§2 Preliminaries

§ 2.1 Basics

λ

$poly(\cdot)$

overwhelming is $\geq 1 - negl$

$\mathcal{H}$

$S(\mathcal{H})$ is the unit sphere $\{x : \|x\|_2 = 1\}$ in $\mathcal{H}$

$\mathcal{L}(\mathcal{H})$

$\mathcal{D}(\mathcal{H})$ density matrices.

$\mathcal{H}_X$ Hilbert space for register X.

$TD(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_{tr}$

ε-close if $TD(\rho, \sigma) \leq \delta$

POVM $\{E_i\}$ on $\mathcal{H}$; $\sum_i E_i = \mathbb{1}$

projective means

projective measurement

"Def^:" "uncomputing".

A quant. alg. can be modelled as a

unitary U acting on $\mathcal{H}$,

then performing a measurement on output register

w/o loss of generality.

(Here) Uncomputing means apply U^+ to the resulting state.

Informal claim: If the measurement outputs same result, w/ overwhelming prob.,

then the trace dist. b/w the final & the original state

is negligible

"oracle for f"

$$O_f : Q|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

"A quantum adversary A w/ access to oracle(s) is query-bounded if it makes at most $p(\lambda)$ queries to each oracle for some polynomial $p(\cdot)$".

§ 2.2 Quantum Random Oracle Model (QROM)

H: a random classical f^n that can be accessed by an adversary in superposition modelled by O_H.

Story: The following taken from [BBBV '97] will be used to reprogram oracles w/o adversarial detection on inputs which are not queried of large weight:

Thm 2.1 ([BBBV '97]). Let: A be an adversary w/ oracle access to $H: \{0,1\}^m \to \{0,1\}^n$ making at most T queries.

Def^n: (i) $|\phi_i\rangle$ as the global state after A makes i queries
(ii) $W_y(|\phi_i\rangle)$ as the sum of squared amplitudes in $|\phi_i\rangle$ of terms in which A queries H on input y.

Let: (i) $\epsilon > 0$ &

(ii) $F \subseteq [0, T-1] \times \{0,1\}^m$ be a set of time-string pairs s.t. $\sum_{(i,y) \in F} w_y (|\phi_i\rangle) \leq \frac{\epsilon^2}{T}$.

Let: H' be an oracle obtained after reprogramming H on input $(i,y) \in F$ to arbitrary outputs.

Define: $|\phi_i'\rangle$ as above for H'.

Then, $T D(|\phi_T\rangle, |\phi_T'\rangle) \leq \epsilon/2$

NB: The theorem can be extended to mixed states by convexity.

§ 2.3 More on Jordan's lemma

This version is, from [Reg05] & [Vid21]: adapted

Lemma 2.2. Let . $w \in [0,1]$

. $\mathcal{H}$ be a finite-dimensional Hilbert space

. Π_0 Π_1 be any two projectors in $\mathcal{H}$

Then, (i) $\exists$ an orthogonal decomposition of $\mathcal{H}$ into two dimensional subspaces $\mathcal{H} = \bigoplus_i S_i$ that are invariant under both Π_0 & Π_1

(ii) S_i is spanned by one or two eigenvectors of

$$w\Pi_0 + (1-w)\Pi_1$$

(iii) Whenever S_i is 2-dimensional,

$\exists$ a basis for it in which Π_0 & Π_1,

(restricted on S_i)

take the form:

$$\Pi_{0,S_i} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \& \quad \Pi_{1 S_i} = \begin{pmatrix} c_i^2 & c_i s_i \\ c_i s_i & s_i^2 \end{pmatrix}$$

where $c_i = \cos\theta_i$, $s_i = \sin\theta_i$ for some principle angle $\theta_i \in [0, \pi/2]$.

[Proof. For the $w = 1/2$ case, see [Reg05] or [Vid21]
& the generalization is apparently straightforward

□]

Story: They additionally show a relation b/w the eigenvalues in the same Jordan Block.

Lemma 2.3 For any two projectors Π_0 Π_1,

let (i) S_i be a 2-dimensional subspace
(as described in Lemma 2.2).

(ii) $|\phi_0\rangle$, $|\phi_1\rangle$ be the two eigenvectors (of
$w\Pi_0 + (1-w)\Pi_1$ that span S_i)
w/ eigenvalues λ_0 λ_1 resp.

Then, it holds that $\lambda_0 + \lambda_1 = 1$.

⌈Proof. Restrict to S_i. Then, (take $w = 1/2$; general case goes through similarly)

NB: $\lambda_0 + \lambda_1 = tr\left((\Pi_{0,S_i} + \Pi_{1,S_i})/2 \right)$

$= \frac{1 + c_i^2 + s_i^2}{2} = 1$

⌊□

Corollary 2.4 For any two projectors Π_0 Π_1,

let $|\phi_0\rangle$ & $|\phi_1\rangle$ be two eigenvectors of

$w\Pi_0 + (1-w)\Pi_1$

w/ eigenvalues λ_0 λ_1.

If $\lambda_0 + \lambda_1 \neq 1$ & $\lambda_0 \neq \lambda_1$, then

$\langle \phi_0 | \Pi_0 | \phi_1 \rangle = \langle \phi_0 | \Pi_1 | \phi_1 \rangle = 0$.

⌈Proof. If $\lambda_0 + \lambda_1 \neq 1$, then

NB1: Lemma 2.3 says that $|\phi_0\rangle$ & $|\phi_1\rangle$ cannot be in the same Jordan Block.

Also, we have

NB2: $\Pi_0 |\phi_0\rangle$ stays in the same Jordan Block as $|\phi_0\rangle$ (that how we defined S_i)

Conclusion $|\phi_0\rangle$ is orthogonal to $|\phi_1\rangle$.

⌊□

§ 2.4 Measuring Success Probability

story: Preliminaries on how to measure the
success prob of quantum programs
(wrt a test distribution).

(Me: of inputs I suppose)

: classically, this is easy to estimate to inverse poly precision.

- Suppose the test distribution can be sampled from efficiently.

- To estimate the success prob., simply run the program many times.

- Quantumly: This idea doesn't work because the quantum program may get consumed — we are given only one copy.
One must therefore "rewind the program" — but this is difficult in general.

Measure Probability:

Story: In [Zha20], Zhandry formalises a "measurement operator" for estimating the success prob of a quantum program.

: This operator is efficient to implement, but

discussed shortly

Zhandry also shows how to efficiently

estimate the probability w/

large statistical confidence in

the same work

(following the idea in QMA amplification [MW'05]).

Intuition:

- Suppose a POVM specifies whether a quantum program succeeds or not.
- Note that this does not specify the post-measurement state.
- Zhandry shows that,

for any POVM $P = (P, \mathbb{1} - P)$

there is a nice projective measurement Σ s.t.

the post-measurement state is an

eigenvector of P.

Me: the whole point seems to be that one can measure using this projective measurement w/o affecting the "prob of success" when the POVM is measured later. (this happens ∵ the projective measurement commutes w/ the POVM P)

: The projector is constructed simply using the eigenvectors (and eigenvalues) of P — but this process may not be efficient

• More precisely,

(i) $\mathcal{E}$ outputs a real number $p \in [0,1]$ from the "probability" the set of eigenvalues of P.

(Yes. $\mathcal{E}$ is taken to output a real number)

(ii) The post-measurement state upon obtaining outcome p is an eigenvector of P w/ eigenvalue p

(it's also an eigenvector of $Q = \mathbb{1} - P$ w/ eigenvalue $1-p$)

Me: $\mathcal{E}$ is basically constructed (inefficiently) as follows:

• NB: P & $Q = \mathbb{1} - P$ have common eigenvectors ∵ they commute.

• P has eigenbasis $\{|\psi_i\rangle\}$ w/ eigenvalues $\{\lambda_i\}$.

• The formal statement is as follows

(the construction above essentially proves the Thm)

Thm 2.5 (Inefficient Measurement).

Let $P = (P, Q)$ be a binary outcome POVM.

Let D be the set of eigenvalues of P.

$\exists$ a projective measurement $\Sigma = \{E_p\}_{p \in D}$

w/ index set D s.t.

(0) $\rho_p := E_p \rho E_p$ is the sub-normalized post measurement state $\forall \rho$.

(1) $\forall \; p \in D$, ρ_p is an eigenvector of P

w/ eigenvalue p

(2) The prob. of ρ when measured wrt

P is $\tau[P\rho] = \sum_{p \in D} \tau[P\rho_p]$.

Story: . Suppose $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$. (recall: $P = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$

Then, measuring $|\psi\rangle$ using Σ yields $|\psi_i\rangle$ w.p. $|\alpha_i|^2$.

Thm 2.6 (Inefficient Threshold measurement).

Let $P = (P, Q)$ be a binary outcome POVM.

Let P have eigenbasis $\{|\psi_i\rangle\}$ w eigenvalues $\{\lambda_i\}$.

Then, $\forall \; r \in (0,1)$ $\exists$ a projective measurement

$\Sigma_r = (E_{\leq r}, E_{>r})$ s.t.

(1) $E_{\leq \gamma} := \sum_{\lambda_i \leq \gamma} |\psi_i\rangle\langle\psi_i|$

(2) $E_{>\gamma} := \sum_{\lambda_i > \gamma} |\psi_i\rangle\langle\psi_i|$

Similarly, $\forall \quad \gamma \in (0, 1/2)$, $\exists$ projectors $\mathcal{E}'_\gamma = (\tilde{E}_{\leq\gamma}, \tilde{E}_{>\gamma})$ s.t.

(1) $\tilde{E}_{\leq \gamma} := \sum_{|\lambda_i - \frac{1}{2}| \leq \gamma} |\psi_i\rangle\langle\psi_i|$

(2) $\tilde{E}_{>\gamma} := \sum_{|\lambda_i - \frac{1}{2}| > \gamma} |\psi_i\rangle\langle\psi_i|$

Me: Don't know why any of these are called "theorems".

Efficient Measurement.

Story: . The projective measurements $\mathcal{E}$ above, cannot in general be efficiently computed.

. However, Zhandry [Zha20] showed that when the POVM is a mixture of projective measurements efficient approximation is possible.

This uses a technique first introduced by Marriott & Watrous [MW05].

- A situation of interest:

A random challenge x is sampled.

The program is evaluated on this input

And the output is checked.

this may be captured by a POVM $P = (P, Q)$ as follows:

$$P = \frac{1}{R} \sum_x \underbrace{V_x}_{\text{projector}}$$

R: size of challenge space.

Me: I guess if $|\psi\rangle$ is a "program",

V_x a kind of "universal machine" that reads the program & with auxiliary input set to x

Π_x some measurement that checks the output.

Then U_x can be $\Pi_x V_x$

- The following is adapted from Thm 6.2 in [Zha20] & Lemma 3 in [ALL+21]

Thm 2.7 (Efficient Threshold Measurement).

Let $P_b = (P_b, Q_b)$ be a binary outcome POVM on Hilbert space $\mathcal{H}_b$ that is a mixture of projectors.

$\forall \; b \in \{1, 2\}$.

- $P_b = \sum_i \lambda_i^b |\psi_i^b\rangle\langle\psi_i^b|$.

- $\gamma_1, \gamma_2 \in (0,1)$

$0 < \epsilon < \min\left(\frac{\gamma_1}{2}, \frac{\gamma_2}{2}, 1-\gamma_1, 1-\gamma_2\right)$

$\delta > 0$

be arbitrarily chosen

Then, $\exists$ efficient binary-outcome quantum algorithms. (interpreted as the POVM element corresponding to outcome 1)

$$ATI^{\epsilon,\delta}_{p,\gamma} \quad \text{s.t.}$$

$\forall$ quantum programs $\rho \in \mathcal{D}(\mathcal{H}_1) \otimes \mathcal{D}(\mathcal{H}_2)$

the following about the product algorithm

$$ATI^{\epsilon,\delta}_{p_1,\gamma_1} \otimes ATI^{\epsilon\,\delta}_{p_2,\gamma_2}$$

holds:

(b) Let $(E^b_{\le\gamma}, E^b_{>\gamma})$ be the inefficient threshold measurement in Thm 2.6 for $\mathcal{H}_b$.

(1) The prob. of measuring 1 on both registers satisfies

$$Tr\left[\left(ATI^{\epsilon\,\delta}_{p_1,\gamma_1} \otimes ATI^{\epsilon\,\delta}_{p_2,\gamma_2}\right)\rho\right] \geq$$

$$Tr\left[\left(E^1_{>\gamma_1+\epsilon} \otimes E^2_{>\gamma_2+\epsilon}\right)\rho\right] - 2\delta$$

(2) The post-measurement state ρ' after getting outcome (i,j) is 4δ-close to a state in

$$\text{span}\left\{|\psi_i^1\rangle|\psi_j^2\rangle\right\}_{i,j:\ \lambda_i^1 > \gamma_1 - 2\epsilon,\ \lambda_j^2 > \gamma_2 - 2\epsilon}$$

(3) The running time of the algorithm is polynomial in

$$\{\text{the running time of } P_1, \text{ " " } P_2, \tfrac{1}{\epsilon}, \log(1/\delta)\}.$$

Intuition: The theorem says — if the quantum state ρ has weight w on eigenvectors of (P_1, P_2) w/ eigenvalues greater than $(\gamma_1+\epsilon, \gamma_2+\epsilon)$ then, the quantum algorithm will produce a post measurement state (w.p. at least $w-2\delta$) s.t. it has weight $1-4\delta$ on eigenvectors w/ eigenvalues greater than $(\gamma_1-2\epsilon, \gamma_2-2\epsilon)$.

Story: In this paper, we focus on indistinguishability games — and therefore interested in projective measurements that "project onto" eigenvalues away from $\frac{1}{2}$ (i.e. doing better than random guessing)

We therefore use the symmetric version of theorem 2.7.

Thm 2.8 (Efficient Symmetric Threshold Measurement).

Let • $P_b = (P_b, Q_b)$

• $P_b = \sum_i \lambda_i^b |\psi_i^b\rangle\langle\psi_i^b|$] be as before.

Let • $\gamma_1, \gamma_2 \in (0, 1/2)$

• $0 < \epsilon < \min(\gamma_1/2, \gamma_2/2)$

• $\delta > 0$

be chosen arbitrarily.

Then, $\exists$ binary-outcome quantum algorithms (interpreted as the POVM element corresponding to outcome 1),

$$SATI^{\epsilon,\delta}_{P_b,\gamma} \quad s\text{-}1.$$

$\forall$ $\rho \in D(\mathcal{H}_1) \otimes D(\mathcal{H}_2)$, the following about $SATI^{\epsilon\delta}_{P_1,\gamma_1} \otimes SATI^{\epsilon\delta}_{P_2,\gamma_2}$ holds:

(0) Let $(\tilde{E}^b_{\le \gamma_b}, \tilde{E}^b_{>\gamma_b})$ be as in Thm 2.6 for $\mathcal{H}_b$.

(2) The post-measurement state ρ' after getting (1,1) is 4δ-close to a state in

$$\text{span}\{|\psi_i^1\rangle|\psi_j^2\rangle\}_{i,j:\ |\lambda_i^1 - 1/2| > \gamma_1 - 2\epsilon,\ |\lambda_i^2 - 1/2| > \gamma_2 - 2\epsilon}$$

(3) The run-time of the algorithm is polynomial in the running time of P_1, P_2 & $\{1/\epsilon, \log(1/\delta)\}$.

§ 2.5 Uncloneable Encryption

Story : In this subsection, we look at the def^ of uncloneable encryption as in [AK21]

this is a variant of the original def^ in [BL20]

(where they forced m_0, m_1 to be uniformly random).

: Here, m_0, m_1 are arbitrary.

Def^ 2-9 An uncloneable encryption scheme, is a triple of algorithms (Gen, Enc, Dec) w/ the following syntax.

- Gen(1^λ) — on input a security parameter 1^λ, returns a classical key sk

- Enc(sk, $|m\rangle\langle m|$) — on input the key sk, & the message $|m\rangle\langle m|$ for $m \in \{0,1\}^{poly(\lambda)}$, outputs a quant. ciphertext ρ_{ct}

- Dec(sk, ρ_{ct}) — takes as input the key sk, the quant. ciphertext ρ_{ct} & outputs a message ρ_m as a quantum state

It must satisfy the following:
correctness &
uncloneability
which are defined as follows:

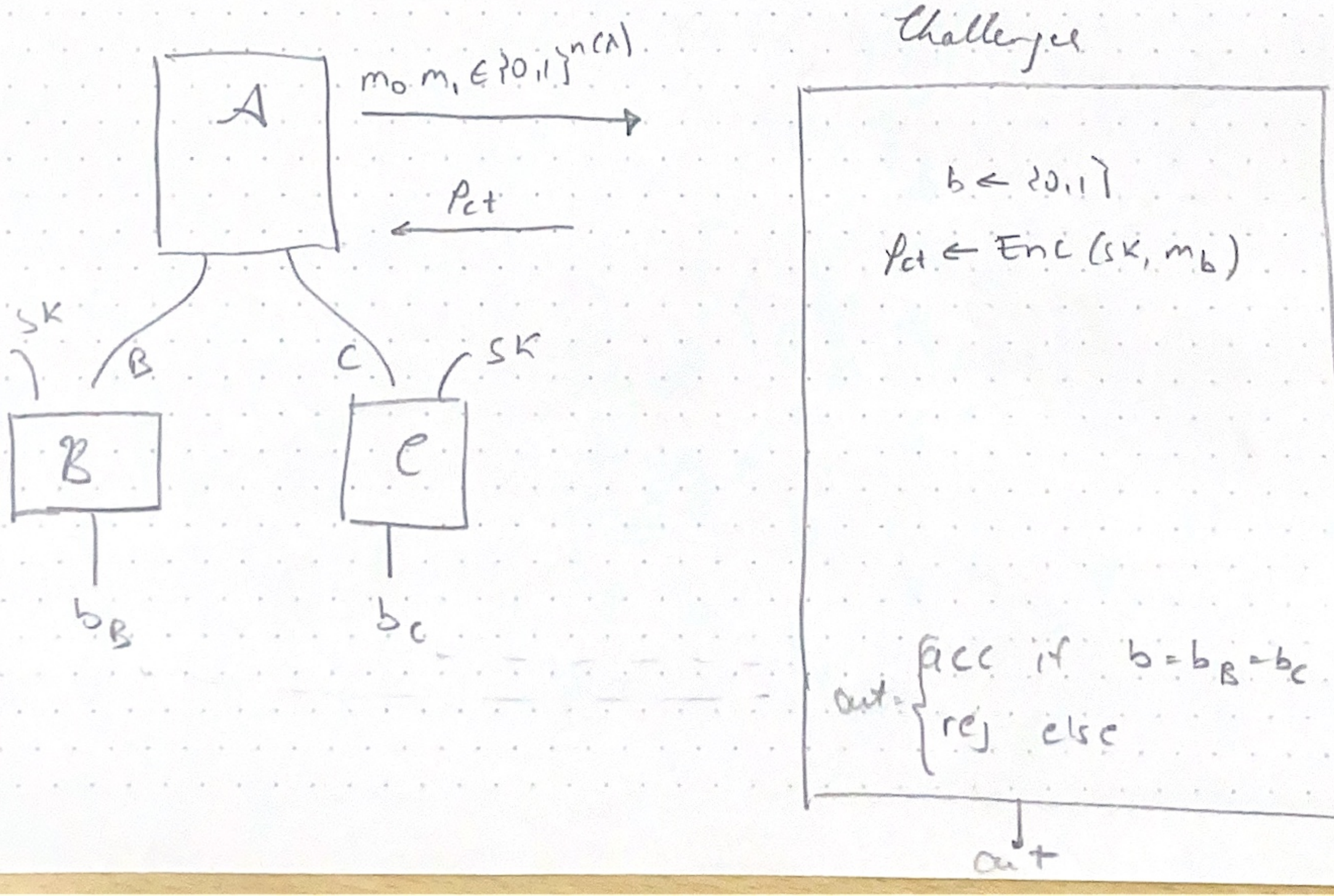
Correctness. $\forall$ $sk \leftarrow Gen(1^\lambda)$,

$$tr\left(|m\rangle\langle m| \; Dec(sk, Enc(sk, |m\rangle\langle m|))\right) \geq 1 - negl(\lambda)$$

Uncloneability. (we focus on uncloneable IND-CPA security)

(Def^n 2.10 Uncloneable IND-CPA game).

- Let $\lambda \in \mathbb{N}^+$
- Given an encryption scheme Σ, consider the following game against (A, B, C).



- Let $\mathrm{adv}_{\mathcal{G},\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda)$ (what is $\mathcal{G}$?) denote the prob. of winning the game above.

- The $\mathcal{S}$ is said to be information theoretically secure (computationally) if for all adversaries $(\mathcal{G},\mathcal{A},\mathcal{B},\mathcal{C})$ (all efficient) (what is $\mathcal{G}$?)

$$\mathrm{adv}_{\mathcal{G},\mathcal{A},\mathcal{B},\mathcal{C}}(\lambda) \leq \frac{1}{2} + \mathrm{negl}(\lambda)$$

§3 On the impossibility of Deterministic Schemes

Story: Let's define deterministic schemes first.

Def^ 3.1 (Deterministic Scheme). An encryption scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is a deterministic encryp^ scheme if

- Enc can be realised as a unitary U_{SK} acting on the plaintext register $|m\rangle$ & ancillary bits are init. to $|0\rangle$, resulting in a pure state ciphertext $|C_{SK}\rangle$ of length λ.
- Dec acts as $U_{SK}^{\dagger}$ & then measures in the