## Chapter 33

## Random Walks V

By Sariel Har-Peled, March 19, $2024{ }^{(1)}$

"Is there anything in the Geneva Convention about the rules of war in peacetime?" Stanko wanted to know, crawling back toward the truck. "Absolutely nothing," Caulec assured him. "The rules of war apply only in wartime. In peacetime, anything goes."

Romain Gary, Gasp

### 33.1. Explicit expander construction

We state here a few facts about expander graphs without proofs (see also Theorem 33.4.4).
Definition 33.1.1. And $(n, d, c)$-expander is a $d$-regular bipartite graph $G=(X, Y$, E$)$, where $|X|=|Y|=n / 2$. Here, we require that for any $S \subseteq X$, we have

$$
|\Gamma(S)| \geq\left(1+c\left(1-\frac{2|S|}{n}\right)\right)|S|
$$

The Margulis-Gabber-Galil expander. For a positive $m$, let $n=2 m^{2}$. Each vertex in $X$ and $Y$ above, is interpreted as a pair $(a, b)$, where $a, b \in \mathbb{Z}_{m}=\{0, \ldots, m-1\}$. A vertex $(a, b) \in X$ is connected to the vertices

$$
(a, b), \quad(a, a+b), \quad(a, a+b+1), \quad(a+b, b), \quad \text { and } \quad(a+b+1, b)
$$

in $Y$, where the addition is done module $m$.
Theorem 33.1.2 ([GG81]). The above graph is 5 regular, and it is $(n, 5,(2-\sqrt{3}) / 4)$-expander.
Specrtral gap and expansion. We remind the reader that a $d$-regular graph, then its adjacency matrix $\mathrm{M}(\mathrm{G})$ has (as its biggest eigenvalue) the eigenvalue $\lambda_{1}=d$. In particular, let $\left|\lambda_{1}\right| \geq\left|\lambda_{2}\right| \geq \ldots \geq\left|\lambda_{n}\right|$ be the eigenvalues of $M(G)$. We then have the following:
Theorem 33.1.3. If G is an (n,d,c)-expander then $\mathrm{M}(\mathrm{G})$ has $\left|\lambda_{2}\right| \leq d-\frac{c^{2}}{1024+2 c^{2}}$.
Theorem 33.1.4. If $\mathrm{M}(\mathrm{G})$ has $\left|\lambda_{2}\right| \leq d-\varepsilon$, then G is ( $n, d, c$-expander with $c \geq \frac{2 d \varepsilon-\varepsilon^{2}}{d^{2}}$.

### 33.2. Rapid mixing for expanders

Here is another equivalent definition of an expander.
Definition 33.2.1. Let $\mathrm{G}=(V, E)$ be an undirected $d$-regular graph. The graph G is a ( $n, d, c$ )-expander (or just $c$-expander), for every set $S \subseteq V$ of size at most $|V| / 2$, there are at least $c d|S|$ edges connecting $S$ and $\bar{S}=V \backslash S$; that is $e(S, \bar{S}) \geq c d|S|$,

[^0]Guaranteeing aperiodicity. Let G be a ( $n, d, c$ )-expander. We would like to perform a random walk on G . The graph $G$ is connected, but it might be periodic (i.e., bipartite). To overcome this, consider the random walk on $G$ that either stay in the current state with probability $1 / 2$ or traverse one of the edges. Clearly, the resulting Markov Chain (MC) is aperiodic. The resulting transition matrix is

$$
\mathrm{Q}=\mathrm{M} / 2 d+\mathcal{I} / 2,
$$

where M is the adjacency matrix of G and $\mathcal{I}$ is the identity $n \times n$ matrix. Clearly Q is doubly stochastic. Furthermore, if $\widehat{\lambda}_{i}$ is an eigenvalue of M , with eigenvector $v_{i}$, then

$$
\mathrm{Q} v_{i}=\frac{1}{2}\left(\frac{\mathrm{M}}{d}+\mathcal{I}\right) v_{i}=\frac{1}{2}\left(\frac{\widehat{\lambda_{i}}}{d}+1\right) v_{i} .
$$

As such, $\left(\widehat{\lambda_{i}} / d+1\right) / 2$ is an eigenvalue of Q . Namely, if there is a spectral gap in the graph G , there would also be a similar spectral gap in the resulting MC. This MC can be generated by adding to each vertex $d$ self loops, ending up with a $2 d$-regular graph. Clearly, this graph is still an expander if the original graph is an expander, and the random walk on it is aperiodic.

From this point on, we would just assume our expander is aperiodic.

### 33.2.1. Bounding the mixing time

For a MC with $n$ states, we denote by $\pi=\left(\pi_{1}, \ldots, \pi_{n}\right)$ its stationary distribution. We consider only nicely behave MC that fall under Theorem 33.4.1. As such, no state in the MC has zero stationary probability.

Definition 33.2.2. Let $\mathrm{q}^{(t)}$ denote the state probability vector of a Markov chain defined by a transition matrix Q at time $t \geq 0$, given an initial distribution $\mathrm{q}^{(0)}$. The relative pairwise distance of the Markov chain at time $t$ is

$$
\Delta(t)=\max _{i} \frac{\left|\mathbf{q}_{i}^{(t)}-\pi_{i}\right|}{\pi_{i}}
$$

Namely, if $\Delta(t)$ approaches zero then $\mathbf{q}^{(t)}$ approaches $\pi$.
We remind the reader that we saw a construction of a constant degree expander with constant expansion. In its transition matrix $Q$, we have that $\widehat{\lambda_{1}}=1$, and $-1 \leq \widehat{\lambda_{2}}<1$, and furthermore the spectral gap $\widehat{\lambda_{1}}-\widehat{\lambda_{2}}$ was a constant (the two properties are equivalent, but we proved only one direction of this).

We need a slightly stronger property (that does hold for our expander construction). We have that $\widehat{\lambda_{2}} \geq$ $\max _{i=2}^{n}\left|\widehat{\lambda}_{i}\right|$.

Theorem 33.2.3. Let Q be the transition matrix of an aperiodic ( $n, d, c$ )-expander. Then, for any initial distribution $\mathrm{q}^{(0)}$, we have that

$$
\Delta(t) \leq n^{3 / 2}\left(\widehat{\lambda_{2}}\right)^{t} .
$$

Since $\widehat{\lambda_{2}}$ is a constant smaller than 1 , the distance $\Delta(t)$ drops exponentially with $t$.
Proof: We have that $\mathrm{q}^{(t)}=\mathrm{q}^{(0)} \mathrm{Q}^{t}$. Let $\mathcal{B}(\mathrm{Q})=\left\langle v_{1}, \ldots, v_{n}\right\rangle$ denote the orthonormal eigenvector basis of Q (see Definition 33.4.2 $\mathrm{p}_{6}$, and write $\mathrm{q}^{(0)}=\sum_{i=1}^{n} \alpha_{i} v_{i}$. Since $\widehat{\lambda}_{1}=1$, we have that

$$
\mathbf{q}^{(t)}=\mathbf{q}^{(0)} \mathbf{Q}^{t}=\sum_{i=1}^{n} \alpha_{i}\left(v_{i} \mathbf{Q}^{t}\right)=\sum_{i=1}^{n} \alpha_{i}\left(\widehat{\lambda_{i}}\right)^{t} v_{i}=\alpha_{1} v_{1}+\sum_{i=2}^{n} \alpha_{i}\left(\widehat{\lambda_{i}}\right)^{t} v_{i} .
$$

Since $v_{1}=(1 / \sqrt{n}, \ldots, 1 / \sqrt{n})$, and $\left|\widehat{\lambda_{i}}\right| \leq \widehat{\lambda_{2}}<1$, for $i>1$, we have that $\lim _{t \rightarrow \infty}\left(\widehat{\lambda_{i}}\right)^{t}=0$, and thus

$$
\pi=\lim _{t \rightarrow \infty} \mathrm{q}^{(t)}=\alpha_{1} v_{1}+\sum_{i=2}^{n} \alpha_{i}\left(\lim _{t \rightarrow \infty}\left(\widehat{\lambda}_{i}\right)^{t}\right) v_{i}=\alpha_{1} v_{1} .
$$

Now, since $v_{1}, \ldots, v_{n}$ is an orthonormal basis, and $\mathrm{q}^{(0)}=\sum_{i=1}^{n} \alpha_{i} v_{i}$, we have that $\left\|\mathrm{q}^{(0)}\right\|_{2}=\sqrt{\sum_{i=1}^{n} \alpha_{i}^{2}}$. Thus implies that

$$
\begin{aligned}
\left\|\mathbf{q}^{(t)}-\pi\right\|_{1} & =\left\|\mathbf{q}^{(t)}-\alpha_{1} v_{1}\right\|_{1}=\left\|\sum_{i=2}^{n} \alpha_{i}\left(\widehat{\lambda_{i}}\right)^{t} v_{i}\right\|_{1} \leq \sqrt{n}\left\|\sum_{i=2}^{n} \alpha_{i}\left(\widehat{\lambda_{i}}\right)^{t} v_{i}\right\|_{2}=\sqrt{n} \sqrt{\sum_{i=2}^{n}\left(\alpha_{i}\left(\widehat{\lambda_{i}}\right)^{t}\right)^{2}} \\
& \leq \sqrt{n}\left(\widehat{\lambda_{2}}\right)^{t} \sqrt{\sum_{i=2}^{n}\left(\alpha_{i}\right)^{2} \leq \sqrt{n}\left(\widehat{\lambda_{2}}\right)^{t}\left\|\mathbf{q}^{(0)}\right\|_{2} \leq \sqrt{n}\left(\widehat{\lambda_{2}}\right)^{t}\left\|\mathbf{q}^{(0)}\right\|_{1}=\sqrt{n}\left(\widehat{\lambda_{2}}\right)^{t},}
\end{aligned}
$$

since $\mathrm{q}^{(0)}$ is a distribution. Now, since $\pi_{i}=1 / n$, we have

$$
\Delta(t)=\max _{i} \frac{\left|\mathbf{q}_{i}^{(t)}-\pi_{i}\right|}{\pi_{i}}=\max _{i} n\left|\mathbf{q}_{i}^{(t)}-\pi_{i}\right| \leq n \max _{i}\left\|\mathbf{q}^{(t)}-\pi\right\|_{1} \leq n \sqrt{n}\left(\widehat{\lambda_{2}}\right)^{t} .
$$

### 33.3. Probability amplification by random walks on expanders

We are interested in performing probability amplification for an algorithm that is a BPP algorithm (see Definition 33.4.3). It would be convenient to work with an algorithm which is already somewhat amplified. That is, we assume that we are given a BPP algorithm Alg for a language $L$, such that
(A) If $x \in L$ then $\mathbb{P}[\operatorname{Alg}(x)$ accepts $] \geq 199 / 200$.
(B) If $x \notin L$ then $\mathbb{P}[\operatorname{Alg}(x)$ accepts $] \leq 1 / 200$.

We assume that Alg requires a random bit string of length $n$. So, we have a constant degree expander $G$ (say of degree $d$ ) that has at least $200 \cdot 2^{n}$ vertices. In particular, let

$$
U=|V(\mathrm{G})|,
$$

and since our expander construction grow exponentially in size (but the base of the exponent is a constant), we have that $U=O\left(2^{n}\right)$. (Translation: We can not quite get an expander with a specific number of vertices. Rather, we can guarantee an expander that has more vertices than we need, but not many more.)

We label the vertices of $G$ with all the binary strings of length $n$, in a round robin fashion (thus, each binary string of length $n$ appears either $\left\lceil|V(\mathrm{G})| / 2^{n}\right\rceil$ or $\left\lfloor|V(\mathrm{G})| / 2^{n}\right\rfloor$ times $)$. For a vertex $v \in V(\mathrm{G})$, let $\mathrm{s}(v)$ denote the binary string associated with $v$.

Consider a string $x$ that we would like to decide if it is in $L$ or not. We know that at least $99 / 100 U$ vertices of G are labeled with "random" strings that would yield the right result if we feed them into Alg (the constant here deteriorated from 199/200 to 99/100 because the number of times a string appears is not identically the same for all strings).

The algorithm. We perform a random walk of length $\mu=\alpha \beta k$ on G , where $\alpha$ and $\beta$ are constants to be determined shortly, and $k$ is a parameter. To this end, we randomly choose a starting vertex $X_{0}$ (this would require $n+O(1)$ bits). Every step in the random walk, would require $O(1)$ random bits, as the expander is a constant degree expander, and as such overall, this would require $n+O(k)$ random bits.

Now, lets $X_{0}, X_{1}, \ldots, X_{\mu}$ be the resulting random walk. We compute the result of

$$
Y_{i}=\operatorname{Alg}\left(x, r_{i}\right), \quad \text { for } \quad i=0, \ldots, v, \quad \text { and } v=\alpha k,
$$

where $r_{i}=\mathrm{s}\left(X_{i \cdot \beta}\right)$. Specifically, we use the strings associated with nodes that are in distance $\beta$ from each other along the path of the random walk. We return the majority of the bits $Y_{0}, \ldots, Y_{\alpha k}$ as the decision of whether $x \in L$ or not.

We assume here that we have a fully explicit construction of an expander. That is, given a vertex of an expander, we can compute all its neighbors in polynomial time (in the length of the index of the vertex). While the construction of expander shown is only explicit it can be made fully explicit with more effort.

### 33.3.1. The analysis

Intuition. Skipping every $\beta$ nodes in the random walk corresponds to performing a random walk on the graph $\mathrm{G}^{\beta}$; that is, we raise the graph to power $\beta$. This new graph is a much better expander (but the degree had deteriorated). Now, consider a specific input $x$, and mark the bad vertices for it in the graph G. Clearly, we mark at most $1 / 100$ fraction of the vertices. Conceptually, think about these vertices as being uniformly spread in the graph and far apart. From the execution of the algorithm to fail, the random walk needs to visit $\alpha k / 2$ bad vertices in the random walk in $\mathrm{G}^{k}$. However, the probability for that is extremely small - why would the random walk keep stumbling into bad vertices, when they are so infrequent?

The real thing. Let $Q$ be the transition matrix of $G$. We assume, as usual, that the random walk on $G$ is aperiodic (if not, we can easily fix it using standard tricks), and thus ergodic. Let $B=Q^{\beta}$ be the transition matrix of the random walk of the states we use in the algorithm. Note, that the eigenvalues (except the first one) of B "shrink". In particular, by picking $\beta$ to be a sufficiently large constant, we have that

$$
\widehat{\lambda_{1}}(\mathrm{~B})=1 \quad \text { and } \quad\left|\widehat{\lambda_{i}}(\mathrm{~B})\right| \leq \frac{1}{10}, \quad \text { for } i=2, \ldots, U
$$

For the input string $x$, let W be the matrix that has 1 in the diagonal entry $\mathrm{W}_{i i}$, if and only $\operatorname{Alg}(x, \mathrm{~s}(i))$ returns the right answer, for $i=1, \ldots, U$. (We remind the reader that $\mathrm{s}(i)$ is the string associated with the $i$ th vertex, and $U=|V(\mathrm{G})|$.) The matrix W is zero everywhere else. Similarly, let $\overline{\mathrm{W}}=\mathcal{I}-\mathrm{W}$ be the "complement" matrix having 1 at $\overline{\mathrm{W}}_{i i}$ iff $\operatorname{Alg}(x, \mathrm{~s}(i))$ is incorrect. We know that W is a $U \times U$ matrix, that has at least $(99 / 100) U$ ones on its diagonal.

Lemma 33.3.1. Let Q be a symmetric transition matrix, then all its eigenvalues of Q are in the range $[-1,1]$.
Proof: Let $p \in \mathbb{R}^{n}$ be an eigenvector with eigenvalue $\lambda$. Let $p_{i}$ be the coordinate with the maximum absolute value in $p$. We have that

$$
\left|\lambda p_{i}\right|=\left|(p \mathrm{Q})_{i}\right|=\left|\sum_{j=1}^{U} p_{j} \mathrm{Q}_{j i}\right| \leq \sum_{j=1}^{U}\left|p_{j}\right|\left|\mathrm{Q}_{j i}\right| \leq\left|p_{i}\right| \sum_{j=1}^{U}\left|\mathrm{Q}_{j i}\right|=\left|p_{i}\right| .
$$

This implies that $|\lambda| \leq 1$.
(We used the symmetry of the matrix, in implying that $Q$ eigenvalues are all real numbers.)

Lemma 33.3.2. Let Q be a symmetric transition matrix, then for any $p \in \mathbb{R}^{n}$, we have that $\|p \mathrm{Q}\|_{2} \leq\|p\|_{2}$.
Proof: Let $\mathcal{B}(\mathrm{Q})=\left\langle v_{1}, \ldots, v_{n}\right\rangle$ denote the orthonormal eigenvector basis of Q , with eigenvalues $1=\lambda_{1}, \ldots, \lambda_{n}$. Write $p=\sum_{i} \alpha_{i} v_{i}$, and observe that

$$
\|p \mathrm{Q}\|_{2}=\left\|\sum_{i} \alpha_{i} v_{i} \mathrm{Q}\right\|_{2}=\left\|\sum_{i} \alpha_{i} \lambda_{i} v_{i}\right\|_{2}=\sqrt{\sum_{i} \alpha_{i}^{2} \lambda_{i}^{2}} \leq \sqrt{\sum_{i} \alpha_{i}^{2}}=\|p\|_{2},
$$

since $\left|\lambda_{i}\right| \leq 1$, for $i=1, \ldots, n$, by Lemma 33.3.1.
Lemma 33.3.3. Let $\mathrm{B}=\mathrm{Q}^{\beta}$ be the transition matrix of the graph $\mathrm{G}^{\beta}$. For all vectors $p \in \mathbb{R}^{n}$, we have:
(i) $\|p \mathrm{BW}\| \leq\|p\|$, and
(ii) $\|p \mathrm{~B} \overline{\mathrm{~W}}\| \leq\|p\| / 5$.

Proof: (i) Since multiplying a vector by W has the effect of zeroing out some coordinates, its clear that it can not enlarge the norm of a matrix. As such, $\|p \mathrm{BW}\|_{2} \leq\|p \mathrm{~B}\|_{2} \leq\|p\|_{2}$ by Lemma 33.3.2.
(ii) Write $p=\sum_{i} \alpha_{i} v_{i}$, where $v_{1}, \ldots, v_{n}$ is the orthonormal basis of Q (and thus also of B ), with eigenvalues $1=\hat{\lambda}_{1}, \ldots, \hat{\lambda}_{n}$. We remind the reader that $v_{1}=(1,1, \ldots, 1) / \sqrt{n}$. Since $\bar{W}$ zeroes out at least $99 / 100$ of the entries of a vectors it is multiplied by (and copy the rest as they are), we have that

$$
\left\|v_{1} \overline{\mathrm{~W}}\right\| \leq \sqrt{(n / 100)(1 / \sqrt{n})^{2}} \leq 1 / 10=\left\|v_{1}\right\| / 10
$$

Now, for any $x \in \mathbb{R}^{U}$, we have $\|x \overline{\mathrm{~W}}\| \leq\|x\|$. As such, we have that

$$
\begin{aligned}
\|p \mathrm{~B} \overline{\mathrm{~W}}\|_{2} & =\left\|\sum_{i} \alpha_{i} v_{i} \mathrm{~B} \overline{\mathrm{~W}}\right\|_{2} \leq\left\|\alpha_{1} v_{1} \mathrm{~B} \overline{\mathrm{~W}}\right\|+\left\|\sum_{i=2}^{U} \alpha_{i} v_{i} \mathrm{~B} \overline{\mathrm{~W}}\right\| \\
& \leq\left\|\alpha_{1} v_{1} \overline{\mathrm{~W}}\right\|+\left\|\left(\sum_{i=2}^{U} \alpha_{i} v_{i} \widehat{\lambda}_{i}^{\beta}\right) \overline{\mathrm{W}}\right\| \leq \frac{\left|\alpha_{1}\right|}{10}+\left\|\sum_{i=2}^{U} \alpha_{i} v_{i} \widehat{\lambda}_{i}^{\beta}\right\| \\
& \leq \frac{\left|\alpha_{1}\right|}{10}+\sqrt{\sum_{i=2}^{U}\left(\alpha_{i} \widehat{\lambda}_{i}^{\beta}\right)^{2}} \leq \frac{\left|\alpha_{1}\right|}{10}+\frac{1}{10} \sqrt{\sum_{i=2}^{U} \alpha_{i}^{2}} \leq \frac{\|p\|}{10}+\frac{1}{10}\|p\| \leq \frac{\|p\|}{5},
\end{aligned}
$$

since $\left|\lambda_{i}^{\beta}\right| \leq 1 / 10$, for $i=2, \ldots, n$.
Consider the strings $r_{0}, \ldots, r_{v}$. For each one of these strings, we can write down whether its a "good" string (i.e., Alg return the correct result), or a bad string. This results in a binary pattern $b_{0}, \ldots, b_{k}$. Given a distribution $p \in \mathbb{R}^{U}$ on the states of the graph, its natural to ask what is the probability of being in a "good" state. Clearly, this is the quantity $\|p \mathrm{~W}\|_{1}$. Thus, if we are interested in the probability of a specific pattern, then we should start with the initial distribution $p^{0}$, truncate away the coordinates that represent an invalid state, apply the transition matrix, again truncate away forbidden coordinates, and repeat in this fashion till we exhaust the pattern. Clearly, the $\ell_{1}$-norm of the resulting vector is the probability of this pattern. To this end, given a pattern $b_{0}, \ldots, b_{k}$, let $\mathcal{S}=\left\langle S_{0}, \ldots, S_{v}\right\rangle$ denote the corresponding sequence of "truncating" matrices (i.e., $S_{i}$ is either W or $\left.\overline{\mathrm{W}}\right)$. Formally, we set $S_{i}=\mathrm{W}$ if $\operatorname{Alg}\left(x, r_{i}\right)$ returns the correct answer, and set $S_{i}=\overline{\mathrm{W}}$ otherwise.

The above argument implies the following lemma.
Lemma 33.3.4. For any fixed pattern $b_{0}, \ldots, b_{v}$ the probability of the random walk to generate this pattern of random strings is $\left\|p^{(0)} S_{0} \mathrm{~B} S_{1} \ldots \mathrm{~B} S_{v}\right\|_{1}$, where $\mathcal{S}=\left\langle S_{0}, \ldots, S_{v}\right\rangle$ is the sequence of W and $\overline{\mathrm{W}}$ encoded by this pattern.

Theorem 33.3.5. The probability that the majority of the outputs $\operatorname{Alg}\left(x, r_{0}\right), \operatorname{Alg}\left(x, r_{1}\right), \ldots, \operatorname{Alg}\left(x, r_{k}\right)$ is incorrect is at most $1 / 2^{k}$.

Proof: The majority is wrong, only if (at least) half the elements of the sequence $\mathcal{S}=\left\langle S_{0}, \ldots, S_{\nu}\right\rangle$ belong to $\bar{W}$. Fix such a "bad" sequence $\mathcal{S}$, and observe that the distributions we work with are vectors in $\mathbb{R}^{U}$. As such, if $p^{0}$ is the initial distribution, then we have that

$$
\mathbb{P}[\mathbf{S}]=\left\|p^{(0)} S_{0} \mathrm{~B} S_{1} \ldots \mathrm{~B} S_{v}\right\|_{1} \leq \sqrt{U}\left\|p^{(0)} S_{0} \mathrm{~B} S_{1} \ldots \mathrm{~B} S_{v}\right\|_{2} \leq \sqrt{U} \frac{1}{5^{v / 2}}\left\|p^{(0)}\right\|_{2}
$$

by Lemma 33.3.6 below (i.e., Cauchy-Schwarz inequality) and by repeatedly applying Lemma 33.3.3, since half of the sequence $\mathcal{S}$ are $\overline{\mathrm{W}}$, and the rest are W . The distribution $p^{(0)}$ was uniform, which implies that $\left\|p^{(0)}\right\|_{2}=1 / \sqrt{U}$. As such, let $\mathcal{S}$ be the set of all bad patterns (there are $2^{v-1}$ such "bad" patterns). We have

$$
\mathbb{P}[\text { majority is bad }] \leq 2^{v} \sqrt{U} \frac{1}{5^{v / 2}}\left\|p^{(0)}\right\|_{2}=(4 / 5)^{v / 2}=(4 / 5)^{\alpha k / 2} \leq \frac{1}{2^{k}},
$$

for $\alpha=7$.

### 33.3.2. Some standard inequalities

Lemma 33.3.6. For any vector $\mathbf{v}=\left(v_{1}, \ldots, v_{d}\right) \in \mathbb{R}^{d}$, we have that $\|\mathbf{v}\|_{1} \leq \sqrt{d}\|\mathbf{v}\|_{2}$.
Proof: We can safely assume all the coordinates of $\mathbf{v}$ are positive. Now,

$$
\|\mathbf{v}\|_{1}=\sum_{i=1}^{d} v_{i}=\sum_{i=1}^{d} v_{i} \cdot 1=|\mathbf{v} \cdot(1,1, \ldots, 1)| \leq \sqrt{\sum_{i=1}^{d} v_{i}^{2}} \sqrt{\sum_{i=1}^{d} 1^{2}}=\sqrt{d}\|\mathbf{v}\|
$$

by the Cauchy-Schwarz inequality.

### 33.4. Tools from previous lecture

Theorem 33.4.1 (Fundamental theorem of Markov chains). Any irreducible, finite, and aperiodic Markov chain has the following properties.
(i) All states are ergodic.
(ii) There is a unique stationary distribution $\pi$ such that, for $1 \leq i \leq n$, we have $\pi_{i}>0$.
(iii) For $1 \leq i \leq n$, we have $\mathrm{f}_{i i}=1$ and $\mathrm{h}_{i i}=1 / \pi_{i}$.
(iv) Let $N(i, t)$ be the number of times the Markov chain visits state $i$ in $t$ steps. Then

$$
\lim _{t \rightarrow \infty} \frac{N(i, t)}{t}=\pi_{i} .
$$

Namely, independent of the starting distribution, the process converges to the stationary distribution.
Definition 33.4.2. Given a random walk matrix $Q$ associated with a $d$-regular graph, let $\mathcal{B}(Q)=\left\langle v_{1}, \ldots, v_{n}\right\rangle$ denote the orthonormal eigenvector basis defined by $\mathbb{Q}$. That is, $v_{1}, \ldots, v_{n}$ is an orthonormal basis for $\mathbb{R}^{n}$, where all these vectors are eigenvectors of Q and $v_{1}=1^{n} / \sqrt{n}$. Furthermore, let $\widehat{\lambda}_{i}$ denote the $i$ th eigenvalue of Q , associated with the eigenvector $v_{i}$, such that $\widehat{\lambda_{1}} \geq \widehat{\lambda_{2}} \geq \cdots \geq \widehat{\lambda_{n}}$.

Definition 33.4.3. The class BPP (for Bounded-error Probabilistic Polynomial time) is the class of languages that have a randomized algorithm Alg with worst case polynomial running time such that for any input $x \in \Sigma^{*}$, we have
(i) If $x \in L$ then $\mathbb{P}[\operatorname{Alg}(x)$ accepts $] \geq 3 / 4$.
(ii) If $x \notin L$ then $\mathbb{P}[\operatorname{Alg}(x)$ accepts $] \leq 1 / 4$.

Theorem 33.4.4 (Fundamental theorem of algebraic graph theory). Let $\mathrm{G}=\mathrm{G}(V, E)$ be an undirected (multi)graph with maximum degree $d$ and with $n$ vertices. Let $\lambda_{1} \geq \lambda_{2} \geq \cdots \geq \lambda_{n}$ be the eigenvalues of $\mathrm{M}(\mathrm{G})$ and the corresponding orthonormal eigenvectors are $e_{1}, \ldots, e_{n}$. The following holds.
(i) If G is connected then $\lambda_{2}<\lambda_{1}$.
(ii) For $i=1, \ldots, n$, we have $\left|\lambda_{i}\right| \leq d$.
(iii) $d$ is an eigenvalue if and only if G is regular.
(iv) If G is $d$-regular then the eigenvalue $\lambda_{1}=d$ has the eigenvector $e_{1}=\frac{1}{\sqrt{n}}(1,1,1, \ldots, 1)$.
(v) The graph G is bipartite if and only if for every eigenvalue $\lambda$ there is an eigenvalue $-\lambda$ of the same multiplicity.
(vi) Suppose that G is connected. Then G is bipartite if and only if $-\lambda_{1}$ is an eigenvalue.
(vii) If G is $d$-regular and bipartite, then $\lambda_{n}=d$ and $e_{n}=\frac{1}{\sqrt{n}}(1,1, \ldots, 1,-1, \ldots,-1)$, where there are equal numbers of $1 s$ and $-1 s$ in $e_{n}$.

## References

[GG81] O. Gabber and Z. Galil. Explicit constructions of linear-sized superconcentrators. J. Comput. Syst. Sci., 22(3): 407-420, 1981.


[^0]:    ${ }^{(1)}$ This work is licensed under the Creative Commons Attribution-Noncommercial 3.0 License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

