CS 6815: Lecture 24

Instructor: Eshan Chattopadhyay Scribes: William Gao, Lucy Li

November 20, 2018

1 Lossless Condensers

Definition 1.1. *We define* $\phi_V(G,k) = \frac{1}{k} \cdot \min_{S \subseteq [V]} \{|\Gamma(S) \setminus S| \colon |S| = k\}$

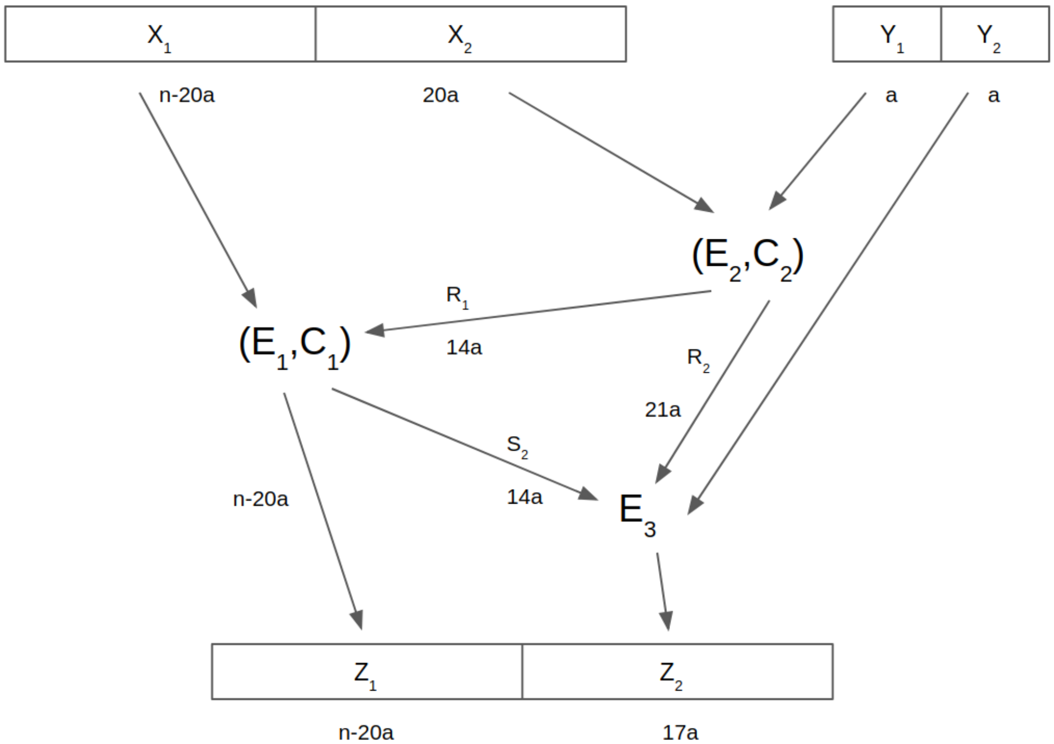
1. For a random $(n, d)-$graph,
$$\phi_V(G, \varepsilon_n) \geq d - 2.01$$

2. [3] For a Ramanujan expander (the best possible spectral expander),
$$\phi_V(G, \varepsilon_n) \approx \frac{d}{2}$$

Consider a $(k_{max}, \varepsilon)-$lossless vertex expander that is a bipartite graph with N nodes on the left and M nodes on the right, where each of the left nodes has degree D. Then we can say that if a subset S of nodes on the left side has $|S| \leq k_{max}$, then $|\Gamma(S)| \geq (1-\varepsilon) \cdot |S| \cdot D$.

We can build a $(k_{max} \leq N, \varepsilon)$-lossless expander on (N, M, D)-bipartite graphs (N is number of nodes on the left, M is the number of nodes on the right, and D is the left degree), for $M \leq D^2 \cdot k_{max}^{1+\alpha}$, $D = \textbf{poly}(\log N, \frac{1}{\varepsilon}, \frac{1}{\alpha})$ [2].

Theorem 1.2. *$\forall \varepsilon > 0$, for $M = \Theta(N), D = O_\varepsilon(1)$, there exist D-regular (N, M)-bipartite expanders with are $(\Omega(\frac{M}{D}), \varepsilon)$-lossless. [1]*



The ingredients to the construction for the above theorem as shown by the diagram are as follows:

1. A Permutation Conductor $(E_1, C_1) : \{0,1\}^{n-20} \times \{0,1\}^{14a} \to \{0,1\}^{n-20a} \times \{0,1\}^{14a}$
   (a) (E_1, C_1) is a permutation
   (b) For any $k \leq n - 30a$, if X is an $(n - 20a, k)$ source, $E_1(X, U_{14a})$ is $\varepsilon-$close to $(n - 20a, k + 6a)$ source.
2. $(E_2, C_2) : \{0,1\}^{20a} \times \{0,1\}^{a} \to \{0,1\}^{14a} \times \{0,1\}^{21a}$. For $k_1 \leq 14a$, if Y is a $(20a, k_1)$ source
   (a) $E_2(Y, U_a)$ is $\varepsilon-$close to a $(14a, k_1)-$source.
   (b) (E_2, C_2) is lossless. $(E_2, C_2)(Y, U_a)$ is $\varepsilon-$close to a $(35a, k_1 + a)$ source.
3. $E_3 : \{0,1\}^{35a} \times \{0,1\}^{a} \to \{0,1\}^{17a}$ is lossless up to $15a$ entropy.

We note that E_2 and E_3 exist due to the probabilistic method.

Claim 1.3. *The constructed function $\{0,1\}^n \times \{0,1\}^{2a} \to \{0,1\}^{n-17a}$ is lossless up to $n - 30a$. This means that if we start with a source X with entropy $k \leq n - 30a$, then the output will be ε-close to a source with entropy $k + 2a$.*

Proof. Case (i): $\forall x_1 \in \mathrm{Supp}(X_1), H_\infty(X_2 \mid X_1 = x_1) \geq 14a$.
In this case, we observe that since R_1 is ε-close to uniform and $H_\infty(X_1) \geq k - 20a$, we can conclude that $H_{\infty,\varepsilon}(Z_1) \geq k - 14a$.

Case (ii): $\forall x_1 \in \mathrm{Supp}(X_1), H_\infty(X_2 \mid X_1 = x_1) < 14a$.
In this case, we know that $H_\infty(X_1) \geq k - 14a$, $H_\infty(R_1) = H_\infty(X_2)$, and $H_\infty(X_1, R_1) = k$. Then, because (E_1, C_1) is a permutation, since the input contains k bits of entropy, so does the output. From these two cases, we can conclude that

$$H_{\infty,\varepsilon}(Z_1) \geq k - 14a$$

Next, we know that $H_\infty(Z_1, S_2, R_2) = k + a$, since (E_2, C_2) and (E_1, C_1) are lossless. This means that for all z_1,

$$H_{\infty,\varepsilon}(S_2, R_2 \mid Z_1 = z_1) \leq 15a.$$

E_3 is lossless up to $15a$ bits of entropy, so

$$H_{\infty,\varepsilon}(Z_2 \mid Z_1 = z_1) = H_{\infty,\varepsilon}(S_2, R_2 \mid Z_1 = z_1) + a.$$

Finally,

$$H_{\infty,\varepsilon}(Z_1, Z_2) = H_{\infty,\varepsilon}(Z_1, R_2, S_2) + a = k + 2a.$$

$\square$

References

[1] M Capalbo, O Reingold, S Vadhan, and A Wigderson. Randomness conductors and constant degree expansions beyond the degree 2 barrier. In *Proc. ACM STOC*, pages 659–668, 2002.

[2] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from parvaresh–vardy codes. *Journal of the ACM (JACM)*, 56(4):20, 2009.

[3] Nabil Kahale. Eigenvalues and expansion of regular graphs. *Journal of the ACM (JACM)*, 42(5):1091–1106, 1995.