CS761 Derandomization and Pseudorandomness **2022-23 Sem I**

Lecture 16: 06-10-2022

Scribe: Amit Rajaraman *Lecturer: Rohit Gurjar*

We had stated the following at the end of the previous lecture.

Theorem 16.1 (Yao)**.** *Let D be a distribution on $\{0,1\}^m$. Suppose that for any i and any circuit of size $2S$,*

$$\Pr_{y\sim D}[C(y_1,\ldots,y_i)=y_{i+1}]<\frac{1}{2}+\epsilon.$$

Then, for any circuit B of size S,

$$\left|\Pr_{y\sim D}[B(y)=1]-\Pr_{y\sim U_m}[B(y)=1]\right|<m\epsilon.$$

Proof. We shall show the contrapositive of the statement. Let B be a circuit of size S such that

$$\Pr_{y\sim D}[B(y)=1]-\Pr_{y\sim U_m}[B(y)=1]\geq m\epsilon.$$

We remove the modulus because if the other inequality is true, we can instead consider the probability that the output value is 0. Define a sequence of distributions $D_0, D_1, \ldots, D_m$, where D_i is obtained by drawing x from D, and then replacing the last $m-ii$ coordinates with draws from the uniform distribution. That is, a draw is $(y_1,\ldots,y_i,z_{i+1},\ldots,z_m)$, where $y\sim D$ and $z\sim U_m$. Note that $D_0=U_m$ and $D_m=D$, and also that D_i and D_{i-1} differ only at the ith bit.
Let

$$P_i=\Pr_{r\sim D_i}[B(r)=1].$$

Because $P_m-P_0\geq m\epsilon$, there is some i such that $P_i-P_{i-1}\geq\epsilon$.
We shall give an algorithm to predict y_i given $y_1,\ldots,y_{i-1}$ (for $y\sim D$). Randomly draw $z\sim U_m$. If $B(y_1,\ldots,y_{i-1},z_i,\ldots,z_m)=1$, then output z_i, and if it is 0 then output $1-z_i$. For the sake of succinctness, let $x=(y_1,\ldots,y_{i-1},z_i,\ldots,z_m)$. Now, the probability of success is

$$\frac{1}{2}\left(\underbrace{\Pr[B(x)=1\mid y_i=z_i]}_{P_i}+\underbrace{\Pr[B(x)=0\mid y_i=1-z_i]}_{(1-\alpha),\text{ say}}\right)$$

We have

$$P_{i-1}=\Pr[B(x)=1]=\frac{1}{2}\left(\Pr[B(x)=1\mid y_i=z_i]+\Pr[B(x)=1\mid y_i=1-z_i]\right)=\frac{1}{2}(P_i+\alpha).$$

Therefore,

$$\text{probability of success}=\frac{1}{2}(P_i+1-\alpha)=\frac{1}{2}+P_i-P_{i-1}\geq\frac{1}{2}+\epsilon.$$

To get the final circuit C, note that on a random choice of $z\sim U_m$ in our algorithm, we succeed with probability at least $(1/2)+\epsilon$. That is, the expected probability of success is at least $(1/2)+\epsilon$. Therefore, there exists some specific choice which gives a probability of success at least $(1/2)+\epsilon$, which is precisely what we want. □

Let us now come to the proof of the Nisan-Wigderson result, which we restate.

Theorem 16.2 (Nisan-Wigderson)**.** *If there exists a function computable in time $2^{O(n)}$ with $H_{avg}(f)\geq 2^{2n/3}$, then there exists a $(2^{\ell/45})$-PRG and in particular,* $\mathsf{BPP}=\mathsf{P}$.

The idea is as follows. Inspired by the one-bit extension in the previous lecture, we would like to consider a collection of subsets of $[\ell]$, and apply a hard function f to each of them to get one extra bit to append. In all, the number of bits we append is the number of subsets we choose. If we choose all subsets to be disjoint, then the resulting new bits are completely independent of each other, but we do not get exponentially many new bits. Therefore, we allow some small amount of intersection of the subsets, and thus some small amount of correlation, without compromising the uncorrelation of the new bits by too much.

Definition 16.3. *An* (ℓ, k, d)-combinatorial design *is a collection* $I_1, \ldots, I_r \subset \{1, 2, \ldots, \ell\}$ *of size* k *subsets such that for distinct* $i, j \in [r]$, $|I_i \cap I_j| \leq d$.

Proposition 16.4. *For* $k = \ell/30, d = k/3$, *there exists an* (ℓ, k, d)*-design of size at least* $2^{d/10} \geq 2^{\ell/900}$.

One can construct such a set by keep selecting random sets (each element selected independently with probability say, $2k/\ell$). One can argue that with good probability the generated sets all have size at least k and their intersections at most d.

Proof of Nisan-Wigderson. Set $\ell = 900 \log n$, and k as from the above.
Fix some combinatorial design $\mathcal{I} = \{I_1, \ldots, I_n\}$ guaranteed by the above proposition, and let $f : \{0,1\}^k \to \{0,1\}$ be a hard function. Then, given $z \in \{0,1\}^\ell$, the final pseudorandom bits we output are $f(z_{I_r})$ for each $r \in [n]$. For simplicity, denote $f(I_r) = f(z_{I_r})$.
Let f be computable in time $2^{O(k)}$ and $H_{\text{avg}}(f) \geq 2^{2k/3}$. Denote the resulting PRG by $\text{NW}^f_{\mathcal{I}}$. We shall show that $\text{NW}^f_{\mathcal{I}}(U_\ell)$ is $(n^{20}/2, 1/10)$-pseudorandom.
Now, we shall use Yao, by showing unpredictability instead. That is, we are done if we show that for any circuit C of size at most $n^{20}/2$,

$$\Pr_{z \sim U_\ell}\left[C(f(z_{I_1}), \ldots, f(z_{I_{i-1}})) = f(z_{I_i})\right] \leq \frac{1}{2} + \frac{\epsilon}{n},$$

where $\epsilon = 1/10$.
Suppose otherwise, and let C be a circuit violating the above. Let $z' = z_{[\ell]\setminus I_i}$, and $z'' = z_{I_i}$. Let $f_j(z) = f(z_{I_j})$ for each j. Then,

$$\Pr_{z \sim U_\ell}\left[C(f_1(z', z''), \ldots, f_{i-1}(z', z'')) = f(z'')\right] > \frac{1}{2} + \frac{\epsilon}{n}.$$

By averaging argument we can say that there exists a fixing of z' bits such that above probability does not decrease (this was done in precisely the same way in Yao's Theorem). We abuse notation to denote the new functions by f_j as well. Then,

$$\Pr_{z \sim U_\ell}\left[C(f_1(z''), \ldots, f_{i-1}(z'')) = f(z'')\right] > \frac{1}{2} + \frac{\epsilon}{n}.$$

using this, we get a circuit for f that succeeds with probability at least $(1/2) + \frac{\epsilon}{n}$ (recall $n = 2^{k/30}$). The crucial observation here is that each $f_j(z'')$ uses at most d bits (because $|I_i \cap I_j| \leq d$). By taking trivial circuits for each $f_j(z'')$, which are each of size at most about $d2^d$, we get a circuit for $f(z'')$ of size $d2^d 2^{d/10} + 2^{2d}/2 \leq 2^{2d} = n^{20}$, contradicting the hardness of f. □