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

Lecture 18: October 31

Lecturer: Eshan Chattopadhyay *Scribe: Abhishek Shetty*

18.1 Explicit Expanders from Parvaresh-Vardy Codes

In this lecture, we will show that the graph G constructed from the Parvaresh–Vardy codes are unbalanced vertex expanders.

Theorem 18.1 *G is $\left(K = h^m, A = q - (n-1)(h-1)m\right)$ vertex expander.*

Proof: Let $T \subseteq \mathbb{F}_q^{m+1}$ be a subset of the right vertices such that $|T| \leq AK - 1$. Let $S = \text{List}(T) = \{f_0 : \Gamma(f_0) \subseteq T\}$. We would like to show that $|S| \leq K - 1$. To do this, we use the polynomial method.

First, we construct a polynomial Q that vanishes on T. To this end, consider polynomials $Q(Y, Y_1, \dots Y_m)$ whose only non-zero coefficients are on monomials of the form $Y^i M_j(Y_1, \dots, Y_m)$ for $0 \leq i \leq A-1$ and $0 \leq j \leq K-1$. Here, $M_j(Y_1, \dots Y_m) = \prod_{l=1}^{m} Y_l^{j_{l-1}}$ where $j = \sum_{l=0}^{m-1} j_l h^l$ is the base-h representation of j. Requiring Q to vanish on T gives us a system of $AK-1$ equations in AK unknowns. Thus, we have a non-trivial set of solutions, from which we pick the one with the smallest Y degree. Note that this implies that if we write Q as

$$Q(Y, Y_1, \dots, Y_m) = \sum_{j=0}^{K-1} p_j(Y) M_j(Y_1, \dots Y_m)$$

where $p_i(Y)$ are univariate, at least one of the p_i's are non-zero mod $E(Y)$. Here E is the irreducible polynomial used in the construction of the Parvaresh–Vardy code.

Next, consider the $F(Y) \in S$. It is easy to see that, for all $y \in \mathbb{F}_q$

$$Q\left(y, f_0(y), \dots, f_{m-1}(y)\right) = 0$$

where $f_i = f^{h^i} \mod E$. This shows that $Q\left(y, f_0(y), \dots, f_{m-1}(y)\right)$ which is a univariate polynomial in y of degree at most $A - 1 + (n-1)(h-1)m$, has q roots. Since we assumed that $A - 1 + (n-1)(h-1)m < q$, we get that $Q\left(y, f_0(y), \dots, f_{m-1}(y)\right) \equiv 0$.

Now, we think of $f(Y)$ as an element of $\mathbb{F} = \mathbb{F}_q[Y]/E(Y)$. Thus, $f(Y)$ is a root of the polynomial $P(z)$ over $\mathbb{F}$ given by

$$\begin{aligned} P(z) &= Q\left(Y, z, z^h, \dots z^{h^{m-1}}\right) \mod E(Y) \\ &= \sum_{j=0}^{K-1} \left(p_j(Y) \mod E(Y)\right) z^j. \end{aligned}$$

As we noted earlier that this polynomial is non-zero. Since every $f(Y) \in S$ is a root of P, we have that $|S| \leq \deg(P) \leq K - 1$ as required. ■

Recall that given N, K, $\epsilon > 0$ and $\alpha > 1$, we can set $h = \left({}^{\log N \log K}/_{\epsilon}\right)^{1/\alpha}$, q to be power of 2 in $\left(h^{1+\alpha}, 2h^{1+\alpha}\right)$ and $m = \log_h(K)$, to get $|L| = q^n > N$, $|R| \leq q^{m+1} < q^2 K^{1+\alpha}$, $D \leq q \leq O\left(\frac{\log N \log K}{\epsilon}\right)^{1+1/\alpha}$ and $A \geq (1-\epsilon)q$.

18.2 Two-source Extractors

Given the definition of seeded extractors, it is natural to ask whether we get any gaurentees if the seed was not entirely uniform. One can show the following lemma about sources that are deficient.

Lemma 18.2 *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a* (k, ϵ) *strong seeded extractor. Then,*

$$d_{TV}\left(\left(Y, \mathrm{Ext}\left(X, Y\right)\right), \left(Y, U_m\right)\right) \leq \epsilon 2^{\lambda},$$

for every (n, k) *source* X *and* $(d, d - \lambda)$ *source* Y*.*

For further discussion on this, see [Raz06]. This discussion on weak seeds further motivates the following question: Can one extract randomness from two independent weak sources of randomness? This leads to the definition of two-source extractors.

Definition 18.3 (Two-Source Extractors) *A function* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ *is said to be a* (k_1, k_2, ϵ) *two-source extractor if for every* (n, k_1) *source* X *and* (n, k_2) *source* Y*, we have*

$$d_{TV}\left(\mathrm{Ext}\left(X, Y\right), U_m\right) \leq \epsilon.$$

18.2.1 Graph view of Two-Source Extractors

There is a natural way to view a function $f : [N] \times [M] \to \{0,1\}$ as a bipartite graph G_f with the left vertices corresponding to $[N]$ and the right vertices corresponding to $[M]$. Given a pair $(x, y) \in [N] \times [M]$, G_f has an edge between x and y if and only if $f(x, y) = 1$. With this construction in hand, we can interpret two source extractors as bipartite graphs. First, consider the following property that is well-studied in extremal graph theory.

Definition 18.4 (Bipartite k-Ramsey Graphs) *A graph bipartite* G *is said to be a bipartite* k*-Ramsey graph if it does not contain any* $K \times K$ *complete bipartite subgraph or any* $K \times K$ *independent set.*

Given this definition, we note that two-source extractors with constant error gives us bipartite Ramsey graphs. This can be seen by observing that flat k sources correspond to 2^k subsets and extractor property gaurentees that roughly half of the possible edges between subsets are present in the graph.

Lemma 18.5 *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *be a* $(k, k, 0.1)$ *two-source extractor. Then,* G_{Ext} *is a bipartite* 2^k*-Ramsey graph on* $2^n \times 2^n$ *nodes.*

18.2.2 Existence and Constructions of Two-Source Extractors

As with seeded extractors, we can use the probabilistic method to show that two-source extractors do indeed exist.

Theorem 18.6 (Existence of Two-source Extractors) *There exist* $\left(O\left(\log n\right), O\left(\log n\right), O\left(1\right)\right)$ *two-source extractors for output length* $m = 1$*.*

Proof: Consider a random function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Let X, Y be flat k-sources. We say that f is bad for X, Y if

$$\left| \Pr_{X,Y} \left[f\left(X, Y\right) = 1 \right] - 0.5 \right| \geq \epsilon.$$

Note that

$$\Pr_{X,Y} \left[f\left(X, Y\right) = 1 \right] = \frac{1}{k_1 k_2} \sum_{x,y} f\left(x, y\right).$$

Since f is a random function, each $f(x, y)$ is an independent Bernoulli random variable. Using the Chernoff bound, we get

$$\Pr_{f} \left[f \text{ is bad for } X, Y \right] \leq 2^{-\Omega\left(\epsilon^2 k_1 k_2\right)}.$$

Taking the union bound over all flat sources X and Y, we get

$$\Pr_{f} \left[\exists X, Y \text{ such that } f \text{ is bad for } X, Y \right] \leq \binom{n}{k_1}\binom{n}{k_2} 2^{-\Omega\left(\epsilon^2 k_1 k_2\right)}.$$

Using the Stirling approximation for the binomial coefficients, we get

$$\Pr_{f} \left[\exists X, Y \text{ such that } f \text{ is bad for } X, Y \right] \leq \left(\frac{ne}{k_1}\right)^{k_1} \left(\frac{ne}{k_2}\right)^{k_2} 2^{-\Omega\left(\epsilon^2 k_1 k_2\right)}.$$

Setting $k_1 = k_2 = O\left(\log n\right)$ and $\epsilon = O\left(1\right)$, we get the probability to be less than one as required. ■

With a bit more care, one can show that we can show that, we can pick $k_1 = k_2 = \log n - 2\log\epsilon + 1$. Next, we show a simple construction of an explicit two-source extractor. To do this, we define the inner product function $\mathrm{IP} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ to be $\mathrm{IP}\left(x, y\right) = \langle x, y \rangle$ where the inner product is taken over $\mathbb{F}_2$. In the next class, we will show that the inner product function is an extractor for sources with more than half the total possible entropy.

Theorem 18.7 *For every $\delta > 0$, $\mathrm{IP} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is a $\left(\left(1/2 + \delta\right) n, \left(1/2 + \delta\right) n, 2^{-\Omega(n)}\right)$ two-source extractor.*

References

[Raz06] R. Raz, Extractors with Weak Random Seeds, *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing* (2006), pp. 11–20.