CS225: Pseudorandomness Prof. Salil Vadhan

Lecture 16: List-Decodable Codes vs. Extractors & Expanders

April 12, 2007

Based on scribe notes by xxxx.

Previously, we have seen close connections between expanders and extractors (and related objects, such as condensers). In this lecture, we will see how these objects are also closely related to list-decodable codes, by presenting all of them in a single, list-decoding-like framework.

1 List-decoding views of expanders and extractors

We consider a code $\mathrm{Enc} : [N] \to [M]^D$ as corresponding *syntactically* to an extractor $\mathrm{Ext} : [N] \times [D] \to [D] \times [M]$ and an expander with neighbor function $\Gamma : [N] \times [D] \to [D] \times [M]$, via the correspondence:

$$\mathrm{Ext}(x, y) = \Gamma(x, y) = (y, \mathcal{C}(x)_y).$$

Note that this yields extractors and expanders with output/right-hand-side $[D] \times [M]$ and where the first component equals the seed/edge-label. (Recall that for such an extractor Ext, the second component is called a *strong* extractor.) Conversely, any such extractor or expander yields a code Enc.

For a subset $T \subseteq [D] \times [M]$ and $\varepsilon \in [0, 1]$, we define

$$\begin{aligned} \mathrm{LIST}(T, \varepsilon) &\stackrel{\mathrm{def}}{=} \{x : \Pr_y[(y, \mathrm{Enc}(x)_y) \in T] \geq \varepsilon\} \\ &= \{x : \Pr_y[\mathrm{Ext}(x, y) \in T] \geq \varepsilon\} \\ &= \{x : \Pr_y[\Gamma(x, y) \in T] \geq \varepsilon\} \end{aligned}$$

We can formulate the standard list-decoding property of codes in this language as follows:

Lemma 1 $\mathrm{Enc} : [N] \to [M]^D$ *is* $(1 - 1/M - \varepsilon, K)$ *list-decodable iff for every* $r \in [M]^D$*, we have*

$$|\mathrm{LIST}(T_r, 1/M + \varepsilon)| \leq K,$$

where $T_r = \{(y, r_y) : y \in [D]\}$.

Now let's look at extractors.

Lemma 2 *If* $\mathrm{Ext} : [N] \times [D] \to [M]$ *is a* (k, ε) *extractor then for every* $T \subseteq [D] \times [M]$*, we have*

$$|\mathrm{LIST}(T, \mu(T) + \varepsilon)| < K, \tag{1}$$

where $K = 2^k$.

Conversely, if (1) holds for every $T \subseteq [D] \times [M]$*, then* Ext *is a* $(k + \log(1/\varepsilon), 2\varepsilon)$ *extractor.*

This lemma says that the extractor property is equivalent to a "list-decoding-like property," up to a factor of 2 in the error ε and an extra additive entropy loss of $\log(1/\varepsilon)$ (both of which are usually considered insignificant).

Let's compare this to the standard list-decoding property of codes as formulated in Lemma 1. Note that the only difference between the condition in Lemma 1 and the one in Lemma 2 is that in the former, we restrict to sets T of the form T_r. That is, we restrict to sets $T \subseteq [D] \times [M]$ that contain exactly one element of the form $(y, \cdot)$ for each y.

Corollary 3 *If* $\mathrm{Ext} : [N]\times[D] \to [D]\times[M]$ *is a* (k, ε) *extractor (satisfying* $\mathrm{Ext}(x, y) = (y, \mathrm{Ext}'(x, y))$*), then the corresponding code* Enc *is* $(1 - 1/M - \varepsilon, K)$ *list-decodable.*

A converse holds when the alphabet size is small.

Proposition 4 *If* $\mathrm{Enc} : [N] \to [M]^D$ *is* $(1 - 1/M - \varepsilon, K)$ *list-decodable, then the corresponding function* $\mathrm{Ext} : [N] \times [D] \to [D] \times [M]$ *given by* $\mathrm{Ext}(x, y) = (y, \mathrm{Enc}(x)_y)$ *is a* $(k + \log(1/\varepsilon), M \cdot \varepsilon)$ *extractor. extractor.*

Proof: Let X be a k-source. Then the statistical difference between $\mathrm{Ext}(X, U_{[D]})$ and $U_{[D]} \times U_{[M]}$ equals

$$\begin{aligned}
\Delta(\mathrm{Ext}(X, U_{[D]}), U_{[D]} \times U_{[M]}) &= \mathop{\mathrm{E}}_{y \stackrel{\mathrm{R}}{\leftarrow} Y} \left[\Delta(\mathrm{Enc}(X)_y, U_{[M]})\right] \\
&\leq \frac{M}{2} \mathop{\mathrm{E}}_{y \stackrel{\mathrm{R}}{\leftarrow} Y} \left[\max_z \Pr[\mathrm{Enc}(X)_y = z] - 1/M\right]
\end{aligned}$$

where the last inequality follows from the ℓ_1 formulation of statistical difference.

So if we define $r \in [M]^D$ by setting r_y to be the value z maximizing $\Pr[\mathrm{Enc}(X)_y = z] - 1/M$, we have:

$$\begin{aligned}
\Delta(\mathrm{Ext}(X, U_{[D]}), U_{[D]} \times U_{[M]}) &\leq \frac{M}{2} \cdot (\Pr[(Y, \mathrm{Enc}(X)_Y) \in T_r] - 1/M), \\
&\leq \frac{M}{2} \cdot (\Pr[X \in \mathrm{LIST}(T_r, 1/M + \varepsilon)] + \varepsilon) \\
&\leq \frac{M}{2} \cdot \left(2^{-(k+\log(1/\varepsilon)} \cdot K + \varepsilon\right) \\
&\leq M \cdot \varepsilon.
\end{aligned}$$

■

Thus, the quantitative relationship between extractors and list-decodable codes deteriorates extremely fast as the output length/alphabet size increases. Nevertheless, the list-decoding view of extractors as given in Lemma **??** turns out to be quite useful (as we will see later in the course).

For expanders, the list-decoding view is quite simple to state and prove.

Lemma 5 $\Gamma : [N] \times [D] \to [D] \times [M]$ *is an* $(= K, A)$ *expander iff for every set* $T \subseteq [D] \times [M]$ *such that* $|T| < KA$*, we have:*

$$|\mathrm{LIST}(T, 1)| < K.$$

On one hand, this list-decoding property seems easier to establish than the ones for codes and extractors because we look at $\mathrm{LIST}(T, 1)$ instead of $\mathrm{LIST}(T, \mu(T) + \varepsilon)$. On the other hand, to get expansion (i.e. $A > 1$), we require a very tight relationship between $|T|$ and $|\mathrm{LIST}(T, 1)|$. In the setting of extractors or codes, we would not care much about a factor of 2 loss in $|\mathrm{LIST}(T)|$, as this corresponds to 1 bit of entropy loss for extractors or just a slightly larger list size for codes. But here it corresponds to a factor 2 loss in expansion, which can be quite significant. In particular, we cannot afford it if we are trying to get $A = (1 - \varepsilon) \cdot D$, as we will be in the next section.

2 Expanders from Parvaresh–Vardy Codes

Consider the bipartite multigraph obtained from the Parvaresh–Vardy codes via the above correspondence. That is, we define $\Gamma : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q \times \mathbb{F}_q^m$

$$\Gamma(f, y) = [y, f_0(y), f_1(y), \ldots, f_{m-1}(y)], \tag{2}$$

where $f(Y)$ is a polynomial of degree at most $n - 1$ over $\mathbb{F}_q$, and we define $f_i(Y) = f(Y)^{h^i} \bmod E(Y)$, where E is a fixed irreducible polynomial of degree n over $\mathbb{F}_q$. (Note that we are using $n - 1$ instead of d to denote degree of f.)

Theorem 6 *The graph $\Gamma : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q^{m+1}$ defined above is a (K_{max}, A) expander for $K_{max} = h^m$ and $A = q - nhm$.*

Proof: Let K be any integer less than or equal to $K_{max} = h^m$, and let $A = q - nmh$. By Lemma 5, it suffices to show that for every set $T \subseteq \mathbb{F}_q^{m+1}$ of size at most $AK - 1$, we have $|\mathrm{LIST}(T)| \le K - 1$. We begin by doing the proof for $K = K_{max} = h^m$, and later describe the modifications to handle smaller values of K. The proof goes along the same lines as the list-decoding algorithm for the Parvaresh–Vardy codes from last lecture.

Step 1: Find a low-degree Q vanishing on T. We find a nonzero polynomial $Q(Y, Z_0, \ldots, Z_{m-1})$ of degree at most $d_Y = A - 1$ in its first variable Y and at most $h - 1$ in each of the remaining variables such that $Q(z) = 0$ for all $z \in T$. (Compare this to $Q(r, r(y)) = 0$ for all $y \in \mathbb{F}_q$ in the list-decoding algorithm, which corresponds to taking $T = T_r$.)

This is possible because

$$A \cdot h^m = AK > |T|.$$

Moreover, we may assume that Q is not divisible by $E(Y)$. If it is, we can divide out all the factors of $E(Y)$, which will not affect the conditions $Q(z) = 0$ since E has no roots (being irreducible).

Step 2: Argue that each $f(Y) \in \mathrm{LIST}(r)$ is a 'root' of a related univariate polynomial Q^*. First, we argue as in the list-decoding algorithm that if $f \in \mathrm{LIST}(r, 1)$, we have

$$Q(Y, f_0(Y), \ldots, f_{m-1}(Y)) = 0.$$

This is ensured because

$$q > A - 1 + nmh.$$

(In the list-decoding algorithm, the left-hand side of this inequality was εq, since we were bounding $|\mathrm{LIST}(T_r, \varepsilon)|$.)

Once we have this, we can reduce both sides modulo $E(Y)$ and deduce

$$\begin{aligned} 0 &= Q(Y, f_0(Y), f_2(Y), \ldots, f_{m-1}(Y)) \bmod E(Y) \\ &= Q(Y, f(Y), f(Y)^2, \ldots, f(Y)^{m-1}) \bmod E(Y) \end{aligned}$$

Thus, if we define the univariate polynomial

$$Q^*(Z) = Q(Y, Z, Z^h, \ldots, Z^{h^{m-1}}) \bmod E(Y),$$

then $f(Y)$ is a root of Q^* over the field $\mathbb{F}_q[Y]/E(Y)$.

Observe that Q^* is nonzero because Q is not divisible by $E(Y)$ and has degree at most $h-1$ in each Z_i. Thus,

$$|\mathrm{LIST}(T, 1)| \leq \deg(Q^*) \leq h - 1 + (h-1)\cdot h + (h-1)\cdot h^2 + \cdots + (h-1)\cdot h^{m-1} = K - 1.$$

(Compare this to the list-decoding algorithm, where our primary goal was to efficiently enumerate the elements of $\mathrm{LIST}(T, \varepsilon)$, as opposed to bound its size.)

Handling smaller values of K. We further restrict $Q(Y, Z_1, \ldots, Z_m)$ to only have nonzero coefficients on form $Y^i \mathrm{Mon}_j(Z_1, \ldots, Z_m)$ for $0 \leq i \leq A-1$ and $0 \leq j \leq K-1 \leq h^m - 1$, where $\mathrm{Mon}_j(Z_1, \ldots, Z_m) = Z_1^{j_0} \cdots Z_m^{j_{m-1}}$ and $j = j_0 + j_1 h + \cdots + j_{m-1} h^{m-1}$ is the base-h representation of j. Note that this gives us $AK > |T|$ monomials, so Step 1 is possible. Moreover $M_j(Z, Z^h, Z^{h^2}, \ldots, Z^{h^{m-1}}) = Z^j$, so the degree of Q^* is at most $K-1$, and we get the desired list-size bound in Step 3. ■

We now set parameters to deduce the expander we used in Lecture 13 (to get a condenser).

Theorem 7 *For every constant $\alpha > 0$, every $N \in \mathbb{N}$, $K \leq N$, and $\varepsilon > 0$, there is an explicit $(K, (1-\varepsilon)D)$ expander with N left-vertices, M right-vertices, left-degree $D = O((\log N)(\log K)/\epsilon)^{1+1/\alpha}$ and $M \leq D^2 \cdot K^{1+\alpha}$. Moreover, D is a power of 2.*

Proof: Let $n = \log N$ and $k = \log K_{\max}$. Let $h = \lceil (nk/\varepsilon)^{1/\alpha} \rceil$ and let q be the power of 2 in the interval $(h^{1+\alpha}, 2h^{1+\alpha}]$.

Set $m = \lceil (\log K_{\max})/(\log h) \rceil$, so that $h^{m-1} \leq K_{\max} \leq h^m$. Then, by Theorem 6, the graph $\Gamma : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q^{m+1}$ defined in (2) is an (h^m, A) expander for $A = q - nhm$. Since $K_{\max} \leq h^m$, it is also a (K_{max}, A) expander.

Note that the number of left-vertices in Γ is $q^n \geq N$, and the number of right-vertices is

$$M = q^{m+1} \leq q^2 \cdot h^{(1+\alpha)\cdot(m-1)} \leq q^2 \cdot K_{\max}^{1+\alpha}.$$

The degree is

$$D = q \leq 2h^{1+\alpha} = O(nk/\epsilon)^{1+1/\alpha} = O((\log N)(\log K_{\max})/\epsilon)^{1+1/\alpha}.$$

To see that the expansion factor $A = q - nhm \geq q - nhk$ is at least $(1-\varepsilon)D = (1-\varepsilon)q$, note that

$$nhk \leq \varepsilon \cdot h^{1+\alpha} \leq \varepsilon q,$$

where the first inequality holds because $h^\alpha \geq nk/\varepsilon$.

Finally, the construction is explicit because a representation of $\mathbb{F}_q$ for q a power of 2 (i.e. an irreducible polynomial of degree $\log q$ over $\mathbb{F}_2$) as well as an irreducible polynomial $E(Y)$ of degree n over $\mathbb{F}_q$ can be found in time $\mathrm{poly}(n, \log q) = \mathrm{poly}(\log N, \log D)$. ■