Interactive Proofs for Quantum Devices

Anish Banerjee

Contents

Acknowledgements

These notes were prepared as part of an independent study of Prof. Thomas Vidick's [Vid20] course, under the guidance of Prof. Venkata Koppula and Dr. Mahesh Sreekumar Rajasree.

§1. Lecture 1: Introduction

This course deals with two papers:

1. **Classical Verification of Quantum Computations** [Mah23].
   - This paper addresses the question of verification of quantum computation: given classical data that is obtained from a quantum device that claims to have the ability to execute arbitrary quantum circuits (of poly size), how can a classical verifier ensure that the reported data indicates the correct outcome of the computation?
   - Not all problems that can be solved in quantum polynomial time are believed to lie in the class NP - not all quantum computations have outcomes that can be certified using an easily verifiable classical witness.
   - All problems in BQP have a classical randomized polynomial time interactive verification procedure; however, in this procedure, the prover may be asked to perform computations that are harder than BQP (BQP$\subseteq$IP).
   - However, the paper shows that every polynomial-time quantum computation can be verified by classical PPT verifier by interacting with a quantum **polynomial-time** prover as long as one can ascertain that the quantum device cannot break LWE assumption.
2. **MIP*=RE** [JNV+22].
   - **MIP*** designates all those computational problems that can be decided efficiently in classical randomized polynomial time by asking classical questions to two infinitely powerful untrusted quantum provers sharing entanglement.
   - **RE** denotes all problems for which there is an algorithm running in any amount of time that eventually halts with the answer "yes" when this is the case (but it need not halt in other cases).

At their heart, both works identify means by which a classical verifier is able to certify an appropriate "quantum computation workspace" within one or two quantum devices, using only classical interaction with it. It is like tying a "classical leash around the quantum system." The classical signatures of quantum processes that can be leveraged to certify an entire computation are:

1. Uncertainty principle
2. Quantum non-locality

1.1. What is a qubit?

Definition 1.1 (Qubit, Take 1)**.** A qubit is a triple $(\mathcal{H}, X, Z)$ consisting of a separable Hilbert space $\mathcal{H}$ and a pair of Hermitian operators X, Z acting on a $\mathcal{H}$ such that $X^2 = Z^2 = \mathbb{I}$ and $\{X, Z\} = 0$ (Mutually incompatible observables).

- Separable means that the Hilbert space has a countable basis. Quantum states can also live in non-separable $\mathcal{H}$ but we make this restriction for convenience.
- We also take the eigenvalues of X and Z to be ± 1.
- X, Z are self inverses. So $XZ = 0$ is not possible. Thus $\{X, Z\} = 0 \implies [X, Z] \neq 0$.

Lemma 1.1. $\{X, Z\} = 0 \implies$ Any vector in the basis of X makes an angle of $\pi/4$ with the basis vectors of Z

Proof. Let $|\psi\rangle$ be an eigenvector of X with eigenvalue ϵ. Then

$$\langle\psi| (XZ + ZX) |\psi\rangle = 2\epsilon \langle\psi| Z |\psi\rangle = 0$$
$$\implies \langle\psi| Z |\psi\rangle = 0 \tag{1.1}$$

Let Z_0 and Z_1 be the projectors on the positive and negative eigenspaces of Z. Then, we can write $Z = Z_0 - Z_1$. This implies

$$\begin{aligned}\langle\psi| Z |\psi\rangle &= \langle\psi| (Z_0 - Z_1) |\psi\rangle \\ &= \langle\psi| Z_0 |\psi\rangle - \langle\psi| Z_1 |\psi\rangle \\ &= 0 \quad \text{from Equation (1.1)}\end{aligned}$$

So, the components of $|\psi\rangle$ along the eigenspaces of Z are equal and opposite. This is equivalent to it making an angle of $\pi/4$ with both eigenspaces of Z ■

Lemma 1.2 (Jordan's Lemma)**.** Let P, Q be the projections on a separable Hilbert space $\mathcal{H}$. Then there exists an orthogonal decomposition

$$\mathcal{H} = \oplus_i \mathcal{S}_i$$

such that each S_i is a 1 or 2-dimensional subspace that is stable (invariant) by P and Q. Furthermore, whenever $\mathcal{S}_i$ is 2-dimensional, there is an orthonormal basis for it in which P and Q take the form

$$P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad Q = \begin{pmatrix} c_i^2 & c_i s_i \\ c_i s_i & s_i^2 \end{pmatrix}$$

(restricted to the subspace $\mathcal{S}$) where $c_i = \cos(\theta_i)$ and $s_i = \sin(\theta_i)$, $\theta \in [0, \pi/2)$ may depend on S_i. In other words, there exists a basis of $\mathbb{C}^d$ in which P and Q are simultaneously block diagonal.

Informally, when only two projections are concerned, we can reduce the analysis to a 2-dimensional problem. Also, both P and Q are block diagonal matrices having the same block sizes with respect to a particular basis.

Proof. Consider $R = P + Q$. R is Hermitian and has an orthonormal set of eigenvectors, which forms a basis for $\mathcal{H}$. Now, let $|\phi\rangle$ be an eigenvector of R with eigenvalue λ.

$$Q |\phi\rangle = R |\phi\rangle - P |\phi\rangle = \lambda |\phi\rangle - P |\phi\rangle \tag{1.2}$$

Let $\mathcal{S} = \text{span}(|\phi\rangle, P |\phi\rangle)$. We take two cases:

1. $P |\phi\rangle = \mu |\phi\rangle$. Then $|\phi\rangle$ is a simultaneous eigenvector of P and Q due to Equation (1.2). Note that $\mu \in \{0, 1\}$ as P is a projector. So $\mathcal{S} = \text{span}(|\phi\rangle)$ is 1-dimensional and P, Q are either identity or 0 on $\mathcal{S}$.
2. $P |\phi\rangle$ is linearly independent of $|\phi\rangle$. This implies $Q |\phi\rangle$ is also linearly independent of $|\phi\rangle$ due to Equation (1.2). Then $\mathcal{S}$ is stable (invariant) under P, i.e., $P |\psi\rangle \in \mathcal{S}, \forall |\psi\rangle \in \mathcal{S}$. Moreover,

   $$QP |\phi\rangle = Q(R - Q) |\phi\rangle = (\lambda - 1)Q |\phi\rangle$$

   so $\mathcal{S}$ is stable under Q too.

   Normalise the vectors $\{P |\phi\rangle, |\phi\rangle - P |\phi\rangle\}$ to obtain the orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle\}$ of $\mathcal{S}$. It is easy to check that $P |\psi_1\rangle = |\psi_1\rangle$ and $P |\psi_2\rangle = 0$, therefore, we can write $P = |\psi_1\rangle\langle\psi_1|$.

Let $|\Phi\rangle = Q|\phi\rangle$. Observe that $Q|\Phi\rangle = |\Phi\rangle$ and $Q\left|\Phi^{\perp}\right\rangle = 0$. In the basis of $\{|\psi_1\rangle, |\psi_2\rangle\}$ we can write $|\Phi\rangle = \cos\theta_i |\phi_1\rangle + e^{i\phi}\sin\theta_i |\phi_2\rangle = \cos\theta_i |\phi_1\rangle + \sin\theta_i |\phi_2\rangle$ where we overload $|\phi_2\rangle$ by absorbing the global phase $e^{i\phi}$ into it. Also, we can assume without loss of generality that $\theta \in (0, \pi/2]$. Take

$$\begin{aligned} Q &= |\Phi\rangle\langle\Phi| \\ &= (c_i|\psi_1\rangle + s_i|\psi_2\rangle)(c_i^*\langle\psi_1| + s_i^*\langle\psi_2|) \\ &= c_i^2|\psi_1\rangle\langle\psi_1| + c_i s_i(|\psi_1\rangle\langle\psi_2| + |\psi_2\rangle\langle\psi_1|) + s_i^2|\psi_2\rangle\langle\psi_2| \end{aligned}$$

Thus we have, with respect to $\{|\psi_1\rangle, |\psi_2\rangle\}$

$$P_{|\mathcal{S}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad Q_{|\mathcal{S}} = \begin{pmatrix} c_i^2 & c_i s_i \\ c_i s_i & s_i^2 \end{pmatrix}$$

Finally, since $\mathcal{S}$ is stable by both P and Q, it is stable under $R = P + Q$, so it has a basis made of eigenvectors of R - the vector $|\phi\rangle$ we started from, and it's orthogonal in R. Proceeding in this way inductively lets us identify an eigenbasis of R such that its vectors are either isolated (stable by both P and Q) or in pairs (spanning a 2D subspace that is stable by both P and Q) ■

Lemma 1.3. Let $(\mathcal{H}, X, Z)$ be a qubit. Then there is a Hilbert space $\mathcal{H}'$ and an isomorphism $\mathcal{H} \simeq \mathbb{C}^2 \otimes \mathcal{H}'$ such that under the same isomorphism, $X \simeq \sigma_X \otimes \mathbb{I}$ and $Z \simeq \sigma_Z \otimes \mathbb{I}$

This implies that qubits only exist in spaces of even or infinite dimension. They don't exist in dimension 1 (all operators commute).

Proof. Let $P = \frac{1}{2}(Z + \mathbb{I})$ and $Q = \frac{1}{2}(X + \mathbb{I})$. Then P, Q are projectors on $\mathcal{H}$, and we can decompose them by Lemma 1.2. Using $\{X, Z\} = 0$ it follows:

1. $[P, Q] = \frac{1}{4}[X, Z]$. There cannot be any 1D blocks because these necessarily commute
2. Let $\{|e_i\rangle, |f_i\rangle\}$ be the basis for $\mathcal{S}_i$ consistent with Jordan's lemma, i.e., with respect to this basis, we have

$$P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}(\mathbb{I} + Z) \qquad Q = \begin{pmatrix} c_i^2 & c_i s_i \\ c_i s_i & s_i^2 \end{pmatrix} = \frac{1}{2}(\mathbb{I} + X)$$

which gives

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$X = \begin{pmatrix} 2c_i^2 - 1 & 2c_i s_i \\ 2c_i s_i & 2s_i^2 - 1 \end{pmatrix} = \begin{pmatrix} \cos(2\theta_i) & \sin(2\theta_i) \\ \sin(2\theta_i) & -\cos(2\theta_i) \end{pmatrix}$$

Now using $\{X, Z\} = 0$ we obtain $\theta = \frac{\pi}{4}$. So, in every subspace $\mathcal{S}_i$, Z acts exactly as σ_Z and X as σ_X.

It is important to note that the matrices take the above form in the basis $\{|e_i\rangle, |f_i\rangle\}$. This change from the standard basis can be performed by a similarity transformation ($X \to OXO^{\dagger}$) on the operators.

Let $\mathcal{H}'$ have canonical basis $\{|i\rangle\}$ where i ranges over the block indices in the decomposition of P and Q. The required isomorphism is obtained by mapping

$$|e_i\rangle \in \mathcal{H} \to |0\rangle \otimes |i\rangle \in \mathbb{C}^2 \otimes \mathcal{H}'$$

$$|f_i\rangle \in \mathcal{H} \to |1\rangle \otimes |i\rangle \in \mathbb{C}^2 \otimes \mathcal{H}'$$

Observe that we crucially used that fact that the basis $\{|e_i\rangle, |f_i\rangle\}$ is orthonormal and the subspaces $\mathcal{S}_i$ are also orthogonal. ■

1.2. Multiple Qubits

What we mean by a system having $n-$ qubits is that:

1. It should have n copies of one qubit, so there should be $(X_1, Z_1), (X_2, Z_2), \ldots, (X_n, Z_n)$, on $\mathcal{H}$ such that each pair satisfies the definition of a qubit.
2. The qubits should be independent.

Definition 1.2 (n-Qubits, Take 1)**.** A system of $n-$ qubits is a tuple $(\mathcal{H}, X_1, Z_1 \ldots X_n, Z_n)$ consisting of a separable Hilbert space $\mathcal{H}$ and n pairs of Hermitian operators (X_i, Z_i) for $i \in [n]$ acting on $\mathcal{H}$ such that:

1. For each $i \in [n]$, $(\mathcal{H}, X_i, Z_i)$ is a qubit
2. For each $i \neq j \in [n]$, qubits i and j are independent:

$$[X_i, X_j] = [Z_i, X_j] = [X_i, Z_j] = [Z_i, Z_j] = 0$$

Let's examine why the definition encompasses the concept of independence in terms of measurement, specifically that the order of measurement is irrelevant. Consider a two-qubit system, and we aim to demonstrate that the expectation of measuring the second qubit in the computational basis (i.e., $\langle\phi| Z_2 |\phi\rangle$) is equivalent to the expectation of measuring the first qubit in the Hadamard basis and subsequently measuring the second qubit in the standard basis.

After measuring the first qubit, the state is either in $\frac{X_1^0 |\phi\rangle}{\sqrt{\langle\phi| X_1^0 X_1^0 |\phi\rangle}}$ with probability $\langle\phi| X_1^0 X_1^0 |\phi\rangle$ or in $\frac{X_1^1 |\phi\rangle}{\sqrt{\langle\phi| X_1^1 X_1^1 |\phi\rangle}}$ with probability $\langle\phi| X_1^1 X_1^1 |\phi\rangle$, where $X_1 = X_1^0 - X_1^1$ is the spectral decomposition of X. Therefore, the expectation can be expressed as:

$$\begin{aligned}
\text{Expectation} &= \langle\phi| X_1^0 X_1^0 |\phi\rangle \times \frac{\langle\phi| X_1^0 Z_2 X_1^0 |\phi\rangle}{\langle\phi| X_1^0 X_1^0 |\phi\rangle} + \langle\phi| X_1^1 X_1^1 |\phi\rangle \times \frac{\langle\phi| X_1^1 Z_2 X_1^1 |\phi\rangle}{\langle\phi| X_1^1 X_1^1 |\phi\rangle} \\
&= \langle\phi| X_1^0 Z_2 X_1^0 |\phi\rangle + \langle\phi| X_1^1 Z_2 X_1^1 |\phi\rangle \\
&= \langle\phi| (X_1^0 Z_2 X_1^0 + X_1^1 Z_2 X_1^1) |\phi\rangle \\
&= \langle\phi| (X_1^0 Z_2 X_1^0 + X_1^1 Z_2 X_1^1 - X_1^1 Z_2 X_1^0 - X_1^0 Z_2 X_1^1) |\phi\rangle \\
&= \langle\phi| X_1 Z_2 X_1 |\phi\rangle \\
&= \langle\phi| Z_2 X_1 X_1 |\phi\rangle \\
&= \langle\phi| Z_2 |\phi\rangle
\end{aligned}$$

The fourth equality is also a consequence of the commutator relation $[X_1, Z_2] = 0$: We have $[X_1, Z_2] = 0$. This implies $X_1 Z_2 - Z_2 X_1 = 0$. Substituting $X_1 = X_1^0 - X_1^1$, we get $X_1^0 Z_2 - X_1^1 Z_2 - Z_2 X_1^0 + Z_2 X_1^1 = 0$. We left multiply by X_1^0 and right multiply by X_1^1 to get $X_1^0 Z_2 X_1^1 - X_1^0 X_1^1 Z_2 X_1^1 - X_1^0 Z_2 X_1^0 X_1^1 + X_1^0 Z_2 X_1^1 = 0$. Since $X_1^0 X_1^1 = X_1^1 X_1^0 = 0$, we have $2 \cdot X_1^0 Z_2 X_1^1 = 0$. So, $X_1^1 Z_2 X_1^0 = X_1^0 Z_2 X_1^1 = 0$. The sixth equality is due to the fact that $[X_1, Z_2] = 0 \implies X_1 Z_2 = Z_2 X_1$.

Lemma 1.4. Let $(\mathcal{H}, X_1, Z_1, \ldots, X_n, Z_n)$ be a system of n qubits. Then there exists a Hilbert space $\mathcal{H}'$ and an isomorphism

$$\mathcal{H} \simeq \underbrace{\mathbb{C}^2 \times \mathbb{C}^2 \ldots \mathbb{C}^2}_{n \text{ times}} \otimes \mathcal{H}'$$

such that under the same isomorphism, for every $i \in [n]$ and $W \in \{X, Z\}$,

$$W_i \simeq \sigma_{W_i} \otimes \mathbb{I}_{\mathcal{H}'}$$

here σ_{W_i} is the Pauli W operator acting on the i^{th} copy of $\mathbb{C}^2$

Proof. Proof is by induction on n. Base case is proved in the previous lemma. Let $(\mathcal{H}, X_1, Z_1, \ldots, X_{n+1}, Z_{n+1})$ be a system of $n+1$ qubits. Then by the induction hypothesis, we have a space $\mathcal{H}'$ and isomorphism π'
Claim: Let W be an Hermitian operator on $\mathcal{H}$ such that $[W, X_i] = [W, Z_i] = 0, \forall i \in [n]$. Then there exists W' Hermitian acting on $\mathcal{H}'$ such that under π', $W \simeq \mathbb{I}_{(\mathbb{C}^2)^{\otimes n}} \otimes W'$. In other words, the first n qubits will be left unchanged by the action of W

Proof. Introduce the following notation for $a \in \{0,1\}^n$:

$$\sigma_W(a) = \sigma_{W_1}^{a_1} \otimes \sigma_{W_2}^{a_2} \cdots \otimes \sigma_{W_n}^{a_n}$$

Now, since any linear operator U can be decomposed in the Pauli basis as $U = \sum_i a_i \sigma_i$, we can write

$$W = \sum_{a,b \in \{0,1\}^n} \sigma_X(a)\sigma_Z(b) \otimes W_{a,b}$$

$W_{a,b}$ are arbitrary operators on $\mathcal{H}'$, need not be Hermitian (absorb the constant a_i in $W_{a,b}$).

$$\sigma_X(c)\sigma_Z(d)W = \sum_{a,b} \sigma_X(c)\sigma_Z(d)\sigma_X(a)\sigma_Z(b) \otimes W_{a,b} = \sum_{a,b} (-1)^{a \cdot d} \sigma_X(a+c)\sigma_Z(b+d) \otimes W_{a,b}$$

where we used $\sigma_X\sigma_Z = -\sigma_Z\sigma_X$. Similarly,

$$W\sigma_X(c)\sigma_Z(d) = \sum_{a,b} \sigma_X(a)\sigma_Z(b)\sigma_X(c)\sigma_Z(d) \otimes W_{a,b} = \sum_{a,b} (-1)^{b \cdot c} \sigma_X(a+c)\sigma_Z(b+d) \otimes W_{a,b}$$

Since W commutes with both X_i and Z_i,the above equations must be equal because

$$\sigma_X(c)\sigma_Z(d)W = \sigma_X(c)W\sigma_Z(d) = W\sigma_X(c)\sigma_Z(d)$$

Now, since $\sigma_X(a)\sigma_Z(b)$ are linearly independent, $(-1)^{b \cdot c} W_{a,b} = (-1)^{a \cdot d} W_{a,b}$. Unless $a = b = 0$, we can find c, d such that $(-1)^{b \cdot c} \neq (-1)^{a \cdot d}$. So

$$W_{a,b} = \begin{cases} \mathbb{I} \otimes W_{0,0} & a, b = (0,0) \\ 0 & \text{Otherwise} \end{cases}$$

Since W is Hermitian, hence $W_{0,0}$ is Hermitian too. ■

Using the claim for $W = X_{n+1}$ and $W = Z_{n+1}$ we obtain X'_{n+1}, Z'_{n+1} such that $(\mathcal{H}', X'_{n+1}, Z'_{n+1})$ is a qubit (can verify from the definition: $W^2 = \mathbb{I}$ and anti-commutator is zero). Then, using Lemma 1.3, we can find the isomorphism and compose it with π' to obtain the induction step. ■

The statement of Lemma 1.4 can be reformulated in the language of group representation theory: The n qubit **Weyl-Hisenberg group** is the $2 \cdot 4^n$ element group

$$G_n = \{(-1)^c \sigma_X(a)\sigma_Z(b) | a, b \in \{0,1\}^n; c \in \{0,1\}\}$$

that is generated by the n qubit σ_X and σ_Z matrices. Then ϕ defined as

$$\phi((-1)^c\sigma_X(a)\sigma_Z(b)) = (-1)^c\prod_i X_i^{a_i}\prod_i Z_i^{b_i}$$

forms a representation of G_n. The lemma can be adapted to show that any representation of G_n that in addition send $-1 \mapsto -1$ as ϕ does, must be a direct sum of copies of the representation by Pauli matrices.

1.3. Approximate Qubits

Exercise 1.1. Suppose that X, Z are binary observables on $\mathcal{H}$ such that $\|\{X, Z\}\| \leq \epsilon$ for some $\epsilon \geq 0$, where $\|\cdot\|$ is the spectral norm. Show that there exists a qubit $(\mathcal{H}, X', Z')$ such that

$$\left\|X - X'\right\| \leq \delta(\epsilon) \qquad \left\|Z - Z'\right\| \leq \delta(\epsilon)$$

. State the best dependence δ you can get.

Solution 1.1

Using Jordan's Lemma, we can still decompose $\mathcal{H} = \oplus_i \mathcal{S}_i$ where $\mathcal{S}_i$ are one or two-dimensional.

1. For the 1D case, since the corresponding projectors act as identity or 0 on the subspace, X', Z' must act as $\pm\mathbb{I}$ on the subspace. Hence $\{X, Z\} = \pm 2$ which is not possible for small enough $\epsilon < 2$. Thus, there cannot be any 1D subspaces.

2. For the 2D case,

$$X_{|\mathcal{S}_i} = \begin{pmatrix} c_i & s_i \\ s_i & -c_i \end{pmatrix} \qquad Z_{|\mathcal{S}_i} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Using the condition on the norm of the anti-commutator, we obtain

$$\|\{XZ + ZX\}\| \leq \epsilon \implies \left\|\{X_{|\mathcal{S}_i}Z_{|\mathcal{S}_i} + Z_{|\mathcal{S}_i}X_{|\mathcal{S}_i}\}\right\| \leq \epsilon \implies 2c^2\|\mathbb{I}\| \leq \epsilon \implies c^2 \leq \frac{\epsilon}{2}$$

The qubit $(\mathcal{H}, X', Z')$ will have a decomposition

$$X'_{|\mathcal{S}_i} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z'_{|\mathcal{S}_i} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Since $Z - Z' = 0$, we bound the norm of $X - X'$ by finding the largest eigenvalue of $X_{|\mathcal{S}_i} - X'_{|\mathcal{S}_i}$:

$$\lambda = \sqrt{c^2 + 2(1-s)} - c = O(\sqrt{\epsilon})$$

Thus $\delta(\epsilon) = O(\sqrt{\epsilon})$

Theorem 1.5 ([CRSV17]). Let $X_1, Z_1, \cdots, X_n, Z_n$ be binary observables on $\mathcal{H}$ and $\epsilon \geq 0$ such that

$$\frac{\epsilon}{(1-\epsilon)^2} \leq \frac{1}{64n}$$

and $\left\|\{X_i, Z_i\}\right\| \leq \epsilon$ for all $i \neq j \in [n]$ and $S, T \in \{X, Z\}$. Then there exists binary observables $X'_1, Z'_1 \ldots X'_n, Z'_n$ on $\mathcal{H}$ such that $\{X'_i, Z'_i\} = 0$, $[S'_i, T'_j] = 0$ and moreover for all $i \neq j \in [n]$ and $S, T \in \{X, Z\}$

$$\left\|S'_j - S_j\right\| \leq \frac{4n\epsilon}{(1-\epsilon)^2} + \epsilon$$

§2. Lecture 2: Testing a qubit

In this section, we will be developing an operational definition of the qubit, which we can test. The condition of the operator anti-commutator being zero is not something we can directly test based on experimental data alone. We can only find the expectation values of some observable on a state $|\psi\rangle$ via experiment.

2.1. Interactive Proofs

Definition 2.1 (Interactive Proof System)**.** An interactive proof system, or sometimes a "test", for a hypothesis H is the specification of a verifier V in an interactive protocol between V and the prover P with the following properties: (In the protocol, both V and P may be provided with some auxiliary input: x_V for V and ρ_P for P)

1. **Completeness:** whenever H (which may depend on x_V or ρ_P) is satisfied, there is a way for an honest P to be accepted in the protocol with high probability $c \in [0,1]$, termed as the "completeness parameter."
2. **Soundness:** whenever H is false, no prover can succeed in the protocol with probability higher than a small quantity $s \in [0,1]$, termed as the "soundness parameter."

2.2. An operational definition of a qubit

Now, we will start using the density matrix representation for a quantum state. Since we don't want to rule out the possibility that the prover may share entanglement with the environment, we don't assume that their initial state is a pure state $|\psi\rangle$, instead, we assume $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}'$, where $\mathcal{H}'$ corresponds to the space associated with the environment.
When an interactive experiment is executed, the only observable data accessible to the experimentalist are the expectation values. An important consequence of this is that we cannot hope to achieve a characterization of the prover's observable itself but instead may only make assertions about the action of the observable on the state.

$$\langle\psi| O |\psi\rangle = \langle U\psi| UOU^\dagger |U\psi\rangle$$

Thus, the two models of the prover, using the state $|\psi\rangle$ and observable O or using $|U\psi\rangle$ with the observable $UOU^\dagger$ lead exactly to the same observed data.

Definition 2.2 (Qubit, Take 2)**.** A qubit is a triple $(|\psi\rangle, X, Z)$ such that $|\psi\rangle \in S(\mathcal{H})$, where $\mathcal{H}$ is a separable Hilbert space, and X, Z are Hermitian operators on $\mathcal{H}$, $X^2 = Z^2 = \mathbb{I}$ such that

$$\{X, Z\} |\psi\rangle = 0$$

This is a weakened definition from our earlier one. We don't require $\{X, Z\} = 0$ here.

Lemma 2.1. Let $(|\psi\rangle, X, Z)$ be a qubit in $\mathcal{H}$. Then there exists a Hilbert space $\mathcal{H}'$ and an isometry $V : \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}'$ such that

$$VX |\psi\rangle = (\sigma_X \otimes \mathbb{I})V |\psi\rangle \qquad VZ |\psi\rangle = (\sigma_Z \otimes \mathbb{I})V |\psi\rangle$$

An isometry (or congruence or congruent transformation) is a distance-preserving transformation between metric spaces. Let X, Y be metric spaces with metrics d_X, d_Y. A map $f : X \to Y$ is an isometry if for $a, b \in X$

$$d_X(a, b) = d_Y(f(a), f(b))$$

The lemma no longer says $X \simeq \sigma_X \otimes \mathbb{I}$, but only that it has the same action on the state up to the *isometry* (not necessarily *isomorphism*) V. $\mathcal{H}$ can now have an odd dimension.

Proof. Let $P = \frac{1}{2}(Z + \mathbb{I})$ and $Q = \frac{1}{2}(X + \mathbb{I})$ be two projection operators. Using Jordan's lemma, we can decompose $\mathcal{H} = \oplus_i \mathcal{S}_i$ into 1D and 2D subspaces such that with respect to some basis, P and Q are block diagonal matrices. Let us also write $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$ where $|\psi_i\rangle \in \mathcal{S}_i$ are the basis elements.

- For 1D subspaces, $\{X, Z\}_{|\mathcal{S}_i} = 2p_i q_i$ where p_i, q_i are the appropriate diagonal elements in $2P - \mathbb{I}$ and $2Q - \mathbb{I}$. Moreover, since the projectors are either 0 or identity on the one-dimensional subspaces, we obtain $p_i = \pm 1, q_i = \pm 1$, and hence the anti-commutator is ± 2. Since $\{X, Z\}|\psi\rangle = 0$, this implies $(\{X, Z\}|\psi\rangle)_{|\mathcal{S}_i} = \pm 2\alpha_i = 0$. Hence, α_i must be zero for the one-dimensional blocks.
- For the 2D subspaces, we can write, in the appropriate basis

$$X_{|\mathcal{S}_i} = \begin{pmatrix} c_i & s_i \\ s_i & -c_i \end{pmatrix} \qquad Z_{|\mathcal{S}_i} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

  and we obtain $\{X, Z\}_{|\mathcal{S}_i} = 2c_i\mathbb{I} \implies \{X, Z\}^2_{|\mathcal{S}_i} = 4c_i^2\mathbb{I}$.

$$\alpha_i \{X, Z\}_{|\mathcal{S}_i} |\psi_i\rangle = 0 \implies \|\alpha\|^2 \langle\psi_i| \{X, Z\}^2_{|\mathcal{S}_i} |\psi_i\rangle = 0 \implies 4c_i^2\alpha_i^2 = 0$$

  Thus either $\alpha_i = 0$ or $c_i = 0$

Thus, for any subspaces $\mathcal{S}_i$ on which $|\psi\rangle$ has non-zero mass, it must be that $\{X, Z\}_{|\mathcal{S}_i} = 0$, as operators. In other words, for all 1D subspaces, $\alpha_i = 0$. And, for the rest of non-zero α_i's, $X_{|\mathcal{S}_i}$ is σ_X. But we cannot conclude anything about the other 2D blocks where $|\psi\rangle$ has no mass.
The Isometry: Let $\mathcal{H} = \oplus_{i\in[\ell_1]}\mathcal{S}_i \oplus \mathcal{T}_{i\in[\ell_2]} \oplus_{i\in[\ell_3]} \mathcal{U}_i$ where

- $\mathcal{S}_i$ are the 2D subspaces where $\alpha_i \neq 0$
- $\mathcal{T}_i$ are the 2D subspaces where $c_i \neq 0$
- $\mathcal{U}_i$ are the 1D subspaces

For basis $|e_i\rangle, |f_i\rangle$ (wrt Jordan's lemma) in $\mathcal{S}_i$, set

$$V|e_i\rangle = |0\rangle \otimes |i\rangle$$

$$V|f_i\rangle = |1\rangle \otimes |i\rangle$$

For basis $|e_i\rangle, |f_i\rangle$ (wrt Jordan's lemma) in $\mathcal{T}_i$, set

$$V|e_i\rangle = |0\rangle \otimes |\ell_1 + i\rangle$$

$$V|f_i\rangle = |1\rangle \otimes |\ell_1 + i\rangle$$

For basis $|e_i\rangle$ (wrt Jordan's lemma) in $\mathcal{U}_i$, set

$$V|e_i\rangle = |0\rangle \otimes |\ell_1 + \ell_2 + i\rangle$$

Observe that V is an isometry from $\mathcal{H}$ to $\mathcal{C}^2 \otimes \mathcal{H}'$ where the dimension of $\mathcal{H}'$ is $\ell_1 + \ell_2 + \ell_3$. Dimension of $\mathcal{H}$ is $2(\ell_1 + \ell_2) + \ell_3$ whereas dimension of $\mathcal{C}^2 \otimes \mathcal{H}'$ is $2(\ell_1 + \ell_2 + \ell_3)$. And $VX_{|\mathcal{S}_i} = \sigma_X$ and $VZ_{|\mathcal{S}_i} = \sigma_Z$. For the rest, it does not matter because $\alpha_i = 0$, so $\alpha V X_{|\mathcal{T}_i} = \alpha V X_{|\mathcal{U}_i} = 0$.

■

This extends to the approximate case as well:

Exercise 2.1. Say that $(|\psi\rangle, X, Z)$ is an $\epsilon-$ approximate qubit if $\left\|\{X,Z\}|\psi\rangle\right\| \leq \epsilon$. Show that there is an isometry $V : \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}'$ such that for $W \in \{X, Z\}$

$$\left\|(W - V^\dagger(\sigma_W \otimes \mathbb{I})V)|\psi\rangle\right\|^2 \leq O(\epsilon)$$

Now, let's connect the idea of interactive proofs with the above definition of a qubit.

Definition 2.3. We say a family of conditional distributions $\{p(\cdot|x)\}_{x\in\mathcal{X}}$ self-tests a qubit if for any state $|\psi\rangle \in S(\mathcal{H})$ and the family of POVM $\{P_a^x\}_{a\in\mathcal{A}}$ for $x \in \mathcal{X}$ such that $p(a|x) = \langle\psi| P_a^x |\psi\rangle$ for all a, x there is an isometry $V : \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}'$ and $x_0, z_0 \in \mathcal{X}$ such that the measurements P^{x_0}, P^{z_0} have only two possible outcomes 0,1 and moreover

$$V(P_0^{x_0} - P_1^{x_0})|\psi\rangle = (\sigma_X \otimes \mathbb{I})V|\psi\rangle \qquad V(P_0^{z_0} - P_1^{z_0})|\psi\rangle = (\sigma_Z \otimes \mathbb{I})V|\psi\rangle$$

2.3. A first test for a qubit

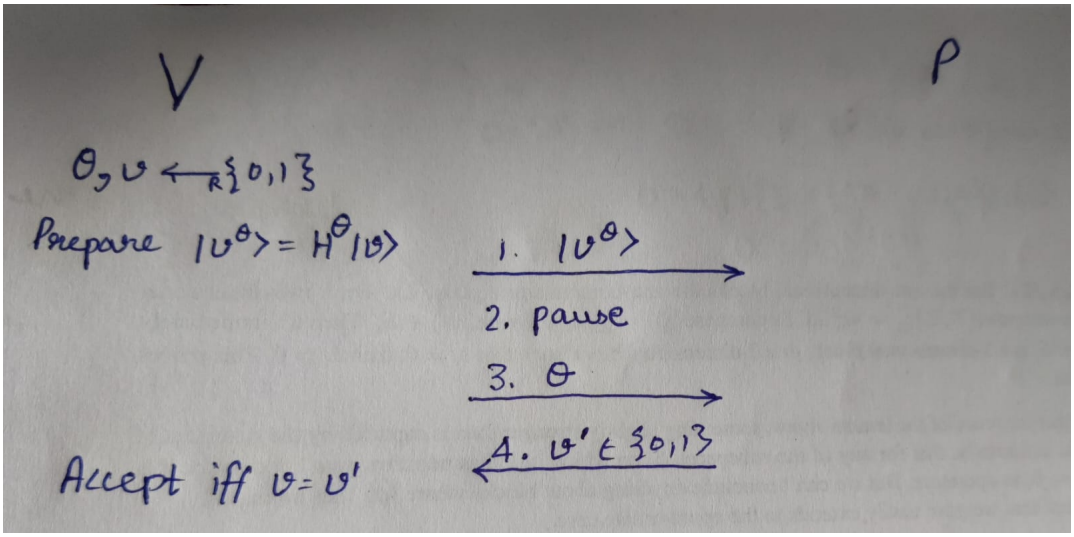

Figure 1: First test with quantum communication

Lemma 2.2. Suppose P succeeds in the protocol with probability 1. Then P has a qubit.

Before we go to the proof of the lemma, let us clarify a few points:

- *What does it mean for the prover to have a qubit?*

  It means that he has $(|\psi\rangle, X, Z)$ such that $\{X, Z\} = 0$. Even a classical prover can measure the qubit in the computational basis as soon as he gets it. This doesn't imply he has a qubit since he cannot perform anti-commuting measurements.

- *How can the verifier prepare qubits if he is classical?*

  We can have a third party prepare the qubits and give one to the verifier and others to the prover. (See Fig. 2)

- *How do we check that the winning probability is 1?*

  We can never be sure, but assuming that the prover behaves in an iid fashion and by repeating the protocol $K \approx (1/\epsilon)\log(1/\delta)$ times and observing K successes, we can conclude with confidence $1-\delta$ that the prover's intrinsic probability of succeeding is at least $1-\epsilon$. Let p be the winning probability of the prover. Then the probability of observing K wins is p^k. Taking $p < 1-\epsilon$

  $$\Pr[K \text{ wins}] < (1-\epsilon)^K < e^{-\epsilon K} = \delta$$

  So the prover has a chance at most δ to succeed in the K repetitions.

- *Is this a self-test of the qubit?*

  We can try to say that the family $\{p(v' \mid \theta, v) = 1_{v'=v}\}$ self-tests the qubit, but it doesn't fit into the definition for following reasons:

  - It is not a 1-round protocol
  - There is quantum communication between V and P
  - The verifier maintains some private information v

Proof. For proving the lemma, we use the alternate protocol (Fig. 2).

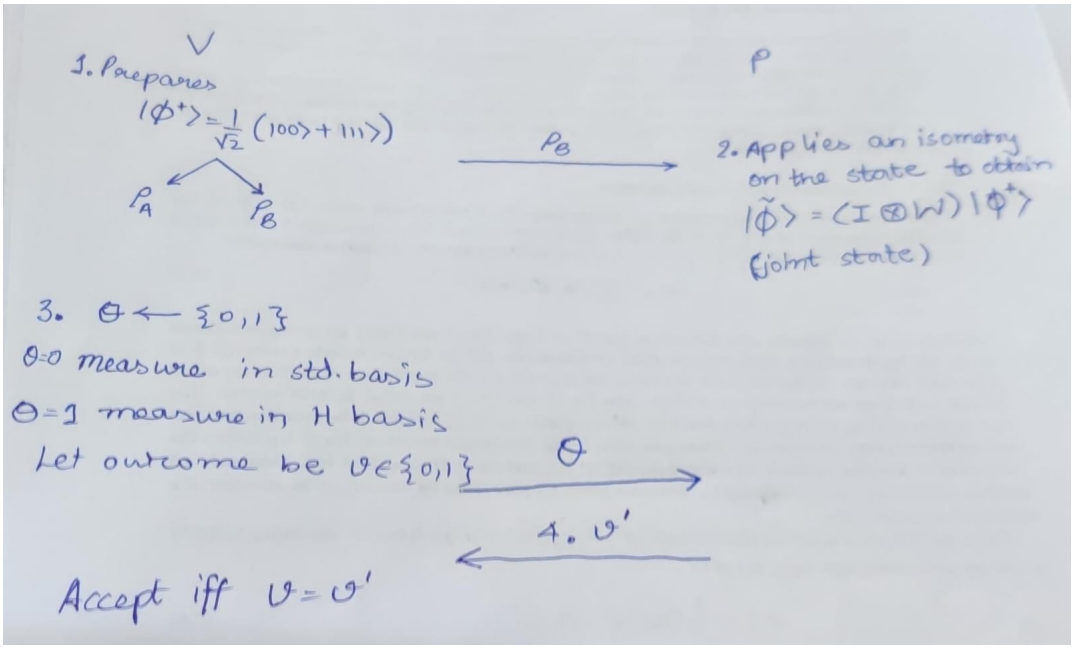

Figure 2: First test modified

Both protocols are identical from the perspective of the prover.
In fact, if we use a state $|\psi\rangle_{AB} \in \mathbb{C}^2_A \otimes \mathcal{H}_B$, we will show that even in this variant, to succeed, the prover must have a qubit.
It will generally be convenient to assume that any measurement that the prover makes can be modeled by a projective measurement. This can be guaranteed by **Naimark's theorem**. This is proved in Section 2.2.8 of [NC10], and we state it here for reference:

Lemma 2.3 (Projective Measurements + Unitary Transformations = General Measurements)**.** Let Q be a quantum system and $\{M_m\}$ be a general measurement on Q. Then these are equivalent to projective measurement $P_m = \mathbb{I}_Q \otimes |m\rangle\langle m|$ on the space $Q \otimes M$ where M is the ancilla space and $\{|m\rangle\}$ forms its orthonormal basis.

Note that using Naimark's may require extending the Hilbert space by adding ancilla qubits to $|\psi\rangle$. This operation is an isometry that one should not forget to include in the conclusion one is making – it is another reason for including the isometry V.
For each value of θ, the prover has a (projective) measurement $\{P_0^\theta, P_1^\theta\}$ with associated binary observable $P^\theta = P_0^\theta - P_1^\theta$ which he applies on his part of the state to obtain v'. The winning probability can be written as:

$$\begin{aligned}\Pr\left[v = v'\right] &= \frac{1}{2}\Pr\left[v = v'|\theta = 0\right] + \frac{1}{2}\Pr\left[v = v'|\theta = 1\right] \\ &= \frac{1}{2}(\langle\psi|\left(|0\rangle\langle 0| \otimes P_0^0\right)|\psi\rangle + \langle\psi|\left(|1\rangle\langle 1| \otimes P_1^0\right)|\psi\rangle) \\ &+ \frac{1}{2}(\langle\psi|\left(|+\rangle\langle +| \otimes P_0^1\right)|\psi\rangle + \langle\psi|\left(|-\rangle\langle -| \otimes P_1^1\right)|\psi\rangle)\end{aligned}$$

Now using

$$|0\rangle\langle 0| = \frac{1}{2}(\mathbb{I} + \sigma_Z) \qquad |1\rangle\langle 1| = \frac{1}{2}(\mathbb{I} - \sigma_Z) \qquad |+\rangle\langle +| = \frac{1}{2}(\mathbb{I} + \sigma_X) \qquad |-\rangle\langle -| = \frac{1}{2}(\mathbb{I} - \sigma_X)$$

$$\Pr\left[v = v'\right] = \frac{1}{2} + \frac{1}{4}(\langle\psi|\,\sigma_Z \otimes P^0\,|\psi\rangle + \langle\psi|\,\sigma_X \otimes P^1\,|\psi\rangle)$$

We observe that for $\Pr[v = v'] = 1$, we must have $\langle\psi|\,\sigma_Z \otimes P^0\,|\psi\rangle = \langle\psi|\,\sigma_X \otimes P^1\,|\psi\rangle = 1$. This implies that P^0, P^1 anti-commute, as is shown in the following lemma.

Lemma 2.4.

$$\langle\psi|\,\sigma_Z \otimes P^0\,|\psi\rangle = \langle\psi|\,\sigma_X \otimes P^1\,|\psi\rangle = 1 \implies (\mathbb{I} \otimes \{P^0, P^1\})\,|\psi\rangle = 0$$

Intuitively, if P^0, P^1 were compatible, then since P^1 can be used to predict the outcome of σ_X and P^0 can be used to predict the outcome of σ_Z, we will be able to predict the outcome of two incompatible observables by simultaneously measuring the compatible observables, a contradiction.

Proof.

$$\langle\psi|\,\sigma_Z \otimes P^0\,|\psi\rangle = 1 \implies \underbrace{\langle\psi|\,(\sigma_Z \otimes \mathbb{I})}_{\langle\psi_1|}\underbrace{(\mathbb{I} \otimes P^0)\,|\psi\rangle}_{|\psi_2\rangle} = 1$$

Now if for any unit vectors $|\psi_1\rangle, |\psi_2\rangle$ $\langle\psi_1|\psi_2\rangle = 1$ then we must have $|\psi_1\rangle = |\psi_2\rangle$. So,

$$\mathbb{I} \otimes P^0\,|\psi\rangle = \sigma_X \otimes \mathbb{I}\,|\psi\rangle \qquad\qquad \mathbb{I} \otimes P^1\,|\psi\rangle = \sigma_z \otimes \mathbb{I}\,|\psi\rangle$$

Using these

$$\begin{aligned}(\mathbb{I} \otimes P^0P^1)\,|\psi\rangle &= (\mathbb{I} \otimes P^0)(\mathbb{I} \otimes P^1)\,|\psi\rangle \\ &= (\mathbb{I} \otimes P^0)(\sigma_Z \otimes \mathbb{I})\,|\psi\rangle \\ &= (\sigma_Z \otimes \mathbb{I})(\mathbb{I} \otimes P^0)\,|\psi\rangle \\ &= \sigma_Z\sigma_X \otimes \mathbb{I}\,|\psi\rangle \\ &= -\sigma_X\sigma_Z \otimes \mathbb{I}\,|\psi\rangle \\ &= -(\mathbb{I} \otimes P^1P^0)\,|\psi\rangle\end{aligned}$$

$$\implies (\mathbb{I} \otimes \{P^0, P^1\})\,|\psi\rangle = 0$$

■

Hence $(|\psi\rangle, P^0, P^1)$ is the required qubit. ■

Exercise 2.2. Show that if P wins with probability $1-\epsilon$, then he has a $\delta(\epsilon)$- approximate qubit for some δ.

Exercise 2.3. The proof can be adapted to show a bit more than we extracted from it. By using Lemma 2.1, show that under the same assumptions as in the claim there must exist an isometry $V : \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}'$ on $\mathcal{H}$ under which $(\mathbb{I}_{\mathbb{C}^2} \otimes V) |\psi\rangle = |\phi^+\rangle \otimes |\phi'\rangle$, where $|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is an EPR pair, they must do so in order to win with probability 1.

2.4. A test for Quantum Memory

The main drawback of the above test is that it requires one qubit on the verifier's side to test one on the prover's side, while we want the verifier to be classical. Also, it doesn't extend to success probabilities less than 1. Practically, we would expect the prover to win with probability $1-\epsilon$, where ϵ can be made smaller with higher confidence by repeating the protocol.
This section will analyze a scaled-up version of the above protocol using information theoretic techniques Appendix B. This method can yield better quantitative results but allows us to certify less (only the prover's dimension and not the observable he uses).
Recall that the Von-Neumann entropy for state σ is given as

$$H(\sigma) = -\operatorname{tr}(\sigma \ln \sigma) = -\sum_i \lambda_i \ln \lambda_i$$

where λ_i are the non-zero eigenvalues of σ.
We will also require the chain rule : $H(\rho_A \otimes \rho_B) = H(\rho_A) + H(\rho_B)$

Definition 2.4 (Classical Quantum System)**.** A system of the form:

$$\rho_{XA} = \sum_x p_x |x\rangle \langle x|^X \otimes \rho_x^A$$

is said to be in a cq-state.

The conditional Von-Neumann Entropy is given by

$$H(A \mid B)_\rho = H(\rho_{AB}) - H(\rho_B)$$

This quantity can be negative but never more negative than the quantum dimension of B. Suppose for an arbitrary state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, we can decompose B into a classical register C and a quantum register Q:

$$\rho_B = \sum_c p_c |c\rangle\langle c| \otimes \rho_c \in \mathcal{H}_C \otimes \mathcal{H}_Q$$

Then $\rho_{AB} = \sum_c p_c |c\rangle\langle c|_C \otimes \rho'_c$ where $\rho'_c \in \mathcal{H}_A \otimes \mathcal{H}_Q$ such that $\operatorname{tr}_A(\rho'_c) = \rho_c$.

$$\begin{aligned}
H(A|B)_\rho &= H(\rho_{AB}) - H(\rho_B) \\
&= H(p_c) + \sum_c p_c H(\rho'_c) - H(p_c) - \sum_c p_c H(\rho_c) \\
&= \sum_c p_c (H(\rho'_c) - H(\rho_c)) \\
&\geq \min_c (H(\rho'_c) - H(\rho_c)) \\
&= \min_c \left(H(A \mid Q)_{\rho'_c} \right) \\
\implies H(A|B)_\rho &\geq -\log \dim \mathcal{H}_Q
\end{aligned}$$

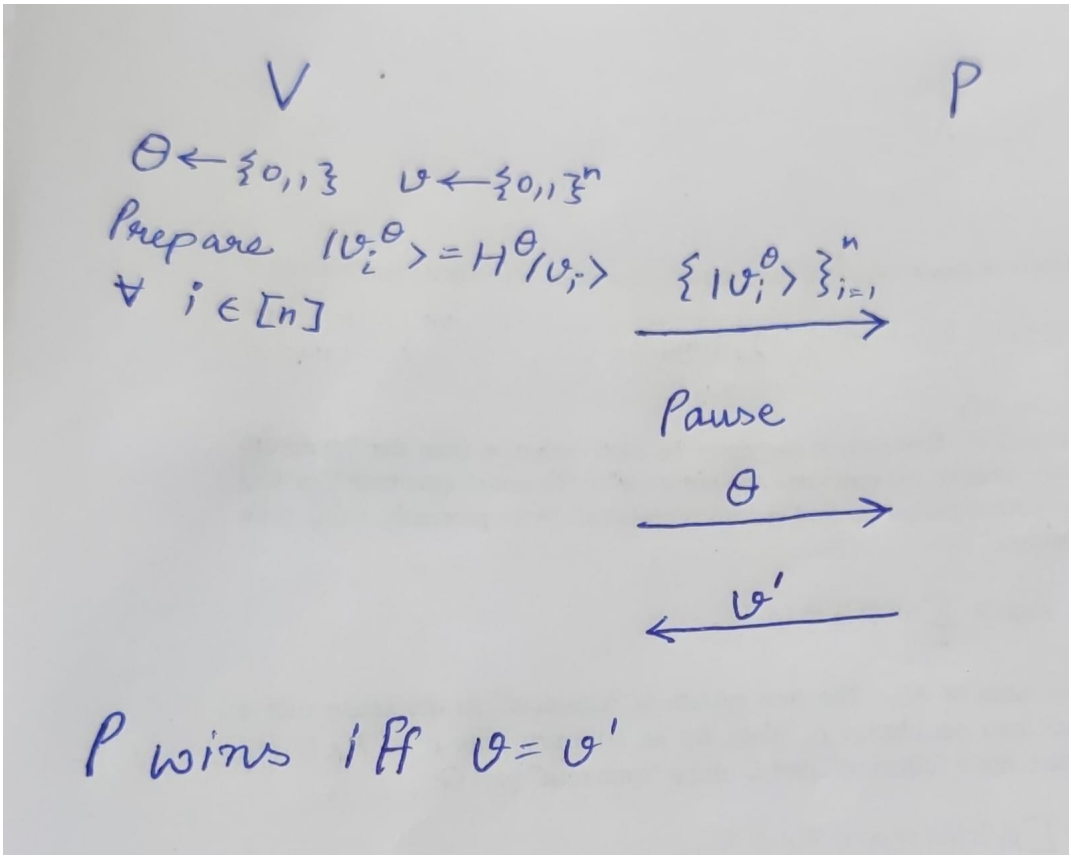

Figure 3: Testing large quantum memory

2.4.1. A test for large quantum memory

Lemma 2.5. Suppose P succeeds in the protocol with probability 1. Then P has quantum memory of dimension 2^n

§3. Lecture 4: Testing a Qubit under Computational Assumptions

So far, everything we have done is "information-theoretic," which means that they are independent of the model of computation used. In this lecture, we start making assumptions of a computational nature, such as 'this class of adversaries cannot solve this problem.'

3.1. Computational Assumptions

3.1.1. PPT and QPT

Since our protocols involve interactions between a prover and a verifier, our computational model will consist of several rounds, where in each round the prover or the verifier performs a computation to transition from an input and an initial state to an output and a final state.
To understand what we mean by a verifier (or prover) to be efficient, we will need to talk about families of verifiers. The verifier is specified by a classical Turing machine M which takes as input 1^n (where n is the size parameter) and 1^λ (where λ is the security parameter) and outputs an explicit classical description of a sequence of circuits that can be used to implement the verifier for problems of size n and with security λ. We say the verifier (prover) is probabilistic polynomial time or PPT (quantum polynomial time or QPT) if M runs in time polynomial in n. Note that this implies that the input size for the circuit, as well as the number of gates, is polynomial in n.

3.1.2. Claw-free functions

Let $\mathcal{M} = \{0,1\}^{m(\lambda)}$ and $\mathcal{K} = \{0,1\}^{k(\lambda)}$

Definition 3.1 (Claw-free functions)**.** A family $\mathcal{F} = \{f_{\mathsf{pk}} : \mathcal{M} \to \mathcal{M}\}_{\mathsf{pk}\in\mathcal{K}}$ is claw-free against classical (quantum) adversaries if

- **Efficient Computation:** There exists a PPT procedure that given pk and x returns $f_{\mathsf{pk}}(x)$
- $\mathbf{2-to-1}$: For every $\lambda \in \mathbb{N}$ and $\mathsf{pk} \in \mathcal{K}$, f_{pk} is 2-to-1.
- **Claw-free:** For every PPT(QPT) procedure $\mathcal{A}$, there exists a negligible function $\mu : \mathbb{N} \to \mathbb{N}$ such that for every λ the advantage of $\mathcal{A}$ in determining a 'claw' is negligible:

$$\Pr_{\mathsf{pk}\leftarrow\mathcal{K}}\left[(x_0,x_1) \leftarrow \mathcal{A}(1^\lambda,\mathsf{pk}) \mid x_0 \neq x_1, f_{\mathsf{pk}}(x_0) = f_{\mathsf{pk}}(x_1)\right] \leq \mu(\lambda)$$

3.1.3. Hardcore Bits

Definition 3.2 (Adaptive Hardcore Bit Assumption)**.** There is a claw-free family of functions $\mathcal{F} = \{f_{\mathsf{pk}}\}$ such that for any QPT adversary $\mathcal{A}$ there is a negligible function μ such that:

$$\left|\Pr_{\mathsf{pk}\leftarrow\mathcal{K}}\left[(x,d) \leftarrow \mathcal{A}(1^\lambda,\mathsf{pk}), \{x_0,x_1\} \leftarrow f_{\mathsf{pk}}^{-1}(f_{\mathsf{pk}}(x)) : d \neq 0^m \text{ and } d\cdot(x_0+x_1) = 0\right] - \frac{1}{2}\right| \leq \mu(\lambda)$$

In other words, the advantage of the adversary in Fig. 4 is negligible

No quantum polynomial time algorithm can simultaneously return an element x in the domain of f and an *equation* d such that letting $\{x_0,x_1\}$ be the two pre-images of $f_{\mathsf{pk}}(x)$ under f_{pk} it holds that $d \neq 0^m$ and $d\cdot(x_0+x_1) = 0$.

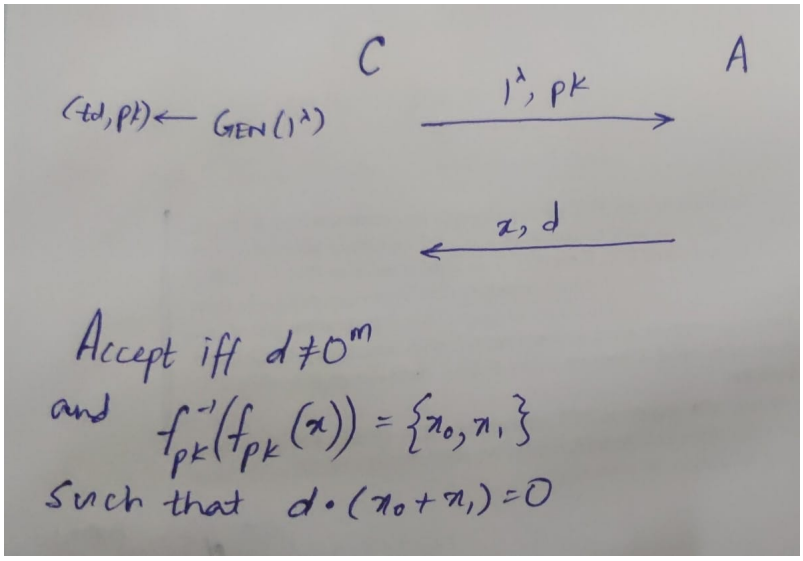

Figure 4: Adaptive Hardcore Bit Game

Given a function f, a hardcore bit for f is a 1-bit function h such that given $f(x)$ but not x, it is hard to predict $h(x)$. Here, the hardcore bit underlies the assumption that $h(x) = d \cdot (x_0 + x_1)$ for any $d \neq 0^m$. The **Goldreich-Levin Theorem** implies that if f is indeed claw-free, then it is hard to predict $h(x)$ for a *random* d. Further, we call it 'adaptive' because we allow the adversary to choose the equation d without requiring that this equation is uniformly distributed.

3.2. A computational test for a qubit

Assumptions

(F1) **Efficient Computation:** There is a 2-to-1 claw-free function family $\mathcal{F} = \{f_{\mathsf{pk}}\}$ equipped with an efficient key generation procedure $\text{GEN}(1^\lambda)$ such that for each pk the function f_{pk} can be evaluated efficiently.

(F2) **Adaptive Hardcore Bit:** The function family $\mathcal{F}$ satisfies Definition 3.2.

(F3) **Trapdoor:** In addition to pk, $\text{GEN}(1^\lambda)$ returns a trapdoor td, such that given $(\mathsf{pk}, \mathsf{td}, y)$ where $y \in \mathsf{range}(f_{\mathsf{pk}})$, it is possible to efficiently recover two pre-images x_0 and x_1 of y.

(F4) **Efficient Labelling Procedure:** For any pk and any y in the range of f_{pk} the tow pre-images of y are labelled x_0 and x_1 using some canonical efficient procedure. Given (pk, x) where $x \in \mathcal{M}$, it is possible to efficiently determine if x is the x_0 or the x_1 pre-image of $y = f(x)$. Let $b : \mathcal{M} \to \{0,1\}$ be the labeling procedure; it may depend on pk.

Theorem 3.1. Let $\mathcal{F}$ satisfy (F1)-(F4). Then the following hold for Fig. 5

- **Completeness:** There is a QPT prover that succeeds with probability 1 in the protocol.
- **Soundness:** Suppose a QPT prover P succeeds with probability 1 in the protocol. Then P has a (near-perfect) qubit.

Proof.

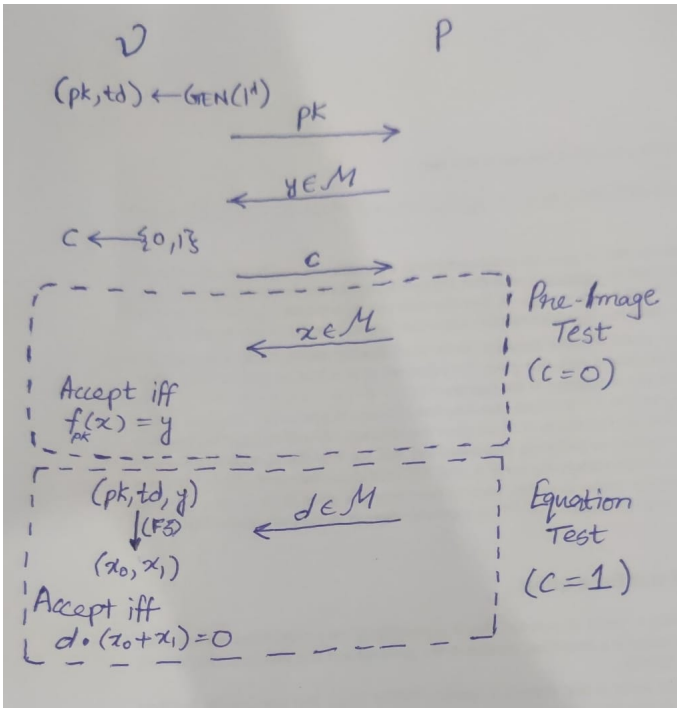

Figure 5: Protocol $\mathfrak{P}$

Completeness

It follows from the Simon's Algorithm. The final state obtained in the algorithm is

$$\frac{|x_0\rangle + |x_1\rangle}{\sqrt{2}} |f(x)\rangle$$

where $f(x_0) = f(x_1) = f(x)$ and $x_0 + x_1 = s$. P returns $y = f(x)$ in step 2. Now, if $c = 0$, he measures the first register in the computational basis to obtain a pre-image of y. Otherwise, he measures in the Hadamard basis:

$$\frac{|x_0\rangle + |x_1\rangle}{\sqrt{2}} \xrightarrow{H^{\otimes m}} \frac{1}{\sqrt{2^{m+1}}} \sum_d ((-1)^{x_0 \cdot d} + (-1)^{x_1 \cdot d}) |d\rangle = \frac{1}{\sqrt{2^{m+1}}} \sum_d (-1)^{x_0 \cdot d} (1 + (-1)^{(x_0 + x_1) \cdot d}) |d\rangle$$

Upon measuring, we obtain a $|d\rangle$ such that $d \cdot (x_0 + x_1) = 0$

Soundness:

Step1: Modelling Let $|\psi\rangle$ be the state of the prover at the end of step 2. Let $\{\Pi_x\}$ and $\{M_d\}$ be the POVM measurements taken by P upon receiving $c = 0$ and $c = 1$ respectively.

- We can take Π, M to be PVM by Naimark's Theorem.
- We assume that P has a register X with initial state $|0^m\rangle$
- Any projective measurement on $|\psi\rangle$ can be considered a unitary transformation followed by a standard basis measurement of X. So, we take the following circuits for simulating measurement of Π and M.
- For further simplifying, take $U_0' = I, U_1' = U_1 U_0^\dagger$ and $|\psi'\rangle = U_0 |\psi\rangle$ as the unitary transforms and the state with P after step 2 respectively.

Step2: Establishing a Qubit

■

§A. Quantum Interactive Proofs, Semidefinite Programs and Multiplicative weights

Reference: [Gha21] lecture 8
There are several quantum complexity classes depending on the type of communication between the prover and the verifier:

- **BQP:** No communication
- **QMA:** One way quantum communication from prover to verifier
- **QCMA:** One way classical communication from prover to verifier
- **QIP:** Interactive communication between prover and verifier

In this section, we will study the proof QIP=PSPACE. But before that, we study Multiplicative Weights Algorithm and Semi-definite Programs.

A.1. The Multiplicative Weights Algorithm

If it worked once, it is likely to work again

Imagine we have a set of E of n experts, and T rounds of some process for which we wish to take the experts' advice into account. In each round $t \in [T]$, we have a probability distributioin p^t over E. We imagine that the environment now assigns a 'cost' to each expert's choice in round t denoted $-1 \leq c_i^t \leq 1$.
Ideally, we would want to choose the best expert, i.e.

$$\min_{i\in[n]} \sum_{t=1}^{T} c_i^t$$

and follow him through all the rounds. However, that is not possible practically, but we can get quite close to the optimal.
Define the expected cost for round t as

$$C_t := \sum_{i=1}^{n} p_i^t c_i^t = \langle c^t, p^t \rangle$$

and for all rounds as

$$C = \sum_{t=1}^{T} C_t$$

Theorem A.1. Fix $0 < \epsilon \leq 1/2$. Then, for any expert E_i after T rounds of the MW algorithm obtains expected cost

$$C \leq \sum_{t=1}^{T} c_i^t + \left[\epsilon \sum_{t=1}^{T} |c_i^t| + \frac{\ln n}{\epsilon} \right]$$

Proof. Define potential function

$$\Phi_t = \sum_i w_i^t$$

Upper Bound:

$$\Phi_{t+1} = \sum_i w_i^{t+1} \leq \sum_i w_i^t (1 - \epsilon c_i^t) = \Phi_t (1 - \epsilon \sum_i c_i^t p_i^t) \leq \Phi_t e^{-\epsilon \langle c_i^t, p_i^t \rangle}$$

Algorithm 1: MW Algorithm

Data: Parameters: $0 < \epsilon \leq 1/2$, weights $w_i = 1$ for E_i

for $t = 1$ **to** T **do**

  Pick E_i with probability $w_i^t / \sum_i w_i^t$;

  Obtain costs c^t for round t from the environment;

  Update weight of **all** E_i as

$$w_i^{t+1} \leftarrow \begin{cases} w_i^t(1-\epsilon)^{c_i^t} & \text{if } c_i^t \geq 0 \\ w_i^t(1+\epsilon)^{-c_i^t} & \text{if } c_i^t < 0 \end{cases}$$

Since $\Phi_1 = n$, $\Phi_{T+1} \leq e^{-\epsilon \sum_i \langle c_i^t, p_i^t \rangle} = e^{-\epsilon C}$

Lower Bound: $w_i^t \geq 0 \implies \Phi_t > w_i^t$ Now

$$w_i^{t+1} = \begin{cases} w_i^t(1-\epsilon)^{c_i^t} & \text{if } c_i^t \geq 0 \\ w_i^t(1+\epsilon)^{-c_i^t} & \text{if } c_i^t < 0 \end{cases}$$

$$\ln\left(w_i^{t+1}\right) = \ln\left(w_i^t\right) + \begin{cases} \ln(1-\epsilon)c_i^t & \text{if } c_i^t \geq 0 \\ -\ln(1+\epsilon)c_i^t & \text{if } c_i^t < 0 \end{cases}$$

Now we use the inequality $\ln(1-\epsilon) \geq -\epsilon - \epsilon^2$ and $\ln(1+\epsilon) \geq \epsilon - \epsilon^2$

$$\ln\left(w_i^{t+1}\right) \geq \ln\left(w_i^t\right) - \epsilon c_i^t - \epsilon^2 |c_i^t|$$

Now use induction to prove

$$\ln\left(w_i^{t+1}\right) \geq \epsilon \sum_t c_i^t - \epsilon^2 \sum_t |c_i^t|$$

Using this with the upper bound, we obtain the required expression. ■

Some important inequalities used in the above proof:

- $(1-\epsilon)^x \leq (1-\epsilon x)$ for $x \in [0,1]$
- $(1+\epsilon)^{-x} \leq (1-\epsilon x)$ for $x \in [-1,0]$
- $\ln(1-\epsilon) \geq -\epsilon - \epsilon^2$ for $0 < \epsilon \leq 1/2$
- $\ln(1+\epsilon) \geq \epsilon - \epsilon^2$ for $0 < \epsilon \leq 1/2$
- $e^{-x} \geq 1 - x$ for $x > 0$

A.2. Quantum Interactive Proofs

Definition A.1 (m round Quantum Verifier)**.** An m round quantum verifier is a P-uniform circuit family $Q = \{Q_{n,1}, Q_{n,2}, \ldots, Q_{n,m}\}$ acting on three registers:

- An input register A containing $x \in \{0,1\}^n$
- A message register M consisting of $p(n)$ qubits
- An ancilla or private register V consisting of $q(n)$ qubits

for some polynomials $p, q : \mathbb{N} \to \mathbb{N}$. We imagine the verifier acts in rounds, applying circuit $Q_{n,i}$ in round $i \in [m]$. Before round 1, message and private registers are initialized to zero.

Definition A.2 (m round Quantum Prover)**.** Same as Definition A.1 but the circuit family need not be P-uniform

Definition A.3 (Quantum Interactive Proof Systems (QIP))**.** A promise problem $\mathcal{A} = (\mathcal{A}_{yes}, \mathcal{A}_{no}, \mathcal{A}_{inv})$ is in QIP if there exists a polynomial $m : \mathbb{N} \to \mathbb{N}$ and m-round quantum verifier satisfying for $x \in \{0,1\}^n$

- Completeness: $x \in \mathcal{A}_{yes} \implies \exists P^m$ acceptance probability $\geq 2/3$
- Soundness: $x \in \mathcal{A}_{no} \implies \forall P^m$ acceptance probability $\leq 1/3$
- Invalid: accept or reject arbitrarily

Remark. 2 rounds of communication suffice to capture the entire class of QIP. Moreover, the second message in the protocol (first from the verifier to the prover) can be a random toss of a fair coin.

A.3. Semidefinite Programming

Semidefinite Programming is the extension of Linear Programming to the case where the vectors are replaced by Hermitian Matrices and the inequality constraints are replaced by $\succeq$

Definition A.4 (Standard Form)**.** To define the standard form, we require the following:

1. A cost matrix $C \in \text{Herm}(\mathcal{X})$
2. A constraint matrix $D \in \text{Herm}(\mathcal{Y})$
3. A linear constraint map $\Psi : \text{Herm}(\mathcal{X}) \to \text{Herm}(\mathcal{Y})$

Here $\mathcal{X}$ and $\mathcal{Y}$ are fixed complex vector spaces. The primal SDP is given by Table 1

Primal SDP (P)	**Dual SDP (D)**
sup: $\text{tr}(CX)$	inf: $\text{tr}(DY)$
subject to: $\Psi(X) \preceq D$	subject to: $\Psi^*(Y) \succeq D$
$X \succeq 0$	$Y \succeq 0$

Table 1: Primal and Dual SDP

- The **variable** being optimized over is $X \in \text{Herm}(\mathcal{X})$
- The **feasible region** is the set of all "valid assignments", i.e. those satisfying the constraints
- The **objective function** being maximized, $\text{tr}(CX) = \text{tr}\left(C^\dagger X\right) = \langle C, X\rangle$ is linear in X.
- The map Ψ must be **Hermiticity Preserving** for the inequalities to be well defined (positive semi-definite)
- Once an SDP is in the standard form, we can formulate the corresponding dual SDP, with the **adjoint map** $\Psi^* : \text{Herm}(\mathcal{X}) \to \text{Herm}(\mathcal{Y})$ satisfying

$$\langle A, \Psi(B)\rangle = \langle \Psi^*(A), B\rangle$$

Examples:

1. Is $I \succeq X$?
   Sol: One of the methods is to show that $\langle\psi|(I-X)|\psi\rangle$ is PSD for any general $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
   Another way is to see that
   $$I - X \succeq I - \|X\|_\infty I \succeq 0$$
   Yet another way is
   $$I - X = |+\rangle\langle+| + |-\rangle\langle-| - (|+\rangle\langle+| - |-\rangle\langle-|) = 2|-\rangle\langle-|$$
   which is PSD.
2. Is $I \succeq 2X$?
   Sol: Take $\langle+|(I-2X)|+\rangle$
3. Let $\Psi : \mathcal{L}(\mathbb{C}^n) \to \mathbb{C}$ be the trace function. What will be Ψ^*?
   Sol:
   $$\langle A, \Psi(B)\rangle = \langle \Psi^*(A), B\rangle$$
   $$\implies \operatorname{tr}\big(A \operatorname{tr}(B)\big) = \operatorname{tr}\big(\Psi^*(A)B\big)$$
   Take $\Psi^*(A) = \operatorname{tr}(A)I$. Uniqueness guarantees this is the only solution.
4. The simplest example of an SDP is the calculation of the largest eigenvalue of a Hermitian matrix $C \in \mathrm{Herm}(\mathbb{C}^n)$

Duality Theory

Let p and d denote the optimal values for a primal and corresponding dual SDP. These values satisfy **weak duality**

$$p \leq d$$

Theorem A.2 (Slater's constraint qualification)**.** If there is a strictly feasible solution X (i.e. $X \succ 0, \Psi(X) \prec D$) then **strong duality** ($p = d$) holds.

Runtime

To solve SDP in poly-time, we need the following conditions:

1. The feasible region must be contained in a ball of radius R
2. The feasible region must contain a ball of radius r

Then the runtime (Ellipsoid method) is polynomial in

- Input (encodings of C, Ψ, D)
- $\log R$
- $\log \frac{1}{r}$
- $\log \frac{1}{\epsilon}$

where ϵ is the additive error for the solution

§B. Entropy and Information

Here, we review the concept of entropy, which is instrumental to the understanding of Quantum Information.

B.1. Shannon Entropy

Shannon Entropy of a random variable X quantifies how much information we gain, on average, *after* we learn the value of X. Alternatively, it measures the amount of uncertainty we had *before* knowing the value of X. Both these views are complementary. Also, the information content of a random variable should not depend on the labels attached to the different values that the random variable may take. Thus, the entropy is defined in terms of the probabilities and not the values of the random variable.

Definition B.1 (Shannon Entropy)**.** Let X be a random variable having the probability distribution $\{p_i\}_{i\in[n]}$. Then Shannon entropy of X is

$$H(X) = H(p_1 \dots p_n) = -\sum_x p_x \log p_x$$

Intuitive justification: [NC10] Suppose we are trying to quantify how much information is provided by an event E, which may occur probabilistically. We do this by using an *information function* $I(E)$ whose value is determined by E. Suppose the following assumptions are made about this function:

1. $I(E)$ is a function of only the probability of E, not the outcomes themselves. So we can write $I = I(p), p \in [0,1]$
2. I is a smooth function
3. $I(pq) = I(p) + I(q)$ - the information gained when two independent events occur with individual probabilities p, q is the sum of the information gained from each event alone.

Cauchy proved that the only continuous solution of the functional equation $f(x) + f(y) = f(xy)$, where $f(x)$ is defined for all real numbers x, is the function $f(x) = a \log x$ for some constant a

B.2. Basic Properties of Entropy

B.2.1. Binary Entropy

For a Bernoulli Random variable, the binary entropy is

$$H_{\text{bin}}(p) := -p \log(p) - (1-p) \log(1-p)$$

Properties:

- $H_{\text{bin}}(0) = H_{\text{bin}}(1) = 0$
- $H_{\text{bin}}(p)$ attains its maximum value of 1 at $p = \frac{1}{2}$
- **Strict Concavity of binary entropy**

  $$H_{\text{bin}}(px_1 + (1-p)x_2) \geq pH_{\text{bin}}(x_1) + (1-p)H_{\text{bin}}(x_2) \qquad 0 \leq p, x_1, x_2 \leq 1$$

  with equality only for $p = 0, 1$ or $x_1 = x_2$

B.2.2. Relative Entropy

Relative entropy of two distributions $p(x), q(x)$ is a measure of the closeness of two probability distributions.

$$H(p(x)||q(x)) := -\sum_x p(x)\log\frac{q(x)}{p(x)} = -H(X) - \sum_x p(x)\log(q(x))$$

Theorem B.1 (Non-negativity of Relative Entropy)**.**

$$H(p(x)||q(x)) \geq 0$$

with equality iff $p(x) = q(x)$ for all x

Proof. An important inequality:

$$\ln x \leq x - 1$$

with equality iff $x = 1$. It can also be written as

$$-\log(x) \geq \frac{1-x}{\ln 2}$$

$$H(p(x)||q(x)) = -\sum_x p(x)\log\frac{q(x)}{p(x)} \geq \frac{1}{\ln 2}\sum_x p(x)\left(1 - \frac{q(x)}{p(x)}\right) = 0$$

■

Theorem B.2. Suppose X is a random variable with d outcomes. Then $H(X) \leq \log(d)$ with equality iff X is uniformly distributed over the d outcomes.

Proof. Let $q(x)$ be a uniformly random distribution over the d outcomes.

$$H(p(x)||q(x)) = -\sum_x p(x)\log\left(\frac{1}{dp(x)}\right) = \log(d) - H(X) \geq 0$$

■

Theorem B.3 (Subadditivity of Shannon Entropy)**.**

$$H(p(x,y)||p(x)p(y)) = H(p(x)) + H(p(y)) - H(p(x,y))$$

Theorem B.1 implies

$$H(X,Y) \leq H(X) + H(Y)$$

with equality iff X, Y are independent random variables.

Proof.

$$H(p(x,y)||p(x)p(y)) = -\sum_{xy} p(xy)(\log(p(x)) + \log(p(y))) - H(p(x,y)) = H(p(x)) + H(p(y)) - H(p(x,y))$$

■

B.2.3. Conditional entropy and mutual information

Definition B.2 (Joint Entropy)**.**

$$H(X,Y) := -\sum_{x,y} p(x,y)\log\big(p(x,y)\big)$$

It measures our total uncertainty about the pair (X,Y).

Definition B.3 (Conditional Entropy)**.**

$$H(X \mid Y) := H(X,Y) - H(Y)$$

It measures how uncertain we are, on average, about the value of X if we know that of Y.

Definition B.4 (Mutual Information)**.**

$$H(X:Y) := H(X) + H(Y) - H(X,Y) = H(X) - H(X \mid Y)$$

It measures how much information X, Y have in common. Also $H(X:Y) = H(X) - H(X \mid Y)$

Definition B.5 (Basic Properties of Shannon Entropy)**.**

1. $H(X,Y) = H(Y,X)$
2. $H(X:Y) = H(Y:X)$
3. $H(Y \mid X) \geq 0$ and thus $H(X:Y) \leq H(X), H(X:Y) \leq H(Y)$ with equality iff Y is a function of $X - Y = f(X)$
4. **Subadditivity** $H(X,Y) \leq H(X) + H(Y)$ with equality iff X and Y are independent random variables.
5. $H(Y \mid X) \leq H(Y)$ and thus $H(X:Y) \geq 0$ with equality iff X and Y are independent random variables.
6. **Strong Subadditivity** $H(X,Y,Z) + H(Y) \leq H(X,Y) + H(Y,Z)$ with equality iff $Z \to Y \to X$ forms a Markov chain.
7. **Conditioning Reduces Entropy** $H(X \mid Y,Z) \leq H(X \mid Y)$

B.3. Entropic Quantum Uncertainty Principle

The uncertainty principle of quantum mechanics tells us that for observables C, D

$$\Delta(C)\Delta(D) \geq \frac{|\langle\psi|\,[C,D]\,|\psi\rangle|}{2}$$

Theorem B.4 (Entropic Uncertainty Principle)**.** Let C, D be observables on $\mathcal{H}_A$ and $f(C,D) = \max_{c,d} |\langle c|d\rangle|$ be the maximum fidelity between any two eigenvectors of C, D. Suppose the quantum system is prepared in the state $|\psi\rangle$.

Then, the entropic uncertainty principle states:

$$H(C) + H(D) \geq 2\log\left(\frac{1}{f(C,D)}\right)$$

Here, the entropies are calculated using $p(c)$ – the probability distribution associated with the measurement of observable C, with associated entropy $H(C)$ and $q(d)$ – the probability distribution associated with the measurement of observable D, with associated entropy $H(D)$.

- When C, D are binary observables, then $f(C,D)$ is the cosine of the smallest angle between the eigenspaces of C, D.
- If C, D have an eigenvector in common the $f(C,D) = 1$ and the RHS vanishes.
- If C, D anti-commute, then the angle between any of their vectors is $\pi/4$, and the RHS becomes 1. So there is at least 1 bit of uncertainty between the outcomes of measuring C, D

Interpret the above result as a statement about the difficulty of a prediction task:

1. The Adversary $\mathcal{A}$ prepares an arbitrary state $|\psi\rangle$ and sends it to the challenger $\mathcal{C}$.
2. $\mathcal{C}$ selects $\theta \leftarrow \{0,1\}$ and measures $|\psi\rangle$ using C if $\theta = 0$ or D if $\theta = 1$, obtaining c or d respectively. It sends θ to the prover $\mathcal{P}$.
3. $\mathcal{P}$ returns its guess c' or d' depending on θ.
4. $\mathcal{A}$ succeeds if the guess is correct.

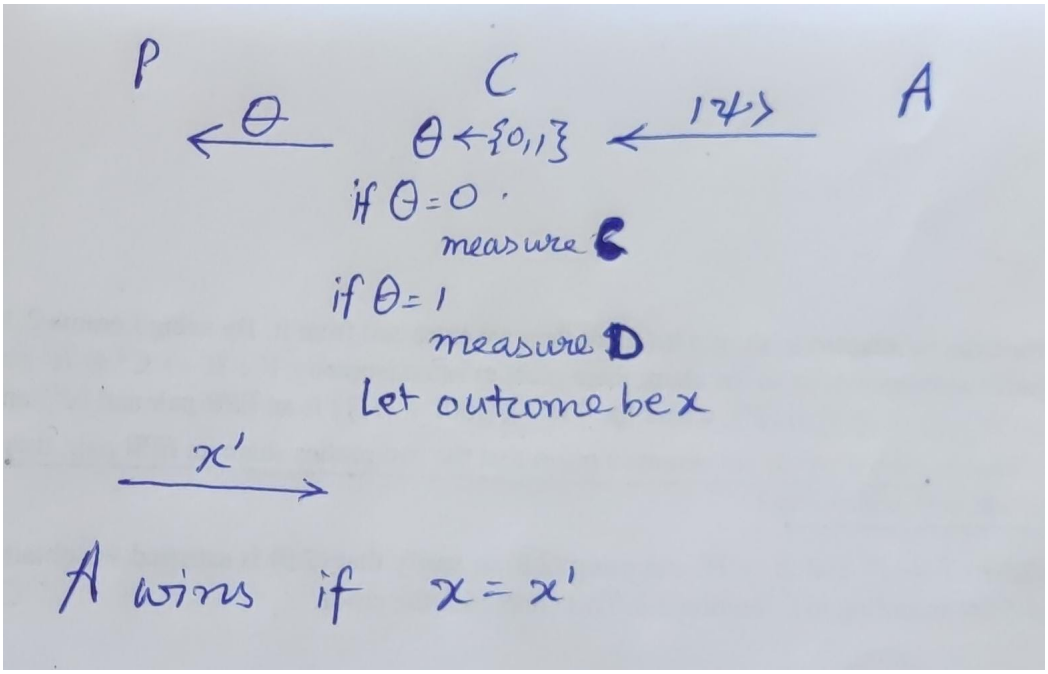

Figure 6: Uncertainty Game

If we set C to σ_X and D to σ_Z, then using Fig. 2, we can conclude that $\mathcal{A}$ succeeds perfectly ($\mathcal{P}$ and $\mathcal{C}$ need to share an EPR pair before starting the game).

Theorem B.5. Let C, D be observables on $\mathcal{H}_A$ and $f(C,D) = \max_{c,d} |\langle c|d\rangle|$ be the maximum fidelity between any two eigenvectors of C, D. Let ρ_{AB} be an arbitrary density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$. Let $C(\rho), D(\rho) \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ denote the post-measurement states after a measurement of A using the observables C and D respectively. Then

$$H(A \mid B)_{C(\rho)} + H(A \mid B)_{D(\rho)} \geq 2\log\left(\frac{1}{f(C,D)}\right) + H(A \mid B)$$

References

[CRSV17] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Overlapping qubits. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2017. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2017.48, doi:10.4230/LIPICS.ITCS.2017.48.

[Gha21] Sevag Gharibian. Quantum complexity theory, 2021. URL: https://groups.uni-paderborn.de/fg-qi/data/QCT_Masterfile.pdf.

[JNV+22] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip*=re, 2022. arXiv:2001.04383.

[Mah23] Urmila Mahadev. Classical verification of quantum computations, 2023. arXiv:1804.01082.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge, 2010. URL: http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf.

[Vid20] Thomas Vidick. Interactive proofs with quantum devices, 2020. URL: http://users.cms.caltech.edu/~vidick/teaching/fsmp/.