Last Class

- Finished Razborov's lower bound for Clique
- Natural Proofs

Today

- Natural Proofs, and their limitations
- Remark
  - A uniform lower bound
  - Frontiers

Natural property:

$C_n \subseteq F_n$ - Largeness $\Pr_{f \in F_n}[f \in C_n] \geq \frac{1}{2^{O(n)}}$

($F_n = \{f: \{0,1\}^n \to \{0,1\}\}$

- Constructivity: Given truth table of $f_n \in F_n$
  Can tell if $f_n \in C_n$ in $2^{O(n)}$ time

Any proof based on a "formal complexity measure" yields largeness

Def: $\mu(x_i)=1$, $\mu(\bar{x}_i)=1$, $\mu(f \vee g) \leq \mu(f)+\mu(g)$, $\mu(f \wedge g) \leq \mu(f)+\mu(g)$

Let $C_n = \{f_n \mid \mu(f_n) \geq S\}$

Claim: If $\exists f \in f_n$, $\mu(f) \geq S$, then at least $\frac{1}{4}$ of fcns $g \in F_n$ satisfies $\mu(g) \geq \frac{S}{4}$

Pf: $f = g \oplus (g \oplus f) = (g \vee \bar{h}) \wedge (\bar{g} \vee h)$ $(h = g \oplus f)$

If less than $\frac{1}{4}$ of fcns $g \in F_n$ satisfies $\mu(g) \geq \frac{S}{4}$,

We can find g satisfies $\mu(g), \mu(\bar{g}), \mu(h), \mu(\bar{h}) < \frac{S}{4}$.

which means $\mu(f) \overset{<}{\#} S$. contradiction.

Def: A natural property is $\mathcal{C}$ useful (for some class of circuits $\mathcal{C}$)
if for any sequence $\{g_n\}$ of fcns computed by a circuits in $\mathcal{C}$.
$g_n \notin C_n$ $\forall$ large enough n. (or infinitely ~~often~~ often)

Eg: $\oplus \notin AC^0$

"Theorem": If sub-exponentially hard pseudo-random function exists
(or even if sub-exp hard one-way function exists)
then there is no natural property that is useful against P/poly.

Some crypto definitions

One-way functions: A family of functions $f: \{0,1\}^* \to \{0,1\}$
is a T-hard ($T: \mathbb{N} \to \mathbb{N}$) one-way fcns if:

(i) f is computable efficiently (poly time)

(ii) $\Pr_{\substack{x \in \{0,1\}^n \\ y = f(x)}} [A(y) = x' \wedge f(x') = y] < \frac{1}{T(n)}$ $\forall$ $T(n)$-~~$\mathcal{A}$~~ algorithm A.
(possibly randomized)

Pseudo~~random~~ random generators (PRG)

$G: \{0,1\}^* \to \{0,1\}^*$ is a stretch $\ell(n)$-PRG if

(1) G maps $\{0,1\}^n \to \{0,1\}^{\ell(n)}$

(2) G can be efficiently computed in poly(n) time.

(3) $\forall$ Probabilistic Machine A running in time $T(n)$

$$\left| \Pr_{r \in \{0,1\}^n} [A(G(r)) = 1] - \Pr_{s \in \{0,1\}^{\ell(n)}} [A(s) = 1] \right| < \frac{1}{T(n)}$$

(r: seed)

Theorem (HILL)

If one-way functions exists ~~=~~, then $\exists$ strech $n^{O(1)}$ PRG exists.

Pseudo random functions (PRF)

A T-hard PRF $\{f_k\}_{k\in\{0,1\}^*}$ is a family of functions

① $f_k : \{0,1\}^{|k|} \to \{0,1\}^{|k|}$, polytime computable given k.

② ~~It is~~ pseudorandom. $\forall$ T(n) randomized machine

$$\left| \Pr_{k\in\{0,1\}^m}[A^{f_k()}(1^m)=1] - \Pr_{g_m \in F_{\{0,1\}^m \to \{0,1\}^m}}[A^{g_m}(1^m)=1] \right| \le \frac{1}{T(n)}$$

One-way function $\Rightarrow$ Pseudo random generators $\Rightarrow$ Pseudo random functions

Subexponentially hard:

$T = 2^{n^\varepsilon}$ for some $\varepsilon > 0$

Pf of "Theorem":

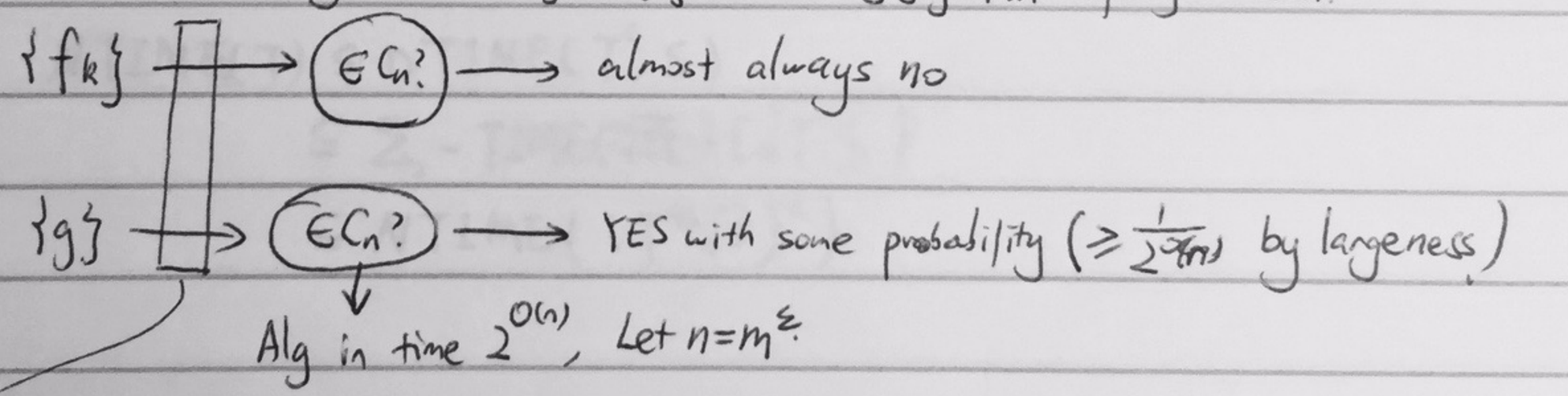
If P/ptoly - useful natural property $\{C_n\}$ exists $\Rightarrow \exists$ no 2^{n^ε}-hard PRF.

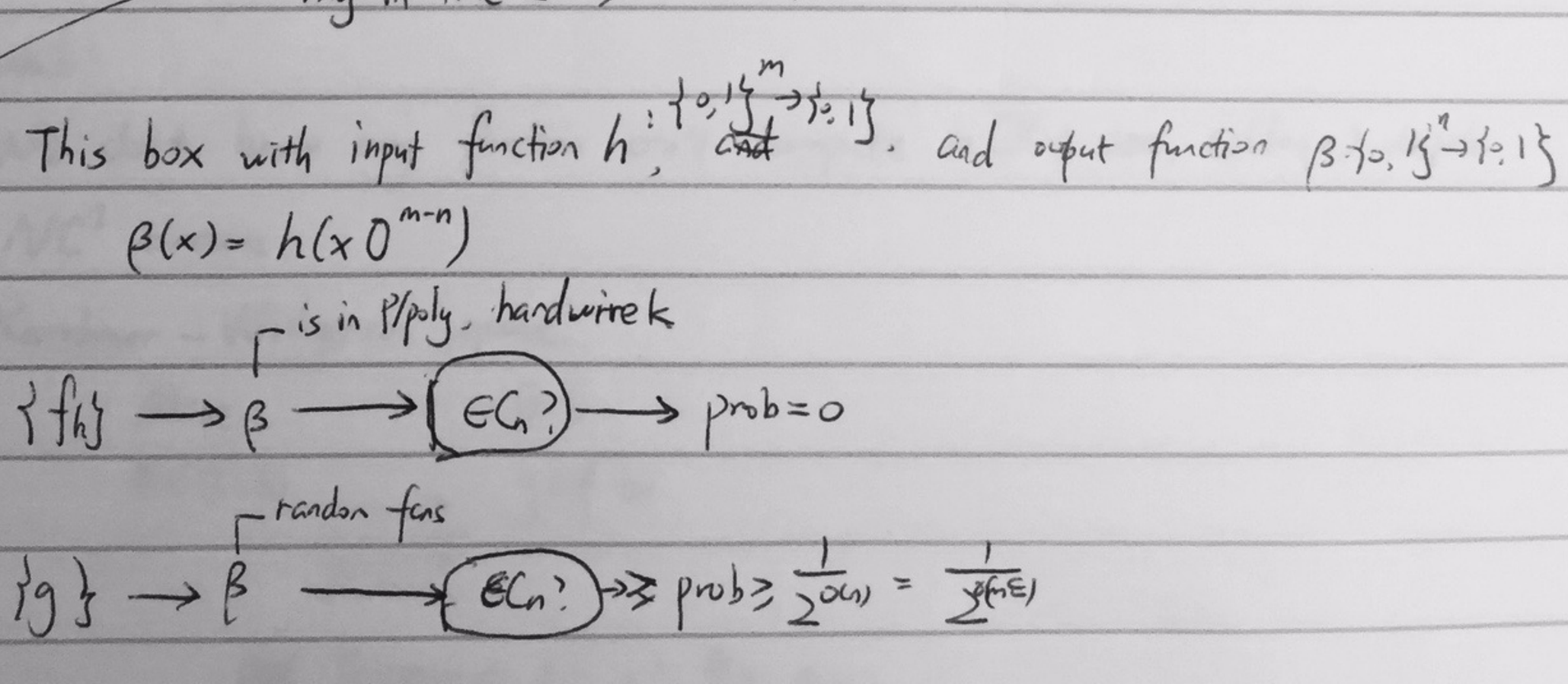
Given $\{f_k\}$

It's equivallent to break even one bit, some we can assume

$f_k : \{0,1\}^m \to \{0,1\}$ $\quad g : \{0,1\}^m \to \{0,1\}$

We need to distinguish $\{f_k\}_{k\in\{0,1\}^m}$ vs $\{g\}_{g\in F_m}$ uniformly random.





A uniform lower bound

$SAT \notin TIME(n)$ open

$SAT \notin SPACE(\log n)$ open

However there is no algo for SAT running in $O(n)$ time & $O(\log n)$ space

Def: $DTISP(T(n), S(n))$ = language that can be decided by a TM M with $O(T(n))$ time & $O(S(n))$ space.

Thm: $SAT \notin DTISP(n^{c-\varepsilon}, n^{o(1)})$, $\forall \varepsilon > 0$. $c = \sqrt{2}$ [Lipton-Viglas]

[Fortnow-van Melkebeek]

Later $c = \sqrt{2} \to \phi(\frac{\sqrt{5}+1}{2}) \to 2\cos\frac{\pi}{7}$ (Ryan Williams)

$T(n) \cdot S(n) \geq n^{1.8}$

Idea: Trade time for alternation, and vice versa.

$DTISP(T, S) \subseteq \Sigma_2\text{-}TIME(\sqrt{TS})$

~~Stace SA~~

If $NTIME(T) \subseteq DTIME(T^c, S)$, then

$NTIME(T) \subseteq DTIME(T^c, S)$

$\subseteq \Sigma_2\text{-}TIME(\sqrt{T^c S})$

$\subseteq NTIME((T^{c/2}\sqrt{S})^c)$

Next week:

- We don't know any function can't compute in $O(n)$ size, $O(\log n)$ depth NC^1 circuits.
- Karchmer-Widgerson game.

Alice $x \in f^{-1}(1)$ — Bob $y \in f^{-1}(0)$

~~Def~~ Determine $\forall i$ s.t. ~~f~~ $x_i \neq y_i$