Lower bounds on quantum query complexity Part I

Marc Kaplan
Telecom ParisTech - University of Edinburgh

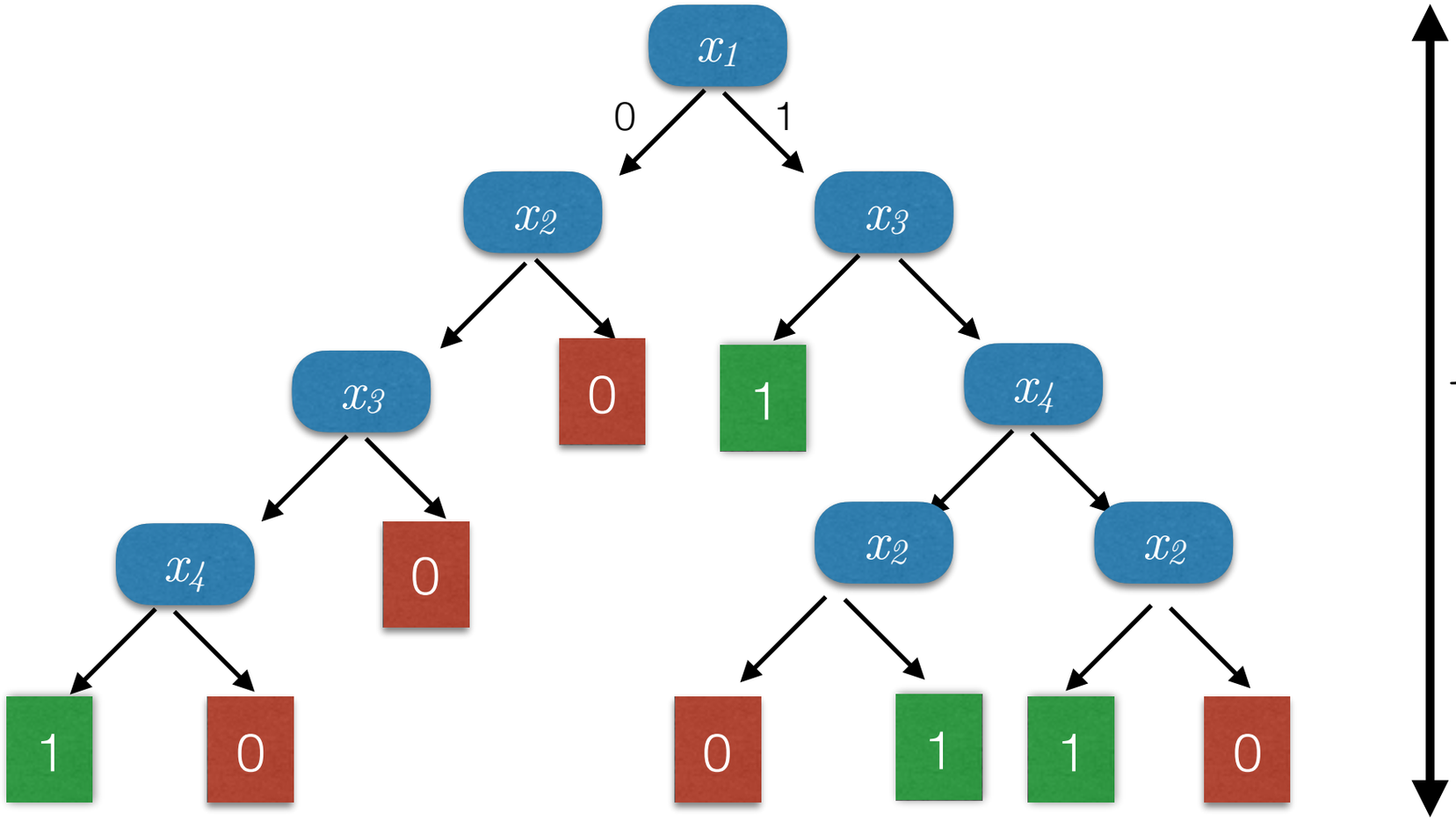
Decision Tree

- Input x in $\{0,1\}^n$

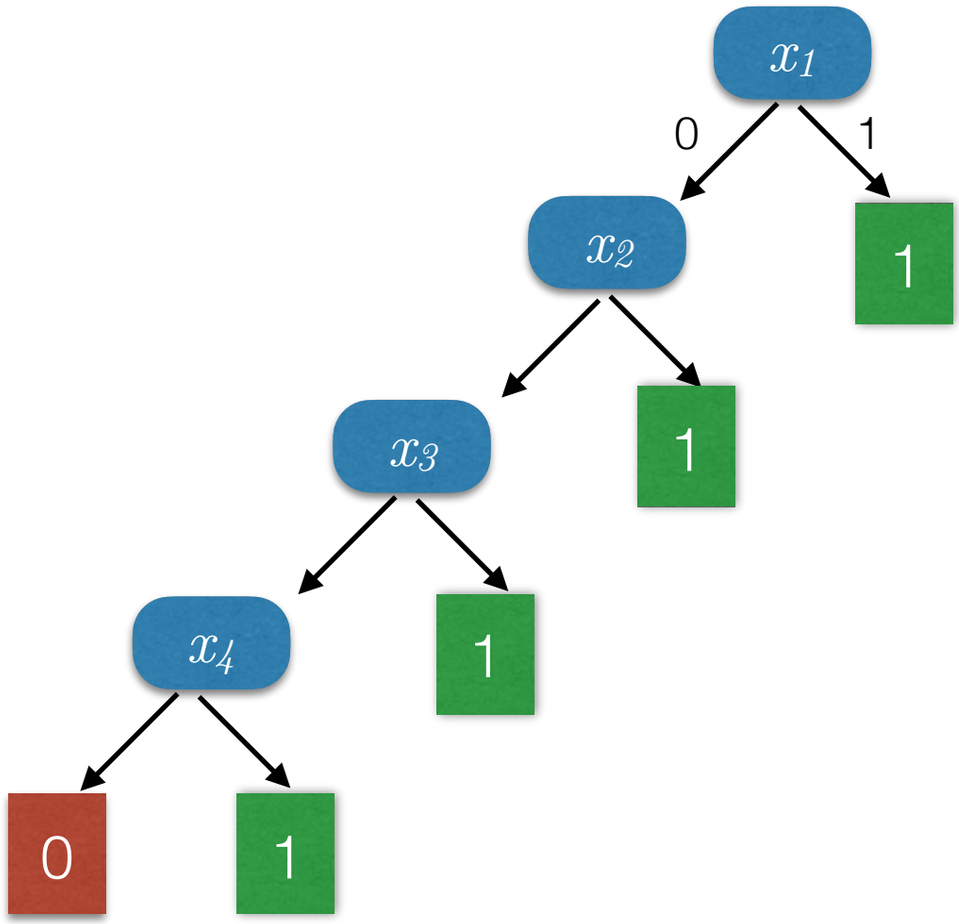
- $f(x)$: a question about x

- x is read through queries of the form: $i \rightarrow x_i$

Decision Tree



Decision Tree

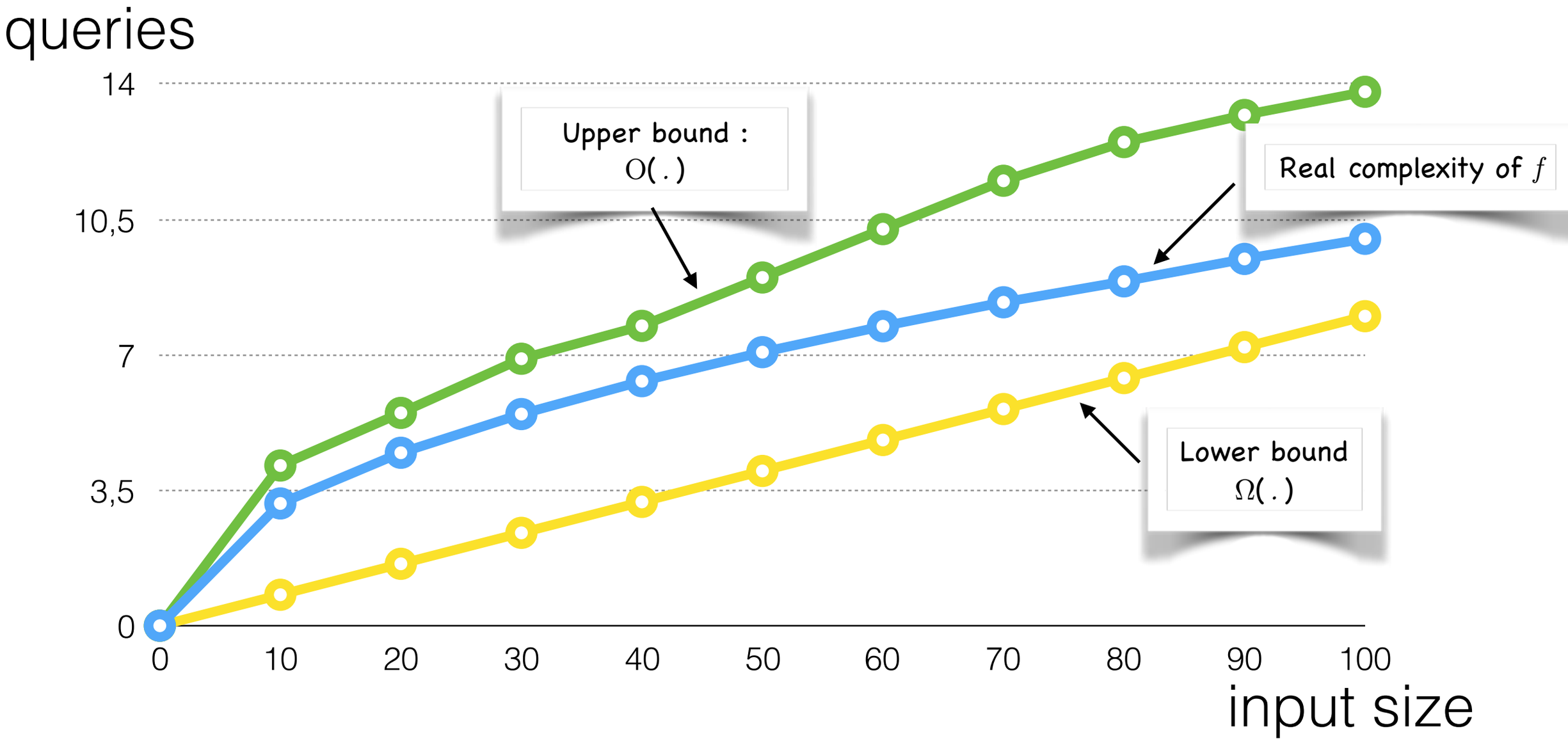


Computes the OR function

Quantum Query Complexity

- Unstructured search (OR function)
    - Given x in $\{0,1\}^n$, $f(x)=1$ iff there exists i s.t. $x_i=1$
        - Grover's algorithm: $n^{1/2}$ quantum queries to x
- Element distinctness
    - Given x in $[M]^n$, $f(x)=1$ iff there exists (i,j) s.t. $x_i=x_j$
    - Ambainis' algorithm: $n^{2/3}$ quantum queries to x

Lower bounds

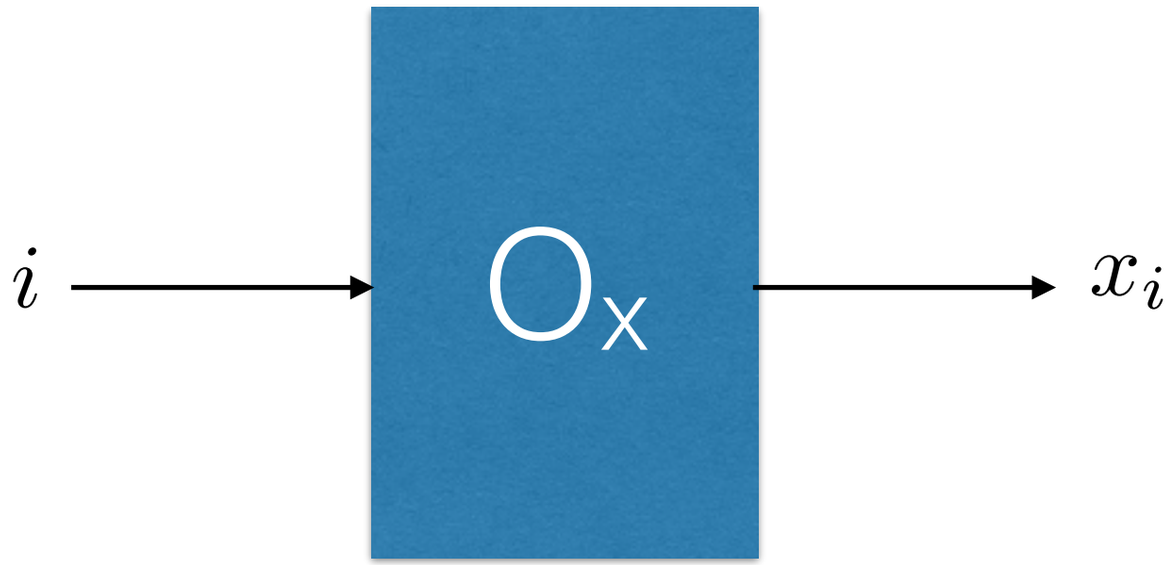


It’s possible to prove lower bounds on query complexity!

Lower bounds

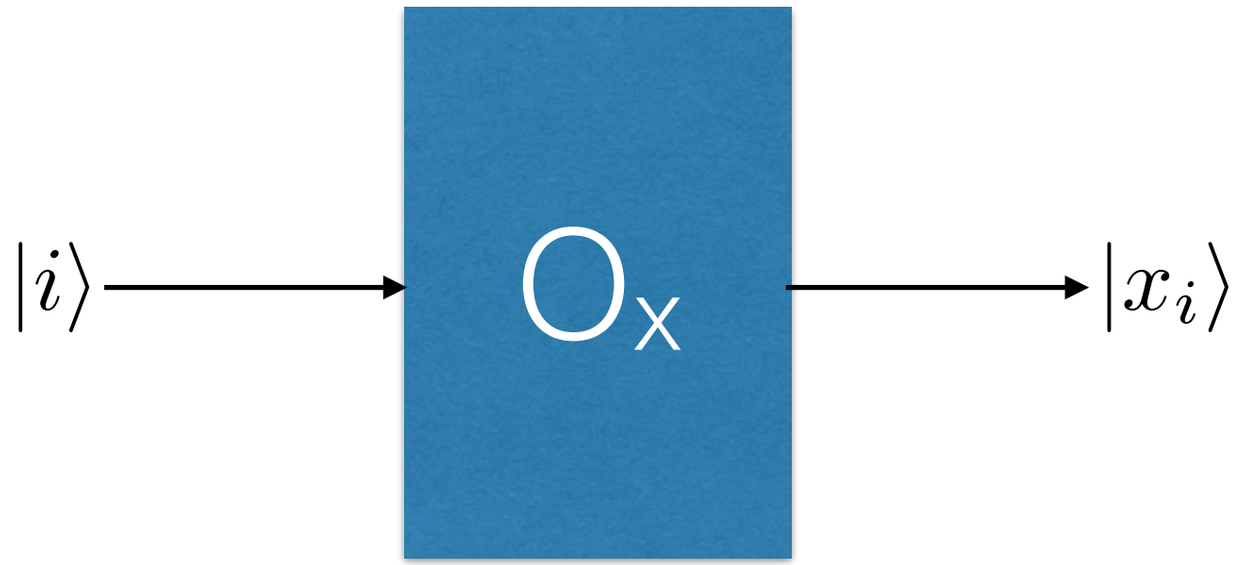
- We focus on Lower Bound **Methods**
    - Polynomial method
    - Adversary method

From classical to quantum queries

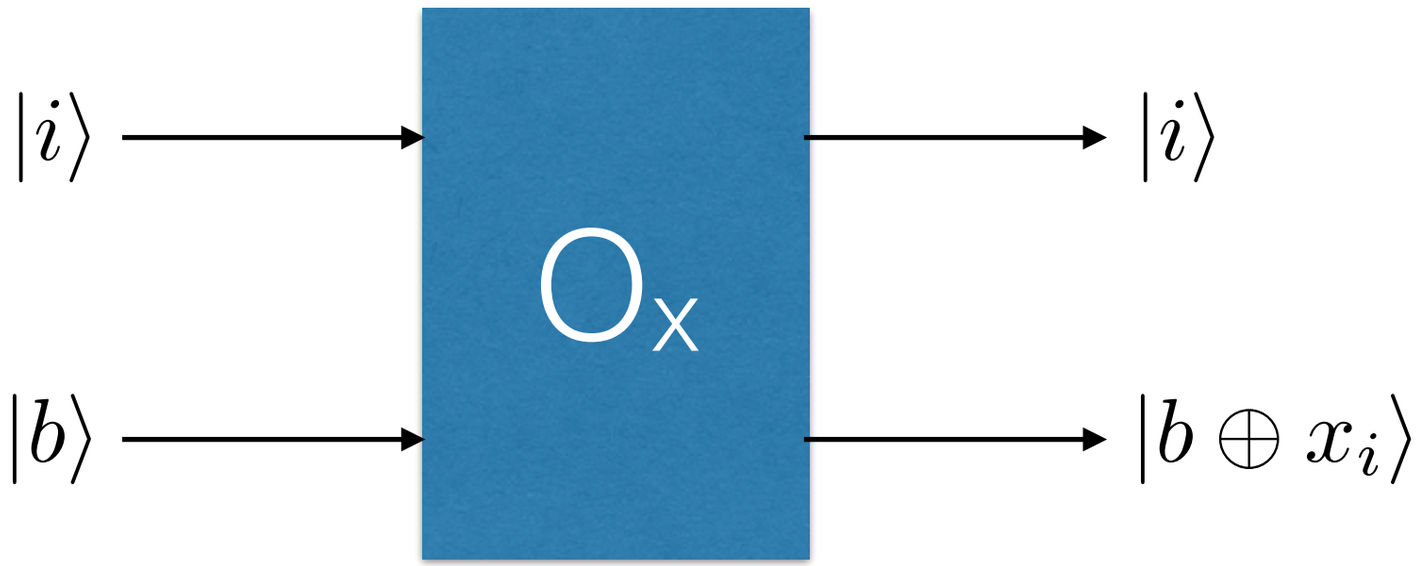


- The input is given as a black box
- Complexity = number of queries to the box

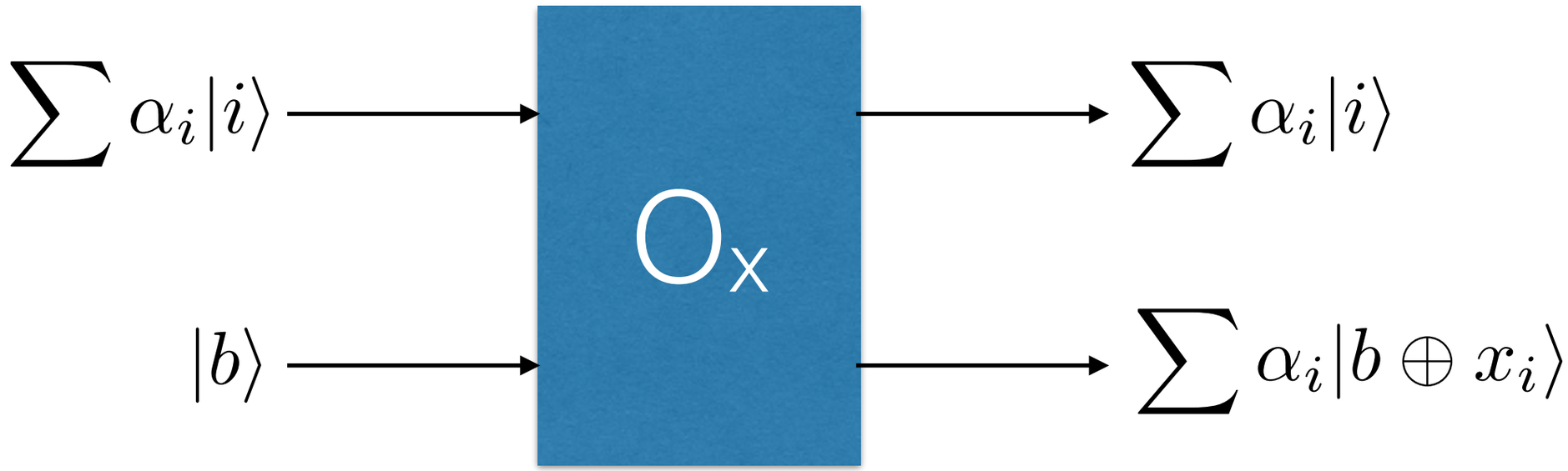
From classical to quantum queries



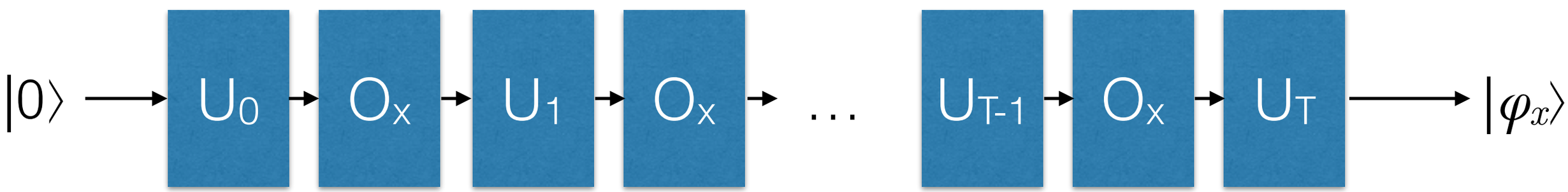
From classical to quantum queries



From classical to quantum queries



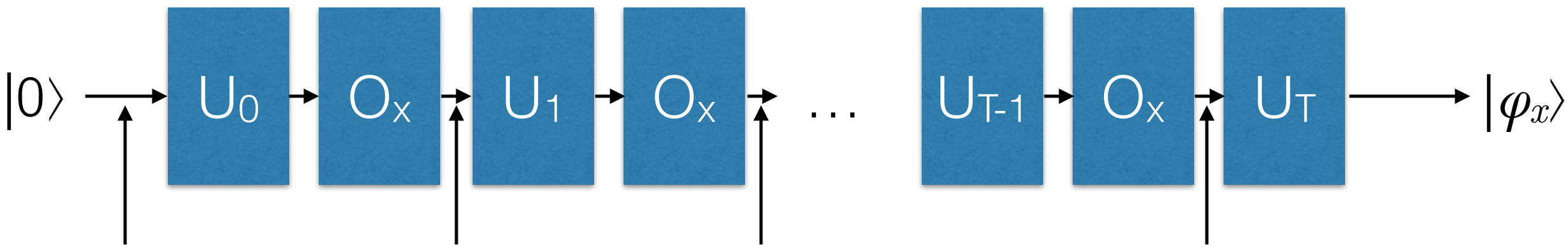
Quantum query circuit



One big unitary transform

- Measuring $|\varphi_x\rangle$ returns $f(x)$ with high probability
- $Q_\varepsilon(f) = T$
- Lower bound on time complexity

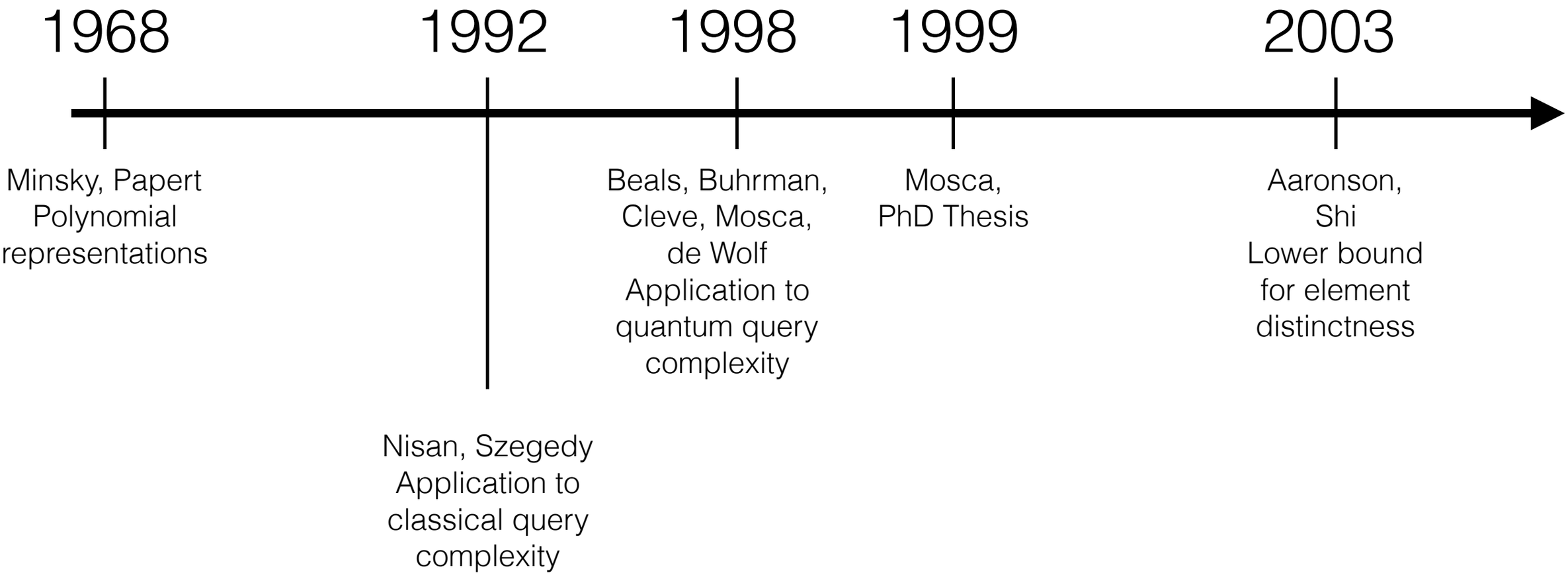
Quantum query circuit



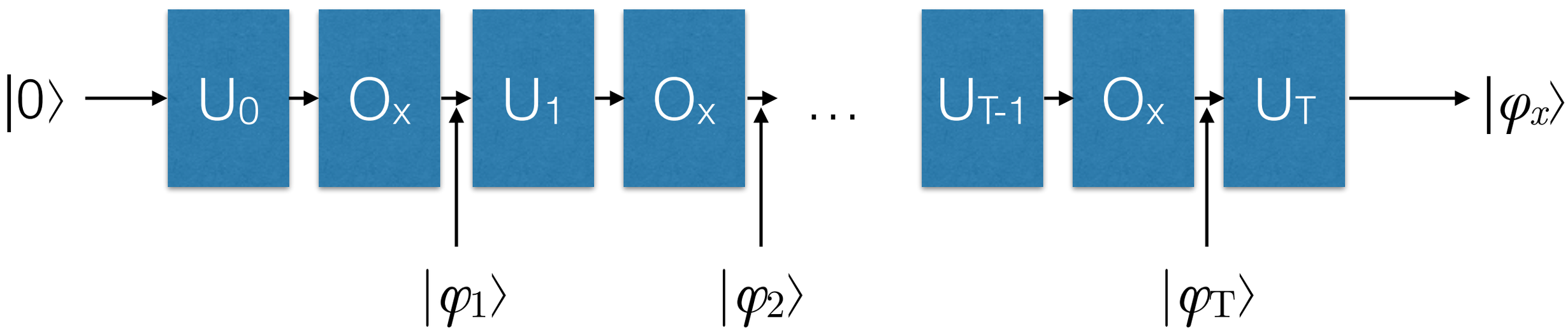
- Q_i : a quantity that grows like the number of queries.

The polynomial method

History of the Polynomial method

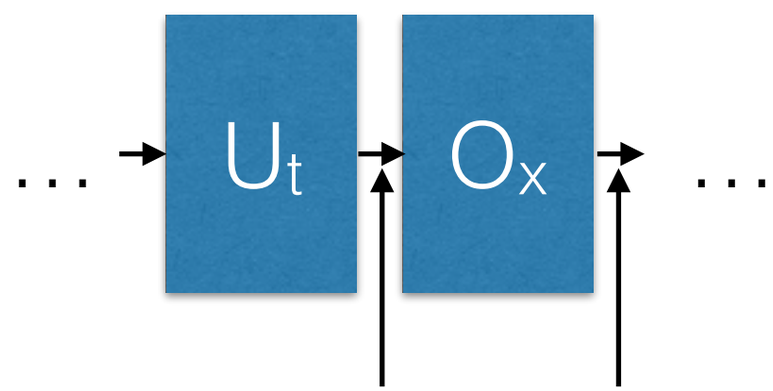


Quantum query circuit



Follow the evolution of the internal state of the algorithm

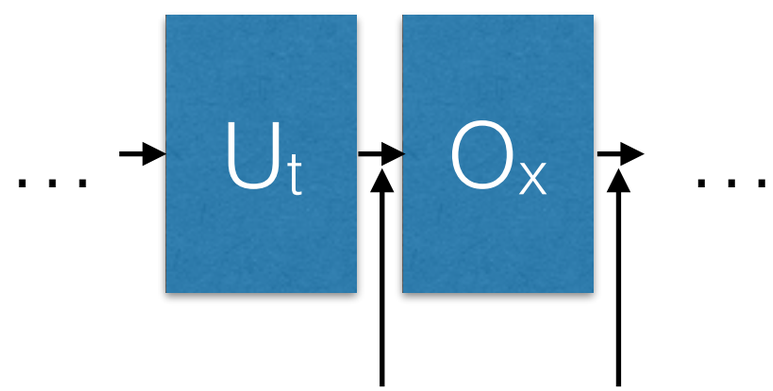
Quantum query circuit



$$|\psi\rangle \qquad |\varphi_t\rangle$$

$$|\psi\rangle = \sum_{i,b,w} P_{i,b,w}|i\rangle|b\rangle|w\rangle$$

Quantum query circuit



$|\psi\rangle \qquad |\varphi_t\rangle$

$$|\psi\rangle = \sum_{i,b,w} P_{i,b,w} |i\rangle|b\rangle|w\rangle$$

<u>Key idea</u>

The coefficients are polynomials of degree at most t-1

Quantum query circuit

$$|\psi\rangle = \sum_{i,b,w} P_{i,b,w} \overbrace{|i\rangle|b\rangle}|w\rangle$$

Query registers

Workging register

$$|\varphi_t\rangle = \sum_{i,b,w} P_{i,b,w}|i\rangle|b \oplus x_i\rangle|w\rangle$$

Quantum query circuit

$$|\varphi_t\rangle = \sum_{i,b,w} P_{i,b,w}|i\rangle|b \oplus x_i\rangle|w\rangle$$

$$P_{i,0,w}|i\rangle|0\rangle + P_{i,1,w}|i\rangle|1\rangle \quad \text{If } x_i = 0$$

$$P_{i,1,w}|i\rangle|0\rangle + P_{i,0,w}|i\rangle|1\rangle \quad \text{If } x_i = 1$$

$$\sum_b [(1 - x_i)P_{i,b,w} + x_i P_{i,1-b,w}]|i\rangle|b\rangle$$

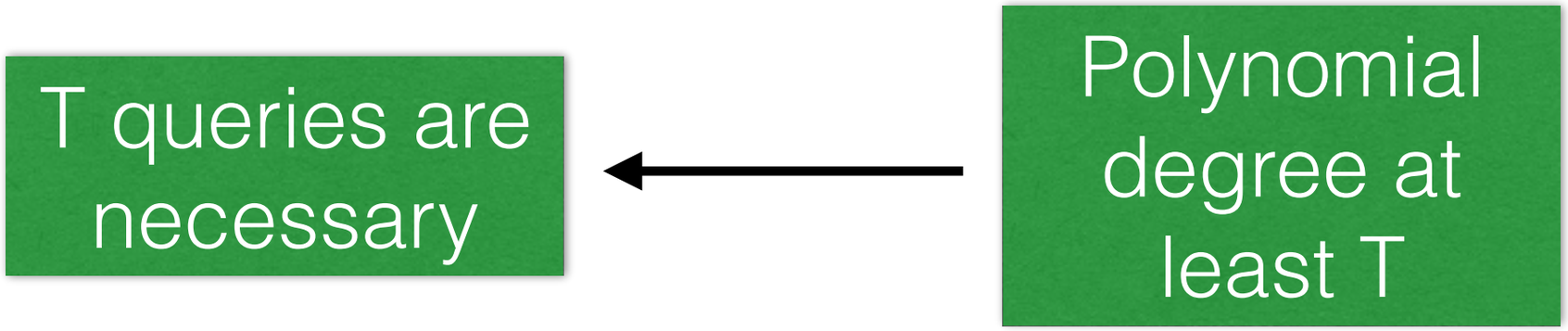
The variables of the polynomial (multilinear)

Polynomial method

T queries are sufficient → Polynomial degree at most T

$$\widetilde{deg}(f) \leq 2T$$

Polynomial method



$$Q_\varepsilon(f) \geq \frac{\widetilde{deg}(f)}{2}$$

Applying the polynomial method: the OR function

$$x = (x_1, \ldots, x_n)$$

$$f(x) = x_1 \vee \ldots \vee x_n$$

Summary of the proof

To lower bound the degree

- Symmetrize the function to make it univariate
- Prove a lower bound on the degree of a univariate polynomial

Symmetrization (Minsky, Papert)

$$f^{sym}(x) = \frac{\sum_{\pi \in S_n} f(\pi(x))}{n!}$$

Theorem:

if f is a degree T mutlilinear polynomial, then there exists a univariate polynomial g of degree at most T such that:

$$g(|x|) = f^{sym}(x)$$

Symmetrization (Minsky, Papert)

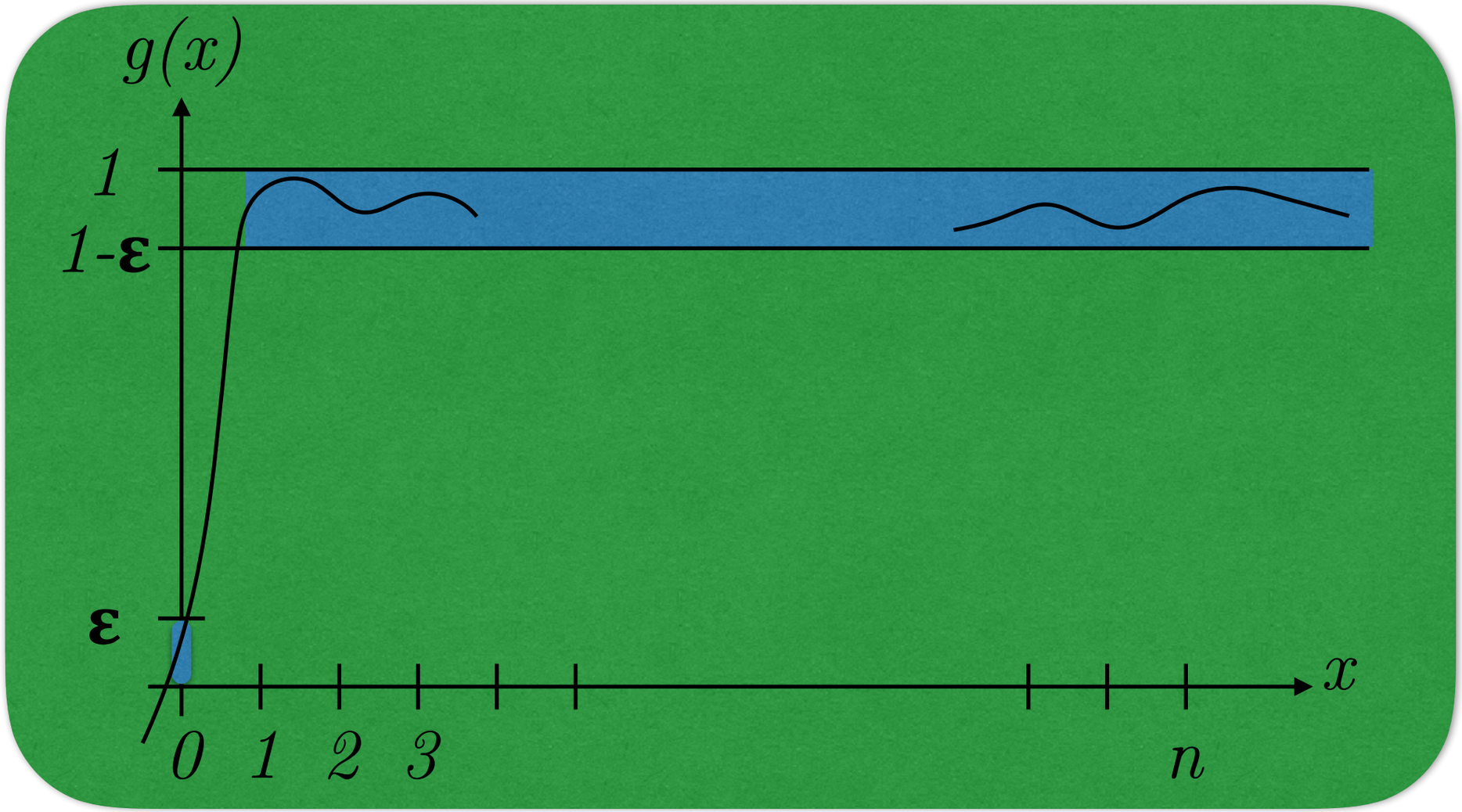
$$f^{sym}(x) = \frac{\sum_{\pi \in S_n} f(\pi(x))}{n!}$$

Proof sketch

- $f^{sym} = c_0 + c_1 V_1 + \ldots + c_n V_n$, where V_i is the sum of all degree i monomials

$$g(|x|) = c_0 + c_1 \binom{|x|}{1} + \ldots + c_n \binom{|x|}{n}$$

Lower bound for univariate polynomials (Paturi, 92)



$$\deg(f) = \Omega(\sqrt{n})$$

Applying the polynomial method: Maximum gap for total function

For a total function f : $D(f) \leq O(\widetilde{def}(f)^6)$

$$\downarrow$$

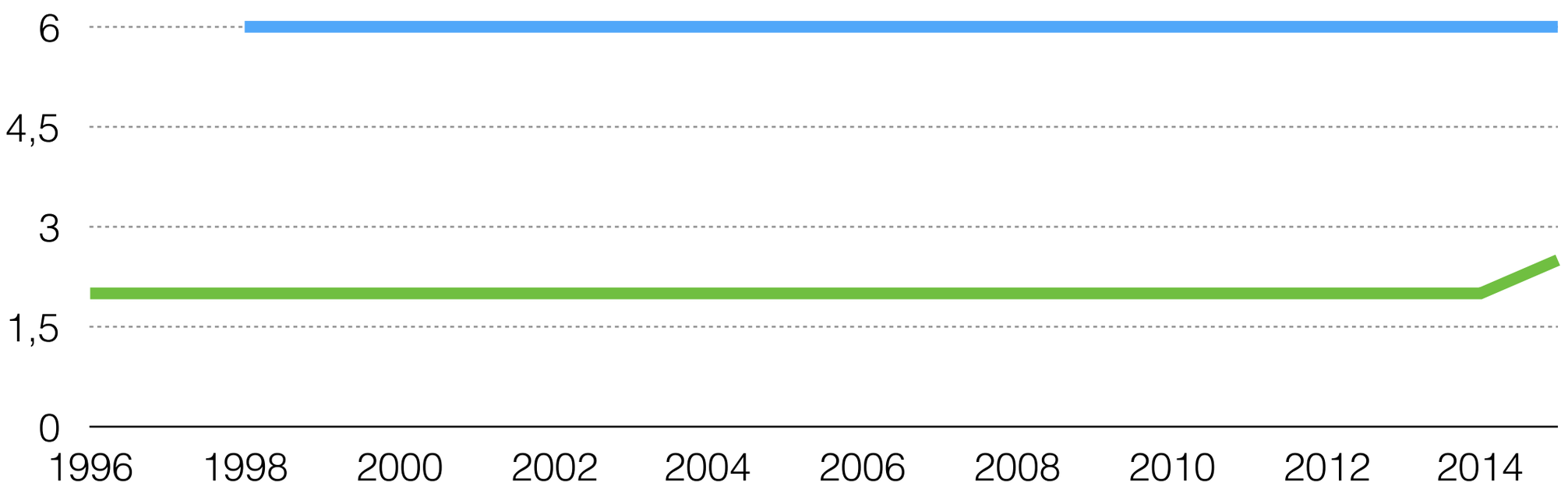
$$D(f) = O(\widetilde{deg}(f)^6)$$

Maximum gap for total function

1996: $D(OR_n) = Q_\varepsilon(OR_n)^2$

1998: $Q_\varepsilon(f) \leq D(f) \leq O(Q_\varepsilon(f)^6)$

2015: $\Omega(R_\varepsilon(f)) = \Omega(Q_\varepsilon(f)^{2.5})$



Other applications

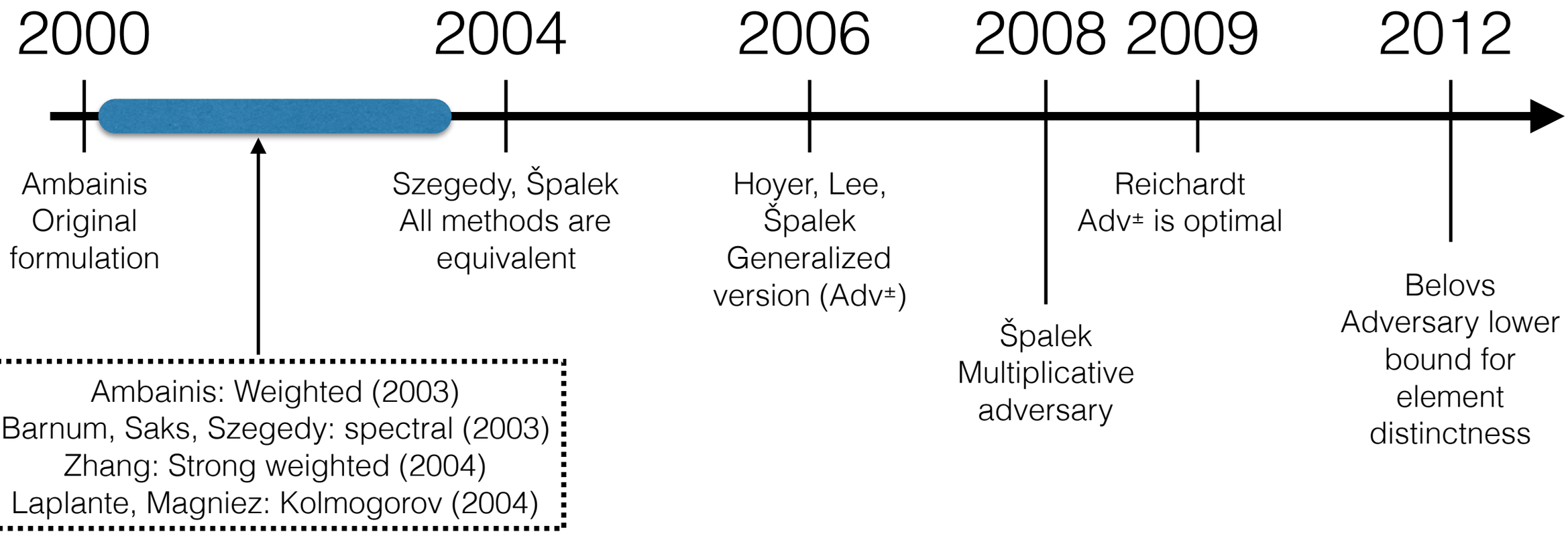
- Aaronson, Shi: $n^{2/3}$ Lower bound on Element Distinctness

- Various functions: statistics, threshold functions, read-once formulas, etc…

- Extension to communication complexity

The Adversary method

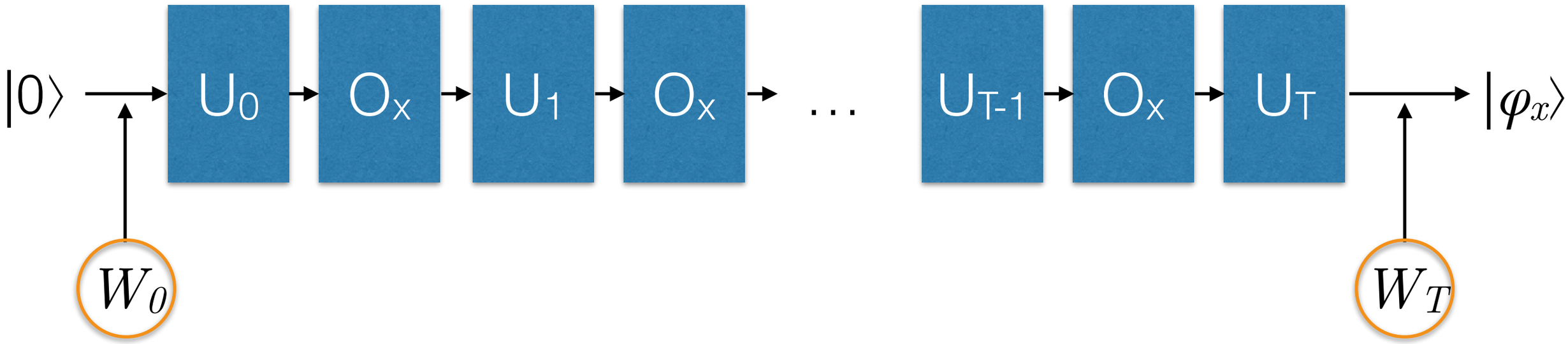
History of the Adversary method



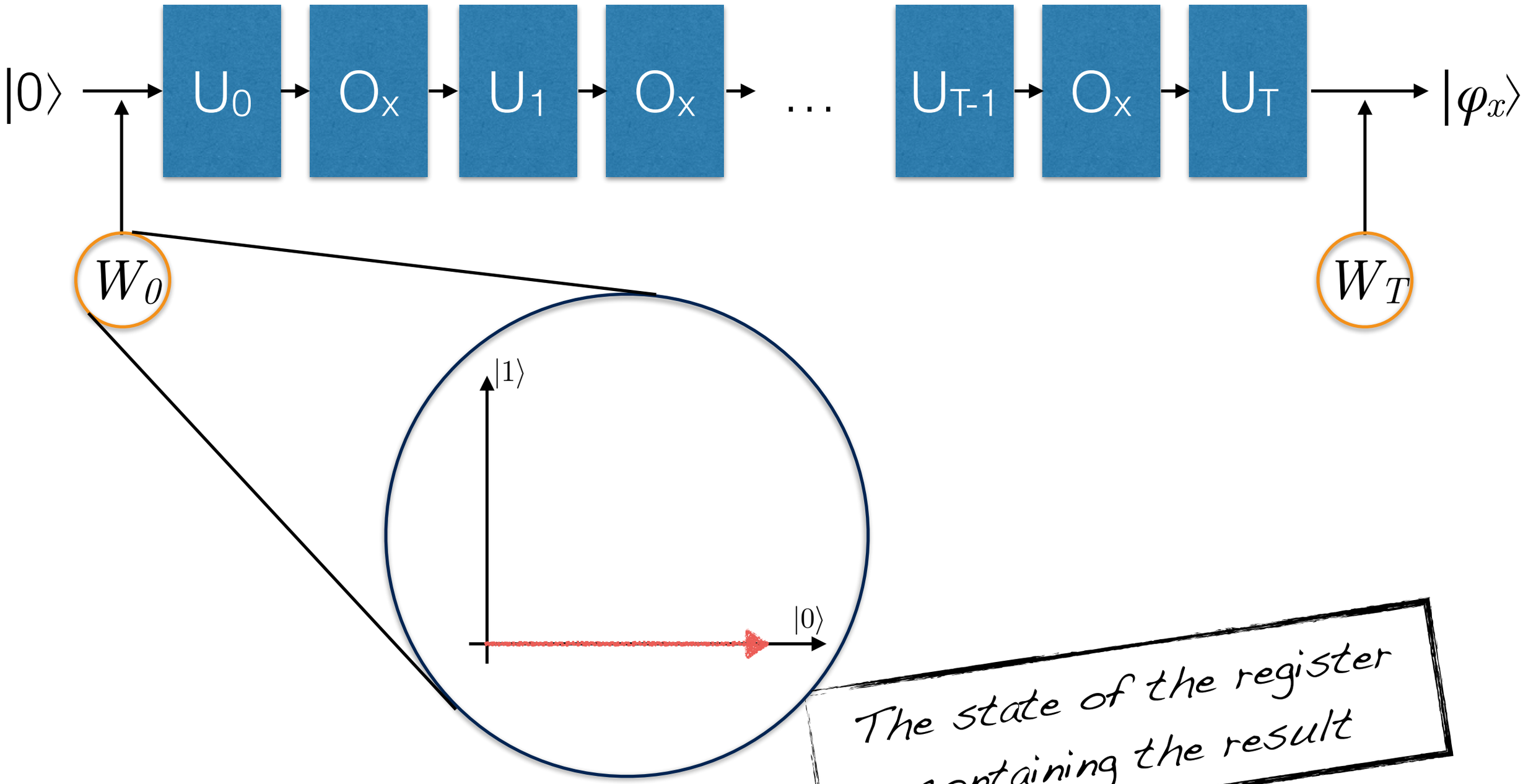
Adversary method(s)

- Original adversary method
- Weighted adversary method
- Spectral adversary method
- Generalized adversary method

Adversary method

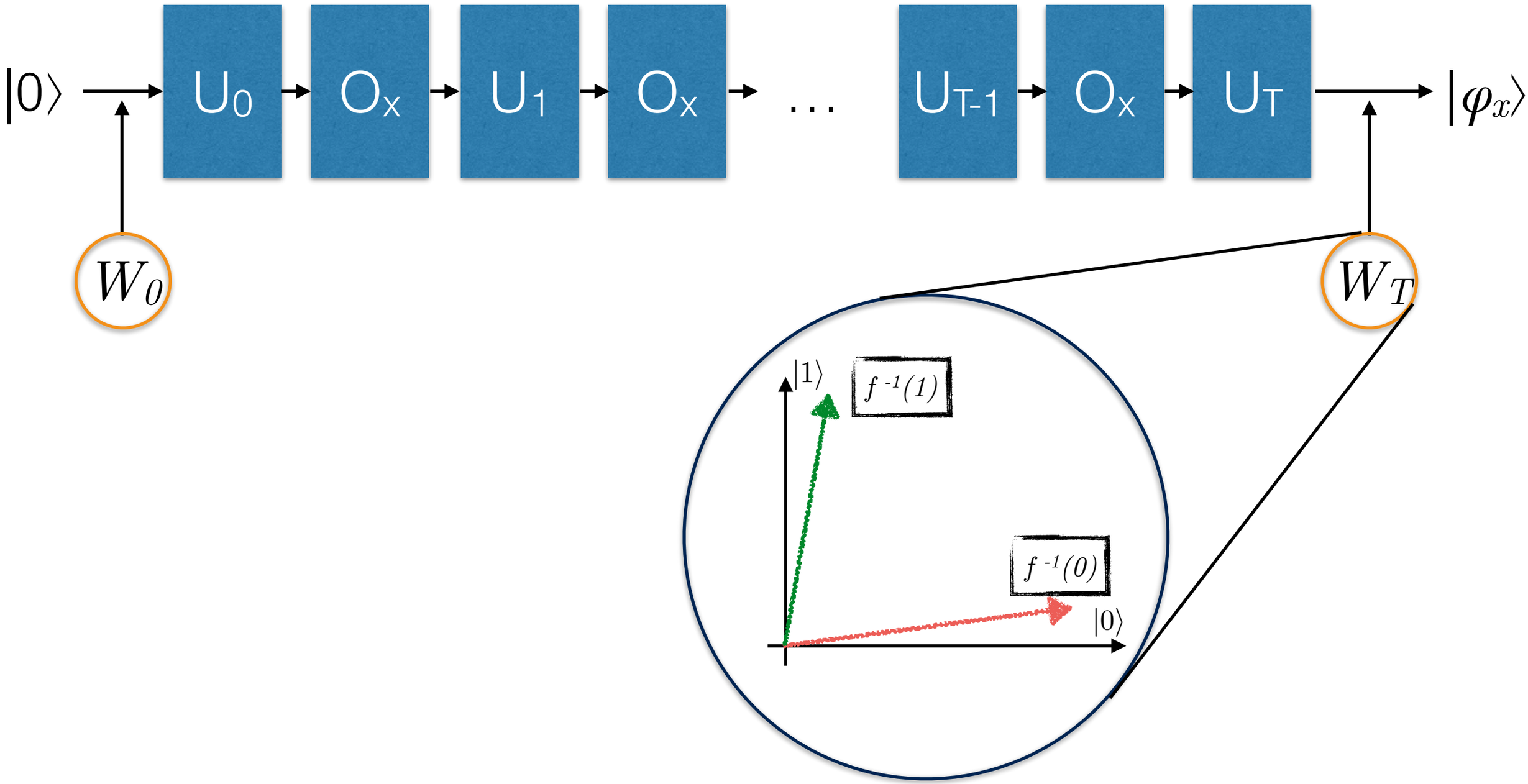


Adversary method

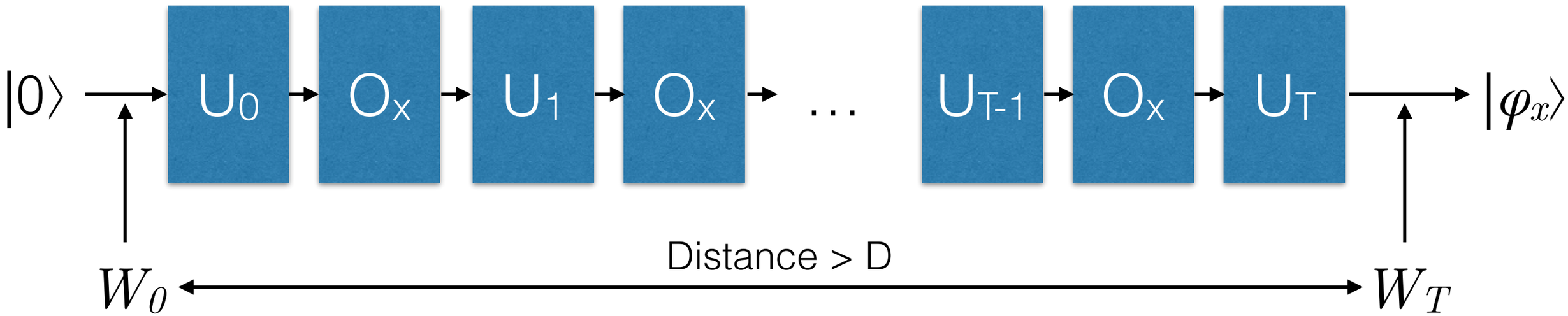


The state of the register containing the result

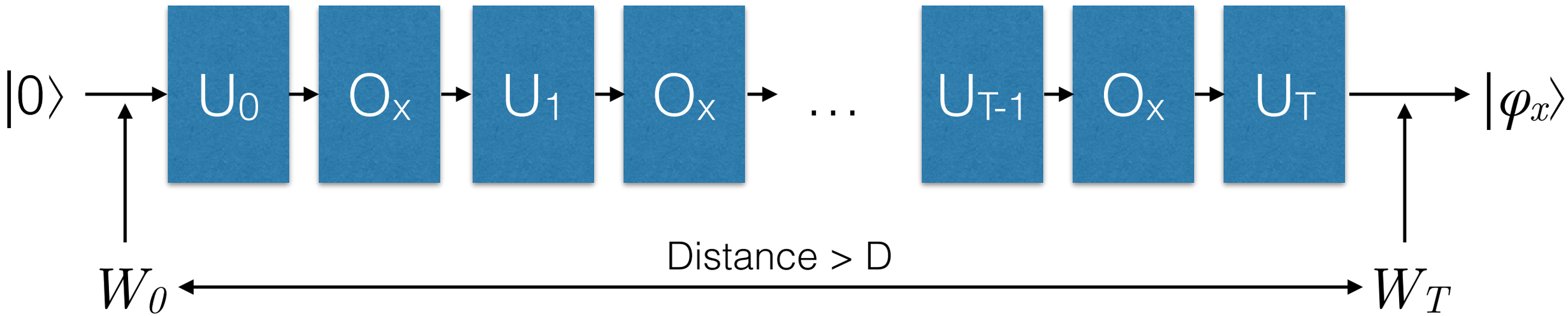
Adversary method

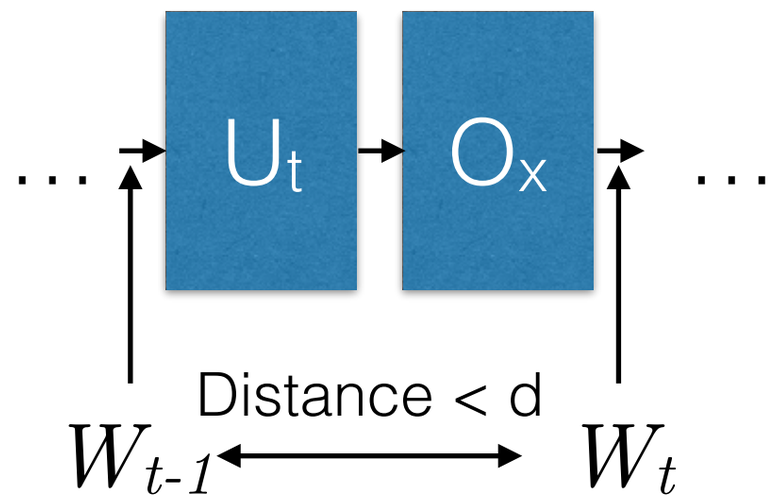


Adversary method



Adversary method





Adversary method