CS 6815 Pseudorandomness and Combinatorial Constructions **Fall 2019**

Lecture 17: October 29

Lecturer: Eshan Chattopadhyay *Scribe: Renee Mirka*

17.1 Introduction

Today's lecture discusses explicit vertex expanders from list-decodable codes and introduces Parvaresh-Vardy codes.

17.2 Vertex Expanders

Recall a D-left regular bipartite graph G is a (K, A)-*bipartite vertex expander* with parts L and R ($|L| = N, |R| = M$) if $\forall S \subset L$ with $|S| = K, |\Gamma(S)| \geq AK$.

We know there are probabilistic bounds for these sizes, namely $A = (1-\epsilon)D, D = O(\frac{log(N/M)}{\epsilon})$, and $M = O(\frac{KD}{\epsilon})$. Furthermore, spectral methods do not go beyond $A \sim D/2$ or $M << N$ achieving $D \sim log(N)$.

Note: our discussion will focus on unbalanced expanders (lots of nodes on the left and few on the right).

17.3 Graphs from Codes and List View of Expanders

Given a (ρ, W)-list decodable code $\mathcal{C} : [N] \to [M]^D$, we can construct a corresponding bipartite graph in the following way. Let $L = [N]$ and $R = M \times [D]$. Then, for $x \in L$, we add an edge from x to $(i, \mathcal{C}(x)_i)$ for $1 \leq i \leq D$. In other words, $\Gamma(x) = \{(i, \mathcal{C}(x)_i) : i \in [D]\}$. Notice that this graph is left D-regular. See the figure below for an illustration.

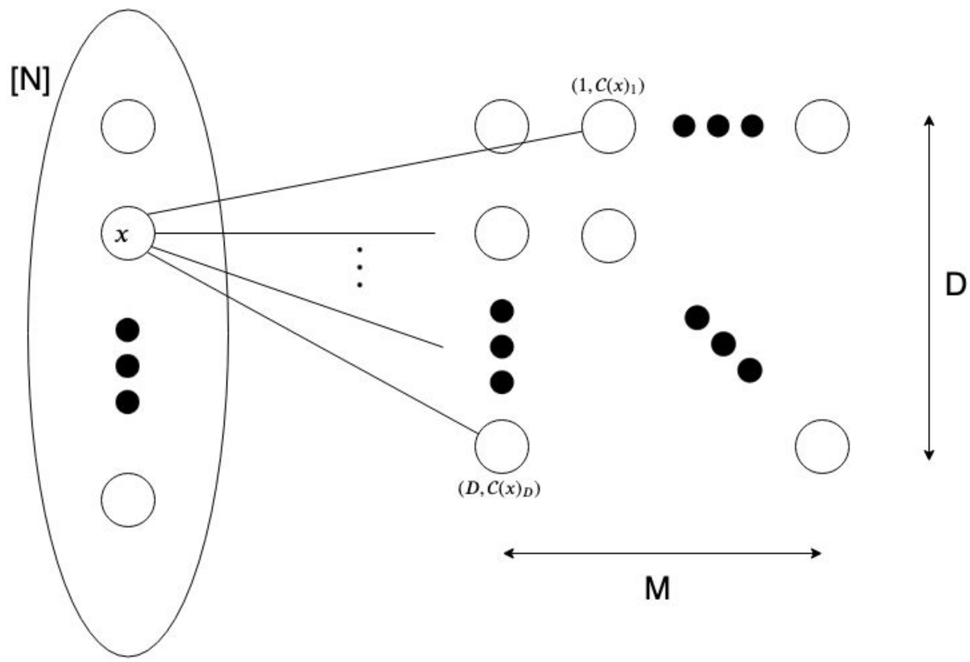
We can also consider the list view of expanders. For any $T \subset R$, define $List(T) = \{x \in L : \Gamma(x) \subset T\}$. Similarly, for $\epsilon > 0$, $List(T, \epsilon) = \{x \in L : |\Gamma(x) \cap T| \geq \epsilon D\}$. Note: $List(T) = List(T, 1)$.

Claim 17.1 *Let $\lambda = (\lambda_1, \dots, \lambda_D)$ be a received corrupted word. If $T_\lambda = \{(i, \lambda_i) : i \in [D]\}$, then $|List(T_\lambda, \rho)| \leq W$.*

Proof: If $x \in List(T_\lambda, \rho)$, that means $\Delta(\mathcal{C}(x), \lambda) \leq (1-\rho)D$. Since $\mathcal{C}$ is (ρ, W)-list decodable, there are at most W such x's. ■

Remark: in general, we can't say much about *List*.

On the other hand, G is a (K, A) D-regular bipartite vertex expander $\iff$ for any $T \subset R, |T| \leq AK - 1, |List(T)| \leq K - 1$. (Observe that the latter is simply the contrapositive of the former.)



*We need to bound $List(T, 1)$ for all "small" Ts but LD codes bound "structured" Ts.
*For expanders, we really care about exact size of $List(T, 1)$ (even constants matter!!). But for list decodable codes, exact size of $List$ does not matter.

17.4 Parvaresh-Vardy Codes

Fix a finite field $\mathbb{F}_q$ and message space $f \in Poly_{\leq n-1}$ [univariate polynomials over $\mathbb{F}_q$ with degree $\leq n-1$]. The encoding will map messages from $\mathbb{F}_q^n$ to $\mathbb{F}_{q^m}^q$ with $\mathcal{C} \subset \Sigma^q, |\Sigma| = q^m = |\mathbb{F}_{q^m}|$. Intuitively, we're taking a polynomial f and sending it to a set of polynomials $f_1, \ldots, f_m$ and evaluating each f_i at all points in $\mathbb{F}_q$.

Let $E(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$. Consider the extension field $F = \mathbb{F}_q[x]/E(x)$. Think of $f \in F$ and compute $f_i = (f)^{h^i}$, $i = 0, 1, \ldots, m-1$ (note h is not yet set). Also, note $f_0 = f$, and we can think of each $f_i \in Poly_{\leq n-1}$.

Then, the list-decoding radius of PV code (with appropriate choice of parameters) is $1 - r^{2/3}$ (where r is the relative rate). Recall for RS it's $1 - r^{1/2}$.

We can now consider the graph G from the PV code. We have $L = \mathbb{F}_q^n =_{\leq n-1}$ and $\Gamma(f, y) = [y, f_0(y), \ldots f_{m-1}(y)]$ where $f \in Poly_{\leq n-1}$ and $y \in \mathbb{F}_q$. Note that G is a q-left regular graph.

Theorem 17.2 *G is a $(K = h^m, A = q - (n-1)(h-1)m)$ vertex expander.*

We will see the proof next class.

The takeaway is that we can construct a highly-unbalanced graph with near-optimal expansion.

If we're given $N, K, \epsilon, \alpha > 1$, then we define $n = log_2(N), k = log_2(K), h = (nk/\epsilon)^{1/\alpha}, q \in (h^{1+\alpha}, 2h^{1+\alpha})$ a power of 2, and $m = log_h(K)$. Then, $|L| = q^n \geq N, |R| = q^{m+1} \leq q^2 K^{1+\alpha}, D = q \leq O(\frac{log(N)log(K)}{\epsilon})^{1+1/\alpha}$ and $A \geq (1-\epsilon)q$.