Saturday, April 28, 2018 8:10 PM

Uniform dist. over n-bit strings.

Distribution D on $\{0,1\}^n$

D is $(s(n), \epsilon(n))$ - $\boxed{\text{indistinguishable}}$ from U_n if for all $\{C_n\}$, where $|C_n| \le s(n)$

$$\left| \Pr_{y \in U_n}[C(y)=1] - \Pr_{y \leftarrow D}[C(y)=1] \right| \le \epsilon(n).$$

Distribution D is $(s(n), \epsilon(n))$ $\boxed{\text{unpredictable}}$ if for all $\{C_n\}$, $|C_n| \le s(n)$
For all $i = 2, 3, \ldots, n$

$$\Pr_{y \leftarrow D}[C(y_1 \ldots y_{i-1}) = y_i] \le 1/2 + \epsilon(n)$$

Theorem (Yao): If a distribution D over $\{0,1\}^n$ is $(s, \epsilon/n^2)$ - unpredictable then D is (s', ϵ) - indistinguishable for $s' = s - O(n)$

(s', ϵ) distinguisher $\Rightarrow$ $(s' + O(n), \epsilon/n^2)$ predictor.

Sunday, April 29, 2018 8:54 PM

Proof by contradiction.

Given (s, ϵ) distinguisher C:

$$\left| \overset{p_0}{\Pr_{y \leftarrow U_n} [C(y) = 1]} - \overset{p_n}{\Pr_{y \leftarrow D} [C(y) = 1]} \right| > \epsilon$$

We will show a $(S + O(n), \epsilon/n^2)$ predictor (for some i)

$$\Pr_{y \leftarrow D} [P(y_1, \ldots, y_{i-1}) = y_i] > \frac{1}{2} + \frac{\epsilon}{\cancel{n^2}\ 2n}$$

Consider hybrid distributions between D + U_n:

D_i: $\underbrace{b_1 b_2 \cdots b_i}_{\text{induced by } D} \underbrace{b_{i+1} \cdots b_n}_{\text{uniform}}$

generate $b_1 b_2 \cdots b_n$

toss out $b_{i+1} \cdots b_n$.

$U_n = D_0 \quad D_1 \quad - \ - \ - \quad D_n = D$

$D_0 = U_n$ and $D_n = D$.

Let $p_i = \Pr_{y \leftarrow D_i} [C(y) = 1]$

$p_0 = \Pr_{y \leftarrow U_n} [C(y) = 1]$

$p_n = \Pr_{y \leftarrow D} [C(y) = 1]$.

by assumption $|p_n - p_0| > \epsilon$

$$\epsilon < |p_n - p_0| \leq \sum_{i=1}^{n} |p_i - p_{i-1}|$$

$\Rightarrow i$ such that $|p_i - p_{i-1}| > \epsilon/n$.

Assume w.l.o.g. that $p_i > p_{i-1}$ otherwise just toggle the output.

$\overset{\epsilon}{\overline{p_0 \quad p_1}} \quad - \ - \ - \quad p_n$

Wed May 9, 2018 - page 3

Sunday, April 29, 2018 8:54 PM

differ only in i^{th} bit.

D_i $\quad b_1\, b_2 \cdots b_i\; b_{i+1}\, b_{i+2} \cdots b_n$

D_{i+1} $\quad b_1\, b_2 \cdots b_i\; b_{i+1}\, b_{i+2} \cdots b_n$

$$\underbrace{\Pr_{y \leftarrow D_{i+1}}[C(y)=1]}_{p_{i+1}} - \underbrace{\Pr_{y \leftarrow D_i}[C(y)=1]}_{p_i} > \frac{\epsilon}{n}.$$

Use this to build a predictor Pred :

Input: $b_1 b_2 \cdots b_i$

Generate $y_{i+1}\, y_{i+2} \cdots y_n$ at random.

Evaluate $C(b_1 b_2 \cdots b_i\, y_{i+1}\, y_{i+2} \cdots y_n)$

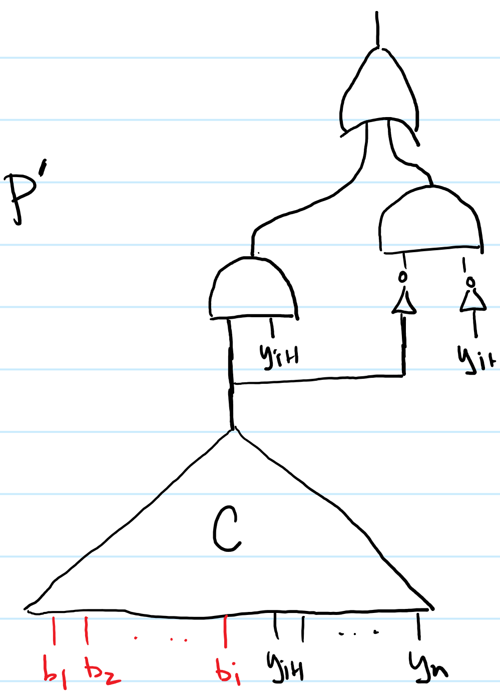
If $1 \rightarrow$ output y_{i+1}

If $0 \rightarrow$ output $\neg y_{i+1}$

Claim

$$\text{Prob}_{\substack{b_1 b_2 \cdots b_{i+1} \leftarrow D \\ y_{i+1} y_{i+2} \cdots y_n \leftarrow U}} \left[\text{Pred}(b_1 b_2 \cdots b_i) = b_{i+1}\right] > \frac{1}{2} + \frac{\epsilon}{2n}.$$

P'



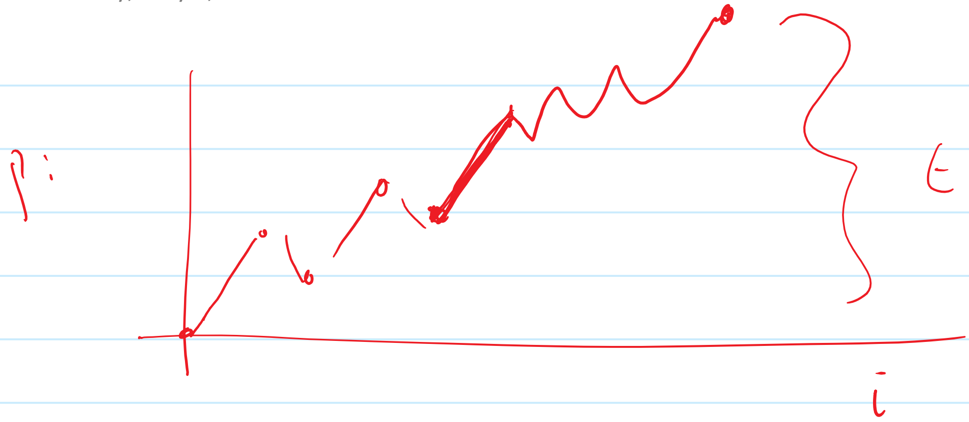
- Generate $b_1 b_2 \cdots b_i\, b_{i+1}$ according to D.
- Feed $b_1 \cdots b_i$ + random $y_{i+1} \cdots y_n$ into circuit.
- Prob output $= b_{i+1}$?

$\Rightarrow$ Select $y_{i+1} \cdots y_n$ to maximize probability. $\rightarrow y^*$

$\Rightarrow$ Hard code y^* into circuit.

Wed May 9, 2018 - page 3.5

Wednesday, May 9, 2018 10:11 AM



$$\sum_{\vec b} \sum_{\vec y} \text{Prob}(\vec b) \cdot \text{Prob}(\vec y) \cdot C(\vec b \, \vec y)$$

$$\sum_{\vec y \in U} \sum_{\vec b \in D} \text{Prob}(\vec b)\, \text{Prob}(\vec y) \; C(\vec b, \vec y)$$

$$\sum_{\vec y \in U} \text{Prob}(\vec y) \sum_{\vec b \in D} \text{Prob}(\vec b) \cdot C(\vec b \, \vec y).$$

Wed May 9, 2018 - page 4

Wednesday, May 9, 2018 7:25 AM

$$\text{Prob}(b_1 \cdots b_i)\, 2^{-n+i+1} \left(\frac{\text{Prob}(b_{i+1} \mid -) + \text{Prob}(\bar{b}_{i+1} \mid -)}{2} \right)$$

$\frac{1}{2}$

$=$

3 different distributions:

D_i $\quad b_1 b_2 \cdots b_i\, y_{i+1} y_{i+2} \cdots y_n.$

D_{i+1} $\quad b_1 b_2 \cdots b_i\, b_{i+1}\, y_{i+2} \cdots y_n$

D^*_{i+1} $\quad b_1\, b_2\, b_i\, \bar{b}_{i+1}\, y_{i+2} \cdots y_n$

$\to \text{Prob}(b_1 \cdots b_i) \cdot \frac{1}{2} \cdot 2^{-n+i+1}$

$\text{Prob}(b_1 \cdots b_i)\, \text{Prob}(b_{i+1} \mid b_1 \cdots b_i)\, 2^{-n+i+1}$

$+\ \text{Prob}(b_1 \cdots b_i)\, \text{Prob}(\bar{b}_{i+1} \mid b_1 \cdots b_i)\, 2^{-n+i+1}$

$+ \quad = 1$

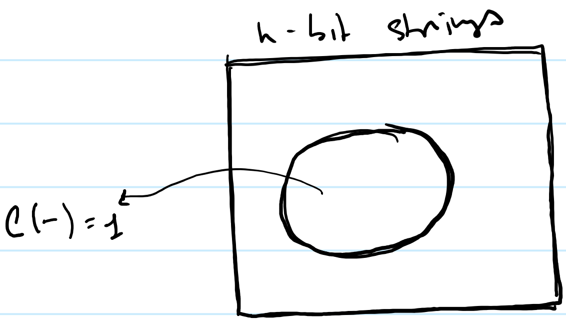
$$D_i = \frac{D_{i+1} + D^*_{i+1}}{2}$$

$$p_i = \frac{p_{i+1} + p^*_{i+1}}{2}.$$

$\text{Prob}[\,C(b_1 \cdots b_i\, y_{i+1} \cdots y_n) = 1\,]$

$\text{Prob}[\,C(b_1 \cdots b_i\, b_{i+1}\, y_{i+2} \cdots y_n)\,]$

$\text{Prob}[\,C(b_1 \cdots b_i\, \bar{b}_{i+1}\, y_{i+2} \cdots y_n)\,]$



Tuesday, May 8, 2018 2:52 PM

Claim $\text{Prob}_{\substack{b_1 b_2 \cdots b_{i+1} \leftarrow D \\ y_{i+1} y_{i+2} \cdots y_n \leftarrow U}} \left[\text{Pred}(b_1 b_2 \cdots b_i) = b_{i+1} \right] > \frac{1}{2} + \frac{\epsilon}{n}.$

$$\text{Prob}\left[\text{Pred}(b_1 \cdots b_i) = b_{i+1} \mid b_{i+1} = y_{i+1}\right] \cdot \text{Prob}\left[b_{i+1} = y_{i+1}\right]^{1/2}$$

$$+ \text{Prob}\left[\text{Pred}(b_1 \cdots b_i) = b_{i+1} \mid b_{i+1} \neq y_{i+1}\right] \cdot \text{Prob}\left[b_{i+1} \neq y_{i+1}\right]^{1/2}$$

y_{i+1} is random.

$$\frac{1}{2} \cdot p_i + \frac{1}{2}(1 - p_{i+1}^*) = \frac{1}{2} p_i + \frac{1}{2}(1 - 2p_i + p_{i+1})$$

$$= \frac{1}{2} + \frac{1}{2}(p_{i+1} - p_i) \geq \frac{1}{2} + \frac{\epsilon}{2n}.$$

$$\text{Prob}_{\substack{b_1 b_2 \cdots b_{i+1} \leftarrow D \\ y_{i+2} y_{i+3} \cdots y_n \leftarrow U}}\left[C(b_1 b_2 \cdots b_{i+1} y_{i+2} \cdots y_n) = 1\right] = p_{i+1}.$$

$$\text{Prob}_{\substack{b_1 b_2 \cdots b_{i+1} \leftarrow D \\ y_{i+2} y_{i+3} \cdots y_n \leftarrow U.}}\left[C(b_1 b_2 \cdots \overline{b_{i+1}}\, y_{i+2} \cdots y_n) = 0\right] = 1 - p_{i+1}^*$$

seed size $= t$

2^t

$$p_{i+1}^* = \text{Prob}_{\substack{b_1 b_2 \cdots b_{i+1} \leftarrow D \\ y_{i+2} y_{i+3} \cdots y_n \leftarrow U.}}\left[C(b_1 b_2 \cdots \overline{b_{i+1}}\, y_{i+2} \cdots y_n) = 1\right]$$

$$\frac{p_{i+1} + p_{i+1}^*}{2} = p_i. \implies p_{i+1}^* = 2p_i - p_{i+1}$$