Hybrid arguments: ...

Wednesday, 11 November 2020 3:56 PM

Suppose there is an ϵ-dist:

p_f p_u. $f : \{0,1\}^k \to \{0,1\}^\ell$.

$| E_{dist}(p_f) - E_{dist}(p_u) | \geq \epsilon$.

$dist : \{0,1\}^\ell \to \{0,1\}$.

For $0 \leq i \leq \ell$

q_i be the distribution on $(Z_2)^\ell$ where first i bits are generated by f and remaining $\ell - i$ bits are uniformly generated.

$$\begin{cases} q_0 - p_u \text{ on } \{0,1\}^\ell. \\ q_\ell - p_f \end{cases}$$

$|E(q_0) - E(q_\ell)| \geq \epsilon$.

$|a-b| \leq |a-c| + |c-b|$

$|x+y| \leq |x| + |y|$.

$|a - c + c - b|$

$|a-b| \leq |a-a_1| + |a_1 - a_2| + |a_2 - a_3| \dots |a_n - b|$

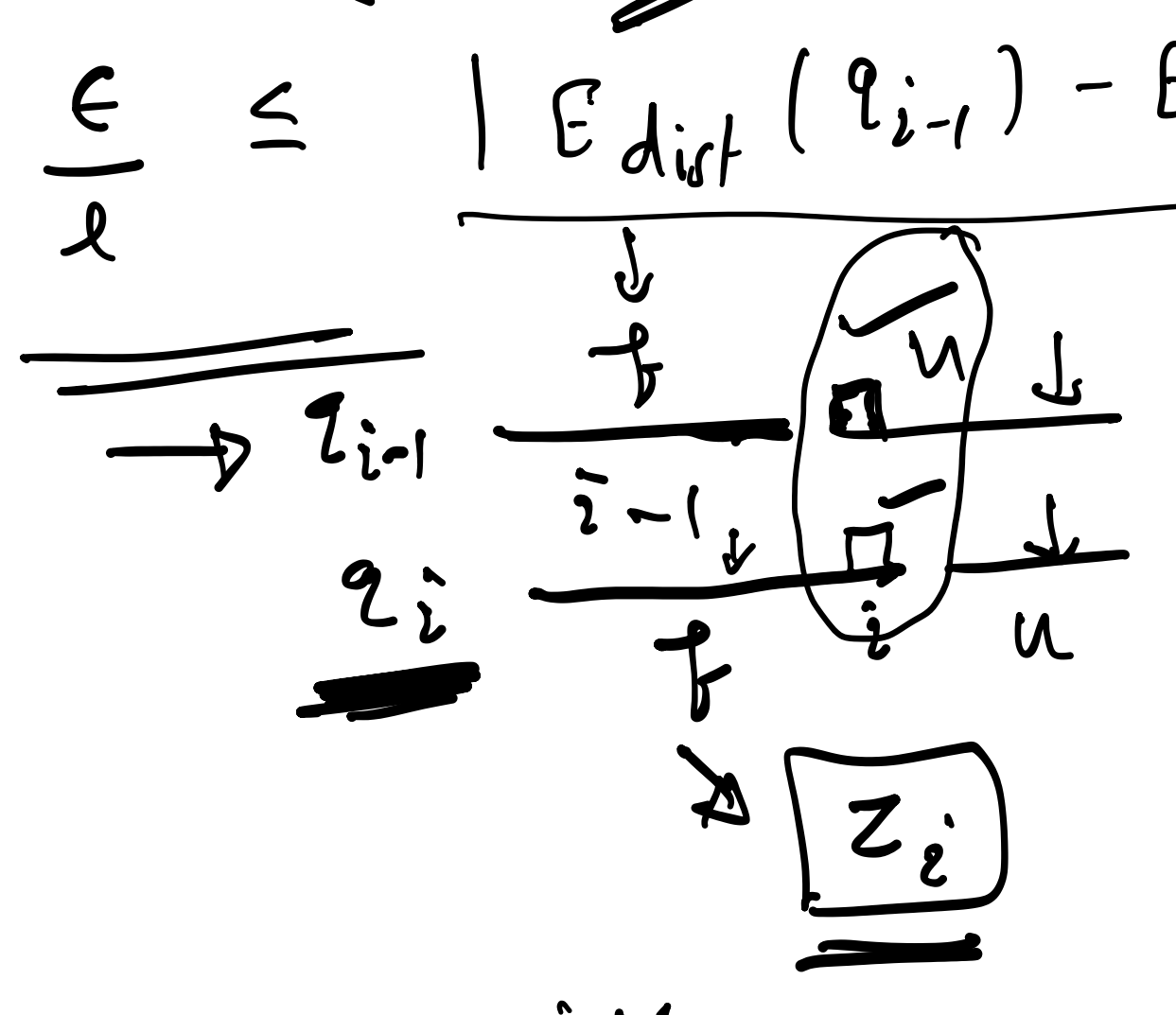
$(a-b) = a - a_1 + a_1 - a_2 + a_2 \dots - a_n + a_n - b$.

$$\epsilon \leq | E_{dist}(q_0) - E_{dist}(q_\ell) |$$

$$\leq \sum_{i=1}^{\ell} | E_{dist}(q_{i-1}) - E_{dist}(q_i) |$$

$\Rightarrow \exists$ an $i \ni$

$$\frac{\epsilon}{\ell} \leq | E_{dist}(q_{i-1}) - E_{dist}(q_i) |$$



$NBP : \{Z_2^{i-1}\} \to Z_2$. ?

$(\dots)$ $i-1$ bits gen by f

// Consider the case //

$$E_{dist}(q_{i-1}) - E_{dist}(q_i) \geq \frac{\epsilon}{\ell}.$$

$dst(z_1 z_2 \dots z_\ell) = 1$
dst believes that $z_1 z_2 \dots z_\ell$ is generated by q_{i-1}

$dst(z_1 \dots z_\ell) = 0$
dst believes that $z_1 \dots z_\ell$ is generated by q_i.

if $dst(z_1 \dots z_\ell) = 1$
then dst believes that z_i is uniform.

if $dst(z_1 \dots z_\ell) = 0$
- - - - - z_i is generated by f.

$NBP(z^{i-1}) \to (z_1 \dots z_{i-1})$
(1) choose $z_i \dots z_\ell$ uniformly
$z = dst(z_1 z_2 \dots z_{i-1} z_i \dots z_\ell)$
Return $(z + z_i) \bmod 2$.

Suppose $z = 1$, $\Rightarrow$ dst believes z_i is uniform
$\Rightarrow$ dst bec f would produce only $\bar{z}_i$.
$\Rightarrow$ NBP should output $\bar{z}_i$.

Suppose $z = 0$ dst believes $z_1 \dots z_\ell$ is gen by q_i
$\Rightarrow z_i$ is generated by f
$\Rightarrow z_i$ must be output

$\rightarrow ((z_i + z) \bmod 2)$

$$\geq \frac{1}{2} + \frac{\epsilon}{\ell}$$

$$\sum_{z^{i-1} \in (Z_2)^{i-1}} p_f(z^{i-1}) \times Pr[z_i = nbp(z^{i-1})]$$

$$q_{i-1}(z^\ell) \times Pr(Z_i = z_i) | z^{i-1}$$

$$= \frac{q_i(z^\ell)}{2}.$$

$$q_{i-1}(z^\ell) \times Pr(Z_i = z_i \mid z^{i-1})$$

$$= q_{i-1}(z^{i-1}) \times \frac{1}{2^{\ell-i+1}} \times Pr(Z_i = z_i \mid z_{i-1})$$

$$= \frac{q_i(z^i)}{2} \cdot \frac{1}{2^{\ell-i}}$$

$$= \frac{q_i(z^\ell)}{2}$$

$q_{i-1}(z^\ell)$

$q_{i-1}(z^{i-1}) \cdot (\ell - i + 1)$ uniform bits

$$q_{i-1}(z^\ell) \times Pr(Z_i = z_i \mid z^{i-1}) = \frac{q_i(z^\ell)}{2}. \quad (***)$$

Advantage of NBP

$$= \sum_{z^{i-1} \in (Z_2)^{i-1}} p_f(z^{i-1}) \cdot Pr(Z_i = NBP(z^{i-1}))$$

$$= \sum_{z^\ell \in (Z_2)^\ell} q_{i-1}(z^\ell) \cdot Pr(Z_i = NBP(z^{i-1}))$$

z^i if $dst(z^\ell) = 0$

$$= \sum_{z^\ell \in (Z_2)^\ell} q_{i-1}(z^\ell) \Big[Pr(Dist(z^\ell) = 0) \times Pr(Z_i = z_i \mid z^{i-1}) + Pr(Dst(z^\ell) = 1) \times Pr(Z_i \neq z_i \mid z^{i-1}) \Big]$$

$$= \sum q_{i-1}(z^\ell) \Big[1 - Pr(Dist(z^\ell) = 1) \times Pr(Z_i = z_i) + Pr(Dst(z^\ell) = 1)(1 - Pr(Z_i = z_i \mid z^{i-1})) \Big].$$

$$= \sum_{z^\ell} \Big[q_{i-1}(z^\ell) \cdot Pr(Z_i = z_i \mid z^{i-1}) \Big] \to \frac{q_i(z^\ell)}{2}.$$
$$- 2 \cdot q_{i-1}(z^\ell) \cdot Pr(Dst(z^\ell) = 1) \cdot Pr(Z = z_i \mid z^{i-1})$$
$$+ q_{i-1}(z^\ell) \cdot Pr(Dst(z^\ell) = 1)$$

$$= \frac{1}{2} + \{ q_{i-1}(z^\ell) \cdot Pr(Dst(z^\ell) = 1) \to E_{q_{i-1}}$$
$$- q_i(z^\ell) \cdot Pr(Dst(z^\ell) = 1) \} \; E_{q_i}$$

$$\geq \frac{1}{2} + \frac{\epsilon}{\ell}$$

---

if g have an ϵ dist between p_f & p_u

$\Rightarrow g$ have $\frac{\epsilon}{\ell}$ dist betw q_{i-1} & q_i.

$\Rightarrow$

Stinson pp 330-335

Next class only on 23rd