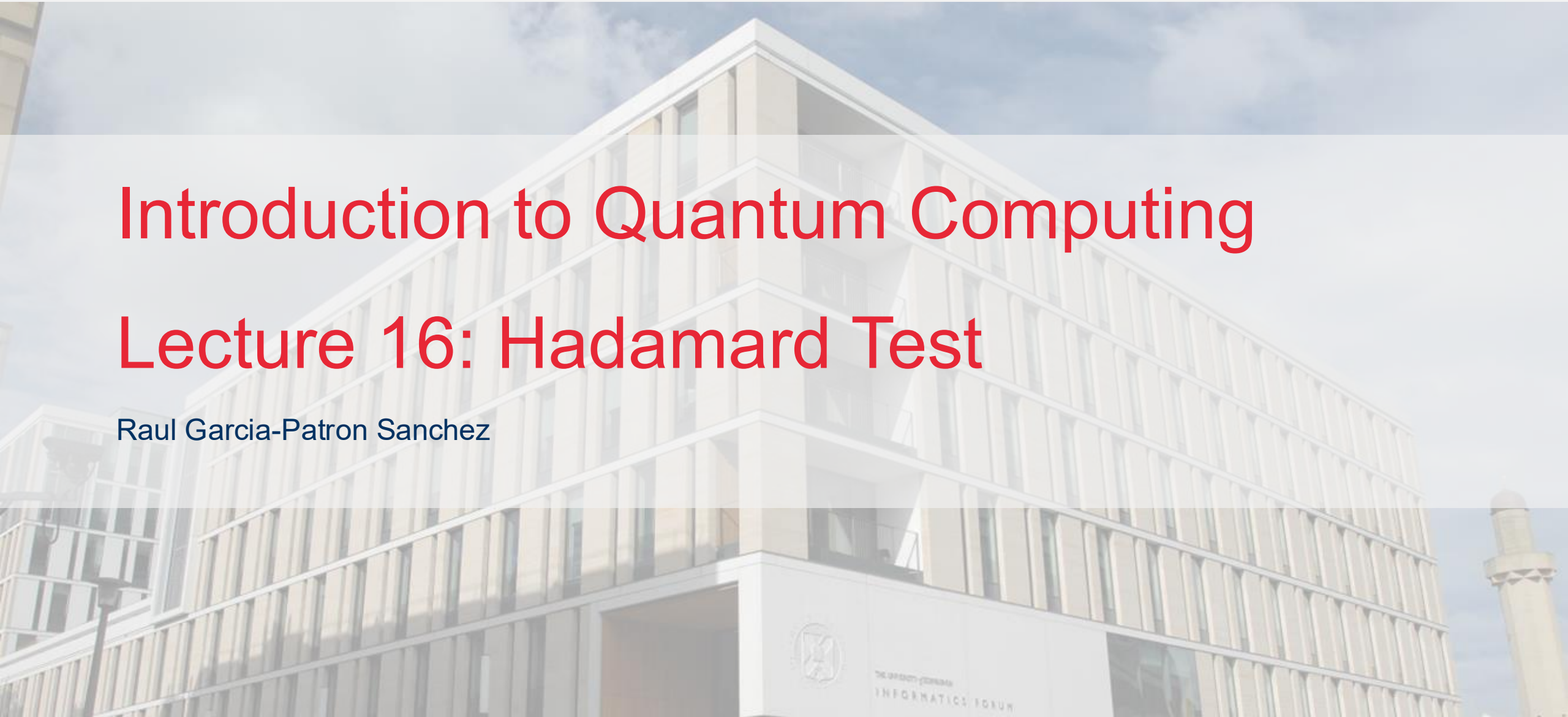


THE UNIVERSITY of EDINBURGH
informatics

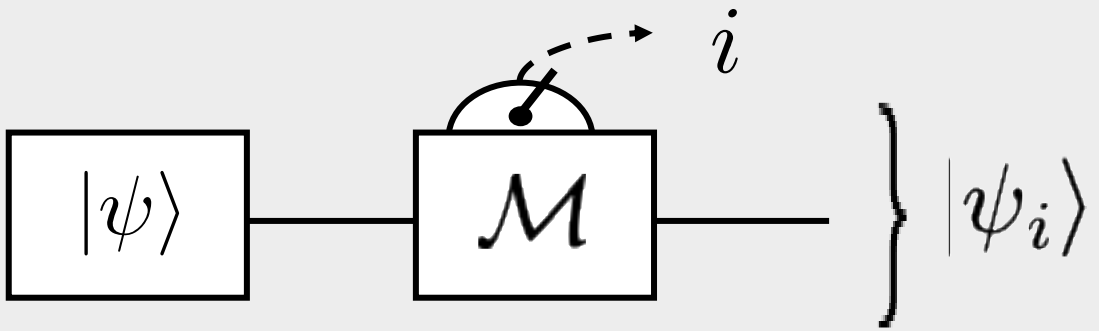
# Introduction to Quantum Computing

# Lecture 16: Hadamard Test

Raul Garcia-Patron Sanchez

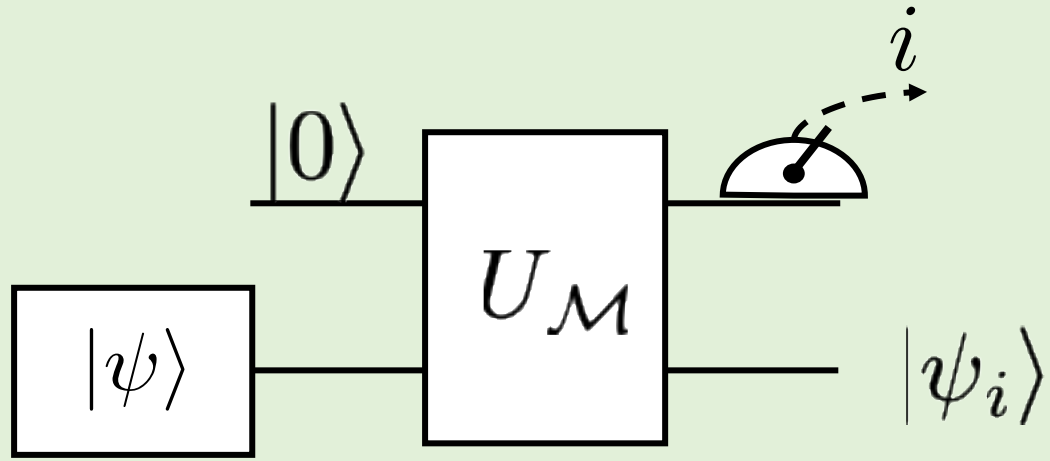
# From the definition to designing a circuit implementing it

$$\Pi_0 + \Pi_1 = I_d \qquad P(i) = ||\Pi_i|\psi\rangle||^2$$




$$\text{Update: } |\psi_i\rangle = \frac{\Pi_i|\psi\rangle}{||\Pi_i|\psi\rangle||}$$

We need to find the circuit $U_{\mathcal{M}}$



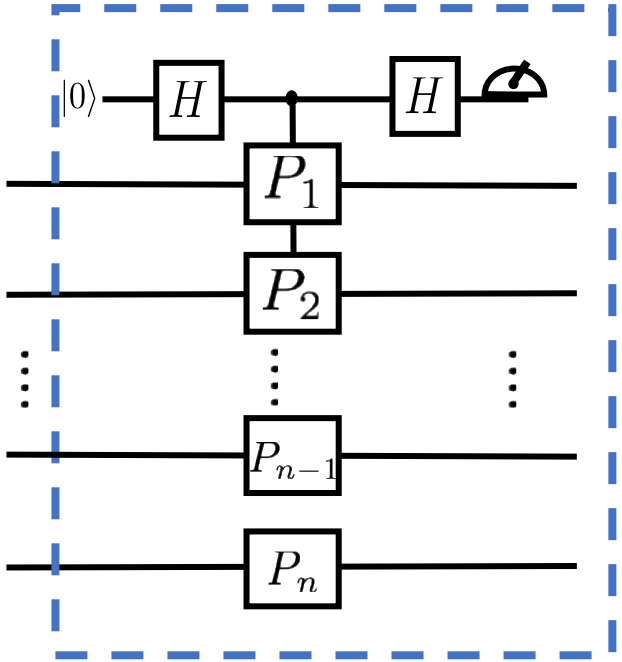
# General parity check

$$P = \sigma_1 \otimes \ldots \otimes \sigma_n = \Pi_0 - \Pi_1$$

$$\sigma_i \in \{I, X, Y, Z\}$$

$$P\Pi_x = (-1)^x \Pi_x$$

$$\Pi_0 + \Pi_1 = I_{2^n}$$

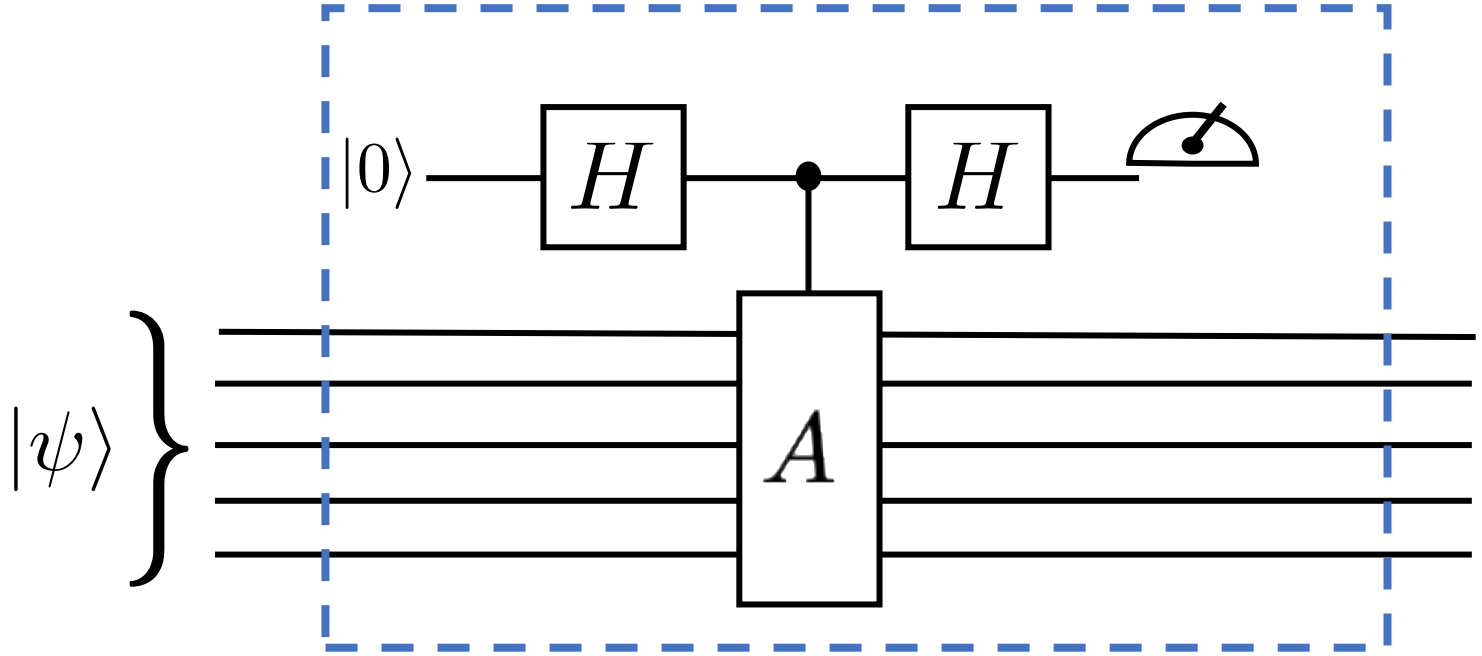



Example: $Z_1 \otimes Z_2$ parity

$$(Z_1 \otimes Z_2)|x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| = (-1)^{x_1 \oplus x_2}|x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2|$$

# Hadamard Test – binary outcome measurements

We want to ask the question: "Are you in subspace $\Pi_0$ or $\Pi_1$?




- Parity checks in quantum error correction
- SWAP test: overlap between quantum states, measurement of purity with two copies

# Hadamard Test – unitary is observable with ±1 eigenvalues

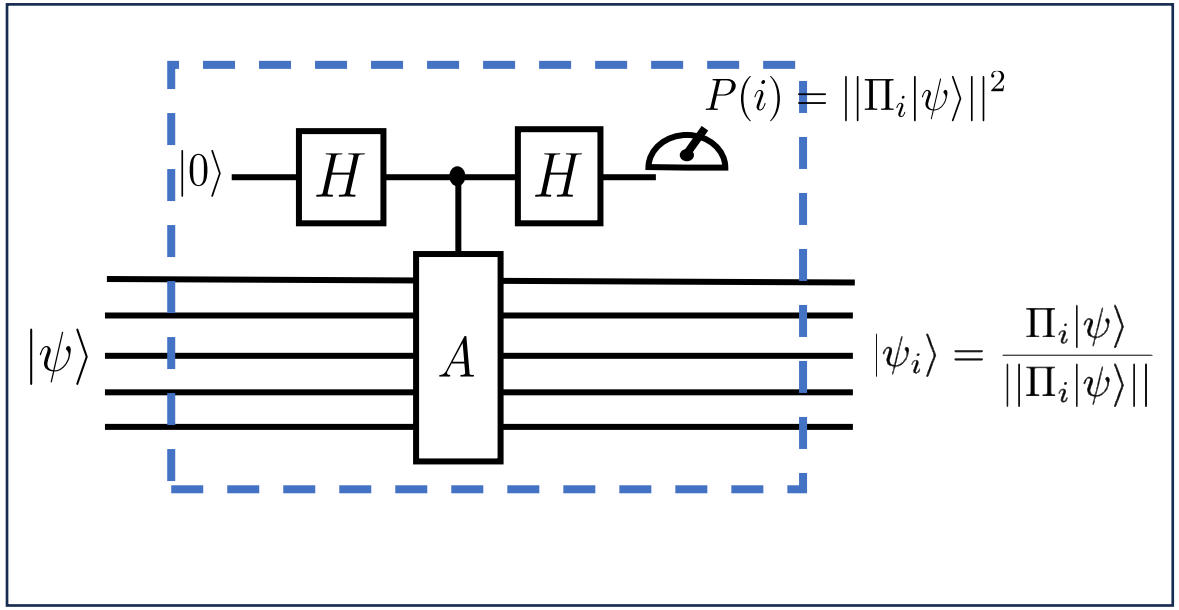
Observable ±1 eigenvalues

$$A = \Pi_0 - \Pi_1 \quad \text{(spectral decomposition)}$$

$$\Pi_0 + \Pi_1 = I_{2^n} \quad \text{(completeness)}$$

$$A\Pi_x = (-1)^x \Pi_x \quad \text{(eigenspaces)}$$

$$AA^\dagger = A^2 = I_{2^n} \quad \text{(unitarity)}$$




- $A\Pi_1 = (\Pi_0 - \Pi_1)\Pi_1 = \Pi_0\Pi_1 - \Pi_1^2 = -\Pi_1$

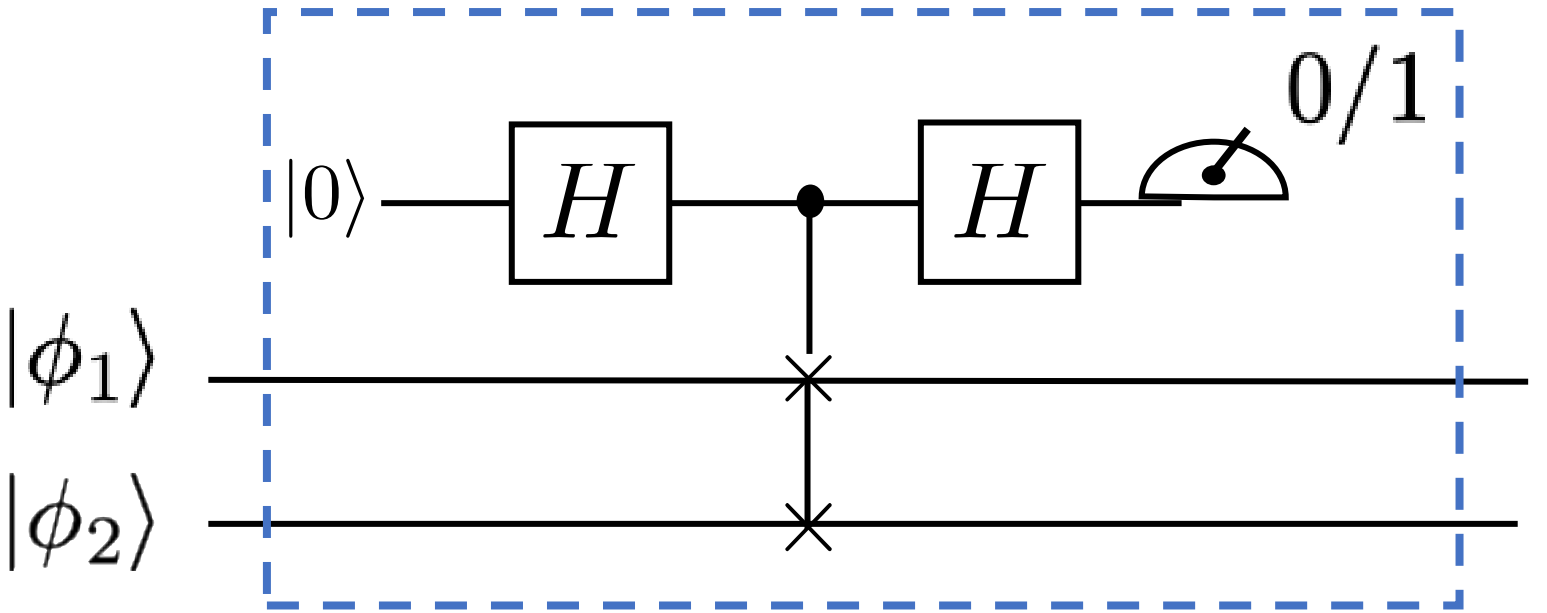
- $A$ is also a unitary matrix

$$AA^\dagger = (\Pi_0 - \Pi_1)(\Pi_0 - \Pi_1) = \Pi_0^2 - \Pi_0\Pi_1 - \Pi_1\Pi_0 + \Pi_1^2 = \Pi_0 + \Pi_1 = I_{2^n}$$



# SWAP Test

# Two-qubit SWAP Test




$$P(0) - P(1) = |\langle\phi_1|\phi_2\rangle|^2$$

We need to run multiple experiments to estimate $P(0) - P(1)$

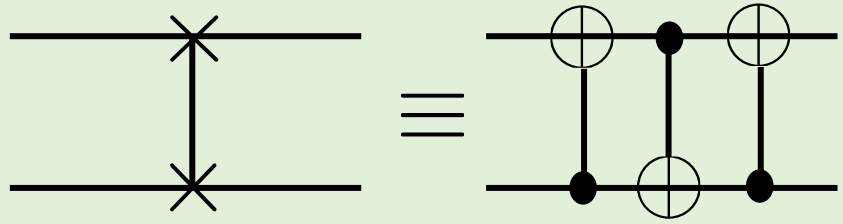
For precision $\epsilon$ we need $O(1/\epsilon^2)$ circuit runs

Hidden assumption: We are assuming we can prepare same copies every time (not specific to quantum)

# Two-qubit SWAP gate

SWAP (permutation) gate

$$U_{\mathrm{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



Do there exist $\{a, b, c, d\}$ s.t.

$$U_{\mathrm{SWAP}} = a|\Phi^+\rangle\langle\Phi^+| + b|\Phi^-\rangle\langle\Phi^-| + c|\Psi^+\rangle\langle\Psi^+| + d|\Psi^-\rangle\langle\Psi^-|?$$

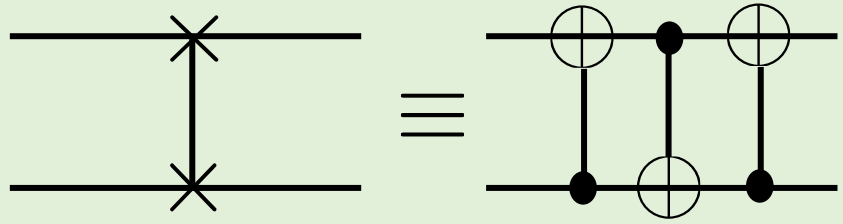
Bell basis $\quad |\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B) \qquad |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B)$

$$|\Phi^\pm\rangle\langle\Phi^\pm| = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & \pm 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \pm 1 & 0 & 0 & 1 \end{bmatrix} \qquad |\Psi^\pm\rangle\langle\Psi^\pm| = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & \pm 1 & 0 \\ 0 & \pm 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

# Two-qubit SWAP gate

SWAP (permutation) gate

$$U_{\mathrm{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



$$U_{\mathrm{SWAP}} = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| - |\Psi^-\rangle\langle\Psi^-|$$

$$\Pi_0 = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+|$$

$$\Pi_1 = |\Psi^-\rangle\langle\Psi^-|$$

$$U_{\mathrm{SWAP}} = \Pi_0 - \Pi_1 \qquad U_{\mathrm{SWAP}}\Pi_x = (-1)^x \Pi_x$$

Bell basis

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B \pm |1\rangle_A \otimes |1\rangle_B)$$

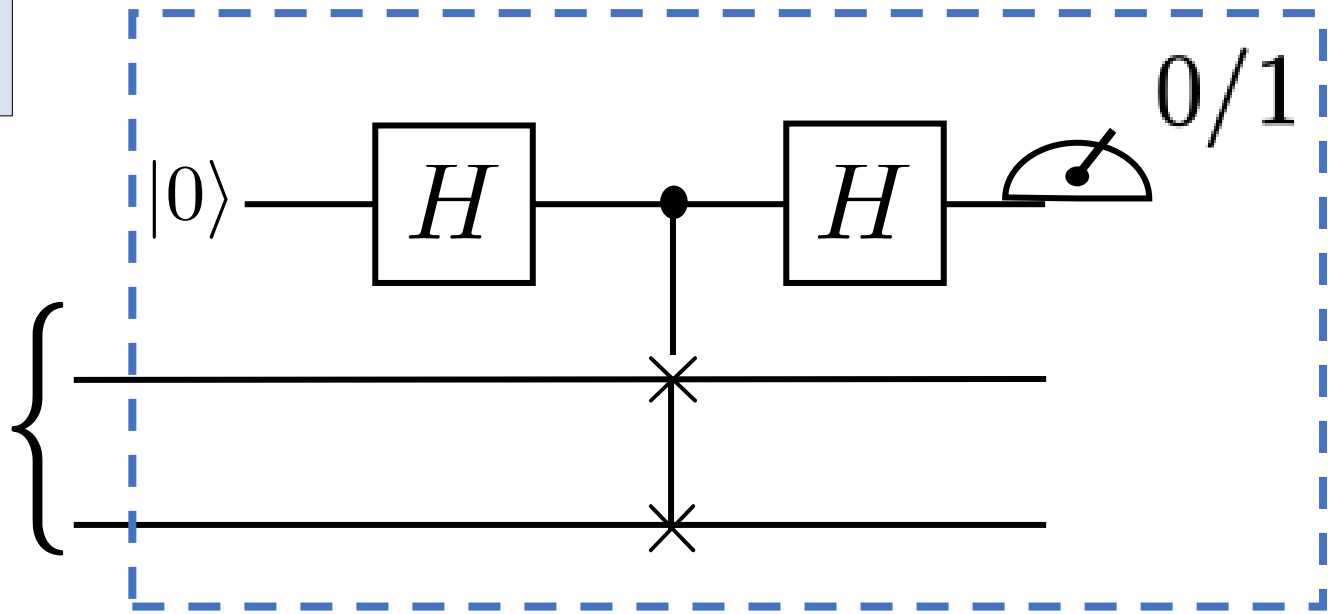
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B \pm |1\rangle_A \otimes |0\rangle_B)$$

$$|\Phi^\pm\rangle\langle\Phi^\pm| = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & \pm 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \pm 1 & 0 & 0 & 1 \end{bmatrix} \qquad |\Psi^\pm\rangle\langle\Psi^\pm| = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & \pm 1 & 0 \\ 0 & \pm 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

# Two-qubit SWAP Test

$$U_{\text{SWAP}}\Pi_x = (-1)^x \Pi_x$$
$$\Pi_0 + \Pi_1 = I_4$$

$$|\psi\rangle = \Pi_0|\psi\rangle + \Pi_1|\psi\rangle$$




$$|0\rangle \otimes |\psi\rangle \xrightarrow{H\otimes I\otimes I} (|0\rangle + |1\rangle)/\sqrt{2} \otimes (\Pi_0|\psi\rangle + \Pi_1|\psi\rangle)$$

$$\xrightarrow{\text{c-SWAP}} 1/\sqrt{2}\,(|0\rangle \otimes (\Pi_0|\psi\rangle + \Pi_1|\psi\rangle) + |1\rangle \otimes U_{\text{SWAP}}(\Pi_0|\psi\rangle + \Pi_1|\psi\rangle))$$

$$= 1/\sqrt{2}\,(|0\rangle \otimes (\Pi_0|\psi\rangle + \Pi_1|\psi\rangle) + |1\rangle \otimes (\Pi_0|\psi\rangle - \Pi_1|\psi\rangle))$$

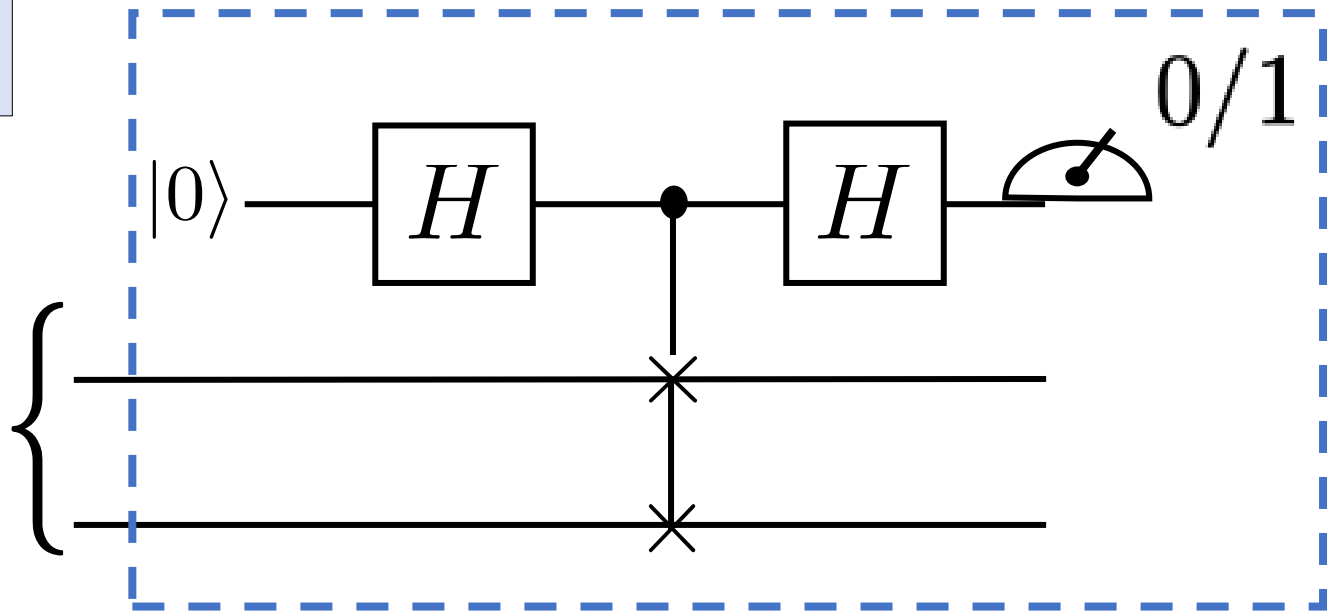
$$= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \Pi_0|\psi\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \Pi_1|\psi\rangle = |+\rangle \otimes \Pi_0|\psi\rangle + |-\rangle \otimes \Pi_1|\psi\rangle$$

$$\xrightarrow{H\otimes I\otimes I} |0\rangle \otimes \Pi_0|\psi\rangle + |1\rangle \otimes \Pi_1|\psi\rangle$$

# Two-qubit SWAP Test

$$U_{\mathrm{SWAP}} = \Pi_0 - \Pi_1$$
$$\Pi_0 + \Pi_1 = I_4$$

$$|\psi\rangle = \Pi_0|\psi\rangle + \Pi_1|\psi\rangle$$

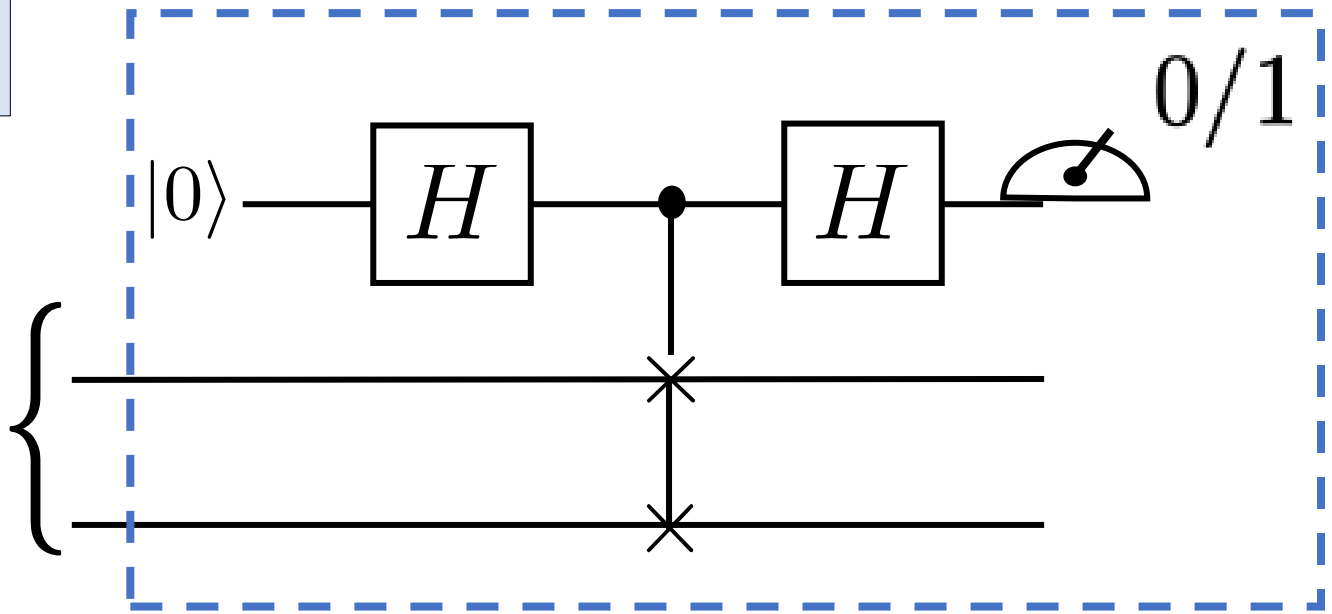



$$|0\rangle \otimes |\psi\rangle \rightarrow |0\rangle \otimes \Pi_0|\psi\rangle + |1\rangle \otimes \Pi_1|\psi\rangle$$

# Two-qubit SWAP Test

$$U_{\text{SWAP}} = \Pi_0 - \Pi_1$$
$$\Pi_0 + \Pi_1 = I_4$$

$$|\psi\rangle = \Pi_0|\psi\rangle + \Pi_1|\psi\rangle$$




$$|0\rangle \otimes |\psi\rangle \rightarrow |0\rangle \otimes \Pi_0|\psi\rangle + |1\rangle \otimes \Pi_1|\psi\rangle = |\tilde{\phi}\rangle$$

$$\tilde{\Pi}_y = |y\rangle\langle y| \otimes I_4$$
$$\tilde{\Pi}_0 + \tilde{\Pi}_1 = I_8$$

$$\tilde{\Pi}_0 = |0\rangle\langle 0| \otimes I$$

$$\tilde{\Pi}_0|\tilde{\phi}\rangle = (|0\rangle\langle 0| \otimes I)(|0\rangle \otimes \Pi_0|\psi\rangle + |1\rangle \otimes \Pi_1|\psi\rangle) = |0\rangle \otimes \Pi_0|\psi\rangle$$

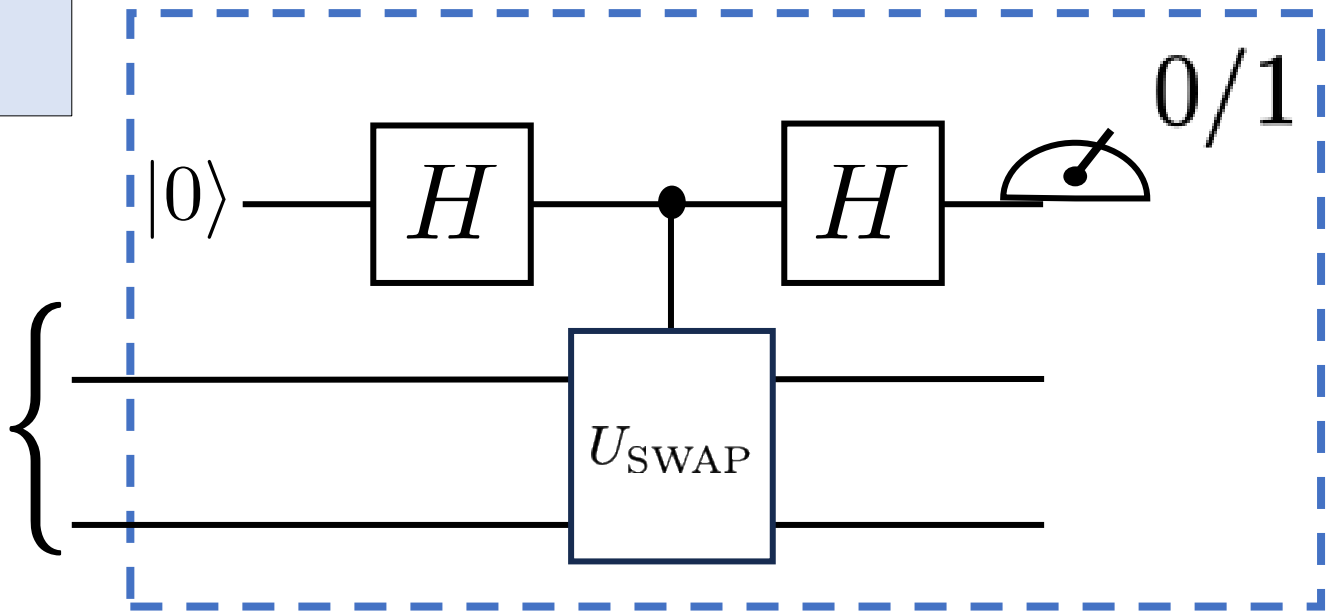
$$P(0) = ||\tilde{\Pi}_0|\tilde{\phi}\rangle||^2 = (\langle\tilde{\phi}|\tilde{\Pi}_0)(\tilde{\Pi}_0|\tilde{\phi}\rangle) = (\langle 0| \otimes \langle\psi|\Pi_0)(|0\rangle \otimes \Pi_0|\psi\rangle)$$

$$= \langle 0|0\rangle\langle\psi|\Pi_0^2|\psi\rangle = \langle 0|0\rangle\langle\psi|\Pi_0|\psi\rangle = ||\Pi_0|\psi\rangle||^2$$

# SWAP Test – Bias of probabilities

$$U_{\text{SWAP}} = \Pi_0 - \Pi_1$$
$$\Pi_0 + \Pi_1 = I_4$$

$$|\psi\rangle = \Pi_0|\psi\rangle + \Pi_1|\psi\rangle$$




$$P(0) = ||\tilde{\Pi}_0|\tilde{\phi}\rangle||^2 = ||\Pi_0|\psi\rangle||^2 \qquad P(1) = ||\tilde{\Pi}_1|\tilde{\phi}\rangle||^2 = ||\Pi_1|\psi\rangle||^2$$

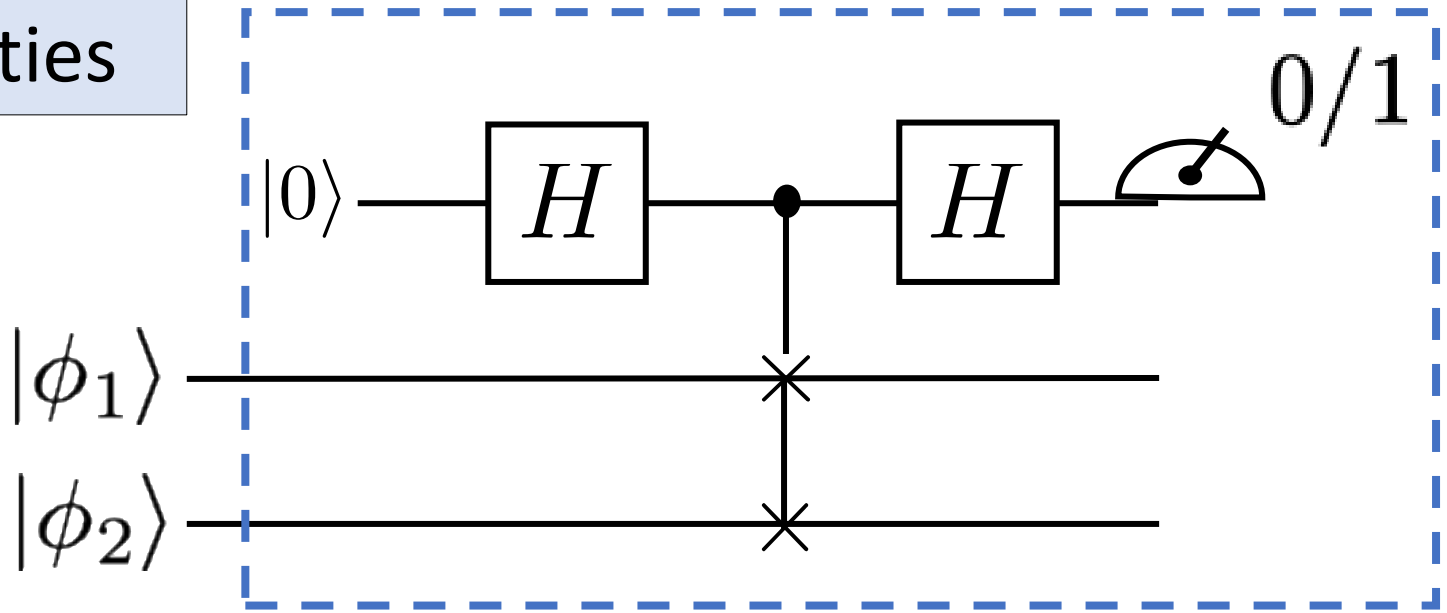
$$\begin{aligned} P(0) - P(1) &= ||\Pi_0|\psi\rangle||^2 - ||\Pi_1|\psi\rangle||^2 \\ &= \langle\psi|\Pi_0^\dagger\Pi_0|\psi\rangle - \langle\psi|\Pi_1^\dagger\Pi_1|\psi\rangle \\ &= \langle\psi|\Pi_0|\psi\rangle - \langle\psi|\Pi_1|\psi\rangle = \langle\psi|\Pi_0 - \Pi_1|\psi\rangle \\ &= \langle\psi|U_{\text{SWAP}}|\psi\rangle \end{aligned}$$

Expectation value of $U_{\text{SWAP}}$ on state $|\psi\rangle$

# SWAP Test – Bias of probabilities

$$U_{\text{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U_{\text{SWAP}} = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| - |\Psi^-\rangle\langle\Psi^-|$$




$$P(0) - P(1) = \langle\psi|U_{\text{SWAP}}|\psi\rangle$$

$$= \langle\phi_1| \otimes \langle\phi_2|U_{\text{SWAP}}|\phi_1\rangle \otimes |\phi_2\rangle$$

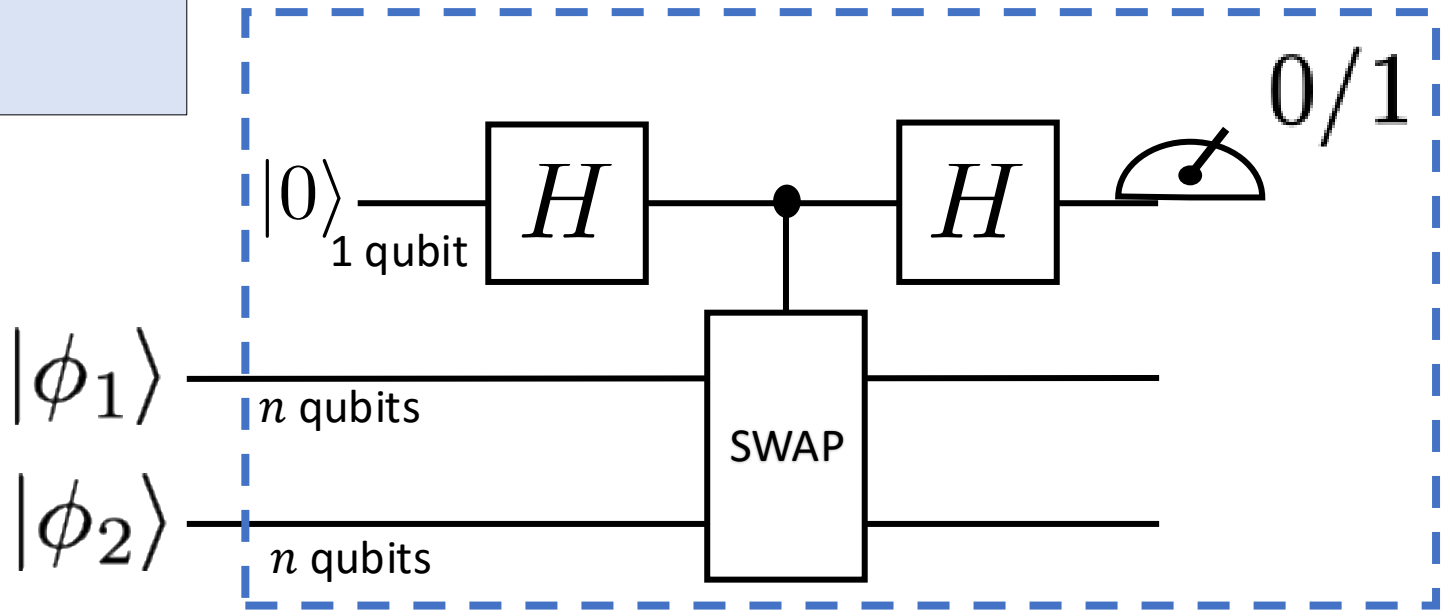
$$= (\langle\phi_1| \otimes \langle\phi_2|)(|\phi_2\rangle \otimes |\phi_1\rangle)$$

$$= \langle\phi_1|\phi_2\rangle\langle\phi_2|\phi_1\rangle$$

$$= \langle\phi_1|\phi_2\rangle\langle\phi_1|\phi_2\rangle^* = |\langle\phi_1|\phi_2\rangle|^2$$

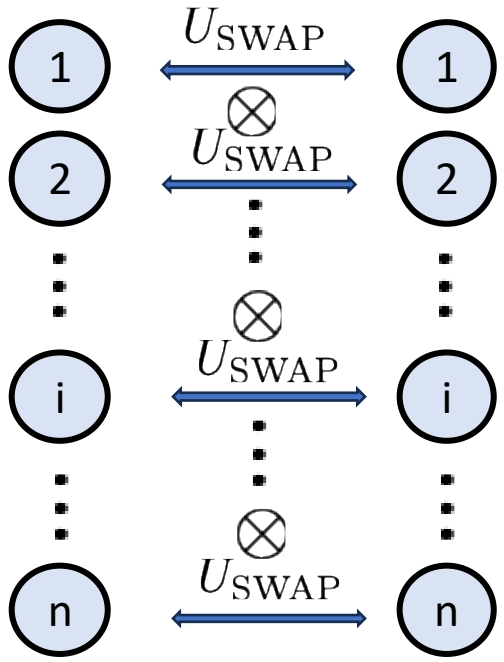
# SWAP Test – Multiple qubits

Single qubit registers
The Hadamard test needs to control the exchange of the two qubits done with a controlled-SWAP gate.




Multiple-qubit registers
The Hadamard test needs to control
the exchange of the two $n$-qubit registers.

The exchange is done:
1. Pair together the i-th qubits of each register
2. Apply controlled-SWAP gate on each pair (controlled by the upper qubit)





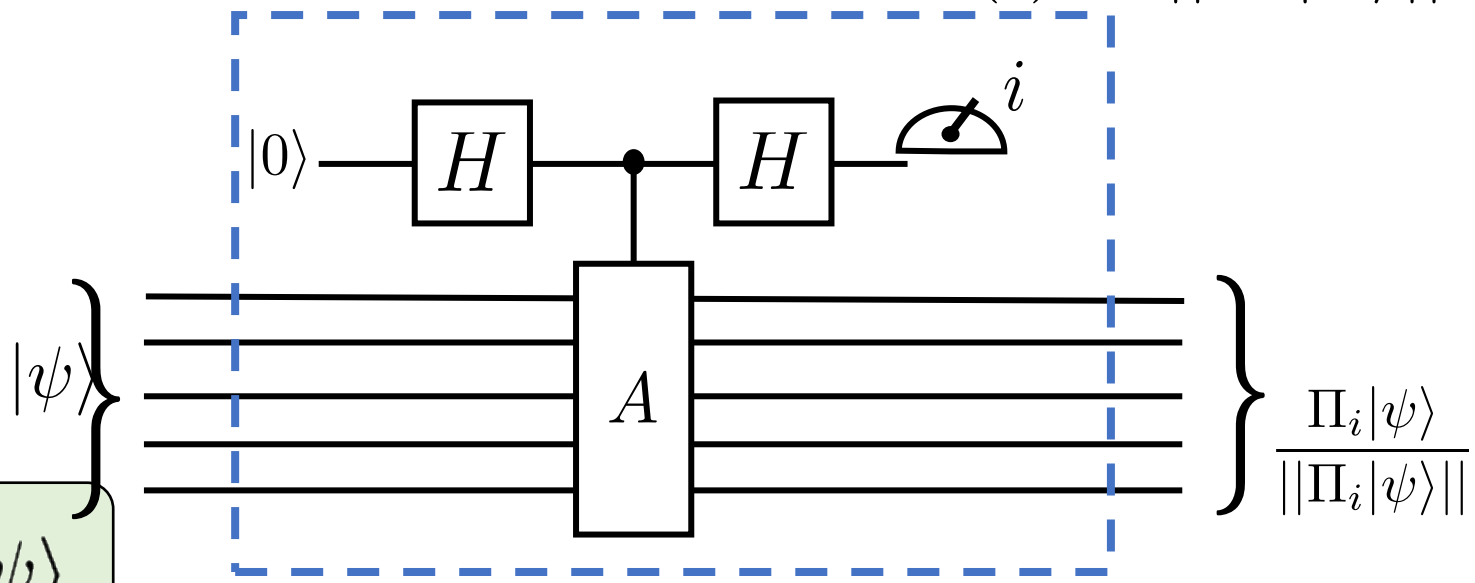
# General Hadamard Test

# General $\pm 1$ eigenvalues measurement

$$\mathcal{H} = \mathcal{H}_0 \oplus \mathcal{H}_1$$

$$\Pi_0 + \Pi_1 = I_{2^n}$$
$$A = \Pi_0 - \Pi_1$$
$$A\Pi_x = (-1)^x \Pi_x$$
$$AA^\dagger = A^2 = I$$

$$P(i) = ||\Pi_i|\psi\rangle||^2$$




$$|\tilde{\phi}\rangle = |0\rangle \otimes \Pi_0|\psi\rangle + |1\rangle \otimes \Pi_1|\psi\rangle$$

$$\tilde{\Pi}_0 = |0\rangle\langle 0| \otimes I$$

$$P(0) = ||\tilde{\Pi}_0|\tilde{\phi}\rangle||^2 = ||\Pi_0|\psi\rangle||^2$$

$$\frac{\tilde{\Pi}_0|\tilde{\phi}\rangle}{||\tilde{\Pi}_0|\tilde{\phi}\rangle||} = \frac{|0\rangle \otimes \Pi_0|\psi\rangle}{||\Pi_0|\psi\rangle||} = |0\rangle \otimes \frac{\Pi_0|\psi\rangle}{||\Pi_0|\psi\rangle||}$$

$$P(0) - P(1) = \langle\psi|A|\psi\rangle$$

Expectation value of $A$ on state $|\psi\rangle$

THE UNIVERSITY of EDINBURGH
informatics



# Subroutine for quantum simulation

# Quantum simulation in one slide

Time-dynamics of a quantum system: $e^{-i\hat{H}t}|\psi\rangle$

The Hamiltonian encodes the "physics": $\hat{H} = \hat{H}^\dagger = \sum_w h_w$

$h_w$ are "Hamiltonian terms": $h_w = h_w^\dagger$

encoding interactions between parts of the system

Always defined over some topology: lattice, graph, etc

$e^{-i\hat{H}t}$ is a unitary operator

$$\hat{H} = \sum_j E_j |v_j\rangle\langle v_j|$$

$$e^{-i\hat{H}t} = \sum_j e^{-iE_j t} |v_j\rangle\langle v_j|$$

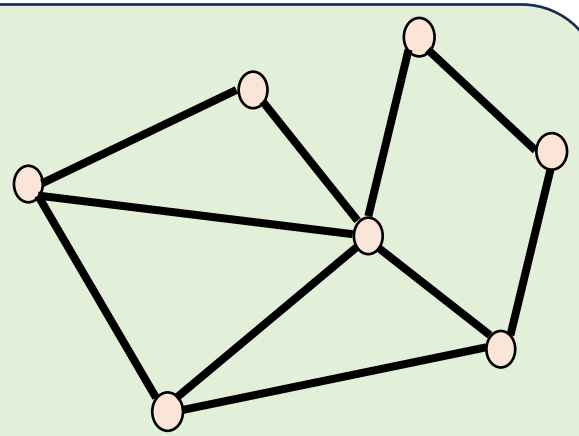
Knowing the eigenbasis $|v_j\rangle$ is a very hard problem in the general case, even for quantum computers.

Nonetheless, quantum computers can implement $e^{-i\hat{H}t}$ efficiently for "realistic" Hamiltonians (e.g. local).

## Ising Model

Each vertex is a qubit (spin)

$$H_I = \sum_{(i,j)\in E(G)} \gamma_{i,j} Z_i \otimes Z_j$$



Commuting Hamiltonian:

If all $h_w$ commute among themselves

$$e^{-i\hat{H}t} = \prod_w e^{-ih_w t}$$

# Quantum simulation in one slide

Time-dynamics of a quantum system: $e^{-i\hat{H}t}|\psi\rangle$

The Hamiltonian encodes the "physics": $\hat{H} = \hat{H}^\dagger = \sum_w h_w$

$h_i$ are "Hamltonian terms": $h_w = h_w^\dagger$

encoding interactions between parts of the system

Always defined over some topology: lattice, graph, etc

$e^{-i\hat{H}t}$ is a unitary operator

$$\hat{H} = \sum_j E_j |v_j\rangle\langle v_j|$$

$$e^{-i\hat{H}t} = \sum_j e^{-iE_j t} |v_j\rangle\langle v_j|$$

Non-commuting: Trotterization and other tricks

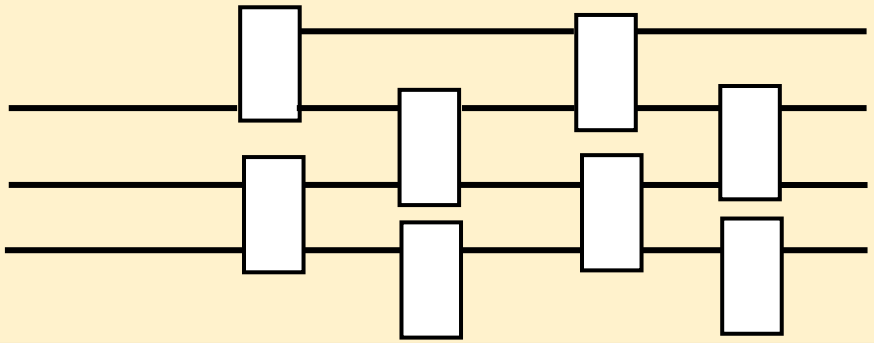
$$e^{-i\hat{H}\Delta t} \approx \prod_{w'} e^{-ih_{w'}\Delta t}$$

Approximation for small time steps

Commuting Hamiltonian:

If all $h_w$ commute among themselves

$$e^{-i\hat{H}t} = \prod_w e^{-ih_w t}$$



Any set of $h_w$ without overlapping qubits can be implemented in parallel.

Solve a coloring problem to optimize depth.

# Pauli-string rotation

Pauli rotations $e^{-i\theta P}$ are useful subroutines in quantum simulation and beyond.

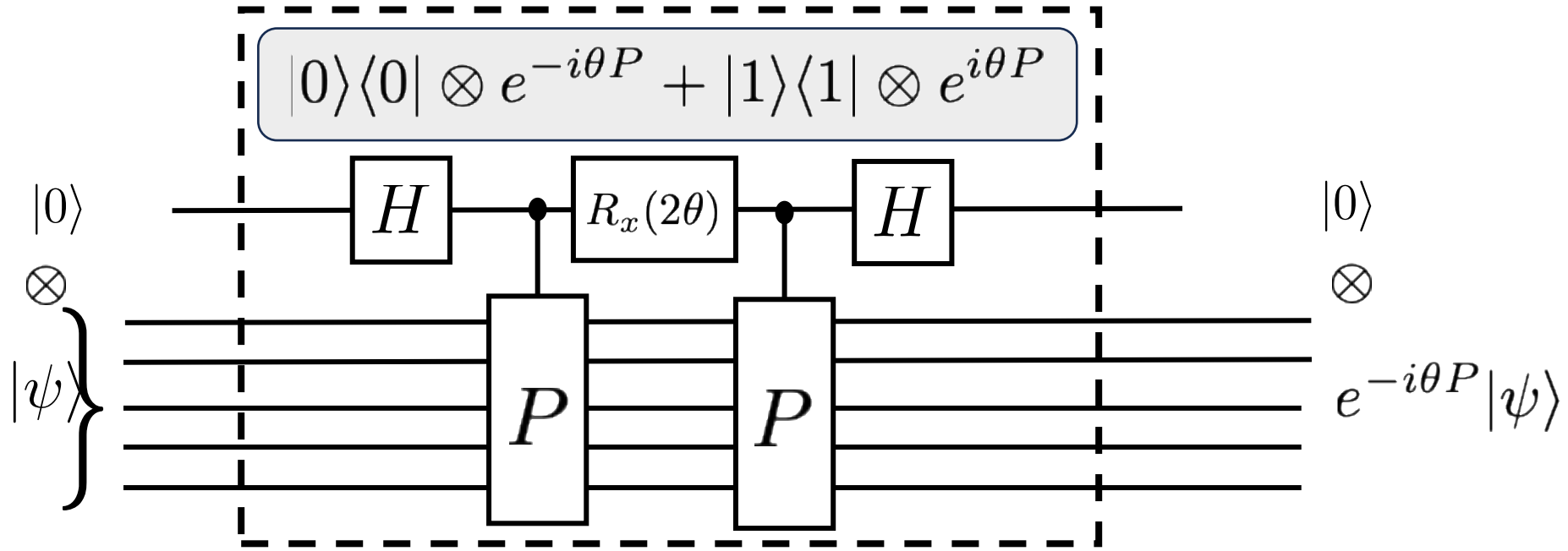
Single-qubit rotations

$$R_x(2\theta) = e^{-i\theta X} \quad R_y(2\theta) = e^{-i\theta Y} \quad R_z(2\theta) = e^{-i\theta Z}$$

$$e^{-i\hat{H}\Delta t} \approx \prod_{w'} e^{-i\theta_{w'} P_{w'}}$$

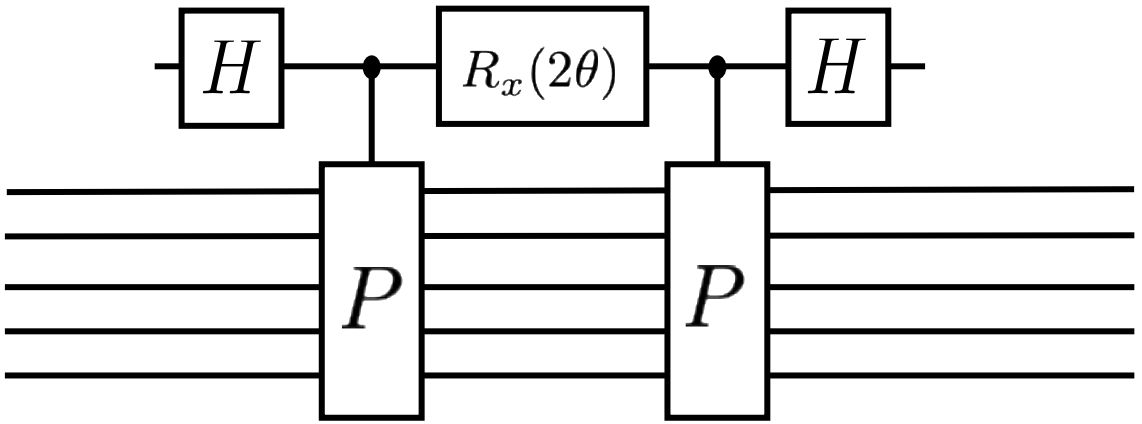
$$e^{-i\theta P} = \cos\theta I_{2^n} - i \sin\theta P$$
$$e^{-i\theta P} = e^{-i\theta}\Pi_0 + e^{i\theta}\Pi_1$$

$$\Pi_0 + \Pi_1 = I_{2^n}$$
$$P = \Pi_0 - \Pi_1$$

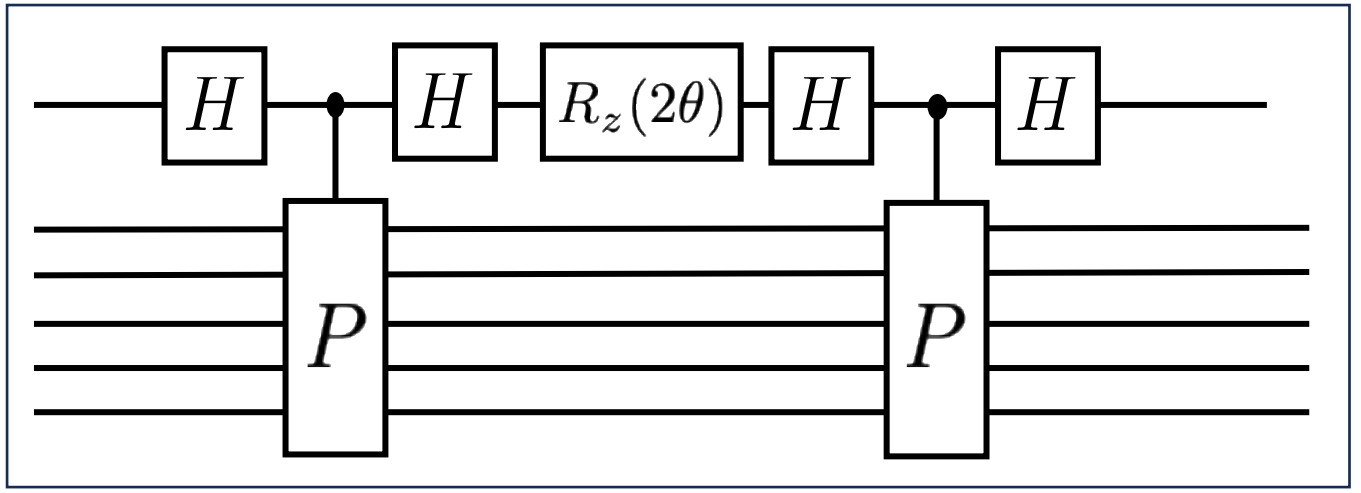


# Pauli-string rotation – Proof

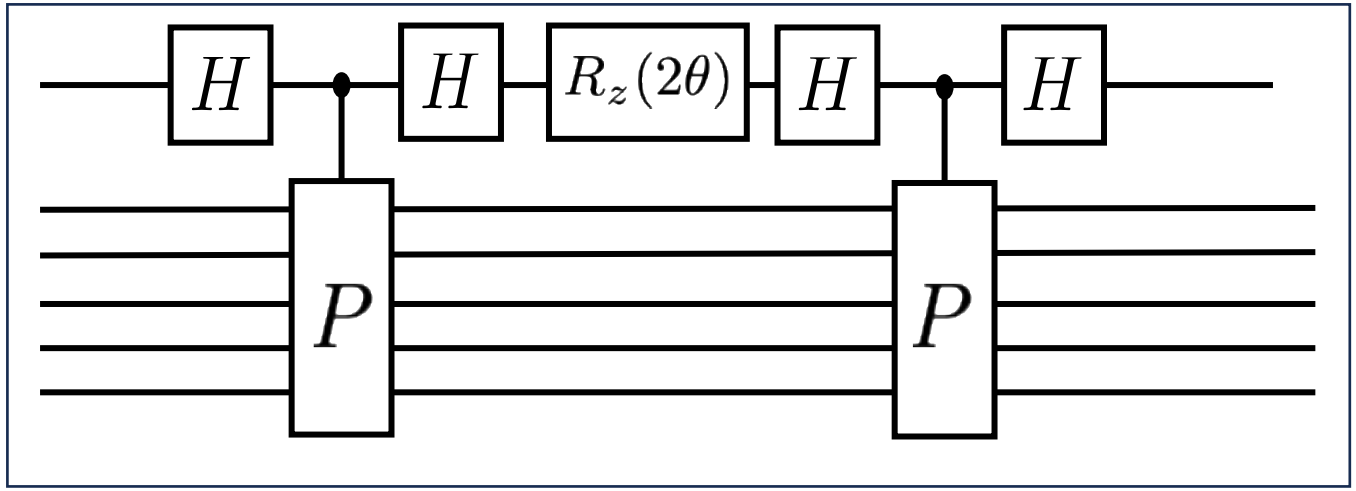
$$|0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{i\theta P}$$




$$\begin{aligned} R_x(2\theta) = e^{-i\theta X} &= \cos\theta I - i\sin\theta X \\ &= \cos\theta H^2 - i\sin\theta HZH \\ &= H(\cos\theta I - i\sin\theta Z)H \\ &= He^{-i\theta Z}H = HR_z(2\theta)H \end{aligned}$$



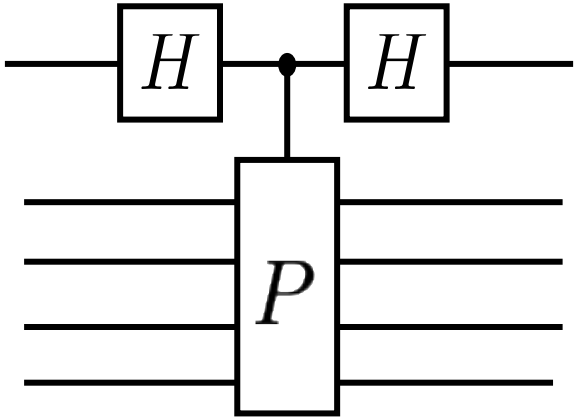
# Pauli-string rotation – Proof




$$|0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{i\theta P}$$

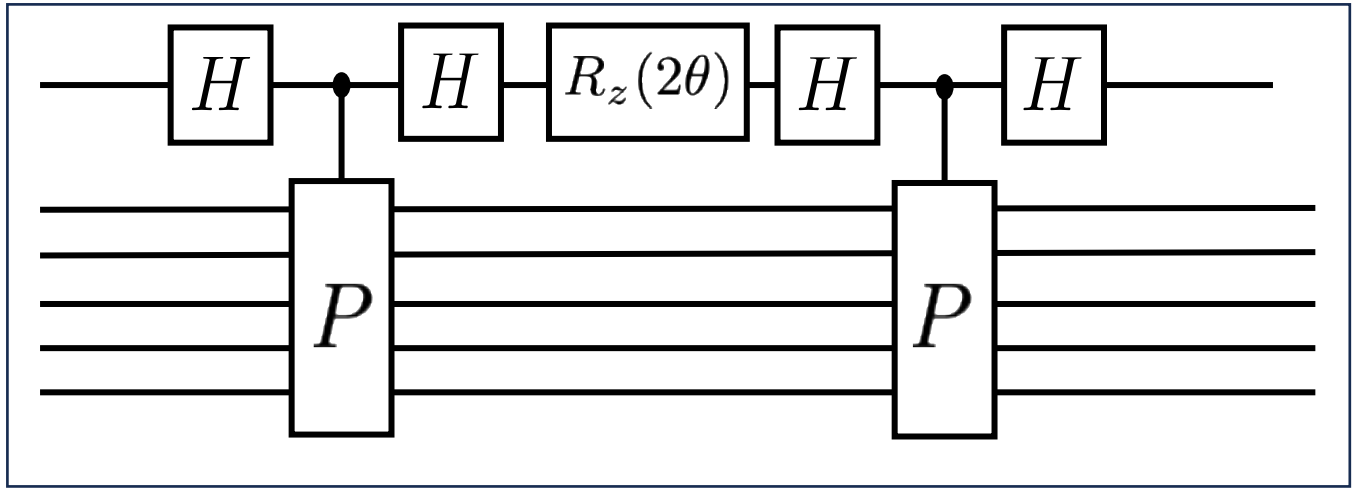
$$|\pm\rangle\langle\pm| = \frac{I \pm X}{2}$$

$$I \otimes \Pi_0 + X \otimes \Pi_1$$




$$\begin{aligned}
&(H \otimes I_{2^n})(|0\rangle\langle 0| \otimes I_{2^n} + |1\rangle\langle 1| \otimes P)(H \otimes I_{2^n}) \\
&\quad = |+\rangle\langle +| \otimes I_{2^n} + |-\rangle\langle -| \otimes P \\
&\quad = \frac{I+X}{2} \otimes (\Pi_0 + \Pi_1) + \frac{I-X}{2} \otimes (\Pi_0 - \Pi_1) \\
&\quad = \frac{I+X}{2} \otimes \Pi_0 + \frac{I+X}{2} \otimes \Pi_1 + \frac{I-X}{2} \otimes \Pi_0 - \frac{I-X}{2} \otimes \Pi_1 \\
&\quad = \left(\frac{I+X}{2} + \frac{I-X}{2}\right) \otimes \Pi_0 + \left(\frac{I+X}{2} - \frac{I-X}{2}\right) \otimes \Pi_1 \\
&\quad = I \otimes \Pi_0 + X \otimes \Pi_1
\end{aligned}$$

# Pauli-string rotation – Proof

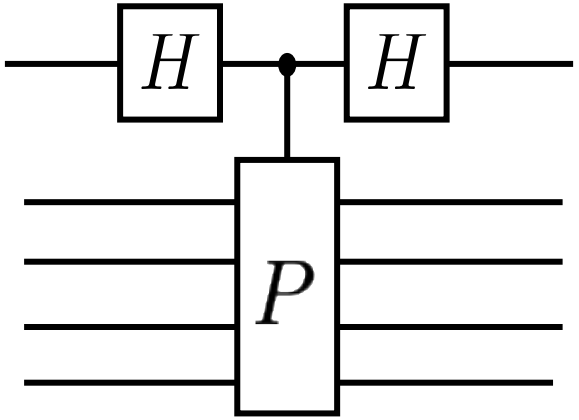



$$|0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{i\theta P}$$

$$e^{-i\theta P} = \cos\theta I_{2^n} - i\sin\theta P$$
$$e^{-i\theta P} = e^{-i\theta}\Pi_0 + e^{i\theta}\Pi_1$$

$$e^{-i\theta Z} = e^{-i\theta}|0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|$$

$$I \otimes \Pi_0 + X \otimes \Pi_1$$




$$|0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{i\theta P}$$

$$\Pi_0\Pi_1 = 0$$

$$(I \otimes \Pi_0 + X \otimes \Pi_1)(e^{-i\theta}|0\rangle\langle 0| \otimes I_{2^n} + e^{i\theta}|1\rangle\langle 1| \otimes I_{2^n})(I \otimes \Pi_0 + X \otimes \Pi_1)$$
$$= e^{-i\theta}|0\rangle\langle 0| \otimes \Pi_0 + e^{i\theta}|1\rangle\langle 1| \otimes \Pi_0 + e^{-i\theta}|1\rangle\langle 1| \otimes \Pi_1 + e^{+i\theta}|0\rangle\langle 0| \otimes \Pi_1$$
$$= |0\rangle\langle 0| \otimes (e^{-i\theta}\Pi_0 + e^{i\theta}\Pi_1) + |1\rangle\langle 1| \otimes (e^{i\theta}\Pi_0 + e^{-i\theta}\Pi_1)$$
$$= |0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{i\theta P}$$

# References

**Reading references**

1. Quantum simulation: NC 4.7
2. Pauli rotation gadget: NC 4.7.3

NC ≣ Michael Nielsen and Isaac Chuang, Quantum Computation and Quantum Information
Cambridge University Press (2010)