# Toward Entailment Checking: Explore Eigenmarking Search

*Tatpong Katanyukul*

Computer Engineering, Khon Kaen University, Thailand

*inCACCT 2025, 17-18 April, Chandigarh University, India*

# Big Picture

- Entailment is central to logic reasoning.
- Model checking goes through all combinations of logical symbols for validation of entailment: $O(2^n)$.
- Our work is to propose improved quantum search targeting a more efficient model checking.

# Logic Entailment: Model Checking

$KB \vDash \alpha$ if and only if, in **every truth scenario** in which KB is true, $\alpha$ is true.

Model checking = truth evaluation given truth values of all symbols.

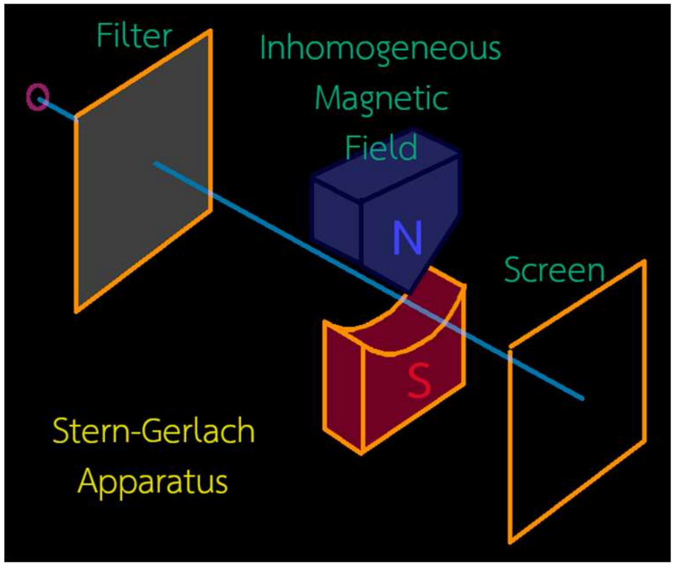
KB:
- Durians are spiky.
- Durians are yummy.

$\alpha_1$: Montong durian is spiky.
$\alpha_2$: Montong durian is not spiky.
$\alpha_3$: There is life on Mars.
$\alpha_4$: There is no life on Mars.

| Spiky Montong | Life on Mars | KB | $\alpha_1$ | $\alpha_2$ | $\alpha_3$ | $\alpha_4$ | |
|---|---|---|---|---|---|---|---|
| F | F | F | F | T | F | T | |
| F | T | F | F | T | T | F | $O(2^n)$ |
| T | F | **T** | T | F | F | T | |
| T | T | **T** | T | F | T | F | |

$KB \vDash \alpha_1$ $KB \nvDash \alpha_2$ $KB \nvDash \alpha_3$ $KB \nvDash \alpha_4$

# Quantum Computing and Quantum Mechanical Properties




- Quantum computing utilizes quantum mechanical properties for computing.

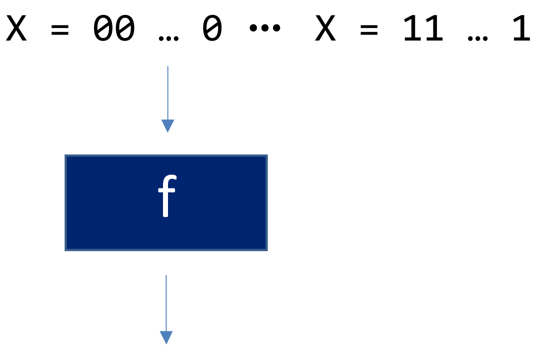
- The quantum effect is more prominent at a small scale.
  - Linear evolution
  - Measurement
  - **Superposition**, Entanglement, Tunneling.

# Grover Search

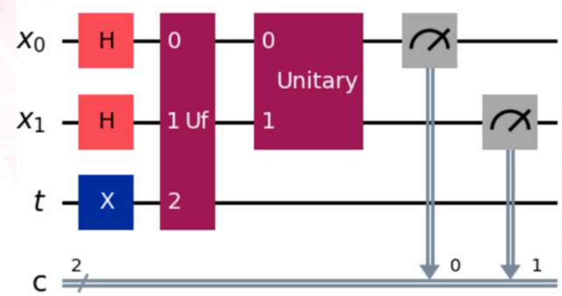
- Problem: Given unknown $f(\cdot)$, find an answer $x' \in \{0,1\}^n$ : $f(x') = 1$
- Promise: one and only one answer $x'$: $f(x') = 1$ and $f(x) = 0$ for all $x \neq x'$.

- Classical approach: trial-and-error
  - Average computation cost ~ $O\left(\frac{N}{2}\right) = O(2^{n-1})$
  - All possible candidates $N = 2^n$.

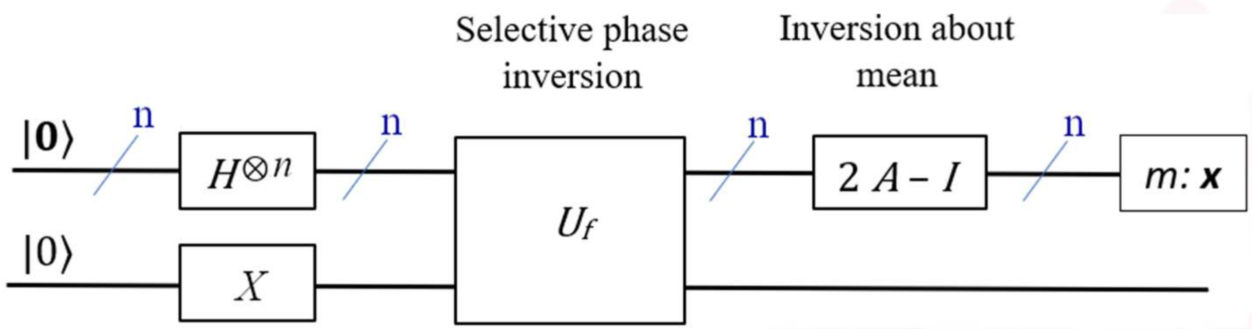
*Classical*




Grover search



# Grover Algorithm: Key Ideas




- Evolve the probability amplitude of the answer eigenstate such that when measured, the answer is more likely to be observed.
- ~ Parallelism using superposition!

- Implementation:
  - Selective phase inversion: mark the answer.
  - Inversion about the mean: amplify the answer's probability amplitude.
    - This relies on that the answer is minority!

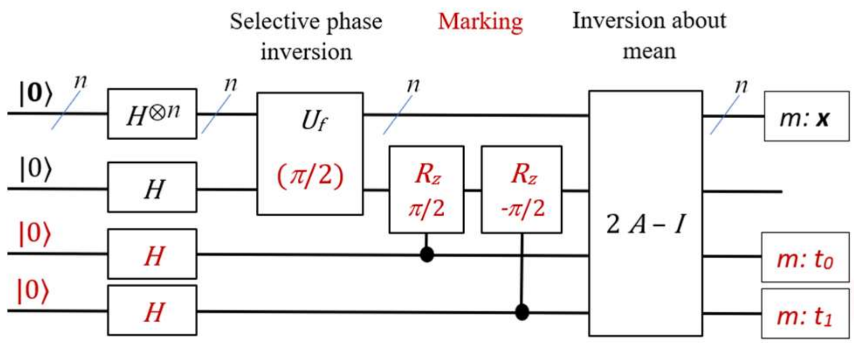
# Challenges and Our Approach

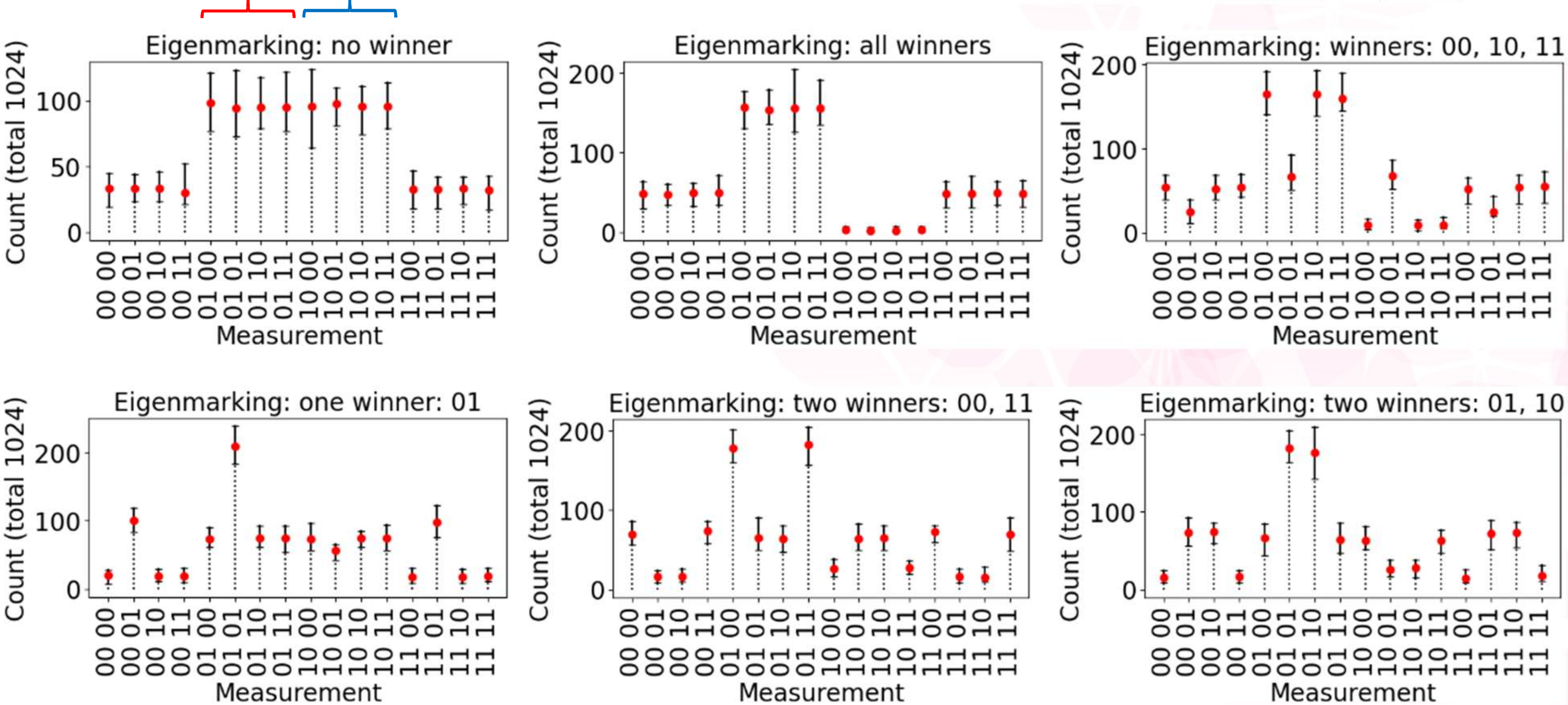
| Spiky Montong | Life on Mars | KB | $\alpha_1$ | $\alpha_2$ | $\alpha_3$ | $\alpha_4$ | |
|---|---|---|---|---|---|---|---|
| F | F | F | F | T | F | T | |
| F | T | F | F | T | T | F | |
| T | F | **T** | T | F | F | T | |
| T | T | **T** | T | F | T | F | |

When KB = T, No F 2 Fs 1 F 1 F

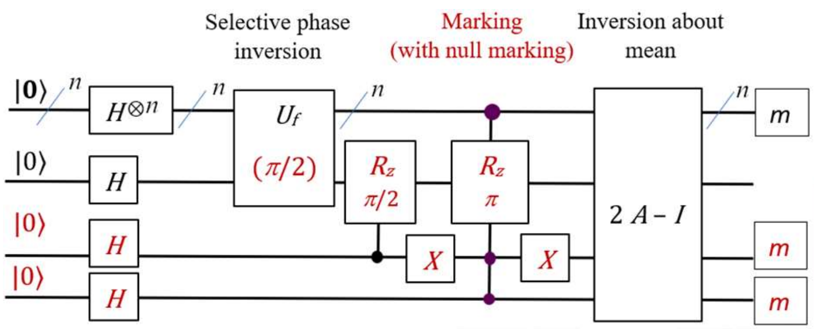
- Original Grover search addresses 1-F case.
- Our approach:
  - Additional qubits
    - Maintain minority condition for Grover amplification
    - Facilitate easy identification of no-winner case

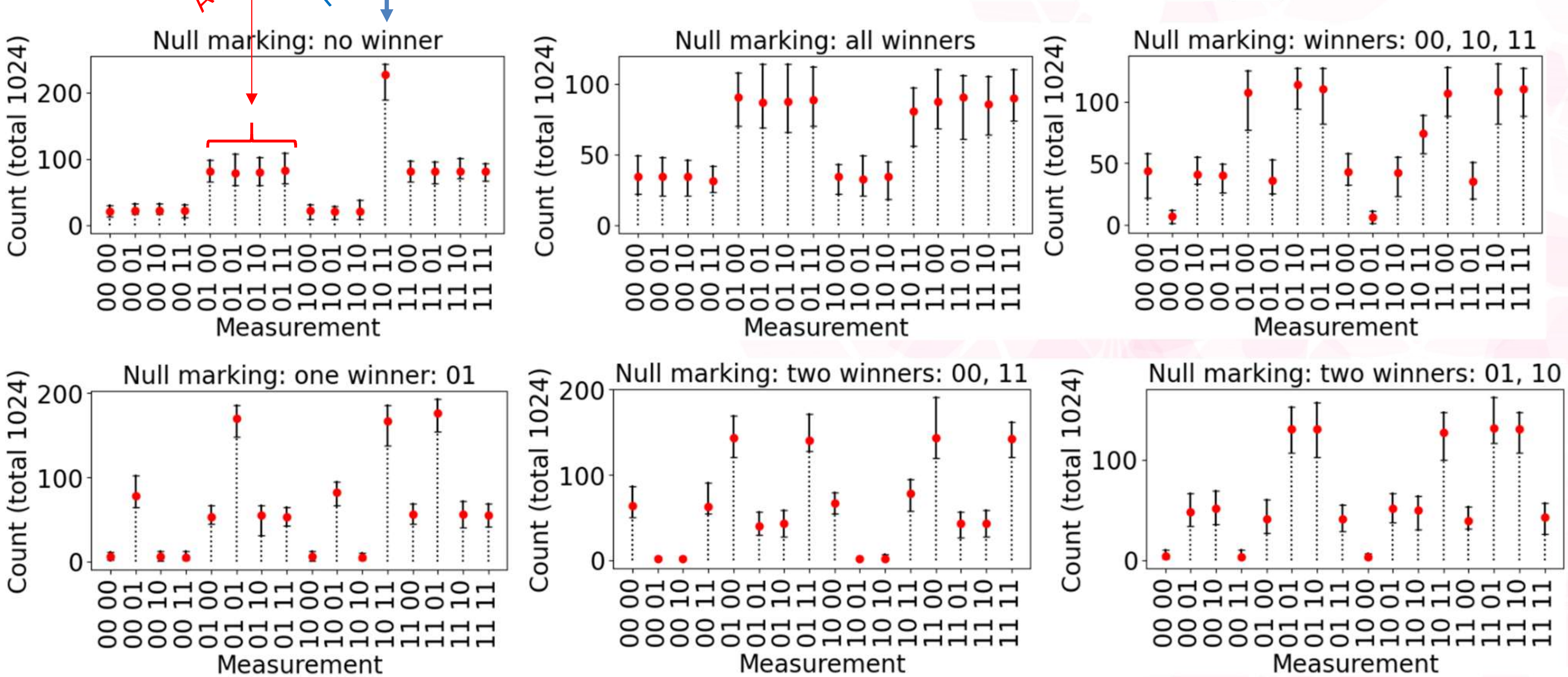
# Eigenmarking



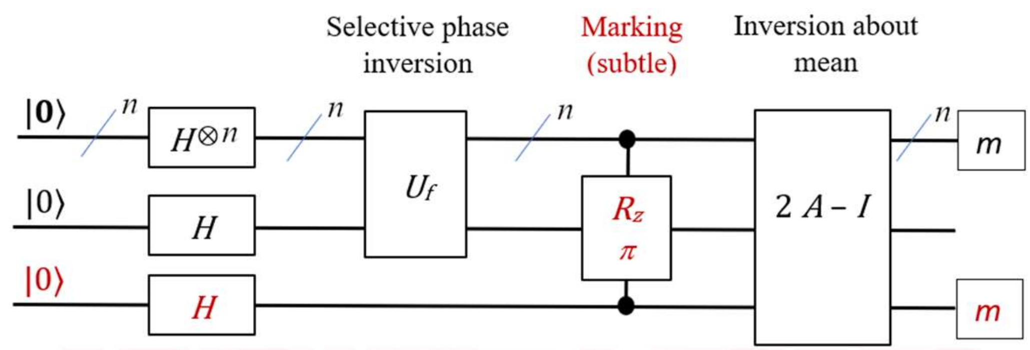



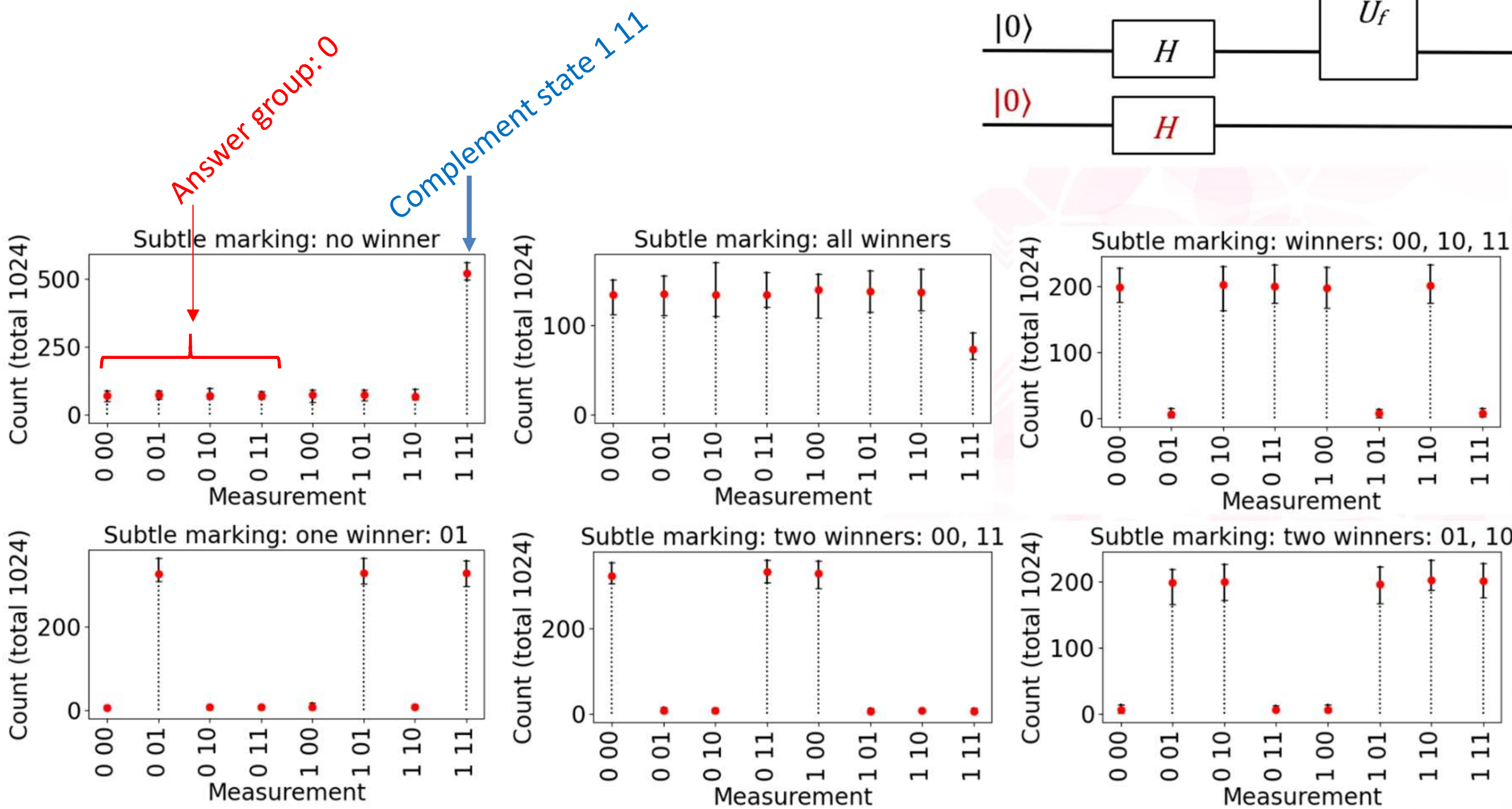
# Null Eigenmarking



# Subtle Eigenmarking



# Conclusion & Discussion

- The ideas work! (at least for a two-qubit case, in a simulator.)
- Quality of outcomes
  - Eigenmarking
    - Better at suppressing chances of dummy states: best global winning margin.
    - Quite well on distinguishability: best relative scores.
  - Subtle marking
    - Quite well on every aspect:
      - best local winning margin,
      - best absolute distinguishability.

- Architectural aspect: subtle marking requires less modification, but needs multiple-qubit controls.
- Limitations: *Scalability?* (more qubits) *Reliability?* (theoretical analysis) *Robustness?* (real QC)

KKU มหาวิทยาลัยขอนแก่น
KHON KAEN UNIVERSITY


image: https://commons.wikimedia.org/wiki/File:%E0%B8%A7%E0%B8%B1%E0%B8%94%E0%B8%9E%E0%B8%A3%E0%B8%B0%E0%B8%98%E0%B8%B2%E0%B8%95%E0%B8%B8%E0%B8%82%E0%B8%B2%E0%B8%A1%E0%B9%81%E0%B8%81%E0%B9%88%E0%B8%99.jpg

# Logic Entailment

$KB \vDash \alpha$ if and only if, in every model (truth scenario) in which KB is true, $\alpha$ is true.

KB:

- Durians are spiky.
- Durians are yummy.

$\alpha_1$: Montong durian is spiky. $KB \vDash \alpha_1$

$\alpha_2$: Montong durian is not spiky. $KB \nvDash \alpha_2$

$\alpha_3$: There is life on Mars. $KB \nvDash \alpha_3$

$\alpha_4$: There is no life on Mars. $KB \nvDash \alpha_4$

## Note

- $KB \vDash \alpha$ means $\alpha$ agrees with what KB said.
- $KB \nvDash \alpha$ means $\alpha$ is not what is said by KB.

# Quantum State and Superposition

- Superposition: a quantum state is a combination of eigenstates:

$$|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle + c_3|\psi_3\rangle + \cdots + c_N|\psi_N\rangle$$

or vector representation

$$|\psi\rangle = [c_1 \quad c_2 \quad c_3 \quad \cdots \quad c_N\ ]^T$$

## Quantum Computing

In short, we can control quantum state evolution by unitary operator $U$ through manipulation of the system energy,

$$|\psi'\rangle = U\,|\psi\rangle.$$

And we can measure the state and collapse it to one of the eigenstates with probability,

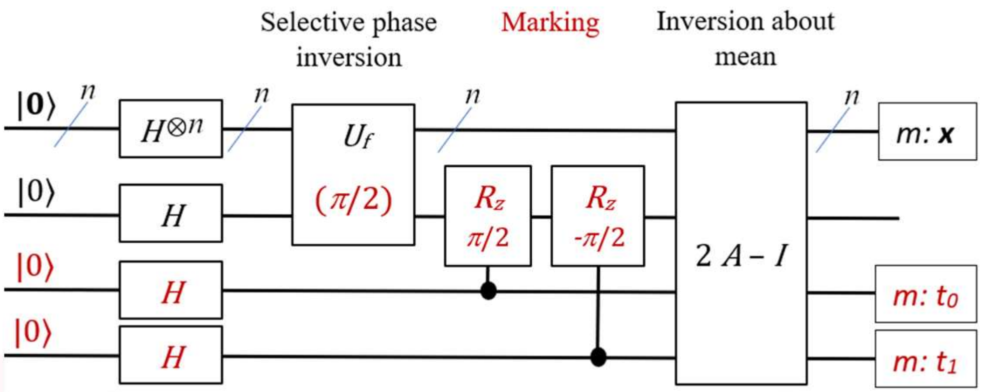
$$\Pr[\,|\psi'\rangle = |\psi_i\rangle\,] = |c_i|^2.$$

# Shortcomings of Original Grover in Entailment Context

- Designed for a lone match search.
  - Mitigation:
    - Probabilistic control over # applications.
    - Time-out to handle a no-winner case.

- Entailment checking is likely to have multiple matches or no match at all
  - No match $\Rightarrow$ no violation: the entailment is validated.

# Eigenmarking

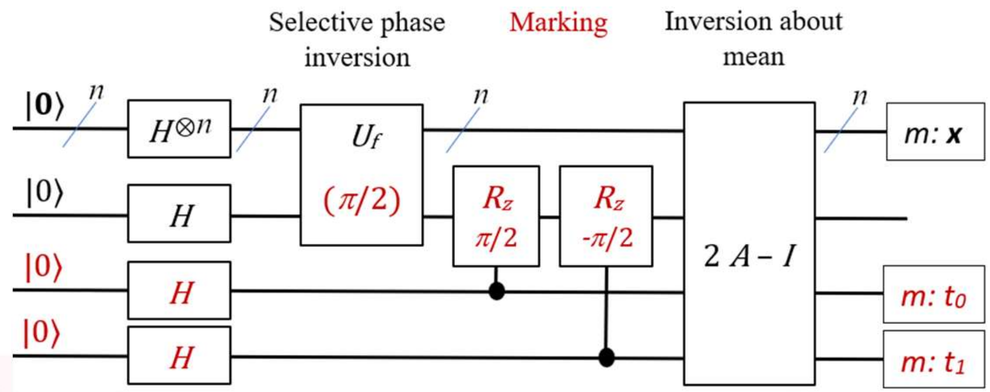



- Tag 00, $\phi(\boldsymbol{x}') = \frac{\pi}{2} + 0 + 0 = \frac{\pi}{2}$ and $\phi(\boldsymbol{x}) = 0 + 0 + 0 = 0$.
- Tag 01, $\phi(\boldsymbol{x}') = \frac{\pi}{2} + 0 + \frac{\pi}{2} = \pi$ and $\phi(\boldsymbol{x}) = 0 + 0 + \frac{\pi}{2} = \frac{\pi}{2}$.
- Tag 10, $\phi(\boldsymbol{x}') = \frac{\pi}{2} - \frac{\pi}{2} + 0 = 0$ and $\phi(\boldsymbol{x}) = 0 - \frac{\pi}{2} + 0 = -\frac{\pi}{2}$.
- Tag 11, $\phi(\boldsymbol{x}') = \frac{\pi}{2} = \frac{\pi}{2}$ and $\phi(\boldsymbol{x}) = 0 = 0$.

- With winners, tag 01 has the answer(s): $\phi(\boldsymbol{x}') = \pi$ while others having $-\frac{\pi}{2}, 0, \frac{\pi}{2}$.
  - But all-winner and no-winner may look the same.

# Eigenmarking: Cases

| Tag | $\phi(x')$ | $\phi(x)$ | |
|---|---|---|---|
| 00 | $\pi/2$ | $0$ | |
| 01 | $\pi$ | $\pi/2$ | |
| 10 | $0$ | $-\pi/2$ | |
| 11 | $\pi/2$ | $0$ | |



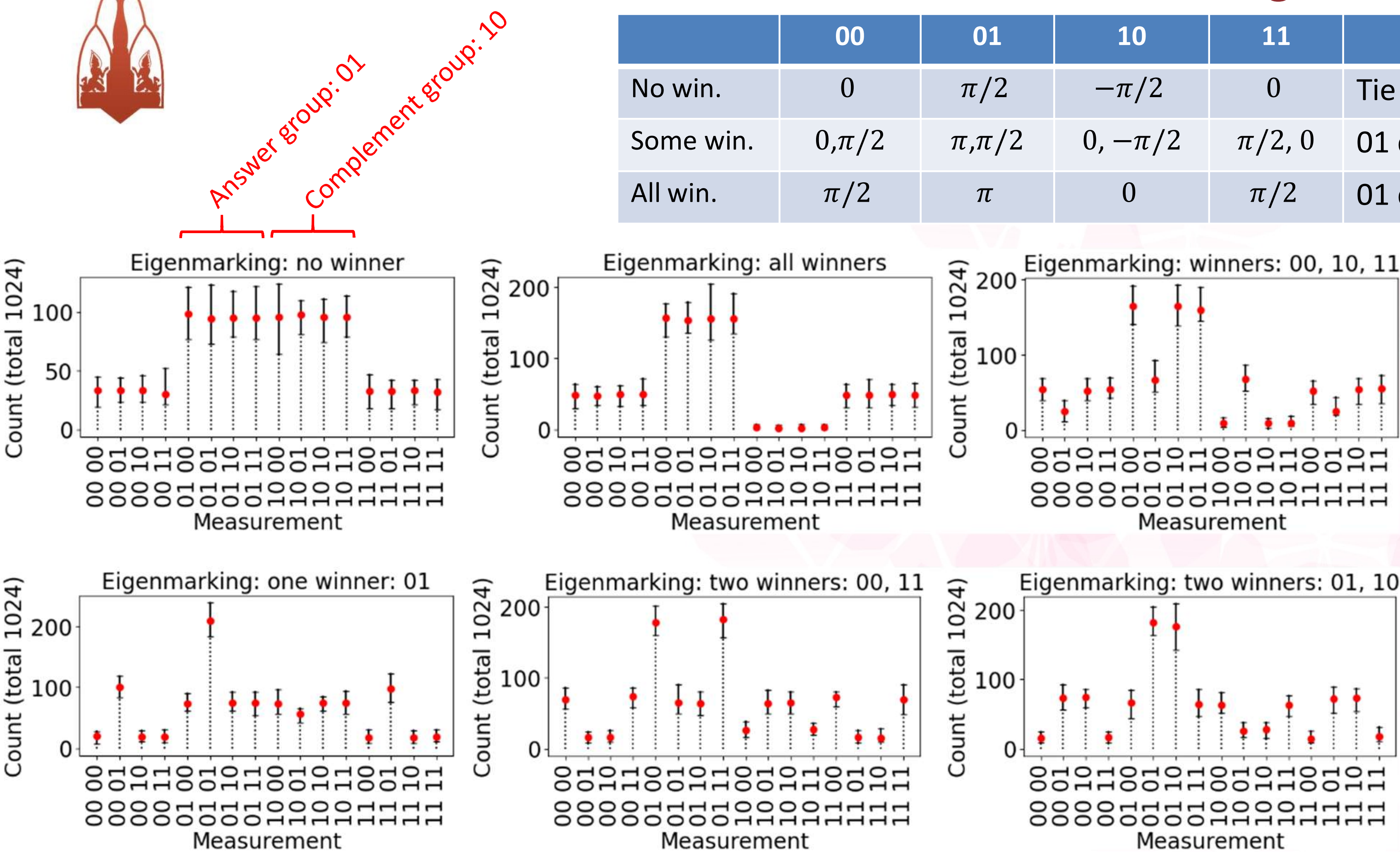

| | 00 | 01 | 10 | 11 | |
|---|---|---|---|---|---|
| No win. | $0$ | $\pi/2$ | $-\pi/2$ | $0$ | |
| Some win. | $0,\pi/2$ | $\pi,\pi/2$ | $0, -\pi/2$ | $\pi/2, 0$ | |
| All win. | $\pi/2$ | $\pi$ | $0$ | $\pi/2$ | |

Our target

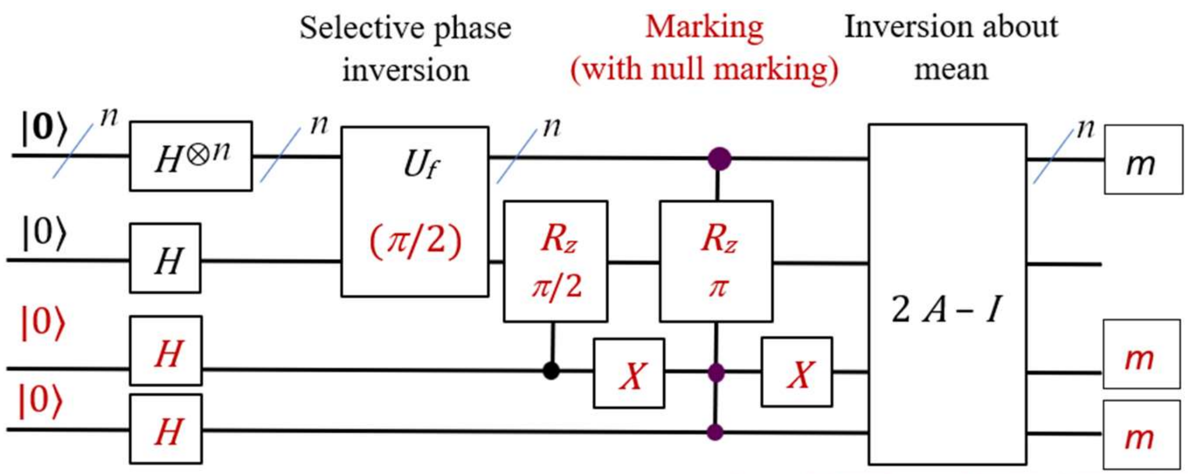
Complementary, esp., in no win.

# Results: Eigenmarking

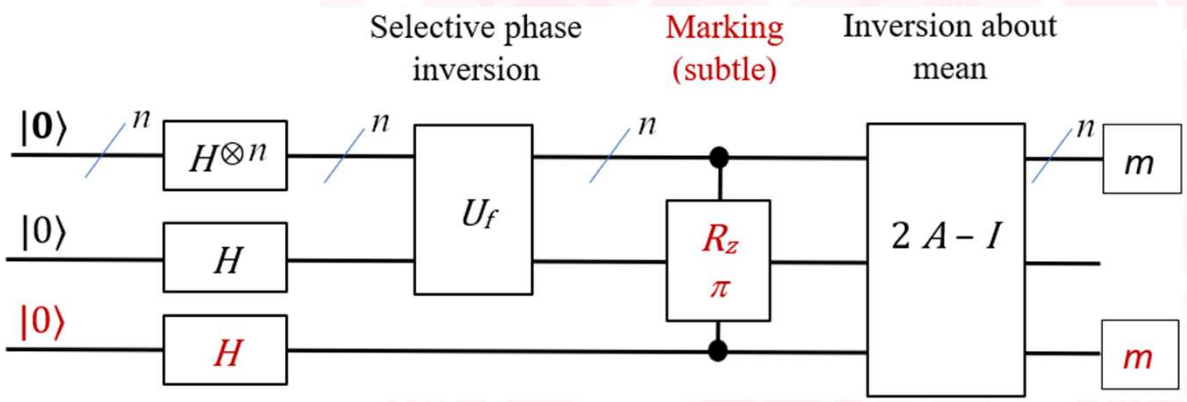
| | 00 | 01 | 10 | 11 | |
|---|---|---|---|---|---|
| No win. | $0$ | $\pi/2$ | $-\pi/2$ | $0$ | Tie 01 and 10 |
| Some win. | $0, \pi/2$ | $\pi, \pi/2$ | $0, -\pi/2$ | $\pi/2, 0$ | 01 dominates |
| All win. | $\pi/2$ | $\pi$ | $0$ | $\pi/2$ | 01 dominates |



# Null and Subtle Eigenmarkings



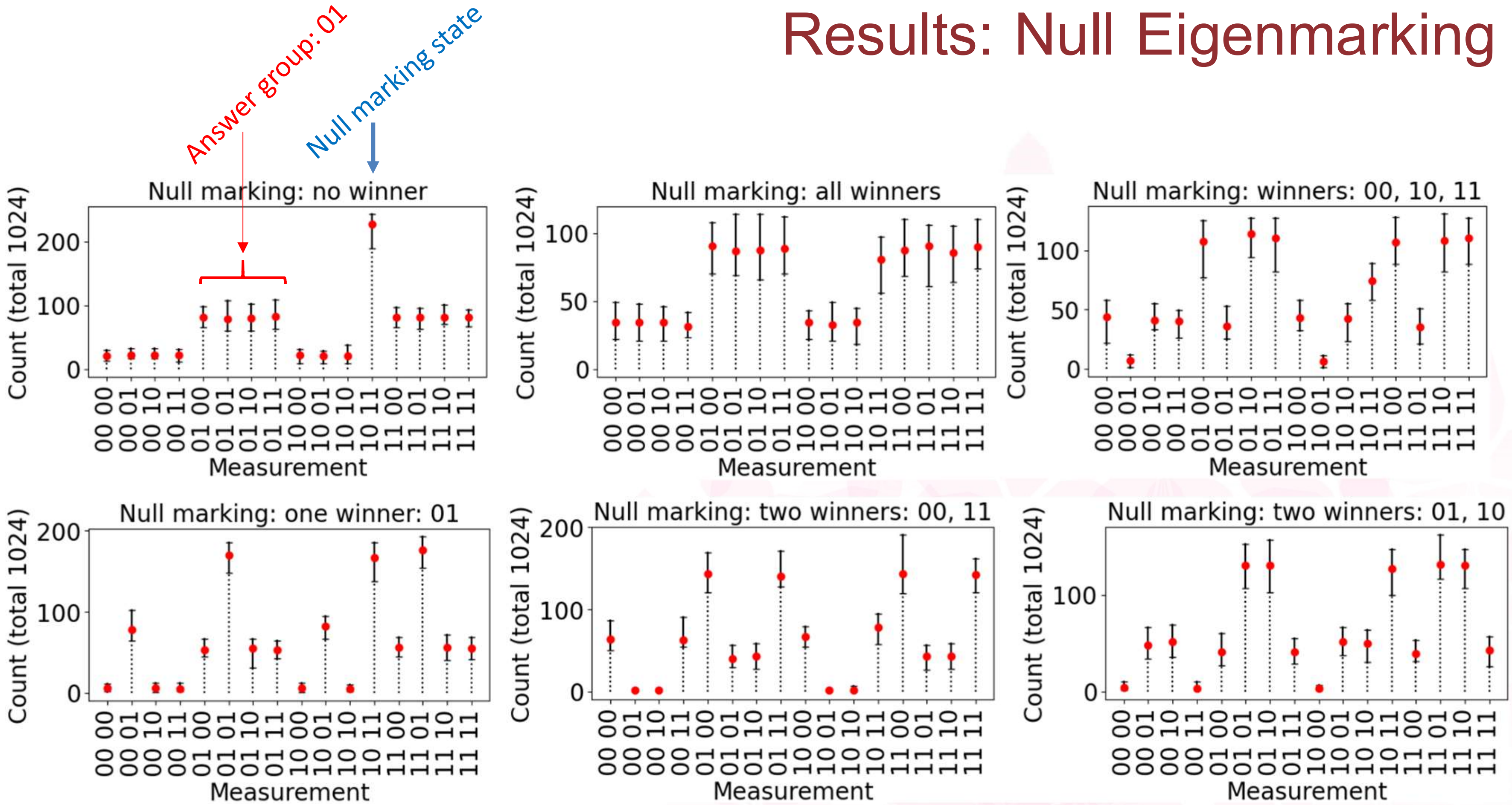

Null marking
- Explicit no-winner state 10 11
- In entailment checking, No-winner ~ no violation!



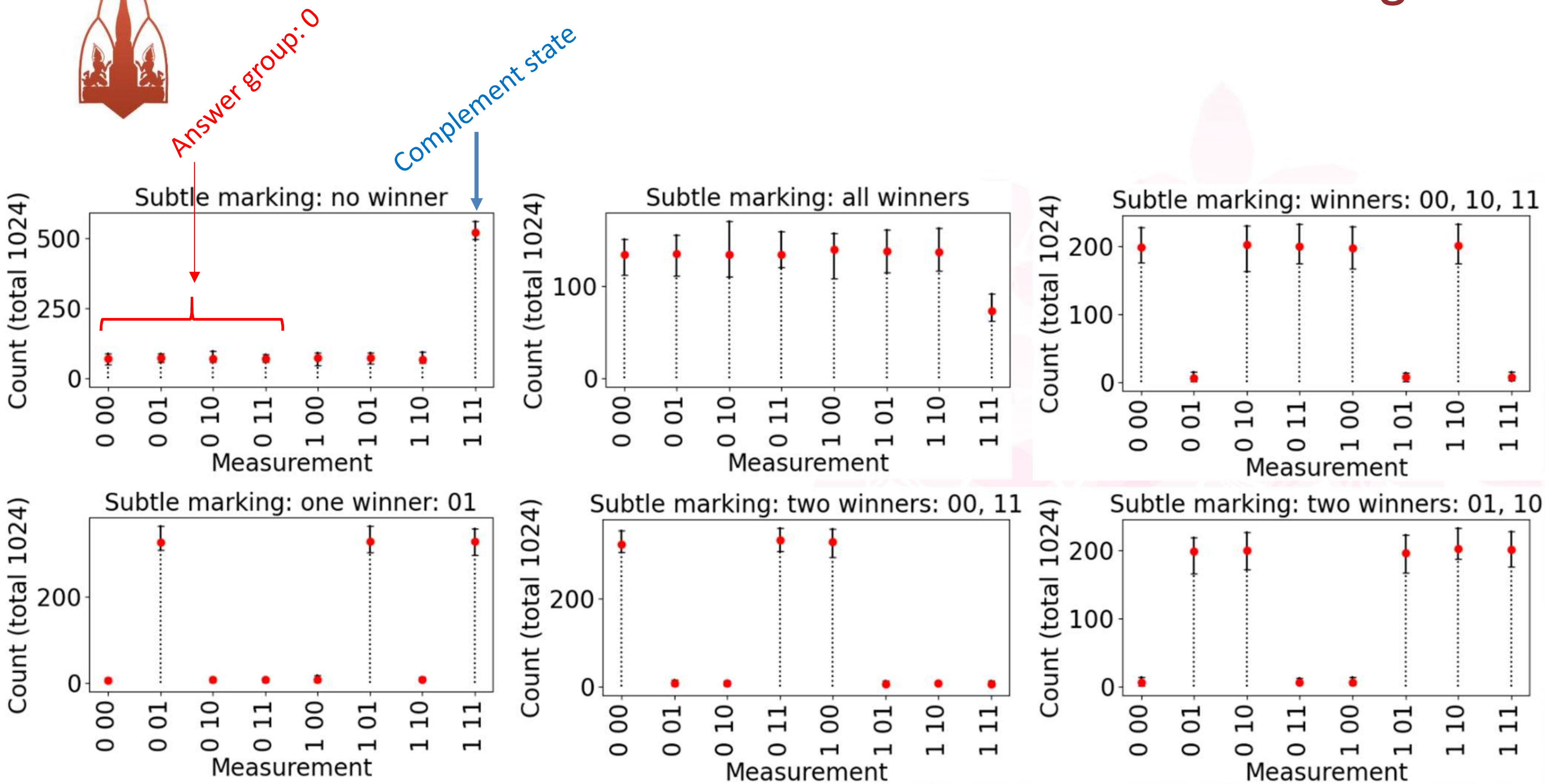

Subtle marking
- Only one extra qubit!
- No change to $U_f$

Cons
- Multiple-qubit control

# Results: Null Eigenmarking



# Results: Subtle Eigenmarking



# Final Results: Get The Winner

Relative difference between #counts (observed) of winning states and ones of non-winning state.

$$W = (c - c')/c'$$

| Scheme | Relative winning margin | | Local prefix |
|---|---|---|---|
| | Global | Local | |
| Eigen. | [0.57, $\boxed{\textbf{1.10}}$, 1.76](0.2) | [0.67, **1.49**, 2.60](0.3) | 01 |
| Null. | [-0.44, **-0.09**, 0.27](0.1) | [0.62, **1.82**, 4.74](0.5) | 01 |
| Subtle. | [-0.37, **0.31**, 6.12](1.4) | [0.28, $\boxed{\textbf{25.72}}$, 197.00](15.8) | 0 |

E.g., $W = 1.1$ means that chance of seeing the winning state $c \approx 1.1\, c' + c' \approx 2.1\, c'$.

# Final Results: Some Win VS No Win

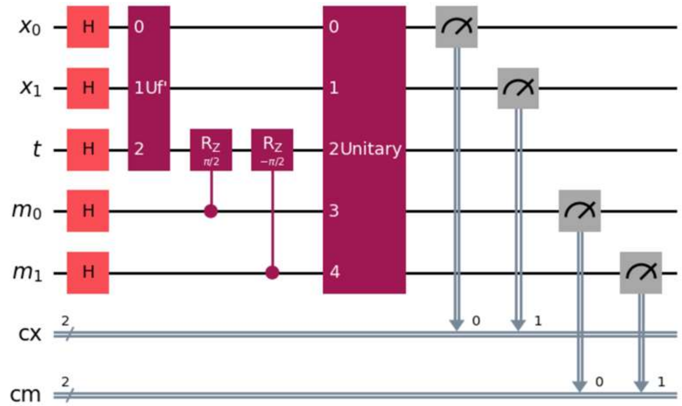
| Scheme | Distinguishability | | | |
|---|---|---|---|---|
| | Worst-case | | Average-case | |
| | $D$ | $D/\lvert\bar{M}_0\rvert$ | $d$ | $d/\lvert\bar{M}_0\rvert$ |
| Eigen. | 0.190 | $\boxed{19.000}$ | 0.532 | $\boxed{53.188}$ |
| Null. | 0.220 | 0.524 | 0.548 | 1.306 |
| Subtle. | $\boxed{0.550}$ | 0.753 | $\boxed{1.140}$ | 1.561 |

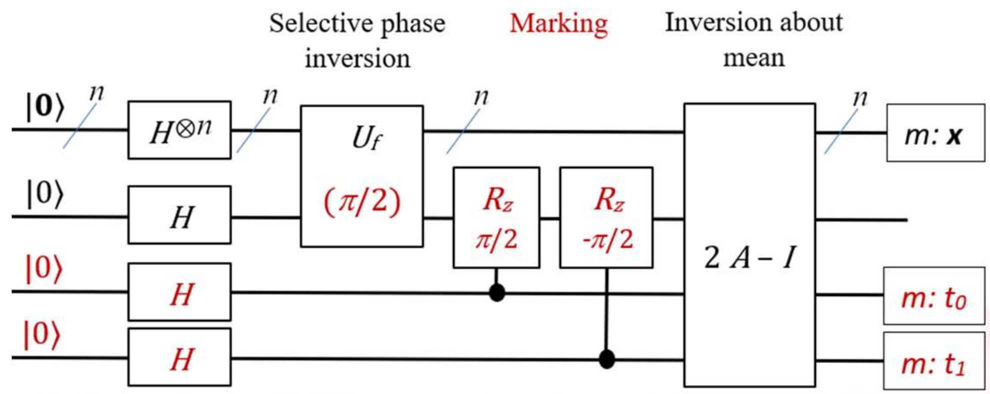
Distinguishability ~ gap between at least some win vs no win.

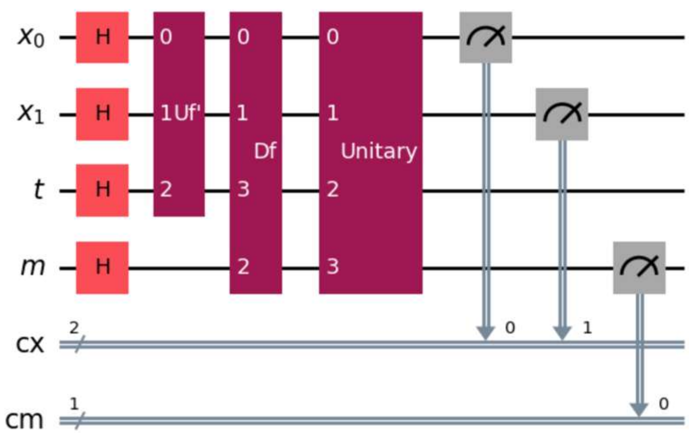
Worst-case: worst score of the winner *vs* best score of the non-winner

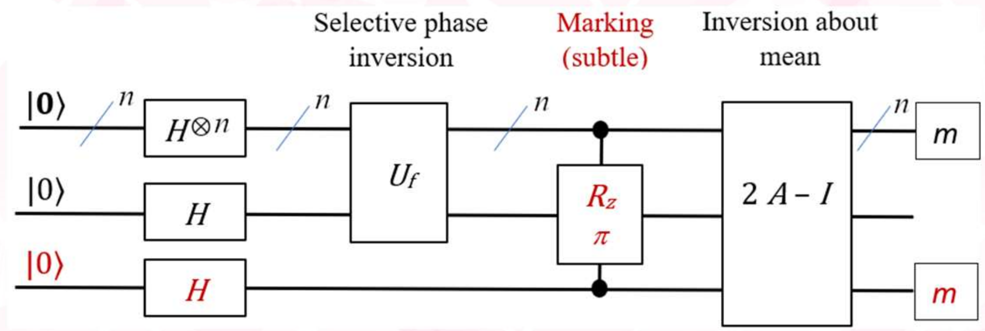
$$D = \frac{\min_{i>0} \min M_i - \max M_0}{\lvert \max M_0 \rvert}$$

# Architectures



# Logic Entailment: Theorem Proving

$KB \vDash \alpha$ if and only if, in every model (truth scenario) in which KB is true, $\alpha$ is true.

KB:

- Durians are spiky.
- Durians are yummy.

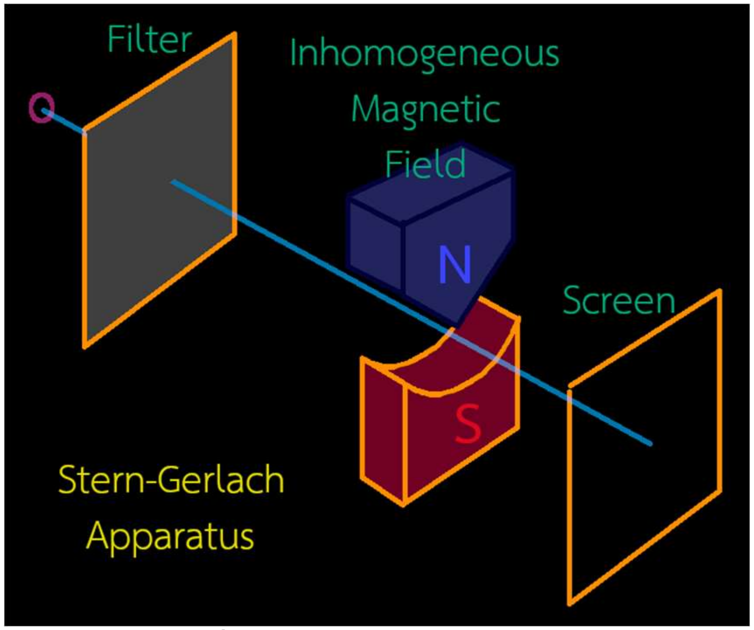
| | |
|---|---|
| $\alpha_1$: Montong durian is spiky. | $KB \vDash \alpha_1$ |
| $\alpha_2$: Montong durian is not spiky. | $KB \nvDash \alpha_2$ |
| $\alpha_3$: There is life on Mars. | $KB \nvDash \alpha_3$ |
| $\alpha_4$: There is no life on Mars. | $KB \nvDash \alpha_4$ |

## Note

- $KB \vDash \alpha$ means $\alpha$ agrees with what KB said.
- $KB \nvDash \alpha$ means $\alpha$ is not what is said by KB.

# Eigenstates

## Stern-Gerlach Experiments



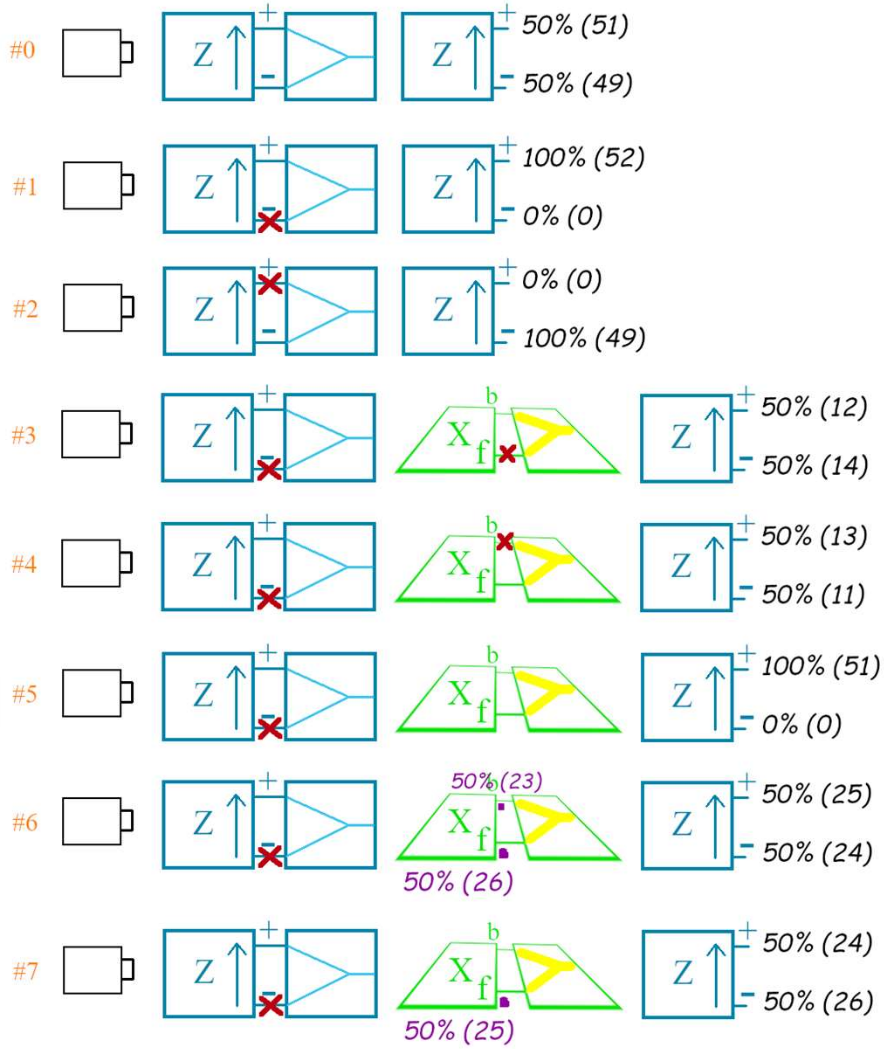

Z ↓ SG Apparatus

- Vertical Magnetic Field (Z ↓)
    - Results: Up, Down
    - Eigenstates: $|u\rangle, |d\rangle$
- Horizontal Magnetic Field (X ·)
    - Results: Front, Back
    - Eigenstates: $|f\rangle, |b\rangle$
- Eigenstates depend on measurement operators.

# Superposition

## Stern-Gerlach Experiments

- #5, which way do the silver atoms go through x-magnetic field?
- Another word, what is the state at that moment?
    - If $|\psi_2\rangle = |f\rangle$, c.f. #4
    - If $|\psi_2\rangle = |b\rangle$, c.f. #3
    - It is "superposition".



# Eigenstates and Measurement

$$|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle + c_3|\psi_3\rangle + \cdots + c_N|\psi_N\rangle$$

- Observability: when measured, the state collapses to one of its eigenstates upon measurement.

  - Eigenstates correspond to the measurement operator.

  - Probability of an eigenstate to which the state collapses is:
    - $\Pr[\,|\psi'\rangle = |\psi_i\rangle\,] = |c_i|^2$

# Quantum State Evolution

Given Hamiltonian (energy operator) $\widehat{H}$, quantum state evolution is described by Schrödinger equation:

$$i\,\bar{h}\,\frac{\partial\,|\,\psi\,\rangle}{\partial\,t} = \widehat{H}|\,\psi\,\rangle$$

Solution: $|\psi'\rangle = |\psi\rangle\,\exp(-\frac{i}{\bar{h}}\,\widehat{H}\,t)$ where $|\psi'\rangle$ is the next state.

- Let unitary operator $U \equiv \exp\left(-\frac{i}{\bar{h}}\,\widehat{H}\,t\right)$ for a specific time $t$,

$$|\psi'\rangle = U\,|\psi\rangle$$

# Tensor Product: Properties

Combining vector spaces together to form larger vector spaces

- Tensor product, $V \otimes W$
  - For an arbitrary scalar $z$ and elements $|v\rangle$ of $V$ and $|w\rangle$ of $W$,
    $$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle).$$
  - For arbitrary $|v_1\rangle$ and $|v_2\rangle$ in $V$ and $|w\rangle$ in $W$,
    $$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle.$$
  - For arbitrary $|v\rangle$ in $V$ and $|w_1\rangle$ and $|w_2\rangle$ in $W$,
    $$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle.$$

# Tensor Product

Combining vector spaces together to form larger vector spaces

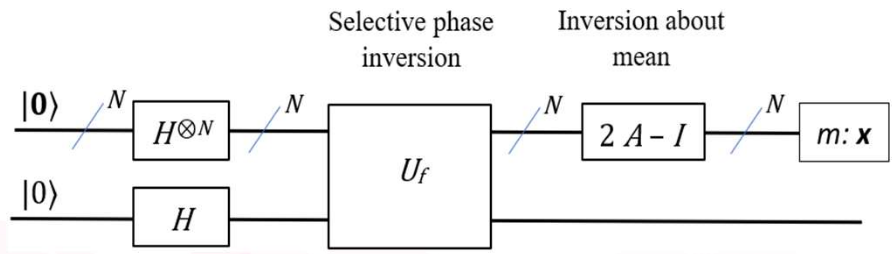
$A$: $m \times n$ matrix, B: $p \times q$ matrix,

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}$$

E.g.,

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 3 \\ 4 \end{bmatrix} \\ 2 \begin{bmatrix} 3 \\ 4 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \\ 6 \\ 8 \end{bmatrix}$$

# Related Matrices: Hadamard




- $H^{\otimes(N+1)}$
  - $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
  - $H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & 1\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ 1\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & -1\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$
  - $H^{\otimes 3} = \frac{1}{2\sqrt{2}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$

# Related Matrices: Selection

- $U_f = |\boldsymbol{x}'\rangle\langle\boldsymbol{x}'| \otimes R_z(\pi) + \sum_{x\in\widetilde{X}} |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes I$ and $R_z(\pi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix}$.
- E.g., $N = 2$, $\boldsymbol{x}' = \mathtt{01}$

$$U_f = \begin{bmatrix} 0 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} + \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$U_f = \begin{bmatrix} 0 & 0 & & & & & & \\ 0 & 0 & & & & & & \\ & & 1 & 0 & & & & \\ & & 0 & e^{i\pi} & & & & \\ & & & & 0 & 0 & & \\ & & & & 0 & 0 & & \\ & & & & & & 0 & 0 \\ & & & & & & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & & & & & & \\ 0 & 1 & & & & & & \\ & & 0 & 0 & & & & \\ & & 0 & 0 & & & & \\ & & & & 1 & 0 & & \\ & & & & 0 & 1 & & \\ & & & & & & 1 & 0 \\ & & & & & & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & e^{i\pi} & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix}.$$

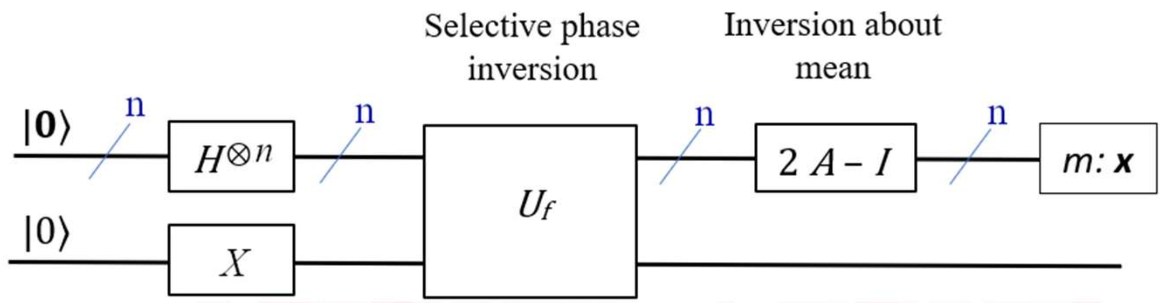
- Note $e^{i\pi} = -1$

# Grover Algorithm

- Have operator $U_f$ represent $f$: flip phase of $y$ if $x = x'$.
- Prepare $|\boldsymbol{x}_0\rangle = |\mathbf{0}\rangle$.
- Apply Hadamard: $|\boldsymbol{x}_1\rangle = H|\boldsymbol{x}_0\rangle$.
- Do Phase Inversion: $|\boldsymbol{x}_2, y_2\rangle = |\boldsymbol{\psi}_2\rangle = U_f|\boldsymbol{x}_1, 1\rangle$.
- Inverse about the mean on the input: $|\boldsymbol{x}_3\rangle = (2A - I)|\boldsymbol{x}_2\rangle$.
- Apply for $J$ times: $J = \mathrm{round}\left(\frac{\pi}{4}\sqrt{N} - \frac{1}{2}\right)$ where $N = 2^n$.
- Measure the qubits.


- Have operator $U_f$ represent $f$: flip phase of $y$ if $x = x'$.
- Prepare $|\boldsymbol{x}_0\rangle = |\mathbf{0}\rangle$.
- Apply Hadamard: $|\boldsymbol{x}_1\rangle = H|\boldsymbol{x}_0\rangle$.
- Do Phase Inversion: $|\boldsymbol{x}_2, y_2\rangle = |\boldsymbol{\psi}_2\rangle = U_f|\boldsymbol{x}_1, 1\rangle$.
- Inverse about the mean on the input: $|\boldsymbol{x}_3\rangle = (2A - I)|\boldsymbol{x}_2\rangle$.
- Apply for $J$ times: $J = \mathrm{round}\left(\frac{\pi}{4}\sqrt{N} - \frac{1}{2}\right)$ where $N = 2^n$.
- Measure the qubits.

# Grover Algorithm: Examples

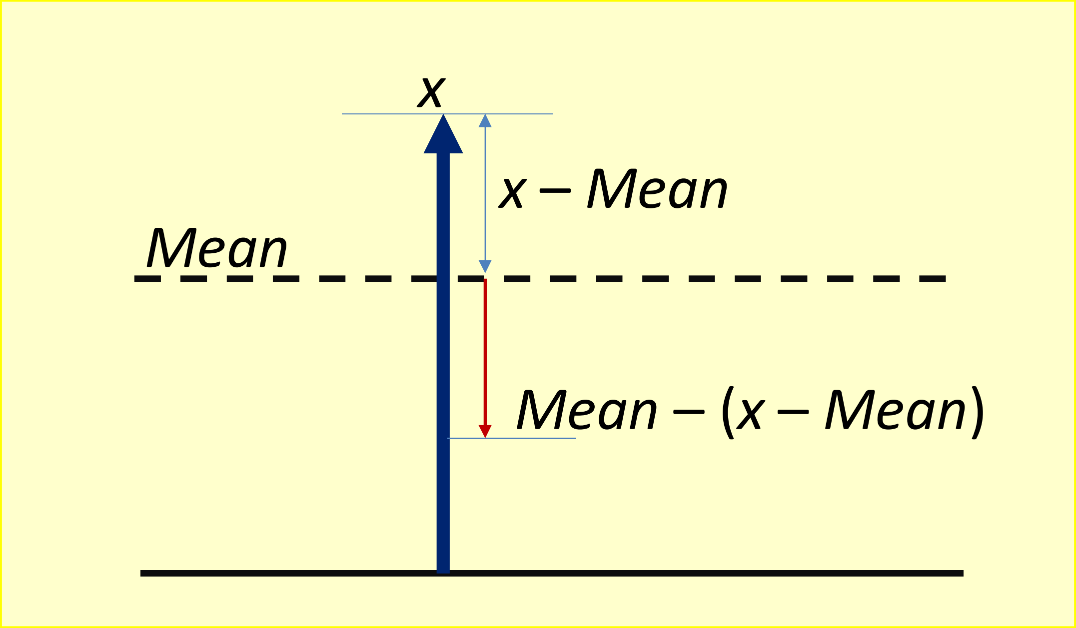



- E.g., $n$ = 2 and $|x'\rangle = |01\rangle$,
  - $|\boldsymbol{x}_0\rangle = |00\rangle = [1\ 0\ 0\ 0]^T$.
  - $|\boldsymbol{x}_1\rangle = H|00\rangle = \frac{1}{2}[1\ 1\ 1\ 1]^T$.
  - $|\boldsymbol{\psi}_1\rangle = |\boldsymbol{x}_1, 1\rangle = \frac{1}{2}[0,1,0,1,0,1,0,1]^T$.
  - $|\boldsymbol{x}_2, y\ \rangle = U_f|\boldsymbol{x}_1, 1\ \rangle = \frac{1}{2}[0, 1, 0, -1, 0, 1, 0,1]^T$.
  - $|\boldsymbol{x}_2\rangle|y_2\rangle = \frac{1}{2}[1, -1,1,1]^T \otimes [0,1]^T$
  - $|\boldsymbol{x}_2\rangle = \frac{1}{2}[1, -1,1,1]^T$
  - $|\boldsymbol{x}_3\rangle = (2A - I)|\boldsymbol{x}_2\rangle = [0,1,0,0]^T$.
  - $J = \text{round}\left(\frac{\pi}{4}\sqrt{4} - \frac{1}{2}\right) = 1$.
  - Measure $|\boldsymbol{x}_3\rangle$ and get eigenstate $|01\rangle$ with probability 1.

# Related Matrices: Average

- $A = \frac{1}{2^N}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}$

- $I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$




- Inversion about mean: $\bar{x} - (x - \bar{x}) = 2\bar{x} - x$
  - $That\ is,$ $(2A - I)X$ where $AX$ computes the mean.