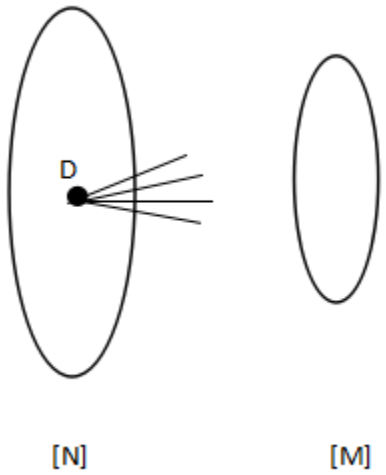
Lecture 14 : Construction of a Lossless Condenser/Expander; Special types of Graphs

Topics in Pseudo-randomness and Complexity Theory (Spring 2018)
Rutgers University
Swastik Kopparty
Scribe: Vibha Sridhar, Nikolas Melissaris

1 Problem Statement

What we want is a lossless condenser/expander. For this, we will consider a bipartite graph described below.



The left hand side is set 1,2,...k,..N and the right hand size is set 1,2,..,k,..,M. The degree is D, and $\forall$ S $\subseteq$ L, where $|S|$ = k, and the size of the neighborhood of S : $|\mathcal{N}(S)| \geq$ (1-ϵ)Dk

2 Proposed Construction

[N] = P $\subset$ $(F_q\ [x])^m$

This is 'm' tuples of univariate polynomials which can be viewed as specifying a curve, and where P is a special set of curves and m is the dimensions of the curves.

[m] = $(F_q)^{m+1}$

[D] = F_q

For $(P_1, P_2, \ldots, P_m) \in P$, $x \in F_q$, the x^{th} neighbor of $(P_1, P_2, \ldots, P_m)$ is $(x, P_1(x), \ldots, P_m(x))$.

3 Construction of P

Pick some integer d, and some irreducible polynomial $R(x)$ of degree 'd'.

Consider the set $P = \{ (A(x), A(x)^e, A(x^{e^2}), \ldots, A(x^{e^{m-1}})) \bmod R(x) : A(x) \in F_q, \deg(A) < d \}$

Here, the output of $Q(x, P_1(x), \ldots, P_m(x)) = 0)$ is a polynomial $\in F_q[x]$.

The reason for such a definition of P(x) is the analogous problem where we want a set of integer points such that no low degree polynomial can vanish on too many of these points. This property was proved in the last class : $\forall\ Q(x, Y_1, \ldots, Y_m) \neq 0$, where $\deg_{Y_i}(Q) < e$, $(\#\ (P_1, \ldots, P_m) \in P$ such that $Q(x, P_1(x), \ldots, P_m(x)) = 0) \leq e^m$. In other words, P is a set of curves and in how many curves can Q vanish on ?

Analyze the expansion property

$\forall\ k \leq e^k$, $\forall\ T \subseteq (F_q)^{m+1}$, with $|T| < (1- \epsilon)qk$, and $S = \{(P_1, \ldots, P_m) \in P$ such that $\forall\ x \in F_q\ (x, P_1(x), \ldots, P_m(x)) \in T \}$

Want to show that : $|S| \leq k$

For simplicity, we will show this for $k = e^m$

Proof. Take $T \leq (F_q)^{m+1}$ with $|T| < (1- \epsilon)qk$:

For a small set on the right hand side (RHS)), the set of vertices in the left whose full neighborhood is contained in that must be small. If we prove $|S| \leq k$, this means that for sets of size k, their neighborhood must be bigger. The proof strategy used is geared towards understanding subsets on the RHS.

1. Find $Q(X, Y_1, \ldots, Y_m) = \sum_{\substack{i_0, i_1, \ldots, i_m \\ 0 < i_0 < (1-\epsilon)q \\ 0 \leq i_r < e}} a_{i_0, i_1, \ldots, i_m}\ X^i\ Y_1^{i_1}\ \ldots\ Y_m^{i_m} \neq 0$

such that $Q(t) = 0$, $\forall\ t \in T$.

We are finding a polynomial such that the X degree is at most $(1- \epsilon)q$ and all the Y_i degree is at most e.

There is a non-zero polynomial of low degree that vanishes at all points of T.

Recall that we did the construct for $m = 1$ in the previous class and that had only one polynomial P.

2. For $(P_1, \ldots, P_m) \in S$, define $h(x) = Q(x, P_1(x), \ldots, P_m(x))$.

We know that $\forall\ x \in F_q$, $h(x) = 0$.

This is because x vanishes at all t, $P_1(x), \ldots, P_m(x)$ all lie inside T and Q vanishes at every point of T. So, this composition vanishes at every x.

So, deg(h) = (1- ϵ)q + med

As we want deg(h) < q, we assume that m*e*d < ϵq.

Now that we have deg(h) < q, and h vanishes on all points of F_q, this means that we have a univariate polynomial of degree < q vanishing on all points of F_q

Therefore the formal polynomial, h(X) = 0.

$\Rightarrow Q(X, P_1(X), ..., P_m(X)) = 0$

3. By choice of P, the number of such (P_1,..., P_m) $\in P <$ e^m.

So, $|S| < e^m$.

□

Note that this set T is the optimal size set such that we can always produce a polynomial that vanishes on e^m of these points. This has ultimately constructed an optimal expander in terms of the right neighborhood as a function of the left neighborhood.

We are looking at expansion of sets of size k = e^m so, sets of size k expand nearly optimal.

Even though we proved this only for k = e^m, this by itself implies that sets of some size expand near optimally, hence smaller sets have to also expand near optimally, as we can't have small sets not expand and suddenly have the big sets expand near optimally. All sets have to expand.

3.1 Unraveling these parameters :

Here, q is the left degree, and N is the size of P.

$$N = |P| = q^d$$

1. D = q
2. M = q^{m+1}
3. K = e^m
4. med < ϵq

We take q = $\frac{med}{\epsilon}$, where m, e, and d are arbitrary parameters.

Consider the following cases :

1. KD vs. M

   This is an expander that takes sets of size K and expands them, and wants to know how close can that be to N.

$$KD = e^m\ q$$

$$M = q^{m+1}$$

$$\frac{KD}{M} = (\frac{e}{q})^m = (\frac{\epsilon}{md})^m$$

If we take KD $\approx M^{0.99}$ i.e it is not that sets of optimal size expand, but it is lossless expansion for pretty large sets. It only goes to sets of size KD where KD ≈ 0.99

e $\approx q^{0.99}$

M = $q^{0.001}$

d = $q^{0.001}$

$\epsilon = 0.001$

KD = $q^{0.99+1}$

So, m = q^{m+1}

Note : m can be large, but not too large as it will make $\frac{KD}{M}$ small.

2. D vs. M

   This becomes, q vs. $q^{m+1} \approx q^{q^{0.001}}$

   $\Rightarrow$ D = (log m)(log log M)

3. D vs. N

   This becomes q vs. q^d

   $\Rightarrow$ D = (log N)(log log N)

4. N vs. M

   Now, let M = $q^{0.0001}$

   $q^{q^{0.01}}$ vs. $q^{q^{0.0001}}$

   n = $2^{(logN)^{\frac{1}{10}}}$

   This relation shows that for an 'a' bit long distribution, we get 0.99a bits of entropy inside k bits of randomness.

Note : The values taken gives a poly logarithmic degree graph with almost perfect expansion. Sets on the left hand side expand to the right hand side without any loss of entropy.

The application of these objects is in randomized extraction, we give a weak random source as input on the left hand side, and use pure randomness to pick a uniformly random neighbor, and the resulting lossless expansion (which implies lossless condensing) means that the right hand side is now ϵ-close to the distribution having even more entropy.

In all of the above cases, we produce an output distribution whose entropy is lossless.

4 Special kind of graphs: Superconcentrators

We want to show that computing Mx for given x requires many operations, where M is some fixed $n \times n$ matrix. We will focus on *linear circuits* which have gates with unbounded fan-in which compute a certain linear combination of its input.

Concretely we want to show that any linear circuit for $x \mapsto Mx$ requires many wires.

Fact 1. *There exists matrices M such that $\Theta(n^{2-\epsilon})$ wires are needed $\forall\ \epsilon > 0$*

\# of M over $\mathbb{F}_2 = 2^{n^2}$
\# of circuits with ω wires is $\leq (n+\omega)^2$
We convert all the gates with big fan in to gates with fan in 2.
For each wire we write down `(input gate, output gate)` which both are in $[n+\omega]$.
So if $\left((n+\omega)^2\right)^{\omega} < 2^{n^2}$ then there exists M which needs $> \omega$ wires where $\omega = n^{2-\epsilon}$.

Proposal: Take a matrix which is very non-singular, like the Cauchy matrix. The Cauchy matrix has elements of the form $\dfrac{1}{a_i - b_j}$, where $a_i \neq b_j$, $\forall i, j$ and a_i, b_i are the columns and rows respectively.

Lemma 2. *Any square submatrix has full rank.*

If M is very non-singular then any linear circuit from M has the following property:
Fix any

- $S \subseteq$ inputs
- $T \subseteq$ outputs, where $|S| = |T|$

There should be $|S|$ vertex disjoint paths from S to T.

Definition 3. *A superconcetrator with n sources and n sinks is a directed acyclic graph such that:*

- $\forall\ S \subseteq$ *sources*
- $\forall\ T \subseteq$ *sinks, where* $|S| = |T|$

there are $|S|$ vertex disjoint paths from S to T.

Conjecture 4. *(Valiant) Any superconcentrator with n sources and n sinks has $\omega(n)$ edges.*

Theorem 5. *There exists superconcentrators with $O(n)$ edges.*

Proof. We use bipartite expanders of constant degree such that $|L| = n$ and $|R| = \frac{3n}{4}$ and for each $S \subseteq L$ where $|S| \leq n/2$ we have that $\Gamma(S) \geq |S|$. We will construct G by starting from $K_{1,1}$ which will be our base $G(L_1, R_1)$.
G_i has $2i$ layers of vertices $L_i, L_{i-1}, \ldots, R_{i-1}, R_i$ where $\dfrac{|L_j|}{|L_{j-1}|} = \dfrac{|R_j|}{|R_{j-1}|} = \dfrac{4}{3}$. The graph between L_j

and L_{j-1} is a bipartite expander and the same applies for the graph between R_j and R_{j-1}. To the edges from the expanders, we add a perfect matching between L_j and R_j for each j.

After i steps we are going to have $O\left((4/3)^i\right)$ nodes and the number of edges is linear in the number of vertices as we have used constant degree expanders at each step, and adding a perfect matching just increases their degree by 1. In more detail ,the number of edges in an n vertex graph constructed by this method, $e(n)$ will be given by the recurrence $e(n) \leq cn + n + e(3n/4)$ for a constant c. Solving this, we get a linear number of edges.

To show that this is a superconcentrator we need to show that that there are at least $|S|$ edge disjoint paths from S to T, where $S \subseteq L_i$ and $T \subseteq R_i$ and we'll do this by using induction.

Base case: For $i = 1$ this is easy to verify.

Now assume that our claim holds for G_{i-1} and consider two cases for the size of $|S|$:

1. $|S| = |T| \leq \dfrac{|L_i|}{2}$

   From Hall's Theorem we have that there is a perfect matching between S and $\Gamma(S) \cap L_{i-1}$ and similarly for T and $\Gamma(T) \cap R_{i-1}$. It suffices to show that the number of edge disjoint paths between $\Gamma(S) \cap L_{i-1}$ and $\Gamma(T) \cap R_{i-1}$ is at least $|S| = |T| = |\Gamma(S) \cap L_{i-1}| = \Gamma(T) \cap R_{i-1}$ which is true from the induction step.

2. $|S| = |T| > \dfrac{|L_i|}{2}$

   By the previous argument we can't handle this case. The solution is to use the edges that directly connect L and R.

   By the pigeonhole principle, there are at least $|S| - \dfrac{|L_i|}{2}$ vertices in S that are directly connected by the matching to vertices in T. The remaining vertices (of which there are at most $\dfrac{|L_i|}{2}$) are handled by argument we made in the previous case.

□