BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Roth's Theorem: A Dense Enough Set Has a 3-AP

Exposition by William Gasarch
and
Kelin Zhu

April 11, 2025

The Erdös-Turan Conjecture

The Erdös-Turan Conjecture

Def Let $N \in \mathbb{N}$. Let $A \subseteq [N]$. The density of A is $|A|/N$.

The Erdös-Turan Conjecture

Def Let $N \in \mathbb{N}$. Let $A \subseteq [N]$. The density of A is $|A|/N$.

Szemerédi's Thm For all $\delta > 0$, for all k, there exists $N = N(\delta, k)$ such that the following holds:

The Erdös-Turan Conjecture

Def Let $N \in \mathbb{N}$. Let $A \subseteq [N]$. The density of A is $|A|/N$.

Szemerédi's Thm For all $\delta > 0$, for all k, there exists $N = N(\delta, k)$ such that the following holds:

If $A \subseteq [N]$ and A has density $\geq \delta$ then A has a k-AP.

The Erdös-Turan Conjecture

Def Let $N \in \mathbb{N}$. Let $A \subseteq [N]$. The density of A is $|A|/N$.

Szemerédi's Thm For all $\delta > 0$, for all k, there exists $N = N(\delta, k)$ such that the following holds:

If $A \subseteq [N]$ and A has density $\geq \delta$ then A has a k-AP.

We won't do the (hard) proof. We will do:

The Erdös-Turan Conjecture

Def Let $N \in \mathbb{N}$. Let $A \subseteq [N]$. The density of A is $|A|/N$.

Szemerédi's Thm For all $\delta > 0$, for all k, there exists $N = N(\delta, k)$ such that the following holds:

If $A \subseteq [N]$ and A has density $\geq \delta$ then A has a k-AP.

We won't do the (hard) proof. We will do:

1) Some easy cases, and

The Erdös-Turan Conjecture

Def Let $N \in \mathbb{N}$. Let $A \subseteq [N]$. The density of A is $|A|/N$.

Szemerédi's Thm For all $\delta > 0$, for all k, there exists $N = N(\delta, k)$ such that the following holds:

If $A \subseteq [N]$ and A has density $\geq \delta$ then A has a k-AP.

We won't do the (hard) proof. We will do:

1) Some easy cases, and

2) The $k = 3$ case which involves the Discrete Fourier Transform.

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.
We can assume $N \equiv 0 \pmod 3$.

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.

We can assume $N \equiv 0 \pmod 3$.

Look at

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.
We can assume $N \equiv 0 \pmod 3$.
Look at

$$\{1,2,3\},\{4,5,6\},\ldots,\{N-2,N-1,N\}.$$

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.
We can assume $N \equiv 0 \pmod 3$.
Look at

$$\{1,2,3\},\{4,5,6\},\ldots,\{N-2,N-1,N\}.$$

Case 1 $\exists x \equiv 1 \pmod 3$, $\{x, x+1, x+2\} \in A$. A has a 3-AP.

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.
We can assume $N \equiv 0 \pmod 3$.
Look at

$$\{1,2,3\},\{4,5,6\},\ldots,\{N-2,N-1,N\}.$$

Case 1 $\exists x \equiv 1 \pmod 3$, $\{x,x+1,x+2\} \in A$. A has a 3-AP.

Case 2 $\forall x \equiv 1 \pmod 3$, $|\{x,x+1,x+2\} \cap A| \leq 2$. Then

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.
We can assume $N \equiv 0 \pmod 3$.
Look at

$$\{1, 2, 3\}, \{4, 5, 6\}, \ldots, \{N-2, N-1, N\}.$$

Case 1 $\exists x \equiv 1 \pmod 3$, $\{x, x+1, x+2\} \in A$. A has a 3-AP.

Case 2 $\forall x \equiv 1 \pmod 3$, $|\{x, x+1, x+2\} \cap A| \leq 2$. Then $|A| \leq 2 \times \frac{N}{3} \leq 0.667N < 0.67N$

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.
We can assume $N \equiv 0 \pmod 3$.
Look at

$$\{1, 2, 3\}, \{4, 5, 6\}, \ldots, \{N-2, N-1, N\}.$$

Case 1 $\exists x \equiv 1 \pmod 3$, $\{x, x+1, x+2\} \in A$. A has a 3-AP.

Case 2 $\forall x \equiv 1 \pmod 3$, $|\{x, x+1, x+2\} \cap A| \leq 2$. Then
$|A| \leq 2 \times \frac{N}{3} \leq 0.667N < 0.67N$
This contradicts A having density ≥ 0.67.

An Easy Case

Thm Let $N \geq 3$. Let $A \subseteq [N]$ of density ≥ 0.67. Then A contains a 3-AP.
We can assume $N \equiv 0 \pmod 3$.
Look at

$$\{1,2,3\},\{4,5,6\},\ldots,\{N-2,N-1,N\}.$$

Case 1 $\exists x \equiv 1 \pmod 3$, $\{x, x+1, x+2\} \in A$. A has a 3-AP.

Case 2 $\forall x \equiv 1 \pmod 3$, $|\{x, x+1, x+2\} \cap A| \leq 2$. Then
$|A| \leq 2 \times \frac{N}{3} \leq 0.667N < 0.67N$
This contradicts A having density ≥ 0.67.

There may be a HW where you are asked to prove theorems like the 0.67-Theorem.

Roth's Theorem

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

Roth's Theorem

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds
For all $A \subseteq [N]$ of density $\geq \delta$, A has a 3-AP.

Roth's Theorem

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

For all $A \subseteq [N]$ of density $\geq \delta$, A has a 3-AP.

The **Intuition** behind the proof will be short and clear.

Roth's Theorem

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds
For all $A \subseteq [N]$ of density $\geq \delta$, A has a 3-AP.

The **Intuition** behind the proof will be short and clear.

The **formal proof** will be long and use interesting math.

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

1) A looks **random**. Then A will have a 3-AP.

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

1) A looks **random**. Then A will have a 3-AP.

2) There is a very large AP $N' \subseteq [N]$

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

1) A looks **random**. Then A will have a 3-AP.

2) There is a very large AP $N' \subseteq [N]$

$$N' = \{a, a+d, \ldots, a+kd\}$$

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

1) A looks **random**. Then A will have a 3-AP.

2) There is a very large AP $N' \subseteq [N]$

$$N' = \{a, a + d, \ldots, a + kd\}$$

such that
$A \cap N'$ has density $\delta' > \delta$ in N'.

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

1) A looks **random**. Then A will have a 3-AP.

2) There is a very large AP $N' \subseteq [N]$

$$N' = \{a, a+d, \ldots, a+kd\}$$

such that
$A \cap N'$ has density $\delta' > \delta$ in N'.

Can view $A \cap N'$ as a denser-than-δ subset of N'.

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

1) A looks **random**. Then A will have a 3-AP.

2) There is a very large AP $N' \subseteq [N]$

$$N' = \{a, a+d, \ldots, a+kd\}$$

such that
$A \cap N'$ has density $\delta' > \delta$ in N'.

Can view $A \cap N'$ as a denser-than-δ subset of N'.

Repeat this procedure until either you get the **Random** case or the density is ≥ 0.67.

Intuition Behind Roth's Theorem

Given $A \subseteq [N]$ of density δ we show one of the following happens.

1) A looks **random**. Then A will have a 3-AP.

2) There is a very large AP $N' \subseteq [N]$

$$N' = \{a, a+d, \ldots, a+kd\}$$

such that
$A \cap N'$ has density $\delta' > \delta$ in N'.

Can view $A \cap N'$ as a denser-than-δ subset of N'.

Repeat this procedure until either you get the **Random** case or the density is ≥ 0.67.

Much of what I said here isn't quite right, but thats the intuition.

How Will δ' and δ Relate

What if the δ increase as follows;
δ,

How Will δ' and δ Relate

What if the δ increase as follows;
δ,
$\delta + \frac{\delta^{100}}{2}$,

How Will δ' and δ Relate

What if the δ increase as follows;

δ,

$\delta + \frac{\delta^{100}}{2}$,

$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.

How Will δ' and δ Relate

What if the δ increase as follows;

δ,

$\delta + \frac{\delta^{100}}{2}$,

$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.

$\delta + \frac{\delta^2}{2} + \frac{\delta^{100}}{2^2} + \frac{\delta^{100}}{2^3}$.

How Will δ' and δ Relate

What if the δ increase as follows;

δ,

$\delta + \frac{\delta^{100}}{2}$,

$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.

$\delta + \frac{\delta^2}{2} + \frac{\delta^{100}}{2^2} + \frac{\delta^{100}}{2^3}$.

$\vdots$

How Will δ' and δ Relate

What if the δ increase as follows;

δ,

$\delta + \frac{\delta^{100}}{2}$,

$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.

$\delta + \frac{\delta^2}{2} + \frac{\delta^{100}}{2^2} + \frac{\delta^{100}}{2^3}$.

$\vdots$

Then density is always

How Will δ' and δ Relate

What if the δ increase as follows;

δ,

$\delta + \frac{\delta^{100}}{2}$,

$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.

$\delta + \frac{\delta^2}{2} + \frac{\delta^{100}}{2^2} + \frac{\delta^{100}}{2^3}$.

$\vdots$

Then density is always

$< \delta + \delta^{100} \sum_{i=1}^{\infty} \frac{1}{2^i} = \delta + \delta^{100}$.

How Will δ' and δ Relate

What if the δ increase as follows;
δ,
$\delta + \frac{\delta^{100}}{2}$,
$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.
$\delta + \frac{\delta^2}{2} + \frac{\delta^{100}}{2^2} + \frac{\delta^{100}}{2^3}$.
$\vdots$
Then density is always
$< \delta + \delta^{100} \sum_{i=1}^{\infty} \frac{1}{2^i} = \delta + \delta^{100}$.
If $\delta = \frac{1}{10}$ then density is always $< \frac{1}{10} + \frac{1}{10^{100}}$.

How Will δ' and δ Relate

What if the δ increase as follows;

δ,

$\delta + \frac{\delta^{100}}{2}$,

$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.

$\delta + \frac{\delta^2}{2} + \frac{\delta^{100}}{2^2} + \frac{\delta^{100}}{2^3}$.

$\vdots$

Then density is always

$< \delta + \delta^{100} \sum_{i=1}^{\infty} \frac{1}{2^i} = \delta + \delta^{100}$.

If $\delta = \frac{1}{10}$ then density is always $< \frac{1}{10} + \frac{1}{10^{100}}$.

Much less than 0.67.

How Will δ' and δ Relate

What if the δ increase as follows;

δ,

$\delta + \frac{\delta^{100}}{2}$,

$\delta + \frac{\delta^{100}}{2} + \frac{\delta^{100}}{2^2}$.

$\delta + \frac{\delta^2}{2} + \frac{\delta^{100}}{2^2} + \frac{\delta^{100}}{2^3}$.

$\vdots$

Then density is always

$< \delta + \delta^{100} \sum_{i=1}^{\infty} \frac{1}{2^i} = \delta + \delta^{100}$.

If $\delta = \frac{1}{10}$ then density is always $< \frac{1}{10} + \frac{1}{10^{100}}$.

Much less than 0.67.

We increase δ enough so that the density goes to ∞.

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.
Let

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.
Let

$\delta_0 = \delta$.

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.
Let

$\delta_0 = \delta$.

$\delta_n = \delta_{n-1} + \frac{\delta_{n-1}^2}{80}$
Clearly δ_n is increasing.

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.
Let

$\delta_0 = \delta$.

$\delta_n = \delta_{n-1} + \frac{\delta_{n-1}^2}{80}$
Clearly δ_n is increasing.

Hence
$\delta_n \geq \delta_{n-1} + \frac{\delta_0^2}{80}$.

How Will δ' and δ Relate?

We will later get $\delta' \ge \delta + \frac{\delta^2}{80}$.
Let

$\delta_0 = \delta$.

$\delta_n = \delta_{n-1} + \frac{\delta_{n-1}^2}{80}$
Clearly δ_n is increasing.

Hence
$\delta_n \ge \delta_{n-1} + \frac{\delta_0^2}{80}$.
One can show by induction that

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.
Let

$\delta_0 = \delta$.

$\delta_n = \delta_{n-1} + \frac{\delta_{n-1}^2}{80}$
Clearly δ_n is increasing.

Hence
$\delta_n \geq \delta_{n-1} + \frac{\delta_0^2}{80}$.
One can show by induction that

$\delta_n \geq \delta_0 + n\frac{\delta_0^2}{80}$.

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.
Let

$\delta_0 = \delta$.

$\delta_n = \delta_{n-1} + \frac{\delta_{n-1}^2}{80}$
Clearly δ_n is increasing.

Hence
$\delta_n \geq \delta_{n-1} + \frac{\delta_0^2}{80}$.
One can show by induction that

$\delta_n \geq \delta_0 + n\frac{\delta_0^2}{80}$.

Take $n = \left\lceil \frac{80}{\delta_0^2} \right\rceil$ to get
$\delta_n \geq \delta_0 + 1$.

How Will δ' and δ Relate?

We will later get $\delta' \geq \delta + \frac{\delta^2}{80}$.
Let

$\delta_0 = \delta$.

$\delta_n = \delta_{n-1} + \frac{\delta_{n-1}^2}{80}$
Clearly δ_n is increasing.

Hence
$\delta_n \geq \delta_{n-1} + \frac{\delta_0^2}{80}$.
One can show by induction that

$\delta_n \geq \delta_0 + n\frac{\delta_0^2}{80}$.

Take $n = \left\lceil \frac{80}{\delta_0^2} \right\rceil$ to get
$\delta_n \geq \delta_0 + 1$.

Hence $\lim^{n\to\infty} \delta_n = \infty$.

We Will Operate in $\mathbb{Z}_N$, not $[N]$

We will prove the following:
Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

We Will Operate in $\mathbb{Z}_N$, not $[N]$

We will prove the following:

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.

We Will Operate in $\mathbb{Z}_N$, not $[N]$

We will prove the following:

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.

Objection! What if the 3-AP is $N-2, N-1, 0$? Then we don't have a 3-AP in $[N]$ like we want to.

We Will Operate in $\mathbb{Z}_N$, not $[N]$

We will prove the following:

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.

Objection! What if the 3-AP is $N-2, N-1, 0$? Then we don't have a 3-AP in $[N]$ like we want to.

Next slide will deal with this.

Why $\mathbb{Z}_N$ Is Fine

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

Why $\mathbb{Z}_N$ Is Fine

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds
For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.

Why $\mathbb{Z}_N$ Is Fine

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds
For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.
We assume 3 divides N.

Why $\mathbb{Z}_N$ Is Fine

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds

For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.

We assume 3 divides N.

View A as

$A \cap \{0, \ldots, N/3\} \cup \{N/3 + 1, \ldots, 2N/3\} \cup \{2N/3, \ldots, N-1\}$.

Why $\mathbb{Z}_N$ Is Fine

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds
For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.
We assume 3 divides N.

View A as
$A \cap \{0, \ldots, N/3\} \cup \{N/3 + 1, \ldots, 2N/3\} \cup \{2N/3, \ldots, N - 1\}$.
Case 1 The density of $A \cap \{N/3 + 1, \ldots, 2N/3\}$ is $\geq \delta/5$. Then do the proof on $A \cap \{N/3 + 1, \ldots, 2N/3\}$ is $\geq \delta/5$. Will get a legit 3-AP

Why $\mathbb{Z}_N$ Is Fine

Roth's Theorem For all $\delta > 0$ there exists $N = N(\delta)$ such that the following holds
For all $A \subseteq \mathbb{Z}_N$ of density $\geq \delta$, A has a 3-AP.
We assume 3 divides N.

View A as
$A \cap \{0, \ldots, N/3\} \cup \{N/3 + 1, \ldots, 2N/3\} \cup \{2N/3, \ldots, N-1\}$.
Case 1 The density of $A \cap \{N/3 + 1, \ldots, 2N/3\}$ is $\geq \delta/5$. Then do the proof on $A \cap \{N/3 + 1, \ldots, 2N/3\}$ is $\geq \delta/5$. Will get a legit 3-AP

Case 2 The density of $A \cap \{N/3 + 1, \ldots, 2N/3\}$ is $< \delta/5$. One can show that either $A \cap \{0, \ldots, N/3\}$ or $A \cap \{N/3 + 1, \ldots, 2N/3\}$ is $> \delta$ (by enough so that if we keep doing this get > 0.67).

Detour:
Discrete Fourier Transform

Discrete Fourier Transform

Discrete Fourier Transform (DFT) Let $N \in \mathbb{N}$. Let $\chi(z) = e^{\frac{-2\pi iz}{N}}$. Then, the DFT of a function $f : \mathbb{Z}_N \to \mathbb{C}$, denoted as $\widehat{f}$, is defined as:

$$\widehat{f}(m) = \sum_{x=0}^{N-1} f(x)\chi(-mx)$$

We will use usually use this with f being the indicator function of a set $A \subseteq \mathbb{Z}_N$.

QUESTIONS FOR KELIN ON DFT-CAN WAIT

1) How does the DFT compare to the usual FT?

2) In the usual FT is some coefficient being small significant?

3) What is the intuition behind Plancherel equation? Is the proof easy- just pushing symbols around, or not? I think there is a similar equation for FT. Is the proof similar? Identical?

4) You have *Convolution (unconventional)* What is this unconventional? What is the intuition behind convolution? Is the proof easy- just pushing symbols around, or not? I think there is a similar equation for FT. Is the proof similar? Identical?

KELIN- Possible CHANGES FOR THE SLIDES-CAN WAIT

1) We might want to NOT use $\chi(z)$ and just use $\frac{-2\pi iz}{N}$.

2) In Math (though perhaps not in the papers you've been reading) z usually goes through the complex numbers. Hence we might want to define use x instead of z.

3) These are all LATER changes that we MIGHT NOT MAKE and are NOT THAT IMPORTANT. But I note them here to remind us.

Large and Small Fourier Coefficients

Let $A \subseteq \mathbb{Z}_N$. We view A as a 0-1 valued function in the obvious way.

Large and Small Fourier Coefficients

Let $A \subseteq \mathbb{Z}_N$. We view A as a 0-1 valued function in the obvious way.
$\widehat{A}(m) = \sum_{x=0}^{N-1} A(x)\chi(-mx)$

Large and Small Fourier Coefficients

Let $A \subseteq \mathbb{Z}_N$. We view A as a 0-1 valued function in the obvious way.

$\widehat{A}(m) = \sum_{x=0}^{N-1} A(x)\chi(-mx)$

Note that $\widehat{A}(0) = \sum_{x=0}^{N-1} A(x)\chi(0) = \sum_{x=0}^{N-1} A(x) = |A|$.

Large and Small Fourier Coefficients

Let $A \subseteq \mathbb{Z}_N$. We view A as a 0-1 valued function in the obvious way.

$\widehat{A}(m) = \sum_{x=0}^{N-1} A(x)\chi(-mx)$

Note that $\widehat{A}(0) = \sum_{x=0}^{N-1} A(x)\chi(0) = \sum_{x=0}^{N-1} A(x) = |A|$.

Informal Fact

Large and Small Fourier Coefficients

Let $A \subseteq \mathbb{Z}_N$. We view A as a 0-1 valued function in the obvious way.

$\widehat{A}(m) = \sum_{x=0}^{N-1} A(x)\chi(-mx)$

Note that $\widehat{A}(0) = \sum_{x=0}^{N-1} A(x)\chi(0) = \sum_{x=0}^{N-1} A(x) = |A|$.

Informal Fact

1) If $\max_{x\neq 0} \widehat{A}(x)$ is small then A looks random.

Large and Small Fourier Coefficients

Let $A \subseteq \mathbb{Z}_N$. We view A as a 0-1 valued function in the obvious way.

$\widehat{A}(m) = \sum_{x=0}^{N-1} A(x)\chi(-mx)$

Note that $\widehat{A}(0) = \sum_{x=0}^{N-1} A(x)\chi(0) = \sum_{x=0}^{N-1} A(x) = |A|$.

Informal Fact

1) If $\max_{x\neq 0} \widehat{A}(x)$ is small then A looks random.

1) If $\max_{x\neq 0} \widehat{A}(x)$ is large then A looks non-random.

Large and Small Fourier Coefficients

Let $A \subseteq \mathbb{Z}_N$. We view A as a 0-1 valued function in the obvious way.

$\widehat{A}(m) = \sum_{x=0}^{N-1} A(x)\chi(-mx)$

Note that $\widehat{A}(0) = \sum_{x=0}^{N-1} A(x)\chi(0) = \sum_{x=0}^{N-1} A(x) = |A|$.

Informal Fact

1) If $\max_{x \neq 0} \widehat{A}(x)$ is small then A looks random.

1) If $\max_{x \neq 0} \widehat{A}(x)$ is large then A looks non-random.

See next few slide for examples.

Small Fourier Coefficients

Let A be the set of quadratic Residues mod 199. This is a random-looking set.

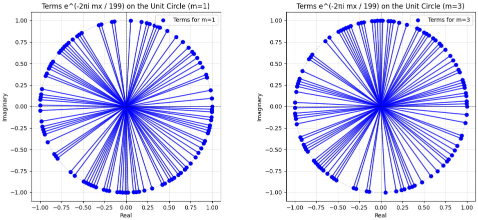

Figure: Left: Summands of $\widehat{A}(1)$. Right: Summands of $\widehat{A}(3)$

Left $\widehat{A}(1) = \sum_{x=0}^{198} A(x)\chi(-x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(1)$ is small.

Small Fourier Coefficients

Let A be the set of quadratic Residues mod 199. This is a random-looking set.

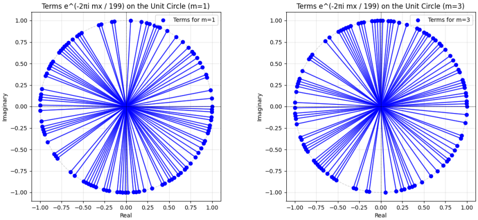

Figure: Left: Summands of $\widehat{A}(1)$. Right: Summands of $\widehat{A}(3)$

Left $\widehat{A}(1) = \sum_{x=0}^{198} A(x)\chi(-x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(1)$ is small.

Right $\widehat{A}(3) = \sum_{x=0}^{198} A(x)\chi(-3x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(3)$ is small.

Small Fourier Coefficients

Let A be the set of quadratic Residues mod 199. This is a random-looking set.

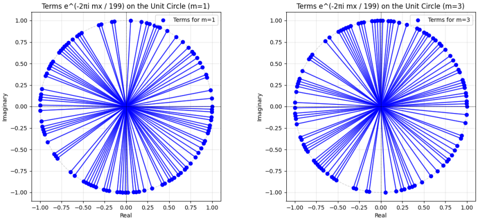

Figure: Left: Summands of $\widehat{A}(1)$. Right: Summands of $\widehat{A}(3)$

Left $\widehat{A}(1) = \sum_{x=0}^{198} A(x)\chi(-x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(1)$ is small.

Right $\widehat{A}(3) = \sum_{x=0}^{198} A(x)\chi(-3x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(3)$ is small.

All of the $\widehat{A}(m)$ for $m \neq 0$ are small.

Large Fourier Coefficients

We look at a non-random set A and two of its Fourier Coefficients.

Large Fourier Coefficients

We look at a non-random set A and two of its Fourier Coefficients.

The set A is: formed as follows.

Large Fourier Coefficients

We look at a non-random set A and two of its Fourier Coefficients.

The set A is: formed as follows.

Take the union of the following sets.
$\{10, 20, \ldots, 190\}$ (an AP- not random)

Large Fourier Coefficients

We look at a non-random set A and two of its Fourier Coefficients.

The set A is: formed as follows.

Take the union of the following sets.
$\{10, 20, \ldots, 190\}$ (an AP- not random)

$\{16, 26, 36, \ldots, 186\}$ (an AP- not random)

Large Fourier Coefficients

We look at a non-random set A and two of its Fourier Coefficients.

The set A is: formed as follows.

Take the union of the following sets.
$\{10, 20, \ldots, 190\}$ (an AP- not random)

$\{16, 26, 36, \ldots, 186\}$ (an AP- not random)

$\{17, 18, 59\}$ (Some noise tossed in)

Large Fourier Coefficients

Let A be the AP from the prior slide.

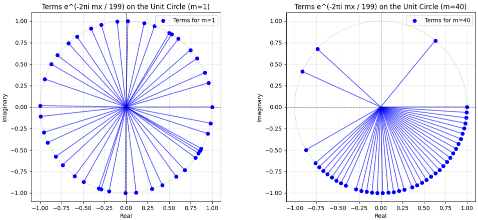

Figure: Left: Summands of $\widehat{A}(1)$. Right: Summands of $\widehat{A}(40)$

Left $\widehat{A}(1) = \sum_{x=0}^{N} A(x)\chi(-x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(1)$ is small.

Large Fourier Coefficients

Let A be the AP from the prior slide.

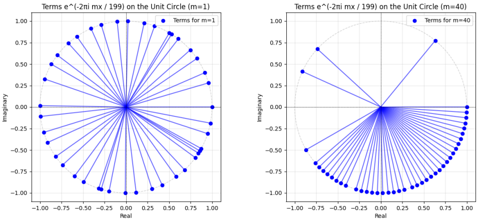

Figure: Left: Summands of $\widehat{A}(1)$. Right: Summands of $\widehat{A}(40)$

Left $\widehat{A}(1) = \sum_{x=0}^{N} A(x)\chi(-x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(1)$ is small.

Right $\widehat{A}(40) = \sum_{x=0}^{198} A(x)\chi(-40x)$. The blue dots on the circle are the summands. Note that they mostly **do not** cancel out, so $\widehat{A}(40)$ is large.

Large Fourier Coefficients

Let A be the AP from the prior slide.

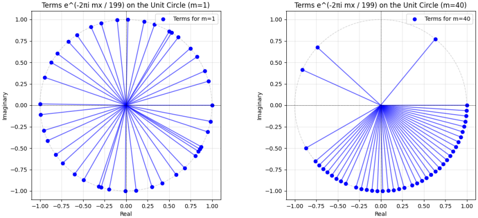

Figure: Left: Summands of $\widehat{A}(1)$. Right: Summands of $\widehat{A}(40)$

Left $\widehat{A}(1) = \sum_{x=0}^{N} A(x)\chi(-x)$. The blue dots on the circle are the summands. Note that they mostly cancel out, so $\widehat{A}(1)$ is small.

Right $\widehat{A}(40) = \sum_{x=0}^{198} A(x)\chi(-40x)$. The blue dots on the circle are the summands. Note that they mostly **do not** cancel out, so $\widehat{A}(40)$ is large.

Non-Rand Since A is non-random, $\exists m \neq 0$, $\widehat{A}(m)$ large.

PROJECT-Write Programs For The Following

Random Sets Given N, Form $A = QR_N$, the set of quad residues mod N. Then find, $\forall m \in A - \{0\}$, $\widehat{A}(m)$. Find the max M Should have $M \ll |A|$.

Non-Rand Sets Given N and $a, d, L \in \mathbb{Z}_N$ $(d, L \neq 0)$, first form

$$A = \{a, a+d, \ldots, a+Ld\} \text{ The arithmetic is mod } N \;.$$

Then find, $\forall m \in A - \{0\}$, $\widehat{A}(m)$. Find the max M. Should have M large, perhaps close to $|A|$.

Non-Rand Sets? Given N and $x, y, L \in \mathbb{Z}_N$ $(d, L \neq 0)$, first form A a random union of x AP's of length y. Then find, $\forall m \in A - \{0\}$, $\widehat{A}(m)$. Find the max M. For which x, y is M small? large?

Plan For The Proof

Let Q be the number of 3-AP's in A.

Plan For The Proof

Let Q be the number of 3-AP's in A. We will obtain

$$Q = \frac{1}{N}|B|^2|A| + E$$

Plan For The Proof

Let Q be the number of 3-AP's in A. We will obtain

$$Q = \frac{1}{N}|B|^2|A| + E$$

where $|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B|$.

Plan For The Proof

Let Q be the number of 3-AP's in A. We will obtain

$$Q = \frac{1}{N}|B|^2|A| + E$$

where $|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B|$.

Case 1 $A \cap [N/3, 2N/3]$ has low density. Then one of $A \cap [0, N/3 - 1]$ or $\cap[2N/3 + 1, N]$ has density $> \delta$.

Plan For The Proof

Let Q be the number of 3-AP's in A. We will obtain

$$Q = \frac{1}{N}|B|^2|A| + E$$

where $|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B|$.

Case 1 $A \cap [N/3, 2N/3]$ has low density. Then one of $A \cap [0, N/3 - 1]$ or $\cap[2N/3 + 1, N]$ has density $> \delta$.

Case 2 $A \cap [N/3, 2N/3]$ has high density $> \delta$. has density $> \delta$.

Plan For The Proof

Let Q be the number of 3-AP's in A. We will obtain

$$Q = \frac{1}{N}|B|^2|A| + E$$

where $|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B|$.

Case 1 $A \cap [N/3, 2N/3]$ has low density. Then one of $A \cap [0, N/3 - 1]$ or $\cap[2N/3 + 1, N]$ has density $> \delta$.

Case 2 $A \cap [N/3, 2N/3]$ has high density $> \delta$. has density $> \delta$.

Case 3 $A \cap [N/3, 2N/3]$ has medium density and $\max_{m \neq 0} |\widehat{A}(m)|$ is "small". Then $|Q| \geq 1$, so A has a 3-AP.

Plan For The Proof

Let Q be the number of 3-AP's in A. We will obtain

$$Q = \frac{1}{N}|B|^2|A| + E$$

where $|E| \le \max_{m \neq 0} |\widehat{A}(m)||B|$.

Case 1 $A \cap [N/3, 2N/3]$ has low density. Then one of $A \cap [0, N/3 - 1]$ or $\cap[2N/3 + 1, N]$ has density $> \delta$.

Case 2 $A \cap [N/3, 2N/3]$ has high density $> \delta$. has density $> \delta$.

Case 3 $A \cap [N/3, 2N/3]$ has medium density and $\max_{m \neq 0} |\widehat{A}(m)|$ is "small". Then $|Q| \ge 1$, so A has a 3-AP.

Case 4 $\max_{m \neq 0} |\widehat{A}(m)|$ is "large" (possibly negative so Q could be 0) then there is a long AP P such that A has density $> \delta$ in P.

Initial Setup

1) We assume that N is odd so that 2 is invertible in Z_N. If N is even, we may replace N with $N + 1$ leading to a negligible change in density.

Initial Setup

1) We assume that N is odd so that 2 is invertible in Z_N. If N is even, we may replace N with $N+1$ leading to a negligible change in density.

2) Let $B = A \cap [\frac{N}{3}, \frac{2N}{3})$.

Initial Setup

1) We assume that N is odd so that 2 is invertible in Z_N. If N is even, we may replace N with $N+1$ leading to a negligible change in density.

2) Let $B = A \cap [\frac{N}{3}, \frac{2N}{3})$.

3) If x, y, z is a 3-AP in Z_N such that $x + z \equiv 2y \pmod{N}$, with $x, y \in B$ and $z \in A$, then it is also a 3-AP in $\mathbb{N}$.

Initial Setup

1) We assume that N is odd so that 2 is invertible in Z_N. If N is even, we may replace N with $N+1$ leading to a negligible change in density.

2) Let $B = A \cap [\frac{N}{3}, \frac{2N}{3})$.

3) If x, y, z is a 3-AP in Z_N such that $x + z \equiv 2y \pmod{N}$, with $x, y \in B$ and $z \in A$, then it is also a 3-AP in $\mathbb{N}$.

4) Q be the number of 3-APs in A where $x, y \in B$.

Initial Setup

1) We assume that N is odd so that 2 is invertible in Z_N. If N is even, we may replace N with $N+1$ leading to a negligible change in density.

2) Let $B = A \cap [\frac{N}{3}, \frac{2N}{3})$.

3) If x, y, z is a 3-AP in Z_N such that $x + z \equiv 2y \pmod{N}$, with $x, y \in B$ and $z \in A$, then it is also a 3-AP in $\mathbb{N}$.

4) Q be the number of 3-APs in A where $x, y \in B$.

5) We will express Q as a summation involving A and B.

Initial Setup

1) We assume that N is odd so that 2 is invertible in Z_N. If N is even, we may replace N with $N+1$ leading to a negligible change in density.

2) Let $B = A \cap [\frac{N}{3}, \frac{2N}{3})$.

3) If x, y, z is a 3-AP in Z_N such that $x + z \equiv 2y \pmod{N}$, with $x, y \in B$ and $z \in A$, then it is also a 3-AP in $\mathbb{N}$.

4) Q be the number of 3-APs in A where $x, y \in B$.

5) We will express Q as a summation involving A and B.

6) We will express Q as a summation involving $\widehat{A}$ and $\widehat{B}$.

Q As a Summation Involving A and B

All summations are from 0 to $N - 1$ with some conditions added.

Q As a Summation Involving A and B

All summations are from 0 to $N-1$ with some conditions added.

$Q = \sum_{x,y,z,x+z\equiv 2y} B(x)B(y)A(z)$

Q As a Summation Involving A and B

All summations are from 0 to $N-1$ with some conditions added.

$Q = \sum_{x,y,z,x+z\equiv 2y} B(x)B(y)A(z)$

We want to have a summation without conditions. Consider

Q As a Summation Involving A and B

All summations are from 0 to $N - 1$ with some conditions added.

$Q = \sum_{x,y,z,x+z\equiv 2y} B(x)B(y)A(z)$

We want to have a summation without conditions. Consider

$\sum_m \sum_{x,y,z} B(x)B(y)A(z)\chi(-m(x+z-2y))$

Q As a Summation Involving A and B

All summations are from 0 to $N-1$ with some conditions added.

$Q = \sum_{x,y,z,x+z\equiv 2y} B(x)B(y)A(z)$

We want to have a summation without conditions. Consider

$\sum_m \sum_{x,y,z} B(x)B(y)A(z)\chi(-m(x+z-2y))$

When $x+z=2y$, $\chi(-m(x+z-2y)=1$ so we get NQ as a subsum.

Q As a Summation Involving A and B

All summations are from 0 to $N-1$ with some conditions added.

$Q = \sum_{x,y,z,x+z\equiv 2y} B(x)B(y)A(z)$

We want to have a summation without conditions. Consider

$\sum_m \sum_{x,y,z} B(x)B(y)A(z)\chi(-m(x+z-2y))$

When $x+z=2y$, $\chi(-m(x+z-2y)) = 1$ so we get NQ as a subsum.

We claim that all of the other terms cancel out.

KELIN: WHY DO THE OTHER TERMS CANCEL OUT?

Q As a Summation Involving A and B

All summations are from 0 to $N-1$ with some conditions added.

$Q = \sum_{x,y,z,x+z\equiv 2y} B(x)B(y)A(z)$

We want to have a summation without conditions. Consider

$\sum_m \sum_{x,y,z} B(x)B(y)A(z)\chi(-m(x+z-2y))$

When $x+z=2y$, $\chi(-m(x+z-2y)=1$ so we get NQ as a subsum.

We claim that all of the other terms cancel out.

KELIN: WHY DO THE OTHER TERMS CANCEL OUT?

Hence

$\sum_m \sum_{x,y,z,m} B(x)B(y)A(z)\chi(-m(x+z-2y)) = NQ$

Q As a Summation Involving A and B

All summations are from 0 to $N-1$ with some conditions added.

$Q = \sum_{x,y,z,x+z\equiv 2y} B(x)B(y)A(z)$

We want to have a summation without conditions. Consider

$\sum_m \sum_{x,y,z} B(x)B(y)A(z)\chi(-m(x+z-2y))$

When $x+z=2y$, $\chi(-m(x+z-2y)=1$ so we get NQ as a subsum.

We claim that all of the other terms cancel out.

KELIN: WHY DO THE OTHER TERMS CANCEL OUT?

Hence

$\sum_m \sum_{x,y,z,m} B(x)B(y)A(z)\chi(-m(x+z-2y)) = NQ$

So

$Q = \frac{1}{N}\sum_{x,y,z,m} B(x)B(y)A(z)\chi(-m(x+z-2y))$

Q As a Summation Involving $\widehat{A}$ and $\widehat{B}$

$Q = \frac{1}{N} \sum_{x,y,z,m} B(x)B(y)A(z)\chi(-m(x+z-2y))$

KELIN: FILL IN HOW DO YOU GET FROM THE LINE ABOVE TO THE LINE BELOW

$Q = \frac{1}{N} \sum_{m} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the Sum Into a Big Part and an Error Term

$$Q = \frac{1}{N} \sum_m \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$$

Split the Sum Into a Big Part and an Error Term

$Q = \frac{1}{N} \sum_m \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the sum into two parts:

Split the Sum Into a Big Part and an Error Term

$Q = \frac{1}{N}\sum_m \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the sum into two parts:

$\boldsymbol{m = 0}$ We get $\frac{1}{N}\sum_m \widehat{B}(0)\widehat{B}(0)\widehat{A}(0) = \frac{1}{N}|B|^2|A|$.

Split the Sum Into a Big Part and an Error Term

$Q = \frac{1}{N}\sum_m \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the sum into two parts:

$\boldsymbol{m = 0}$ We get $\frac{1}{N}\sum_m \widehat{B}(0)\widehat{B}(0)\widehat{A}(0) = \frac{1}{N}|B|^2|A|$.

$\boldsymbol{m \neq 0}$ We get $\frac{1}{N}\sum_{m\neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the Sum Into a Big Part and an Error Term

$Q = \frac{1}{N}\sum_m \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the sum into two parts:

$\boldsymbol{m = 0}$ We get $\frac{1}{N}\sum_m \widehat{B}(0)\widehat{B}(0)\widehat{A}(0) = \frac{1}{N}|B|^2|A|$.

$\boldsymbol{m \neq 0}$ We get $\frac{1}{N}\sum_{m\neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

We denote this sum by E for error.

Split the Sum Into a Big Part and an Error Term

$Q = \frac{1}{N}\sum_m \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the sum into two parts:

$\boldsymbol{m = 0}$ We get $\frac{1}{N}\sum_m \widehat{B}(0)\widehat{B}(0)\widehat{A}(0) = \frac{1}{N}|B|^2|A|$.

$\boldsymbol{m \neq 0}$ We get $\frac{1}{N}\sum_{m\neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$
We denote this sum by E for error.

Despite the name, it might be large.
If $|E|$ is large and negative then you may get $|Q| \leq 0$.

Split the Sum Into a Big Part and an Error Term

$Q = \frac{1}{N} \sum_m \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Split the sum into two parts:

$\boldsymbol{m = 0}$ We get $\frac{1}{N} \sum_m \widehat{B}(0)\widehat{B}(0)\widehat{A}(0) = \frac{1}{N}|B|^2|A|$.

$\boldsymbol{m \neq 0}$ We get $\frac{1}{N} \sum_{m \neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$
We denote this sum by E for error.

Despite the name, it might be large.
If $|E|$ is large and negative then you may get $|Q| \leq 0$.

We will analyze E very carefully.

Bounding $|E|$ Using Elementary Math

$E = \frac{1}{N} \sum_{m \neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

Bounding $|E|$ Using Elementary Math

$$E = \frac{1}{N} \sum_{m \neq 0} \widehat{B}(m) \widehat{B}(-2m) \widehat{A}(m)$$

$$E = \frac{1}{N} \sum_{m \neq 0} \widehat{A}(m) \widehat{B}(m) \widehat{B}(-2m)$$

Bounding $|E|$ Using Elementary Math

$$E = \frac{1}{N}\sum_{m\neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$$

$$E = \frac{1}{N}\sum_{m\neq 0} \widehat{A}(m)\widehat{B}(m)\widehat{B}(-2m)$$

$$|E| = \frac{1}{N}\sum_{m\neq 0} |\widehat{A}(m)|\widehat{B}(m)\widehat{B}(-2m)|$$

Bounding $|E|$ Using Elementary Math

$$E = \frac{1}{N} \sum_{m \neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$$

$$E = \frac{1}{N} \sum_{m \neq 0} \widehat{A}(m)\widehat{B}(m)\widehat{B}(-2m)$$

$$|E| = \frac{1}{N} \sum_{m \neq 0} |\widehat{A}(m)|\widehat{B}(m)\widehat{B}(-2m)|$$

$$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_{m \neq 0} |\widehat{B}(m)\widehat{B}(-2m)|$$

Bounding $|E|$ Using Elementary Math

$E = \frac{1}{N}\sum_{m\neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

$E = \frac{1}{N}\sum_{m\neq 0} \widehat{A}(m)\widehat{B}(m)\widehat{B}(-2m)$

$|E| = \frac{1}{N}\sum_{m\neq 0} |\widehat{A}(m)||\widehat{B}(m)\widehat{B}(-2m)|$

$|E| \leq \frac{1}{N}\max_{m\neq 0} |\widehat{A}(m)|\sum_{m\neq 0} |\widehat{B}(m)\widehat{B}(-2m)|$

When $m = 0$, $\widehat{B}(m)\widehat{B}(2m) = |B|^2 \geq 0$. Since the last line is an inequality we can add the $m = 0$ back into it.

Bounding $|E|$ Using Elementary Math

$E = \frac{1}{N} \sum_{m \neq 0} \widehat{B}(m)\widehat{B}(-2m)\widehat{A}(m)$

$E = \frac{1}{N} \sum_{m \neq 0} \widehat{A}(m)\widehat{B}(m)\widehat{B}(-2m)$

$|E| = \frac{1}{N} \sum_{m \neq 0} |\widehat{A}(m)||\widehat{B}(m)\widehat{B}(-2m)|$

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_{m \neq 0} |\widehat{B}(m)\widehat{B}(-2m)|$

When $m = 0$, $\widehat{B}(m)\widehat{B}(2m) = |B|^2 \geq 0$. Since the last line is an inequality we can add the $m = 0$ back into it.

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_{m} |\widehat{B}(m)\widehat{B}(-2m)|$

Bounding $|E|$ Using The Cauchy-Schwarts Inequality

$$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)\widehat{B}(-2m)|$$

Bounding $|E|$ Using The Cauchy-Schwarts Inequality

$|E| \le \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)\widehat{B}(-2m)|$

Recall that Cauchy-Schwartz inequality

Bounding $|E|$ Using The Cauchy-Schwarts Inequality

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)\widehat{B}(-2m)|$

Recall that Cauchy-Schwartz inequality

If $x, y \in \mathbb{C}^n$, $|\sum_{i=1}^n x_i y_i| \leq (\sum_{i=1}^n |x_i^2|)^{1/2} (\sum_{i=1}^n |y_i^2|)^{1/2}$.

Bounding $|E|$ Using The Cauchy-Schwarts Inequality

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)\widehat{B}(-2m)|$

Recall that Cauchy-Schwartz inequality

If $x, y \in \mathbb{C}^n$, $|\sum_{i=1}^n x_i y_i| \leq (\sum_{i=1}^n |x_i^2|)^{1/2} (\sum_{i=1}^n |y_i^2|)^{1/2}$.

Apply this to $\sum_m \widehat{B}(m)\widehat{B}(-2m)|$ to get

Bounding $|E|$ Using The Cauchy-Schwarts Inequality

$|E| \leq \frac{1}{N} \max_{m\neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)\widehat{B}(-2m)|$

Recall that Cauchy-Schwartz inequality

If $x, y \in \mathbb{C}^n$, $|\sum_{i=1}^n x_i y_i| \leq (\sum_{i=1}^n |x_i^2|)^{1/2}(\sum_{i=1}^n |y_i^2|)^{1/2}$.

Apply this to $\sum_m \widehat{B}(m)\widehat{B}(-2m)|$ to get

$|E| \leq \frac{1}{N} \max_{m\neq 0} |\widehat{A}(m)|(\sum_m |\widehat{B}(m)^2|)^{1/2}(\sum_m |\widehat{B}(-2m)|^2)^{1/2}$.

Bounding $|E|$ Using that 2 is Invertible Mod N

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (\sum_m |\widehat{B}(m)^2|)^{1/2} (\sum_m |\widehat{B}(-2m)|^2)^{1/2}.$

Bounding $|E|$ Using that 2 is Invertible Mod N

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (\sum_m |\widehat{B}(m)^2|)^{1/2} (\sum_m |\widehat{B}(-2m)|^2)^{1/2}$.

Since 2 is invertible mod N we have

Bounding $|E|$ Using that 2 is Invertible Mod N

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (\sum_m |\widehat{B}(m)^2|)^{1/2} (\sum_m |\widehat{B}(-2m)|^2)^{1/2}$.

Since 2 is invertible mod N we have

$$\sum_m |\widehat{B}(-2m)| = \sum_m |\widehat{B}(m)|$$

Bounding $|E|$ Using that 2 is Invertible Mod N

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (\sum_m |\widehat{B}(m)^2|)^{1/2} (\sum_m |\widehat{B}(-2m)|^2)^{1/2}$.

Since 2 is invertible mod N we have

$$\sum_m |\widehat{B}(-2m)| = \sum_m |\widehat{B}(m)|$$

Hence

Bounding $|E|$ Using that 2 is Invertible Mod N

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (\sum_m |\widehat{B}(m)^2|)^{1/2} (\sum_m |\widehat{B}(-2m)|^2)^{1/2}$.

Since 2 is invertible mod N we have

$$\sum_m |\widehat{B}(-2m)| = \sum_m |\widehat{B}(m)|$$

Hence

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

Bounding $|E|$ Using that 2 is Invertible Mod N

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| (\sum_m |\widehat{B}(m)^2|)^{1/2} (\sum_m |\widehat{B}(-2m)|^2)^{1/2}$.

Since 2 is invertible mod N we have

$$\sum_m |\widehat{B}(-2m)| = \sum_m |\widehat{B}(m)|$$

Hence

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

We want to bound $|\sum_m |\widehat{B}(m)^2|$ in terms of B.

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

"Recall" Plancherel Theorem

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

“Recall” Plancherel Theorem

$\sum_{x \in Z_N} |f(x)|^2 = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

"Recall" Plancherel Theorem

$\sum_{x \in Z_N} |f(x)|^2 = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

In the case where f is an indicator function for a set we get

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

"Recall" Plancherel Theorem

$\sum_{x \in Z_N} |f(x)|^2 = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

In the case where f is an indicator function for a set we get

$\sum_{x \in Z_N} f(x) = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

"Recall" Plancherel Theorem

$\sum_{x \in Z_N} |f(x)|^2 = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

In the case where f is an indicator function for a set we get

$\sum_{x \in Z_N} f(x) = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

Apply this to $\frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$ to get

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

"Recall" Plancherel Theorem

$\sum_{x \in Z_N} |f(x)|^2 = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

In the case where f is an indicator function for a set we get

$\sum_{x \in Z_N} f(x) = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

Apply this to $\frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$ to get

$|E| \leq \max_{m \neq 0} |\widehat{A}(m)| \sum_m B(m) \leq \max_{m \neq 0} |\widehat{A}(m)||B|$

Bounding $|E|$ Using Plancherel Theorem

$|E| \leq \frac{1}{N} \max_{m \neq 0} |\widehat{A}(m)| \sum_m |\widehat{B}(m)^2|$

"Recall" Plancherel Theorem

$\sum_{x \in Z_N} |f(x)|^2 = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

In the case where f is an indicator function for a set we get

$\sum_{x \in Z_N} f(x) = \frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$

Apply this to $\frac{1}{N} \sum_{m \in Z_N} |\widehat{f}(m)|^2$ to get

$|E| \leq \max_{m \neq 0} |\widehat{A}(m)| \sum_m B(m) \leq \max_{m \neq 0} |\widehat{A}(m)||B|$

We are done bounding $|E|$.

Four Cases

The proof now goes into four cases:

Four Cases

The proof now goes into four cases:

Case 1 $|B| < \frac{|A|}{5}$. We show $A \cap [0, \frac{N}{3} - 1]$ or $A \cap [\frac{2N}{3}, N]$ has density $\geq \frac{6\delta}{5}$.

Four Cases

The proof now goes into four cases:

Case 1 $|B| < \frac{|A|}{5}$. We show $A \cap [0, \frac{N}{3} - 1]$ or $A \cap [\frac{2N}{3}, N]$ has density $\geq \frac{6\delta}{5}$.

Case 2 $|B| > \frac{11|A|}{30}$. We show B has density $\frac{11\delta}{10}$.

Four Cases

The proof now goes into four cases:

Case 1 $|B| < \frac{|A|}{5}$. We show $A \cap [0, \frac{N}{3} - 1]$ or $A \cap [\frac{2N}{3}, N]$ has density $\geq \frac{6\delta}{5}$.

Case 2 $|B| > \frac{11|A|}{30}$. We show B has density $\frac{11\delta}{10}$.

Case 3 $\frac{|A|}{5} \leq |B| \leq \frac{11|A|}{30}$ and $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$. We show that, if N is large enough, $Q \geq 1$. This is not quite enough to get a 3-AP in A but we will deal with that later.

Four Cases

The proof now goes into four cases:

Case 1 $|B| < \frac{|A|}{5}$. We show $A \cap [0, \frac{N}{3} - 1]$ or $A \cap [\frac{2N}{3}, N]$ has density $\geq \frac{6\delta}{5}$.

Case 2 $|B| > \frac{11|A|}{30}$. We show B has density $\frac{11\delta}{10}$.

Case 3 $\frac{|A|}{5} \leq |B| \leq \frac{11|A|}{30}$ and $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$. We show that, if N is large enough, $Q \geq 1$. This is not quite enough to get a 3-AP in A but we will deal with that later.

Case 4 $\max_{m \neq 0} |\widehat{A}(m)| > \frac{\delta^2 N}{10}$. (We do not need info on $|B|$.). There is a long AP P such that the density of A in P is $\geq \delta + \frac{\delta^2}{40}$.

Four Cases

The proof now goes into four cases:

Case 1 $|B| < \frac{|A|}{5}$. We show $A \cap [0, \frac{N}{3} - 1]$ or $A \cap [\frac{2N}{3}, N]$ has density $\geq \frac{6\delta}{5}$.

Case 2 $|B| > \frac{11|A|}{30}$. We show B has density $\frac{11\delta}{10}$.

Case 3 $\frac{|A|}{5} \leq |B| \leq \frac{11|A|}{30}$ and $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$. We show that, if N is large enough, $Q \geq 1$. This is not quite enough to get a 3-AP in A but we will deal with that later.

Case 4 $\max_{m \neq 0} |\widehat{A}(m)| > \frac{\delta^2 N}{10}$. (We do not need info on $|B|$.). There is a long AP P such that the density of A in P is $\geq \delta + \frac{\delta^2}{40}$.

After the 4 cases we recap and see why we have the theorem.

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$A = (A \cap [0, \frac{N}{3} - 1]) \cup B \cup (A \cap [\frac{2N}{3}, N])$, and $|B| < \frac{|A|}{5}$ so

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$A = (A \cap [0, \frac{N}{3} - 1]) \cup B \cup (A \cap [\frac{2N}{3}, N])$, and $|B| < \frac{|A|}{5}$ so

$$\left(A \cap \left[0, \frac{N}{3} - 1\right]\right) \cup \left(A \cap \left[\frac{2N}{3}, N\right]\right) \geq \frac{4|A|}{5}.$$

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$A = (A \cap [0, \frac{N}{3} - 1]) \cup B \cup (A \cap [\frac{2N}{3}, N])$, and $|B| < \frac{|A|}{5}$ so

$$\left(A \cap \left[0, \frac{N}{3} - 1\right]\right) \cup \left(A \cap \left[\frac{2N}{3}, N\right]\right) \geq \frac{4|A|}{5}.$$

We can assume $A \cap [0, \frac{N}{3} - 1] \geq \frac{2|A|}{5}$.

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$A = (A \cap [0, \frac{N}{3} - 1]) \cup B \cup (A \cap [\frac{2N}{3}, N])$, and $|B| < \frac{|A|}{5}$ so

$$\left(A \cap \left[0, \frac{N}{3} - 1\right]\right) \cup \left(A \cap \left[\frac{2N}{3}, N\right]\right) \geq \frac{4|A|}{5}.$$

We can assume $A \cap [0, \frac{N}{3} - 1] \geq \frac{2|A|}{5}$.

Since$|A| \geq \delta N$ we have $\frac{2|A|}{5} \geq \frac{2\delta N}{5}$.

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$A = (A \cap [0, \frac{N}{3} - 1]) \cup B \cup (A \cap [\frac{2N}{3}, N])$, and $|B| < \frac{|A|}{5}$ so

$$\left(A \cap \left[0, \frac{N}{3} - 1\right]\right) \cup \left(A \cap \left[\frac{2N}{3}, N\right]\right) \ge \frac{4|A|}{5}.$$

We can assume $A \cap [0, \frac{N}{3} - 1] \ge \frac{2|A|}{5}$.

Since$|A| \ge \delta N$ we have $\frac{2|A|}{5} \ge \frac{2\delta N}{5}$.

$$A \cap \left[0, \frac{N}{3} - 1\right] \ge \frac{2|A|}{5} \ge \frac{2\delta N}{5} = (6\delta/5)N/3.$$

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$A = (A \cap [0, \frac{N}{3} - 1]) \cup B \cup (A \cap [\frac{2N}{3}, N])$, and $|B| < \frac{|A|}{5}$ so

$$\left(A \cap \left[0, \frac{N}{3} - 1\right]\right) \cup \left(A \cap \left[\frac{2N}{3}, N\right]\right) \ge \frac{4|A|}{5}.$$

We can assume $A \cap [0, \frac{N}{3} - 1] \ge \frac{2|A|}{5}$.

Since$|A| \ge \delta N$ we have $\frac{2|A|}{5} \ge \frac{2\delta N}{5}$.

$$A \cap \left[0, \frac{N}{3} - 1\right] \ge \frac{2|A|}{5} \ge \frac{2\delta N}{5} = (6\delta/5)N/3.$$

Hence $A \cap [0, \frac{N}{3} - 1]$ has density $6\delta/5$.

Case 1: $|B| < \frac{|A|}{5}$

Case 1 $|B| < \frac{|A|}{5}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$A = (A \cap [0, \frac{N}{3} - 1]) \cup B \cup (A \cap [\frac{2N}{3}, N])$, and $|B| < \frac{|A|}{5}$ so

$$\left(A \cap \left[0, \frac{N}{3} - 1\right]\right) \cup \left(A \cap \left[\frac{2N}{3}, N\right]\right) \geq \frac{4|A|}{5}.$$

We can assume $A \cap [0, \frac{N}{3} - 1] \geq \frac{2|A|}{5}$.

Since$|A| \geq \delta N$ we have $\frac{2|A|}{5} \geq \frac{2\delta N}{5}$.

$$A \cap \left[0, \frac{N}{3} - 1\right] \geq \frac{2|A|}{5} \geq \frac{2\delta N}{5} = (6\delta/5)N/3.$$

Hence $A \cap [0, \frac{N}{3} - 1]$ has density $6\delta/5$.

That is all we need.

Case 2: $|B| > \frac{11|A|}{30}$

Case 2 $|B| > \frac{11|A|}{30}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

Case 2: $|B| > \frac{11|A|}{30}$

Case 2 $|B| > \frac{11|A|}{30}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$|B| > \frac{11|A|}{30} \geq \frac{11\delta N}{30} = \frac{11\delta}{10}\frac{N}{3}$.

Case 2: $|B| > \frac{11|A|}{30}$

Case 2 $|B| > \frac{11|A|}{30}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$|B| > \frac{11|A|}{30} \geq \frac{11\delta N}{30} = \frac{11\delta}{10}\frac{N}{3}$.

Since $B \subseteq [\frac{N}{3}, \frac{2N}{3} - 1]$, B is a set of density $\frac{11}{10}$.

Case 2: $|B| > \frac{11|A|}{30}$

Case 2 $|B| > \frac{11|A|}{30}$. Recall that $B = A \cap [\frac{N}{3}, \frac{2N}{3} - 1]$.

$|B| > \frac{11|A|}{30} \geq \frac{11\delta N}{30} = \frac{11\delta}{10}\frac{N}{3}$.

Since $B \subseteq [\frac{N}{3}, \frac{2N}{3} - 1]$, B is a set of density $\frac{11}{10}$.

That is all we need.

Case 3: $\frac{|A|}{5} \leq |B| \leq \frac{11|A|}{30}$ & $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

Case 3: $\frac{|A|}{5} \leq |B| \leq \frac{11|A|}{30}$ & $\max_{m\neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

$$|Q| = \frac{1}{N}|B|^2|A| + E.$$

Case 3: $\frac{|A|}{5} \leq |B| \leq \frac{11|A|}{30}$ & $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

$|Q| = \frac{1}{N}|B|^2|A| + E$. Always True.

Case 3: $\frac{|A|}{5} \le |B| \le \frac{11|A|}{30}$ & $\max_{m\neq 0}|\widehat{A}(m)| \le \frac{\delta^2 N}{10}$

$|Q| = \frac{1}{N}|B|^2|A| + E$. Always True.

$|E| \le \max_{m\neq 0}|\widehat{A}(m)||B|$.

Case 3: $\frac{|A|}{5} \le |B| \le \frac{11|A|}{30}$ & $\max_{m\neq 0} |\widehat{A}(m)| \le \frac{\delta^2 N}{10}$

$|Q| = \frac{1}{N}|B|^2|A| + E$. Always True.

$|E| \le \max_{m\neq 0} |\widehat{A}(m)||B|$. Always True.

Case 3: $\frac{|A|}{5} \le |B| \le \frac{11|A|}{30}$ & $\max_{m \neq 0} |\widehat{A}(m)| \le \frac{\delta^2 N}{10}$

$|Q| = \frac{1}{N}|B|^2|A| + E$. Always True.

$|E| \le \max_{m \neq 0} |\widehat{A}(m)||B|$. Always True.

Plan

Case 3: $\frac{|A|}{5} \le |B| \le \frac{11|A|}{30}$ & $\max_{m\ne 0} |\widehat{A}(m)| \le \frac{\delta^2 N}{10}$

$|Q| = \frac{1}{N}|B|^2|A| + E$. Always True.

$|E| \le \max_{m\ne 0} |\widehat{A}(m)||B|$. Always True.

Plan

We want to show $Q \ge 1$ (This is not quite enough, but we deal with it later.)

Case 3: $\frac{|A|}{5} \leq |B| \leq \frac{11|A|}{30}$ & $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

$|Q| = \frac{1}{N}|B|^2|A| + E$. Always True.

$|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B|$. Always True.

Plan

We want to show $Q \geq 1$ (This is not quite enough, but we deal with it later.)

1) We use $|B| \geq \frac{|A|}{5}$ to show that $\frac{1}{N}|B|^2|A|$ is large.

Case 3: $\frac{|A|}{5} \le |B| \le \frac{11|A|}{30}$ & $\max_{m\ne 0} |\widehat{A}(m)| \le \frac{\delta^2 N}{10}$

$|Q| = \frac{1}{N}|B|^2|A| + E$. Always True.

$|E| \le \max_{m\ne 0} |\widehat{A}(m)||B|$. Always True.

Plan

We want to show $Q \ge 1$ (This is not quite enough, but we deal with it later.)

1) We use $|B| \ge \frac{|A|}{5}$ to show that $\frac{1}{N}|B|^2|A|$ is large.

2) We use $|B| \le \frac{11|A|}{30}$ and $\max_{m\ne 0} \widehat{A}(m)| \le \frac{\delta^2 N}{10}$ to show $|E|$ is small.

1) Using $|B| \geq \frac{|A|}{5}$

1) Using $|B| \geq \frac{|A|}{5}$

Since $|B| \geq \frac{|A|}{5}$ we have

1) Using $|B| \geq \frac{|A|}{5}$

Since $|B| \geq \frac{|A|}{5}$ we have

$$\frac{1}{N}|B|^2|A| \geq \frac{|A|^3}{25N}.$$

1) Using $|B| \geq \frac{|A|}{5}$

Since $|B| \geq \frac{|A|}{5}$ we have

$$\frac{1}{N}|B|^2|A| \geq \frac{|A|^3}{25N}.$$

Since $|A| \geq \delta N$ we have

1) Using $|B| \geq \frac{|A|}{5}$

Since $|B| \geq \frac{|A|}{5}$ we have

$$\frac{1}{N}|B|^2|A| \geq \frac{|A|^3}{25N}.$$

Since $|A| \geq \delta N$ we have

$$\frac{|A|^3}{25N} \geq \frac{\delta^3 N^2}{25}.$$

1) Using $|B| \geq \frac{|A|}{5}$

Since $|B| \geq \frac{|A|}{5}$ we have

$$\frac{1}{N}|B|^2|A| \geq \frac{|A|^3}{25N}.$$

Since $|A| \geq \delta N$ we have

$$\frac{|A|^3}{25N} \geq \frac{\delta^3 N^2}{25}.$$

Ushot

1) Using $|B| \geq \frac{|A|}{5}$

Since $|B| \geq \frac{|A|}{5}$ we have

$$\frac{1}{N}|B|^2|A| \geq \frac{|A|^3}{25N}.$$

Since $|A| \geq \delta N$ we have

$$\frac{|A|^3}{25N} \geq \frac{\delta^3 N^2}{25}.$$

Ushot

$$\frac{1}{N}|B|^2|A| \geq \frac{\delta^3 N^2}{25}.$$

2) Using $|B| \le \frac{11|A|}{30}$ and $\max_{m\neq 0} |\widehat{A}(m)| \le \frac{\delta^2 N}{10}$

2) Using $|B| \leq \frac{11|A|}{30}$ and $\max_{m\neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

$|E| \leq \max_{m\neq 0} |\widehat{A}(m)||B|.$

2) Using $|B| \leq \frac{11|A|}{30}$ and $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

$|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B|$.

Since $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$ and $|B| \leq \frac{11|A|}{30}$

2) Using $|B| \leq \frac{11|A|}{30}$ and $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

$|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B|$.

Since $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$ and $|B| \leq \frac{11|A|}{30}$

$$|E| \leq \max_{m \neq 0} |\widehat{A}(m)||B| \leq \frac{\delta^2 N}{10} \times \frac{11|A|}{30} \leq \frac{\delta^2 N}{10} \times \frac{11\delta N}{30} = \frac{11\delta^3 N^2}{300}$$

Lower Bound on $|Q|$

$$|Q| = |B|^2|A| + E \geq \frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300}$$

Lower Bound on $|Q|$

$$|Q| = |B|^2|A| + E \geq \frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300}$$

Want N such that $|Q| \geq 1$.

Lower Bound on $|Q|$

$$|Q| = |B|^2|A| + E \geq \frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300}$$

Want N such that $|Q| \geq 1$.

Here is the subtle point we alluded to earlier. Q is the set of all 3-AP's in A. This includes 3-APs of the form x, x, x. So we really want $Q - |A| \geq 1$. Since $|A| \sim \delta N$ we really need $Q - \delta N \geq 1$.

Lower Bound on $|Q|$

$$|Q| = |B|^2|A| + E \geq \frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300}$$

Want N such that $|Q| \geq 1$.

Here is the subtle point we alluded to earlier. Q is the set of all 3-AP's in A. This includes 3-APs of the form x, x, x. So we really want $Q - |A| \geq 1$. Since $|A| \sim \delta N$ we really need $Q - \delta N \geq 1$.

$\frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300} - \delta N \geq 1$

Lower Bound on $|Q|$

$$|Q| = |B|^2|A| + E \geq \frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300}$$

Want N such that $|Q| \geq 1$.

Here is the subtle point we alluded to earlier. Q is the set of all 3-AP's in A. This includes 3-APs of the form x, x, x. So we really want $Q - |A| \geq 1$. Since $|A| \sim \delta N$ we really need $Q - \delta N \geq 1$.

$\frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300} - \delta N \geq 1$

$(\frac{\delta^3}{25} - \frac{11\delta^3}{300})N^2 - \delta N \geq 1$

Lower Bound on $|Q|$

$$|Q| = |B|^2|A| + E \geq \frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300}$$

Want N such that $|Q| \geq 1$.

Here is the subtle point we alluded to earlier. Q is the set of all 3-AP's in A. This includes 3-APs of the form x, x, x. So we really want $Q - |A| \geq 1$. Since $|A| \sim \delta N$ we really need $Q - \delta N \geq 1$.

$\frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300} - \delta N \geq 1$

$(\frac{\delta^3}{25} - \frac{11\delta^3}{300})N^2 - \delta N \geq 1$

$\frac{\delta^3}{300} N^2 - \delta N \geq 1.$

Lower Bound on $|Q|$

$$|Q| = |B|^2|A| + E \geq \frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300}$$

Want N such that $|Q| \geq 1$.

Here is the subtle point we alluded to earlier. Q is the set of all 3-AP's in A. This includes 3-APs of the form x, x, x. So we really want $Q - |A| \geq 1$. Since $|A| \sim \delta N$ we really need $Q - \delta N \geq 1$.

$\frac{\delta^3 N^2}{25} - \frac{11\delta^3 N^2}{300} - \delta N \geq 1$

$(\frac{\delta^3}{25} - \frac{11\delta^3}{300})N^2 - \delta N \geq 1$

$\frac{\delta^3}{300}N^2 - \delta N \geq 1.$

We leave it to the reader to determine N large enough so that this inequality holds.

Case 4: $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

1) Let r be such that $|\widehat{A}(r)|$ is maximized.

Case 4: $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

1) Let r be such that $|\widehat{A}(r)|$ is maximized.
2) Let $x = |\widehat{A}(r)|$.

Case 4: $\max_{m\neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

1) Let r be such that $|\widehat{A}(r)|$ is maximized.
2) Let $x = |\widehat{A}(r)|$.
3) Note that $x > \frac{\delta^2 N}{10}$

Case 4: $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

1) Let r be such that $|\widehat{A}(r)|$ is maximized.
2) Let $x = |\widehat{A}(r)|$.
3) Note that $x > \frac{\delta^2 N}{10}$

We will use these later.

Case 4: $\max_{m \neq 0} |\widehat{A}(m)| \leq \frac{\delta^2 N}{10}$

1) Let r be such that $|\widehat{A}(r)|$ is maximized.
2) Let $x = |\widehat{A}(r)|$.
3) Note that $x > \frac{\delta^2 N}{10}$

We will use these later.

We want a large AP P st A has density $> \delta$ in it.

The Difference d For The AP P We Seek

Let r be as on the last slide.

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

Map $x \in \mathbb{Z}_N$ to the interval that $rx \pmod{N}$ is in.

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

Map $x \in \mathbb{Z}_N$ to the interval that $rx \pmod{N}$ is in.

Pigeonhole Principle: $\exists p < q$ that map to same interval.

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

Map $x \in \mathbb{Z}_N$ to the interval that $rx \pmod{N}$ is in.

Pigeonhole Principle: $\exists p < q$ that map to same interval.

Hence $r(p-q) \le \sqrt{N} \pmod{N}$.

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

Map $x \in \mathbb{Z}_N$ to the interval that $rx \pmod{N}$ is in.

Pigeonhole Principle: $\exists p < q$ that map to same interval.

Hence $r(p-q) \leq \sqrt{N} \pmod{N}$. Let $d = p - q$.

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

Map $x \in \mathbb{Z}_N$ to the interval that $rx \pmod{N}$ is in.

Pigeonhole Principle: $\exists p < q$ that map to same interval.

Hence $r(p-q) \le \sqrt{N} \pmod{N}$. Let $d = p - q$.

We can assume $\frac{\sqrt{N}}{6} \in \mathbb{N}$.

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

Map $x \in \mathbb{Z}_N$ to the interval that $rx \pmod{N}$ is in.

Pigeonhole Principle: $\exists p < q$ that map to same interval.

Hence $r(p-q) \leq \sqrt{N} \pmod{N}$. Let $d = p - q$.

We can assume $\frac{\sqrt{N}}{6} \in \mathbb{N}$.

Let P be the AP

The Difference d For The AP P We Seek

Let r be as on the last slide.

Divide $\mathbb{Z}_N$ into roughly $\sqrt{N}$ intervals of size roughly $\sqrt{N}$.

Map $x \in \mathbb{Z}_N$ to the interval that $rx \pmod{N}$ is in.

Pigeonhole Principle: $\exists p < q$ that map to same interval.

Hence $r(p-q) \le \sqrt{N} \pmod{N}$. Let $d = p - q$.

We can assume $\frac{\sqrt{N}}{6} \in \mathbb{N}$.

Let P be the AP

$$\left\{ \frac{-d\sqrt{N}}{6}, \frac{-d\sqrt{N}}{6} + d, \frac{-d\sqrt{N}}{6} + 2d, \cdots, 0, d, 2d, \cdots, \frac{d\sqrt{N}}{6}. \right\}$$

DFT of P

P is

$$\left\{\frac{-d\sqrt{N}}{6}, \frac{-d\sqrt{N}}{6}+d, \frac{-d\sqrt{N}}{6}+2d, \cdots, 0, d, 2d, \cdots, \frac{d\sqrt{N}}{6}.\right\}$$

DFT of P

P is

$$\left\{ \frac{-d\sqrt{N}}{6}, \frac{-d\sqrt{N}}{6} + d, \frac{-d\sqrt{N}}{6} + 2d, \cdots, 0, d, 2d, \cdots, \frac{d\sqrt{N}}{6}. \right\}$$

We need information on $\chi(-rx)$ as $x \in P$.

DFT of P

P is

$$\left\{\frac{-d\sqrt{N}}{6}, \frac{-d\sqrt{N}}{6}+d, \frac{-d\sqrt{N}}{6}+2d, \cdots, 0, d, 2d, \cdots, \frac{d\sqrt{N}}{6}.\right\}$$

We need information on $\chi(-rx)$ as $x \in P$.
$\chi(-rx) = e^{2\pi irx/N}$

DFT of P

P is

$$\left\{ \frac{-d\sqrt{N}}{6}, \frac{-d\sqrt{N}}{6} + d, \frac{-d\sqrt{N}}{6} + 2d, \cdots, 0, d, 2d, \cdots, \frac{d\sqrt{N}}{6}. \right\}$$

We need information on $\chi(-rx)$ as $x \in P$.
$\chi(-rx) = e^{2\pi i rx/N}$
$\chi(-rx)$ depends on $rx \pmod{N}$

DFT of P

P is

$$\left\{ \frac{-d\sqrt{N}}{6}, \frac{-d\sqrt{N}}{6} + d, \frac{-d\sqrt{N}}{6} + 2d, \cdots, 0, d, 2d, \cdots, \frac{d\sqrt{N}}{6}. \right\}$$

We need information on $\chi(-rx)$ as $x \in P$.
$\chi(-rx) = e^{2\pi i rx/N}$
$\chi(-rx)$ depends on $rx \pmod N$
We know that $rd \leq \sqrt{N} \pmod N$.

DFT of P

P is

$$\left\{\frac{-d\sqrt{N}}{6}, \frac{-d\sqrt{N}}{6}+d, \frac{-d\sqrt{N}}{6}+2d, \cdots, 0, d, 2d, \cdots, \frac{d\sqrt{N}}{6}.\right\}$$

We need information on $\chi(-rx)$ as $x \in P$.
$\chi(-rx) = e^{2\pi irx/N}$
$\chi(-rx)$ depends on $rx \pmod N$
We know that $rd \le \sqrt{N} \pmod N$.
We know that $|x| \le \frac{d\sqrt{N}}{6}$.
KELIN: FINISH THIS FOR ME TO GET $|\widehat{P}(r) \ge |P|/2$.

Small Detour: Convolution

Def If $f, g \colon \mathbb{Z}_N \to \mathbb{C}$ then the **convolution** of f and g, denoted $f * g$, is a function from $: \mathbb{Z}_N \to \mathbb{C}$ defined

Small Detour: Convolution

Def If $f, g : \mathbb{Z}_N \to \mathbb{C}$ then the **convolution** of f and g, denoted $f * g$, is a function from $: \mathbb{Z}_N \to \mathbb{C}$ defined

$$(f * g)(x) = \sum_y f(y)g(x - y).$$

Thm For all m, $\widehat{f * g}(m) = \widehat{f}(m)\widehat{g}(m)$.