Harmonic Analysis on Vector Spaces over Finite Fields

Anthony Carbery

November 29, 2006

1 PRELIMINARIES

1.1 Harmonic analysis on locally compact abelian groups

Let G be a locally compact abelian group. Familiar examples are $\mathbb{R}^n$, $\mathbb{T}^n$ and $\mathbb{Z}^n$.

- A **character** χ is a (continuous) homomorphism $\chi : G \to \mathbb{S}^1 := \{z \in \mathbb{C} : |z| = 1\}$.
- The **dual group** G^* is the class of all characters of G with multiplication $\chi_1\chi_2(g) := \chi_1(g)\chi_2(g)$ and identity $\iota : g \mapsto 1$
- G^* is also an abelian group.

Examples

- (i) $G = \mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z} = \{0, 1, 2, ..., N-1\}$ with addition modulo N. For $0 \leq n \leq N-1$ let $\gamma_n : G \to \mathbb{S}^1$, $\gamma_n(m) = \exp(2\pi imn/N)$. Then $\{\gamma_0, ..., \gamma_{N-1}\}$ is a complete list of the characters so that $\mathbb{Z}_N^*$ is isomorphic to $\mathbb{Z}_N$. An example of a primitive N'th root of unity is $\omega := \exp 2\pi i/N$.
- (ii) $G = \mathbb{T} = \mathbb{R}/\mathbb{Z}$; for $n \in \mathbb{Z}$ let $\gamma_n : G \to \mathbb{S}^1$, $\gamma_n(x) = \exp(2\pi inx)$. Then $G^* = \{\gamma_n : n \in \mathbb{Z}\}$ so that G^* is isomorphic to $\mathbb{Z}$.
- (iii) $G = \mathbb{Z}$; for $\theta \in \mathbb{T}$ let $\gamma_\theta : G \to \mathbb{S}^1$, $\gamma_\theta(n) = \exp(2\pi in\theta)$. Then $G^* = \{\gamma_\theta : \theta \in \mathbb{T}\}$ so that G^* is isomorphic to $\mathbb{T}$.
- (iv) $G = \mathbb{R}$; for $\xi \in \mathbb{R}$ let $\gamma_\xi : G \to \mathbb{S}^1$, $\gamma_\xi(x) = \exp(2\pi ix\xi)$. Then $G^* = \{\gamma_\xi : \xi \in \mathbb{R}\}$ so that G^* is isomorphic to $\mathbb{R}$.
- (v) $(G_1 \times G_2)^*$ is isomorphic to $G_1^* \times G_2^*$.

- **Haar measure on G.** This is the unique (up to scalar multiples) translation-invariant measure on G. For $\mathbb{Z}_N$ and $\mathbb{Z}$ counting measure does the job while for $\mathbb{R}$ and $\mathbb{T}$ Lebesgue measure works.

- **Fourier Transform.** For a (complex-valued) function f defined on G and $\gamma \in G^*$ we define

$$\hat{f}(\gamma) = \int_G f(x)\overline{\gamma(x)}\, dx;$$

  this gives $\hat{f}$ as a function on G^*.

- **Fourier Inversion.** We have the inversion formula

$$f(x) = c\int_{G^*} \hat{f}(\gamma)\gamma(x)\, d\gamma$$

  where c depends on the normalisations given to the Haar measures.

- **Plancherel/Parseval.** For a constant c depending on the normalisations,

$$\int |\hat{f}(\gamma)|^2\, d\gamma = c\int |f(x)|^2\, dx$$

  and, more generally

$$\int \hat{f}\overline{\hat{g}}\, d\gamma = c\int f\overline{g}\, dx.$$

Examples

- (i) $G = \mathbb{R}$. If we use standard Lebesgue measure the constants in inversion and Parseval are both 1.

- (ii) $G = \mathbb{T}$, $G^* = \mathbb{Z}$. With normalised Lebesgue measure on $\mathbb{T}$ and counting measure on $\mathbb{Z}$ the constants in inversion and Parseval are both 1.

- (iii) $G = \mathbb{Z}_N$. With ω a primitive N'th root of unity and standard counting measure on G and G^* we have

$$f(m) = \frac{1}{N}\sum_n \hat{f}(n)\omega^{mn}$$

  and

$$\sum_n |\hat{f}(n)|^2 = N\sum_m |f(m)|^2.$$

For more details on Fourier analysis on LCA groups consult the book *Fourier Analysis on Groups* by Walter Rudin.

1.2 Euclidean harmonic analysis

Euclidean space $\mathbb{R}^n$ possesses a rich geometric structure not shared by general LCA groups. It is this which makes classical harmonic analysis such a rewarding subject to study. For example:

- linear and affine structure: lines, planes, k-planes, passing through the origin or not....
- nonlinear and curved structure: curves, surfaces, k-dimensional surfaces.....
- nice families of automorphisms: invertible linear transformations such as rotations, and, in particular, dilations....
- above all: the vector space structure: one can multiply vectors by scalars to induce linear structure and group actions; one can multiply scalars by scalars to induce curved and nonlinear structure – for example $\mathbb{S}^1 = \{x^2 + y^2 = 1\}$.

1.3 Basics of finite fields

Let $\mathbb{F}$ be a finite field. The most obvious example is $\mathbb{Z}_p$ where p is a prime. The **characteristic** of $\mathbb{F}$ is the unique prime p such that $x+x+x+....+x$ (p times) $= 0$ for all $x \in \mathbb{F}$. Thus $\mathbb{Z}_p$ has characteristic p.

Fact: any finite field of characteristic p is the "splitting field of the polynomial $x^{p^k} - x$ over $\mathbb{Z}_p$" for some $k \in \mathbb{N}$. As a vector space it is of dimension k over the base field $\mathbb{Z}_p$. Thus $|\mathbb{F}| = p^k$ and $\mathbb{F}$ has a subfield isomorphic to $\mathbb{Z}_p$. We shall sometimes denote "the" field with p^k members as $\mathbb{F}_{p^k}$.

The (additive) characters of $\mathbb{F}_p$ have been described above: for any $a \in \mathbb{F}_p$, the map $e_a : x \mapsto \exp(2\pi i a x/p)$ is a character, and the totality of such is found as a ranges over $\mathbb{F}_p$. If $a \neq 0$, we say that e_a is a nonprincipal character, and then $\{e_a(b\ \cdot\ ) : b \in \mathbb{F}_p\}$ is a listing of the characters. If e is a nonprincipal character then

$$\sum_{x \in \mathbb{F}_p} e(x) = 0.$$

The additive characters of $\mathbb{F}_{p^k}$ are a little harder to describe. There is a special map, the "trace map" $T_k : \mathbb{F}_{p^k} \to \mathbb{F}_p$ which is used to list them. (When $k = 1$, T_1 is just the identity; for more details in the general case see the exercises.) For each $a \in \mathbb{F}_{p^k}$, the map $e_a : x \mapsto \exp(2\pi i T_k(ax)/p)$ is a character. Once again if $a \neq 0$, we say that e_a is a nonprincipal character, and then $\{e_a(b\ \cdot\ ) : b \in \mathbb{F}_{p^k}\}$ is a listing of the characters. If e is a nonprincipal character then

$$\sum_{x \in \mathbb{F}_{p^k}} e(x) = 0.$$

1.4 Harmonic analysis on vector spaces over finite fields

Let $\mathbb{F}$ be a finite field of characteristic p. Let e be a fixed nonprincipal character of $\mathbb{F}$. With $e_\tau(t) = e(\tau t)$, $\{e_\tau : \tau \in \mathbb{F}\}$ is the complete list of characters of $\mathbb{F}$ as above.

Now let V be an n-dimensional vector space over $\mathbb{F}$. We can fix a basis and regard it in the usual way as $V = \mathbb{F}^n$, the cartesian product of n copies of $\mathbb{F}$. Then $\mathbb{F}^n$ is a locally compact abelian group and we can describe its Fourier analysis in terms of the nonprincipal character e of $\mathbb{F}$.

Indeed, the characters are e_ξ, indexed by $\xi \in \mathbb{F}^{n*}$ (the dual group) and are given by

$$\begin{aligned} e_\xi(x) &= e(x \cdot \xi) = e(x_1\xi_1 + ... + x_n\xi_n) \\ &= e_{\xi_1}(x_1).....e_{\xi_n}(x_n). \end{aligned}$$

(Note that although we employ the "dot product" notation $x \cdot \xi$, there is no inner product structure here. Also, there is a slight ambuguity in the subscripts applied to e but it will be clear from context whether they are vectors or scalars.)

Note that we have

$$\sum_{x \in \mathbb{F}^n} e(x \cdot \xi) = \begin{cases} |\mathbb{F}|^n & \xi = 0 \\ 0 & \xi \neq 0. \end{cases}$$

For $f : \mathbb{F}^n \to \mathbb{C}$ its Fourier transform $\hat{f} : \mathbb{F}^{n*} \to \mathbb{C}$ is given by

$$\hat{f}(\xi) = \int_{\mathbb{F}^n} f(x)e(-x \cdot \xi)dx \quad = \quad \sum_{x \in \mathbb{F}^n} f(x)e(-x \cdot \xi)$$

Thus integration on $\mathbb{F}^n$ is with respect to un-normalised counting measure.

The Fourier inversion formula is

$$\begin{aligned} f(x) &= \frac{1}{|\mathbb{F}|^n} \sum_{\xi \in \mathbb{F}^{n*}} \hat{f}(\xi)e(x \cdot \xi) \\ &= \int_{\mathbb{F}^{n*}} \hat{f}(\xi)e(x \cdot \xi)d\xi \\ &= (\hat{f})^\vee(x) \ . \end{aligned}$$

Thus integration on $\mathbb{F}^{n*}$ is with respect to normalised counting measure; the total mass of $\mathbb{F}^{n*}$ is 1.

For the record, let us define the inverse Fourier transform of a function g defined on $\mathbb{F}^{n*}$ by

$$g^\vee(x) = \frac{1}{|\mathbb{F}|^n} \sum_{\xi \in \mathbb{F}^{n*}} g(\xi)e(x \cdot \xi).$$

We have chosen these normalisations in part because now Plancherel's theorem comes out with constant 1, so that

$$\int_{\mathbb{F}^{n*}} |\hat{f}(\xi)|^2 \, d\xi = \int_{\mathbb{F}^n} |f(x)|^2 \, dx.$$

The trivial estimate

$$\sup_{\xi} |\hat{f}(\xi)| \leq \int_{\mathbb{F}^n} |f(x)| \, dx$$

also emerges with constant 1.

Convolution on $\mathbb{F}^n$ is defined in the usual way with respect to the standard unnormalised counting measure; on $\mathbb{F}^{n*}$ convolution is with respect to normalised counting measure. See the exercises for some standard facts about convolutions.

If σ is a measure on $\mathbb{F}^{n*}$ defined via its action on a function ϕ by

$$\begin{aligned} \langle \phi, \sigma \rangle &= \int_{\mathbb{F}^{n*}} \phi(\xi) d\sigma(\xi) \\ &= \frac{1}{|\mathbb{F}|^n} \sum_{\xi \in \mathbb{F}^{n*}} \phi(\xi) w(\xi) \end{aligned}$$

we identify σ with the function w. In particular, if $p : \mathbb{F}^k \to \mathbb{F}^{n*}$ parametrises a "k-dimensional surface in $\mathbb{F}^{n*}$", $(1 \leq k < n)$ then the "surface measure" σ_p associated to p is given by

$$\begin{aligned} \langle \phi, \sigma_p \rangle &= \frac{1}{|\mathbb{F}|^k} \sum_{s \in \mathbb{F}^k} \phi(p(s)) \\ &= \frac{1}{|\mathbb{F}|^n} \sum_{\xi \in \mathbb{F}^{n*}} \phi(\xi) \, |\mathbb{F}|^{n-k} \#p^{-1}(\xi). \end{aligned}$$

Thus the measure σ_p is associated with the function $w(\xi) = |\mathbb{F}|^{n-k} \, \#p^{-1}(\xi)$. (Note that the total mass of σ_p is 1.) The inverse Fourier transform of σ_p is given by

$$\sigma_p^\vee(x) = \langle e(\, \cdot \, x), \sigma_p \rangle = |\mathbb{F}|^{-k} \sum_{s \in \mathbb{F}^k} e(x \cdot p(s)),$$

and, more generally, if g is a function defined on the image of p,

$$(g d\sigma_p)^\vee(x) = |\mathbb{F}|^{-k} \sum_{s \in \mathbb{F}^k} e(x \cdot p(s)) g(p(s)).$$

2 SINGULAR AND OSCILLATORY INTEGRALS

2.1 Hilbert transform

Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ is **not** an ordered field. On the other hand, if $\mathrm{char}(\mathbb{F}) > 2$, we can define a notion of positivity.

Definition For $x \in \mathbb{F}$, let

$$\mathrm{sgn}(x) = \begin{cases} 1 & \text{if there is a } y \in \mathbb{F} \setminus \{0\} \text{ with } y^2 = x \\ 0 & x = 0 \\ -1 & \text{otherwise} \end{cases}$$

Those familiar with number theory will recognise this as the Legendre symbol. We say $x > 0$ if $\mathrm{sgn}(x) = 1$, and $x < 0$ if $\mathrm{sgn}(x) = -1$. Note that it is **not** true that $x,\ y\ > 0 \implies x + y > 0$, nor that $x > 0 \implies -x < 0$ when -1 is a square, (which happens when $|\mathbb{F}| - 1$ is a multiple of 4, see the exercises). On the other hand $\{x : x < 0\} = \{\gamma x : x > 0\}$ for all $\gamma < 0$, and $x, y > 0$ implies $xy > 0$. In fact, sgn is multiplicative. i.e. $\mathrm{sgn}(xy) = \mathrm{sgn}(x)\mathrm{sgn}(y)$. Once again, see the exercises.

In analogy with the euclidean case we use the sgn symbol to define the Hilbert transform. For f defined on $\mathbb{F}^*$ and $x \in \mathbb{F}$ we let

$$(Hf)^\vee(x) = \mathrm{sgn}(x) f^\vee(x).$$

Then H is a convolution operator on $\mathbb{F}^*$, $(Hf)(\xi) = K * f(\xi)$, with Hilbert kernel

$$K(\xi) = \mathrm{sgn}^\wedge(\xi) = \int_{\mathbb{F}} \mathrm{sgn}(x) e(-x\xi)\ dx = \sum_{x \in \mathbb{F}} \mathrm{sgn}(x) e(-x\xi).$$

Now for $\xi = 0$, $K(\xi) = 0$ as the sets of positive and negative elements of $\mathbb{F}$ have the same cardinality $\frac{|\mathbb{F}|-1}{2}$, (exercise). If $\xi \neq 0$,

$$K(\xi) = \sum_x \mathrm{sgn}(x\xi^{-1}) e(-x)$$

$$= \sum_x \mathrm{sgn}(x)\ \mathrm{sgn}(\xi)^{-1} e(-x) = \mathrm{sgn}(\xi) K(1).$$

In particular,

$$K(\xi) = \begin{cases} K(1) & \xi > 0 \\ 0 & \xi = 0 \\ -K(1) & \xi < 0 \end{cases}$$

and

$$K(-\xi) = K(\xi)\ \mathrm{sgn}(-1).$$

So if we understand $K(1)$ we understand the Hilbert kernel. Most important for us is its size, $|K(1)|$, which we can determine using the fact that sgn is an eigenfunction of the Fourier transform operator with eigenvalue $K(1)$ and by using the fact that doing two succesive inverse Fourier transforms gets you back to where you started (modulo a normalisation).

Indeed, $\mathrm{sgn}^\wedge = K(1)\ \mathrm{sgn}$, so $\mathrm{sgn}^{\wedge\wedge} = K(1)\ \mathrm{sgn}^\wedge = K(1)^2\ \mathrm{sgn}$. But for any function h, $h^{\wedge\wedge}(\cdot) = |\mathbb{F}|\ h(-\cdot)$ (exercise). Hence

$$\mathrm{sgn}^{\wedge\wedge} = |\mathbb{F}|\ \mathrm{sgn}(-\cdot) = |\mathbb{F}|\ \mathrm{sgn}(-1)\ \mathrm{sgn}(\cdot)$$

Combining the identities we see

$$K(1)^2 = |\mathbb{F}|\ \ \mathrm{sgn}(-1)$$

from which we deduce that

$$|K(\xi)| = \begin{cases} |\mathbb{F}|^{1/2} & \xi \neq 0 \\ 0 & \xi = 0. \end{cases}$$

Moreover, when $|\mathbb{F}| - 1$ is a multiple of 4, $K(\xi)$ is real, and otherwise it is imaginary.

For the behaviour of H as a convolution operator and remarks on other singular integrals, see the exercises.

2.2 Gauss sums

We have seen above that

$$K(-1) = \sum_{x\in\mathbb{F}} \mathrm{sgn}(x)e(x) = \sum_{x>0} e(x) - \sum_{x<0} e(x).$$

On the other hand,

$$0 = \sum_{x>0} e(x) + \sum_{x<0} e(x) + 1$$

as e is a nonprincipal character. Adding, we see

$$\sum_{x\in\mathbb{F}} e(x^2) = 2\sum_{y>0} e(y)\ \ + 1 = K(-1) = K(1)\ \mathrm{sgn}(-1)$$

Now $K(1)^2 = |\mathbb{F}|\ \mathrm{sgn}(-1)$ and so

$$|\sum_{x\in\mathbb{F}} e(x^2)| = |\mathbb{F}|^{1/2}.$$

In fact, we have:

Proposition 1 *If $a \neq 0$ and char $\mathbb{F} > 2$, then*

$$|\sum_{x\in\mathbb{F}} e(ax^2 + bx + c)| = |\mathbb{F}|^{1/2}.$$

Proof We can complete the square to reduce to the case $b = 0$. Multiplicativity of characters further reduces to the case $c = 0$. If $a > 0$ the result is clear because sgn is multiplicative. Finally if $a < 0$, $\{ax^2 : x \in \mathbb{F}\}$ consists of 0 and all the negatives counted twice, while $\{x^2 : x \in \mathbb{F}\}$ consists of 0 and all the positives counted twice. Thus

$$\sum_{x\in\mathbb{F}} e(ax^2) + \sum_{x\in\mathbb{F}} e(x^2) = 2\sum_{y\in\mathbb{F}} e(y) = 0.$$

Hence $|\sum_{x\in\mathbb{F}} e(ax^2)| = 0$ also. □

Remark More can be said about the precise argument of the complex numbers $K(1)$ and $\sum e(x^2)$. For example if $\mathbb{F}$ is $\mathbb{Z}_p$, then $\sum e(x^2) = p^{1/2}\ i^{(\frac{p-1}{2})^2}$, and $K(1) = p^{1/2}\ (-i)^{(\frac{p-1}{2})^2}$. This amounts essentially to Gauss's law of quadratic reciprocity; we will not need this result in what follows.

2.3 Exponential sums and decay estimates – van der Corput's lemma in finite fields

Let $\mathbb{F}$ be a finite field of characteristic greater than 2. Let $p(t) = at^2 + bt + c$ be a polynomial of degree at most 2 over $\mathbb{F}$. Then we have just seen above that

$$|\sum_{t\in\mathbb{F}} e(p(t))| = |\mathbb{F}|^{1/2}$$

if $a \neq 0$; if $a = 0$ then the sum is zero except when b is also zero – in which case there is no cancellation and the sum has magnitude $|\mathbb{F}|$.

What about polynomials of degree higher than 2?

It turns out that there is a remarkable theorem of A. Weil which has everything we need, and which serves as an analogue of van der Corput's lemma in the finite field setting. For convenience we state Weil's theorem in a slightly more general form due to Carlitz; we use the notation $(\cdot, \cdot)$ to denote greatest common divisor.

Theorem 2 *Let $\mathbb{F}$ be a finite field and let $p : \mathbb{F} \to \mathbb{F}$ a polynomial of degree d. If $(char\ \mathbb{F}\ , d) = 1$ or, more generally, if p is* **not** *of the form $g^{char\ \mathbb{F}} - g + \alpha$, then*

$$|\sum_{s\in\mathbb{F}} e(p(s))| \leq (d-1)\,|\mathbb{F}|^{\frac{1}{2}}\,.$$

Remarks. 1. Clearly the nontrivial cases are $d \geq 3$.

2. If p is if the form $g^{\text{char }\mathbb{F}} - g + \alpha$, then $|\sum_{s\in\mathbb{F}} e(p(s))| = |\mathbb{F}|$.

3. The theorem is sharp.

4. Polynomials of degree d behave just like quadratics in this setting.

As an immediate Corollary we have:

Corollary 3 *Let $p : \mathbb{F} \to \mathbb{F}^{n*}$ be a polynomial curve of degree $d \geq 2$ such that im p lies in no proper affine subspace of $\mathbb{F}^{n*}$. If char $\mathbb{F} > d$, and $x \neq 0$, then*

$$|\sum_{t\in\mathbb{F}} e(x \cdot p(t))| \leq (d-1)|\mathbb{F}|^{1/2},$$

so that

$$\left|\sigma_p^\vee(x)\right| \leq (d-1)\,|\mathbb{F}|^{-\frac{1}{2}}\,.$$

Proof For $x \neq 0$ apply Weil's theorem to the (non-constant!) polynomial $s \mapsto x \cdot p(s)$. □

Remark Note that the condition that im p lie in no proper affine subspace of $\mathbb{F}^{n*}$ is necessary for there to be a nontrivial estimate for $\sigma_p^\vee$ when $x \neq 0$.

This is our desired decay estimate for the (inverse) Fourier transform of a surface-carried measure when the surface is a curve. So far so good. Is there a corresponding estimate for higher-dimensional surfaces? The picture here is less clear. In the first place one would want a higher-dimensional version of Weil's theorem. The good news is that such a theorem has been proved, by Deligne:

Theorem 4 *Let $\mathbb{F}$ be a finite field, $p : \mathbb{F}^k \to \mathbb{F}$ a polynomial of degree d. Suppose that $(char\ \mathbb{F}\ , d) = 1$ and that if $p^{(d)}$ is the part of p which is homogeneous of degree d, then $\{p^{(d)} = 0\}$ defines a nonsingular hypersurface in $P_{\mathbb{F}}^{k-1}$. Then*

$$|\sum_{t\in\mathbb{F}^k} e(p(t))| \leq (d-1)^k\,|\mathbb{F}|^{k/2}\ \ .$$

The bad news is that it is not so straightforward in practice to verify the hypotheses of Deligne's theorem; in particular the terms "nonsingular hypersurface" and "$P_{\mathbb{F}}^{k-1}$" require an algebraic-geometric interpretation. Examples show that without these hypotheses the estimate may fail; see the exercises. However the case $d = 2$ can be analysed explicitly using Gauss sums. Indeed, if char $\mathbb{F} > 2$ and $p : \mathbb{F}^k \to \mathbb{F}$ is a polynomial of degree 2, then we can complete the square (via an invertible linear transformation of $\mathbb{F}^k$) to reduce to the case $\tilde{p}(t) = t_1^2 + ... + t_r^2 + \gamma t_{r+1}^2 + ... + \gamma t_s^2 + \sum_{j=1}^k \alpha_j t_j + \beta$ for some $1 \leq r \leq s \leq k$ (where γ is some fixed non-zero non-square). Now $\tilde{p}$ splits into a sum of quadratics in each variable separately, and so $\sum_t e(\tilde{p}(t))$ factorises as the product of exponential sums of quadratic functions of each of the t_j's, which we have dealt with above. If any $\alpha_j \neq 0$ for $j = s+1, s+2, ..., k$, we will get zero in the corresponding factor. If not, we get s factors of modulus $(d-1)|\mathbb{F}|^{1/2}$ and $(k-s)$ factors of modulus $|\mathbb{F}|$. Thus if the quadratic p has full rank, we get the optimal estimate $(d-1)^k|\mathbb{F}|^{k/2}$ for the exponential sum.

In order to deal with the issue of decay estimates for inverse Fourier transorms of measures we shall adopt a more naive approach, and content ourselves with constructing, for each k and n with $1 \leq k < n$, polynomial surfaces $p : \mathbb{F}^k \to \mathbb{F}^{n*}$ of degree d (depending on k and n) which enjoy the optimal estimates

$$|\sum_{t \in \mathbb{F}^k} e(x \cdot p(t))| \leq (d-1)^k |\mathbb{F}|^{k/2}$$

and thus

$$|\sigma_p^\vee(x)| \leq (d-1)^k |\mathbb{F}|^{-k/2}.$$

whenever $x \neq 0$ and char $\mathbb{F} > d$. (To see that these are indeed optimal see the exercises.)

Proposition 5 *Let $1 \leq k < n$ and let $d = n - k + 1$. If char $\mathbb{F} > d$, define the polynomial surfaces $p : \mathbb{F}^k \to \mathbb{F}^{n*}$ of degree d by*

$$p(t) = (t_1, t_2, ..., t_k, t_1^2 + t_2^2 + ... + t_k^2, t_1^3 + ... + t_k^3, ..., t_1^{n-k+1} + ... + t_k^{n-k+1}).$$

Then for $x \neq 0$,

$$|\sum_{t \in \mathbb{F}^k} e(x \cdot p(t))| \leq (d-1)^k |\mathbb{F}|^{k/2}$$

and

$$|\sigma_p^\vee(x)| \leq (d-1)^k |\mathbb{F}|^{-k/2}.$$

Proof We note that with $p_j(t_j) = (0, ..0, t_j, 0.., 0, t_j^2, t_j^3, ..., t_j^{n-k+1})$ (with the t_j in the j-th place) we have $p(t) = \sum_{j=1}^k p_j(t_j)$ and

$$x \cdot p(t) = \sum_{j=1}^k x \cdot p_j(t_j)$$

so that

$$\sum_{t\in\mathbb{F}^k} e(x\cdot p(t)) = \prod_{j=1}^{k}\sum_{t_j\in\mathbb{F}} e(x\cdot p_j(t_j)).$$

Now

$$x\cdot p_j(t_j) = x_j t_j + \sum_{m=k+1}^{n} x_m t_j^{m-k+1}.$$

So if $x\neq 0$ but $x_{k+1},.....,x_n$ are all zero, at least one other $x_j\neq 0$, and so we get 0 from the j'th term in the product. If some $x_{k+1},....,x_n\neq 0$ we can apply Weil's theorem to each factor to conclude that

$$|\sum_{t\in\mathbb{F}^k} e(x\cdot p(t))| \leq (n-k)^k|\mathbb{F}|^{k/2}$$

if char $\mathbb{F} > n-k+1$. □

Remark When $k=n-1$ we can choose the final component q of p to be any quadratic form of full rank. Indeed, we may assume that q has already been diagonalised (after completing the square) and then $x\cdot p(t) = x_1t_1+x_2t_2+...+x_{n-1}t_{n-1}+x_nq(t)$. If $x\neq 0$ but $x_n=0$, some other $x_j\neq 0$, in which case we get 0. If $x_n\neq 0$ then $x\cdot p(t)$ is a quadratic of full rank and so we may apply the remarks following the statement of Deligne's theorem to obtain the desired estimate.

3 AVERAGES AND MAXIMAL AVERAGES OVER POLYNOMIAL SURFACES

3.1 Background

Let $p:\mathbb{F}^k\to\mathbb{F}^{n*}$ be a polynomial surface with $1\leq k<n$. Let σ_p be the surface measure associated to p as previously defined. In this section we will first study the averaging operators

$$f\mapsto f*\sigma_p;$$

for ξ fixed $f*\sigma_p(\xi)$ represents the average value of f over the translate of im p by ξ.

Before proceeding further we need to review basic convolution inequalities – Young's inequalities – and to do this we need to discuss the somewhat nonsensical notion of L^p-spaces over vector spaces over finite fields. This notion is nonsensical since all the L^p spaces are the same and consist of the class of all complex valued functions defined on $\mathbb{F}^{n*}$. However what is relevant is the L^p

norm on this class and we shall, in accordance with our previous conventions, define it with respect to normalised counting measure:

Definition For $1 \leq p \leq \infty$ and $f : \mathbb{F}^{n*} \to \mathbb{C}$ the L^p norm of f is defined as

$$\|f\|_p = \left(\int_{\mathbb{F}^{n*}} |f(\xi)|^p \, d\xi \right)^{1/p} = |\mathbb{F}|^{-n/p} \left(\sum_{\xi \in \mathbb{F}^n} |f(\xi)|^p \right)^{1/p}.$$

Young's inequalities can now be stated as follows. Let $1 \leq p, q, r \leq \infty$ with $1/r = 1/p + 1/q - 1$. Then

$$\|f * g\|_r \leq \|f\|_p \|g\|_q.$$

It is not difficult to give an elementary proof of this inequality. But it can also be proved using interpolation.

Indeed, notice that the range of allowed exponents $(1/p, 1/q, 1/r)$ is precisely the convex hull of the three points $(1, 1, 1)$, $(1, 0, 0)$ and $(0, 1, 0)$. The first of these is trivial and can be regarded as an L^1 to L^1 estimate for a convolution operator with kernel in L^1. By duality the same operator is bounded on L^∞, giving the point $(1, 0, 0)$. Symmetry gives the point $(0, 1, 0)$. Interpolation now gives the remaining cases, see the exercises. (In the euclidean case there is a lot more subltely going on, as away from the boundary the best constant in Young's inequality is *strictly* less than 1. This is a deep result of Beckner. But that would be the subject of a different course of lectures.....)

The results in this section are due to Stones, Wright and the lecturer.

3.2 Averages

Let $p : \mathbb{F}^k \to \mathbb{F}^{n*}$ be a polynomial of degree d. Let $\sigma = \sigma_p$ be the surface measure associated to p as above. While there is no question about the *boundedness* of the convolution operators $f \mapsto f * \sigma$ between various L^p and L^q spaces over $\mathbb{F}^n$, what is of interest is when the bounds can be taken to be independent of $|\mathbb{F}|$. That is, we wish to determine for which $1 \leq p, q \leq \infty$ we have

$$\|f * \sigma\|_{L^q(\mathbb{F}^{n*})} \leq C \, \|f\|_{L^p(\mathbb{F}^{n*})} \tag{1}$$

with the constant C depending possibly on k, n, d and $\max_{\xi \in \mathbb{F}^{n*}} \#p^{-1}(\xi)$, but *not* upon $|\mathbb{F}|$ in any explicit way.

Why do we wish to do this?

We are very much motivated by the corresponding euclidean problems. In that setting, σ is a finite measure associated to a compact piece of k-dimensional

surface in $\mathbb{R}^n$; convolution with σ is then a local operation and can be thought of taking place on chunks of $\mathbb{R}^n$ (cubes, balls etc.) of finite volume. So we may as well be working with measures σ of unit mass supported in the unit cube in $\mathbb{R}^n$ of mass one, and functions similarly supported. Hence the normalisations we employ in our study. Furthermore, one can imagine Riemann sums for the euclidean convolutions and L^p-norm evaluations as approximating the genuine article; one of course wants estimates independent of the fineness of the mesh in the Riemann sums. Back in our current case the fineness of the mesh is measured by the quantity $|\mathbb{F}|^{-1}$, and so we are seeking estimates which do not explicitly depend on $|\mathbb{F}|$.

Since σ has total mass 1, (1) always holds if $p = q$ by Young's inequality, with $C = 1$. Since $\mathbb{F}^{n*}$ has total mass 1 it continues to hold with $C = 1$ when $1 \leq q \leq p \leq \infty$. So the main interest is what happens when $1 \leq p < q \leq \infty$.

Let us first consider what conditions on p and q our requirement for constants independent of $|\mathbb{F}|$ imposes. Let

$$\begin{aligned} f(\xi) &= \begin{cases} 1 & \xi = 0 \\ 0 & \xi \neq 0 \end{cases} \\ &= |\mathbb{F}|^{-n} \delta_0(\xi) \end{aligned}$$

(where δ_0 is understood to have mass 1). Then

$$\|f\|_{L^p(\mathbb{F}^{n*})} = |\mathbb{F}|^{-n/p}.$$

On the other hand,

$$f * \sigma(\xi) = |\mathbb{F}|^{-n} \sigma(\xi) = |\mathbb{F}|^{-k} \#p^{-1}(\xi),$$

so that

$$\begin{aligned} \|f * \sigma\|_{L^q(\mathbb{F}^{n*})} &= |\mathbb{F}|^{-k} \left(\frac{1}{|\mathbb{F}|^n} \sum_{\xi} \#p^{-1}(\xi)^q \right)^{\frac{1}{q}} \\ &\geq |\mathbb{F}|^{-k} |\mathbb{F}|^{\frac{k-n}{q}} \quad (\text{as } q \geq 1). \end{aligned}$$

So in order for (1) to hold we must have

$$|\mathbb{F}|^{-k+\frac{k-n}{q}} \leq C |\mathbb{F}|^{-\frac{n}{p}} .$$

Thus (1) can hold with C independent of $|\mathbb{F}|$ only when

$$\frac{n}{p} \leq k + \frac{n-k}{q} .$$

By duality we obtain that if (1) holds with C independent of $|\mathbb{F}|$, then $\left(\frac{1}{p}, \frac{1}{q}\right)$ must lie in the convex hull of the points $(0,1),(1,1),(0,0)$ and $\left(\frac{n}{2n-k}, \frac{n-k}{2n-k}\right)$. The last of these points is where the interest lies.

In the case that the image of p contains an s-dimensional affine subspace of $\mathbb{F}^{n*}$, it makes sense to test (1) on the characteristic function of an s-plane in $\mathbb{F}^{n*}$, yielding the necessary condition $\frac{1}{q} \geq \frac{1}{p} - \frac{k-s}{n-s}$. This provides a further necessary condition in addition to the one above when $s > k/2$.

In summary:

Proposition 6 *Suppose that (1) holds with a constant independent of $|\mathbb{F}|$. Then $(1/p, 1/q)$ lies in the convex hull of the points $(0,1),(1,1),(0,0)$ and $\left(\frac{n}{2n-k}, \frac{n-k}{2n-k}\right)$. Furthermore if the image of p contains an s-dimensional subspace with $s > k/2$, we must also have $\frac{1}{q} \geq \frac{1}{p} - \frac{k-s}{n-s}$.*

Our first main result shows that the necessary conditions of the last proposition are in many cases sufficient:

Theorem 7 *Let $1 \leq k < n$ and $d \geq 2$ Let $p : \mathbb{F}^k \to \mathbb{F}^{n*}$ be a polynomial of degree d such that the optimal decay estimate*

$$|\sigma^\vee(x)| \leq (d-1)^k |\mathbb{F}|^{-k/2}$$

holds whenever $x \neq 0$. Then

$$\|f * \sigma\|_{L^{\frac{2n-k}{n-k}}(\mathbb{F}^{n*})} \leq A \|f\|_{L^{\frac{2n-k}{n}}(\mathbb{F}^{n*})}$$

when $A = 1 + (d-1)^{k\frac{2n-2k}{2n-k}} \left[\max_\xi \#p^{-1}(\xi)\right]^{\frac{k}{2n-k}}$.

Remarks 1. Interpolation with trivial results gives the full range of exponents for which convolution with σ_p is bounded with a constant independent of $|\mathbb{F}|$.

2. The second term appearing in A is merely a convex combination of $(d-1)^k$ and $\max \#p^{-1}(\xi)$, and thus A can be taken to be independent of n as well as $|\mathbb{F}|$.

Proof of Theorem 7 We ("Littlewood-Paley") decompose $\sigma^\vee$ as

$$\sigma^\vee = \sigma^\vee \chi_{x \neq 0} + \delta_0$$

(recalling that $\sigma^\vee(0) = \text{mass of } \sigma = 1$).

Correspondingly we have

$$\sigma = \hat{K} + 1$$

where $K(x) = \sigma^\vee(x)\chi_{x\neq 0}$ satisfies $\|K\|_\infty \leq (d-1)^k |\mathbb{F}|^{-k/2}$ by assumption.

Now the theorem follows from the following three estimates:

- $\|f * 1\|_q \leq \|f\|_p \quad (1 \leq p, q \leq \infty)$
- $\|f * \hat{K}\|_\infty \leq \|\hat{K}\|_\infty \|f\|_1 = \|\sigma - 1\|_\infty \|f\|_1 \leq |\mathbb{F}|^{n-k} \max_\xi \#p^{-1}(\xi) \|f\|_1$
- $\|f * \hat{K}\|_2 = \|f^\vee K\|_2 \leq \|K\|_\infty \|f^\vee\|_2 \leq (d-1)^k |\mathbb{F}|^{-k/2} \|f\|_2$.

□

If the optimal decay estimate holds, then im p is precluded from containing any affine subspace of dimension greater than $k/2$. Whether or not the optimal decay estimate is compatible with subspaces of dimension *less than or equal to* $k/2$ is explored in the exercises. Partial results on the bounds of convolution with σ_p when im p does contain an affine subspace of dimension greater than $k/2$ are also explored in the exercises.

What we have proved here is a finite field analogue of Littman's theorem, a version of which is as follows. Suppose we have a positive finite measure σ on $\mathbb{R}^n$ which, for each $\lambda > 1$, can be decomposed as

$$\sigma = \sigma^\lambda + \sigma_\lambda$$

where $\|\sigma^\lambda\|_\infty \leq C\lambda$ and $\|\hat{\sigma_\lambda}\|_\infty \leq C\lambda^{-(n-1)/2}$. Then convolution with σ is of restricted-weak type $(((n+1)/n), n+1)$. It is a good exercise to prove this result. Littman worked in the context of σ being the normalised surface measure on the unit sphere $\mathbb{S}^{n-1}$ and in fact proved the strong-type $(((n+1)/n), n+1)$ result. The decomposition of σ comes about by breaking up the Fourier transform of σ into two pieces, one supported near the origin, the other supported far from the origin. Notice that this is exactly what we have done above.

3.3 Maximal averages

In this subsection we first fix an indexing set $\mathcal{A}$ and, for each $\alpha \in \mathcal{A}$, we have a polynomial $p_\alpha : \mathbb{F}^k \to \mathbb{F}^{n*}$ of degree at most d. (The maximal degree d is common for all the p_α.) We consider the maximal averaging operator

$$f \mapsto \sup_{\alpha\in\mathcal{A}} |f * \sigma_{p_\alpha}| .$$

Once again we wish to examine the mapping properties of this operator with respect to the L^p norms. That is, we wish to determine those exponents p for which we have

$$\left\| \sup_{\alpha \in \mathcal{A}} |f * \sigma_\alpha| \right\|_p \leq C \|f\|_p \tag{2}$$

with C depending as before on k, n, d and $\max_{\alpha \in \mathcal{A}} \max_{\xi} \#p_\alpha^{-1}(\xi)$, as well as on the sizes of the indexing set $\mathcal{A}$ and of $\bigcup_{\alpha \in \mathcal{A}} \text{im } p_\alpha$.

Let us first examine what restrictions on the exponent p this imposes.

Let us suppose that $\#\left(\bigcup_{\alpha \in \mathcal{A}} \text{im } p_\alpha \right) \simeq |\mathbb{F}|^{k+r}$. Take $f = |\mathbb{F}|^{-n} \delta_0$ as in the previous subsection above. As before, $\|f\|_p = |\mathbb{F}|^{-n/p}$, while $f * \sigma_\alpha(\xi) \geq |\mathbb{F}|^{-k}$ on im p_α, so that $\sup_\alpha |f * \sigma_\alpha(\xi)| \geq |\mathbb{F}|^{-k}$ on $\bigcup_{\alpha \in \mathcal{A}} \text{im } p_\alpha$. Thus

$$\begin{aligned} \left\| \sup_\alpha |f * \sigma_\alpha| \right\|_p &\geq |\mathbb{F}|^{-k} \left(\# \left(\bigcup_{\alpha \in \mathcal{A}} \text{im } p_\alpha \right) |\mathbb{F}|^{-n} \right)^{\frac{1}{p}} \\ &= |\mathbb{F}|^{-n/p} |\mathbb{F}|^{-k + \frac{k+r}{p}} \quad . \end{aligned}$$

Consequently if (2) is to hold with C independent of $|\mathbb{F}|$ we must have $p \geq \frac{k+r}{k}$. Obviously when $p = \infty$ (2) holds, so the main interest is what happens at $p = \frac{k+r}{k}$.

One may think of the index 'r' as measuring the "number of parameters" in $\mathcal{A}$: if $\#\text{im } p_\alpha \approx |\mathbb{F}|^k$ for each α and the distinct im p_α are essentially disjoint, then $\# \bigcup_{\alpha \in \mathcal{A}} \text{im } p_\alpha \approx |\mathbb{F}|^k \#\mathcal{A}$. Our assumption then corresponds to $\#\mathcal{A} \approx |\mathbb{F}|^r$.

Theorem 8 *Let $1 \leq k < n$, $d \geq 2$ and char $\mathbb{F} > d$. Let $\mathcal{A}$ be an indexing set satisfying $\#\mathcal{A} \leq D |\mathbb{F}|^r$. For $\alpha \in \mathcal{A}$ suppose $p_\alpha : \mathbb{F}^k \to \mathbb{F}^{n*}$ is a polynomial of degree at most d such that the optimal decay estimate*

$$|\sigma_\alpha(x)^\vee| \leq (d-1)^{k/2} |\mathbb{F}|^{-k/2}$$

holds when $x \neq 0$. Suppose also that $\# \bigcup_{\alpha \in \mathcal{A}} im\ p_\alpha \leq D |\mathbb{F}|^{k+\tilde{r}}$ for some $\tilde{r} \leq r$. If $r \leq k$, then

$$\left\| \sup_{\alpha \in \mathcal{A}} |f * \sigma_\alpha| \right\|_{L^{\frac{2\tilde{r}-r+k}{\tilde{r}-r+k}}(\mathbb{F}^{n*})} \leq B \|f\|_{L^{\frac{2\tilde{r}-r+k}{\tilde{r}-r+k}}(\mathbb{F}^{n*})}$$

where B depends only upon d, k, D and $\max_\alpha \max_\xi \#p_\alpha^{-1}(\xi)$.

Remarks 1. This is the sharp estimate when $\tilde{r} = r$ as indicated above.

2. Once again, the constant B depends neither on $|\mathbb{F}|$ nor the dimension n, and in this case the L^p exponent is also independent of n.

3. If p is a fixed polynomial whose σ enjoys the optimal decay estimate, and if p_α is an affine image of p, i.e. $p_\alpha = A_\alpha p + b_\alpha$ where A_α is an invertible $n \times n$ matrix over $\mathbb{F}$ and $b_\alpha \in \mathbb{F}^{n*}$, then σ_α enjoys the same estimate.

4. One cannot entirely dispense with the hypothesis $r \leq k$. Stones has observed that if we take the polynomial p to be arbitrary and p_α to be suitable translates of p, then having the constant independent of $|\mathbb{F}|$ forces $r \leq k$. Indeed, for $s \in \mathbb{F}^{r*}$ we define $p_s = p + (s, 0)$ and $E = \bigcup_{s' \in \mathbb{F}^{(n-r)*}} \{(0, s') - \text{im } p\}$. Then $|E| \leq |\mathbb{F}|^{n-r+k}$, and so $\|\chi_E\|_p \leq |\mathbb{F}|^{\frac{k-r}{p}}$. On the other hand, if for $y \in \mathbb{F}^{n*}$ we set $y = (s, s') \in \mathbb{F}^{r*} \times \mathbb{F}^{(n-r)*}$, then $\chi_E * \sigma_s(y) = 1$. (We have $\chi_E * \sigma_s(y) \leq 1$ always, and with equality iff $\chi_E = 1$ on $y - \text{im } p_s = (s, s') - (\text{im } p + (s, 0)) = (0, s') - \text{im } p$. But E is the union of these, so that $\sup_s \chi_E * \sigma_s(y) = 1$ for all $y \in \mathbb{F}^n$, and so $\| \sup_s \chi_E * \sigma_s \|_p = 1$. Hence $r \leq k$. It is to be noted that a similar phenomenon occurs in the euclidean case when we use translations. We do not know whether it is necessary that $r \leq k$ when we use only *dilations* of a given fixed p.

Proof of Theorem 8 As in Theorem 6 we write $\sigma^\vee = \sigma^\vee \chi_{x \neq 0} + \delta_0$ and $\sigma_\alpha = \hat{K}_\alpha + 1$. Once again we have $\|f * 1\|_p \leq \|f\|_p$ for all p, so it is enough to show

$$\left\| \sup_{\alpha \in \mathcal{A}} \left| f * \hat{K}_\alpha \right| \right\|_{\frac{2\tilde{r}-r+k}{\tilde{r}-r+k}} \leq B \|f\|_{\frac{2\tilde{r}-r+k}{\tilde{r}-r+k}} .$$

When $r \leq k$, $1 \leq \frac{2\tilde{r}-r+k}{\tilde{r}-r+k} \leq 2$, and we obtain the desired estimate by interpolation between $p = 1$ and $p = 2$.

- $p = 1$ estimate:

  For each α and ξ,

$$\begin{aligned} \left| \hat{K}_\alpha(\xi) \right| &= |\sigma_\alpha(\xi) - 1| \\ &\leq |\mathbb{F}|^{n-k} \, \# p_\alpha^{-1}(\xi) + 1 \\ &\leq M \, |\mathbb{F}|^{n-k} \, \chi_{\bigcup\limits_\alpha \text{im } p_\alpha}(\xi) + 1 \end{aligned}$$

  where $M = \sup\limits_\alpha \sup\limits_\xi \# p_\alpha^{-1}(\xi)$, so that

$$\int\limits_{\mathbb{F}^{n*}} \sup_\alpha \left| \hat{K}_\alpha(\xi) \right| d\xi \leq 1 + M \, |\mathbb{F}|^{-k} \, \# \bigcup_\alpha \text{im } p_\alpha \, .$$

Thus,

$$\begin{aligned}\left\|\sup_\alpha \left|f * \hat{K}_\alpha\right|\right\|_1 &\leq \left\||f| * \sup_\alpha \left|\hat{K}_\alpha\right|\right\|_1 \\ &\leq \left[1 + M\,|\mathbb{F}|^{-k} \,\#\left(\bigcup_{\alpha\in\mathcal{A}} \text{im } p_\alpha\right)\right] \|f\|_1 \\ &\leq \left[1 + MD\,|\mathbb{F}|^{\tilde{r}}\right] \|f\|_1 .\end{aligned}$$

- $p = 2$ estimate:
  We have

$$\begin{aligned}\left\|\sup_\alpha \left|f * \hat{K}_\alpha\right|\right\|_2 &\leq \left\|\left(\sum_\alpha \left|f * \hat{K}_\alpha\right|^2\right)^{\frac{1}{2}}\right\|_2 \\ &= \left(\sum_\alpha \left\|f * \hat{K}_\alpha\right\|_2^2\right)^{\frac{1}{2}} \\ &\leq \left(\sum_\alpha \left\|\hat{f}\right\|_2^2 \|K_\alpha\|_\infty^2\right)^{\frac{1}{2}} \\ &\leq (d-1)^k\,|\mathbb{F}|^{-k/2}\,(\#\mathcal{A})^{\frac{1}{2}}\,\|f\|_2 \\ &\leq (d-1)^k D^{\frac{1}{2}}\,|\mathbb{F}|^{\frac{r-k}{2}}\,\|f\|_2 \ .\end{aligned}$$

  Interpolation now shows that the bound on $L^{\frac{2\tilde{r}-r+k}{\tilde{r}-r+k}}$ is essentially a convex combination of MD and $(d-1)^k D^{\frac{1}{2}}$. □

Remark If, in the notation of Theorem 8, $\#\mathcal{A} \approx |\mathbb{F}|^r$ and $\#\bigcup \text{im } p_\alpha \approx |\mathbb{F}|^{k+\tilde{r}}$ with $\tilde{r} < r \leq k$, the L^p exponent $(2\tilde{r} - r + k)/(\tilde{r} - r + k)$ is worse than the expected $(\tilde{r} + k)/k$. This is likely due to the inefficiency of estimating an ℓ^∞ norm by an ℓ^2 one in the $p = 2$ estimate.

What we have done here is prove a finite field version of the Stein–Bourgain spherical maximal theorem, (if one consders the case $k = n - 1$ and $r = 1$). The spherical maximal theorem concerns behaviour of the maximal operator $f \mapsto \sup_t |f * \sigma_t|$ where σ is the normalised surface measure on $\mathbb{S}^{n-1}$ and the subscript t denotes dilation. Stein proved that this operator is bounded on L^p if and only if $p > n/(n-1)$ when $n \geq 3$, and Bourgain extended this to $n = 2$ and also obtained the sharp restricted weak-type $n/(n-1)$ estimate when $n \geq 3$. Interestingly the restricted weak-type fails when $n = 2$ as Tao has shown (unpublished) using the Kakeya set. In the finite field case we get the strong-type estimate in all dimensions very easily. The argument we have given is based upon Bourgain's restricted weak-type argument.

The argument of Stones given in Remark 4 above does not preclude some version of Theorem 8 holding when $r > k$ if for example we take *dilations* rather than translations of a given p for our family $\{p_\alpha\}$. This variant would seem to present a true analogue of the situation Bourgain handled in the two-dimensional euclidean case, where the difficulty was the fact that there was no directly available L^2 estimate.

4 RESTRICTION

Most of the material in this section is taken from the paper "Restriction and Kakeya phenomena for finite fields" by Mockenhoupt and Tao, which appeared in Duke Math J. a year or two back. The notes here will therefore be a little more concise in places.

4.1 Preliminaries

With $p : \mathbb{F}^k \to \mathbb{F}^{n*}$ a polynomial of degree d and $\sigma_p = \sigma$ as before, we wish to examine the restriction operator

$$f \mapsto \hat{f}|_{\text{im } p}$$

with respect to the norms $L^{q'}(\mathbb{F}^n)$ and $L^{p'}(d\sigma)$. That is, we want to study when we have

$$\|\hat{f}(p(\cdot))\|_{L^{p'}(\mathbb{F}^{k*})} \leq C\|f\|_{L^{q'}(\mathbb{F}^n)}$$

with C independent of $|\mathbb{F}|$. By duality, this is equivalent to the "extension" estimate

$$\| \ (gd\sigma)^\vee \|_{L^q(\mathbb{F}^n)} \leq C\|g\|_{L^p(d\sigma)}.$$

4.2 Necessary conditions

- Testing the extension estimate on $g = 1$ and using $\|\sigma^\vee\|_q \geq C|\mathbb{F}|^{n/q-k/2}$ (see the exercises) gives
$$\frac{1}{q} \leq \frac{k}{2n} \ .$$
- Testing the extension estimate on the characteristic function of a singleton gives
$$\frac{1}{q} \leq \frac{k}{np'} \ .$$

- If im p contains an affine subspace V of dimension s, testing on $g = \chi_{\{t\,:\,p(t)\in V\}}$ gives
$$\frac{1}{q} \leq \frac{k-s}{n-s}\frac{1}{p'}.$$
This is more restrictive as s increases. See the exercises.

The first two tests lead to the conjecture that if im p contains no nontrivial affine subspaces, then
$$\|(g\ d\sigma)^\vee\|_{L^{2n/k}} \leq C\|g\|_{L^2}.$$

4.3 Positive results: even exponents q – multiplying out à la Fefferman-Zygmund

Lemma 9 *Let $p : \mathbb{F}^k \to \mathbb{F}^{n*}$ be a polynomial. Let $q = 2r$ be an even integer. Suppose that*
$$|\{(t_1, ..., t_r) \in (\mathbb{F}^k)^r : \xi = p(t_1) + ... + p(t_r)\}| \leq A$$
for all $\xi \in \mathbb{F}^{n*}$. Then
$$\|(gd\sigma)^\vee\|_{L^q(\mathbb{F}^n)} \leq A^{1/q}|\mathbb{F}|^{(n/q-k/2)}\|g\|_2.$$

Proof

$$\|(gd\sigma)^\vee\|_q^q = \|(gd\sigma)^\vee\|_{2r}^{2r} = \int_{\mathbb{F}^n} |(gd\sigma)^\vee.....(gd\sigma)^\vee|^2 = \int_{\mathbb{F}^{n*}} |\ gd\sigma * ..... * gd\sigma|^2$$

where there are r factors of $gd\sigma$ in each of the previous two lines.

Now

$$gd\sigma * ..... * gd\sigma(\xi) = \frac{|\mathbb{F}|^{n-k}}{|\mathbb{F}|^{k(r-1)}} \sum_{t_1,...,t_r;\ p(t_1)+.....+p(t_r)=\xi} g(p(t_1))).....g(p(t_r))$$

$$\leq A^{1/2}\frac{|\mathbb{F}|^{n-k}}{|\mathbb{F}|^{k(r-1)}}(\sum_{t_1,...,t_r;\ p(t_1)+.....+p(t_r)=\xi} |g(p(t_1))).....g(p(t_r))|^2)^{1/2}.$$

(In fact, we have

$$\int_{\mathbb{F}^{n*}} |\ gd\sigma * ..... * gd\sigma|^2$$
$$= \frac{|\mathbb{F}|^{n-k}}{|\mathbb{F}|^{k(r-1)}} \sum_{t_1,...,t_r;s_1,...,s_r:\ p(t_1)+.....+p(t_r)=p(s_1)+.....+p(s_r)} g(p(t_1))).....g(p(t_r))\overline{g(p(s_1))).....g(p(s_r))},$$

a formula which we shall make use of in Theorem 12 below.)

Therefore

$$\int_{\mathbb{F}^{n*}} |\, gd\sigma * ..... * gd\sigma|^2 \leq A \frac{|\mathbb{F}|^{2(n-k)}}{|\mathbb{F}|^{2k(r-1)+n}} \sum_{\xi \in \mathbb{F}^{n*}} \sum_{t_1,...,t_r;\ p(t_1)+.....+p(t_r)=\xi} |g(p(t_1)).....g(p(t_r))|^2$$

$$= A|\mathbb{F}|^{n-kr}(\frac{1}{|\mathbb{F}|^k} \sum_{t \in \mathbb{F}^k} |g(p(t))|^2)^r = A|\mathbb{F}|^{n-kr}\|g\|_2^{2r}.$$

Hence

$$\|(gd\sigma)^\vee\|_{L^q(\mathbb{F}^n)} \leq A^{1/q}|\mathbb{F}|^{(n/q-k/2)}\|g\|_2.$$

□

This argument is originally due to Zygmund (after Fefferman). Note that a certain flexibility in the condition of the lemma is possible, i.e. if the cardinality condition is violated for a sufficiently small number of ξ, the estimate will still hold.

Corollary 10 *Suppose char $\mathbb{F} > n$. Consider the curve $p(t) = (t, t^2, ..., t^n)$. Then*

$$\|(gd\sigma_p)^\vee\|_{2n} \leq C\|g\|_2$$

where C is absolute, depending only upon n.

Proof For all ξ the set $\{(t_1, ..., t_n) : t_1^j + ... + t_n^j = \xi_j,\ 1 \leq j \leq n\}$ has cardinality at most $n!$, by Newton's identities. So we get the conclusion of the lemma with $C = (n!)^{1/2n} \sim (n/e)^{1/2}$. □

Corollary 11 *Suppose $n \geq 3$ and that char $\mathbb{F} > 2$. Let $p(t_1, ..., t_{n-1}) = (t_1, ..., t_{n-1}, t_1^2 + t_2^2 + ... + t_{n-1}^2)$. Then*

$$\|(gd\sigma_p)^\vee\|_{L^4(\mathbb{F}^n)} \leq 2^{1/4}\|g\|_2.$$

Proof Consider for $\xi = (\xi', \xi_n) \in \mathbb{F}^n$ the equations

$$s + t = \xi'$$

$$s \cdot s + t \cdot t = \xi_n.$$

For ξ fixed this system has at most $A = 2|\mathbb{F}|^{n-2}$ solutions $(s, t) \in \mathbb{F}^{n-1} \times \mathbb{F}^{n-1}$. Indeed, for each *fixed* $s_1, ..., s_{n-2}$ (which determine $t_1, ..., t_{n-2}$), the remaining coordinate s_{n-1} satisfies the quadratic

$$s \cdot s + (\xi' - s) \cdot (\xi' - s) = \xi_n$$

and thus there are at most two such s_{n-1}, (each determining a corresponding t_{n-1}).

So with $k = n-1,\ r = 2$ and $q = 4$ the power of $|\mathbb{F}|$ in $A^{1/q}$ is $(n-2)/4$ which cancels with $(n/q - k/2) = (n/4 - (n-1)/2) = -(n-2)/4$. □

The same result holds with the same proof if p is the graph of any quadratic form of full rank $n-1$. It also holds irrespective of whether the quadratic surface contains higher-dimensional subspaces – which is quite possible. This is therefore the best result we can expect without further qualification on the geometric nature of the paraboloid.

Specialising now to $n = 3$ and the case where -1 is not a square, the paraboloid contains no lines and so the conjecture states that there should be an L^2 – L^3 estimate for the extension operator. The significance of the next result is that the point $(5/8, 1/4)$ lies on the line joining $(1/2, 1/3)$ to $(1, 0)$.

Theorem 12 *Suppose that char $\mathbb{F} > 2$, that -1 is not a square and that p is the graph of the paraboloid. Then*

$$\|(gd\sigma_p)^\vee\|_{L^4(\mathbb{F}^3)} \leq C\|g\|_{L^{8/5}(\mathbb{F}^{2*})}$$

where C is absolute. (In fact, we can take $C = 2^{1/4}$.)

This result was proved up to logarithmic factors of $|\mathbb{F}|$ by Mockenhoupt and Tao. In the present formulation the result and argument are new and arose in conversation between Bennett, Garrigos, Wright and the lecturer. Mockenhoupt and Tao use an incidence geometry approach and galilean invariance properties, while our approach is somewhat more direct. (The underlying ideas are nevertheless of course the same.) In the light of recent sharp results of Tao on the euclidean restriction phenomenon it would be of interest to further improve this result towards $(1/2, 1/3)$. For a nonoptimal improvement see the next subsection.

Proof We multiply out the L^4 norm as in the remark during the proof of Lemma 9. Using injectivity of p we identify $g(p(s))$ as $g(s)$. In what follows, summation is over all available variables subject to the specific constraints listed. We may assume that g takes nonnegative values. Let

$$Q(g_1, g_2, g_3, g_4) = \sum_{p(s_1)+p(s_2)=p(s_3)+p(s_4)} g_1(s_1)g_2(s_2)g_3(s_3)g_4(s_4).$$

After clearing factors of $|\mathbb{F}|$ we see that we have to show

$$Q(g, g, g, g) \leq C\|g\|_{8/5}^4$$

where, for the rest of this proof, all ℓ^q norms are taken with *counting measure*, (in violation of our general convention).

By symmetry and multilinear interpolation it suffices to show

$$Q(g_1, g_2, g_3, g_4) \leq C\|g_1\|_2\|g_2\|_2\|g_3\|_2\|g_4\|_1, \tag{1}$$

at least when $g_1 = \chi_{E_1}$ and $g_2 = \chi_{E_2}$.

Now

$$\begin{aligned} Q(g_1, g_2, g_3, g_4) \leq \|g_4\|_1 \sup_{s_4} & \sum_{p(s_1)+p(s_2)=p(s_3)+p(s_4)} g_1(s_1)g_2(s_2)g_3(s_3) \\ \leq & \|g_4\|_1\|g_3\|_2 \sup_{s_4} \left(\sum_{s_3} \left(\sum_{p(s_1)+p(s_2)=p(s_3)+p(s_4)} g_1(s_1)g_2(s_2) \right)^2 \right)^{1/2} \\ = \|g_4\|_1\|g_3\|_2 \sup_{s_4} & \left(\sum_{p(s_1)+p(s_2)=p(s_3)+p(s_4)=p(s_1')+p(s_2')} g_1(s_1)g_2(s_2)g_1(s_1')g_2(s_2') \right)^{1/2} \\ = & \|g_4\|_1\|g_3\|_2 \sup_{s_4} \tilde{Q}_{p(s_4)}(g_1, g_2, g_1, g_2)^{1/2} \end{aligned}$$

where

$$\tilde{Q}_\lambda(g_1, g_2, h_1, h_2) = \sum_{p(s_1)+p(s_2)=p(s_1')+p(s_2')\in \mathrm{im}p+\lambda} g_1(s_1)g_2(s_2)h_1(s_1')h_2(s_2').$$

So we shall be finished if we can show that, uniformly in s_4, with $\lambda = p(s_4)$, we have

$$\tilde{Q}_\lambda(\chi_{E_1}, \chi_{E_2}, \chi_{E_1}, \chi_{E_2}) \leq C|E_1||E_2|. \tag{2}$$

Fix μ and let $\lambda = (\mu, \mu^2)$.

We first consider terms where one of the variables, say s_2', equals μ. The contribution of such terms to (2) is dominated by

$$\begin{aligned} \chi_{E_2}(\mu) & \sum_{p(s_1)+p(s_2)=p(s_1')+p(\mu)} \chi_{E_1}(s_1)\chi_{E_2}(s_2)\chi_{E_1}(s_1') \\ \leq & \sum_{p(s_1')-p(s_2)\in\ \mathrm{im}p-p(\mu)} \chi_{E_2}(s_2)\chi_{E_1}(s_1') \\ \leq & |E_2||E_1| \end{aligned}$$

which is fine. Similarly for s_1, s_2 or $s_1' = \mu$.

We next consider terms where $s_1' = s_2$. The contribution of such terms to (2) is dominated by

$$\begin{aligned}
&\sum_{p(s_1)+p(s_2)=p(s_2)+p(s_2')\in \mathrm{im}p+p(\mu)} \chi_{E_1}(s_1)\chi_{E_2}(s_2)\chi_{E_1}(s_2)\chi_{E_2}(s_2') \\
&= \sum_{p(s_1)+p(s_2)\in \mathrm{im}p+p(\mu)} \chi_{E_1}(s_1)\chi_{E_2}(s_2)\chi_{E_1}(s_2)\chi_{E_2}(s_1) \\
&= \sum_{p(s_1)+p(s_2)\in \mathrm{im}p+p(\mu)} \chi_{E_1\cap E_2}(s_1)\chi_{E_1\cap E_2}(s_2) \\
&\le |E_1\cap E_2|^2 \\
&\le |E_1||E_2|,
\end{aligned}$$

where in the first equality we have used injectivity of p. These terms are also fine.

Finally we consider those remaining terms where $s_1' \neq s_2$ and $s_1', s_2 \neq \mu$. The contribution of such terms to (2) is dominated by

$$\begin{aligned}
&\|\chi_{E_1}(s_1)\|_\infty \|\chi_{E_1}(s_1')\|_1 \sup_{s_1'\neq\mu} \sum_{p(s_1)+p(s_2)=p(s_1')+p(s_2')\in \mathrm{im}p+p(\mu);\ s_2\neq s_1',\mu} \chi_{E_2}(s_2)\chi_{E_2}(s_2') \\
&= |E_1| \sup_{s_1'\neq\mu} \sum_{p(s_1')+p(s_2')\in\ (\mathrm{im}p+p(\mu))\cap(\mathrm{im}p+p(s_2));\ s_2\neq s_1',\mu} \chi_{E_2}(s_2)\chi_{E_2}(s_2').
\end{aligned}$$

In the last sum here, the variables of summation are s_2 and s_2'; the parameters s_1' and $\mu \neq s_1'$ are fixed.

Now $p(s_1')+p(s_2') \in \mathrm{im}\ p+p(\mu)$ if and only if $(s_1'+s_2'-\mu)^2 = s_1'^2+s_2'^2-\mu^2$, if and only if $\mu^2-(s_1'+s_2')\cdot\mu+s_1'\cdot s_2' = 0$, if and only if $(\mu-s_1')\cdot(\mu-s_2') = 0$. Similarly $p(s_1')+p(s_2') \in \mathrm{im}\ p+p(s_2)$ if and only if $(s_2-s_1')\cdot(s_2-s_2') = 0$.

Temporarily fix s_2 also, with s_2, s_1' and μ all distinct, and consider the two simultaneous equations for $s_2' \in \mathbb{F}^2$:

$$\begin{aligned}
(\mu-s_1')\cdot(\mu-s_2') &= 0 \\
(s_2-s_1')\cdot(s_2-s_2') &= 0
\end{aligned} \tag{3}$$

If $\mu - s_1'$ is not parallel to $s_2 - s_1'$, there will be a unique solution $s_2' = \gamma(s_2)$ (with γ depending on s_1' and μ), and then

$$\begin{aligned}
&\sum_{p(s_1')+p(s_2')\in(\mathrm{im}p+p(\mu))\cap(\mathrm{im}p+p(s_2));\ s_2\neq s_1',\mu;\ \mu-s_1' \text{ not parallel to } s_2-s_1'} \chi_{E_2}(s_2)\chi_{E_2}(s_2') \\
&\qquad \le \sum_{s_2} \chi_{E_2}(s_2)\chi_{E_2}(\gamma(s_2)) \\
&\qquad \le |E_2| \times 1 \\
&\qquad = |E_2|,
\end{aligned}$$

and so the contribution of such terms to (2) is once again less than or equal to $|E_1||E_2|$.

We still have to consider the possibility that $\mu - s_1'$ *is* parallel to $s_2 - s_1'$ for certain s_2 with $s_2 \neq s_1', \mu$ (where of course $s_1' \neq \mu$). Fortunately this case does not occur under the hypotheses that -1 is not a square, as we shall now see. Indeed, if $(s_2 - s_1') = \beta(\mu - s_1')$ for some nonzero β, the equations (3) for s_2' are consistent if and only if $\beta(\beta-1)(\mu - s_1') \cdot (\mu - s_1') = 0$. Since -1 is not a square and $\mu \neq s_1'$ we cannot have $(\mu - s_1') \cdot (\mu - s_1') = 0$, β is non-zero by hypothesis, and β cannot be 1 either as this would entail $s_2 = \mu$. Thus when -1 is not a square the contribution to the sum from these terms is empty.

Collecting terms, we see that (2) holds with $C = 4$, and that the Theorem holds with $C = 2^{1/4}$.

□

Remarks. 1. Had we tried to estimate $\tilde{Q}_\lambda(\chi_{E_1}, \chi_{E_2}, \chi_{E_1'}, \chi_{E_2'})$, we would have obtained an estimate dominated by something like $|E_1'||E_2| + |E_2 \cap E_1'||E_1 \cap E_2'| + |E_1||E_2'| \leq C(|E_1| + |E_1'|)(|E_2| + |E_2'|)$.

2. As a consequece of (1) we have the following Radon transform like estimate

$$\sum_{s,t \in \mathbb{F}^2,\ s \cdot t = 0} f(s)g(s+t)h(t) \leq C\|f\|_{\ell^{2,1}}\|g\|_{\ell^{2,1}}\|h\|_{\ell^{2,1}}$$

under the hypothesis that -1 is not a square and char $\mathbb{F} > 2$.

3. If we had not assumed that -1 is not a square in the above proof, we would have had to have considered the contribution occuring when $\mu - s_1'$ *is* parallel to $s_2 - s_1'$ for certain s_2 with $s_2 \neq s_1', \mu$ (and $s_1' \neq \mu$). Indeed, suppose $\alpha^2 = -1$. Then $(\mu - s_1') \cdot (\mu - s_1') = 0$ whenever $\mu - s_1'$ lies on the line through the origin in $\mathbb{F}^2$ with slope $\pm\alpha$, that is whenever $\mu - s_1' = (t, \pm\alpha t)$ for some $t \in \mathbb{F} \setminus \{0\}$. When μ and s_1' are related in this way, there will be for each fixed s_2 a whole line of solutions s_2' to equations (3). This forces an extra factor of $|\mathbb{F}|$ in the estimate for (2), which translates as an extra factor of $|\mathbb{F}|^{1/8}$ in the statement of Theorem 12. But $|\mathbb{F}|^{1/8}\|g\|_{L^{8/5}(\mathbb{F}^{2*})} \leq \|g\|_{L^2(\mathbb{F}^{2*})}$ so that we recover Corollary 11 in the case $n = 3$.

4.4 Positive results: the Stein-Tomas-Bourgain method

Suppose that σ is a positive measure on $\mathbb{F}^{n*}$ such that

$$|\sigma^\vee(x)| \leq B \text{ for } x \neq 0.$$

Suppose that for some $(1/p_0\ , 1/q_0)$ satisfying $1/q_0 \leq \max\{1/p_0\ , 1/2\}$ and A we have

$$\|\hat{f}\|_{L^{p_0'}(d\sigma)} \leq A\ \|f\|_{L^{q_0'}(\mathbb{F}^n)}.$$

We would like to mimic the Stein-Tomas method from euclidean harmonic analysis to obtain an estimate such as

$$\|\hat{f}\|_{L^{p'}(d\sigma)} \leq C\{1 + B^{\frac{1}{2}(1-\frac{q_0}{q})} A^{\frac{q_0}{q}}\} \|f\|_{L^{q'}(\mathbb{F}^n)}$$

for $(1/p\ , 1/q)$ on the line joining $(1/p_0\ , 1/q_0)$ to $(1/2\ , 0)$.

We would like to do this as in the previous section by writing $\sigma^\vee$ as

$$\sigma^\vee = \sigma^\vee \chi_{x \neq 0} + \delta_0 = \sigma_1^\vee + \sigma_2^\vee$$

and obtaining an easy estimate for the contribution coming from σ_2 and a more subtle one for the σ_1 part.

Now $\sigma_2 = 1$ on $\mathbb{F}^{n*}$ and it thus satisfies $\|(gd\sigma_2)^\vee\|_q \leq \|g\|_{L^p(d\sigma_2)}$ if $1/q \leq 1/2$ and $1/q \leq 1/p$. (When $p = 1$ and $q = \infty$ this is trivial and when $p = q = 2$ it is Plancherel. Now interpolate and use Hölder's inequality on the unit measure space $\mathbb{F}^{n*}$.) By duality we have $\|\hat{f}\|_{L^{p'}(d\sigma_2)} \leq \|f\|_{q'}$ for the same p, q.

So it remains to get the desired estimate for σ_1.

By the estimate for σ_2 in the previous paragraph, the second hypothesis applies also to σ_1 with at worst a change in A, that is

$$\|\hat{f}\|_{L^{p_0'}(d\sigma_1)} \leq (A^{p_0'} + 1)^{1/p_0'} \ \|f\|_{L^{q_0'}(\mathbb{F}^n)} \leq (A+1)\ \|f\|_{L^{q_0'}(\mathbb{F}^n)}.$$

(This is assuming $1/q_0 \leq \max\{1/p_0\ , 1/2\}$.)

On the other hand, with $\tilde{f}(\cdot) = f(-\cdot)$,

$$\int |\hat{f}|^2 d\sigma_1 = \int \tilde{f}\ f * \sigma_1^\vee$$

$$\leq \|f\|_1^2 \|\sigma_1^\vee\|_\infty \leq B\|f\|_{L^1(\mathbb{F}^n)}^2.$$

Hence

$$\|\hat{f}\|_{L^2(d\sigma_1)} \leq B^{1/2} \|f\|_{L^1(\mathbb{F}^n)}.$$

Interpolating between these two estimates gives that for $(1/p\ , 1/q)$ on the line joining $(1/p_0\ , 1/q_0)$ to $(1/2\ , 0)$,

$$\|\hat{f}\|_{L^{p'}(d\sigma)} \leq \{1 + B^{\frac{1}{2}(1-\frac{q_0}{q})} (A+1)^{\frac{q_0}{q}}\} \|f\|_{L^{q'}(\mathbb{F}^n)}.$$

In fact the argument we have just given is erroneous. (Why?) We therefore adopt a slightly different approach.

Theorem 13 *Suppose that σ is a positive measure on $\mathbb{F}^{n*}$ such that*

$$|\sigma^\vee(x)| \le B \text{ for } x \ne 0.$$

Suppose that for some $(1/p_0\ , 1/q_0)$ and A we have

$$\|\hat{f}\|_{L^{p_0'}(d\sigma)} \le A\ \|f\|_{L^{q_0'}(\mathbb{F}^n)}.$$

Then for $(1/p\ , 1/q)$ satisfying $p' \le \min\{p_0',\ 2\}$ and $q' \le 2$ we have

$$\|\hat{f}\|_{L^{p'}(d\sigma)} \le \{A^{\frac{q_0}{q}}(2B^{1/2})^{1-\frac{q_0}{q}} + 2\}\|f\|_{L^{q'}(\mathbb{F}^n)}.$$

Proof Let $f = \chi_E$ with E a subset of $\mathbb{F}^n$. As we have seen above, there are two estimates available for $\|\hat{\chi_E}\|_{L^{p'}(d\sigma)}$. The first, by hypothesis, is

$$\|\hat{\chi_E}\|_{L^{p'}(d\sigma)} \le \|\hat{\chi_E}\|_{L^{p_0'}(d\sigma)} \le A|E|^{1/q_0'}$$

since $p' \le p_0'$. For the second, since $p' \le 2$,

$$\|\hat{\chi_E}\|^2_{L^{p'}(d\sigma)} \le \|\hat{\chi_E}\|^2_{L^2(d\sigma)} = \int \tilde{f}\ f * \sigma^\vee = \int \tilde{f}\ f * \sigma_1^\vee + \int \tilde{f}\ f * \sigma_2^\vee$$

and, as σ_2 is identically one, this is less than or equal to

$$\le B\|f\|_1^2 + \|f\|_2^2 = B|E|^2 + |E|.$$

Now

$$\min\{A|E|^{1/q_0'}, (B|E|^2 + |E|)^{1/2}\} \le \min\{A|E|^{1/q_0'}, B^{1/2}|E| + |E|^{1/2}\}$$

$$\le \min\{A|E|^{1/q_0'}, B^{1/2}|E| + |E|^{1/q'}\}$$

since $q' \le 2$.

When $|E|^{1/q'} \ge B^{1/2}|E|$ this last expression is at most $2|E|^{1/q'}$ while if $|E|^{1/q'} \le B^{1/2}|E|$ the last expression is at most $(A|E|^{1/q_0'})^\theta(2B^{1/2}|E|)^{1-\theta}$ for any $\theta \in [0,1]$.

So for any such $\theta \in [0,1]$,

$$\|\hat{\chi_E}\|_{L^{p'}(d\sigma)} \le (A|E|^{1/q_0'})^\theta(2B^{1/2}|E|)^{1-\theta} + 2|E|^{1/q'}$$

and if we choose θ to satisfy $1/q' = \theta/q_0' + (1-\theta)/1$ we obtain

$$\|\hat{\chi_E}\|_{L^{p'}(d\sigma)} \le \{A^\theta(2B^{1/2})^{1-\theta} + 2\}|E|^{1/q'}$$

$$= \{A^{q_0/q}(2B^{1/2})^{1-q_0/q} + 2\}|E|^{1/q'}.$$

This establishes the theorem when f is the characteristic function of a set. The general case can be proved by a variant of the argument given (see the paper of Mockenhoupt and Tao) or by an interpolation argument. In fact in the paper of Mockenhoupt and Tao the theorem is proved with constant $\{2A^{\frac{q_0}{q}}B^{1/2(1-\frac{q_0}{q})}+1\}$ for general f.

□

Thus we can effectively "interpolate" not along the line joining $(1/p_0, 1/q_0)$ to $(1/2, 0)$ but only along the vertical line joining $(\min\{1/p_0,\ 1/2\}\ , 1/q_0)$ to $(\min\{1/p_0,\ 1/2\}\ , 0)$.

Corollary 14 *If σ is the measure associated to a k-dimensional surface such that $|\sigma^\vee(x)| \leq C|\mathbb{F}|^{-k/2}$ for $x \neq 0$, then*

$$\|(gd\sigma)^\vee\|_{\frac{2(2n-k)}{k}} \leq C\|g\|_2.$$

Proof If $p_0' = 2 = q_0'$, then we have the second hypothesis of the theorem with $A = |\mathbb{F}|^{\frac{n-k}{2}}$, by identifying the measure σ with the function $|\mathbb{F}|^{n-k}\#p^{-1}(\cdot)$ and applying Plancherel. The first hypothesis holds with $B = |\mathbb{F}|^{-k/2}$. For the appropriate choice of $q = 2(2n-k)/k$ the powers of $|\mathbb{F}|$ coming from A and B in the conclusion cancel. □

When $k = n-1$ we recover the Stein–Tomas index $\frac{2(n+1)}{(n-1)}$. This is the index q in the sharp L^2 extension theorem $\|(gd\sigma)^\vee\|_q \leq C\|g\|_2$ in the euclidean setting where σ is the normalised surface measure on the unit sphere $\mathbb{S}^{n-1}$. This theorem is due to Stein after an earlier non sharp version by Tomas. For the proof of the Stein–Tomas theorem see the exercises. Another application of this method is:

Theorem 15 *Suppose that char $\mathbb{F} > 2$, that -1 is not a square and that p is the graph of the paraboloid. Then*

$$\|(gd\sigma_p)^\vee\|_{L^{\frac{18}{5}}(\mathbb{F}^3)} \leq C\|g\|_{L^2(\mathbb{F}^{2*})}$$

where C is absolute.

Once again, this theorem was proved up to logarithmic terms in $|\mathbb{F}|$ by Mockenhoupt and Tao. The improvement here stems from the corresponding improvement in Theorem 12 above. This time conformal invariance rather than galilean invariance plays a role, and parts of the argument are the finite field analogue of the lecturer's paper "Restriction implies Bochner–Riesz for paraboloids".

Proof Note that $1/4 < 5/18 < 5/16 < 1/3$. By Theorem 13 it suffices to show

$$\|(gd\sigma_p)^\vee\|_{L^{\frac{16}{5}}(\mathbb{F}^3)} \leq C|\mathbb{F}|^{1/16}\|g\|_{L^2(\mathbb{F}^{2*})},$$

(which, since $5/16 < 1/3$, is not optimal if we believe the restriction conjecture to be true). It is therefore enough to show

$$| \langle f, f * d\sigma^\vee \rangle | \leq C|\mathbb{F}|^{1/8} \|f\|^2_{L^{16/11}(\mathbb{F}^3)},$$

(which Vega has suggested might be obtained directly, perhaps thinking about Gutiérrez's work), or

$$| \langle f, h * d\sigma^\vee \rangle | \leq C|\mathbb{F}|^{1/8} \|f\|_{L^{16/11}} \|h\|_{L^{16/11}}$$

which in turn follows from

$$| \langle f, h * d\sigma^\vee \rangle | \leq C|\mathbb{F}|^{1/8} \|f\|_{L^{4/3}} \|h\|_{L^{8/5}}$$

by symmetry and interpolation since $(11/16, 11/16)$ is the midpoint of the line joining $(3/4, 5/8)$ and $(5/8, 3/4)$. By duality it is therefore enough to show

$$\|h * d\sigma^\vee\|_4 \leq C|\mathbb{F}|^{1/8} \|h\|_{L^{8/5}},$$

which corresponds to a convolution estimate for Bochner–Riesz means. (Note that we are working with counting measure on $\mathbb{F}^3$ on both sides of this inequality.) Indeed, with the usual splitting $\sigma^\vee = \sigma^\vee \chi_{x \neq 0} + \delta_0 \ = K(x) + \delta_0$, the contribution of δ_0 is trivial as $\|h * \delta_0\|_4 = \|h\|_4 \leq \|h\|_{8/5} \leq |\mathbb{F}|^{1/8} \|h\|_{L^{8/5}}$ since $4 > 8/5$. So we have to show

$$\|h * K\|_4 \leq C|\mathbb{F}|^{1/8} \|h\|_{L^{8/5}}.$$

By translation invariance, slicing and the triangle inequality (cf. the Carleson–Sjölin/Hörmander reduction of an $\mathbb{R}^n - \mathbb{R}^n$ multiplier estimate to a stronger $\mathbb{R}^{n-1} - \mathbb{R}^n$ oscillatory integral estimate), this is an immediate consequence of

$$\|h * K\|_4 \leq C|\mathbb{F}|^{-1/4} \|h\|_{L^{8/5}}$$

for h supported on the plane $x_3 = 0$, which we now establish.

A calculation (completing the square) shows that when $x_3 \neq 0$,

$$K(x) = |\mathbb{F}|^{-2} S(x_3)^2 e(-\tfrac{x' \cdot x'}{4x_3})$$

where S is a gauss sum with absolute value $|\mathbb{F}|^{1/2}$. (This is analogous to the euclidean formula for the Fourier transform of the parabolic Bochner–Riesz multiplier as $|x_n|^{-(n-1)/2} \exp\{2\pi i |x'|^2 / x_n\}$.) So for h supported on the plane $x_3 = 0$,

$$|h * K(x)| = |\mathbb{F}| \ |(h d\sigma)^\vee(\tfrac{x'}{2x_3}, \tfrac{-1}{4x_3})|.$$

Performing the obvious change of variables, and using Theorem 12,

$$\|h * K\|_4 = |\mathbb{F}| \ \|(h d\sigma)^\vee\|_4 \quad \leq |\mathbb{F}| \ \|h\|_{L^{8/5}(\mathbb{F}^{2*})} \leq |\mathbb{F}|^{-1/4} \ \|h\|_{L^{8/5}(\mathbb{F}^3)}$$

which finishes the proof. □

Effectively, this argument shows how to take an $L^p - L^q$ extension estimate with some power $|\mathbb{F}|^a$, convert it to an $L^p - L^q$ estimate for convolution with the Bochner–Riesz kernel with some other power $|\mathbb{F}|^{a'}$, thence, via symmetry and interpolation, to an $L^r - L^2$ restriction estimate – or an $L^2 - L^{r'}$ extension estimate with $1/r = 1/2(1/p + 1/q')$ with power $|\mathbb{F}|^{a'/2}$, and finally, using Theorem 13, into an $L^2 - L^s$ extension theorem with $1/s < 1/r'$. Basically we win if, with input $a = 0$, the index $1/s$ is bigger than the original $1/q$. (A necessary condition for this to happen is $1/r' > 1/q$, which is $1/q < 1/p$.)

Further study of convolution with the Bochner–Riesz kernel is merited. For example, is the $L^{8/5} - L^4$ convolution estimate in the above proof sharp?

It is interesting to note that the state of the art in euclidean restriction is currently more advanced than that in the finite field case. The recent paper of Tao on bilinear restriction in GAFA, and as yet unpublished work of Bennett, Tao and the lecturer on multilinear restriction (to appear in Acta Mathematica) are crying out to be understood in the finite field setting.