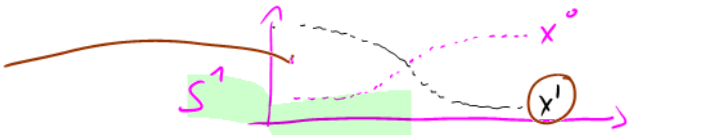
$p^0_z := \Pr[X^0 = z]$

$p^1_z := \Pr[X^1 = z]$

$d_z := \frac{p^1_z}{p^0_z + p^1_z}$



$\Pr[\, d_z \geq \Delta \mid z \in S^1]$

$z \leftarrow X^1$

Statistical Tools:

Expectation

$\mathbb{E}(\mathcal{A}) := \sum_{z \in \mathrm{Supp}(\mathcal{A})} z \cdot \Pr[\mathcal{A} = z]$

$\mathbb{R}$ $0,1$

Markov: + general − not very tight

non-negative random variables $\mathcal{A}$

positive real numbers v

$$\Pr[\mathcal{A} \geq v \cdot \mathbb{E}(\mathcal{A})] \leq \frac{1}{v}$$

Chernoff + very tight + useful specialcase − special case

$p \leq \frac{1}{2}$ $\quad \Pr[\mathrm{Exp}_i = 1] = p$

$$\Pr\left[\sum_{i=1}^{n} \mathrm{Exp}_i > (p+\epsilon)n\right] < 2 \cdot e^{-\epsilon^2 n}$$

$0,1$

ϵ small, ϵ^2 smaller

X^0, X^1 $\quad \Delta(X^0, X^1)(n) := SD(X^0(1^n), X^1(1^n))$

$\delta(n)$ is a $CD(X^0, X^1)$

$\rightarrow$ $\Delta(X^0, X^1) \geq \delta(n) + n^{-c}$

Claim: $f(b, r) := X^b(r)$ is a distributional OWF.

Proof: Assume tow. contr. $\forall$ const c_f

$\exists$ PPT adversary $\mathcal{A}$

$SD\left[\left(\mathcal{A}(f(U_1, U_{|r|}), f(U_1, U_{|r|})\right), \left(U_1, U_{|r|}, f(U_1, U_{|r|})\right)\right] \leq n^{-c_f}$ for large n.

to show: transform $\mathcal{A}$ into PPT $\mathcal{D}$

$X^b(1^n; r)$

$\mathcal{D}(z)$

For $i = 1 \ldots t$

$b_i \| r_i \leftarrow \mathcal{A}(z)$

$b \leftarrow \mathrm{MAJ}\, b_i$

ret b.

$\Pr[1 = \mathcal{D}(X^1)] - \Pr[1 = \mathcal{D}(X^0)]$ $\quad$ $p^{1\|1} \geq 1$

$\geq \Pr[X' \in S^1] \cdot p^{1\|1} - \Pr[X^0 \in S^1] \cdot p^{0\|1}$

$+ \Pr[X' \in S^-] \cdot p^{1\|-} - \Pr[X^0 \in S^-] \cdot p^{0\|-}$

$+ \Pr[X' \in S^0] \cdot p^{1\|0} - \Pr[X^0 \in S^0] \cdot p^{0\|0}$

$\geq (1-\epsilon)\Delta(X^0, X') + \epsilon \cdot 0 - \epsilon$

$= (1-\epsilon)\Delta(X^0, X') - \epsilon$

$S^0 := \{z : \Pr[X^0 = z] > \Pr[X' = z]\}$

$S^- := \{z : \Pr[X^0 = z] = \Pr[X' = z]\}$

$S^1 := \{z : \Pr[X^0 = z] < \Pr[X' = z]\}$

$p^{1\|1} := \Pr[1 = D(x') \mid x' \in S^1]$

$p^{1\|-} := \Pr[1 = D(x') \mid x' \in S^-]$

Claim:

$p^{1\|1} \geq 1 - \epsilon$

$p^{0\|0} \leq \epsilon$

$(1-\epsilon)\Delta(X^0, X') - \epsilon > \delta(n)$

$\Leftrightarrow \Delta(n) - \delta(n) > 2\epsilon$

$n^{-c} > 2\epsilon$

Task: Choose c_f & t s.t. $2\epsilon < n^{-c}$

$\mathcal{D}(z)$ We can choose t

For $i = 1 \ldots t$

$b_i \| r_i \leftarrow \mathcal{A}(z)$

$b \leftarrow \mathrm{MAJ}\, b_i$

ret b.