# Polynomial Freiman Isomorphisms

Philip Matchett Wood

Department of Mathematics
Rutgers University
New Brunswick, New Jersey

April 5, 2008

Clay-Fields Conference on Additive Combinatorics, Number Theory, and Harmonic Analysis

Joint work with Van H. Vu and Melanie Matchett Wood.

# Freiman homomorphisms (review)

Let $Z, W$ be additive groups, with subsets $A \subset Z$ and $B \subset W$.

# Freiman homomorphisms (review)

Let $Z, W$ be additive groups, with subsets $A \subset Z$ and $B \subset W$.

## Definition

A **Freiman homomorphism** of order $k$ is a map $\phi : A \to B$ that is "nearly a group homomorphism", i.e.,

if $a_1 + a_2 + \cdots + a_k = a'_1 + a'_2 + \cdots + a'_k$, then

$\phi(a_1) + \phi(a_2) + \cdots + \phi(a_k) = \phi(a'_1) + \phi(a'_2) + \cdots + \phi(a'_k)$.

# Freiman homomorphisms (review)

Let $Z, W$ be additive groups, with subsets $A \subset Z$ and $B \subset W$.

**Definition**

A **Freiman homomorphism** of order $k$ is a map $\phi : A \to B$ that is "nearly a group homomorphism", i.e.,
if $a_1 + a_2 + \cdots + a_k = a'_1 + a'_2 + \cdots + a'_k$, then

$\phi(a_1) + \phi(a_2) + \cdots + \phi(a_k) = \phi(a'_1) + \phi(a'_2) + \cdots + \phi(a'_k)$.

- $\phi$ is a Freiman isomorphism of order $k$ if $\phi^{-1}$ is also a Freiman homomorphism of order $k$.

# Freiman homomorphisms (review)

Let $Z, W$ be additive groups, with subsets $A \subset Z$ and $B \subset W$.

## Definition

A **Freiman homomorphism** of order $k$ is a map $\phi : A \to B$ that is "nearly a group homomorphism", i.e.,
if $a_1 + a_2 + \cdots + a_k = a_1' + a_2' + \cdots + a_k'$, then

$$\phi(a_1) + \phi(a_2) + \cdots + \phi(a_k) = \phi(a_1') + \phi(a_2') + \cdots + \phi(a_k').$$

- $\phi$ is a Freiman isomorphism of order $k$ if $\phi^{-1}$ is also a Freiman homomorphism of order $k$.

## Freiman Isomorphism Lemma

Let $A$ be a finite subset of a torsion-free additive group $Z$.
Then for every $k$ and every sufficiently large $p$ depending on $k$ and $A$, there exists a Freiman isomorphism of order $k$ to $\mathbb{Z}/p\mathbb{Z}$.

# Freiman homomorphisms (review)

Let $Z, W$ be additive groups, with subsets $A \subset Z$ and $B \subset W$.

### Definition

A **Freiman homomorphism** of order $k$ is a map $\phi : A \to B$ that is "nearly a group homomorphism", i.e.,
if $a_1 + a_2 + \cdots + a_k = a_1' + a_2' + \cdots + a_k'$, then

$$\phi(a_1) + \phi(a_2) + \cdots + \phi(a_k) = \phi(a_1') + \phi(a_2') + \cdots + \phi(a_k').$$

- $\phi$ is a Freiman isomorphism of order $k$ if $\phi^{-1}$ is also a Freiman homomorphism of order $k$.

### Freiman Isomorphism Lemma

Let $A$ be a finite subset of a torsion-free additive group $Z$.
Then for every $k$ and every sufficiently large $p$ depending on $k$ and $A$, there exists a Freiman isomorphism of order $k$ to $\mathbb{Z}/p\mathbb{Z}$.

- For example, to prove Freiman's Theorem for torsion free groups, one maps to $\mathbb{Z}/p\mathbb{Z}$ using a Freiman isomorphism.

# Freiman homomorphisms (review)

Let $Z, W$ be additive groups, with subsets $A \subset Z$ and $B \subset W$.

### Definition

A **Freiman homomorphism** of order $k$ is a map $\phi : A \to B$ that is "nearly a group homomorphism", i.e.,
if $a_1 + a_2 + \cdots + a_k = a'_1 + a'_2 + \cdots + a'_k$, then

$$\phi(a_1) + \phi(a_2) + \cdots + \phi(a_k) = \phi(a'_1) + \phi(a'_2) + \cdots + \phi(a'_k).$$

- $\phi$ is a Freiman isomorphism of order $k$ if $\phi^{-1}$ is also a Freiman homomorphism of order $k$.

### Freiman Isomorphism Lemma

Let $A$ be a finite subset of a torsion-free additive group $Z$.
Then for every $k$ and every sufficiently large $p$ depending on $k$ and $A$, there exists a Freiman isomorphism of order $k$ to $\mathbb{Z}/p\mathbb{Z}$.

**Question:** Are there cases where one would want to preserve additive and multiplicative properties simultaneously?

# The Sum-Product Problem

Consider a finite subset $A \subset \mathbb{Z}$.

Define: $$\begin{aligned} A + A &:= \{a_1 + a_2 : a_i \in A\}, \text{ and} \\ AA &:= \{a_1 a_2 : a_i \in A\}. \end{aligned}$$

**Goal**: show $|A + A| + |AA|$ is large with respect to $|A|$.

# The Sum-Product Problem

Consider a finite subset $A \subset \mathbb{Z}$.

Define: $$\begin{aligned} A + A &:= \{a_1 + a_2 : a_i \in A\}, \text{ and} \\ AA &:= \{a_1 a_2 : a_i \in A\}. \end{aligned}$$

**Goal**: show $|A + A| + |AA|$ is large with respect to $|A|$.

---

Can we map the problem to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$?

# The Sum-Product Problem

Consider a finite subset $A \subset \mathbb{Z}$.

Define: $$\begin{aligned} A + A &:= \{a_1 + a_2 : a_i \in A\}, \text{ and} \\ AA &:= \{a_1 a_2 : a_i \in A\}. \end{aligned}$$

**Goal**: show $|A + A| + |AA|$ is large with respect to $|A|$.

---

Can we map the problem to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$?

- A Freiman isomorphism is **not** suitable, because of multiplication.

# The Sum-Product Problem

Consider a finite subset $A \subset \mathbb{Z}$.

Define: $A + A := \{a_1 + a_2 : a_i \in A\}$, and
$AA := \{a_1 a_2 : a_i \in A\}$.

**Goal**: show $|A + A| + |AA|$ is large with respect to $|A|$.

---

Can we map the problem to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$?

- A Freiman isomorphism is **not** suitable, because of multiplication.
- However, we *can* just choose a large enough prime $p$.

# The Sum-Product Problem

Consider a finite subset $A \subset \mathbb{Z}$.

Define: $A + A := \{a_1 + a_2 : a_i \in A\}$, and
$AA := \{a_1 a_2 : a_i \in A\}$.

**Goal**: show $|A + A| + |AA|$ is large with respect to $|A|$.

---

Can we map the problem to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$?

- A Freiman isomorphism is **not** suitable, because of multiplication.
- However, we *can* just choose a large enough prime $p$.
- E.g., take $p > \max\{2\,|x| : x \in (A + A) \cup (AA) \cup A\}$.
  Then, $|A| = |A \bmod p|$,

$$|A + A| = |A + A \bmod p|\,, \quad \text{and} \quad |AA| = |AA \bmod p|$$

# The Sum-Product Problem

Consider a finite subset $A \subset \mathbb{Z}$.

Define: $A + A := \{a_1 + a_2 : a_i \in A\}$, and
$AA := \{a_1 a_2 : a_i \in A\}$.

**Goal**: show $|A + A| + |AA|$ is large with respect to $|A|$.

---

Can we map the problem to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$?

- A Freiman isomorphism is **not** suitable, because of multiplication.
- However, we *can* just choose a large enough prime $p$.
- E.g., take $p > \max\{2\,|x| : x \in (A + A) \cup (AA) \cup A\}$.
  Then, $|A| = |A \bmod p|$,

$$|A + A| = |A + A \bmod p|, \quad \text{and} \quad |AA| = |AA \bmod p|$$

**Question**

What if $A \subset \mathbb{C}$, the complex numbers?

# A new mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.

# A new mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.

Then, there exists an infinite sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

**Main Theorem**

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

- Examples of characteristic zero integral domains: $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$.

# A new mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

- Examples of characteristic zero integral domains: $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$.
- $\phi$ is a ring homomorphism, so for all $a, b \in \mathbb{Z}[S]$, $\phi(ab) = \phi(a)\phi(b)$ and $\phi(a + b) = \phi(a) + \phi(b)$.

# A new mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

- Examples of characteristic zero integral domains: $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$.
- $\phi$ is a ring homomorphism, so for all $a, b \in \mathbb{Z}[S]$, $\phi(ab) = \phi(a)\phi(b)$ and $\phi(a + b) = \phi(a) + \phi(b)$.
- Also $\phi(0) = 0$ and $\phi(1) = 1$.

# A new mapping theorem

**Main Theorem**

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

- Examples of characteristic zero integral domains: $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$.
- $\phi$ is a ring homomorphism, so for all $a, b \in \mathbb{Z}[S]$, $\phi(ab) = \phi(a)\phi(b)$ and $\phi(a+b) = \phi(a) + \phi(b)$.
- Also $\phi(0) = 0$ and $\phi(1) = 1$.
- Example: Set $L := \{(s_1 + s_2) - (s_3 + s_4) : s_i \in S\} \setminus \{0\}$ to get a Freiman <u>iso</u>mophism of order 2 from $S$, so

$$|S + S| = |\phi(S) + \phi(S)|\,.$$

# A polynomial Freiman Isomorphism Lemma

## Corollary

Let $A$ be a finite subset of a characteristic zero integral domain $D$. Given a system of $m$ polynomial equations with integer coefficients

$$f_j(x_1, x_2, \ldots, x_n) = 0, \qquad \text{where } 1 \leq j \leq m,$$

# A polynomial Freiman Isomorphism Lemma

## Corollary

Let $A$ be a finite subset of a characteristic zero integral domain $D$. Given a system of $m$ polynomial equations with integer coefficients

$$f_j(x_1, x_2, \ldots, x_n) = 0, \qquad \text{where } 1 \leq j \leq m,$$

there exists a sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[A] \to \mathbb{Z}/p\mathbb{Z}$ that is a bijective map from $A$ to $B$

# A polynomial Freiman Isomorphism Lemma

## Corollary

Let $A$ be a finite subset of a characteristic zero integral domain $D$. Given a system of $m$ polynomial equations with integer coefficients

$$f_j(x_1, x_2, \ldots, x_n) = 0, \qquad \text{where } 1 \leq j \leq m,$$

there exists a sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[A] \to \mathbb{Z}/p\mathbb{Z}$ that is a bijective map from $A$ to $B$ where $(a_1, \ldots, a_n) \in A^n$ is a solution to the system in $D$ if and only if $(\phi(a_1), \ldots, \phi(a_n))$ is a solution to the system in $\mathbb{Z}/p\mathbb{Z}$.

# A polynomial Freiman Isomorphism Lemma

## Corollary

Let $A$ be a finite subset of a characteristic zero integral domain $D$. Given a system of $m$ polynomial equations with integer coefficients

$$f_j(x_1, x_2, \ldots, x_n) = 0, \quad \text{where } 1 \leq j \leq m,$$

there exists a sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[A] \to \mathbb{Z}/p\mathbb{Z}$ that is a bijective map from $A$ to $B$ where $(a_1, \ldots, a_n) \in A^n$ is a solution to the system in $D$ if and only if $(\phi(a_1), \ldots, \phi(a_n))$ is a solution to the system in $\mathbb{Z}/p\mathbb{Z}$.

- implies the Freiman Isomorphism Lemma by setting
$$f_1(x_1, \ldots, x_{2k}) = x_1 + \cdots + x_k - (x_{k+1} + \cdots + x_{k+k}).$$

# A polynomial Freiman Isomorphism Lemma

## Corollary

Let $A$ be a finite subset of a characteristic zero integral domain $D$. Given a system of $m$ polynomial equations with integer coefficients

$$f_j(x_1, x_2, \ldots, x_n) = 0, \quad \text{where } 1 \le j \le m,$$

there exists a sequence of primes with positive density such that for each prime $p$ there exists a ring homomorphism $\phi : \mathbb{Z}[A] \to \mathbb{Z}/p\mathbb{Z}$ that is a bijective map from $A$ to $B$ where $(a_1, \ldots, a_n) \in A^n$ is a solution to the system in $D$ if and only if $(\phi(a_1), \ldots, \phi(a_n))$ is a solution to the system in $\mathbb{Z}/p\mathbb{Z}$.

- implies the Freiman Isomorphism Lemma by setting
$$f_1(x_1, \ldots, x_{2k}) = x_1 + \cdots + x_k - (x_{k+1} + \cdots + x_{k+k}).$$
- Follows from the mapping theorem by setting
$L := ((A - A) \cup \{f_j(a_1, \ldots, a_n) : a_i \in A, 1 \le j \le m\}) \setminus \{0\}$

# Application: Sum-Product estimates

**Theorem (Katz and Shen, slightly improving Garaev, 2007)**

*Let $p$ be a prime and let $A$ be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| \leq p^{1/2}$. Then there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log|A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

# Application: Sum-Product estimates

**Theorem (Katz and Shen, slightly improving Garaev, 2007)**

*Let $p$ be a prime and let $A$ be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| \leq p^{1/2}$. Then there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log |A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

- $A$ a finite subset of a characteristic zero integral domain.

# Application: Sum-Product estimates

**Theorem (Katz and Shen, slightly improving Garaev, 2007)**

*Let $p$ be a prime and let $A$ be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| \leq p^{1/2}$. Then there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log|A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

- $A$ a finite subset of a characteristic zero integral domain. Plan: apply mapping theorem.

# Application: Sum-Product estimates

**Theorem (Katz and Shen, slightly improving Garaev, 2007)**

*Let $p$ be a prime and let $A$ be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| \leq p^{1/2}$. Then there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log|A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

- $A$ a finite subset of a characteristic zero integral domain. Plan: apply mapping theorem. Let

$$\begin{aligned} L := \{a_1 - a_2 : a_1, a_2 \in A\} & \quad (\text{so } |A| = |\phi(A)|) \\ \cup \{(a_1a_2) - (a_3a_4) : a_i \in A\} & \quad (\text{so } |AA| = |\phi(A)\phi(A)|) \\ \cup \{(a_1+a_2) - (a_3+a_4) : a_i \in A\} & \quad (\text{so } \phi \text{ preserves } |A+A|). \end{aligned}$$

# Application: Sum-Product estimates

**Theorem (Katz and Shen, slightly improving Garaev, 2007)**

*Let $p$ be a prime and let $A$ be a subset of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| \leq p^{1/2}$. Then there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log |A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

- $A$ a finite subset of a characteristic zero integral domain. Plan: apply mapping theorem. Let

$$\begin{aligned} L := \{a_1 - a_2 : a_1, a_2 \in A\} & \quad (\text{so } |A| = |\phi(A)|) \\ \cup \{(a_1 a_2) - (a_3 a_4) : a_i \in A\} & \quad (\text{so } |AA| = |\phi(A)\phi(A)|) \\ \cup \{(a_1 + a_2) - (a_3 + a_4) : a_i \in A\} & \quad (\text{so } \phi \text{ preserves } |A+A|). \end{aligned}$$

- Take $p > |A|^2$, and find desired map $\phi$, which depends on $p$.

# Application: Sum-Product estimates (continued)

- Apply the mapping theorem to place the problem in $\mathbb{Z}/p\mathbb{Z}$, and then apply the Katz-Shen or Garaev sum-product estimate in $\mathbb{Z}/p\mathbb{Z}$.

# Application: Sum-Product estimates (continued)

- Apply the mapping theorem to place the problem in $\mathbb{Z}/p\mathbb{Z}$, and then apply the Katz-Shen or Garaev sum-product estimate in $\mathbb{Z}/p\mathbb{Z}$.

**Corollary**

*For every finite subset $A$ of a characteristic zero integral domain, there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log|A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

# Application: Sum-Product estimates (continued)

- Apply the mapping theorem to place the problem in $\mathbb{Z}/p\mathbb{Z}$, and then apply the Katz-Shen or Garaev sum-product estimate in $\mathbb{Z}/p\mathbb{Z}$.

**Corollary**

*For every finite subset $A$ of a characteristic zero integral domain, there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log |A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

Note: Best known sum-product estimate in $\mathbb{C}$ has exponent $14/11$ (Solymosi, 2005) and is proven with clever use of the topology of the complex plane.

# Application: Sum-Product estimates (continued)

- Apply the mapping theorem to place the problem in $\mathbb{Z}/p\mathbb{Z}$, and then apply the Katz-Shen or Garaev sum-product estimate in $\mathbb{Z}/p\mathbb{Z}$.

## Corollary

*For every finite subset $A$ of a characteristic zero integral domain, there exist absolute constants $c > 0$ and $\alpha > 0$ such that*

$$c\frac{|A|^{14/13}}{(\log|A|)^{\alpha}} \leq \max\{|A+A|, |AA|\}.$$

Note: Best known sum-product estimate in $\mathbb{C}$ has exponent $14/11$ (Solymosi, 2005) and is proven with clever use of the topology of the complex plane. Improvements in $\mathbb{Z}/p\mathbb{Z}$ would yield (via mapping) improvements in any characteristic zero integral domain.

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós
  $\Pr(M_n \text{ is singular}) \leq o(1)$.

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977)
  $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977)
  $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.
- 1995, Kahn, Komlós, Szemeredi
  $$\Pr(M_n \text{ is singular}) \leq .999^n.$$

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977)
  $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.
- 1995, Kahn, Komlós, Szemeredi
  $$\Pr(M_n \text{ is singular}) \leq .999^n.$$
- 2005, Tao, Vu
  $$\Pr(M_n \text{ is singular}) \leq .939^n.$$

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977)
  $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.
- 1995, Kahn, Komlós, Szemeredi
  $$\Pr(M_n \text{ is singular}) \leq .999^n.$$
- 2006, Tao, Vu
  $$\Pr(M_n \text{ is singular}) \leq \left(\tfrac{3}{4} + o(1)\right)^n.$$

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977)
  $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.
- 1995, Kahn, Komlós, Szemeredi
  $$\Pr(M_n \text{ is singular}) \leq .999^n.$$
- 2006, Tao, Vu
  $$\Pr(M_n \text{ is singular}) \leq \left(\tfrac{3}{4} + o(1)\right)^n.$$
- 2008, Bourgain, Vu, W.
  $$\Pr(M_n \text{ is singular}) \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

(Note $1/\sqrt{2} \approx 0.7071$.)

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977)
  $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.
- 1995, Kahn, Komlós, Szemeredi
  $$\Pr(M_n \text{ is singular}) \leq .999^n.$$
- 2006, Tao, Vu
  $$\Pr(M_n \text{ is singular}) \leq \left(\tfrac{3}{4} + o(1)\right)^n.$$
- 2008, Bourgain, Vu, W.
  $$\Pr(M_n \text{ is singular}) \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

(Note $1/\sqrt{2} \approx 0.7071$.)

**Question:** Can we extend to the case where $M_n$ has entries in $\mathbb{C}$?

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977)
  $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.
- 1995, Kahn, Komlós, Szemeredi
  $$\Pr(M_n \text{ is singular}) \leq .999^n.$$
- 2006, Tao, Vu
  $$\Pr(M_n \text{ is singular}) \leq \left(\tfrac{3}{4} + o(1)\right)^n.$$
- 2008, Bourgain, Vu, W.
  $$\Pr(M_n \text{ is singular}) \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

  (Note $1/\sqrt{2} \approx 0.7071$.)

**Question:** Can we extend to the case where $M_n$ has entries in $\mathbb{C}$?

**Issue:** The Tao-Vu approach relies on the identity

$$\mathbf{1}_{\{x=0\}} = \int_0^1 exp(2\pi i x t)\, dt$$

# The singularity probability of discrete random matrices

Let $M_n$ be a random $n$ by $n$ matrix where each entry is $+1$ or $-1$ independently with probability $1/2$.

**Goal:** Bound the probability that $M_n$ is singular ($\det(M_n) = 0$).

- 1967, Komlós (improved 1977) $\Pr(M_n \text{ is singular}) \leq O(1/\sqrt{n}) \leq o(1)$.
- 1995, Kahn, Komlós, Szemeredi
$$\Pr(M_n \text{ is singular}) \leq .999^n.$$
- 2006, Tao, Vu
$$\Pr(M_n \text{ is singular}) \leq \left(\frac{3}{4} + o(1)\right)^n.$$
- 2008, Bourgain, Vu, W.
$$\Pr(M_n \text{ is singular}) \leq \left(\frac{1}{\sqrt{2}} + o(1)\right)^n.$$

(Note $1/\sqrt{2} \approx 0.7071$.)

**Question:** Can we extend to the case where $M_n$ has entries in $\mathbb{C}$?

**Issue:** The Tao-Vu approach relies on the identity

$$\mathbf{1}_{\{x=0\}} = \int_0^1 exp(2\pi i x t)\, dt, \text{ which is false for } x \in \mathbb{C}.$$

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$.*

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$. Assume that for any entry $\alpha$, we have $\max_x \Pr(\alpha = x) \leq p$.*

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$. Assume that for any entry $\alpha$, we have $\max_x \Pr(\alpha = x) \leq p$. Then*

$$\Pr(M_n \textit{ is singular}) \leq \left(\sqrt{p} + o(1)\right)^n.$$

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$. Assume that for any entry $\alpha$, we have $\max_x \Pr(\alpha = x) \le p$. Then*

$$\Pr(M_n \textit{ is singular}) \le \left(\sqrt{p} + o(1)\right)^n.$$

Proof ideas:

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$. Assume that for any entry $\alpha$, we have $\max_x \Pr(\alpha = x) \leq p$. Then*

$$\Pr(M_n \textit{ is singular}) \leq \left(\sqrt{p} + o(1)\right)^n.$$

Proof ideas:

- The determinant is a polynomial

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$. Assume that for any entry $\alpha$, we have $\max_x \Pr(\alpha = x) \leq p$. Then*

$$\Pr(M_n \text{ is singular}) \leq \left(\sqrt{p} + o(1)\right)^n .$$

Proof ideas:

- The determinant is a polynomial, so use the polynomial version of the mapping theorem to pass to $\mathbb{Z}/Q\mathbb{Z}$, for $Q$ a huge prime (depending on $n$).

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$. Assume that for any entry $\alpha$, we have $\max_x \Pr(\alpha = x) \le p$. Then*

$$\Pr(M_n \text{ is singular}) \le \left(\sqrt{p} + o(1)\right)^n .$$

Proof ideas:

- The determinant is a polynomial, so use the polynomial version of the mapping theorem to pass to $\mathbb{Z}/Q\mathbb{Z}$, for $Q$ a huge prime (depending on $n$).
- Generalize Tao-Vu approach to allow the entries to have different distributions and take values other than $\pm 1$.

# Application: bounding the singularity probability

**Theorem (Bourgain, Vu, W., 2008)**

*Let $D$ be a characteristic zero integral domain, and $M_n$ is an $n$ by $n$ random matrix with independent discrete entries taking values in $D$. Assume that for any entry $\alpha$, we have $\max_x \Pr(\alpha = x) \leq p$. Then*

$$\Pr(M_n \text{ is singular}) \leq \left(\sqrt{p} + o(1)\right)^n.$$

Proof ideas:

- The determinant is a polynomial, so use the polynomial version of the mapping theorem to pass to $\mathbb{Z}/Q\mathbb{Z}$, for $Q$ a huge prime (depending on $n$).
- Generalize Tao-Vu approach to allow the entries to have different distributions and take values other than $\pm 1$.
- A new idea gives the square root.

# Proof of the mapping theorem

**Main Theorem**

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.

Then, there exists an infinite sequence of primes with positive density such that for each prime $p$, there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

# Proof of the mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$, there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

**General Approach:** successively map $\mathbb{Z}[S]$ into various rings until we finally reach $\mathbb{Z}/p\mathbb{Z}$. Then let $\phi$ be the composition of all the maps.

# Proof of the mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$, there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

**General Approach:** successively map $\mathbb{Z}[S]$ into various rings until we finally reach $\mathbb{Z}/p\mathbb{Z}$. Then let $\phi$ be the composition of all the maps.

Three main ingredients:

# Proof of the mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$, there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

**General Approach:** successively map $\mathbb{Z}[S]$ into various rings until we finally reach $\mathbb{Z}/p\mathbb{Z}$. Then let $\phi$ be the composition of all the maps.

Three main ingredients:

1. The primitive element theorem (a result from algebra).

# Proof of the mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$, there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

**General Approach:** successively map $\mathbb{Z}[S]$ into various rings until we finally reach $\mathbb{Z}/p\mathbb{Z}$. Then let $\phi$ be the composition of all the maps.

Three main ingredients:

1. The primitive element theorem (a result from algebra).
2. Hilbert's Nullstellensatz (from algebraic geometry).

# Proof of the mapping theorem

## Main Theorem

Given: $S$ a finite subset of a characteristic zero integral domain $D$,
$L$ a finite set of non-zero elements of $\mathbb{Z}[S] \subset D$.
Then, there exists an infinite sequence of primes with positive density such that for each prime $p$, there exists a ring homomorphism $\phi : \mathbb{Z}[S] \to \mathbb{Z}/p\mathbb{Z}$ with $0 \notin \phi(L)$.

**General Approach:** successively map $\mathbb{Z}[S]$ into various rings until we finally reach $\mathbb{Z}/p\mathbb{Z}$. Then let $\phi$ be the composition of all the maps.

Three main ingredients:

1. The primitive element theorem (a result from algebra).
2. Hilbert's Nullstellensatz (from algebraic geometry).
3. Frobenius Density Theorem (or Chebotarev Density Theorem; a tool from number theory).