Some Details from Lectures

Ernie Croot

April 26, 2007

Here, I will describe some details from my recent lectures, which are not so well explained in the note on Freiman's Theorem on the course webpage.

1 A Fact about Lattices that I Used

First, in one of the lemmas I presented in class, I said that the lattice $\Lambda \subseteq \mathbb{R}^k$ generated by the $k+1$ vectors

$$c \ = \ (c_1, ..., c_k), \ (N, 0, ..., 0), \ (0, N, 0, ..., 0), \ (0, 0, ..., N),$$

has $|\det(\Lambda)| = N^{k-1}$ when c_1 is coprime to N. I had said that one way to see this is to form a basis for the lattice consisting of k vectors as follows: First, let

$$c' \ = \ (1, c_2', ..., c_k'), \text{ where } c_i' \ \equiv \ c_i c_1^{-1} \pmod{N}.$$

Then, I claimed that Λ is generated by the vectors

$$c', \ (0, N, 0, ..., 0), \ ..., \ (0, 0, ..., N), \tag{1}$$

and using this basis it is obvious that $|\det(\Lambda)| = N^{k-1}$.

Let me now expound upon these comments, by showing that this new basis does indeed generate the lattice: First, it is obvious that $c' \in \Lambda$, because

$$c' \ \in \ sc + N\mathbb{Z}^k, \text{ where } s \equiv c_1^{-1} \pmod{N}.$$

This then establishes that Λ contains the sublattice generated by the vectors (1). To show that sublattice is actually equal to Λ, it suffices to show that it contains the two vectors

$$c \ \text{ and } \ (N, 0, 0, ..., 0).$$

First, we realize that

$$c - c_1 c' \ = \ (0, t_2 N, t_3 N, ..., t_k N), \text{ where } t_i \in \mathbb{Z}.$$

Clearly, then c lies in the span of the vectors (1).

Now consider

$$Nc' \ = \ (N, c_2' N, c_3' N, ..., c_k' N) \ = \ (N, 0, 0, ..., 0) + L,$$

where L is an integer linear combination of

$$(0, N, 0, ..., 0), \ (0, 0, N, ..., 0), \ ..., \ (0, 0, ..., N).$$

It follows that $(N, 0, ..., 0)$ is also in our sublattice, and so the proof that $|\det(\Lambda)| = N^{k-1}$ is complete.

2 On a Lemma of Ruzsa

I thought I would give here an intuitive discussion of a certain lemma of Ruzsa which played a central role in the proof of Freiman's Theorem. This lemma stated that:

Lemma. Suppose that A is a finite set of integers. Then, for any prime

$$N \ > \ 2|kA - kA|,$$

there exists a subset $A' \subseteq A$ of size at least $|A|/k$ which is Freiman k-isomorphic to a subset of $\mathbb{Z}/N\mathbb{Z}$.

In class I mentioned (while addressing a question of Adam Marcus) a result in passing that was first proved by P. Erdős, which is somewhat helpful in understanding Ruzsa's proof (at least as far as what sorts of ideas one should look for to prove a lemma of the same flavor as Ruzsa's above). The way I think of Ruzsa's proof is that one can produce lots and lots of Freiman k-homomorphisms φ from subsets $A' \subseteq A$ to $\mathbb{Z}/N\mathbb{Z}$, each parameterized by some integer q that appears in intermediate steps of the proof, such that there are more choices for q than there are potential obstructions that keep any of the φ from being a Freiman k-*isomorphism*. So, by a counting argument one discovers that there exists a q, and therefore a map φ, which results in a Freiman k-isomorphism.

This theorem of Erdős is as follows.

Theorem. Suppose that A is a finite set of integers. Then, there exists a subset $A' \subseteq A$ satisfying $|A'| \geq |A|/3$, such that A' is "sum-free", meaning that it has no solutions

$$x + y \;=\; z, \quad x, y, z \in A'.$$

Erdős's proof is as follows: Let p be a prime number exceeding twice the maximum absolute value of the elements of A. Then, if we mod the elements of A out by p, each of the residues that result are distinct; furthermore, if the dilate these residues by multiplying by a number q that is coprime to p, then the new residues are also distinct. We are describing here a mapping

$$\begin{aligned} \varphi \;:\; A &\;\rightarrow\; \mathbb{Z}/pZ \\ a &\;\rightarrow\; qa \pmod{p}. \end{aligned}$$

Now, it is easy to see that

$$a + b = c,\; a, b, c \in A \;\;\Longrightarrow\;\; \varphi(a) + \varphi(b) \equiv \varphi(c) \pmod{p}.$$

So, if

$$S \;\subseteq\; \mathrm{img}(\varphi)$$

is sum-free, then

$$A' \;:=\; \varphi^{-1}(S) \;\subseteq\; A$$

is also sum-free.

A simple counting (or averaging) argument proves that there exists some number q coprime to p such that the image of φ maps at least $|A|/3$ of the elements of A into the interval $[p/3, 2p/3)$ modulo p. Noting that the set of integers in this interval form a sum-free set, even when considered modulo p, it follows that there exists q and a set $S \subseteq [p/3, 2p/3) \bmod p$ that is sum-free and satisfies $|S| \geq |A|/3$. So, A' is also sum-free and satisfies

$$|A'| \;=\; |S| \;\geq\; |A|/3.$$

2.1 The Proof of Ruzsa's Lemma

To prove Ruzsa's lemma, we start by letting p be any prime satisfying

$$p \ > \ k(\mathrm{MAX}A \ - \ \mathrm{MIN}A). \tag{2}$$

The first part of Ruza's proof bears more than a passing resemblence to Erdős's proof detailed previously: For an integer $1 \leq q \leq p-1$ (which is necessarily coprime to p) we consider the mapping

$$\begin{array}{rccl} \varphi_q \ : & A & \rightarrow & \mathbb{Z}/p\mathbb{Z} \\ & a & \rightarrow & qa \pmod{p}. \end{array}$$

It is obvious that this is a Freiman k-homomorpism for all k (since it is a group homomorphism); however, what takes a little bit of work to see (though not much) is that, in fact, inequality (2) implies that

$$\varphi_q \text{ is a Freiman } k - \text{isomorphism.}$$

The trouble with working with the group $\mathbb{Z}/p\mathbb{Z}$ to prove Ruzsa's lemma is that it is potentially too large (much larger than $2|kA-kA|$). So what we want to do is compress the images of φ_q in $\mathbb{Z}/p\mathbb{Z}$ somehow; and, Ruzsa's idea was to map subsets of $\mathbb{Z}/p\mathbb{Z}$ down to $\mathbb{Z}/N\mathbb{Z}$, where N is any prime satisfying

$$N \ > \ 2|kA - kA|.$$

Note that this N is potentially quite a bit smaller than p, which is good.

But now we have another problem, which is that if we let ψ be any mapping from $\mathbb{Z}/p\mathbb{Z}$ down to $\mathbb{Z}/N\mathbb{Z}$, it cannot be an injective Freiman k-homomorphism, let alone an injective group homomorphism.

Ok, so ψ cannot be a Freiman k-homomorphism; however, if we restrict ourselves to an integer interval I of residues mod p of width at most p/k, then on that interval we can pick ψ to be a Freiman k-homomorphism. One has to be a little careful here in descrbing this (due to the fact that residues mod p are not integers, so the mapping is tricky to define because of "type" issues): Let $\iota : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}$ be any embedding mapping consecutive residues to consecutive integers, such that the residues in I are mapped to consecutive

integers (not all "obvious embeddings" have this last property). Then, one choice for our ψ is

$$\begin{array}{rcccl} \psi & := & \psi_I & : & I \quad \to \quad \mathbb{Z}/N\mathbb{Z} \\ & & & & n \quad \to \quad \iota(n) \pmod N. \end{array}$$

To prove Ruzsa's lemma, then, we just need to focus on the following claim.

Claim. There exists $1 \leq q \leq p-1$, such that more than $|A|/k$ of the images $\varphi_q(a)$ land in an interval I of width $\leq p/k$; and, if we let

$$A' \ := \ \varphi_q^{-1}(I) \cap A,$$

then the composition $\psi_I \circ \varphi_q$ is a Freiman k-isomorphism.

Note that regardless of what q we pick, $\psi|_I \circ \varphi_q$ is *always* a Freiman k-*homomorphism* from A' into $\mathbb{Z}/N\mathbb{Z}$; however, only special q are "good", meaning that they result in a k-*isomorphism*.

Now, if q is "bad", then it means that there exist elements

$$a_1, ..., a_k, a_1', ..., a_k' \ \in \ A',$$

such that

$$a_1 + \cdots + q_k \ \neq \ a_1' + \cdots + a_k',$$

yet when we consider the integers $b_1, ..., b_k, b_1', ..., b_k'$ satisfying

$$b_i \ \equiv \ qa_i \pmod p, \text{ and } b_i' \ \equiv \ qa_i' \pmod p,$$

which are choosen so that they (the b_i and b_i') lie in some interval I of width at most p/k, then they will satisfy

$$b_1 + \cdots + b_k \ - \ b_1' - \cdots - b_k' \ \in \ (-p, p),$$

(this is easy to see) and

$$N \mid (b_1 + \cdots + b_k \ - \ b_1' - \cdots - b_k')$$

(this is by design, since we are assuming q is "bad").

This puts severe restrictions on what our "bad" q can be, because it means that, modulo p, we must have that

$$\begin{aligned} a_1 + \cdots + a_k - a'_1 - \cdots - a'_k &\equiv q^{-1}(b_1 + \cdots + b_k - b'_1 - \cdots - b'_k) \pmod{p} \\ &\equiv q^{-1}Nm \pmod{p}, \end{aligned}$$

where m is the integer

$$m \;=\; \frac{b_1 + \cdots + b_k - b'_1 - \cdots - b'_k}{N} \;\in\; (-p/N,\; p/N).$$

So, the number of possibilities for a "bad" q is at most the number of expressions $a_1 + \cdots + a_k - a'_1 - \cdots - a'_k$ times the number of choices for m; that product is at most

$$2|kA - kA|(p-1)/N,$$

which will be smaller than $p-1$ (the number of available q satisfying $1 \leq q \leq p-1$) as soon as

$$N \;>\; 2|kA - kA|.$$