STARTING OF THE ACTUAL TECHNICAL PART

§ 2 Preliminaries

Global Notation:

λ: Security parameter.

negl : any negligible f^n

i.e. f s.t. $\forall$ constants $c \in \mathbb{N}$
$\exists$ $N \in \mathbb{N}$
s.t. $\forall$ $n > N$,
$f(n) < n^{-c}$

Let: A be an alphabet.
$x \in A^n$

Def^n: $h(x)$ = # non zero values of x. (Hamming Distance)

$w(x) := \frac{h(x)}{n}$ (relative Hamming distance)

Let: $x, y \in A^n$

Def^n: $\Delta(x,y) := w(x \ominus y)$ is the relative Hamming distance b/w x & y

(∵ wherever x & y match, $x \ominus y$ does not see a contribution at those indices)

§ 2.1 Quantum preliminaries

X : Used for both the system/register & the associated Hilbert space $\mathbb{C}^{2^n}$

n-qubit register.

Recall : Pure & mixed states.

· Quantum operation := CPTP map from X to Y,

i.e. $F(\rho^X) = \tau^Y$

Not^n: $Y \leftarrow F(X)$.

(leaving states implicit)

: Unitary $U: X \to X$ $\quad U^\dagger U = UU^\dagger = \mathbb{I}^X$

: Projector : Π function s.t. $\Pi^2 = \Pi$

Projective Measurement : $\{\Pi_i\}$ projectors s.t.

$$\sum \Pi_i = \mathbb{I}$$

: Trace : Tr

Partial trace : Tr^Y – claim unique operation s.t.

$\forall (\rho, \tau)^{XY}$, $\mathrm{Tr}^Y(\rho, \tau) = \mathrm{Tr}(\tau)\rho$.

: Trace Distance $\quad TD(\rho,\tau) := \frac{1}{2}\|\rho-\tau\|_1$

$$:= \frac{1}{2}\mathrm{tr}\sqrt{(\rho-\tau)^\dagger(\rho-\tau)}$$

: TD is an upper bound on the prob. that any (even unbounded) alg. distinguishes ρ & τ.

Lemma 2.1 (Gentle measurement [Win 99]).

Let
- ρ^* be a quantum state.
- $(\Pi, \mathbb{1}-\Pi)$ be a proj measurement on X s.t. $\mathrm{tr}(\Pi\rho) \geq 1-\delta$.
- $\rho' := \frac{\Pi\rho\Pi}{\mathrm{tr}(\Pi\rho)}$ ~ post-selected state (to first outcome) after measuring ρ

Then $\quad TD(\rho,\rho') \leq 2\sqrt{\delta}$.

Notation: For $x,\theta \in \{0,1\}^\lambda$, $\quad |x\rangle_\theta := H^{\theta_1}|x_1\rangle \otimes \cdots \otimes H^{\theta_\lambda}|x_\lambda\rangle$

Notation: Non-uniform quantum poly Time (QPT) machine

$\{A_\lambda, |\psi\rangle_\lambda\}_{\lambda\in\mathbb{N}}$ a family of

poly-sized quantum machines A_λ
where each is initialized w/ a poly-sized advice state $|\psi_\lambda\rangle$

Each A_λ is in general described by a CPTP map.

: $y \leftarrow A(x)$, we mean the machine A takes register x & produces register y.

(states are implicit)

: Interactive machine : sequence of quant. operations with designated input/output & work register.

§ 2.2 The XOR extractor

Story: the XOR function is a good randomness extractor from certain quantum sources of entropy — even given quantum side info.

Theorem 2.2 Let
- X be an n-qubit register, and
- consider any quantum state $|\gamma\rangle^{A,X}$ of the form

$$\sum_{u.\, h(u) < n/2} |\psi_u\rangle^A \otimes |u\rangle^X$$

(recall that
$h(\cdot)$ denotes the Hamming weight)

- $\rho^{A,P}$ be the mixed state that results from measuring x in the Hadamard basis to produce a string $x \in \{0,1\}^n$ & writing $\bigoplus_{i\in[n]} x_i$ into a single qubit register P.

Then it holds that

$$\rho^{A,P} = \mathrm{tr}^x\left(|\Psi\rangle\langle\Psi|\right) \otimes \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right).$$

Proof

Story. Write the state on $A\times P$ from applying Hadamards & recording the parity in P.

We use $p(x) := \bigoplus_{i\in[n]} x_i$.

$$\text{Def}^n: |\Psi\rangle^{A\times P} := \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} \underbrace{\left(\sum_{u:h(u)<n/2} (-1)^{u\cdot x} |\psi_u\rangle^A\right)}_{:=|\phi_x\rangle^A} |x\rangle^X |p(x)\rangle^P$$

NB: $\mathrm{Tr}^X |\Psi\rangle\langle\Psi| = \rho^{AP}$

$$\therefore \rho^{AP} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} |\phi_x\rangle\langle\phi_x| \otimes |p(x)\rangle\langle p(x)|$$

$$= \frac{1}{2^n} \sum_{x:\, p(x)=0} |\phi_x\rangle\langle\phi_x| \otimes |0\rangle\langle 0| +$$

$$\frac{1}{2^n} \sum_{x:\, p(x)=1} |\phi_x\rangle\langle\phi_x| \otimes |1\rangle\langle 1|$$

$$= \frac{1}{2^n} \sum_{x:\, p(x)=0} \left(\sum_{\substack{u_1, u_2: \\ h(u_1), h(u_2) < n/2}} (-1)^{(u_1 \oplus u_2)\cdot x} |\psi_{u_1}\rangle\langle\psi_{u_2}| \right) \otimes |0\rangle\langle 0|$$

$$+ \frac{1}{2^n} \sum_{x:\, p(x)=1} \left(\sum_{\substack{u_1, u_2: \\ h(u_1), h(u_2) < n/2}} (-1)^{(u_1 \oplus u_2)\cdot x} |\psi_{u_1}\rangle\langle\psi_{u_2}| \right) \otimes |1\rangle\langle 1|$$

$$= \sum_{\substack{u_1, u_2: \\ h(u_1), h(u_2) < n/2}} |\psi_{u_1}\rangle\langle\psi_{u_2}| \otimes \left(\frac{1}{2^n} \sum_{x:\, p(x)=0} (-1)^{(u_1 \oplus u_2)\cdot x} |0\rangle\langle 0| + \right.$$

$$\left. \frac{1}{2^n} \sum_{x:\, p(x)=1} (-1)^{(u_1 \oplus u_2)\cdot x} |1\rangle\langle 1| \right)$$

Claim 2.3: For any $u \in \{0,1\}^n$ s.t. $u \notin \{0^n, 1^n\}$, it holds that

$$\sum_{x:\, p(x)=0} (-1)^{u\cdot x} = \sum_{x:\, p(x)=1} (-1)^{u\cdot x} = 0$$

NB: $u_1 \oplus u_2$ is never equal to 1 $\because h(u_1), h(u_2) < n/2$.

$u_1 \oplus u_2 = 0$ when $u_1 = u_2$.

So $\sum_{x:\, p(x)=0} (-1)^{(u_1 \oplus u_2)\cdot x}$ essentially behaves like a delta, $2^{\frac{n}{2}} \delta_{u_1, u_2}$

as does $\sum_{x:\, p(x)=1} (-1)^{(u_1 \oplus u_2)\cdot x}$

$$= \sum_{u : h(u) < n/2} |\psi_u\rangle\langle\psi_u| \otimes \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \right)$$

$$= \mathrm{Tr}^*(|r\rangle\langle r|) \otimes \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \right)$$ □

Story: So it remains to prove the claim

[Proof of Claim 2.3:

Suppose: $u \notin \{0^n, 1^n\}$.

Define: $S_0 = \{i : u_i = 0\}$ indices where u is zero
$S_1 = \{i : u_i = 1\}$ indices where u is one.

Def^n: Let $y_0 \in \{0,1\}^{|S_0|}$
$y_1 \in \{0,1\}^{|S_1|}$ &

$x_{y_0 y_1} \in \{0,1\}^n$ is the n-bit string

that is y_0 on S_0 &

y_1 on S_1.

(e.g. $u = \underbrace{000}\ \underbrace{111}$

$S_0 = 1,2,3$
$S_1 = 4,5,6$

$x_{100,010} = 100\,010$

$\therefore x_{100,010}$ restricted to indices S_0 is 100
" " S_1 is 010.)

$x : P(x) = 0$ $\quad$ $x : P(x) = 1$

Then, note:

$$\sum_{x : p(x)=0} (-1)^{u \cdot x} = \sum_{\substack{y_0 \in \{0,1\}^{|S_0|} \\ y_1 \in \{0,1\}^{|S_1|} \\ : p(x_{y_0 y_1})=0}} (-1)^{u \cdot x_{y_0 y_1}}$$

(NB: $u \cdot x_{y_0 y_1} = \underbrace{(1 \cdots 1)}_{|S_1| \text{ many 1's}} \cdot y_1 = p(y_1)$ ∵ y_0 is on indices where u is zero)

$$[*] = \sum_{\substack{y_0 \in \{0,1\}^{|S_0|} \\ y_1 \in \{0,1\}^{|S_1|} \\ : p(x_{y_0 y_1})=0}} (-1)^{p(y_1)}$$

(NB: $p(x_{y_0 y_1}) = p(y_0 y_1)$ ∵ $x_{y_0 y_1}$ is just $y_0 y_1$ but re-arranged

: For a given y_1, half the y_0's would make $p(y_0 y_1) = 0$.)

$$= \sum_{y_1 \in \{0,1\}^{|S_1|}} 2^{|S_0|-1} (-1)^{p(y_1)}$$

$$= 0$$

Closing argument: $p(x_{y_0 y_1}) = 0$ was used starting [*] &

The same equalities also hold when

$$p(x_{y_0 y_1}) = 1$$

$$\therefore \sum_{x : p(x)=0} (-1)^{u \cdot x} = \sum_{x : p(x)=1} (-1)^{u \cdot x} = 0.$$

□

consider the state in Train

§2.3 Quantum Rewinding.

Story: The following from Watrous's famous paper [Wat'06] will be used here.

(I'll look into the proof later)

Lemma 2.4 Let
- Q be a quantum circuit
  - input: n-qubit register
  - output: b a classical bit
    m-qubit register
- $p(|\psi\rangle) :=$ Prob that $b=0$ when executing Q on $|\psi\rangle$
  ($|\psi\rangle$: n-qubit state)
- $p_0, q \in (0,1)$ &
  $\epsilon \in (0, 1/2)$ be c.t.

(i) $\forall$ $|\psi\rangle$ (n-qubit), $\quad p_0 \le p(|\psi\rangle)$

(ii) $\forall$ $|\psi\rangle$, $\quad |p(|\psi\rangle) - q| < \epsilon$

(iii) $\quad p_0(1-p_0) \le q(1-q)$