The probabilistic method

Mikhail Gabdullin

Steklov Mathematical Institute,
Krasovskii Institute of Mathematics and Mechanics

Yekaterinburg, 19th of December

The idea

Trivial observation: if $a_1, ..., a_n$ are real numbers such that

$$\sum_{i=1}^{n} a_i \geqslant 0,$$

then there exists j with $a_j \geqslant 0$.

It will be more convenient for us to write not a sum but average:

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant 0.$$

Analogously,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \leqslant 0 \quad \Longrightarrow \quad \exists a_j \leqslant 0.$$

Further,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant C \quad \Longleftrightarrow \quad \frac{1}{n}\sum_{i=1}^{n}(a_i - C) \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant C$$

(all the same with $\leqslant$, $>$ or $<$).

We can just take $C = \frac{1}{n}\sum_{i=1}^{n} a_i$.

Trivial observation: if $a_1, ..., a_n$ are real numbers such that

$$\sum_{i=1}^{n} a_i \geqslant 0,$$

then there exists j with $a_j \geqslant 0$.

It will be more convenient for us to write not a sum but average:

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant 0.$$

Analogously,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \leqslant 0 \quad \Longrightarrow \quad \exists a_j \leqslant 0.$$

Further,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant C \quad \Longleftrightarrow \quad \frac{1}{n}\sum_{i=1}^{n}(a_i - C) \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant C$$

(all the same with $\leqslant$, $>$ or $<$).

We can just take $C = \frac{1}{n}\sum_{i=1}^{n} a_i$.

Trivial observation: if $a_1, ..., a_n$ are real numbers such that

$$\sum_{i=1}^{n} a_i \geqslant 0,$$

then there exists j with $a_j \geqslant 0$.

It will be more convenient for us to write not a sum but average:

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant 0.$$

Analogously,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \leqslant 0 \quad \Longrightarrow \quad \exists a_j \leqslant 0.$$

Further,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant C \quad \Longleftrightarrow \quad \frac{1}{n}\sum_{i=1}^{n}(a_i - C) \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant C$$

(all the same with $\leqslant$, $>$ or $<$).

We can just take $C = \frac{1}{n}\sum_{i=1}^{n} a_i$.

Trivial observation: if $a_1, ..., a_n$ are real numbers such that

$$\sum_{i=1}^{n} a_i \geqslant 0,$$

then there exists j with $a_j \geqslant 0$.

It will be more convenient for us to write not a sum but average:

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant 0.$$

Analogously,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \leqslant 0 \quad \Longrightarrow \quad \exists a_j \leqslant 0.$$

Further,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant C \quad \Longleftrightarrow \quad \frac{1}{n}\sum_{i=1}^{n}(a_i - C) \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant C$$

(all the same with $\leqslant$, $>$ or$<$).

We can just take $C = \frac{1}{n}\sum_{i=1}^{n} a_i$.

Trivial observation: if $a_1, ..., a_n$ are real numbers such that

$$\sum_{i=1}^{n} a_i \geqslant 0,$$

then there exists j with $a_j \geqslant 0$.

It will be more convenient for us to write not a sum but average:

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant 0.$$

Analogously,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \leqslant 0 \quad \Longrightarrow \quad \exists a_j \leqslant 0.$$

Further,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant C \quad \Longleftrightarrow \quad \frac{1}{n}\sum_{i=1}^{n}(a_i - C) \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant C$$

(all the same with $\leqslant$, $>$ or$<$).

We can just take $C = \frac{1}{n}\sum_{i=1}^{n} a_i$.

Trivial observation: if $a_1, ..., a_n$ are real numbers such that

$$\sum_{i=1}^{n} a_i \geqslant 0,$$

then there exists j with $a_j \geqslant 0$.

It will be more convenient for us to write not a sum but average:

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant 0.$$

Analogously,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \leqslant 0 \quad \Longrightarrow \quad \exists a_j \leqslant 0.$$

Further,

$$\frac{1}{n}\sum_{i=1}^{n} a_i \geqslant C \quad \Longleftrightarrow \quad \frac{1}{n}\sum_{i=1}^{n}(a_i - C) \geqslant 0 \quad \Longrightarrow \quad \exists a_j \geqslant C$$

(all the same with $\leqslant$, $>$ or $<$).

We can just take $C = \frac{1}{n}\sum_{i=1}^{n} a_i$.

The first moment method

Theorem (The first moment method)

Let $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^{n} a_i$*. Then there exist* $a_i \geqslant \mathbb{E}a$ *and* $a_j \leqslant \mathbb{E}a$*. The same is true with* $\leqslant, >, <$ *instead of* $\geqslant$*.*

It is the most simple (but very useful) variant of probabilistic method.

Theorem (The first moment method)

Let $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^{n} a_i$. *Then there exist* $a_i \geqslant \mathbb{E}a$ *and* $a_j \leqslant \mathbb{E}a$. *The same is true with* $\leqslant, >, <$ *instead of* $\geqslant$.

It is the most simple (but very useful) variant of probabilistic method.

The pigeonhole principle:

Let $n+1$ rabbits be in n boxes (pigeons in holes). Then what?

Then some hole contains at least two pigeons.

Let j denote the number of a hole and a_j be the number of pigeons there. Then

$$\frac{1}{n}\sum_{j=1}^{n} a_j = \mathbb{E}a_j = \frac{n+1}{n} = 1 + 1/n$$

and there exists j with $a_j \geqslant 1 + 1/n$. Since a_j are integers, we can find $a_j \geqslant 2$.

More generally, if there are m pigeons in n holes, then

$$\mathbb{E}a_j = \frac{m}{n}$$

and there exist $a_i \leqslant \left\lfloor \frac{m}{n} \right\rfloor$ and $a_j \geqslant \left\lceil \frac{m}{n} \right\rceil$.

The pigeonhole principle:

Let $n+1$ rabbits be in n boxes (pigeons in holes). Then what?

Then some hole contains at least two pigeons.

Let j denote the number of a hole and a_j be the number of pigeons there. Then

$$\frac{1}{n}\sum_{j=1}^{n} a_j = \mathbb{E}a_j = \frac{n+1}{n} = 1 + 1/n$$

and there exists j with $a_j \geqslant 1 + 1/n$. Since a_j are integers, we can find $a_j \geqslant 2$.

More generally, if there are m pigeons in n holes, then

$$\mathbb{E}a_j = \frac{m}{n}$$

and there exist $a_i \leqslant \lfloor \frac{m}{n} \rfloor$ and $a_j \geqslant \lceil \frac{m}{n} \rceil$.

The pigeonhole principle:

Let $n+1$ rabbits be in n boxes (pigeons in holes). Then what?

Then some hole contains at least two pigeons.

Let j denote the number of a hole and a_j be the number of pigeons there. Then

$$\frac{1}{n}\sum_{j=1}^{n} a_j = \mathbb{E}a_j = \frac{n+1}{n} = 1 + 1/n$$

and there exists j with $a_j \geqslant 1 + 1/n$. Since a_j are integers, we can find $a_j \geqslant 2$.

More generally, if there are m pigeons in n holes, then

$$\mathbb{E}a_j = \frac{m}{n}$$

and there exist $a_i \leqslant \lfloor \frac{m}{n} \rfloor$ and $a_j \geqslant \lceil \frac{m}{n} \rceil$.

The pigeonhole principle:

Let $n+1$ rabbits be in n boxes (pigeons in holes). Then what?

Then some hole contains at least two pigeons.

Let j denote the number of a hole and a_j be the number of pigeons there. Then

$$\frac{1}{n}\sum_{j=1}^{n} a_j = \mathbb{E}a_j = \frac{n+1}{n} = 1+1/n$$

and there exists j with $a_j \geqslant 1+1/n$. Since a_j are integers, we can find $a_j \geqslant 2$.

More generally, if there are m pigeons in n holes, then

$$\mathbb{E}a_j = \frac{m}{n}$$

and there exist $a_i \leqslant \lfloor \frac{m}{n} \rfloor$ and $a_j \geqslant \lceil \frac{m}{n} \rceil$.

The pigeonhole principle:

Let $n+1$ rabbits be in n boxes (pigeons in holes). Then what?

Then some hole contains at least two pigeons.

Let j denote the number of a hole and a_j be the number of pigeons there. Then

$$\frac{1}{n}\sum_{j=1}^{n} a_j = \mathbb{E}a_j = \frac{n+1}{n} = 1 + 1/n$$

and there exists j with $a_j \geqslant 1 + 1/n$. Since a_j are integers, we can find $a_j \geqslant 2$.

More generally, if there are m pigeons in n holes, then

$$\mathbb{E}a_j = \frac{m}{n}$$

and there exist $a_i \leqslant \lfloor \frac{m}{n} \rfloor$ and $a_j \geqslant \lceil \frac{m}{n} \rceil$.

The pigeonhole principle:

Let $n+1$ rabbits be in n boxes (pigeons in holes). Then what?

Then some hole contains at least two pigeons.

Let j denote the number of a hole and a_j be the number of pigeons there. Then

$$\frac{1}{n}\sum_{j=1}^{n} a_j = \mathbb{E}a_j = \frac{n+1}{n} = 1 + 1/n$$

and there exists j with $a_j \geqslant 1 + 1/n$. Since a_j are integers, we can find $a_j \geqslant 2$.

More generally, if there are m pigeons in n holes, then

$$\mathbb{E}a_j = \frac{m}{n}$$

and there exist $a_i \leqslant \lfloor \frac{m}{n} \rfloor$ and $a_j \geqslant \lceil \frac{m}{n} \rceil$.

The pigeonhole principle:

Let $n+1$ rabbits be in n boxes (pigeons in holes). Then what?

Then some hole contains at least two pigeons.

Let j denote the number of a hole and a_j be the number of pigeons there. Then

$$\frac{1}{n}\sum_{j=1}^{n} a_j = \mathbb{E}a_j = \frac{n+1}{n} = 1 + 1/n$$

and there exists j with $a_j \geqslant 1 + 1/n$. Since a_j are integers, we can find $a_j \geqslant 2$.

More generally, if there are m pigeons in n holes, then

$$\mathbb{E}a_j = \frac{m}{n}$$

and there exist $a_i \leqslant \lfloor \frac{m}{n} \rfloor$ and $a_j \geqslant \lceil \frac{m}{n} \rceil$.

Example 2: Unit vectors

Suppose that $v_1, ..., v_n$ are vectors in a Hilbert space with $\|v_j\| = (v_j, v_j)^{1/2} = 1$. Then there exist numbers $\varepsilon_j \in \{\pm 1\}$ such that

$$\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| \geqslant n^{1/2}.$$

(the same true for $\leqslant n^{1/2}$).

(Note that these bounds cannot be improved: in the case when $\{v_j\}$ is an orthogonal system, we have $\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| = n^{1/2}$ for any choice of signs $\{\varepsilon_j\}$.)

Proof. Let us consider all possible 2^n n-tuples $(\varepsilon_1, ..., \varepsilon_n)$. We have

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = 2^{-n} \sum_{\varepsilon_1, \ldots, \varepsilon_n} \left(\sum_i \varepsilon_i v_i, \sum_j \varepsilon_j v_j \right) = \sum_{i,j} (v_i, v_j) 2^{-n} \sum_{\varepsilon_1, \ldots, \varepsilon_n} \varepsilon_i \varepsilon_j .$$

The inner sum (with fixed i, j) is equal to δ_{ij} (the Kronecker symbol); then

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = \sum_{i=1}^{n} (v_i, v_i) = n$$

and the claim follows.

Suppose that $v_1, ..., v_n$ are vectors in a Hilbert space with $\|v_j\| = (v_j, v_j)^{1/2} = 1$. Then there exist numbers $\varepsilon_j \in \{\pm 1\}$ such that

$$\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| \geqslant n^{1/2}.$$

(the same true for $\leqslant n^{1/2}$).

(Note that these bounds cannot be improved: in the case when $\{v_j\}$ is an orthogonal system, we have $\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| = n^{1/2}$ for any choice of signs $\{\varepsilon_j\}$.)

Proof. Let us consider all possible 2^n n-tuples $(\varepsilon_1, ..., \varepsilon_n)$. We have

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = 2^{-n} \sum_{\varepsilon_1,\ldots,\varepsilon_n} \left(\sum_i \varepsilon_i v_i, \sum_j \varepsilon_j v_j \right) = \sum_{i,j} (v_i, v_j) 2^{-n} \sum_{\varepsilon_1,\ldots,\varepsilon_n} \varepsilon_i \varepsilon_j.$$

The inner sum (with fixed i, j) is equal to δ_{ij} (the Kronecker symbol); then

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = \sum_{i=1}^n (v_i, v_i) = n$$

and the claim follows.

Example 2: Unit vectors

Suppose that $v_1, \dots, v_n$ are vectors in a Hilbert space with $\|v_j\| = (v_j, v_j)^{1/2} = 1$. Then there exist numbers $\varepsilon_j \in \{\pm 1\}$ such that

$$\|\varepsilon_1 v_1 + \dots + \varepsilon_n v_n\| \geqslant n^{1/2}.$$

(the same true for $\leqslant n^{1/2}$).

(Note that these bounds cannot be improved: in the case when $\{v_j\}$ is an orthogonal system, we have $\|\varepsilon_1 v_1 + \dots + \varepsilon_n v_n\| = n^{1/2}$ for any choice of signs $\{\varepsilon_j\}$.)

Proof. Let us consider all possible 2^n n-tuples $(\varepsilon_1, \dots, \varepsilon_n)$. We have

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = 2^{-n} \sum_{\varepsilon_1, \dots, \varepsilon_n} \left(\sum_i \varepsilon_i v_i, \sum_j \varepsilon_j v_j \right) = \sum_{i,j} (v_i, v_j) 2^{-n} \sum_{\varepsilon_1, \dots, \varepsilon_n} \varepsilon_i \varepsilon_j.$$

The inner sum (with fixed i, j) is equal to δ_{ij} (the Kronecker symbol); then

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = \sum_{i=1}^{n} (v_i, v_i) = n$$

and the claim follows.

Example 2: Unit vectors

Suppose that $v_1, ..., v_n$ are vectors in a Hilbert space with $\|v_j\| = (v_j, v_j)^{1/2} = 1$. Then there exist numbers $\varepsilon_j \in \{\pm 1\}$ such that

$$\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| \geqslant n^{1/2}.$$

(the same true for $\leqslant n^{1/2}$).

(Note that these bounds cannot be improved: in the case when $\{v_j\}$ is an orthogonal system, we have $\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| = n^{1/2}$ for any choice of signs $\{\varepsilon_j\}$.)

Proof. Let us consider all possible 2^n n-tuples $(\varepsilon_1, ..., \varepsilon_n)$. We have

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = 2^{-n} \sum_{\varepsilon_1, \ldots, \varepsilon_n} \left(\sum_i \varepsilon_i v_i, \sum_j \varepsilon_j v_j \right) = \sum_{i,j} (v_i, v_j) 2^{-n} \sum_{\varepsilon_1, \ldots, \varepsilon_n} \varepsilon_i \varepsilon_j.$$

The inner sum (with fixed i, j) is equal to δ_{ij} (the Kronecker symbol); then

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = \sum_{i=1}^{n} (v_i, v_i) = n$$

and the claim follows.

Suppose that $v_1, ..., v_n$ are vectors in a Hilbert space with $\|v_j\| = (v_j, v_j)^{1/2} = 1$. Then there exist numbers $\varepsilon_j \in \{\pm 1\}$ such that

$$\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| \geqslant n^{1/2}.$$

(the same true for $\leqslant n^{1/2}$).

(Note that these bounds cannot be improved: in the case when $\{v_j\}$ is an orthogonal system, we have $\|\varepsilon_1 v_1 + ... + \varepsilon_n v_n\| = n^{1/2}$ for any choice of signs $\{\varepsilon_j\}$.)

Proof. Let us consider all possible 2^n n-tuples $(\varepsilon_1, ..., \varepsilon_n)$. We have

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = 2^{-n} \sum_{\varepsilon_1, \dots, \varepsilon_n} \left(\sum_i \varepsilon_i v_i, \sum_j \varepsilon_j v_j \right) = \sum_{i,j} (v_i, v_j) 2^{-n} \sum_{\varepsilon_1, \dots, \varepsilon_n} \varepsilon_i \varepsilon_j.$$

The inner sum (with fixed i, j) is equal to δ_{ij} (the Kronecker symbol); then

$$\mathbb{E}\|\sum_i \varepsilon_i v_i\|^2 = \sum_{i=1}^{n} (v_i, v_i) = n$$

and the claim follows.

There are arbitrary long strings of consecutive positive integers with no primes: for $n \geqslant 2$, the string $n!+2, ..., n!+n$ gives us such an example. It is interesting to obtain a quantitative analog of this statement. Define

$$G(X) := \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

The largest n with $n! + n = \exp(n \log n(1+o(1)) \leqslant X$ is of order $\frac{\log X}{\log \log X}$; so the above example gives us $G(X) \gg \frac{\log X}{\log \log X}$.

But this is worse than a trivial bound! Since $\pi(X) = \frac{X}{\log X}(1+o(1))$, we have

$$\mathbb{E}(p_{n+1} - p_n) = \frac{1}{\pi(X)} \sum_{p_{n+1} \leqslant X} (p_{n+1} - p_n) = \frac{p_{n+1} - 2}{\pi(X)} \gg \log X$$

and therefore $G(X) \gg \log X$. On the other hand, it is not constructive; but in fact we can easily improve the previous construction to get the same bound.

Note that for $X = \prod_{q \leqslant p} q$ all numbers $X+2, ..., X+p$ are composite and $X = \exp((1+o(1))p)$; hence $G(X) \gg \log X$.

There are arbitrary long strings of consecutive positive integers with no primes: for $n \geqslant 2$, the string $n! + 2, ..., n! + n$ gives us such an example. It is interesting to obtain a quantitative analog of this statement. Define

$$G(X) := \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

The largest n with $n! + n = \exp(n \log n(1 + o(1)) \leqslant X$ is of order $\frac{\log X}{\log\log X}$; so the above example gives us $G(X) \gg \frac{\log X}{\log\log X}$.

But this is worse than a trivial bound! Since $\pi(X) = \frac{X}{\log X}(1 + o(1))$, we have

$$\mathbb{E}(p_{n+1} - p_n) = \frac{1}{\pi(X)} \sum_{p_{n+1} \leqslant X} (p_{n+1} - p_n) = \frac{p_{n+1} - 2}{\pi(X)} \gg \log X$$

and therefore $G(X) \gg \log X$. On the other hand, it is not constructive; but in fact we can easily improve the previous construction to get the same bound.

Note that for $X = \prod_{q \leqslant p} q$ all numbers $X + 2, ..., X + p$ are composite and $X = \exp((1 + o(1))p)$; hence $G(X) \gg \log X$.

There are arbitrary long strings of consecutive positive integers with no primes: for $n \geqslant 2$, the string $n!+2, \dots, n!+n$ gives us such an example. It is interesting to obtain a quantitative analog of this statement. Define

$$G(X) := \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

The largest n with $n! + n = \exp(n \log n(1+o(1)) \leqslant X$ is of order $\frac{\log X}{\log \log X}$; so the above example gives us $G(X) \gg \frac{\log X}{\log \log X}$.

But this is worse than a trivial bound! Since $\pi(X) = \frac{X}{\log X}(1+o(1))$, we have

$$\mathbb{E}(p_{n+1} - p_n) = \frac{1}{\pi(X)} \sum_{p_{n+1} \leqslant X} (p_{n+1} - p_n) = \frac{p_{n+1} - 2}{\pi(X)} \gg \log X$$

and therefore $G(X) \gg \log X$. On the other hand, it is not constructive; but in fact we can easily improve the previous construction to get the same bound.

Note that for $X = \prod_{q \leqslant p} q$ all numbers $X+2, \dots, X+p$ are composite and $X = \exp((1+o(1))p)$; hence $G(X) \gg \log X$.

There are arbitrary long strings of consecutive positive integers with no primes: for $n \geqslant 2$, the string $n! + 2, ..., n! + n$ gives us such an example. It is interesting to obtain a quantitative analog of this statement. Define

$$G(X) := \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

The largest n with $n! + n = \exp(n \log n(1 + o(1)) \leqslant X$ is of order $\frac{\log X}{\log \log X}$; so the above example gives us $G(X) \gg \frac{\log X}{\log \log X}$.

But this is worse than a trivial bound! Since $\pi(X) = \frac{X}{\log X}(1 + o(1))$, we have

$$\mathbb{E}(p_{n+1} - p_n) = \frac{1}{\pi(X)} \sum_{p_{n+1} \leqslant X} (p_{n+1} - p_n) = \frac{p_{n+1} - 2}{\pi(X)} \gg \log X$$

and therefore $G(X) \gg \log X$. On the other hand, it is not constructive; but in fact we can easily improve the previous construction to get the same bound.

Note that for $X = \prod_{q \leqslant p} q$ all numbers $X + 2, ..., X + p$ are composite and $X = \exp((1 + o(1))p)$; hence $G(X) \gg \log X$.

Example 3: Large gaps between primes

There are arbitrary long strings of consecutive positive integers with no primes: for $n \geqslant 2$, the string $n! + 2, ..., n! + n$ gives us such an example. It is interesting to obtain a quantitative analog of this statement. Define

$$G(X) := \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

The largest n with $n! + n = \exp(n \log n(1 + o(1)) \leqslant X$ is of order $\frac{\log X}{\log \log X}$; so the above example gives us $G(X) \gg \frac{\log X}{\log \log X}$.

But this is worse than a trivial bound! Since $\pi(X) = \frac{X}{\log X}(1 + o(1))$, we have

$$\mathbb{E}(p_{n+1} - p_n) = \frac{1}{\pi(X)} \sum_{p_{n+1} \leqslant X} (p_{n+1} - p_n) = \frac{p_{n+1} - 2}{\pi(X)} \gg \log X$$

and therefore $G(X) \gg \log X$. On the other hand, it is not constructive; but in fact we can easily improve the previous construction to get the same bound.

Note that for $X = \prod_{q \leqslant p} q$ all numbers $X + 2, ..., X + p$ are composite and $X = \exp((1 + o(1))p)$; hence $G(X) \gg \log X$.

Example 3: Large gaps between primes

There are arbitrary long strings of consecutive positive integers with no primes: for $n \geqslant 2$, the string $n! + 2, ..., n! + n$ gives us such an example. It is interesting to obtain a quantitative analog of this statement. Define

$$G(X) := \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

The largest n with $n! + n = \exp(n \log n(1 + o(1)) \leqslant X$ is of order $\frac{\log X}{\log\log X}$; so the above example gives us $G(X) \gg \frac{\log X}{\log\log X}$.

But this is worse than a trivial bound! Since $\pi(X) = \frac{X}{\log X}(1 + o(1))$, we have

$$\mathbb{E}(p_{n+1} - p_n) = \frac{1}{\pi(X)} \sum_{p_{n+1} \leqslant X} (p_{n+1} - p_n) = \frac{p_{n+1} - 2}{\pi(X)} \gg \log X$$

and therefore $G(X) \gg \log X$. On the other hand, it is not constructive; but in fact we can easily improve the previous construction to get the same bound.

Note that for $X = \prod_{q \leqslant p} q$ all numbers $X + 2, ..., X + p$ are composite and $X = \exp((1 + o(1))p)$; hence $G(X) \gg \log X$.

There are arbitrary long strings of consecutive positive integers with no primes: for $n \geqslant 2$, the string $n! + 2, ..., n! + n$ gives us such an example. It is interesting to obtain a quantitative analog of this statement. Define

$$G(X) := \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

The largest n with $n! + n = \exp(n \log n(1 + o(1)) \leqslant X$ is of order $\frac{\log X}{\log \log X}$; so the above example gives us $G(X) \gg \frac{\log X}{\log \log X}$.

But this is worse than a trivial bound! Since $\pi(X) = \frac{X}{\log X}(1 + o(1))$, we have

$$\mathbb{E}(p_{n+1} - p_n) = \frac{1}{\pi(X)} \sum_{p_{n+1} \leqslant X} (p_{n+1} - p_n) = \frac{p_{n+1} - 2}{\pi(X)} \gg \log X$$

and therefore $G(X) \gg \log X$. On the other hand, it is not constructive; but in fact we can easily improve the previous construction to get the same bound.

Note that for $X = \prod_{q \leqslant p} q$ all numbers $X + 2, ..., X + p$ are composite and $X = \exp((1 + o(1))p)$; hence $G(X) \gg \log X$.

In fact, using the Chinese Remainder Theorem (and being much more clever — some information about smooth numbers and some variants of sieve methods are needed) it is possible prove the following.

Theorem (Erdös-Rankin, 1938; "deterministic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}.$$

Erdös suggested 10000$ for anyone who can prove that

$$G(X) \gg f(X) \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}$$

for some function $f(X) \to \infty$ as $X \to \infty$.

Theorem (Ford, Green, Konyagin, Maynard, Tao, 2018; "deterministic-probabilistic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{\log_3 X}.$$

In fact, using the Chinese Remainder Theorem (and being much more clever — some information about smooth numbers and some variants of sieve methods are needed) it is possible prove the following.

Theorem (Erdös-Rankin, 1938; "deterministic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}.$$

Erdös suggested 10000$ for anyone who can prove that

$$G(X) \gg f(X) \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}$$

for some function $f(X) \to \infty$ as $X \to \infty$.

Theorem (Ford, Green, Konyagin, Maynard, Tao, 2018; "deterministic-probabilistic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{\log_3 X}.$$

Example 3: Large gaps between primes: want larger!

In fact, using the Chinese Remainder Theorem (and being much more clever — some information about smooth numbers and some variants of sieve methods are needed) it is possible prove the following.

Theorem (Erdös-Rankin, 1938; "deterministic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}.$$

Erdös suggested 10000$ for anyone who can prove that

$$G(X) \gg f(X) \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}$$

for some function $f(X) \to \infty$ as $X \to \infty$.

Theorem (Ford, Green, Konyagin, Maynard, Tao, 2018; "deterministic-probabilistic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{\log_3 X}.$$

Example 3: Large gaps between primes: want larger!

In fact, using the Chinese Remainder Theorem (and being much more clever — some information about smooth numbers and some variants of sieve methods are needed) it is possible prove the following.

Theorem (Erdös-Rankin, 1938; "deterministic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}.$$

Erdös suggested 10000$ for anyone who can prove that

$$G(X) \gg f(X) \log X \frac{\log_2 X \log_4 X}{(\log_3 X)^2}$$

for some function $f(X) \to \infty$ as $X \to \infty$.

Theorem (Ford, Green, Konyagin, Maynard, Tao, 2018; "deterministic-probabilistic construction")

We have

$$G(X) \gg \log X \frac{\log_2 X \log_4 X}{\log_3 X}.$$

Let q be a prime and $(ab,q)=1$. Define

$$S_q(a,b)=\sum_{x=1}^{q-1}\exp\left(\frac{2\pi i}{q}(ax^*+bx)\right),$$

where $e_q(u)=\exp\left(\frac{2\pi iu}{q}\right)$ and $x^*x\equiv 1 \pmod q$. Upper estimates of such sums are crucial for finding the asymptotics for the number of solutions of the equation

$$x_1^2+x_2^2+x_3^2+x_4^2=N.$$

The best possible result is due to A.Weil:

$$|S_q(a,b)|\leqslant 2q^{1/2}.$$

Here one cannot replace 2 by $2-\varepsilon$. For now, we can easily show that one cannot replace 2 by $1-\varepsilon$: let $a=1$ and b be chosen uniformly at random from $0,...,q-1$ (in fact, $S_q(a,b)=S_q(1,ab)$ and we can assume $a=1$ wlog). Then (in the last sum the pairs (x,y) with $x=y$ contribute only)

$$\mathbb{E}|S_q(1,b)|^2=\frac{1}{q}\sum_{b=0}^{q-1}|S_q(1,b)|^2=\frac{1}{q}\sum_{b=0}^{q-1}\sum_{x,y=1}^{q-1}e_q(x^*-y^*+bx-by)=$$

$$\sum_{x,y=1}^{q-1}e_q(x^*-y^*)\frac{1}{q}\sum_{b=0}^{q-1}e_q(b(x-y))=q-1.$$

Let q be a prime and $(ab,q)=1$. Define

$$S_q(a,b)=\sum_{x=1}^{q-1}\exp\left(\frac{2\pi i}{q}(ax^*+bx)\right),$$

where $e_q(u)=\exp\left(\frac{2\pi iu}{q}\right)$ and $x^*x\equiv 1 \pmod q$. Upper estimates of such sums are crucial for finding the asymptotics for the number of solutions of the equation

$$x_1^2+x_2^2+x_3^2+x_4^2=N.$$

The best possible result is due to A.Weil:

$$|S_q(a,b)|\leqslant 2q^{1/2}.$$

Here one cannot replace 2 by $2-\varepsilon$. For now, we can easily show that one cannot replace 2 by $1-\varepsilon$: let $a=1$ and b be chosen uniformly at random from $0,...,q-1$ (in fact, $S_q(a,b)=S_q(1,ab)$ and we can assume $a=1$ wlog). Then (in the last sum the pairs (x,y) with $x=y$ contribute only)

$$\mathbb{E}|S_q(1,b)|^2=\frac{1}{q}\sum_{b=0}^{q-1}|S_q(1,b)|^2=\frac{1}{q}\sum_{b=0}^{q-1}\sum_{x,y=1}^{q-1}e_q(x^*-y^*+bx-by)=$$

$$\sum_{x,y=1}^{q-1}e_q(x^*-y^*)\frac{1}{q}\sum_{b=0}^{q-1}e_q(b(x-y))=q-1.$$

Let q be a prime and $(ab,q)=1$. Define

$$S_q(a,b)=\sum_{x=1}^{q-1}\exp\left(\frac{2\pi i}{q}(ax^*+bx)\right),$$

where $e_q(u)=\exp\left(\frac{2\pi iu}{q}\right)$ and $x^*x\equiv 1 \pmod q$. Upper estimates of such sums are crucial for finding the asymptotics for the number of solutions of the equation

$$x_1^2+x_2^2+x_3^2+x_4^2=N.$$

The best possible result is due to A.Weil:

$$|S_q(a,b)|\leqslant 2q^{1/2}.$$

Here one cannot replace 2 by $2-\varepsilon$. For now, we can easily show that one cannot replace 2 by $1-\varepsilon$: let $a=1$ and b be chosen uniformly at random from $0,...,q-1$ (in fact, $S_q(a,b)=S_q(1,ab)$ and we can assume $a=1$ wlog). Then (in the last sum the pairs (x,y) with $x=y$ contribute only)

$$\mathbb{E}|S_q(1,b)|^2=\frac{1}{q}\sum_{b=0}^{q-1}|S_q(1,b)|^2=\frac{1}{q}\sum_{b=0}^{q-1}\sum_{x,y=1}^{q-1}e_q(x^*-y^*+bx-by)=$$

$$\sum_{x,y=1}^{q-1}e_q(x^*-y^*)\frac{1}{q}\sum_{b=0}^{q-1}e_q(b(x-y))=q-1.$$

Let q be a prime and $(ab, q) = 1$. Define

$$S_q(a,b) = \sum_{x=1}^{q-1} \exp\left(\frac{2\pi i}{q}(ax^* + bx)\right),$$

where $e_q(u) = \exp\left(\frac{2\pi i u}{q}\right)$ and $x^* x \equiv 1 \pmod{q}$. Upper estimates of such sums are crucial for finding the asymptotics for the number of solutions of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = N.$$

The best possible result is due to A.Weil:

$$|S_q(a,b)| \leqslant 2q^{1/2}.$$

Here one cannot replace 2 by $2-\varepsilon$. For now, we can easily show that one cannot replace 2 by $1-\varepsilon$: let $a = 1$ and b be chosen uniformly at random from $0, ..., q-1$ (in fact, $S_q(a,b) = S_q(1, ab)$ and we can assume $a = 1$ wlog). Then (in the last sum the pairs (x,y) with $x = y$ contribute only)

$$\mathbb{E}|S_q(1,b)|^2 = \frac{1}{q}\sum_{b=0}^{q-1} |S_q(1,b)|^2 = \frac{1}{q}\sum_{b=0}^{q-1}\sum_{x,y=1}^{q-1} e_q(x^* - y^* + bx - by) =$$

$$\sum_{x,y=1}^{q-1} e_q(x^* - y^*)\frac{1}{q}\sum_{b=0}^{q-1} e_q(b(x-y)) = q-1.$$

Example 4: Large Kloosterman's sums

Let q be a prime and $(ab, q) = 1$. Define

$$S_q(a,b) = \sum_{x=1}^{q-1} \exp\left(\frac{2\pi i}{q}(ax^* + bx)\right),$$

where $e_q(u) = \exp\left(\frac{2\pi i u}{q}\right)$ and $x^* x \equiv 1 \pmod q$. Upper estimates of such sums are crucial for finding the asymptotics for the number of solutions of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = N.$$

The best possible result is due to A.Weil:

$$|S_q(a,b)| \leqslant 2q^{1/2}.$$

Here one cannot replace 2 by $2-\varepsilon$. For now, we can easily show that one cannot replace 2 by $1-\varepsilon$: let $a=1$ and b be chosen uniformly at random from $0, ..., q-1$ (in fact, $S_q(a,b) = S_q(1,ab)$ and we can assume $a=1$ wlog). Then (in the last sum the pairs (x,y) with $x=y$ contribute only)

$$\mathbb{E}|S_q(1,b)|^2 = \frac{1}{q}\sum_{b=0}^{q-1}|S_q(1,b)|^2 = \frac{1}{q}\sum_{b=0}^{q-1}\sum_{x,y=1}^{q-1} e_q(x^* - y^* + bx - by) =$$

$$\sum_{x,y=1}^{q-1} e_q(x^* - y^*)\frac{1}{q}\sum_{b=0}^{q-1} e_q(b(x-y)) = q-1.$$

Let q be a prime and $(ab, q) = 1$. Define

$$S_q(a,b) = \sum_{x=1}^{q-1} \exp\left(\frac{2\pi i}{q}(ax^* + bx)\right),$$

where $e_q(u) = \exp\left(\frac{2\pi i u}{q}\right)$ and $x^* x \equiv 1 \pmod{q}$. Upper estimates of such sums are crucial for finding the asymptotics for the number of solutions of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = N.$$

The best possible result is due to A.Weil:

$$|S_q(a,b)| \leqslant 2q^{1/2}.$$

Here one cannot replace 2 by $2-\varepsilon$. For now, we can easily show that one cannot replace 2 by $1-\varepsilon$: let $a=1$ and b be chosen uniformly at random from $0, \dots, q-1$ (in fact, $S_q(a,b) = S_q(1,ab)$ and we can assume $a=1$ wlog). Then (in the last sum the pairs (x,y) with $x=y$ contribute only)

$$\mathbb{E}|S_q(1,b)|^2 = \frac{1}{q}\sum_{b=0}^{q-1}|S_q(1,b)|^2 = \frac{1}{q}\sum_{b=0}^{q-1}\sum_{x,y=1}^{q-1} e_q(x^* - y^* + bx - by) =$$

$$\sum_{x,y=1}^{q-1} e_q(x^* - y^*)\frac{1}{q}\sum_{b=0}^{q-1} e_q(b(x-y)) = q-1.$$

Thus there exists $b \in \mathbb{Z}_q$ such that $|S_q(1,b)|^2 \geqslant q-1$; it remains to note that $S(1,0) = -1$ and hence this b is not 0.

So, there are $b \in \mathbb{Z}_q^*$ with $|S_q(1,b)| \geqslant \sqrt{q-1}$.

How many b do we have with, say, $|S_q(1,b)| \geqslant 0.5q^{1/2}$?

Turn to the so-called ***popularity principle:***

Theorem (The popularity principle)

Suppose that $a_i \leqslant M$ *and set* $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^n a_i$. *Then* $\mathbb{P}(a_i > 0.5\mathbb{E}a) \geqslant \frac{\mathbb{E}a}{2M}$.

Proof. Obviously,

$$\frac{1}{n}\sum_{i:a_i \leqslant 0.5\mathbb{E}a} a_i \leqslant 0.5\mathbb{E}a.$$

Hence,

$$\frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

But since $a_i \leqslant M$

$$M\mathbb{P}(a_i > 0.5\mathbb{E}a) = M\frac{1}{n}\#\{i : a_i > 0.5\mathbb{E}a\} \geqslant \frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

Thus there exists $b \in \mathbb{Z}_q$ such that $|S_q(1,b)|^2 \geqslant q-1$; it remains to note that $S(1,0) = -1$ and hence this b is not 0.

So, there are $b \in \mathbb{Z}_q^*$ with $|S_q(1,b)| \geqslant \sqrt{q-1}$.

How many b do we have with, say, $|S_q(1,b)| \geqslant 0.5q^{1/2}$?

Turn to the so-called ***popularity principle:***

Theorem (The popularity principle)

Suppose that $a_i \leqslant M$ and set $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^n a_i$. Then $\mathbb{P}(a_i > 0.5\mathbb{E}a) \geqslant \frac{\mathbb{E}a}{2M}$.

Proof. Obviously,

$$\frac{1}{n}\sum_{i:a_i \leqslant 0.5\mathbb{E}a} a_i \leqslant 0.5\mathbb{E}a.$$

Hence,

$$\frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

But since $a_i \leqslant M$

$$M\mathbb{P}(a_i > 0.5\mathbb{E}a) = M\frac{1}{n}\#\{i : a_i > 0.5\mathbb{E}a\} \geqslant \frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

Thus there exists $b \in \mathbb{Z}_q$ such that $|S_q(1,b)|^2 \geqslant q-1$; it remains to note that $S(1,0) = -1$ and hence this b is not 0.

So, there are $b \in \mathbb{Z}_q^*$ with $|S_q(1,b)| \geqslant \sqrt{q-1}$.

How many b do we have with, say, $|S_q(1,b)| \geqslant 0.5q^{1/2}$?

Turn to the so-called ***popularity principle:***

Theorem (The popularity principle)

Suppose that $a_i \leqslant M$ *and set* $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^{n} a_i$. *Then* $\mathbb{P}(a_i > 0.5\mathbb{E}a) \geqslant \frac{\mathbb{E}a}{2M}$.

Proof. Obviously,

$$\frac{1}{n}\sum_{i:a_i \leqslant 0.5\mathbb{E}a} a_i \leqslant 0.5\mathbb{E}a.$$

Hence,

$$\frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

But since $a_i \leqslant M$

$$M\mathbb{P}(a_i > 0.5\mathbb{E}a) = M\frac{1}{n}\#\{i : a_i > 0.5\mathbb{E}a\} \geqslant \frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

Thus there exists $b \in \mathbb{Z}_q$ such that $|S_q(1,b)|^2 \geqslant q-1$; it remains to note that $S(1,0) = -1$ and hence this b is not 0.

So, there are $b \in \mathbb{Z}_q^*$ with $|S_q(1,b)| \geqslant \sqrt{q-1}$.

How many b do we have with, say, $|S_q(1,b)| \geqslant 0.5q^{1/2}$?

Turn to the so-called ***popularity principle:***

Theorem (The popularity principle)

Suppose that $a_i \leqslant M$ *and set* $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^n a_i$. *Then* $\mathbb{P}(a_i > 0.5\mathbb{E}a) \geqslant \frac{\mathbb{E}a}{2M}$.

Proof. Obviously,

$$\frac{1}{n}\sum_{i:a_i \leqslant 0.5\mathbb{E}a} a_i \leqslant 0.5\mathbb{E}a.$$

Hence,

$$\frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

But since $a_i \leqslant M$

$$M\mathbb{P}(a_i > 0.5\mathbb{E}a) = M\frac{1}{n}\#\{i : a_i > 0.5\mathbb{E}a\} \geqslant \frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

Thus there exists $b \in \mathbb{Z}_q$ such that $|S_q(1,b)|^2 \geqslant q-1$; it remains to note that $S(1,0) = -1$ and hence this b is not 0.

So, there are $b \in \mathbb{Z}_q^*$ with $|S_q(1,b)| \geqslant \sqrt{q-1}$.

How many b do we have with, say, $|S_q(1,b)| \geqslant 0.5q^{1/2}$?

Turn to the so-called ***popularity principle:***

Theorem (The popularity principle)

Suppose that $a_i \leqslant M$ *and set* $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^{n} a_i$. *Then* $\mathbb{P}(a_i > 0.5\mathbb{E}a) \geqslant \frac{\mathbb{E}a}{2M}$.

Proof. Obviously,

$$\frac{1}{n}\sum_{i:a_i \leqslant 0.5\mathbb{E}a} a_i \leqslant 0.5\mathbb{E}a.$$

Hence,

$$\frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

But since $a_i \leqslant M$

$$M\mathbb{P}(a_i > 0.5\mathbb{E}a) = M\frac{1}{n}\#\{i : a_i > 0.5\mathbb{E}a\} \geqslant \frac{1}{n}\sum_{i:a_i > 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

Thus there exists $b \in \mathbb{Z}_q$ such that $|S_q(1,b)|^2 \geqslant q-1$; it remains to note that $S(1,0) = -1$ and hence this b is not 0.

So, there are $b \in \mathbb{Z}_q^*$ with $|S_q(1,b)| \geqslant \sqrt{q-1}$.

How many b do we have with, say, $|S_q(1,b)| \geqslant 0.5q^{1/2}$?

Turn to the so-called ***popularity principle:***

Theorem (The popularity principle)

Suppose that $a_i \leqslant M$ *and set* $\mathbb{E}a := \frac{1}{n}\sum_{i=1}^n a_i$. *Then* $\mathbb{P}(a_i > 0.5\mathbb{E}a) \geqslant \frac{\mathbb{E}a}{2M}$.

Proof. Obviously,

$$\frac{1}{n}\sum_{i:a_i\leqslant 0.5\mathbb{E}a} a_i \leqslant 0.5\mathbb{E}a.$$

Hence,

$$\frac{1}{n}\sum_{i:a_i> 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

But since $a_i \leqslant M$

$$M\mathbb{P}(a_i > 0.5\mathbb{E}a) = M\frac{1}{n}\#\{i : a_i > 0.5\mathbb{E}a\} \geqslant \frac{1}{n}\sum_{i:a_i> 0.5\mathbb{E}a} a_i \geqslant 0.5\mathbb{E}a.$$

Recall that (a great theorem)

$$|S_q(1,b)| \leqslant 2q^{1/2};$$

so we have

$$|S_q(1,b)|^2 \leqslant 4q =: M.$$

Also (and that is almost trivial and was shown by us)

$$\mathbb{E}|S_q(1,b)|^2 = q-1.$$

Then by the popularity principle we have

$$\mathbb{P}\left(|S_q(1,b)|^2 \geqslant 0.5(q-1)\right) \geqslant \frac{q-1}{8q}.$$

Fix a large q. Then

$$\mathbb{P}\left(|S_q(1,b)| \geqslant \sqrt{0.5(q-1)}\right) \geqslant \frac{1}{8} - \frac{1}{8q} > 0.12.$$

So for a positive proportion of b we proved the inequality $|S_q(1,b)| \geqslant 0.7q^{1/2}$!

Large Kloosterman's sums are popular! (and we get it «for free»!)

Recall that (a great theorem)

$$|S_q(1,b)| \leqslant 2q^{1/2};$$

so we have

$$|S_q(1,b)|^2 \leqslant 4q =: M.$$

Also (and that is almost trivial and was shown by us)

$$\mathbb{E}|S_q(1,b)|^2 = q-1.$$

Then by the popularity principle we have

$$\mathbb{P}\left(|S_q(1,b)|^2 \geqslant 0.5(q-1)\right) \geqslant \frac{q-1}{8q}.$$

Fix a large q. Then

$$\mathbb{P}\left(|S_q(1,b)| \geqslant \sqrt{0.5(q-1)}\right) \geqslant \frac{1}{8} - \frac{1}{8q} > 0.12.$$

So for a positive proportion of b we proved the inequality $|S_q(1,b)| \geqslant 0.7q^{1/2}$!

Large Kloosterman's sums are popular! (and we get it «for free»!)

Recall that (a great theorem)

$$|S_q(1,b)| \leqslant 2q^{1/2};$$

so we have

$$|S_q(1,b)|^2 \leqslant 4q =: M.$$

Also (and that is almost trivial and was shown by us)

$$\mathbb{E}|S_q(1,b)|^2 = q-1.$$

Then by the popularity principle we have

$$\mathbb{P}\left(|S_q(1,b)|^2 \geqslant 0.5(q-1)\right) \geqslant \frac{q-1}{8q}.$$

Fix a large q. Then

$$\mathbb{P}\left(|S_q(1,b)| \geqslant \sqrt{0.5(q-1)}\right) \geqslant \frac{1}{8} - \frac{1}{8q} > 0.12.$$

So for a positive proportion of b we proved the inequality $|S_q(1,b)| \geqslant 0.7q^{1/2}$!

Large Kloosterman's sums are popular! (and we get it «for free»!)

Recall that (a great theorem)

$$|S_q(1,b)| \leqslant 2q^{1/2};$$

so we have

$$|S_q(1,b)|^2 \leqslant 4q =: M.$$

Also (and that is almost trivial and was shown by us)

$$\mathbb{E}|S_q(1,b)|^2 = q-1.$$

Then by the popularity principle we have

$$\mathbb{P}\left(|S_q(1,b)|^2 \geqslant 0.5(q-1)\right) \geqslant \frac{q-1}{8q}.$$

Fix a large q. Then

$$\mathbb{P}\left(|S_q(1,b)| \geqslant \sqrt{0.5(q-1)}\right) \geqslant \frac{1}{8} - \frac{1}{8q} > 0.12.$$

So for a positive proportion of b we proved the inequality $|S_q(1,b)| \geqslant 0.7q^{1/2}$!

Large Kloosterman's sums are popular! (and we get it «for free»!)

Recall that (a great theorem)

$$|S_q(1,b)| \leqslant 2q^{1/2};$$

so we have

$$|S_q(1,b)|^2 \leqslant 4q =: M.$$

Also (and that is almost trivial and was shown by us)

$$\mathbb{E}|S_q(1,b)|^2 = q-1.$$

Then by the popularity principle we have

$$\mathbb{P}\left(|S_q(1,b)|^2 \geqslant 0.5(q-1)\right) \geqslant \frac{q-1}{8q}.$$

Fix a large q. Then

$$\mathbb{P}\left(|S_q(1,b)| \geqslant \sqrt{0.5(q-1)}\right) \geqslant \frac{1}{8} - \frac{1}{8q} > 0.12.$$

So for a positive proportion of b we proved the inequality $|S_q(1,b)| \geqslant 0.7q^{1/2}$!

Large Kloosterman's sums are popular! (and we get it «for free»!)

Recall that (a great theorem)

$$|S_q(1,b)| \leqslant 2q^{1/2};$$

so we have

$$|S_q(1,b)|^2 \leqslant 4q =: M.$$

Also (and that is almost trivial and was shown by us)

$$\mathbb{E}|S_q(1,b)|^2 = q-1.$$

Then by the popularity principle we have

$$\mathbb{P}\left(|S_q(1,b)|^2 \geqslant 0.5(q-1)\right) \geqslant \frac{q-1}{8q}.$$

Fix a large q. Then

$$\mathbb{P}\left(|S_q(1,b)| \geqslant \sqrt{0.5(q-1)}\right) \geqslant \frac{1}{8} - \frac{1}{8q} > 0.12.$$

So for a positive proportion of b we proved the inequality $|S_q(1,b)| \geqslant 0.7q^{1/2}$!

Large Kloosterman's sums are popular! (and we get it «for free»!)

In fact, using the probabilistic method we can prove not only that a function takes large values. We can prove that some objects do exist!

Toy problem.
Suppose there will be held two conferences on Analytic Number Theory simultaneously with 60 (!) sections. Suppose also that for each section there are at least 7 scientists who are specialists in the corresponding topics. Is it possible to distribute them so that for both conferences all of its sections will not be empty?

Yes!
Let us assign a scientist to each conference with probability $1/2$. Let E_A be the event that a section A of one of the conferences is empty. The probability of E_A is at most 2^{-7}; the probability of ***existence*** of an empty section is

$$\mathbb{P}(\cup_A E_A) \leqslant \sum_A \mathbb{P}(E_A) \leqslant 2 \cdot 60 \cdot 2^{-7} = 120/128 < 1.$$

If there are n scientists, then we have 2^n possibilities and hence there are at least $2^n(1 - 120/128) = 2^{n-4}$ rearrangements of participants with no empty sections.

Again, we proved not only the existence of such rearrangement: we proved that there are many of them.

In fact, using the probabilistic method we can prove not only that a function takes large values. We can prove that some objects do exist!

Toy problem.
Suppose there will be held two conferences on Analytic Number Theory simultaneously with 60 (!) sections. Suppose also that for each section there are at least 7 scientists who are specialists in the corresponding topics. Is it possible to distribute them so that for both conferences all of its sections will not be empty?

Yes!
Let us assign a scientist to each conference with probability $1/2$. Let E_A be the event that a section A of one of the conferences is empty. The probability of E_A is at most 2^{-7}; the probability of ***existence*** of an empty section is

$$\mathbb{P}(\cup_A E_A) \leqslant \sum_A \mathbb{P}(E_A) \leqslant 2 \cdot 60 \cdot 2^{-7} = 120/128 < 1.$$

If there are n scientists, then we have 2^n possibilities and hence there are at least $2^n(1 - 120/128) = 2^{n-4}$ rearrangements of participants with no empty sections.

Again, we proved not only the existence of such rearrangement: we proved that there are many of them.

In fact, using the probabilistic method we can prove not only that a function takes large values. We can prove that some objects do exist!

Toy problem.
Suppose there will be held two conferences on Analytic Number Theory simultaneously with 60 (!) sections. Suppose also that for each section there are at least 7 scientists who are specialists in the corresponding topics. Is it possible to distribute them so that for both conferences all of its sections will not be empty?

Yes!
Let us assign a scientist to each conference with probability $1/2$. Let E_A be the event that a section A of one of the conferences is empty. The probability of E_A is at most 2^{-7}; the probability of ***existence*** of an empty section is

$$\mathbb{P}(\cup_A E_A) \leqslant \sum_A \mathbb{P}(E_A) \leqslant 2 \cdot 60 \cdot 2^{-7} = 120/128 < 1.$$

If there are n scientists, then we have 2^n possibilities and hence there are at least $2^n(1 - 120/128) = 2^{n-4}$ rearrangements of participants with no empty sections.

Again, we proved not only the existence of such rearrangement: we proved that there are many of them.

In fact, using the probabilistic method we can prove not only that a function takes large values. We can prove that some objects do exist!

Toy problem.
Suppose there will be held two conferences on Analytic Number Theory simultaneously with 60 (!) sections. Suppose also that for each section there are at least 7 scientists who are specialists in the corresponding topics. Is it possible to distribute them so that for both conferences all of its sections will not be empty?

Yes!
Let us assign a scientist to each conference with probability $1/2$. Let E_A be the event that a section A of one of the conferences is empty. The probability of E_A is at most 2^{-7}; the probability of ***existence*** of an empty section is

$$\mathbb{P}(\cup_A E_A) \leqslant \sum_A \mathbb{P}(E_A) \leqslant 2 \cdot 60 \cdot 2^{-7} = 120/128 < 1.$$

If there are n scientists, then we have 2^n possibilities and hence there are at least $2^n(1 - 120/128) = 2^{n-4}$ rearrangements of participants with no empty sections.

Again, we proved not only the existence of such rearrangement: we proved that there are many of them.

In fact, using the probabilistic method we can prove not only that a function takes large values. We can prove that some objects do exist!

Toy problem.
Suppose there will be held two conferences on Analytic Number Theory simultaneously with 60 (!) sections. Suppose also that for each section there are at least 7 scientists who are specialists in the corresponding topics. Is it possible to distribute them so that for both conferences all of its sections will not be empty?

Yes!
Let us assign a scientist to each conference with probability $1/2$. Let E_A be the event that a section A of one of the conferences is empty. The probability of E_A is at most 2^{-7}; the probability of ***existence*** of an empty section is

$$\mathbb{P}(\cup_A E_A) \leqslant \sum_A \mathbb{P}(E_A) \leqslant 2 \cdot 60 \cdot 2^{-7} = 120/128 < 1.$$

If there are n scientists, then we have 2^n possibilities and hence there are at least $2^n(1 - 120/128) = 2^{n-4}$ rearrangements of participants with no empty sections.

Again, we proved not only the existence of such rearrangement: we proved that there are many of them.

In fact, using the probabilistic method we can prove not only that a function takes large values. We can prove that some objects do exist!

Toy problem.
Suppose there will be held two conferences on Analytic Number Theory simultaneously with 60 (!) sections. Suppose also that for each section there are at least 7 scientists who are specialists in the corresponding topics. Is it possible to distribute them so that for both conferences all of its sections will not be empty?

Yes!
Let us assign a scientist to each conference with probability $1/2$. Let E_A be the event that a section A of one of the conferences is empty. The probability of E_A is at most 2^{-7}; the probability of ***existence*** of an empty section is

$$\mathbb{P}(\cup_A E_A) \leqslant \sum_A \mathbb{P}(E_A) \leqslant 2 \cdot 60 \cdot 2^{-7} = 120/128 < 1.$$

If there are n scientists, then we have 2^n possibilities and hence there are at least $2^n(1 - 120/128) = 2^{n-4}$ rearrangements of participants with no empty sections.

Again, we proved not only the existence of such rearrangement: we proved that there are many of them.

In fact, using the probabilistic method we can prove not only that a function takes large values. We can prove that some objects do exist!

Toy problem.
Suppose there will be held two conferences on Analytic Number Theory simultaneously with 60 (!) sections. Suppose also that for each section there are at least 7 scientists who are specialists in the corresponding topics. Is it possible to distribute them so that for both conferences all of its sections will not be empty?

Yes!
Let us assign a scientist to each conference with probability $1/2$. Let E_A be the event that a section A of one of the conferences is empty. The probability of E_A is at most 2^{-7}; the probability of ***existence*** of an empty section is

$$\mathbb{P}(\cup_A E_A) \leqslant \sum_A \mathbb{P}(E_A) \leqslant 2 \cdot 60 \cdot 2^{-7} = 120/128 < 1.$$

If there are n scientists, then we have 2^n possibilities and hence there are at least $2^n(1 - 120/128) = 2^{n-4}$ rearrangements of participants with no empty sections.

Again, we proved not only the existence of such rearrangement: we proved that there are many of them.

Once again, the method is instructive but not constructive. Usual people may not understand this:

-Hey, could you help me? There will be held two conferences simultaneously...(bla-bla-bla). Is it possible to distribute the scientists so that for both conferences all of its sections would not be empty?

(here you are thinking, applying the probabilistic method...)

-Yes!
-Oh, nice!! How?
-I don't know.

It is one of the reasons why «we get everything for free».

Once again, the method is instructive but not constructive. Usual people may not understand this:

-Hey, could you help me? There will be held two conferences simultaneously...(bla-bla-bla). Is it possible to distribute the scientists so that for both conferences all of its sections would not be empty?

(here you are thinking, applying the probabilistic method...)

-Yes!
-Oh, nice!! How?
-I don't know.

It is one of the reasons why «we get everything for free».

Example 5: Two conferences

Once again, the method is instructive but not constructive. Usual people may not understand this:

-Hey, could you help me? There will be held two conferences simultaneously...(bla-bla-bla). Is it possible to distribute the scientists so that for both conferences all of its sections would not be empty?

(here you are thinking, applying the probabilistic method...)

-Yes!
-Oh, nice!! How?
-I don't know.

It is one of the reasons why «we get everything for free».

Another combinatorial toy problem.
Suppose a great football (or whatever) tournament with $N = 10^7$ teams is coming. Is it possible that for any 10 teams there will be a team which would beat all of them (draws are not allowed)?

Consider a random directed complete graph $G = (V, E)$ with $|V| = N$ vertices; (i, j) means that the team i won the team j.

For any $i \neq j$ we set $\mathbb{P}((i,j) \in E) = \mathbb{P}((j,i) \in E) = 1/2$. Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 2^{-10}; put $\alpha = 1 - 2^{-10}$.
Let F_A be the event that there are no good v (a bad event — our condition then fails). Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1}N)^{10}}{10!} \alpha^N < 10^{-4000}.$$

Again, we have proved that not one but the vast majority of the tournaments obeys our condition. Nevertheless, we still have no examples from this argument.

Another combinatorial toy problem.
Suppose a great football (or whatever) tournament with $N = 10^7$ teams is coming. Is it possible that for any 10 teams there will be a team which would beat all of them (draws are not allowed)?

Consider a random directed complete graph $G = (V, E)$ with $|V| = N$ vertices; (i, j) means that the team i won the team j.

For any $i \neq j$ we set $\mathbb{P}((i,j) \in E) = \mathbb{P}((j,i) \in E) = 1/2$. Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 2^{-10}; put $\alpha = 1 - 2^{-10}$.
Let F_A be the event that there are no good v (a bad event — our condition then fails). Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1}N)^{10}}{10!} \alpha^N < 10^{-4000}.$$

Again, we have proved that not one but the vast majority of the tournaments obeys our condition. Nevertheless, we still have no examples from this argument.

Another combinatorial toy problem.
Suppose a great football (or whatever) tournament with $N = 10^7$ teams is coming. Is it possible that for any 10 teams there will be a team which would beat all of them (draws are not allowed)?

Consider a random directed complete graph $G = (V, E)$ with $|V| = N$ vertices; (i, j) means that the team i won the team j.

For any $i \neq j$ we set $\mathbb{P}((i,j) \in E) = \mathbb{P}((j,i) \in E) = 1/2$. Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 2^{-10}; put $\alpha = 1 - 2^{-10}$.
Let F_A be the event that there are no good v (a bad event — our condition then fails). Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-4000}.$$

Again, we have proved that not one but the vast majority of the tournaments obeys our condition. Nevertheless, we still have no examples from this argument.

Another combinatorial toy problem.
Suppose a great football (or whatever) tournament with $N = 10^7$ teams is coming. Is it possible that for any 10 teams there will be a team which would beat all of them (draws are not allowed)?

Consider a random directed complete graph $G = (V, E)$ with $|V| = N$ vertices; (i, j) means that the team i won the team j.

For any $i \neq j$ we set $\mathbb{P}((i,j) \in E) = \mathbb{P}((j,i) \in E) = 1/2$. Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 2^{-10}; put $\alpha = 1 - 2^{-10}$.
Let F_A be the event that there are no good v (a bad event — our condition then fails). Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1}N)^{10}}{10!} \alpha^N < 10^{-4000}.$$

Again, we have proved that not one but the vast majority of the tournaments obeys our condition. Nevertheless, we still have no examples from this argument.

Another combinatorial toy problem.
Suppose a great football (or whatever) tournament with $N = 10^7$ teams is coming. Is it possible that for any 10 teams there will be a team which would beat all of them (draws are not allowed)?

Consider a random directed complete graph $G = (V, E)$ with $|V| = N$ vertices; (i, j) means that the team i won the team j.

For any $i \neq j$ we set $\mathbb{P}((i,j) \in E) = \mathbb{P}((j,i) \in E) = 1/2$. Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 2^{-10}; put $\alpha = 1 - 2^{-10}$.
Let F_A be the event that there are no good v (a bad event — our condition then fails). Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-4000}.$$

Again, we have proved that not one but the vast majority of the tournaments obeys our condition. Nevertheless, we still have no examples from this argument.

Another combinatorial toy problem.
Suppose a great football (or whatever) tournament with $N = 10^7$ teams is coming. Is it possible that for any 10 teams there will be a team which would beat all of them (draws are not allowed)?

Consider a random directed complete graph $G = (V, E)$ with $|V| = N$ vertices; (i, j) means that the team i won the team j.

For any $i \neq j$ we set $\mathbb{P}((i,j) \in E) = \mathbb{P}((j,i) \in E) = 1/2$. Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 2^{-10}; put $\alpha = 1 - 2^{-10}$.
Let F_A be the event that there are no good v (a bad event — our condition then fails). Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-4000}.$$

Again, we have proved that not one but the vast majority of the tournaments obeys our condition. Nevertheless, we still have no examples from this argument.

Another combinatorial toy problem.
Suppose a great football (or whatever) tournament with $N = 10^7$ teams is coming. Is it possible that for any 10 teams there will be a team which would beat all of them (draws are not allowed)?

Consider a random directed complete graph $G = (V, E)$ with $|V| = N$ vertices; (i, j) means that the team i won the team j.

For any $i \neq j$ we set $\mathbb{P}((i,j) \in E) = \mathbb{P}((j,i) \in E) = 1/2$. Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 2^{-10}; put $\alpha = 1 - 2^{-10}$.
Let F_A be the event that there are no good v (a bad event — our condition then fails). Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1}N)^{10}}{10!} \alpha^N < 10^{-4000}.$$

Again, we have proved that not one but the vast majority of the tournaments obeys our condition. Nevertheless, we still have no examples from this argument.

But that is quite strange, isn't it? Take 10 best chessplayers. What is the probability that somebody beats all of them?

Ok, let us allow draws and consider the same problem.

For any $i \neq j$ we set

$$\mathbb{P}((i \text{ won } j) \in E) = \mathbb{P}((j \text{ won } i) \in E) = \mathbb{P}((j \text{ made a draw with } i) \in E) = 1/3.$$

Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 3^{-10}; put $\alpha = 1 - 3^{-10}$.
Let F_A be the event that there are no good v. Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-10}.$$

How can one explain this?

Random objects, roughly speaking, have no structure. But usual tournaments do have some structure - say, a group of strong players a group of weak players, or transitivity: if a won b and b won c, then it is quite logical to assume that a won c. Usually have more "dependences" in the life.

We will also show that scores of almost all players in this random tournament are very close to $N/2$. It is also very unusual for the real life.

Example 6: Tournament

But that is quite strange, isn't it? Take 10 best chessplayers. What is the probability that somebody beats all of them?

Ok, let us allow draws and consider the same problem.

For any $i \neq j$ we set

$$\mathbb{P}((i \text{ won } j) \in E) = \mathbb{P}((j \text{ won } i) \in E) = \mathbb{P}((j \text{ made a draw with } i) \in E) = 1/3.$$

Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 3^{-10}; put $\alpha = 1 - 3^{-10}$.
Let F_A be the event that there are no good v. Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-10}.$$

How can one explain this?

Random objects, roughly speaking, have no structure. But usual tournaments do have some structure - say, a group of strong players a group of weak players, or transitivity: if a won b and b won c, then it is quite logical to assume that a won c. Usually have more "dependences" in the life.

We will also show that scores of almost all players in this random tournament are very close to $N/2$. It is also very unusual for the real life.

But that is quite strange, isn't it? Take 10 best chessplayers. What is the probability that somebody beats all of them?

Ok, let us allow draws and consider the same problem.

For any $i \neq j$ we set

$$\mathbb{P}((i \text{ won } j) \in E) = \mathbb{P}((j \text{ won } i) \in E) = \mathbb{P}((j \text{ made a draw with } i) \in E) = 1/3.$$

Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 3^{-10}; put $\alpha = 1 - 3^{-10}$.
Let F_A be the event that there are no good v. Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-10}.$$

How can one explain this?

Random objects, roughly speaking, have no structure. But usual tournaments do have some structure - say, a group of strong players a group of weak players, or transitivity: if a won b and b won c, then it is quite logical to assume that a won c. Usually have more "dependences" in the life.

We will also show that scores of almost all players in this random tournament are very close to $N/2$. It is also very unusual for the real life.

But that is quite strange, isn't it? Take 10 best chessplayers. What is the probability that somebody beats all of them?

Ok, let us allow draws and consider the same problem.

For any $i \neq j$ we set

$$\mathbb{P}((i \text{ won } j) \in E) = \mathbb{P}((j \text{ won } i) \in E) = \mathbb{P}((j \text{ made a draw with } i) \in E) = 1/3.$$

Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 3^{-10}; put $\alpha = 1 - 3^{-10}$.
Let F_A be the event that there are no good v. Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-10}.$$

How can one explain this?

Random objects, roughly speaking, have no structure. But usual tournaments do have some structure - say, a group of strong players a group of weak players, or transitivity: if a won b and b won c, then it is quite logical to assume that a won c. Usually have more "dependences" in the life.

We will also show that scores of almost all players in this random tournament are very close to $N/2$. It is also very unusual for the real life.

But that is quite strange, isn't it? Take 10 best chessplayers. What is the probability that somebody beats all of them?

Ok, let us allow draws and consider the same problem.

For any $i \neq j$ we set

$$\mathbb{P}((i \text{ won } j) \in E) = \mathbb{P}((j \text{ won } i) \in E) = \mathbb{P}((j \text{ made a draw with } i) \in E) = 1/3.$$

Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 3^{-10}; put $\alpha = 1 - 3^{-10}$.
Let F_A be the event that there are no good v. Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-10}.$$

How can one explain this?

Random objects, roughly speaking, have no structure. But usual tournaments do have some structure - say, a group of strong players a group of weak players, or transitivity: if a won b and b won c, then it is quite logical to assume that a won c. Usually have more "dependences" in the life.

We will also show that scores of almost all players in this random tournament are very close to $N/2$. It is also very unusual for the real life.

But that is quite strange, isn't it? Take 10 best chessplayers. What is the probability that somebody beats all of them?

Ok, let us allow draws and consider the same problem.

For any $i \neq j$ we set

$$\mathbb{P}((i \text{ won } j) \in E) = \mathbb{P}((j \text{ won } i) \in E) = \mathbb{P}((j \text{ made a draw with } i) \in E) = 1/3.$$

Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 3^{-10}; put $\alpha = 1 - 3^{-10}$.
Let F_A be the event that there are no good v. Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-10}.$$

How can one explain this?

Random objects, roughly speaking, have no structure. But usual tournaments do have some structure - say, a group of strong players a group of weak players, or transitivity: if a won b and b won c, then it is quite logical to assume that a won c. Usually have more "dependences" in the life.

We will also show that scores of almost all players in this random tournament are very close to $N/2$. It is also very unusual for the real life.

But that is quite strange, isn't it? Take 10 best chessplayers. What is the probability that somebody beats all of them?

Ok, let us allow draws and consider the same problem.

For any $i \neq j$ we set

$$\mathbb{P}((i \text{ won } j) \in E) = \mathbb{P}((j \text{ won } i) \in E) = \mathbb{P}((j \text{ made a draw with } i) \in E) = 1/3.$$

Fix $A \subset V$ with $|A| = 10$ and take $v \in V \setminus A$. The probability that $(v, a) \in E$ for all $a \in A$ (v is good for A) is 3^{-10}; put $\alpha = 1 - 3^{-10}$.
Let F_A be the event that there are no good v. Then $\mathbb{P}(F_A) = \alpha^{N-10}$ and

$$\mathbb{P}(\cup_{|A|=10} F_A) \leqslant \sum_{|A|=10} \mathbb{P}(F_A) \leqslant \binom{N}{10} \alpha^{-10} \alpha^N \leqslant \frac{(\alpha^{-1} N)^{10}}{10!} \alpha^N < 10^{-10}.$$

How can one explain this?

Random objects, roughly speaking, have no structure. But usual tournaments do have some structure - say, a group of strong players a group of weak players, or transitivity: if a won b and b won c, then it is quite logical to assume that a won c. Usually have more "dependences" in the life.

We will also show that scores of almost all players in this random tournament are very close to $N/2$. It is also very unusual for the real life.

Example 7: Sum-free subsets

A set $A \subset \mathbb{Z}$ is said to be sum-free if there are no solutions of the equation $a + b = c$ with $a, b, c \in A$.

Obviously, the set of all odd numbers (or numbers which are congruent $1 \pmod 3$) is sum-free.

Given a finite set $A \subset \mathbb{Z}$, how large can we choose a sum-free subset $B \subset A$?

Theorem (Erdös, 1965)

Let A be a set of non-zero integers. Then A contains a sum-free subset B of size $|B| > |A|/3$.

Proof. The main idea: the set $[1/3, 2/3)$ is a sum-free subset of $[0, 1) = \mathbb{R}/\mathbb{Z}$.

Choose a large prime number $p = 3k + 2$ so that $A \subset [-p/2, p/2] \setminus \{0\}$. We can view A as a subset of $\mathbb{Z}_p$ rather than the integers $\mathbb{Z}$, and observe that a subset B of A will be sum-free in $\mathbb{Z}_p$ if and only if it is sum-free in $\mathbb{Z}$.

A set $A \subset \mathbb{Z}$ is said to be sum-free if there are no solutions of the equation $a + b = c$ with $a, b, c \in A$.

Obviously, the set of all odd numbers (or numbers which are congruent $1 \pmod 3$) is sum-free.

Given a finite set $A \subset \mathbb{Z}$, how large can we choose a sum-free subset $B \subset A$?

Theorem (Erdös, 1965)

Let A be a set of non-zero integers. Then A contains a sum-free subset B of size $|B| > |A|/3$.

Proof. The main idea: the set $[1/3, 2/3)$ is a sum-free subset of $[0, 1) = \mathbb{R}/\mathbb{Z}$.

Choose a large prime number $p = 3k + 2$ so that $A \subset [-p/2, p/2] \setminus \{0\}$. We can view A as a subset of $\mathbb{Z}_p$ rather than the integers $\mathbb{Z}$, and observe that a subset B of A will be sum-free in $\mathbb{Z}_p$ if and only if it is sum-free in $\mathbb{Z}$.

A set $A \subset \mathbb{Z}$ is said to be sum-free if there are no solutions of the equation $a + b = c$ with $a, b, c \in A$.

Obviously, the set of all odd numbers (or numbers which are congruent $1 \pmod 3$) is sum-free.

Given a finite set $A \subset \mathbb{Z}$, how large can we choose a sum-free subset $B \subset A$?

Theorem (Erdös, 1965)

Let A be a set of non-zero integers. Then A contains a sum-free subset B of size $|B| > |A|/3$.

Proof. The main idea: the set $[1/3, 2/3)$ is a sum-free subset of $[0, 1) = \mathbb{R}/\mathbb{Z}$.

Choose a large prime number $p = 3k + 2$ so that $A \subset [-p/2, p/2] \setminus \{0\}$. We can view A as a subset of $\mathbb{Z}_p$ rather than the integers $\mathbb{Z}$, and observe that a subset B of A will be sum-free in $\mathbb{Z}_p$ if and only if it is sum-free in $\mathbb{Z}$.

A set $A \subset \mathbb{Z}$ is said to be sum-free if there are no solutions of the equation $a + b = c$ with $a, b, c \in A$.

Obviously, the set of all odd numbers (or numbers which are congruent $1 \pmod 3$) is sum-free.

Given a finite set $A \subset \mathbb{Z}$, how large can we choose a sum-free subset $B \subset A$?

Theorem (Erdös, 1965)

Let A be a set of non-zero integers. Then A contains a sum-free subset B of size $|B| > |A|/3$.

Proof. The main idea: the set $[1/3, 2/3)$ is a sum-free subset of $[0, 1) = \mathbb{R}/\mathbb{Z}$.

Choose a large prime number $p = 3k + 2$ so that $A \subset [-p/2, p/2] \setminus \{0\}$. We can view A as a subset of $\mathbb{Z}_p$ rather than the integers $\mathbb{Z}$, and observe that a subset B of A will be sum-free in $\mathbb{Z}_p$ if and only if it is sum-free in $\mathbb{Z}$.

A set $A \subset \mathbb{Z}$ is said to be sum-free if there are no solutions of the equation $a + b = c$ with $a, b, c \in A$.

Obviously, the set of all odd numbers (or numbers which are congruent $1 \pmod 3$) is sum-free.

Given a finite set $A \subset \mathbb{Z}$, how large can we choose a sum-free subset $B \subset A$?

Theorem (Erdös, 1965)

Let A be a set of non-zero integers. Then A contains a sum-free subset B of size $|B| > |A|/3$.

Proof. The main idea: the set $[1/3, 2/3)$ is a sum-free subset of $[0, 1) = \mathbb{R}/\mathbb{Z}$.

Choose a large prime number $p = 3k + 2$ so that $A \subset [-p/2, p/2] \setminus \{0\}$. We can view A as a subset of $\mathbb{Z}_p$ rather than the integers $\mathbb{Z}$, and observe that a subset B of A will be sum-free in $\mathbb{Z}_p$ if and only if it is sum-free in $\mathbb{Z}$.

A set $A \subset \mathbb{Z}$ is said to be sum-free if there are no solutions of the equation $a + b = c$ with $a, b, c \in A$.

Obviously, the set of all odd numbers (or numbers which are congruent $1 \pmod 3$) is sum-free.

Given a finite set $A \subset \mathbb{Z}$, how large can we choose a sum-free subset $B \subset A$?

Theorem (Erdös, 1965)

Let A be a set of non-zero integers. Then A contains a sum-free subset B of size $|B| > |A|/3$.

Proof. The main idea: the set $[1/3, 2/3)$ is a sum-free subset of $[0, 1) = \mathbb{R}/\mathbb{Z}$.

Choose a large prime number $p = 3k + 2$ so that $A \subset [-p/2, p/2] \setminus \{0\}$. We can view A as a subset of $\mathbb{Z}_p$ rather than the integers $\mathbb{Z}$, and observe that a subset B of A will be sum-free in $\mathbb{Z}_p$ if and only if it is sum-free in $\mathbb{Z}$.

Now, the set $[k+1, 2k+1] \subset \mathbb{Z}_p$ is sum-free. Choose $x \in \mathbb{Z}_p^*$ uniformly at random; then the random set

$$B := A \cap (x \cdot [k+1, 2k+1]) = \{a \in A : x^{-1}a \in [k+1, 2k+1]\}$$

is also sum-free. We want to find x such that $|B|$ is large. We have

$$\mathbb{E}(|B|) = \sum_{a \in A} \mathbb{P}(a \in B) = \sum_{a \in A} \mathbb{P}(x^{-1}a \in [k+1, 2k+1]) = |A|\frac{k+1}{p-1} > \frac{|A|}{3}.$$

Then we are done.

Now, the set $[k+1, 2k+1] \subset \mathbb{Z}_p$ is sum-free. Choose $x \in \mathbb{Z}_p^*$ uniformly at random; then the random set

$$B := A \cap (x \cdot [k+1, 2k+1]) = \{a \in A : x^{-1}a \in [k+1, 2k+1]\}$$

is also sum-free. We want to find x such that $|B|$ is large. We have

$$\mathbb{E}(|B|) = \sum_{a \in A} \mathbb{P}(a \in B) = \sum_{a \in A} \mathbb{P}(x^{-1}a \in [k+1, 2k+1]) = |A|\frac{k+1}{p-1} > \frac{|A|}{3}.$$

Then we are done.

Now, the set $[k+1, 2k+1] \subset \mathbb{Z}_p$ is sum-free. Choose $x \in \mathbb{Z}_p^*$ uniformly at random; then the random set

$$B := A \cap (x \cdot [k+1, 2k+1]) = \{a \in A : x^{-1}a \in [k+1, 2k+1]\}$$

is also sum-free. We want to find x such that $|B|$ is large. We have

$$\mathbb{E}(|B|) = \sum_{a \in A} \mathbb{P}(a \in B) = \sum_{a \in A} \mathbb{P}(x^{-1}a \in [k+1, 2k+1]) = |A| \frac{k+1}{p-1} > \frac{|A|}{3}.$$

Then we are done.

Consider trygonometric polynomials with coefficients equal to 1 and the norms $\|f\|_q := \left(\int_0^1 |f(x)|^q dx\right)^{1/q}$, $q \geqslant 1$. Suppose $\{n_k\}_{k=1}^N$ are distinct integers; then trivially

$$\left\|\sum_{k=1}^N e(n_k x)\right\|_2 = N^{1/2}$$

(here and in what follows $e(mx) = e^{2\pi i m x}$). On the other hand, by the Cauchi-Schwarz inequality

$$\left\|\sum_{k=1}^N e(n_k x)\right\|_1 \leqslant \left\|\sum_{k=1}^N e(n_k x)\right\|_2 = N^{1/2}.$$

A very natural question is how large $\left\|\sum_{k=1}^N e(n_k x)\right\|_1$ can be. We give a quite precise answer using the first moment method again.

Consider trygonometric polynomials with coefficients equal to 1 and the norms $\|f\|_q := \left(\int_0^1 |f(x)|^q dx\right)^{1/q}$, $q \geqslant 1$. Suppose $\{n_k\}_{k=1}^N$ are distinct integers; then trivially

$$\left\|\sum_{k=1}^N e(n_k x)\right\|_2 = N^{1/2}$$

(here and in what follows $e(mx) = e^{2\pi i m x}$). On the other hand, by the Cauchi-Schwarz inequality

$$\left\|\sum_{k=1}^N e(n_k x)\right\|_1 \leqslant \left\|\sum_{k=1}^N e(n_k x)\right\|_2 = N^{1/2}.$$

A very natural question is how large $\left\|\sum_{k=1}^N e(n_k x)\right\|_1$ can be. We give a quite precise answer using the first moment method again.

Consider trygonometric polynomials with coefficients equal to 1 and the norms $\|f\|_q := \left(\int_0^1 |f(x)|^q dx\right)^{1/q}$, $q \geqslant 1$. Suppose $\{n_k\}_{k=1}^N$ are distinct integers; then trivially

$$\left\|\sum_{k=1}^N e(n_k x)\right\|_2 = N^{1/2}$$

(here and in what follows $e(mx) = e^{2\pi imx}$). On the other hand, by the Cauchi-Schwarz inequality

$$\left\|\sum_{k=1}^N e(n_k x)\right\|_1 \leqslant \left\|\sum_{k=1}^N e(n_k x)\right\|_2 = N^{1/2}.$$

A very natural question is how large $\left\|\sum_{k=1}^N e(n_k x)\right\|_1$ can be. We give a quite precise answer using the first moment method again.

Theorem

Let N be a positive integer and $[N] = \{1, ..., N\}$. Then

$$\#\left\{M \subseteq [N] : \int_0^1 \left|\sum_{k\in M} e(kx)\right| dx \geqslant 0.14N^{1/2}\right\} \geqslant 0.28 \cdot 2^N.$$

The same is true (possibly with worse constants) for the systems $\{\cos 2\pi kx\}$ and $\{\sin 2\pi kx\}$; the proof is almost the same.

Proof. We need a little preparation. Let $f = \{f_l\}_{l=1}^m$ be arbitrary complex numbers; for $q > 0$, define $\|f\|_q = \left(\frac{1}{m}\sum_{l=1}^m |f_l|^q\right)^{1/q}$.

Lemma

We have

$$\|f\|_2 \leqslant \|f\|_1^{1/3}\|f\|_4^{2/3}.$$

This lemma is a simple consequence of Hölder's inequality (with the exponents $3/2$ and 3): we have

$$\|f\|_2^2 = \frac{1}{m}\sum_{l=1}^m |f_l|^{2/3}|f_l|^{4/3} \leqslant \left(\frac{1}{m}\sum_{l=1}^m |f_l|\right)^{2/3}\left(\frac{1}{m}\sum_{l=1}^m |f_l|^4\right)^{1/3} = \|f\|_1^{2/3}\|f\|_4^{4/3}.$$

Theorem

Let N be a positive integer and $[N] = \{1, ..., N\}$. Then

$$\#\left\{M \subseteq [N] : \int_0^1 \left|\sum_{k\in M} e(kx)\right| dx \geqslant 0.14N^{1/2}\right\} \geqslant 0.28 \cdot 2^N.$$

The same is true (possibly with worse constants) for the systems $\{\cos 2\pi kx\}$ and $\{\sin 2\pi kx\}$; the proof is almost the same.

Proof. We need a little preparation. Let $f = \{f_l\}_{l=1}^m$ be arbitrary complex numbers; for $q > 0$, define $\|f\|_q = \left(\frac{1}{m}\sum_{l=1}^m |f_l|^q\right)^{1/q}$.

Lemma

We have

$$\|f\|_2 \leqslant \|f\|_1^{1/3}\|f\|_4^{2/3}.$$

This lemma is a simple consequence of Hölder's inequality (with the exponents $3/2$ and 3): we have

$$\|f\|_2^2 = \frac{1}{m}\sum_{l=1}^m |f_l|^{2/3}|f_l|^{4/3} \leqslant \left(\frac{1}{m}\sum_{l=1}^m |f_l|\right)^{2/3}\left(\frac{1}{m}\sum_{l=1}^m |f_l|^4\right)^{1/3} = \|f\|_1^{2/3}\|f\|_4^{4/3}.$$

Theorem

Let N be a positive integer and $[N] = \{1, ..., N\}$. Then

$$\#\left\{M \subseteq [N] : \int_0^1 \left|\sum_{k\in M} e(kx)\right| dx \geqslant 0.14N^{1/2}\right\} \geqslant 0.28 \cdot 2^N.$$

The same is true (possibly with worse constants) for the systems $\{\cos 2\pi kx\}$ and $\{\sin 2\pi kx\}$; the proof is almost the same.

Proof. We need a little preparation. Let $f = \{f_l\}_{l=1}^m$ be arbitrary complex numbers; for $q > 0$, define $\|f\|_q = \left(\frac{1}{m}\sum_{l=1}^m |f_l|^q\right)^{1/q}$.

Lemma

We have

$$\|f\|_2 \leqslant \|f\|_1^{1/3}\|f\|_4^{2/3}.$$

This lemma is a simple consequence of Hölder's inequality (with the exponents $3/2$ and 3): we have

$$\|f\|_2^2 = \frac{1}{m}\sum_{l=1}^m |f_l|^{2/3}|f_l|^{4/3} \leqslant \left(\frac{1}{m}\sum_{l=1}^m |f_l|\right)^{2/3}\left(\frac{1}{m}\sum_{l=1}^m |f_l|^4\right)^{1/3} = \|f\|_1^{2/3}\|f\|_4^{4/3}.$$

Theorem

Let N be a positive integer and $[N] = \{1, ..., N\}$. Then

$$\#\left\{M \subseteq [N] : \int_0^1 \left|\sum_{k\in M} e(kx)\right| dx \geqslant 0.14 N^{1/2}\right\} \geqslant 0.28 \cdot 2^N.$$

The same is true (possibly with worse constants) for the systems $\{\cos 2\pi kx\}$ and $\{\sin 2\pi kx\}$; the proof is almost the same.

Proof. We need a little preparation. Let $f = \{f_l\}_{l=1}^m$ be arbitrary complex numbers; for $q > 0$, define $\|f\|_q = \left(\frac{1}{m}\sum_{l=1}^m |f_l|^q\right)^{1/q}$.

Lemma

We have

$$\|f\|_2 \leqslant \|f\|_1^{1/3} \|f\|_4^{2/3}.$$

This lemma is a simple consequence of Hölder's inequality (with the exponents $3/2$ and 3): we have

$$\|f\|_2^2 = \frac{1}{m}\sum_{l=1}^m |f_l|^{2/3}|f_l|^{4/3} \leqslant \left(\frac{1}{m}\sum_{l=1}^m |f_l|\right)^{2/3}\left(\frac{1}{m}\sum_{l=1}^m |f_l|^4\right)^{1/3} = \|f\|_1^{2/3}\|f\|_4^{4/3}.$$

Theorem

Let N be a positive integer and $[N]=\{1,...,N\}$. Then

$$\#\left\{M\subseteq[N]:\int_0^1\left|\sum_{k\in M}e(kx)\right|dx\geqslant 0.14N^{1/2}\right\}\geqslant 0.28\cdot 2^N.$$

The same is true (possibly with worse constants) for the systems $\{\cos 2\pi kx\}$ and $\{\sin 2\pi kx\}$; the proof is almost the same.

Proof. We need a little preparation. Let $f=\{f_l\}_{l=1}^m$ be arbitrary complex numbers; for $q>0$, define $\|f\|_q=\left(\frac{1}{m}\sum_{l=1}^m|f_l|^q\right)^{1/q}$.

Lemma

We have

$$\|f\|_2\leqslant\|f\|_1^{1/3}\|f\|_4^{2/3}.$$

This lemma is a simple consequence of Hölder's inequality (with the exponents $3/2$ and 3): we have

$$\|f\|_2^2=\frac{1}{m}\sum_{l=1}^m|f_l|^{2/3}|f_l|^{4/3}\leqslant\left(\frac{1}{m}\sum_{l=1}^m|f_l|\right)^{2/3}\left(\frac{1}{m}\sum_{l=1}^m|f_l|^4\right)^{1/3}=\|f\|_1^{2/3}\|f\|_4^{4/3}.$$

Example 8: Large L_1-norms of polynomials

Now let $\{a_k\}_{k=1}^N$ be arbitrary complex numbers and $\{\varepsilon_k\}_{k=1}^N$ be independent random signes ($\varepsilon_k = \pm 1/2$ with probability $1/2$). Consider

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 = 2^{-N} \sum_{\varepsilon_1, \dots, \varepsilon_N} \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 = \sum_{k,l} a_k \overline{a_l} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l = \sum_k |a_k|^2$$

and

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = 2^{-N} \sum_{\varepsilon_1, \dots, \varepsilon_N} \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = \sum_{k,l,m,n} a_k a_l \overline{a_m a_n} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l \varepsilon_m \varepsilon_n.$$

Here only 4-tuples of the types $(k,k,k,k), (k,l,k,l), (k,k,l,l), (k,l,l,k)$ matter; other tuples give a zero contribution to the RHS; so

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = \sum_k |a_k|^4 + 6 \sum_{k<l} |a_k|^2 |a_l|^2 \leqslant 3 \left(\sum_k |a_k|^2 \right)^2$$

Hence

$$\left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 \right)^{1/4} \leqslant \sqrt[4]{3} \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2}.$$

Now let $\{a_k\}_{k=1}^N$ be arbitrary complex numbers and $\{\varepsilon_k\}_{k=1}^N$ be independent random signes ($\varepsilon_k = \pm 1/2$ with probability $1/2$). Consider

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2 = \sum_{k,l} a_k \overline{a_l} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l = \sum_k |a_k|^2$$

and

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = \sum_{k,l,m,n} a_k a_l \overline{a_m a_n} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l \varepsilon_m \varepsilon_n.$$

Here only 4-tuples of the types $(k,k,k,k), (k,l,k,l), (k,k,l,l), (k,l,l,k)$ matter; other tuples give a zero contribution to the RHS; so

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = \sum_k |a_k|^4 + 6 \sum_{k<l} |a_k|^2 |a_l|^2 \leqslant 3 \left(\sum_k |a_k|^2\right)^2$$

Hence

$$\left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2\right)^{1/2} \leqslant \left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4\right)^{1/4} \leqslant \sqrt[4]{3} \left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2\right)^{1/2}.$$

Now let $\{a_k\}_{k=1}^N$ be arbitrary complex numbers and $\{\varepsilon_k\}_{k=1}^N$ be independent random signes ($\varepsilon_k = \pm 1/2$ with probability $1/2$). Consider

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2 = \sum_{k,l} a_k \overline{a_l} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l = \sum_k |a_k|^2$$

and

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = \sum_{k,l,m,n} a_k a_l \overline{a_m a_n} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l \varepsilon_m \varepsilon_n.$$

Here only 4-tuples of the types $(k,k,k,k), (k,l,k,l), (k,k,l,l), (k,l,l,k)$ matter; other tuples give a zero contribution to the RHS; so

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = \sum_k |a_k|^4 + 6 \sum_{k<l} |a_k|^2 |a_l|^2 \leqslant 3 \left(\sum_k |a_k|^2\right)^2$$

Hence

$$\left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2\right)^{1/2} \leqslant \left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4\right)^{1/4} \leqslant \sqrt[4]{3} \left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2\right)^{1/2}.$$

Now let $\{a_k\}_{k=1}^N$ be arbitrary complex numbers and $\{\varepsilon_k\}_{k=1}^N$ be independent random signes ($\varepsilon_k = \pm 1/2$ with probability $1/2$). Consider

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2 = \sum_{k,l} a_k \overline{a_l} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l = \sum_k |a_k|^2$$

and

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = \sum_{k,l,m,n} a_k a_l \overline{a_m a_n} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l \varepsilon_m \varepsilon_n .$$

Here only 4-tuples of the types $(k,k,k,k), (k,l,k,l), (k,k,l,l), (k,l,l,k)$ matter; other tuples give a zero contribution to the RHS; so

$$\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4 = \sum_k |a_k|^4 + 6 \sum_{k<l} |a_k|^2 |a_l|^2 \leqslant 3 \left(\sum_k |a_k|^2\right)^2$$

Hence

$$\left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2\right)^{1/2} \leqslant \left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^4\right)^{1/4} \leqslant \sqrt[4]{3} \left(\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k a_k\right|^2\right)^{1/2} .$$

Now let $\{a_k\}_{k=1}^N$ be arbitrary complex numbers and $\{\varepsilon_k\}_{k=1}^N$ be independent random signes ($\varepsilon_k = \pm 1/2$ with probability $1/2$). Consider

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 = \sum_{k,l} a_k \overline{a_l} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l = \sum_k |a_k|^2$$

and

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = 2^{-N} \sum_{\varepsilon_1,\dots,\varepsilon_N} \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = \sum_{k,l,m,n} a_k a_l \overline{a_m a_n} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l \varepsilon_m \varepsilon_n .$$

Here only 4-tuples of the types $(k,k,k,k), (k,l,k,l), (k,k,l,l), (k,l,l,k)$ matter; other tuples give a zero contribution to the RHS; so

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = \sum_k |a_k|^4 + 6 \sum_{k<l} |a_k|^2 |a_l|^2 \leqslant 3 \left(\sum_k |a_k|^2 \right)^2$$

Hence

$$\left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 \right)^{1/4} \leqslant \sqrt[4]{3} \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} .$$

Now let $\{a_k\}_{k=1}^N$ be arbitrary complex numbers and $\{\varepsilon_k\}_{k=1}^N$ be independent random signes ($\varepsilon_k = \pm 1/2$ with probability $1/2$). Consider

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 = 2^{-N} \sum_{\varepsilon_1, \dots, \varepsilon_N} \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 = \sum_{k,l} a_k \overline{a_l} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l = \sum_k |a_k|^2$$

and

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = 2^{-N} \sum_{\varepsilon_1, \dots, \varepsilon_N} \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = \sum_{k,l,m,n} a_k a_l \overline{a_m a_n} \mathbb{E}_\varepsilon \varepsilon_k \varepsilon_l \varepsilon_m \varepsilon_n .$$

Here only 4-tuples of the types $(k,k,k,k), (k,l,k,l), (k,k,l,l), (k,l,l,k)$ matter; other tuples give a zero contribution to the RHS; so

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 = \sum_k |a_k|^4 + 6 \sum_{k<l} |a_k|^2 |a_l|^2 \leqslant 3 \left(\sum_k |a_k|^2 \right)^2$$

Hence

$$\left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^4 \right)^{1/4} \leqslant \sqrt[4]{3} \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} .$$

In fact, there is more common Khinchin's inequality: for any $p > 0$ there are constants $A_p, B_p > 0$ such that for any $\{a_k\}$,

$$A_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant B_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p}.$$

Now fix $x \in [0,1]$. We use the lemma with $\{a_k\} = e(kx)$ and $f(\varepsilon) = \sum_{k=1}^N \varepsilon_k e(kx)$ as well as the bound for L_4-norm of $f(\varepsilon)$ to get

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

Integrating this for $x \in [0,1]$ we obtain

$$\mathbb{E}_\varepsilon \int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \int_0^1 \mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

In fact, there is more common Khinchin's inequality: for any $p>0$ there are constants $A_p, B_p > 0$ such that for any $\{a_k\}$,

$$A_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant B_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p}.$$

Now fix $x \in [0,1]$. We use the lemma with $\{a_k\} = e(kx)$ and $f(\varepsilon) = \sum_{k=1}^N \varepsilon_k e(kx)$ as well as the bound for L_4-norm of $f(\varepsilon)$ to get

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

Integrating this for $x \in [0,1]$ we obtain

$$\mathbb{E}_\varepsilon \int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \int_0^1 \mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

In fact, there is more common Khinchin's inequality: for any $p > 0$ there are constants $A_p, B_p > 0$ such that for any $\{a_k\}$,

$$A_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant B_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p}.$$

Now fix $x \in [0,1]$. We use the lemma with $\{a_k\} = e(kx)$ and $f(\varepsilon) = \sum_{k=1}^N \varepsilon_k e(kx)$ as well as the bound for L_4-norm of $f(\varepsilon)$ to get

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

Integrating this for $x \in [0,1]$ we obtain

$$\mathbb{E}_\varepsilon \int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \int_0^1 \mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

In fact, there is more common Khinchin's inequality: for any $p > 0$ there are constants $A_p, B_p > 0$ such that for any $\{a_k\}$,

$$A_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant B_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p}.$$

Now fix $x \in [0,1]$. We use the lemma with $\{a_k\} = e(kx)$ and $f(\varepsilon) = \sum_{k=1}^N \varepsilon_k e(kx)$ as well as the bound for L_4-norm of $f(\varepsilon)$ to get

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

Integrating this for $x \in [0,1]$ we obtain

$$\mathbb{E}_\varepsilon \int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \int_0^1 \mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

In fact, there is more common Khinchin's inequality: for any $p > 0$ there are constants $A_p, B_p > 0$ such that for any $\{a_k\}$,

$$A_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p} \leqslant \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^2 \right)^{1/2} \leqslant B_p \left(\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k a_k \right|^p \right)^{1/p}.$$

Now fix $x \in [0,1]$. We use the lemma with $\{a_k\} = e(kx)$ and $f(\varepsilon) = \sum_{k=1}^N \varepsilon_k e(kx)$ as well as the bound for L_4-norm of $f(\varepsilon)$ to get

$$\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

Integrating this for $x \in [0,1]$ we obtain

$$\mathbb{E}_\varepsilon \int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \int_0^1 \mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx = \|f\|_1 \geqslant \frac{\|f\|_2^3}{\|f\|_4^2} \geqslant \frac{\|f\|_2}{\sqrt{3}} = (N/3)^{1/2}.$$

Example 8: Large L_1-norms of polynomials are popular!

Note that for any $\{\varepsilon_k\} \in \{-1,1\}^N$ the bound

$$\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right| dx \leqslant \left(\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right|^2 dx\right)^{1/2} = N^{1/2} =: M$$

holds. Then the popularity principle gives us

$$\mathbb{P}_\varepsilon\left(\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right| dx \geqslant \frac{N^{1/2}}{2\sqrt{3}}\right) \geqslant \frac{\mathbb{E}_\varepsilon |f(\varepsilon)|}{2M} \geqslant \frac{1}{2\sqrt{3}}.$$

Note that for any $\{\varepsilon_k\} \in \{-1,1\}^N$ the bound

$$\int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx \leqslant \left(\int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right|^2 dx \right)^{1/2} = N^{1/2} =: M$$

holds. Then the popularity principle gives us

$$\mathbb{P}_\varepsilon \left(\int_0^1 \left| \sum_{k=1}^N \varepsilon_k e(kx) \right| dx \geqslant \frac{N^{1/2}}{2\sqrt{3}} \right) \geqslant \frac{\mathbb{E}_\varepsilon |f(\varepsilon)|}{2M} \geqslant \frac{1}{2\sqrt{3}}.$$

Example 8: Large L_1-norms of polynomials are popular!

Fix any $\{\varepsilon_k\}_{k=1}^N$ with $\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right| dx \geqslant \frac{N^{1/2}}{2\sqrt{3}}$ and denote $g(x) = \sum_k \varepsilon_k e(kx)$. Define

$$g^+ = \sum_{k:\varepsilon_k=1} e(kx), \quad g^- = \sum_{k:\varepsilon_k=-1} e(kx)$$

Then

$$\|g^+ - g^-\|_1 = \|g\|_1 \geqslant \frac{N^{1/2}}{2\sqrt{3}} \geqslant 0.288N^{1/2}$$

and

$$\|g^+ + g^-\|_1 = \left\|\sum_{k=1}^N e(kx)\right\|_1 = \frac{4}{\pi^2}\log N + O(1).$$

Hence,

$$\|g^+\|_1 = \left\|\frac{g^+ - g^-}{2} + \frac{g^+ + g^-}{2}\right\|_1 \geqslant \left\|\frac{g^+ - g^-}{2}\right\|_1 - \left\|\frac{g^+ + g^-}{2}\right\|_1 \geqslant 0.14N^{1/2}$$

and analogously for g^-.

Fix any $\{\varepsilon_k\}_{k=1}^N$ with $\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right| dx \geqslant \frac{N^{1/2}}{2\sqrt{3}}$ and denote $g(x) = \sum_k \varepsilon_k e(kx)$. Define

$$g^+ = \sum_{k:\varepsilon_k=1} e(kx), \quad g^- = \sum_{k:\varepsilon_k=-1} e(kx)$$

Then

$$\|g^+ - g^-\|_1 = \|g\|_1 \geqslant \frac{N^{1/2}}{2\sqrt{3}} \geqslant 0.288N^{1/2}$$

and

$$\|g^+ + g^-\|_1 = \left\|\sum_{k=1}^N e(kx))\right\|_1 = \frac{4}{\pi^2}\log N + O(1).$$

Hence,

$$\|g^+\|_1 = \left\|\frac{g^+ - g^-}{2} + \frac{g^+ + g^-}{2}\right\|_1 \geqslant \left\|\frac{g^+ - g^-}{2}\right\|_1 - \left\|\frac{g^+ + g^-}{2}\right\|_1 \geqslant 0.14N^{1/2}$$

and analogously for g^-.

Fix any $\{\varepsilon_k\}_{k=1}^N$ with $\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right| dx \geqslant \frac{N^{1/2}}{2\sqrt{3}}$ and denote $g(x) = \sum_k \varepsilon_k e(kx)$. Define

$$g^+ = \sum_{k:\varepsilon_k=1} e(kx), \quad g^- = \sum_{k:\varepsilon_k=-1} e(kx)$$

Then

$$\|g^+ - g^-\|_1 = \|g\|_1 \geqslant \frac{N^{1/2}}{2\sqrt{3}} \geqslant 0.288N^{1/2}$$

and

$$\|g^+ + g^-\|_1 = \left\|\sum_{k=1}^N e(kx))\right\|_1 = \frac{4}{\pi^2}\log N + O(1).$$

Hence,

$$\|g^+\|_1 = \left\|\frac{g^+ - g^-}{2} + \frac{g^+ + g^-}{2}\right\|_1 \geqslant \left\|\frac{g^+ - g^-}{2}\right\|_1 - \left\|\frac{g^+ + g^-}{2}\right\|_1 \geqslant 0.14N^{1/2}$$

and analogously for g^-.

Fix any $\{\varepsilon_k\}_{k=1}^N$ with $\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right| dx \geqslant \frac{N^{1/2}}{2\sqrt{3}}$ and denote $g(x) = \sum_k \varepsilon_k e(kx)$. Define

$$g^+ = \sum_{k:\varepsilon_k=1} e(kx), \quad g^- = \sum_{k:\varepsilon_k=-1} e(kx)$$

Then

$$\|g^+ - g^-\|_1 = \|g\|_1 \geqslant \frac{N^{1/2}}{2\sqrt{3}} \geqslant 0.288 N^{1/2}$$

and

$$\|g^+ + g^-\|_1 = \left\|\sum_{k=1}^N e(kx))\right\|_1 = \frac{4}{\pi^2}\log N + O(1).$$

Hence,

$$\|g^+\|_1 = \left\|\frac{g^+ - g^-}{2} + \frac{g^+ + g^-}{2}\right\|_1 \geqslant \left\|\frac{g^+ - g^-}{2}\right\|_1 - \left\|\frac{g^+ + g^-}{2}\right\|_1 \geqslant 0.14 N^{1/2}$$

and analogously for g^-.

Fix any $\{\varepsilon_k\}_{k=1}^N$ with $\int_0^1 \left|\sum_{k=1}^N \varepsilon_k e(kx)\right| dx \geqslant \frac{N^{1/2}}{2\sqrt{3}}$ and denote $g(x) = \sum_k \varepsilon_k e(kx)$. Define

$$g^+ = \sum_{k:\varepsilon_k=1} e(kx), \quad g^- = \sum_{k:\varepsilon_k=-1} e(kx)$$

Then

$$\|g^+ - g^-\|_1 = \|g\|_1 \geqslant \frac{N^{1/2}}{2\sqrt{3}} \geqslant 0.288N^{1/2}$$

and

$$\|g^+ + g^-\|_1 = \left\|\sum_{k=1}^N e(kx))\right\|_1 = \frac{4}{\pi^2}\log N + O(1).$$

Hence,

$$\|g^+\|_1 = \left\|\frac{g^+ - g^-}{2} + \frac{g^+ + g^-}{2}\right\|_1 \geqslant \left\|\frac{g^+ - g^-}{2}\right\|_1 - \left\|\frac{g^+ + g^-}{2}\right\|_1 \geqslant 0.14N^{1/2}$$

and analogously for g^-.

Note that the pairs $\{g^+, g^-\}$ are the same for $\{\varepsilon_k\}$ and $\{-\varepsilon_k\}$. Then we see that

$$\#\left\{M \subseteq [N] : \int_0^1 \left|\sum_{k\in M} e(kx)\right| dx \geqslant 0.14N^{1/2}\right\} \geqslant 0.28 \cdot 2^N.$$

Thus for a positive proportion of subsets the correspoding polynomials have large L_1-norm.

Note the more "direct" argument with $\mathbb{P}(\varepsilon_k = 0) = \mathbb{P}(\varepsilon_k = 1) = 1/2$ does not work (then L_4-moments $\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k e(kx)\right|^4$ would be of order N^4 instead of N^2).

Note that the pairs $\{g^+, g^-\}$ are the same for $\{\varepsilon_k\}$ and $\{-\varepsilon_k\}$. Then we see that

$$\#\left\{ M \subseteq [N] : \int\limits_0^1 \left| \sum_{k\in M} e(kx) \right| dx \geqslant 0.14 N^{1/2} \right\} \geqslant 0.28 \cdot 2^N .$$

Thus for a positive proportion of subsets the correspoding polynomials have large L_1-norm.

Note the more "direct" argument with $\mathbb{P}(\varepsilon_k = 0) = \mathbb{P}(\varepsilon_k = 1) = 1/2$ does not work (then L_4-moments $\mathbb{E}_\varepsilon \left| \sum_{k=1}^N \varepsilon_k e(kx) \right|^4$ would be of order N^4 instead of N^2).

Note that the pairs $\{g^+, g^-\}$ are the same for $\{\varepsilon_k\}$ and $\{-\varepsilon_k\}$. Then we see that

$$\#\left\{M \subseteq [N] : \int_0^1 \left|\sum_{k\in M} e(kx)\right| dx \geqslant 0.14N^{1/2}\right\} \geqslant 0.28 \cdot 2^N.$$

Thus for a positive proportion of subsets the correspoding polynomials have large L_1-norm.

Note the more "direct" argument with $\mathbb{P}(\varepsilon_k = 0) = \mathbb{P}(\varepsilon_k = 1) = 1/2$ does not work (then L_4-moments $\mathbb{E}_\varepsilon \left|\sum_{k=1}^N \varepsilon_k e(kx)\right|^4$ would be of order N^4 instead of N^2).

A collection $\mathcal{A}$ of sets is said to be an *antichain* if none of the sets is contained in any other, that is, $A \not\subseteq B$ for any distinct $A, B \in \mathcal{A}$.

Now consider subsets of $\{1, ..., N\}$. What antichains do we have here?

Obviously, a collection all subsets of the same size k form an antichain. It has size $\binom{N}{[N/2]}$ if $k = [N/2]$. In fact, this is the largest antichain.

Theorem (LYM inequality)

Let $\mathcal{A}$ be an antichain of subsets of $[N]$. Then

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1.$$

Since $\binom{N}{|A|} \leqslant \binom{N}{[N/2]}$, it implies that

$$\frac{|\mathcal{A}|}{\binom{N}{[N/2]}} \leqslant \sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1$$

and $|\mathcal{A}| \leqslant \binom{N}{[N/2]}$. The name of the inequality is due to works of Lubell, Meshalkin and Yamamoto.

Example 9: Antichains

A collection $\mathcal{A}$ of sets is said to be an *antichain* if none of the sets is contained in any other, that is, $A \not\subseteq B$ for any distinct $A, B \in \mathcal{A}$.

Now consider subsets of $\{1, ..., N\}$. What antichains do we have here?

Obviously, a collection all subsets of the same size k form an antichain. It has size $\binom{N}{[N/2]}$ if $k = [N/2]$. In fact, this is the largest antichain.

Theorem (LYM inequality)

Let $\mathcal{A}$ be an antichain of subsets of $[N]$. Then

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1.$$

Since $\binom{N}{|A|} \leqslant \binom{N}{[N/2]}$, it implies that

$$\frac{|\mathcal{A}|}{\binom{N}{[N/2]}} \leqslant \sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1$$

and $|\mathcal{A}| \leqslant \binom{N}{[N/2]}$. The name of the inequality is due to works of Lubell, Meshalkin and Yamamoto.

Example 9: Antichains

A collection $\mathcal{A}$ of sets is said to be an *antichain* if none of the sets is contained in any other, that is, $A \not\subseteq B$ for any distinct $A, B \in \mathcal{A}$.

Now consider subsets of $\{1, ..., N\}$. What antichains do we have here?

Obviously, a collection all subsets of the same size k form an antichain. It has size $\binom{N}{[N/2]}$ if $k = [N/2]$. In fact, this is the largest antichain.

Theorem (LYM inequality)

Let $\mathcal{A}$ be an antichain of subsets of $[N]$. Then

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1.$$

Since $\binom{N}{|A|} \leqslant \binom{N}{[N/2]}$, it implies that

$$\frac{|\mathcal{A}|}{\binom{N}{[N/2]}} \leqslant \sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1$$

and $|\mathcal{A}| \leqslant \binom{N}{[N/2]}$. The name of the inequality is due to works of Lubell, Meshalkin and Yamamoto.

A collection $\mathcal{A}$ of sets is said to be an *antichain* if none of the sets is contained in any other, that is, $A \not\subseteq B$ for any distinct $A, B \in \mathcal{A}$.

Now consider subsets of $\{1, ..., N\}$. What antichains do we have here?

Obviously, a collection all subsets of the same size k form an antichain. It has size $\binom{N}{[N/2]}$ if $k = [N/2]$. In fact, this is the largest antichain.

Theorem (LYM inequality)

Let $\mathcal{A}$ be an antichain of subsets of $[N]$. Then

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1.$$

Since $\binom{N}{|A|} \leqslant \binom{N}{[N/2]}$, it implies that

$$\frac{|\mathcal{A}|}{\binom{N}{[N/2]}} \leqslant \sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1$$

and $|\mathcal{A}| \leqslant \binom{N}{[N/2]}$. The name of the inequality is due to works of Lubell, Meshalkin and Yamamoto.

A collection $\mathcal{A}$ of sets is said to be an *antichain* if none of the sets is contained in any other, that is, $A \not\subseteq B$ for any distinct $A, B \in \mathcal{A}$.

Now consider subsets of $\{1, ..., N\}$. What antichains do we have here?

Obviously, a collection all subsets of the same size k form an antichain. It has size $\binom{N}{[N/2]}$ if $k = [N/2]$. In fact, this is the largest antichain.

Theorem (LYM inequality)

Let $\mathcal{A}$ be an antichain of subsets of $[N]$. Then

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1.$$

Since $\binom{N}{|A|} \leqslant \binom{N}{[N/2]}$, it implies that

$$\frac{|\mathcal{A}|}{\binom{N}{[N/2]}} \leqslant \sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1$$

and $|\mathcal{A}| \leqslant \binom{N}{[N/2]}$. The name of the inequality is due to works of Lubell, Meshalkin and Yamamoto.

A collection $\mathcal{A}$ of sets is said to be an *antichain* if none of the sets is contained in any other, that is, $A \not\subseteq B$ for any distinct $A, B \in \mathcal{A}$.

Now consider subsets of $\{1, ..., N\}$. What antichains do we have here?

Obviously, a collection all subsets of the same size k form an antichain. It has size $\binom{N}{[N/2]}$ if $k = [N/2]$. In fact, this is the largest antichain.

Theorem (LYM inequality)

Let $\mathcal{A}$ be an antichain of subsets of $[N]$. Then

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1.$$

Since $\binom{N}{|A|} \leqslant \binom{N}{[N/2]}$, it implies that

$$\frac{|\mathcal{A}|}{\binom{N}{[N/2]}} \leqslant \sum_{A \in \mathcal{A}} \frac{1}{\binom{N}{|A|}} \leqslant 1$$

and $|\mathcal{A}| \leqslant \binom{N}{[N/2]}$. The name of the inequality is due to works of Lubell, Meshalkin and Yamamoto.

Proof of the LYM inequality. We give a probabilistic proof using the method of random maps. Let $\phi\colon [N] \to [N]$ be a random bijection chosen uniformly at random among all $N!$ such bijections. Let $A \subseteq [N]$. Then it is easy to see that

$$\mathbb{P}\left(\phi(A) = \{1, ..., |A|\}\right) = \frac{|A|!(N-|A|)!}{N!} = \frac{1}{\binom{N}{|A|}}.$$

But if $A, B \in \mathcal{A}$ and $A \neq B$, then the events $\phi(A) = \{1, ..., |A|\}$ and $\phi(B) = \{1, ..., |B|\}$ are disjoint. So

$$\sum_{A \in \mathcal{A}} \mathbb{P}\left(\phi(A) = \{1, .., |A|\}\right) = \mathbb{P}\left(\cup_{A \in \mathcal{A}} \left(\phi(A) = \{1, .., |A|\}\right)\right) \leqslant 1$$

and the claim follows.

Proof of the LYM inequality. We give a probabilistic proof using the method of random maps. Let $\phi\colon [N] \to [N]$ be a random bijection chosen uniformly at random among all $N!$ such bijections. Let $A \subseteq [N]$. Then it is easy to see that

$$\mathbb{P}\left(\phi(A) = \{1, ..., |A|\}\right) = \frac{|A|!(N-|A|)!}{N!} = \frac{1}{\binom{N}{|A|}}.$$

But if $A, B \in \mathcal{A}$ and $A \neq B$, then the events $\phi(A) = \{1, ..., |A|\}$ and $\phi(B) = \{1, ..., |B|\}$ are disjoint. So

$$\sum_{A \in \mathcal{A}} \mathbb{P}\left(\phi(A) = \{1, .., |A|\}\right) = \mathbb{P}\left(\cup_{A \in \mathcal{A}}\left(\phi(A) = \{1, .., |A|\}\right)\right) \leqslant 1$$

and the claim follows.

Proof of the LYM inequality. We give a probabilistic proof using the method of random maps. Let $\phi\colon [N] \to [N]$ be a random bijection chosen uniformly at random among all $N!$ such bijections. Let $A \subseteq [N]$. Then it is easy to see that

$$\mathbb{P}\left(\phi(A) = \{1, ..., |A|\}\right) = \frac{|A|!(N - |A|)!}{N!} = \frac{1}{\binom{N}{|A|}}.$$

But if $A, B \in \mathcal{A}$ and $A \neq B$, then the events $\phi(A) = \{1, ..., |A|\}$ and $\phi(B) = \{1, ..., |B|\}$ are disjoint. So

$$\sum_{A \in \mathcal{A}} \mathbb{P}\left(\phi(A) = \{1, .., |A|\}\right) = \mathbb{P}\left(\cup_{A \in \mathcal{A}} \left(\phi(A) = \{1, .., |A|\}\right)\right) \leqslant 1$$

and the claim follows.

Proof of the LYM inequality. We give a probabilistic proof using the method of random maps. Let $\phi\colon [N] \to [N]$ be a random bijection chosen uniformly at random among all $N!$ such bijections. Let $A \subseteq [N]$. Then it is easy to see that

$$\mathbb{P}\left(\phi(A) = \{1, ..., |A|\}\right) = \frac{|A|!(N-|A|)!}{N!} = \frac{1}{\binom{N}{|A|}}.$$

But if $A, B \in \mathcal{A}$ and $A \neq B$, then the events $\phi(A) = \{1, ..., |A|\}$ and $\phi(B) = \{1, ..., |B|\}$ are disjoint. So

$$\sum_{A \in \mathcal{A}} \mathbb{P}\left(\phi(A) = \{1, .., |A|\}\right) = \mathbb{P}\left(\cup_{A \in \mathcal{A}} \left(\phi(A) = \{1, .., |A|\}\right)\right) \leqslant 1$$

and the claim follows.

Theorem

Let $G = (V, E)$ be a graph with n vertices and e edges. Then G contains a bipartite subgraph with at least $e/2$ edges.

Proof. Let $T \subseteq V$ be a random subset given by $\mathbb{P}(x \in T) = 1/2$, with these choices mutually independent. Call an edge $\{x; y\} \in E$ crossing if exactly one of x and y is in T. It is easy to see that the subgraph formed by crossing edges is bipartite.

Let X be the number of crossing edges. We decompose

$$X = \sum_{\{x;y\} \in E} X_{xy},$$

where X_{xy} is the indicator random variable for $\{x; y\}$ being crossing. Then

$$\mathbb{E}X_{xy} = 1/2,$$

as two fair coin flips have probability $1/2$ of being different. Hence

$$\mathbb{E}X = \sum_{\{x;y\}} \mathbb{E}X_{xy} = e/2$$

and $X \geqslant e/2$ for some choice of T as desired.

Theorem

Let $G = (V, E)$ be a graph with n vertices and e edges. Then G contains a bipartite subgraph with at least $e/2$ edges.

Proof. Let $T \subseteq V$ be a random subset given by $\mathbb{P}(x \in T) = 1/2$, with these choices mutually independent. Call an edge $\{x; y\} \in E$ crossing if exactly one of x and y is in T. It is easy to see that the subgraph formed by crossing edges is bipartite.

Let X be the number of crossing edges. We decompose

$$X = \sum_{\{x;y\} \in E} X_{xy},$$

where X_{xy} is the indicator random variable for $\{x; y\}$ being crossing. Then

$$\mathbb{E}X_{xy} = 1/2,$$

as two fair coin flips have probability $1/2$ of being different. Hence

$$\mathbb{E}X = \sum_{\{x;y\}} \mathbb{E}X_{xy} = e/2$$

and $X \geqslant e/2$ for some choice of T as desired.

Theorem

Let $G = (V, E)$ be a graph with n vertices and e edges. Then G contains a bipartite subgraph with at least $e/2$ edges.

Proof. Let $T \subseteq V$ be a random subset given by $\mathbb{P}(x \in T) = 1/2$, with these choices mutually independent. Call an edge $\{x; y\} \in E$ crossing if exactly one of x and y is in T. It is easy to see that the subgraph formed by crossing edges is bipartite.

Let X be the number of crossing edges. We decompose

$$X = \sum_{\{x;y\} \in E} X_{xy},$$

where X_{xy} is the indicator random variable for $\{x; y\}$ being crossing. Then

$$\mathbb{E}X_{xy} = 1/2,$$

as two fair coin flips have probability $1/2$ of being different. Hence

$$\mathbb{E}X = \sum_{\{x;y\}} \mathbb{E}X_{xy} = e/2$$

and $X \geqslant e/2$ for some choice of T as desired.

Theorem

Let $G = (V, E)$ be a graph with n vertices and e edges. Then G contains a bipartite subgraph with at least $e/2$ edges.

Proof. Let $T \subseteq V$ be a random subset given by $\mathbb{P}(x \in T) = 1/2$, with these choices mutually independent. Call an edge $\{x; y\} \in E$ crossing if exactly one of x and y is in T. It is easy to see that the subgraph formed by crossing edges is bipartite.

Let X be the number of crossing edges. We decompose

$$X = \sum_{\{x;y\} \in E} X_{xy},$$

where X_{xy} is the indicator random variable for $\{x; y\}$ being crossing. Then

$$\mathbb{E}X_{xy} = 1/2,$$

as two fair coin flips have probability $1/2$ of being different. Hence

$$\mathbb{E}X = \sum_{\{x;y\}} \mathbb{E}X_{xy} = e/2$$

and $X \geqslant e/2$ for some choice of T as desired.

Theorem

Let $G = (V, E)$ be a graph with n vertices and e edges. Then G contains a bipartite subgraph with at least $e/2$ edges.

Proof. Let $T \subseteq V$ be a random subset given by $\mathbb{P}(x \in T) = 1/2$, with these choices mutually independent. Call an edge $\{x; y\} \in E$ crossing if exactly one of x and y is in T. It is easy to see that the subgraph formed by crossing edges is bipartite.

Let X be the number of crossing edges. We decompose

$$X = \sum_{\{x;y\} \in E} X_{xy},$$

where X_{xy} is the indicator random variable for $\{x; y\}$ being crossing. Then

$$\mathbb{E}X_{xy} = 1/2,$$

as two fair coin flips have probability $1/2$ of being different. Hence

$$\mathbb{E}X = \sum_{\{x;y\}} \mathbb{E}X_{xy} = e/2$$

and $X \geqslant e/2$ for some choice of T as desired.

Suppose that $a = \{a_i\}_{i=1}^n$ be a finite sequence of real numbers. Having defined the expectation $\mathbb{E}a = \frac{1}{n}\sum_{i=1}^n a_i$, we want to get some information about how large the deviation $|a_i - \mathbb{E}a|$ can be. Then it is logical to define the variation

$$\operatorname{Var} a := \mathbb{E}\,|a_i - \mathbb{E}a|^2 = \mathbb{E}a_i^2 - 2\mathbb{E}\left(a_i\mathbb{E}a\right) + (\mathbb{E}a)^2 = \mathbb{E}a^2 - \mathbb{E}^2 a.$$

How to use variation?

Theorem (Markov's inequality)

Let X be a non-negative random variable. Then for any $\lambda > 0$

$$\mathbb{P}(X \geqslant \lambda) \leqslant \frac{\mathbb{E}X}{\lambda}.$$

Proof.

$$\mathbb{E}X = \int_\Omega X d\mu \geqslant \int_{\omega: X(\omega)\geqslant\lambda} X d\mu \geqslant \int_{\omega: X(\omega)\geqslant\lambda} \lambda d\mu = \lambda\mathbb{P}(X \geqslant \lambda).$$

So $X \leqslant 10\mathbb{E}X$ with probability at least 90%.

Suppose that $a = \{a_i\}_{i=1}^n$ be a finite sequence of real numbers. Having defined the expectation $\mathbb{E}a = \frac{1}{n}\sum_{i=1}^n a_i$, we want to get some information about how large the deviation $|a_i - \mathbb{E}a|$ can be. Then it is logical to define the variation

$$\operatorname{Var} a := \mathbb{E}\left|a_i - \mathbb{E}a\right|^2 = \mathbb{E}a_i^2 - 2\mathbb{E}\left(a_i\mathbb{E}a\right) + (\mathbb{E}a)^2 = \mathbb{E}a^2 - \mathbb{E}^2 a.$$

How to use variation?

Theorem (Markov's inequality)

Let X be a non-negative random variable. Then for any $\lambda > 0$

$$\mathbb{P}(X \geqslant \lambda) \leqslant \frac{\mathbb{E}X}{\lambda}.$$

Proof.

$$\mathbb{E}X = \int_\Omega X d\mu \geqslant \int_{\omega:X(\omega)\geqslant\lambda} X d\mu \geqslant \int_{\omega:X(\omega)\geqslant\lambda} \lambda d\mu = \lambda\mathbb{P}(X \geqslant \lambda).$$

So $X \leqslant 10\mathbb{E}X$ with probability at least 90%.

Suppose that $a = \{a_i\}_{i=1}^n$ be a finite sequence of real numbers. Having defined the expectation $\mathbb{E}a = \frac{1}{n}\sum_{i=1}^n a_i$, we want to get some information about how large the deviation $|a_i - \mathbb{E}a|$ can be. Then it is logical to define the variation

$$\operatorname{Var} a := \mathbb{E}\,|a_i - \mathbb{E}a|^2 = \mathbb{E}a_i^2 - 2\mathbb{E}\,(a_i\mathbb{E}a) + (\mathbb{E}a)^2 = \mathbb{E}a^2 - \mathbb{E}^2 a.$$

How to use variation?

Theorem (Markov's inequality)

Let X be a non-negative random variable. Then for any $\lambda > 0$

$$\mathbb{P}(X \geqslant \lambda) \leqslant \frac{\mathbb{E}X}{\lambda}.$$

Proof.

$$\mathbb{E}X = \int_{\Omega} X d\mu \geqslant \int_{\omega : X(\omega) \geqslant \lambda} X d\mu \geqslant \int_{\omega : X(\omega) \geqslant \lambda} \lambda d\mu = \lambda \mathbb{P}(X \geqslant \lambda).$$

So $X \leqslant 10\mathbb{E}X$ with probability at least 90%.

Suppose that $a = \{a_i\}_{i=1}^n$ be a finite sequence of real numbers. Having defined the expectation $\mathbb{E}a = \frac{1}{n}\sum_{i=1}^n a_i$, we want to get some information about how large the deviation $|a_i - \mathbb{E}a|$ can be. Then it is logical to define the variation

$$\operatorname{Var} a := \mathbb{E}\,|a_i - \mathbb{E}a|^2 = \mathbb{E}a_i^2 - 2\mathbb{E}\,(a_i\mathbb{E}a) + (\mathbb{E}a)^2 = \mathbb{E}a^2 - \mathbb{E}^2 a.$$

How to use variation?

Theorem (Markov's inequality)

Let X be a non-negative random variable. Then for any $\lambda > 0$

$$\mathbb{P}(X \geqslant \lambda) \leqslant \frac{\mathbb{E}X}{\lambda}.$$

Proof.

$$\mathbb{E}X = \int_{\Omega} X d\mu \geqslant \int_{\omega: X(\omega)\geqslant\lambda} X d\mu \geqslant \int_{\omega: X(\omega)\geqslant\lambda} \lambda d\mu = \lambda\mathbb{P}(X \geqslant \lambda).$$

So $X \leqslant 10\mathbb{E}X$ with probability at least 90%.

Suppose that $a = \{a_i\}_{i=1}^n$ be a finite sequence of real numbers. Having defined the expectation $\mathbb{E}a = \frac{1}{n}\sum_{i=1}^n a_i$, we want to get some information about how large the deviation $|a_i - \mathbb{E}a|$ can be. Then it is logical to define the variation

$$\operatorname{Var} a := \mathbb{E}\,|a_i - \mathbb{E}a|^2 = \mathbb{E}a_i^2 - 2\mathbb{E}\,(a_i\mathbb{E}a) + (\mathbb{E}a)^2 = \mathbb{E}a^2 - \mathbb{E}^2 a.$$

How to use variation?

Theorem (Markov's inequality)

Let X be a non-negative random variable. Then for any $\lambda > 0$

$$\mathbb{P}(X \geqslant \lambda) \leqslant \frac{\mathbb{E}X}{\lambda}.$$

Proof.

$$\mathbb{E}X = \int_\Omega X d\mu \geqslant \int_{\omega : X(\omega)\geqslant\lambda} X d\mu \geqslant \int_{\omega : X(\omega)\geqslant\lambda} \lambda d\mu = \lambda\mathbb{P}(X \geqslant \lambda).$$

So $X \leqslant 10\mathbb{E}X$ with probability at least 90%.

Suppose that $a = \{a_i\}_{i=1}^n$ be a finite sequence of real numbers. Having defined the expectation $\mathbb{E}a = \frac{1}{n}\sum_{i=1}^n a_i$, we want to get some information about how large the deviation $|a_i - \mathbb{E}a|$ can be. Then it is logical to define the variation

$$\operatorname{Var} a := \mathbb{E}\,|a_i - \mathbb{E}a|^2 = \mathbb{E}a_i^2 - 2\mathbb{E}\,(a_i \mathbb{E}a) + (\mathbb{E}a)^2 = \mathbb{E}a^2 - \mathbb{E}^2 a.$$

How to use variation?

Theorem (Markov's inequality)

Let X be a non-negative random variable. Then for any $\lambda > 0$

$$\mathbb{P}(X \geqslant \lambda) \leqslant \frac{\mathbb{E}X}{\lambda}.$$

Proof.

$$\mathbb{E}X = \int\limits_{\Omega} X d\mu \geqslant \int\limits_{\omega : X(\omega) \geqslant \lambda} X d\mu \geqslant \int\limits_{\omega : X(\omega) \geqslant \lambda} \lambda d\mu = \lambda \mathbb{P}(X \geqslant \lambda).$$

So $X \leqslant 10\mathbb{E}X$ with probability at least 90%.

Theorem (Chebyshev's inequality)

Let $\lambda > 0$. *Then we have*

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) \leqslant \frac{1}{\lambda^2}.$$

Proof. By Markov's inequality

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) = \mathbb{P}\left(|X - \mathbb{E}X|^2 \geqslant \lambda^2 \operatorname{Var} X\right) \leqslant \frac{\mathbb{E}|X - \mathbb{E}X|^2}{\lambda^2 \operatorname{Var} X} = \frac{1}{\lambda^2}.$$

So $X = \mathbb{E}X + O(\lambda \operatorname{Var}^{1/2} X)$ with probability $1 - O\left(\frac{1}{\lambda^2}\right)$.

The quantity $\sigma := \operatorname{Var}^{1/2} X$ is called *the standard deviation* of X.

This works good when variation is small with respect to expectation.

Theorem (Chebyshev's inequality)

Let $\lambda > 0$. *Then we have*

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) \leqslant \frac{1}{\lambda^2}.$$

Proof. By Markov's inequality

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) = \mathbb{P}\left(|X - \mathbb{E}X|^2 \geqslant \lambda^2 \operatorname{Var} X\right) \leqslant \frac{\mathbb{E}|X - \mathbb{E}X|^2}{\lambda^2 \operatorname{Var} X} = \frac{1}{\lambda^2}.$$

So $X = \mathbb{E}X + O(\lambda \operatorname{Var}^{1/2} X)$ with probability $1 - O\left(\frac{1}{\lambda^2}\right)$.

The quantity $\sigma := \operatorname{Var}^{1/2} X$ is called *the standard deviation* of X.

This works good when variation is small with respect to expectation.

Theorem (Chebyshev's inequality)

Let $\lambda > 0$. Then we have

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) \leqslant \frac{1}{\lambda^2}.$$

Proof. By Markov's inequality

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) = \mathbb{P}\left(|X - \mathbb{E}X|^2 \geqslant \lambda^2 \operatorname{Var} X\right) \leqslant \frac{\mathbb{E}|X - \mathbb{E}X|^2}{\lambda^2 \operatorname{Var} X} = \frac{1}{\lambda^2}.$$

So $X = \mathbb{E}X + O(\lambda \operatorname{Var}^{1/2} X)$ with probability $1 - O\left(\frac{1}{\lambda^2}\right)$.

The quantity $\sigma := \operatorname{Var}^{1/2} X$ is called *the standard deviation* of X.

This works good when variation is small with respect to expectation.

Theorem (Chebyshev's inequality)

Let $\lambda > 0$. *Then we have*

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) \leqslant \frac{1}{\lambda^2}.$$

Proof. By Markov's inequality

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) = \mathbb{P}\left(|X - \mathbb{E}X|^2 \geqslant \lambda^2 \operatorname{Var} X\right) \leqslant \frac{\mathbb{E}|X - \mathbb{E}X|^2}{\lambda^2 \operatorname{Var} X} = \frac{1}{\lambda^2}.$$

So $X = \mathbb{E}X + O(\lambda \operatorname{Var}^{1/2} X)$ with probability $1 - O\left(\frac{1}{\lambda^2}\right)$.

The quantity $\sigma := \operatorname{Var}^{1/2} X$ is called *the standard deviation* of X.

This works good when variation is small with respect to expectation.

Theorem (Chebyshev's inequality)

Let $\lambda > 0$. *Then we have*

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) \leqslant \frac{1}{\lambda^2}.$$

Proof. By Markov's inequality

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda \operatorname{Var}^{1/2} X\right) = \mathbb{P}\left(|X - \mathbb{E}X|^2 \geqslant \lambda^2 \operatorname{Var} X\right) \leqslant \frac{\mathbb{E}|X - \mathbb{E}X|^2}{\lambda^2 \operatorname{Var} X} = \frac{1}{\lambda^2}.$$

So $X = \mathbb{E}X + O(\lambda \operatorname{Var}^{1/2} X)$ with probability $1 - O\left(\frac{1}{\lambda^2}\right)$.

The quantity $\sigma := \operatorname{Var}^{1/2} X$ is called *the standard deviation* of X.

This works good when variation is small with respect to expectation.

Example 11: $\omega(n)$

Let n be chosen uniformly at random from $[1,x]\cap\mathbb{Z}$ and define $\omega(n)=\sum_{p|n}1$ to be the number of prime divisors of n. Then (x is a large positive integer)

$$\mathbb{E}\omega(n)=\frac{1}{x}\sum_{n\leqslant x}\sum_{p|n}1=\frac{1}{x}\sum_{p\leqslant x}\sum_{n\leqslant x,p|n}1=\frac{1}{x}\sum_{p\leqslant x}\left[\frac{x}{p}\right]=$$

$$\frac{1}{x}\sum_{p\leqslant x}\left(\frac{x}{p}-\left\{\frac{x}{p}\right\}\right)=\sum_{p\leqslant x}\frac{1}{p}+O(1)=\log\log x+O(1).$$

It is not hard to show that

$$\operatorname{Var}\omega(n)=O(\log\log x).$$

Let $f(x)\to\infty$ as $x\to\infty$. Then by Chebyshev's inequality we have

$$\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant f(x)(\log\log x)^{1/2}\right)\ll\frac{1}{f(x)^2}=o(1),\quad x\to\infty.$$

So if we take randomly $n\leqslant x$, then $\omega(n)\sim\log\log x$ almost surely (with probability $1-o(1)$, $x\to\infty$). In particular, for any fixed $\varepsilon>0$

$$\mathbb{P}\left((1-\varepsilon)\log\log x\leqslant\omega(n)\leqslant(1+\varepsilon)\log\log x\right)=1-O\left(\frac{1}{\varepsilon^2\log\log x}\right).$$

Let n be chosen uniformly at random from $[1,x]\cap\mathbb{Z}$ and define $\omega(n)=\sum_{p|n}1$ to be the number of prime divisors of n. Then (x is a large positive integer)

$$\mathbb{E}\omega(n)=\frac{1}{x}\sum_{n\leqslant x}\sum_{p|n}1=\frac{1}{x}\sum_{p\leqslant x}\sum_{n\leqslant x,p|n}1=\frac{1}{x}\sum_{p\leqslant x}\left[\frac{x}{p}\right]=$$
$$\frac{1}{x}\sum_{p\leqslant x}\left(\frac{x}{p}-\left\{\frac{x}{p}\right\}\right)=\sum_{p\leqslant x}\frac{1}{p}+O(1)=\log\log x+O(1).$$

It is not hard to show that

$$\operatorname{Var}\omega(n)=O(\log\log x).$$

Let $f(x)\to\infty$ as $x\to\infty$. Then by Chebyshev's inequality we have

$$\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant f(x)(\log\log x)^{1/2}\right)\ll\frac{1}{f(x)^2}=o(1),\quad x\to\infty.$$

So if we take randomly $n\leqslant x$, then $\omega(n)\sim\log\log x$ almost surely (with probability $1-o(1)$, $x\to\infty$). In particular, for any fixed $\varepsilon>0$

$$\mathbb{P}\left((1-\varepsilon)\log\log x\leqslant\omega(n)\leqslant(1+\varepsilon)\log\log x\right)=1-O\left(\frac{1}{\varepsilon^2\log\log x}\right).$$

Let n be chosen uniformly at random from $[1,x]\cap\mathbb{Z}$ and define $\omega(n)=\sum_{p|n}1$ to be the number of prime divisors of n. Then (x is a large positive integer)

$$\mathbb{E}\omega(n)=\frac{1}{x}\sum_{n\leqslant x}\sum_{p|n}1=\frac{1}{x}\sum_{p\leqslant x}\sum_{n\leqslant x,p|n}1=\frac{1}{x}\sum_{p\leqslant x}\left[\frac{x}{p}\right]=$$
$$\frac{1}{x}\sum_{p\leqslant x}\left(\frac{x}{p}-\left\{\frac{x}{p}\right\}\right)=\sum_{p\leqslant x}\frac{1}{p}+O(1)=\log\log x+O(1).$$

It is not hard to show that

$$\operatorname{Var}\omega(n)=O(\log\log x).$$

Let $f(x)\to\infty$ as $x\to\infty$. Then by Chebyshev's inequality we have

$$\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant f(x)(\log\log x)^{1/2}\right)\ll\frac{1}{f(x)^2}=o(1),\quad x\to\infty.$$

So if we take randomly $n\leqslant x$, then $\omega(n)\sim\log\log x$ almost surely (with probability $1-o(1)$, $x\to\infty$). In particular, for any fixed $\varepsilon>0$

$$\mathbb{P}\left((1-\varepsilon)\log\log x\leqslant\omega(n)\leqslant(1+\varepsilon)\log\log x\right)=1-O\left(\frac{1}{\varepsilon^2\log\log x}\right).$$

Let n be chosen uniformly at random from $[1,x]\cap\mathbb{Z}$ and define $\omega(n)=\sum_{p|n}1$ to be the number of prime divisors of n. Then (x is a large positive integer)

$$\mathbb{E}\omega(n)=\frac{1}{x}\sum_{n\leqslant x}\sum_{p|n}1=\frac{1}{x}\sum_{p\leqslant x}\sum_{n\leqslant x,p|n}1=\frac{1}{x}\sum_{p\leqslant x}\left[\frac{x}{p}\right]=$$
$$\frac{1}{x}\sum_{p\leqslant x}\left(\frac{x}{p}-\left\{\frac{x}{p}\right\}\right)=\sum_{p\leqslant x}\frac{1}{p}+O(1)=\log\log x+O(1).$$

It is not hard to show that

$$\operatorname{Var}\omega(n)=O(\log\log x).$$

Let $f(x)\to\infty$ as $x\to\infty$. Then by Chebyshev's inequality we have

$$\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant f(x)(\log\log x)^{1/2}\right)\ll\frac{1}{f(x)^2}=o(1),\quad x\to\infty.$$

So if we take randomly $n\leqslant x$, then $\omega(n)\sim\log\log x$ almost surely (with probability $1-o(1)$, $x\to\infty$). In particular, for any fixed $\varepsilon>0$

$$\mathbb{P}\left((1-\varepsilon)\log\log x\leqslant\omega(n)\leqslant(1+\varepsilon)\log\log x\right)=1-O\left(\frac{1}{\varepsilon^2\log\log x}\right).$$

Let n be chosen uniformly at random from $[1,x]\cap\mathbb{Z}$ and define $\omega(n)=\sum_{p|n}1$ to be the number of prime divisors of n. Then (x is a large positive integer)

$$\mathbb{E}\omega(n)=\frac{1}{x}\sum_{n\leqslant x}\sum_{p|n}1=\frac{1}{x}\sum_{p\leqslant x}\sum_{n\leqslant x,p|n}1=\frac{1}{x}\sum_{p\leqslant x}\left[\frac{x}{p}\right]=$$

$$\frac{1}{x}\sum_{p\leqslant x}\left(\frac{x}{p}-\left\{\frac{x}{p}\right\}\right)=\sum_{p\leqslant x}\frac{1}{p}+O(1)=\log\log x+O(1).$$

It is not hard to show that

$$\operatorname{Var}\omega(n)=O(\log\log x).$$

Let $f(x)\to\infty$ as $x\to\infty$. Then by Chebyshev's inequality we have

$$\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant f(x)(\log\log x)^{1/2}\right)\ll\frac{1}{f(x)^2}=o(1),\quad x\to\infty.$$

So if we take randomly $n\leqslant x$, then $\omega(n)\sim\log\log x$ almost surely (with probability $1-o(1)$, $x\to\infty$). In particular, for any fixed $\varepsilon>0$

$$\mathbb{P}\left((1-\varepsilon)\log\log x\leqslant\omega(n)\leqslant(1+\varepsilon)\log\log x\right)=1-O\left(\frac{1}{\varepsilon^2\log\log x}\right).$$

Let n be chosen uniformly at random from $[1,x]\cap\mathbb{Z}$ and define $\omega(n)=\sum_{p|n}1$ to be the number of prime divisors of n. Then (x is a large positive integer)

$$\mathbb{E}\omega(n)=\frac{1}{x}\sum_{n\leqslant x}\sum_{p|n}1=\frac{1}{x}\sum_{p\leqslant x}\sum_{n\leqslant x,p|n}1=\frac{1}{x}\sum_{p\leqslant x}\left[\frac{x}{p}\right]=$$

$$\frac{1}{x}\sum_{p\leqslant x}\left(\frac{x}{p}-\left\{\frac{x}{p}\right\}\right)=\sum_{p\leqslant x}\frac{1}{p}+O(1)=\log\log x+O(1).$$

It is not hard to show that

$$\operatorname{Var}\omega(n)=O(\log\log x).$$

Let $f(x)\to\infty$ as $x\to\infty$. Then by Chebyshev's inequality we have

$$\mathbb{P}\left(|\omega(n)-\log\log x|\geqslant f(x)(\log\log x)^{1/2}\right)\ll\frac{1}{f(x)^2}=o(1),\quad x\to\infty.$$

So if we take randomly $n\leqslant x$, then $\omega(n)\sim\log\log x$ almost surely (with probability $1-o(1)$, $x\to\infty$). In particular, for any fixed $\varepsilon>0$

$$\mathbb{P}\left((1-\varepsilon)\log\log x\leqslant\omega(n)\leqslant(1+\varepsilon)\log\log x\right)=1-O\left(\frac{1}{\varepsilon^2\log\log x}\right).$$

Let $M(N)$ be the number of distinct integers in an $N \times N$ multiplication table. Is it true that $M(N) = o(N^2)$ as $N \to \infty$?

Yeap. Indeed, almost all numbers $i, j \in \{1, ..., N\}$ have approximately $\log\log N$ prime factors (in fact, even if we count them with multiplicity). Then almost all products ij have approximately $2\log\log N$ prime factors counted with multiplicity. But there are only $O\left(\frac{N^2}{\log\log N}\right)$ such numbers up to N^2.

Theorem (Erdös, 1960)

We have

$$M(N) = \frac{N^2}{(\log N)^{\delta+o(1)}},$$

where $\delta := 1 - \frac{1+\log\log 2}{\log 2} = 0.086...$.

Theorem (Ford, 2008)

We have

$$M(N) \asymp \frac{N^2}{(\log N)^{\delta}(\log\log N)^{3/2}}.$$

Let $M(N)$ be the number of distinct integers in an $N \times N$ multiplication table. Is it true that $M(N) = o(N^2)$ as $N \to \infty$?

Yeap. Indeed, almost all numbers $i, j \in \{1, ..., N\}$ have approximately $\log\log N$ prime factors (in fact, even if we count them with multiplicity). Then almost all products ij have approximately $2\log\log N$ prime factors counted with multiplicity. But there are only $O\left(\frac{N^2}{\log\log N}\right)$ such numbers up to N^2.

Theorem (Erdös, 1960)

We have

$$M(N) = \frac{N^2}{(\log N)^{\delta + o(1)}},$$

where $\delta := 1 - \frac{1+\log\log 2}{\log 2} = 0.086...$.

Theorem (Ford, 2008)

We have

$$M(N) \asymp \frac{N^2}{(\log N)^{\delta}(\log\log N)^{3/2}}.$$

Let $M(N)$ be the number of distinct integers in an $N \times N$ multiplication table. Is it true that $M(N) = o(N^2)$ as $N \to \infty$?

Yeap. Indeed, almost all numbers $i, j \in \{1, ..., N\}$ have approximately $\log\log N$ prime factors (in fact, even if we count them with multiplicity). Then almost all products ij have approximately $2\log\log N$ prime factors counted with multiplicity. But there are only $O\left(\frac{N^2}{\log\log N}\right)$ such numbers up to N^2.

Theorem (Erdös, 1960)

We have

$$M(N) = \frac{N^2}{(\log N)^{\delta + o(1)}},$$

where $\delta := 1 - \frac{1+\log\log 2}{\log 2} = 0.086...$.

Theorem (Ford, 2008)

We have

$$M(N) \asymp \frac{N^2}{(\log N)^{\delta}(\log\log N)^{3/2}}.$$

Corollary: Erdös's Multiplication Table Problem

Let $M(N)$ be the number of distinct integers in an $N \times N$ multiplication table. Is it true that $M(N) = o(N^2)$ as $N \to \infty$?

Yeap. Indeed, almost all numbers $i, j \in \{1, ..., N\}$ have approximately $\log\log N$ prime factors (in fact, even if we count them with multiplicity). Then almost all products ij have approximately $2\log\log N$ prime factors counted with multiplicity. But there are only $O\left(\frac{N^2}{\log\log N}\right)$ such numbers up to N^2.

Theorem (Erdös, 1960)

We have

$$M(N) = \frac{N^2}{(\log N)^{\delta + o(1)}},$$

where $\delta := 1 - \frac{1+\log\log 2}{\log 2} = 0.086....$

Theorem (Ford, 2008)

We have

$$M(N) \asymp \frac{N^2}{(\log N)^{\delta}(\log\log N)^{3/2}}.$$

What about standard values of $\omega(p-1)$, where p is prime?

Let a prime $p \leqslant x$ be chosen uniformly at random from $[1,x] \cap \mathcal{P}$. Using an advanced result from ANT (the so-called Bombieri-Vinogradov theorem) it is easy to deduce that

$$\mathbb{E}\omega(p-1) = \log\log x + O(1)$$

and

$$\operatorname{Var}\omega(p-1) = O(\log\log x)$$

So again by Chebyshev's inequality $\omega(p-1) \sim \log\log x$ almost surely.

So in some sense the numbers $p-1$ for primes $p \leqslant x$ behave like random numbers $n \leqslant x$.

What about standard values of $\omega(p-1)$, where p is prime?

Let a prime $p \leqslant x$ be chosen uniformly at random from $[1,x] \cap \mathcal{P}$. Using an advanced result from ANT (the so-called Bombieri-Vinogradov theorem) it is easy to deduce that

$$\mathbb{E}\omega(p-1) = \log\log x + O(1)$$

and

$$\mathrm{Var}\,\omega(p-1) = O(\log\log x)$$

So again by Chebyshev's inequality $\omega(p-1) \sim \log\log x$ almost surely.

So in some sense the numbers $p-1$ for primes $p \leqslant x$ behave like random numbers $n \leqslant x$.

What about standard values of $\omega(p-1)$, where p is prime?

Let a prime $p \leqslant x$ be chosen uniformly at random from $[1, x] \cap \mathcal{P}$. Using an advanced result from ANT (the so-called Bombieri-Vinogradov theorem) it is easy to deduce that

$$\mathbb{E}\omega(p-1) = \log\log x + O(1)$$

and

$$\operatorname{Var} \omega(p-1) = O(\log\log x)$$

So again by Chebyshev's inequality $\omega(p-1) \sim \log\log x$ almost surely.

So in some sense the numbers $p-1$ for primes $p \leqslant x$ behave like random numbers $n \leqslant x$.

What about standard values of $\omega(p-1)$, where p is prime?

Let a prime $p \leqslant x$ be chosen uniformly at random from $[1, x] \cap \mathcal{P}$. Using an advanced result from ANT (the so-called Bombieri-Vinogradov theorem) it is easy to deduce that

$$\mathbb{E}\omega(p-1) = \log\log x + O(1)$$

and

$$\operatorname{Var}\omega(p-1) = O(\log\log x)$$

So again by Chebyshev's inequality $\omega(p-1) \sim \log\log x$ almost surely.

So in some sense the numbers $p-1$ for primes $p \leqslant x$ behave like random numbers $n \leqslant x$.

Example 12: $\omega(p-1)$

What about standard values of $\omega(p-1)$, where p is prime?

Let a prime $p \leqslant x$ be chosen uniformly at random from $[1,x] \cap \mathcal{P}$. Using an advanced result from ANT (the so-called Bombieri-Vinogradov theorem) it is easy to deduce that

$$\mathbb{E}\omega(p-1) = \log\log x + O(1)$$

and

$$\operatorname{Var}\omega(p-1) = O(\log\log x)$$

So again by Chebyshev's inequality $\omega(p-1) \sim \log\log x$ almost surely.

So in some sense the numbers $p-1$ for primes $p \leqslant x$ behave like random numbers $n \leqslant x$.

Sometimes the second method does not work (and this is ok).

Let $\tau(n) = \sum_{d|n} 1$ be the divisor function. Then

$$\mathbb{E}\tau(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\sum_{n\leqslant x, d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\left[\frac{x}{d}\right] = \sum_{d\leqslant x}\frac{1}{d} + O(1) = \log x + O(1).$$

One can prove that

$$\operatorname{Var}\tau(n) = \frac{1}{6\zeta(2)}\log^3 x + O(\log^2 x).$$

So the standard deviation is of order $\log^{3/2} x$ which is much larger than $\mathbb{E}\tau(n)$ and the second moment method fails.

Nevertheless, we do have asymptotics almost surely here.

Theorem (a folklore one)

For any $\varepsilon > 0$ we have

$$\mathbb{P}\left((\log x)^{(\log 2-\varepsilon)} \leqslant \tau(n) \leqslant (\log x)^{(\log 2+\varepsilon)}\right) = 1 - o(1), \quad x \to \infty.$$

Sometimes the second method does not work (and this is ok).

Let $\tau(n) = \sum_{d|n} 1$ be the divisor function. Then

$$\mathbb{E}\tau(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\sum_{n\leqslant x, d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\left[\frac{x}{d}\right] = \sum_{d\leqslant x}\frac{1}{d} + O(1) = \log x + O(1).$$

One can prove that

$$\operatorname{Var}\tau(n) = \frac{1}{6\zeta(2)}\log^3 x + O(\log^2 x).$$

So the standard deviation is of order $\log^{3/2} x$ which is much larger than $\mathbb{E}\tau(n)$ and the second moment method fails.

Nevertheless, we do have asymptotics almost surely here.

Theorem (a folklore one)

For any $\varepsilon > 0$ we have

$$\mathbb{P}\left((\log x)^{(\log 2-\varepsilon)} \leqslant \tau(n) \leqslant (\log x)^{(\log 2+\varepsilon)}\right) = 1 - o(1), \quad x \to \infty.$$

Sometimes the second method does not work (and this is ok).

Let $\tau(n) = \sum_{d|n} 1$ be the divisor function. Then

$$\mathbb{E}\tau(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\sum_{n\leqslant x, d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\left[\frac{x}{d}\right] = \sum_{d\leqslant x}\frac{1}{d} + O(1) = \log x + O(1).$$

One can prove that

$$\mathrm{Var}\,\tau(n) = \frac{1}{6\zeta(2)}\log^3 x + O(\log^2 x).$$

So the standard deviation is of order $\log^{3/2} x$ which is much larger than $\mathbb{E}\tau(n)$ and the second moment method fails.

Nevertheless, we do have asymptotics almost surely here.

Theorem (a folklore one)

For any $\varepsilon > 0$ we have

$$\mathbb{P}\left((\log x)^{(\log 2-\varepsilon)} \leqslant \tau(n) \leqslant (\log x)^{(\log 2+\varepsilon)}\right) = 1 - o(1), \quad x \to \infty.$$

Example 13: $\tau(n)$

Sometimes the second method does not work (and this is ok).

Let $\tau(n) = \sum_{d|n} 1$ be the divisor function. Then

$$\mathbb{E}\tau(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\sum_{n\leqslant x, d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\left[\frac{x}{d}\right] = \sum_{d\leqslant x}\frac{1}{d} + O(1) = \log x + O(1).$$

One can prove that

$$\operatorname{Var}\tau(n) = \frac{1}{6\zeta(2)}\log^3 x + O(\log^2 x).$$

So the standard deviation is of order $\log^{3/2} x$ which is much larger than $\mathbb{E}\tau(n)$ and the second moment method fails.

Nevertheless, we do have asymptotics almost surely here.

Theorem (a folklore one)

For any $\varepsilon > 0$ we have

$$\mathbb{P}\left((\log x)^{(\log 2-\varepsilon)} \leqslant \tau(n) \leqslant (\log x)^{(\log 2+\varepsilon)}\right) = 1 - o(1), \quad x \to \infty.$$

Example 13: $\tau(n)$

Sometimes the second method does not work (and this is ok).

Let $\tau(n) = \sum_{d|n} 1$ be the divisor function. Then

$$\mathbb{E}\tau(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\sum_{n\leqslant x, d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\left[\frac{x}{d}\right] = \sum_{d\leqslant x}\frac{1}{d} + O(1) = \log x + O(1).$$

One can prove that

$$\operatorname{Var}\tau(n) = \frac{1}{6\zeta(2)}\log^3 x + O(\log^2 x).$$

So the standard deviation is of order $\log^{3/2} x$ which is much larger than $\mathbb{E}\tau(n)$ and the second moment method fails.

Nevertheless, we do have asymptotics almost surely here.

Theorem (a folklore one)

For any $\varepsilon > 0$ we have

$$\mathbb{P}\left((\log x)^{(\log 2-\varepsilon)} \leqslant \tau(n) \leqslant (\log x)^{(\log 2+\varepsilon)}\right) = 1 - o(1), \quad x \to \infty.$$

Sometimes the second method does not work (and this is ok).

Let $\tau(n) = \sum_{d|n} 1$ be the divisor function. Then

$$\mathbb{E}\tau(n) = \frac{1}{x}\sum_{n\leqslant x}\sum_{d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\sum_{n\leqslant x, d|n} 1 = \frac{1}{x}\sum_{d\leqslant x}\left[\frac{x}{d}\right] = \sum_{d\leqslant x}\frac{1}{d} + O(1) = \log x + O(1).$$

One can prove that

$$\operatorname{Var}\tau(n) = \frac{1}{6\zeta(2)}\log^3 x + O(\log^2 x).$$

So the standard deviation is of order $\log^{3/2} x$ which is much larger than $\mathbb{E}\tau(n)$ and the second moment method fails.

Nevertheless, we do have asymptotics almost surely here.

Theorem (a folklore one)

For any $\varepsilon > 0$ we have

$$\mathbb{P}\left((\log x)^{(\log 2-\varepsilon)} \leqslant \tau(n) \leqslant (\log x)^{(\log 2+\varepsilon)}\right) = 1 - o(1), \quad x \to \infty.$$

Example 14: Good intersection with a hyperplane

Let $a = (a_1, ..., a_d), b = (b_1, ..., b_d) \in \mathbb{Z}_p^d$. Define

$$ab = (a, b) = a_1 b_1 + ... + a_d b_d \in \mathbb{Z}_p.$$

Define a hyperplane $L \subseteq \mathbb{Z}_p^d$ to be any set of the form

$$L = L_{\eta,u} = \{x \in \mathbb{Z}_p^d : x\eta = u\},$$

where $\eta \in \mathbb{Z}_p^d$, $\eta \neq 0$, and $u \in \mathbb{Z}_p$.

Lemma

Let $A \subset \mathbb{Z}_p^d$ and $|A| = \delta p^d$. Then there exists a hyperplane $L \subset \mathbb{Z}_p^d$ such that

$$|A \cap L| = p^{d-1}(\delta + \theta \delta^{1/2} p^{-(d-1)/2}),$$

where $|\theta| \leqslant 1$.

Proof. Let us choose a hyperplane (that is, a pair $(\eta, u) \in \mathbb{Z}_p^d \times \mathbb{Z}_p$) uniformly at random and consider the random variable

$$\xi = |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u)$$

Example 14: Good intersection with a hyperplane

Let $a = (a_1, ..., a_d), b = (b_1, ..., b_d) \in \mathbb{Z}_p^d$. Define

$$ab = (a, b) = a_1 b_1 + ... + a_d b_d \in \mathbb{Z}_p.$$

Define a hyperplane $L \subseteq \mathbb{Z}_p^d$ to be any set of the form

$$L = L_{\eta,u} = \{x \in \mathbb{Z}_p^d : x\eta = u\},$$

where $\eta \in \mathbb{Z}_p^d$, $\eta \neq 0$, and $u \in \mathbb{Z}_p$.

Lemma

Let $A \subset \mathbb{Z}_p^d$ and $|A| = \delta p^d$. Then there exists a hyperplane $L \subset \mathbb{Z}_p^d$ such that

$$|A \cap L| = p^{d-1}(\delta + \theta \delta^{1/2} p^{-(d-1)/2}),$$

where $|\theta| \leqslant 1$.

Proof. Let us choose a hyperplane (that is, a pair $(\eta, u) \in \mathbb{Z}_p^d \times \mathbb{Z}_p$) uniformly at random and consider the random variable

$$\xi = |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u)$$

Let $a = (a_1, ..., a_d), b = (b_1, ..., b_d) \in \mathbb{Z}_p^d$. Define

$$ab = (a, b) = a_1 b_1 + ... + a_d b_d \in \mathbb{Z}_p.$$

Define a hyperplane $L \subseteq \mathbb{Z}_p^d$ to be any set of the form

$$L = L_{\eta,u} = \{x \in \mathbb{Z}_p^d : x\eta = u\},$$

where $\eta \in \mathbb{Z}_p^d$, $\eta \neq 0$, and $u \in \mathbb{Z}_p$.

Lemma

Let $A \subset \mathbb{Z}_p^d$ and $|A| = \delta p^d$. Then there exists a hyperplane $L \subset \mathbb{Z}_p^d$ such that

$$|A \cap L| = p^{d-1}(\delta + \theta\delta^{1/2} p^{-(d-1)/2}),$$

where $|\theta| \leqslant 1$.

Proof. Let us choose a hyperplane (that is, a pair $(\eta, u) \in \mathbb{Z}_p^d \times \mathbb{Z}_p$) uniformly at random and consider the random variable

$$\xi = |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u)$$

Let $a = (a_1, ..., a_d), b = (b_1, ..., b_d) \in \mathbb{Z}_p^d$. Define

$$ab = (a, b) = a_1 b_1 + ... + a_d b_d \in \mathbb{Z}_p.$$

Define a hyperplane $L \subseteq \mathbb{Z}_p^d$ to be any set of the form

$$L = L_{\eta,u} = \{x \in \mathbb{Z}_p^d : x\eta = u\},$$

where $\eta \in \mathbb{Z}_p^d$, $\eta \neq 0$, and $u \in \mathbb{Z}_p$.

Lemma

Let $A \subset \mathbb{Z}_p^d$ and $|A| = \delta p^d$. Then there exists a hyperplane $L \subset \mathbb{Z}_p^d$ such that

$$|A \cap L| = p^{d-1}(\delta + \theta\delta^{1/2} p^{-(d-1)/2}),$$

where $|\theta| \leqslant 1$.

Proof. Let us choose a hyperplane (that is, a pair $(\eta, u) \in \mathbb{Z}_p^d \times \mathbb{Z}_p$) uniformly at random and consider the random variable

$$\xi = |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u)$$

Example 14: Good intersection with a hyperplane

Let $r = p^d - 1$. Then

$$\mathbb{E}\xi = \frac{1}{rp} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u) =$$

$$\frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} 1(x\eta = u) = \frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} 1 = \frac{|A|}{p}$$

It is not hard to prove that

$$\operatorname{Var} \xi < \delta p^{d-1}.$$

Then for some $\lambda > 1$

$$\sigma = \operatorname{Var}^{1/2} \xi = \frac{\delta p^{d-1}}{\lambda}$$

Thus by Chebyshev's inequality

$$\mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \delta^{1/2} p^{(d-1)/2}) = \mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \lambda\sigma) \leqslant \frac{1}{\lambda^2} < 1,$$

and hence there exists a hyperplane $L_{\eta,u}$ such that

$$\xi = |A \cap L_{\eta,u}| = \delta p^{d-1} + \theta \delta^{1/2} p^{(d-1)/2}$$

for some $\theta < 1$. The claims follows.

Example 14: Good intersection with a hyperplane

Let $r = p^d - 1$. Then

$$\mathbb{E}\xi = \frac{1}{rp} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u) =$$

$$\frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} 1(x\eta = u) = \frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} 1 = \frac{|A|}{p}$$

It is not hard to prove that

$$\operatorname{Var}\xi < \delta p^{d-1}.$$

Then for some $\lambda > 1$

$$\sigma = \operatorname{Var}^{1/2}\xi = \frac{\delta p^{d-1}}{\lambda}$$

Thus by Chebyshev's inequality

$$\mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \delta^{1/2} p^{(d-1)/2}) = \mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \lambda\sigma) \leqslant \frac{1}{\lambda^2} < 1,$$

and hence there exists a hyperplane $L_{\eta,u}$ such that

$$\xi = |A \cap L_{\eta,u}| = \delta p^{d-1} + \theta\delta^{1/2} p^{(d-1)/2}$$

for some $\theta < 1$. The claims follows.

Let $r = p^d - 1$. Then

$$\mathbb{E}\xi = \frac{1}{rp} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u) =$$

$$\frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} 1(x\eta = u) = \frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} 1 = \frac{|A|}{p}$$

It is not hard to prove that

$$\operatorname{Var} \xi < \delta p^{d-1}.$$

Then for some $\lambda > 1$

$$\sigma = \operatorname{Var}^{1/2} \xi = \frac{\delta p^{d-1}}{\lambda}$$

Thus by Chebyshev's inequality

$$\mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \delta^{1/2} p^{(d-1)/2}) = \mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \lambda\sigma) \leqslant \frac{1}{\lambda^2} < 1,$$

and hence there exists a hyperplane $L_{\eta,u}$ such that

$$\xi = |A \cap L_{\eta,u}| = \delta p^{d-1} + \theta \delta^{1/2} p^{(d-1)/2}$$

for some $\theta < 1$. The claims follows.

Example 14: Good intersection with a hyperplane

Let $r = p^d - 1$. Then

$$\mathbb{E}\xi = \frac{1}{rp} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u) =$$

$$\frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} 1(x\eta = u) = \frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} 1 = \frac{|A|}{p}$$

It is not hard to prove that

$$\operatorname{Var} \xi < \delta p^{d-1}.$$

Then for some $\lambda > 1$

$$\sigma = \operatorname{Var}^{1/2} \xi = \frac{\delta p^{d-1}}{\lambda}$$

Thus by Chebyshev's inequality

$$\mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \delta^{1/2} p^{(d-1)/2}) = \mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \lambda\sigma) \leqslant \frac{1}{\lambda^2} < 1,$$

and hence there exists a hyperplane $L_{\eta,u}$ such that

$$\xi = |A \cap L_{\eta,u}| = \delta p^{d-1} + \theta \delta^{1/2} p^{(d-1)/2}$$

for some $\theta < 1$. The claims follows.

Let $r = p^d - 1$. Then

$$\mathbb{E}\xi = \frac{1}{rp} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} |A \cap L_{\eta,u}| = \sum_{x \in A} 1(x\eta = u) =$$

$$\frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} \sum_{u \in \mathbb{Z}_p} 1(x\eta = u) = \frac{1}{rp} \sum_{x \in A} \sum_{\eta \in \mathbb{Z}_p^d \setminus \{0\}} 1 = \frac{|A|}{p}$$

It is not hard to prove that

$$\operatorname{Var} \xi < \delta p^{d-1}.$$

Then for some $\lambda > 1$

$$\sigma = \operatorname{Var}^{1/2} \xi = \frac{\delta p^{d-1}}{\lambda}$$

Thus by Chebyshev's inequality

$$\mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \delta^{1/2} p^{(d-1)/2}) = \mathbb{P}(|\xi - \mathbb{E}\xi| \geqslant \lambda\sigma) \leqslant \frac{1}{\lambda^2} < 1,$$

and hence there exists a hyperplane $L_{\eta,u}$ such that

$$\xi = |A \cap L_{\eta,u}| = \delta p^{d-1} + \theta \delta^{1/2} p^{(d-1)/2}$$

for some $\theta < 1$. The claims follows.

Consider again random complete directed subgraph (tournament) $G = (V, E)$ with $|V| = N = 10^7$.

For a vertex $v \in V$ set $d_v := \#\{u \in V : (v, u) \in E\}$ (scores of a). Fix v and consider the random variable

$$X_v = d_v - (N - 1 - d_v) = 2d_v - N + 1$$

(the number of wins minus the number of losses). Then $d_v = \frac{1}{2}(N - 1 + X_v)$. Note that

$$X = \sum_{u \neq v} \varepsilon_u,$$

where $\mathbb{P}(\varepsilon_u = 1) = \mathbb{P}(\varepsilon_u = -1) = 1/2$ and ε_u are jointly independent. Then

$$\mathbb{E}X_v = 0$$

and

$$\mathrm{Var}\, X_v = \sum_{u \neq v} \mathrm{Var}\, \varepsilon_u = N - 1.$$

Also for this case we have a great improvement of Chebyshev's inequality

Theorem (Chernoff's inequality)

Suppose that random variables $X_1, ..., X_n$ are jointly independent such that $\mathbb{E}X_i = 0$ and $|\mathbb{E}X_i| \leqslant 1$. Define $X = X_1 + ... + X_n$ and $\sigma := \mathrm{Var}^{1/2} X$. Then for any $\lambda \geqslant 0$

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda\sigma\right) \leqslant 2 \max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

Consider again random complete directed subgraph (tournament) $G = (V, E)$ with $|V| = N = 10^7$.

For a vertex $v \in V$ set $d_v := \#\{u \in V : (v, u) \in E\}$ (scores of a). Fix v and consider the random variable

$$X_v = d_v - (N - 1 - d_v) = 2d_v - N + 1$$

(the number of wins minus the number of losses). Then $d_v = \frac{1}{2}(N - 1 + X_v)$. Note that

$$X = \sum_{u \neq v} \varepsilon_u,$$

where $\mathbb{P}(\varepsilon_u = 1) = \mathbb{P}(\varepsilon_u = -1) = 1/2$ and ε_u are jointly independent. Then

$$\mathbb{E}X_v = 0$$

and

$$\operatorname{Var} X_v = \sum_{u \neq v} \operatorname{Var} \varepsilon_u = N - 1.$$

Also for this case we have a great improvement of Chebyshev's inequality

Theorem (Chernoff's inequality)

Suppose that random variables $X_1, ..., X_n$ are jointly independent such that $\mathbb{E}X_i = 0$ and $|\mathbb{E}X_i| \leqslant 1$. Define $X = X_1 + ... + X_n$ and $\sigma := \operatorname{Var}^{1/2} X$. Then for any $\lambda \geqslant 0$

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda\sigma\right) \leqslant 2 \max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

Consider again random complete directed subgraph (tournament) $G = (V, E)$ with $|V| = N = 10^7$.

For a vertex $v \in V$ set $d_v := \#\{u \in V : (v, u) \in E\}$ (scores of a). Fix v and consider the random variable

$$X_v = d_v - (N - 1 - d_v) = 2d_v - N + 1$$

(the number of wins minus the number of losses). Then $d_v = \frac{1}{2}(N - 1 + X_v)$. Note that

$$X = \sum_{u \neq v} \varepsilon_u,$$

where $\mathbb{P}(\varepsilon_u = 1) = \mathbb{P}(\varepsilon_u = -1) = 1/2$ and ε_u are jointly independent. Then

$$\mathbb{E}X_v = 0$$

and

$$\operatorname{Var} X_v = \sum_{u \neq v} \operatorname{Var} \varepsilon_u = N - 1.$$

Also for this case we have a great improvement of Chebyshev's inequality

Theorem (Chernoff's inequality)

Suppose that random variables $X_1, ..., X_n$ are jointly independent such that $\mathbb{E}X_i = 0$ and $|\mathbb{E}X_i| \leqslant 1$. Define $X = X_1 + ... + X_n$ and $\sigma := \operatorname{Var}^{1/2} X$. Then for any $\lambda \geqslant 0$

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda\sigma\right) \leqslant 2\max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

Consider again random complete directed subgraph (tournament) $G = (V, E)$ with $|V| = N = 10^7$.

For a vertex $v \in V$ set $d_v := \#\{u \in V : (v, u) \in E\}$ (scores of a). Fix v and consider the random variable

$$X_v = d_v - (N - 1 - d_v) = 2d_v - N + 1$$

(the number of wins minus the number of losses). Then $d_v = \frac{1}{2}(N - 1 + X_v)$. Note that

$$X = \sum_{u \neq v} \varepsilon_u,$$

where $\mathbb{P}(\varepsilon_u = 1) = \mathbb{P}(\varepsilon_u = -1) = 1/2$ and ε_u are jointly independent. Then

$$\mathbb{E}X_v = 0$$

and

$$\operatorname{Var} X_v = \sum_{u \neq v} \operatorname{Var} \varepsilon_u = N - 1.$$

Also for this case we have a great improvement of Chebyshev's inequality

Theorem (Chernoff's inequality)

Suppose that random variables $X_1, ..., X_n$ are jointly independent such that $\mathbb{E}X_i = 0$ and $|\mathbb{E}X_i| \leqslant 1$. Define $X = X_1 + ... + X_n$ and $\sigma := \operatorname{Var}^{1/2} X$. Then for any $\lambda \geqslant 0$

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda\sigma\right) \leqslant 2\max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

Example 15: The exponential moment method

Consider again random complete directed subgraph (tournament) $G = (V, E)$ with $|V| = N = 10^7$.

For a vertex $v \in V$ set $d_v := \#\{u \in V : (v, u) \in E\}$ (scores of a). Fix v and consider the random variable

$$X_v = d_v - (N - 1 - d_v) = 2d_v - N + 1$$

(the number of wins minus the number of losses). Then $d_v = \frac{1}{2}(N - 1 + X_v)$. Note that

$$X = \sum_{u \neq v} \varepsilon_u,$$

where $\mathbb{P}(\varepsilon_u = 1) = \mathbb{P}(\varepsilon_u = -1) = 1/2$ and ε_u are jointly independent. Then

$$\mathbb{E}X_v = 0$$

and

$$\operatorname{Var} X_v = \sum_{u \neq v} \operatorname{Var} \varepsilon_u = N - 1.$$

Also for this case we have a great improvement of Chebyshev's inequality

Theorem (Chernoff's inequality)

Suppose that random variables $X_1, \ldots, X_n$ are jointly independent such that $\mathbb{E}X_i = 0$ and $|\mathbb{E}X_i| \leqslant 1$. Define $X = X_1 + \ldots + X_n$ and $\sigma := \operatorname{Var}^{1/2} X$. Then for any $\lambda \geqslant 0$

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda\sigma\right) \leqslant 2\max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

Consider again random complete directed subgraph (tournament) $G = (V, E)$ with $|V| = N = 10^7$.

For a vertex $v \in V$ set $d_v := \#\{u \in V : (v, u) \in E\}$ (scores of a). Fix v and consider the random variable

$$X_v = d_v - (N - 1 - d_v) = 2d_v - N + 1$$

(the number of wins minus the number of losses). Then $d_v = \frac{1}{2}(N - 1 + X_v)$. Note that

$$X = \sum_{u \neq v} \varepsilon_u,$$

where $\mathbb{P}(\varepsilon_u = 1) = \mathbb{P}(\varepsilon_u = -1) = 1/2$ and ε_u are jointly independent. Then

$$\mathbb{E}X_v = 0$$

and

$$\operatorname{Var} X_v = \sum_{u \neq v} \operatorname{Var} \varepsilon_u = N - 1.$$

Also for this case we have a great improvement of Chebyshev's inequality

Theorem (Chernoff's inequality)

Suppose that random variables $X_1, ..., X_n$ are jointly independent such that $\mathbb{E}X_i = 0$ and $|\mathbb{E}X_i| \leqslant 1$. Define $X = X_1 + ... + X_n$ and $\sigma := \operatorname{Var}^{1/2} X$. Then for any $\lambda \geqslant 0$

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda\sigma\right) \leqslant 2 \max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

Consider again random complete directed subgraph (tournament) $G = (V, E)$ with $|V| = N = 10^7$.

For a vertex $v \in V$ set $d_v := \#\{u \in V : (v, u) \in E\}$ (scores of a). Fix v and consider the random variable

$$X_v = d_v - (N - 1 - d_v) = 2d_v - N + 1$$

(the number of wins minus the number of losses). Then $d_v = \frac{1}{2}(N - 1 + X_v)$. Note that

$$X = \sum_{u \neq v} \varepsilon_u,$$

where $\mathbb{P}(\varepsilon_u = 1) = \mathbb{P}(\varepsilon_u = -1) = 1/2$ and ε_u are jointly independent. Then

$$\mathbb{E}X_v = 0$$

and

$$\operatorname{Var} X_v = \sum_{u \neq v} \operatorname{Var} \varepsilon_u = N - 1.$$

Also for this case we have a great improvement of Chebyshev's inequality

Theorem (Chernoff's inequality)

Suppose that random variables $X_1, ..., X_n$ are jointly independent such that $\mathbb{E}X_i = 0$ and $|\mathbb{E}X_i| \leqslant 1$. Define $X = X_1 + ... + X_n$ and $\sigma := \operatorname{Var}^{1/2} X$. Then for any $\lambda \geqslant 0$

$$\mathbb{P}\left(|X - \mathbb{E}X| \geqslant \lambda\sigma\right) \leqslant 2 \max\left(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}\right).$$

In our case we have (say)

$$\mathbb{P}\left(|X_v| \geqslant 20(N\log N)^{1/2}\right) \leqslant 2e^{-100\log N} = 2N^{-100}.$$

So $|X_v| \leqslant 20(N\log N)^{1/2}$ with extremely high probability $1 - 2N^{-100}$.

Recall $d_v = \frac{1}{2}(N - 1 + X_v)$; then

$$\mathbb{E}d_v = \frac{N-1}{2}$$

and it follows that

$$\mathbb{P}\left(|d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-100}$$

and

$$\mathbb{P}\left(\exists v : |d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-99}$$

So in a random tournament all players are almost equal with extremely high probability.

It is not the real life.

In our case we have (say)

$$\mathbb{P}\left(|X_v| \geqslant 20(N\log N)^{1/2}\right) \leqslant 2e^{-100\log N} = 2N^{-100}.$$

So $|X_v| \leqslant 20(N\log N)^{1/2}$ with extremely high probability $1-2N^{-100}$.

Recall $d_v = \frac{1}{2}(N-1+X_v)$; then

$$\mathbb{E}d_v = \frac{N-1}{2}$$

and it follows that

$$\mathbb{P}\left(|d_v-(N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-100}$$

and

$$\mathbb{P}\left(\exists v : |d_v-(N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-99}$$

So in a random tournament all players are almost equal with extremely high probability.

It is not the real life.

In our case we have (say)

$$\mathbb{P}\left(|X_v| \geqslant 20(N\log N)^{1/2}\right) \leqslant 2e^{-100\log N} = 2N^{-100}.$$

So $|X_v| \leqslant 20(N\log N)^{1/2}$ with extremely high probability $1-2N^{-100}$.

Recall $d_v = \frac{1}{2}(N-1+X_v)$; then

$$\mathbb{E}d_v = \frac{N-1}{2}$$

and it follows that

$$\mathbb{P}\left(|d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-100}$$

and

$$\mathbb{P}\left(\exists v : |d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-99}$$

So in a random tournament all players are almost equal with extremely high probability.

It is not the real life.

In our case we have (say)

$$\mathbb{P}\left(|X_v| \geqslant 20(N\log N)^{1/2}\right) \leqslant 2e^{-100\log N} = 2N^{-100}.$$

So $|X_v| \leqslant 20(N\log N)^{1/2}$ with extremely high probability $1-2N^{-100}$.

Recall $d_v = \frac{1}{2}(N-1+X_v)$; then

$$\mathbb{E}d_v = \frac{N-1}{2}$$

and it follows that

$$\mathbb{P}\left(|d_v-(N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-100}$$

and

$$\mathbb{P}\left(\exists v : |d_v-(N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-99}$$

So in a random tournament all players are almost equal with extremely high probability.

It is not the real life.

In our case we have (say)

$$\mathbb{P}\left(|X_v| \geqslant 20(N\log N)^{1/2}\right) \leqslant 2e^{-100\log N} = 2N^{-100}.$$

So $|X_v| \leqslant 20(N\log N)^{1/2}$ with extremely high probability $1 - 2N^{-100}$.

Recall $d_v = \frac{1}{2}(N - 1 + X_v)$; then

$$\mathbb{E}d_v = \frac{N-1}{2}$$

and it follows that

$$\mathbb{P}\left(|d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-100}$$

and

$$\mathbb{P}\left(\exists v : |d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-99}$$

So in a random tournament all players are almost equal with extremely high probability.

It is not the real life.

In our case we have (say)

$$\mathbb{P}\left(|X_v| \geqslant 20(N\log N)^{1/2}\right) \leqslant 2e^{-100\log N} = 2N^{-100}.$$

So $|X_v| \leqslant 20(N\log N)^{1/2}$ with extremely high probability $1 - 2N^{-100}$.

Recall $d_v = \frac{1}{2}(N-1+X_v)$; then

$$\mathbb{E}d_v = \frac{N-1}{2}$$

and it follows that

$$\mathbb{P}\left(|d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-100}$$

and

$$\mathbb{P}\left(\exists v : |d_v - (N-1)/2| > 20(N\log N)^{1/2}\right) \leqslant 2N^{-99}$$

So in a random tournament all players are almost equal with extremely high probability.

It is not the real life.

Consider the function $f\colon [0,1] \to \mathbb{R}$,

$$f(x) = \begin{cases} 1000, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Suppose we do not know what f is but want to prove that it has large values. Suppose we can compute

$$\mathbb{E}f = \int_0^1 f(x)dx = 10.$$

Then by the first moment method we get that there exists x such that $f(x) \geqslant 10$. Not so impressive, right?

How to fix this?

Consider the function $f\colon [0,1] \to \mathbb{R}$,

$$f(x) = \begin{cases} 1000, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Suppose we do not know what f is but want to prove that it has large values. Suppose we can compute

$$\mathbb{E}f = \int_0^1 f(x)dx = 10.$$

Then by the first moment method we get that there exists x such that $f(x) \geqslant 10$. Not so impressive, right?

How to fix this?

Again the first moment method: a problem

Consider the function $f\colon [0,1] \to \mathbb{R}$,

$$f(x) = \begin{cases} 1000, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Suppose we do not know what f is but want to prove that it has large values. Suppose we can compute

$$\mathbb{E}f = \int_0^1 f(x)dx = 10.$$

Then by the first moment method we get that there exists x such that $f(x) \geqslant 10$. Not so impressive, right?

How to fix this?

Consider the function $f\colon [0,1] \to \mathbb{R}$,

$$f(x) = \begin{cases} 1000, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Suppose we do not know what f is but want to prove that it has large values. Suppose we can compute

$$\mathbb{E}f = \int_0^1 f(x)dx = 10.$$

Then by the first moment method we get that there exists x such that $f(x) \geqslant 10$. Not so impressive, right?

How to fix this?

Let $g(x)$ be any non-negative function on $[0, 1]$ such that $\int_0^1 g(x)dx = 1$ and define

$$\mathbb{E}f = \int_0^1 f(x)g(x)dx.$$

Then

$$\int_0^1 (f(x) - \mathbb{E}f)\, g(x)dx = \int_0^1 f(x)g(x)dx - \mathbb{E}f = 0$$

and hence there exists x with $f(x) \geqslant \mathbb{E}f$. We are not forced to take $g(x) \equiv 1$ at all!

Let $g(x)$ be any non-negative function on $[0,1]$ such that $\int_0^1 g(x)dx = 1$ and define

$$\mathbb{E}f = \int_0^1 f(x)g(x)dx.$$

Then

$$\int_0^1 (f(x) - \mathbb{E}f)\, g(x)dx = \int_0^1 f(x)g(x)dx - \mathbb{E}f = 0$$

and hence there exists x with $f(x) \geqslant \mathbb{E}f$. We are not forced to take $g(x) \equiv 1$ at all!

Let $g(x)$ be any non-negative function on $[0,1]$ such that $\int_0^1 g(x)dx = 1$ and define

$$\mathbb{E}f = \int_0^1 f(x)g(x)dx.$$

Then

$$\int_0^1 (f(x) - \mathbb{E}f)\, g(x)dx = \int_0^1 f(x)g(x)dx - \mathbb{E}f = 0$$

and hence there exists x with $f(x) \geqslant \mathbb{E}f$. We are not forced to take $g(x) \equiv 1$ at all!

Let $g(x)$ be any non-negative function on $[0,1]$ such that $\int_0^1 g(x)dx = 1$ and define

$$\mathbb{E}f = \int_0^1 f(x)g(x)dx.$$

Then

$$\int_0^1 (f(x) - \mathbb{E}f)\, g(x)dx = \int_0^1 f(x)g(x)dx - \mathbb{E}f = 0$$

and hence there exists x with $f(x) \geqslant \mathbb{E}f$. We are not forced to take $g(x) \equiv 1$ at all!

Let f be as above and

$$g(x) = \begin{cases} 2, & \text{if } 0 \leqslant x \leqslant 1/2; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\mathbb{E}f = 20$ and hence $\max f(x) \geqslant 20$.

Ok, let

$$g(x) = \begin{cases} 10, & \text{if } 0 \leqslant x \leqslant 1/10; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 100$.

Finally, let

$$g(x) = \begin{cases} 100, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 1000$ and it is the best possible.

The moral 1: our measure needs to be concentrated on the set of large values of f.

The moral 2: we need to have a good guess for what this set is!

Let f be as above and

$$g(x) = \begin{cases} 2, & \text{if } 0 \leqslant x \leqslant 1/2; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\mathbb{E}f = 20$ and hence $\max f(x) \geqslant 20$.

Ok, let

$$g(x) = \begin{cases} 10, & \text{if } 0 \leqslant x \leqslant 1/10; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 100$.

Finally, let

$$g(x) = \begin{cases} 100, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 1000$ and it is the best possible.

The moral 1: our measure needs to be concentrated on the set of large values of f.

The moral 2: we need to have a good guess for what this set is!

Let f be as above and

$$g(x) = \begin{cases} 2, & \text{if } 0 \leqslant x \leqslant 1/2; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\mathbb{E}f = 20$ and hence $\max f(x) \geqslant 20$.

Ok, let

$$g(x) = \begin{cases} 10, & \text{if } 0 \leqslant x \leqslant 1/10; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 100$.

Finally, let

$$g(x) = \begin{cases} 100, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 1000$ and it is the best possible.

The moral 1: our measure needs to be concentrated on the set of large values of f.

The moral 2: we need to have a good guess for what this set is!

Let f be as above and

$$g(x) = \begin{cases} 2, & \text{if } 0 \leqslant x \leqslant 1/2; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\mathbb{E}f = 20$ and hence $\max f(x) \geqslant 20$.

Ok, let

$$g(x) = \begin{cases} 10, & \text{if } 0 \leqslant x \leqslant 1/10; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 100$.

Finally, let

$$g(x) = \begin{cases} 100, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E}f = 1000$ and it is the best possible.

The moral 1: our measure needs to be concentrated on the set of large values of f.

The moral 2: we need to have a good guess for what this set is!

Let f be as above and

$$g(x) = \begin{cases} 2, & \text{if } 0 \leqslant x \leqslant 1/2; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\mathbb{E} f = 20$ and hence $\max f(x) \geqslant 20$.

Ok, let

$$g(x) = \begin{cases} 10, & \text{if } 0 \leqslant x \leqslant 1/10; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E} f = 100$.

Finally, let

$$g(x) = \begin{cases} 100, & \text{if } 0 \leqslant x \leqslant 1/100; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\max f(x) \geqslant \mathbb{E} f = 1000$ and it is the best possible.

The moral 1: our measure needs to be concentrated on the set of large values of f.

The moral 2: we need to have a good guess for what this set is!

Suppose we want to study large values of the Riemann zeta-function $\zeta(s)$ on the critical line $s = 1/2 + it$. Here the first moment method works normally. It gives us (a result of Hardy-Littlewood)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^2 dt \sim \log T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \geqslant (1+o(1)) \log^{1/2} T, \quad T \to \infty,$$

or (a result of Ingham)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^4 dt \sim \frac{1}{2\pi^2} \log^4 T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \gg \log T.$$

But no other moment are known.

Suppose we want to study large values of the Riemann zeta-function $\zeta(s)$ on the critical line $s = 1/2 + it$. Here the first moment method works normally. It gives us (a result of Hardy-Littlewood)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^2 dt \sim \log T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \geqslant (1+o(1))\log^{1/2} T, \quad T\to\infty,$$

or (a result of Ingham)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^4 dt \sim \frac{1}{2\pi^2}\log^4 T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \gg \log T.$$

But no other moment are known.

Suppose we want to study large values of the Riemann zeta-function $\zeta(s)$ on the critical line $s = 1/2 + it$. Here the first moment method works normally. It gives us (a result of Hardy-Littlewood)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^2 dt \sim \log T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \geqslant (1+o(1)) \log^{1/2} T, \quad T \to \infty,$$

or (a result of Ingham)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^4 dt \sim \frac{1}{2\pi^2} \log^4 T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \gg \log T.$$

But no other moment are known.

Suppose we want to study large values of the Riemann zeta-function $\zeta(s)$ on the critical line $s = 1/2 + it$. Here the first moment method works normally. It gives us (a result of Hardy-Littlewood)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^2 dt \sim \log T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \geqslant (1+o(1))\log^{1/2} T, \quad T\to\infty,$$

or (a result of Ingham)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^4 dt \sim \frac{1}{2\pi^2}\log^4 T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \gg \log T.$$

But no other moment are known.

Suppose we want to study large values of the Riemann zeta-function $\zeta(s)$ on the critical line $s = 1/2 + it$. Here the first moment method works normally. It gives us (a result of Hardy-Littlewood)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^2 dt \sim \log T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \geqslant (1+o(1))\log^{1/2} T, \quad T\to\infty,$$

or (a result of Ingham)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^4 dt \sim \frac{1}{2\pi^2}\log^4 T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \gg \log T.$$

But no other moment are known.

Suppose we want to study large values of the Riemann zeta-function $\zeta(s)$ on the critical line $s = 1/2 + it$. Here the first moment method works normally. It gives us (a result of Hardy-Littlewood)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^2 dt \sim \log T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \geqslant (1+o(1)) \log^{1/2} T, \quad T \to \infty,$$

or (a result of Ingham)

$$\frac{1}{T}\int_0^T |\zeta(1/2+it)|^4 dt \sim \frac{1}{2\pi^2} \log^4 T$$

and hence

$$\max_{t\in[0,T]} |\zeta(1/2+it)| \gg \log T.$$

But no other moment are known.

Example 17: Large values of $\zeta(s)$

Fix $1/2 < \sigma < 1$. To estimate from below $\max_{T \leqslant t \leqslant 2T} |\zeta(\sigma + it)|$ people use measures $\varphi(t) = \frac{1}{J} \left| \prod_{p \leqslant x} \left(1 + \frac{l_p}{p^{it}}\right) \right|^2$ (x is a parameter), where $J = \int_T^{2T} \varphi(t) dt$.

Then using the first moment method it can be shown that there exists $c = c(\sigma) > 0$ such that

$$\zeta(\sigma + it) = \Omega\left(\exp\left(c \frac{(\log |t|)^{1-\sigma}}{\log \log |t|}\right)\right)$$

(for this we set $l_p = 1$ for all p) and

$$\zeta^{-1}(\sigma + it) = \Omega\left(\exp\left(c \frac{(\log |t|)^{1-\sigma}}{\log \log |t|}\right)\right).$$

(for this we set $l_p = -1$ for all p).

Here $F(t) = \Omega(G(t))$ means that there exist an absolute constant $C > 0$ and a sequence t_k such that $t_k \to \infty$ and

$$|F(t_k)| \geqslant CG(t_k).$$

Fix $1/2 < \sigma < 1$. To estimate from below $\max_{T \leqslant t \leqslant 2T} |\zeta(\sigma + it)|$ people use measures $\varphi(t) = \frac{1}{J} \left| \prod_{p \leqslant x} \left(1 + \frac{l_p}{p^{it}}\right) \right|^2$ (x is a parameter), where $J = \int_T^{2T} \varphi(t) dt$.

Then using the first moment method it can be shown that there exists $c = c(\sigma) > 0$ such that

$$\zeta(\sigma + it) = \Omega\left(\exp\left(c \frac{(\log |t|)^{1-\sigma}}{\log \log |t|}\right)\right)$$

(for this we set $l_p = 1$ for all p) and

$$\zeta^{-1}(\sigma + it) = \Omega\left(\exp\left(c \frac{(\log |t|)^{1-\sigma}}{\log \log |t|}\right)\right).$$

(for this we set $l_p = -1$ for all p).

Here $F(t) = \Omega(G(t))$ means that there exist an absolute constant $C > 0$ and a sequence t_k such that $t_k \to \infty$ and

$$|F(t_k)| \geqslant CG(t_k).$$

Fix $1/2 < \sigma < 1$. To estimate from below $\max_{T\leqslant t\leqslant 2T} |\zeta(\sigma+it)|$ people use measures $\varphi(t) = \frac{1}{J}\left|\prod_{p\leqslant x}\left(1+\frac{l_p}{p^{it}}\right)\right|^2$ (x is a parameter), where $J = \int_T^{2T}\varphi(t)dt$.

Then using the first moment method it can be shown that there exists $c = c(\sigma) > 0$ such that

$$\zeta(\sigma+it) = \Omega\left(\exp\left(c\frac{(\log|t|)^{1-\sigma}}{\log\log|t|}\right)\right)$$

(for this we set $l_p = 1$ for all p) and

$$\zeta^{-1}(\sigma+it) = \Omega\left(\exp\left(c\frac{(\log|t|)^{1-\sigma}}{\log\log|t|}\right)\right).$$

(for this we set $l_p = -1$ for all p).

Here $F(t) = \Omega(G(t))$ means that there exist an absolute constant $C > 0$ and a sequence t_k such that $t_k \to \infty$ and

$$|F(t_k)| \geqslant CG(t_k).$$

Fix $1/2 < \sigma < 1$. To estimate from below $\max_{T \leqslant t \leqslant 2T} |\zeta(\sigma + it)|$ people use measures $\varphi(t) = \frac{1}{J} \left| \prod_{p \leqslant x} \left(1 + \frac{l_p}{p^{it}}\right) \right|^2$ (x is a parameter), where $J = \int_T^{2T} \varphi(t) dt$.

Then using the first moment method it can be shown that there exists $c = c(\sigma) > 0$ such that

$$\zeta(\sigma + it) = \Omega\left(\exp\left(c \frac{(\log |t|)^{1-\sigma}}{\log \log |t|}\right)\right)$$

(for this we set $l_p = 1$ for all p) and

$$\zeta^{-1}(\sigma + it) = \Omega\left(\exp\left(c \frac{(\log |t|)^{1-\sigma}}{\log \log |t|}\right)\right).$$

(for this we set $l_p = -1$ for all p).

Here $F(t) = \Omega(G(t))$ means that there exist an absolute constant $C > 0$ and a sequence t_k such that $t_k \to \infty$ and

$$|F(t_k)| \geqslant CG(t_k).$$

Books

T.Tao, V.Vu, “Additive combinatorics”, Cambridge Stud. Adv. Math., Vol. 105.

N.Alon, J.H.Spencer, “The probabistic method”

MERCI BEAUCOUP POUR VOTRE ATTENTION !