Random Walks on Graphs

Following Spielman, Chapter 10. For the randomness extractors part, see Chapter 6 of Vadhan's monograph.

Gil Cohen

November 16, 2020

Overview

1. Basic definitions
2. The stable distribution
3. The rate of convergence
4. Applications to randomness extractors

Random walks

Let $G = (V, E)$ be an undirected graph, and $\mathbf{p}$ a probability distribution on V, thought of as a vector $\mathbf{p} \in \mathbb{R}^V$.

A random step on G, starting from a probability distribution $\mathbf{p}$, is the process in which we

1. Sample v according to $\mathbf{p}$;
2. Sample a neighbor u of v uniformly at random, and return u.

If $\mathbf{p}_{\text{new}}$ is distribution over V after taking a random step, then for every $v \in V$,

$$\mathbf{p}_{\text{new}}(v) = \sum_{u \in \Gamma(v)} \frac{\mathbf{p}(u)}{\deg(u)}.$$

Random walks

$$\mathbf{p}_{\text{new}}(v) = \sum_{u \in \Gamma(v)} \frac{\mathbf{p}(u)}{\deg(u)}.$$

Note that

$$\mathbf{p}_{\text{new}} = \mathbf{W}_G \mathbf{p} = \mathbf{M}_G \mathbf{D}_G^{-1} \mathbf{p}$$

A length t random walk is the probabilistic process of taking t consecutive random steps. The corresponding distributions are given by

$$\mathbf{p}_t = \mathbf{W}\mathbf{p}_{t-1} = \mathbf{W}^2 p_{t-2} = \cdots = \mathbf{W}^t \mathbf{p}_0.$$

The normalized adjacency matrix

We define to the normalized adjacency matrix of G by

$$\mathbf{A}_G = \mathbf{D}_G^{-1/2}\mathbf{M}_G\mathbf{D}_G^{-1/2}.$$

Note that $\mathbf{A}_G$ is symmetric for undirected graph G and that $\mathbf{A}_G = \mathbf{D}_G^{-1/2}\mathbf{W}_G\mathbf{D}_G^{1/2}$.

Claim

ψ is an eigenvector of $\mathbf{A}$ of eigenvalue ω if and only if $\mathbf{D}^{1/2}\psi$ is an eigenvector of $\mathbf{W}$ of eigenvalue ω.

The normalized adjacency matrix

A fact you should know (and prove to yourself!)

Lemma

For $n \times n$ *matrices* $\mathbf{A}, \mathbf{B}$,

$$\phi_{\mathbf{AB}}(x) = \phi_{\mathbf{BA}}(x).$$

More generally, if $\mathbf{A}$ *is an* $n \times m$ *matrix and* $\mathbf{B}$ *an* $m \times n$ *matrix with* $n > m$ *then*

$$\phi_{\mathbf{AB}}(x) = x^{n-m}\phi_{\mathbf{BA}}(x).$$

In particular, the spectrum remains the same (and the kernel increase when $n \neq m$*).*

The normalized adjacency matrix

We denote the eigenvalues of $\mathbf{W}$ by $\omega_1 \geq \omega_2 \geq \cdots \geq \omega_n$. Note that the degree vector $\mathbf{d}$ is an eigenvector of $\mathbf{W}$ of eigenvalue $\omega_1 = 1$. Indeed,

$$\mathbf{Wd} = (\mathbf{MD}^{-1})d = \mathbf{M}(\mathbf{D}^{-1}\mathbf{d}) = \mathbf{M1} = \mathbf{d}.$$

Define

$$\psi_1 = \frac{\sqrt{\mathbf{d}}}{\|\sqrt{\mathbf{d}}\|} = \sqrt{\frac{\mathbf{d}}{\mathbf{1}^T\mathbf{d}}}.$$

Thus, ψ_1 is an eigenvector of $\mathbf{A}$ of eigenvalue 1. The Perron-Frobenius Theorem implies that $\mathrm{Spec}(\mathbf{W}) = \mathrm{Spec}(\mathbf{A}) \subset [-1, 1]$.

The stable distribution

We denote $\omega(G) = \max(\omega_2, -\omega_n)$. By Perron-Frobenius, G is connected and not bipartite if and only if $\omega(G) < 1$.

Theorem

Assume that G is connected and not bipartite. Then, a random walk from any initial distribution converges to the stable distribution

$$\boldsymbol{\pi} = \frac{\mathbf{d}}{\mathbf{1}^T\mathbf{d}}.$$

Extra space for the proof

The rate of convergence

Theorem

Let $p_0 = e(u)$ *for some* $u \in V$. *Then, for every* $v \in V$,

$$|p_t(v) - \pi(v)| \leq \omega(G)^t \cdot \sqrt{\frac{\deg(v)}{\deg(u)}}.$$

Extra space for the proof

Overview

1 Basic definitions

2 The stable distribution

3 The rate of convergence

4 Applications to randomness extractors

Seeded extractors

Definition

A distribution X has min entropy k if $\forall x, \Pr[X = x] \leq 2^{-k}$.

Claim

A distribution with min entropy k is a convex combination of distributions each is uniform over a set of size at least 2^k.

Seeded extractors

Definition

The statistical distance (aka total variation distance) between two distribution X, Y with support contained in D is given by

$$\mathbf{SD}(X, Y) = \max_{T \subseteq D} |\Pr[X \in T] - \Pr[Y \in T]|.$$

If $\mathbf{SD}(X, Y) \leq \varepsilon$ we write $X \approx_\varepsilon Y$.

Seeded extractors

Claim

$$\mathbf{SD}(X, Y) = \frac{1}{2} \cdot \|X - Y\|_1 = \sum_{z \in D} |X(z) - Y(z)|.$$

Seeded extractors

Definition

A function $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}^m$ is a (k,ε)-seeded extractor if for every k-source X, $\mathrm{Ext}(X,Y) \approx_\varepsilon U_m$.

Proposition

For every $n \geq k$ and ε there exists a (k,ε)-seeded extractor with

$$s = \log(n-k) + 2\log\frac{1}{\varepsilon} + O(1)$$

$$m = k - 2\log\frac{1}{\varepsilon} - O(1).$$

Seeded extractors from random walks

The construction of Ext.

Set $s = td$. Consider a $D = 2^d$-regular graph G on $N = 2^n$ vertices. On input $x \in \{0,1\}^n$, $y \in \{0,1\}^s$ proceed as follows:

1. Interpret the given sample $x \sim X$ as a vertex.
2. Take a length-t random walk on G and return the last vertex on the path.

analysis.

While we can proceed as before, we will take a slightly different approach. Write $\mathbf{p}$ for the distribution induced by X.

Seeded extractors from random walks

Claim

It holds that $\|\mathbf{p}_t - \boldsymbol{\pi}\|_2 \leq 2\omega(G)^t \cdot 2^{-k/2}$.

Claim

For every $\mathbf{x} \in \mathbb{R}^N$, $\|x\|_1 \leq \sqrt{N} \cdot \|x\|_2$.

Hence,

$$\mathbf{SD}(\mathrm{Ext}(X, Y), U) \leq 2\omega(G)^t \cdot 2^{(n-k)/2}.$$

We will later see that there are graphs with $\omega(G) = O\left(\frac{1}{\sqrt{D}}\right)$.

Thus, $s = n - k + 2\log\frac{1}{\varepsilon} + O(1)$.

Extra space for the proof

Extra space for the proof