The Space-Time Cost of Purifying Quantum Computations

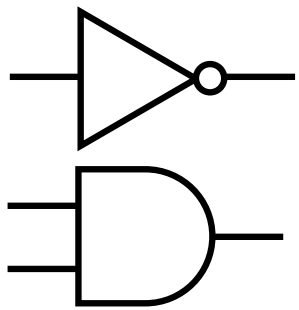
Mark Zhandry
NTT Research

Let’s start with a purely classical question …

Irreversible (typical) computing

NOT

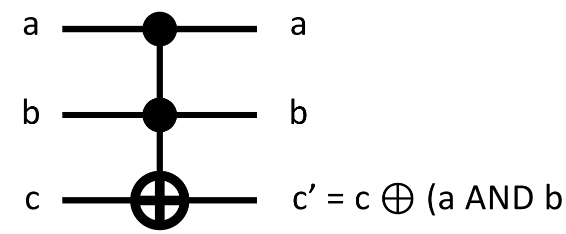
AND



AND is logically irreversible:
if output is **0**, inputs could be **00,01,10**

Reversible computing

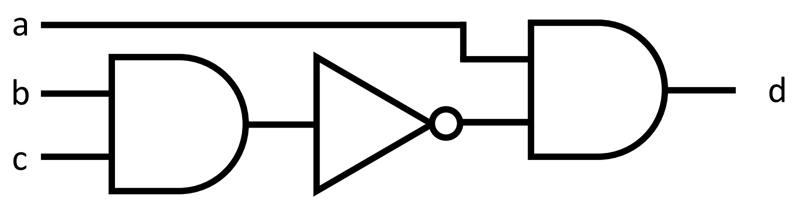
TOFFOLI (T)

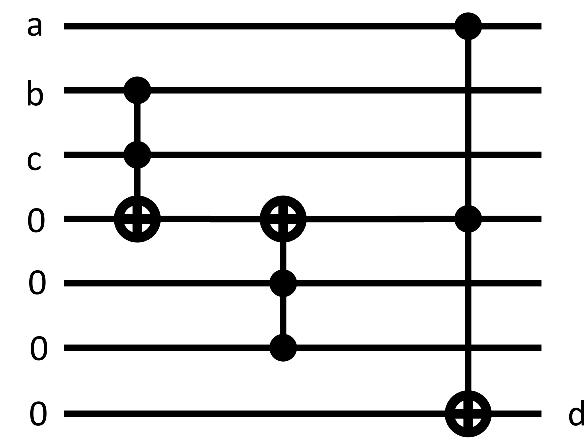


T is logically reversible: $\mathbf{T^2 = I}$

[Landauer'61]: logically irreversible operations must dissipate energy
→ in principle, reversible more energy efficient than irreversible

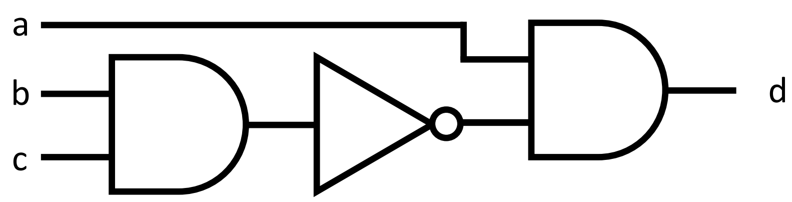
Making Computations Reversible: **The Easy Way**

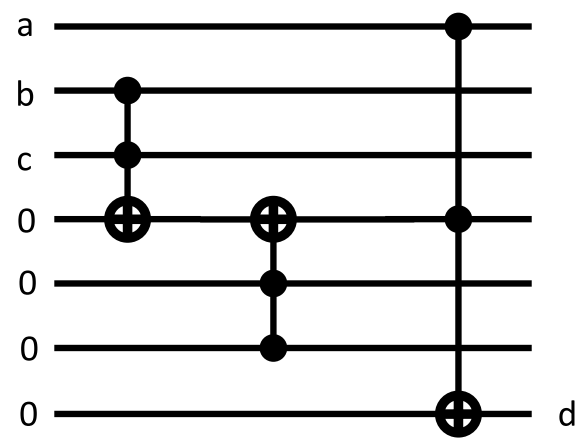




Easy Thm: Time **T** irreversible comp → Time **O(T)** reversible comp

Making Computations Reversible: **The Easy Way**



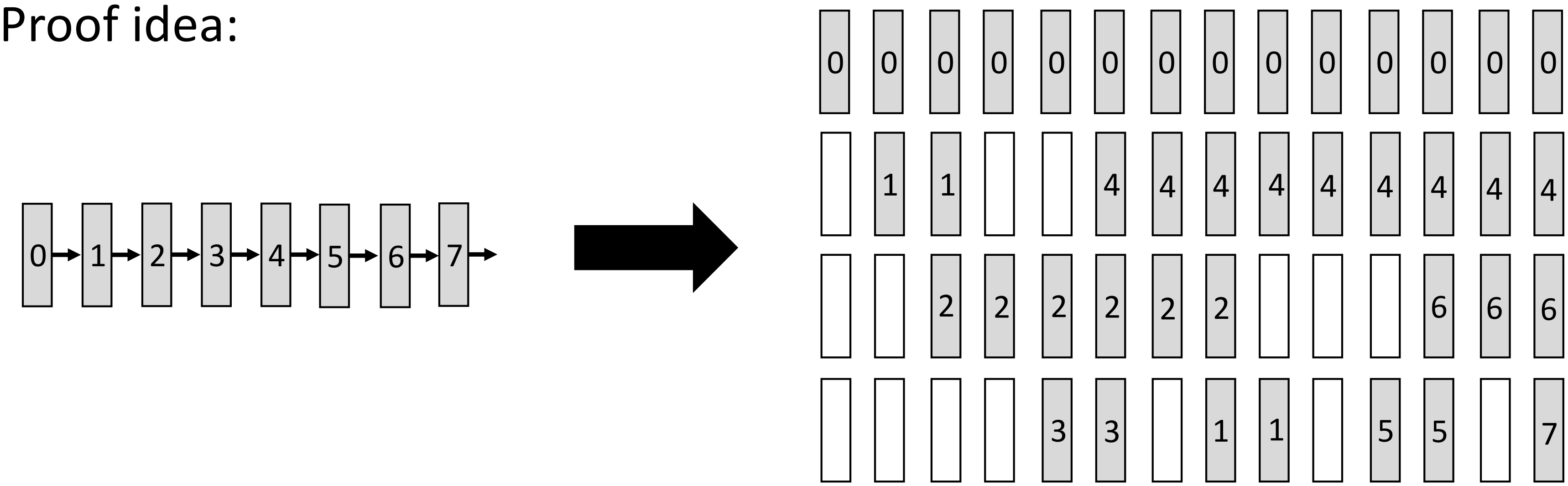


Easy Thm: Time **T**, Space **S** irreversible comp → Time **O(T)**, Space **O(T)** reversible comp

Making Computations Reversible: **Preserving Space and Time**

Thm [Bennett'89]:
Time **T**, Space **S** irreversible comp → Time $\mathbf{T^{O(1)}}$, Space **O(S log T)** reversible comp

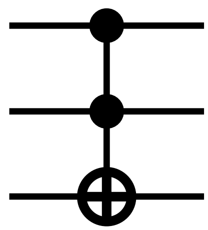
Proof idea:

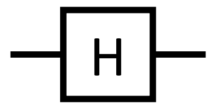


Back to quantum …

Quantum computing

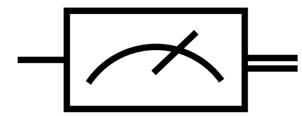
Unitary Gates



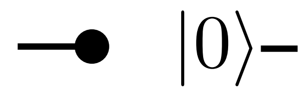


$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Measurement



Reset

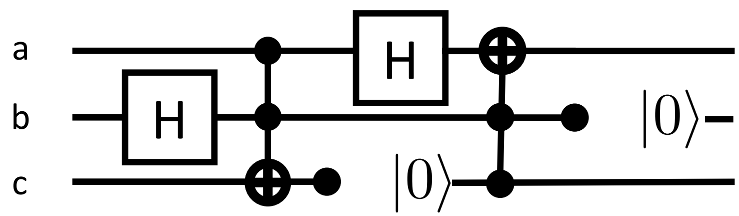


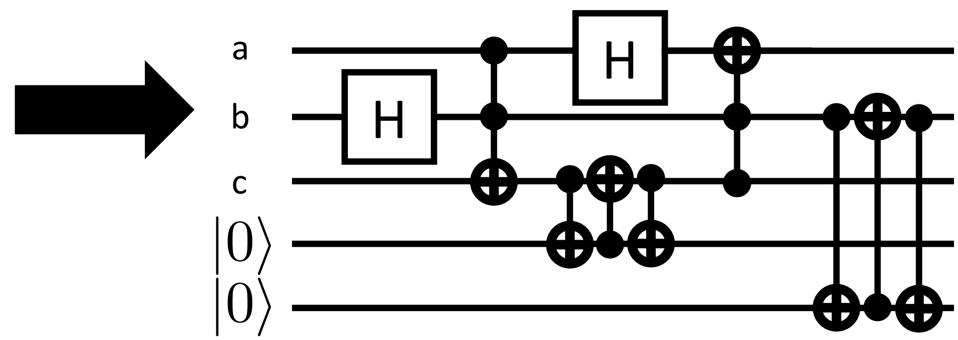
I'm going to call anything non-unitary a "measurement"

Problems with (intermediate) measurements:

→ Subject to Landauer's Principle
→ Not amenable to certain algorithmic techniques (e.g. amplitude amplification)
→ Not directly handled by many query complexity lower bounds
→ Not applicable to certain cryptographic proof techniques (e.g. rewinding)

Making Quantum Computations Unitary: **Delayed Measurements**

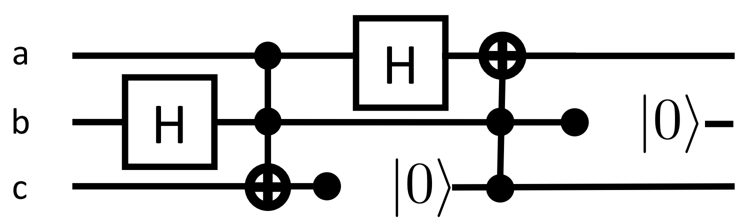


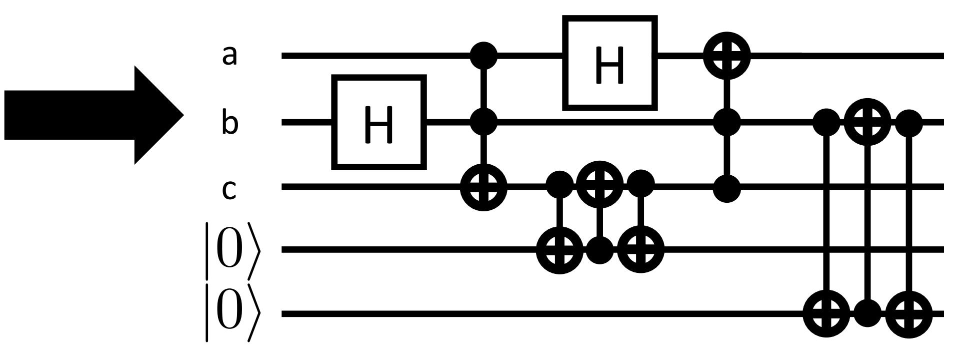


Principle of Delayed Measurements:

Time **T** comp w/ measurements→ Time **O(T)** unitary comp

Making Quantum Computations Unitary: **Delayed Measurements**





Principle of Delayed Measurements:

Time **T**, Space **S** comp w/ measurements→ Time **O(T)**, Space **O(T)** unitary comp

Making Quantum Computations Unitary: **Preserving Space**

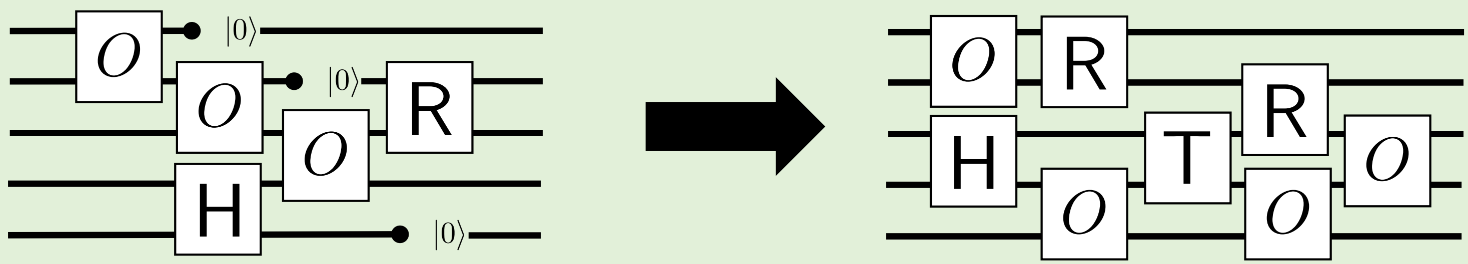
Thm [Fefferman-Remscrim'21, Girish-Raz-Zhan'21]:
Time **T**, Space **S** w/ measurements → Time **Poly(T,2^S)**, Space **O(S)** unitary

Thm [Girish-Raz'22]:
Time **T**, Space **S** **unital comp** → Time **Poly(T)**, Space **O(S log T)** unitary

For intermediate space (**log T << S << T**), existing results for general measurements give huge blowup in time or space

Q: Can (intermediate) measurements be eliminated in a simultaneously space- and time-efficient way?

Def: “Black Box” Purifier:



Transformation must

(1) Work for **any** unitary **O** (but can depend arbitrarily on **O**)

(2) Preserve functionality

(3) Eliminate all non-unitary gates

Observation: Delayed measurements, FR’21, GRZ’21, RS’22, natural quantum analogs of Bennett’89 are all black box

Main Result

Thm: For any "Black Box" purifier:

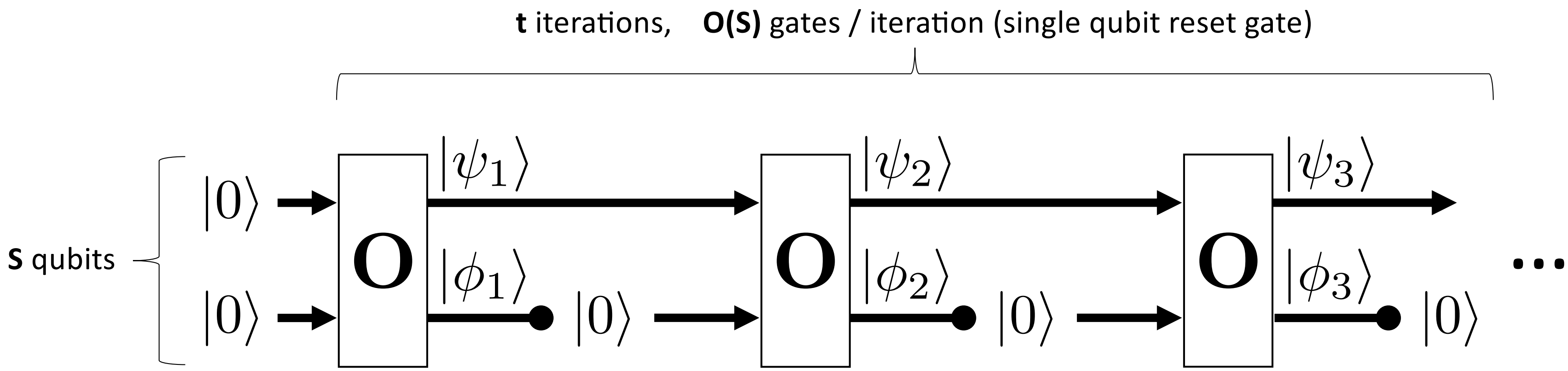
Time **T**, Space **S** w/ general measurements → Time $\mathbf{2^{\Omega(S)}}$ or Space $\mathbf{\Omega(T)}$

Prior work essentially optimal given current techniques

Note: Unconditional lower bound unlikely:

BQL=BQP ➔ can eliminate measurements efficiently in both space and time

Intuition:



For general **O**, only way to perform computation requires either:

(1) Storing all the $|\phi_i\rangle$ → space **Ω(T)**

(2) Having the full description of the $|\phi_i\rangle$ baked into the circuit → size $\mathbf{2^{\Omega(S)}}$

Proof Idea

Observation: Existing quantum space lower bound techniques work for both unitary and non-unitary computation

→ Usually, this is a good thing!

→ We need a technique that works for unitary, but fails for non-unitary

Step 1: Simulation

O

desc$(|\psi_1\rangle)$
desc$(|\psi_2\rangle)$
desc$(|\psi_3\rangle)$

desc$(|\phi_1\rangle)$
desc$(|\phi_2\rangle)$
desc$(|\phi_3\rangle)$

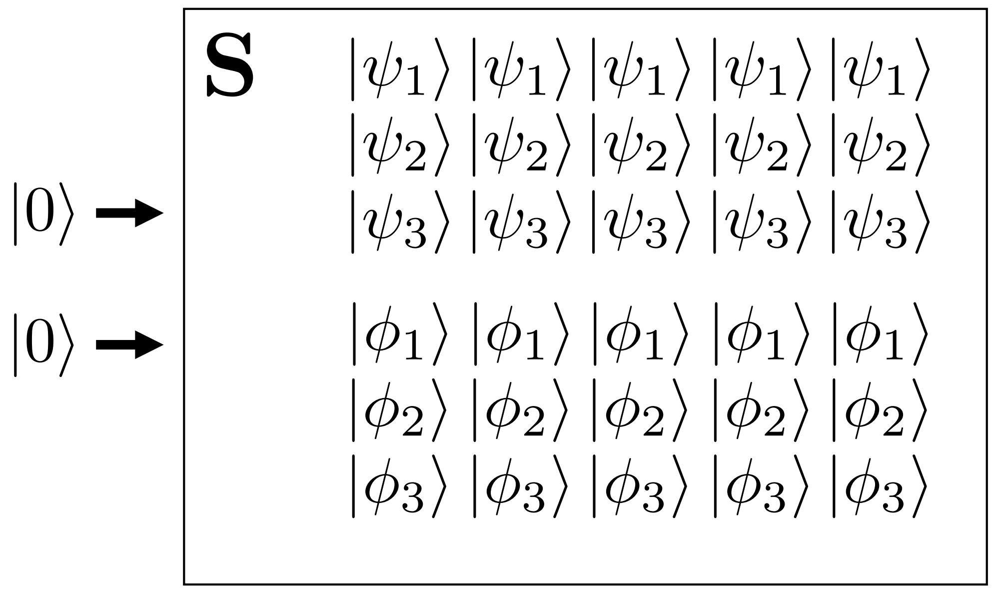
$\Rightarrow$

S

$$|\psi_1\rangle\ |\psi_1\rangle\ |\psi_1\rangle\ |\psi_1\rangle\ |\psi_1\rangle$$
$$|\psi_2\rangle\ |\psi_2\rangle\ |\psi_2\rangle\ |\psi_2\rangle\ |\psi_2\rangle$$
$$|\psi_3\rangle\ |\psi_3\rangle\ |\psi_3\rangle\ |\psi_3\rangle\ |\psi_3\rangle$$

$$|\phi_1\rangle\ |\phi_1\rangle\ |\phi_1\rangle\ |\phi_1\rangle\ |\phi_1\rangle$$
$$|\phi_2\rangle\ |\phi_2\rangle\ |\phi_2\rangle\ |\phi_2\rangle\ |\phi_2\rangle$$
$$|\phi_3\rangle\ |\phi_3\rangle\ |\phi_3\rangle\ |\phi_3\rangle\ |\phi_3\rangle$$

Step 1: Simulation



Step 1: Simulation

$|\psi_1\rangle \longleftarrow$

$|\phi_1\rangle \longleftarrow$

S

$$|\psi_1\rangle\,|\psi_1\rangle\,|\psi_1\rangle\,|\psi_1\rangle$$
$$|\psi_2\rangle\,|\psi_2\rangle\,|\psi_2\rangle\,|\psi_2\rangle\,|\psi_2\rangle$$
$$|\psi_3\rangle\,|\psi_3\rangle\,|\psi_3\rangle\,|\psi_3\rangle\,|\psi_3\rangle$$

$$|\phi_1\rangle\,|\phi_1\rangle\,|\phi_1\rangle\,|\phi_1\rangle$$
$$|\phi_2\rangle\,|\phi_2\rangle\,|\phi_2\rangle\,|\phi_2\rangle\,|\phi_2\rangle$$
$$|\phi_3\rangle\,|\phi_3\rangle\,|\phi_3\rangle\,|\phi_3\rangle\,|\phi_3\rangle$$

Step 1: Simulation

$|\psi_1\rangle \rightarrow$

$|0\rangle \rightarrow$

$\mathbf{S}$

$$\begin{array}{ccccc}
|\psi_1\rangle & |\psi_1\rangle & |\psi_1\rangle & |\psi_1\rangle & \\
|\psi_2\rangle & |\psi_2\rangle & |\psi_2\rangle & |\psi_2\rangle & |\psi_2\rangle \\
|\psi_3\rangle & |\psi_3\rangle & |\psi_3\rangle & |\psi_3\rangle & |\psi_3\rangle \\
 & & & & \\
|\phi_1\rangle & |\phi_1\rangle & |\phi_1\rangle & |\phi_1\rangle & \\
|\phi_2\rangle & |\phi_2\rangle & |\phi_2\rangle & |\phi_2\rangle & |\phi_2\rangle \\
|\phi_3\rangle & |\phi_3\rangle & |\phi_3\rangle & |\phi_3\rangle & |\phi_3\rangle
\end{array}$$

Step 1: Simulation

$|\psi_2\rangle \leftarrow$

$|\phi_2\rangle \leftarrow$

$\mathbf{S}$

$|\psi_1\rangle\ |\psi_1\rangle\ |\psi_1\rangle\ |\psi_1\rangle\ |\psi_1\rangle$

$|\psi_2\rangle\ |\psi_2\rangle\ |\psi_2\rangle\ |\psi_2\rangle$

$|\psi_3\rangle\ |\psi_3\rangle\ |\psi_3\rangle\ |\psi_3\rangle\ |\psi_3\rangle$

$|\phi_1\rangle\ |\phi_1\rangle\ |\phi_1\rangle\ |\phi_1\rangle$

$|\phi_2\rangle\ |\phi_2\rangle\ |\phi_2\rangle\ |\phi_2\rangle$

$|\phi_3\rangle\ |\phi_3\rangle\ |\phi_3\rangle\ |\phi_3\rangle\ |\phi_3\rangle$

Step 2: Simulator's space decreases

Let c_i be number of $|\psi_i\rangle$ given out, d_i the number of $|\phi_i\rangle$

Lemma: (whp, assuming #(**O**) << **2**$^{\mathbf{S}}$)

$$c_i, d_i \geq 0 \qquad\qquad d_{i+1} = d_i - c_i$$

[Ji-Liu-Song'18]
+ [Z'19]
+ Haar random

Cor: if algorithm ever computes $|\psi_t\rangle$, must have

$$d_1, \cdots, d_t \geq 1$$

→ space of simulator decreases by **Ω(tS)**

Step 3:

Thm: For unitary algorithms, simulator's space + algorithm's space can't decrease

Cor: algorithms space must be $\boldsymbol{\Omega(tS) = \Omega(T)}$

Thanks!