Addendum to the paper "Randomness in Interactive Proofs"*

Mihir Bellare Oded Goldreich† Shafi Goldwasser

May 2, 1997

Contents: We reproduce a result regarding random walks on expander graphs which is implicit in [BGG90]. The presentation in [BGG90] makes an unnecessary step (i.e., modifying the random walk). The presentation below is obtained by omitting this step and instantiating one parameter (i.e., $L = 1$).

1 Introduction

A fundamental discovery of Ajtai, Komlos, and Szemerédi [AKS87] is that random walks on expander graphs provide a good approximation to repeated indepdendent attempts to hit any arbitrary fixed subset of sufficient density (within the vertex set). The importance of this discovery stems from the fact that a random walk on an expander can be generated using much fewer random coins than required for generating indepdendent samples in the vertex set. Precise formulations of the above discovery were given in [AKS87, CW89, GILVZ90] culminating in Kahale's optimal analysis [K91, Sec. 6].

Theorem 1.1 (Expander Random Walk Theorem [K91, Cor. 6.1]): *Let $G = (V, E)$ be an expander graph of degree d and λ be an upper bound on the absolute value of all eigenvalues, save the biggest one, of the adjacency matrix of the graph. Let W be a subset of V and $\rho \stackrel{\rm def}{=} |W|/|V|$. Then the fraction of random walks* (in G) *of* (edge) *length ℓ which stay within W is at most*

$$\rho \cdot \left(\rho + (1-\rho) \cdot \frac{\lambda}{d}\right)^{\ell}$$

A more general bound (which is weaker for the above special case) is implicit in [BGG90]:

Theorem 1.2 (Expander Random Walk Theorem – general case): *Let $G = (V, E)$, d and λ be as above. Let $W_0, W_1, ..., W_\ell$ be subsets of V with densities $\rho_0, ..., \rho_\ell$, respectively. Then the fraction of random walks* (in G) *of* (edge) *length ℓ which intersect $W_0 \times W_1 \times \cdots \times W_\ell$ is at most*

$$\sqrt{\rho_0} \cdot \prod_{i=1}^{\ell} \alpha_i$$

where $\alpha_i \stackrel{\rm def}{=} \min\{1, \max\{\sqrt{2\rho_i}, \sqrt{2} \cdot \frac{\lambda}{d}\}\}$.

Below we reproduce (and slightly adapt) the argument of [BGG90].

*Appeared in *Computational Complexity*, Vol. 4, No. 4 (1993), pages 319–354. Extended abstract in *31st FOCS*, 1990, pages 318–326.

†Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel. Email: oded@wisdom.weizmann.ac.il.

2 Proof of Theorem 1.2

Let A be a matrix representing the random walk on G (i.e., A is the adjacency matrix of G divided by the degree, d). We consider an orthonormal eigenvalue basis $u_1, \ldots, u_n$, where u_i being an eigenvector of A with eigenvalue λ_i. Without loss of generality $\lambda_1 = 1$ (and $u_1 = (n^{-1/2}, \ldots, n^{-1/2})$). Thus, $|\lambda_i| \leq \bar{\lambda} \stackrel{\text{def}}{=} \lambda/d$ for $i = 2, ..., n$. We let V_1 be the space spanned by u_1 and V_2 the space orthogonal to V_1 which is spanned by $u_2, \ldots, u_n$.

Let $||x||$ denote the Euclidean norm of $x \in \mathcal{R}^n$.

Claim 1: For any $x \in V_2$,

$$||Ax|| \leq \bar{\lambda} \cdot ||x|| \tag{1}$$

Proof: Since $u_2, \ldots, u_n$ is a basis for V_2 there are real numbers $c_2, \ldots, c_n$ such that $x = \sum_{i=2}^n c_i u_i$. But $Au_i = \lambda_i u_i$ and the vectors $u_2, \ldots, u_n$ are orthonormal, so

$$||Ax||^2 \ = \ ||\sum_{i=2}^n c_i A u_i||^2 \ = \ ||\sum_{i=2}^n c_i \lambda_i u_i||^2 \ = \ \sum_{i=2}^n c_i^2 \lambda_i^2 \ .$$

Since $|\lambda_i| \leq \bar{\lambda}$ for $i = 2, ..., n$.

$$||Ax||^2 \ \leq \ \bar{\lambda}^2 \sum_{i=2}^n c_i^2 \ = \ \bar{\lambda}^2 \, ||x||^2$$

which proves the claim. ■

Using a similar argument, we have $||Ax|| \leq ||x||$ for any $x \in \mathcal{R}^n$. Let e_i be the n-vector with 1 in position i and zeroes elsewhere. Define the projection matrix P_j as having its i-th column equal to e_i if $i \in W_j$ and the 0 vector otherwise. Note that $||P_j u_1||^2 \ = \ \rho_j$.

Claim 2: For any $x \in \mathcal{R}^n$ and any $j = 1, \ldots, v$,

$$||P_j A x|| \leq \sqrt{2} \cdot \max\{\sqrt{\rho_j}, \bar{\lambda}\} \, ||x|| \tag{2}$$

and $||P_j A x|| \leq ||x||$.

Proof: Let $x = x_1 + x_2$ where $x_1 = c_1 u_1 \in V_1$ and $x_2 \in V_2$. Then

$$\begin{aligned} ||P_j A x|| & \leq \ ||P_j A x_1|| + ||P_j A x_2|| \\ & \leq \ ||P_j x_1|| + ||A x_2|| \\ & \leq \ [2\,(||P_j x_1||^2 + ||A x_2||^2)]^{1/2} \end{aligned}$$

Here the first inequality is by the triangle inequality. The second uses the fact that $Ax_1 = x_1$ and $||P_j y|| \leq ||y||$ for any $y \in \mathcal{R}^n$. The third is just an application of the inequality $a + b \leq [2(a^2 + b^2)]^{1/2}$. Clearly, $||P_j x_1||^2 \leq \rho_j ||x_1||^2$. On the other hand, since A maps V_2 into itself we can apply Eq. (1) to conclude that $||Ax_2|| \leq \bar{\lambda}||x_2||$. Putting all this together we get

$$||P_j A x|| \ \leq \ [2\,(\rho_j ||x_1||^2 + \bar{\lambda}^2 ||x_2||^2)]^{1/2} = \sqrt{2 \max\{\rho_j, \bar{\lambda}^2\}} \, ||x||$$

as desired. Finally, observe that $||P_j A x|| \leq ||P_j x|| \leq ||x||$. ■

Let $||x||_1$ denote the L_1 norm (that is, the sum of the absolute values of the components) of $x \in \mathcal{R}^n$. Now let $x = (1/n, \ldots, 1/n) = n^{-1/2} u_1$ be the n vector corresponding to the uniform distribution and set

$$y \ = \ P_\ell A \cdots P_1 A P_0 x \ .$$

Eq. (2) implies that $\|y\| \leq \prod_{i=0}^{\ell} \alpha_i \cdot \|x\| = \prod_{i=0}^{\ell} \alpha_i \cdot n^{-1/2}$, where the α_i's are as in the statement of the theorem (with $\alpha_0 = \sqrt{\rho_0}$). Thus, the probability that a random walk, starting at the uniform distribution x, and terminating after ℓ steps at distribution y, visits a vertex in the set W_i at step i for $i = 0, 1, ..., \ell$ is

$$\|y\|_1 \leq \sqrt{n}\,\|y\| \leq \prod_{i=0}^{\ell} \alpha_i$$

and the theorem follows.

References

[AKS87] M. Ajtai, J. Komlos, E. Szemerédi, "Deterministic Simulation in LogSpace", *Proc. 19th STOC*, 1987, pp. 132–140.

[BGG90] M. Bellare, O. Goldreich, and S. Goldwasser "Randomness in Interactive Proofs", *Computational Complexity*, Vol. 4, No. 4 (1993), pp. 319–354.

[CW89] A. Cohen and A. Wigderson, "Dispensers, Deterministic Amplification, and Weak Random Sources", *30th FOCS*, 1989, pp. 14–19.

[GILVZ90] O. Goldreich, R. Impagliazzo, L.A. Levin, R. Venkatesan, and D. Zuckerman, "Security Preserving Amplification of Hardness", *31st FOCS*, pp. 318–326, 1990.

[K91] N. Kahale, "Eigenvalues and Expansion of Regular Graphs", *Journal of the ACM*, 42 (5), pages 1091–1106, September 1995. Combines works reported in *32nd FOCS (1991)* (pages 398–404) and *33rd FOCS (1992)* (pages 296–303).