L18

5/8/2020

Dirichlet forms & R.E. Oracle

Igor Pak

G - finite group, $V = \mathbb{R}[G]$

$$\langle \varphi, \psi \rangle := \sum_{x \in G} \varphi(x)\,\psi(x) = |G|\, \mathbb{E}_{x \in G \text{ uniform}} [\varphi(x)\,\psi(x)]$$

$$\mathcal{E}_\pi(\varphi, \varphi) := \langle (1 - P_\pi)\varphi, \varphi \rangle = |G| \cdot \mathbb{E}\left[(\varphi(X_0) - \varphi(X_1))\,\varphi(X_0)\right]$$

where $X_0 \leftarrow \text{unif}$, $X_1 = X_0 \pi$

$$[P_\pi \varphi](x) := \sum_{y \in G} \varphi(xy)\,\pi(y)$$

Let $\pi, \widetilde{\pi} \leftarrow$ dist on G s.t.

$$\mathcal{E}_{\widetilde{\pi}}(\varphi, \varphi) \le A\, \mathcal{E}_\pi(\varphi, \varphi) \quad \forall \varphi$$

Then $\quad (1 - \widetilde{\lambda}_i) \le A\,(1 - \lambda_i)$

$\Rightarrow$ r.w. applications via D&S-C Thm

Formally $G = \langle S \rangle \Rightarrow \pi(x) = \frac{1}{|G|} \quad \forall s \in S$

$$M_\pi = (a_{xy})_{x,y \in G} \qquad a_{xy} = \pi(x^{-1}y)$$

$\pi(x) = \pi(x^{-1}) \; \forall x \in G \Rightarrow M = M^T \Rightarrow \lambda_i \in \mathbb{R}$

$\not\Leftrightarrow \; S = S^{-1}$ /

Eigenvalues $1 = \lambda_0 > \lambda_1 > \dots > \lambda_{|G|-1} \geq -1$

If $1 \in S \Rightarrow \lambda_{|G|-1} > -1$

$\pi(1) \geq \frac{1}{2} \Rightarrow \lambda_i \geq 0$

Operators $Q := 1 - P_\pi$ on V

Prop $\forall \; Q = Q^T$

$$\min_{\varphi \in V} \frac{\langle Q\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} = \text{smallest eig of } Q$$

▷ $\max_{\varphi} \frac{\langle P_\pi \varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} = \max$ eig of $P_\pi = b$

$$\min_{\varphi} \frac{\langle Q\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} = \min_{\varphi : \sum_x \varphi(x) = 0} \frac{\langle Q\varphi, \varphi \rangle}{\langle \varphi, \varphi \rangle} = \lambda_1$$ ☒

Th $Q = Q^T$ symm operator on V

[min-max principle] $q_0 \le q_1 \le \dots \le q_n$ eig.

$$m(W) := \min \left\{ \frac{\langle Qf, f \rangle}{\langle f, f \rangle} , f \in W \subseteq V \right\}$$

Then

$$q_i = \max \{ m(W) : \dim W = i \}$$

▷ Exc Hint: take $W = \langle v_0 v_1 \dots v_{i-1} \rangle$ ☒

Th $\Rightarrow$ $(1 - \tilde{\lambda}_i) \le A (1 - \lambda_i)$

Random Elements Oracle

$G = \langle S \rangle$ ← Black Box group

$S = \{s_1 .. s_k\}$, $s_i \in S_N$, $GL(n, \mathbb{F}_q)$, etc.

Want: random elts $x \in G$

$\Leftrightarrow$ Probab distr $Q(x)$ on G s.t.

$sep(Q, U) < \varepsilon$, $\varepsilon > 0$ / $\varepsilon = 1/2$ V /

Alg [Babai, 1991]

$R \leftarrow S \cup S^{-1}$

[$x \leftarrow$ Lazy random walk for L steps

$R \leftarrow R + x$

Repeat ℓ times

Output last x

Th [Babai]

$L = O((\log |G|)^4)$

$\ell = O(\log |G|)$

works

Note: $4 \to 3$ [P]

Proof Outline $\Gamma = \Gamma(G, S)$

$X \subseteq G$ subset, $|X| \leq \frac{|G|}{2}$

Main L after $t = O(\text{diam}_\Gamma(X)\, N\, |S| \log |G|)$ steps

lazy r.w. $\notin X$ w/ $Pr > \frac{1}{2}$

Here $\text{diam}_\Gamma(X)$, N defined as in D-SC thm

D $\leftarrow$ Exc on using Dirichlet forms.

Hint: take $\pi(x) = \frac{1}{|X|}$ $\forall x \in X$, $\pi(x) = 0$ oth. ▨

Consider ε R-cube

$C_S = \{ s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}, \varepsilon_i \in \{0,1\} \} \subseteq G$

$X := C^{-1}C$, $g \in G$ s.t. $g \notin C^{-1}C$

$\Rightarrow C_{S \cup g} = \{ s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} g^\alpha, \alpha \in \{0,1\} \} = C_S \cup C_S g$

$\Rightarrow$ By ML each iteration $\in C_S^{-1} C_S$ w/ $P_i > \frac{1}{2}$

for $t = O(K \cdot 2 \cdot K \cdot \log|G|)$
(K: diam, N, |R|)

Using random subproducts $\rightarrow$ $K \leq O(\log|G|)$

after $\ell = O(\log|G|)$ iterations $\in$ R-cube

will double $\Omega(\log|G|)$ times until

$C_R^{-1} C_R > |G|/2$ $\Rightarrow$ $|R| = O(\log|G|)$ ▼ times

$\Rightarrow$ $t = O((\log|G|)^3)$

Exc $|X| > |G|/2$ $\Rightarrow$ $X^2 = G$

Moreover distr. $\approx$ uniform.

Why $3 < 4$? (in our case)

Cooperman - Dixon Alg

Alg (G, S) ← Black Box

$R \leftarrow S$

$h \leftarrow s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k}$, $R = \{s_1, \ldots s_k\}$

$R \leftarrow R + h$

Repeat ℓ times

Th [Dixon, 2006] / Conj. By Cooperman '02

$\ell = O(\log|G|)$

works

PROOF IDEA:

0) $X \subset G$, $X^2 \simeq X \Rightarrow X \simeq$ subgroup

1) $s_1^{\varepsilon_1} \cdots s_k^{\varepsilon_k} \cdot h^d = C \cup C^2$ w/ $Pr \geq \frac{1}{2}$ ← similar

2) $P(h \in \text{subgroup}) \geq \frac{1}{2}$

---

not 2) ⇒ doubling w/ $P > .\text{tons} > 0$