§ 2 Preliminaries

§ 2.1 Basic Notation

(standard quantum & crypto)

Lemma 2.1 (Quantum one-time pad).
For any m-qubit state ρ,

$$\frac{1}{4^m} \sum_{x \in \{0,1\}^m} \sum_{z \in \{0,1\}^m} X^x Z^z \rho Z^z X^x = \frac{\mathbb{I}^{\otimes m}}{2^m}$$

§ 2.2 Pseudorandom Quantum State Generators

Story: We review PRSGs. ([JLS'18, BS19, BS20])

Def^n 2.1 (Pseudorandom quantum state generators (PRSGs))

A pseudorandom quantum state generator (PRSG) is a QPT algorithm StateGen that
on input $k \in \{0,1\}^n$,
outputs an m-qubit state $|\phi_k\rangle$ satisfying the following security condition:

For any polynomial t &
any non-uniform QPT adversary A,
$\exists$ a negligible function negl s.t.
$\forall n$,

$$\mathrm{negl}(\lambda) \geq \left| \Pr_{k \leftarrow \{0,1\}^n}\left[1 \leftarrow A(|\phi_k\rangle^{\otimes t(n)})\right] - \Pr_{|\psi\rangle \leftarrow \mu_m}\left[1 \leftarrow A(|\psi\rangle^{\otimes t})\right] \right|$$

where μ_m is the Haar measure on n-qubit states.

Remark 2.1 In the most general case, statehen is the following QPT alg:

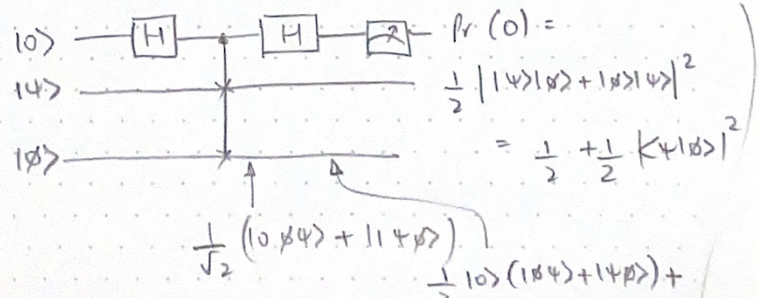
- on input $k \in \{0,1\}^\lambda$, it first computes a classical description of a unitary quantum circuit U_k
- & next applies U_k on the all zero $|0\ldots0\rangle$ to generate $|\Phi_k\rangle_{AB} := U_k |0\ldots0\rangle$.
- Outputs the n-qubit state $\rho_k := \mathrm{tr}_B\left(|\Phi_k\rangle\langle\Phi_k|_{AB}\right)$.

NB: ρ_k is, on an average, almost pure.

(∵ otherwise the security is broken by a QPT adv. who runs the SWAP test on two copies)

Proof Consider: A that runs SWAP test on two copies of the received state & outputs the result of the test.

Recall SWAP test



case: When $\rho_k^{\otimes t}$ is sent for uniform k,

$\Pr[A \text{ outputs } 1]$ is $\dfrac{1 + \frac{1}{2^n}\sum_k \mathrm{tr}(\rho_k^2)}{2}$.

When t copies of the Haar random state $|\psi\rangle^{\otimes t}$ is sent,

$\Pr[A \text{ outputs } 1] = 1$.

Thus, for security to hold,
it must be that

$$\frac{1 + \frac{1}{2^n}\sum_k \mathrm{tr}(\rho_k^2)}{2} \approx_{negl} 1$$

$\square$ $\Rightarrow$ purity of $\rho_k = \frac{1}{2^n}\sum_k \mathrm{tr}(\rho_k^2) \approx_{negl} 1$.

Simplifn (Notn): In this work, for simplicity, we take ρ_k to be pure & denote it by $|\phi_k\rangle$.

Claim: the same results hold even if the state is negligibly close to pure.

NR: Thus, StateGen produces $|\Phi_k\rangle_{AB} = |\phi_k\rangle_A \otimes \underbrace{|\eta_k\rangle_B}$,
where this is an aux state.

Simplifn: Assume no aux state is generated
(as part of the state generated by StateGen)

Claim: The same result holds, even if aux. registers are present.

Story: [Kre21]'s oracle separation considers the case w/ pure output & no aux qubits — so this is enough for showing commitments exist w/o OWFs.

: What is needed for the construction, is a weaker version of PRSGs where the security is satisfied only for $t=1$.

: We call them single-copy-secure PRSGs.

Def^n 2.2 (Single-copy-secure PRSGs).

A single-copy PRSG is a QPT alg. stateGen that on input $k \in \{0,1\}^n$, outputs an m-qubit state $|\phi_k\rangle$ which satisfies the following notion of security:

$$\mathrm{negl}(n) \geq \left| \Pr_{k \leftarrow \{0,1\}^n} \left[1 \leftarrow \mathcal{A}(|\phi_k\rangle)\right] - \Pr_{|\psi\rangle \leftarrow \mu_m} \left[1 \leftarrow \mathcal{A}(|\psi\rangle)\right] \right|$$

where μ_m is the Haar measure.

Remark 2.2. could use $\frac{\mathbb{I}^{\otimes m}}{2^m}$ (: single copy of an m-qubit Haar random state is exactly the same as the max mixed state).

Remark 2.3

From the NB in Remark 2.1,
recall that ρ_k produced by Statehen
must be pure for a PRSG.
But for a single-copy PRSG, this is not
true — the SWAP test doesn't work
with a single copy &
(W.l.o.g.) a trivial construction:
Statehen simply outputs
the max mixed state $\frac{\mathbb{1}_m}{2^n}$
$\forall\ k \in \{0,1\}^n$.

Thus, for the single-copy PRSG case,
they <u>assume</u> that the output is pure,
i.e. $\rho_k = |\phi_k\rangle\langle\phi_k|$.

Remarks 2.4 / **§2.5 are skipped for now but briefly—**

single-copy PRSG construction is potentially easier.
e.g. construction from PRG
$G: \{0,1\}^n \to \{0,1\}^m$ is
$|\phi_k\rangle = |G(k)\rangle \quad \forall k \in \{0,1\}^n$

Shouldn't a single-copy PRSG w/
$m \geq n+1$
be a PRG as well?
∵ measure $|\phi_k\rangle$ in
computational basis
/
would contradict [Kre 21]
∴ PRSG would give PRG

No contradiction ∵ the process of measuring
is not deterministic — PRG are deterministic

§3 Commitments

story: We look at the construction & prove its security.

§3.1 Definition

story: We first look at the formal def^n of non-interactive quantum commitments

Def^n 3.1 (Non-interactive quantum commitments (Syntax)).

A non-interactive quantum commitment scheme is the following protocol

- Commit phase:

  Let $b \in \{0,1\}$ be the bit to commit

  The sender generates a quantum state $|\psi_b\rangle_{RC}$ on register R & C,

  and

  sends register C to the receiver.

  The states $\{|\psi_b\rangle\}_{b\in\{0,1\}}$

  can be generated in quantum poly-time from the all zero state.

- Reveal phase:

  The sender sends b & register R to the receiver.

  The receiver measures RC in $\{|\psi_b\rangle\langle\psi_b|, \mathbb{1} - |\psi_b\rangle\langle\psi_b|\}$.

If the result is $|\psi_b\rangle\langle\psi_b|$,
the receiver outputs b. (Also called "opens b")

Else,
the receiver outputs $\perp$.

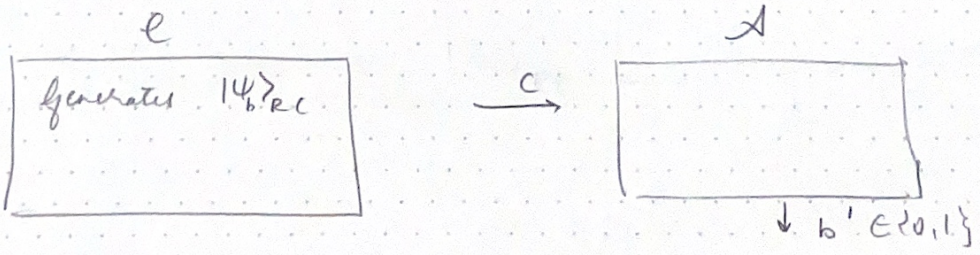
(NB: $\because$ $\{|\psi_b\rangle\}_{b\in\{0,1\}}$ can be generated in quantum poly-time from the all 0 state, the measurement $\{|\psi_b\rangle\langle\psi_b|, \mathbb{I} - |\psi_b\rangle\langle\psi_b|\}$ can be implemented efficiently.)

Def^n 3.2 (Perfect correctness). A commitment scheme has perfect correctness if:

when the honest sender commits to $b \in \{0,1\}$,
the prob. that the honest receiver opens b is 1.

Story: computational hiding is as follows:

Def^n 3.3 (Computational hiding). Consider the following security game $Exp(b)$ w/ parameter $b\in\{0,1\}$ b/w a challenger C & a QPT adversary A.



We say that a non-interactive quantum commitment scheme is computationally binding if

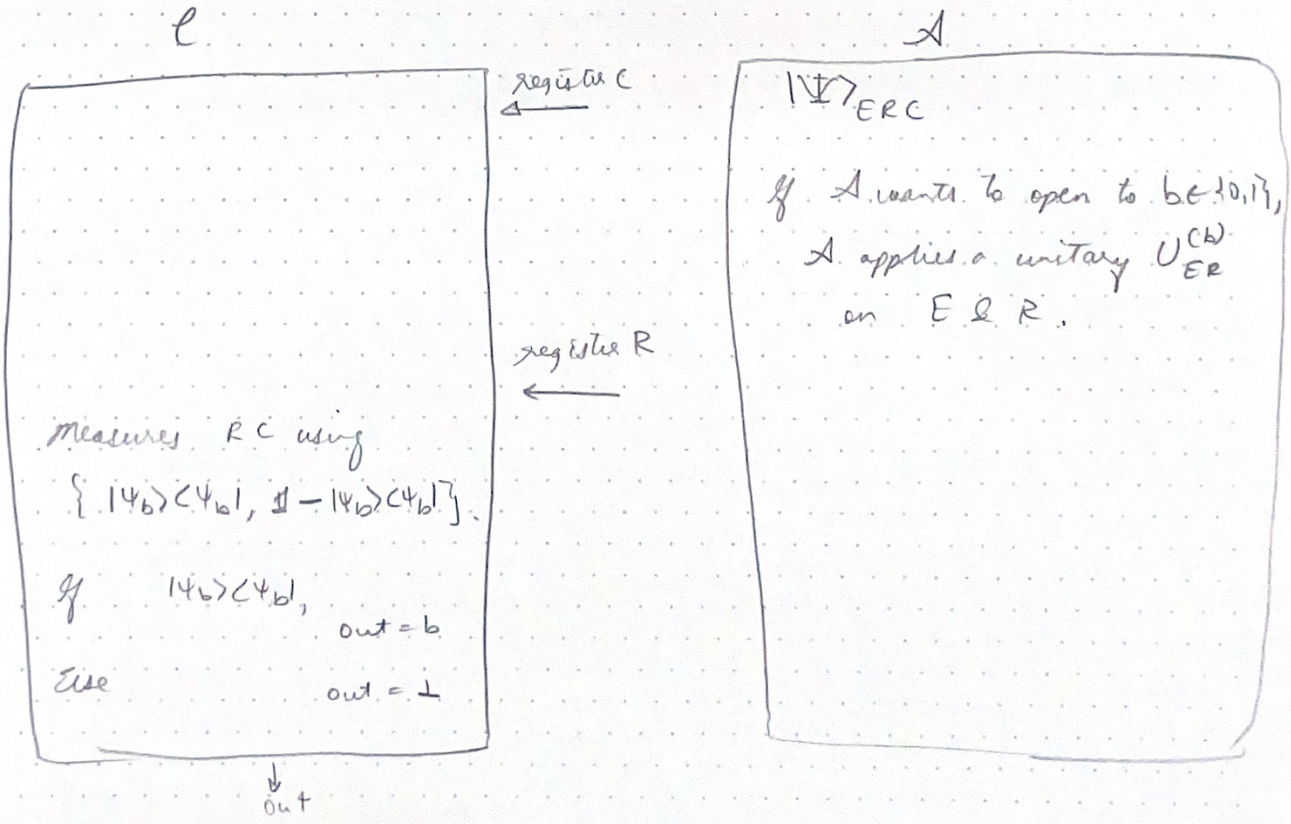
for any QPT adversary A,

$\exists$ a negligible function negl s.t.

$$|\Pr[\mathrm{Exp}(0)=1] - \Pr[\mathrm{Exp}(1)=1]| \leq \mathrm{negl}(\lambda)$$

Story: We consider sum-binding [Unr'16] as the definition of binding

Def^ 3.4 (Statistical Binding).
Consider the following security game b/w a challenger $\mathcal{C}$ & an adversary A.



Let p_b be the prob. that A makes C open $b \in \{0,1\}$,

i.e. $p_b := \langle \psi_b | \, tr_E \left(U_{ER}^{(b)} |\Psi\rangle\langle\Psi|_{ERC} \, U_{ER}^{(b)\dagger} \right) | \psi_b \rangle_{RC}$.

We say that the commitment scheme is
statistical sum-binding if
for any unbounded A
$\exists$ a negligible negl s.t.

$$p_0 + p_1 \leq 1 + \text{negl}(\lambda).$$

§ 3.2 Construction

Story: We now look at their construction formally.

Notn: Stateken denotes a single-copy secure PRSG that,
on input $k \in \{0,1\}^n$,
outputs an m-qubit state $|\phi_k\rangle$.
: $b \in \{0,1\}$ denotes the bit to be committed.

Defn (Commit Phase).
The sender generates[1]

$$|\psi_b\rangle := \frac{1}{\sqrt{2^{2m+n}}} \sum_{x,z \in \{0,1\}^m} \sum_{k \in \{0,1\}^n} |x,z,b\rangle_R \otimes P_{x,z}^b |\phi_k\rangle_C$$

& sends register C to the receiver
where $P_{x,z} := \bigotimes_{j=1}^{m} X_j^{x_j} Z_j^{z_j}$

[1] Apparently an "equivalent construction" is $\sum_{x \in \{0,1\}^m} |x\rangle|x\rangle$ for $b=0$
$\sum_{k \in \{0,1\}^n} |k\rangle|\phi_k\rangle$ for $b=1$.

(Reveal Phase)

1. The sender sends register R & the bit b to the receiver.
2. The receiver measures the state with
$$\{|\psi_b\rangle\langle\psi_b|,\ \mathbb{I} - |\psi_b\rangle\langle\psi_b|\}.$$
If the result is $|\psi_b\rangle\langle\psi_b|$,
the receiver outputs b.
Otherwise,
the receiver outputs $\perp$.

(NB: Such a measurement can be done efficiently —
apply $V_b^\dagger$ s.t. $|\psi_b\rangle = V_b|0\ldots0\rangle$
& measure in computational basis to
see whether the result is $0\ldots0$)

Story: It is clear that this construction satisfies perfect correctness.

Remark 3.1

NB: If the construction is modified slightly,
the communication in the reveal phase
can be classical.
(details in Appendix A).

[Idea: One-time pad register R & send both R & C during commit
In reveal, send the key for the pad + the bit b
Recall: For any non-interactive commitment (as in Def^ 3.1)
(commit phase)
a sender generates $|\psi_b\rangle_{RC}$ & sends
register C to the receiver
(which is the commit phase).

(reveal phase) the bit b & register R are sent to the receiver.
The receiver runs verification.

Modification: (commit phase) The sender chooses $x, z \leftarrow \{0,1\}^{|R|}$, applies $X^x Z^z$ on register R of the state $|\psi_b\rangle_{RC}$ & sends both R & C to the receiver.

(reveal phase) The sender sends the bit b to open & to the receiver the strings (x, z).

The receiver applies $X^x Z^z$ on register R & runs the original verification algorithm.

Justification: Hiding is clear — before the reveal phase, register R appears max. mixed & hiding of the original protocol applies.

Binding: Suppose there is an attack in the new scheme. One can run this same attack in the original scheme — the attacker can be simulated in the original scheme.

(End of Remark 3.1)

Remark 3.2 This construction can be extended to more general cases — where ancillas are used in PRGs.

Suppose, the PRSG generates $|\phi_k\rangle \otimes |\eta_k\rangle$ & outputs $|\phi_k\rangle$ (i.e. $|\eta_k\rangle$ is an ancilla).

Then hiding & binding hold if we replace $|\psi_b\rangle$

with the following:

$$\frac{1}{\sqrt{2^{2m+n}}} \sum_{x,z\in\{0,1\}^m} \sum_{k\in\{0,1\}^n} \left(|x,z,k\rangle\otimes|\psi_k\rangle\right)_R \otimes P^b_{x,z} |\phi_k\rangle_C .$$

§3.3 Computational Hiding

Theorem 3.1 (Computational Hiding)
The construction in §3.2 satisfies computational hiding

Proof of Theorem 3.1

Story: We start by defining $Hyb_0(b)$ which is the same as the original experiment.

Def^n $Hyb_0(b)$:

Challenger $C(b)$

Generates $|\Psi_0\rangle := \frac{1}{\sqrt{2^{2m+n}}} \sum_{x,z\in\{0,1\}^m} \sum_{k\in\{0,1\}^n} |x,z,k\rangle_R \otimes P^b_{x,z} |\phi_k\rangle_C$

registers → A

A → out $= b' \in \{0,1\}$

Story: $Hyb_1(b)$ is as follows

Def^n $Hyb_1(b)$:

$C(b)$

If $b=0$, generate $|\Psi\rangle_C \leftarrow \mu_m$ (Haar random m-qubit)

If $b=1$, generate $|\Psi_1\rangle_{RC}$

registers → A

A → out $= b' \in \{0,1\}$

Lemma 3.1 $\left| \Pr[Hyb_0(b)=1] - \Pr[Hyb_1(b)=1] \right| \leq \mathrm{negl}(\lambda)$

for each $b \in \{0,1\}$.

[Proof of Lemma 3.1

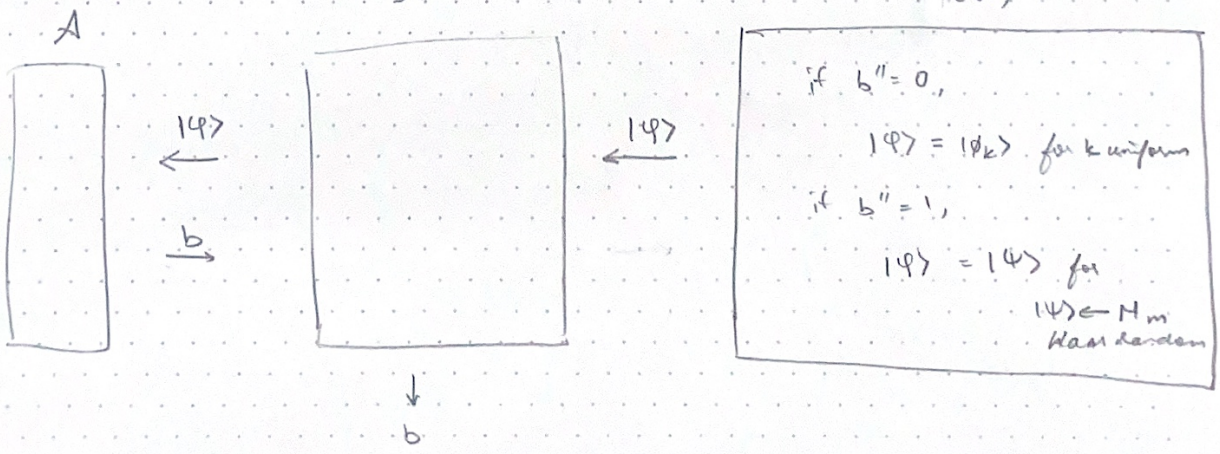
NB: Clearly, $\Pr[Hyb_0(1)=1] = \Pr[Hyb_1(1)=1]$

Story We show $\left| \Pr[Hyb_0(0)=1] - \Pr[Hyb_1(0)=1] \right| \leq \mathrm{negl}(\lambda)$.

Suppose (for contradiction): $\left| \Pr[Hyb_0(0)=1] - \Pr[Hyb_1(0)=1] \right| \geq \text{non-negl}(\lambda)$.

Story: Then one can construct an adversary $\mathcal{A}'$ that breaks the security of the PRSG.

Construction of $\mathcal{A}'$:



NB: When $b''=0$, $\mathcal{A}$ sees $Hyb_0(0)$

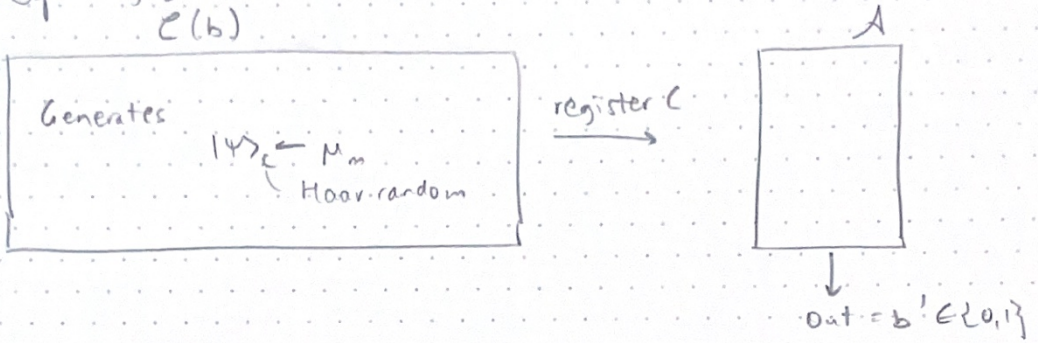
When $b''=1$, $\mathcal{A}$ sees $Hyb_1(0)$.

Thus, $\mathcal{A}'$ breaks the security of the PRSG

□

Story: We define $Hyb_2(b)$ as follows:

Def^n: $Hyb_2(b)$:



Lemma 3.2

$$\left| Pr[Hyb_1(b)=1] - Pr[Hyb_2(b)=1] \right| \leq negl(\lambda)$$

$\forall \; b \in \{0,1\}$

[Proof of Lemma 3.2

NB: $Pr[Hyb_1(0)=1] = Pr[Hyb_2(0)=1]$ is clear

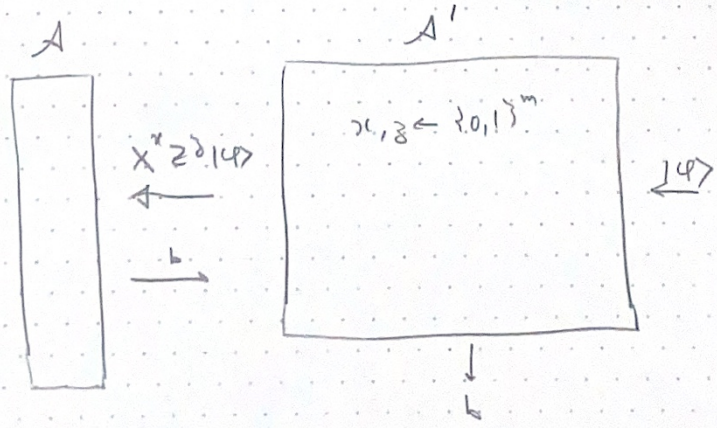
Story: We show that

$$\left| Pr[Hyb_1(1)=1] - Pr[Hyb_2(1)=1] \right| \leq negl(\lambda)$$

Suppose: $\left| Pr[Hyb_1(1)=1] - Pr[Hyb_2(1)=1] \right| \geq non\text{-}negl(\lambda)$.

(for contradiction)

Story: We can then construct an adversary $\mathcal{A}'$ that breaks the security of a PRSG.



$\mathcal{C}'(b'')$

if $b''=0$

$|\psi\rangle = |\phi_k\rangle$ for uniform k

if $b''=1$

$|\psi\rangle = |\psi\rangle$ for $|\psi\rangle \leftarrow \mu_m$ Haar Random

□ NB: When $b''=0$, simulates $Hyb_1(1)$

When $b''=1$, simulates $Hyb_2(1)$. $\therefore$ breaks security of the PRSG.

NB: Clearly, $\Pr[H_{y b_2}(0)=1] = \Pr[H_{y b_2}(1)=1]$.

$\therefore$ Combining Lemma 3.1 & 3.2, we conclude that

$$\left|\Pr[H_{y b_0}(0)=1] - \Pr[H_{y b_0}(1)=1]\right| \leq \mathrm{negl}.$$

□

§3.4 Statistical Binding

Theorem 3.2 (Statistical Binding). The construction in §3.2 satisfies statistical sum-binding (Def^ 3.4).

[Proof

Recall: $F(\rho,\sigma) := \left(\mathrm{tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)^2$ is the fidelity b/w ρ & σ.

Recall: Def^ 3.4 of sum-binding.

NB: $$p_b = \langle\psi_b|_{RC}\, \mathrm{tr}_E\left(U_{ER}^{(b)}\, |\Psi\rangle\langle\Psi|_{ERC}\, U_{ER}^{(b)\dagger}\right) |\psi_b\rangle_{RC}$$

$$= F\left(|\psi_b\rangle_{RC}, \mathrm{tr}_E\left(U_{ER}^{(b)}\, |\Psi\rangle\langle\Psi|_{ERC} U_{ER}^{(b)+}\right)\right)$$

$\left(\because F(\rho,\sigma) = \langle\sigma|\rho|\sigma\rangle \text{ if } \sigma = |\sigma\rangle\langle\sigma| \text{ is pure.}\right)$

$$\leq F\left(\mathrm{tr}_R\left(|\psi_b\rangle\langle\psi_b|_{RC}\right), \mathrm{tr}_{RE}\left(U_{ER}^{(b)}\, |\Psi\rangle\langle\Psi|_{ERC} U_{ER}^{(b)+}\right)\right)$$

$\left(\because F(\rho_{AB},\sigma_{AB}) \leq F(\rho_A,\sigma_A)\right)$

$$= F\left(\mathrm{tr}_R\left(|\psi_b\rangle\langle\psi_b|_{RC}\right), \mathrm{tr}_{RE}\left(|\Psi\rangle\langle\Psi|_{ERC}\right)\right).$$

NB 2: $$p_0 + p_1 \leq 1 + \sqrt{F\left(\mathrm{tr}_R\left(|\psi_0\rangle\langle\psi_0|_{RC}\right), \mathrm{tr}_R\left(|\psi_1\rangle\langle\psi_1|_{RC}\right)\right)}$$

$\left(\because F(\rho,\xi) + F(\sigma,\xi) \leq 1 + \sqrt{F(\rho,\sigma)}\right)$

$$= 1 + \sqrt{F\left(\frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|, \frac{1}{2^{2m}}\frac{1}{2^n}\sum_{x,z}\sum_k X^x Z^z |\phi_k\rangle\langle\phi_k| X^x Z^z\right)}$$

(using the def^{n}s)

$$= 1 + \sqrt{F\left(\frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|, \frac{\mathbb{I}^{\otimes n}}{2^n}\right)}$$

$$= 1 + \left\| \sum_{i=1}^{\xi} \sqrt{\lambda_i}\, \frac{1}{\sqrt{2^m}} |\lambda_i\rangle\langle\lambda_i| \right\|_1$$

(denoting the diagonalis^n of $\frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|$ as $\sum_{i=1}^{\xi} \lambda_i |\lambda_i\rangle\langle\lambda_i|$ & using $F = \mathrm{tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)$)

$$= 1 + \sum_{i=1}^{\xi} \sqrt{\lambda_i}\, \frac{1}{\sqrt{2^m}}$$

$$\leq 1 + \underbrace{\sqrt{\sum_{i=1}^{\xi} \lambda_i}}_{=1 \text{ by normalis}^n \text{ of } \frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|} \sqrt{\sum_{i=1}^{\xi} \frac{1}{2^m}}$$

using Cauchy–Schwarz $a \cdot b \leq \|a\|_1 \|b\|_1$

$$\leq 1 + \sqrt{\frac{2^n}{2^m}} \qquad (\because \xi \leq 2^n)$$

$$\leq 1 + \frac{1}{\sqrt{2^{(c-1)n}}} \qquad (\because m \geq cn \text{ for } c > 1)$$

$-m \leq -cn$

$m - n$

$n - m \leq n - cn$

$n - m \leq (1-c)n$

$m - n \geq (c-1)n$

□