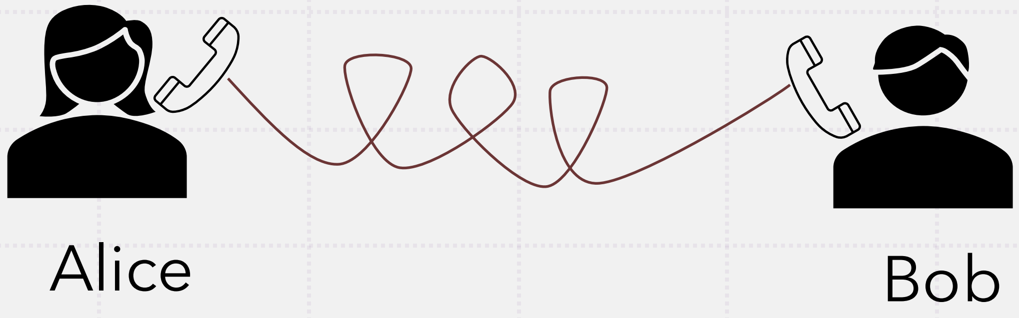
Julia Freund

Institut für Theoretische Physik (Universität Innsbruck)

Principles and Applications of Quantum Information

Motivation

Secure communication
Key exchange



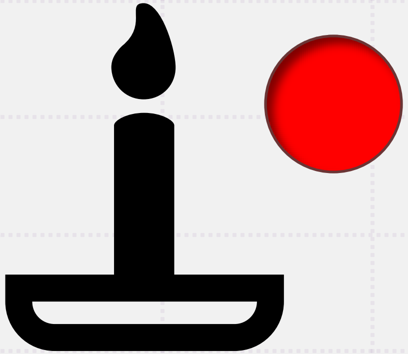
Traveling
Sales-person
Problem

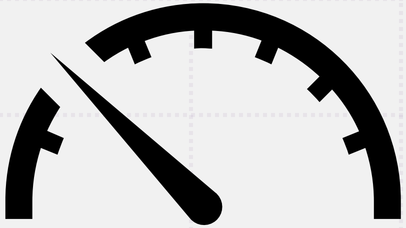
How can we use quantum particles to exchange a key between Alice & Bob?

Can a quantum computer solve NP-hard problems faster than a classical computer?

Factoring Problem (RSA)

Classical Light Source

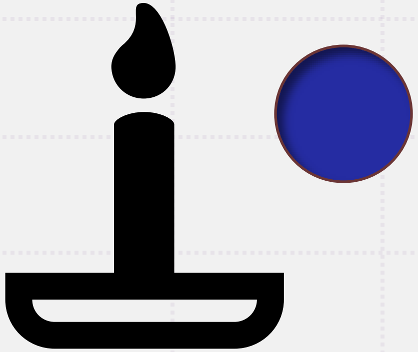




red

100%

What makes quantum particles different from classical particles?



blue

100%

Quantum Light Source

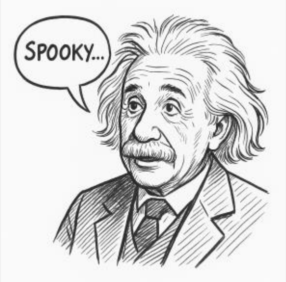
Superposition

red

50%

blue

50%



red

50%

blue

50%

Entanglement

red

100%

Definition of a quantum bit

$|0\rangle$ = (red circle) = "0" bit

$|1\rangle$ = (blue circle) = "1" bit

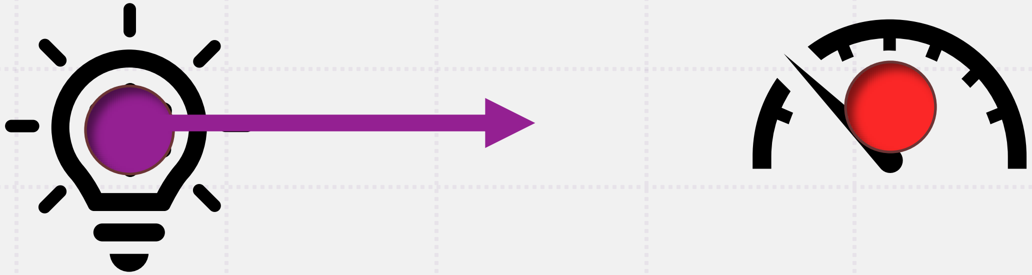
Quantum bit – qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

α ~ probability that we find 0 (red)

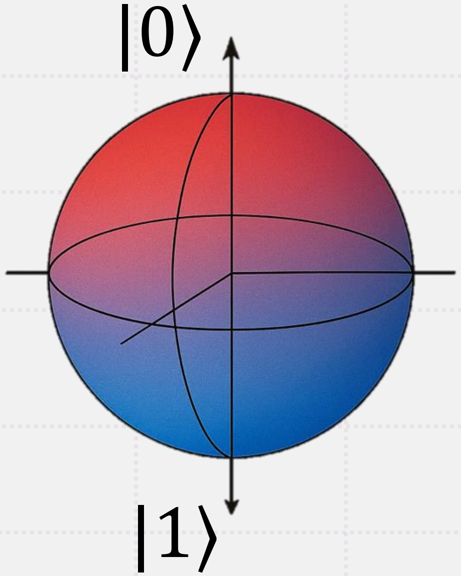
β ~ probability that we find 1 (blue)

Superposition



red 50%

blue 50%



$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Deutsch-Josza Algorithm (1)

Task: determine if function f is **constant** or **balanced**

Boolean function: $f:\{0,1\} \mapsto \{0,1\}$

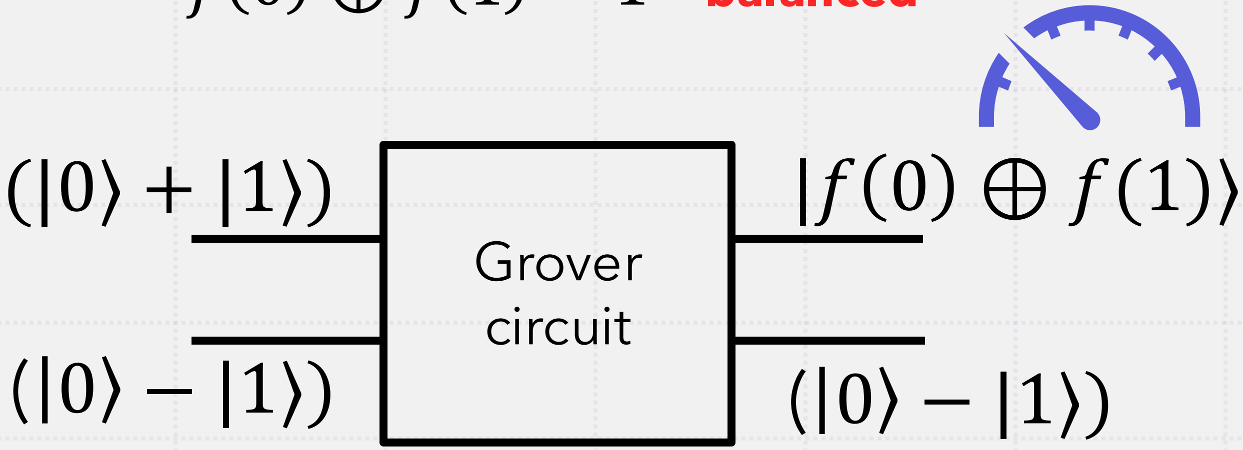
$f_1: 0 \mapsto 0$, $1 \mapsto 0$; $f_2: 0 \mapsto 1$, $1 \mapsto 1$ } **constant**

$f_3: 0 \mapsto 0$, $1 \mapsto 1$; $f_4: 0 \mapsto 1$, $1 \mapsto 0$ } **balanced**

Quantum strategy:

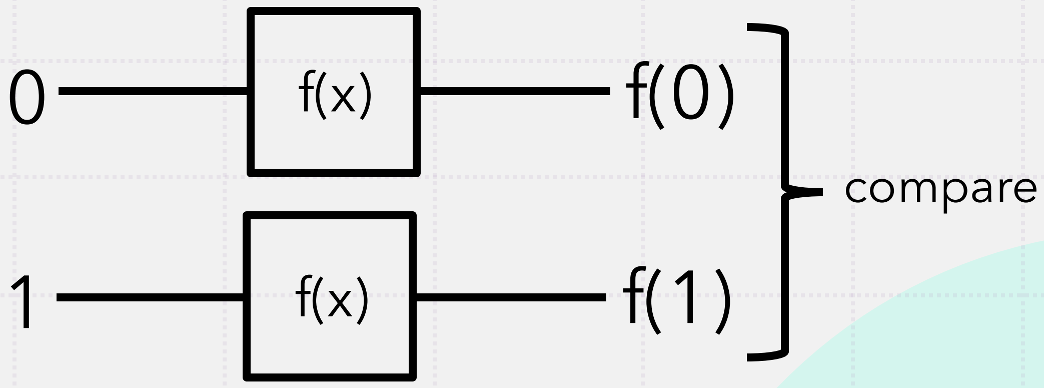
$f(0) \oplus f(1) = 0$ **constant**

$f(0) \oplus f(1) = 1$ **balanced**



1 step

Classical strategy:



2 steps

Deutsch-Josza Algorithm (2)

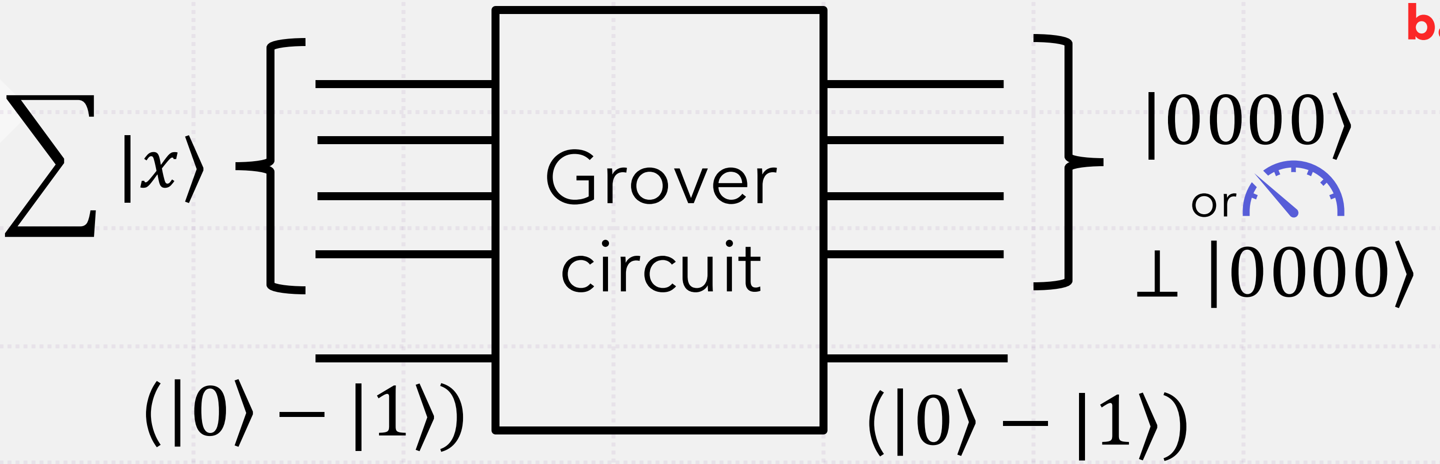
Generalization to m bit function: $f: \{0,1\}^m \mapsto \{0,1\}$

Promise: $f(x) = const. \forall x \in \{0,1\}^m$ **constant**

$$f(x) = \begin{cases} 0, & \forall x \in M_0 \\ 1, & \forall x \in M_1 \end{cases} \quad \text{with} \quad \begin{array}{l} M_0 \cup M_1 = \{0,1\}^m \\ M_0 \cap M_1 = 0 \\ |M_0| = |M_1| = 2^{m-1} \end{array}$$

balanced

Quantum strategy:

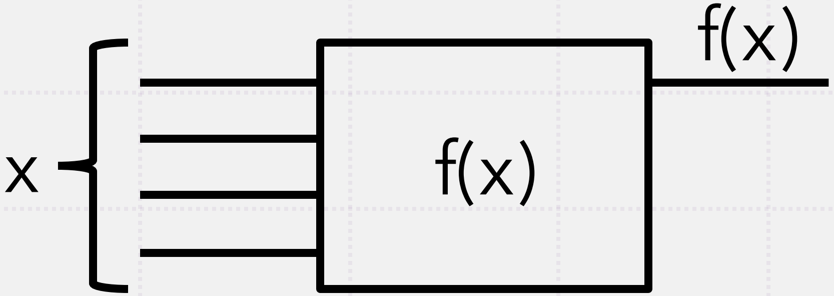


$|0000\rangle$ **constant**

Something else, e.g.:
$|0010\rangle$ **balanced**

1 step

Classical strategy:



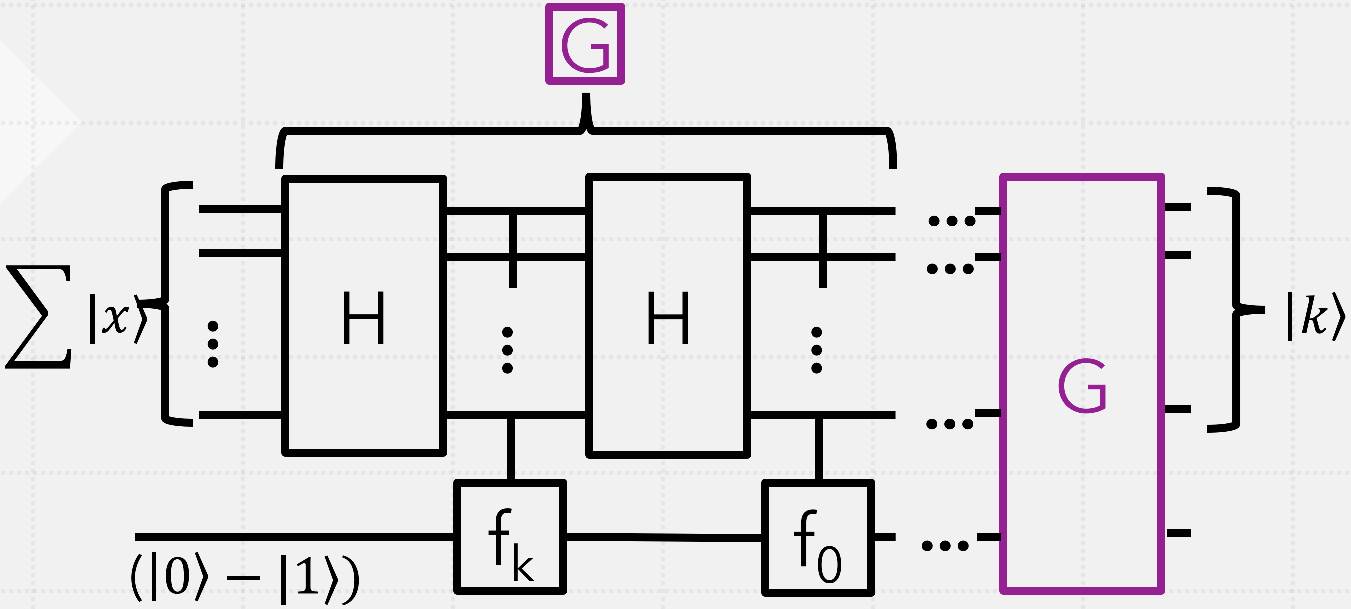
$2^{m-1}+1$ steps/repetitions

(in the worst case to be 100% sure about it)

Other Algorithms

Grover's Algorithm: $f: \{0,1\}^m \mapsto \{0,1\}$

$f(x) = \begin{cases} 1, & x = k \\ 0, & x \neq k \end{cases}$ $N = 2^m$ Numbers/ Bit patterns



Classically: $\mathcal{O}(N)$

Quantum: $\mathcal{O}(\sqrt{N})$ times we apply G

with probability $p = 1 - 1/\sqrt{N}$

Shor's Algorithm:

Prime number factorization

$N = p \cdot q$ N is a m bit number

Task: find p and q

Classical: $\mathcal{O}(\sqrt{N})$ Exponential in N

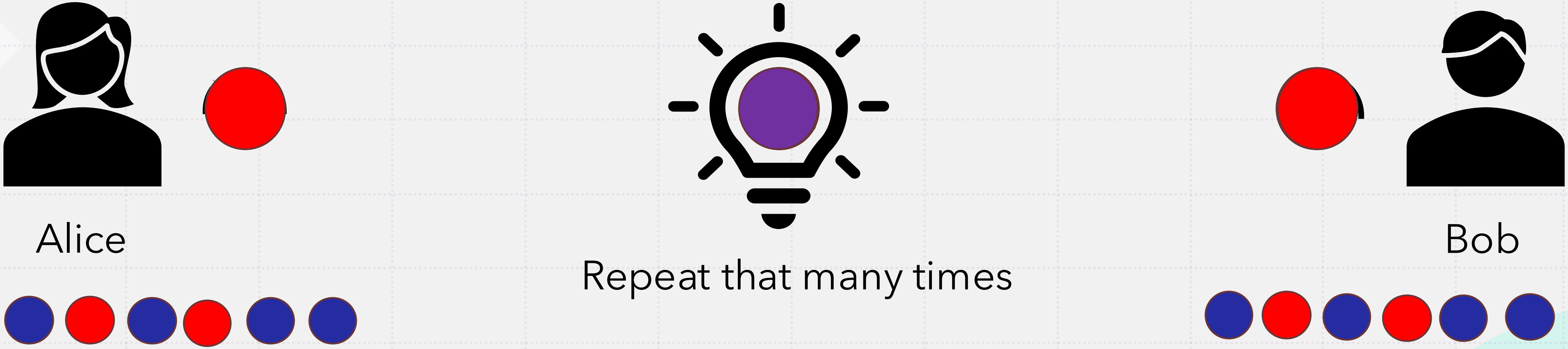
Quantum:

$\mathcal{O}((\log N)^2)$ → $\mathcal{O}(m^2)$

Exponential in number of bits m

Quantum Key Distribution

= 101011101001 (random sequence of 0, 1)



= 101011...

Eavesdropper detection

= 101011...

Teleportation

Alice has a qubit in the state: $|\Psi\rangle$

Task: get Bob the state

Alice and Bob share an **entangled state**