is not only the size but also finer diophantine properties of θ which come into play and determine when m_k is small.

This is not the case for all discrete exponential sums; for example, if we examine the multiplier $m(\eta) = \sum_{k\geq 1} m_k(\eta)$ associated to the discrete Hilbert transform

$$Hf(m) \;:=\; \sum_{n\in\mathbb{Z}\setminus\{0\}} \frac{f(m-n)}{n} \quad \text{where} \quad m_k(\theta) \;:=\; \sum_{2^k\leq|n|<2^{k+1}} \frac{e^{2\pi i\theta n}}{n},$$

one can easily establish the analgous bounds $|m_k(\theta)| \leq C\min(2^k|\theta|, [2^k\theta|]^{-1})$ to (22) and here we see that only the size $|\theta|$ of θ matter. This is connected to the fact that we can pass from the classical Hilbert transform

$$\mathcal{H}f(x) \;:=\; p.v.\int_{\mathbb{R}} f(x-t)\frac{dt}{t}$$

to H in much the same way as we did from $\mathcal{M}$ to M which is also connected to the fact that the linear phase $\phi(n) := \theta n$ does not change much when we pass from one value of n to the next $n+1$ – the difference (or derivative) $\phi(n+1)-\phi(n) = \theta$ of ϕ being smaller than 1 and this allows us to compare well the discrete sum with the corresponding integral.

We record a well-known result which we will find useful; see [63], page 198 for a proof.

Lemma 3.3. *Suppose that $\phi \in C^1[a,b]$ is a real-valued phase satisfying $|\phi'(t)| \leq \sigma$ for $t \in [a,b]$ and for some $\sigma \in (0,1]$. Then*

$$\Big|\sum_{a\leq n<b} e^{2\pi i\phi(n)} \;-\; \int_a^b e^{2\pi i\phi(x)}dx\Big| \;\leq\; C \tag{26}$$

for some constant $C = C_\sigma$ depending only on σ but otherwise independent of a, b and ϕ.

Note that the phase $\phi(n) = \theta n^2 + \psi n$ arising in the exponential sums m_k does not have a small derivative $\phi'(n) = 2\theta n + \psi$ and so in general we have no control where the point $e^{2\pi i\phi(n+1)}$ lands on the circle $\mathbb{T}$, perhaps having wrapped around the circle many times compared to where the point $e^{2\pi i\phi(n)}$ is located – in this way we see

the issue is related to the equidistribution of the fractional parts $\{\langle n^2\theta + n\psi\rangle\}$ in the unit interval $[0,1)$.

To analyse the sum $m_k(\psi,\theta)$ for a given value of k and fixed θ,ψ, we will examine the real number θ at a certain scale $K = K(k) > 2$ given by k by approximating it by a rational a/q with control of the denominator q. This is efficiently achieved by Dirichlet's Principle which states we can find a unique rational a/q in lowest terms (that is, $gcd(a,q) = 1$) such that $|\theta - a/q| \le 1/qK$ while $1 \le q \le K$. To see this, simply consider the sequence of $K+1$ fractional parts $\{0, \langle\theta\rangle, \langle 2\theta\rangle, \dots, \langle K\theta\rangle\}$ (here $\langle x\rangle := x - \lfloor x\rfloor$ denotes the difference of x with its integer part), two of which must lie within a distance $1/K$ of each other, say $|\langle j\theta\rangle - \langle k\theta\rangle| \le 1/K$ for some $0 \le j < k \le K$. Unraveling this gives the desired approximation. We could have achieved this approximation using the continued fraction expansion of θ but we choose to use Dirichlet's Principle, not only for its simplicity, but it is also more robust in multi-dimensional situations.

We fix our rational approximation a/q of θ and write $\alpha = \theta - a/q$; note that $\alpha = \alpha(k)$ also depends on k as well as θ. With q fixed, there is a unique integer b such that[5] $|q\psi - b| \le 1/2$ (unless $q\psi$ is an integer or half-integer in which case there are at most three choices for b) and we write $\beta = \psi - b/q$. We break up the sum m_k into blocks of q elments by writing each n in the sum uniquely as $n_r(\ell) = \ell q + r$ where $0 \le r \le q-1$ so that the phase $(\ell q+r)^2\theta + (\ell q+r)\psi = (\ell q+r)^2\alpha + (\ell q+r)\beta + (r^2a + rb)/q \bmod q$. Hence

$$m_k(\psi,\theta) \;=\; \sum_{r=0}^{q-1} e^{2\pi i(ar^2+br)/q}\Big[\sum_{\ell: 2^k \le |n_r(\ell)| < 2^{k+1}} \frac{e^{2\pi i[(\ell q+r)^2\alpha + (\ell q+r)\beta]}}{\ell q + r}\Big]$$

and for fixed $0 \le r < q$, we will try to use Proposition 3.3 with the phase $\phi(\ell) := (\ell q + r)^2\alpha + (\ell q + r)\beta$. Note that for ℓ in the range of the inner sum, $|\phi'(\ell)| = |2(\ell q + r)q\alpha + q\beta| \le 42^k/K + 1/2$. If we choose $K \ge 10\,2^k$, then $|\phi'(\ell)| \le 9/10$ and so a variant of Proposition 3.3 applied to the inner sum yields

$$m_k(\psi,\theta) = \sum_{r=0}^{q-1} e^{2\pi i(ar^2+br)/q}\Big[\int_{t: 2^k \le |n_r(t)| < 2^{k+1}} \frac{e^{2\pi i[(tq+r)^2\alpha + (tq+r)\beta]}}{tq + r} dt\Big] + O(q/2^k).$$

Making the change of variables $s = tq + r$ in the integral effectively gives a multiplicative representation of m_k into two factors $m_k(\psi,\theta) = G_q(a,b)\mathfrak{m}_k(\beta,\alpha) + O(q/2^k)$ where G_q is a classical Gauss sum (we have already encountered this sum in the context of finite fields which corresponds to the case q being prime in the current context) and $\mathfrak{m}_k$ is the oscillatory integral appearing as a dyadic piece of the multiplier $\mathfrak{m}_{par}$ associated to $\mathcal{H}_{par}$. More precisely,

$$G_q(a,b) := \frac{1}{q}\sum_{r=o}^{q-1} e^{2\pi i(ar^2+br)/q} \quad \text{and} \quad \mathfrak{m}_k(\beta,\alpha) := \int_{2^k \le |s| < 2^{k+1}} e^{2\pi i(\alpha s^2 + \beta s)}\frac{ds}{s}.$$

From (22), we know that $\sum_k |\mathfrak{m}_k(\xi,\eta)| \le C$, uniformly in ξ and η. This seems promising since clearly, $|G_q(a,b)| \le 1$, but there are two issues; 1) $\alpha = \alpha(k)$,

[5] an alternative method is to try to simultaneously approximate both θ and ψ by rationals with the same denominator q – the argument in Dirichlet's Principle extends to this setting showing there are integers a, b and q such that $|\theta - a/q|, |\psi - b/q| \le 1/q\sqrt{K}$ while we still have $1 \le q \le K$.

$\beta = \beta(k)$ and $q = q_k$ all depend on k and 2) the error term $O(q/2^k)$ is not necessarily summable in k since all we know is $1 \le q \le K(k)$ and we need $K(k) \ge 10\,2^k$.

The second issue will be sorted if we restrict our attention to those θ such that the approximating rational a/q has small denominator, say $1 \le q \le 2^{k/2}$ so that the error terms $O(q/2^k)$ are summable. However if q is large, then the original sum $m_k(\psi, \theta)$ has a lot of cancellation and one can directly estimate m_k in this case and show that it is small. This observation is fundamental and goes back to Hardy and Littlewood in the early part of the twentieth century. We prove here a special instance of *Weyl's inequality* which gives a good bound on m_k when q is large.

Proposition 3.4. *Suppose $|\theta - a/q| \le 1/q^2$ for some a/q with $gcd(a, q) = 1$. Then for any $1 \le J < N$, we have*

$$\Big|\sum_{n=J}^{N} e^{2\pi i(\theta n^2 + \psi n)}\Big| \;\le\; 100\big[\log N(N + q + N^2/q)\big]^{1/2} \tag{27}$$

Proof. Let us call the sum in (27) S and the phase $\phi(n) = \alpha n^2 + \beta n$ so that $S = \sum_{n=J}^{N} e^{2\pi i\phi(n)}$. The basic technique here is to consider the square

$$|S|^2 \;=\; \sum_{m=J}^{N}\sum_{n=J}^{N} e^{2\pi i(\phi(n)-\phi(m))} \;=\; \sum_{m=J}^{N}\sum_{h=J-m}^{N-m} e^{2\pi i(\phi(m+h)-\phi(m))} \;=$$

$$N + \sum_{h=1}^{N-1}\sum_{m=1}^{N-h} e^{2\pi i(\phi(m+h)-\phi(m))} + \sum_{h=J-N}^{-1}\sum_{m=J-h}^{N} e^{2\pi i(\phi(m+h)-\phi(m))} := N + I + II$$

and reduce matters to considering, for a fixed h, a linear phase $g(m) = \phi(m+h) - \phi(m) = 2\theta hm + c(h)$ whereby we can efficiently estimate the inner sums in I and II above by evaluating them as geometric series.

In general if we considered an exponential sum with a general polynomial phase $\phi(n) = \theta n^d + \cdots$, the squaring techinque reduces one to considering an exponential sum with the difference phase (for fixed h) $g(m) = \phi(m+h) - \phi(m) = d\theta h m^{d-1} + \cdots$ of one degree less and an inductiion argument can then be used to give a bound on the original exponential sum. This is known as Weyl differencing and leads to estimates which are collectively known as Weyl estimates. We will see now how this plays out in the quadratic case.

For I and II above, we use the geometric series formula $\sum_{m=a}^{b} z^m = (z^{b+1} - z^a)/(z-1)$ for $z \ne 1$ to bound

$$|I| \le \sum_{h=1}^{N-1}\Big|\sum_{m=1}^{N-h} e^{2\phi i[2\theta hm]}\Big| \le \sum_{h=1}^{N-1} \min(N, 1/|1 - e^{2\pi i 2\theta h}|) \le \sum_{h=1}^{N-1} \min(N, [2\|2\theta h\|]^{-1})$$

where $\|\alpha\|$ denotes the distance from α to the integers $\mathbb{Z}$. Using the property that $|\theta - a/q| \le 1/q^2$ for some a/q with $gcd(a,q) = 1$, one can show (see the Exercises)

$$\sum_{h=1}^{N-1} \min(N, 1/\|2\theta h\|) \;\le\; \sum_{j=1}^{2N} \min(N, 1/\|\theta j\|) \;\le\; 10^3 \log N(N + q + N^2/q) \tag{28}$$

Similarly $|II| \le 10^3 \log N(N + q + N^2/q)$ which finishes the proof of (27). □

Before we apply Proposition 3.4 to the sum m_k, we note that the same squaring technique, reducing to a geometric series, is even more simple when applied to the Gauss sums $G_q(a,b)$ and in fact shows (see the Exercises)

$$|G_q(a,b)| \;\le\; 2/\sqrt{q} \quad \text{when} \quad gcd(a,q) = 1. \tag{29}$$

We now apply Proposition 3.4 with $J = 2^k$ and $N \le 2^{k+1}$ to $m_k(\psi,\theta)$ with our approximation $|\theta - a/q| \le 1/q^2$ for some rational a/q with $gcd(a,q) = 1$, together with a summation by parts argument, shows that

$$|m_k(\psi,\theta)| \;\le\; 10^3\sqrt{k}\big(q^{-1/2} + 2^{-k/2}\big) \tag{30}$$

if $1 \le q \le 10\,2^k$ and this is a good estimate if q is large, say larger than $2^{k/2}$.

The Circle Method. The above discussion hopefully motivates the circle method: the angular fourier variable θ lies on the circle (more precisely, we have $e^{2\pi i\theta} \in \mathbb{T}$) and the behaviour of the exponential sum $m_k(\psi,\theta)$ depends on the diophantine properties of θ; namely if we choose a scale K, say $K = 10\,2^k$, then by Dirichlet's Principle we can find a rational approximation a/q to θ with $gcd(a,q) = 1$ so that $|\theta - a/q| \le 1/qK$ with $1 \le q \le K$.

Now if q is large, say $2^{k/2} \le q$, then there is a lot of cancellation in the sum defining m_k and (30) implies $|m_k(\psi,\theta)| \le C\sqrt{k}\,2^{-k/2}$. On the other hand if q is small, say $1 \le q \le 2^{k/2}$, then we can *evaluate* m_k showing that $m_k(\psi,\theta) = G_q(a,b)\mathfrak{m}_k(\beta,\alpha) + O(2^{-k/2})$. This lies at the core of the Hardy-Littlewood-Ramanujun circle method: we split the points $e^{2\pi i\theta}$ of the circle $\mathbb{T}$ into two classes: the *major arcs*, those θ so that $1 \le q \le 2^{k/2}$ is small and the *minor arcs*, those θ so that $q \ge 2^{k/2}$ is large.

For our problem at hand, we are fixing θ (and ψ) and summing $m_k(\psi,\theta)$ over $k \in \mathbb{N}$ and so we take a slightly different view from other problems amenable to the circle method in that we split the parameter k (not θ as it is fixed) into $Maj = \{k : q = q_k \le 2^{k/2}\}$ and $Min = \{k : q = q_k \ge 2^{k/2}\}$ and write

$$m_k(\psi,\theta) \;=\; \sum_{k\in Maj} m_k(\psi,\theta) \;+\; \sum_{k\in Min} m_k(\psi,\theta) \;:=\; m_{Maj}(\psi,\theta) + m_{Min}(\psi,\theta).$$

On the other hand, for problems like Waring's problem where we would like to count the number of ways we can write an integer $N \ge 1$ as a sum of s kth powers, we split the points θ of the circle $\mathbb{T}$ into *major* and *minor* arcs. If we denote $R_{k,s}(N)$ as this count of representations of N,

then

$$R_{k,s}(N) \;=\; \int_{\mathbb{T}} \Big[\sum_{n=1}^{N} e^{2\pi i n^k \theta}\Big]^s e^{-2\pi i N\theta}\, d\theta$$

and given a scale $K = K_{k,s}(N)$ we approximate each θ as before by rationals a/q such that $|\theta - a/q| \le 1/qK$ and split the circle $\mathbb{T} = Major \cup Minor$ into major and minor arcs depending on the size of q.

For $k \in Min$, the bound $|m_k(\psi,\theta)| \le C2^{-k/3}$ holds and so we have a uniform bound for $m_{Min}(\psi,\theta)$. For m_{Maj}, we have

$$m_{Maj}(\psi,\theta) \;=\; \sum_{k\in Maj} G_q(a,b)\mathfrak{m}_k(\beta,\alpha) \;+\; E(\psi,\theta) \tag{31}$$

where E is uniformly bounded in ψ and θ. Recall that $q = q_k$, $\alpha = \alpha(k), \beta = \beta(k), a = a(k)$ and $b = b(k)$ all depend on k as well as depending on θ and ψ.

It may be the case that there are several values of $k \in Maj$ which give the same value of $q = q_k$; so we let $Q_1 < Q_2 < \cdots$ enumerate the distinct values of $\{q_k\}_{k\in Maj}$ and observe that

$$2 \;\le\; Q_{j+1}/Q_j \quad \text{for all} \;\; j \ge 1; \tag{32}$$

that is, the sequence $\{Q_j\}$ forms a lacunary sequence and in particular, $2^j \le Q_j$. To prove (32), note that if $q_k = Q_j$ and $q_\ell = Q_{j+1}$, then $q_k < q_\ell$ and so the rationals a_k/q_k and a_ℓ/q_ℓ arising in the approximation of θ at different scales are distinct. Furthermore $k,\ell \in Maj$ implies that $10\,q_k \le K(k)$, $10\,q_\ell \le K(\ell)$ since $K(j) = 10\,2^j$ and $q_j \le 2^j$ if $j \in Maj$. This in turn implies $1/(q_j K(j)) \le (1/10)q_J^{-2}$ for $j \in Maj$ and so

$$\frac{1}{q_k q_\ell} \;\le\; \Big|\frac{a_k q_\ell - a_\ell q_k}{q_k q_\ell}\Big| \;\le\; |\theta - a_k/q_k| + |\theta - a_\ell/q_\ell| \;\le\; \frac{1}{10}\big[1/q_k^2 + 1/q_\ell^2\big].$$

Hence $1 \le (1/10)(q_\ell/q_k + q_k/q_\ell) \le (1/10)(Q_{j+1}/Q_j + 1)$ and this gives (32).

We regroup the sum in (31), writing

$$\sum_{k\in Maj} G_{q_k}(a(k),b(k))\mathfrak{m}_k(\beta(k),\alpha(k)) \;=\; \sum_{j\ge 1}\sum_{k:q_k=Q_j} G_{Q_j}(a_j,b_j)\mathfrak{m}_k(\beta_j,\alpha_j)$$

where for k with $q_k = Q_j$, we write $\alpha_j = \alpha(k), \beta_j = \beta(k), a_j = a(k)$ and $b_j = b(k)$. The Gauss sum S_{G_j} does not depend on k and can be factored out of the inner sum, leaving for the inner sum $\sum_{k:q_k=Q_j} \mathfrak{m}_k(\beta_j,\alpha_j)$ which is uniformly bounded by an application (22) as already observed. This, together with the Gauss bound $|G_{Q_j}(a_j,b_j)| \le 2Q_j^{-1/2}$ in (29), shows via (32) that the sum in (31) (and hence $m_{Maj}(\psi,\theta)$) is uniformly bounded in θ and ψ.

Exercises

3.1. Suppose we knew that the pointwise limits (20) held for a dense set of functions in some $L^p(X,\mu)$. Use the fact that the corresponding maximal function f^* is

bounded on $L^p(X,\mu)$, $\|f^*\|_p \le C_p\|f\|_p$, to show that (20) holds for all $f \in L^p(X,\mu)$. Hint: show that

$$\big\{x \in X : |\limsup_{N\to\infty} A_N f(x) - \liminf_{N\to\infty} A_N f(x)| > \epsilon\big\}$$

has μ measure zero for any $\epsilon > 0$. Here $A_N f(x) = 1/N \sum_{n=1}^N f(T^n x)$.

3.2 Go through Calderón's Transference Prinicple argument with Bourgain's maximal function f^*_{sq}, showing it suffices to bound M_{sq} on the integers $\mathbb{Z}$. Furthermore, show how the weak-type bound $\mu(x \in X : f^*(x) \ge \lambda) \le C\lambda^{-1}\|f\|_1$ can be reduced to the analagous bound for the Hardy-Littlewood maximal function M on $\mathbb{Z}$.

3.3 Show that $\#\{n \in \mathbb{Z} : M\phi(n) \ge \lambda\} \le C\lambda^{-1}\|\phi\|_{\ell^1}$ via the following covering lemma argument: first it suffices to bound $\#F$ for any finite subset $F \subset \{n : M\phi(n) \ge \lambda\}$ as long as our bounds are independent of $\#F$. Note that for every $m \in F$, there is an $N = N(m)$ such that $N(m) \le \lambda^{-1}\sum_{n=1}^{N(m)} \phi(m+n)$. From the finite covering $F \subset \cup_{m\in F}[m, m+N(m)]$, extract a subcovering $F \subset \cup_{j=1}^M [m_j, m_j + N(m_j)]$ of pairwise disjoint intervals with the property that $F \subset \{[m_j - N(m_j), m_j + N(m_j)]\}_{j=1}^M$ (use a greedy algorithm – pick m_1 such that $N(m_1)$ is the largest and then pick the largest m_2 among those intervals which do not intersect $[m_1, m_1 + N(m_1)]$, etc...). Unravel this to deduce the desired bound.

3.4 Use the bound for M in the previous exercise to show that for every $p > 1$, there is a constant C_p such that $\|M\phi\|_{\ell^p} \le C_p\|\phi\|_{\ell^p}$. Hint: use the formula

$$\|M\phi\|_{\ell^p} \;=\; p\int_0^\infty \#\{n : M\phi(n) \ge \lambda\}\lambda^{p-1}d\lambda$$

and split $\phi = \phi_1 + \phi_2$ where $\phi_1(n) = \phi(n)\chi_{\{m:\phi(m)\ge\nu\}}(n)$ for an appropriate choice of $\nu = \nu(\lambda)$ which guarantees that $\{n : M\phi_2(n) \ge \lambda/2\} = \emptyset$.

3.5 Show that ℓ^p bounds for M_{sq} follow from ℓ^p bounds for M_{par}.

3.6 Use van der Corpurt's Lemma 3.2 to prove the basic bounds (22).

3.7 Show how (23) follows from (22).

In the following exercises, 3.8 - 3.11, we fill in the steps showing how L^p boundedness for $\mathcal{H}_{par}$ follows from the multiplier bounds (22). Exercise 3.11 however requires knowledge of Calderón-Zygmund theory.

3.8 Show that there exists a smooth function Ψ such that $\mathrm{supp}(\widehat{\Psi}) \subset \{\zeta : 1/4 \le \rho(\zeta) \le 4\}$ and that for all $\zeta \ne 0$,

$$\sum_{k\in\mathbb{Z}} \widehat{\Psi_k}(\zeta) \;=\; 1$$

where Ψ_k is defined so that $\widehat{\Psi_k}(\zeta) = \widehat{\Psi}(2^{-k}\zeta)$.

3.9 Show that we can write $\mathcal{H}_{par}f(x,y) = \sum_\ell G_\ell f(x,y)$ where $G_\ell f(x,y) = \sum_k \mathcal{H}_k[\Psi_{k+\ell} * f](x,y)$.

3.10 Show that there is an $\epsilon > 0$ such that $\|G_\ell f\|_2 \leq C2^{-\epsilon|\ell|}\|f\|_2$.

3.11 Using Calderón-Zygmund theory adapted to parabolic dilations (see for example, [49]), show that $|\{|G_\ell f(x,y) \geq \lambda\}| \leq C|\ell|\|f\|_1$. Now interpolate to deduce that for every $1 < p \leq 2$, there is an $\epsilon_p > 0$ such that $\|G_\ell f\|_p \leq C2^{-\epsilon_p|\ell|}\|f\|_p$ from which $L^p, 1 < p < \infty$ bounds for $\mathcal{H}_{par}$ follow.

3.12 Show the pointwise bound $\mathcal{M}_{par}f(x,y) \leq C \sup_k |M_k f(x,y)|$ and verify (24).

3.13 The strong maximal function in $\mathbb{R}^2$ is defined as

$$\mathcal{M}_{strong}f(x,y) \;=\; \sup_{h,k>0}\Big|\frac{1}{hk}\int_0^h\int_0^k f(x-s,y-t)\;dsdt\Big|.$$

By showing the pointwise bound $\mathcal{M}_{strong}f(x,y) \leq \mathcal{M}^1\mathcal{M}^2 f(x,y)$ where $\mathcal{M}^j, j = 1,2$ are the classical Hardy-Littlewood maximal functions in the directions x and y respectively, show that $\mathcal{M}_{strong}$ is bounded on all $L^p(\mathbb{R}^2), 1 < p \leq \infty$.

3.14 Using the exercise above, show that $\sup_k |\phi_k * f(x,y)|$ is bounded on all $L^p(\mathbb{R}^2), 1 < p \leq \infty$. In fact $f \to \sup_k |\phi_k * f(x,y)|$ satisfies a weak-type bound on L^1 by a standard covering lemma argument – try this!

3.15 Fill in the details establishing the bounds in (25). Furthermore, follow the lines of argument in Exercises 3.8 - 3.11 to show that S and hence $\mathcal{M}_{par}$ is bounded on all $L^p(\mathbb{R}^2), 1 < p \leq \infty$.

3.16 Give the details for a proof of Dirichlet's Principle: given any $x \in \mathbb{R}$ and $K > 2$, there is a unique rational a/q in reduced form such that $1 \leq q \leq K$ and $|qx - a| \leq 1/K$. Formulate and prove a multi-dimenaional version of Dirichlet's Principle as indicated in a footnote above.

3.17 State and prove a variant of Proposition 3.3 used above to estimate the exponential sum m_k.

3.18 Prove the inequality $|G_q(a,b)| \leq 2\,q^{-1/2}$ when $gcd(a,q) = 1$ stated in (29).

Establish the bound in (28) by completing the following exercises.

3.19 For L real numbers $\alpha_1, \ldots, \alpha_L$ satisfying $\|\alpha_j - \alpha_k\| \geq M^{-1}$ for every $j \neq k$ with $L \leq M$, show

$$\sum_{j=1}^{L} \min(N, \|\alpha_j\|^{-1}) \;\leq\; 6(N+M)\log(N).$$

Hint: Reduce to nonnegative $\alpha_j \in [0, 1/2]$.

3.20 Let $\alpha \in \mathbb{R}$ and a/q a rational in reduced form such that $|\alpha - a/q| \leq q^{-2}$. Show that

$$\sum_{j=1}^{H} \min(N, \|j\alpha\|^{-1}) \ \leq \ 24 \log(N)[N + q + H + NH/q].$$

Hint: if $0 < |j - k| \leq q/2$, then $\|j\alpha - k\alpha\| \geq 1/2q$.

4. The third perspective

Investigating these problems in the discrete setting of rings with lots of divisors is a new endeavour and our first aim in these last lectures will be to explain how divisors can be used as different scales to view the problem at hand. We will illustrate this for the Fourier Restriction Problem. We will also look at how harmonic analysis arguments are translated in these discrete settings and see how various number-theoretic problems arise. In many cases these problems have been well-studied by number theorists and we can simply use known results and estimates *off the shelf* to come to the desired conclusion. But one can also turn the tables around and examine these elementary problems from number theory which arise from a harmonic analysis point of view. This can be profitable and we will demonstrate this by looking at some basic problems involving complete exponential sums and polynomial congruences.

Fourier Restriction Problem mod N

Recall that the classical Fourier Restriction Problem from euclidean spaces was introduced by Mockenhaupt and Tao [44] in the setting of finite fields. The problem is set out in (13) and asks for the $L^p - L^q$ bounds to be uniform in the number of elements of the finite field. Here we generalise this model slightly and propose the following Fourier Restriction Problem in the setting of an arbitrary finite abelian group G.

Let $S \subset \widehat{G}^n$ be a set of frequencies in the n-fold product of the dual group $\widehat{G}$, equipped with normalised counting measure. We consider the $L^p - L^q$ Fourier restriction estimates

$$\big(\frac{1}{\#S} \sum_{y \in S} |\widehat{f}(y)|^q\big)^{1/q} \ \leq \ C_{p,q,n} \big(\sum_{x \in G^n} |f(x)|^p\big)^{1/p}. \tag{33}$$

The best constant $C_{p,q,n}$ in (33) will be denoted by $R_{p \to q}(S)$ and the basic problem is to determine, for a given set of frequencies S, those exponents p and q for which $R_{p \to q}(S)$ is "essentially" independent of the cardinality of G.

Given Dvir's resolution of the finite field Kakaya problem [23] and given that we seem to be a far way from resolving the euclidean Kakeya problem, it is natural to ask how well the finite field setting models the euclidean setting for these problems. As we already mentioned before, one difference is that there are not many scales to work with in the finite field setting (clearly manifested when studying the Fourier transform of measures carried along curves or surfaces; these are exponential sums in the finite field setting and the famous A. Weil (or more generally Deligne) estimates show that either we are in the nondegenerate case (nonvanishing curvature with optimal exponential sum estimates) or we are in the completely degenerate case where only trivial estimates hold). However when we move from the finite field setting (e.g., the integers modulo a prime p) to the setting of the finite ring of integers modulo N for general N, the divisors of N give us additional scales to work with and it is proposed here that this setting models the euclidean setting more closely.

We will see that this is indeed the case for the Fourier Restriction Problem. As a sample theorem we have the corresponding Stein-Tomas L^2 restriction theorem for the paraboloid $S = \{(\vec{y}, y_1^2 + \cdots + y_{n-1}^2) : \ \vec{y} = (y_1, \ldots, y_{n-1})\}$ in $[\mathbb{Z}/N\mathbb{Z}]^n_*$ which we state here informally.

Informal statement Let S be the paraboloid in $[\mathbb{Z}/N\mathbb{Z}]^n_*$ as described above. Then the Fourier restriction estimate (33) holds for $q = 2$ if and only if $1 \leq p \leq 2(n+1)/(n+3)$.

In the following section we will formulate precisely the Fourier restriction problem in the setting of $[\mathbb{Z}/N\mathbb{Z}]^n$; see (34).

Notation and formulation of problem. Let us introduce some notation which will facilitate the comparison between the ring of integers modulo N and the euclidean setting. First, we give a size to elements $x \in \mathbb{Z}/N\mathbb{Z}$; set $|x| := N/gcd(x, N)$ (when $N = p^L$ where p is prime, one can think of $|\cdot|$ as a 'normalised p-adic valuation' – normalised with respect to the ring $\mathbb{Z}/p^L\mathbb{Z}$). This notation is extended to elements $\vec{x} = (x_1, \ldots, x_n)$ in $[\mathbb{Z}/N\mathbb{Z}]^n$ by $\|(x_1, \ldots, x_n)\| := N/gcd(x_1, \ldots, x_n, N)$. Next we define the partial ordering among integers $a \leq b$ if and only if $a \,|\, b$ in order to compare various sizes $|\cdot|$; for example, $|x| \leq |y|$ if and only if $gcd(y, N) \,|\, x$.

To get some feeling for this notation we introduce the family of balls $\{\mathcal{B}_d\}_{d|N}$, indexed by the divisors of N which will play an important role later:

$$\mathcal{B}_d \ := \ \{\vec{x} \in [\mathbb{Z}/N\mathbb{Z}]^n : \ \|\vec{x}\| \leq d\}.$$

One easily verifies that an element $\vec{x} = (x_1, \ldots, x_n)$ lies in $\mathcal{B}_d$ if and only if N/d divides each component x_j.

As mentioned above this notation helps us carry out an analogy with euclidean notions. This analogy is more precise if we restrict our attention to powers $N = p^L$ of a fixed prime p in which case the divisors become totally ordered; and in particular the above balls $\{\mathcal{B}_{p^r}\}_{0\leq r\leq L}$ form a one parameter sequence of nested sets. As another simple illustration, which is relevant for the discussion below, compare the "integrals"

$$\int_{|x|\geq 1} \frac{1}{|x|^a}\, dx \quad \text{and} \quad \sum_{x=0}^{N-1} \frac{1}{|x|^a};$$

the euclidean integral of course converges if and only if $a > 1$ and the mod N "integral" disentangles as $\sum_{d|N} \phi(d) d^{-a}$ where ϕ is the Euler totient function; $\phi(d)$ counts the postive integers $m \leq d$ such that $gcd(m, d) = 1$. When $N = p^L$ this sum is uniformly bounded if and only if $a > 1$[6] whereas for general N this is true only when $a > 2$; when $a < 1$ the sum can grow like a power of N. However in the range $1 \leq a \leq 2$, one can show (see the Execises) that for every $\epsilon > 0$, there is a constant C_ϵ such that $\sum_{d|N} \phi(d) d^{-a} \leq C_\epsilon N^\epsilon$ – for quantities A, B depending on N, we introduce the notation $A \ll B$ to mean for every $\epsilon > 0$, there is a constant C_ϵ such that $A \leq C_\epsilon N^\epsilon B$. Hence the previous estimate can be succinctly represented by $\sum_{d|N} \phi(d) d^{-a} \ll 1$.

For this reason it is natural to pose the Fourier Restriction Problem in the setting of the integers mod N for general N in the following precise way: given a set of frequencies S in the dual group of $[\mathbb{Z}/N\mathbb{Z}]^n_*$, determine the exponents p and q so that

$$\big(\frac{1}{\#S} \sum_{y\in S} |\widehat{f}(y)|^q\big)^{1/q} \ \ll \ \big(\sum_{x\in[\mathbb{Z}/N\mathbb{Z}]^n} |f(x)|^p\big)^{1/p} \tag{34}$$

holds. The implicit constant $C_\epsilon = C_{\epsilon,p,q,n}$ in the above $\ll$ is allowed to depend on p, q and n.

For the paraboloid $S \subset [\mathbb{Z}/N\mathbb{Z}]^n_*$, we have the following precise statement.

Theorem 4.1. *Let S be the paraboloid in $[\mathbb{Z}/N\mathbb{Z}]^n_*$ as described above. Then the Fourier restriction estimate* (34) *holds for $q = 2$ if and only if $1 \leq p \leq 2(n + 1)/(n + 3)$.*

Necessary conditions. We now examine necessary conditions for the estimates (34) to hold when $S = \{(y_1, \ldots, y_{n-1}, y_1^2 + \cdots + y_{n-1}^2)\}$ is the paraboloid in $[\mathbb{Z}/N\mathbb{Z}]^n_*$. In this case (34) can be written as

$$\Big(\frac{1}{N^{n-1}} \sum_{\vec{y}\in[\mathbb{Z}/N\mathbb{Z}]^{n-1}_*} |\widehat{f}(\vec{y}, y_1^2 + \cdots + y_{n-1}^2)|^q\Big)^{1/q} \ \leq \ C_\epsilon N^\epsilon \, \|f\|_{L^p([\mathbb{Z}/N\mathbb{Z}]^n)}$$

where the L^p norm on the right is the same as the one appearing in (34) which is computed with respect to counting measure on $[\mathbb{Z}/N\mathbb{Z}]^n$; also $\vec{y} = (y_1, \ldots, y_{n-1})$.

[6] strictly speaking, a bound independent of L *and* p is only true if $a - 1 \geq 1/\log(p)$

Recall that in the finite field setting (which is the case in the current setting if we restrict the integers N to be prime and then ask for estimates to be uniform over all primes), the necessary conditions for the restricition estimates to hold for the paraboloid were given by $p' \geq qn/(n-1)$ and $p' \geq 2n/(n-1)$. These conditions are less restrictive than the ones arising in the euclidean settings where we have $p' \geq q(n-1)/(n+1)$ and $p' \geq 2n/(n-1)$ as necessary conditions. We claimed then that this is due to the lack of scales in the finite field setting and now we will see that scaling arguments in the euclidean setting have exact analogues in the mod N setting and here we will arrive at the same necessary conditions as in the euclidean setting.

We adapt the usual scaling argument in the euclidean setting; fix a divisor d of N so that its square d^2 is also a divisor (this forces $d = 1$ if N is prime) and consider the parabolic box

$$\mathcal{P} \;=\; \{(\vec{y}, t) \in [\mathbb{Z}/N\mathbb{Z}]^n : \; \|\vec{y}\| \leq |d|, \; |t| \leq |d^2|\}$$

where we are employing our notation above. Unraveling this notation we see that an element $(\vec{y}, t) = (y_1, \ldots, y_{n-1}, t)$ belongs to $\mathcal{P}$ if and only if $d \,|\, y_j$ for each j and $d^2 \,|\, t$. We apply f with $\widehat{f} = \chi_{\mathcal{P}}$ to (34) and easily check that the left hand side is equal to $1/d^{(n-1)/q}$. On the other hand a simple computation shows that $f(x_1, \ldots, x_n) = 1/d^{n+1}$ if N/d divides each $x_j, 1 \leq j \leq n-1$, N/d^2 divides x_n and $f = 0$ otherwise. Hence the L^p norm on the right hand side is equal to $1/d^{(n+1)/p'}$ and so (34) reduces to

$$d^{-\frac{n-1}{q}} \;\ll\; d^{-\frac{n+1}{p'}};,$$

and if this is to hold we see then $q\frac{n+1}{n-1} \leq p'$ which is the same restriction on the exponents as in the euclidean setting.

Given this relation on the exponents we now examine the possible L^p range. The analysis which follows is nearly the same as that already given in the finite field setting (we reach the same necessary condition $p' \geq 2n/(n-1)$) but we repeat it as we wish to emphasise the close resemblance with euclidean arguments.

By duality (34) is equivalent to

$$\Big(\sum_{\vec{x} \in [\mathbb{Z}/N\mathbb{Z}]^n} |\mathcal{E}g(\vec{x})|^{p'} \Big)^{1/p'} \;\ll\; \Big(\frac{1}{N^{n-1}} \sum_{\vec{y} \in [\mathbb{Z}/N\mathbb{Z}]^{n-1}} |g(\vec{y})|^{q'} \Big)^{1/q'} \tag{35}$$

where $\mathcal{E}$ is the extension operator

$$\mathcal{E}g(\vec{x}) \;=\; \frac{1}{N^{n-1}} \sum_{\vec{y} \in [\mathbb{Z}/N\mathbb{Z}]^{n-1}} g(\vec{y}) e^{2\pi i (x_1 y_1 + \cdots x_{n-1} y_{n-1} + x_n [y_1^2 + \cdots + y_{n-1}^2])/N}.$$

When $g = 1$, $\mathcal{E}1(\vec{x}) = \prod_{j=1}^{n-1} G_N(x_j, x_n)$ where

$$G_N(a, b) \;=\; \frac{1}{N} \sum_{t=0}^{N-1} e^{2\pi i (at + bt^2)/N}$$

is the Gauss sum we encountered before. Recall that (29) states $|G_N(a,b)| \leq 2N^{-1/2}$ if $gcd(a,N) = 1$, however in the present case, a and N may share some divisors and we need to examine $G_N(a,b)$ for gerneral choices of a and b.

One can check (see the Exercises) that $G_N(a,b)$ vanishes unless $gcd(b,N) \mid a$ (or $|a| \leq |b|$ using our notation) in which case $|G_N(a,b)| = \sqrt{gcd(b,N)/N}$, say when N is odd (or $|G_N(a,b)| = 1/\sqrt{|b|}$ using our notation). Plugging $g = 1$ into (35) we see that the right hand side is equal to 1 whereas the p' power of the left hand side is equal to (when N is odd)

$$\sum_{d|N} \sum_{gcd(x_n,N)=d} \Big(\frac{N}{d}\Big)^{n-1} \Big(\frac{d}{N}\Big)^{\frac{p'}{2}(n-1)} \;=\; \sum_{d|N} \phi(d)\, d^{-(n-1)(\frac{p'}{2}-1)}$$

which from the above discussion shows that if (35) is to hold, then necessarily $p' \geq 2n/(n-1)$ which matches the euclidean range of p, up to the endpoint anyway.

So in particular, when $q = 2$, we see that (34) fails for the paraboloid if $p > (2n+2)/(n+3)$. In the next two sections we will see that (34) in fact holds for the paraboloid when $q = 2$ in the optimal range $1 \leq p \leq (2n+2)/(n+3)$. In the two dimensional case, $n = 2$, we will then establish the full range of $L^p - L^q$ restriction estimates which again will match with the classical euclidean estimates.

An interlude: Comparing exponential sums to oscillatory integrals

Here we take the opportunity to start to examine the close connection between oscillatory integrals of the form[a]

$$I(\vec{a}) \;=\; \int_0^1 e^{2\pi i[a_d t^d + a_{d-1} t^{d-1} + \cdots + a_1 t]} dt$$

and complete exponential sums

$$S(\vec{a}) \;=\; \frac{1}{N} \sum_{t \bmod N} e^{2\pi i[a_d t^d + a_{d-1} t^{d-1} + \cdots + a_1 t]/N}$$

where $\vec{a} = (a_1, \ldots, a_d)$ is a d-tuple of real numbers in the first (integral) case whereas it is a d-tuple of integers in the second (sum) case. The sum defining S is taken over any complete set of residues mod N; for example, we can take $t = 0, 1, \ldots, N-1$. In both cases we have $|I(\vec{a})|, |S(\vec{a})| \leq 1$ and we are interested in estimates which which improve this trivial bound.

We start with examining these oscillatory objects when the polynomial phase is quadratic $a_2 t^2 + a_1 t$ in which case the sum $S(\vec{a}) = G_N(a_1, a_2)$ is the Gauss sum which we have seen several times already. We had noted that when N is odd, $S(a,b) = G_N(a,b)$ vanishes unless $|a| \leq |b|$

in which case $|S(a,b)| = |b|^{-1/2}$ – here we are using our notation $|b| = N/gcd(b,N)$ and $|a| \leq |b|$ means $gcd(b,N)|a$.

Often a complete exponential sum vanishes when it does not *see* the critical points of its phase – the corresponding situation for oscillatory integrals is that there is rapid decay (manifested by repeated integration by parts) when there are no critical points detected in the interval of integration. In this way, we see that the oscillatory integral $I(a,b)$ behaves very similarly to $S(a,b)$. In fact,

$$I(a,b) \ = \ \int_0^1 e^{2\pi i[bt^2+at]}dt$$

rapidly decays if the critical point $t = -a/2b$ of the phase $bt^2 + at$ lies outside the interval $[0,1]$ or $|b| \leq |a|$ and if $|a| \leq |b|$, then completing the square of the phase and making a simple change of variables shows $|I(a,b)| = c|b|^{-1/2} + O(|b|^{-1})$ as $|b| \to \infty$ – this can made precise if a smooth cut-off ϕ is inserted in the definition of I.

This may seem special to quadratic phases but the uncanny similarities persist in the general case. A useful estimate for $I(\vec{a})$ in euclidean harmonic analysis is

$$|I(\vec{a})| \ \leq \ C_d\|\vec{a}\|^{-1/d} \tag{36}$$

where $\|\vec{a}\|$ is any norm on $\mathbb{R}^d$ (all norms on $\mathbb{R}^d$ are equivalent after-all!). This is optimal with respect to uniform decay as measured with respect to some norm of the coefficients $\vec{a}$. In general, as a complex-valued function on $\mathbb{R}^d$, $I(\vec{a})$ is very complicated (H. Duistermaat based much of this theory about oscillatory integrals on his study of $I(\vec{a})$) and knowing what $L^q(\mathbb{R}^d)$ spaces $I(\vec{a})$ belongs to is a non-trivial problem. Understanding the range of q where this is true is important in euclidean harmonic analysis (connected with the Fourier restriction problem to the curve $t \to (t, t^2, \ldots, t^d)$) and important in classical number theory (connected to Tarry's problem) – we will come back to this point later.

Using our notation $\|\vec{a}\| = \max(|a_1|, \ldots, |a_d|)$ for elements in $\mathbb{Z}/N\mathbb{Z}$, a classical result of Hua [33] from the 1930s can be formulated as the estimate[b] $|S(\vec{a})| \leq C_d\|\vec{a}\|^{-1/d}$ which of course looks very similar to the basic estimate for the oscillatory integral $I(\vec{a})$. Again this result is optimal as a uniform bound with respect to the "norm" of the coefficients $\vec{a}$. This should be contrasted with A. Weil's estimate [57] for these sums over finite fields (this being the case when N is prime) where the decay rate $1/d$ is improved to $1/2$.

Another interesting and important case to study is the two term phase $bt^d + ab$ for general $d \geq 2$, the corresponding exponential sum $S_{a,b} := S(a,0,\ldots,0,b)$ arises in Waring's Problem of representing integers as sums of dth powers. We may assume $gcd(b,N) = 1$ and in this case

Hua's estimate above reads $|S_{a,b}| \leq C_d \|(a,b)\|^{-1/d} = C_d N^{-1/d}$ which again is the optimal uniform bound for all choices of a and b with $gcd(b,N) = 1$. Hua observed though that if the linear coefficient a is also coprime to N (that is, $gcd(a,N) = 1$), then one can achieve the square root (finite field) decay; more generally he proved $|S_{a,b}| \ll N^{-1/2} gcd(a,N)$ and used this to improve upon Vinogradov's work on the major arcs in Waring's problem – Chapter 4 in [56].

Since Hua proved this estimate (and given its connection with Waring's problem), several improvements were made, culminating in the bound $|S_{a,b}| \ll N^{-1/2}[gcd(a,N)]^{(d-2)/2(d-1)}$ established by Loxton and Vaughan in [42], and together with Hua's general estimate $|S_{a,b}| \ll N^{-1/d}$ gives us a fairly complete picture of the sum $S_{a,b}$. One could have guessed the Loxton-Vaughan estimate by examining the corresponding oscillatory integral

$$I_{a,b} := \int_0^1 e^{2\pi i[bt^d + at]} dt$$

where an application of van der Corput's Lemma 3.2 shows $|I_{a,b}| \leq C_d |b|^{-1/2} [|b|/|a|]^{(d-2)/2(d-1)]}$ holds and an application of stationary phase shows this is sharp in the region $|a| \leq |b|$ where this bound beats the bound in (36), $|I_{a,b}| \leq C_d |b|^{-1/d}$. Using our notation $|\cdot|$ in the mod N setting shows that these estimates for $S_{a,b}$ and $I_{a,b}$ match!

The sum $S_{a,b}$ also arises in the Fourier Restriction Problem mod N for the curve $t \to (t, t^d)$ and the Loxton-Vaughan estimate for $S_{a,b}$ is crucial in order to obtain the full range of $L^p - L^q$ estimates.

The exponential sum $S_{a,b}$ only served as a model case for Loxton and Vaughan and in [42], they went on to prove sharp bounds for $S(\vec{a})$ for general polynomial phases. It is interesting to compare the general Loxton-Vaughan estimate to an incredibly sharp and stable bound for the oscillatory integral $I(\vec{a})$ due to Phong and Stein [46] which played a key role in their analysis of certain degenerate Fourier Integral Operators. One finds that the general Loxton-Vaughan bound is a weak form of the Phong-Stein bound and it is natural to ask whether the full strength of the Phong-Stein estimate holds for the exponential sums $S(\vec{a})$. It turns out it does hold and so one has a strengthening of the Loxton-Vaughan estimate, see [60]. This gives an interesting illustration of how ideas from harmonic analysis can be used in purely number-theoretic problems.

[a] A more accurate comparison can be made if we replace the sharp cut-off $\chi_{[0,1]}(t)$ in the oscillatory integral I with a smooth cut-off $\phi(t)$ which is identically 1 in a neighborhood of $[0,1]$ but we will ignore this subtlety here

[b] strictly speaking Hua proved the estimate $|S(\vec{a})| \ll \|\vec{a}\|^{-1/d}$ but his arguments have been refined to give the stated estimate; see for example [13] and [53]

Exercises

4.1 Recall the notation of size $|x| = N/gcd(x, N)$ for integers x and partial ordering $a \leq b$ if $a|b$ between integers a, b. Show that comparing sizes $|x| \leq |y|$ is equivalent to $gcd(y, N)|x$.

4.2 Fix a divisor d of N and recall the definition of $\mathcal{B}_d$. Show what $\vec{x} = (x_1, \ldots, x_d) \in \mathcal{B}_d$ if and only if N/d divides every x_j.

4.3 Let $d(n) = \sum_{d|n} 1$ be the number of divisors of an integer n. Show that $d(n) \ll 1$ – recall the notation $d(n) \ll 1$ used in the text means for every $\epsilon > 0$ there is a constant C_ϵ such that $d(n) \leq C_\epsilon n^\epsilon$.

Hint: note that if $n = p_1^{a_1} \cdots p_r^{a_r}$ is the prime factorisation of n, then $d(n)/n^\epsilon = \prod_{j=1}^r (a_j+)/p_j^{\epsilon a_j}$ and use the bound $(a+1)/p^{\epsilon a} \leq 1$ if $p \geq 2^{1/\epsilon}$.

4.4 Show that for $1 \leq a \leq 2$, $\sum_{d|n} \phi(n)/n^a \ll 1$ where ϕ is Euler's totient function.

4.5 Show the properties for the Gauss sum $G_N(a, b)$ stated in the text; namely, show that $G_N(a, b)$ vanishes unless $gcd(b, N) \mid a$ in which case $|G_N(a, b)| = \sqrt{gcd(b, N)/N}$ when N is odd.

4.6 Put in a smooth cut-off function in the definition of $I(a, b)$ and make the analysis given above regarding $I(a, b)$ precise.

4.7 Use van der Corput's Lemma 3.2 to show that $|I(\vec{a})| \leq C_d \|\vec{a}\|^{-1/d}$.

4.8 Show the claimed bound $|I_{a,b}| \leq C_d |b|^{-1/2} [|b|/|a|]^{(d-2)/2(d-1)}$.

An abstract L^2 restriction theorem

It is often more convenient to think of the Fourier restriction problem in terms of a given measure μ instead of proving an a priori estimate for the operation of restricting the Fourier transform of functions to a given set of frequencies S in the dual space; that is, to examine the a priori inequalities

$$\Big(\int |\hat{f}(y)|^q \, d\mu(y) \Big)^{1/q} \;\leq\; C \, \|f\|_{L^p}$$

where in practice we think of the measure μ as being supported on a set of frequencies S, perhaps a surface measure if S is an algebraic variety.

As is well-known many L^2 restriction results (where $q = 2$ in the above inequality) follow from two ingredients; the decay of the Fourier transform of μ (often related to the Fourier dimension of the support S of μ) and the regularity of μ – behaviour of μ on balls B_r – which can be related to some geometric dimension of S. These two ingredients are nicely blended in a general L^2 restriction argument and in this

section, we give this argument in a sufficiently abstract setting to include many known results and to suit our needs.

Let G be a locally compact abelian (LCA) group with Haar measure m, equipped with a one parameter family of nested translation-invariant balls $\{B_r^G\}_{r>0}$, $B_r^G(x) = x+B_r^G(0)$ and $B_r^G(0) \subset B_s^G(0)$ whenever $r < s$, whose union is all of G and satisfying the regularity property

(R) $m(B_r^G(0)) \leq C_1\, r^n$.

Also suppose that its dual group $\widehat{G}$ with Haar measure m', normalised so that the inversion formula (and hence Plancherel's theorem) holds, is equipped with a dual family of translation-invariant balls $\{B_s^{\widehat{G}}(y)\}_{s>0}$. Furthermore suppose there is a family of real-valued functions $\{\varphi_r\}$ on G so that $\varphi_r = 1$ on $B_r^G(0)$, $\mathrm{supp}(\varphi_r) \subset B_{2r}^G(0)$, $\|\varphi_r\|_{L^\infty(G)} \leq C_2$ and satisfying

(Φ) $|\widehat{\varphi}_r(y)| \leq C_3 s^{-n}$ whenever $-y \notin B_s^{\widehat{G}}(0)$ and $s > 1/r$.

It is important in applications that the family of balls $\{B_r^G\}$, as well as the dual family $\{B_s^{\widehat{G}}\}$, do not necessarily arise from a metric, or even a quasimetric. This will be the case in our basic application where the underlying LCA group arises from the ring of integers mod N.

For many applications we can take $\varphi_r = \chi_{B_r^G(0)}$ but only in cases where the characteristic functions of the balls B_r^G are smooth enough, in the sense that (Φ) holds. This will be the case in our main application, when $G = [\mathbb{Z}/N\mathbb{Z}]^n$ and the balls arise from the sets $\{\mathcal{B}_d\}$ described in the previous section. It is also the case when G is a finite dimensional vector space over any locally compact field whose topology arises from a nonarchimedian metric (the balls being the natural ones defined in terms of the metric). However when $G = \mathbb{R}^n$ and $n \geq 2$, the characteristic function of euclidean balls are not smooth enough; that is, (Φ) does not hold. But in this case we can simply take smoothed out versions of characteristic functions; for instance, $\varphi_r(x) = \phi(x/r)$ for some fixed $\phi \in C_c^\infty(\mathbb{R}^n)$ so that $\phi = 1$ on $B_1(0)$ and $\mathrm{supp}(\phi) \subset B_2(0)$.

One can view conditions (R) and (Φ) as prescribing a dimension ($= n$) to G; (R) $\leftrightarrow$ Geometric dimension and (Φ) $\leftrightarrow$ Fourier dimension.

For our restriction theorem we will need a finite (positive) measure μ supported on the dual group $\widehat{G}$ satisfying

(Rμ) $\mu(B_s^{\widehat{G}}(y)) \leq C_4 s^a$ for some $a < n$, uniformly in $y \in \widehat{G}$, and

(Fμ) $|\widehat{\mu}(x)| \leq C_5 r^{-b/2}$ for all $-x \notin B_r^G(0)$.

Theorem 4.2. *Let G be a LCA group and μ be finite measure on $\widehat{G}$ with all the properties described above. Then*

$$\Big(\int_{\widehat{G}} |\hat{f}(y)|^2\, d\mu(y)\Big)^{1/2} \;\leq\; C\|f\|_{L^p(G,m)} \tag{37}$$

holds for $1 \leq p \leq p_0$ where $p_0 = (n-a+[b/2])/(n-a+[b/4])$. Furthermore the constant C in (37) depends only on $p, n, C_1, C_2, C_3, C_4, C_5, a$ and b.

Proof. We give the proof here only in the range $1 \leq p < p_0$ and in this case, it suffices by real interpolation to establish (37) at the endpoint $p = p_0$ for characteristic functions $f = \chi_E$, $E \subset G$. For this, we use an argument due to A. Carbery. To obtain the strong-type bound at $p = p_0$, one can use a recent argument due to J.G. Bak and A. Seeger [4] but this is somewhat more involved and we have decided to present only the slightly weaker result here.

By duality,

$$\int_{\widehat{G}} |\widehat{\chi}_E(y)|^2\, d\mu(y) \;=\; \int_G \chi_E(x)\overline{\chi_E * (d\mu)^\vee}(x)\, dm(x)$$

and we will write this last integral as $I+II$ via the decomposition $\mu = \mu_1+\mu_2$ where $\widehat{\mu}_1(-x) = (\mu)^\vee(x)\varphi_r(x)$ and $\widehat{\mu}_2(-x) = (\mu)^\vee(x)[1-\varphi_r(x)]$ for some appropriate value of $r > 0$ chosen later. Since

$$|II| \;\leq\; m(E)\|\chi_E * (d\mu_2)^\vee\|_{L^\infty(G)} \;\leq\; m(E)^2\|(d\mu_2)^\vee\|_{L^\infty(G)}$$

and by (Fμ), $\|(d\mu_2)^\vee\|_{L^\infty(G)} \leq 2C_2C_5r^{-b/2}$, we have $|II| \leq 2C_2C_5m(E)^2r^{-b/2}$. On the other hand by Cauchy-Schwarz and Plancherel,

$$|I| \;\leq\; m(E)^{1/2}\,\|\chi_E{*}(d\mu_1)^\vee\|_{L^2(G)} \;=\; m(E)^{1/2}\,\|\big(\chi_E{*}(d\mu_1)^\vee\big)^\wedge\|_{L^2(\widehat{G})} \leq m(E)\|\mu_1\|_{L^\infty}.$$

But $\mu_1(y) = \widehat{\varphi}_r * d\mu(y)$ and so

$$\mu_1(y) \;=\; \int_{B^{\widehat{G}}_{1/r}(y)} \widehat{\varphi}_r(y-z)d\mu(z) \;+\; \sum_{k\geq 1}\int_{B^{\widehat{G}}_{2^k/r}\setminus B^{\widehat{G}}_{2^{k-1}/r}(y)} \widehat{\varphi}_r(y-z)d\mu(z)$$

which we write as $J_1 + J_2$. Since $\|\widehat{\varphi}_r\|_{L^\infty(\widehat{G})} \leq C_2m(B^G_r(0))$, we find

$$|J_1| \;\leq\; C_2m(B^G_r(0))\mu(B^{\widehat{G}}_{1/r}(y)) \;\leq C_2C_1C_4\, r^{n-a};$$

and since $|\widehat{\varphi}_r(y-z)| \leq C_3[r/2^{k-1}]^n$ whenever $z \notin B^{\widehat{G}}_{2^{k-1}/r}(y)$ by (Φ), we also find via (Rμ) that

$$|J_2| \;\leq\; C_3\sum_{k\geq 1}[r/2^{k-1}]^n\mu(B^{\widehat{G}}_{2^k/r}(y)) \leq AC_3C_4\, r^{n-a}$$

where $A = 2^n/(2^{n-a}-1)$. Putting things together we have

$$|I| \;\leq\; [AC_3C_4 + C_1C_2C_4]m(E)r^{n-a}.$$

Now choosing r so that $r^{n-a+b/2} \sim m(E)$ finishes the proof. □

Theorem 37 generalises an L^2 restriction theorem of A. Greenleaf in [29] where $G = \mathbb{R}^n, n \geq 2$ with the usual euclidean balls and μ is carried along a subvariety of lower dimension (which in turn generalises the Tomas-Stein L^2 restriction theorem

for the sphere; see [55] and [49]). In [43] Greenleaf's theorem was generalised to include the one dimensional $\mathbb{R}^1$ setting but no endpoint $p = p_0$ estimate was proved. The result of Bak and Seeger [4] extends this result to the endpoint $p = p_0$. Theorem 37 provides a generalisation of the L^2 restriction in [43] and [4]. Finally Theorem 37 can be applied in the setting of $\mathbb{Q}_p^n$ where $\mathbb{Q}_p$ is the field of p-adic numbers (or more generally, when $G = \mathbb{F}^n$ and $\mathbb{F}$ is any local field), giving the analogue of the L^2 restriction in [43] and [4] in this setting.

In [44] a similar L^2 restriction argument is given, based on an argument of Bourgain, in the setting of finite fields; due to the fact that there are effectively only two scales to work with, one even obtains a strong type estimate at the endpoint and in particular the Fourier restriction estimate at $p_0 = (2n+2)/(n+3)$ holds for the paraboloid in finite fields.

L^2 restriction in $\mathbb{Z}/N\mathbb{Z}$

In this section we will apply Theorem 37 to obtain L^2 restriction theorems when $G = [\mathbb{Z}/N\mathbb{Z}]^n$. For this purpose we introduce the following one parameter nested family of balls:

$$B_r^G(0) \;=\; \bigcup_{d|N;d\leq r} \mathcal{B}_d$$

where the sets $\mathcal{B}_d = \{\vec{x} : \|\vec{x}\| \leq d\}$ were introduced previously (**warning**: the above union is taken over all divisors d which are less than r in the usual sense whereas the inequality $\|\vec{x}\| \leq d$ defining $\mathcal{B}_d$ is taken in the sense of the notation introduced above). When $N = p^L$ is a power of a fixed prime p, the sets $\mathcal{B}_d$ are already nested and $B_r^G(0) = \mathcal{B}_r$ when r is a divisor. We then define $B_r^G(x) := x + B_r^G(0)$ and note that (using m to denote counting measure on $G = [\mathbb{Z}/N\mathbb{Z}]^n$)

$$m(B_r^G(0)) \;\leq\; \sum_{d|N;d\leq r} m(\mathcal{B}_d) \;=\; \sum_{d|N;d\leq r} d^n \;\leq\; \big[\sum_{d|N} 1\big]\; r^n$$

which verifies (R) with $C_1 = C_\epsilon N^\epsilon$.

The dual balls $B_r^{\widehat{G}}$ will be defined in terms of the sets

$$\mathcal{C}_d \;:=\; \{\vec{x} \in [\mathbb{Z}/N\mathbb{Z}]_*^n :\; \|\vec{x}\| \leq |d|\} \;=\; \{\vec{x} = (x_1, \ldots, x_n) :\; d \,|\, x_j,\; 1 \leq j \leq n\},$$

indexed by the divisors of N. In fact we define

$$B_r^{\widehat{G}}(0) \;:=\; \bigcup_{d|N;d\geq 1/r} \mathcal{C}_d$$

and then $B_r^{\widehat{G}}(x) := x + B_r^{\widehat{G}}(0)$. For the family of functions φ_r we simply take $\varphi_r := \chi_{B_r^G(0)}$ and our next goal is to establish (Φ) which can be written in this situation as

$$\Big|\sum_{\vec{x}\in B_r^G(0)} e^{2\pi i \vec{y}\cdot\vec{x}/N}\Big| \;\leq\; C_3\, s^{-n} \quad \text{for} \quad -\vec{y} \notin B_s^{\widehat{G}}(0), \quad \text{whenever } s > 1/r. \tag{38}$$

By the inclusion-exclusion principle the sum on the left hand side of (38) is equal to

$$\sum_{\substack{d|N\\ d\leq r}} \sum_{\vec{x}\in\mathcal{B}_d} e^{2\pi i\vec{y}\cdot\vec{x}/N} - \frac{1}{2} \sum_{\substack{d|N\\ d\leq r}} \sum_{\substack{d'|N, d'\neq d\\ d'\leq r}} \sum_{\vec{x}\in\mathcal{B}_d\cap\mathcal{B}_{d'}} e^{2\pi i\vec{y}\cdot\vec{x}/N} + \cdots := \sum_{j=1}^{Q} I_j$$

where $Q = \sum_{d|N, d\leq r} 1$ and the jth term I_j is a sum taken over all jth-fold products $\mathcal{B}_{d_1}\cap\cdots\cap\mathcal{B}_{d_j}$, $d_1,\ldots,d_j$ are j distinct divisors of N all of which are less than r.

We make the simple observation that for any j tuple $(d_1,\ldots,d_j)$ of distinct divisors of N, $\mathcal{B}_{d_1}\cap\cdots\cap\mathcal{B}_{d_j} = \mathcal{B}_d$ where $d = gcd(d_1,\ldots,d_j)$ is a divisor of N. Furthermore $d\leq r$ since each divisor $d_\ell\leq r$ and for such a d,

$$\sum_{\vec{x}\in\mathcal{B}_d} e^{2\pi i\vec{y}\cdot\vec{x}/N} \;=\; d^n \quad \text{if} \quad \vec{y}\in\mathcal{C}_d$$

and vanishes otherwise. But $-\vec{y}\notin B_s^{\widehat{G}}(0)$ precisely means that $\vec{y}\notin\mathcal{C}_d$ for all $d\geq 1/s$ and therefore $\vec{y}\in\mathcal{C}_d$ forces $d\leq 1/s$. Therefore each sum

$$\sum_{\vec{x}\in\mathcal{B}_d} e^{2\pi i\vec{y}\cdot\vec{x}/N}, \quad \sum_{\vec{x}\in\mathcal{B}_d\cap\mathcal{B}_{d'}} e^{2\pi i\vec{y}\cdot\vec{x}/N}, \quad \sum_{\vec{x}\in\mathcal{B}_d\cap\mathcal{B}_{d'}\cap\mathcal{B}_{d''}} e^{2\pi i\vec{y}\cdot\vec{x}/N},$$

etc... gives a contribution of s^{-n} but unfortunately the total number of such sums is exponential in the number of divisors of N which is unacceptable.

Therefore we fix a divisor d_* with $\vec{y}\in\mathcal{C}_{d_*}$ and attempt to see some cancellation in the coefficient of d_*^n in the sum $\sum_{j=1}^{Q} I_j$ above. For each $1\leq j\leq Q$ we need to count the number of j-tuples $(d_1,\ldots,d_j)$ of distinct divisors of N, each satisfying $d_\ell\leq r$, so that $d_* = gcd(d_1,\ldots,d_j)$. Let's call this number U_j; the contribution to the coefficient of d_*^n from I_j is then $(-1)^{j+1}U_j$ and our goal is to show that $\sum_{j=1}^{Q}(-1)^{j+1}U_j$ has an acceptable bound. Clearly $U_1 = 1$ and to understand U_j for $j\geq 2$, we introduce some notation. Let $N = p_1^{a_1}\cdots p_m^{a_m}$ and $d_* = p_1^{s_1}\cdots p_m^{s_m}$ and note that if $d_* = gcd(d_1,\ldots,d_j)$ where each $d_\ell\leq r$, then for any $d\in\{d_1,\ldots,d_j\}, d = p_1^{k_1}\cdots p_m^{k_m}$ with $s_\ell\leq k_\ell < s_\ell + M_\ell, 1\leq\ell\leq m$ for some natural numbers $\{M_1,\ldots,M_m\}$ depending on N, d_* and r; clearly $M_k\leq a_k$ for each $1\leq k\leq m$.

Let R denote the total number of divisors $d = p_1^{k_1}\cdots p_m^{k_m}$ of N satisfying $d\leq r$ and $s_\ell\leq k_\ell, 1\leq\ell\leq m$. A simple counting argument shows that $U_2 = 2(R-1) + (2^m - 2)M_1\cdots M_m$.

ANALYSIS INCOMPLETE: we need to finish the analysis of each U_j and bound the sum $\sum_{j=1}^{Q}(-1)^{j+1}U_j$ and hence $\sum_{j=1}^{Q} I_j$.

We are now in a position to employ the L^2 restriction theorem, Theorem 37, in the setting $G = [\mathbb{Z}/N\mathbb{Z}]^n$ whenever we have a measure μ supported in the dual group $\widehat{G}$ satisfying the regularity condition (Rμ) and decay estimate (Fμ).

L^2 restriction to paraboloids and the proof of Theorem 4.1. Let us complete the proof of the L^2 Fourier Restriction Theorem 4.1 for the paraboloid $S = \{(x_1, \dots, x_{n-1}, x_1^2 + \cdots + x_{n-1}^2)\}$; here we take the natural measure μ carried by S whose Fourier transform is

$$\widehat{\mu}(\vec{x}) \;=\; \frac{1}{N^{n-1}} \sum_{\vec{y} \in [\mathbb{Z}/N\mathbb{Z}]_*^{n-1}} e^{2\pi i (x_1 y_1 + \cdots + x_{n-1} y_{n-1} + x_n [y_1^2 + \cdots + y_{n-1}^2])/N}.$$

As we have seen, this exponential sum can be written as a product of Gauss sums $\widehat{\mu}(\vec{x}) = \prod_{j=1}^{n-1} G_N(x_j, x_n)$ which vanishes unless $gcd(x_1, \dots, x_n, N) = gcd(x_n, N)$ (or $\|\vec{x}\| = |x_n|$ using our notation) in which case

$$|\widehat{\mu}(\vec{x})| \;\le\; 2\,|x_n|^{-\frac{n-1}{2}} \;=\; 2\,\|\vec{x}\|^{-\frac{n-1}{2}}.$$

Now if $\vec{x} \notin B_r^G(0)$, then $\vec{x} \notin \mathcal{B}_d$ for all divisors d of N satisfying $d \le r$ which implies $r \le N/d' = \|\vec{x}\|$ where $d' = gcd(x_1, \dots, x_n, N)$. Therefore

$$|\widehat{\mu}(\vec{x})| \;\le\; 2\,r^{-(n-1)/2} \qquad \text{whenever} \qquad \vec{x} \notin B_r^G(0)$$

and this shows that (Fμ) holds with $C_5 = 2$ and $b = n-1$. Finally to verify (Rμ), we observe

$$\mu(B_r^G(\vec{x})) \;\le\; \sum_{d|N; d \le r} \mu(\vec{x} + \mathcal{B}_d) \;\le\; \sum_{d|N; d \le r} d^{n-1} \;\le\; \Big[\sum_{d|N} 1\Big]\, r^{n-1}$$

which shows that (Rμ) holds with $C_4 = C_\epsilon N^\epsilon$ and $a = n-1$. Now appealing to Theorem 37 completes the proof of Theorem 4.1.

We remark here that in the finite field setting, the L^2 restriction result Theorem 4.1 gives the same estimate as in Proposition 2.2 but is far from sharp as we expect that the necessary condition $p' \ge 2n/(n-1)$ is likely to be sufficient if S does not contain any affine subspaces.

L^2 restriction to the moment curve. As in the euclidean setting L^2 restriction arguments based only on the isotropic decay of the Fourier transform of μ (the condition $(F\mu)$ should be thought of as a generalised notion of isotropic decay) will not give sharp results outwith the setting of hypersurfaces S. To illustrate this (and to initiate a discussion for what comes next) we consider the case when S is the curve given by $S = \{(t, t^2, \dots, t^n) : t \in \mathbb{Z}/N\mathbb{Z}\}$. The measure μ in this case has the following exponential sum as its Fourier transform,

$$\widehat{\mu}(\vec{x}) \;=\; \frac{1}{N} \sum_{t=0}^{N-1} e^{2\pi i (x_1 t + x_2 t^2 + \cdots + x_n t^n)/N}$$

which has been thoroughly studied by number theorists, starting with Hua's [33] classical estimate $|\widehat{\mu}(\vec{x})| \le A_n \|\vec{x}\|^{-1/n}$ (using our notation) discussed previously. Therefore as above, one verifies that in this case (Fμ) holds with $C_5 = A_n$ and $b = 2/n$ and (Rμ) holds with $a = 1$ so that Theorem 37 gives an L^2 restriction estimate for the curve S in the range $1 \le p \le (n^2 - n + 1)/(n^2 - n + [1/2])$.

That this range may not be optimal is seen by the scaling argument used previously for the paraboloid. Here one uses the anisotropic boxes

$$\mathcal{P} \;=\; \{(x_1,\dots,x_n):\; d|x_1,\, d^2|x_2,\dots,d^n|x_n\}$$

where d is divisor of N so that d^n is also a divisor. One then checks as before that (34) can only hold when

$$q\,\frac{n(n+1)}{2} \;\le\; p' \tag{39}$$

which corresponds to the euclidean exponents. When $q=2$, this gives the larger range $1\le p\le (n^2+n)/(n^2+n-1)$ (a strictly larger range when $n\ge 3$, the case when the curve S is not a hypersurface). We remark again that this scaling argument does not work in the setting of finite fields and recall that in this case, Corollary 2.4 shows that the necessary and sufficient conditions for all (finite field) restriction estimates (13) to the moment curve $S=\{(t,t^2,\dots,t^n)\}$ are $p'\ge nq$ and $p'\ge 2n$. We will return to this case in the setting of $\mathbb{Z}/N\mathbb{Z}$ in the following section.

L^2 restriction for other surfaces. One could of course consider more general algebraic varieties S, say parametrised by $S=\{(\vec{x},p_{k+1}(\vec{x}),\dots,p_n(\vec{x})) :\; \vec{x}=(x_1,\dots,x_k)\}$ for some $1\le k<n$ and polynomials $p_j\in\mathbb{Z}[X_1,\dots,X_k]$, $k+1\le j\le n$; the measure μ in this case is the natural one carried by this variety and one easily verifies (as in the case of the paraboloid) that (Rμ) holds with $C_4=C_\epsilon N^\epsilon$ and $a=k$. Therefore if we have an exponential sum estimate for the Fourier transform of μ satisfying (Fμ) for some $b>0$, then we can employ Theorem 37 to obtain an L^2 restriction estimate and the natural question arises whether such a result is sharp. If the polynomials p_j are homogeneous then one could use the scaling argument as before to deduce a necessary condition on the exponents p and q for (34) to hold; namely that $q(k+\sum_{j=k+1}^n m_j)\le kp'$ where m_j is the degree of homogeneity of the polynomial p_j. Let us now further restrict ourselves to hypersurfaces S, so $k=n-1$, and let m denote the homogeneous degree of $f(\vec{x}):=p_n(x_1,\dots,x_{n-1})$; the necessary condition for (34) to hold when $q=2$ then reads

$$2(1+\frac{m}{n-1}) \;\le\; p' \tag{40}$$

so that Theorem 37 would give a sharp L^2 restriction result if (Fμ) holds for $b=2(n-1)/m$. Such decay estimates for exponent sums are known for the Fourier transform of surface measures μ_f of $S_f=\{(x_1,\dots,x_{n-1},f(x_1,\dots,x_{n-1})\}$ for particular choices of f,

$$\widehat{\mu}_f(\vec{x},x_n) \;=\; \frac{1}{N^{n-1}}\sum_{\vec{y}\in[\mathbb{Z}/N\mathbb{Z}]^{n-1}} e^{2\pi i(\vec{x}\cdot\vec{y}+x_nf(\vec{y}))/N}.$$

For instance sharp estimates for the exponential sum $\widehat{\mu}_f$ when $N=p^L$ is a power of a prime p follow from work of J. Denef and S. Sperber [20] (see also [16] and [17]), resolving a conjecture of J. Igusa under a nondegeneracy condition of the homogeneous polynomial f. We now describe their work.

Let $g(\vec{y}) = \sum a_\alpha \vec{y}^\alpha$ be a homogeneous polynomial with integer coefficients. The *Newton polyhedron* $\Delta = \Delta(g)$ of g is the convex hull of the union of all orthants (or hyperoctants) $\alpha + \mathbb{R}^n_+$ in $\mathbb{R}^n$ with $a_\alpha \neq 0$ and we say that g is nondegenerate with respect to it's Newton polyhedron Δ if $g_\tau(\vec{y}) := \sum_{\alpha\in\tau} a_\alpha \vec{y}^\alpha$ has no critical points in $(\mathbb{C}\setminus 0)^{n-1}$ for each compact face τ of Δ. Let $d(g) \in \mathbb{R}$ be the infimum of all $\beta > 0$ such that $\beta\mathbf{1} \in \Delta$ – the exponent $d(g)$ is known as the Newton distance of g. Under these conditions[7] it was shown in [20], [16] and [17] that the exponential sum

$$\mathcal{S}_g \;=\; p^{-L(n-1)} \sum_{\vec{y}\in[\mathbb{Z}/p^L\mathbb{Z}]^{n-1}} e^{2\pi i g(\vec{y})/p^L}$$

has the uniform estimate $|\mathcal{S}_g| \ll p^{-L/d(g)}$ for almost every prime p (that is, all but finitely many primes p) where C is a constant independent of p and L, depending only on Δ. Many times $d(f) = m/(n-1)$ but it can happen that $d(f) \geq m/(n-1)$.

One can now follow the arguments in [20], [16] and [17] and establish the following lemma.

Lemma 4.3. *Suppose that $f \in \mathbb{Z}[X_1, \ldots, X_{n-1}]$ is homogeneous and is nondegenerate with respect to its Newton polyhedron. Then for $N = p^L$, $(F\mu)$ holds for $\widehat{\mu}_f$ for almost every prime p with $b = 2/d(g)$ and $c_5 = C_\epsilon p^{\epsilon L}$.*

One can refine the scaling argument producing the necessary condition (40) for surfaces S_f given by a homogeneous polynomial f in cases where $d(f) \geq m/(n-1)$ to see that $p' \geq 2(d(f)+1)$ is a further necessary condition, see [62]. Hence Lemma 4.3, together with the above discussion gives the following proposition.[8]

Proposition 4.4. *Suppose that $f \in \mathbb{Z}[X_1, \ldots, X_{n-1}]$ is homogeneous and is nondegenerate with respect to its Newton polyhedron. Then with $N = p^L$ restricted to be powers of prime numbers, the L^2 restriction result (so $q = 2$ in (34)) holds for almost every prime p if and only if $p' \geq 2(d(f)+1)$.*

When $n = 3$ we can drop the nondegeneracy condition and treat an arbitrary homogeneous polynomial $f(x, y)$. This follows from a recent full resolution of the Igusa conjecture for exponential sums of binary forms [61]. Interestingly the approach and inspiration in the general case for $n = 3$ is different from the work in the nondegenerate case and takes a harmonic analysis perspective espoused in these lectures with inspiration from work of Phong, Stein and J. Sturm [46], [47] and I.A. Ikromov and D. Müller [37] and [38].

The decay rate for $\mathcal{S}_f$ is now measured in terms of the *height* $h(f)$ of f, being defined as $h(f) = \sup_z d_z(f)$ where the supremum is taken over all smooth local coordinate systems $z = (x, y)$ of the origin and $d_z(f)$

[7] In [20]. it was further assumed that no vertex of F_0 belongs to $\{0, 1\}^{n-1}$. This assumption was removed in [16] and [17].

[8] Using the arguments in [16] and [17], it is also possible to extend Proposition 4.4 to treat quasi-homogeneous polynomials f.

denotes the *Newton distance* of f in the coordinates z. In [61], the following uniform bound for $\mathcal{S}_f$ was established for general homogeneous polynomials f.

Lemma 4.5. *Let $f \in \mathbb{Z}[X,Y]$ be any homogeneous polynomial. Then*

$$|\mathcal{S}_f| \ll p^{-L/h(f)} \tag{41}$$

holds for almost every prime p. Furthermore, $(F\mu)$ holds for $\widehat{\mu}_f$ for almost every prime p with $b = 2/h(f)$ and $c_5 = C_\epsilon p^{\epsilon L}$.

It turns out that scaling argument used to establish the necessary condition $p' \geq 2(1+m/(n-1)) = 2+2m$ can be again refined to show $p' \geq 2(h(f)+1)$ is necessary, see [62]. Hence we have the following extention of Proposition 4.4 when $n = 3$.[a]

Proposition 4.6. *Suppose that $f \in \mathbb{Z}[X,Y]$ is homogeneous. Then with $N = p^L$ restricted to be powers of prime numbers, the L^2 restriction result (so $q = 2$ in (34)) holds for almost every prime p if and only if $p' \geq 2(h(f)+1)$.*

[a] also quasi-homogeneous polynomials are treated in [61], giving the same result.

Propositions 4.4 and 4.6 should be compared to results by Ikromov and Müller [38] where these bounds were obtained in the euclidean setting for general smooth $f(x,y)$ of finite type.

Fourier restriction for curves

In this section we consider the Fourier restriction problem (34) for the curve $S = \{(t, t^2, \dots, t^n) : t \in \mathbb{Z}/N\mathbb{Z}\}$. In the previous section we remarked that a scaling argument gives rise to the necessary condition (39) for the Fourier restriction estimates (34) to hold which match the euclidean condition. We now explore the possible L^p range for (34) to hold for S; by duality (34) is equivalent to

$$\Big(\sum_{\vec{x} \in [\mathbb{Z}/N\mathbb{Z}]^n} |\mathcal{E}b(\vec{x})|^{p'} \Big)^{1/p'} \leq C_{\epsilon,p,q,n} N^\epsilon \Big(\frac{1}{N} \sum_{t \in \mathbb{Z}/N\mathbb{Z}} |b(t)|^{q'} \Big)^{1/q'} \tag{42}$$

where $\mathcal{E}$ is the extension operator

$$\mathcal{E}b(\vec{x}) = \frac{1}{N} \sum_{t \in \mathbb{Z}/N\mathbb{Z}} b(t)\, e^{2\pi i (x_1 t + x_2 t^2 + \cdots + x_n t^n)/N}.$$

When $b = 1$ the right hand side of (42) is $C_{\epsilon,p,q,n} N^\epsilon$ and the left hand side is the $L^{p'}$ norm of the function

$$f(x_1, \dots, x_n) := \frac{1}{N} \sum_{t \in \mathbb{Z}/N\mathbb{Z}} e^{2\pi i (x_1 t + x_2 t^2 + \cdots + x_n t^n)/N} \tag{43}$$

and so it becomes of interest to determine the L^r range where

$$\|f\|_{L^r([\mathbb{Z}/N\mathbb{Z}]^n)} \leq C_{\epsilon,r} N^\epsilon \tag{44}$$

holds for every $\epsilon > 0$. The corresponding euclidean problem is to determine the $L^r(\mathbb{R}^n)$ spaces for which the oscillatory integral

$$g(x_1, \dots, x_n) \;=\; \int_0^1 e^{2\pi i(x_1 t + x_2 t^2 + \cdots + x_n t^n)}\, dt$$

belongs to and this in turn gives rise to a necessary condition on the L^p range for restriction problem for the curve $t \to (t, t^2, \dots, t^n)$ in $\mathbb{R}^n$. As we have already indicated, the L^r norm of the oscillatory integral g arises as the singular integral in Tarry's problem from number theory and so there has been considerable interest to determine when the singular integral is finite. G.I. Arkhipov, V.N Chubarikov and A.A. Karatsuba showed that the L^r norm of the oscillatory integral g is finite if and only if $r > 0.5n(n+1) + 1$; see [2]. Reinforcing our theme of these lectures, we have the following proposition whose proof we relegate to an appendix of these notes.

Proposition 4.7. *The inequality* (44) *holds if* $r > 0.5n(n+1) + 1$ *and fails if* $r < 0.5n(n+1) + 1$.

The endpoint $r = 0.5n(n+1)+1$ is left open but nevertheless we have the additional necessary condition $p' \geq 0.5n(n+1) + 1$ for the restriction problem (34) to hold for the curve $S = \{(t, \dots, t^n)\}$ in $[\mathbb{Z}/N\mathbb{Z}]^n$. We now turn to examining sufficient conditions for (34) to hold for S and we will see that known methods from the euclidean setting can be carried out in $\mathbb{Z}/N\mathbb{Z}$ if a certain number-theoretic conjecture is true; more precisely, for a fixed n-tuple $\vec{y} := (y_1, \dots, y_n)$ of integers mod N, we need a precise count of the number of solutions to the following system of mod N Diophantine equations:

$$\begin{array}{rcll} x_1 + x_2 + \cdots + x_n & = & y_1 + y_2 + \cdots + y_n & \\ x_1^2 + x_2^2 + \cdots + x_n^2 & = & y_1^2 + y_2^2 + \cdots + y_n^2 & \\ & \vdots & & \mod N \\ x_1^n + x_2^n + \cdots + x_n^n & = & y_1^n + y_2^n + \cdots + y_n^n. & \end{array} \tag{45}$$

Conjecture If $T_{\vec{y}}$ denotes the number of n-tuples $(x_1, \dots, x_n) \in [\mathbb{Z}/N\mathbb{Z}]^n$ solving (45), then $\#T_{\vec{y}} \ll \prod_{j<k} gcd(y_j - y_k, N)$ which in our notation reads $\#T_{\vec{y}} \ll N^{n(n-1)/2} \prod_{j<k} |y_j - y_k|^{-1}$.

In fact if this conjecture holds, we will see that the necessary conditions (39) are in fact sufficient but we will only achieve this in the restricted L^p range, $p' \geq 0.5n(n+2)$; this is the mod N analogue of the M. Christ euclidean restriction result in [14]. In fact we simply follow his argument, using our notation to pass between the euclidean world and the setting of the ring of integers mod N. Undoubtedly if we followed instead the *off-spring* method of Drury in [21], then we would be obtain the (possibly) complete L^p range, $p' > 0.5n(n+1) + 1$, again subject to the conjecture above. However we have not yet carried out Drury's analysis in this context.

Theorem 4.8. *If the* **Conjecture** *is true, then* (34) *holds for the curve* $S = \{(t, t^2, \dots, t^n) : t \in \mathbb{Z}/N\mathbb{Z}\}$ *lying in the dual* $\widehat{G}$ *of the group* $G = [\mathbb{Z}/N\mathbb{Z}]^n$ *if* (39) *and* $p' \geq 0.5n(n+2)$ *hold.*

Proof. The proof is a repetition of the proof of Proposition 2.3 in the finite field setting which proceeds by duality and where our goal is to prove

$$\|(bd\mu)^\vee\|_{p'} \ \ll \ \|g\|_{q'}; \tag{46}$$

here μ is surface measure on the moment curve S. We proceed step by step exactly as in Proposition 2.3 up to (18) which this context reads as

$$\|bd\mu * \cdots * bd\mu\|_r^r \ \leq \ \frac{1}{N^n} \sum_{\vec{t} \in [\mathbb{Z}/N\mathbb{Z}]^n} \prod_{i=1}^n |b(t_i)|^r \, [\#T_{\vec{t}}]^{r-1} \tag{47}$$

where $nr' = p'$.

To this point we have followed the euclidean argument in [14] where the change of variables $\vec{y} = \Phi(\vec{t})$ (performed twice) introduces the Jacobian factor

$$J_\Phi(\vec{t}) \ = \ \prod_{1 \leq j < k \leq n} |t_j - t_k|$$

and it's reciprocal, leading in the euclidean setting to

$$\|bd\mu * \cdots * bd\mu\|_r^r \ \leq \ \int_{\vec{t} \in \mathbb{R}^n} \prod_{i=1}^n |b(t_i)|^r \prod_{j<k} \frac{1}{|t_j - t_k|^{r-1}} \, d\vec{t}.$$

Given our perspective that the euclidean world is closely modeled by what happens in the ring of integers mod N, this in part led us to the **Conjecture** above since with our mod N notation, if $\#T_{\vec{t}} \ll \prod_{j<k} gcd(t_j - t_k, N) = N^{n(n-1)/2} \prod_{j<k} |t_j - t_k|^{-1}$, then (47) above reads

$$\|bd\mu * \cdots * bd\mu\|_r^r \ll \frac{1}{N^n} \sum_{\vec{t} \in [\mathbb{Z}/N\mathbb{Z}]^n} \prod_{i=1}^n |b(t_i)|^r \prod_{j<k} \Big[\frac{N^{n(n-1)/2}}{|t_j - t_k|}\Big]^{r-1}.$$

The **Conjecture** puts us in a position to appeal to a multilinear fractional integral inequality of Christ. Although presented in the euclidean setting in [14] the proof goes over to the mod N setting which we state in the following way: if $g_{i,j}$ are functions on $\mathbb{Z}/N\mathbb{Z}$, then

$$\frac{1}{N^n} \sum_{\vec{t} \in [\mathbb{Z}/N\mathbb{Z}]^n} \prod_{i=1}^n f_i(t_i) \prod_{j<k} g_{j,k}(t_j - t_k) \leq C_s \prod \|f_i\|_s \prod \|g_{j,k}\|_{t,\infty} \tag{48}$$

holds whenever $s^{-1} + t^{-1}(n-1)/2 \leq 1$ and $1 \leq s < n$, where

$$\|g\|_{t,\infty} \ := \ \sup_{\lambda > 0} \lambda \Big[N^{-1} \big| \{t \in \mathbb{Z}/N\mathbb{Z} : g(t) \geq \lambda\} \big| \Big]^{1/t}$$

denotes the weak-type Lorentz norm. The first step in Christ's proof is to observe that a simple interpolation argument gives (48) with the weak-type norms $\|\cdot\|_{t,\infty}$ replaced by the strong-type L^t norms $\|\cdot\|_t$ in the larger L^s range, $1 \le s \le n$.

In fact this is all we need for our purposes since we will apply the multilinear estimates to the functions $g_{j,k}(t) = gcd(t,N)^{r-1}$ with $t = 1/(r-1)$ and we are allowing for an ϵ loss in the estimates:

$$\|gcd(\cdot,N)\|_1 = \frac{1}{N}\sum_{t\in\mathbb{Z}/N\mathbb{Z}} gcd(t,N) = \frac{1}{N}\sum_{d|N} d \sum_{t:gcd(t,N)=d} 1 = \sum_{d|N}\frac{\phi(d)}{d} \le \sum_{d|N} 1.$$

However for the class of integers $N = p^M$ where p is prime, the divisors are totally ordered and one easily verifies the weak-type norms of $gcd(\cdot,p^M)$ are uniformly bounded whereas the L^1 norm is equal to M and so if one seeks stronger Fourier restriction theorems where completely uniform bounds are sought, then the full strength of Christ's multilinear inequality would be needed.

Returning to our situation though, we obtain via the first step of Christ's argument (simple interpolation) the following inequality: if $0 \le \gamma$ then

$$\frac{1}{N^n}\sum_{\vec{t}\in[\mathbb{Z}/N\mathbb{Z}]^n}\prod_{i=1}^n f(t_i)\prod_{j<k} gcd(t_j-t_k,N)^\gamma \;\le\; C_{s,\gamma,\epsilon}N^\epsilon\|f\|_s^n \tag{49}$$

holds if $\gamma \le 2/n$ and $s^{-1} + \gamma(n-1)/2 \le 1$. As in the euclidean setting the restrictions on the exponents s and γ are sharp. In fact the scaling argument we have used previously with $f = \chi_{\mathcal{B}_d}$, d a divisor of N shows necessarily that $s^{-1} + \gamma(n-1)/2 \le 1$. Now plugging the function $f = 1$ into (49) shows that $\gamma \le 2/n$ must hold; in fact for $N = p^L$ where $L > n$ and p is a prime, the left hand side of (49) is made smaller by restricting the summation to

$$\sum_{t_n=0}^{p^L-1}\sum_{u_{n-1}=0}^{L}\sum_{\substack{t_{n-1}=0\\ p^{u_{n-1}}\|t_{n-1}-t_n}}^{p^L-1}\sum_{\substack{u_{n-2}=0\\ u_{n-2}<u_{n-1}}}^{L}\sum_{\substack{t_{n-2}=0\\ p^{u_{n-2}}\|t_{n-2}-t_{n-1}}}^{p^L-1}\cdots\sum_{\substack{u_1=0\\ u_1<u_2}}^{L}\sum_{\substack{t_1=0\\ p^{u_1}\|t_1-t_2}}^{p^L-1}$$

and the summand $\prod_{j<k} gcd(t_j-t_k,p^L)^\gamma$ over this restricted range of summation is equal to

$$\prod_{j=1}^{n-1} gcd(t_j - t_{j+1}, p^L)^{\gamma(n-j)}$$

which readily shows that

$$p^{-Ln}\sum_{\vec{t}\in[\mathbb{Z}/p^L\mathbb{Z}]^n}\prod_{j<k} gcd(t_j-t_k,p^L)^\gamma \;\ge\; 2^{-n^2}p^{(n-1)[\gamma n/2-1]L}$$

and this forces $\gamma \le 2/n$.

Using the **Conjecture** we can now apply (49) to the right hand side of (47) with $\gamma = r-1$ and s satisfying $sr = p'$ (the restriction $\gamma \le 2/n$ needed for the application

of (49) is equivalent to $p' \geq 0.5n(n+2)$ and the condition $s^{-1} + \gamma(n-1)/2 \leq 1$ is equivalent to $p' \geq qn(n+1)/2)$, and this shows that (46) holds with $qn(n+1)/2 \leq p'$ in the range $p' \geq 0.5n(n+2)$ which finishes the proof of Theorem 4.8 modulo the number-theoretic **Conjecture**. □

The conjecture is easy to establish when $n = 2$ (this is Exercise 2.14) and so in this case the necessary conditions $p' \geq 3q$ and $p' \geq 4$ match the sufficient conditions of Proposition 4.8 giving us a complete characterisation when the Fourier restriction estimates in (34) hold for the parabola $S = \{(t, t^2)\}$. This coincides with the euclidean resolution of the restriction conjecture in two dimensions [26] and [64], up to the endpoint $p = 4/3$.

Theorem 4.9. *For the parabola $S = \{(t, t^2) : t \in \mathbb{Z}/N\mathbb{Z}\}$, (34) holds if and only if $p' \geq 3q$ and $p' \geq 4$.*

Appendix: Proof of Proposition 4.7

The problem of finding those exponents r so that (44) holds is closely related to determining the convergence exponent for the singular series $\sigma_{k,m}$ in Tarry's problem; more precisely

$$\sigma_{k,m} \;=\; \sum_{q_1=1}^{\infty}\cdots\sum_{q_k=1}^{\infty}\sum_{a_1=1}^{q_1}{}'\cdots\sum_{a_k=1}^{q_k}{}'\Big|B\Big(\frac{a_k}{q_k},\cdots,\frac{a_1}{q_1}\Big)\Big|^{2m}$$

was shown by ?? to converge if and only if $2m > 0.5k(k+1)+2$. Here $\sum_{a=1}^{q}{}'$ denotes that the sum is computed over those a which are coprime to q and

$$B\Big(\frac{a_k}{q_k},\cdots,\frac{a_1}{q_1}\Big) \;=\; \frac{1}{q_1\cdots q_k}\sum_{x=1}^{q_1\cdots q_k}\exp 2\pi i\Big(\frac{a_k}{q_k}x^k+\cdots+\frac{a_1}{q_1}x\Big).$$

Back to our problem of computing the L^r norm of f above, we note that it suffices to establish (44) for $N=p^L$ where p is prime, uniformly in p and L. Restricting to $N=p^L$, we observe that

$$\|f\|^r_{L^r([\mathbb{Z}/p^L\mathbb{Z}]^n)} \;=\; \sum_{s=0}^{L}\sum_{\substack{a_n=0\\ p\not| gcd(a_n,\ldots,a_1)}}^{p^s-1}\cdots\sum_{a_1=0}^{p^s-1}\big|p^{-s}S(p^s,a_n,\ldots,a_1)\big|^r$$

where $S(p^s,a_n,\ldots,a_1)=\sum_{x=1}^{p^s}e^{2\pi i(a_nx^n+\cdots+a_1x)/p^s}$. The sums $S(p^s,a_n,\ldots a_1)$ play a key role in the analysis of the singular series σ and one finds, using Theorem 2.3 in [1], that if $r\ge 2n$ (which we can safely assume),

$$\begin{aligned}\|f\|^r_{L^r([\mathbb{Z}/p^L\mathbb{Z}]^n)} \;&\le\; 1+n^rp^{-2}+n^{2r+n+1}\sum_{j=1}^{\infty}p^{-j(r-0.5n(n+1)-1)}\\ &+\; n^{2r}\sum_{s>n}s^n\sum_{j\ge(s-1)/n}p^{-j(r-0.5n(n+1)-1)}\end{aligned}$$

if $p>n$ and if $p\le n$,

$$\|f\|^r_{L^r([\mathbb{Z}/p^L\mathbb{Z}]^n)} \;\le\; C_n\big[1+\sum_{s\ge n+2\omega+1}s^np^{-(s-2\omega-1)/n[r-0.5n(n+1)-1]}\big]$$

where $\omega=\lfloor\log n/\log p\rfloor$. From these estimates one readily sees that (44) holds uniformly in p and L if $r>0.5n(n+1)+1$.

In the opposite direction we will obtain a lower bound for the L^r norm of f for any prime $p>n$ and $L=n$; we first observe that $\|f\|^r_{L^r([\mathbb{Z}/p^n\mathbb{Z}]^n)}$

$$\ge\sum_{\substack{a_n=0\\ p\not| a_n}}^{p^n-1}\sum_{\substack{a_{n-1}=0\\ p|\ a_{n-1}}}^{p^n-1}\cdots\sum_{\substack{a_1=0\\ p^{n-1}|\ a_1}}^{p^n-1}\sum_{c=0}^{p-1}\Big|p^{-n}\sum_{x=0}^{p^n-1}e^{2\pi i(a_n(x+c)^n+\cdots+a_1(x+c))/p^n}\Big|^r.$$

This follows from the injectivity of the map

$$\Phi(a_n,\ldots,a_1,c) \;=\; \big(a_n,na_nc+a_{n-1},\ldots,\sum_{j=1}^{n}ja_jc^{j-1}\big)\ \mathrm{mod}\ [\mathbb{Z}/p^n\mathbb{Z}]^n$$

from

$$\big\{(a_n,\dots,a_1,c)\in[\mathbb{Z}/p^n\mathbb{Z}]^n\times\mathbb{Z}/p\mathbb{Z}:p\not|\,a_n,\,p^{n-j}\mid a_j,1\le j\le n-1\big\}\ \text{ to }\ [\mathbb{Z}/p^n\mathbb{Z}]^n$$

which is easily verified by writing the a_j in their p-adic expansion and observing that the coefficients in these expansions are uniquely determined. This reduction is the mod N analogue of restricting the corresponding euclidean oscillatory integral g to a small neighborhood of the 2 dimensional cone where most of the contribution arises. Therefore

$$\|f\|^r_{L^r([\mathbb{Z}/p^n\mathbb{Z}]^n)}\ \ge\ \sum_{\substack{a_n=0\\ p\not|\,a_n}}^{p^n-1}\sum_{b_{n-1}=0}^{p^{n-1}-1}\cdots\sum_{b_1=0}^{p-1}p\,\Big|p^{-n}\sum_{x=0}^{p^n-1}\exp 2\pi i(\frac{a_n}{p^n}x^n+\cdots+\frac{b_1}{p}x)\Big|^r$$

and the inner sum is exactly equal to p^{n-1} which one sees by decomposing the sum by $x=z+p^{n-1}y$ so that

$$\sum_{x=0}^{p^n-1}\exp 2\pi i(\frac{a_n}{p^n}x^n+\cdots+\frac{b_1}{p}x)=\sum_{z=0}^{p^{n-1}-1}\exp 2\pi i(\frac{a_n}{p^n}z^n+\cdots+\frac{b_1}{p}z)\sum_{y=0}^{p-1}e^{2\pi i[na_nz^{n-1}]y/p};$$

the inner sum vanishes unless $p\,|z$ since $p>n$ and $p\not|\,a_n$. So finally we arrive at the estimate

$$\|f\|^r_{L^r([\mathbb{Z}/p^n\mathbb{Z}]^n)}\ \ge\ (1/2)p^{n+(n-1)+\cdots+1}p^{1-r}\ =\ (1/2)p^{0.5n(n+1)+1-r}$$

which shows that (44) fails if $r<0.5n(n+1)+1$.

References

[1] G.I. Arkipov, V.N. Chubarikov, and A.A. Karatsuba, *The theory of multiple trigonometric sums*, (Russian), Nauka, Moscow, 1987.

[2] G.I. Arkipov, V.N. Chubarikov, and A.A. Karatsuba, *Exponent of convergence of the singular integral in the Tarry problem*, (Russian) Dokl. Akad. Nauk SSSR **248** (1979), no.2, 268-272.

[3] G.I. Arkipov and K.I. Oskolkov, *On a special trigonometric series and its applications*, Mat. Sib. **134** (1987), 147-158.

[4] J.G. Bak and A. Seeger, *Extensions of the Stein-Tomas theorem*, Math. Res. Letters, **18** (2011), 767-781.

[5] J. Bourgain, *Besicovitch-type maximal operators and applications to Fourier analysis*, Geom. and Funct. Anal. **22** (1991), 147-187.

[6] J. Bourgain, *An approach to pointwise ergodic theorems* in Geometric aspects of functional analysis, Lecture Notes in Math., 1317, Springer, Berlin, 1988, 204223.

[7] J. Bourgain, *On the maximal ergodic theorem for certain subsets of the integers*, Israel J. Math. **61** (1988), 39-72.

[8] J. Bourgain, *On the pointwise ergodic theorem on L^p for arithmetic sets*, Israel J. Math. **61** (1988), 73-84.

[9] J. Bourgain, *Pointwise ergodic theorems for arithmetic sets; With an appendix by the author, Harry Furstenberg, Yitzhak Katznelson and Donald S. Ornstein*, Inst. Hautes tudes Sci. Publ. Math. No. 69 (1989), 5-45.

[10] Z. Buczolich and D. Mauldin, *Divergent Square Averages*, Annals Math. **171** (2010), 1479-1530.

[11] L. Carleson, *On convergence and growth of partial sums of Fourier series*, Acta Math. **116** (1966), 135-157.

[12] L. Carleson and P. Sjölin, *Oscillatory integrals and a multiplier problem for the disc*, Studia Math. **44** (1972), 287-299.

[13] J.R. Chen, *On Professor Huas estimate of exponential sums*, Sci. Sinica 20 (1977), 711-719.

[14] M. Christ, *On the restriction of the Fourier transform to curves: endpoint results and degenerate cases*, Trans. Amer. Math. Soc. **287** (1985), 223-238.

[15] M. Christ, J. Duoandikoetxea, and J. L. Rubio de Francia, *Maximal operators associated to the Radon transform and the Calderón-Zygmund method of rotations*, Duke Math. J. **53** (1986), 189-209.

[16] R. Cluckers, *Igusa and Denef-Sperber conjectures on nondegenerate p-adic exponential sums*, Duke Math. J. **141** (2008), no. 1, 205-216.

[17] R. Cluckers, *Exponential sums: questions by Denef, Sperber and Igusa* Trans. Amer. Math. Soc. **362** (2010), no. 7, 3745-3756.

[18] A. Cordóba, *The Kakeya maximal function and the spherical summation multipliers*, Amer. J. Math. **99** (1977), 1-22.

[19] R.O. Davies, *Some remarks on the Kakeya problem*, Proc.Camb. Phil. Soc. **69** (1971), 417-421.

[20] J. Denef and S. Sperber, *Exponential sums mod p^n and Newton polydegra*, Bull. Belg. Math. Soc. Simon Stevin **suppl.** (2001), 55-63.

[21] S.W. Drury,*Restriction of Fourier transforms to curves*, Ann. Inst. Fourier, **35** (1985), 117-123.

[22] S.W. Drury, *L^p estimates for the x-ray transform*, Ill. J. Math **27** (1983), 125-129.

[23] Z. Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. **22** (2009), 1093-1097.

[24] J. Ellenberg, R. Oberlin and T. Tao, *The Kakeya set and maximal conjectures for algebraic varieties over finite fields*, to appear in Mathematika.

[25] E.B. Fabes, *Parabolic Partial Differential Equations and Singular Integrals*, Phd Thesis, University of Chicago, 1965.

[26] C. Fefferman, *Inequalities for strongly singular convolutions operators*, Acta Math. **124** (1970), 9-36.

[27] C. Fefferman, *The multiplier problem for the ball*, Ann. Math. **94** (1971), 330-336.

[28] C. Fefferman, *A note on spherical summation mutlipliers*, Israel J. Math. **15** (1973), 44-52.
[29] A. Greenleaf, *Principal curvature in harmonic analysis*, Indiana U. Math. J. **30** (1981), 519-537.
[30] L. Guth and N. Katz, *On the Erdös distinct distance problem in the plane*, preprint.
[31] L. Guth and N. Katz, *Algebraic methods in discrete analogs of the Kakeya problem*, Adv. Math. **225** (2010), no. 5, 28282839.
[32] G.H. Hardy and J.E. Littlewood, *A maximal theorem with functional -theoretic applications*, Acta Math. **54** (1930), 81-116.
[33] L.K. Hua, *On an exponential sum*, J. Chinese Math. Soc. **20** (1940), 301-312..
[34] L.K. Hua, *Additive theory of prime numbers*, Translations of Mathematical Monographs, Amer. Math. Soc., volume 13, 1965.
[35] L.K. Hua, *An introduction to number theory*, Springer-Verlag, 1982.
[36] R.A. Hunt, *On the convergence of Fourier series* in *Orthogonal Expansions and their Continuous Analogues*, Southern Illinois University Press, 1968.
[37] I.A. Ikromov and D. Müller, *On adapted coordinate systems*, Trans. Amer. Math. Soc. **363** (2011), no. 6, 2821-2848.
[38] I.A. Ikromov and D. Müller, *Uniform estimates for the Fourier transform of surface carried measures in* $\mathbb{R}^3$ *and an application to Fourier restriction*, J. Fourier Anal. Appl., **17** (2011), 1292-1332.
[39] A. Ionescu and S. Wainger, L^p *boundedness for discrete singular Radon transforms*, J. Amer. Math. Soc., **19** (2008), 357-383.
[40] A. Ionescu, A. Magyar, E.M. Stein and S. Wainger, *Discrete Radon transforms and applications to ergodic theory*, Acta Math. **198** (2008), 231-298.
[41] H. Kaplan, M. Sharir, E. Shustin, *On lines and joints*, Discrete Comput. Geom. **44** (2010), no. 4, 838843.
[42] J.H. Loxton and R. C. Vaughan, *The estimatimation of complete exponential sums*, Can. Math. Bull., **28** (1985), 440-454.
[43] G. Mockenhaupt, *Salem sets and restriciton properties of fourier transforms*, Geom. Anal. Funct. Anal. **10** (2000), 1579-1587.
[44] G. Mockenhaupt and T. Tao, *Kakeya and restriction phenomena for finite fields*, Duke Math. J. **121** (2004), 35-74.
[45] R. Quilodrán, *The joints problem in* $\mathbb{R}^n$, SIAM J. Discrete Math. **23** (2009/10), no. 4, 22112213.
[46] D.H. Phong and E.M. Stein, *Oscillatory integrals with polynomial phases*, Inventiones, textbf110 (1992), 39-62.
[47] D.H. Phong, E.M. Stein and J.A. Sturm, *On the growth and stability of real analytic functions*, Amer. J. Math **121** (1999), 519-554.
[48] P. Sjölin, *Fourier multipliers and estimates for the Fourier transform of measures carried by smooth curves in* $\mathbb{R}^2$, Studia Math., **51** (1974), 169-182.
[49] E.M Stein, *Harmonic Analysis*, Princeton University Press, 1993.
[50] E.M. Stein and S. Wainger, *The estimation of an integral arising in multiplier transformations*, Studia Math., **35** (1970), 101104.
[51] E.M. Stein and S. Wainger, *Problems in harmonic analysis related to curvature*, Bull. Amer. Soc., **84** (1978), 1239-1295.
[52] E.M. Stein and S. Wainger, *Discrete analogues of singular Radon transforms*, Bull. Amer. Math. Soc., **23** (1990), 537544.
[53] S.B. Steckin, *Estimate on a complete rational trigonometric sum*, Proc. Steklov Inst., **143** (1977), 188-220.
[54] T. Tao, *The Böchner-Riesz conjecture implies the restriction conjection*, Duke Math. J. **96** (1999), 363-376.
[55] P.A. Tomas, *A restriction theorem for the Fourier transform*, Bull. Amer. Math. Soc. **81** (1975), 477-478.
[56] R.C. Vaughan, *The Hardy-Littlewood Method*, Cambridge University Press, 1997.
[57] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA, **34** (1948), 204-207.
[58] T. Wolff, *Recent work connected with the Kakeya problem*, Prospects in mathematics, Princeton, N.J. 1996, 129-162.

[59] T. Wolff, *An improved bound for Kakeya type maximal functions*, Revista Mat. Iberoamericana. **11** (1995). 651674.
[60] J. Wright, *From oscillatory integrals to complete exponential sums*, Math. Res. Letters **18** (2011), no. 2, 231-250.
[61] J. Wright, *On a conjecture of Igusa for binary forms*, preprint.
[62] J.Wright, *The Fourier Restriction Problem in rings of integers*, preprint.
[63] A. Zygmund, *Trigonometric Series*, Cambridge University Press, 1959.
[64] A. Zygmund, *On Fourier coefficients and transforms of functoins of two variables*, Studia Math. **50** (1974), 189-202.

Maxwell Institute of Mathematical Sciences and the School of Mathematics, University of Edinburgh, JCMB, King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, Scotland

E-mail address: J.R.Wright@@ed.ac.uk