Lecture 4. Linearity of expectation; Derandomization.

Crossing lemma is not well-known in a long time, until 1997 when László Székely surprisingly applied it to some geometric problems

Applications of crossing lemma.

Incidence geometry. $I(P, L) = |\{(p, \ell) \in P \times L : p \in \ell\}|$. ($P$: points, L: lines.)

Example: $P = [k] \times [2k^2]$. $L = \{y = mx + b : m \in [k], b \in [k^2]\}$

Each line contains k points. Taking $n = k^3$. $I(P, L) = n^{4/3}$

Can we do better? Trivial bound $I(P, L) \le |P||L|$

Easy bound: every pair of points determine at most 1 line.

$$I(P,L)^2 = \left(\sum_{\ell \in L} \sum_{p \in P} [p \in \ell]\right)^2 \le |L| \cdot \sum_{\ell \in L} \left(\sum_{p \in P} [p \in \ell]\right)^2 \quad \text{Cauchy-Schwarz}$$

$$= |L| \cdot \sum_{p_1 p_2 \in P} \sum_{\ell \in L} [p_1 \in \ell] \cdot [p_2 \in \ell] \quad \text{if } p_1 \neq p_2 \ \exists \text{ unique } \ell.$$

$$\le |L| \left(I(P, L) + |P|\right) \quad \le |L| \left(|L| + 2|P|^2\right).$$

$$\Rightarrow I(P, L) \lesssim |P||L|^{1/2} + |L| \quad I(P, L) \lesssim |L||P|^{1/2} + |P|. \quad n^{3/2}.$$

Now applying crossing lemma. Construct a graph $G = (V, E)$.

$V = P$. $E = \{(p_1, p_2) : \exists \ell \in L, p_1, p_2 \in \ell$. and no points between them$\}$

$$|E| = \sum_{\ell \in L} |P \cap \ell| - 1 \quad \ge \frac{1}{2} \left(I(P, L) - |L|\right). \quad cr(G) \le |L|^2$$

So $|L|^2 \geq cr(G) \gtrsim \frac{|E|^3}{|V|^2} \gtrsim \frac{I(P,L)^3}{|P|^2}$ if $I(P,L) \geq 8|P|$.

Theorem (Szemerédi-Trotter, 1983) proof by Székely, 1997.

$I(P,L) \lesssim |P|^{2/3}|L|^{2/3} + |P| + |L|$ ($n^{4/3}$ if $|P| = |L| \approx n$).

Unit distance problem. $O(n)$ for $\sqrt{n} \times \sqrt{n}$ grid.

Conjecture (Erdős 1946). For any n points. # of unit dist $\leq n^{1+o(1)}$

Progress: Erdős $O(n^{1.5})$. Józsa-Szemerédi 1973 $o(n^{1.5})$.

Beck-Spencer. 1984. $O(n^{1.444})$ Spencer-Szemerédi-Trotter, 1984. $O(n^{4/3})$.

Proof (by Székely, 1997). For each point p. if ≥ 2 points have unit distance to p. draw a unit circle centred at p. Also, for any pair of (p,q). if ≥ 1 arcs between them, only keep one. Now we have a drawing of a graph with n vertices and m edges. where $m \geq (\#\text{unit dist} - n)/2$. Since any two circles intersects at ≤ 2 points. $cr \leq 2\binom{n}{2} \Rightarrow \#ud \leq n^{4/3}$. □

Application of Szemerédi-Trotter: randomness extractor.

Suppose we have some inputs from a distribution over a set S of size 2^n. Hope to extract n random bits. $Ext: \{0,1\}^m \to \{0,1\}^n$.

Adversary: S is unknown. so even extracting one bit is impossible.

Example: rand8() → rand7(). rejection sampling?

$7^{16} < 8^{15}$. 15 bits rand8() → 16 bits rand7().

However. suppose the joint sampler is broken. Only produce $\frac{1}{2}$ results.

Two solutions: seeded extractor or seedless multisource extractor.

Seedless: get inputs from several independent sources.

Theorem (Benny Chor & Oded Goldreich, 1988). 2-sources.

Let $\bar{F}(x,y) = (-1)^{\langle x,y\rangle}$. Then $\forall S.T \subseteq \{0,1\}^n$. we have.

$$\left|\mathbb{E}_{x\sim S, y\sim T}\left[\bar{F}(x,y)\right]\right| \le \sqrt{\frac{2^n}{|S||T|}}. \quad (\text{note that } \mathrm{dist}(\bar{F}, U_2) = \frac{|\mathbb{E}[\bar{F}]|}{2}).$$

So inner product is a (k,ε)- extractor for $k > n/2 + \log(1/\varepsilon)$.

For 2-sources, this is almost the optimal so far. Best known: $(\frac{1}{2}-\varepsilon)n$.

by Jean Bourgain, 2005 but probabilistic argument shows $k \sim \log n$.

Multi-source: BIW Theorem $(\delta n, \varepsilon)$-extractor by Szemerédi-Trotter

Theorem (Boaz Barak. Russell Impagliazzo & Avi Wigderson. 2006).

$\forall \delta > 0$, $\exists \ell = (1/\delta)^{O(1)}$ and poly-time function f. s.t. $\forall$ independent

$X_1 \ldots X_\ell$ with support size $> 2^{\delta n}$. $\mathrm{dist}(f(X_1,\ldots,X_\ell), U_n) < 2^{-\Omega(n)}$.

Theorem (Jean Bourgain, Nets Katz & Terence Tao, 2004). in $\mathbb{F}^2$

Suppose $\mathbb{F} = \mathbb{F}_p$ for prime p. Let L be n lines and P be n points.

If $\exists \delta > 0$ s.t. $p^\delta < n < p^{2-\delta}$ then $\exists \varepsilon > 0$. $I(P, L) = O(n^{\frac{3}{2}-\varepsilon})$.

Lemma. Let $\delta > 0$ and $\mathbb{F}$ be a prime field where finite-field ST holds. Suppose $A, B, C \subseteq \mathbb{F}$ of size $|\mathbb{F}|^\delta < n < |\mathbb{F}|^{1-\delta}$. Then $\exists \varepsilon > 0$ s.t. $|A + BC| > n^{1+\varepsilon}$. where $A + BC \triangleq \{a + bc : a \in A, b \in B, c \in C\}$.

Proof. Let $S(x) = |\{(a, b, c) \in A \times B \times C : a + bc = x\}|$. So.

$\sum_{x \in A+BC} S(x) = n^3$. If $|A + BC| < n^{1+\varepsilon}$ then by Cauchy-Schwarz,

$$\sum S(x)^2 \geq \frac{(\sum S(x))^2}{|A + BC|} \geq n^{5-\varepsilon}$$

Now define $T = \{x : S(x) > n^{2-2\varepsilon}\}$.

Then $n^{1-2\varepsilon} \leq |T| \leq n^{1+2\varepsilon}$. Let $R = \{(a, b, c, x) : x \in T, a + bc = x\}$.

So $|R| \geq n^{3-4\varepsilon}$. But R can be viewed as incidence set on $\mathbb{F}^2$.

Let $P = C \times T$ be points and $L = \{l_{a,b} : Y = bX + a\}$ be lines.

$|P| \leq n^{2+2\varepsilon}$. $|L| \leq n^2$. but $I(P, L) \geq n^{3-4\varepsilon}$. contradiction. $\square$.

Now we construct the randomness extractor: $f_1(X_1, X_2, X_3) = X_1 + X_2 X_3$

$f_2(X_1, \ldots, X_9) = (X_1 + X_2 X_3) + (X_4 + X_5 X_6)(X_7 + X_8 X_9)$ ----.

$f_k(X_1 \ldots X_{3^k}) = f_{k-1}(X_1, \ldots X_{3^{k-1}}) + f_{k-1}(X_{3^{k-1}+1}, \ldots X_{2 \cdot 3^{k-1}}) \cdot f_{k-1}(X_{2 \cdot 3^{k-1}+1} \ldots X_{3^k})$.

After $\ell = O(\log 1/\delta)$ steps. support of f_ℓ will be almost $|\mathcal{F}|$.

Probabilistic method in set systems

partial order. chain. antichain. In particular, consider $\subseteq$ order.

Let $\tilde{\mathcal{F}}$ be a family of subsets of $[n]$. $\tilde{\mathcal{F}}$ is called an antichain if $\forall x, y \in \tilde{\mathcal{F}}.\ x \not\subseteq y$. Example: $\tilde{\mathcal{F}} = \binom{[n]}{k}$ maximize when $k = \frac{n}{2}$.

Theorem (Sperner, 1928). If $\tilde{\mathcal{F}}$ is an antichain of $[n]$. $|\tilde{\mathcal{F}}| \le \binom{n}{n/2}$.

Theorem (LYM inequality; Bollobás 1965, Lubell 1966, Meshalkin 1963

Yamamoto 1954). If $\tilde{\mathcal{F}}$ is an antichain of $[n]$, then $\sum_{S \in \tilde{\mathcal{F}}} \frac{1}{\binom{n}{|S|}} \le 1$.

Proof. consider a random permutation π of $[n]$. Construct a chain

$C_\pi = \{\{\pi(1)\}, \{\pi(1), \pi(2)\}, \dots \{\pi(1), \pi(2), \dots, \pi(n)\}\}$. $\forall S \in \tilde{\mathcal{F}}$.

$X_S = \begin{cases} 1 & S \in C_\pi \\ 0 & \text{o.w.} \end{cases}$ So $\mathbb{E}[X_S] = \Pr[S \in C_\pi] = \frac{|S|!\,(n-|S|)!}{n!} = \frac{1}{\binom{n}{|S|}}$.

Since $\tilde{\mathcal{F}}$ is an antichain. $\sum X_S = |\tilde{\mathcal{F}} \cap C_\pi| \le 1 \Rightarrow \sum \mathbb{E}[X_S] \le 1$. $\square$

Intersecting set families: $\tilde{\mathcal{F}}$ is intersecting if $\forall x, y \in \tilde{\mathcal{F}}.\ x \wedge y \neq \phi$

Example: $\tilde{\mathcal{F}}$ = all subsets of size k containing 1. $|\tilde{\mathcal{F}}| = \binom{n-1}{k-1}$.

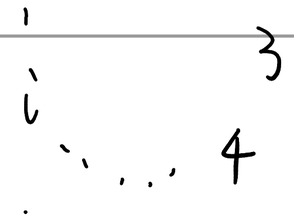
Remark: we assume $n \ge 2k$. since o.w. $\tilde{\mathcal{F}} = \binom{[n]}{k}$ is intersecting.

Theorem (Erdős–Ko–Rado 1961. proved in 1938) If $n \ge 2k$. and

$\mathcal{F}$ is an intersecting family of k-element subsets. then $|\mathcal{F}| \le \binom{n-1}{k-1}$.

Proof. (by Gyula Katona) Let π be a random permutation of $[n]$.

consider a circle and all contiguous blocks of size k.



$C_\pi = \{\{\pi(i+j \bmod n) : j \in [k]\} : i \in [n]\}$ (let $0 = n$)

$\forall S \in \mathcal{F}$ $X_S = \begin{cases} 1 & S \in C_\pi \\ 0 & \text{o.w.} \end{cases}$ So $\mathbb{E}[X_S] = \Pr[S \in C_\pi] = n/\binom{n}{k}$.

Since $\mathcal{F}$ is an intersecting family. $\sum X_S = |\mathcal{F} \cap C_\pi| \le k$. Suppose

$S \in C_\pi$. $\exists\ 2(k-1)$ other subsets in C_π intersecting S. but they can

be paired off into $k-1$ distinct pairs. so $\sum \mathbb{E}[X_S] \le k$. $\square$

Turán's theorem revisit.

Theorem. (Caro 1979, Wei 1981). $\alpha(G) \ge \sum_{v \in V(G)} (\deg(v)+1)^{-1}$.

Proof. Consider a random permutation π of V. Let I be the

set of vertices that appear before all its neighbours. Then I ind set.

$\forall v \in V.\ \Pr[v \in I] = \frac{1}{\deg(v)+1} \Rightarrow \mathbb{E}[|I|] = \sum_v (\deg(v)+1)^{-1}$. $\square$.

Taking the component. n-vertex graph has clique of size $\ge \sum \frac{1}{n-\deg(v)}$.

Applying Jensen's inequality. clique size $\ge n(n-2m/n)^{-1} = (1-\frac{2m}{n})^{-1}$.

Rearranging gives $m \le (1-\frac{1}{r})\frac{n^2}{2}$ if is not K_r-free $\Rightarrow$ Turán.

Derandomization via expectation: finding independent sets.

Algorithmic proof of the Caro-Wei inequality: sorting vertices in degree-non-decreasing order. Assign each vertex weight $\frac{1}{deg(v)+1}$

Greedily construct independent sets: at each step. take the first vertex and remove all its neighbours. then total weight removed ≤ 1.

Another algorithm based on conditional expectation: check vertices in an arbitrary order. For each vertex. there are 2 choices. Note that $\mathbb{E}[X] = \mathbb{E}[X|\mathcal{E}]\Pr[\mathcal{E}] + \mathbb{E}[X|\bar{\mathcal{E}}]\Pr[\mathcal{E}]$ where X is the size of independent sets and $\mathcal{E}$ is the event of taking v. At least one of $\mathbb{E}[X|\mathcal{E}]$ and $\mathbb{E}[X|\bar{\mathcal{E}}]$ is not less than $\mathbb{E}[X]$.

Another example: Max Cut. For each vertex. uniformly mark 0 or 1.