Notes on Pseudorandomness

Naman Kumar

March 13, 2024

Abstract

The following document contains some notes related to Pseudorandomness by Salil Vadhan.

Contents

1 Expanders

Problem 2.9 (Spectral Graph Theory). Let M be the random walk matrix for a d-regular *undirected* graph $G = (V, E)$ on n vertices. We allow G to have self-loops and multiple edges. Recall that the uniform distribution is an eigenvector of M of eigenvalue $\lambda_1 = 1$. Prove the following statements. (Hint: for intuition, it may help to think about what the statements mean for the behaviour of the random walk on G.)

(1) All eigenvalues of M have absolute value at most 1.

Proof. Consider any eigenvector e that corresponds to any eigenvalue λ. We know that $eM = \lambda e$. Suppose that e_i is the index of e with the highest absolute value. We know that

$$\sum_{j=1}^{n} e_j M_{ji} = \lambda e_i.$$

Since e_i is the element with the highest absolute value, we have that

$$\sum_{j=1}^{n} e_j M_{ji} \leq e_i \sum_{j=1}^{n} M_{ji} = e_i.$$

It follows that $\lambda e_i \leq e_i$, implying that $\lambda \leq 1$. □

(2) G is disconnected $\iff$ 1 is an eigenvalue of multiplicity at least 2.

Proof. Suppose that there are two subsets $A, B \subseteq V$ where A and B are completely disconnected. We define e_X for each $X \subseteq V$ to be

$$e_X := \left(\frac{\mathbb{1}_X(i)}{|X|} \right)_{i \in V}$$

Then $e_A M = e_A$ and $e_b M = e_B$, but e_A and e_B are linearly independent. Thus the graph G has eigenvalue 1 with multiplicity at least 2. For the reverse implication, suppose there is a vector v with an eigenvalue 1 where $u \neq v$. Then the subspace spanned by $\langle u, v \rangle$ is part of the eigenspace of 1. Set $v' = c_1 u + c_2 v$ such that v' is zero on at least one index and non-negative on the others; this is possible since v and u are linearly independent and each index of u is non-negative. Then $v'M = c_1 uM + c_2 vM = v'$. We can interpret v' as a probability distribution by setting $w = \frac{v'}{\|v'\|}$. Then w is a probability distribution. Note that $wM = w$ since w is in the eigenspace of 1 as well.

It follows that $\lim_{t \to \infty} wM^t = w$. However, w has some index i such that $w_i = 0$. This means that for arbitrarily many steps, the probability of reaching the vertex

i when starting from any non-zero vertex w_j in w is 0. This immediately implies that there is no path from j to i, and thus G is disconnected. □

(3) G is bipartite $\iff$ -1 is an eigenvalue of M.

Proof. We order the vertices in M as the vertices in A first and the vertices in B second. Then consider the vector

$$e := \left(\frac{\chi_A(i)}{n}\right)_{i \in V}$$

where χ_A is -1 if $i \in A$ and 1 otherwise. Then this is an eigenvector with eigenvalue -1. Now suppose that -1 is an eigenvalue of M, with corresponding eigenvector e. Then $eM = -e$ and $eM^2 = e$. Note that M^2 is also a random-walk matrix for a different undirected multigraph G^2, the graph formed by connecting $(u, v) \in G^2 \iff \exists t : (u, t), (t, v) \in G$. Then e is an eigenvector of M^2 with eigenvalue 1. It follows that either $e = u$ or $e \neq u$. However $e = u$ is not possible since otherwise $eM = e \implies e = \mathbf{0}$, which is obviously false. Thus $e \neq u$ and so G^2 is disconnected. This means there exist sets $A, B \subseteq V$ such that there is no even-length walk from A to B. In particular, this implies that there is no odd-length cycle in the graph (since such a cycle would 'force' an even-length walk from A to B assuming that G were connected, which it is). This means that G is bipartite. □