Lecture 20:

The Adversary Method

for Quantum Query Lower Bounds

Quantum query model: recap

Secret N-bit input string w

You can query a coordinate j to find out w_j

In fact, you can query *superpositions*…

Given access to $Q_w^{\pm}$ which implements $|j\rangle \mapsto (-1)^{w_j}|j\rangle$

Trying to solve some fixed *decision problem* φ on w

Cost: *only* the number of uses of $Q_w^{\pm}$

Example: φ = "OR", deciding if w has at least one 1

Grover's Algorithm: Solves φ = "OR" with cost $\lesssim \sqrt{N}$

Think of $\varphi = (\textbf{YES}, \textbf{NO})$, where **YES** and **NO** are subsets of strings.
In "OR" example, **YES** = {all N-bit strings with at least one 1}, **NO** = $\{00\cdots0\}$

If **YES** $\cup$ **NO** $=$ {all strings}, φ is called "total"; otherwise, φ is "partial/promise"

How to prove Lower Bounds on quantum query algorithms…

[Bennett–Bernstein–Brassard–Vazirani ca. '96]:
Proved a cost lower bound for φ = "OR": $\gtrsim \sqrt{N}$ queries are ***necessary***.
They called their technique the Hybrid Method.

[Beals–Buhrman–Cleve–Mosca–de Wolf '98]: The Polynomial Method.

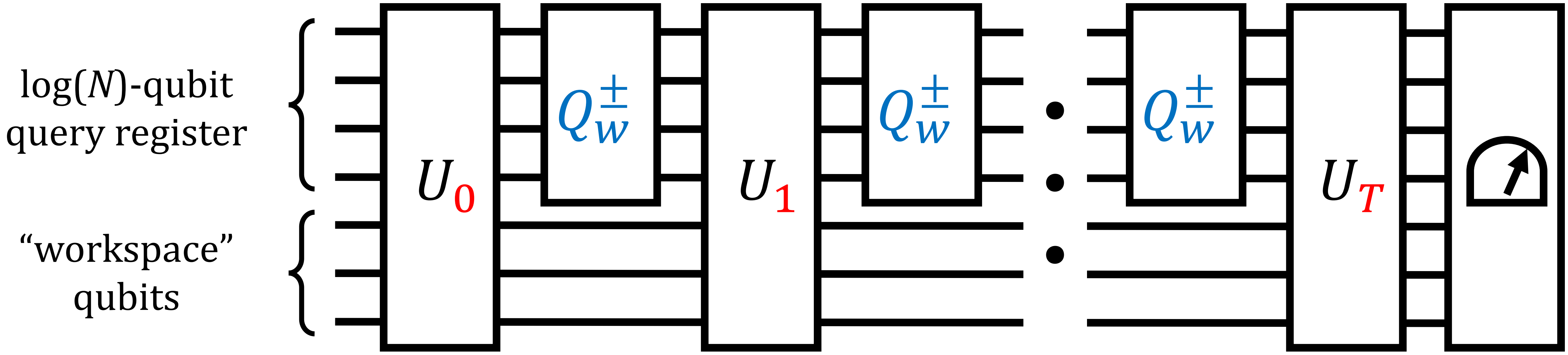
[Ambainis '00]: The (Basic) Adversary Method.

[Many groups]: Variants on the Adversary Method.

[Høyer–Lee–Špalek '07]: "Negative-weights", aka General Adversary Method.

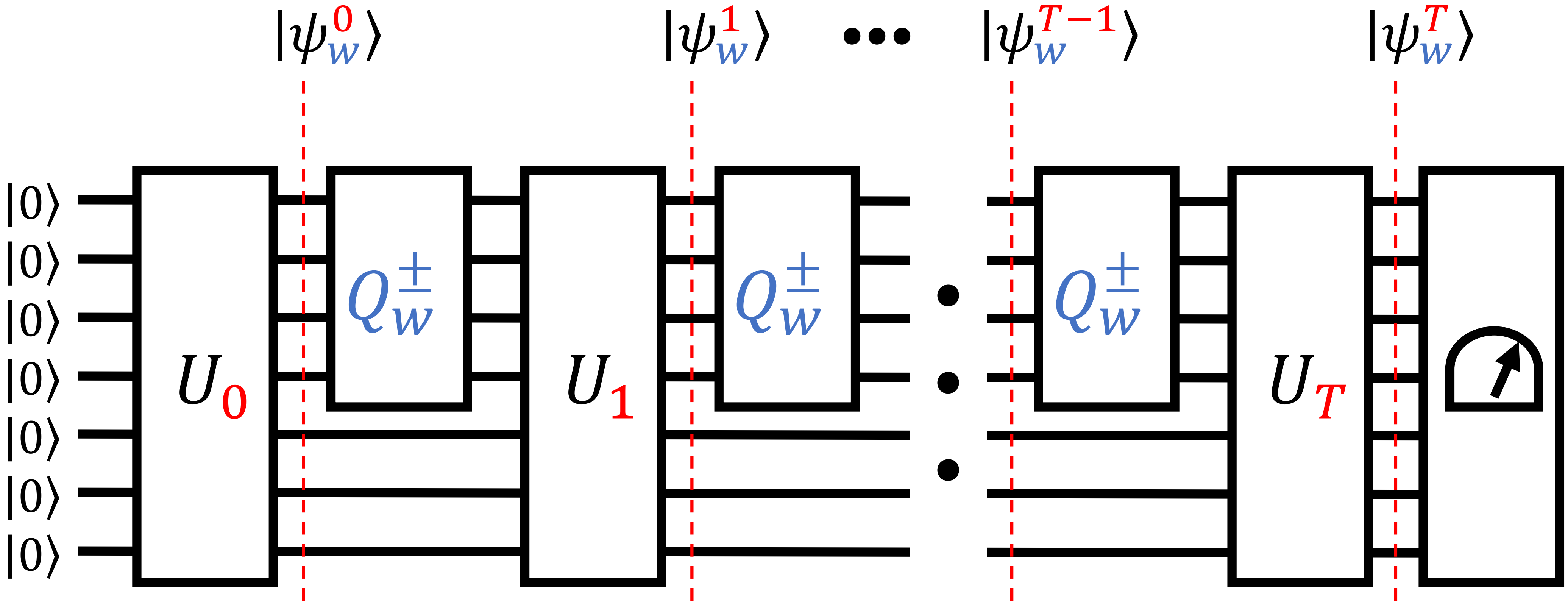
[Reichardt '09]: The General Adversary Method is *optimal*
— there is always a matching upper bound (query algorithm)!

A generic T-query algorithm:



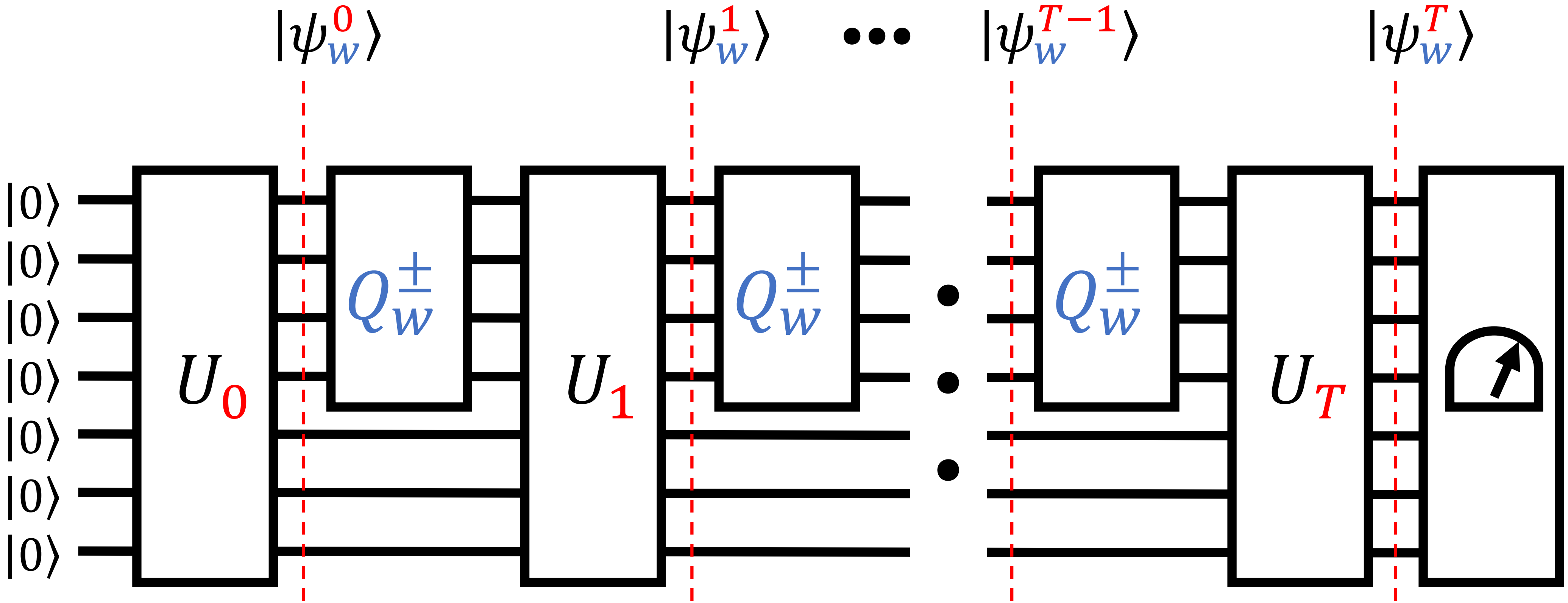
Secret N-bit input string w defines the behavior of $Q_w^{\pm}$

An algorithm supposedly solving $\varphi = (\mathbf{YES}, \mathbf{NO})$:



Secret N-bit input string w defines the behavior of $Q_w^\pm$

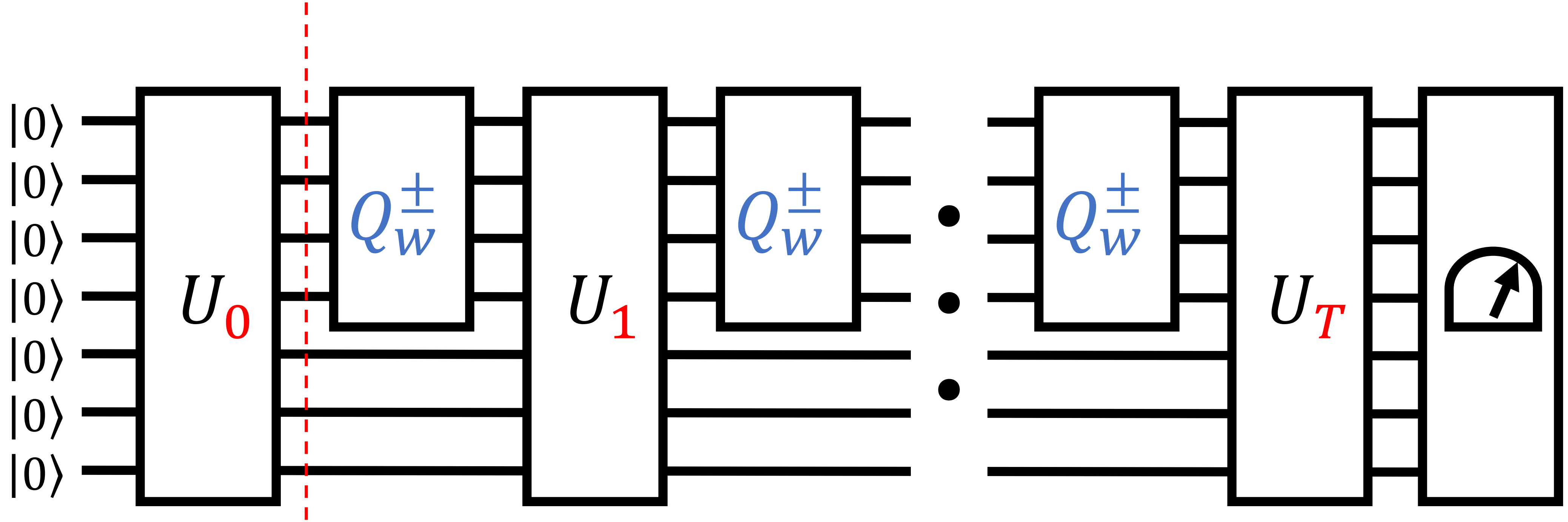
An algorithm supposedly solving $\varphi = (\mathbf{YES}, \mathbf{NO})$:



An "adversary" picks some $y \in \mathbf{YES}$ and some $z \in \mathbf{NO}$ and considers running your algorithm with $w = y$ or with $w = z$.

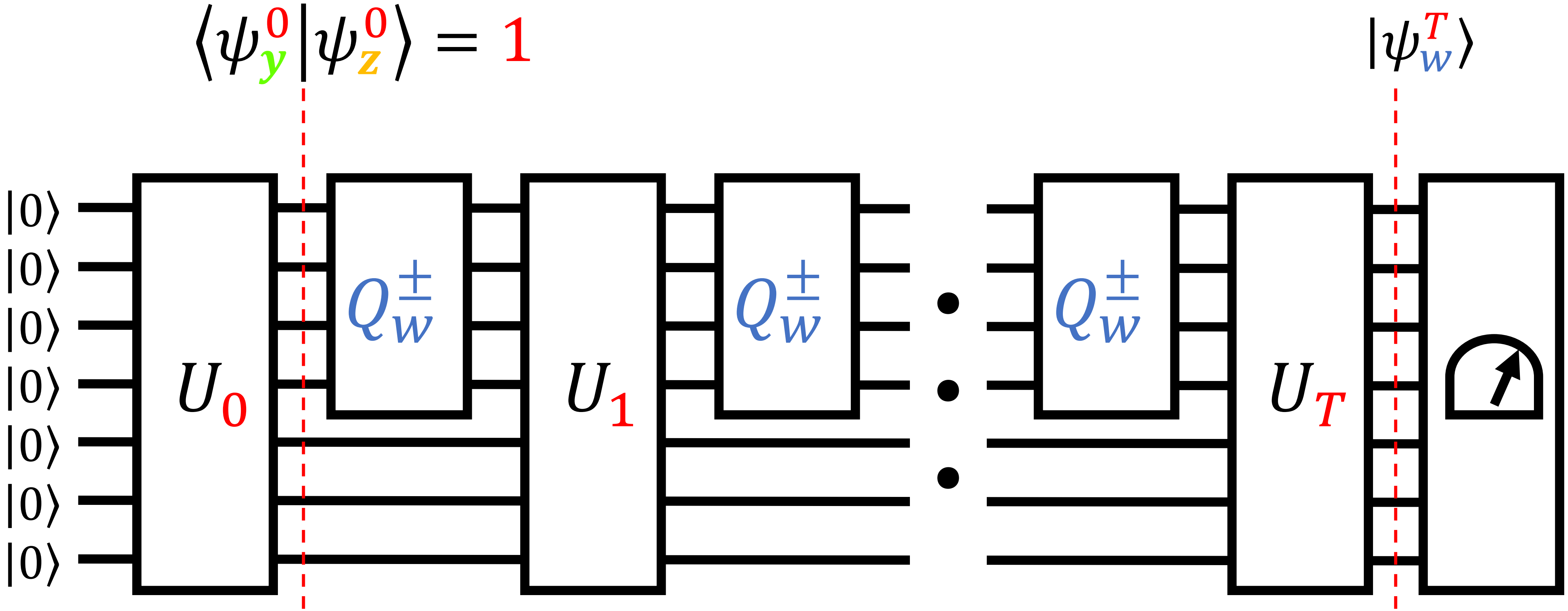
An algorithm supposedly solving $\varphi = (\mathbf{YES}, \mathbf{NO})$:

$|\psi_w^0\rangle$ Clearly: $|\psi_y^0\rangle = |\psi_z^0\rangle$; i.e., $\langle\psi_y^0|\psi_z^0\rangle = 1$



An "adversary" picks some $y \in \mathbf{YES}$ and some $z \in \mathbf{NO}$ and considers running your algorithm with $w = y$ or with $w = z$.

An algorithm supposedly solving $\varphi = (\mathbf{YES}, \mathbf{NO})$:



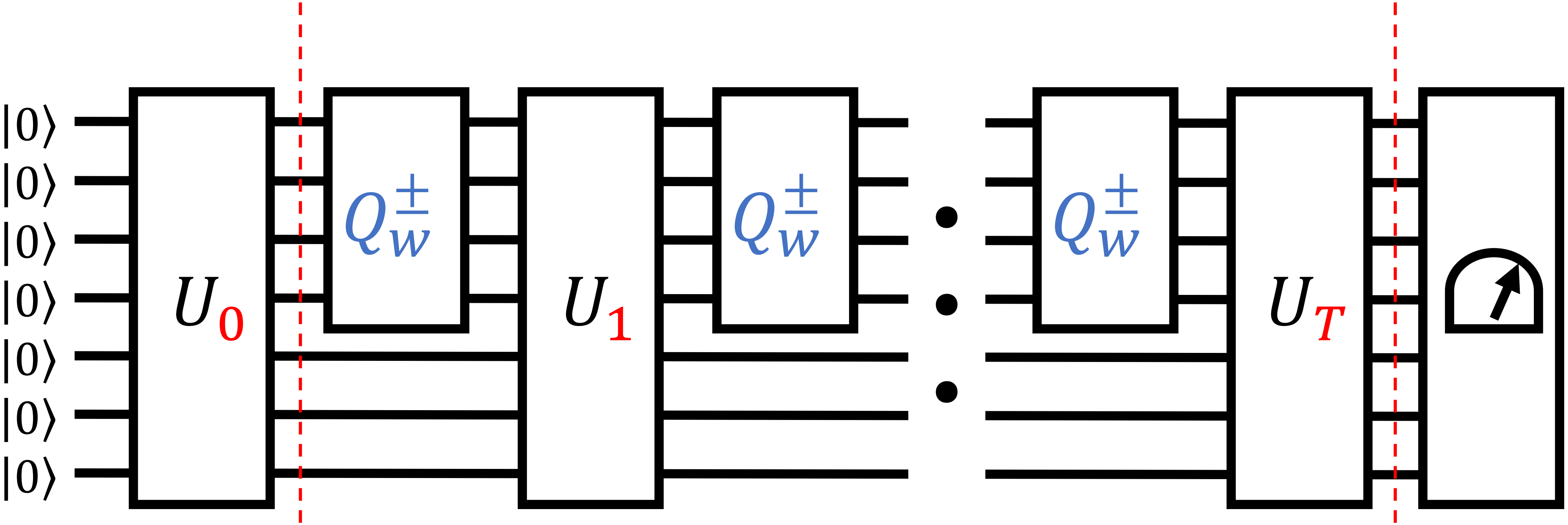
An "adversary" picks some $y \in$ **YES** and some $z \in$ **NO** and considers running your algorithm with $w = y$ or with $w = z$.

An algorithm supposedly solving $\varphi = (\mathbf{YES}, \mathbf{NO})$:

Algorithm must be able to *discriminate* between $|\psi_y^T\rangle$ and $|\psi_z^T\rangle$ with high probability, because it must "accept" y and "reject" z.

$\langle \psi_y^0 | \psi_z^0 \rangle = 1$

Clearly: $\langle \psi_y^T | \psi_z^T \rangle \neq 1$



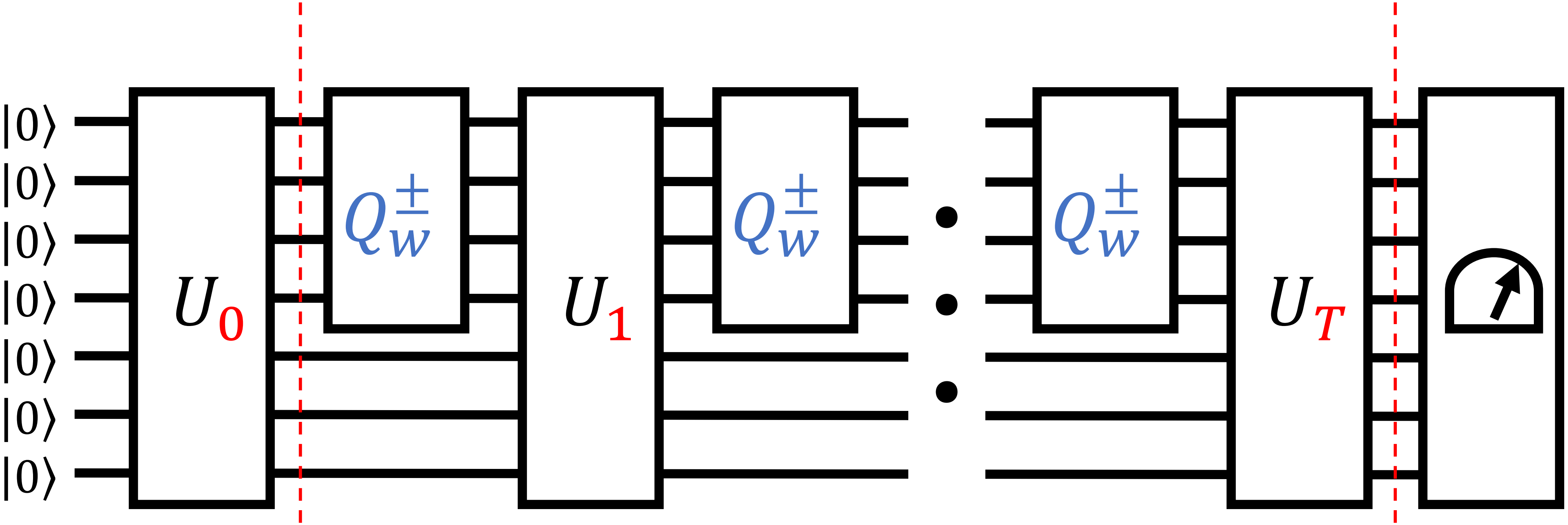
An "adversary" picks some $y \in \mathbf{YES}$ and some $z \in \mathbf{NO}$ and considers running your algorithm with $w = y$ or with $w = z$.

An algorithm supposedly solving $\varphi = (\textbf{YES}, \textbf{NO})$:

Algorithm must be able to *discriminate* between $|\psi_y^T\rangle$ and $|\psi_z^T\rangle$ with high probability, because it must "accept" y and "reject" z.

$$\langle\psi_y^0|\psi_z^0\rangle = 1$$

In fact, we better have $|\langle\psi_y^T|\psi_z^T\rangle| \leq .99$



An "adversary" picks some $y \in$ **YES** and some $z \in$ **NO** and considers running your algorithm with $w = y$ or with $w = z$.

An algorithm supposedly solving $\varphi = (\text{YES}, \text{NO})$:

Algorithm must be able to *discriminate* between $|\psi_y^T\rangle$ and $|\psi_z^T\rangle$ with high probability, because it must "accept" y and "reject" z.

$$\langle\psi_y^0|\psi_z^0\rangle = 1$$

In fact, we better have $|\langle\psi_y^T|\psi_z^T\rangle| \leq .99$

Recall **Lecture 4.5, "Discriminating Two Qubits"**:

Given two quantum states $|u\rangle$ and $|v\rangle$,
the probability with which they can be distinguished by *any* quantum algorithm is a function of the angle between them.

An "adversary" picks some $y \in$ YES and some $z \in$ NO
and considers running your algorithm with $w = y$ or with $w = z$.

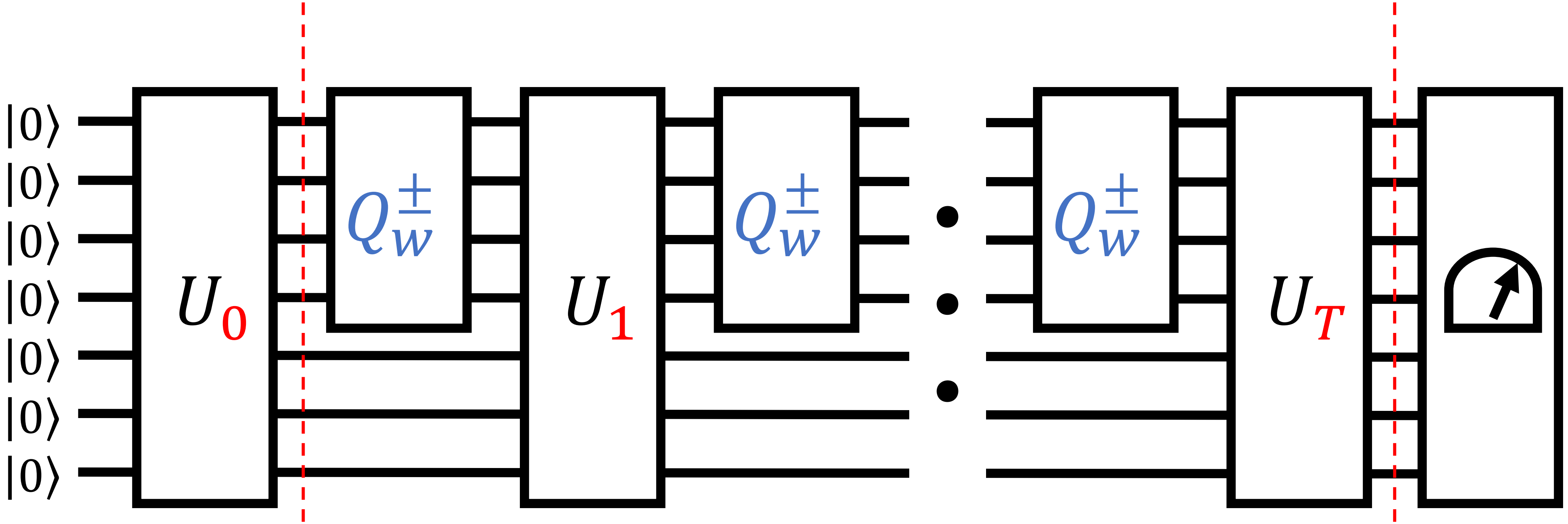
Possible idea: define $\text{Progress}_t = |\langle \psi_y^t | \psi_z^t \rangle|$

Suppose we can show $|\text{Progress}_t - \text{Progress}_{t+1}| \leq \delta$

This would imply: $T \geq .01/\delta$ ☺

$\langle \psi_y^0 | \psi_z^0 \rangle = 1$

We have $|\langle \psi_y^T | \psi_z^T \rangle| \leq .99$



An "adversary" picks some $y \in$ **YES** and some $z \in$ **NO**
and considers running your algorithm with $w = y$ or with $w = z$.

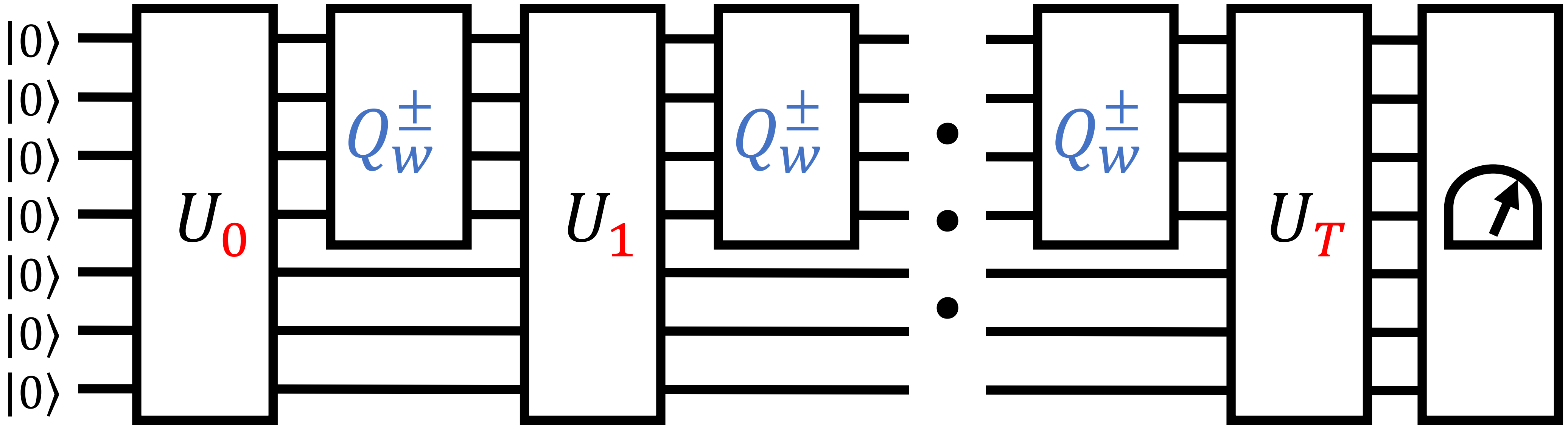
Possible idea: define $\text{Progress}_t = |\langle\psi_y^t|\psi_z^t\rangle|$

Suppose we can show $|\text{Progress}_t - \text{Progress}_{t+1}| \leq \delta$

This would imply: $T \geq .01/\delta$ ☺

Note: Applying unitary U_t does not affect $|\langle\psi_y^t|\psi_z^t\rangle|$

So suffices to analyze how $Q_w^{\pm}$ affects Progress



An "adversary" picks some $y \in$ **YES** and some $z \in$ **NO**
and considers running your algorithm with $w = y$ or with $w = z$.

Possible idea: define $\text{Progress}_t = |\langle \psi_y^t | \psi_z^t \rangle|$

Suppose we can show $|\text{Progress}_t - \text{Progress}_{t+1}| \leq \delta$

This would imply: $T \geq .01/\delta$ ☺

Note: Applying unitary U_t does not affect $|\langle \psi_y^t | \psi_z^t \rangle|$

So suffices to analyze how $Q_w^{\pm}$ affects Progress

This is a good idea, but a little too simple

Doesn't suffice to focus on a *single* $y \in$ **YES** and a *single* $z \in$ **NO**

If it did, would show that many queries needed to distinguish $w = y$ from $w = z$

But this only requires **1** query: since $y \neq z$, there exists j such that $y_j \neq z_j$

Need to have a *bunch* of y's versus a *bunch* of z's

An "adversary" picks some $y \in$ **YES** and some $z \in$ **NO**
and considers running your algorithm with $w = y$ or with $w = z$.

[Ambainis '00]

Super-Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, suppose $Y \subseteq \text{YES}$, $Z \subseteq \text{NO}$ are such that:

- for each $y \in Y$, there are at least m strings $z \in Z$ with $\text{dist}(y, z) = 1$
- for each $z \in Z$, there are at least m' strings $y \in Y$ with $\text{dist}(y, z) = 1$

Then $\text{Q}(\varphi)$, the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m'}$.

we'll show $\geq .005 \sqrt{m\, m'}$

$\text{dist}(y, z)$ = Hamming distance,
# of coordinates where y, z differ

Super-Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, suppose $\boldsymbol{Y} \subseteq \text{YES}$, $\boldsymbol{Z} \subseteq \text{NO}$ are such that:

- for each $\boldsymbol{y} \in \boldsymbol{Y}$, there are at least m strings $\boldsymbol{z} \in \boldsymbol{Z}$ with dist($\boldsymbol{y}$, $\boldsymbol{z}$) = 1
- for each $\boldsymbol{z} \in \boldsymbol{Z}$, there are at least m' strings $\boldsymbol{y} \in \boldsymbol{Y}$ with dist($\boldsymbol{y}$, $\boldsymbol{z}$) = 1

Then Q(φ), the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m'}$.

<u>Example use #1</u>: φ = "OR" (Decision-Grover)

Take $\boldsymbol{Y} = \{000001, 000010, 000100, 001000, 010000, 100000\}$.

Take $\boldsymbol{Z} = \{000000\}$. (Well, at least for N = 6.)

$m = 1$, $m' = N$ $\Rightarrow$ Q(φ) $\gtrsim \sqrt{N}$ ☺

Super-Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, suppose $\boldsymbol{Y} \subseteq \text{YES}$, $\boldsymbol{Z} \subseteq \text{NO}$ are such that:

- for each $\boldsymbol{y} \in \boldsymbol{Y}$, there are at least m strings $\boldsymbol{z} \in \boldsymbol{Z}$ with $\text{dist}(\boldsymbol{y}, \boldsymbol{z}) = 1$
- for each $\boldsymbol{z} \in \boldsymbol{Z}$, there are at least m' strings $\boldsymbol{y} \in \boldsymbol{Y}$ with $\text{dist}(\boldsymbol{y}, \boldsymbol{z}) = 1$

Then $\text{Q}(\varphi)$, the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m'}$.

<u>Example use #2</u>: φ: Decide if w has at least k 1's, or less than k 1's

Take $\boldsymbol{Y} = \{\text{all strings with exactly } k \text{ 1's}\}$.

Take $\boldsymbol{Z} = \{\text{all strings with exactly } k-1 \text{ 1's}\}$.

$m = k, \;\; m' = N - k + 1$

$$\Rightarrow \;\; \text{Q}(\varphi) \gtrsim \sqrt{k(N-k+1)}, \text{ which is } \gtrsim \sqrt{kN} \text{ for } k \leq \frac{N}{2}$$

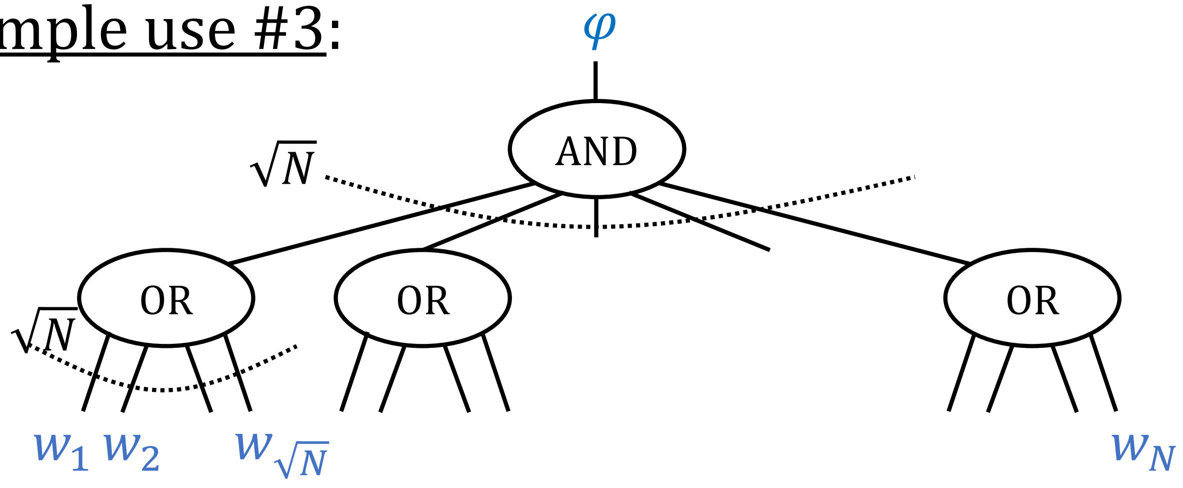
Super-Basic Adversary Method:

For φ = (YES, NO), suppose $Y \subseteq$ YES, $Z \subseteq$ NO are such that:

- for each $y \in Y$, there are at least m strings $z \in Z$ with dist(y, z) = 1
- for each $z \in Z$, there are at least m' strings $y \in Y$ with dist(y, z) = 1

Then Q(φ), the quantum query complexity of φ, is $\gtrsim \sqrt{m\,m'}$.

Example use #3:



YES = strings with a 1 in each 'block'
NO = strings with a block of all 0's

Y = strings with *exactly* one 1 per block
Z = strings with exactly one all-0's block, all other blocks having exactly one 1

$m = \sqrt{N}$, $m' = \sqrt{N}$ $\Rightarrow$ Q(φ) $\gtrsim \sqrt{N}$

This lower bound is sharp, and not known to be attainable by the "Polynomial Method"

Super-Basic Adversary Method:

For φ = (YES, NO), suppose $Y \subseteq$ YES, $Z \subseteq$ NO are such that:

- for each $y \in Y$, there are at least m strings $z \in Z$ with dist(y, z) = 1
- for each $z \in Z$, there are at least m' strings $y \in Y$ with dist(y, z) = 1

Then Q(φ), the quantum query complexity of φ, is $\gtrsim \sqrt{m\,m'}$.

Proof: Define $R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

(These are *particularly challenging* pairs of inputs for the algorithm:
the algorithm needs to give different answers on them,
but there is only a single coordinate where they are different.)

Super-Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, suppose $Y \subseteq \text{YES}$, $Z \subseteq \text{NO}$ are such that:

- for each $y \in Y$, there are at least m strings $z \in Z$ with $\text{dist}(y, z) = 1$
- for each $z \in Z$, there are at least m' strings $y \in Y$ with $\text{dist}(y, z) = 1$

Then Q(φ), the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m'}$.

Proof: Define $R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

Define $\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$, where $|\psi_w^t\rangle$ is state after t^{th} query, on input w

We have $\text{Progress}_0 = |R|$ and $\text{Progress}_T \leq .99|R|$

the latter because $\left|\langle \psi_y^T | \psi_z^T \rangle\right| \leq .99$ must hold for all $y \in Y$, $z \in Z$

Super-Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, suppose $Y \subseteq \text{YES}$, $Z \subseteq \text{NO}$ are such that:

- for each $y \in Y$, there are at least m strings $z \in Z$ with $\text{dist}(y, z) = 1$
- for each $z \in Z$, there are at least m' strings $y \in Y$ with $\text{dist}(y, z) = 1$

Then $\text{Q}(\varphi)$, the quantum query complexity of φ, is $\gtrsim \sqrt{m\,m'}$.

Proof: Define $R = \{\, (y, z) : \text{dist}(y, z) = 1 \,\} \subseteq Y \times Z$

Define $\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$, where $|\psi_w^t\rangle$ is state after t^{th} query, on input w

We have $\text{Progress}_0 = |R|$ and $\text{Progress}_T \leq .99|R|$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \frac{2}{\sqrt{m\,m'}}|R|$ for all t.

$\Rightarrow$ $T \geq .005\sqrt{m\,m'}$, as desired.

- for each $y \in Y$, there are at least m strings $z \in Z$ with $\mathrm{dist}(y, z) = 1$
- for each $z \in Z$, there are at least m' strings $y \in Y$ with $\mathrm{dist}(y, z) = 1$

$$R = \{ (y, z) : \mathrm{dist}(y, z) = 1 \} \subseteq Y \times Z \qquad \mathrm{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\mathrm{Progress}_t - \mathrm{Progress}_{t+1} \leq \frac{2}{\sqrt{m\, m'}} |R|$ for all t.

- for each $y \in Y$, there are at least m strings $z \in Z$ with $\text{dist}(y, z) = 1$
- for each $z \in Z$, there are at least m' strings $y \in Y$ with $\text{dist}(y, z) = 1$

$$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z \qquad \text{Progress}_t = \sum_{(y,z)\in R} \left| \langle \psi_y^t | \psi_z^t \rangle \right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \le \frac{2}{\sqrt{m\, m'}} |R|$ for all t.

---

for each $y \in Y$, there are at least m strings $z \in Z$ with $\text{dist}(y, z) = 1$

Hence $|R| \ge m\,|Y|$

Similarly $|R| \ge m'|Z|$

So $2|R| \ge m|Y| + m'|Z|$

Claim is even stronger if RHS is $\frac{1}{\sqrt{m\, m'}}(m|Y| + m'|Z|) = \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} |\langle \psi_y^t | \psi_z^t \rangle|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Recall: Unitaries don't affect Progress, just the $Q_w^{\pm}$ queries.

Fix any t and $t+1$ ("before" and "after")

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

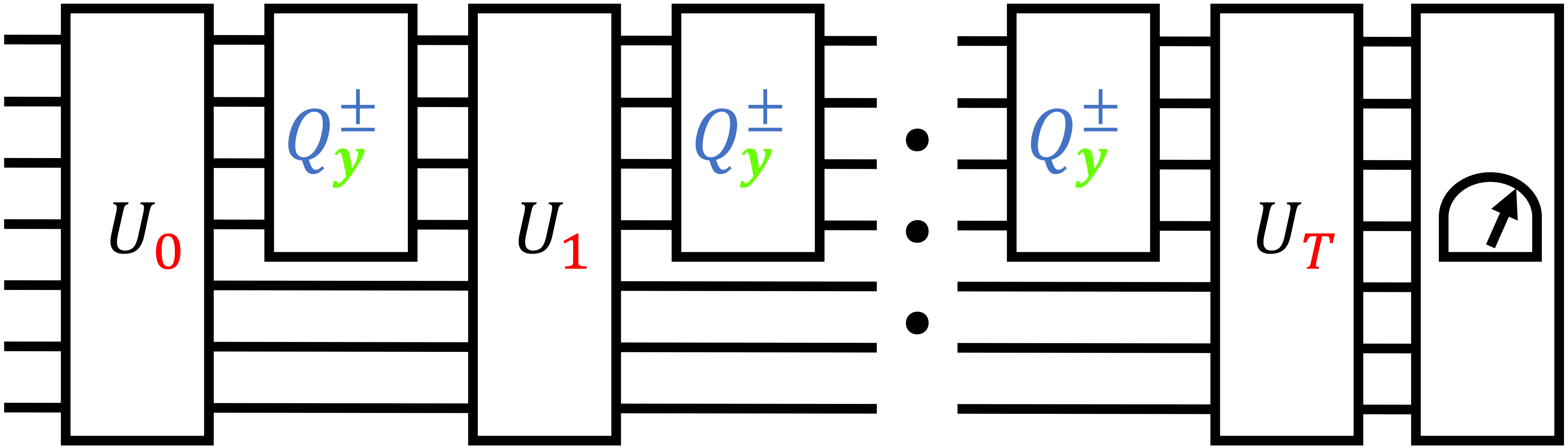
$$R = \{\, (y, z) : \text{dist}(y, z) = 1 \,\} \subseteq Y \times Z \qquad \text{Progress}_t = \sum_{(y,z)\in R} |\langle \psi_y^t | \psi_z^t \rangle|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle$

"After": $|\psi_y^{t+1}\rangle$



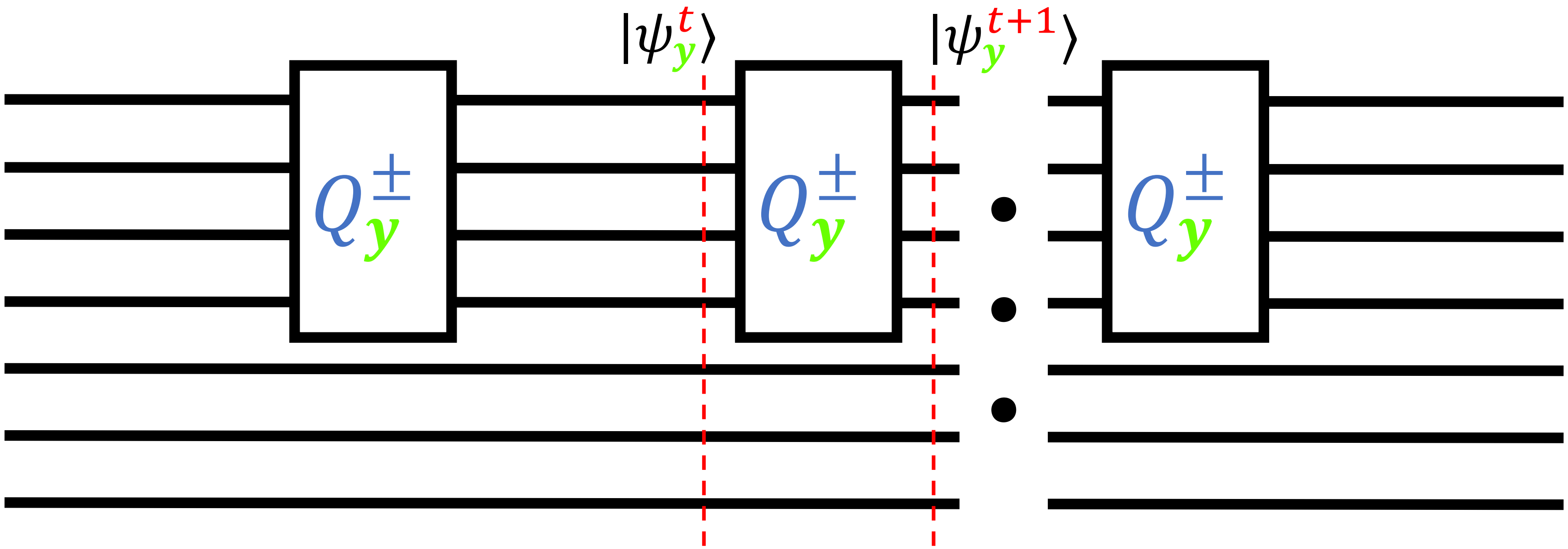
$$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z \qquad \text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle$

"After": $|\psi_y^{t+1}\rangle$



$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$\text{Progress}_t = \sum_{(y,z)\in R} |\langle \psi_y^t | \psi_z^t \rangle|$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and t+1

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle = |1\rangle \otimes (\text{stuff}_1) + |2\rangle \otimes (\text{stuff}_2) + \cdots + |N\rangle \otimes (\text{stuff}_N)$

query register

workspace register

We have collected like terms based on the query register.

"After": $|\psi_y^{t+1}\rangle$

Let $|\phi_j\rangle$ be a unit vector in the direction of (stuff_j)

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} |\langle \psi_y^t | \psi_z^t \rangle|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and t+1

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle = \alpha_1|1\rangle \otimes |\phi_1\rangle + \alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + \alpha_N|N\rangle \otimes |\phi_N\rangle$

We have collected like terms based on the query register.

"After": $|\psi_y^{t+1}\rangle$

Let $|\phi_j\rangle$ be a unit vector in the direction of (stuff_j)

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle = \alpha_1|1\rangle \otimes |\phi_1\rangle + \alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + \alpha_N|N\rangle \otimes |\phi_N\rangle$

Each $|\phi_j\rangle$ is unit, and $\sum_j |\alpha_j|^2 = 1$.

"After": $|\psi_y^{t+1}\rangle$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$\text{Progress}_t = \sum_{(y,z)\in R} \left| \langle \psi_y^t | \psi_z^t \rangle \right|$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle = \alpha_1|1\rangle \otimes |\phi_1\rangle + \alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + \alpha_N|N\rangle \otimes |\phi_N\rangle$

Each $|\phi_j\rangle$ is unit, and $\sum_j |\alpha_j|^2 = 1$.

$Q_y^{\pm}$

The j^{th} amplitude is multiplied by $(-1)^{y_j}$

"After": $|\psi_y^{t+1}\rangle = (-1)^{y_1}\alpha_1|1\rangle \otimes |\phi_1\rangle + (-1)^{y_2}\alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + (-1)^{y_N}\alpha_N|N\rangle \otimes |\phi_N\rangle$

$R = \{ (y, z) : \mathrm{dist}(y, z) = 1 \} \subseteq Y \times Z$

$\text{Progress}_t = \sum_{(y,z)\in R} \left| \langle \psi_y^t | \psi_z^t \rangle \right|$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle = \alpha_1|1\rangle \otimes |\phi_1\rangle + \alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + \alpha_N|N\rangle \otimes |\phi_N\rangle$

$|\psi_z^t\rangle = \beta_1|1\rangle \otimes |\chi_1\rangle + \beta_2|2\rangle \otimes |\chi_2\rangle + \cdots + \beta_N|N\rangle \otimes |\chi_N\rangle$

Each $|\phi_j\rangle$ is unit, and $\sum_j |\alpha_j|^2 = 1$.

"After": $|\psi_y^{t+1}\rangle = (-1)^{y_1}\alpha_1|1\rangle \otimes |\phi_1\rangle + (-1)^{y_2}\alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + (-1)^{y_N}\alpha_N|N\rangle \otimes |\phi_N\rangle$

$|\psi_z^{t+1}\rangle = (-1)^{z_1}\beta_1|1\rangle \otimes |\chi_1\rangle + (-1)^{z_2}\beta_2|2\rangle \otimes |\chi_2\rangle + \cdots + (-1)^{z_N}\beta_N|N\rangle \otimes |\chi_N\rangle$

$$R = \{\, (y, z) : \mathrm{dist}(y, z) = 1 \,\} \subseteq Y \times Z \qquad \mathrm{Progress}_t = \sum_{(y,z)\in R} \left| \langle \psi_y^t | \psi_z^t \rangle \right|$$

Claim: $\mathrm{Progress}_t - \mathrm{Progress}_{t+1} \le \sqrt{\frac{m}{m'}}\,|Y| + \sqrt{\frac{m'}{m}}\,|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle = \alpha_1|1\rangle \otimes |\phi_1\rangle + \alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + \alpha_N|N\rangle \otimes |\phi_N\rangle$

$|\psi_z^t\rangle = \beta_1|1\rangle \otimes |\chi_1\rangle + \beta_2|2\rangle \otimes |\chi_2\rangle + \cdots + \beta_N|N\rangle \otimes |\chi_N\rangle$

Each $|\phi_j\rangle$ is unit, and $\sum_j |\alpha_j|^2 = 1$.

$\langle \psi_y^t | \psi_z^t \rangle = \overline{\alpha_1}\beta_1\langle \phi_1|\chi_1\rangle + \overline{\alpha_2}\beta_2\langle \phi_2|\chi_2\rangle + \cdots + \overline{\alpha_N}\beta_N\langle \phi_N|\chi_N\rangle$

"After": $|\psi_y^{t+1}\rangle = (-1)^{y_1}\alpha_1|1\rangle \otimes |\phi_1\rangle + (-1)^{y_2}\alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + (-1)^{y_N}\alpha_N|N\rangle \otimes |\phi_N\rangle$

$|\psi_z^{t+1}\rangle = (-1)^{z_1}\beta_1|1\rangle \otimes |\chi_1\rangle + (-1)^{z_2}\beta_2|2\rangle \otimes |\chi_2\rangle + \cdots + (-1)^{z_N}\beta_N|N\rangle \otimes |\chi_N\rangle$

These signs are all the same — except for in coordinate j^*

$$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z \qquad \text{Progress}_t = \sum_{(y,z)\in R} \left| \langle \psi_y^t | \psi_z^t \rangle \right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}\,|Y| + \sqrt{\frac{m'}{m}}\,|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate j^*

"Before": $|\psi_y^t\rangle = \alpha_1|1\rangle \otimes |\phi_1\rangle + \alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + \alpha_N|N\rangle \otimes |\phi_N\rangle$

$|\psi_z^t\rangle = \beta_1|1\rangle \otimes |\chi_1\rangle + \beta_2|2\rangle \otimes |\chi_2\rangle + \cdots + \beta_N|N\rangle \otimes |\chi_N\rangle$

Each $|\phi_j\rangle$ is unit, and $\sum_j |\alpha_j|^2 = 1$.

$\langle \psi_y^t | \psi_z^t \rangle = \overline{\alpha_1}\beta_1\langle \phi_1|\chi_1\rangle + \overline{\alpha_2}\beta_2\langle \phi_2|\chi_2\rangle + \cdots + \overline{\alpha_N}\beta_N\langle \phi_N|\chi_N\rangle$

"After": $|\psi_y^{t+1}\rangle = (-1)^{y_1}\alpha_1|1\rangle \otimes |\phi_1\rangle + (-1)^{y_2}\alpha_2|2\rangle \otimes |\phi_2\rangle + \cdots + (-1)^{y_N}\alpha_N|N\rangle \otimes |\phi_N\rangle$

$|\psi_z^{t+1}\rangle = (-1)^{z_1}\beta_1|1\rangle \otimes |\chi_1\rangle + (-1)^{z_2}\beta_2|2\rangle \otimes |\chi_2\rangle + \cdots + (-1)^{z_N}\beta_N|N\rangle \otimes |\chi_N\rangle$

$\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle = \overline{\alpha_1}\beta_1\langle \phi_1|\chi_1\rangle + \overline{\alpha_2}\beta_2\langle \phi_2|\chi_2\rangle + \cdots - \overline{\alpha_{j^*}}\beta_{j^*}\langle \phi_{j^*}|\chi_{j^*}\rangle + \cdots + \overline{\alpha_N}\beta_N\langle \phi_N|\chi_N\rangle$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before":

Each $|\phi_j\rangle$ is unit, and $\sum_j |\alpha_j|^2 = 1$.

$$\langle \psi_y^t | \psi_z^t \rangle = \overline{\alpha_1}\beta_1\langle \phi_1 | \chi_1 \rangle + \overline{\alpha_2}\beta_2\langle \phi_2 | \chi_2 \rangle + \cdots + \overline{\alpha_N}\beta_N\langle \phi_N | \chi_N \rangle$$

"After":

$$\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle = \overline{\alpha_1}\beta_1\langle \phi_1 | \chi_1 \rangle + \overline{\alpha_2}\beta_2\langle \phi_2 | \chi_2 \rangle + \cdots - \overline{\alpha_{j^*}}\beta_{j^*}\langle \phi_{j^*} | \chi_{j^*} \rangle + \cdots + \overline{\alpha_N}\beta_N\langle \phi_N | \chi_N \rangle$$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before":

$$\langle \psi_y^t | \psi_z^t \rangle = \overline{\alpha_1}\beta_1\langle \phi_1|\chi_1\rangle + \overline{\alpha_2}\beta_2\langle \phi_2|\chi_2\rangle + \cdots + \overline{\alpha_N}\beta_N\langle \phi_N|\chi_N\rangle$$

Each $|\phi_j\rangle$ is unit, and $\sum_j |\alpha_j|^2 = 1$.

"After":

$$\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle = \overline{\alpha_1}\beta_1\langle \phi_1|\chi_1\rangle + \overline{\alpha_2}\beta_2\langle \phi_2|\chi_2\rangle + \cdots - \overline{\alpha_{j^*}}\beta_{j^*}\langle \phi_{j^*}|\chi_{j^*}\rangle + \cdots + \overline{\alpha_N}\beta_N\langle \phi_N|\chi_N\rangle$$

$$\langle \psi_y^t | \psi_z^t \rangle - \langle \psi_y^{t+1} | \psi_z^{t+1} \rangle = 2\,\overline{\alpha_{j^*}}\beta_{j^*}\langle \phi_{j^*}|\chi_{j^*}\rangle \quad \Rightarrow \quad \left|\langle \psi_y^t | \psi_z^t \rangle - \langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq 2\,|\alpha_{j^*}| \cdot |\beta_{j^*}|$$

$R = \{ (y, z) : \mathrm{dist}(y, z) = 1 \} \subseteq Y \times Z$

$\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before":

$$\langle \psi_y^t | \psi_z^t \rangle = \overline{\alpha_1}\beta_1 \langle \phi_1 | \chi_1 \rangle + \overline{\alpha_2}\beta_2 \langle \phi_2 | \chi_2 \rangle + \cdots + \overline{\alpha_N}\beta_N \langle \phi_N | \chi_N \rangle$$

Each $|\phi_j\rangle$ is unit, and $\sum_j \left|\alpha_j\right|^2 = 1$.

"After":

$$\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle = \overline{\alpha_1}\beta_1 \langle \phi_1 | \chi_1 \rangle + \overline{\alpha_2}\beta_2 \langle \phi_2 | \chi_2 \rangle + \cdots - \overline{\alpha_{j^*}}\beta_{j^*} \langle \phi_{j^*} | \chi_{j^*} \rangle + \cdots + \overline{\alpha_N}\beta_N \langle \phi_N | \chi_N \rangle$$

(triangle inequality)

$$\left|\langle \psi_y^t | \psi_z^t \rangle\right| - \left|\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq \left|\langle \psi_y^t | \psi_z^t \rangle - \langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq 2\, \left|\alpha_{j^*}\right| \cdot \left|\beta_{j^*}\right|$$

$R = \{ (y, z) : \mathrm{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}\,|Y| + \sqrt{\frac{m'}{m}}\,|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

"Before":

$$\langle \psi_y^t | \psi_z^t \rangle = \overline{\alpha_1}\beta_1 \langle \phi_1 | \chi_1 \rangle + \overline{\alpha_2}\beta_2 \langle \phi_2 | \chi_2 \rangle + \cdots + \overline{\alpha_N}\beta_N \langle \phi_N | \chi_N \rangle$$

Each $|\phi_j\rangle$ is unit, and $\sum_j \left|\alpha_j\right|^2 = 1$.

"After":

$$\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle = \overline{\alpha_1}\beta_1 \langle \phi_1 | \chi_1 \rangle + \overline{\alpha_2}\beta_2 \langle \phi_2 | \chi_2 \rangle + \cdots - \overline{\alpha_{j^*}}\beta_{j^*} \langle \phi_{j^*} | \chi_{j^*} \rangle + \cdots + \overline{\alpha_N}\beta_N \langle \phi_N | \chi_N \rangle$$

$$\left|\langle \psi_y^t | \psi_z^t \rangle\right| - \left|\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq 2\,\left|\alpha_{j^*}\right| \cdot \left|\beta_{j^*}\right|$$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$ $\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate j^*

$$\left|\langle \psi_y^t | \psi_z^t \rangle\right| - \left|\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq 2\left|\alpha_{j^*}\right| \cdot \left|\beta_{j^*}\right|$$

A math trick: For any real a, b, and $h > 0$: $2ab \leq ha^2 + (1/h)b^2$

Proof 1: AM-GM inequality: ab is the geometric mean of ha^2 and $(1/h)b^2$

Proof 2: Certainly: $0 \leq \left(\sqrt{h}\,a - \sqrt{1/h}\,b\right)^2$

Expanding: $0 \leq ha^2 + (1/h)b^2 - 2ab$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate j^*

$$\left|\langle \psi_y^t | \psi_z^t \rangle\right| - \left|\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq 2 \left|\alpha_{j^*}\right| \cdot \left|\beta_{j^*}\right|$$

A math trick: For any real a, b, and $h > 0$: $2ab \leq ha^2 + (1/h)b^2$

Apply this above, with $a = \left|\alpha_{j^*}\right|,\ b = \left|\beta_{j^*}\right|,\ h = \sqrt{\frac{m}{m'}}$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

$$\left|\langle \psi_y^t | \psi_z^t \rangle\right| - \left|\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq \sqrt{\frac{m}{m'}} \left|\alpha_{j^*}\right|^2 + \sqrt{\frac{m'}{m}} \left|\beta_{j^*}\right|^2$$

A math trick: For any real a, b, and $h > 0$: $2ab \leq ha^2 + (1/h)b^2$

Apply this above, with $a = \left|\alpha_{j^*}\right|,\ b = \left|\beta_{j^*}\right|,\ h = \sqrt{\frac{m}{m'}}$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} |\langle \psi_y^t | \psi_z^t \rangle|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

$$|\langle \psi_y^t | \psi_z^t \rangle| - |\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle| \leq \sqrt{\frac{m}{m'}} \left|\alpha_{j^*}\right|^2 + \sqrt{\frac{m'}{m}} \left|\beta_{j^*}\right|^2$$

Finally, coordinate j^* really depends on the pair (y, z), so let's write it as

$j^*(y, z)$

$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z$

$$\text{Progress}_t = \sum_{(y,z)\in R} |\langle \psi_y^t | \psi_z^t \rangle|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$

Consider any pair $(y, z) \in R$

They differ on some coordinate j^*

$$|\langle \psi_y^t | \psi_z^t \rangle| - |\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle| \leq \sqrt{\frac{m}{m'}}\, |\alpha_{j^*(y,z)}|^2 + \sqrt{\frac{m'}{m}}\, |\beta_{j^*(y,z)}|^2$$

Finally, coordinate j^* really depends on the pair (y, z), so let's write it as

$j^*(y, z)$

$$R = \{ (y, z) : \text{dist}(y, z) = 1 \} \subseteq Y \times Z \qquad \text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \le \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and t+1 Consider any pair $(y, z) \in R$ They differ on some coordinate $j^*(y, z)$

$$\left|\langle \psi_y^t | \psi_z^t \rangle\right| - \left|\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \le \sqrt{\frac{m}{m'}} \left|\alpha_{j^*(y,z)}\right|^2 + \sqrt{\frac{m'}{m}} \left|\beta_{j^*(y,z)}\right|^2$$

Also, to be scrupulous about notation, the α_j's come from $|\psi_y^t\rangle$, and thus depend on y.

Similarly, the β_j's depend on z.

$$R = \{ (y, z) : \mathrm{dist}(y, z) = 1 \} \subseteq Y \times Z \qquad \text{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$$

Claim: $\text{Progress}_t - \text{Progress}_{t+1} \leq \sqrt{\frac{m}{m'}}|Y| + \sqrt{\frac{m'}{m}}|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate $j^*(y, z)$

$$\left|\langle \psi_y^t | \psi_z^t \rangle\right| - \left|\langle \psi_y^{t+1} | \psi_z^{t+1} \rangle\right| \leq \sqrt{\frac{m}{m'}} \left|\alpha_{j^*(y,z)}^{(y)}\right|^2 + \sqrt{\frac{m'}{m}} \left|\beta_{j^*(y,z)}^{(z)}\right|^2$$

Summing over all $(y, z) \in R$:

$$\text{Progress}_t - \text{Progress}_{t+1} \leq \sum_{(y,z)\in R} \sqrt{\frac{m}{m'}} \left|\alpha_{j^*(y,z)}^{(y)}\right|^2 + \sum_{(y,z)\in R} \sqrt{\frac{m'}{m}} \left|\beta_{j^*(y,z)}^{(z)}\right|^2$$

Final claim: $\sum_{(y,z)\in R} \left|\alpha_{j^*(y,z)}^{(y)}\right|^2 \leq |Y|$ (and similarly for the second term, completing the proof)

$R = \{\, (y, z) : \mathrm{dist}(y, z) = 1 \,\} \subseteq Y \times Z$

$\mathrm{Progress}_t = \sum_{(y,z)\in R} \left|\langle \psi_y^t | \psi_z^t \rangle\right|$

Claim: $\mathrm{Progress}_t - \mathrm{Progress}_{t+1} \le \sqrt{\frac{m}{m'}}\,|Y| + \sqrt{\frac{m'}{m}}\,|Z|$

Fix any t and $t+1$ Consider any pair $(y, z) \in R$ They differ on some coordinate $j^*(y, z)$

Final claim: $\sum_{(y,z)\in R} \left|\alpha_{j^*(y,z)}^{(y)}\right|^2 \le |Y|$

For each $y \in Y$, if you go over all z such that $(y, z) \in R$, the associated $j^*(y, z)$ are distinct.

So for each $y \in Y$, you're summing a *subset* of all possible $\left|\alpha_j^{(y)}\right|^2$. Which is at most 1.

So indeed the overall sum is at most $|Y|$. $\blacksquare$

[Ambainis ’00]

Super-Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, suppose $\boldsymbol{Y} \subseteq \text{YES}$, $\boldsymbol{Z} \subseteq \text{NO}$ are such that:

- for each $\boldsymbol{y} \in \boldsymbol{Y}$, there are at least m strings $\boldsymbol{z} \in \boldsymbol{Z}$ with $\text{dist}(y, z) = 1$
- for each $\boldsymbol{z} \in \boldsymbol{Z}$, there are at least m' strings $\boldsymbol{y} \in \boldsymbol{Y}$ with $\text{dist}(y, z) = 1$

Then $\text{Q}(\varphi)$, the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m'}$.

[Ambainis '00]

~~Super~~-Basic Adversary Method:

For φ = (YES, NO), suppose $\boldsymbol{Y} \subseteq$ YES, $\boldsymbol{Z} \subseteq$ NO are such that:

- for each $\boldsymbol{y} \in \boldsymbol{Y}$, there are at least m strings $\boldsymbol{z} \in \boldsymbol{Z}$ with dist($\boldsymbol{y}$, $\boldsymbol{z}$) = 1
- for each $\boldsymbol{z} \in \boldsymbol{Z}$, there are at least m' strings $\boldsymbol{y} \in \boldsymbol{Y}$ with dist($\boldsymbol{y}$, $\boldsymbol{z}$) = 1

Then Q(φ), the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m'}$.

[Ambainis '00]

Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, let $\boldsymbol{Y} \subseteq \text{YES}$, $\boldsymbol{Z} \subseteq \text{NO}$.

Let $R \subseteq \boldsymbol{Y} \times \boldsymbol{Z}$ be a set of "hard-to-distinguish" pairs, such that:

- for each $\boldsymbol{y} \in \boldsymbol{Y}$, there are at least m strings $\boldsymbol{z} \in \boldsymbol{Z}$ with $(\boldsymbol{y}, \boldsymbol{z}) \in R$
- for each $\boldsymbol{z} \in \boldsymbol{Z}$, there are at least m' strings $\boldsymbol{y} \in \boldsymbol{Y}$ with $(\boldsymbol{y}, \boldsymbol{z}) \in R$

Also, for each coordinate j, define $R_j = \{(\boldsymbol{y}, \boldsymbol{z}) \in R : \boldsymbol{y}_j \neq \boldsymbol{z}_j\}$

(namely, all the pairs distinguishable by querying coordinate j).

Assume:

- for each $\boldsymbol{y} \in \boldsymbol{Y}$ and j, there are at *most* ℓ strings $\boldsymbol{z} \in \boldsymbol{Z}$ with $(\boldsymbol{y}, \boldsymbol{z}) \in R_j$
- for each $\boldsymbol{z} \in \boldsymbol{Z}$ and j, there are at *most* ℓ' strings $\boldsymbol{y} \in \boldsymbol{Y}$ with $(\boldsymbol{y}, \boldsymbol{z}) \in R_j$

Then $Q(\varphi)$, the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m' / \ell\, \ell'}$.

Proof: Exercise!

(Only tiny modifications needed to the proof we saw.)

Exercise #2: Recall that Grover Search only needs $\lesssim \sqrt{N/k}$ queries to find a 1 if it's promised there are at least k 1's. (Assume $k \leq N/2$.)

Use the Basic Adversary Method to show $\gtrsim \sqrt{N/k}$ queries are necessary for the promise problem:

$\varphi =$ "decide if w has no 1's, or at least k 1's".

Basic Adversary Method:

For $\varphi = (\text{YES}, \text{NO})$, let $Y \subseteq \text{YES}$, $Z \subseteq \text{NO}$.

Let $R \subseteq Y \times Z$ be a set of "hard-to-distinguish" pairs, such that:

- for each $y \in Y$, there are at least m strings $z \in Z$ with $(y, z) \in R$
- for each $z \in Z$, there are at least m' strings $y \in Y$ with $(y, z) \in R$

Also, for each coordinate j, define $R_j = \{(y, z) \in R : y_j \neq z_j\}$

(namely, all the pairs distinguishable by querying coordinate j).

Assume:

- for each $y \in Y$ and j, there are at *most* ℓ strings $z \in Z$ with $(y, z) \in R_j$
- for each $z \in Z$ and j, there are at *most* ℓ' strings $y \in Y$ with $(y, z) \in R_j$

Then $Q(\varphi)$, the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m' / \ell\, \ell'}$.

General ("Negative-Weights") Adversary Method:

For φ = (YES, NO), let $Y \subseteq$ YES, $Z \subseteq$ NO.

Let $R \subseteq Y \times Z$ be a set of "hard-to-distinguish" pairs, such that:

- for each $y \in Y$, there are at least m strings $z \in Z$ with $(y, z) \in R$
- for each $z \in Z$, there are at least m' strings $y \in Y$ with $(y, z) \in R$

Also, for each coordinate j, define $R_j = \{(y, z) \in R : y_j \neq z_j\}$

(namely, all the pairs distinguishable by querying coordinate j).

Assume:

- for each $y \in Y$ and j, there are at *most* ℓ strings $z \in Z$ with $(y, z) \in R_j$
- for each $z \in Z$ and j, there are at *most* ℓ' strings $y \in Y$ with $(y, z) \in R_j$

Then Q(φ), the quantum query complexity of φ, is $\gtrsim \sqrt{m\, m' / \ell\, \ell'}$.

General ("Negative-Weights") Adversary Method:

A story for another time!