Quantum query complexity

Lecture 3

The recording method

Materials: https://yassine-hamoudi.github.io/pcmi2023/

Focus of this lecture

- In this lecture, the input is a non-Boolean vector

$$x \in \{0,\ldots,n-1\}^n$$ (vs. $x \in \{0,1\}^n$ in the other lectures)

drawn uniformly at random.

- We care about average-case analysis (vs. worst-case in the other lectures)

- This setup is important in cryptography, where x models an ideal hash function $x : \{1,\ldots,n\} \rightarrow \{0,\ldots,n-1\}$ (the "Random Oracle Model")

Classical recording method

A straightforward (yet useful) lower bound method that consists of sampling and recording the input on-the-fly

At the beginning: $x = (\emptyset, \emptyset, \ldots, \emptyset)$

Whenever i is queried:

- if $x_i \neq \emptyset$ then return x_i
- if $x_i = \emptyset$ then sample $y \sim \{0, \ldots, n-1\}$, record $x_i \leftarrow y$ and return y

SEARCH problem: Find i such that $x_i = 1$

Randomized algorithm

Input

$x = (\emptyset, \emptyset, \emptyset, \emptyset)$

$\xrightarrow{x_2?}$

$\xleftarrow{x_2 = 2}$

$x = (\emptyset, 2, \emptyset, \emptyset)$

$\xrightarrow{x_1?}$

$\xleftarrow{x_1 = 0}$

$x = (0, 2, \emptyset, \emptyset)$

$\xrightarrow{x_4?}$

$\xleftarrow{x_4 = 1}$

$x = (0, 2, \emptyset, 1)$

$\xrightarrow{x_1?}$

$\xleftarrow{x_1 = 0}$

$x = (0, 2, \emptyset, 1)$

If it want to succeeds, the algorithm must essentially wait until 1 is present in the record

$\Delta_t = \Pr(1 \in \text{record after} \leq t \text{ queries})$

- $\Delta_0 = 0$ *(initial condition)*
- $\Delta_{t+1} \leq \Delta_t + 1/n$ *(evolution)*

$\Rightarrow T = \Omega(n)$ queries for $\Delta_T \geq 2/3$

Quantum recording method

(a.k.a. compressed oracles)

Obstacle to quantum recording

Quantum algorithm

Input

$x = (\emptyset, \emptyset, \emptyset, \emptyset)$

$$\frac{1}{\sqrt{n}} \sum_i |i, 0\rangle \ ?$$

$\longrightarrow$

$x = (2,\ 0,\ 2,\ 1)$

$\longleftarrow$

$$\frac{1}{\sqrt{n}} \sum_i |i, x_i\rangle$$

Query all indices at the same time, in superposition.

The record is full after just 1 query!

Construction

We construct a "quantum way" of recording queries:

1. Purification of the input

2. Definition of the quantum sampling operator

3. Definition of the quantum recording operator

Quantum query operator

Binary alphabet

$b, x_i \in \{0,1\}$

$O_x |i, b\rangle = |i, b \oplus x_i\rangle$

$\updownarrow$ same query complexity (cf Problem Session 1)

$O_x^{\pm} |i, b\rangle = (-1)^{b \cdot x_i} |i, b\rangle$

Larger alphabet

$b, x_i \in \{0,1,\ldots,n-1\}$

$O_x |i, b\rangle = |i, b + x_i \bmod n\rangle$

$\updownarrow$

$$\boxed{O_x^{\pm} |i, b\rangle = \omega^{b \cdot x_i} |i, b\rangle}$$

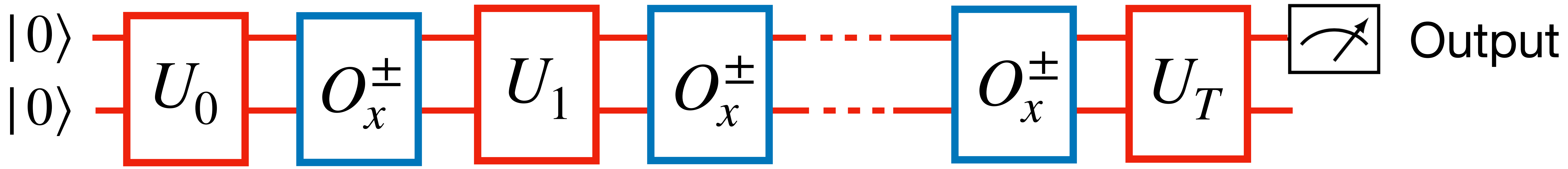
where $\omega = e^{2i\pi/n}$ is the n-th root of unity

1. Purification of the input

The state of an algorithm after t queries is:

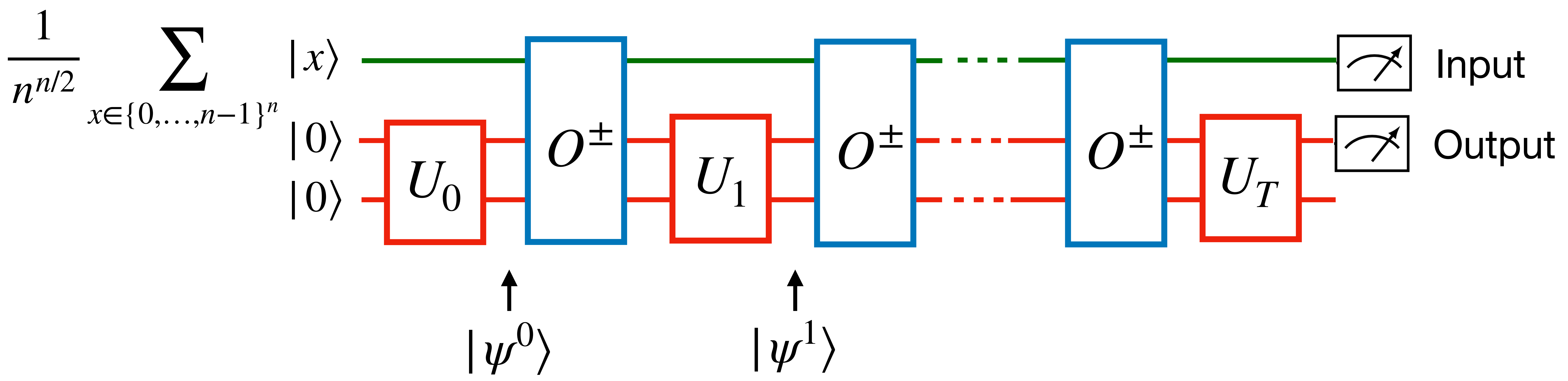
$$|\psi_x^t\rangle = U_t O_x^{\pm} U_{t-1} O_x^{\pm} \dots U_0 |0,0\rangle$$

where $O_x^{\pm}|i,b\rangle = \omega^{b\cdot x_i}|i,b\rangle$



1. Purification of the input

We add a register that contains a purification of the uniform input distribution



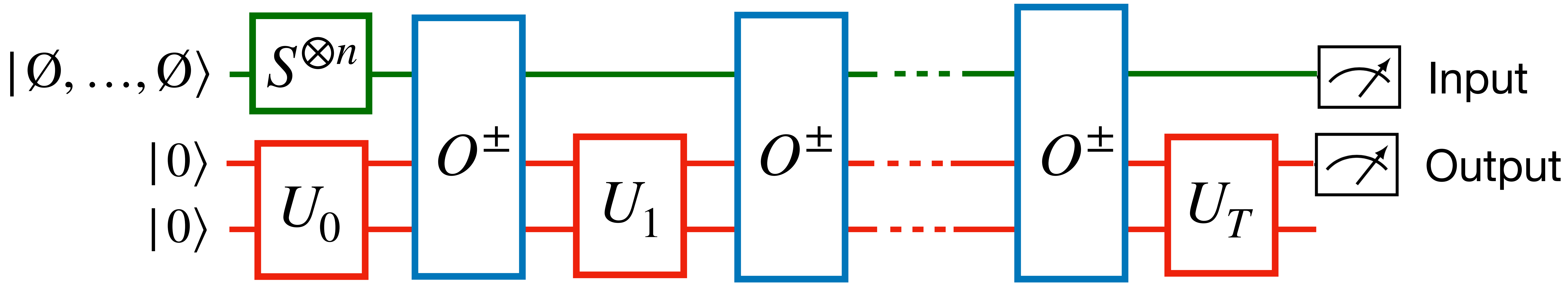
Mathematically,

$$O^{\pm}(|x\rangle \otimes |i,b\rangle) = |x\rangle \otimes O_x^{\pm}|i,b\rangle = \omega^{bx_i}|x\rangle \otimes |i,b\rangle$$

$$|\psi^t\rangle = \frac{1}{n^{n/2}} \sum_{x \in \{0,\ldots,n-1\}^n} |x\rangle \otimes |\psi_x^t\rangle$$

2. Quantum sampling operator

We start with an empty record and immediately "sample" all coordinates:



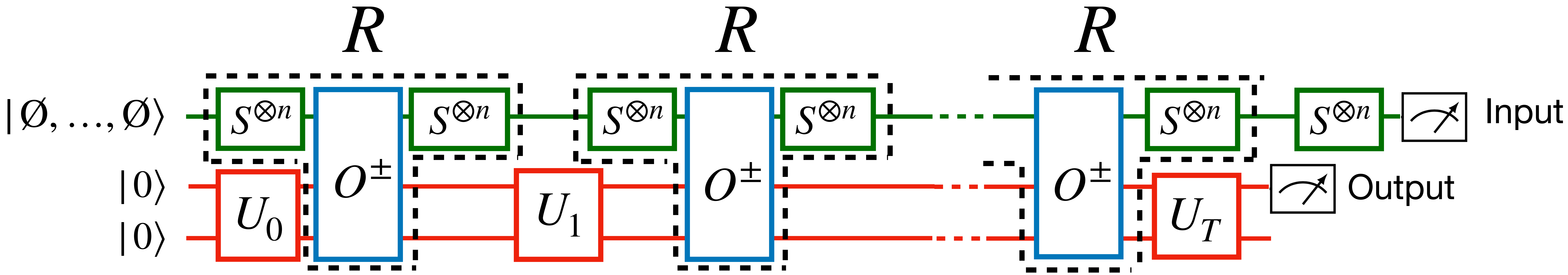
Sampling operator:

$$\textcolor{red}{S}\,|\varnothing\rangle = \frac{1}{\sqrt{n}} \sum_{0 \le y < n} |y\rangle$$

(extended into a unitary Hermitian operator)

3. Quantum recording operator

We "split" the identity into $\mathrm{Id} = S^{\otimes n} S^{\otimes n}$ after each query:



Sampling operator:

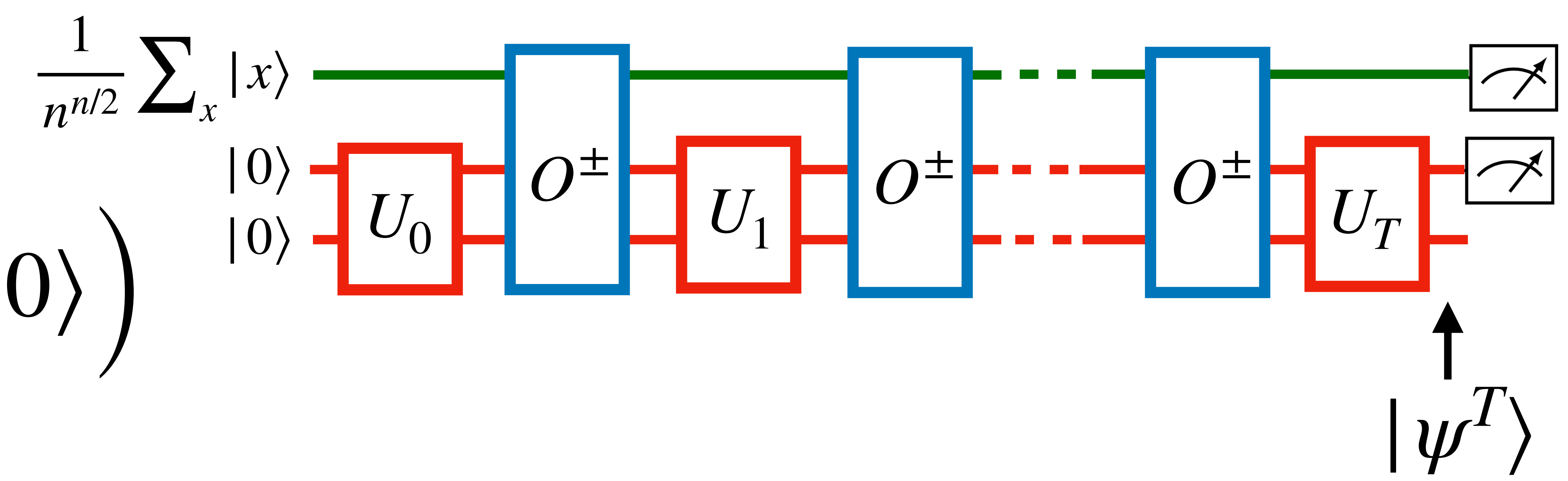
$$S|\varnothing\rangle = \frac{1}{\sqrt{n}} \sum_{0 \le y < n} |y\rangle$$

Recording operator:

$$R = (S^{\otimes n} \otimes \mathrm{Id})\, O^{\pm}\, (S^{\otimes n} \otimes \mathrm{Id})$$

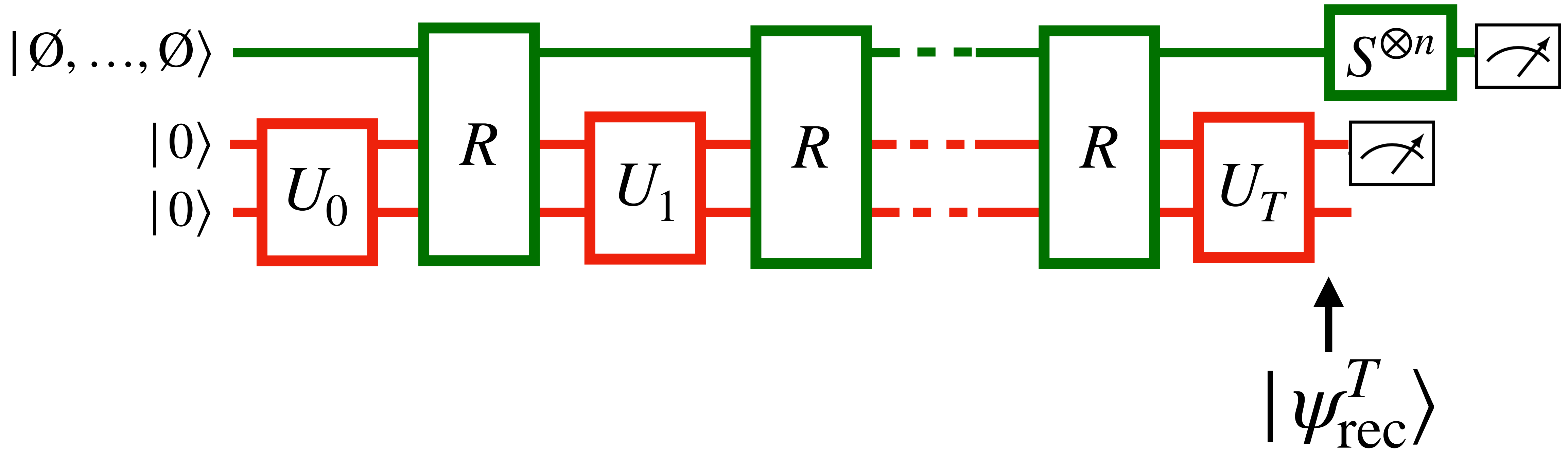
Standard query model:

$$|\psi^T\rangle = U_T O^{\pm} U_{T-1} O^{\pm} \ldots U_0 \Big(\frac{1}{n^{n/2}} \sum_x |x\rangle \otimes |0,0\rangle \Big)$$



Recording query model:

$$|\psi^T_{\text{rec}}\rangle = U_T R U_{T-1} R \ldots U_0 \big(|\emptyset, \ldots, \emptyset\rangle \otimes |0,0\rangle \big)$$



By construction: $|\psi^t\rangle = (S^{\otimes n} \otimes \text{Id}) |\psi^t_{\text{rec}}\rangle$

What did we gain from this construction?

R behaves as classical recording, up to low-error terms

<u>Proposition:</u> When $b \neq 0$, the recording query operator R acts as:

$$R\,|\ldots, x_{i-1}, \emptyset, x_{i+1}, \ldots\rangle \otimes |i, b\rangle \;=\; |\ldots, x_{i-1}\rangle \left(\frac{1}{\sqrt{n}} \sum_{0 \le y < n} \omega^{by} |y\rangle \right) |x_{i+1}, \ldots\rangle \otimes |i, b\rangle$$

$$R\,|\ldots, x_{i-1}, y, x_{i+1}, \ldots\rangle \otimes |i, b\rangle \;=\; |\ldots, x_{i-1}\rangle \left(\omega^{by} |y\rangle + |\mathrm{error}_y\rangle \right) |x_{i+1}, \ldots\rangle \otimes |i, b\rangle$$

where $|\mathrm{error}_y\rangle = \dfrac{\omega^{by}}{\sqrt{n}} |\emptyset\rangle + \displaystyle\sum_{0 \le z < n} \frac{1 - \omega^{by} - \omega^{bz}}{n} |z\rangle$

Application to Search

SEARCH problem: Find i such that $x_i = 1$

Recall the classical progress measure: $\Delta_t = \Pr(1 \in \text{record after} \leq t \text{ queries})$

We extend it to quantum states and quantum recording:

$$\Pi = \left(\sum_{1 \in x} |x\rangle\langle x|\right) \otimes \mathrm{Id} \qquad \Delta_t = \| \Pi \, | \psi^t_{\mathrm{rec}} \rangle \|^2$$

(projects onto states containing 1 in the input record)

Lemma 1: $\Delta_0 = 0$

Lemma 2: $\sqrt{\Delta_{t+1}} \leq \sqrt{\Delta_t} + \sqrt{10/n}$ ← Note the square roots. This is where it differs from classical recording!

$\Rightarrow T = \Omega(\sqrt{n})$ queries for $\Delta_T \geq 2/3$