CSG399: Gems of Theoretical Computer Science. Lecture 2. Jan. 13, 2009.
Instructor: Emanuele Viola Scribe: Ravi Sundaram

Stretching by 1 bit and Yao's next bit predictor

1 A first non-trivial generator

We restate and prove the theorem begun at the end of last class. The theorem exhibits a simple non-trivial generator that extends the seed by one bit.

Theorem 1. *Let $f : \{0,1\}^l \to \{0,1\}$ satisfy $COR_{uniform}(f, \textit{circuits of size } w) \le \epsilon$. Then, $G(x) = x \circ f(x), G : \{0,1\}^l \to \{0,1\}^{l+1}$ fools circuits of size $w - O(1)$ with error ϵ.*

Proof. Suppose for contradiction that circuit C distinguishes G from the uniformly random distribution, i.e.

$$|E_{x \in uniform}e[C(x \circ f(x))] - E_{x,u \in uniform}e[C(x \circ u)]| > \epsilon$$

where $x \in \{0,1\}^l$ and $u \in \{0,1\}$. Then for $b \in \{0,1\}$ consider the circuit $C'_b(x)$ defined as

$$\boxed{C'_b(x) := C(x \circ b) + b,}$$

(here addition is the usual addition over GF_2).

$$\begin{aligned}
& E_{b \in uniform}[COR_{uniform}(C'_b, f)] \\
= \;& E_{b \in uniform}[|E_{x \in uniform}e[C'_b(x) + f(x)]|] \\
\ge \;& |E_{b,x \in uniform}e[C'_b(x) + f(x)]| \\
= \;& |E_{b,x \in uniform}e[C(x \circ b) + b + f(x)]| \\
= \;& \left| \frac{1}{2} E_{x \in uniform}e[C(x \circ f(x)) + f(x) + f(x)] + \frac{1}{2} E_{x \in uniform}e[C(x \circ \overline{f(x)}) + \overline{f(x)} + f(x)] \right| \\
= \;& \left| \frac{1}{2} E_{x \in uniform}e[C(x \circ f(x))] - \frac{1}{2} E_{x \in uniform}e[C(x \circ \overline{f(x)})] \right|.
\end{aligned}$$

But note that

$$E_{x,u \in uniform}e[C(x \circ u)] = \frac{1}{2} E_{x \in uniform}e[C(x \circ f(x))] + \frac{1}{2} E_{x \in uniform}e[C(x \circ \overline{f(x)})]$$

and hence we can rewrite the above as

$$\begin{aligned}
= \;& \left| \frac{1}{2} E_{x \in uniform}e[C(x \circ f(x))] + \frac{1}{2} E_{x \in uniform}e[C(x \circ f(x))] - E_{x,u \in uniform}e[C(x \circ u)] \right| \\
= \;& |E_{x \in uniform}e[C(x \circ f(x))] - E_{x,u \in uniform}e[C(x \circ u)]| \\
> \;& \epsilon \quad \text{by our initial assumption that } C \text{ is a circuit that ``breaks'' } G.
\end{aligned}$$

Hence we have shown that

$$E_{b\in uniform}[COR_{uniform}(C'_b, f)] > \epsilon$$

This implies that there exists $b \in \{0,1\}$ such that $COR_{uniform}(C'_b, f)] > \epsilon$. Let us denote by C' the circuit C'_b corresponding to this b. Observe that $size(C') = size(C) + O(1)$. Thus the existence of a circuit C of size $w - O(1)$ that "breaks" generator G implies the existence of a circuit C' of size at most w that has high correlation with f, which is a contradiction. Hence, the theorem is proved. $\square$

The above theorem gives us a way to stretch seeds from length l to $l+1$ given a hard function, i.e. one that has low-correlation with any circuit of the given size. But ideally, we would like to get a generator that stretches seeds of length s to $n >> s$, e.g. $n = 2^{\Omega(s)}$.

A naive attempt would be to divide the input into blocks of length l and stretch each block from length l to $l+1$, i.e. $G(x_1, x_2, \ldots, x_k) = x_1 \circ f(x_1) \circ x_2 \circ f(x_2) \ldots x_k \circ f(x_k)$, where $x_i \in \{0,1\}^l, 1 \le i \le k$. However, as is easily seen, the stretch ratio n/s obtained by this scheme continues to be unchanged at $(l+1)/l$, even though this blockwise extender is a valid pseudorandom generator (prove as exercise).

2 The Nisan-Wigderson Construction

The idea of the Nisan-Wigderson construction is to output a concatenation of bits obtained by evaluating the hard function on nearly disjoint subsets of the bits of the seed. We give details below.

Definition 2 (Design). *$(S_1, S_2, \ldots S_n)$ is a design from a universe of size s, with set size l and intersection size α if*

- $S_i \subseteq [s], 1 \le i \le n$
- $|S_i| = l, 1 \le i \le n$
- $|S_i \cap S_j| \le \alpha, 1 \le i, j \le n$

A typical choice of parameters is $s \approx l, n \gg l, \alpha \approx \log n$.

Now we state the construction as well as the theorem of Nisan and Wigderson. The statement of the construction requires the following notation: let $x \in \{0,1\}^s, S \subseteq [s]$, then we use $x|S$ to denote the bits of x indexed by S.

Theorem 3 (Nisan-Wigderson). *Let $f : \{0,1\}^l \to \{0,1\}$ satisfy*

$$COR_{uniform}(f, \textit{circuits of size } w) \le 1/w.$$

Let $n = w^{\frac{1}{3}}$. Let $(S_1, S_2, \ldots, S_n)$ be a design over a universe of size s with set size l and intersection size $\alpha = \log n = \frac{1}{3}\log w$. Then the Nisan-Wigderson generator $G : \{0,1\}^s \to \{0,1\}^n$ defined as

$$G(x) = f(x|S_1) \circ f(x|S_2) \ldots \circ f(x|S_n)$$

fools circuits of size n with error $1/n$.

Note how the output length n of the generator is essentially w, i.e., the hardness we start from. Note we parameterized the circuit size and the correlation by the same w.

The proof of the theorem requires a lemma which we state and prove below.

Lemma 4 (Yao's next bit predictor)**.** *Let $D = D_1 D_2 \dots D_n$ be a distribution on $\{0,1\}^n$. Let $U = U_1 U_2 \dots U_n$ be the uniform distribution on $\{0,1\}^n$. Suppose $C : \{0,1\}^n \to \{0,1\}$ is a circuit such that*

$$|Ee[C(U)] - Ee[C(D)]| > \epsilon$$

Then there exists an index $i, 1 \leq i \leq n$ and a circuit C', $size(C') \leq size(C) + O(1)$ such that

$$|Ee[C'(D_1 D_2 \dots D_{i-1}) + D_i]| > \frac{\epsilon}{n}$$

Proof. The proof is in two phases. In the first phase, we use the "hybrid method" to obtain a circuit $\overline{C}$ that distinguishes between two adjacent hybrids, namely $D_1 D_2 \dots D_i$ and $D_1 D_2 \dots D_{i-1} U_i$. In the second phase we use the same trick as in our construction of a generator that stretches l bits to $l+1$ bits.

First phase. Let

$$H_i := D_1 D_2 \dots D_i U_{i+1} \dots U_n,$$

, for $0 \leq i \leq n$. By the assumption of the lemma we have that

$$|Ee[C(H_0)] - Ee[C(H_n)]| > \epsilon.$$

But

$$\begin{aligned}
& |Ee[C(H_0)] - Ee[C(H_n)]| \\
\leq \; & |Ee[C(H_0)] - Ee[C(H_1)] + Ee[C(H_1)] - Ee[C(H_2)] + Ee[C(H_2)] \dots \\
& \dots + Ee[C(H_{n-1})] - Ee[C(H_n)]| \\
\leq \; & \Sigma_{i=0}^{n-1} |Ee[C(H_i)] - Ee[C(H_{i+1})|.
\end{aligned}$$

Therefore $\exists i, 0 \leq i \leq n-1$ such that $|Ee[C(H_i)] - Ee[C(H_{i+1})| > \epsilon/n$. But

$$\begin{aligned}
& Ee[C(H_i)] - Ee[C(H_{i+1})] \\
= \; & E_{U_{i+1} \dots U_n} \left[E_{D_1 \dots D_{i-1}, U_i} e[C(D_1 \dots D_{i-1} U_i U_{i+1} \dots U_n)] - E_{D_1 \dots D_i} e[C(D_1 \dots D_i U_{i+1} \dots U_n)] \right].
\end{aligned}$$

Hence there exists a choice of $U_{i+1} \dots U_n$ such that

$$|Ee[C(H_i)] - Ee[C(H_{i+1})]| \geq \epsilon/n.$$

Let $\overline{C}$ be the circuit obtained by fixing this choice in the circuit C. Then we have that

$$|Ee[\overline{C}(D_1 \dots D_{i-1} U_i)] - Ee[\overline{C}(D_1 \dots D_i)]| > \frac{\epsilon}{n}$$

Second phase. As before for $b \in \{0,1\}$ define the circuit $C'_b(x)$ as

$$\boxed{C'_b(x) := \overline{C}(x \circ b) + b,}$$

(here addition is the usual addition over GF_2). Now consider

$$\begin{aligned}
& E_{b \in uniform} |E_D e[C'_b(D_1 \ldots D_{i-1}) + D_i]| \\
\geq\ & |E_{b \in uniform, D} e[C'_b(D_1 \ldots D_{i-1}) + D_i]| \\
=\ & |E_{b \in uniform, D} e[\overline{C}(D_1 \ldots D_{i-1} \circ b) + b + D_i]| \\
=\ & \left| \frac{1}{2} E_D e[\overline{C}(D_1 \ldots D_{i-1} D_i) + D_i + D_i] + \frac{1}{2} E_D e[\overline{C}(D_1 \ldots D_{i-1} \overline{D_i}) + \overline{D_i} + D_i] \right| \\
=\ & \left| \frac{1}{2} E_D e[\overline{C}(D_1 \ldots D_{i-1} D_i)] - \frac{1}{2} E_D e[\overline{C}(D_1 \ldots D_{i-1} \overline{D_i})] \right|
\end{aligned}$$

But note that

$$E_{U_i \in uniform, D} e[\overline{C}(D_1 \ldots D_{i-1} U_i)] = \frac{1}{2} E e[\overline{C}(D_1 \ldots D_i)] + \frac{1}{2} E e[\overline{C}(D_1 \ldots D_{i-1} \overline{D_i})]$$

and hence we can rewrite the above as

$$\begin{aligned}
=\ & \left| \frac{1}{2} E_D e[\overline{C}(D_1 \ldots D_{i-1} D_i)] + \frac{1}{2} E_D e[\overline{C}(D_1 \ldots D_{i-1} D_i)] - E_{U_i \in uniform, D} e[\overline{C}(D_1 \ldots D_{i-1} U_i)] \right| \\
=\ & \left| E_D e[\overline{C}(D_1 \ldots D_{i-1} D_i)] - E_{U_i \in uniform, D} e[\overline{C}(D_1 \ldots D_{i-1} U_i)] \right| \\
>\ & \frac{\epsilon}{n} \quad \text{by the inequality from the first phase.}
\end{aligned}$$

To summarize, putting the two phases together, we have shown that

$$E_{b \in uniform} |E_D e[C'_b(D_1 \ldots D_{i-1}) + D_i]| > \frac{\epsilon}{n}.$$

This implies that there exists $b \in \{0, 1\}$ such that $|E_D e[C'_b(D_1 \ldots D_{i-1}) + D_i]| > \epsilon/n$. Let us denote by C' the circuit C'_b corresponding to this b. Observe that $size(C') \leq size(\overline{C}) + O(1) \leq size(C) + O(1)$. Thus we have demonstrated the existence of a circuit C' (of the appropriate size) and an index i such that the circuit predicts the value of the i bit (given the first $i - 1$ bits) with the required probability. Hence, the lemma is proved. $\square$

We will complete the proof of the Nisan Wigderson theorem in the next class.