Pseudo Randomness.

Wednesday, 28 October 2020 4:00 PM

$m_1, \dots m_k$

$p_1 \dots p_k$.

$p_1' \dots p_k'$

$\sum | p_i - p_i' | = 0$

Distinguisher: $D : \{\ \} \to \{0,1\}$.

Deterministic Dist: A is a subset.

$D^{-1}(1)$ will act as the 'TEST'.

$D_1 : \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}$.

$D_2 . \frac{1}{4}, \frac{1}{4}, \frac{1}{2}, \cancel{0}$

1 3 2 4

$D : \{0,1,2,3,4\} \to \{0,1\}$

$: \{odd\} - 1 \to D_2$

$\{even\} - 0 \to D_1$

$D(\boxed{3}) = 1$ — biased one:

$D(\boxed{1}) = 1 \to$ biased one:

D_1 – prob $1/2$

D_2 prob $1/2$ }.

$Pr(D(x) = 1)$

$D^{-1}(1) = \{1,3\}$.

$D_1 \quad p_1 p_2 = 1/4 , \frac{1}{4} = 1/2$

$D_2 \quad p_1', p_2' = \frac{1}{4}, \frac{1}{4} = \frac{1}{2}$

$| \underset{D_1}{P}(D^{-1}(1)) - \underset{D_2}{P}(D^{-1}(1)) | = 0$.

$D : \{1,2,3,4\} \to \{0,1\}$

2 or 3 $\to$ biased.

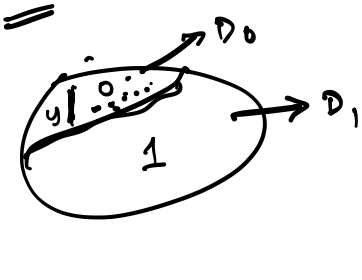
1 or 4 $\to$ unbiased.

ϵ - dist:

$| D$ is correct $- D$ is wrong $| \geq \epsilon$.

$D_0 \quad D_1 \quad \{0,1\}^n$.

$D : \{0,1\}^n \to \{0,1\}$



$\boxed{y}$.

$\alpha \quad \sum_{z \in D^{-1}(0)} p_{D_0}(z)$ — right.

$\beta \quad \sum_{z \in D^{-1}(0)} p_{D_1}(z)$. — wrong.

$|\alpha - \beta|$

$(1-\alpha) - (1-\beta)$ $|(\beta - \alpha)|$

$D_0 \quad D_1 \quad \{0,1\}^n$

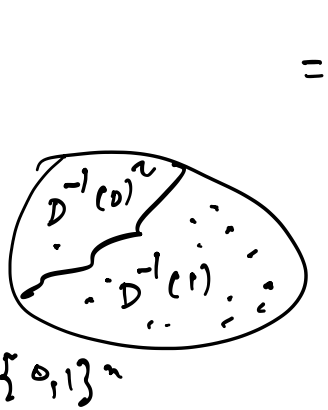
$p_1, p_2 \dots p_{2^n} \quad q_1, q_2 \dots q_{2^n}$

$\boxed{y}$ is outcome of an exp.

$D : \{0,1\}^n \to \{0,1\}$.

if $D(y) = 1$, { D says y is generated by D_1 }

$= 0$ { D says y is generated by D_0 }



if $y \in D^{-1}(1) \to D$ is correct

if y is generated by D_1

Pr y gen. by $D_1 \in D^{-1}(1)$

$= \sum_{i \in D^{-1}(1)} q_i$

Dr y is indeed gen by D_0

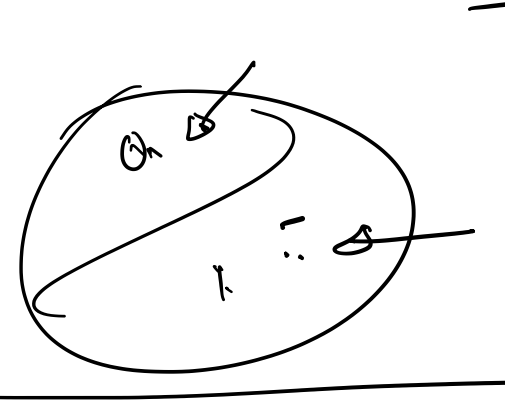
$\sum_{i \in D^{-1}(1)} p_i$.

$E_0 \quad Pr_{D_0}(D(y) = 1)$ — Wrong.

$E_1 \quad Pr_{D_1}(D(y) = 1)$. — Correct

$| E_0 - E_1 | \geq \epsilon$

$| E_0 - E_1 | \leq neg(n) \quad \{= 0\}$



$D : \{0,1\}^n \to \{0,1\}$.

$\boxed{y}$ — p_y — D_0

— q_y — D_1

$q_y \cdot Pr(D(y) = 1)$

$E_1 = \sum_{y \in \{0,1\}^n} q_y \cdot Pr(D(y) = 1)$

$E_0 = \sum_{y \in \{0,1\}^n} p_y \cdot Pr(D(y) = 1)$.

$E_1 = \sum_{y \in D^{-1}(1)} q_y$.

$E_0 = \sum_{y \in D^{-1}(1)} p_y$

The prob that y in $D^{-1}(1)$ is generated by D_0 is $\sum_{y \in D^{-1}(1)} p_y$

So ~~[illegible]~~ when y is dec as generated by D_1 as done by D, then D is wrong.

$\therefore$ D is wrong with prob E_0.

The prob that y in $D^{-1}(1)$ is generated by D_1 is

$E_1 = \sum_{y \in D^{-1}(1)} q_y$.

$\therefore$ When this event occurs & when D declares that y is generated by D_1, it is correct.

D is correct with prob E_1.

~~Distin~~ D is called ϵ - Distinguisher if $| E_0 - E_1 | \geq \epsilon$.

---

if the outcome is generated by D_1 & if D says the outcome is by D_1, then D is correct.

if the outcome is generated by D_0 & if D says it is generated by D_1 the D is wrong.

if $y \in D^{-1}(1)$, D says y is generated by D_1

if $Pr(D(y) = 1) = t_y$.

Then D says y is generated by D_1 with prob t_y.

For Det D:

$(Cor - err)| = | \sum_{y \in D^{-1}(1)} q_y - \sum_{y \in D^{-1}(1)} p_y |$

for Rand D.

$| \quad | = | \sum_{y \in \{0,1\}^n} q_y \cdot t_y - \sum_{y \in \{0,1\}^n} p_y \cdot t_y$

E_0, E_1

---

perfect Randomness – Uniform Dist

PRBG URBG $\to$

$\downarrow$

Deterministic algo.

$f : \{0,1\}^k \to \{0,1\}^l, \quad l \geq k+1$.

$\to f$ is poly – in k. $\{\Rightarrow l$ is also poly in k$\}$.

$\boxed{D : \{0,1\}^l \to \{0,1\}}$

$y \in \{0,1\}^l$ – either generated by f or uniform Dis (coin toss) (l unbiased coin toss)

Let D be a PPT

page 62 – Jonathan Katz. (2nd edi).

$G : \{0,1\}^n \to \{0,1\}^l, \quad l \geq n+1$

$| \underset{s \in \{0,1\}^n}{Pr}(D(G(s)) = 1) - \underset{r \in \{0,1\}^l}{Pr}(D(r) = 1) |$

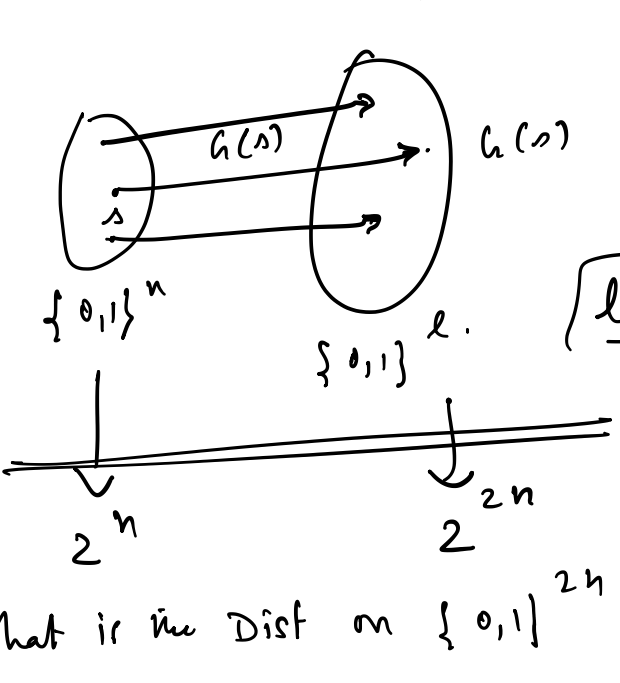
$\leq neg(n)$

$D : \{0,1\}^l \to \{0,1\}$

output of $G \in \{0,1\}^l$

we assume ~~s~~ s is unknown

$\therefore$ s is uniform $\in \{0,1\}^n$.



$\boxed{l = 2n}$

What is the Dist on $\{0,1\}^{2n}$ induced by G?

$G \updownarrow \underbrace{\frac{1}{2^n}, \frac{1}{2^n} \dots \frac{1}{2^n}}_{2^n}, \underbrace{0, 0, 0, \dots 0}_{2^{2n} - 2^n}$ $\frac{(2^n - 1)}{2^n}$.

$\updownarrow \frac{1}{2^{2n}} \frac{1}{2^{2n}} \frac{1}{2^{2n}} \dots \frac{1}{2^{2n}} \dots \frac{1}{2^{2n}}$

$\{ \frac{poly}{2^{2n}} = neg$ small

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

f is one way fun.

$hc(x)$.

$x \in \{0,1\}^n$

$\downarrow$

$\underbrace{f(x)}_{n} \| \underbrace{hc(x)}_{1}$

$\left\{ \begin{array}{l} G(x) = f(x) \| hc(x) \\ \{0,1\}^n \to \{0,1\}^{n+1} \end{array} \right\}$

$\downarrow$

$\{0,1\}^{n+1}$ uniform

page 258 – 259 (Katz, 2nd ed)

$f : \underset{\underset{seed}{\downarrow}}{\{0,1\}^n} \to \{0,1\}^l, \quad l > n$

$l = n+1$.

---

f is a one-way permutation: //

$s \underset{u}{\leftarrow} \{0,1\}^n, \quad f(s) \underset{u}{\leftarrow} \{0,1\}^n$.

$hc(s) \quad \left\{ \frac{f(s) \| hc(s)}{r \in \{0,1\}^{n+1}} \right\}$

$hc : \{0,1\}^* \to \{0,1\}$. hardcore for f.

$\underset{x \leftarrow \{0,1\}^n}{Pr} [A(1^n, f(x)) = hc(x)]$

for any PPT A $\leq \frac{1}{2} + neg(n)$

$D : \{0,1\}^{n+1} \to \{0,1\}$.

$\left\{ \begin{array}{l} \underset{r \leftarrow \{0,1\}^{n+1}}{Pr} [D(r) = 1] \\ - \underset{s \leftarrow \{0,1\}^n}{Pr} [D(G(s)) = 1] \end{array} \right.$

$\leq neg(n)$.

$\to G(s) = \underbrace{f(s)}_{n} \| \underbrace{hc(s)}_{1}$ — ①

$|G(s)| = n+1$

For any PPT D

$\underset{r \leftarrow \{0,1\}^{n+1}}{Pr} [D(r) = 1]$ //

$= \underset{r \in \{0,1\}^n, r' \in \{0,1\}}{Pr} \quad Pr(D(r \| r') = 1)$

$= \underset{s \leftarrow \{0,1\}^n, r' \in \{0,1\}}{Pr} \quad (D(f(s) \| r') = 1)$

$= \frac{1}{2} \cdot Pr(D(f(s)) \| hc(s))$

$+ \frac{1}{2} \cdot Pr(D(f(s)) \| \overline{hc(s)})$

$\underset{r \leftarrow \{0,1\}^{n+1}}{Pr} (D(r) = 1)$ ||

$\left\{ \begin{array}{l} = \underset{s \leftarrow \{0,1\}^n}{Pr} (D(f(s) \| hc(s)) = 1) \cdot \frac{1}{2} \\ + \underset{s \leftarrow \{0,1\}^n}{Pr} D(f(s) \| \overline{hc}(s)) = 1) \cdot \frac{1}{2} \end{array} \right.$

$- \underset{s \in \{0,1\}^n}{Pr} [D(\underbrace{f(s) \| hc(s)}_{G(s)}) = 1)$

$= \frac{1}{2} [Pr(D(f(s) \| \overline{hc}(s)) = 1)$

$- Pr(D(f(s) \| hc(s)) = 1)]$

To prove (neg)

$\to \| \underset{r \leftarrow \{0,1\}^{n+1}}{Pr}(D(r) = 1) - \underset{s \in \{0,1\}^n}{Pr}(D(f(s) \| hc(s)) = 1)$

$\leq neg(n)$

$\to$ we prove this $\left\{ \frac{1}{2} \left[\begin{array}{l} \underset{s \leftarrow \{0,1\}^n}{Pr} (D(f(s) \| \overline{hc}(s)) = 1) \\ - \underset{s \leftarrow \{0,1\}^n}{Pr} (D(f(s) \| hc(s)) = 1) \end{array} \right] \right.$

$\leq neg(n)$.

A – PPT Going to use D.

A is attempting to guess $hc(s)$ using $y = f(s)$

~~A(f(s))~~.

$A(y). \equiv A(f(s))$.

① choose uniform $r' \in \{0,1\}$.

② Run $D(y \| r')$

③ if D outputs 0, A outputs r'. (as the guess for HC(s))

if D outputs 1 ||

A outputs $\overline{r'}$. (as the guess for HC(s))

Now we compute the $Pr(A(y) = hc(s))$

$= Pr(A(f(s)) = hc(s))$

$= \frac{1}{2} \cdot Pr(A(f(s)) = hc(s)) | hc(s) = r')$

$+ \frac{1}{2} \cdot Pr[A(f(s)) = hc(s)) | hc(s) \neq r')$

$[Pr(A) = Pr(A|x) \cdot Pr(x) + Pr(A|\bar{x}) \cdot Pr(\bar{x})$

When ~~Since~~ $hc(s) = r'$

we want A to output r'.

A outputs r' iff $D(y \| r') = 0$.

iff $D(y \| hc(s)) = 0$.

iff $D(f(s) \| hc(s)) = 0$

$\to \left\{ \begin{array}{l} Pr(A \text{ outputs } hc(s)) \text{ when } r' = hc(s) \\ = Pr(D(f(s) \| hc(s)) = 0) \\ = 1 - Pr(D(f(s) \| hc(s)) = 1) \end{array} \right.$

$Pr(A$ outputs $hc(s))$ when $r' \neq hc(s)$.

$\Rightarrow \overline{r'} = hc(s)$

$= Pr(D(f(s) \| \overline{hc}(s)) = 1)$

$Pr(A$ outputs $hc(s))$ ||

$= \frac{1}{2} Pr(A$ outputs $hc(s))$ when $r' = hc(s)$

$+ \frac{1}{2} \cdot Pr(A$ outputs $hc(s)|$ when $r' \neq hc(s)$

$= \frac{1}{2} [1 - Pr[D(f(s) \| hc(s)) = 1]]$

$+ \frac{1}{2} [Pr(D(f(s) \| \overline{hc}(s)) = 1]$

$= \frac{1}{2} + \frac{1}{2} (Pr(D(f(s) \| \overline{hc}(s)) = 1$

$- Pr(D(f(s) \| hc(s) = 1))$

$= \frac{1}{2} + neg(n)$

$\Rightarrow Pr(D(f(s) \| \overline{hc}(s)) = 1)$

$- D(f(s) \| hc(s)) = 1)$

$= neg(n)$

We proved what we want ✓

$\underset{r \leftarrow \{0,1\}^{n+1}}{Pr} \quad D(r) = 1 \quad \to \frac{G(s)}{f(s) \| hc(s)}$

$- \underset{s \leftarrow \{0,1\}^n}{Pr} \quad D(\underbrace{f(s) \| hc(s)}_{G(s)}) = 1$

$= neg(n)$ ✓

$\overset{(n+1)}{r} = \overset{n}{\bar{r}} \| \overset{1 \text{ rand}}{r'}$

$-1 + \frac{1}{2} \frac{1}{2} \left\{ \begin{array}{l} f(s) \| hc(s) \\ \| \overline{hc}(s) \end{array} \right\}$ conditionally,

$D(f(s) \| \overline{hc}(s)))$

(n+1) random bit.

algo (n+1) bits.

$D : \{0,1\}^{n+1} \to \{0,1\}$

~~$Pr[D(r) = 1]$~~ ; .8 .

$\underset{x \leftarrow \{0,1\}^{n+1}}{Pr} D(x) = 1$

~~.61~~ .72

$\underset{\substack{x = G(s) \\ s \leftarrow \{0,1\}^n}}{Pr} D(x) = 1$

~~.64999999~~

.72000000l

p 258 - 259

J. Katz.

prangan55@gmail.com