A probabilistic construction and its derandomization

Mihalis Kolountzakis

University of Crete

Tripods NSF REU/GradStemForAll2020 (Rochester)
August 12, 2020

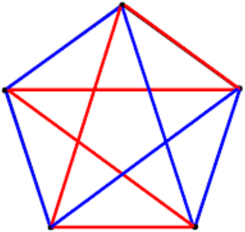
Define random object; prove that it has required properties

Works suprisingly often.

"Non-constructive"

Example: edge coloring K_n

Color the edges of K_n for few monochromatic triangles



Method: Just randomly color every edge red or blue.

EXAMPLE: EDGE COLORING K_n: ANALYSIS

Write $I_j = \mathbf{1}\,(\text{triangle } j \text{ is monochromatic})$.

Number of monochromatic triangles is then $X = \sum_{j=1}^{\binom{n}{3}} I_j$

$\mathbb{E}\left[X\right] = \sum_{j=1}^{\binom{n}{3}} \frac{1}{4} = \frac{1}{4}\binom{n}{3} = \frac{n(n-1)(n-2)}{24}$

There is a coloring with $X \leq \mathbb{E}\left[X\right]$.

How to construct such a coloring?

Method of conditional expectations:

- Toss your coins one by one.
- Take care to be on the right side of luck each time!

How to choose I_1 to be red or blue?

$$\mathbb{E}[X] = \mathbb{E}[X \mid I_1 = \text{red}] \tfrac{1}{2} + \mathbb{E}[X \mid I_1 = \text{blue}] \tfrac{1}{2}$$

so one of $\mathbb{E}[X \mid I_1 = \text{red}]$, $\mathbb{E}[X \mid I_1 = \text{blue}]$ is $\leq \mathbb{E}[X]$.

Calculate and choose that one!

The method of conditional expectations

Having chosen $I_1 = c_1, \ldots, I_k = c_k$ we have

$$\mathbb{E}[X \mid I_1 = c_1, \ldots, I_k = c_k] =$$

$$\mathbb{E}[X \mid I_1 = c_1, \ldots, I_k = c_k, I_{k+1} = \textit{red}]\,\frac{1}{2} +$$

$$\mathbb{E}[X \mid I_1 = c_1, \ldots, I_k = c_k, I_{k+1} = \textit{blue}]\,\frac{1}{2}$$

Choose the color $I_{k+1} = c_{k+1}$ so as to have

$$\mathbb{E}[X \mid I_1 = c_1, \ldots, I_k = c_k, I_{k+1} = c_{k+1}] \leq \mathbb{E}[X \mid I_1 = c_1, \ldots, I_k = c_k]$$

In the end

$$\mathbb{E}[X \mid I_1 = c_1, \ldots, I_n = c_n] \leq \mathbb{E}[X] = \frac{1}{4}\binom{n}{3}$$

Additive bases for the integers

$E \subseteq \mathbb{N} = \{1, 2, \dots\}$

Representation function:
$r_E(x) = \left|\left\{(a, b) \in E^2 : \ x = a + b, \ a \leq b\right\}\right|$
$=$ in how many ways we can write $x = e_1 + e_2$

E is Additive basis:
for $x \geq 2$ we have $r_E(x) > 0$. E.g. $E = \{1, 2, 4, 6, \dots\}$.

E is Asymptotic additive basis:
for all suffiently large $x \in \mathbb{N}$ we have $r_E(x) > 0$.

General problem:
find *thin* (asymptotic additive) bases
(small but positive $r_E(x)$)

Theorem (Erdős 1956)

There are constants $c_1, c_2 > 0$, set $E \subseteq \mathbb{N}$ and integer x_0 such that

$$c_1 \ln x \leq r_E(x) \leq c_2 \ln x, \quad (x \geq x_0).$$

Probabilistic proof.

Open problems:
(a) Can the function $\ln x$ be reduced?
(b) Can we achieve the existence of $\lim_{x\to\infty} \frac{r_E(x)}{\ln x}$?
(c) Non-probabilistic proof?

Conjecture (Erdős–Turán)

If for $E \subseteq \mathbb{N}$ we eventually have $r_E(x) > 0$ then

$$\limsup_{x\to\infty} r_E(x) = \infty.$$

$K > 0$ is a constant to be determined later.

Define the probabilities (for $x = 1, 2, \ldots$)

$$p_x = \begin{cases} K\left(\frac{\ln x}{x}\right)^{1/2} & \text{if this is in} \in [0,1] \\ 0 & \text{else} \end{cases}.$$

Define the *random set* $E \subseteq \mathbb{N}$ by taking

$$\mathbb{P}\left[x \in E\right] = p_x, \quad (x \in \mathbb{N})$$

independently for all $x \in \mathbb{N}$.

In other words, we toss a coin for each natural number.

The representation function

We show $\mathbb{P}\left[\text{our set has the required property}\right] > 0$.

Define RVs $\chi_j = \mathbf{1}\left(j \in E\right)$, for $j \in \mathbb{N}$. Independent with $\mathbb{E}\left[\chi_j\right] = p_j$.

For the representation function we have

$$r_E(x) = \sum_{j=1}^{\lfloor x/2 \rfloor} \chi_j \chi_{x-j}.$$

$r_E(x)$: sum of independent $0-1$ valued RVs.

The Chernoff large deviation inequality

$X_1, \ldots, X_N$ independent $0-1$ valued RVs and $S = X_1 + \cdots + X_N$, $\mu = \mathbb{E}[S]$. For $\epsilon > 0$ we have

$$\mathbb{P}[|S - \mu| \geq \epsilon\mu] \leq 2e^{-c_\epsilon \mu},$$

where

$$0 < c_\epsilon = \min\left\{\epsilon^2/2, -\ln\left(e^\epsilon(1+\epsilon)^{-(1+\epsilon)}\right)\right\}$$

depends only on ϵ.

Exponential dependence on μ:
due to structure of S as a sum of independent RVs.

Very easy to use for combinatorial problems. Only need to know μ.

Larger μ: better inequality
$\Rightarrow$ RVs S with large μ are easier to control.

Calculate the mean value

Let $p_j \neq 0$ for $j \geq j_0$ and $p_j = 0$ for $j < j_0$.

For x odd and large (similarly for x even):

$$
\begin{aligned}
\mathbb{E}\left[r_E(x)\right] &= \sum_{j=1}^{\lfloor x/2 \rfloor} \mathbb{E}\left[\chi_j \chi_{x-j}\right] \\
&= \sum_{j=1}^{\lfloor x/2 \rfloor} \mathbb{E}\left[\chi_j\right] \mathbb{E}\left[\chi_{x-j}\right] \quad (x \text{ odd } \Rightarrow j \neq x-j, \text{ independence}) \\
&= \sum_{j=j_0}^{\lfloor x/2 \rfloor} p_j p_{x-j} \\
&= \sum_{j=j_0}^{\lfloor x/2 \rfloor} K^2 \left(\frac{\ln j \ln(x-j)}{j(x-j)} \right)^{1/2}
\end{aligned}
$$

Calculate the mean value (continued)

$$\mathbb{E}\left[r_E(x)\right] = \sum_{j=j_0}^{\lfloor x/2 \rfloor} K^2 \left(\frac{\ln j \ln(x-j)}{j(x-j)}\right)^{1/2}$$

<u>Upper bound:</u> $\mathbb{E}\left[r_E(x)\right] \leq K^2 \ln x \sum_{j=1}^{\lfloor x/2 \rfloor} \left(\frac{1}{j(x-j)}\right)^{1/2}$

<u>Lower bound:</u> $\mathbb{E}\left[r_E(x)\right] \geq \frac{K^2}{4} \ln x \sum_{j=\sqrt{x}}^{\lfloor x/2 \rfloor} \left(\frac{1}{j(x-j)}\right)^{1/2}$

Calculate the mean value (continued)

But for $x \to \infty$:

$$\sum_{j=1}^{\lfloor x/2 \rfloor} \left(\frac{1}{j(x-j)} \right)^{1/2} = \sum_{j=1}^{\lfloor x/2 \rfloor} \frac{1}{x} \left(\frac{1}{\frac{j}{x}(1-\frac{j}{x})} \right)^{1/2} \to \int_0^{1/2} \left(\frac{1}{s(1-s)} \right)^{1/2} ds$$

(Riemann sum for $I = \int_0^{1/2} \left(\frac{1}{s(1-s)} \right)^{1/2} ds$)

Similarly $\sum_{j=\sqrt{x}}^{\lfloor x/2 \rfloor} \left(\frac{1}{j(x-j)} \right)^{1/2} \to I = \int_0^{1/2} \left(\frac{1}{s(1-s)} \right)^{1/2} ds$

So, for large x we have the right order of magnitude:

$$\frac{IK^2}{8} \ln x \leq \quad \mathbb{E}\left[r_E(x) \right] \quad \leq 2IK^2 \ln x.$$

Control the deviation of the RVs

Bad events: $A_x = \{|r_E(x) - \mathbb{E}[r_E(x)]| \geq \epsilon \mathbb{E}[r_E(x)]\}$
with $\epsilon = \frac{1}{2}$.

By Chernoff's inequality:

$$\begin{aligned}
\mathbb{P}[A_x] &\leq 2e^{-c_\epsilon \mathbb{E}[r_E(x)]} \\
&\leq 2e^{-c_\epsilon C_1 \ln x} \\
&= 2x^{-C_1 c_\epsilon} \\
&= 2x^{-c_\epsilon l K^2/8}.
\end{aligned}$$

Choose K so that the exponent $c_\epsilon l K^2/8 > 1$. It follows that

$$\sum_{x=1}^{\infty} \mathbb{P}[A_x] \leq \sum_{x=1}^{\infty} 2x^{-c_\epsilon l K^2/8} < \infty.$$

Convergence of $\sum_x \mathbb{P}[A_x] \Rightarrow$ there is x_0 such that

$$\sum_{x \geq x_0} \mathbb{P}[A_x] < \frac{1}{2},$$

so that with probability $\geq 1/2$ none of the $A_x, x \geq x_0$ holds.

For $x \geq x_0$:

$$r_E(x) \geq \frac{1}{2}\mathbb{E}[r_E(x)] \geq \frac{IK^2}{16} \ln x$$

and

$$r_E(x) \leq \frac{3}{2}\mathbb{E}[r_E(x)] \leq 3IK^2 \ln x.$$

How to derandomize?

Can we produce a good additive basis E by listing its elements one by one?

Not clear we can do so, however slowly.

Tricky point:
our choice for $n \in E$ affects the representation function forever.

For $g(x) = (x \log x)^{1/2}$ define the *modified representation function*

$$r'(x) = |\{(a,b) \in E^2 \; : \; x = a + b \;\; \& \;\; g(x) \le a \le b\}|.$$

Deciding $n \in E$ only affects

$$r'(x) \text{ for } x \le G(n),$$

where

$$G(n) = g^{-1}(n) \sim \frac{n^2}{\log n}.$$

A MODIFIED PROBABILISTIC PROOF, CONTINUED

Also observe that

$$r'(x) \leq r(x) \leq r'(x) + s(x),$$

where

$$s(x) = |E \cap [x - g(x), x]|.$$

One can (as in Erdős' proof) calculate easily

$$\mathbb{E}\left[r'(x)\right] \sim CK^2 \log x$$

and

$$\mathbb{E}\left[s(x)\right] \sim K \log x,$$

and the expectations of the r.v.'s $r(x)$ and $s(x)$ have the right order of magnitude.

A modified probabilistic proof, continued

The *bad events* are

$$A_x = \left\{ |r'(x) - \mathbb{E}\left[r'(x)\right]| > \frac{1}{2}\mathbb{E}\left[r'(x)\right] \right\}$$

$$B_x = \left\{ s(x) - \mathbb{E}\left[s(x)\right] > \frac{1}{2}\mathbb{E}\left[s(x)\right] \right\}.$$

Chernoff Large Deviation Lemma gives

$$\mathbb{P}\left[A_x\right] \leq 2x^{-\alpha}$$

and

$$\mathbb{P}\left[B_x\right] \leq 2x^{-\beta}.$$

Can make $\alpha, \beta > 1$ by choosing K large.

A modified probabilistic proof, continued

We have

$$\sum_{x=n_0}^{\infty} \mathbb{P}[A_x] + \mathbb{P}[B_x] < 1 \quad \text{for some } n_0.$$

We get a set E with

$$\frac{1}{2}\mathbb{E}\left[r'(x)\right] \leq r'(x) \leq \frac{3}{2}\mathbb{E}\left[r'(x)\right]$$

and

$$s(x) \leq \frac{3}{2}\mathbb{E}[s(x)].$$

Together these imply

$$C_1 \log x \leq r(x) \leq C_2 \log x$$

for $x \geq n_0$.

This concludes the alternative probabilistic proof of Erdős' theorem.

Derandomizing the proof. The strategy.

We showed that for some $n_0 \in \mathbb{N}$ the complement of the bad event

$$B = \bigcup_{x \geq n_0} (A_x \cup B_x)$$

has positive probability, since

$$\sum_{x \geq n_0} \mathbb{P}[A_x] + \mathbb{P}[B_x] < 1.$$

Have to construct a "point" (set of integers) $E \notin B$.

At the n-th step we output 1 or 0 to denote $n \in E$ or not.

Will take time *polynomial* in n to enumerate to n.

Derandomizing the proof. Restriction event.

Let the RVs $\chi_j = \mathbf{1}(j \in E)$.

Restriction event: $R(a_1, \ldots, a_n) = \{\chi_1 = a_1, \ldots, \chi_n = a_n\}$.

Goal: Pick the a_n successively so that

$$b(a_1, \ldots, a_n) := \sum_{x \geq n_0} \mathbb{P}\left[A_x \mid R(a_1, \ldots, a_n)\right] + \mathbb{P}\left[B_x \mid R(a_1, \ldots, a_n)\right]$$

is non-increasing.

If so then

$$E = (a_1, a_2, \ldots)$$

is in no bad event.

Derandomizing the proof. Deciding the next $n \in E$.

If $p_n = \mathbb{P}[n \in E]$ in our probabilistic proof then

$$b(a_1, \ldots, a_{n-1}) = p_n b(a_1, \ldots, a_{n-1}, 1) + (1 - p_n) b(a_1, \ldots, a_{n-1}, 0)$$

by the law of total probability.

Hence one of $b(a_1, \ldots, a_{n-1}, 1), b(a_1, \ldots, a_{n-1}, 0)$ is

$$\leq b(a_1, \ldots, a_{n-1}).$$

How to find which?

Derandomizing the proof. Deciding if $n \in E$.

We have to compute efficiently the sign of

$$\begin{aligned}\Delta &= b(a_1, \ldots, a_{n-1}, 1) - b(a_1, \ldots, a_{n-1}, 0) \\ &= \sum_{x=n}^{G(n)} \mathbb{P}\left[A_x \mid R(a_1, \ldots, a_{n-1}, 1)\right] - \mathbb{P}\left[A_x \mid R(a_1, \ldots, a_{n-1}, 0)\right] + \\ &\quad + \mathbb{P}\left[B_x \mid R(a_1, \ldots, a_{n-1}, 1)\right] - \mathbb{P}\left[B_x \mid R(a_1, \ldots, a_{n-1}, 0)\right].\end{aligned}$$

Thanks to the modified representation function (remember $G(n) = g^{-1}(n) \sim \frac{n^2}{\log n}$)

$$r'(x) = |\{(a, b) \in E^2 \ : \ x = a + b \ \ \& \ \ g(x) \leq a \leq b\}|.$$

this is a finite sum with a polynomial number of terms.

The end

Thanks for your attention.