MASSACHUSETTS INSTITUTE OF TECHNOLOGY

6.265/15.070J Lecture 18 April 24, SP17
Lecturer: Guy Bresler Scribe notes by Emily Meigs

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They are posted to serve class purposes.*

Hardcore-model (independent sets)

Content.

- Hardness
- Slow mixing for local Markov chain
- Belief propagation

1 Review of the model

1.1 Independent set model

Let graph $G = (V, E)$ and we have $P_\lambda(I) = \frac{1}{2}\lambda^{|I|}$ where I is an independent set and $\lambda > 0$ is the ”activity”.

1.2 Glauber dynamics

- Pick uniformly at random a node $v \in V$
- Update: include v if none of its neighbors are in the independent set with probability $\frac{\lambda}{1+\lambda}$

2 Facts

Focusing on $\lambda = 1$.

1. (a) There can be no polynomial time sampling algorithm unless NP = RP.
   (b) Same holds for graphs of max degree $\Delta = 6$ [Sly, 2010]
2. Glauber dynamics mixes fast if $\Delta \leq 5$

Proof. We will first prove part 1(a). Assume we have a black box for sampling uniformly at random independent sets. Take $G = (V, E)$ with $|V| = n$. We will show how to answer in polynomial time with probability $\geq \frac{3}{4}$ "is there an independent set of size $\geq k$ in G?" Produce a new graph G' on nr vertices:

1. Replace $u \in V(G)$ with r nodes R_u
2. If $(u, v) \in E(G)$ then $R_u \times R_u \in E(G')$

Claim: Can choose $r = cn$ such that we get an independent set of size $\geq k$ if and only if it exists in G.
Consider an independent set $\geq k$ in G. This corresponds to $(2^r - 1)^k$ independent sets in G' of size $\geq k$. The number of independent sets of size $< k$ in G correspond to $\leq 2^n(2^r - 1)^{k-1}$ independent sets in G'.
So Pr[independent set $\geq k$ in G'] $\geq \frac{(2^r-1)^k}{(2^r-1)^k+2^n(2^r-1)^{k-1}}$.

□

3 Slow mixing for any local Markov chain ($\Delta = 6$)

Definition 1. *A Markov chain with Ω = independent sets γ **- local** if at each step it changes at most γn nodes.*

Theorem 1 (Dyer-Freize-Jerrum)**.** *There exists some γ and a sequence of graphs with max degree $\Delta = 6$, such that any γ-local Markov chain with stationary distribution $\pi = Unif(\Omega)$ has $t_{mix} \geq e^{cn}$.*

Theorem 2 (Conductance)**.** *For any Markov chain and all $S \subseteq \Omega$ with $\pi(S) \leq \frac{1}{2}$, $t_{mix} \geq \frac{1}{4\Phi(S)}$, where $\Phi(S) = \frac{C(S,\bar{S})}{\pi(S)}$ and $C(S, \bar{S}) = \sum_{x \in S, y \in \bar{S}} \pi(x)P(x, y)$.*

Corollary 3. *Assuming π is uniform on the allowable states, $t_{mix} \geq \frac{|S|}{4|\delta S|}$ where δS is the states in S connected to $\bar{S}$.*

Proof. Want to show $\Phi(S) \leq \frac{|\delta S|}{|S|}$. $\pi(S) = \frac{|S|}{|\Omega|}$.

$$\begin{aligned} C(S, \bar{S}) &= \sum_{x \in S} \sum_{y \in \bar{S}} \pi(x)P(x, y) \\ &= \sum_{x \in \delta S} \pi(x) \sum_{y \in \bar{S}} P(x, y) \\ &\leq \pi(\delta S) = \frac{|\delta S|}{|\Omega|} \end{aligned}$$

□

Proof. (Theorem 1) Let $G = (L, R, E)$ where L is the set of left nodes and R is the set of right nodes and $|L| = |R| = n$. Add a random perfect matching to E and do this $\Delta = 6$ times. Now define (α, β) independent set where $\alpha n = |I \cap L|$ and $\beta n = |I \cap R|$. Then let:
$I_{left} = \{(\alpha, \beta) \text{ ind. sets with } \alpha > \beta\}$
$I_{right} = \{(\alpha, \beta) \text{ ind. sets with } \alpha < \beta\}$
$I_{mid} = \{(\alpha, \beta) \text{ ind. sets in strip}\}$ where the strip is of width γ around the line $\alpha = \beta$ in the α vs. β plot.
We will apply the corollary with S = smaller of I_{left} and I_{right} and $\delta S \subseteq I_{mid}$.
Let $\epsilon(\alpha, \beta) =$ expected # of (α, β) independent sets. So $\epsilon(\alpha, \beta) = \binom{n}{\alpha n}\binom{n}{\beta n}[\frac{\binom{(1-\beta)n}{\alpha n}}{\binom{n}{\alpha n}}]^{\Delta}$.

$\binom{n}{\alpha n} = [\frac{1}{\alpha^{\alpha}(1-\alpha)^{(1-\alpha)}}]^n \, \Theta(\frac{1}{\sqrt{n}})$

$\epsilon(\alpha, \beta) = [\frac{(1-\beta)^{(\Delta-1)(1-\beta)}(1-\alpha)^{(\Delta-1)(1-\alpha)}}{\alpha^{\alpha}\beta^{\beta}(1-\alpha-\beta)^{\Delta(1-\alpha-\beta)}}]^{n+o(n)} = exp(f(\alpha, \beta)(n+o(n)))$

Properties of f:

- f is symmetric in (α, β) and has no local maximum other than the global
- If $\Delta \leq 5$, then there is a unique global maximum at $\alpha = \beta$
- If $\Delta \geq 6$, then there are two symmetric global maxima

(α^*, β^*) is one of the local maxima in $\Delta = 6$ with $\alpha^* = 0.035$, $\beta^* = 0.408$ and $f(\alpha^*, \beta^*) > c = 0.71 \Rightarrow \epsilon(\alpha^*, \beta^*) \geq e^{cn}$ for sufficiently large n. $\gamma = 0.35$
$f(\alpha, \beta) \leq c - 4\delta$, $\delta = 0.0001$ when in the γ-strip.

$$\mathbb{E}[|I_{mid}|] \leq \sum_{\alpha,\beta \text{in strip}} \epsilon(\alpha, \beta) \leq n^2 e^{(c-4\delta)n} \leq e^{(c-3\delta)n}$$

$$\Pr[|I_{mid}| \geq e^{(c-2\delta)n}] \leq e^{-\delta n}$$

Deterministically $|\{(\alpha, \beta) \text{ indep. sets with } I \cap L = \alpha n\}| \geq \binom{n}{\alpha n} 2^{(1-\Delta\alpha)n} \geq e^{(c-2\delta)\alpha}$ where the last inequality comes from Stirling's approximation and optimizing over α. Let α_0 be the value where the bound above is obtained (and similarly define β_0). Let:
$A = \{(\alpha, \beta) : \alpha \geq \alpha_0, \beta \leq \beta_0\}$,
$B = \{(\alpha, \beta) : \alpha \geq \alpha_0, \beta \geq \beta_0, \alpha \leq \beta\}$,
$C = \{(\alpha, \beta) : \alpha \leq \alpha_0, \beta \geq \beta_0\}$,
$D = \{(\alpha, \beta) : \alpha_0 \leq \alpha, \beta_0 \leq \beta, \alpha \leq \beta\}$.
Then $I_{left} \supseteq A \cup D$ and $I_{right} \supseteq C \cup B$. So using the corollary we get $\frac{|S|}{4|\delta S|} \geq e^{\delta n}$. □

4 Tree recursions

We are looking at π_Δ tree rooted at ρ.

Claim: For any set $A \subseteq \delta n$,
$\Pr[\rho \in I | \delta n \cap I = A] \in [\Pr[\rho \in I | \delta n \subseteq I], \Pr[\rho \in I | \delta n \cap I = \emptyset]]$
(Note: flipped when the level is even or odd).

Let $q(v) = \Pr[v \in I | p(v) \notin I]$ where $p(v)$ is the parent of v. Let the children of v be $w_1, w_2, ..., w_{\Delta-1}$. $R_{v \to p(v)} = \frac{q(v)}{1-q(v)}$.

Claim: $\mathbb{R}_{v \to p(v)} = \lambda \prod_{w \in N(v) \setminus p(v)} \frac{1}{1+R_{w \to v}}$.
Note: add a fictitious parent for ρ and condition on $p(\rho) \notin I$.
The claim is true by $\frac{1}{1+R_{w \to v}} = 1 - q(w) = \Pr(w \notin I | v \notin I)$.

$$\begin{aligned} q(v) = \Pr[v \in I | p(v) \notin I] &= \Pr[v \in I | p(v) \notin I; w_1, ..., w_{\Delta-1} \notin I] \Pr[w_1, ... w_{\Delta-1} \notin I | p(v) \notin I] \\ &= \frac{1}{2}[\Pr[w_1, ..., w_{\Delta-1} \notin I | v \notin I] \Pr[v \notin I | p(v) \notin I] \\ &+ \Pr[w_1, ..., w_{\Delta-1} \notin I | v \in I] \Pr[v \in I | p(v) \notin I]] \\ &= \frac{1}{2}[\prod \frac{1}{1+R}(1 - q(v)) q(v)] \end{aligned}$$

Then rearrange to get the recursion in the claim.

Think of $R_{v \to p(v)}$ as $f(x) = \lambda(\frac{1}{1+x})^{\Delta-1}$, $f \circ f(x)$.

The discussion will be finished at the beginning of next lecture.