Finite field models in additive combinatorics

Julia Wolf
University of Bristol

Emerging applications of finite fields
RICAM, Linz
10th December 2013

What is additive number theory?

Here is a sample of questions that fall into this category:

What is additive number theory?

Here is a sample of questions that fall into this category:

- How dense can a subset of the first N integers be before it is bound to contain a 3-term arithmetic progression?

What is additive number theory?

Here is a sample of questions that fall into this category:

- How dense can a subset of the first N integers be before it is bound to contain a 3-term arithmetic progression?
  $\rightarrow$ **Roth's theorem**

What is additive number theory?

Here is a sample of questions that fall into this category:

- How dense can a subset of the first N integers be before it is bound to contain a 3-term arithmetic progression?
  $\rightarrow$ **Roth's theorem**
- If a subset of the first N integers has small sumset, what can we say about its structure?

What is additive number theory?

Here is a sample of questions that fall into this category:

- How dense can a subset of the first N integers be before it is bound to contain a 3-term arithmetic progression?
  $\rightarrow$ **Roth's theorem**
- If a subset of the first N integers has small sumset, what can we say about its structure?
  $\rightarrow$ **Freiman's theorem**

What is additive number theory?

Here is a sample of questions that fall into this category:

- How dense can a subset of the first N integers be before it is bound to contain a 3-term arithmetic progression?
  $\rightarrow$ **Roth's theorem**
- If a subset of the first N integers has small sumset, what can we say about its structure?
  $\rightarrow$ **Freiman's theorem**
- If a subset of the first N integers contains many arithmetic progressions of length 4, what can we say about its structure?

What is additive number theory?

Here is a sample of questions that fall into this category:

- How dense can a subset of the first N integers be before it is bound to contain a 3-term arithmetic progression?
  $\rightarrow$ **Roth's theorem**
- If a subset of the first N integers has small sumset, what can we say about its structure?
  $\rightarrow$ **Freiman's theorem**
- If a subset of the first N integers contains many arithmetic progressions of length 4, what can we say about its structure?
  $\rightarrow$ **Quadratic inverse theorem**

What is additive number theory?

Here is a sample of questions that fall into this category:

- How dense can a subset of the first N integers be before it is bound to contain a 3-term arithmetic progression?
  $\rightarrow$ **Roth's theorem**
- If a subset of the first N integers has small sumset, what can we say about its structure?
  $\rightarrow$ **Freiman's theorem**
- If a subset of the first N integers contains many arithmetic progressions of length 4, what can we say about its structure?
  $\rightarrow$ **Quadratic inverse theorem**

Quantitatively all three of these questions are wide open.

What is the finite field model?

Instead of considering

the interval $\{1, 2, \ldots, N\}$

What is the finite field model?

Instead of considering

the interval $\{1, 2, \ldots, N\}$ or the cyclic group $\mathbb{Z}/N\mathbb{Z}$,

What is the finite field model?

Instead of considering

$$\text{the interval } \{1, 2, \ldots, N\} \text{ or the cyclic group } \mathbb{Z}/N\mathbb{Z},$$

we consider the vector space of dimension n over a finite field $\mathbb{F}_p$ for small fixed p.

What is the finite field model?

Instead of considering

$$\text{the interval } \{1, 2, \dots, N\} \text{ or the cyclic group } \mathbb{Z}/N\mathbb{Z},$$

we consider the vector space of dimension n over a finite field $\mathbb{F}_p$ for small fixed p.

The results we look for are always asymptotic in the size of the group, that is, in N or p^n.

What is the finite field model?

Instead of considering

$$\text{the interval } \{1, 2, \dots, N\} \text{ or the cyclic group } \mathbb{Z}/N\mathbb{Z},$$

we consider the vector space of dimension n over a finite field $\mathbb{F}_p$ for small fixed p.

The results we look for are always asymptotic in the size of the group, that is, in N or p^n.

Popular choices are $\mathbb{F}_3^n$ for Roth's theorem, $\mathbb{F}_2^n$ for Freiman's theorem and $\mathbb{F}_5^n$ for the inverse theorem.

What are the advantages of the finite field model?

This new setting is very pleasant to work with since it is much more "algebraic":

What are the advantages of the finite field model?

This new setting is very pleasant to work with since it is much more "algebraic":

- While $\mathbb{Z}/N\mathbb{Z}$ has no non-trivial subgroups, there is a plentiful supply of subspaces in $\mathbb{F}_p^n$.

What are the advantages of the finite field model?

This new setting is very pleasant to work with since it is much more "algebraic":

- While $\mathbb{Z}/N\mathbb{Z}$ has no non-trivial subgroups, there is a plentiful supply of subspaces in $\mathbb{F}_p^n$.
- Linear independence has to be thought of in an approximate way in $\mathbb{Z}/N\mathbb{Z}$. On the other hand, $\mathbb{F}_p^n$ is just a vector space equipped with the standard basis.

What are the advantages of the finite field model?

This new setting is very pleasant to work with since it is much more "algebraic":

- While $\mathbb{Z}/N\mathbb{Z}$ has no non-trivial subgroups, there is a plentiful supply of subspaces in $\mathbb{F}_p^n$.
- Linear independence has to be thought of in an approximate way in $\mathbb{Z}/N\mathbb{Z}$. On the other hand, $\mathbb{F}_p^n$ is just a vector space equipped with the standard basis.

In addition, $\mathbb{F}_p^n$, especially $p = 2$, is of practical importance in computer science.

What are the advantages of the finite field model?

This new setting is very pleasant to work with since it is much more "algebraic":

- While $\mathbb{Z}/N\mathbb{Z}$ has no non-trivial subgroups, there is a plentiful supply of subspaces in $\mathbb{F}_p^n$.
- Linear independence has to be thought of in an approximate way in $\mathbb{Z}/N\mathbb{Z}$. On the other hand, $\mathbb{F}_p^n$ is just a vector space equipped with the standard basis.

In addition, $\mathbb{F}_p^n$, especially $p = 2$, is of practical importance in computer science.

Working in $\mathbb{F}_p^n$ has saved many trees so far as arguments tend to become much shorter and cleaner.

What questions can we ask in the finite field model?

But most importantly, there is a way of transferring the finite field arguments to the integers.

What questions can we ask in the finite field model?

But most importantly, there is a way of transferring the finite field arguments to the integers.
$\rightarrow$ **Bourgainization**.

What questions can we ask in the finite field model?

But most importantly, there is a way of transferring the finite field arguments to the integers.
$\rightarrow$ **Bourgainization**.

- Roth's theorem: How dense can a subset of $\mathbb{F}_3^n$ be before it is bound to contain a 3-term arithmetic progression?

What questions can we ask in the finite field model?

But most importantly, there is a way of transferring the finite field arguments to the integers.
$\rightarrow$ **Bourgainization**.

- Roth's theorem: How dense can a subset of $\mathbb{F}_3^n$ be before it is bound to contain a 3-term arithmetic progression?
- Freiman's theorem: If a subset of $\mathbb{F}_2^n$ has small sumset, what can we say about its structure?

What questions can we ask in the finite field model?

But most importantly, there is a way of transferring the finite field arguments to the integers.
$\rightarrow$ **Bourgainization**.

- Roth's theorem: How dense can a subset of $\mathbb{F}_3^n$ be before it is bound to contain a 3-term arithmetic progression?
- Freiman's theorem: If a subset of $\mathbb{F}_2^n$ has small sumset, what can we say about its structure?
- Quadratic inverse theorem: If a subset of $\mathbb{F}_5^n$ contains many arithmetic progressions of length 4, what can we say about its structure?

What questions can we ask in the finite field model?

But most importantly, there is a way of transferring the finite field arguments to the integers.
$\rightarrow$ **Bourgainization**.

- Roth's theorem: How dense can a subset of $\mathbb{F}_3^n$ be before it is bound to contain a 3-term arithmetic progression?
- Freiman's theorem: If a subset of $\mathbb{F}_2^n$ has small sumset, what can we say about its structure?
- Quadratic inverse theorem: If a subset of $\mathbb{F}_5^n$ contains many arithmetic progressions of length 4, what can we say about its structure?

... and many more.

The discrete Fourier transform

Question

How does discrete Fourier analysis help us locate arithmetic structures such as arithmetic progressions in dense sets?

The discrete Fourier transform

Question

How does discrete Fourier analysis help us locate arithmetic structures such as arithmetic progressions in dense sets?

- Fourier transform: $\widehat{f}(t) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\omega^{t \cdot x}$

The discrete Fourier transform

Question

How does discrete Fourier analysis help us locate arithmetic structures such as arithmetic progressions in dense sets?

- Fourier transform: $\widehat{f}(t) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\omega^{t \cdot x}$
- Fourier inversion: $f(x) = \sum_{t \in \widehat{\mathbb{F}_p^n}} \widehat{f}(t)\omega^{-t \cdot x}$

The discrete Fourier transform

Question

How does discrete Fourier analysis help us locate arithmetic structures such as arithmetic progressions in dense sets?

- Fourier transform: $\widehat{f}(t) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\omega^{t \cdot x}$
- Fourier inversion: $f(x) = \sum_{t \in \widehat{\mathbb{F}_p^n}} \widehat{f}(t)\omega^{-t \cdot x}$
- Parseval's identity: $\mathbb{E}_{x \in \mathbb{F}_p^n} |f(x)|^2 = \sum_{t \in \widehat{\mathbb{F}_p^n}} |\widehat{f}(t)|^2$

The discrete Fourier transform

Question

How does discrete Fourier analysis help us locate arithmetic structures such as arithmetic progressions in dense sets?

- Fourier transform: $\widehat{f}(t) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\omega^{t \cdot x}$
- Fourier inversion: $f(x) = \sum_{t \in \widehat{\mathbb{F}_p^n}} \widehat{f}(t)\omega^{-t \cdot x}$
- Parseval's identity: $\mathbb{E}_{x \in \mathbb{F}_p^n} |f(x)|^2 = \sum_{t \in \widehat{\mathbb{F}_p^n}} |\widehat{f}(t)|^2$

Note that $\widehat{1_A}(0) = \alpha$ whenever $A \subseteq \mathbb{F}_p^n$ is a subset of density α,

The discrete Fourier transform

Question

How does discrete Fourier analysis help us locate arithmetic structures such as arithmetic progressions in dense sets?

- Fourier transform: $\widehat{f}(t) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\omega^{t \cdot x}$
- Fourier inversion: $f(x) = \sum_{t \in \widehat{\mathbb{F}_p^n}} \widehat{f}(t)\omega^{-t \cdot x}$
- Parseval's identity: $\mathbb{E}_{x \in \mathbb{F}_p^n} |f(x)|^2 = \sum_{t \in \widehat{\mathbb{F}_p^n}} |\widehat{f}(t)|^2$

Note that $\widehat{1_A}(0) = \alpha$ whenever $A \subseteq \mathbb{F}_p^n$ is a subset of density α, and that $\|\widehat{f}\|_2^2 = \alpha$ in this case.

The discrete Fourier transform

Question

How does discrete Fourier analysis help us locate arithmetic structures such as arithmetic progressions in dense sets?

- Fourier transform: $\widehat{f}(t) := \mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\omega^{t \cdot x}$
- Fourier inversion: $f(x) = \sum_{t \in \widehat{\mathbb{F}_p^n}} \widehat{f}(t)\omega^{-t \cdot x}$
- Parseval's identity: $\mathbb{E}_{x \in \mathbb{F}_p^n} |f(x)|^2 = \sum_{t \in \widehat{\mathbb{F}_p^n}} |\widehat{f}(t)|^2$

Note that $\widehat{1_A}(0) = \alpha$ whenever $A \subseteq \mathbb{F}_p^n$ is a subset of density α, and that $\|\widehat{f}\|_2^2 = \alpha$ in this case. Write N for $|\mathbb{F}_p^n| = p^n$.

Counting 3-term arithmetic progressions in dense sets

Definition

We say a set $A \subseteq \mathbb{F}_p^n$ is uniform if the largest non-trivial Fourier coefficient of its characteristic function is small.

Counting 3-term arithmetic progressions in dense sets

Definition

We say a set $A \subseteq \mathbb{F}_p^n$ is uniform if the largest non-trivial Fourier coefficient of its characteristic function is small.

Fact

If a subset $A \subseteq \mathbb{F}_3^n$ of density α is uniform, then it contains the expected number α^3 of 3-term progressions.

Counting 3-term arithmetic progressions in dense sets

Definition

We say a set $A \subseteq \mathbb{F}_p^n$ is uniform if the largest non-trivial Fourier coefficient of its characteristic function is small.

Fact

If a subset $A \subseteq \mathbb{F}_3^n$ of density α is uniform, then it contains the expected number α^3 of 3-term progressions.

$$\mathbb{E}_{x,d \in \mathbb{F}_3^n} 1_A(x) 1_A(x+d) 1_A(x+2d)$$

Counting 3-term arithmetic progressions in dense sets

Definition

We say a set $A \subseteq \mathbb{F}_p^n$ is uniform if the largest non-trivial Fourier coefficient of its characteristic function is small.

Fact

If a subset $A \subseteq \mathbb{F}_3^n$ of density α is uniform, then it contains the expected number α^3 of 3-term progressions.

$$\mathbb{E}_{x,d \in \mathbb{F}_3^n} 1_A(x) 1_A(x+d) 1_A(x+2d) \quad = \quad \sum_{t \in \widehat{\mathbb{F}_3^n}} |\widehat{1_A}(t)|^2 \widehat{1_A}(t)$$

Counting 3-term arithmetic progressions in dense sets

Definition

We say a set $A \subseteq \mathbb{F}_p^n$ is uniform if the largest non-trivial Fourier coefficient of its characteristic function is small.

Fact

If a subset $A \subseteq \mathbb{F}_3^n$ of density α is uniform, then it contains the expected number α^3 of 3-term progressions.

$$\begin{aligned}\mathbb{E}_{x,d\in\mathbb{F}_3^n} 1_A(x)1_A(x+d)1_A(x+2d) &= \sum_{t\in\widehat{\mathbb{F}_3^n}} |\widehat{1_A}(t)|^2\widehat{1_A}(t) \\ &= \alpha^3 + \sum_{t\neq 0} |\widehat{1_A}(t)|^2\widehat{1_A}(t)\end{aligned}$$

Counting 3-term arithmetic progressions in dense sets

Definition

We say a set $A \subseteq \mathbb{F}_p^n$ is uniform if the largest non-trivial Fourier coefficient of its characteristic function is small.

Fact

If a subset $A \subseteq \mathbb{F}_3^n$ of density α is uniform, then it contains the expected number α^3 of 3-term progressions.

$$\begin{aligned}
\mathbb{E}_{x,d\in\mathbb{F}_3^n} 1_A(x)1_A(x+d)1_A(x+2d) &= \sum_{t\in\widehat{\mathbb{F}_3^n}} |\widehat{1_A}(t)|^2\widehat{1_A}(t) \\
&= \alpha^3 + \sum_{t\neq 0} |\widehat{1_A}(t)|^2\widehat{1_A}(t) \\
&\approx \alpha^3
\end{aligned}$$

Proving Roth's Theorem in $\mathbb{F}_3^n$

Theorem (Meshulam, 1995)

Let $A \subseteq \mathbb{F}_3^n$ be a subset of density α containing no 3-APs. Then

$$\alpha \leq \frac{1}{\log N}.$$

Outline of the proof:

Proving Roth's Theorem in $\mathbb{F}_3^n$

Theorem (Meshulam, 1995)

Let $A \subseteq \mathbb{F}_3^n$ be a subset of density α containing no 3-APs. Then

$$\alpha \leq \frac{1}{\log N}.$$

Outline of the proof:

- Suppose A is uniform, then A contains plenty of 3-APs.

Proving Roth's Theorem in $\mathbb{F}_3^n$

Theorem (Meshulam, 1995)

Let $A \subseteq \mathbb{F}_3^n$ be a subset of density α containing no 3-APs. Then

$$\alpha \leq \frac{1}{\log N}.$$

Outline of the proof:

- Suppose A is uniform, then A contains plenty of 3-APs.
- Therefore A is non-uniform, that is, there exists $t \neq 0$ s.t. $|\widehat{1_A}(t)|$ is large.

Proving Roth's Theorem in $\mathbb{F}_3^n$

Theorem (Meshulam, 1995)

Let $A \subseteq \mathbb{F}_3^n$ be a subset of density α containing no 3-APs. Then

$$\alpha \leq \frac{1}{\log N}.$$

Outline of the proof:

- Suppose A is uniform, then A contains plenty of 3-APs.
- Therefore A is non-uniform, that is, there exists $t \neq 0$ s.t. $|\widehat{1_A}(t)|$ is large.
- This in turn implies that 1_A has increased density on an affine subspace of codimension 1.

Proving Roth's Theorem in $\mathbb{F}_3^n$

Theorem (Meshulam, 1995)

Let $A \subseteq \mathbb{F}_3^n$ be a subset of density α containing no 3-APs. Then

$$\alpha \leq \frac{1}{\log N}.$$

Outline of the proof:

- Suppose A is uniform, then A contains plenty of 3-APs.
- Therefore A is non-uniform, that is, there exists $t \neq 0$ s.t. $|\widehat{1_A}(t)|$ is large.
- This in turn implies that 1_A has increased density on an affine subspace of codimension 1.
- Repeat the argument with 1_A restricted to this subspace.

A recent improvement

Improving this simple argument has proved surprisingly difficult.

Theorem (Bateman-Katz, 2011)

There exists $\epsilon > 0$ such that any 3-term progression free set $A \subseteq \mathbb{F}_3^n$ has density

$$\alpha \leq \frac{1}{(\log N)^{1+\epsilon}}.$$

A recent improvement

Improving this simple argument has proved surprisingly difficult.

Theorem (Bateman-Katz, 2011)

There exists $\epsilon > 0$ such that any 3-term progression free set $A \subseteq \mathbb{F}_3^n$ has density

$$\alpha \leq \frac{1}{(\log N)^{1+\epsilon}}.$$

The proof involves an intricate argument about the structure of the large Fourier spectrum of 1_A.

3-term progression free sets

Can we construct large progression-free sets?

3-term progression free sets

Can we construct large progression-free sets?

Theorem (Edel, 2004)

There exists a 3-term progression free subset of $\mathbb{F}_3^n$ of size

$$\Omega(N^{.7249})$$

3-term progression free sets

Can we construct large progression-free sets?

Theorem (Edel, 2004)

There exists a 3-term progression free subset of $\mathbb{F}_3^n$ *of size*

$$\Omega(N^{.7249})$$

Question

Can this be improved to $(3 - o(1))^n$*?*

3-term progression free sets

Can we construct large progression-free sets?

Theorem (Edel, 2004)

There exists a 3-term progression free subset of $\mathbb{F}_3^n$ *of size*

$$\Omega(N^{.7249})$$

Question

Can this be improved to $(3 - o(1))^n$*?*

Recall that $N = 3^n$.

Counting 4-term progressions in dense sets

The same Fourier argument works for any linear configuration defined by a single linear equation. However:

Counting 4-term progressions in dense sets

The same Fourier argument works for any linear configuration defined by a single linear equation. However:

Fact

Fourier analysis is not sufficient for counting longer progressions.

Counting 4-term progressions in dense sets

The same Fourier argument works for any linear configuration defined by a single linear equation. However:

Fact

Fourier analysis is not sufficient for counting longer progressions.

For example, the following set is uniform in the Fourier sense but contains many *more* than the expected number of 4-APs.

$$A = \{x \in \mathbb{F}_p^n : x \cdot x = 0\}$$

Counting 4-term progressions in dense sets

The same Fourier argument works for any linear configuration defined by a single linear equation. However:

Fact

Fourier analysis is not sufficient for counting longer progressions.

For example, the following set is uniform in the Fourier sense but contains many *more* than the expected number of 4-APs.

$$A = \{x \in \mathbb{F}_p^n : x \cdot x = 0\}$$

$$x^2 - 3(x+d)^2 + 3(x+2d)^2 - (x+3d)^2 = 0$$

The structure of sets with small sumset

Two observations:

- In general, $A + A$ can be of size up to $|A|^2$.

The structure of sets with small sumset

Two observations:

- In general, $A + A$ can be of size up to $|A|^2$.
- Subspaces have very small sumset: $|V + V| = |V|$.

The structure of sets with small sumset

Two observations:

- In general, $A + A$ can be of size up to $|A|^2$.
- Subspaces have very small sumset: $|V + V| = |V|$.

Question

Is the converse also true? That is, does a set with small sumset necessarily look like a subspace?

The structure of sets with small sumset

Two observations:

- In general, $A + A$ can be of size up to $|A|^2$.
- Subspaces have very small sumset: $|V + V| = |V|$.

Question

Is the converse also true? That is, does a set with small sumset necessarily look like a subspace?

The extent to which a set is additively closed is quantified by the doubling constant K, which satisfies $|A + A| \leq K|A|$.

The structure of sets with small sumset

Theorem (Ruzsa, 1994)

Let $A \subseteq \mathbb{F}_p^n$ satisfy $|A+A| \leq K|A|$. Then A is contained in the coset of some subspace $H \leqslant \mathbb{F}_p^n$ of size at most $K^2 p^{K^4}|A|$.

The structure of sets with small sumset

Theorem (Ruzsa, 1994)

Let $A \subseteq \mathbb{F}_p^n$ satisfy $|A+A| \leq K|A|$. Then A is contained in the coset of some subspace $H \leqslant \mathbb{F}_p^n$ of size at most $K^2 p^{K^4}|A|$.

There are improvements to this bound due to Green-Tao, Schoen and Sanders.

The structure of sets with small sumset

Theorem (Ruzsa, 1994)

Let $A \subseteq \mathbb{F}_p^n$ satisfy $|A+A| \leq K|A|$. Then A is contained in the coset of some subspace $H \leqslant \mathbb{F}_p^n$ of size at most $K^2 p^{K^4}|A|$.

There are improvements to this bound due to Green-Tao, Schoen and Sanders.

Ruzsa's proof proceeds by choosing a maximal set $X \subseteq 2A - 2A$ such that $x + A$ are disjoint for $x \in X$. Then one uses inequalities concerning the size of iterated sumsets.

Counting 4-term progressions

Gowers introduced a series of uniformity norms known as the U^k norms.

Counting 4-term progressions

Gowers introduced a series of uniformity norms known as the U^k norms.
The U^2 norm is equivalent to the Fourier transform:
$\|f\|_{U^2} = \|\widehat{f}\|_4$,

Counting 4-term progressions

Gowers introduced a series of uniformity norms known as the U^k norms.
The U^2 norm is equivalent to the Fourier transform:
$\|f\|_{U^2} = \|\widehat{f}\|_4$, or in physical space,

$$\|f\|_{U^2}^4 = \mathbb{E}_{x,a,b} f(x)f(x+a)f(x+b)f(x+a+b).$$

Counting 4-term progressions

Gowers introduced a series of uniformity norms known as the U^k norms.
The U^2 norm is equivalent to the Fourier transform:
$\|f\|_{U^2} = \|\widehat{f}\|_4$, or in physical space,

$$\|f\|_{U^2}^4 = \mathbb{E}_{x,a,b} f(x)f(x+a)f(x+b)f(x+a+b).$$

Definition (Gowers, 1998)

For a function $f : \mathbb{F}_p^n \to [-1,1]$, we define the U^3 *norm* via

$$\begin{aligned}\|f\|_{U^3}^8 &= \mathbb{E}_{x,a,b,c} f(x)f(x+a)f(x+b)f(x+c) \\ &\quad f(x+a+b)f(x+a+c)f(x+b+c)f(x+a+b+c)\end{aligned}$$

Counting 4-term progressions

The U^3 norm controls the count of 4-term progressions.

Counting 4-term progressions

The U^3 norm controls the count of 4-term progressions.

Proposition (Gowers, 1998)

If $f : \mathbb{F}_p^n \to [-1,1]$, *then*

$$|\mathbb{E}_{x,d} f(x)f(x+d)f(x+2d)f(x+3d)| \leq \|f\|_{U^3}.$$

Counting 4-term progressions

The U^3 norm controls the count of 4-term progressions.

Proposition (Gowers, 1998)

If $f : \mathbb{F}_p^n \to [-1,1]$, *then*

$$|\mathbb{E}_{x,d} f(x)f(x+d)f(x+2d)f(x+3d)| \leq \|f\|_{U^3}.$$

In particular, if $\|1_A - \alpha\|_{U^3}$ is small, then

$$\mathbb{E}_{x,d} 1_A(x)1_A(x+d)1_A(x+2d)1_A(x+3d) \approx \alpha^4.$$

The U^3 inverse theorem

What can we say if the U^3 norm is large?

The U^3 inverse theorem

What can we say if the U^3 norm is large?

Theorem (Green-Tao 2008, Gowers 1998)

Suppose that $f : \mathbb{F}_p^n \to [-1,1]$ *is such that* $\|f\|_{U^3} \geq \delta$. *Then there exists a quadratic phase function* ϕ *such that*

$$|\mathbb{E}_x f(x)\phi(x)| \geq c(\delta).$$

The U^3 inverse theorem

What can we say if the U^3 norm is large?

Theorem (Green-Tao 2008, Gowers 1998)

Suppose that $f : \mathbb{F}_p^n \to [-1,1]$ *is such that* $\|f\|_{U^3} \geq \delta$. *Then there exists a quadratic phase function* ϕ *such that*

$$|\mathbb{E}_x f(x)\phi(x)| \geq c(\delta).$$

A quadratic phase function is a function of the form ω^q, where q is a quadratic form.

The U^3 inverse theorem

What can we say if the U^3 norm is large?

Theorem (Green-Tao 2008, Gowers 1998)

Suppose that $f : \mathbb{F}_p^n \to [-1,1]$ *is such that* $\|f\|_{U^3} \geq \delta$. *Then there exists a quadratic phase function* ϕ *such that*

$$|\mathbb{E}_x f(x)\phi(x)| \geq c(\delta).$$

A quadratic phase function is a function of the form ω^q, where q is a quadratic form.

The proof of the inverse theorem uses Freiman's theorem in a crucial way.

Sets containing no longer progressions

From these two ingredients one can deduce Szemerédi's theorem for longer progressions, for which we state the best known bound below.

Sets containing no longer progressions

From these two ingredients one can deduce Szemerédi's theorem for longer progressions, for which we state the best known bound below.

Theorem (Green-Tao, 2006-2010)

Let $A \subseteq \mathbb{F}_5^n$ be a set containing no 4-term arithmetic progressions. Then its density α satisfies

$$\alpha \leq (\log N)^{-2^{-22}}.$$

Sets containing no longer progressions

From these two ingredients one can deduce Szemerédi's theorem for longer progressions, for which we state the best known bound below.

Theorem (Green-Tao, 2006-2010)

Let $A \subseteq \mathbb{F}_5^n$ be a set containing no 4-term arithmetic progressions. Then its density α satisfies

$$\alpha \leq (\log N)^{-2^{-22}}.$$

The proof proceeds via a density increment strategy similar to the one we saw in Meshulam's theorem earlier.

Sets containing no longer progressions

Theorem (Lin-W., 2008)

There exist k-term progression free subsets of $\mathbb{F}_q^n$ of size

$$\Omega((q^{2(k-1)} + q^{k-1} - 1)^{n/2k}).$$

Sets containing no longer progressions

Theorem (Lin-W., 2008)

There exist k-term progression free subsets of $\mathbb{F}_q^n$ of size

$$\Omega((q^{2(k-1)} + q^{k-1} - 1)^{n/2k}).$$

In particular, there is a 4-term progression-free subset of $\mathbb{F}_5^n$ of size

$$\Omega(N^{\log 15749/8 \log 5}) = \Omega(N^{.7506}).$$

Sets containing no longer progressions

Theorem (Lin-W., 2008)

There exist k-term progression free subsets of $\mathbb{F}_q^n$ of size

$$\Omega((q^{2(k-1)} + q^{k-1} - 1)^{n/2k}).$$

In particular, there is a 4-term progression-free subset of $\mathbb{F}_5^n$ of size

$$\Omega(N^{\log 15749/8 \log 5}) = \Omega(N^{.7506}).$$

The proof is entirely algebraic/combinatorial, adapting work of Bierbrauer.

Counting monochromatic 3-term progressions

In this section we shall briefly consider the group $\mathbb{Z}_N$ with N prime.

Counting monochromatic 3-term progressions

In this section we shall briefly consider the group $\mathbb{Z}_N$ with N prime.

Fact

If $\mathbb{Z}_N$ (or $\mathbb{F}_p^n$) is 2-coloured and one of the colour classes has density α, then there are precisely $(\alpha^3 + (1-\alpha)^3)N^2$ monochromatic 3-term progressions.

Counting monochromatic 3-term progressions

In this section we shall briefly consider the group $\mathbb{Z}_N$ with N prime.

Fact

If $\mathbb{Z}_N$ (or $\mathbb{F}_p^n$) is 2-coloured and one of the colour classes has density α, then there are precisely $(\alpha^3 + (1-\alpha)^3)N^2$ monochromatic 3-term progressions.

As an immediate consequence we have:

Counting monochromatic 3-term progressions

In this section we shall briefly consider the group $\mathbb{Z}_N$ with N prime.

Fact

If $\mathbb{Z}_N$ (or $\mathbb{F}_p^n$) is 2-coloured and one of the colour classes has density α, then there are precisely $(\alpha^3 + (1-\alpha)^3)N^2$ monochromatic 3-term progressions.

As an immediate consequence we have:

Fact

If $\mathbb{Z}_N$ (or $\mathbb{F}_p^n$) is 2-coloured, then there are at least $\frac{1}{4}N^2$ monochromatic 3-term progressions.

Counting monochromatic 3-term progressions

The number of monochromatic 3-term progression equals

Counting monochromatic 3-term progressions

The number of monochromatic 3-term progression equals

$$\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_A(x)1_A(x+d)1_A(x+2d)+\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_{A^C}(x)1_{A^C}(x+d)1_{A^C}(x+2d)$$

Counting monochromatic 3-term progressions

The number of monochromatic 3-term progression equals

$$\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_A(x)1_A(x+d)1_A(x+2d)+\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_{A^C}(x)1_{A^C}(x+d)1_{A^C}(x+2d)$$

$$= \sum_{t\in\widehat{\mathbb{F}_p^n}} |\widehat{1_A}(t)|^2\widehat{1_A}(t) + \sum_{t\in\widehat{\mathbb{Z}_p}} |\widehat{1_{A^C}}(t)|^2\widehat{1_{A^C}}(t)$$

Counting monochromatic 3-term progressions

The number of monochromatic 3-term progression equals

$$\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_A(x)1_A(x+d)1_A(x+2d)+\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_{A^C}(x)1_{A^C}(x+d)1_{A^C}(x+2d)$$

$$= \sum_{t\in\widehat{\mathbb{F}_p^n}} |\widehat{1_A}(t)|^2\widehat{1_A}(t) + \sum_{t\in\widehat{\mathbb{Z}_p}} |\widehat{1_{A^C}}(t)|^2\widehat{1_{A^C}}(t)$$

$$= \alpha^3 + (1-\alpha)^3$$

Counting monochromatic 3-term progressions

The number of monochromatic 3-term progression equals

$$\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_A(x)1_A(x+d)1_A(x+2d)+\mathbb{E}_{x,d\in\mathbb{F}_p^n} 1_{A^C}(x)1_{A^C}(x+d)1_{A^C}(x+2d)$$

$$= \sum_{t\in\widehat{\mathbb{F}_p^n}} |\widehat{1_A}(t)|^2\widehat{1_A}(t) + \sum_{t\in\widehat{\mathbb{Z}_p}} |\widehat{1_{A^C}}(t)|^2\widehat{1_{A^C}}(t)$$

$$= \alpha^3 + (1-\alpha)^3$$

since $\widehat{1_A}(t) = -\widehat{1_{A^C}}(t)$ for $t \neq 0$.

Counting monochromatic 4-term progressions

Question

Is there a simple such formula for 4-term progressions?

Counting monochromatic 4-term progressions

Question

Is there a simple such formula for 4-term progressions?

- No.

Counting monochromatic 4-term progressions

Question

Is there a simple such formula for 4-term progressions?

- No.
- We have already seen that the Fourier transform is not sufficient for counting 4-term progressions in dense sets.

Counting monochromatic 4-term progressions

Question

Is there a simple such formula for 4-term progressions?

- No.
- We have already seen that the Fourier transform is not sufficient for counting 4-term progressions in dense sets.
- Because we are using 2 colours only, the colouring problem is closely related to density problems such as Szemerédi's theorem.

Counting monochromatic 4-term progressions

Theorem (W., 2010)

- *There exists a 2-colouring of $\mathbb{Z}_N$ with fewer than*

$$\frac{1}{8}\left(1-\frac{1}{259200}\right)N^2$$

monochromatic 4-term progressions.

Counting monochromatic 4-term progressions

Theorem (W., 2010)

- *There exists a 2-colouring of* $\mathbb{Z}_N$ *with fewer than*

$$\frac{1}{8}\left(1-\frac{1}{259200}\right)N^2$$

monochromatic 4-term progressions.

- *Any 2-colouring of* $\mathbb{Z}_N$ *contains at least*

$$\frac{1}{16}N^2$$

monochromatic 4-term progressions.

Counting monochromatic 4-term progressions

The proof of the upper bound is based on Gowers's positive answer to the following question.

Counting monochromatic 4-term progressions

The proof of the upper bound is based on Gowers's positive answer to the following question.

Question

Are there any subsets of $\mathbb{Z}_N$ that are uniform but contain fewer than the expected number of 4-term progressions?

Counting monochromatic 4-term progressions

The proof of the upper bound is based on Gowers's positive answer to the following question.

Question

Are there any subsets of $\mathbb{Z}_N$ that are uniform but contain fewer than the expected number of 4-term progressions?

- The construction is also based on the quadratic identity we saw earlier.

Counting monochromatic 4-term progressions

The proof of the upper bound is based on Gowers's positive answer to the following question.

Question

Are there any subsets of $\mathbb{Z}_N$ that are uniform but contain fewer than the expected number of 4-term progressions?

- The construction is also based on the quadratic identity we saw earlier.
- In addition, the set thus obtained is linearly uniform, which allows us to carry out all computations involving 3-term configurations with complete accuracy.

A result of Lu and Peng

Theorem (Lu-Peng, 2011)

A result of Lu and Peng

Theorem (Lu-Peng, 2011)

- *There exists a 2-coloring of $\mathbb{Z}_N$ with fewer than*

$$\frac{17}{150}N^2 = \frac{1}{8}\left(1 - \frac{7}{75}\right)N^2$$

monochromatic 4-term progressions.

A result of Lu and Peng

Theorem (Lu-Peng, 2011)

- *There exists a 2-coloring of $\mathbb{Z}_N$ with fewer than*

$$\frac{17}{150}N^2 = \frac{1}{8}\left(1 - \frac{7}{75}\right)N^2$$

monochromatic 4-term progressions.

- *Any 2-coloring of $\mathbb{Z}_N$ contains at least*

$$\frac{7}{96}N^2$$

monochromatic 4-term progressions.

A result of Lu and Peng

- By computation, they find a *good* example on [1,22] and tile that around the group $\mathbb{Z}_N$. They then proceed by a combinatorial counting argument.

A result of Lu and Peng

- By computation, they find a *good* example on [1,22] and tile that around the group $\mathbb{Z}_N$. They then proceed by a combinatorial counting argument.
- So was our complicated construction, using ideas from quadratic Fourier analysis, unnecesessary?

A result of Lu and Peng

- By computation, they find a *good* example on [1,22] and tile that around the group $\mathbb{Z}_N$. They then proceed by a combinatorial counting argument.
- So was our complicated construction, using ideas from quadratic Fourier analysis, unnecesessary?
- It turns out that any such colouring *must* have quadratic structure. Why?

Quadratic structure is required

If

$$\mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d)$$

Quadratic structure is required

If

$$\mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d)$$

$$+\mathbb{E}_{x,d} 1_{A^C}(x) 1_{A^C}(x+d) 1_{A^C}(x+2d) 1_{A^C}(x+3d)$$

Quadratic structure is required

If

$$\mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d)$$

$$+\mathbb{E}_{x,d} 1_{A^C}(x) 1_{A^C}(x+d) 1_{A^C}(x+2d) 1_{A^C}(x+3d)$$

$$\not\approx \alpha^4 + (1-\alpha)^4$$

Quadratic structure is required

If

$$\mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d)$$

$$+\mathbb{E}_{x,d} 1_{A^C}(x) 1_{A^C}(x+d) 1_{A^C}(x+2d) 1_{A^C}(x+3d)$$

$$\not\approx \alpha^4 + (1-\alpha)^4$$

then either $1_A - \alpha$ or $1_{A^C} - (1-\alpha)$ (and therefore both) must have large U^3 norm,

Quadratic structure is required

If

$$\mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d)$$

$$+\mathbb{E}_{x,d} 1_{A^C}(x) 1_{A^C}(x+d) 1_{A^C}(x+2d) 1_{A^C}(x+3d)$$

$$\not\approx \alpha^4 + (1-\alpha)^4$$

then either $1_A - \alpha$ or $1_{A^C} - (1-\alpha)$ (and therefore both) must have large U^3 norm, and therefore quadratic structure by the inverse theorem!

Quadratic structure is required

If

$$\mathbb{E}_{x,d} 1_A(x) 1_A(x+d) 1_A(x+2d) 1_A(x+3d)$$

$$+\mathbb{E}_{x,d} 1_{A^C}(x) 1_{A^C}(x+d) 1_{A^C}(x+2d) 1_{A^C}(x+3d)$$

$$\not\approx \alpha^4 + (1-\alpha)^4$$

then either $1_A - \alpha$ or $1_{A^C} - (1-\alpha)$ (and therefore both) must have large U^3 norm, and therefore quadratic structure by the inverse theorem!

Question

Can we describe this quadratic structure explicitly?

Limitations of the finite field model

- Because of the exponential growth of the finite field model, computational problems can actually become harder in the finite field model.

Limitations of the finite field model

- Because of the exponential growth of the finite field model, computational problems can actually become harder in the finite field model.
- Sometimes questions become trivial.

Limitations of the finite field model

- Because of the exponential growth of the finite field model, computational problems can actually become harder in the finite field model.
- Sometimes questions become trivial.
- Quantitatively strong proofs often show remarkable dissimilarities.

Limitations of the finite field model

- Because of the exponential growth of the finite field model, computational problems can actually become harder in the finite field model.
- Sometimes questions become trivial.
- Quantitatively strong proofs often show remarkable dissimilarities.
- The finite field model as defined here can only deal with purely additive problems. For problems involving multiplicative structure, the function field model is more appropriate.

Bibliography

- M. Bateman and N. Katz, *New bounds on cap sets*, 2011.
- Y. Edel, *Extensions of generalized product caps*, 2004.
- B. Green, *Finite field models in additive combinatorics*, 2005.
- B. Green, *Montréal lecture notes on quadratic Fourier analysis*, 2006.
- Y. Lin and J. Wolf, *Subsets of $\mathbb{F}_q^n$ containing no k-term progressions*, 2010.
- T. Sanders, *On the Bogolyubov-Ruzsa lemma*, 2010.
- J. Wolf, *The number of monochromatic 4-term progressions in $\mathbb{Z}_p$*, 2010.