# Lecture 6

# Random graphs IV: The existence of expanders

## 6.1 Expansion in the permutation model

We split the proof of the fact that random graphs are expanders over a couple of lemmas.

The first lemma will be about random walks on the symmetric group. Given a finite set $W = \{a_1, \ldots, a_k\}$, we will write

$$W^r = \left\{ a_{i_1}^{\varepsilon_1} \cdots a_{i_k}^{\varepsilon_k};\ i_j \in \{1, \ldots, k\},\ \varepsilon_i \in \{\pm 1\} \right\}.$$

We have

$$|W^r| = (2k)^r.$$

Let $\mathbb{P}_r$ denote the uniform probability measure on this finite set.

Furthermore, given $\pi_1, \ldots, \pi_k \in \mathfrak{S}_n$ and $w \in W^r$,

$$w(\pi_1, \ldots, \pi_k) \in \mathfrak{S}_n$$

will be the permutation obtained by replacing $a_i^{\varepsilon}$ by $\pi_i^{\varepsilon}$ for all $i = 1, \ldots, k$ and $\varepsilon \in \{\pm 1\}$. As such, we can speak of the set of fixed points of $w(\pi_1, \ldots, \pi_k)$, which we will denote by

$$\mathrm{Fix}(w(\pi_1, \ldots, \pi_k))$$

The relation between eigenvalues and random walks we will use is:

**Lemma 6.1.** *Let $\pi_1, \dots, \pi_k \in \mathfrak{S}_n$ and set $G = G(\pi_1, \dots, \pi_k)$. Furthermore, set $\rho(G) = \lambda(G)/2k$. Then*

$$\rho(G)^{2r} \leq \mathbb{E}_{2r}\left[|\mathrm{Fix}(w(\pi_1, \dots, \pi_k))|\right] - 1$$

*for all $r \in \mathbb{N}$.*

*Proof.* Given a $2k$-regular graph $G$ on $n$ vertices, set $P(G) = A(G)/2k$. Note that

$$\mathrm{tr}\left(P(G)^{2r}\right) = \frac{1}{(2k)^{2r}}\mathrm{tr}\left(A(G)^{2r}\right) = \frac{1}{(2k)^{2r}}\sum_{i=1}^{n}\lambda_i(G)^{2r} = 1 + \frac{1}{(2k)^{2r}}\sum_{i=2}^{n}\lambda_i(G)^{2r}$$

for all $r \in \mathbb{N}$. Recall that all eigenvalues $\lambda_i(G)$ are real. Since even powers of real numbers are positive, we obtain that

$$\rho(G)^{2r} \leq \mathrm{tr}\left(P(G)^{2r}\right) - 1.$$

Recall from Exercise 4.2(a) that $\left(A(G)^{2r}\right)_{ij}$ counts the number of walks from vertex $i$ to vertex $j$ in $2r$ steps. This means that $\mathrm{tr}\left(A(G)^{2r}\right)$ counts the number of closed walks of $2r$ steps. Because $(2k)^{2r}$ counts all walks of $2r$ steps, $\mathrm{tr}\left(P(G)^{2r}\right)$ can be interpreted probabilistically. Indeed we have

$$\mathrm{tr}\left(P(G)^{2r}\right) = \sum_{i=1}^{n} p_{i,2r},$$

where $p_{i,2r}$ is the probability that a random walk of $2r$ steps on $G$, starting at vertex $i$ ends at vertex $i$ again.

Now we use that our graphs are built out of permutations. We can think of the edges in $G(\pi_1, \dots, \pi_k)$ as being labeled by the permutations $\pi_i$ and their inverses $\pi_i^{-1}$. As such, the walks of length $2r$ on $G(\pi_1, \dots, \pi_k)$ correspond one to one to words in the $2k$ letters $\{\pi_1, \pi_1^{-1}, \dots, \pi_k, \pi_k^{-1}\}$. Furthermore, if

$$w(\pi_1, \dots, \pi_k) = \pi_{i_1}^{\varepsilon_1} \cdots \pi_{i_{2r}}^{\varepsilon_{2r}} \in \mathfrak{S}_n$$

is such a word of length $2r$ (so $\varepsilon_i \in \{\pm 1\}$), then the vertex we reach by starting at $i$ and tracing $w$ is given by $w(i)$. Because we are considering closed walks, we need to understand how often $w(i) = i$. In other words, we have

$$\mathrm{tr}\left(P(G)^{2r}\right) = \mathbb{E}_{2r}\left[|\mathrm{Fix}(w)|\right].$$

Putting this together with our upper estimate on $\rho(G)$ proves the lemma. $\square$

The lemma above translates the question of the expansion of a random graph into a question on random words of a given length in random permutations. As such, we will break the argument into two parts: first we consider the properties of a random word and then consider the number of fixed points of a word with this given structure.

We start with the properties of words. Let $w \in W_r$, we call $w = (w_1, \dots w_r)$ *reduced* if there is no $i \in \{1, \dots, r-1\}$ so that $w_i = w_{i+1}^{-1}$. Given a word that is not reduced, we can reduce it by successively removing all the pairs of consecutive letters that are each others inverses. The shorter word we obtain by doing this, will be called $\mathrm{red}(w)$.

We call a reduced word $w$ *bad* if there exist words $w_a$ and $w_b$ so that $w = w_a w_b^j w_a^{-1}$ for some $j \geq 2$.

**Lemma 6.2.** *Let $k \geq 2$ and $r \in \mathbb{N}$. We have*

$$\mathbb{P}_{2r}\left[\mathrm{red}(w) \text{ is bad or empty}\right] \leq \frac{r+1}{(k/2)^r}.$$

*Proof.* To count the number of words with bad reductions, we first count words in the three letters $\{(, ), *\}$. A word $w = w_1 \cdots w_{2r}$ in these letters is called *admissible* if the following conditions hold:

1. $w$ contains as many open as closed brackets:
$$\left|\{i;\ w_i = \text{ ( }\}\right| = \left|\{i;\ w_i = \text{ ) }\}\right|.$$
2. No bracket in $w$ is closed before it is opened: for any $i = 1, \dots, 2r$:
$$\left|\{j \leq i;\ w_j = \text{ ( }\}\right| \geq \left|\{j \leq i;\ w_j = \text{) }\}\right|.$$
3. Stars only appear when all brackets have been closed: if $w_i = *$ then
$$\left|\{j < i;\ w_j = \text{ ( }\}\right| = \left|\{j < i;\ w_j = \text{ ) }\}\right|.$$

For example, the word $(())() * * * *(())$ is admissible, whereas the words $((*))$ and $)($ are not.

Now suppose $w \in W^{2r}$. We obtain an admissible word in $\{(, ), *\}$ from a reduction of $w$ to $\mathrm{red}(w)$ as follows: place a $*$ in place of every letter that

remains and place a pair of brackets ( and ) for every pair of inverses that cancel against each other at some point in the reduction. For example, if

$$w = a_1 \cdot a_2^{-1} \cdot a_2 \cdot a_1^{-1} \cdot a_3 \cdot a_1$$

then a corresponding word in $\{(,), *\}$ is

$$(()) * *.$$

Note however that the word in $\{(,), *\}$ depends on the reduction. For instance, from different reductions of $a_1 \cdot a_2^{-1} \cdot a_2 \cdot a_1^{-1} \cdot a_1 \cdot a_3$, we obtain $(()) * *$ or $*()()*$.

Nonetheless, we can obtain all words $w \in W^{2r}$ that reduce to a word of length $2l$ by filling in admissible words in $\{(,), *\}$ with $2l$ stars (we just obtain some words multiple times). Note that the case $l = 0$ corresponds to words with an empty reduction.

To count the number of words with a bad reduction, our strategy will be to count the number of admissible words in $\{(,), *\}$ with the right number of stars and then count the number of ways to fill them in.

Note that if a word in $\{(,), *\}$ is admissible and has $2l$ stars, then the position of the $r - l$ open brackets determine the word entirely. Indeed, once the open brackets have been filled in, every remaining place needs to be either a closed bracket or a star. To fill these letters in, we read the open places from right to left. If a star is allowed, we put a star in that place, if not, we put in a closed bracket. As such, the number of admissible words of length $2r$ with $2l$ stars is

$$\binom{2r}{r-l}$$

All that remains is to bound the number of choices for the bad word we put in place of the stars and the pairs of letters we put in place of the brackets.

Let us start with the former. We need to build a word of length $2l$ of the form $w_a \cdot w_b^j w_a^{-1}$. Note that once the lengths of $w_a$ and $w_b$ are given, $j$ is determined. Furthermore, the length $l_b$ of $w_b$ satisfies

$$l_b \leq (2l - 2l_a)/2 = l - l_a$$

So we obtain that the number of bad words of length $2l$ is at most

$$\sum_{l_a=0}^{l}(2k)^{l-l_a}\cdot(2k)^{l_a}=(l+1)\cdot(2k)^l.$$

After this, we need to count how many ways there are to fill in the brackets. Once the letters corresponding to the open brackets have been chosen, the letters corresponding to the closed brackets are fixed. As such there are

$$(2k)^{r-l}$$

choices for this.

This means that the number of words with a bad or empty reduction can be bounded by

$$\sum_{l=0}^{r}\binom{2r}{r-l}(l+1)(2k)^r\leq(r+1)(2k)^r\sum_{l=0}^{r}\binom{2r}{r-l}\leq(r+1)2^{2r}\cdot(2k)^r.$$

Dividing by the total number of words of length $r$, we obtain the bound. □

Our next intermediate goal will be to bound the probability

$$\mathbb{P}_{n,k}^{\text{perm}}[w(\pi_1,\ldots,\pi_k)(1)=1]$$

for any fixed word $w\in W^s$ for some $s\leq 2k$.

We will control this probability using the following heuristic that goes through the word $w$ step by step (or letter by letter):

- Set $v_0=1$.
- Let $w_i$ denote the $i^{th}$ letter of $w$ (read from the right). Suppose $w_i(\pi_1,\ldots,\pi_k)=\pi_j^{\varepsilon}$
  - If $\pi_j^{\varepsilon}(v_{i-1})$ has not yet been chosen, randomly pick $\pi_j^{\varepsilon}(v_{i-1})$ (among the vertices that have not yet been assigned to the range of $\pi_j$) and set
    $$v_i=\pi_j^{\varepsilon}(v_{i-1}).$$
    In this case the $i^{th}$ step is called *free*.

- If $\pi_j^{\varepsilon}(v_{i-1})$ has already been chosen, set

$$v_i = \pi_j^{\varepsilon}(v_{i-1}).$$

In this case the $i^{th}$ step is called *forced*.

Note that

$$\mathbb{P}[v_s = 1] = \mathbb{P}_{n,k}^{\text{perm}}[w(\pi_1, \ldots, \pi_k)(1) = 1].$$

We claim:

**Lemma 6.3.** *Let $0 < s \leq 2r$ and let $w \in W^s$ be a good reduced word. Then*

$$\mathbb{P}_{n,k}^{\text{perm}}[w(\pi_1, \ldots, \pi_k)(1) = 1] \leq \frac{1}{n-2r} + \frac{16 \cdot r^4}{(n-2r)^2}.$$

*Proof.* Let us call the $i^{th}$ step in the process above a *coincidence* if it is free and moreover if $v_i$ is a vertex that has already been seen before.

Note that the fact that $w$ is reduced implies that if $w(\pi_1, \ldots, \pi_k)(1) = 1$ then at least one coincidence must occur. As such, we obtain the bound

$$\mathbb{P}_{n,k}^{\text{perm}}[w(1) = 1] \leq \mathbb{P}\left[\begin{matrix}\text{Exactly one coincidence} \\ \text{occurs and } v_s = 1\end{matrix}\right] + \mathbb{P}\left[\begin{matrix}\text{At least two} \\ \text{coincidences occur}\end{matrix}\right].$$

Let us denote the event that a coincidence occurs at step $i$ by $C_i$. Before the $i^{th}$ step there are at most $i$ vertices that have already been visited. Likewise, there are at least $n - i$ vertices that have not yet been assigned to the range of $\pi_j$. As such:

$$\mathbb{P}[C_i |\ v_0 = 1, \ldots, v_{i-1} = u_{i-1}] \leq \frac{i}{n-i} \leq \frac{2r}{n-2r}.$$

Note that this bound does not depend on the conditioning. Hence:

$$\begin{aligned}
\mathbb{P}\left[\begin{matrix}\text{At least two} \\ \text{coincidences occur}\end{matrix}\right] &\leq \sum_{1 \leq i < j \leq 2r} \mathbb{P}[C_i \text{ and } C_j] \\
&= \sum_{1 \leq i < j \leq 2r} \mathbb{P}[C_i]\, \mathbb{P}[C_j |\ C_i] \\
&\leq \sum_{1 \leq i < j \leq 2r} \frac{4 \cdot r^2}{(n-2r)^2} \\
&\leq \frac{16 \cdot r^4}{(n-2r)^2}. \qquad (6.1)
\end{aligned}$$

So, we need to show that

$$\mathbb{P}\begin{bmatrix}\text{Exactly one coincidence}\\ \text{occurs and } v_s = 1\end{bmatrix} \leq \frac{1}{n-2r}.$$

If $w(\pi_1, \ldots, \pi_k)(1) = 1$, then $w$ gives rise to a closed cycle in the graph $G(\pi_1, \ldots, \pi_k)$. If only one coincidence occurs, then this cycle must look like the cycle in Figure 6.1: a (possibly empty) "tail" starting at vertex 1 with a circuit attached to it. The coincidence happens at the vertex where the tail is attached ($v$ in the image), after which all the steps are forced.

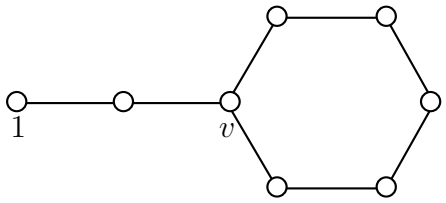


Figure 6.1: A cycle with a tail.

The word $w$ could run through this cycle in multiple ways: it can run through the circuit multiple times. However, we necessarily have $w = w_a w_b w_a^{-1}$, where $w_a$ corresponds to the tail and $w_b$ is non-empty, since $w$ is reduced. If the word were to run through the circuit multiple times, the word $w_b$ would be a power. This can't happen since we are assuming $w$ is good. Finally, we claim that the decomposition $w = w_a w_b w_a^{-1}$ is uniquely determined by $w$. Indeed, we claim $w_b$ (the word corresponding to the cycle) is not of the form $tw't^{-1}$ for any $t \in W$. Indeed, if this were the case, then the step where the coincidence is supposed to occur would be forced. This observation uniquely determines $w_b$ and hence also $w_a$.

Let $t_1$ be the step where the coincidence occurs. That is, $t_1$ is obtained by adding the number of letters of $w_a$ and $w_b$ together (again, this is fixed once $w$ is fixed). Likewise, let $t_0$ be the number of letters of $w_a$. So

$$v = v_{t_0}.$$

We need that step $t_1$ is free and that the vertex $v$ is chosen. We have

$$\mathbb{P}\begin{bmatrix}\text{Step } t_1 \text{ if free}\\ \text{and } v_{t_1} = v_{t_0}\end{bmatrix} \leq \frac{1}{n-t_1} \leq \frac{1}{n-2r}.$$

Note that the latter bound does not depend on when the coincidence occurs. So we obtain

$$\mathbb{P}\left[\begin{matrix}\text{Exactly one coincidence}\\ \text{occurs and } v_s = 1\end{matrix}\right] \leq \frac{1}{n-2r}. \tag{6.2}$$

Adding the bounds (6.1) and (6.2) together, we obtain the lemma. □

We are now ready to prove that random graphs are expander graphs:

**Theorem 6.4.** *[BS87] Fix $k \in \mathbb{N}$. We have*

$$\mathbb{E}_{n,k}^{\text{perm}}[\lambda(G)] \leq 2^{1/2} \cdot (2k)^{3/4} \cdot (1 + o(1))$$

*as $n \to \infty$.*

*Proof.* From Lemma 6.1 we obtain:

$$\mathbb{E}_{n,k}^{\text{perm}}[\rho(G)] \leq \mathbb{E}_{n,k}^{\text{perm}}[\rho(G)^{2r}]^{1/2r} \leq (\mathbb{E}_{n,k}^{\text{perm}}[\mathbb{E}_{2r}\left[|\text{Fix}(w(\pi_1, \ldots, \pi_k))|\right]] - 1)^{1/2r}$$

We have

$$\begin{aligned}
\mathbb{E}_{n,k}^{\text{perm}}[\mathbb{E}_{2r}\left[|\text{Fix}(w(\pi_1, \ldots, \pi_k))|\right]] &= \frac{\sum_{w \in W^{2r}} \sum_{\pi_1, \ldots, \pi_k \in \mathfrak{S}_n} |\text{Fix}(w(\pi_1, \ldots, \pi_k))|}{(2k)^{2r} \cdot (n!)^k} \\
&= \frac{1}{(2k)^{2r}} \sum_{w \in W^{2r}} \sum_{i=1}^{n} \mathbb{P}_{n,k}^{\text{perm}}[w(i) = i] \\
&= \frac{1}{(2k)^{2r}} \sum_{w \in W^{2r}} n \cdot \mathbb{P}_{n,k}^{\text{perm}}[w(1) = 1]
\end{aligned}$$

Using Lemma 6.3, we obtain

$$\begin{aligned}
\mathbb{E}_{n,k}^{\text{perm}}[\mathbb{E}_{2r}\left[|\text{Fix}(w(\pi_1, \ldots, \pi_k))|\right]] \leq\ & \frac{n}{n-2r} + \frac{16 \cdot r^4 \cdot n}{(n-2r)^2} \\
& + \mathbb{P}_{2r}[\text{red}(w) \text{ is bad or empty}].
\end{aligned}$$

Now we apply Lemma 6.2 and get

$$\mathbb{E}_{n,k}^{\text{perm}}[\mathbb{E}_{2r}\left[|\text{Fix}(w(\pi_1, \ldots, \pi_k))|\right]] \leq \frac{n}{n-2r} + \frac{16 \cdot r^4 \cdot n}{(n-2r)^2} + \frac{r+1}{(k/2)^r},$$

for all $n, r \in \mathbb{N}$. Now all we have to do is make a clever choice for $r$. $r(n) = 2\log_{k/2}(n)$ will do. We obtain

$$\mathbb{E}_{n,k}^{\mathrm{perm}}[\mathbb{E}_{2r}\left[|\mathrm{Fix}(w(\pi_1,\ldots,\pi_k))|\right]] - 1 = \frac{2r(n)}{n-2r(n)} + O(\log(n)^4/n)$$

So, if we plug this into our earlier bound, we get that there exists a constant $C > 0$ so that

$$\begin{aligned}
\mathbb{E}_{n,k}^{\mathrm{perm}}[\rho(G)] &\leq \left(\frac{C\log(n)^4}{n}\right)^{\frac{1}{4\log_{k/2}(n)}} \\
&= \exp\left(\frac{\log(n)+\log(C)+4\log(\log(n))}{4\log(n)}\log(k/2)\right) \\
&= \left(\frac{2}{k}\right)^{\frac{1}{4}-\frac{\log(C)+4\log(\log(n))}{4\log(n)}} \\
&= \left(\frac{2}{k}\right)^{\frac{1}{4}}\cdot(1+o(1)),
\end{aligned}$$

as $n \to \infty$.

This implies that

$$\mathbb{E}_{n,k}^{\mathrm{perm}}[\lambda(G)] = 2k\cdot\mathbb{E}_{n,k}^{\mathrm{perm}}[\rho(G)] = 2^{1/2}\cdot(2k)^{3/4}\cdot(1+o(1)),$$

as $n \to \infty$. □

Like we said before, this proves the existence of expander graphs:

**Corollary 6.5.** *Let $k \geq 3$. There exists a sequence $(G_n)_n$ of $2k$-regular graphs that forms an expander graph.*

*Proof.* For every $n \in \mathbb{N}$ there must be a set of permutations $\pi_1,\ldots,\pi_k \in \mathfrak{S}_n$ so that

$$\lambda(G(\pi_1,\ldots,\pi_k)) \leq \mathbb{E}_{n,k}^{\mathrm{perm}}[\lambda(G)] < 2k,$$

where we used $k \geq 3$ for the strict inequality. If we choose one such graph for every $n$, we obtain an expander sequence. □

## 6.2 Exercises

**Exercise 6.1.** *The diameter of an expander.* Given a connected graph $G$, the diameter of $G$ is given by:

$$\operatorname{diam}(G) = \sup\left\{\mathrm{d}\left(v, w\right);\ v, w \in V(G)\right\},$$

where $\mathrm{d}\left(v, w\right)$ denotes the distance between $v$ and $w$: the number of edges in the shortest path between $v$ and $w$. Moreover, given $v \in V(G)$ and $r \in \mathbb{N}$, let

$$B_r(v) = \{w \in V(G);\ \mathrm{d}\left(v, w\right) \leq r\}$$

denote the ball of radius $r$ around $v$.

(a) Let $k \geq 3$ and let $G$ be a connected $k$-regular graph on $n$ vertices. Furthermore suppose $G$ has at least one pair of vertices that do not share an edge. Show that

$$\operatorname{diam}(G) \geq \log_{k-1}(n) + \log(e/k).$$

*Hint: Use the fact that $B_{\operatorname{diam}(G)}(v)$ covers the whole graph $G$ for any $v \in V(G)$.*

(b) For every $k \geq 3$ give an example of a sequence of $k$-regular graphs $(G_n)_n$ so that $|V(G_n)| \to \infty$ as $n \to \infty$ and $\operatorname{diam}(G_n)$ is linear in $V(G_n)$.

(c) Let $k \geq 3$ and let $G$ be a connected $k$-regular graph on $n$ vertices. Show that

$$|B_r(v)| \geq \min\left\{\frac{n}{2}, \left(1 + \frac{h(G)}{k}\right)^r\right\}.$$

(d) Let $k \geq 3$ and let $G$ be a connected $k$-regular graph on $n$ vertices. Set $\beta = 1 + h(G)/k$. Show that

$$\operatorname{diam}(G) \leq 2\log_\beta(n) + 3$$

and conclude that if $(G_n)_n$ is an expander graph, then there exist a constant $C > 0$ (independent of $n$) so that

$$\frac{1}{C}\log(|V(G_n)|) \leq \operatorname{diam}(G_n) \leq C\log(|V(G_n)|)$$

for all $n \in \mathbb{N}$.

*Hint: Take two vertices $v, w \in G$ that realize the diameter and expand balls around them of a radius $r$ so that $|B_r(v)| \geq n/2$ and $|B_r(w)| \geq n/2$, where $r$ is the minimal radius with this property.*

**Exercise 6.2.** A simple random walk on a graph $G$ starting at $v \in V(G)$ is a sequence of random variables $X_r : \Omega \to V(G)$, $r \in \mathbb{N}$ with

$$X_0(\omega) = v$$

for all $\omega \in \Omega$ and

$$\mathbb{P}[X_{r+1} = v |\, X_r = w] = A(G)_{vw} / \deg(w),$$

where $A(G)$ is the adjacency matrix of $G$.

In what follows, fix $k \geq 3$ and let $G$ be a connected $k$-regular graph on vertices $\{1, \ldots, n\}$.

(a) Set $P(G) = A(G)/k$. Show that

$$\mathbb{P}[X_r = i |\, X_0 = j] = \left(P(G)^r\right)_{ij}.$$

(b) Show that

$$\left| \left(P(G)^r\right)_{ij} - \frac{1}{n} \right| \leq \left(\frac{\lambda(G)}{k}\right)^r \cdot (n-1).$$

(c) Fix $j \in \{1, \ldots, n\}$ and let $\mathbb{P}^{\star r} : \mathcal{P}(V(G)) \to [0,1]$ be the probability measure on $V(G)$ given by:

$$\mathbb{P}^{\star r}[S] = \mathbb{P}[X_r \in S |\, X_0 = j]$$

for all $S \subset V(G)$. Furthermore, let $\mathbb{U} : \mathcal{P}(V(G)) \to [0,1]$ denote the uniform probability measure on $V(G)$. That is:

$$\mathbb{U}[S] = |S| / n$$

for all $S \subset V(G)$. Show that

$$\mathrm{d_{TV}}\left(\mathbb{P}^{\star r}, \mathbb{U}\right) \leq \frac{n \cdot (n-1)}{2} \left(\frac{\lambda(G)}{k}\right)^r.$$

*Hint: Use Exercise 2.1(a).*

# Bibliography

[BS87] A. Broder and E. Shamir. On the second eigenvalue of random regular graphs. In *The 28th Annual Symposium on Foundations of Computer Science*, pages 286–294. 1987.