$\underbrace{|\psi\rangle}_{\mathcal{H}_p}$ = STATE AFTER P SEND y

- $c=0$ W.L.O.G. (b, x_b) IS OBTAINED AS RESULT OF A PROJECTIVE MEASUREMENT $\{\Pi_{x,b}\}_{x,b}$ ACTING ON $\mathcal{H}_M$

$$\cancel{U^* \underbrace{|\psi\rangle}_{\mathcal{H}_p} \underbrace{|0\rangle}_{\mathcal{H}_M} \longrightarrow \underbrace{|\psi'\rangle}_{\mathcal{H}_p \mathcal{H}_M}}$$

$$\cancel{|\psi\rangle = U^* |\psi\rangle}$$

- $C=1$ WLOG d IS OBTAINED BY A PROJ. MEASUREMET $\{M_d\}_d$ ACTING ON $\mathcal{H}_M$

$$U \underbrace{|\psi\rangle}_{\mathcal{H}_p} \underbrace{|0\rangle}_{\mathcal{H}_M} \longrightarrow \underbrace{|\psi'\rangle}_{\mathcal{H}_p \otimes \mathcal{H}_M}$$

$|\psi\rangle$ OBSERVABLES :

$$Z = \sum_{x \in D_r,\, b \in \{0,1\}} (-1)^b \, |x_{b,b}\rangle\langle x_{b,b}| \otimes I_p$$

+1 : x is a "0" preimage of y

~~+1~~ −1 : x is a "1" preimage of y

$$X = \sum_d (-1)^{d \cdot Bit(x_0) \oplus Bit(x_1)} \qquad U^\dagger (H^{\otimes m} \otimes I_p)^\dagger \underbrace{(|d\rangle\langle d| \otimes I_p)}_{\text{proj}_d \text{ onto}} (H^{\otimes m} \otimes I_p) U$$

+1 : d is "VALID"

−1 : d is "INVALID"

Claim: $(|\psi\rangle, X, Z)$ is a QUBIT.

$$(XZ + ZX)|\psi\rangle \approx 0$$

$XZ + ZX$ is Hermitian

$$(XZ+ZX)^\dagger = (XZ)^\dagger + (ZX)^\dagger = Z^\dagger X^\dagger + X^\dagger Z^\dagger = ZX + XZ = XZ + ZX$$

PROOF:

$$\frac{1}{2}\|(XZ+ZX)|\psi\rangle\|^2 =$$

$$= \frac{1}{2}\langle\psi| \underbrace{(XZ+ZX)^\dagger}_{\text{Lemma 1}} (XZ+ZX)|\psi\rangle$$

$$= \frac{1}{2}\langle\psi|(XZ+ZX)^2|\psi\rangle$$

$$= \langle\psi|XZ_0XZ_0|\psi\rangle + \langle\psi|Z_1XZ_1X|\psi\rangle + \langle\psi|Z_0XZ_0X|\psi\rangle + \langle\psi|XZ_1XZ_1|\psi\rangle$$

for any two binary observables (X, Z):

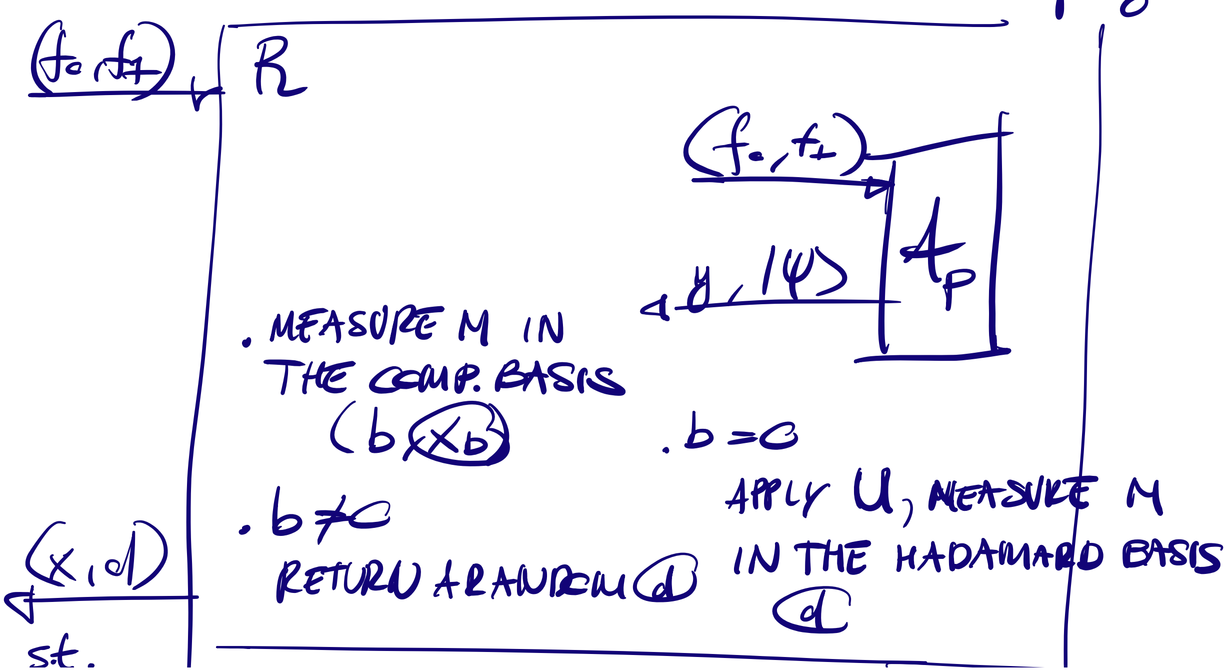
$$\tfrac{1}{2}(XZ+ZX)^2 = XZ_0XZ_0 + Z_1XZ_1X + Z_0XZ_0X + XZ_1XZ_1$$

$(Z = Z_0 - Z_1)$ Lemma 2

$X|\psi\rangle = |\psi\rangle$ (P succeeds w.p. 1)

$$= 2\Big(\underbrace{\langle\psi|Z_0XZ_0|\psi\rangle}_{\approx\, negl(\lambda)} + \underbrace{\langle\psi|Z_1XZ_1|\psi\rangle}_{\approx\, negl(\lambda)}\Big)$$

ASSUME TOWARDS CONTRADICTION THAT $\geq \frac{1}{poly}$



X IS A VALID PREIMAGE OF y
AND $d \cdot (B(x_0) \oplus B(x_1)) = 0$

wp 1/2: $b = 1$

$$Pr[\text{success}] = \frac{1}{2} \underbrace{\langle \psi | Z_1 | \psi \rangle}_{\text{prob that } Z_1 \text{ succeeds on } |\psi\rangle} \to \frac{1}{2}$$

$*$

$\Rightarrow$ prob $b = 1$

$b = 0$

$$Pr[\text{success}] = \langle \psi | Z_0 X_0 Z_0 | \psi \rangle$$

$$= \frac{1}{2}\left(\langle \psi | Z_0 | \psi \rangle + \underbrace{\langle \psi | Z_0 X Z_0 | \psi \rangle}\right)$$

$\langle \psi | Z_0 | \psi \rangle \to \frac{1}{2}$

$$X = X_0 - X_1$$

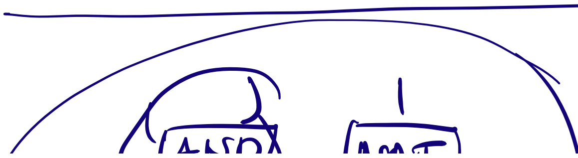
$$X_0 + X_1 = I$$

$$\Rightarrow X_0 = \frac{1}{2}(I + X)$$

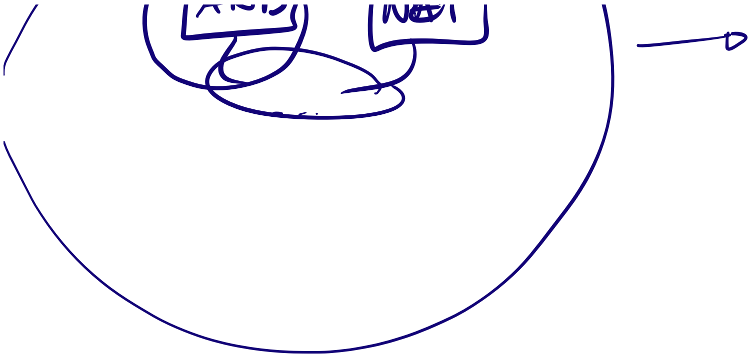
$$\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2}\left(\frac{1}{2} + \underbrace{\langle \psi | Z_0 X Z_0 | \psi \rangle}\right)$$

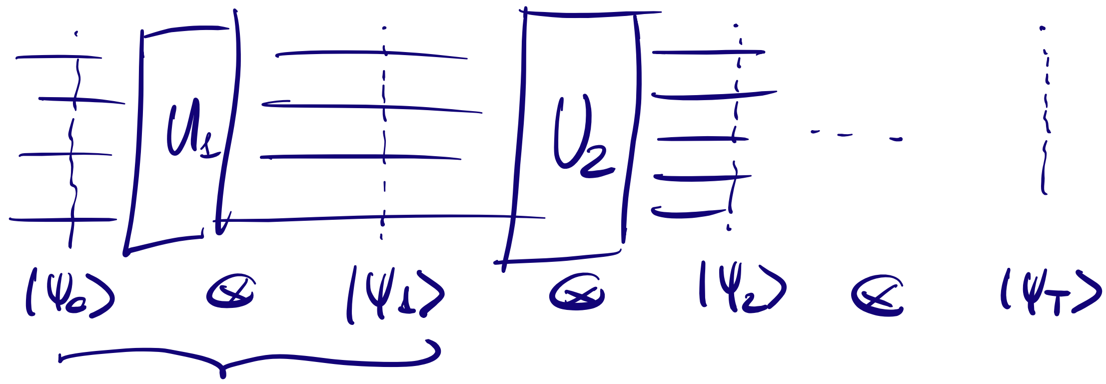
$$= \frac{1}{2} + \frac{1}{poly}$$

$\blacksquare$



$(x_1 \vee x_2 \vee x_3) \wedge \ldots$





CAT

$$\frac{1}{\sqrt{2}}\Big(|\underbrace{000\ldots0}_{n\text{-qubits}}\rangle + |1\ldots1\rangle\Big) = |\psi^+\rangle$$

$$- \qquad |\psi^-\rangle$$

$$|\psi_{hist}\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} \underbrace{|t\rangle}_{\text{clock}} \underbrace{|\psi_t\rangle}$$

- H_{in} = INITIAL STATE
- H_{prop} = PROPAGATION
- H_{clock} = CLOCK

LOCAL HAMILTONIAN

Given a T-gates quantum circuit we define the local Hamiltonian H_c as

$$H_c = -\sum_{i,j} \frac{J_{ij}}{2} \left(\underbrace{\sigma_{x_i} \sigma_{x_j}} + \sigma_{z_i} \sigma_{z_j} \right)$$

$(i \neq j \in poly(T))$

real coefficients

x_0

giulio.malavolta@hotmail.it