

Class 18: Agenda and Questions

1 Warm-Up

Group Work

Suppose that X is a k -source on $\{0, 1\}^n$. Let $N = 2^n$. Let $\sigma \in \mathbb{R}^N$ be the “vectorized” version of the pmf of X . That is, $\sigma_i = \Pr[X = i] \quad \forall i \in \{0, \dots, N - 1\}$, where we associate a number $i < N$ with its binary expansion in $\{0, 1\}^n$.

1. Why is $\|\sigma\|_\infty \leq 2^{-k}$?
2. Argue that $\|\sigma\|_2 \leq 2^{-k/2}$.

Hint: Use the fact that for any vector x , $\|x\|_2^2 \leq \|x\|_\infty \|x\|_1$ (why is this true?).

2 Questions?

Questions from the minilectures, quiz, warm-up? (Expanders, extractors?)

3 Recap

Recall the definition of a (k, ε) -extractor:

Definition 1. A function $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is a (k, ε) extractor if, for all k -sources X on $\{0, 1\}^n$, $\|\text{Ext}(X, U_d) - U_m\| \leq \varepsilon$.

Above, $\|\cdot\|$ is the total variation distance, and U_d refers to the uniform distribution on d bits. Suppose that $G = (V, E)$ is an (undirected, unweighted) degree- D expander graph with $|V| = N$, and with expansion parameters $\lambda(G) \leq 1/2$. Recall that $\lambda(G) = \max\{\lambda_2, |\lambda_N|\}$, where $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_N$ are the eigenvalues of A , where A is the *normalized adjacency matrix* of G . (aka, A_{ij} is $1/D$ if $\{i, j\} \in E$ and is zero otherwise).

4 Extractors *from* expanders

Some slides illustrating a construction of an extractor. A description is below for reference.

Let $\varepsilon > 0$. Let $N = 2^n$ and fix a bijection between $\{0, 1\}^n$ and V , where V is the vertex set of G above. Fix any $k \leq n$. Let $d = \log(D) \cdot \ell$, where $\ell = (n - k)/2 + \log(1/\varepsilon)$. Consider the following function $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^n$. On input $x, s \in \{0, 1\}^n \times \{0, 1\}^d$:

- Treat $x \in \{0, 1\}^n$ as an element of V .
- Treat $s \in \{0, 1\}^d$ as a string of ℓ numbers in $\{0, 1, \dots, D\}$. (That is, break up s into ℓ chunks, each $\log(D)$ bits long). Say these numbers are a_1, a_2, \dots, a_ℓ .
- Consider the following walk on G : let $x^{(0)} = x$. For $i = 1, 2, \dots, \ell$, get from $x^{(i-1)}$ to $x^{(i)}$ by choosing the a_i 'th neighbor of $x^{(i-1)}$.
- Output $x^{(\ell)} \in V$, which we treat as an element of $\{0, 1\}^n$.

5 Group work: this is a good extractor!

In this section, you'll show that Ext is a (k, ε) extractor.

Group Work

1. Let σ be the “vectorized” pmf of X (as in the warm-up). Explain why the distribution of $\text{Ext}(X, U_d)$ is given by $A^\ell \cdot \sigma$. (Recall that A is the normalized adjacency matrix of G).
2. Let $\pi = \frac{1}{N}\mathbf{1}$ be the vector that corresponds to the uniform distribution. Explain why

$$\|U_n - \text{Ext}(X, U_d)\| = \|\pi - A^\ell \cdot \sigma\| \leq \frac{\sqrt{N}}{2} \lambda(G)^\ell \|\pi - \sigma\|_2.$$

Hint: Mimic a computation that we did in the Expanders minilecture to show that random walks mix quickly when $\lambda(G)$ is small.

3. Argue that $\|\pi - \sigma\|_2 \leq 2 \cdot 2^{-k/2}$.

Hint: To get started, note that $\|\pi - \sigma\|_2 \leq \|\pi\|_2 + \|\sigma\|_2$ by the triangle inequality.

4. Assume that G is a good enough expander that $\lambda(G) \leq 1/2$. (It turns out that these exist for large enough degrees D). Conclude that $\|U_n - \text{Ext}(X, U_d)\| \leq \varepsilon$ and thus Ext is a (k, ε) extractor.