CSG399: Gems of Theoretical Computer Science. Lecture 3. Jan. 16, 2009.
Instructor: Emanuele Viola Scribe: Dimitrios Kanoulas

Nisan-Wigderson pseudorandom generator and design constuction

1 Nisan-Wigderson pseudorandom generator

Today we prove the Nisan-Wigderson pseudorandom generator theorem; we also present a design construction.

If $x \in \{0,1\}^s$ and $S \subseteq [s]$, we denote by $x|S$ the $|S|$ bits of x indexed by S.

Theorem 1 (Nisan-Wigderson). *Let $f : \{0,1\}^l \to \{0,1\}$ satisfy COR(f, size w) $\leq \frac{1}{w}$ and set $n := w^{\frac{1}{3}}$ (e.g., think $w = l^{\omega(1)}$). Let $S_1, \ldots, S_n$ be a design over universe of size s, where: $|S_i| = l$, $|S_i \cap S_j| \leq \alpha$ and $\alpha = \log n = \frac{1}{3}\log w$.*

Then the Nisan-Wigderson generator $G : \{0,1\}^s \to \{0,1\}^n$ defined as

$$G(x) = f(x|S_1) \cdots f(x|S_n)$$

fools circuits of size n with error $\frac{1}{n}$.

Proof. Assume for the sake of contradiction that there exists a circuit c which "breaks" the generator:

$$\left|E_{x\in\{0,1\}^s} e[c(G(s))] - E_u e[c(u)]\right| \geq \frac{1}{n},$$

where u is uniformly distributed over $\{0,1\}^n$. By Yao's next-bit predictor Lemma we have: $\exists c' : |c'| \leq |c| + O(1), \exists i \leq n$:

$$\left|E_{x\in\{0,1\}^s} e[c'(f(x|S_1)\cdots f(x|S_{i-1})) + f(x|S_i)]\right| \geq \frac{1}{n^2}.$$

From c' we will construct another circuit $\bar{c}$ that correlates with f, giving a contradiction.

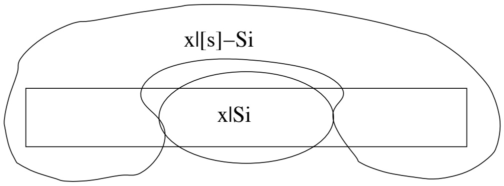

Figure 1: Input x

We break the input x in two parts: $x|([s] - S_i)$ and $x|S_i$ (Figure 1), and write:

$$E_{x|[s]-S_i}\left[\left|E_{x|S_i} e[c'(f(x|S_1)\cdots f(x|S_{i-1})) + f(x|S_i)]\right|\right] \geq \frac{1}{n^2}.$$

We now fix $x|[s] - S_i$ to a value that maximizes the above expectation, and for $j < i$ we let $f_j(x|S_i \cap S_j)$ be the function $f(x|S_j)$ where the bits of x outside of S_i are fixed accordingly. For this fixing and notation we:

$$\left|E_{x|S_i} e[c'(f_1(x|S_1 \cap S_i) \cdots f_{i-1}(x|S_{i-1} \cap S_i)) + f(x|S_i)]\right| \geq \frac{1}{n^2} \qquad (\star)$$

Note. *Each f_j is a function of α bits of $x|S_i$, and thus computable by a circuit of size $O(\alpha 2^\alpha)$.*

Now we are going to exhibit the circuit $\bar{c}$ that correlates with $f(x|S_i)$. Given an input $y \in \{0,1\}^l$, we let $x \in \{0,1\}^s$ be such that $y = x|S_i$, and the other bits of x are fixed as before, and $\bar{c}$ outputs:

$$\bar{c}(y) := c'(f_1(x|S_1 \cap S_i) \cdots f_{i-1}(x|S_{i-1} \cap S_i)).$$

Correlation: By our definition of $\bar{c}$ and $(\star)$, we have

$$E_y e[\bar{c}(y) + f(y)] \geq \frac{1}{n^2} = \frac{1}{(w^{\frac{1}{3}})^2} = \frac{1}{w^{\frac{2}{3}}} \gg \frac{1}{w}.$$

Size of $\bar{c}$: We need to show that the size of circuit $\bar{c}$ is less than w. Recalling that $n = w^{1/3}$ and $\alpha = \log n$, we have:

$$\begin{aligned}
Size(\bar{c}) &\leq |c'| + \text{size required to compute } f_i(x|S_1 \cap S_i) \cdots f_{i-1}(x|S_{i-1} \cap S_i) \\
&\leq |c| + O(1) + (i-1)O(\alpha 2^\alpha) \\
&\leq n + O(1) + nO(n \log n) \\
&\leq O(n^2 \log n), \\
&\leq O(w^{\frac{2}{3}} \log w^{\frac{1}{3}}) \\
&\ll w.
\end{aligned}$$

Thus, we have constructed a circuit of size at most w which has correlation at least $1/w$ with f. This contradicts our hypothesis and proves the theorem. □

We mention the following corollary, whose "in particular part" is Problem 1.

Corollary 2. *For every fixed $\epsilon > 0$, there exists a constant c: if $f : \{0,1\}^l \to \{0,1\}$ is computable in time $2^{O(l)}$ and $COR(f,\ size\ 2^{\epsilon l}) \leq \frac{1}{2^{\epsilon l}}$, then $\exists$ generator: $G : \{0,1\}^{c \log n} \to \{0,1\}^n$ that fools circuits of size n with error $1/n$ and it is computable in time* poly(n)*. In particular, $P = BPP$.*

Impagliazzo and Wigderson have strengthened the above result to hold under the weaker hypothesis that $COR(f,\ size\ 2^{\epsilon l}) < 1$, as opposed to $COR(f,\ size\ 2^{\epsilon l}) \leq \frac{1}{2^{\epsilon l}}$. In particular, this leads to the following striking disjunction:

Either SAT : $\{0,1\}^\ell \to \{0,1\}$ has circuits of size $2^{\ell/100000}$ for arbitrarily large ℓ, or P=BPP.

Back from heaven, our goal now is to get an unconditional result. Specifically, we will construct a generator $G : \{0,1\}^{\log^{O(1)} n} \to \{0,1\}^n$ that fools small circuits of fixed depth. We start with the design construction (which of course can be used in other contexts too).

Design Construction

Now we will see how we can construct designs. Designs that are good enough for Corollary 2 can be found by an exhaustive brute-force procedure, in $\mathrm{poly}(n)$ time.

We can construct more explicit designs using finite fields. We recall some basic facts about finite fields.

Fact 1. *Fields of size 2^l can be constructed and operations over them can be performed in time* $\mathrm{poly}(l)$. *A polynomial of degree d over a field F, i.e. $P : F \to F$, $P(x) = \sum_{i=0}^{d} x^i c_i$, has at most d roots over F.*

Theorem 3. *$\forall$ h power of 2, $\forall$ constant c, $\exists$ design $S_1, \ldots, S_n$ such that*
$n = 2^h$,
$|S_i \cap S_j| \le h, \forall i \ne j$,
$|S_i| = h^c$,
the universe has size $(set\ size)^2 = h^{2c}$, and
S_i is computable in time $\mathrm{poly}(h)$.

We are packing exponentially many sets whose pairwise intersection is a small power of the set size, over a universe roughly as large as the set size

Proof. Pick a field F of size h^c, note $x \in F$ has size $|x| = \log h = c \log \log n$. Our universe is $F \times F$. Given a string $i \in \{0,1\}^{\log n} = \{0,1\}^h$, construct S_i as follows:

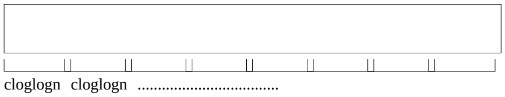

Figure 2: string i

View i as the coefficients of a polynomial p_i over F. The degree of p_i is $\frac{\log n}{c \log \log n} \le \log n = h$. The set S_i will be the graph of the polynomial p_i:

$$S_i := \{(a, p_i(a)) : a \in F\} \subseteq F \times F,$$

cf. Figure 3.

Note $|S_i| = F = h^c$, and we have $n = \{0,1\}^h$ sets.

To bound the intersection size, observe that $|S_i \cap S_j|$ is the number of roots of the polynomial $(p_i - p_j)$. Since $p_i - p_j$ has degree less than h, we bound from above the intersection size by h, using Fact 1.

Finally, using again Fact 1, S_i is computable in $\mathrm{poly}(h)$ time. □

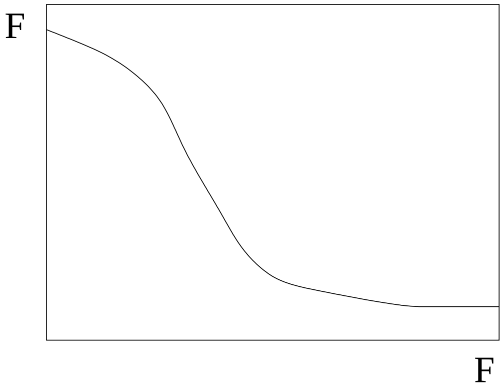

Figure 3: Graph of polynomial

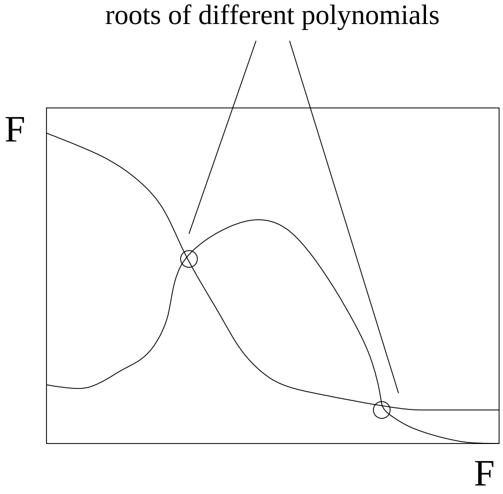

Figure 4: Bound on the intersection size

Constant-depth circuits

The depth of a circuit denotes the maximum distance from an input to an output gate (and recall circuits in these lectures have unbounded fan-in; our complexity measure is the number of wires).

Remark 4. *The depth in Nisan-Wigderson's proof increases by an absolute constant. Therefore, given $f : \{0,1\}^l \to \{0,1\}$ such that COR(f, size w and depth d) $\leq \frac{1}{w}$, the Nisan-Wigderson construction gives a generator $G : \{0,1\}^s \to \{0,1\}^n$ that fools circuits of size n and depth $d - O(1)$ with error $1/n$.*

The complete proof of the next theorem will be given in next lectures.

Theorem 5. *The parity function on l bits, Parity($x_1, \ldots, x_l$) $:= x_1 + \ldots + x_l$ mod 2, satisfies: COR(f, size $w = 2^{l^{\epsilon/d}}$ and depth d) $\leq 1/w$, where ϵ is an absolute constant.*

Now, Problem 2 asks you to put together the Nisan-Wigderson construction, the design construction from the previous section, and the above theorem, to obtain the following.

Corollary 6 (Nisan). $\forall d, \exists$ *explicit generator* $G : \{0,1\}^{\log^{O(d)} n} \to \{0,1\}^n$, *that fools circuits of size* n *and depth* d, *with error* $1/n$.

For an application of this corollary, see Problem 3.