A bilinear Bogolyubov theorem, with applications

Thái Hoàng Lê[1] & Pierre-Yves Bienvenu[2]

[1]University of Mississippi

[2]Institut Camille Jordan

November 11, 2018

Part I: A bilinear Bogolyubov theorem

Subspaces in difference sets

If $A \subset X$, then the density of A in X is $\frac{|A|}{|X|}$.

Subspaces in difference sets

If $A \subset X$, then the density of A in X is $\frac{|A|}{|X|}$.

If $A \subset \mathbf{F}_p^n$ has density $\alpha > 0$, then $A - A$ should contain a large subspace.

Green 2005, Sanders 2010: If $A \subset \mathbf{F}_2^n$ has density $\alpha > 0$, then $A - A$ contains a subspace of dimension $\Omega(\alpha n)$.

Green 2005, Sanders 2010: If $A \subset \mathbf{F}_2^n$ has density $\alpha > 0$, then $A - A$ contains a subspace of dimension $\Omega(\alpha n)$.

However, finite codimension (i.e. dimension $n - c(\alpha)$) is impossible.

Green 2005, Sanders 2010: If $A \subset \mathbf{F}_2^n$ has density $\alpha > 0$, then $A - A$ contains a subspace of dimension $\Omega(\alpha n)$.

However, finite codimension (i.e. dimension $n - c(\alpha)$) is impossible.

Ruzsa 1991, Green 2005: The largest subspace guaranteed to be in $A - A$ cannot have codimension $c(\alpha)\sqrt{n}$ (i.e. dimension $n - c(\alpha)\sqrt{n}$).

Bogolyubov's theorem

The more sumsets we have, the larger subspace we can find.

Bogolyubov's theorem

The more sumsets we have, the larger subspace we can find.

Theorem (Bogolyubov 1939)

If $A \subset \mathbf{F}_p^n$ has density $\alpha > 0$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

Bogolyubov's theorem

The more sumsets we have, the larger subspace we can find.

Theorem (Bogolyubov 1939)

If $A \subset \mathbf{F}_p^n$ has density $\alpha > 0$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

Bogolyubov's theorem

The more sumsets we have, the larger subspace we can find.

Theorem (Bogolyubov 1939)

If $A \subset \mathbf{F}_p^n$ has density $\alpha > 0$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov proved for $A \subset \mathbf{Z}$, with subspaces replaced by Bohr sets.

Bogolyubov's theorem

The more sumsets we have, the larger subspace we can find.

Theorem (Bogolyubov 1939)

If $A \subset \mathbf{F}_p^n$ has density $\alpha > 0$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov proved for $A \subset \mathbf{Z}$, with subspaces replaced by Bohr sets.
- Bogolyubov's proof gives $c(\alpha) = O\left(\frac{1}{\alpha^2}\right)$.

Bogolyubov's theorem

The more sumsets we have, the larger subspace we can find.

Theorem (Bogolyubov 1939)

If $A \subset \mathbf{F}_p^n$ has density $\alpha > 0$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov proved for $A \subset \mathbf{Z}$, with subspaces replaced by Bohr sets.
- Bogolyubov's proof gives $c(\alpha) = O\left(\frac{1}{\alpha^2}\right)$.
- Sanders 2010: $c(\alpha) = O\left(\log^4 \frac{1}{\alpha}\right)$.

Bogolyubov's theorem

The more sumsets we have, the larger subspace we can find.

Theorem (Bogolyubov 1939)

If $A \subset \mathbf{F}_p^n$ has density $\alpha > 0$, then $A + A - A - A$ contains a subspace of codimension $c(\alpha)$.

- Bogolyubov proved for $A \subset \mathbf{Z}$, with subspaces replaced by Bohr sets.
- Bogolyubov's proof gives $c(\alpha) = O\left(\frac{1}{\alpha^2}\right)$.
- Sanders 2010: $c(\alpha) = O\left(\log^4 \frac{1}{\alpha}\right)$.
- If A is a subspace of density α, then $\mathrm{codim}(A) = \log_p \frac{1}{\alpha}$ and $A + A - A - A = A$. Thus we cannot do better than $O\left(\log \frac{1}{\alpha}\right)$.

We are interested in structures arising from subsets $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ of density $\alpha > 0$.

We are interested in structures arising from subsets $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ of density $\alpha > 0$.

Define

$$\begin{aligned}\phi_h A &= \{(x_1 - x_2, y) : (x_1, y), (x_2, y) \in A\},\\ \phi_v A &= \{(x, y_1 - y_2) : (x, y_1), (x, y_2) \in A\}.\end{aligned}$$

We are interested in structures arising from subsets $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ of density $\alpha > 0$.

Define

$$\phi_h A = \{(x_1 - x_2, y) : (x_1, y), (x_2, y) \in A\},$$
$$\phi_v A = \{(x, y_1 - y_2) : (x, y_1), (x, y_2) \in A\}.$$

For a sequence $w_1, w_2, \ldots, w_k$ of h's and v's, $\phi_{w_1 w_2 \cdots w_k}$ denotes $\phi_{w_1} \circ \phi_{w_2} \cdots \circ \phi_{w_k}$.

A bilinear Bogolyubov theorem

Theorem (Bienvenu-L. 2017, Gowers-Milićević 2017)

If $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ has density $\alpha > 0$, then $\phi_{hhvvhh}(A)$ contains a set

$$\{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

where

A bilinear Bogolyubov theorem

Theorem (Bienvenu-L. 2017, Gowers-Milićević 2017)

If $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ has density $\alpha > 0$, then $\phi_{hhvvhh}(A)$ contains a set

$$\{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

where

- *$W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,*

A bilinear Bogolyubov theorem

Theorem (Bienvenu-L. 2017, Gowers-Milićević 2017)

If $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ has density $\alpha > 0$, then $\phi_{hhvvhh}(A)$ contains a set

$$\{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \ldots = Q_r(x, y) = 0\}$$

where

- $W_1 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_1,
- $W_2 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_2,

A bilinear Bogolyubov theorem

Theorem (Bienvenu-L. 2017, Gowers-Milićević 2017)

If $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ has density $\alpha > 0$, then $\phi_{hhvvhh}(A)$ contains a set

$$\{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

where

- $W_1 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_1,
- $W_2 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_2,
- $Q_1, \ldots, Q_r$ *are bilinear forms:* $W_1 \times W_2 \to \mathbf{F}_p$,

A bilinear Bogolyubov theorem

Theorem (Bienvenu-L. 2017, Gowers-Milićević 2017)

If $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ has density $\alpha > 0$, then $\phi_{hhvvhh}(A)$ contains a set

$$\{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \ldots = Q_r(x, y) = 0\}$$

where

- $W_1 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_1,
- $W_2 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_2,
- $Q_1, \ldots, Q_r$ *are bilinear forms:* $W_1 \times W_2 \to \mathbf{F}_p$,

A bilinear Bogolyubov theorem

Theorem (Bienvenu-L. 2017, Gowers-Milićević 2017)

If $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ has density $\alpha > 0$, then $\phi_{hhvvhh}(A)$ contains a set

$$\{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \ldots = Q_r(x, y) = 0\}$$

where

- $W_1 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_1,
- $W_2 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_2,
- $Q_1, \ldots, Q_r$ *are bilinear forms:* $W_1 \times W_2 \to \mathbf{F}_p$,

and $\max(r_1, r_2, r) \leq c(\alpha)$.

A bilinear Bogolyubov theorem

Theorem (Bienvenu-L. 2017, Gowers-Milićević 2017)

If $A \subset \mathbf{F}_p^n \times \mathbf{F}_p^n$ *has density* $\alpha > 0$*, then* $\phi_{hhvvhh}(A)$ *contains a set*

$$\{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

where

- $W_1 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_1*,*
- $W_2 \subset \mathbf{F}_p^n$ *is a subspace of codimension* r_2*,*
- $Q_1, \ldots, Q_r$ *are bilinear forms:* $W_1 \times W_2 \to \mathbf{F}_p$*,*

and $\max(r_1, r_2, r) \leq c(\alpha)$.

Recall Bogolyubov's theorem: if $A \subset \mathbf{F}_p^n$ has density α, then $A + A - A - A$ contains a subspace of codimension $r' \leq c'(\alpha)$ (= zero set of r' linear forms).

Quantitative bounds

$$\phi_{hhvvhh}(A) \supset \{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

- $W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,

Quantitative bounds

$$\phi_{hhvvhh}(A) \supset \{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

- $W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,
- $W_2 \subset \mathbf{F}_p^n$ is a subspace of codimension r_2,

Quantitative bounds

$$\phi_{hhvvhh}(A) \supset \{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

- $W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,
- $W_2 \subset \mathbf{F}_p^n$ is a subspace of codimension r_2,
- $Q_1, \ldots, Q_r$ are bilinear forms: $W_1 \times W_2 \to \mathbf{F}_p$.

Quantitative bounds

$$\phi_{hhvvhh}(A) \supset \{(x, y) \in W_1 \times W_2 : Q_1(x, y) = \ldots = Q_r(x, y) = 0\}$$

- $W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,
- $W_2 \subset \mathbf{F}_p^n$ is a subspace of codimension r_2,
- $Q_1, \ldots, Q_r$ are bilinear forms: $W_1 \times W_2 \to \mathbf{F}_p$.

Quantitative bounds

$$\phi_{hhvvhh}(A) \supset \{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

- $W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,
- $W_2 \subset \mathbf{F}_p^n$ is a subspace of codimension r_2,
- $Q_1, \ldots, Q_r$ are bilinear forms: $W_1 \times W_2 \to \mathbf{F}_p$.

Gowers-Milićević: $\max(r_1, r_2, r) = O\left(\exp\left(\exp\left(\log^{O(1)} \frac{1}{\alpha}\right)\right)\right)$.

Quantitative bounds

$$\phi_{hhvvhh}(A) \supset \{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

- $W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,
- $W_2 \subset \mathbf{F}_p^n$ is a subspace of codimension r_2,
- $Q_1, \ldots, Q_r$ are bilinear forms: $W_1 \times W_2 \to \mathbf{F}_p$.

Gowers-Milićević: $\max(r_1, r_2, r) = O\left(\exp\left(\exp\left(\log^{O(1)} \frac{1}{\alpha}\right)\right)\right)$.

Bienvenu-L.: $\max(r_1, r) = O(\log^{O(1)} \frac{1}{\alpha})$,

Quantitative bounds

$$\phi_{hhvvhh}(A) \supset \{(x,y) \in W_1 \times W_2 : Q_1(x,y) = \ldots = Q_r(x,y) = 0\}$$

- $W_1 \subset \mathbf{F}_p^n$ is a subspace of codimension r_1,
- $W_2 \subset \mathbf{F}_p^n$ is a subspace of codimension r_2,
- $Q_1, \ldots, Q_r$ are bilinear forms: $W_1 \times W_2 \to \mathbf{F}_p$.

Gowers-Milićević: $\max(r_1, r_2, r) = O\left(\exp\left(\exp\left(\log^{O(1)} \frac{1}{\alpha}\right)\right)\right)$.

Bienvenu-L.: $\max(r_1, r) = O(\log^{O(1)} \frac{1}{\alpha})$, and
$r_2 = O\left(\exp\left(\exp\left(\exp\left(\log^{O(1)} \frac{1}{\alpha}\right)\right)\right)\right)$.

Motivated by Sanders' bound $r' = O(\log^4 \frac{1}{\alpha})$, and since the roles of r_1 and r_2 are symmetric, it is natural to conjecture.

Motivated by Sanders' bound $r' = O(\log^4 \frac{1}{\alpha})$, and since the roles of r_1 and r_2 are symmetric, it is natural to conjecture.

Conjecture (Bienvenu-L. 2017)

There exists a sequence $w_1 w_2 \ldots w_k$ of length $O(1)$ such that

$$\max(r_1, r_2, r) = O(\log^{O(1)} \frac{1}{\alpha}).$$

Motivated by Sanders' bound $r' = O(\log^4 \frac{1}{\alpha})$, and since the roles of r_1 and r_2 are symmetric, it is natural to conjecture.

Conjecture (Bienvenu-L. 2017)

There exists a sequence $w_1 w_2 \dots w_k$ of length $O(1)$ such that

$$\max(r_1, r_2, r) = O(\log^{O(1)} \frac{1}{\alpha}).$$

Motivated by Sanders' bound $r' = O(\log^4 \frac{1}{\alpha})$, and since the roles of r_1 and r_2 are symmetric, it is natural to conjecture.

Conjecture (Bienvenu-L. 2017)

There exists a sequence $w_1 w_2 \dots w_k$ of length $O(1)$ such that

$$\max(r_1, r_2, r) = O(\log^{O(1)} \frac{1}{\alpha}).$$

Simple examples show that we cannot do better than this.

Motivated by Sanders' bound $r' = O(\log^4 \frac{1}{\alpha})$, and since the roles of r_1 and r_2 are symmetric, it is natural to conjecture.

Conjecture (Bienvenu-L. 2017)

There exists a sequence $w_1 w_2 \dots w_k$ of length $O(1)$ such that

$$\max(r_1, r_2, r) = O(\log^{O(1)} \frac{1}{\alpha}).$$

Simple examples show that we cannot do better than this.

Theorem (Hosseini-Lovett 2018)

The conjecture is true for the sequence hvvhvvvhh, and

$$\max(r_1, r_2, r) = O(\log^{80} \frac{1}{\alpha}).$$

Part II: Applications

Gowers and Milićević used a variant of the bilinear Bogolyubov theorem to prove a quantitative bound for the inverse theorem for the U^4-norm (first proved by Bergelson, Tao and Ziegler using qualitative methods).

Gowers and Milićević used a variant of the bilinear Bogolyubov theorem to prove a quantitative bound for the inverse theorem for the U^4-norm (first proved by Bergelson, Tao and Ziegler using qualitative methods).

We used the bilinear Bogolyubov theorem to prove an instance of the Möbius randomness principle in function fields.

The Möbius randomness principle

Recall

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ is a product of } k \text{ distinct primes,} \\ 0 & \text{if } n \text{ is not squarefree.} \end{cases}$$

Thus the sequence $\{\mu(n)\}$ is $1, -1, -1, 0, -1, 1, -1, 0, 0, 1, \ldots$.

The Möbius randomness principle

Recall

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ is a product of } k \text{ distinct primes,} \\ 0 & \text{if } n \text{ is not squarefree.} \end{cases}$$

Thus the sequence $\{\mu(n)\}$ is $1, -1, -1, 0, -1, 1, -1, 0, 0, 1, \ldots$.

The **Möbius randomness principle** states that μ is random-like,

The Möbius randomness principle

Recall

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ is a product of } k \text{ distinct primes,} \\ 0 & \text{if } n \text{ is not squarefree.} \end{cases}$$

Thus the sequence $\{\mu(n)\}$ is $1, -1, -1, 0, -1, 1, -1, 0, 0, 1, \ldots$.

The **Möbius randomness principle** states that μ is random-like, i.e. for any bounded, “simple” or “structured” function F, we have

$$\sum_{n=1}^{N} \mu(n) F(n) = o(N).$$

Examples:

1. If $F(n) = 1$, then PNT is equivalent to $\sum_{n=1}^{N} \mu(n) = o(N)$ and RH is equivalent to

$$\sum_{n=1}^{N} \mu(n) = O_\epsilon\left(N^{1/2+\epsilon}\right)$$

for any $\epsilon > 0$.

Examples:

1. If $F(n) = 1$, then PNT is equivalent to $\sum_{n=1}^{N} \mu(n) = o(N)$ and *RH* is equivalent to
$$\sum_{n=1}^{N} \mu(n) = O_\epsilon\left(N^{1/2+\epsilon}\right)$$
for any $\epsilon > 0$.

2. If $F(n)$ is periodic with period q, then $\sum_{n=1}^{N} \mu(n)F(n) = o(N)$ is equivalent to PNT in arithmetic progressions.

Examples:

1. If $F(n) = 1$, then PNT is equivalent to $\sum_{n=1}^{N} \mu(n) = o(N)$ and *RH* is equivalent to
$$\sum_{n=1}^{N} \mu(n) = O_\epsilon\left(N^{1/2+\epsilon}\right)$$
for any $\epsilon > 0$.

2. If $F(n)$ is periodic with period q, then $\sum_{n=1}^{N} \mu(n)F(n) = o(N)$ is equivalent to PNT in arithmetic progressions.

3. We can formulate the Möbius randomness principle in terms of dynamical systems (Sarnak) or computational complexity (Kalai).

Exponential sums

Davenport/Vinogradov (1937): for any $A > 0$,

$$\sum_{n=1}^{N} \mu(n) e(n\alpha) \ll_A \frac{N}{\log^A N}$$

uniformly in $\alpha \in \mathbf{R}/\mathbf{Z}$. Here $e(x) = e^{2\pi i x}$. The implied constant is ineffective.

Exponential sums

Davenport/Vinogradov (1937): for any $A > 0$,

$$\sum_{n=1}^{N} \mu(n) e(n\alpha) \ll_A \frac{N}{\log^A N}$$

uniformly in $\alpha \in \mathbf{R}/\mathbf{Z}$. Here $e(x) = e^{2\pi i x}$. The implied constant is ineffective.

Baker-Harman (1991), Montgomery-Vaughan (unpublished): Assuming GRH, we have

$$\sum_{n=1}^{N} \mu(n) e(n\alpha) \ll_\epsilon N^{3/4+\epsilon}$$

uniformly in $\alpha \in \mathbf{R}/\mathbf{Z}$, for any $\epsilon > 0$.

Since

$$\int_0^1 \left| \sum_{n=1}^{N} \mu(n) e(n\alpha) \right|^2 d\alpha = \sum_{n=1}^{N} |\mu(n)|^2 \gg N,$$

we cannot do better than $N^{1/2}$.

Since

$$\int_0^1 \left| \sum_{n=1}^{N} \mu(n) e(n\alpha) \right|^2 d\alpha = \sum_{n=1}^{N} |\mu(n)|^2 \gg N,$$

we cannot do better than $N^{1/2}$.

Green-Tao (2008, 2012): If $F(n)$ is a nilsequence, then for any $A > 0$,

$$\sum_{n=1}^{N} \mu(n) F(n) \ll_A \frac{N}{\log^A N}.$$

Since

$$\int_0^1 \left|\sum_{n=1}^{N} \mu(n) e(n\alpha)\right|^2 d\alpha = \sum_{n=1}^{N} |\mu(n)|^2 \gg N,$$

we cannot do better than $N^{1/2}$.

Green-Tao (2008, 2012): If $F(n)$ is a nilsequence, then for any $A > 0$,

$$\sum_{n=1}^{N} \mu(n) F(n) \ll_A \frac{N}{\log^A N}.$$

Nilsequences include $F(n) = e\left(\alpha n^2 + \beta n\right)$ and $F(n) = e\left(\lfloor n\alpha \rfloor \beta n\right)$.

Function field analogy

Let $\mathbf{F}_q$ be the finite field on q elements. It has been known since Dedekind-Weber (1882) that $\mathbf{F}_q[t]$ is similar to $\mathbf{Z}$ in many aspects. For example, both are unique factorization domains.

Function field analogy

Let $\mathbf{F}_q$ be the finite field on q elements. It has been known since Dedekind-Weber (1882) that $\mathbf{F}_q[t]$ is similar to $\mathbf{Z}$ in many aspects. For example, both are unique factorization domains.

For $f \in \mathbf{F}_q[t]$, define

$$\mu(f) = \begin{cases} (-1)^k & \text{if } f = cP_1 P_2 \cdots P_k,\ P_i \text{ distinct monic irreducibles,} \\ & \qquad c \in {\mathbf{F}_q}^\times, \\ 0 & \text{if } f \text{ is not squarefree.} \end{cases}$$

Function field analogy

Let $\mathbf{F}_q$ be the finite field on q elements. It has been known since Dedekind-Weber (1882) that $\mathbf{F}_q[t]$ is similar to $\mathbf{Z}$ in many aspects. For example, both are unique factorization domains.

For $f \in \mathbf{F}_q[t]$, define

$$\mu(f) = \begin{cases} (-1)^k & \text{if } f = cP_1P_2\cdots P_k,\ P_i \text{ distinct monic irreducibles,} \\ & \qquad\qquad\qquad\qquad c \in \mathbf{F}_q^{\times}, \\ 0 & \text{if } f \text{ is not squarefree.} \end{cases}$$

RH is true in $\mathbf{F}_q[t]$: for $n \geq 2$,

$$\sum_{\substack{\deg f = n, \\ f \text{ monic}}} \mu(f) = 0.$$

Function field analogy

Let $\mathbf{F}_q$ be the finite field on q elements. It has been known since Dedekind-Weber (1882) that $\mathbf{F}_q[t]$ is similar to $\mathbf{Z}$ in many aspects. For example, both are unique factorization domains.

For $f \in \mathbf{F}_q[t]$, define

$$\mu(f) = \begin{cases} (-1)^k & \text{if } f = cP_1P_2\cdots P_k,\ P_i \text{ distinct monic irreducibles, } c \in \mathbf{F}_q^{\times}, \\ 0 & \text{if } f \text{ is not squarefree.} \end{cases}$$

RH is true in $\mathbf{F}_q[t]$: for $n \geq 2$,

$$\sum_{\substack{\deg f = n, \\ f \text{ monic}}} \mu(f) = 0.$$

Furthermore, GRH is true in $\mathbf{F}_q[t]$ (Weil 1948).

Fix $e_q : \mathbf{F}_q \to \{z \in \mathbf{C} : |z| = 1\}$ to be a nontrivial additive character of $\mathbf{F}_q$, i.e. $e_q(x + y) = e_q(x)e_q(y)$ for any $x, y \in \mathbf{F}_q$.

Fix $e_q : \mathbf{F}_q \to \{z \in \mathbf{C} : |z| = 1\}$ to be a nontrivial additive character of $\mathbf{F}_q$, i.e. $e_q(x+y) = e_q(x)e_q(y)$ for any $x, y \in \mathbf{F}_q$.

Problem. Let $k \geq 1$ and $Q \in \mathbf{F}_q[x_0, x_1, \dots, x_{n-1}]$ be a polynomial of degree k. Show that

$$\sum_{\deg f < n} \mu(f) e_q(Q(f)) = o_{q,k}(q^n)$$

uniformly in Q of degree k. Here $Q(f)$ is Q evaluated at the coefficients of f.

Fix $e_q : \mathbf{F}_q \to \{z \in \mathbf{C} : |z| = 1\}$ to be a nontrivial additive character of $\mathbf{F}_q$, i.e. $e_q(x + y) = e_q(x)e_q(y)$ for any $x, y \in \mathbf{F}_q$.

Problem. Let $k \geq 1$ and $Q \in \mathbf{F}_q[x_0, x_1, \ldots, x_{n-1}]$ be a polynomial of degree k. Show that

$$\sum_{\deg f < n} \mu(f) e_q(Q(f)) = o_{q,k}(q^n)$$

uniformly in Q of degree k. Here $Q(f)$ is Q evaluated at the coefficients of f.

Since we have GRH, we may expect $O_q(q^{c_k n})$ for some constant $c_k < 1$, or even $O_{q,k,\epsilon}(q^{(1/2+\epsilon)n})$.

Our results

Theorem ($k = 1$)

For any $\epsilon > 0$, we have

$$\sum_{\deg f < n} \mu(f) e_q(L(f)) \ll_{\epsilon,q} q^{(3/4+\epsilon)n}$$

uniformly in linear forms $L \in \mathbf{F}_q[x_0, \ldots, x_{n-1}]$.

Our results

Theorem ($k = 1$)

For any $\epsilon > 0$, we have

$$\sum_{\deg f < n} \mu(f) e_q(L(f)) \ll_{\epsilon,q} q^{(3/4+\epsilon)n}$$

uniformly in linear forms $L \in \mathbf{F}_q[x_0, \ldots, x_{n-1}]$.

Theorem ($k = 1$)

For any $\epsilon > 0$, we have

$$\sum_{\deg f < n} \mu(f) e_q(L(f)) \ll_{\epsilon, q} q^{(3/4+\epsilon)n}$$

uniformly in linear forms $L \in \mathbf{F}_q[x_0, \ldots, x_{n-1}]$.

Recall Baker-Harman and Montgomery-Vaughan's bound in $\mathbf{Z}$ (under GRH)

$$\sum_{n=1}^{N} \mu(n) e(\alpha n) \ll N^{3/4+\epsilon}.$$

Our results

Theorem ($k = 1$)

For any $\epsilon > 0$, we have

$$\sum_{\deg f < n} \mu(f) e_q(L(f)) \ll_{\epsilon,q} q^{(3/4+\epsilon)n}$$

uniformly in linear forms $L \in \mathbf{F}_q[x_0, \ldots, x_{n-1}]$.

Recall Baker-Harman and Montgomery-Vaughan's bound in $\mathbf{Z}$ (under GRH)

$$\sum_{n=1}^{N} \mu(n) e(\alpha n) \ll N^{3/4+\epsilon}.$$

Our argument is different from the proof in $\mathbf{Z}$ in some respects.

Theorem ($k = 2$)

Suppose q is odd. There exists an absolute constant c ($c = 1/161$ will do) such that

$$\sum_{\deg f < n} \mu(f) e_q(Q(f)) \ll_q q^{n-n^c}.$$

uniformly in quadratic polynomials $Q \in \mathbf{F}_q[x_0, \ldots, x_{n-1}]$.

Theorem ($k = 2$)

Suppose q is odd. There exists an absolute constant c ($c = 1/161$ will do) such that

$$\sum_{\deg f < n} \mu(f) e_q(Q(f)) \ll_q q^{n-n^c}.$$

uniformly in quadratic polynomials $Q \in \mathbf{F}_q[x_0, \ldots, x_{n-1}]$.

Theorem ($k = 2$)

Suppose q is odd. There exists an absolute constant c ($c = 1/161$ will do) such that

$$\sum_{\deg f < n} \mu(f) e_q(Q(f)) \ll_q q^{n-n^c}.$$

uniformly in quadratic polynomials $Q \in \mathbf{F}_q[x_0, \ldots, x_{n-1}]$.

This is better than what is known in $\mathbf{Z}$ for nilsequences of step 2:

$$\sum_{n=1}^{N} \mu(n) F(n) \ll_{F,A} \frac{N}{\log^A N}$$

for any $A > 0$.

The circle method

The classical circle method deals with exponential sums like

$$\sum_{n=1}^{N} \mu(n) e(\alpha n).$$

To estimate such sums we need to distinguish two cases.

- α is close to a rational with small denominator (α is in the *major arcs*): use our knowledge about the distribution of primes in arithmetic progressions.

The circle method

The classical circle method deals with exponential sums like

$$\sum_{n=1}^{N} \mu(n) e(\alpha n).$$

To estimate such sums we need to distinguish two cases.

- α is close to a rational with small denominator (α is in the *major arcs*): use our knowledge about the distribution of primes in arithmetic progressions.
- α is not in the major arcs (α is in the *minor arcs*): use combinatorial machinery (Vaughan's identity, Vinogradov's Type I/Type II sums) and Cauchy-Schwarz.

In the case of

$$\sum_{\deg f<n} \mu(f) e_q(\Phi(f)),$$

where $\Phi(x) = x^T Mx$ and M is a symmetric matrix, the major arcs and minor arcs correspond to low rank and high rank matrices M. This is because

$$\left| \sum_{x\in\mathbf{F}_q^n} e_q(x^T Mx) \right| \leq q^{n-\mathrm{rank}(M)/2}.$$

We want to show that

$$\left| \sum_{\deg f < n} \mu(f) e_q(\Phi(f)) \right| \leq \delta q^n$$

where $\delta = q^{-n^c}$.

We want to show that

$$\left|\sum_{\deg f<n} \mu(f) e_q(\Phi(f))\right| \leq \delta q^n$$

where $\delta = q^{-n^c}$.

If $\mathrm{rank}(M)$ is small, we can reduce our problem to the linear case.

We want to show that

$$\left|\sum_{\deg f<n} \mu(f) e_q(\Phi(f))\right| \leq \delta q^n$$

where $\delta = q^{-n^c}$.

If $\mathrm{rank}(\mathsf{M})$ is small, we can reduce our problem to the linear case.

Suppose $\left|\sum_{\deg f<n} \mu(f) e_q(\Phi(f))\right| \geq \delta q^n$. We will show that $\mathrm{rank}(\mathsf{M})$ is small, which is a contradiction.

After using Vaughan's identity, Vinogradov's Type I/Type II sums, Cauchy-Schwarz and some combinatorial reasoning, we find that for some $n \ll k \leq n$, the set of pairs

$$P_s := \{(a, b) : a, b \in G_{k+1} \times G_{k+1} : \mathrm{rank}\, M_{a,b} \leq s\}$$

is large (has size $q^{-O(n^c)} q^{2k+2}$) for some $s = O(n^c)$.

After using Vaughan's identity, Vinogradov's Type I/Type II sums, Cauchy-Schwarz and some combinatorial reasoning, we find that for some $n \ll k \leq n$, the set of pairs

$$P_s := \{(a, b) : a, b \in G_{k+1} \times G_{k+1} : \mathrm{rank}\, M_{a,b} \leq s\}$$

is large (has size $q^{-O(n^c)} q^{2k+2}$) for some $s = O(n^c)$.

Here $G_m = \{f : \deg f < m\}$,

$$M_{a,b} = L_a^T M L_b + L_b^T M L_a$$

and L_a is the matrix of the map $G_{n-k} \to G_n, f \mapsto af$.

We know

$$P_s := \{(a, b) : a, b \in G_{k+1} \times G_{k+1} : \mathrm{rank}\, M_{a,b} \leq s\}$$

is large, where $M_{a,b} = L_a^T M L_b + L_b^T M L_a$. Want to show that $\mathrm{rank}\, M$ is small.

We know

$$P_s := \{(a,b) : a,b \in G_{k+1} \times G_{k+1} : \mathrm{rank}\, M_{a,b} \leq s\}$$

is large, where $M_{a,b} = L_a^T M L_b + L_b^T M L_a$. Want to show that $\mathrm{rank}\, M$ is small.

If $\mathrm{rank}\, M_{a,b}, \mathrm{rank}\, M_{a',b} \leq s$, then $\mathrm{rank}\, M_{a-a',b} = \mathrm{rank}\,(M_{a,b} - M_{a',b}) \leq 2s$. Similarly for the second coordinate.

We know

$$P_s := \{(a,b) : a,b \in G_{k+1} \times G_{k+1} : \operatorname{rank} M_{a,b} \leq s\}$$

is large, where $M_{a,b} = L_a^T M L_b + L_b^T M L_a$. Want to show that $\operatorname{rank} M$ is small.

If $\operatorname{rank} M_{a,b}, \operatorname{rank} M_{a',b} \leq s$, then $\operatorname{rank} M_{a-a',b} = \operatorname{rank} (M_{a,b} - M_{a',b}) \leq 2s$. Similarly for the second coordinate.

By repeatedly applying the operations ϕ_h and ϕ_v on P_s, the bilinear Bogolyubov theorem implies that $P_{2^9 s}$ contains a bilinear structure. By exploiting this, we can show that M has low rank, as desired.