Grover's algorithm

Application to a satisfiability problem

Isabelle
isabelle.viarouge@usherbrooke.ca

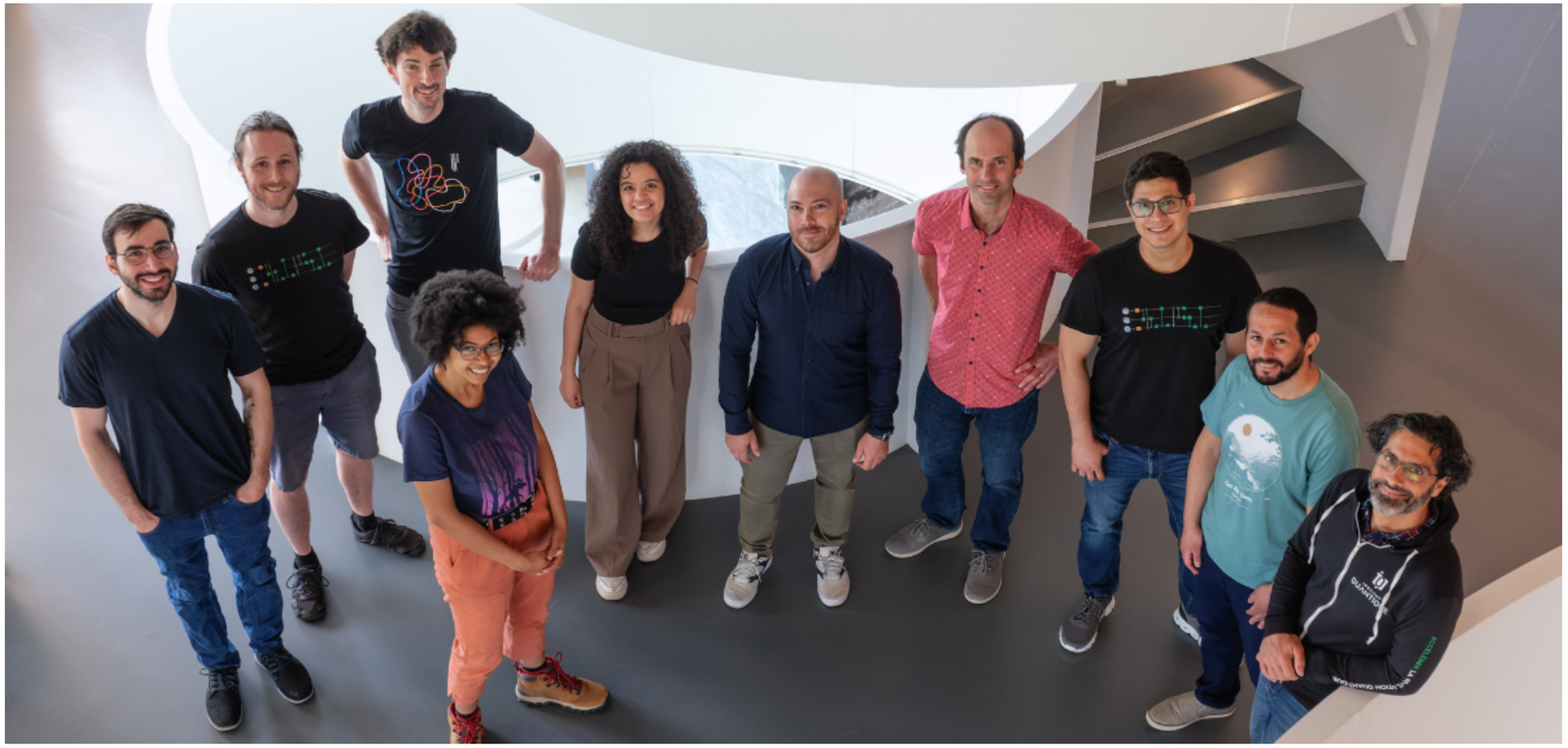
Sherbrooke
November 3rd 2025

UdS Université de Sherbrooke

Who are we?

Quantum algorithm laboratory

ALGOLAB QUANTIQUE



INSTITUT QUANTIQUE

UDS Université de Sherbrooke

Grover ’s Algorithm

Grover’s algorithm **searches** one or several elements satisfying a **given criteria** inside an **unstructured list** of many elements.

Classically, this problem needs $O(N)$ operations on average meanwhile Grover takes $O(\sqrt{N})$ operations.

A Function to Satisfy

A search in an **unstructured list** is analogous to a function taking an **integer** as input and outputting…

$$f(x) = \begin{cases} 0 & \text{For most inputs} \\ 1 & \text{For } x = x^\star \end{cases}$$

We are looking for which **input(s)** the function returns

$$f(x^\star) = 1 \qquad\qquad x^\star = ?$$

Example :

$$f_{774-2159}(x)$$

Natives of the Pincus planet*

The problem

Travellers to the planet Pincus have observed that all its **healthy** natives are **noisy**, unless they are **fearful**. Those who are **fearful** and **quiet** are **happy**, as are those who are **healthy** and **noisy**. The **happy** and **quiet** natives are **healthy**, but those who are **fearful** and **healthy** are **unhappy**. Finally, even though the **unhappy** and **unhealthy** natives are always **afraid**, the **fearful** and **noisy** ones are **healthy.**

Fearful / Courageous

Happy / Unhappy

Unhealthy / Healthy

Noisy / Quiet

What can we deduce about the natives of the Pincus planet?

*Problem adapted from *The Art of Computer Programming*, Volume 4, Donald E. Knuth

Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

A bit of logic

A bit of logic

Logical operators

The **conjunction** (x **and** y) : $x \wedge y$ is true if x is true **and** y is true

The **disjunction** (x **or** y) : $x \vee y$ is true if x is true **or** y is true

The **negation** (**not** x) : $\neg x$ is true if x is false (also written $\bar{x}$)

x	y	$x \wedge y$
F	F	F
T	F	F
F	T	F
T	T	T

x	$\bar{x}$
F	T
T	F

A bit of logic

Logical formula and satisfiability

A **statement** is a composition of **logical variables** using **conjunctions**, **disjunctions** and **negations**.

$$f = (x \wedge \bar{y}) \wedge (\bar{x} \vee z)$$

It is said to be **satisfiable** if we can **assign values** (true/false) so that the formula **evaluates to true**.

x	y	z
F	F	F
T	F	F
F	T	F
T	T	F
F	F	T
T	F	T
F	T	T
T	T	T

A bit of logic

De Morgan's Law

One can convert a **conjunction** (and) into a **disjunction** (or) with the **De Morgan** relation.

$$f = x \wedge y = \neg(\bar{x} \vee \bar{y})$$

For example, suppose the following logical variables describe an object:

- This object is a **fruit** (x is true);
- This object is **yellow** (y is true);
- This object is a **banana** (f is true).

De Morgan's relation tells us that:

If an object is **not a fruit** or **is not yellow**, it is **not a banana**.

A bit of logic

De Morgan law

One can convert a **conjunction** (and) into a **disjunction** (or) with the **De Morgan** relation.

$$f = x \wedge y = \neg(\bar{x} \vee \bar{y})$$

x	y	$x \wedge y$
F	F	F
T	F	F
F	T	F
T	T	T

$\bar{x}$	$\bar{y}$	$\bar{x} \vee \bar{y}$	$\neg(\bar{x} \vee \bar{y})$
T	T	T	F
F	T	T	F
T	F	T	F
F	F	F	T

A bit of logic

Conditional statement

x	y
F	?
T	T

A conditional statement

$$x \rightarrow y$$

implies that if x is true, y is also true. If x is false, nothing is known about y.

For example, suppose the logical variables describe

- Sam ate a **banana** (x is true)
- Sam ate a **fruit** (y is true)

If Sam **ate a banana**, then he **ate a fruit**. If Sam **did not eat a banana**, we **cannot determine** whether he ate a fruit or not.

A bit of logic

Inference rule

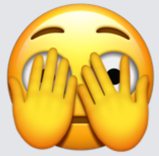
The **inference rule** is used to translate a **conditional proposition** into a **disjunction** which will be **true** if the **conditional proposition** is **satisfied**.

$$x \rightarrow y \qquad \longrightarrow \qquad \bar{x} \vee y$$

x	y	$x \rightarrow y$	$\bar{x} \vee y$
F	F	✓	T
T	F	✗	F
F	T	✓	T
T	T	✓	T

Natives of the Pincus planet

The logical variables

		True (1)	False (0)
	x_0	Fearful	Courageous
	x_1	Happy	Unhappy
	x_2	Unhealthy	Healthy
	x_3	Noisy	Quiet

Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Natives of the Pincus planet

The statements

… **healthy** natives are **noisy**, unless they are **fearful**.

If a native is **healthy** and **courageous**, they are **noisy**.

$$\bar{x}_2 \wedge \bar{x}_0 \rightarrow x_3$$

		Vrai	Faux
🫣	x_0	Fearful	Courageous
😀	x_1	Happy	Unhappy
🤢	x_2	Unhealthy	Healthy
🥳	x_3	Noisy	Quiet

Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Natives of the Pincus planet

Converting a conditional statement into a conjunction

First, we use the **inference rule**

$$\bar{x}_2 \wedge \bar{x}_0 \rightarrow x_3 \longrightarrow \neg(\bar{x}_2 \wedge \bar{x}_0) \vee x_3 \qquad x \rightarrow y \longrightarrow \bar{x} \vee y$$

Then, we use the **De Morgan** rule

$$\neg(\bar{x}_2 \wedge \bar{x}_0) \vee x_3 = x_0 \vee x_2 \vee x_3 \qquad \neg(\bar{x} \wedge \bar{y}) = x \vee y$$

Finally, we combine the two to obtain our **conversion rule**

$$\bar{x}_2 \wedge \bar{x}_0 \rightarrow x_3 = x_0 \vee x_2 \vee x_3 \qquad x \wedge y \rightarrow z = \bar{x} \vee \bar{y} \vee z$$

Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Natives of the Pincus planet

The statements

	$x \wedge y \rightarrow z$	$\longrightarrow \quad \bar{x} \vee \bar{y} \vee z$
If a **healthy** native is **courageous**, they are also **noisy**.	$\bar{x}_2 \wedge \bar{x}_0 \rightarrow x_3$	$x_2 \vee x_0 \vee x_3$
If a native is **fearful** and **quiet**, they are also **happy.**	$x_0 \wedge \bar{x}_3 \rightarrow x_1$	$\bar{x}_0 \vee x_3 \vee x_1$
If a native is **healthy** and **noisy**, they are also **happy**.	$\bar{x}_2 \wedge x_3 \rightarrow x_1$	$x_2 \vee \bar{x}_3 \vee x_1$
If a native is **happy** and **quiet**, they are also **healthy**.	$x_1 \wedge \bar{x}_3 \rightarrow \bar{x}_2$	$\bar{x}_1 \vee x_3 \vee \bar{x}_2$
If a native is **fearful** and **healthy**, they are also **unhappy**.	$x_0 \wedge \bar{x}_2 \rightarrow \bar{x}_1$	$\bar{x}_0 \vee x_2 \vee \bar{x}_1$
If a native is **unhappy** and **unhealthy**, they are also **fearful**.	$\bar{x}_1 \wedge x_2 \rightarrow x_0$	$x_1 \vee \bar{x}_2 \vee x_0$
If a native is **fearful** and **noisy**, they are also **healthy**.	$x_0 \wedge x_3 \rightarrow \bar{x}_2$	$\bar{x}_0 \vee \bar{x}_3 \vee \bar{x}_2$

		VRAI	FAUX
🫣	x_0	Fearful	Courageous
😀	x_1	Happy	Unhappy
🤢	x_2	Unhealthy	Healthy
🥳	x_3	Noisy	Quiet

Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Natives of the Pincus planet

The main statement

We can then assemble the **main statement** of the problem

$$f(x_0, x_1, x_2, x_3) =$$

$$(x_2 \vee x_0 \vee x_3) \wedge (\bar{x}_0 \vee x_3 \vee x_1) \wedge (x_2 \vee \bar{x}_3 \vee x_1) \wedge (\bar{x}_1 \vee x_3 \vee \bar{x}_2) \wedge (\bar{x}_0 \vee x_2 \vee \bar{x}_1) \wedge (x_1 \vee \bar{x}_2 \vee x_0) \wedge (\bar{x}_0 \vee \bar{x}_3 \vee \bar{x}_2)$$

We can deduce how the natives of the planet Pincus are, if we find a **combination** of **logical variables** so that this formula **evaluates to True**.

		VRAI	FAUX
😳	x_0	Fearful	Courageous
😀	x_1	Happy	Unhappy
🤢	x_2	Unhealthy	Healthy
🥳	x_3	Noisy	Quiet

Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Satisfiability problems

The statements

We want to know if there is a configuration that satisfies the **logical formula**

$$f(\overset{?}{x_0}, \overset{?}{x_1}, \overset{?}{x_2}, \overset{?}{x_3}) = 1$$

$$f(x_0, x_1, x_2, x_3) = (x_2 \vee x_0 \vee x_3) \wedge (\bar{x}_0 \vee x_3 \vee x_1) \wedge (x_1 \vee \bar{x}_3 \vee x_2) \wedge (\bar{x}_1 \vee x_3 \vee \bar{x}_2) \wedge (\bar{x}_0 \vee x_2 \vee \bar{x}_1) \wedge (x_1 \vee \bar{x}_2 \vee x_0) \wedge (\bar{x}_0 \vee \bar{x}_3 \vee \bar{x}_2)$$

For example,

$$f(0,0,0,0) = (0 \vee 0 \vee 0) \wedge (1 \vee 0 \vee 0) \wedge (0 \vee 1 \vee 0) \wedge (1 \vee 0 \vee 1) \wedge (1 \vee 0 \vee 1) \wedge (0 \vee 1 \vee 0) \wedge (1 \vee 1 \vee 1) = 0$$

$$f(1,1,1,1) = (1 \vee 1 \vee 1) \wedge (0 \vee 1 \vee 1) \wedge (1 \vee 0 \vee 1) \wedge (0 \vee 1 \vee 0) \wedge (0 \vee 1 \vee 0) \wedge (1 \vee 0 \vee 1) \wedge (0 \vee 0 \vee 0) = 0$$

		VRAI	FAUX
😳	x_0	Fearful	Courageous
😀	x_1	Happy	Unhappy
🤢	x_2	Unhealthy	Healthy
🥳	x_3	Noisy	Quiet

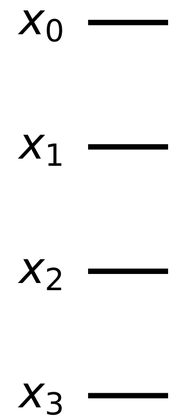
Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Grover’s algorithm

Encoding in qubits

We assign a **qubit** to each **logical variable**

$$f(x_0, x_1, x_2, x_3) \qquad\qquad |x_3 x_2 x_1 x_0\rangle$$



We summarize these variables in the form of a **vector** of binary components or a **basis state**

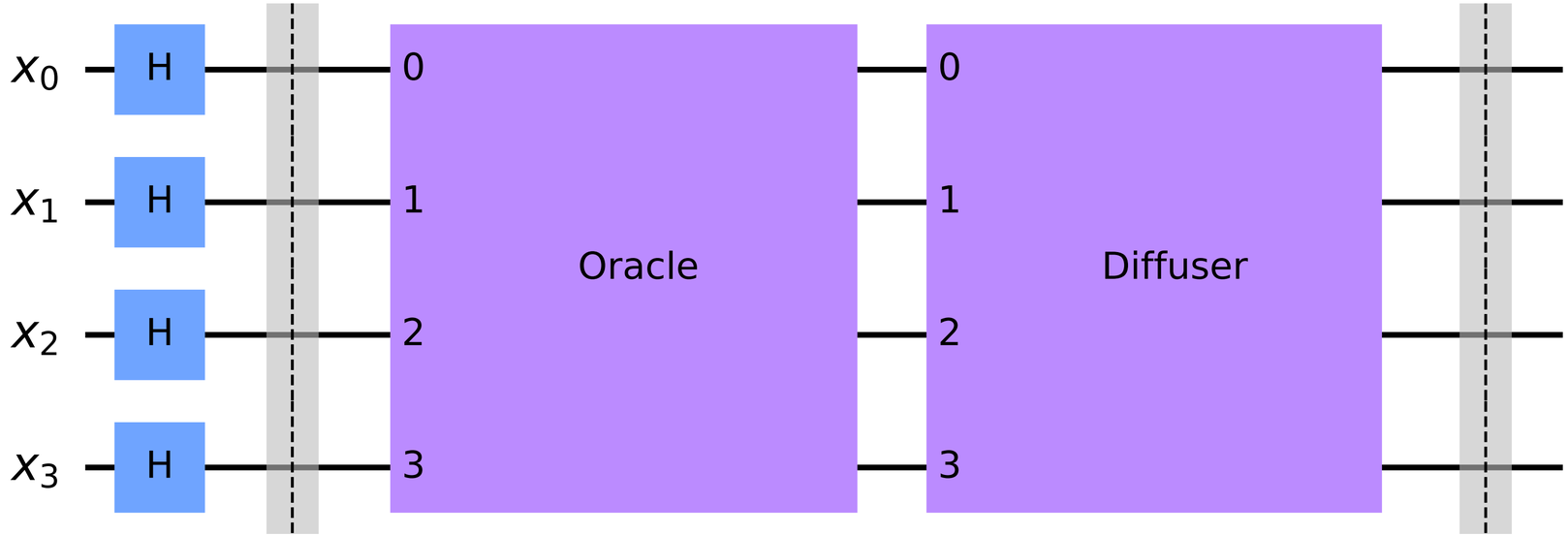
$$\mathbf{x} = (x_0, x_1, x_2, x_3) \qquad\qquad |\mathbf{x}\rangle = |x_3 x_2 x_1 x_0\rangle$$

The **main statement** evaluation is as follows

$$f(\mathbf{x})$$

Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Grover's algorithm



Oracle

Mark the states by reversing their **phase**.

Diffuser

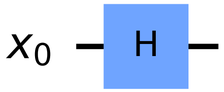
Amplifies the **probabilities** for states whose phase is reversed.

Grover's algorithm

The state of uniform superposition

A **Hadamard gate** on a **qubit** allows to prepare a **superposition**

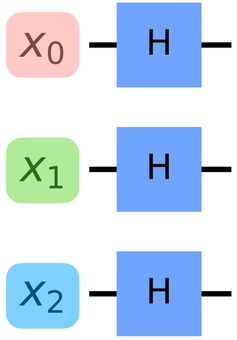
$$\hat{H}\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle$$



Hadamard gates on **several qubits** allow to prepare the **uniform superposition** state

$$|+\rangle \otimes |+\rangle \otimes |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$



Grover's algorithm

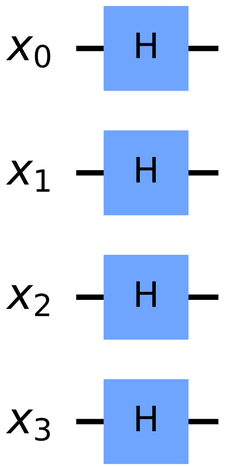
The state of uniform superposition

Hadamard gates on **several qubits** allow to prepare the **uniform superposition** state

$$|+++\rangle = \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

For a system of *n* qubits, the **uniform superposition state** is

$$|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}\rangle$$



and includes all **2^n possibilities.**

Grover's algorithm

The *good* and the *bad* states

For a system of *n* qubits, the **uniform superposition state** is

$$|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}\rangle$$

Among these states, some **satisfy the main statement** f (the good), while the others do not (the bad)

$$|s\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{\mathbf{x} \in B} |\mathbf{x}\rangle + \sum_{\mathbf{x} \in G} |\mathbf{x}\rangle \right)$$

Grover's algorithm

The *good* and the *bad* states

$$|s\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{\mathbf{x} \in B} |\mathbf{x}\rangle + \sum_{\mathbf{x} \in G} |\mathbf{x}\rangle \right)$$

We can therefore write the **uniform superposition state** as a **combination** of **two states**

$$|s\rangle = \cos(\theta/2)\,|b\rangle + \sin(\theta/2)\,|g\rangle$$

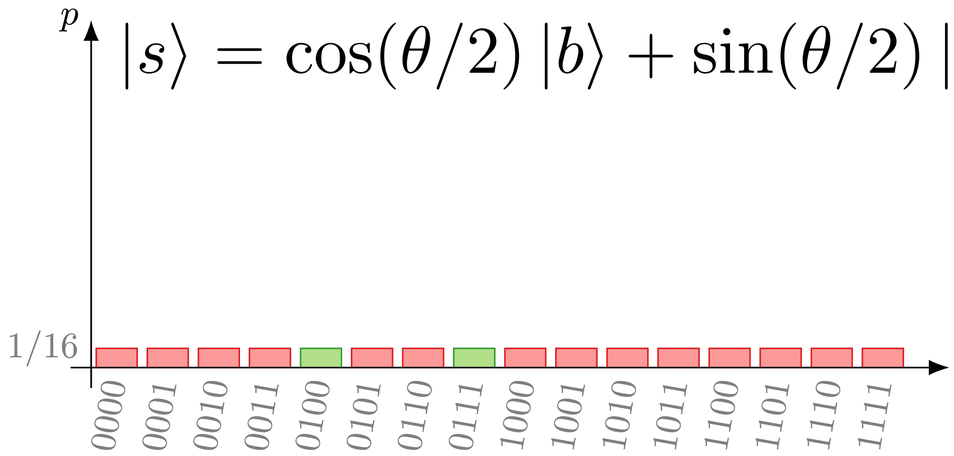
with the states

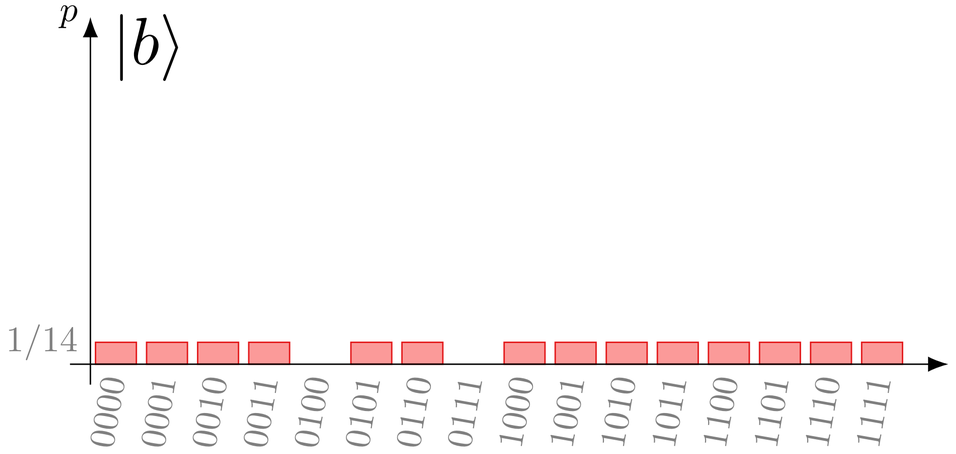
$$\cos(\theta/2)\,|b\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in B} |\mathbf{x}\rangle \qquad \sin(\theta/2)\,|g\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in G} |\mathbf{x}\rangle$$

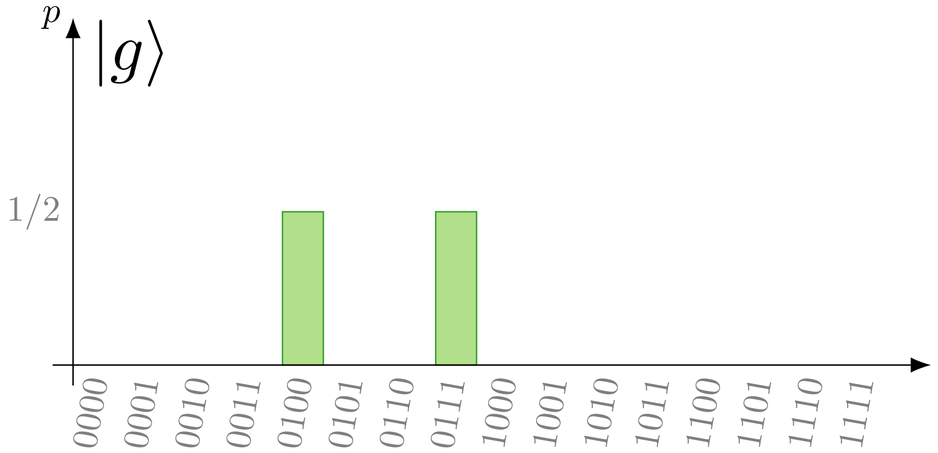
Grover's algorithm

The *good* and the *bad* states

$$|s\rangle = \cos(\theta/2)\,|b\rangle + \sin(\theta/2)\,|g\rangle$$



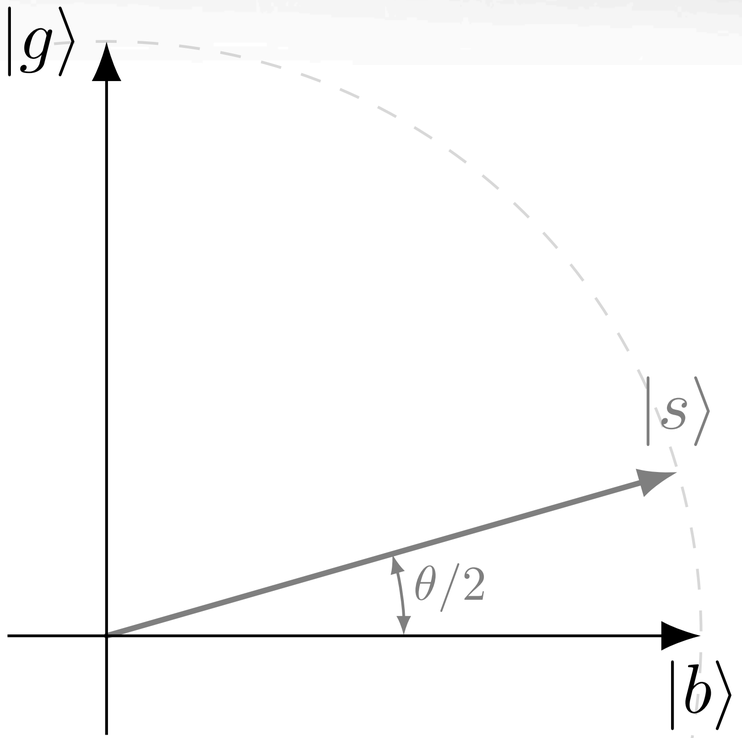




Grover's algorithm

Working principle

$$|s\rangle = \cos(\theta/2)\,|b\rangle + \sin(\theta/2)\,|g\rangle$$

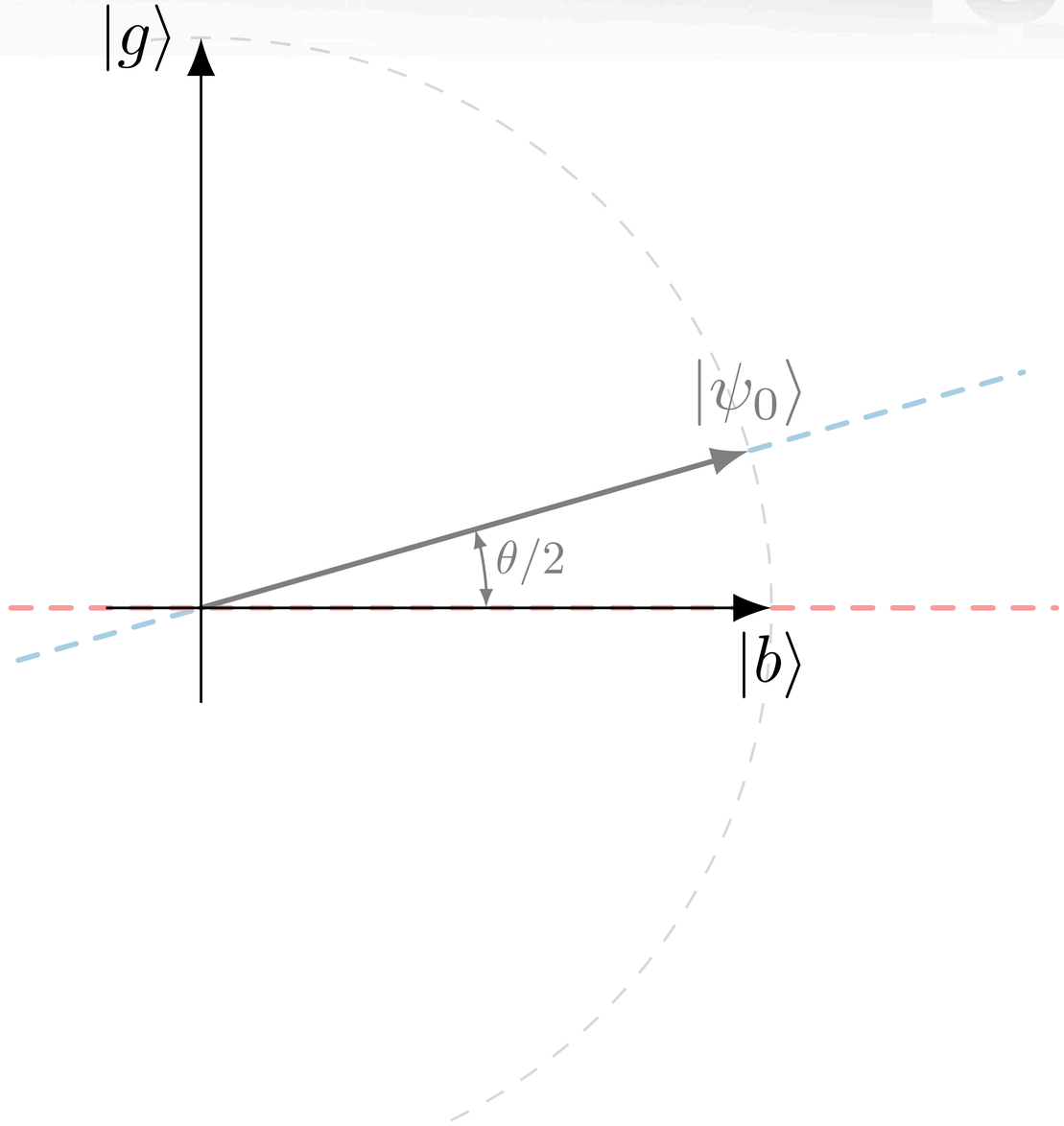


Grover's algorithm

Working principle

$$|\psi_0\rangle = \cos(\theta/2)\,|b\rangle + \sin(\theta/2)\,|g\rangle$$

$$p_g = \sin^2(\theta/2)$$

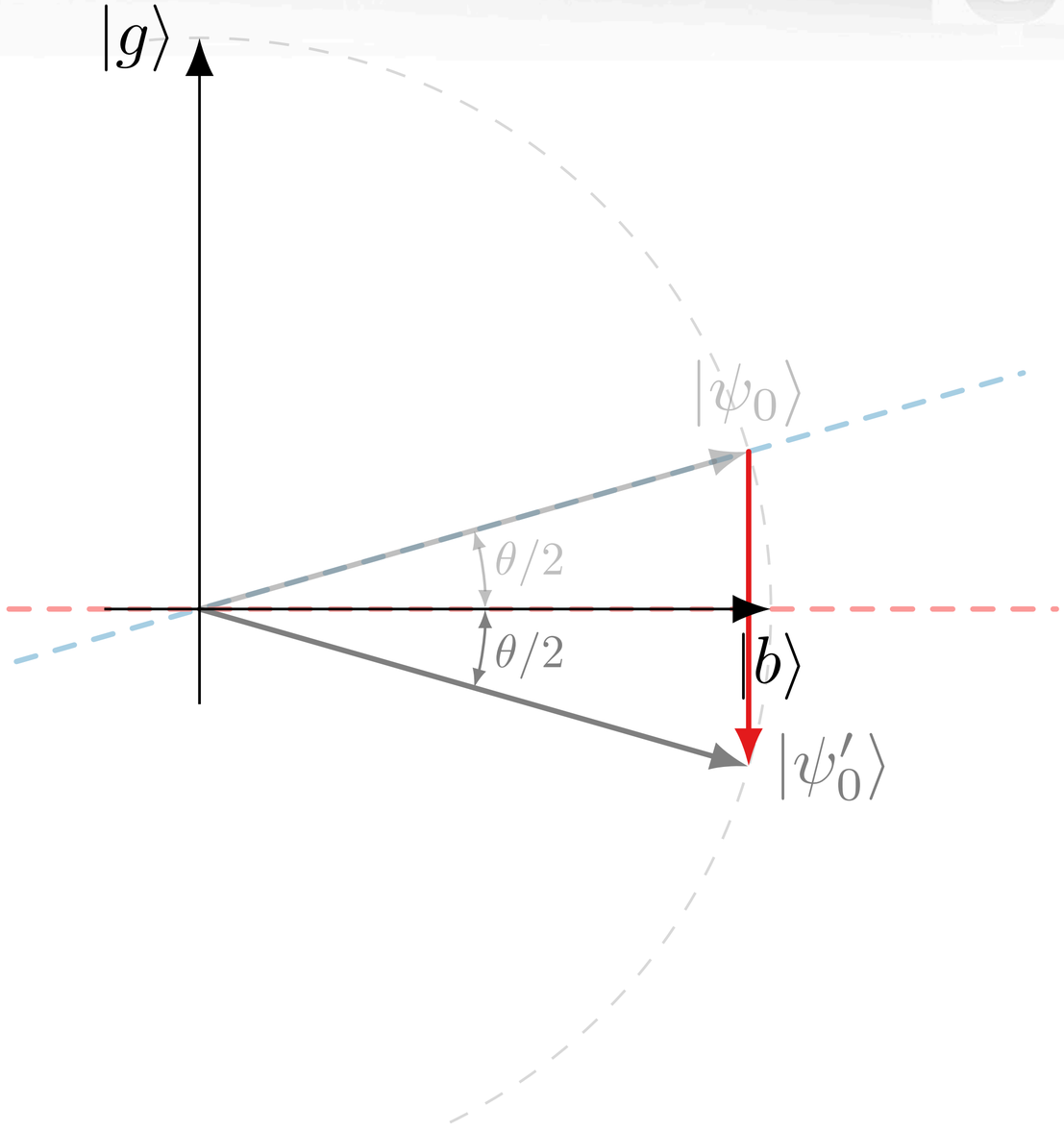


Grover's algorithm

Working principle

$$|\psi_0'\rangle = \cos(\theta/2)\,|b\rangle - \sin(\theta/2)\,|g\rangle$$

$$p_g = \sin^2(\theta/2)$$

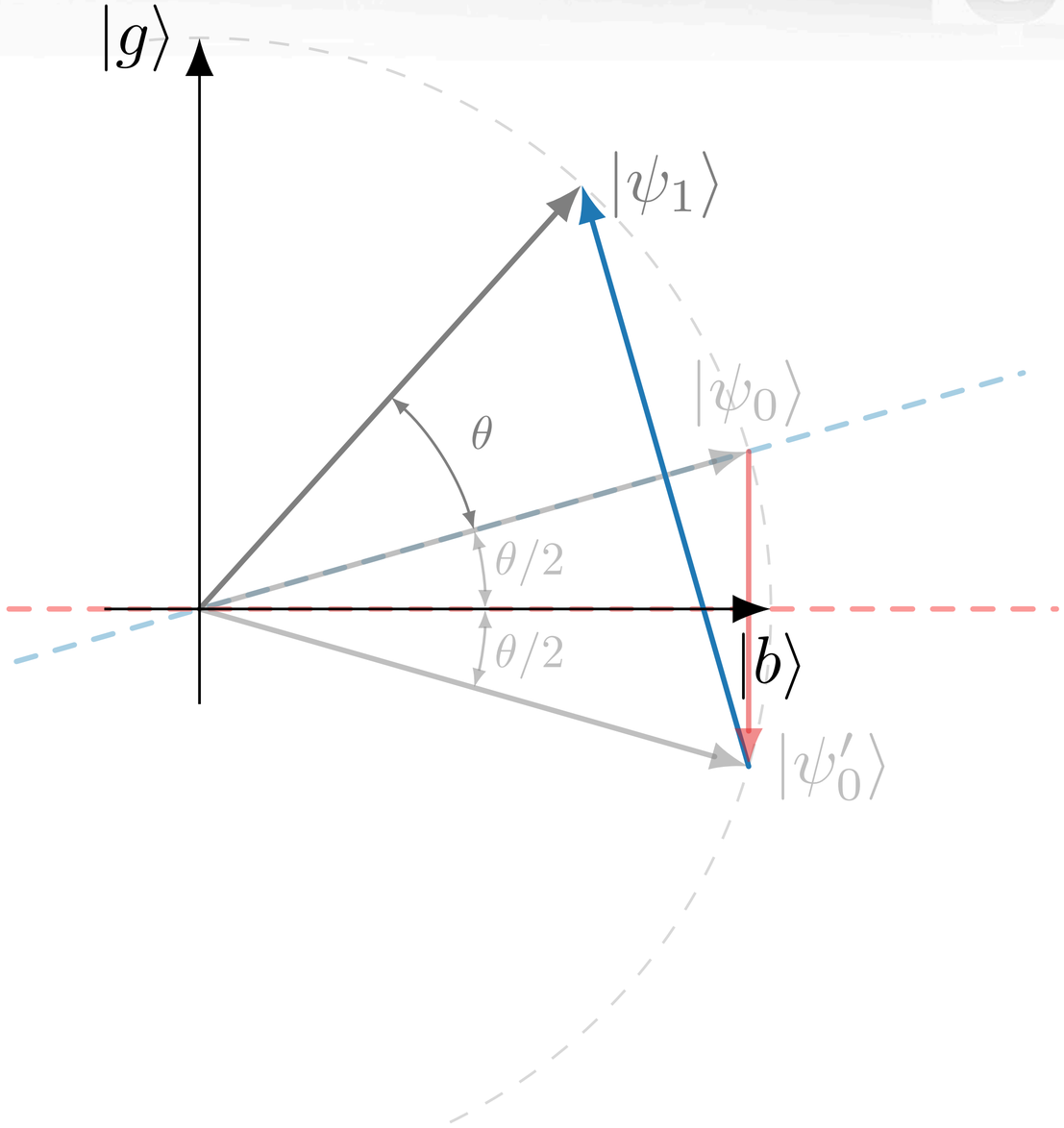


Grover's algorithm

Working principle

$$|\psi_1\rangle = \cos(3\theta/2)\,|b\rangle + \sin(3\theta/2)\,|g\rangle$$

$$p_g = \sin^2(3\theta/2)$$

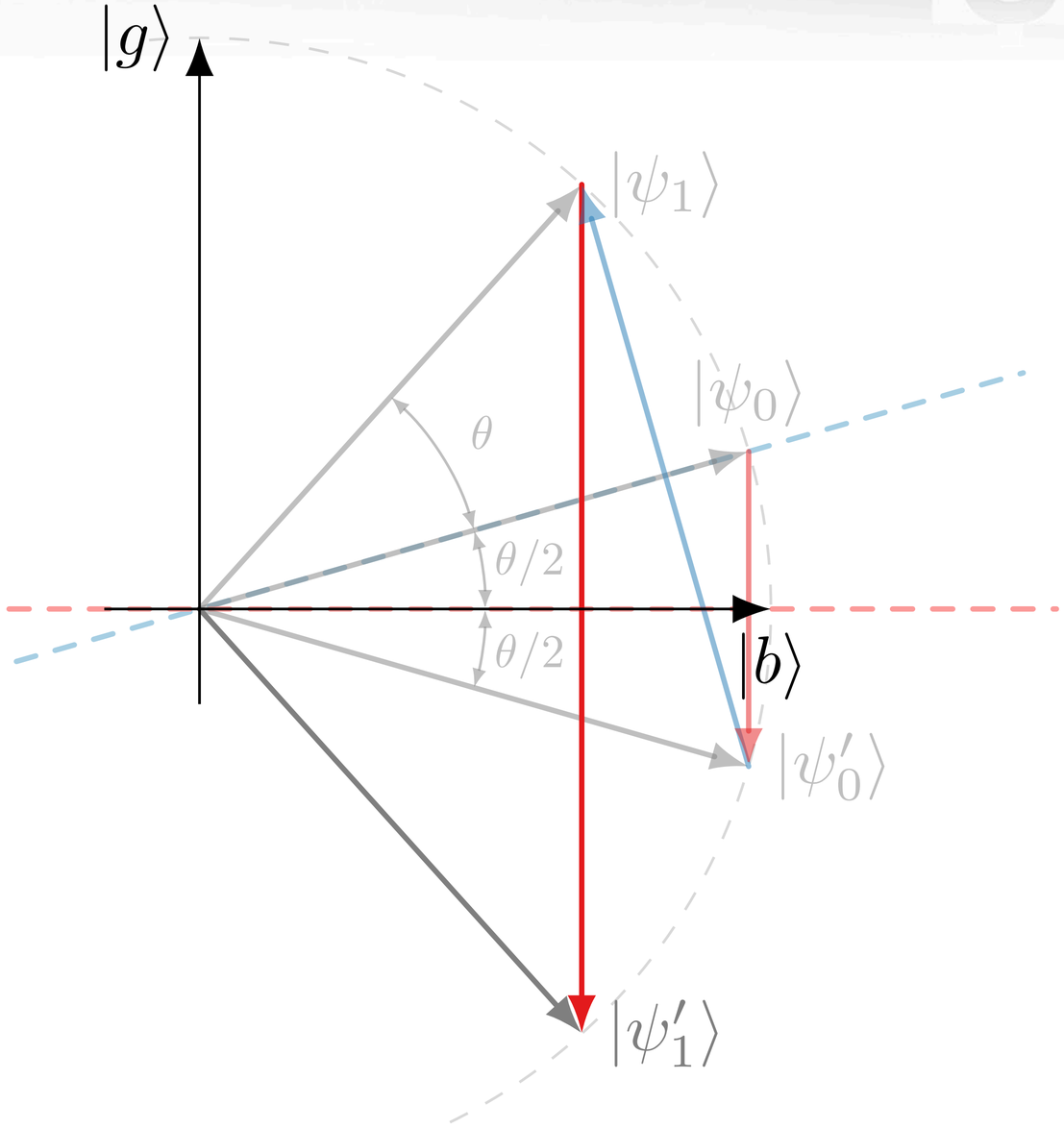


Grover's algorithm

Working principle

$$|\psi_1'\rangle = \cos(3\theta/2)\,|b\rangle - \sin(3\theta/2)\,|g\rangle$$

$$p_g = \sin^2(3\theta/2)$$

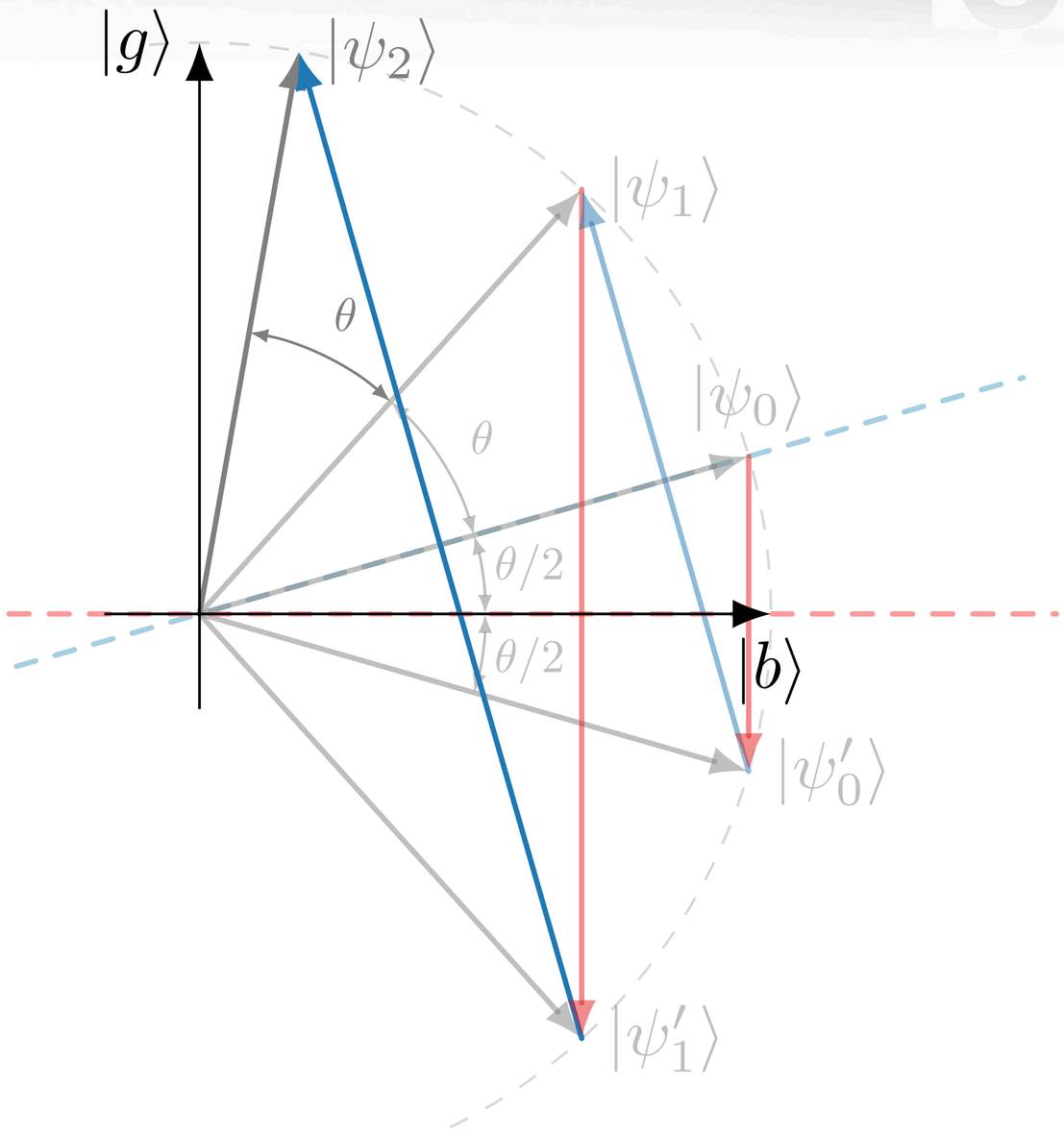


Grover's algorithm

Working principle

$$|\psi_2\rangle = \cos(5\theta/2)\,|b\rangle + \sin(5\theta/2)\,|g\rangle$$

$$p_g = \sin^2(5\theta/2)$$



Grover's algorithm

Working principle

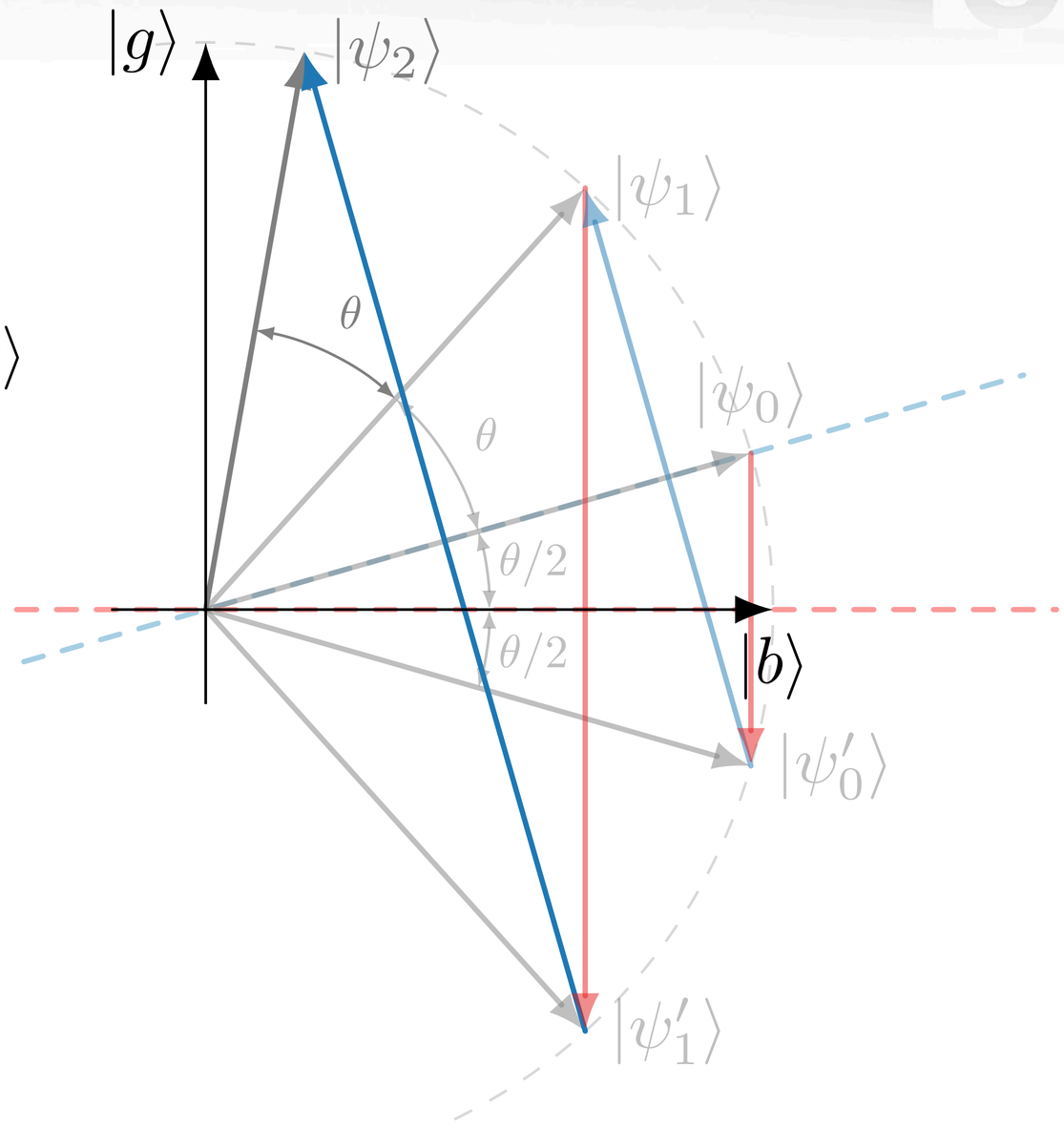
$$|\psi_n\rangle = \cos((n+1/2)\theta)\,|b\rangle + \sin((n+1/2)\theta)\,|g\rangle$$

$$p_g = \sin^2((n+1/2)\theta)$$

Action of the oracle

Action of the diffuser

How can these reflections be achieved?



Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

The diffuser

Diffuser

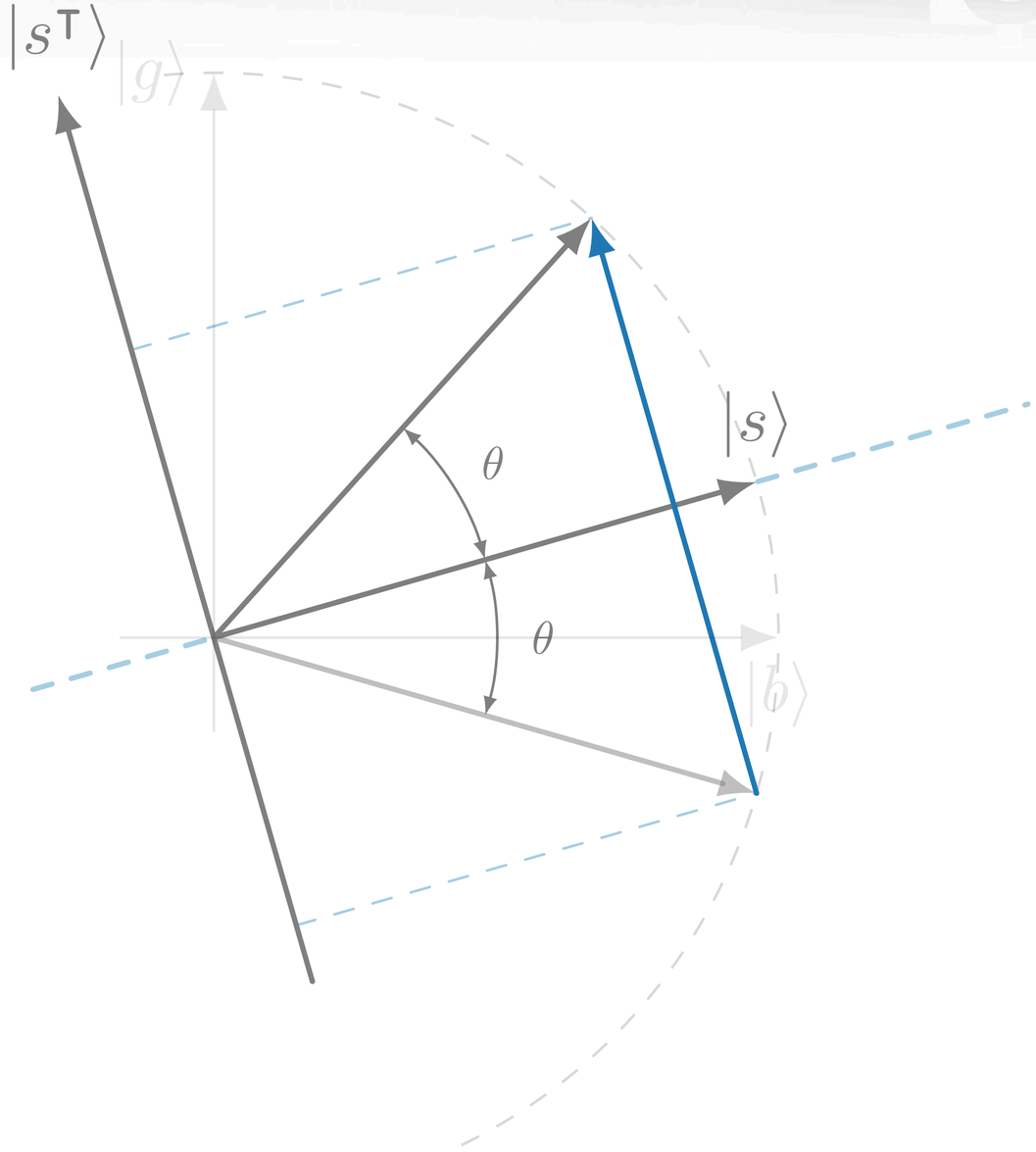
Action

The states can be written as

$$|\phi\rangle = \cos(\theta)\,|s\rangle + \sin(\theta)\,|s^{\mathsf{T}}\rangle$$

We want the diffuser to **reverse** the **phase** of the states **orthogonal** to $|s\rangle$

$$\hat{U}_{\text{diffuser}}\,|\phi\rangle = \cos(\theta)\,|s\rangle - \sin(\theta)\,|s^{\mathsf{T}}\rangle$$

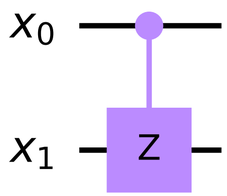


Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Diffuser

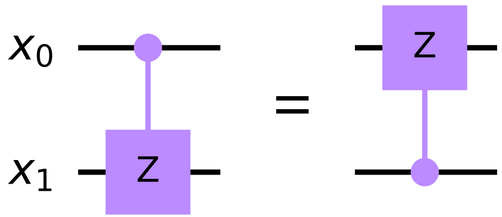
Control-Z gate

The control-Z gate applies a **Z-gate** on a **target qubit** (x_1) if the **control qubit** (x_0) is in the state $|1\rangle$.



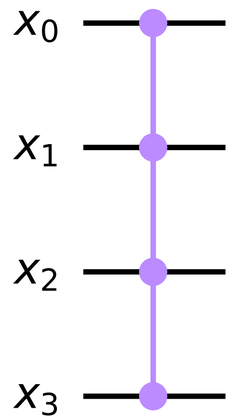
$$C\hat{Z}\,|11\rangle = -\,|11\rangle$$

The control-Z gate is **symmetrical**.



Diffuser

Construction



$$MC\hat{Z}\,|\mathbf{1}\rangle = -\,|\mathbf{1}\rangle$$

$$|\mathbf{1}\rangle = |11\ldots1\rangle$$

From the point of view of the MCZ gate, any state has **two components**

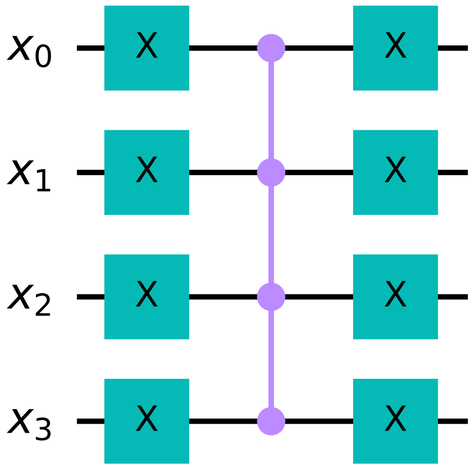
$$|\phi\rangle = \alpha\,|\mathbf{1}\rangle + \beta\,|\mathbf{1}^{\intercal}\rangle$$

Its action is to **reverse the phase** of the state $|\mathbf{1}\rangle$

$$MC\hat{Z}\,|\phi\rangle = -\alpha\,|\mathbf{1}\rangle + \beta\,|\mathbf{1}^{\intercal}\rangle$$

Diffuser

Construction



$$\hat{X}^{\otimes n} |\mathbf{1}\rangle = |\mathbf{0}\rangle$$

$$\hat{X}^{\otimes n} |\mathbf{0}\rangle = |\mathbf{1}\rangle$$

From the point of view of the MCZ gate, any state has **two components**

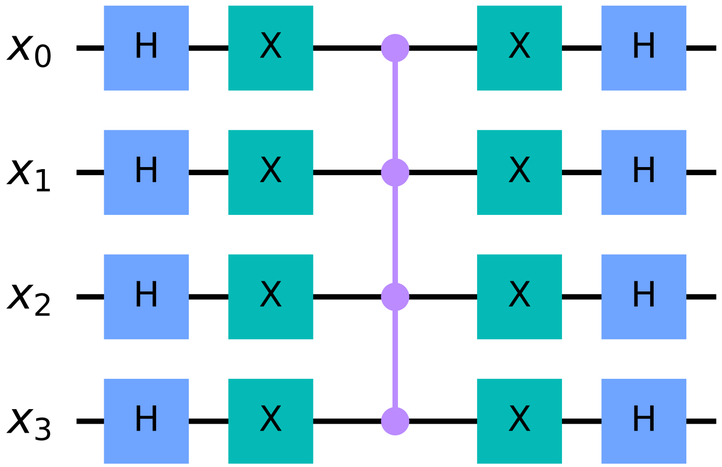
$$|\phi\rangle = \alpha |\mathbf{0}\rangle + \beta |\mathbf{0}^{\intercal}\rangle$$

Its action is to **reverse the phase** of the state $|\mathbf{0}\rangle$

$$\hat{U} |\phi\rangle = -\alpha |\mathbf{0}\rangle + \beta |\mathbf{0}^{\intercal}\rangle$$

Diffuser

Construction



$$\hat{H}^{\otimes n} |\mathbf{0}\rangle = |s\rangle$$

$$\hat{H}^{\otimes n} |s\rangle = |\mathbf{0}\rangle$$

From the point of view of the MCZ gate, any state has **two components**

$$|\phi\rangle = \alpha |s\rangle + \beta |s^{\mathsf{T}}\rangle$$

Its action is to **reverse the phase** of the state $|s\rangle$

$$\hat{U} |\phi\rangle = -\alpha |s\rangle + \beta |s^{\mathsf{T}}\rangle$$

Which is exactly what we need!

$$\hat{U}_{\text{diffuser}} |\phi\rangle = \cos(\theta) |s\rangle - \sin(\theta) |s^{\mathsf{T}}\rangle$$

... except for a - sign, which has no physical consequences.

The oracle

Oracle

Action

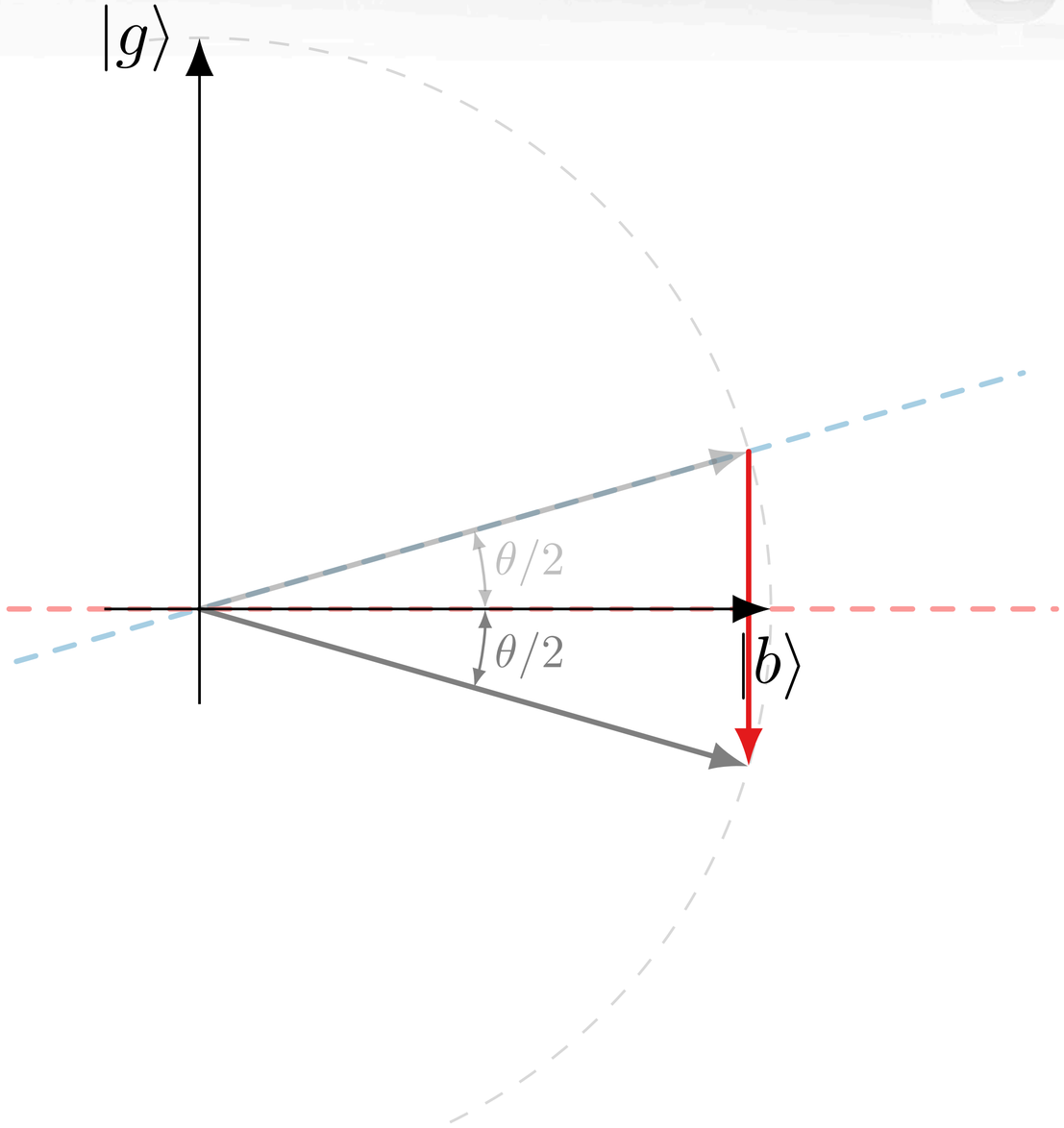
We build the oracle so that it **reverses the phase** of the **good** states

$$\hat{U}_{\text{oracle}} |\mathbf{x}\rangle = \begin{cases} -|\mathbf{x}\rangle & \text{if} \quad \mathbf{x} \in G; \\ |\mathbf{x}\rangle & \text{if} \quad \mathbf{x} \in B. \end{cases}$$

This will allow us to do the desired reflection.

$$\hat{U}_{\text{oracle}} |g\rangle = -|g\rangle$$

$$\hat{U}_{\text{oracle}} |b\rangle = |b\rangle$$



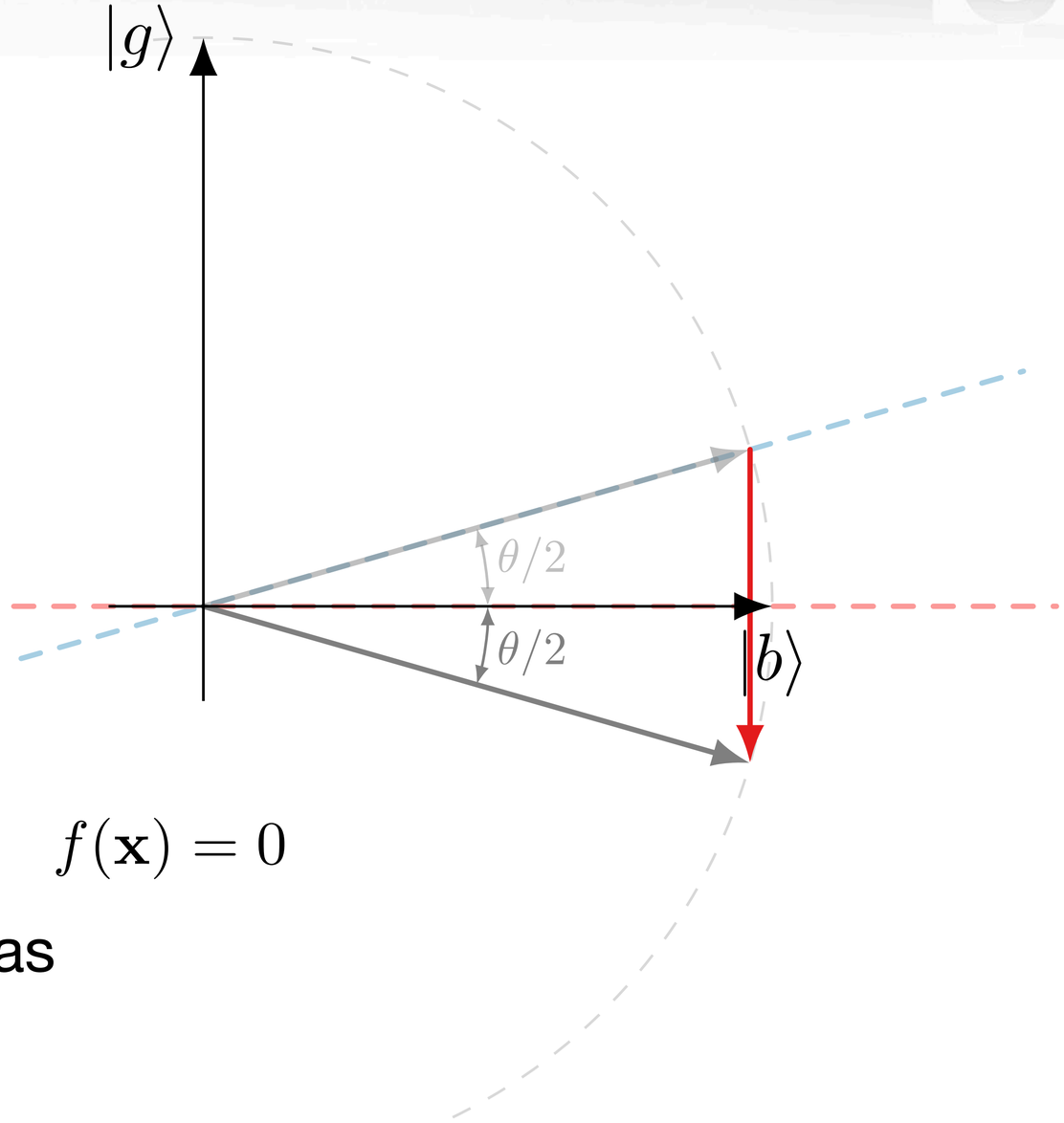
Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Oracle

Action

We build the oracle so that it **reverses the phase** of the **good** states

$$\hat{U}_{\text{oracle}} |\mathbf{x}\rangle = \begin{cases} -|\mathbf{x}\rangle & \text{if} \quad \mathbf{x} \in G; \\ |\mathbf{x}\rangle & \text{if} \quad \mathbf{x} \in B. \end{cases}$$



Let's remember that states are **good** or **bad**

$$\mathbf{x} \in G \quad \text{if} \quad f(\mathbf{x}) = 1 \qquad \mathbf{x} \in B \quad \text{if} \quad f(\mathbf{x}) = 0$$

We can summarize the **effect** of the **oracle** as

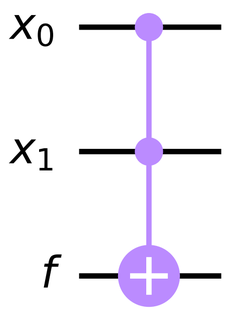
$$\hat{U}_{\text{oracle}} |\mathbf{x}\rangle = (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$$

Logic and quantum gates

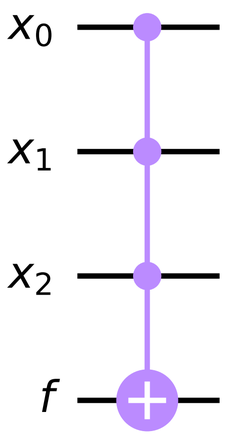
Conjunction (and) gate to qubit

We can write, in an **ancillary qubit**, the evaluation of a **conjunction**.

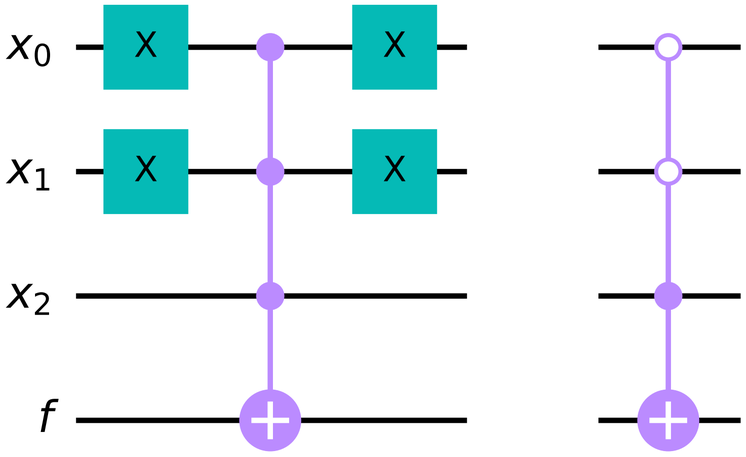
$$f = x_0 \wedge x_1$$



$$f = x_0 \wedge x_1 \wedge x_2$$



$$f = \bar{x}_0 \wedge \bar{x}_1 \wedge x_2$$



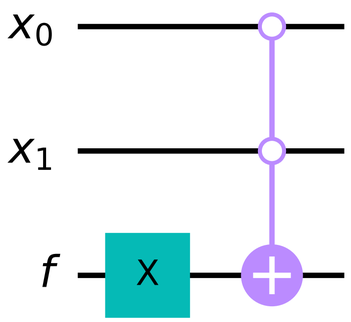
Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique

Logic and quantum gates

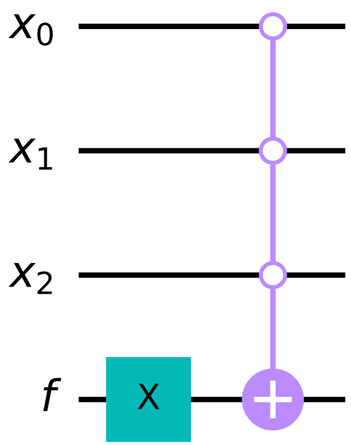
Disjunction (or) gate to qubit

We can write, in an **ancillary qubit**, the evaluation of a **disjunction**.

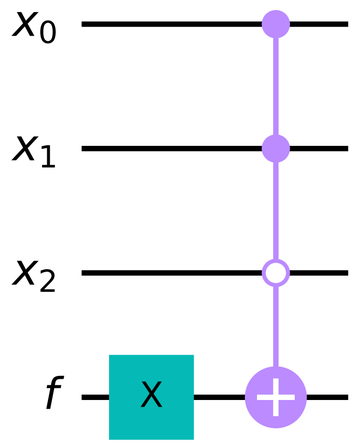
$$f = x_0 \vee x_1 = \neg(\bar{x}_0 \wedge \bar{x}_1)$$



$$f = x_0 \vee x_1 \vee x_2 = \neg(\bar{x}_0 \wedge \bar{x}_1 \wedge \bar{x}_2)$$



$$f = \bar{x}_0 \vee \bar{x}_1 \vee x_2 = \neg(x_0 \wedge x_1 \wedge \bar{x}_2))$$



Oracle

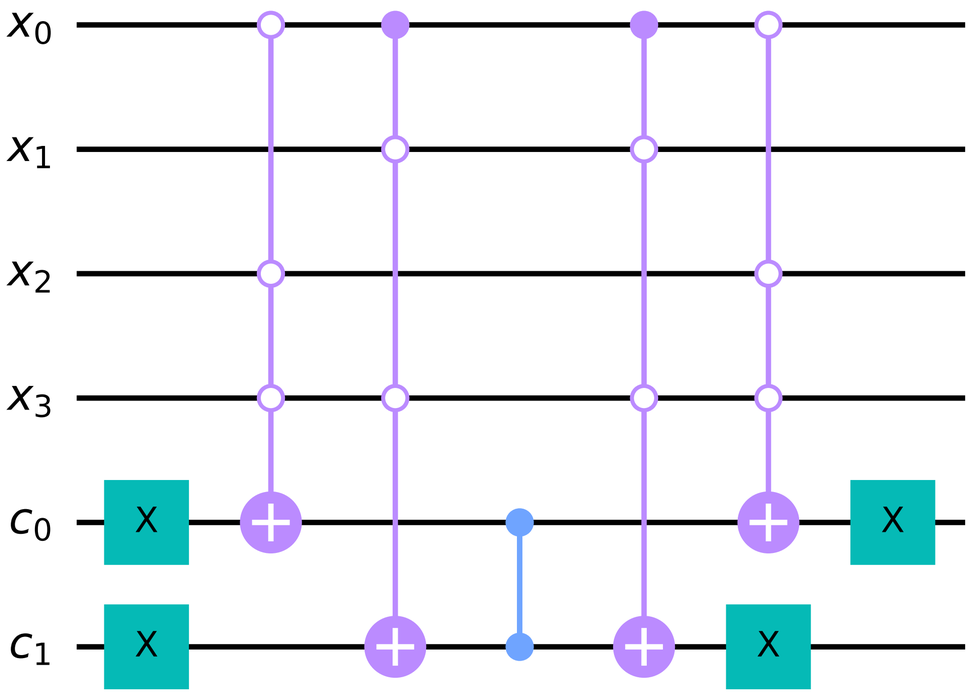
Circuit example

Let's build the **oracle** for the **first two statements** of the problem.

$$f(x_0, x_1, x_2, x_3) = (x_2 \vee x_0 \vee x_3) \wedge (\bar{x}_0 \vee x_3 \vee x_1)$$

$$c_0 = x_2 \vee x_0 \vee x_3$$

$$c_1 = \bar{x}_0 \vee x_3 \vee x_1$$



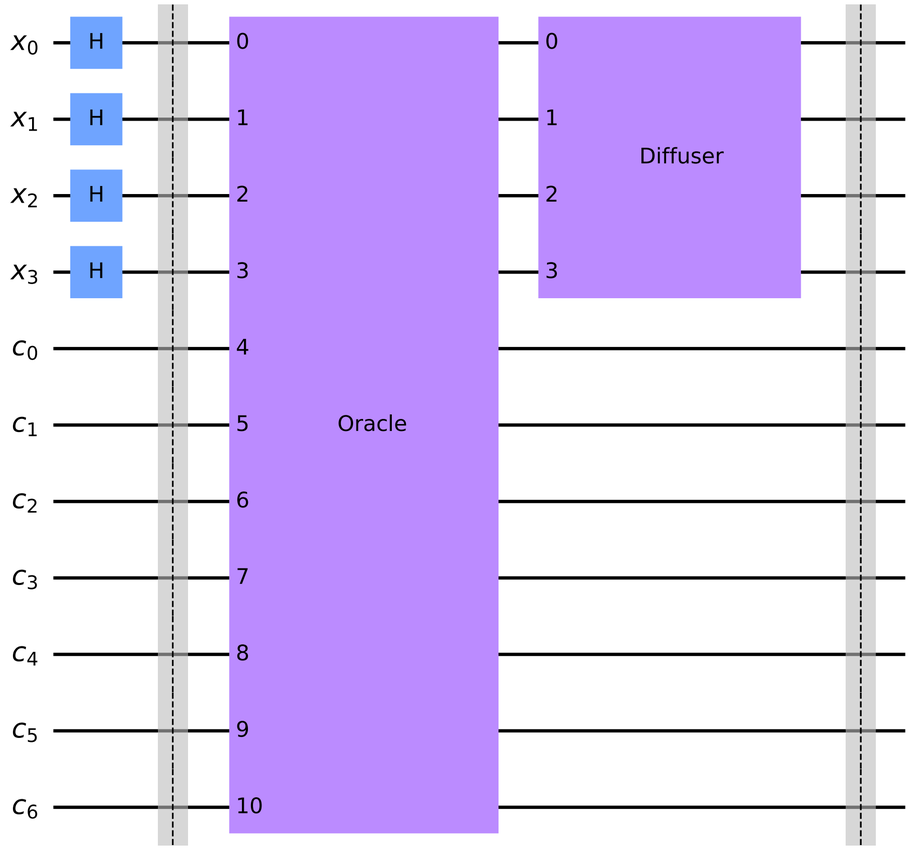
Oracle

Circuit example

Construction of the oracle for the Pincus planet problem.

$$f(x_0, x_1, x_2, x_3) = (x_2 \vee x_0 \vee x_3) \wedge (\bar{x}_0 \vee x_3 \vee x_1) \wedge (x_1 \vee \bar{x}_3 \vee x_2)$$
$$\wedge (\bar{x}_1 \vee x_3 \vee \bar{x}_2) \wedge (\bar{x}_0 \vee x_2 \vee \bar{x}_1) \wedge (x_1 \vee \bar{x}_2 \vee x_0) \wedge (\bar{x}_0 \vee \bar{x}_3 \vee \bar{x}_2)$$

Let's use Python to do this!



Maxime Dion (maxime.dion@usherbrooke.ca) - Institut Quantique