15.3 Expanders and derandomization

Random algorithms use random bits (results of coin-flips) during the computation and are allowed to produce a wrong answer with some small probability. Such algorithms are usually much faster than known deterministic algorithms. But we must pay for this: we must expect errors and it is time consuming to produce random bits. It turns out that expander graphs can help to decrease the error-probability as well as to reduce the number of required random bits.

Suppose we have a boolean function $f : \{0,1\}^n \to \{0,1\}$ and a probabilistic polynomial time algorithm $\mathcal{A}$ that approximates f in the sense that, for random $r \in \{0,1\}^m$ we have:

$$\Pr_r\left[\mathcal{A}(x,r) \neq f(x)\right] \leq \frac{1}{4} \qquad \text{for every } x \in \{0,1\}^n. \tag{15.6}$$

We could reduce the error to 4^{-t} by running the algorithm $2t+1$ times and taking the majority of its outputs as the result. But this requires $(2t+1)m$ coin tosses. We want to reduce errors while using a small number of coin tosses. (A general procedure, when we reduce the number of random bits by modifying a probabilistic algorithm, is called *derandomization*.)

Take a d-regular graph $G = (V,E)$ on $|V| = 2^m$ vertices, and let $\lambda = \lambda_2$ be the second-largest eigenvalue of its adjacency matrix. Let us consider the following algorithm $\mathcal{B}$ that uses only m coin tosses. For a given input x, it picks a vertex $v \in V$ uniformly at random, and outputs

$$\mathcal{B}(x,v) := \text{Majority}_{u \in \Gamma(v)} \mathcal{A}(x,v)\,.$$

Claim 15.7. For every $x \in \{0,1\}^n$,

$$\Pr_v\left[\mathcal{B}(x,v) \neq f(x)\right] \leq 4\left(\frac{\lambda}{d}\right)^2.$$

Proof. Fix an input x. Let $S = \{v \in V : \mathcal{B}(x,v) \neq f(x)\}$ be the set of vertices on which $\mathcal{B}$ errs, and $T = \{v \in V : \mathcal{A}(x,v) \neq f(x)\}$ be the set of vertices on which $\mathcal{A}$ errs. Observe that every vertex $u \in S$ must be adjacent to at least $d/2$ vertices $v \in T$, implying that $e(S,T) \geq d|S|/2$. Moreover, $|T| \leq |V|/4 = n/4$, by (15.6). The Expander Mixing Lemma yields:

$$\begin{aligned} e(S,T) - \frac{d|S| \cdot |T|}{n} &\leq \lambda\sqrt{|S| \cdot |T|} \\ \frac{d|S|}{2} - \frac{d|S|}{4} &\leq \lambda\sqrt{|S|n/4} \\ \frac{d|S|}{4} &\leq \lambda\sqrt{|S|n/4} \end{aligned}$$

from which

$$\Pr_v\left[\mathcal{B}(x,v) \neq f(x)\right] = \frac{|S|}{n} \leq 4\left(\frac{\lambda}{d}\right)^2 .$$

follows. □

So, taking Ramanujan graphs the error probability can be reduced to $4(2/\sqrt{d})^2$ without any increase of the number of random bits!

We will present yet another application of expander graphs to reduce the number of random bits in Sect. 23.3. More applications of expanders as well as their constructions can be found in a beautiful survey paper by Hoory, Linial and Wigderson (2006).

Exercises

15.1 (Unique neighbors)**.** Let $G = (V, E)$ and $S \subseteq V$. A *unique neighbor* of S is a vertex in $\Gamma(S)$ connected by an edge to only one vertex in S. Suppose that G is an (n, d, c)-expander. Show that then every subset S of size $|S| \leq n/2$ has at least $(c - d/2)|S|$ unique neighbors. *Hint*: Let $T \subseteq \Gamma(S)$ be the set of non-unique neighbors and count the number of edges between S and T in two ways.

15.2. Let A be a square symmetric matrix, and λ one of its eigenvalues. Show that, for every integer $k \geq 1$, λ^k is an eigenvalue of A^k.

15.3. Let G be a d-regular graph on n vertices, and A its adjacency matrix. Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of A. Show that the eigenvalues of the adjacency matrix of the complement graph $\overline{G}$ are $n - 1 - d$ and $-1 - \lambda_i$ for $i = 2, \ldots, n$. *Hint*: The adjacency matrix of $\overline{G}$ is $J - I - A$. If vector x is orthogonal to $\mathbf{1}$, then $Jx = \mathbf{0}$.

15.4. Let G be a *bipartite* d-regular graph on n vertices, and A its adjacency matrix. Show that $-d$ is also an eigenvalue of A. *Hint*: If G is bipartite with parts of size p and q with $p + q = n$, then

$$A = \begin{bmatrix} \mathbf{0} & B \\ B^\top & \mathbf{0} \end{bmatrix}$$

for a $p \times q$ matrix B. Take the vector

$$x = (\underbrace{1, \ldots, 1}_{p}, \underbrace{-1, \ldots, -1}_{q}) .$$

15.5. Let $d > 1$ be a constant, and A be the adjacency matrix of a d-regular graph on n vertices. Let $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of A; hence, $\lambda_1 = d$. Let $\lambda = \max_{i \neq 1} |\lambda_i|$. Show that $\lambda \geq (1 - o(1))\sqrt{d}$ as $n \to \infty$. *Hint*: Use the fact that $\lambda_1 + \ldots + \lambda_n$ is the trace of A to estimate the trace of A^2.

15.6. Let A be a square 0-1 matrix with exactly d ones in each row and in each column. Show that then $x^\top Ax \leq d$ holds for every vector $x \in \mathbb{R}^n$ with $\|x\| = 1$. *Hint*: The Birkhoff–Von Neuman theorem and Exercise 13.21.