00000	00100	01000	01100
00001	00101	01001	01101
00010	00110	01010	01110
00011	00111	01011	01111
10000	10100	11000	11100
10001	10101	11001	11101
10010	10110	11010	11110
10011	10111	11011	11111

Introduction to **Quantum Computation**

ICTP-VAST-APCTP winter school
Hanoi, 12/2013

Daniel Nagaj

universität wien

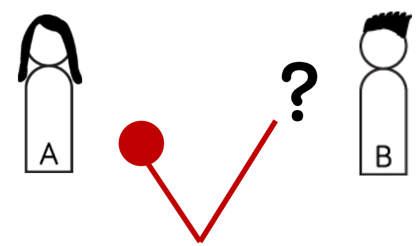
0 Review: 2 qubits

- how does a singlet (EPR pair) look locally?

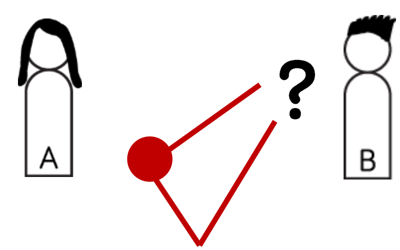
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

$$\rho_A = \mathrm{Tr}_B|\Psi^-\rangle\langle\Psi^-| = \frac{1}{2}\mathbb{I}$$

- what can Bob see on his qubit, if Alice chooses to do I, X, Y or Z on her qubit?



- what could Bob see, if Alice also sends him her qubit?

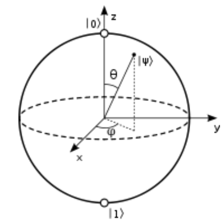


What is wrong with this illustration?

[QIP 2012, UMontréal]

1 **we need a qubit**

and we can use it

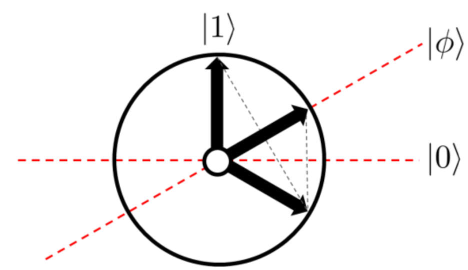


2 **EPR pairs**

give us cool 2-qubit protocols

3 **the algorithms**

that make quantum computing tick



4 **error correction**

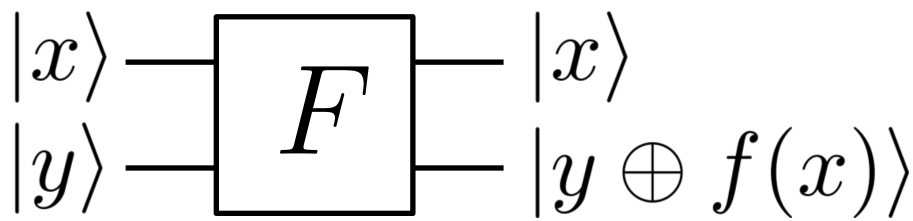
can we really scale up this stuff?

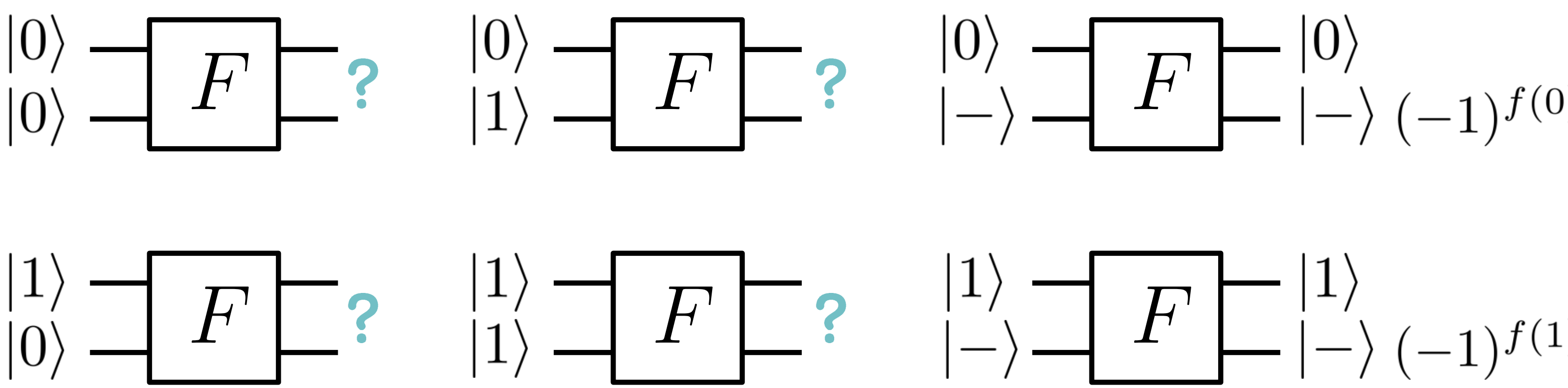
1 Deutsch's problem

$f_i(0)$	$f_i(1)$	
0	0	*constant*
0	1	*balanced*
1	0	*balanced*
1	1	*constant*

- 1-bit function f(x) …
  balanced or constant?

- act on a *superposition*?
  calculate it reversibly?



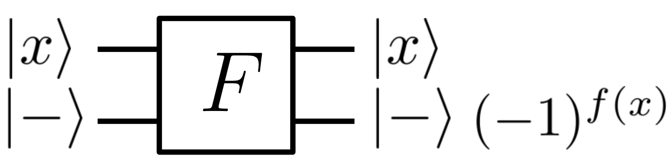


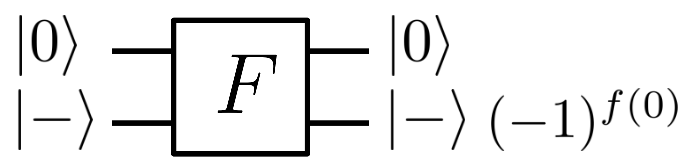
1 Deutsch's problem

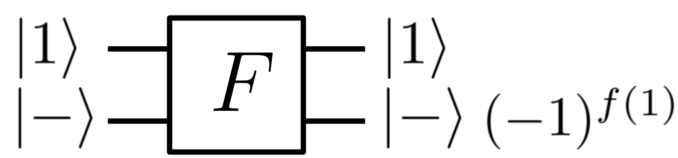
- 1-bit function f(x) …
  balanced or constant?

$f_i(0)$	$f_i(1)$	
0	0	*constant*
0	1	*balanced*
1	0	*balanced*
1	1	*constant*

- act on a *superposition*?
  calculate it reversibly?







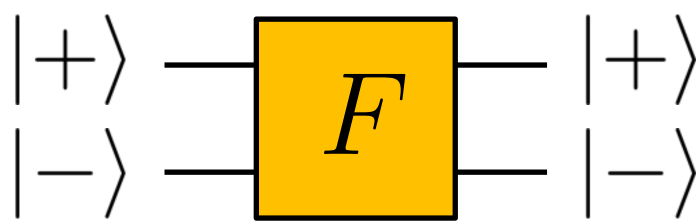
1 Deutsch's problem

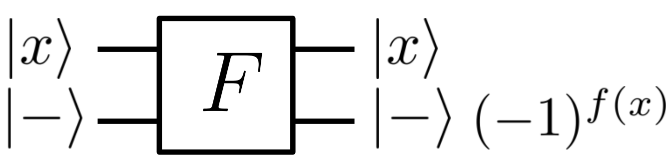
- 1-bit function f(x) …
  balanced or constant?

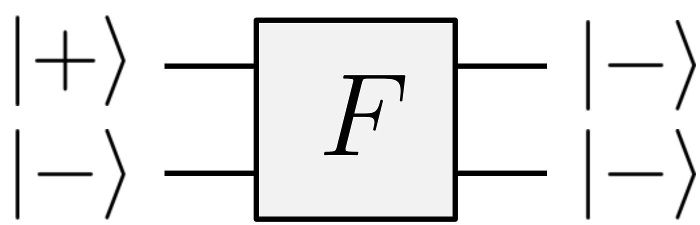
$f_i(0)$	$f_i(1)$	
0	0	*constant*
0	1	*balanced*
1	0	*balanced*
1	1	*constant*

- act on a *superposition*?
  calculate it reversibly?

Balanced/*constant* in 1 query.







1 Simon's problem: find a secret string

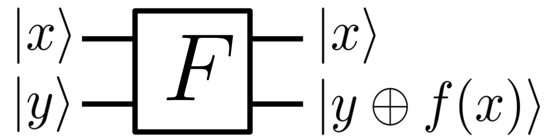
- a function on bit strings with a secret property

$$f(x) = f(x \oplus s) \qquad s = 10110$$

00000	00100	01000	01100
00001	00101	01001	01101
00010	00110	01010	01110
00011	00111	01011	01111
10000	10100	11000	11100
10001	10101	11001	11101
10010	10110	11010	11110
10011	10111	11011	11111

1 Simon's problem

- a function that hides a string $$f(x) = f(x \oplus s)$$
- reversibly, on a superposition



$$|+\rangle^{\otimes n} \otimes |0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

- measure the second register

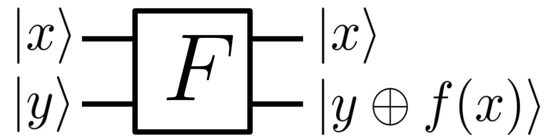
$$\rightarrow \frac{1}{\sqrt{2}} \big(|y\rangle + |y \oplus s\rangle\big) \otimes |f(y)\rangle$$

1 Simon's problem

- a function that hides a string

$$f(x) = f(x \oplus s)$$

- reversibly, on a superposition



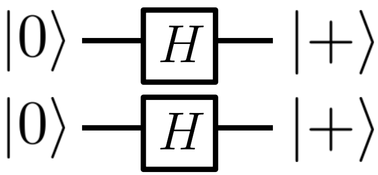
$$|+\rangle^{\otimes n} \otimes |0\rangle \Rightarrow \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$$

- measure the second register (and get rid of it)

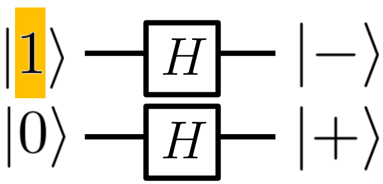
$$\Rightarrow \frac{1}{\sqrt{2}}\left(|y\rangle + |y \oplus s\rangle\right)$$

- apply H to each qubit

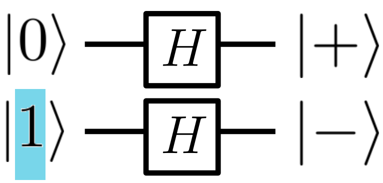
1 Applying the Hadamard to each qubit



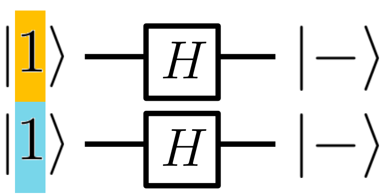
$$|00\rangle + |01\rangle + |10\rangle + |11\rangle \qquad (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$$



$$|00\rangle + |01\rangle - |10\rangle - |11\rangle \qquad (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle)$$



$$|00\rangle - |01\rangle + |10\rangle - |11\rangle$$



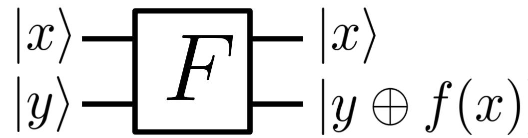
$$|00\rangle - |01\rangle - |10\rangle + |11\rangle$$

$$H^{\otimes n}|y_1\rangle|y_2\rangle \;\propto\; \sum_{z_1,z_2}(-1)^{y_1 z_1 + y_2 z_2}|z_1\rangle|z_2\rangle$$

$$\boxed{H^{\otimes n}|y\rangle = \frac{1}{\sqrt{2^n}}\sum_z (-1)^{y\cdot z}|z\rangle}$$

1 Simon's problem

- a function that hides a string $$f(x) = f(x \oplus s)$$
- reversibly, on a superposition



$$|+\rangle^{\otimes n} \otimes |0\rangle \quad \rightarrow \quad \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$$

- measure the second register (and get rid of it) $$\rightarrow \quad \frac{1}{\sqrt{2}} \left(|y\rangle + |y \oplus s\rangle \right)$$
- apply H to each qubit $$\rightarrow \quad \sum_z \left[(-1)^{y \cdot z} |z\rangle + (-1)^{(y \oplus s) \cdot z} |z\rangle \right]$$

$$H^{\otimes n} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_z (-1)^{y \cdot z} |z\rangle$$

1 Simon's problem

- a function that hides a string $$f(x) = f(x \oplus s)$$
- reversibly, on a superposition $$|x\rangle|y\rangle \xrightarrow{F} |x\rangle|y \oplus f(x)\rangle$$

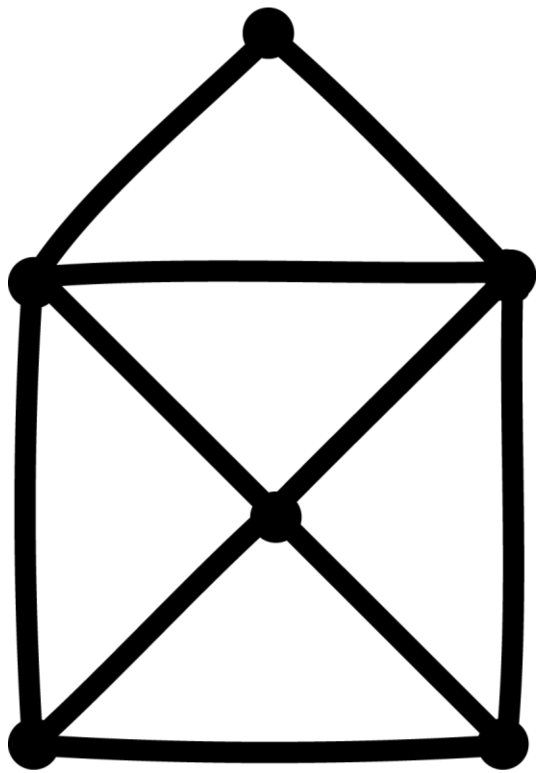
$$|+\rangle^{\otimes n} \otimes |0\rangle \quad \Rightarrow \quad \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$$

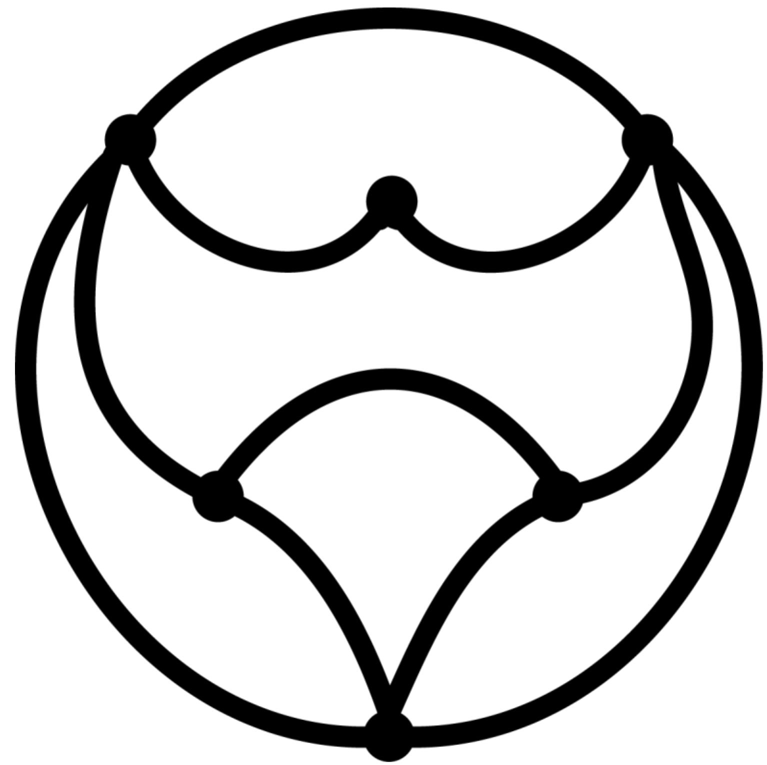
- measure the second register (and get rid of it) $$\Rightarrow \quad \frac{1}{\sqrt{2}}\left(|y\rangle + |y \oplus s\rangle\right)$$
- apply H to each qubit $$\Rightarrow \quad \sum_z \left[(-1)^{y \cdot z}|z\rangle + (-1)^{(y \oplus s)\cdot z}|z\rangle\right]$$

$$\propto \quad \sum_z \left(1 + (-1)^{s \cdot z}\right)|z\rangle$$

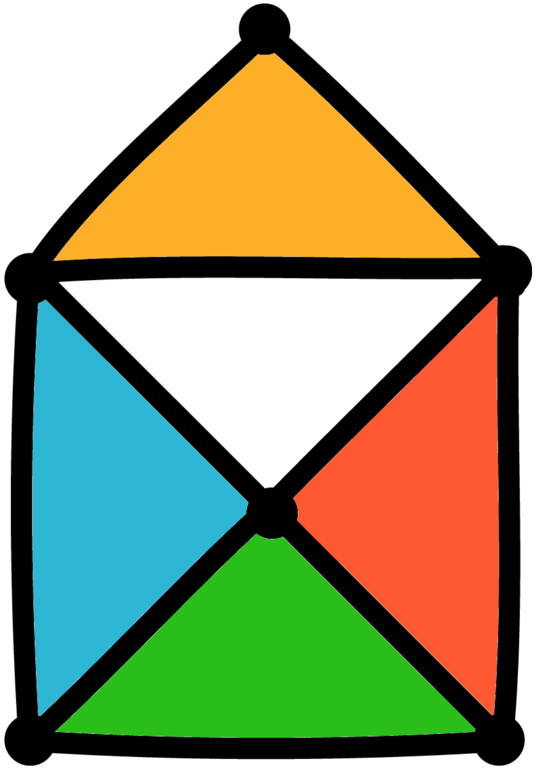
- only *z* orthogonal to the secret *s* survive … repeat a linear # of times & find the secret string

2 A graph isomorphism puzzle





2 A graph isomorphism puzzle



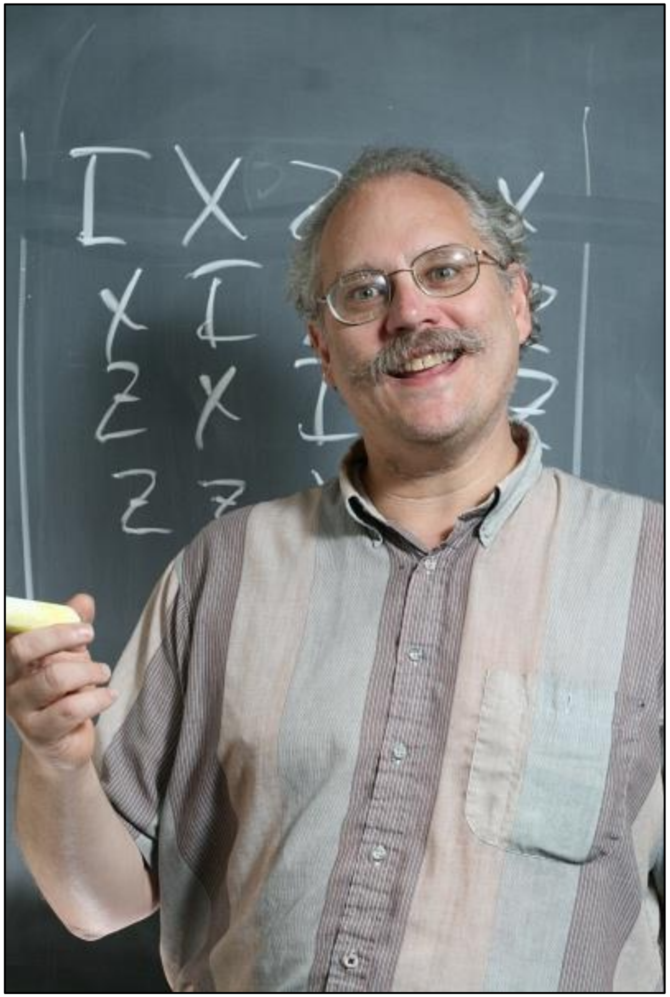
2 A factoring puzzle: is there a divisor < 12?

$$143 = 11 \times 13$$

2 A factoring puzzle: is there a divisor < 50?

$$114991 = 49 \times 1949$$

2 How to find factors?



$$N = p \times q$$

$$exp\left(n^{\frac{1}{3}}\right) \rightarrow n^{3}$$ [Shor94]

classical

quantum

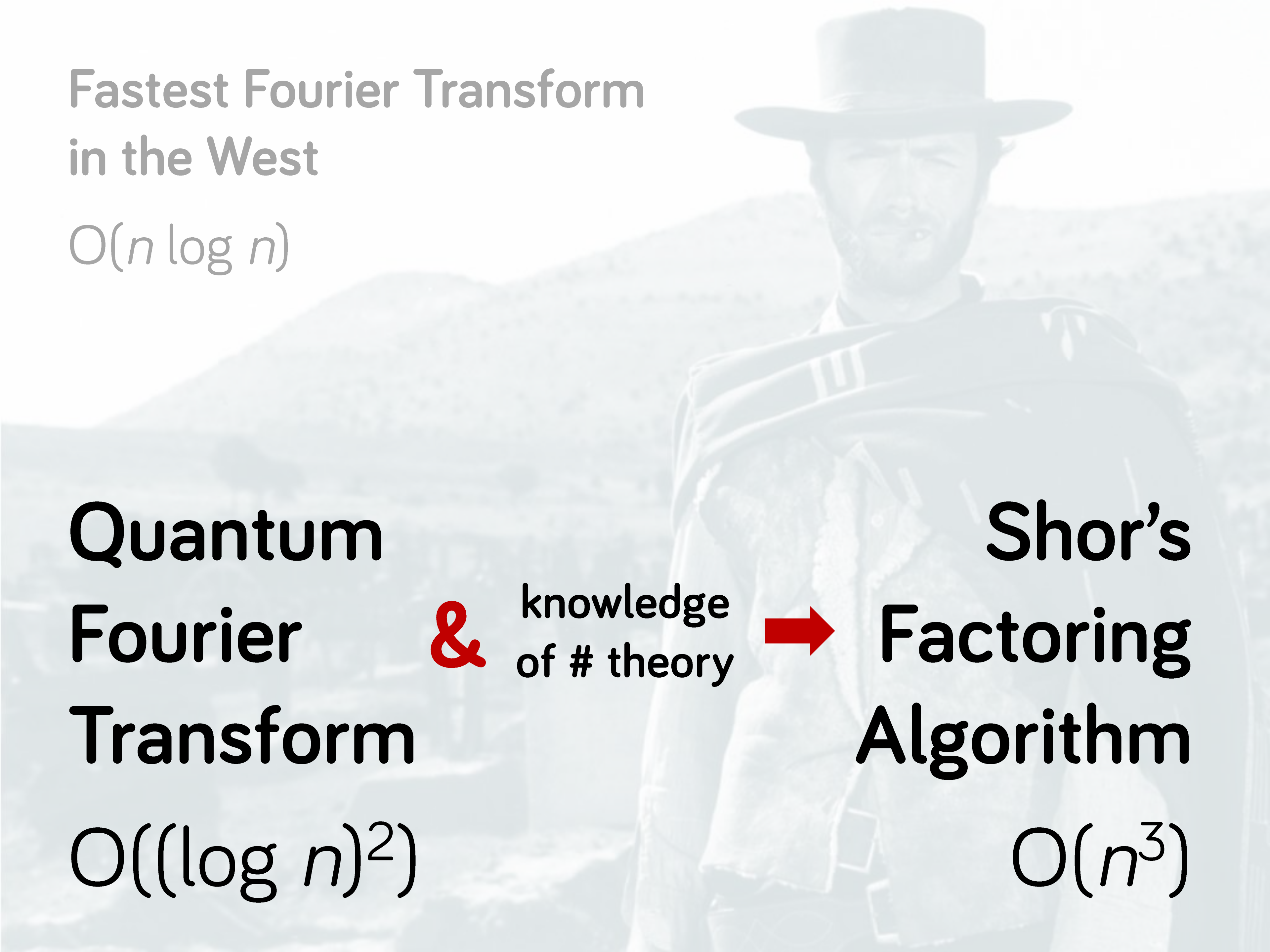
a transformation more interesting or powerful than

H H H H H H H

?

Fastest Fourier Transform in the West

$O(n \log n)$



Fastest Fourier Transform in the West

$O(n \log n)$

Quantum Fourier Transform & knowledge of # theory ➡ **Shor's Factoring Algorithm**

$O((\log n)^2)$

$O(n^3)$

2 Shor: order-finding ➡ factoring, breaking RSA crypto.

PUBLIC

PRIVATE

$$N = p \times q$$

(coprime) e

$$\phi = (p-1) \times (q-1)$$

$$d = e^{-1} \pmod{\phi}$$

ENCODING

$$C = P^e \pmod{N}$$

DECODING

$$P = C^d \pmod{N}$$

- find the order r of some x,

$$x^r = 1 \pmod{N}$$

this has a common factor with N

$$\left(x^{\frac{r}{2}} - 1\right)\left(x^{\frac{r}{2}} + 1\right)$$

3 Unstructured search

- an oracle marking a single element

$$O|w\rangle = -|w\rangle$$

$$O|x\rangle = |x\rangle_{(x \neq w)}$$

- is there any difference from Simon's problem?

00000	00100	01000	01100
00001	00101	01001	01101
00010	00110	01010	01110
00011	00111	01011	01111
10000	10100	11000	11100
10001	10101	11001	11101
10010	10110	11010	11110
10011	10111	11011	11111

- attempt to solve it

$$O|y\rangle = |y\rangle$$

$$O|w\rangle = -|w\rangle$$

only an overall phase!

a superposition
& relative phase

$$O\big(|y\rangle + |w\rangle\big) = \big(|y\rangle - |w\rangle\big)$$

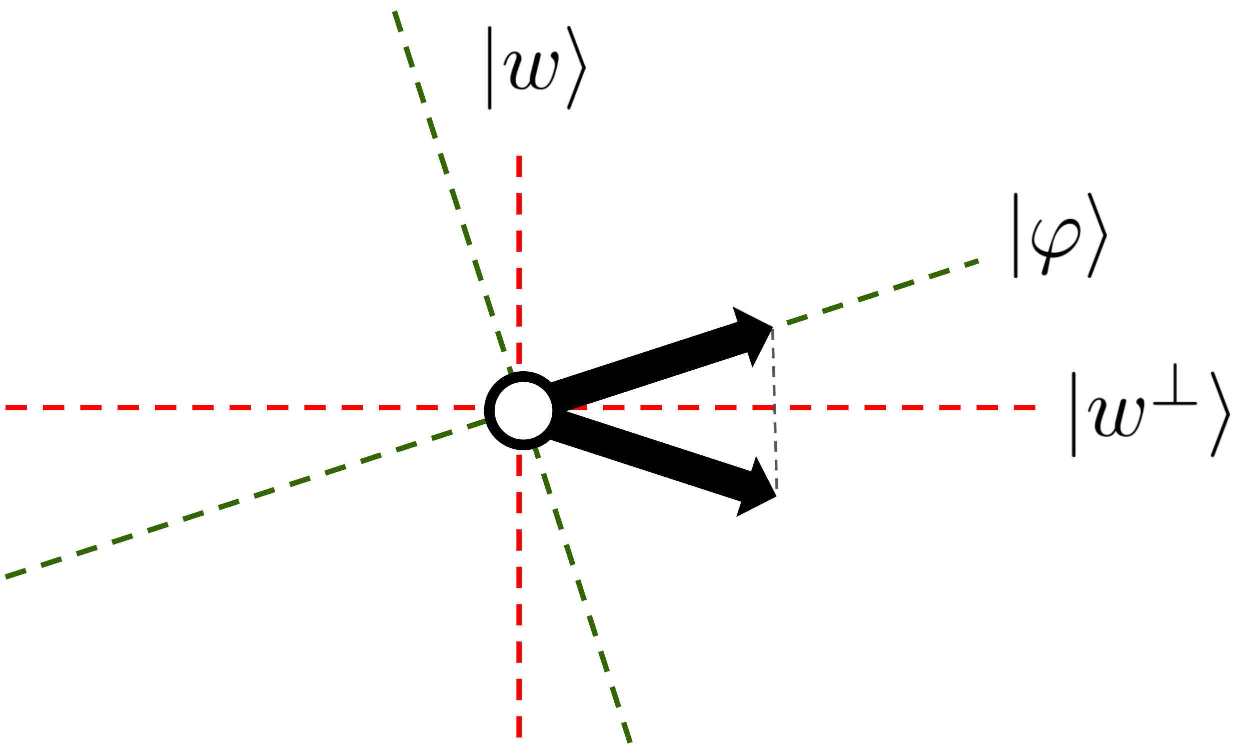
3 Unstructured search

- an oracle marking
  a single element

$$O|w\rangle = -|w\rangle$$

$$O|x\rangle = |x\rangle_{(x \neq w)}$$

- what can we do? ... reflect using the oracle

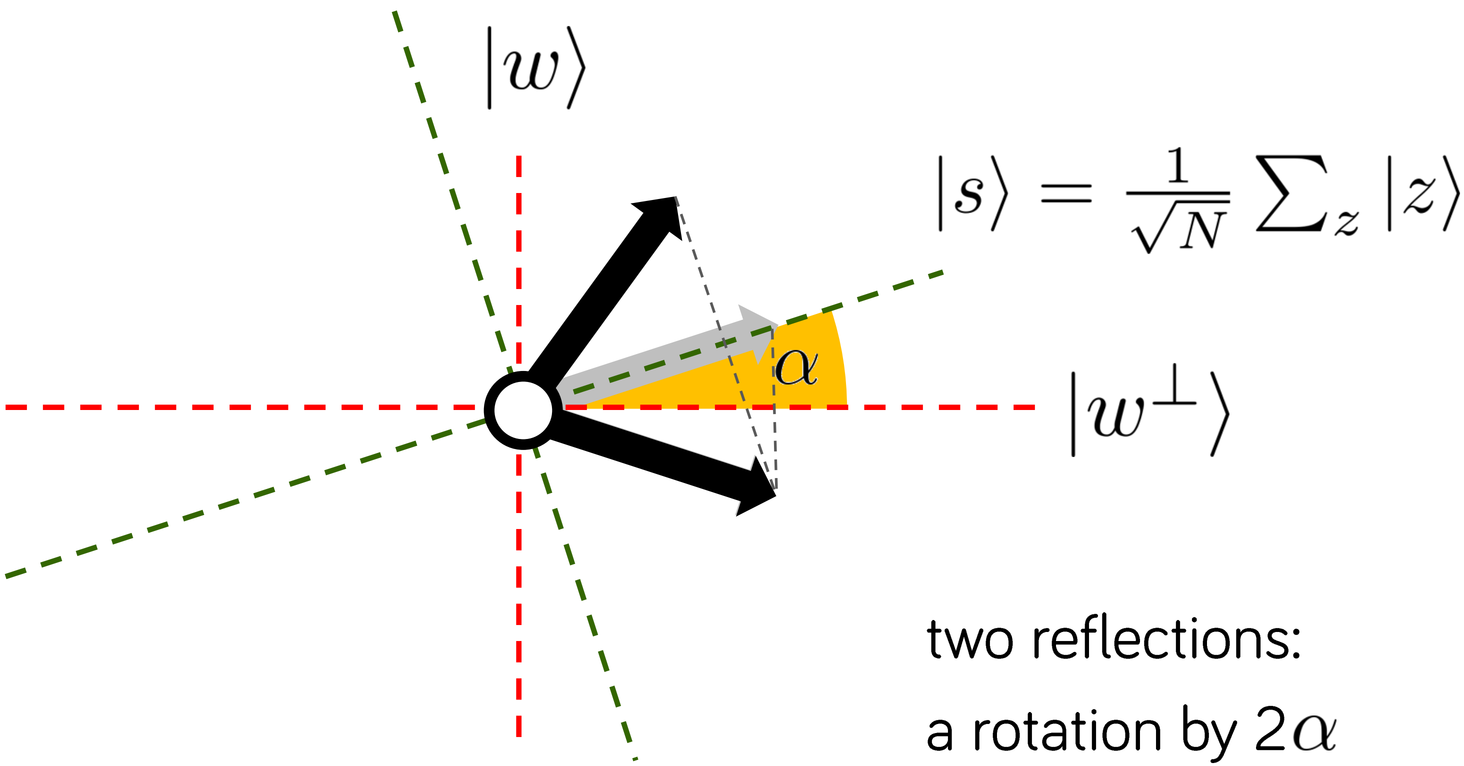


3 Unstructured search

- an oracle marking a single element

$$O|w\rangle = -|w\rangle$$
$$O|x\rangle = |x\rangle_{(x \neq w)}$$

- what can we do? … use a known reflection.



two reflections:

a rotation by 2α

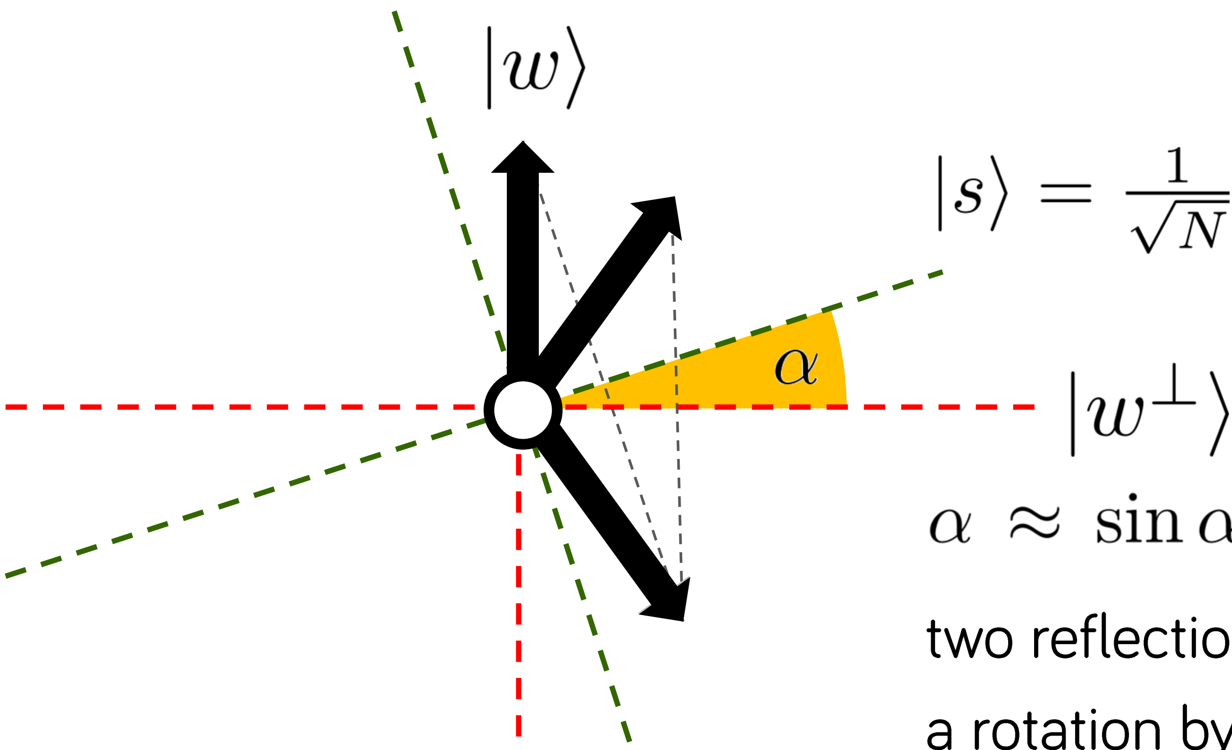
3 Grover's algorithm

- an oracle marking a single element

$$O|w\rangle = -|w\rangle$$

$$O|x\rangle = |x\rangle_{(x \neq w)}$$

- continue … reflect using the oracle … and again using s



$$|s\rangle = \frac{1}{\sqrt{N}} \sum_z |z\rangle$$

$$\alpha \approx \sin\alpha \approx \frac{1}{\sqrt{N}}$$

two reflections:

a rotation by 2α

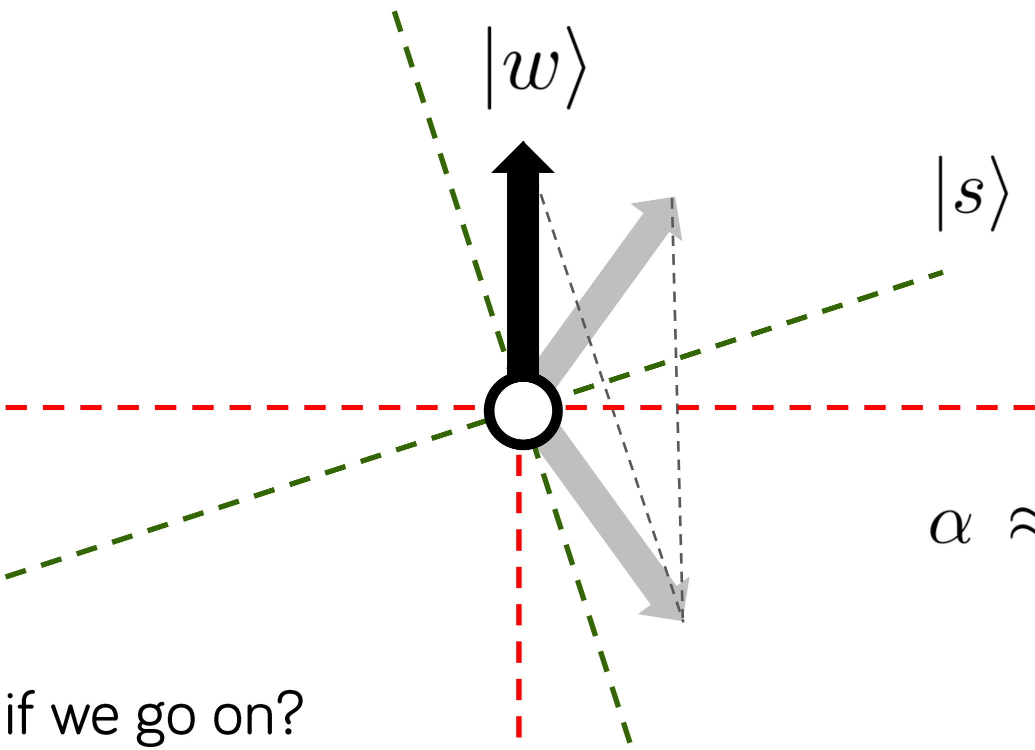
3 Grover's algorithm

- an oracle marking a single element

$$O|w\rangle = -|w\rangle$$

$$O|x\rangle = |x\rangle_{(x \neq w)}$$

- continue … reflect using the oracle … and again using s



$$|s\rangle = \frac{1}{\sqrt{N}} \sum_z |z\rangle$$

$$|w^\perp\rangle$$

$$\alpha \approx \sin\alpha \approx \frac{1}{\sqrt{N}}$$

$\sqrt{N}$ steps

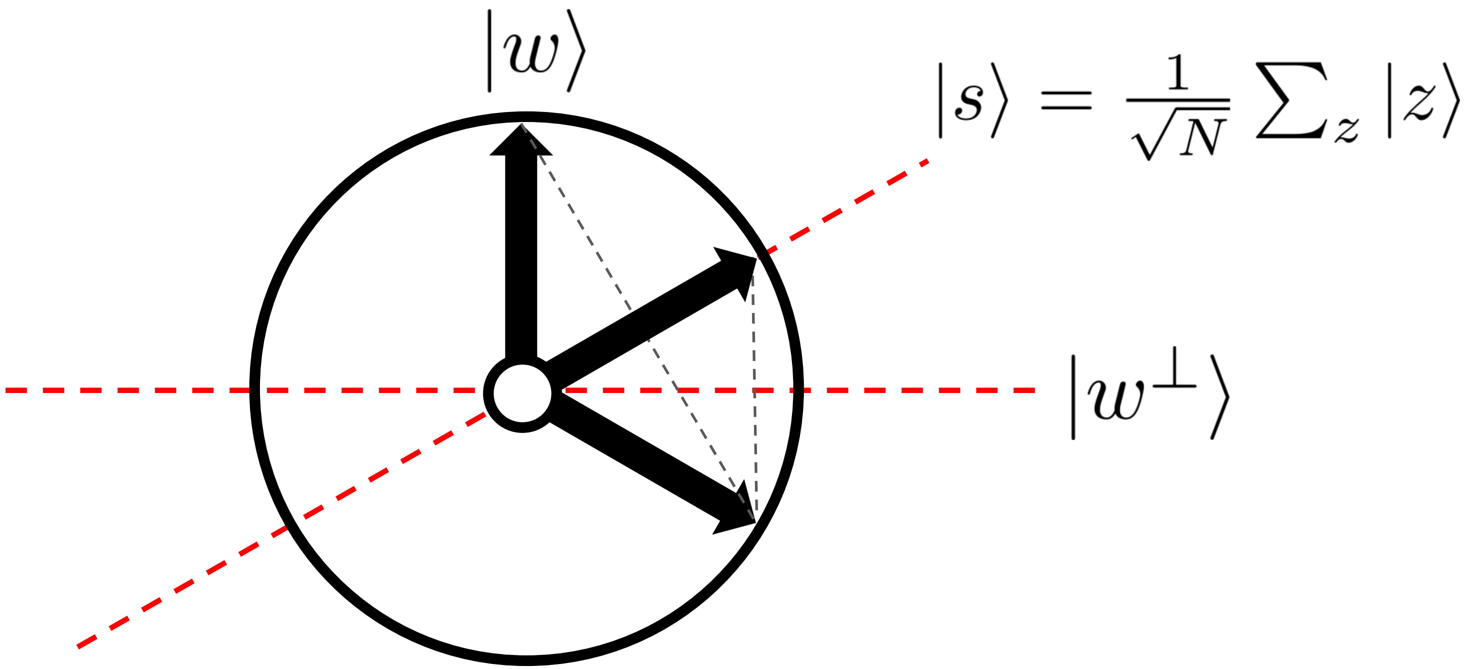
- what if we go on?

3 Grover's algorithm: an example

- an oracle marking a single element

$$O|w\rangle = -|w\rangle$$
$$O|x\rangle = |x\rangle_{(x \neq w)}$$

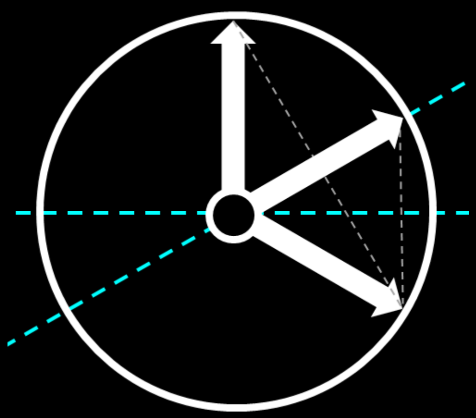
- how does it work for 2 qubits with the marked state $|00\rangle$?



$f_i(0)$	$f_i(1)$
0	0
0	1
1	0
1	1

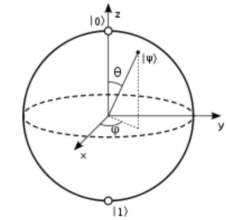
00000
00101
01010
01111
11100
11001
10110
10011

$$N = p \times q$$



1 we need a qubit

and we can use it

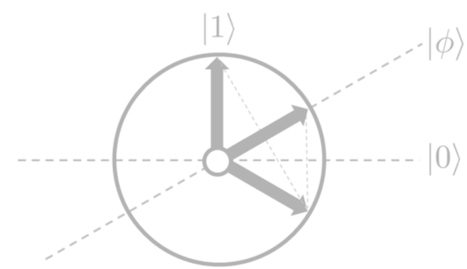


2 EPR pairs

give us cool 2-qubit protocols

3 the algorithms

that make quantum computing tick



4 error correction

can we really scale up this stuff?