# Lec 10 & 11: Random extractors

Extractors: obtaining good randomness from weak randomness

**Def:** $\text{Ext}: [N) \times [D] \longrightarrow [M)$ $(k, \varepsilon)$ extractor

if $\forall$ R.V. $X \in [N]$ with $H_{min}(X) \geq k$

$\text{Ext}(X, U_d) \approx_\varepsilon U_m$

**Thm:** Fix $n, k, \varepsilon$ and take $m = k + d - 2\log 1/\varepsilon + O(1)$

$d = \log(n-k) + 2\log 1/\varepsilon + O(1)$

$\text{Ext}: [N] \times [D] \longrightarrow [M)$ random function

$\Longrightarrow$ Ext is $(k, \varepsilon)$ extractor with high prob.

**Remark** seed size is log (useful for randomized alg.)

randomness size is $k + d$ (get seed back indirectly)

**Strong extractors:** $\text{Ext}: [N) \times [D] \longrightarrow [M)$ strong $(k, \varepsilon)$

exctractor if $\forall X$ $H_{min}(X) \geq k$

$\text{Ext}(X, U_d), U_d \approx_\varepsilon U_{m+d}$

**Thm** Above result holds for $m = k - 2\log 1/\varepsilon + O(1)$

for strong extractors

$$\| P_{\text{Ext}(X, U_d)\, U_d} - P_{U_m} \times P_{U_d} \|_1 \leq \varepsilon$$

**Fact:** $P_{Y|X}$ $Q_{Y|X}$ two prob. dist

$P_X$ marginal dist

$$\| P_{Y|X} \times P_X - Q_{Y|X} \times P_X \|_1 = \mathbb{E}_{x \sim P_X} \| P_{Y|X=x} - Q_{Y|X=x} \|_1$$

$$\mathbb{E}_{s \sim U_d} \| P_{Ext(X, s)} - P_{U_m} \|_1 \leq \epsilon$$

$Ext(\cdot, s)$ is fixed

---

Let $\mathcal{H} \subseteq \{ f : [N] \to [M] \}$

We call $\mathcal{H}$ two universal if

$$\Pr_{h \sim \mathcal{H}} [h(x) = h(x')] \leq \frac{1}{M} \quad \forall\, x, x'$$

$\mathbb{F}_2^n$ as finit field

$s \in \mathbb{F}_2^n$ $(x \cdot s)$ last $m$ bits

$h_s(x) := $ last $m$ bits of $(x \cdot s)$

$\Pr[\, (x+s)$ last bit $= (x'+s)$ last bit $]$

$\Pr[\, (x \cdot s) = (x' \cdot s) \,]$

$(x \cdot s) = y$

$$\sum_{s -} \Pr[x \cdot s = y] \; \Pr[x' \cdot s = y']$$

$$\Pr_s [\, Ext(x, s) = Ext(x', s) \,]$$

$(x \cdot s)_m$ $(x' \cdot s)_m$

$(x \cdot s)$

$(s)_m = (x \cdot s)_m$ $\exists\, R$ $R \| (s)_m$

$0a^s \longmapsto x \cdot s$ $s \cdot (x \oplus x') = (0 \| r)$

If Ext is two universal $m \leq k - 2\log 1/\varepsilon$

$\Longrightarrow$ Ext $(k, \varepsilon)$ strong extractor

---

$$\Pr\left( (Ext(x,s), s) = (Ext(x',s'), s') \right)$$

$$\frac{1}{D} \cdot \Pr_{s}\left[ Ext(x,s) = Ext(x',s) \mid s = s' \right]$$

---

Classical side info

$X, Y$ $\qquad Ext : [N] \times [D] \longrightarrow [M]$

$$P_{Ext(X, U_d), Y, U_d} \approx_\varepsilon P_{U_m} \times P_Y \times P_{U_d}$$

---

Question is how much info can be obtained

$$H_{min}(X|Y) = \mathbb{E}_{y} H_{min}(X|Y=y)$$

$Y, Z$ ind $n$ bit random varib

$B = Ber(1/2)$ $\qquad P(x \mid b=0, y)$

$$X = \begin{cases} Y & B=0 \\ Z & B=1 \end{cases}$$

$$H_{min}(X|Y) = -\log \underbrace{\mathbb{E}_{y} \max_{x} P(x|y)}$$

$$P_{guess}(X|Y) = \sup_{f : \mathcal{Y} \to \mathcal{X}} \Pr[f(Y) = X]$$

If $H_{min}(X|Y) \geq k \Longrightarrow \Pr_{y \sim P_Y}\left[ H_{min}(X|Y=y) \geq k - \log 1/\varepsilon \right]$

$\geq 1-\varepsilon$

**Lem** If $Ext : [N] \times [D) \longrightarrow [M)$ $(k, \varepsilon)$ - extractor

$X, Y$ $\quad H_{min}(X|Y) \geq k + \log 1/\varepsilon$

$$\Longrightarrow \big(Ext(X, U_m), Y\big) \approx_{2\varepsilon} (U_m, Y)$$

**Quantum side infor**

$$\rho_{XA} \xrightarrow{Ext} \rho_{U_m} \otimes \rho_A$$

$$H_{min}(X|A) = \log \frac{1}{P_{guess}(X|A)} \qquad P_{guess}(X|A) = \inf_{\{M_x\}} \sum_x tr(\rho^x M_x)$$

- $\exists$ Ext : 1) it extract randomness wrt classical side info
  2) it cannot extract randomness wrt. quantum side info

- left over hash lemma works for quantum side info