CS 6815: Lecture 19

Instructor: Eshan Chattopadhyay Scribes: Will Gao, Cosmo Viola

11/1/2018

1 Recap: Nisan-Zuckerman PRG

Consider a machine given S space and suppose we want R' random bits. We will see that we can stretch R bits to RS^γ $(0 < \gamma < 1)$ bits using space $O(S)$, $R \geq cS$ for a c we will describe later. To get even greater numbers of random bits, we can compose this construction, producing a chain stretching the number of random bits $S \to S^{1+\gamma} \to S^{1+2\gamma} \to \dots$.

Take an $(\frac{n}{2}, \epsilon')$-extractor with large entropy $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, where $n = cS$ is large. Let $X \sim U_n$ and $Y_i \sim U_d$ for $1 \leq i \leq t$. We define our PRG as outputting the sequence of bits $\text{Ext}(X, Y_1), \dots, \text{Ext}(X, Y_t)$. We will use $n + dt = R$ random bits, and we are producing $mt = R' = RS^\gamma$ random bits. Here, the parameters are:

1. $dt = R - n$
2. $mt = RS^\gamma$
3. Pick $m = \Omega(S)$, i.e. a small constant times S, so $t = \Omega\left(\frac{R}{S^{1-\gamma}}\right)$ and $d = O(S^{1-\gamma})$.

We have extractors such that $d = O\left(\log\left(\frac{S}{\epsilon'}\right)\right)$ where $\epsilon' = 2^{-\Omega(S^{1-\gamma})}$. Thus, we can take $\epsilon = (\epsilon' + \frac{1}{2}S)t$.

2 A Closed But Unpublished Problem

Instead of a final project, we can solve the following problem. Consider a branching program of width 2 and length n, i.e. one of the following form:

The question is to design a PRG for $(2, n)$-ROBPs with a seed $O(\log n)$ in log space. This can be done using an ϵ-biased space, with $\epsilon = \frac{1}{100n}$; all that is left is the proof that this construction works.

3 Seedless (Deterministic) Extraction

Recall that there does not exist an extractor for all $(n, k)-$sources.

Definition 3.1. *Suppose there are two sources* $X \sim (n, k_1), Y \sim (n, k_2)$*.* $Ext: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ *is a* $(n, k_1, k_2, \varepsilon) - 2-$*source extractor if*

$$|Ext(X,Y) - U_m| \le \varepsilon$$

For $k_1 = k_2 \ge \log n + 2\log(1/\varepsilon) + 1$, such extractors exist.

Theorem 3.2. *For all* $\delta > 0$*, there exists an explicit* $2-$*source extractor for* $k_1 + k_2 \ge (1+\delta)n$*,* $m = 1$ *with* $\varepsilon = 2^{(n - k_1 - k_2)/2}$*.*

Proof. Let $x \sim X$, $y \sim Y$ be samples from the sources. Then, the explicit extractor $\text{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is given by $\text{Ext}(x,y) = \langle x, y\rangle$. Let us denote $P_x = \mathbf{Pr}(X = x)$. It follows that

$$\begin{aligned}
\left|\mathop{\mathbb{E}}_{x\sim X, y\sim Y}\left[(-1)^{\langle x,y\rangle}\right]\right|^2 &= \left|\sum_{x\in\text{supp}(X)} \sqrt{P_x}\left(\sqrt{P_x}\mathop{\mathbb{E}}_{y\sim Y}\left[(-1)^{\langle x,y\rangle}\right]\right)\right|^2 \\
&\le \mathop{\mathbb{E}}_{x\sim X}\left(\mathop{\mathbb{E}}_{y\sim Y}\left[(-1)^{\langle x,y\rangle}\right]\right)^2 && \text{(Cauchy-Schwarz)} \\
&\le \frac{1}{2^{k_1}}\sum_{x\in\text{supp}(X)}\left(\mathop{\mathbb{E}}_{y\in Y}\left[(-1)^{\langle x,y\rangle}\right]\right)^2 && \text{(Min-entropy)} \\
&= \frac{2^n}{2^{k_1}}\mathop{\mathbb{E}}_{x\sim U_n}\left(\mathop{\mathbb{E}}_{y\sim Y}\left[(-1)^{\langle x,y\rangle}\right]\right)^2 \\
&= \frac{2^n}{2^{k_1}}\mathop{\mathbb{E}}_{x\sim U_n}\mathop{\mathbb{E}}_{\substack{y\sim Y, y'\sim Y'\\ Y,Y'\text{iid}}}\left[(-1)^{\langle x,y+y'\rangle}\right] && \text{(Product of Indepedent Expectations)} \\
&= \frac{2^n}{2^{k_1}}\mathop{\mathbb{E}}_{y\in Y, y'\in Y'}\mathop{\mathbb{E}}_{x\in U_n}\left[(-1)^{\langle x,y+y'\rangle}\right] \\
&= \frac{2^n}{2^{k_1}}\text{Collision Pr}(Y) && \text{(Only non-zero if collision in } y, y'\text{)} \\
&\le \frac{2^n}{2^{k_1}2^{k_2}}
\end{aligned}$$

□

Theorem 3.3. *There exists an explicit* $2-$*source extractor for* $k_1 \ge (1/2 + \delta)n$*,* $k_2 \ge c\log n$*,* $m = 1$ *with* $\varepsilon = 2^{-\Omega(k_2)}$*.*

Proof. Let $X, Y \sim \mathbb{F}_p$ with $p \ge 2^n$ prime, so $k_1 \ge (1/2 + \delta)\log p$ and $k_2 \ge c\log\log p$. This extractor is based on a Paley graph, the Cayley graph for $\mathbb{Z}/p\mathbb{Z}$, where $p \equiv 1 \pmod 4$. We connect two points if $x + y \equiv r^2 \pmod p$ for some r; equivalently, $x + y$ is a quadratic residue. Then, define the map $\chi : \mathbb{F}_p \to \{-1, 1\}$ as follows:

$$\chi(z) = \begin{cases} 1 & \text{if } z \text{ is a square over } \mathbb{F}_p \\ -1 & \text{otherwise} \end{cases}.$$

Notice that this map preserves multiplication, and if $\chi(x^2) = 1$, then $\chi(x) = \chi(x^{-1})$.

Then, we define

$$\text{Ext}(x,y) = \frac{\chi(x+y) + 1}{2}.$$

In what follows, it could be helpful to think about flat sources; consider

$$\left|\sum_{\substack{x\sim\mathrm{supp}(X)\\ y\sim\mathrm{supp}(Y)}} (-1)^{\mathrm{Ext}(x+y)}\right| = \left|\sum_{\substack{x\sim\mathrm{supp}(X)\\ y\sim\mathrm{supp}(Y)}} \chi(x+y)\right|.$$

In the part of the proof that follows, we will use a big hammer from algebraic geometry, the Weil bound, which we will not prove.

Theorem 3.4 (Weil bound)**.** *Let f be a degree d polynomial over $\mathbb{F}_p$ with $f \neq g^2$ for any g. Then,* $\left|\sum_{x\in\mathbb{F}_p} \chi(f(x))\right| \leq (d-1)\sqrt{p}$.

Also recall Holder's Inequality:

$$\left|\sum_{i=1}^{n} a_i b_i\right| \leq \left(\sum_{i=1}^{n} a_i^p\right)^{1/p} \left(\sum_{i=1}^{n} b_i^q\right)^{1/q} \qquad \frac{1}{p}+\frac{1}{q}=1, \quad p,q>1$$

Observe that

$$\begin{aligned}
\left|\sum_{\substack{x\in\mathrm{supp}(X)\\ y\in\mathrm{supp(Y)}}} (-1)^{\mathrm{Ext}(x,y)}\right|^{2\ell} &= \left|\sum_{\substack{x\in\mathrm{supp}(X)\\ y\in\mathrm{supp}(Y)}} \chi(x+y)\right|^{2\ell} \\
&= \left|\sum_{x\in\mathrm{supp}(X)} 1 \sum_{y\in\mathrm{supp}(Y)} \chi(x+y)\right|^{2\ell} \\
&\leq |\,\mathrm{supp}(X)|^{2\ell-1} \sum_{x\in\mathrm{supp}(X)} \left|\sum_{y\in\mathrm{supp}(Y)} \chi(x+y)\right|^{2\ell} && \text{(Holder's Inequality)} \\
&\leq |\,\mathrm{supp}(X)|^{2\ell-1} \sum_{x\in\mathbb{F}_p} \left|\sum_{y\in\mathrm{supp}(Y)} \chi(x+y)\right|^{2\ell} \\
&\leq |\,\mathrm{supp}(X)|^{2\ell-1} \left|\sum_{\substack{x\in\mathbb{F}_p\\ y_1,\ldots,y_{2\ell}\in\mathrm{supp}(Y)}} \chi(x+y_1)\cdots\chi(x+y_{2\ell})\right| \\
&\leq |\,\mathrm{supp}(X)|^{2\ell-1} \sum_{y_1,\ldots,y_n\in\mathrm{supp}(Y)} \left|\sum_{x\in\mathbb{F}_p} \chi\left(\prod_{i=1}^{2\ell}(x+y_i)\right)\right| && \text{(Triangle Inequality)}
\end{aligned}$$

Let Δ_1 be the number of elements for which all the y_i are distinct and are thus certainly not a square. Let Δ_2 be the number of remaining elements, which might be a square. The preceding inequality implies that

$$\left|\sum_{\substack{x\sim X\\ y\sim Y}} \chi(x+y)\right| \leq |\mathrm{supp}(x)|^{\frac{2\ell-1}{2\ell}} \left(\Delta_1^{\frac{1}{2\ell}} + \Delta_2^{\frac{1}{2\ell}}\right)$$

Then, we can see that

$$\Delta_1 \leq (4\left|\text{supp}(Y)\right|\ell)^{\ell} \leq \left|\text{supp}(Y)\right|^{2\ell}\sqrt{p}(2\ell-1) \text{ by the Weil bound and}$$

$$\Delta_2 \leq \binom{|\operatorname{supp}(Y)|}{2\ell}(2\ell) \leq |\operatorname{supp}(Y)|^{2\ell}.$$

This implies that

$$\left|\sum_{\substack{x\sim X\\ y\sim Y}} \chi(x+y)\right| \leq \frac{p^{\frac{1}{4\ell}}}{\left|\text{supp}(X)\right|^{\frac{1}{2\ell}}} + \frac{2\sqrt{\ell}p^{\frac{1}{2\ell}}}{\left|\text{supp}(Y)\right|^{\frac{1}{2}}\left|\text{supp}(X)\right|^{\frac{\ell}{2}}}$$

Thus, we can set ℓ such that $p^{\frac{1}{\ell}} = |\text{supp}(Y)|$. □