\[ \sum _{x} |x \rangle \text{ if } (x \rangle \rangle \]
\[ \downarrow \]
\[ (|x_0 \rangle + |x_1 \rangle) |y \rangle \]
\[ \downarrow \text{ X basis measurement} \]
\[ \cdot \quad d \cdot (x_0 + x_1) = 0 \]

Modifications to \( \mathcal{F} \):

1) For any \( y \), preimages of \( y \) look like \((0, x_0)\) \((1, x_1)\)

\[ b(x) = \text{ first bit of } x \]
2) A family $\mathcal{S}$ of injective
s.t. given $pk$

can't distinguish $f_{pk} \in \mathcal{S}$

---

Problem has $|\psi_{10}\rangle + |\psi_{11}\rangle$

\[ \sum_x (\alpha |0x\rangle + \beta |1x\rangle) |0^n\rangle \]

compute $f_{pk}$

\[ \sum_x (\alpha |0x\rangle |f_{pk}(0x)\rangle + \beta |1x\rangle |f_{pk}(1x)\rangle) \]
"encoding" : $|d10) + \beta 11)\rangle$

P measures 3rd register to get $y$
returns to $V$

Case 1: $f_{pk} \in F$

$(d_{10}x_{10}) + \beta 11x_{11}) |y\rangle$

Case 2: $f_{pk} \in G$

$|b x > | y\rangle$

Once P has revealed $y$, it has "committed" to $|d10) + \beta 11)\rangle$
Measurement phase:

V decides to run "test round" or a "Hadamard round"

Test round:
Ask for preimage receive box
Check that \( f_{ph}(box) = y \)

Hadamard:
Paul measures the first reg. in X basis (Hadamard basis) to get \( b', d \)

(about it \( b', d = 0^n \))
- If \( \mathbf{f}_{\mathbf{p}} \in \mathcal{F} \) ("X measured")
  Read the measurement outcome as \((-1) b' + d \langle x_0 + x \rangle\),

- If \( \mathbf{f}_{\mathbf{p}} \in \mathcal{G} \) ("Z measured")
  Ignore \( b', d \).
  Record measurement outcome as \((-1)^b \).

\((b, x)\) is preimage of \(Y\) that \(V\) found using \(+d\).

Claim: Suppose \( P \) succeeds w/ prob. \( 1 - \text{negl.} \).
Then \( \exists \) a 1-qubit state \( \rho \)

s.t. \( \text{tr} [ \sigma_2 \rho ] = E [ \text{outcome of } Z \text{- measurement in } \rho ] \)

\( \text{tr} [ \sigma_x \rho ] = E [ \text{outcome of } X \text{- measurement in } \rho ] \)

for 1-qubits

for \( n \)-qubits, computationally indistinguishable

Why?

- For \( Z \) measurements, 1-to-1 function forces collapse in \( Z \) basis
- Prover cannot tell whether an \( X \)-basis or \( Z \)-basis measurement is being performed
Consider the 2+1 case

\[(\alpha |0, x_0\rangle + \beta |1, x, \rangle) |y\rangle\]

By security of \(\Sigma\), prove no one doesn't know \(x_0, x, y\) can't alter the state

Also: \(X_{\text{output}} = (-1)^{b' + d(x_0 + x,)}\)  

Powers only control \(b', d\)

To get \(X_{\text{output}} = +1\) w.h.p., guess \(b', d\) s.t. \(b' + d(x_0 + x,) = 0\)

But you can't \(b'/d\) or hardcore bit assumption
Using measurement protocol to verify BQP [Mohinder '18]

- First need multiqubit version

\[ \ell_{in}|n\rangle \]

\[ \sum_{u_0, u_1} \alpha_u \langle u_1 | x_1 \ldots x_n | u_2 x_2 | f(x) \rangle \]

\[ \vdots \]

\[ \sum_{u_0, u_1} \alpha_u \langle u_1 | x_1 \ldots x_n | 1_{y_1} \rangle \]

Verifier can measure any tensor product of \( X, Z \) on
the qubits
without revealing to prover

2) History state
\[ \langle \psi | H_c | \psi \rangle \leq E_{\text{thresh}} \]
\[ \Rightarrow \quad \text{BQP computation c accepts w.h.p.} \]

\[ H_c = \sum X \otimes 0 \otimes X \ldots \]

- Tell prover to prepare \( |\psi_c\rangle \)
  with low energy

- Run the \( n\)-qubit measurement protocol for many randomly chosen terms in \( H_c \)

compute estimate for \( \langle H_c \rangle \)