Portland State U

F, 04/24/2020

S′20 CS 410/510

Intro to quantum computing

Fang Song

Week 4

- Simon's algorithm
- Reversible computation

Credit: based on slides by Richard Cleve

Exercise: Hadamard

1. What is $H^2 := HH$?

2. What is the matrix form of $H^{\otimes 2} := H \otimes H$?

3. Let $|\psi\rangle = \frac{1}{\sqrt{2^3}} \sum_{x \in \{0,1\}^3} |x\rangle$. What is $H^{\otimes 3}|\psi\rangle$?

Asymptotic notations

$$O(\cdot), \Omega(\cdot), \Theta(\cdot), o(\cdot), \omega(\cdot)$$

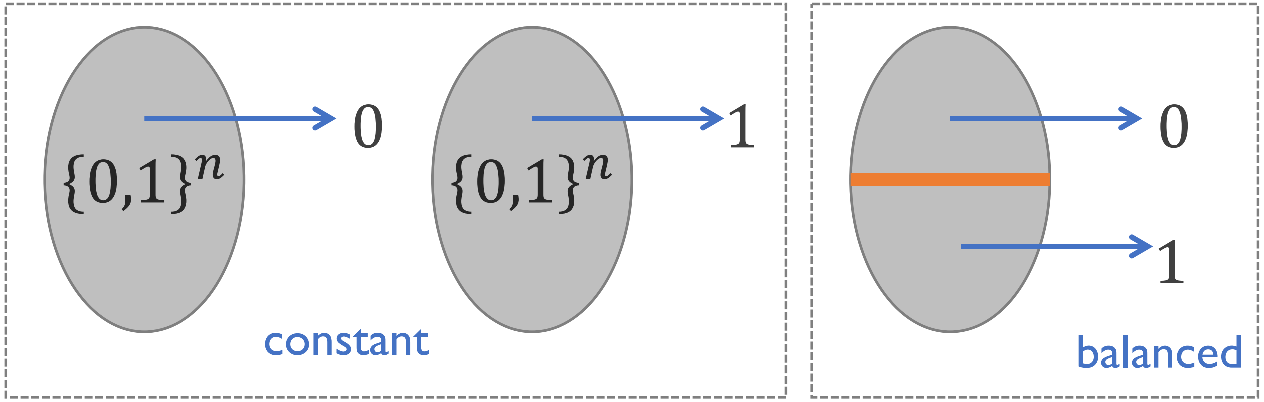
Notation	Definition	Think	Example
$f(n) = O(g(n))$	$\exists c > 0, n_0 > 0, \forall n > n_0$: $0 \leq f(n) \leq cg(n)$	Upper bound	$100n^2 = O(n^3)$
$f(n) = \Omega(g(n))$	$\exists c > 0, n_0 > 0, \forall n > n_0$: $0 \leq cg(n) \leq f(n)$	Lower bound	$100n^2 = \Omega(n^{1.5})$
$f(n) = \Theta(g(n))$	$f(n) = O(g(n))$ & $f(n) = \Omega(g(n))$	Tight bound	$\log(n!) = \Theta(n \log n)$
$o(\cdot), \omega(\cdot)$		Strict upper/lower bound	$n^2 = o(2^n)$ $n^2 = \omega(\log n)$

Reflection on Deutsch-Josza

Given: black-box $f: \{0,1\}^n \rightarrow \{0,1\}$ either constant or balanced

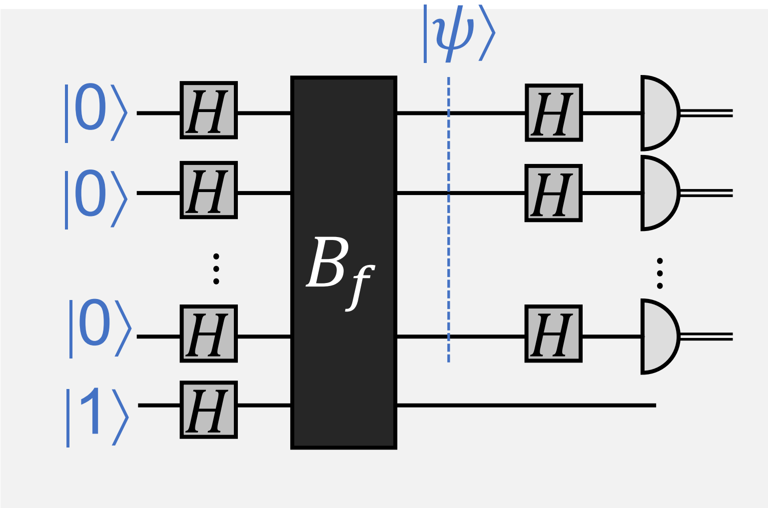
- constant means $f(x) = 0$ for all x, or $f(x) = 1$ for all x
- balanced means $\Sigma_x f(x) = 2^{n-1}$

Goal: decide which case



- Consider all $f: \{0,1\}^n \rightarrow \{0,1\}$
  - # of constant functions ____
  - # of balanced functions ____
  - Total # of functions ____
- This is called a **Promise** problem

Reflection on Deutsch-Josza



$$|\psi\rangle \propto \begin{cases} \pm\sum_{x\in\{0,1\}^n}|x\rangle, & f \text{ constant} \\ \text{orthogonal to } (\pm\sum_x|x\rangle), & f \text{ balanced} \end{cases}$$

How to distinguish between the two cases?

What is $H^{\otimes n}|\psi\rangle$?

- Constant: $H^{\otimes n}|\psi\rangle = \pm|00\ldots0\rangle$
- Balanced: $H^{\otimes n}|\psi\rangle \in (\pm|00\ldots0\rangle)^\perp$

Simon's algorithm

Quantum vs. classical separations

Black-box problem	Classical deterministic	Randomized $\Omega(1)$ prob.	Quantum
Deutsch (1-bit constant vs. balanced)	2 (queries)	2 (queries)	1 (query)
Deutsch-Josza (n-bit constant vs. balanced)	$2^{n-1}+1$	$\Omega(n)$	1 Exact
Simon	$2^{n-1}+1$	$\Omega(\sqrt{2^n})$	$O(n)$ $\Omega(1)$ prob.

Simon's problem

Given: a black-box function $f: \{0,1\}^n \to \{0,1\}^n$

- **Promise:** there exists secret $s \neq 0^n$ such that

  $\forall x \neq x' \in \{0,1\}^n$, $f(x) = f(x')$ iff. $x \oplus x' = s$

Goal: find secret string s.

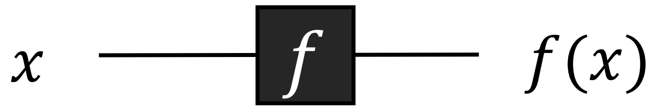
x	$f(x)$
$x_1, x_1 \oplus s$	
$x_2, x_2 \oplus s$	
…	
$x_k, x_k \oplus s$	
…	

Example.

x	$f(x)$
000	011
001	101
010	000
011	010
100	101
101	011
110	010
111	000

What is s in this case? ________

Classical algorithms for Simon

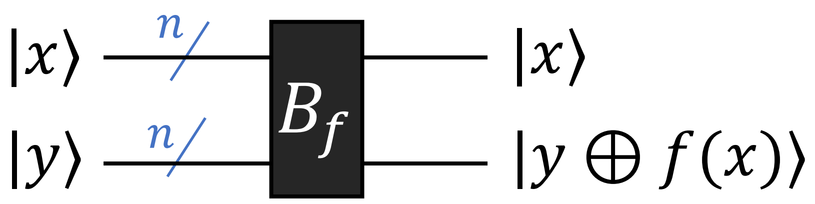


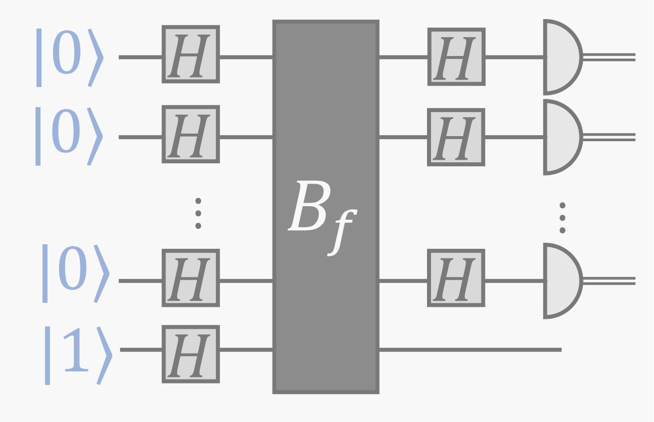
- Search for a collision: an $x \neq y$ such that $f(x) = f(y)$
  - Choose $x_1, x_2, \ldots, x_k \in \{0,1\}^n$ randomly (independently)
  - For all $i \neq j$, if $f(x_i) = f(x_j)$, then output $x_i \oplus x_j$ and halt
- A hard case: s is chosen at random & $f(x)$ is chosen randomly subject to the structure implied by s
- Birthday bound: $k = \Theta(\sqrt{2^n})$ to see a collision with constant (e.g., 3/4) probability
- This strategy is essentially optimal. (NB. You have to rule out all possible randomized algorithms)

A quantum algorithm for Simon

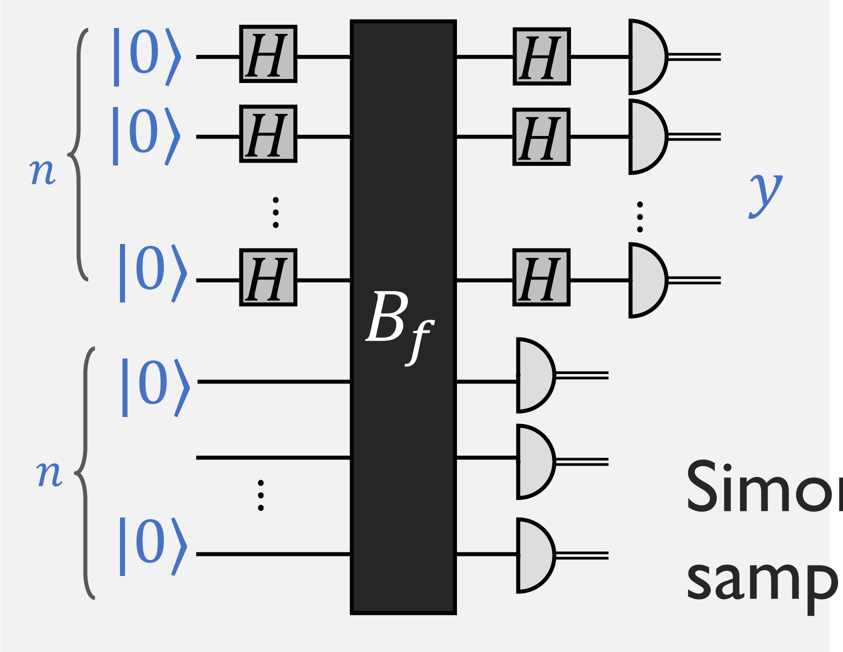
Recall: quantum black-box function

Unitary $B_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$





Deutsch-Josza



Simon's quantum sampling subroutine

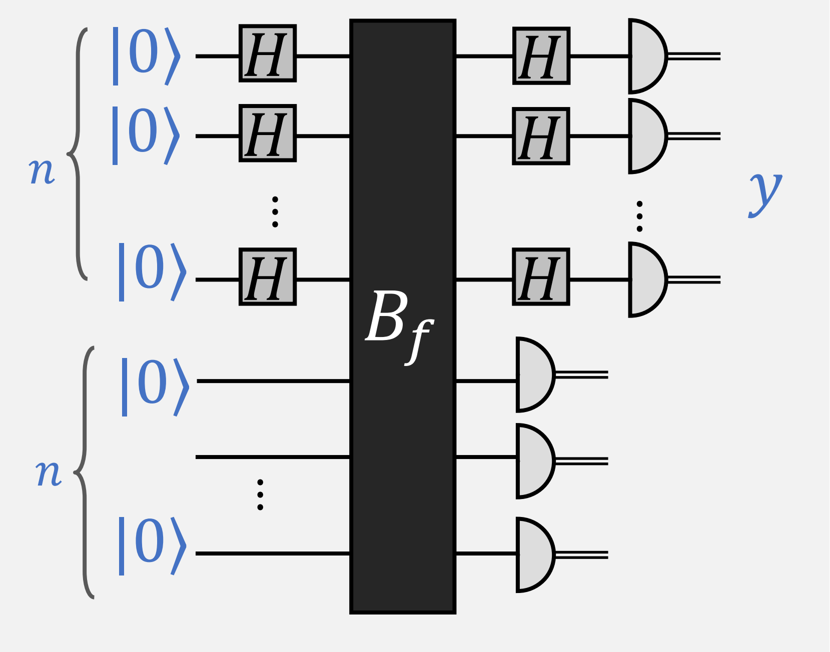
Simon's algorithm

1. Run Simon's quantum sampling subroutine k times.

   Obtain samples $y_1, \dots, y_k$

2. Post-processing.

   Solving linear system to find s



Theorem. $k = O(n)$ quantum queries suffice to find s w. prob. $\geq 1/4$.

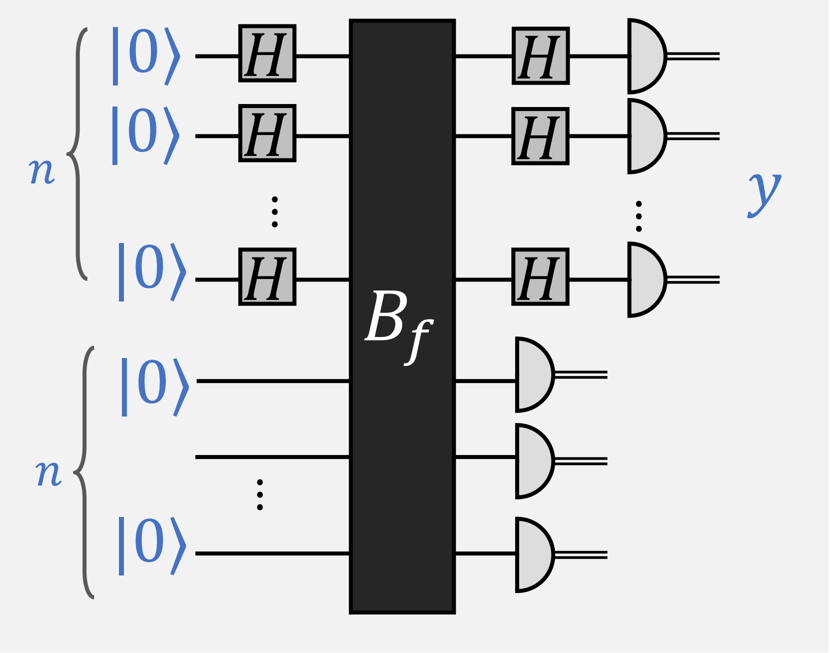
Simon's algorithm: analysis

1. Run Simon's quantum sampling subroutine k times.

   Obtain samples $y_1, \dots, y_k$

2. Classical post-processing on $\{y_i\}$.

   Solving linear system to find s



a What do the samples y_i tell us?

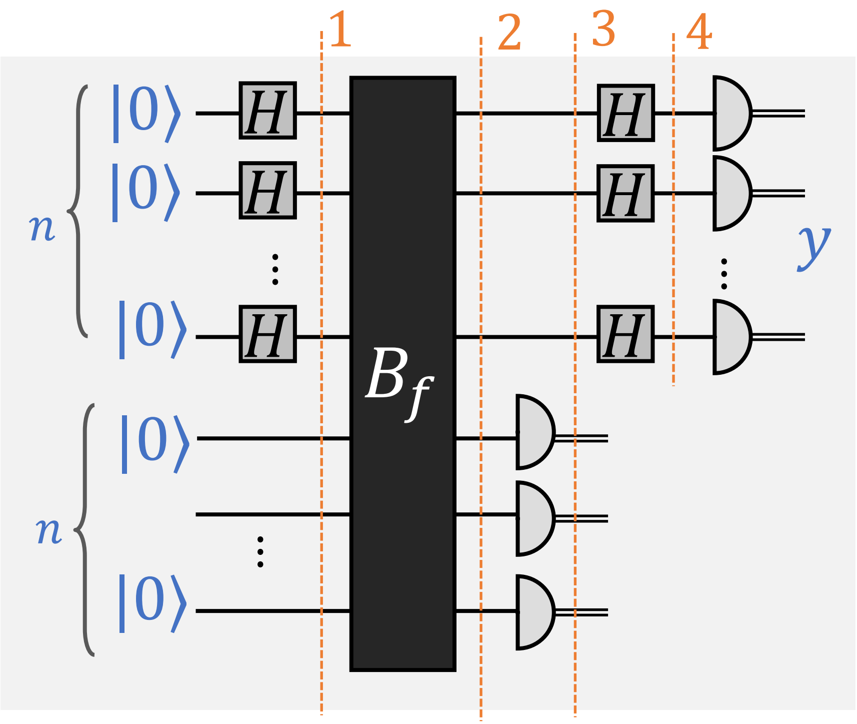
b How many samples are needed?

Remarks on notations

- $xy, \alpha\beta, AB$ usually denotes multiplication (integers, complex numbers, matrices)
- Strings $x, y \in \{0,1\}^n$, $x \cdot y$ denotes dot product, i.e., sum of bit-wise mult. mod 2 (for single bit: $x + y \bmod 2 = x \oplus y, x \cdot y = xy$)
- Concatenation $x||y$

Simon's algorithm: analysis I

a What do the samples y_i tell us?



Simon's algorithm: analysis II

b How many samples are needed?

$$\begin{aligned} y_1 \cdot s &= 0 \\ y_2 \cdot s &= 0 \\ &\cdots \\ y_k \cdot s &= 0 \end{aligned} \quad \Leftrightarrow \quad \begin{pmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{k1} & y_{k2} & \cdots & y_{kn} \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

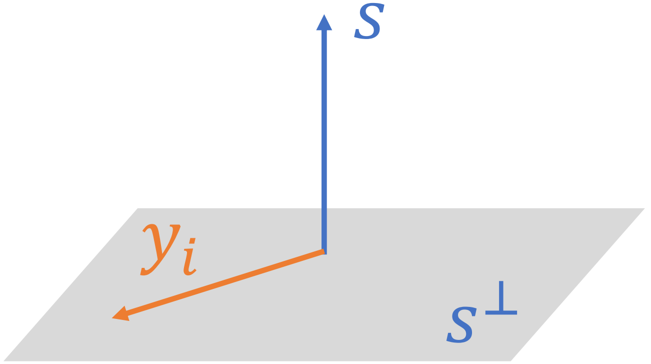
Fact. When $k = n - 1$, unique solution s with prob. $\geq \frac{1}{4}$

$$\Pr[y_1, \dots, y_{n-1} \text{ linearly indep.}] \geq 1/4$$

Efficient algorithm: $O(n^{2.376})$ Coppersmith-Winograd

Simon's algorithm: a geometric interpretation

- Viewing $\{0,1\}^n$ as a vector space
  - $\mathbb{Z}_2 := \{0,1\}$ with addition and multiplication mod 2 is a field
  - $\{0,1\}^n = \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 = \mathbb{Z}_2^n$ is an n-dimensional vector space over $\mathbb{Z}_2$
- Let $x \cdot y = x_1 y_1 + \cdots x_n y_n \bmod 2$ "dot product"
  - $x \cdot y = 0$ can be interpreted as the vectors being "orthogonal" (Not precise: e.g., $\exists x \neq 0, x \cdot x = 0$)



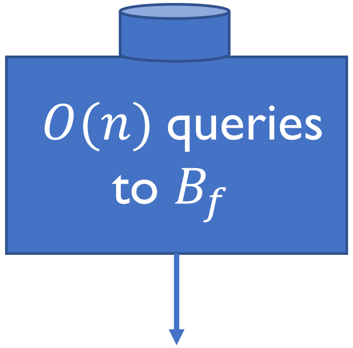
"orthogonal" complement
$s^\perp := \{y : y \cdot s = 0\}$

- Quantum sampling subroutine samples from $s^\perp$ uniformly at random
- $O(n)$ independent samples determines s with constant probability

Recap: quantum speedups

Black-box problem	Classical deterministic	Randomized $\Omega(1)$ prob.	Quantum
Deutsch (1-bit constant vs. balanced)	2 (queries)	2 (queries)	1 (query)
Deutsch-Josza (n-bit constant vs. balanced)	$2^{n-1} + 1$	$\Omega(n)$	1 Exact
Simon	$2^{n-1} + 1$	$\Omega(\sqrt{2^n})$	$O(n)$ $\Omega(1)$ prob.

Exercise: amplifying the success probability



s w.p. $\geq 1/4$

- How to find s with probability $\geq 1 - 2^{-n}$?
- How many quantum queries will be needed?

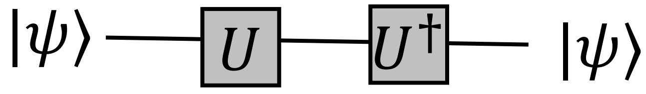
Reversible computation

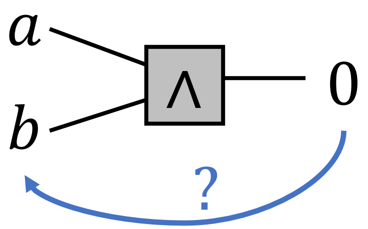
Quantum vs. classical computation

- We've seen a few examples where quantum algorithms outperform classical ones → quantum computer is powerful
- But, wait a second, we haven't even justified a basic goal …

Is a quantum computer (at least) as powerful as a classical computer?
i.e. can an arbitrary efficient classical algorithm (circuit) be converted to an efficient quantum algorithm (circuit)?

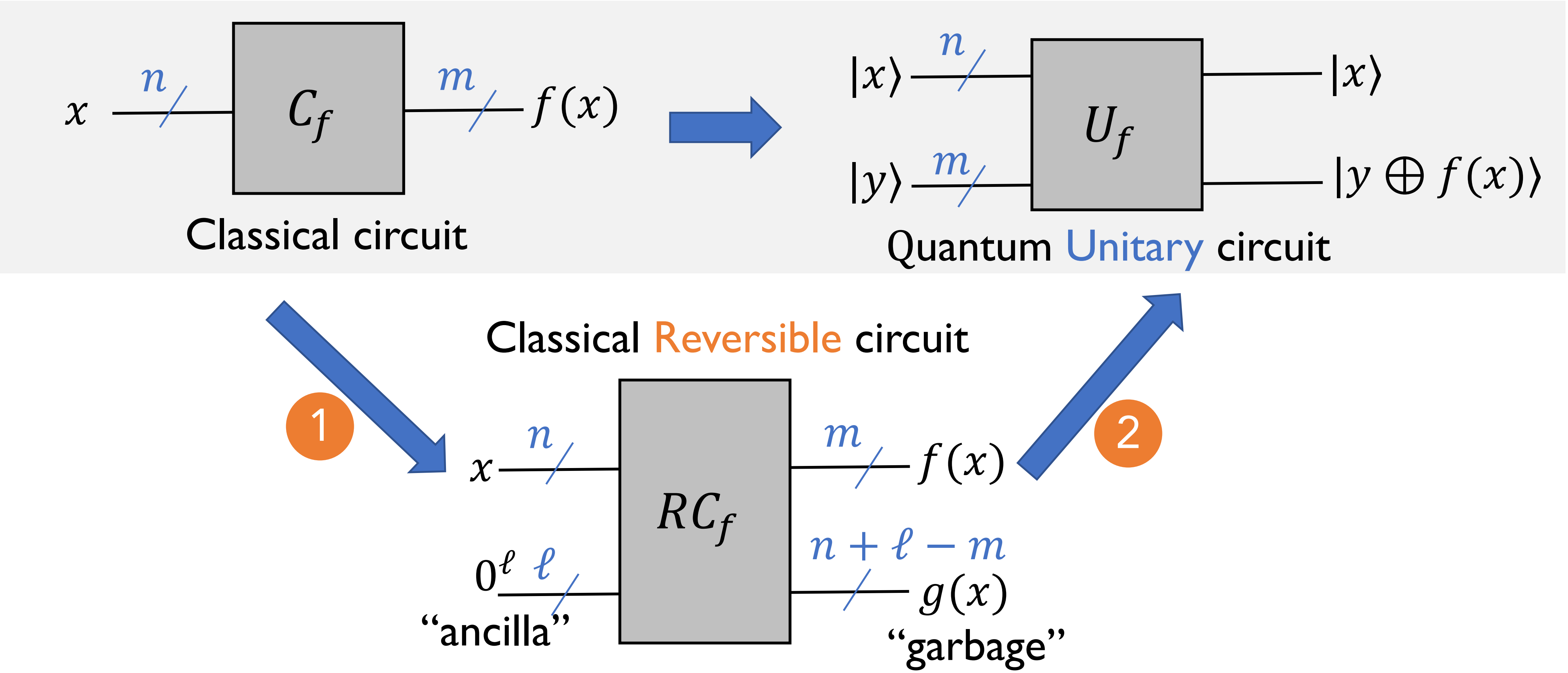
- Not immediate, quantum ckt (w.o. meas.) is unitary ➔ reversible



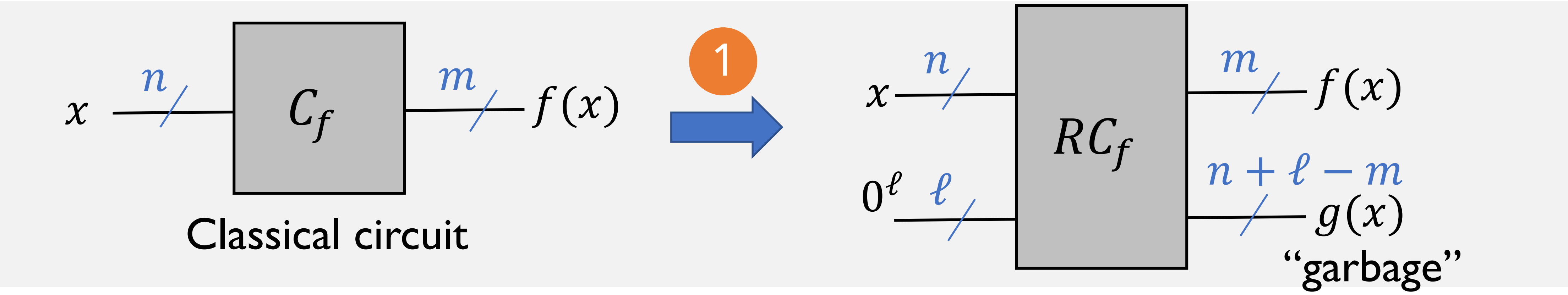


Simulating classical circuit

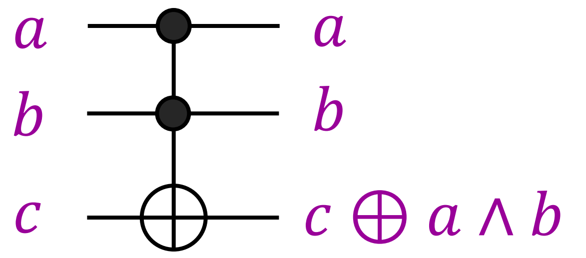
- Consider $f: \{0,1\}^n \to \{0,1\}^m$ Ex. $f(x_1, x_2) = x_1 + x_2 \bmod 2^m, n = 2m$



1. Making classical circuit reversible

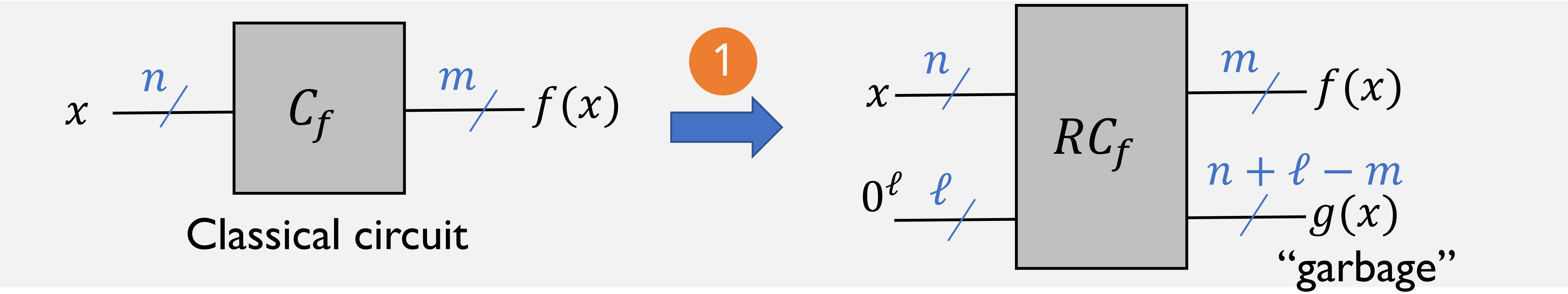


- Def. A Boolean gate is reversible if it has the same input / output size, and the input to output mapping is a bijection.

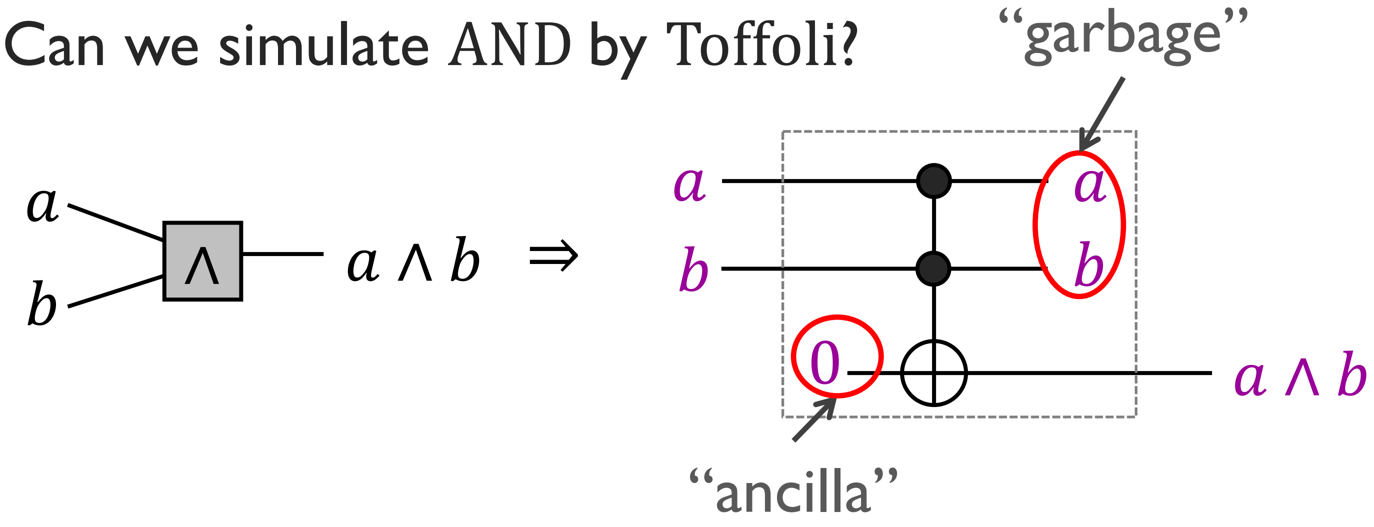


Toffoli gate
(controlled-controlled NOT)
"flip c iff. Both a and b are 1"

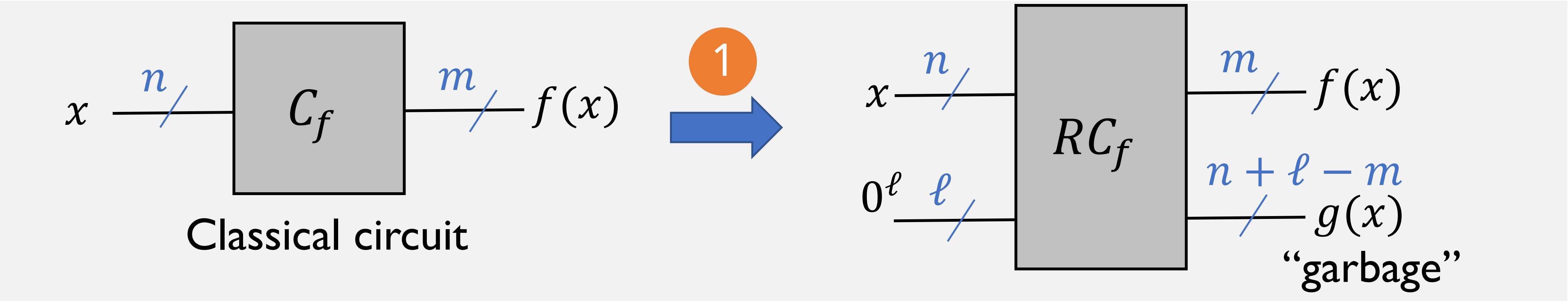
1. Making classical circuit reversible



- **Fact.** {AND, NOT} gates are universal for classical circuits
  - NOT is reversible
  - Can we simulate AND by Toffoli?



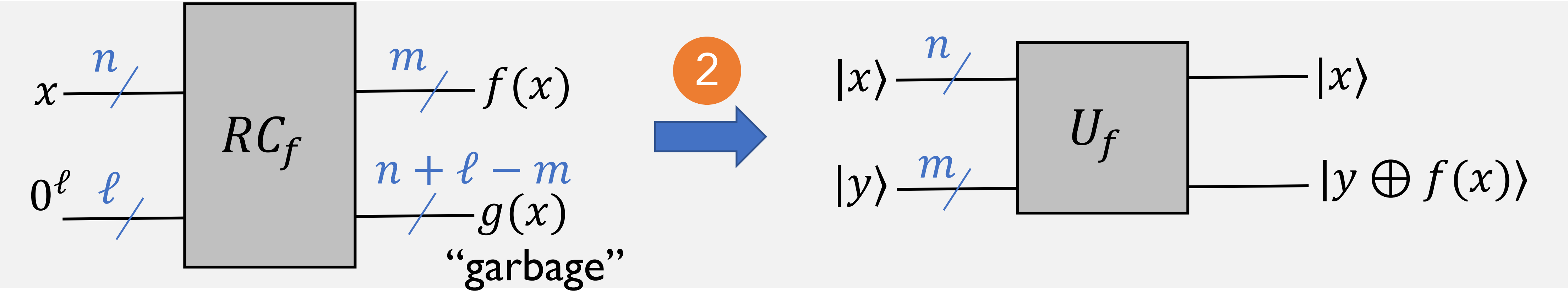
1. Making classical circuit reversible



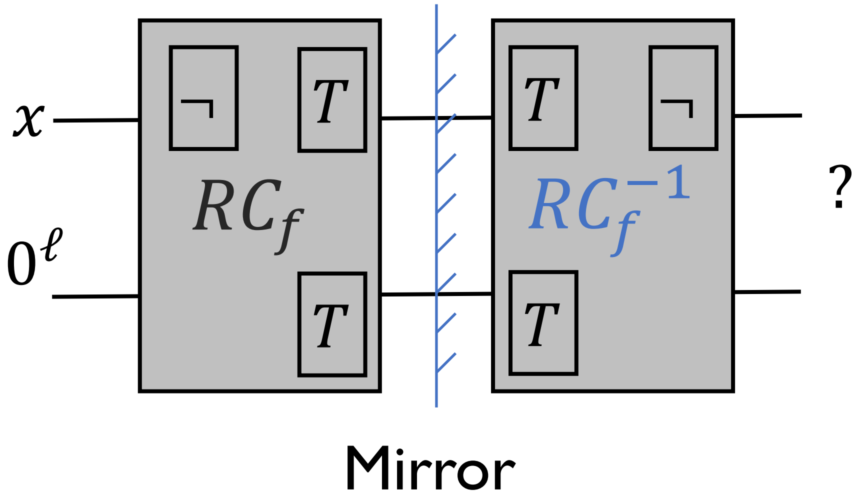
Replace each AND with reversible Toffoli gadget

$|C_f| = k \longrightarrow |RC_f| = O(k)$

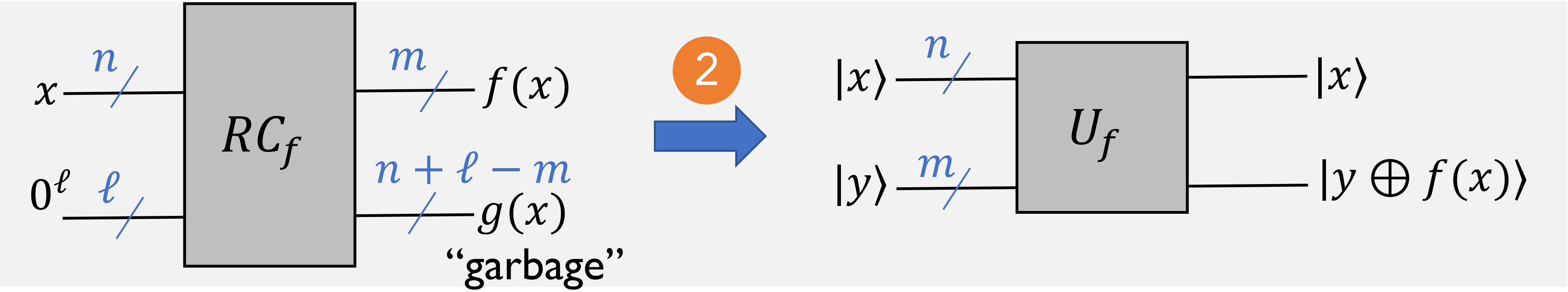
2. Cleaning up the junk



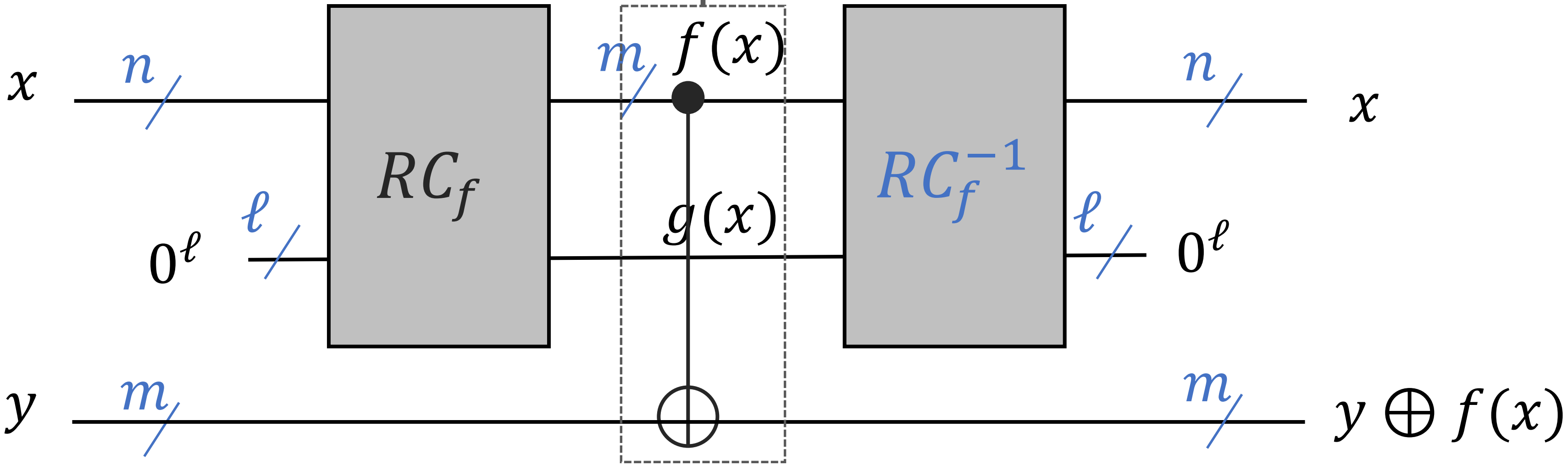
- What does the "mirror" of RC_f do? – it uncomputes

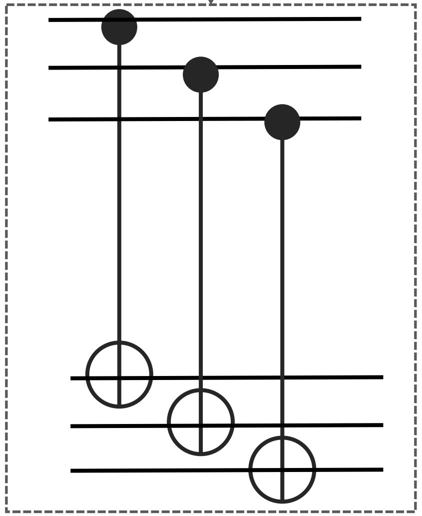


2. Cleaning up the junk

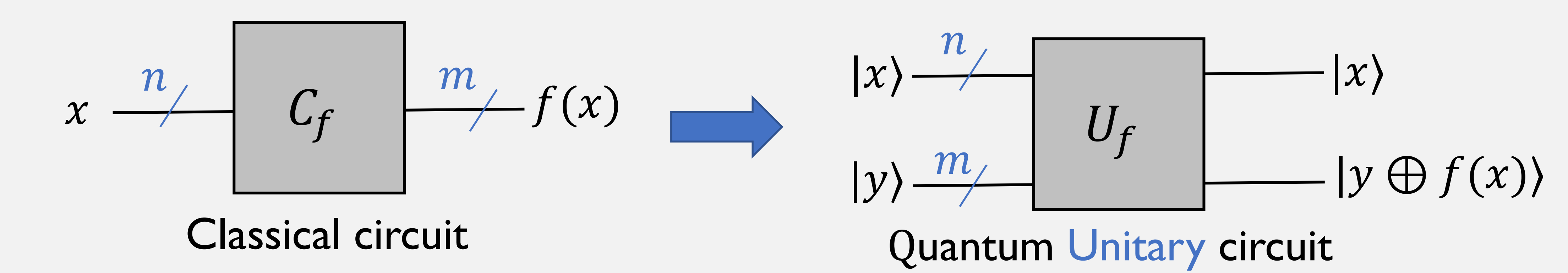


Quantum circuit $U_f: |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ $|U_f| = 2|RC_f| + m$





Summary



$|C_f| = k$ —— $|RC_f| = O(k)$ ⟶ $|U_f| = O(k)$

Corollary. $\mathbf{BPP} \subseteq \mathbf{BQP}$ [More to come in future]

Any problem that a classical computer can solve efficiently can be solved on a quantum computer efficiently too

Logistics

- HW3 due Sunday

- Project
  - Project page: instructions and suggested topics
  - Send me your group information by end of today (April 24 11:59pm AoE).
  - Proposal due next Sunday May 3rd , 11:59pm AoE.
  - Ask for feedback and start brainstorming (e.g., Campuswire private chat rooms)
  - End of today's lecture: group discussion

Project discussion

[CCC report]

- Quantum algorithms
  - List 3 major algorithm design directions
  - What is the prospect of the timeline for quantum algorithms?
- Quantum computing architecture
  - List three major considerations facing a quantum architecture design
- Quantum programming
  - What is the focus of current effort and what future effort would be needed?
- Verification
  - What are the different levels of verification? What tools are needed?

Scratch