CS395T Pseudorandomness and Combinatorial Constructions
Lecture 18, March 22, 2001
Lecturer: Prof. David Zuckerman, Scribe: Peiyush Jain

1 Nisan's generator for space bounded machines

We continue (from Lecture 17) with the proof of correctness of Nisan's PRG.

Definition 1 *$(h_1, h_2, ..., h_k)$ is ϵ good if*

$$|D(G_k(U_n, h_1, h_2, ..., h_k)) - D(U_{n2^k})| \leq \epsilon$$

where U_l is the uniform distribution on l bits and $|\cdot|$ denotes the L_1 norm.

The correctness of Nisan's PRG follows from

Lemma 1

$$\Pr[(h_1, h_2, ..., h_k) \textit{is not } (2^k - 1)\epsilon \textit{ good}] \leq \frac{2^{5S}k}{\epsilon^2 2^n}$$

for $\epsilon = 2^{-2S}$, $n = 12S$.

Proof:
We use induction on k.
Base Case : The $k = 0$ step is trivial.
Induction Step :
Define

$$B_{ij}{}^{\{h_1, h_2, ..., h_k\}} = \{x : G_{k-1}(x, h_1, h_2, ..., h_k) \text{ takes state } i \text{ to state } j\}$$

Define the two events:

$$E_1 : \{h_1, h_2, ..., h_{k-1}\} \text{ is } (2^k - 1)\epsilon \text{ good}$$

$$E_2 : \forall i, l, j \; h_k \text{ is } (2^{-2S}\epsilon, B_{il}{}^{\{h_1, h_2, ..., h_{k-1}\}}, B_{lj}{}^{\{h_1, h_2, ..., h_{k-1}\}}) \text{ good}$$

We will use B_{il} and B_{lj} for notational convenience.
Now, by induction assumption,

$$\Pr[\neg E_1] \leq \frac{2^{5S}(k-1)}{\epsilon^2 2^n}$$

Using a previous Lemma (Lecture 17) we have that,

$$Pr[\neg E_2] \leq \sum_{i,l,j} \frac{\rho(B_{il})\rho(B_{lj})}{2^n \epsilon_1^2}$$

where $\epsilon_1 = 2^{-2S}\epsilon$
Now,

$$\sum_{i,l,j} \frac{\rho(B_{il})\rho(B_{lj})}{2^n \epsilon_1^2}$$

$$= \sum_{i,l} \frac{\rho(B_{il})}{2^n \epsilon_1^2} \quad (\text{as } \sum \rho(B_{lj}) \text{ sums to } 1)$$

$$= \sum_{i} \frac{1}{2^n \epsilon_1^2} = \frac{2^S}{2^n \epsilon_1^2}$$

Hence,

$$Pr[\neg E_2] \leq \frac{2^S}{2^n 2^{-4S} \epsilon^2} = \frac{2^{5S}}{2^n \epsilon^2}$$

We now make the claim that:

$$E_1 \wedge E_2 \Rightarrow \{h_1, h_2, ...h_k\} \text{ is } (2^k - 1)\epsilon \text{ good}$$

To see this, consider

$$|D(G_k(U_n, h_1, h_2, ..., h_k)) - D(U_{n2^k})| \leq \delta_1 + \delta_2$$

where

$$\delta_1 = |D(G_k(U_n, h_1, h_2, ..., h_k)) - D(G_{k-1}^2(U_n, h_1, h_2, ..., h_{k-1}))|$$

$$\delta_2 = |D(G_{k-1}^2(U_n, h_1, h_2, ..., h_{k-1})) - D(U_{n2^k})|$$

where G_{k-1}^2 is the concatenation of two random elements from G_{k-1}. Also,

$$|D(G_{k-1}^2(U_n, h_1, h_2, ..., h_{k-1})) - D(U_{n2^{k-1}}^2)| \leq 2|D(G_{k-1}(U_n, h_1, h_2, ..., h_{k-1})) - D(U_{n2^{k-1}})| \leq 2(2^{k-1} - 1)\epsilon$$

Hence,

$$\delta_2 \leq 2(2^{k-1} - 1)\epsilon$$

Now consider the probability of reaching j under the two distributions of δ_1. Let,

$$p_{ij} = \Pr[\text{going from } i \text{ to } j \text{ under } G_{k-1}^2] = \sum_l \Pr_x[x \in B_{il}] \Pr_x[x \in B_{lj}]$$

$$q_{ij} = \Pr[\text{going from } i \text{ to } j \text{ under } G_k] = \sum_l \Pr_x[x \in B_{il} \wedge h_k(x) \in B_{lj}]$$

Notice that $\Pr_x[x \in B_{il}] = \rho(B_{il})$ and $\Pr_x[x \in B_{lj}] = \rho(B_{lj})$.
Since E_2 is true, we have that $|p_{ij} - q_{ij}| \leq (2^{-2S}\epsilon)2^S = 2^{-S}\epsilon$.

Fix i and let $\vec{p_i}$ denote the vector $[p_{i1}\ p_{i2} ... p_{i2^S}]^T$
Then, δ_1 equals the L_1 norm of $\vec{p_i}$ - $\vec{q_i}$. Now,

$$|\vec{p_i} - \vec{q_i}| \leq 2^S(2^{-S}\epsilon) \leq \epsilon$$

Therefore, we have that

$$|D(G_k(U_n, h_1, h_2, ..., h_k) - D(U_{n2^k})| \leq \epsilon + 2(2^{k-1} - 1)\epsilon = (2^k - 1)\epsilon$$

Hence, $(h_1, h_2, ..., h_k)$ is ϵ good.

$\square$

We can use a PRG for BPL (randomised log space) to build a universal traversal sequence as follows. Say $G : \{0,1\}^l \to \{0,1\}^r$ is a generator fooling space $\log n$ with error $1/(4n^2)$. Choose r large enough so that a random walk of length $t = \frac{r}{\log d}$ visits any particular vertex with probability at least $1 - 1/(4n^2)$.

We claim that the concatenation of $G(x)$ (viewed as an element of $[d]^t$) for all $x \in \{0,1\}^l$ is a universal traversal sequence. To see this, for each vertex v in a d-regular graph $H = (V, E)$ form the layered graph H_v with t layers. The vertices of layer i of H_v are (i, w) for $w \in V$, and (i, w) is connected to $(i + 1, w')$ for all neighbors w' of w, except if $w = v$ then (i, v) is only connected to (i, v). Fix a starting vertex u of the random walk in H. If the walk in H ever visits v the corresponding walk in H_v will end up at (t, v). By the pseudorandomness of G, the probability that a random output of G will end up at (t, v) is at least $1 - 1/(4n^2) - 1/(4n^2) = 1 - 1/(2n^2)$. Hence the probability a random output of G visits all vertices in H starting from u is at least $1 - n/(2n^2) = 1 - 1/(2n)$. Thus the probability that this holds for all starting vertices is at least $1 - n/(2n) = 1/2$. In particular, at least one output of G will visit all the vertices in H, and we have proved our claim.