Essential Components in $\mathbb{F}_p[t]$

Zhenchao Ge & Thái Hoàng Lê

University of Mississippi

Oct. 26-27, 2019

7th annual Mississippi Discrete Math Workshop

For two sets A, B in an abelian group G, we denote

$$A \pm B = \{a \pm b : a \in A, b \in B\}.$$

and denote the k-fold sumset by

$$kA = A + \cdots + A \quad (k \text{ times}).$$

For two sets A, B in an abelian group G, we denote

$$A \pm B = \{a \pm b : a \in A, b \in B\}.$$

and denote the k-fold sumset by

$$kA = A + \cdots + A \quad (k \text{ times}).$$

If $A \subset G$, we denote $\#\{a : a \in A\}$ by $|A|$.

For two sets A, B in an abelian group G, we denote

$$A \pm B = \{a \pm b : a \in A, b \in B\}.$$

and denote the k-fold sumset by

$$kA = A + \cdots + A \quad (k \text{ times}).$$

If $A \subset G$, we denote $\#\{a : a \in A\}$ by $|A|$.

By the *density* of A in G, we mean $\frac{|A|}{|G|}$.

Essential Components in $\mathbb{N}$

Let $\mathbb{N}$ be the set of non-negative integers. For $A \subset \mathbb{N}$, we let

$$A(n) = \#\{a : a \in A, 1 \leq a \leq n\},$$

be the counting function of A.

Essential Components in $\mathbb{N}$

Let $\mathbb{N}$ be the set of non-negative integers. For $A \subset \mathbb{N}$, we let

$$A(n) = \#\{a : a \in A, 1 \leq a \leq n\},$$

be the counting function of A.

The *Schnirelmann density* $\sigma(A)$ is defined by

$$\sigma(A) = \inf_{n \geq 1} \frac{A(n)}{n}.$$

Essential Components in $\mathbb{N}$

Let $\mathbb{N}$ be the set of non-negative integers. For $A \subset \mathbb{N}$, we let

$$A(n) = \#\{a : a \in A, 1 \leq a \leq n\},$$

be the counting function of A.

The *Schnirelmann density* $\sigma(A)$ is defined by

$$\sigma(A) = \inf_{n \geq 1} \frac{A(n)}{n}.$$

Theorem (Schnirelmann's inequality, 1930)

$$\sigma(A+B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B), \qquad \textit{if } 0 \in A \cup B.$$

Essential Components in $\mathbb{N}$

Let $\mathbb{N}$ be the set of non-negative integers. For $A \subset \mathbb{N}$, we let

$$A(n) = \#\{a : a \in A, 1 \leq a \leq n\},$$

be the counting function of A.

The *Schnirelmann density* $\sigma(A)$ is defined by

$$\sigma(A) = \inf_{n \geq 1} \frac{A(n)}{n}.$$

Theorem (Schnirelmann's inequality, 1930)

$$\sigma(A + B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B), \qquad \textit{if } 0 \in A \cup B.$$

Essential Components in $\mathbb{N}$

Let $\mathbb{N}$ be the set of non-negative integers. For $A \subset \mathbb{N}$, we let

$$A(n) = \#\{a : a \in A, 1 \leq a \leq n\},$$

be the counting function of A.

The *Schnirelmann density* $\sigma(A)$ is defined by

$$\sigma(A) = \inf_{n \geq 1} \frac{A(n)}{n}.$$

Theorem (Schnirelmann's inequality, 1930)

$$\sigma(A+B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B), \qquad \textit{if } 0 \in A \cup B.$$

Schnirelmann proved that $cP = \mathbb{N}$, where $P = \{\text{primes}\} \cup \{0, 1\}$ and $c > 0$ is some constant, which was the first unconditional result on the Goldbach conjecture.

Essential Components in $\mathbb{N}$

Schnirelmann Density:

$$\sigma(A) = \inf_{n \geq 1} \frac{A(n)}{n}$$

Essential Components in $\mathbb{N}$

Schnirelmann Density:

$$\sigma(A) = \inf_{n \geq 1} \frac{A(n)}{n}$$

A set $H \subset \mathbb{N}$ is called a *Schnirelmann essential component* if

$$\sigma(A + H) > \sigma(A)$$

whenever $0 < \sigma(A) < 1$.

If $A \subset \mathbb{N}$, the *lower asymptotic density* $\underline{d}(A)$ is defined by

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{A(n)}{n}.$$

A set $H \subset \mathbb{N}$ is called an *asymptotic essential component* if

$$\underline{d}(A + H) > \underline{d}(A)$$

whenever $0 < \underline{d}(A) < 1$.

If $A \subset \mathbb{N}$, the *lower asymptotic density* $\underline{d}(A)$ is defined by

$$\underline{d}(A) = \liminf_{n \to \infty} \frac{A(n)}{n}.$$

A set $H \subset \mathbb{N}$ is called an *asymptotic essential component* if

$$\underline{d}(A + H) > \underline{d}(A)$$

whenever $0 < \underline{d}(A) < 1$.

Theorem (Plünnecke, 1969)

A set of integers is a Schnirelmann essential component if and only if it is an asymptotic essential component and it contains $\{0, 1\}$.

- Schnirelmann's inequality

$$\sigma(A+B) \geq \sigma(A) + \sigma(B)(1 - \sigma(A))$$

implies that any set with a positive Schnirelmann density is an essential component.

- Schnirelmann's inequality

$$\sigma(A+B) \geq \sigma(A) + \sigma(B)(1 - \sigma(A))$$

implies that any set with a positive Schnirelmann density is an essential component.

- Schnirelmann's inequality

$$\sigma(A+B) \geq \sigma(A) + \sigma(B)(1-\sigma(A))$$

  implies that any set with a positive Schnirelmann density is an essential component.

- Khinchin (1933) gave the first example of an essential component with density 0, which is the set of squares.

- Schnirelmann's inequality

$$\sigma(A+B) \geq \sigma(A) + \sigma(B)(1-\sigma(A))$$

  implies that any set with a positive Schnirelmann density is an essential component.

- Khinchin (1933) gave the first example of an essential component with density 0, which is the set of squares.

- Schnirelmann's inequality

$$\sigma(A+B) \geq \sigma(A) + \sigma(B)(1-\sigma(A))$$

  implies that any set with a positive Schnirelmann density is an essential component.

- Khinchin (1933) gave the first example of an essential component with density 0, which is the set of squares.

- Erdős (1936) proved that every basis is an essential component.

  A set H is an additive basis of order k if $kH = \mathbb{N}$ for some $k \in \mathbb{Z}^+$.

- Schnirelmann's inequality

$$\sigma(A+B) \geq \sigma(A) + \sigma(B)(1-\sigma(A))$$

implies that any set with a positive Schnirelmann density is an essential component.

- Khinchin (1933) gave the first example of an essential component with density 0, which is the set of squares.

- Erdős (1936) proved that every basis is an essential component.

A set H is an additive basis of order k if $kH = \mathbb{N}$ for some $k \in \mathbb{Z}^+$.

- Schnirelmann's inequality

$$\sigma(A+B) \geq \sigma(A) + \sigma(B)(1-\sigma(A))$$

implies that any set with a positive Schnirelmann density is an essential component.

- Khinchin (1933) gave the first example of an essential component with density 0, which is the set of squares.

- Erdős (1936) proved that every basis is an essential component.

A set H is an additive basis of order k if $kH = \mathbb{N}$ for some $k \in \mathbb{Z}^+$.

If H is an additive basis of order k, then $H(n) \gg n^{1/k}$.

Q: If H is an essential component, then how small can $H(n)$ be?

Q: If H is an essential component, then how small can $H(n)$ be?

Theorem (Linnik, 1942)

There is an essential component satisfying $H(n) = O(\exp(\log^{\frac{9}{10}} n))$, which hence is not a basis.

Q: If H is an essential component, then how small can $H(n)$ be?

Theorem (Linnik, 1942)

There is an essential component satisfying $H(n) = O(\exp(\log^{\frac{9}{10}} n))$, which hence is not a basis.

Q: If H is an essential component, then how small can $H(n)$ be?

Theorem (Linnik, 1942)

There is an essential component satisfying $H(n) = O(\exp(\log^{\frac{9}{10}} n))$*, which hence is not a basis.*

Theorem (Wirsing, 1976)

For every $\varepsilon > 0$ *there exists an essential component* H *with* $H(n) = O(\exp(\varepsilon\sqrt{\log n}\log\log n))$.

Q: If H is an essential component, then how small can $H(n)$ be?

Q: If H is an essential component, then how small can $H(n)$ be?

Theorem (Ruzsa, 1984)

For every $c > 0$ there exists an essential component H with $H(n) = O((\log n)^{1+c})$.

Q: If H is an essential component, then how small can $H(n)$ be?

Theorem (Ruzsa, 1984)

For every $c > 0$ there exists an essential component H with $H(n) = O((\log n)^{1+c})$.

Q: If H is an essential component, then how small can $H(n)$ be?

Theorem (Ruzsa, 1984)

For every $c > 0$ there exists an essential component H with $H(n) = O((\log n)^{1+c})$.

Ruzsa's construction is probabilistic.

Q: If H is an essential component, then how small can $H(n)$ be?

Theorem (Ruzsa, 1984)

For every $c > 0$ there exists an essential component H with $H(n) = O((\log n)^{1+c})$.

Ruzsa's construction is probabilistic.

Theorem (Ruzsa, 1984)

Suppose $H \subset \mathbb{N}$ such that for any $\varepsilon > 0$, $H(n) \leq (\log n)^{1+\varepsilon}$ holds infinitely often. Then there exists a set $A \subset \mathbb{N}$ such that

$$0 < \underline{d}(A) = \underline{d}(A + H) < 1.$$

Consequently, there does not exists an essential component H with $H(n) \ll (\log n)^{1+o(1)}$.

Essential components in $\mathbb{F}_p[t]$

Define $G := \mathbb{F}_p[t]$. For $A \subset G$, let

$$A_n = \{a : a \in A, \deg(a) < n\}.$$

In particular, $G_n = \{g : \deg(g) < n\}$.

Define $G := \mathbb{F}_p[t]$. For $A \subset G$, let

$$A_n = \{a : a \in A, \deg(a) < n\}.$$

In particular, $G_n = \{g : \deg(g) < n\}$.

The lower asymptotic density $\underline{d}(A)$ is defined by

$$\underline{d}(A) = \liminf_{n \to \infty} \frac{|A_n|}{p^n}.$$

Essential components in $\mathbb{F}_p[t]$

Define $G := \mathbb{F}_p[t]$. For $A \subset G$, let

$$A_n = \{a : a \in A, \deg(a) < n\}.$$

In particular, $G_n = \{g : \deg(g) < n\}$.

The lower asymptotic density $\underline{d}(A)$ is defined by

$$\underline{d}(A) = \liminf_{n \to \infty} \frac{|A_n|}{p^n}.$$

A set $H \subset G = \mathbb{F}_p[t]$ is an essential component if

$$\liminf_{n \to \infty} \frac{|H_n + A_n|}{p^n} > \underline{d}(A),$$

whenever $0 < \underline{d}(A) < 1$.

- H is an essential component in $\mathbb{N}$ if

$$\underline{d}(A+H) > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

- H is an essential component in $\mathbb{N}$ if

$$\underline{d}(A+H) > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

- $H \subset G = \mathbb{F}_p[t]$ is an essential component if

$$\liminf_{n\to\infty} \frac{|H_n + A_n|}{p^n} > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

- H is an essential component in $\mathbb{N}$ if

$$\underline{d}(A+H) > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

- $H \subset G = \mathbb{F}_p[t]$ is an essential component if

$$\liminf_{n\to\infty} \frac{|H_n + A_n|}{p^n} > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

Why not $\underline{d}(A+H) > \underline{d}(A)$?

- H is an essential component in $\mathbb{N}$ if

$$\underline{d}(A+H) > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

- $H \subset G = \mathbb{F}_p[t]$ is an essential component if

$$\liminf_{n\to\infty} \frac{|H_n + A_n|}{p^n} > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

Why not $\underline{d}(A+H) > \underline{d}(A)$?

Note $\mathbb{F}_p[t]$ is a group, in general we have $H_n + A_n \subsetneq (H+A)_n$.

- H is an essential component in $\mathbb{N}$ if

$$\underline{d}(A+H) > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

- $H \subset G = \mathbb{F}_p[t]$ is an essential component if

$$\liminf_{n\to\infty} \frac{|H_n + A_n|}{p^n} > \underline{d}(A), \qquad \text{whenever } 0 < \underline{d}(A) < 1.$$

Why not $\underline{d}(A+H) > \underline{d}(A)$?

Note $\mathbb{F}_p[t]$ is a group, in general we have $H_n + A_n \subsetneq (H+A)_n$.

In particular, if H is infinite, there exists a set A with $\underline{d}(A) = 0$ s.t.

$$A + H = G, \qquad \text{hence} \qquad \underline{d}(A+H) = \liminf_{n\to\infty} \frac{|(A+H)_n|}{p^n} = 1,$$

which is not interesting.

Essential components in $\mathbb{F}_p[t]$

Theorem (Erdős, 1936)

If $kH = \mathbb{N}$ for some positive integer k, then for all n,

$$(A+H)(n) \geq A(n) + \frac{A(n)}{2k}\left(1 - \frac{A(n)}{n}\right).$$

Essential components in $\mathbb{F}_p[t]$

Theorem (Erdős, 1936)

If $kH = \mathbb{N}$ for some positive integer k, then for all n,

$$(A + H)(n) \geq A(n) + \frac{A(n)}{2k}\left(1 - \frac{A(n)}{n}\right).$$

Essential components in $\mathbb{F}_p[t]$

Theorem (Erdős, 1936)

If $kH = \mathbb{N}$ for some positive integer k, then for all n,

$$(A+H)(n) \geq A(n) + \frac{A(n)}{2k}\left(1 - \frac{A(n)}{n}\right).$$

Burke proved the following analog of Erdős' theorem in $\mathbb{F}_p[t]$.

Theorem (Burke, 1984)

If $H \subset \mathbb{F}_p[t] = G$ and there exists a positive integer k s.t. $kH_n = G_n$ for all $n \in \mathbb{N}$, then

$$|A_n + H_n| \geq |A_n| + \frac{|A_n|}{k}\left(1 - \frac{|A_n|}{p^n}\right)$$

holds for all $n \in \mathbb{N}$.

Theorem (Ruzsa, 1984)

For every $c > 0$ there exists an essential component $H \subset \mathbb{N}$ with $H(n) = O((\log n)^{1+c})$.

Theorem (Ruzsa, 1984)

For every $c > 0$ *there exists an essential component* $H \subset \mathbb{N}$ *with* $H(n) = O((\log n)^{1+c})$.

Theorem (Ruzsa, 1984)

For every $c > 0$ *there exists an essential component* $H \subset \mathbb{N}$ *with* $H(n) = O((\log n)^{1+c})$.

We prove the following analog of Ruzsa's theorem.

Theorem (Ruzsa, 1984)

For every $c > 0$ there exists an essential component $H \subset \mathbb{N}$ with $H(n) = O((\log n)^{1+c})$.

We prove the following analog of Ruzsa's theorem.

Theorem 1 (G.-Lê)

For every $c > 0$, there exists an essential component $H \subset \mathbb{F}_p[t]$ such that $|H_n| = O_p(n^{1+c})$.

Theorem (Ruzsa, 1984)

For every $c > 0$ *there exists an essential component* $H \subset \mathbb{N}$ *with* $H(n) = O((\log n)^{1+c})$.

We prove the following analog of Ruzsa's theorem.

Theorem 1 (G.-Lê)

For every $c > 0$, *there exists an essential component* $H \subset \mathbb{F}_p[t]$ *such that* $|H_n| = O_p(n^{1+c})$.

Theorem (Ruzsa, 1984)

For every $c > 0$ there exists an essential component $H \subset \mathbb{N}$ with $H(n) = O((\log n)^{1+c})$.

We prove the following analog of Ruzsa's theorem.

Theorem 1 (G.-Lê)

For every $c > 0$, there exists an essential component $H \subset \mathbb{F}_p[t]$ such that $|H_n| = O_p(n^{1+c})$.

Our method is also probabilistic. We are not able to give an explicit essential component H with counting function $|H_n| = O_p(n^{1+c})$ for small c.

Theorem (Ruzsa, 1984)

Suppose $H \subset \mathbb{N}$ such that for any $\varepsilon > 0$, $H(n) \leq (\log n)^{1+\varepsilon}$ holds infinitely often. Then there exists a set $A \subset \mathbb{N}$ such that

$$0 < \underline{d}(A) = \underline{d}(A + H) < 1.$$

Theorem (Ruzsa, 1984)

Suppose $H \subset \mathbb{N}$ such that for any $\varepsilon > 0$, $H(n) \leq (\log n)^{1+\varepsilon}$ holds infinitely often. Then there exists a set $A \subset \mathbb{N}$ such that

$$0 < \underline{d}(A) = \underline{d}(A + H) < 1.$$

Theorem (Ruzsa, 1984)

Suppose $H \subset \mathbb{N}$ *such that for any* $\varepsilon > 0$, $H(n) \leq (\log n)^{1+\varepsilon}$ *holds infinitely often. Then there exists a set* $A \subset \mathbb{N}$ *such that*

$$0 < \underline{d}(A) = \underline{d}(A + H) < 1.$$

Theorem 2 (G.-Lê)

Suppose $H \subset \mathbb{F}_p[t]$ *such that for any* $\varepsilon > 0$, $|H_n| < n^{1+\varepsilon}$ *holds infinitely often. Then for any* $0 < \delta < 1$, *there exists a set* $A \subset \mathbb{F}_p[t]$ *such that*

$$\delta = \underline{d}(A) = \liminf_{n \to \infty} \frac{|A_n + H_n|}{p^n}.$$

- Our theorem is more precise than Ruzsa's in $\mathbb{N}$. $\underline{d}(A)$ can be any prescribed number.

- Our theorem is more precise than Ruzsa's in $\mathbb{N}$. $\underline{d}(A)$ can be any prescribed number.

- Our theorem is more precise than Ruzsa's in $\mathbb{N}$. $\underline{d}(A)$ can be any prescribed number.

- Our proof is not identical to Ruzsa's, since G is a group but $\mathbb{N}$ is a semi-group. The group structure simplifies some calculation, but it causes extra difficulties.

- Our theorem is more precise than Ruzsa's in $\mathbb{N}$. $\underline{d}(A)$ can be any prescribed number.

- Our proof is not identical to Ruzsa's, since G is a group but $\mathbb{N}$ is a semi-group. The group structure simplifies some calculation, but it causes extra difficulties.

- Our theorem is more precise than Ruzsa's in $\mathbb{N}$. $\underline{d}(A)$ can be any prescribed number.

- Our proof is not identical to Ruzsa's, since G is a group but $\mathbb{N}$ is a semi-group. The group structure simplifies some calculation, but it causes extra difficulties.

One difficulty:

For $a, b \in \mathbb{N}$, we always have $a + b \geq \max\{a, b\}$.

However, for $f, g \in \mathbb{F}_p[t]$, $\deg(f + g)$ could be any integer $\leq \deg(f)$.

Explicit examples of essential components

Theorem (Wirsing, 1976)

For every $c > 0$ there exists an essential component $H \subset \mathbb{N}$ with $H(n) = O(\exp(c\sqrt{\log n}\log\log n))$.

Explicit examples of essential components

Theorem (Wirsing, 1976)

For every $c > 0$ *there exists an essential component* $H \subset \mathbb{N}$ *with* $H(n) = O(\exp(c\sqrt{\log n}\log\log n))$.

Explicit examples of essential components

Theorem (Wirsing, 1976)

For every $c > 0$ there exists an essential component $H \subset \mathbb{N}$ with $H(n) = O(\exp(c\sqrt{\log n}\log\log n))$.

For $f = \sum_{j=0}^{n-1} a_j t^j$, we define $\mathrm{supp}(f) = \{j : a_j \neq 0\}$.

Explicit examples of essential components

Theorem (Wirsing, 1976)

For every $c > 0$ there exists an essential component $H \subset \mathbb{N}$ with $H(n) = O(\exp(c\sqrt{\log n} \log\log n))$.

For $f = \sum_{j=0}^{n-1} a_j t^j$, we define $\operatorname{supp}(f) = \{j : a_j \neq 0\}$.

Theorem 3 (G.-Lê)

Let $\mathbf{1}_n = 1 + t + \cdots t^{n-1}$ and $0 < c < 1$ be a real number. Then

$$H = \cup_{n=1}^{\infty} \{f + \mathbf{1}_n : |\operatorname{supp}(f)| \leq c\sqrt{n}\}$$

is an essential component of $\mathbb{F}_p[t]$ and $|H_n| = \exp\left(O_p(c\sqrt{n} \log n)\right)$.

Now we prove that for a large fixed n, there exists an essential component K in G_n such that $|K| \leq 25n \log p$ and for any $A \subset G_n$,

$$|K + A| \geq |A| + \frac{5}{9}|A| \left(1 - \frac{|A|}{p^n}\right).$$

A Fourier Analysis Tool:

Let $e_p(x) = e^{2\pi ix/p}$. Let $K \subset G_n$ and $(c_k)_{k\in K}$ be arbitrary complex numbers s. t. $\sum_{k\in K} c_k = 1$. Define

$$\xi(x) = \sum_{k\in K} c_k e_p(k \cdot x)$$

for $x \in G_n$.

A Fourier Analysis Tool:

Let $e_p(x) = e^{2\pi ix/p}$. Let $K \subset G_n$ and $(c_k)_{k\in K}$ be arbitrary complex numbers s. t. $\sum_{k\in K} c_k = 1$. Define

$$\xi(x) = \sum_{k\in K} c_k e_p(k \cdot x)$$

for $x \in G_n$.

If there exists $\eta \geq 0$ s.t. $|\xi(x)| \leq \eta$ for all $x \in G_n \setminus \{0\}$, then for any $A \subset G_n$, we have

$$|A + K| \geq |A| + (1 - \eta^2)|A| \left(1 - \frac{|A|}{p^n}\right).$$

A Fourier Analysis Tool:

Let $e_p(x) = e^{2\pi ix/p}$. Let $K \subset G_n$ and $(c_k)_{k\in K}$ be arbitrary complex numbers s. t. $\sum_{k\in K} c_k = 1$. Define

$$\xi(x) = \sum_{k\in K} c_k e_p(k \cdot x)$$

for $x \in G_n$.

If there exists $\eta \geq 0$ s.t. $|\xi(x)| \leq \eta$ for all $x \in G_n \setminus \{0\}$, then for any $A \subset G_n$, we have

$$|A + K| \geq |A| + (1 - \eta^2)|A| \left(1 - \frac{|A|}{p^n}\right).$$

Proof. Cauchy-Schwarz's inequality and Plancherel's identity.

The Idea of the Proof in G_n

Recall that $G = \mathbb{F}_p[t]$. Let $e_p(x) = e^{2\pi i x/p}$.

The Idea of the Proof in G_n

Recall that $G = \mathbb{F}_p[t]$. Let $e_p(x) = e^{2\pi i x/p}$.

Let $K \subset G_n$ and $(c_k)_{k \in K}$ be arbitrary complex numbers s. t. $\sum_{k \in K} c_k = 1$. Define

$$\xi(x) = \sum_{k \in K} c_k e_p(k \cdot x)$$

for $x \in G_n$.

The Idea of the Proof in G_n

Recall that $G = \mathbb{F}_p[t]$. Let $e_p(x) = e^{2\pi i x/p}$.

Let $K \subset G_n$ and $(c_k)_{k \in K}$ be arbitrary complex numbers s. t. $\sum_{k \in K} c_k = 1$. Define

$$\xi(x) = \sum_{k \in K} c_k e_p(k \cdot x)$$

for $x \in G_n$.

If there exists $\eta \geq 0$ s.t. $|\xi(x)| \leq \eta$ for all $x \in G_n \setminus \{0\}$, then for any $A \subset G_n$, we have

$$|A + K| \geq |A| + (1 - \eta^2)|A| \left(1 - \frac{|A|}{p^n}\right).$$

The Idea of the Proof in G_n

Recall that $G = \mathbb{F}_p[t]$. Let $e_p(x) = e^{2\pi i x/p}$.

Let $K \subset G_n$ and $(c_k)_{k\in K}$ be arbitrary complex numbers s. t. $\sum_{k\in K} c_k = 1$. Define

$$\xi(x) = \sum_{k\in K} c_k e_p(k \cdot x)$$

for $x \in G_n$.

If there exists $\eta \geq 0$ s.t. $|\xi(x)| \leq \eta$ for all $x \in G_n \setminus \{0\}$, then for any $A \subset G_n$, we have

$$|A + K| \geq |A| + (1 - \eta^2)|A| \left(1 - \frac{|A|}{p^n}\right).$$

Proof. Cauchy-Schwarz's inequality and Plancherel's identity.

Construction of the set K

Let $\{X_k\}_{k\in G_n}$ be a set of *independent* Bernoulli random variables s.t.

$$\mathbf{P}(X_k = 1) = \frac{\alpha n}{|G_n|}, \quad \text{and} \quad \mathbf{P}(X_k = 0) = 1 - \frac{\alpha n}{|G_n|},$$

where α is a bounded number that will be determined later.

Construction of the set K

Let $\{X_k\}_{k \in G_n}$ be a set of *independent* Bernoulli random variables s.t.

$$\mathbf{P}(X_k = 1) = \frac{\alpha n}{|G_n|}, \quad \text{and} \quad \mathbf{P}(X_k = 0) = 1 - \frac{\alpha n}{|G_n|},$$

where α is a bounded number that will be determined later.

Define

$$K := \{k \in G_n : X_k = 1\}.$$

Construction of the set K

Let $\{X_k\}_{k \in G_n}$ be a set of *independent* Bernoulli random variables s.t.

$$\mathbf{P}(X_k = 1) = \frac{\alpha n}{|G_n|}, \quad \text{and} \quad \mathbf{P}(X_k = 0) = 1 - \frac{\alpha n}{|G_n|},$$

where α is a bounded number that will be determined later.

Define

$$K := \{k \in G_n : X_k = 1\}.$$

In a high probability, K is the set we need.

After some standard calculation and using Chebyshev's inequality, we obtain that for any $\varepsilon > 0$

$$\mathbf{P}(||K| - \alpha n| \geq \varepsilon n) < \frac{\alpha}{\varepsilon^2 n} \to 0 \quad \text{as } n \to \infty. \tag{1}$$

After some standard calculation and using Chebyshev's inequality, we obtain that for any $\varepsilon > 0$

$$\mathbf{P}(||K| - \alpha n| \geq \varepsilon n) < \frac{\alpha}{\varepsilon^2 n} \to 0 \quad \text{as } n \to \infty. \tag{1}$$

For $x \in G_n \setminus \{0\}$, let

$$r(x) := \sum_{k \in G_n} X_k \, e_p(k \cdot x) = \sum_{k \in K} e_p(k \cdot x).$$

After some standard calculation and using Chebyshev's inequality, we obtain that for any $\varepsilon > 0$

$$\mathbf{P}(||K| - \alpha n| \geq \varepsilon n) < \frac{\alpha}{\varepsilon^2 n} \to 0 \quad \text{as } n \to \infty. \tag{1}$$

For $x \in G_n \setminus \{0\}$, let

$$r(x) := \sum_{k \in G_n} X_k \, e_p\,(k \cdot x) = \sum_{k \in K} \, e_p\,(k \cdot x).$$

One can calculate that

$$\mathbf{P}(\max_{x \neq 0} |r(x)| \geq \alpha n/2) \leq p^{-n/9} \to 0 \qquad \text{as } n \to \infty. \tag{2}$$

Goal: Find a sequence of complex number $(c_k)_{k\in K}$ with $\sum_{k\in K} c_k = 1$ such that

$$\max_{x\neq 0} |\xi(x)| = \left|\sum_{k\in K} c_k e_p(k\cdot t)\right| \leq \eta < 1. \tag{3}$$

Goal: Find a sequence of complex number $(c_k)_{k\in K}$ with $\sum_{k\in K} c_k = 1$ such that

$$\max_{x\neq 0} |\xi(x)| = \left|\sum_{k\in K} c_k e_p(k\cdot t)\right| \leq \eta < 1. \tag{3}$$

Let

$$c_k = \frac{X_k}{\sum_{k\in G_n} X_k} = \frac{X_k}{|K|}.$$

By (1) and (2), we can see that

$$\mathbf{P}\left(\max_{x\neq 0} |\xi(x)| \geq \frac{\alpha}{2(\alpha-\varepsilon)}\right) < \frac{\alpha}{\varepsilon^2 n} + \frac{1}{p^{n/9}} \to 0 \qquad \text{as } n\to\infty.$$

In particular, if take $\alpha = 20 \log p$ and let $\varepsilon = 5 \log p$, then

$$\mathbf{P}\left(\max_{x \neq 0} |\xi(x)| < \frac{2}{3}\right) > 1 - \frac{1}{p^{n/9}} - \frac{4}{5n \log p} \to 1, \qquad \text{as } n \to \infty.$$

In particular, if take $\alpha = 20 \log p$ and let $\varepsilon = 5 \log p$, then

$$\mathbf{P}\left(\max_{x \neq 0} |\xi(x)| < \frac{2}{3}\right) > 1 - \frac{1}{p^{n/9}} - \frac{4}{5n \log p} \to 1, \qquad \text{as } n \to \infty.$$

Therefore, in a high probably, $K = \{k : X_k = 1\}$ is an essential component in G_n with $|K| \leq 25n \log p$. □

In particular, if take $\alpha = 20 \log p$ and let $\varepsilon = 5 \log p$, then

$$\mathbf{P}\left(\max_{x \neq 0} |\xi(x)| < \frac{2}{3}\right) > 1 - \frac{1}{p^{n/9}} - \frac{4}{5n \log p} \to 1, \qquad \text{as } n \to \infty.$$

Therefore, in a high probably, $K = \{k : X_k = 1\}$ is an essential component in G_n with $|K| \leq 25n \log p$. □

Summary:

- The key of the proof is to find c_k s.t. $|\sum_{k \in K} c_k e_p(x \cdot k)|$ is uniformly small for all non-zero x.

In particular, if take $\alpha = 20\log p$ and let $\varepsilon = 5\log p$, then

$$\mathbf{P}\left(\max_{x\neq 0}|\xi(x)| < \frac{2}{3}\right) > 1 - \frac{1}{p^{n/9}} - \frac{4}{5n\log p} \to 1, \qquad \text{as } n \to \infty.$$

Therefore, in a high probably, $K = \{k : X_k = 1\}$ is an essential component in G_n with $|K| \leq 25n\log p$. $\square$

Summary:

- The key of the proof is to find c_k s.t. $|\sum_{k\in K} c_k e_p(x\cdot k)|$ is uniformly small for all non-zero x.

In particular, if take $\alpha = 20 \log p$ and let $\varepsilon = 5 \log p$, then

$$\mathbf{P}\left(\max_{x \neq 0} |\xi(x)| < \frac{2}{3}\right) > 1 - \frac{1}{p^{n/9}} - \frac{4}{5n \log p} \to 1, \qquad \text{as } n \to \infty.$$

Therefore, in a high probably, $K = \{k : X_k = 1\}$ is an essential component in G_n with $|K| \leq 25n \log p$. □

Summary:

- The key of the proof is to find c_k s.t. $|\sum_{k \in K} c_k e_p(x \cdot k)|$ is uniformly small for all non-zero x.
- Following this idea, we can prove the existence of an essential component in G, but using more complicated weight functions c_k.

In particular, if take $\alpha = 20 \log p$ and let $\varepsilon = 5 \log p$, then

$$\mathbf{P}\left(\max_{x \neq 0} |\xi(x)| < \frac{2}{3}\right) > 1 - \frac{1}{p^{n/9}} - \frac{4}{5n \log p} \to 1, \qquad \text{as } n \to \infty.$$

Therefore, in a high probably, $K = \{k : X_k = 1\}$ is an essential component in G_n with $|K| \leq 25n \log p$. $\square$

Summary:

- The key of the proof is to find c_k s.t. $|\sum_{k \in K} c_k e_p(x \cdot k)|$ is uniformly small for all non-zero x.
- Following this idea, we can prove the existence of an essential component in G, but using more complicated weight functions c_k.

In particular, if take $\alpha = 20 \log p$ and let $\varepsilon = 5 \log p$, then

$$\mathbf{P}\left(\max_{x \neq 0} |\xi(x)| < \frac{2}{3}\right) > 1 - \frac{1}{p^{n/9}} - \frac{4}{5n \log p} \to 1, \qquad \text{as } n \to \infty.$$

Therefore, in a high probably, $K = \{k : X_k = 1\}$ is an essential component in G_n with $|K| \leq 25 n \log p$. □

Summary:

- The key of the proof is to find c_k s.t. $|\sum_{k \in K} c_k e_p(x \cdot k)|$ is uniformly small for all non-zero x.
- Following this idea, we can prove the existence of an essential component in G, but using more complicated weight functions c_k.
- Note that for a fixed large n, there exists an essential component $H_n \subset G_n$ s.t. $|H_n| = O_p(n)$. However, in G, there is no essential component $H \subset G$ s.t. $|H_n| = O_p(n^{1+o(1)})$.

Thank You!