

Algorithme de Grover

Application à un problème de satisfiabilité

Ibrahim Chegrane

ibrahim.chegrane@usherbrooke.ca

Sherbrooke

07 mai 2025

Qui sommes-nous?

Laboratoire d'algorithmique quantique (AlgoLab)



Algorithme de Grover

L'algorithme de **Grover** est souvent présenté comme offrant un avantage quadratique pour effectuer une **recherche** dans une **base de données non-ordonnée**.

Mais qu'est-ce que ça veut dire?

Les habitants de la planète Pincus*

La problématique

Les voyageurs qui ont séjourné sur la planète Pincus ont observé que tous ses habitants qui sont en **santé** sont **bruyants**, sauf s'ils sont **peureux**. Ceux qui sont **peureux** et **discrets** sont **heureux**, tout comme ceux qui sont en **santé** et **bruyants**. Les habitants **heureux** et **discrets** sont en **santé**, mais ceux qui sont **peureux** et en **santé** sont **tristes**. Finalement, même si les habitants **tristes** et **malades** sont toujours **apeurés**, les **peureux** et **bruyants** sont en **santé**.



Peureux / Courageux



Heureux / Triste



Malade / En santé



Bruyant / Discret

Que peut-ton conclure à propos des habitants de la planète Pincus?

*Scénario tirée et adapté de *The Art of Computer Programming*, Volume 4, Donald E. Knuth

Un peu de logique

Un peu de logique

Opérateurs logiques

La conjonction (x et y) : $x \wedge y$ est vrai si x est vrai et y est vrai

La disjonction (x ou y) : $x \vee y$ est vrai si x est vrai ou y est vrai

La négation (non x) : $\neg x$ est vrai si x est faux (aussi noté \bar{x})

x	y	$x \wedge y$
F	F	F
V	F	F
F	V	F
V	V	V

x	\bar{x}
F	V
V	F

Un peu de logique

Formule logique et satisfiabilité

Une **proposition** est une composition de **variables logiques** à l'aide de **conjonctions**, de **disjonctions** et de **négations**.

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

On dit qu'elle est **satisfiable** si on peut **attribuer des valeurs** (vrai/faux) de sorte que la formule s'évalue à vrai.

x	y	z	$x \wedge \bar{y}$	$\bar{x} \vee z$	f
F	F	F	F	V	F
V	F	F	V	F	F
F	V	F	F	V	F
V	V	F	F	F	F
F	F	V	F	V	F
V	F	V	V	V	V
F	V	V	F	V	F
V	V	V	F	V	F

Un peu de logique

Loi de De Morgan

On peut convertir une **conjonction** (et) en **disjonction** (ou) avec la relation de **De Morgan**.

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

Par exemple, supposons que les variables logiques suivantes décrive un objet:

- Cet objet est un **fruit** (x est vrai);
- Cet objet est **jaune** (y est vrai);
- Cet objet est **une banane** (f est vrai).



La relation de De Morgan nous dit que :

Si un objet n'est **pas un fruit ou n'est pas jaune**, ce n'est **pas une banane**.

Un peu de logique

Loi de De Morgan

On peut convertir une **conjonction** (et) en **disjonction** (ou) avec la relation de **De Morgan**.

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

x	y	$x \wedge y$
F	F	F
V	F	F
F	V	F
V	V	V

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

Un peu de logique

Proposition conditionnelle

Une proposition conditionnelle

$$x \rightarrow y$$

x	y
F	?
V	V

implique que si x est **vrai**, y l'est aussi. Si x est **faux**, on ne sait rien sur y .

Par exemple, supposons que les variables logiques décrivent

- Sam a **mangé une banane** (x est vrai)
- Sam a **mangé un fruit** (y est vrai)



Si Sam a **mangé une banane**, il a donc **mangé un fruit**. Si Sam n'a **pas mangé une banane**, on ne peut **pas conclure** s'il a mangé un fruit ou non.

Un peu de logique

Règle d'inférence

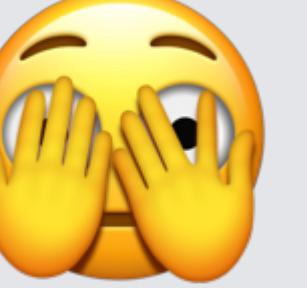
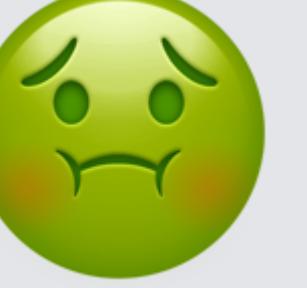
La **règle d'inférence** permet de traduire une **proposition conditionnelle** en une **disjonction** qui sera **vrai** si la **proposition conditionnelle** est respectée.

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

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

Les habitants de la planète Pincus

Les variables logiques

		Vrai (1)	Faux (0)
	x_0	Peureux	Courageux
	x_1	Heureux	Triste
	x_2	Malade	En santé
	x_3	Bruyant	Discret

Les habitants de la planète Pincus

Les propositions

...les habitants qui sont en **santé** sont **bruyants**, sauf s'ils sont **peureux**

Si un habitant en **santé** est **courageux**, il sera **bruyant**.

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

		Vrai	Faux
	x_0	Peureux	Courageux
	x_1	Heureux	Triste
	x_2	Malade	En santé
	x_3	Bruyant	Discret

Les habitants de la planète Pincus

Conversion d'une proposition conditionnel en conjonction

On utilise d'abord la **règle d'inférence**

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

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

Ensuite, la règle de **De Morgan**

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

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

Finalement, on combine les deux pour obtenir notre règle de conversion

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

$$x \wedge y \rightarrow z = \bar{x} \vee \bar{y} \vee z$$

Les habitants de la planète Pincus

Les propositions

Si un habitant en **santé** est **courageux**, il est aussi **bruyant**.

Si un habitant est **peureux** et **discret**, il est aussi **heureux**.

Si un habitant est en **santé** et **bruyant**, il est aussi **heureux**.

Si un habitant est en **heureux** et **discret**, il est aussi en **santé**.

Si un habitant est en **peureux** et en **santé**, il est aussi **triste**.

Si un habitant est en **triste** et **malade**, il est aussi **peureux**.

Si un habitant est en **peureux** et **bruyant**, il est aussi en **santé**.

$$x \wedge y \rightarrow z \quad \longrightarrow \quad \bar{x} \vee \bar{y} \vee z$$

$$\bar{x}_2 \wedge \bar{x}_0 \rightarrow x_3 \quad x_2 \vee x_0 \vee x_3$$

$$x_0 \wedge \bar{x}_3 \rightarrow x_1 \quad \bar{x}_0 \vee x_3 \vee x_1$$

$$\bar{x}_2 \wedge x_3 \rightarrow x_1 \quad x_2 \vee \bar{x}_3 \vee x_1$$

$$x_1 \wedge \bar{x}_3 \rightarrow \bar{x}_2 \quad \bar{x}_1 \vee x_3 \vee \bar{x}_2$$

$$x_0 \wedge \bar{x}_2 \rightarrow \bar{x}_1 \quad \bar{x}_0 \vee x_2 \vee \bar{x}_1$$

$$\bar{x}_1 \wedge x_2 \rightarrow x_0 \quad x_1 \vee \bar{x}_2 \vee x_0$$

$$x_0 \wedge x_3 \rightarrow \bar{x}_2 \quad \bar{x}_0 \vee \bar{x}_3 \vee \bar{x}_2$$

	Vrai	Faux
	x_0	Peureux
	x_1	Heureux
	x_2	Malade
	x_3	Bruyant
		Courageux
		Triste
		En santé
		Discret

Les habitants de la planète Pincus

La proposition principale

On peut alors assembler la **proposition principale** du problème

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

On pourra déduire comment sont les habitants de la planète Pincus, si on trouve une **combinaison des variables logiques** de sorte que cette **formule s'évalue à Vrai**.

		Vrai	Faux	
		x_0	Peureux	Courageux
		x_1	Heureux	Triste
		x_2	Malade	En santé
		x_3	Bruyant	Discret

Problème de satisfiabilité

Les propositions

On cherche à savoir s'il existe une configuration qui satisfait la formule logique

$$f(x_0, x_1, x_2, x_3) = 1$$

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

Par exemple,

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

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

		Vrai	Faux
	x_0	Peureux	Courageux
	x_1	Heureux	Triste
	x_2	Malade	En santé
	x_3	Bruyant	Discret

Algorithme de Grover

Encodage dans les qubits

On attribut un **qubit** à chaque **variable logique**

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

$$|x_3x_2x_1x_0\rangle$$

On résume ces variables sous la forme d'un **vecteur** de composantes binaires ou d'un **état de base**

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

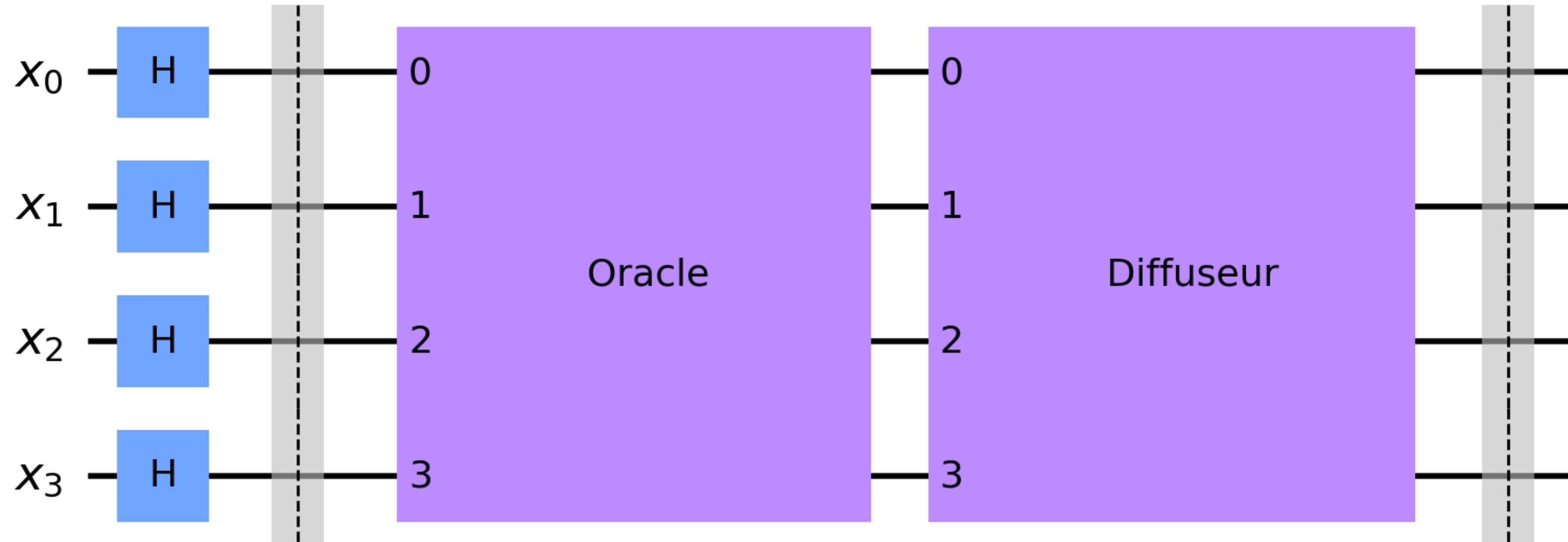
$$|\mathbf{x}\rangle = |x_3x_2x_1x_0\rangle$$

L'évaluation de la **proposition principale** se résume à

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

x_0 —
 x_1 —
 x_2 —
 x_3 —

Algorithme de Grover



Oracle

Marque les états en inversant leur phase.

Diffuseur

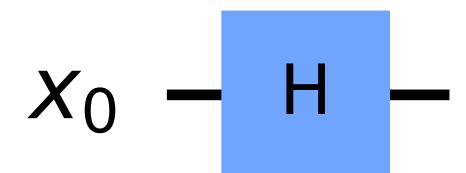
Amplifie les probabilités pour les états dont la phase est inversée.

Algorithme de Grover

L'état de superposition uniforme

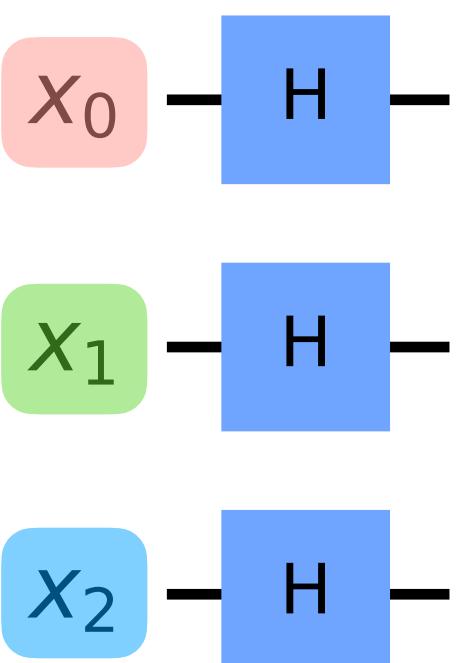
Une porte Hadamard sur un qubit permet de préparer une **superposition**

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



Des portes Hadamard sur plusieurs qubits permettent de préparer l'état de **superposition uniforme**

$$\begin{aligned}
 |+\rangle \otimes |+\rangle \otimes |+\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
 &= \frac{1}{\sqrt{2^3}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle \\
 &\quad + |100\rangle + |101\rangle + |110\rangle + |111\rangle)
 \end{aligned}$$



Algorithme de Grover

L'état de superposition uniforme

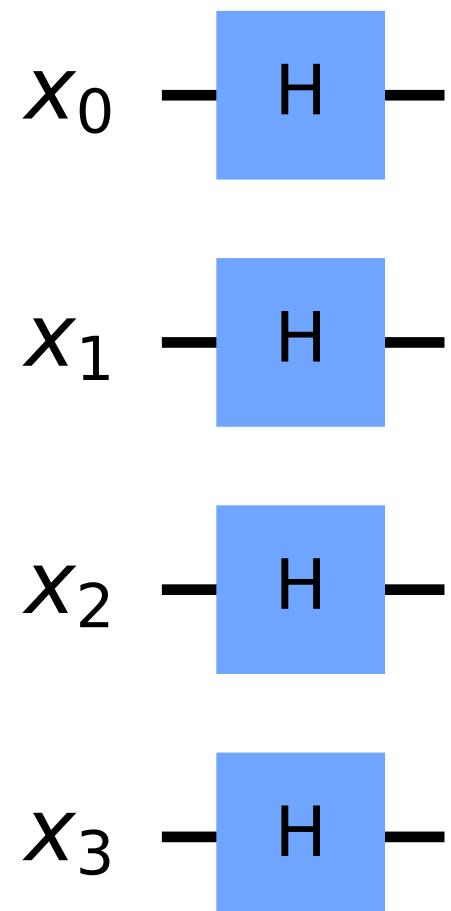
Des portes Hadamard sur plusieurs qubits permettent de préparer l'**état de superposition uniforme**

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

Pour un système de n qubits, l'état de superposition uniforme est

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

et comporte toutes les 2^n possibilités.



Algorithme de Grover

The *good* and the *bad* states

Pour un système de n qubits, l'état de superposition uniforme est

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

Parmi ces états, certains **satisfont** la proposition principale f (the *good*), alors que les autres **ne la satisfont pas** (the *bad*)

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

Algorithme de Grover

The *good* and the *bad* states

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

On peut donc écrire l'état de **superposition uniforme** comme une combinaison de **deux états**

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

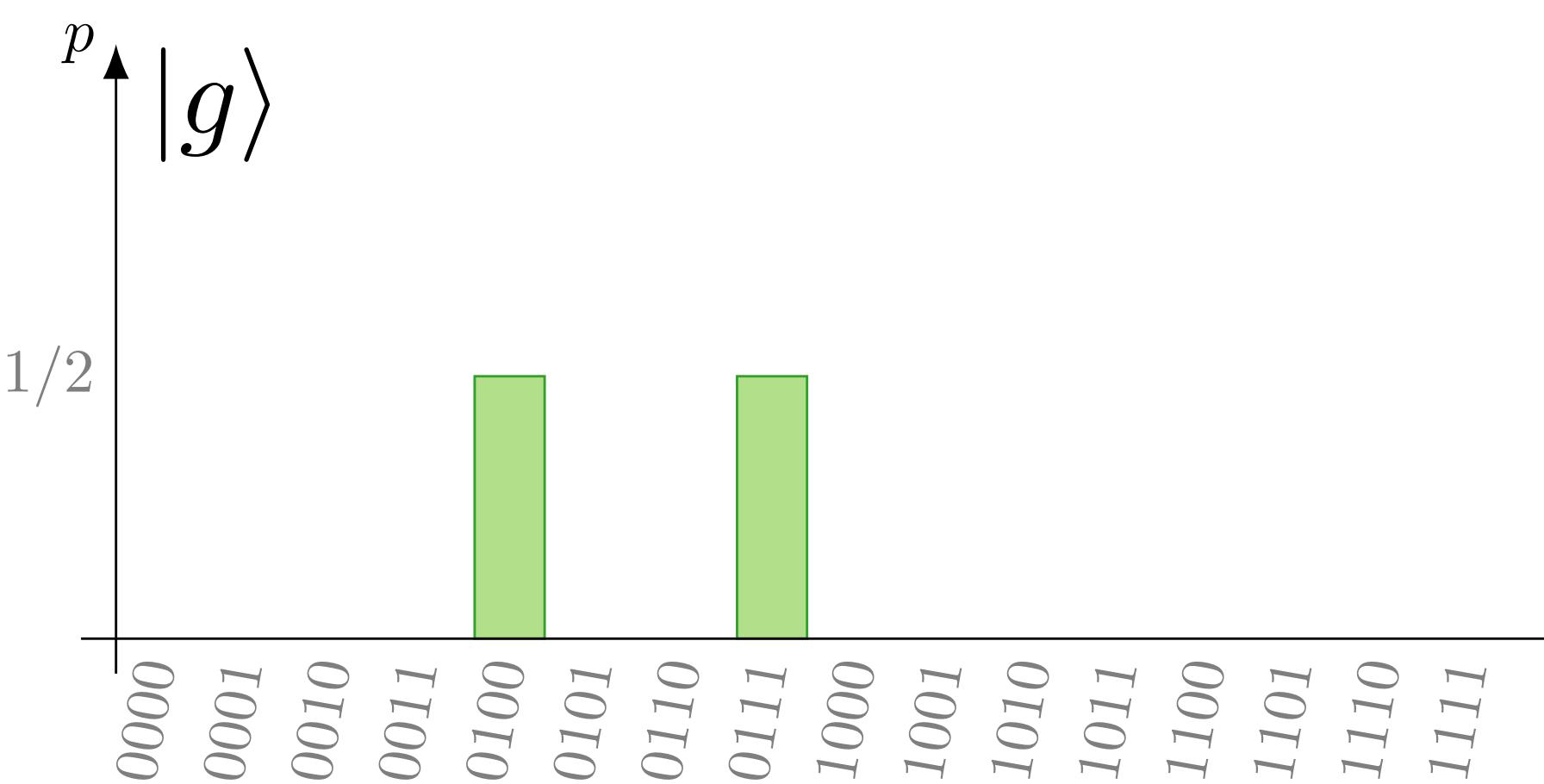
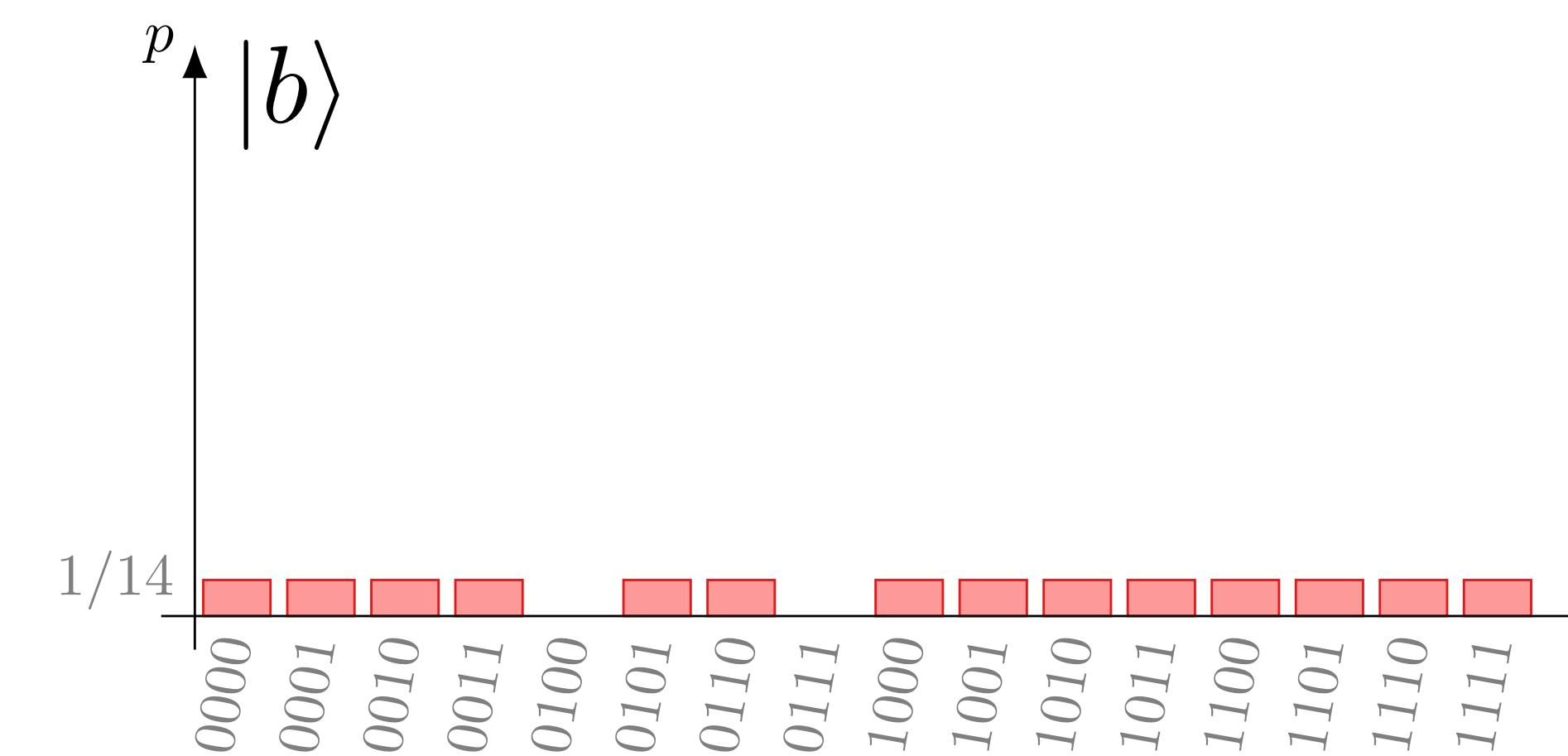
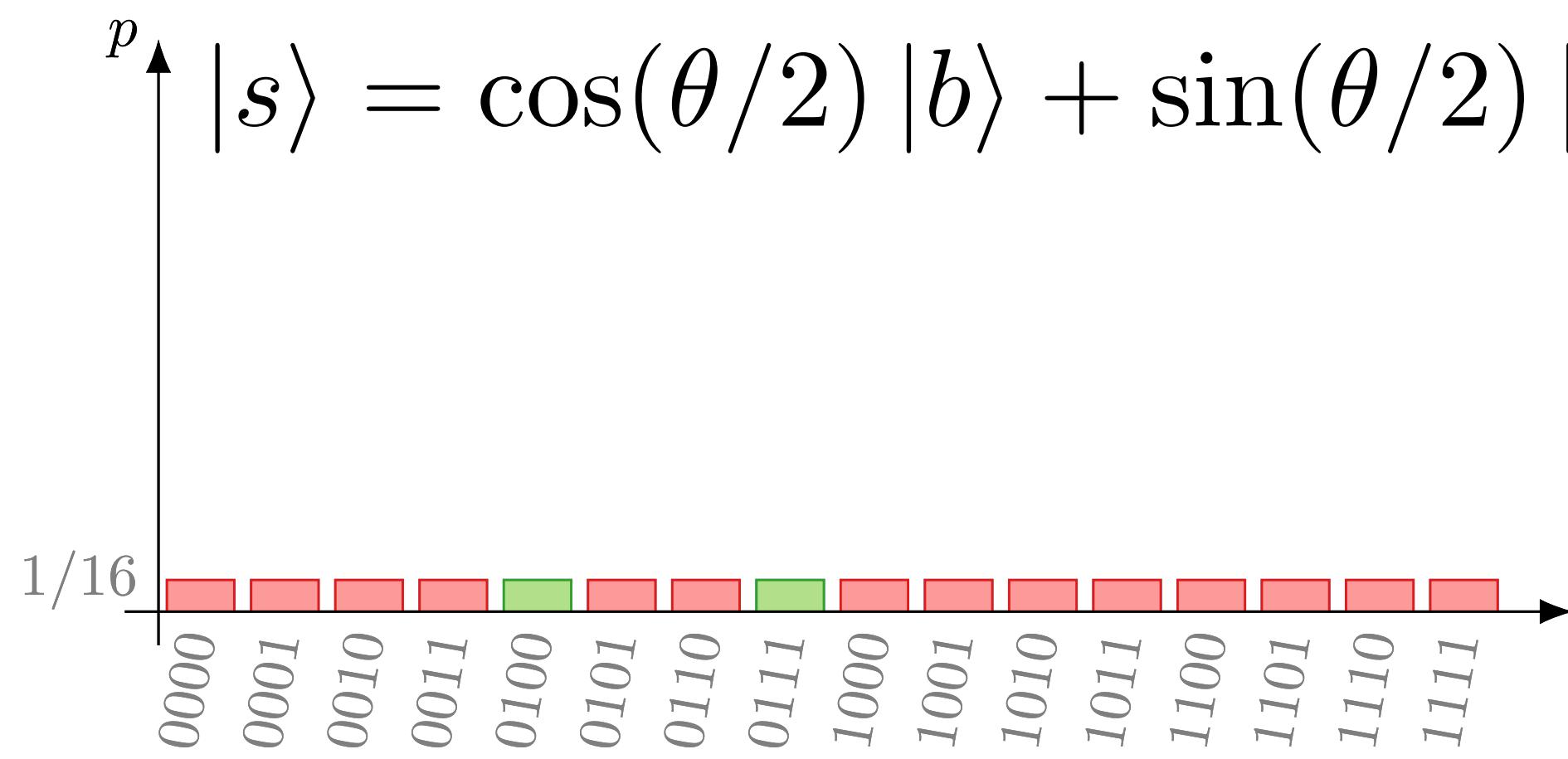
avec les états

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

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

Algorithme de Grover

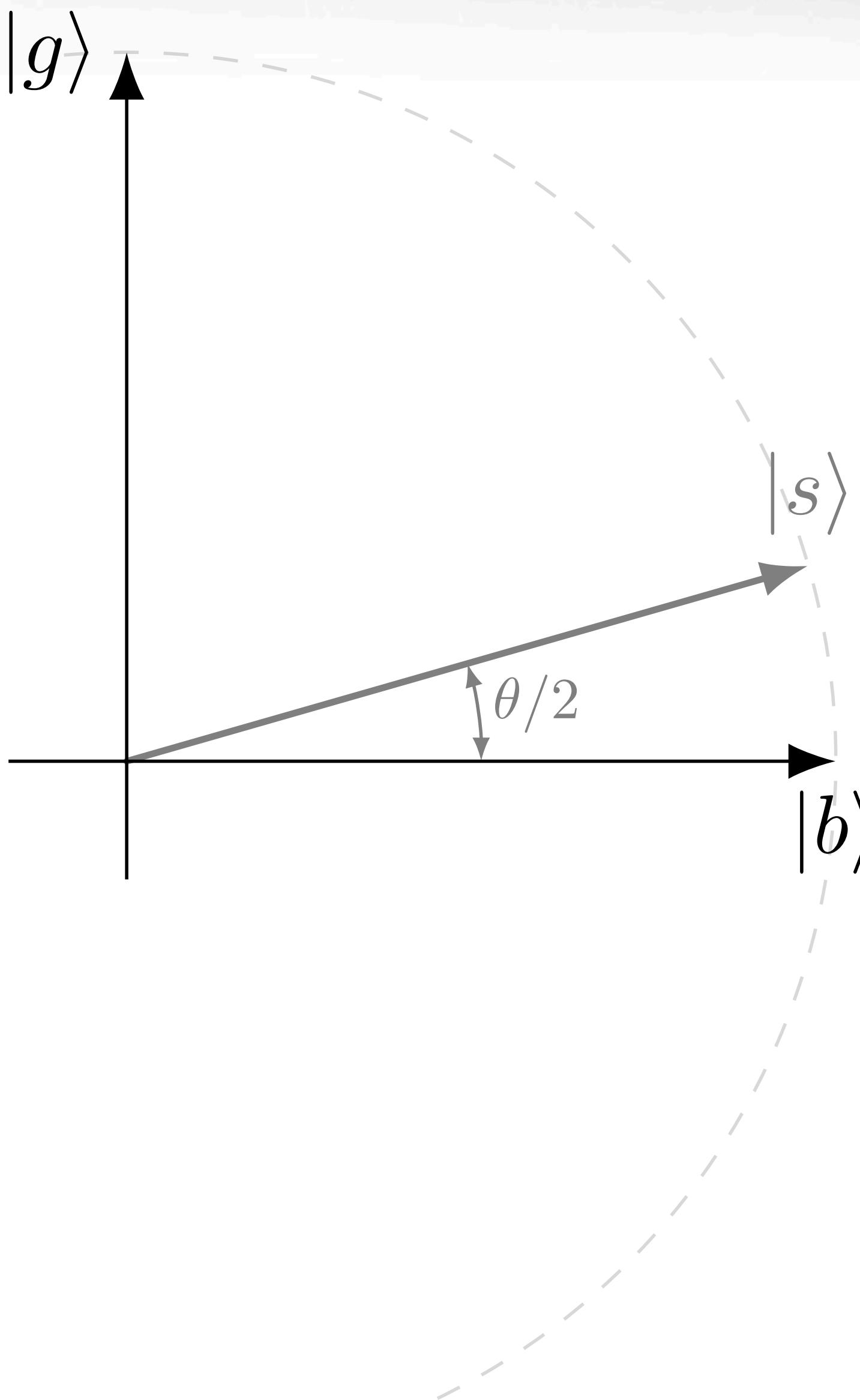
The *good* and the *bad* states



Algorithme de Grover

Principe de fonctionnement

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

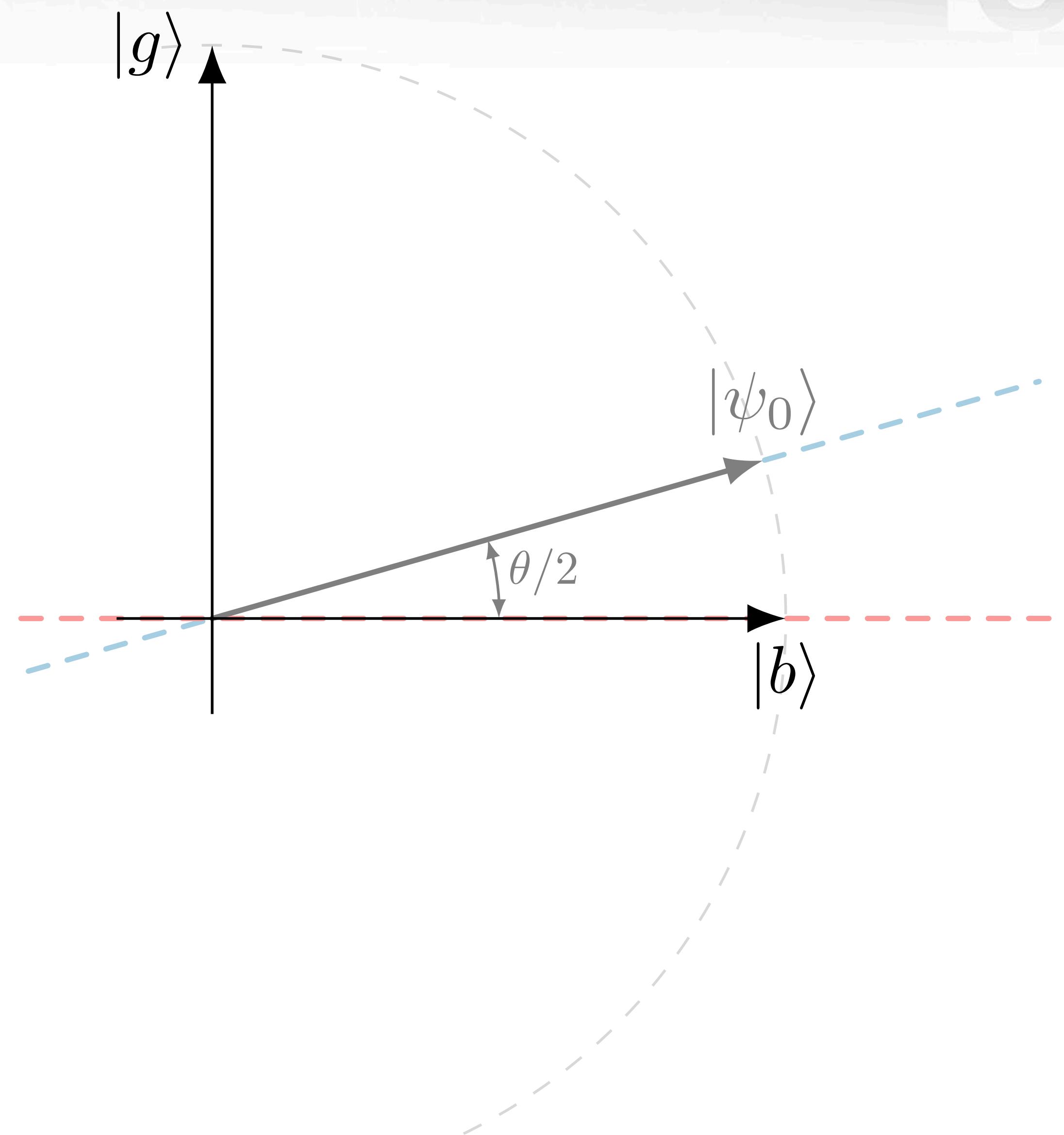


Algorithme de Grover

Principe de fonctionnement

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

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

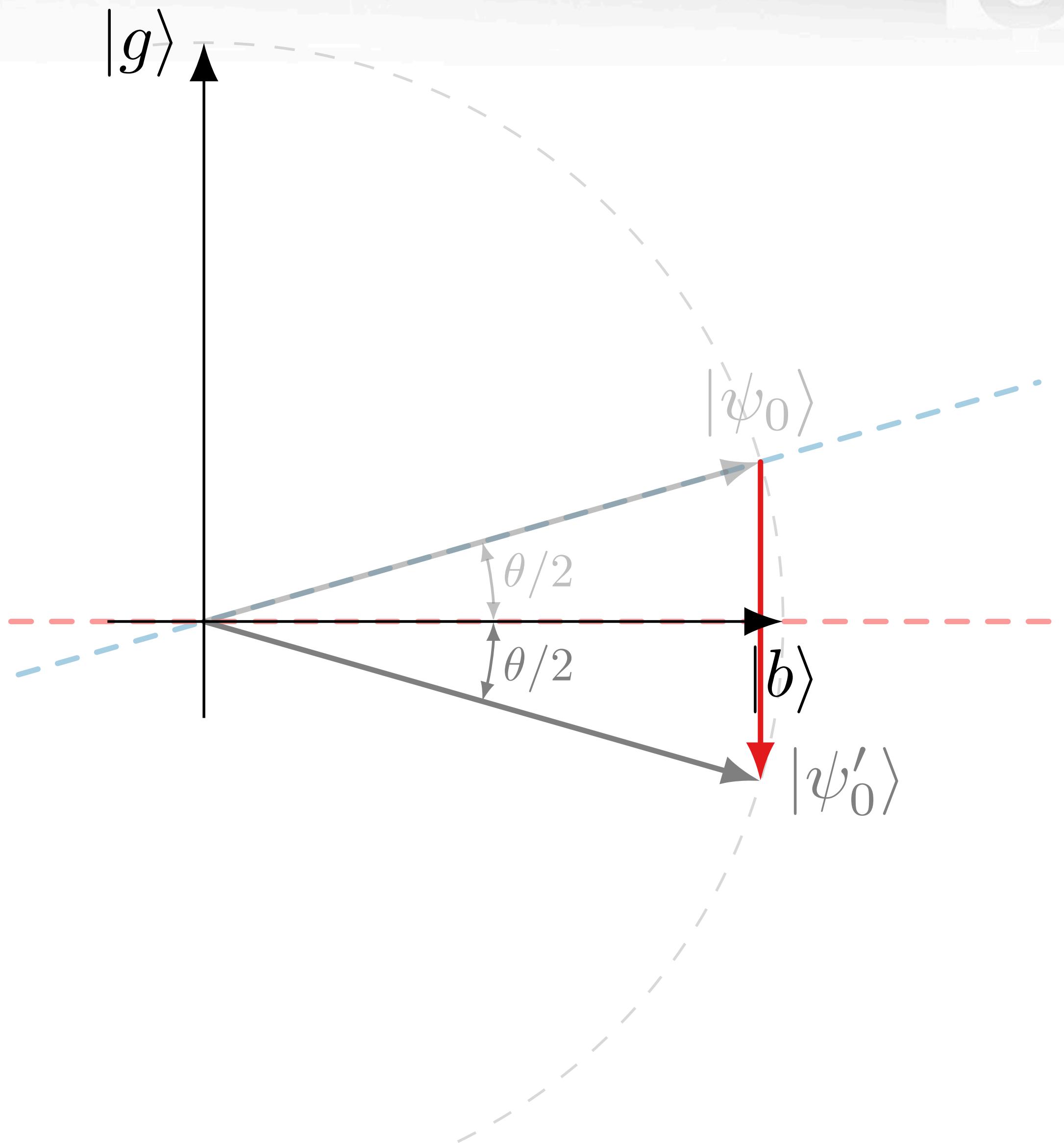


Algorithme de Grover

Principe de fonctionnement

$$|\psi'_0\rangle = \cos(\theta/2) |b\rangle - \sin(\theta/2) |g\rangle$$

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

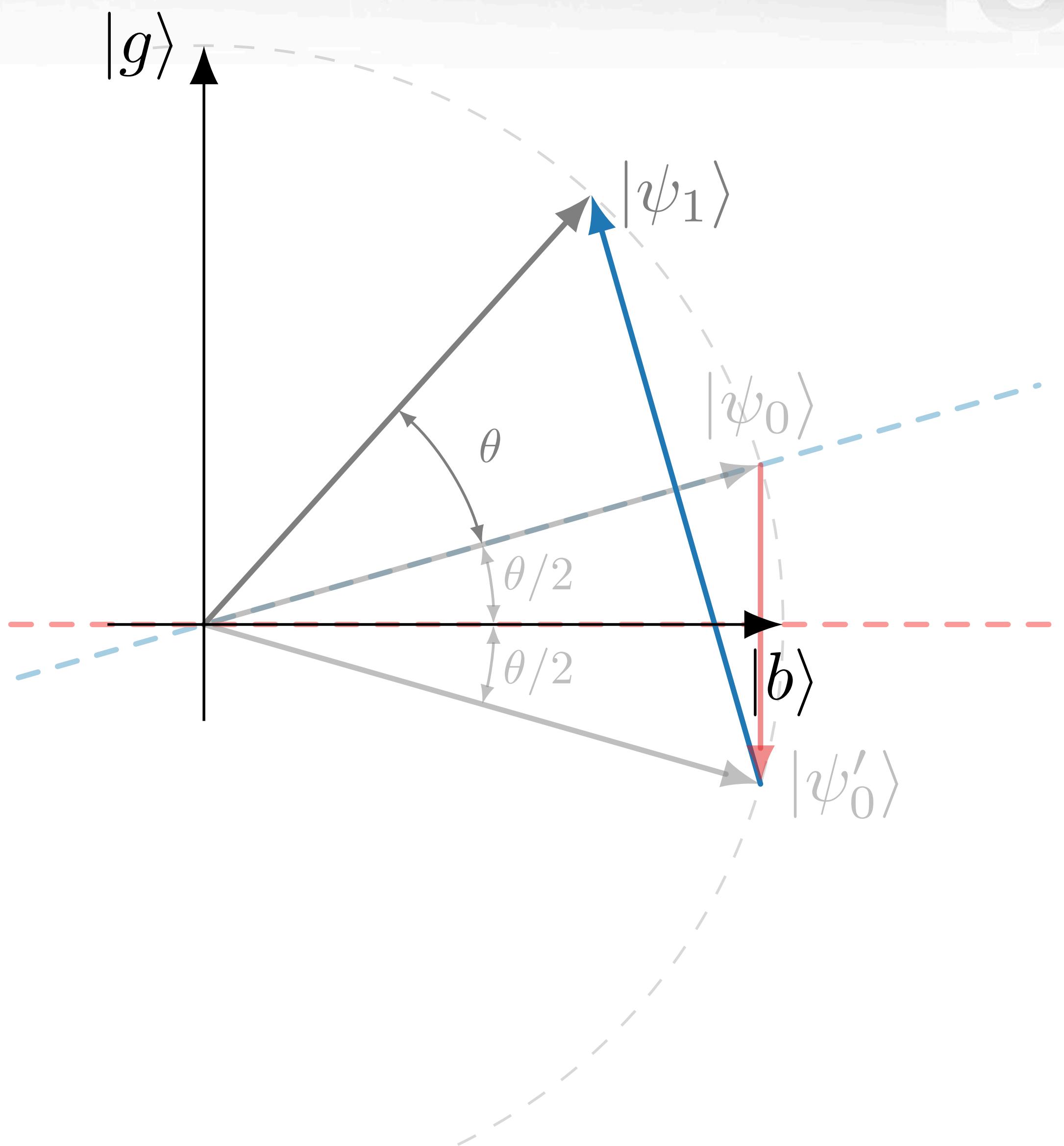


Algorithme de Grover

Principe de fonctionnement

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

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

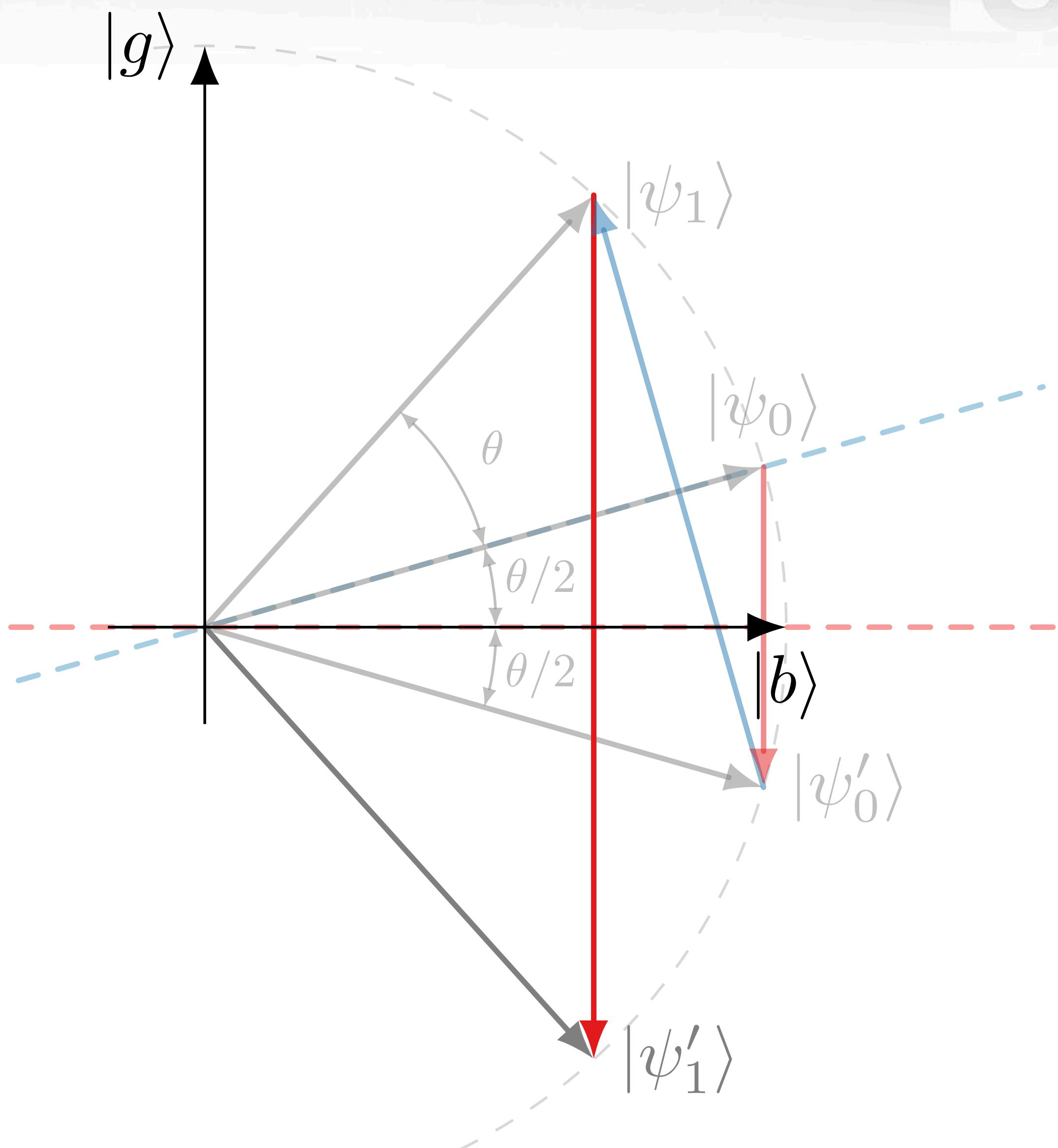


Algorithme de Grover

Principe de fonctionnement

$$|\psi'_1\rangle = \cos(3\theta/2) |b\rangle - \sin(3\theta/2) |g\rangle$$

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

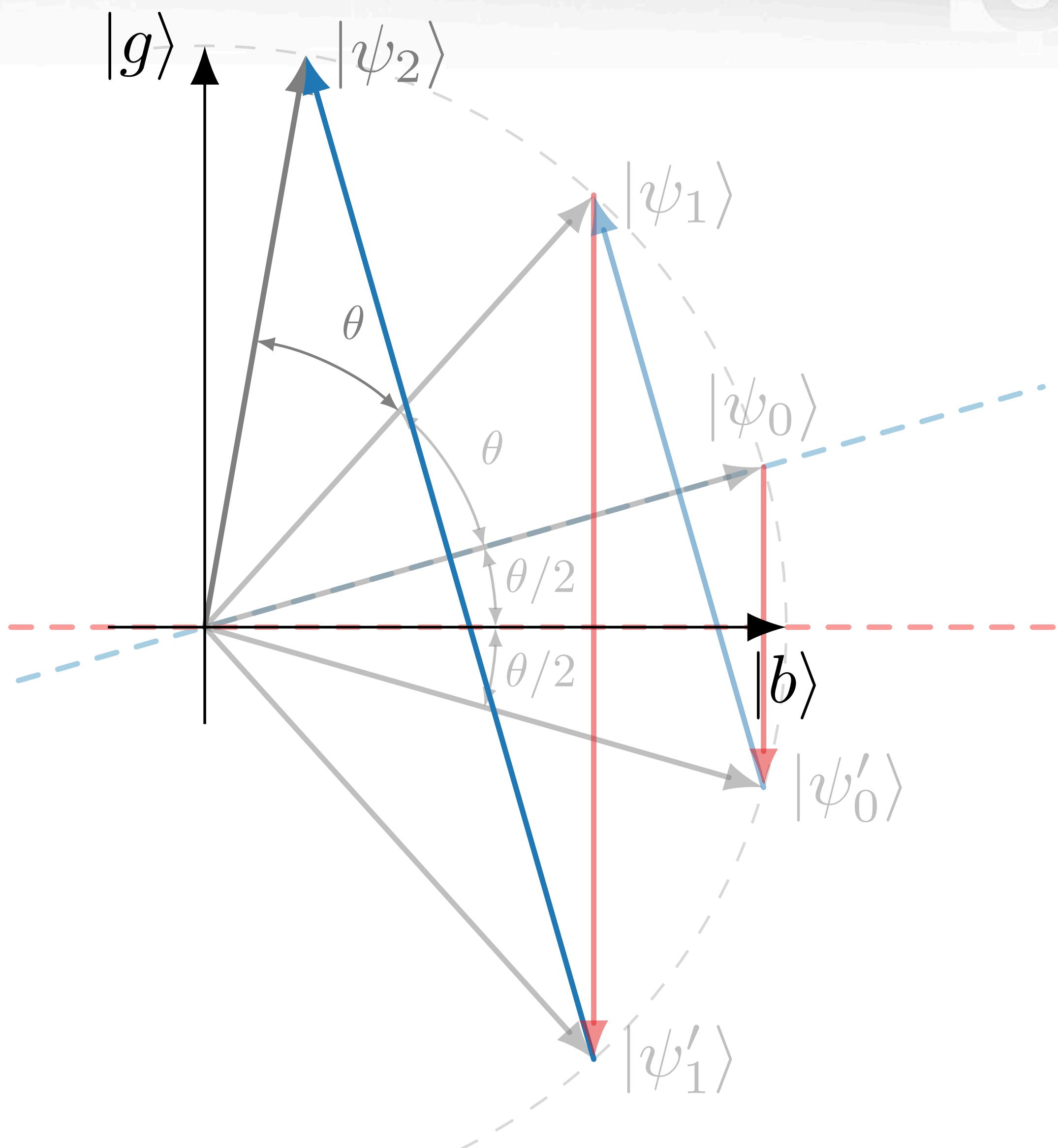


Algorithme de Grover

Principe de fonctionnement

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

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



Algorithme de Grover

Principe de fonctionnement

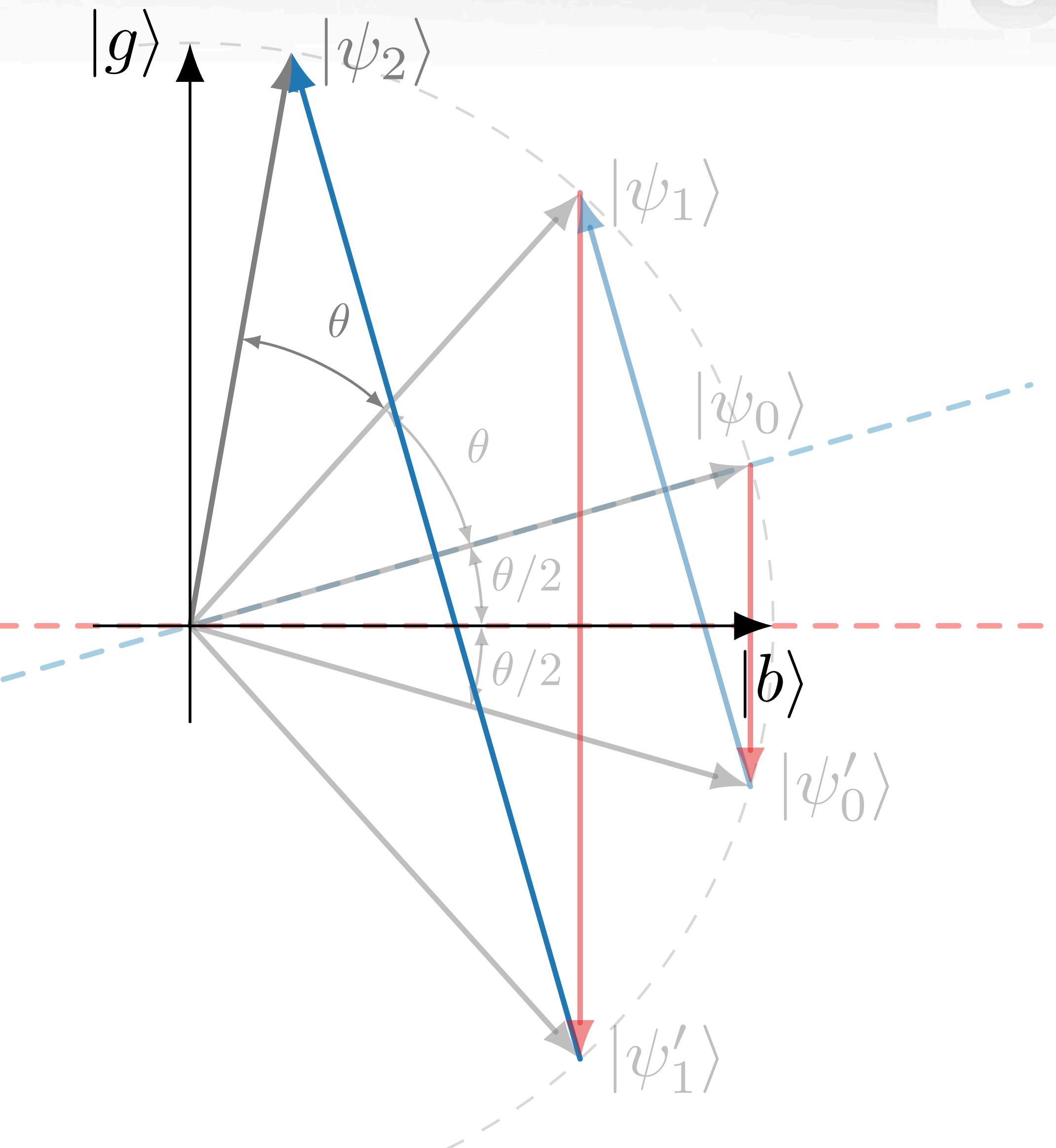
$$|\psi_n\rangle = \cos((n + 1/2)\theta) |b\rangle + \sin((n + 1/2)\theta) |g\rangle$$

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

→ Action de l'oracle

→ Action du diffuseur

Comment peut-on effectuer ces réflexions?



Le diffuseur

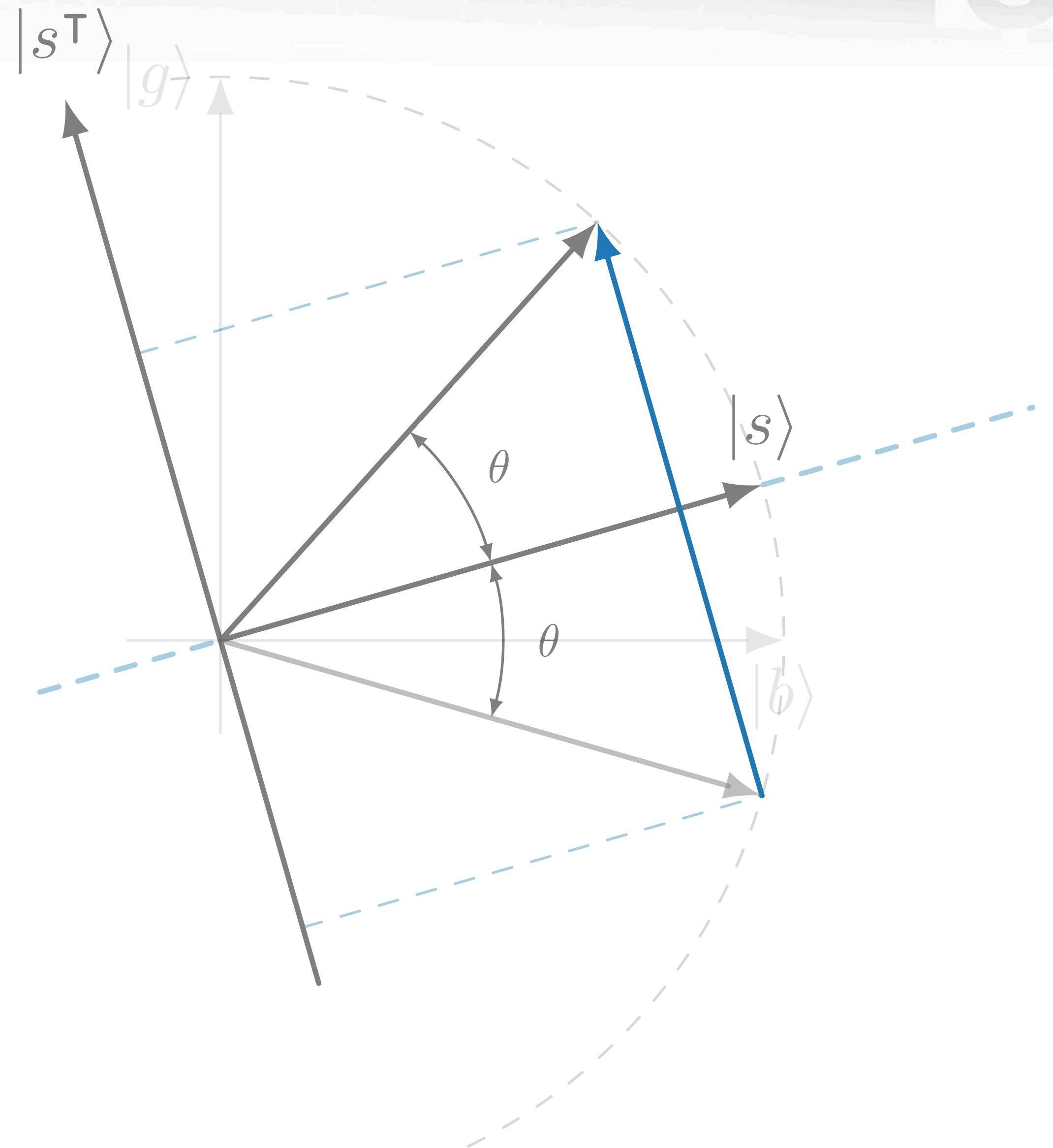
Diffuseur Action

On peut écrire les états

$$|\phi\rangle = \cos(\theta) |s\rangle + \sin(\theta) |s^\top\rangle$$

On veut que le diffuseur **inverse la phase des états orthogonaux à $|s\rangle$**

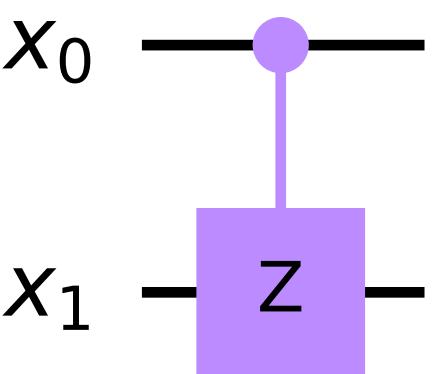
$$\hat{U}_{\text{diffuseur}} |\phi\rangle = \cos(\theta) |s\rangle - \sin(\theta) |s^\top\rangle$$



Diffuseur

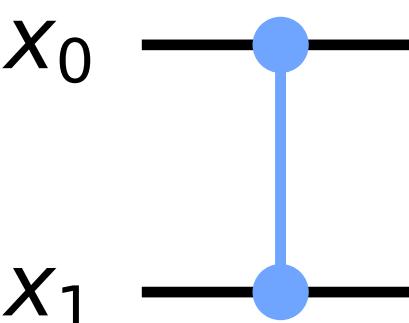
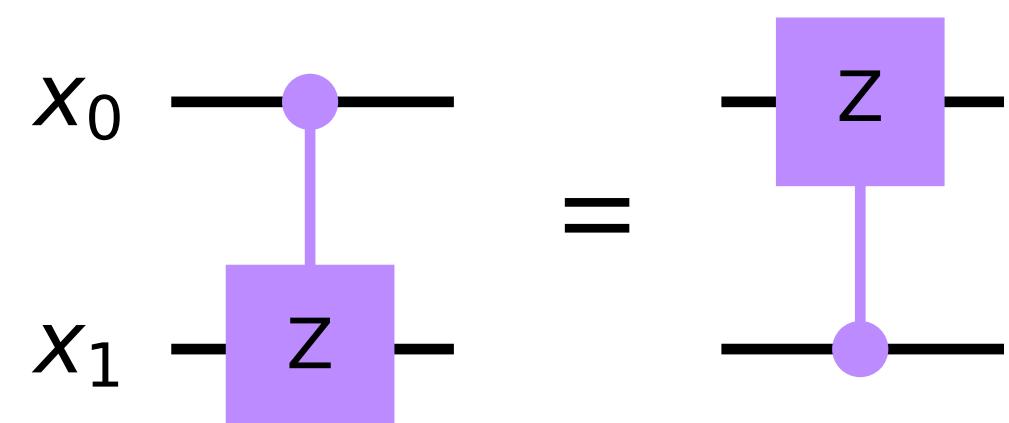
Porte contrôle-Z

La porte contrôle-Z applique une porte Z sur un **qubit cible** (x_1) si le **qubit de contrôle** (x_0) est dans l'état $|1\rangle$.



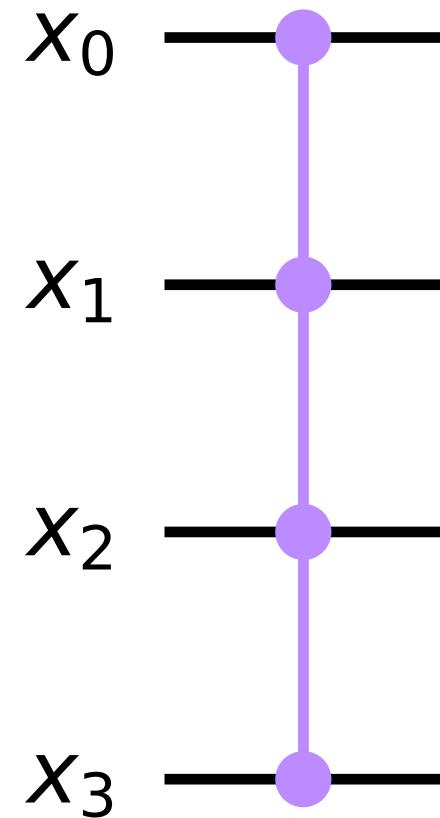
$$C\hat{Z} |11\rangle = -|11\rangle$$

La porte contrôle-Z est **symétrique**.



Diffuseur

Construction



Du point de vue de la porte MCZ, tout état comporte **deux composantes**

$$|\phi\rangle = \alpha |1\rangle + \beta |1^\top\rangle$$

Son action se résume à **inverser la phase** de l'état $|1\rangle$

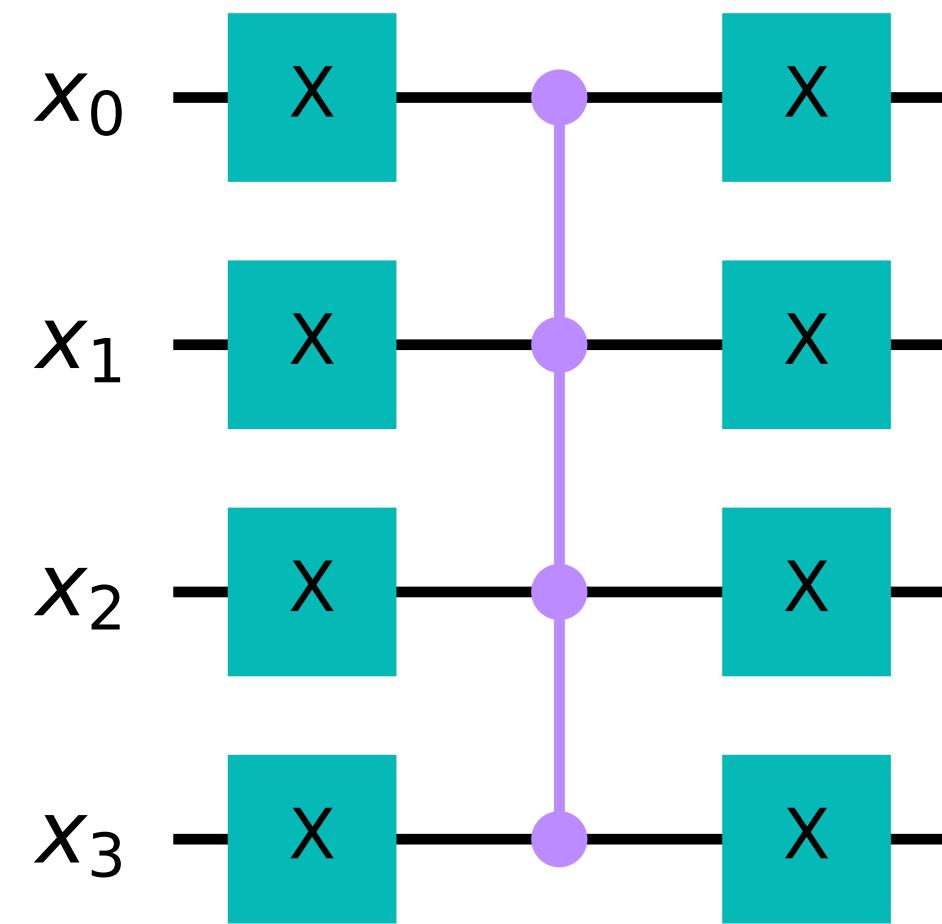
$$MC\hat{Z} |\phi\rangle = -\alpha |1\rangle + \beta |1^\top\rangle$$

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

$$|1\rangle = |11\dots 1\rangle$$

Diffuseur

Construction



Du point de vue de ce circuit, tout état comporte **deux composantes**

$$|\phi\rangle = \alpha |0\rangle + \beta |0^\top\rangle$$

Son action se résume à **inverser la phase** de l'état $|0\rangle$

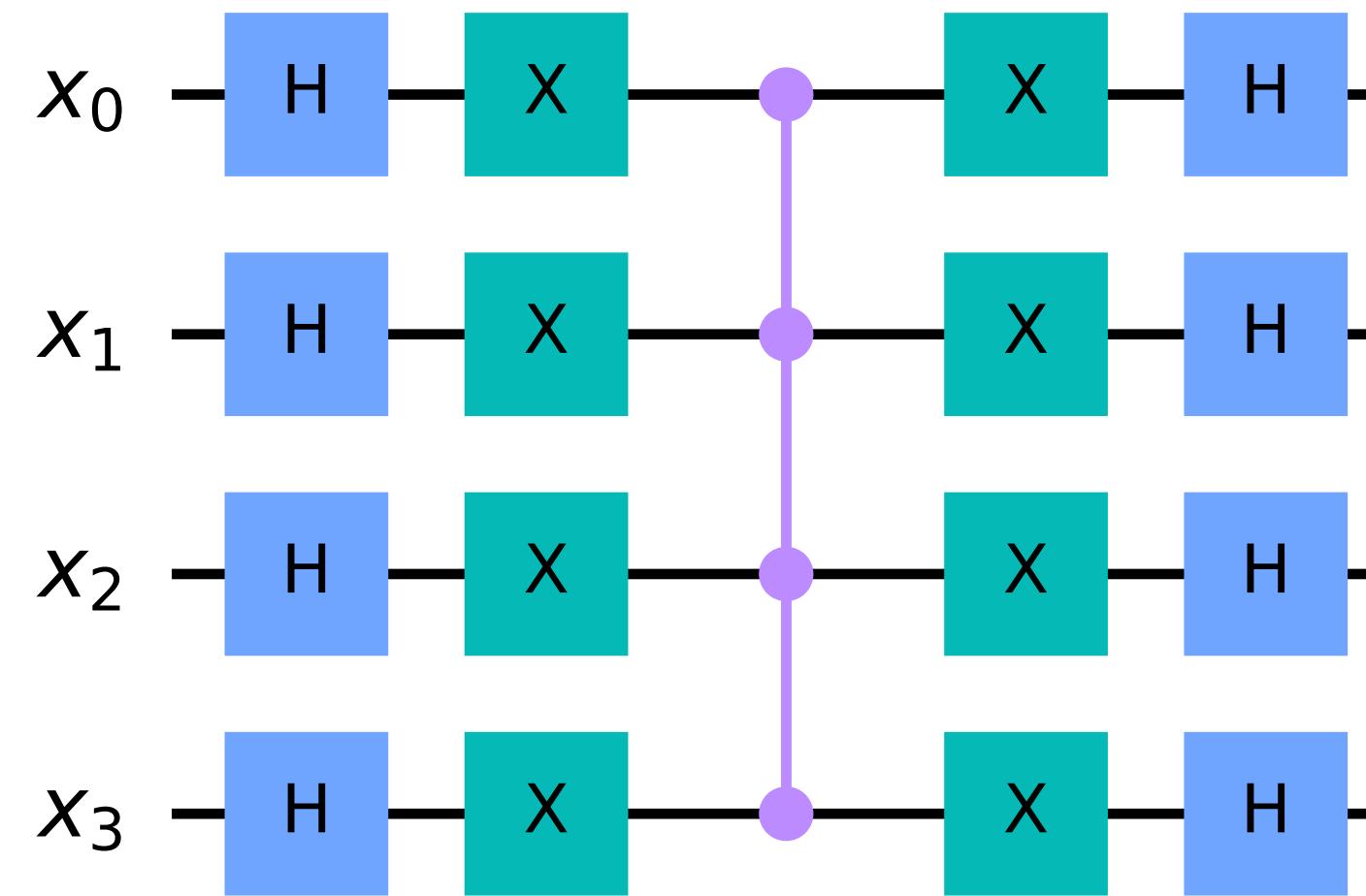
$$\hat{U} |\phi\rangle = -\alpha |0\rangle + \beta |0^\top\rangle$$

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

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

Diffuseur

Construction



Du point de vue de ce circuit, tout état comporte **deux composantes**

$$|\phi\rangle = \alpha |s\rangle + \beta |s^\top\rangle$$

Son action se résume à **inverser la phase** de l'état $|s\rangle$

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

Ce qui correspond exactement à ce dont on a besoin!

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

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

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

... à un signe - près, qui n'a pas de conséquences physiques.

L'oracle

L'oracle

Action

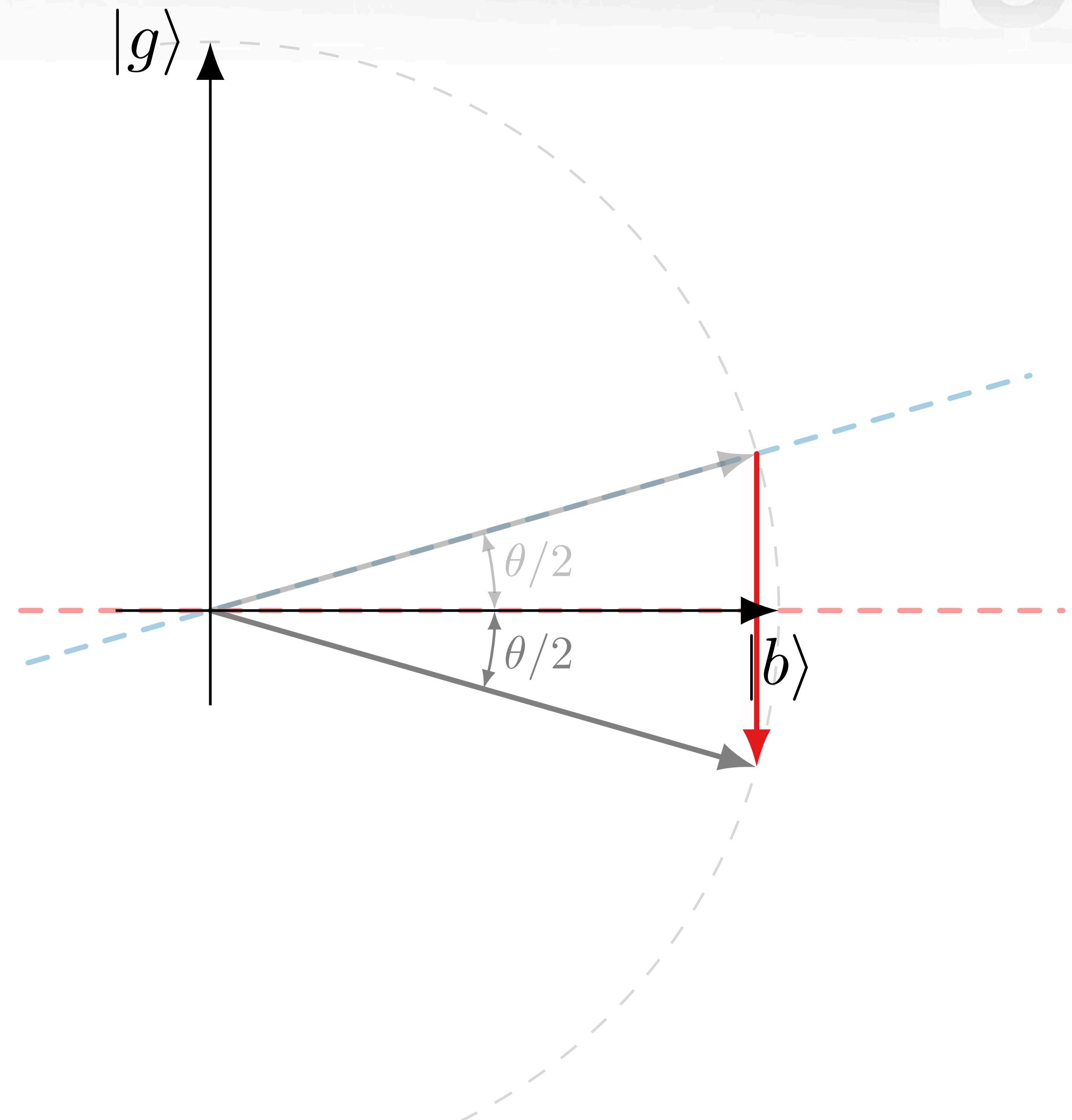
On va construire l'oracle de sorte qu'il **inverse la phase** des états *good*

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

Cela permettra d'effectuer la réflexion voulue.

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

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



L'oracle

Action

On va construire l'oracle de sorte qu'il **inverse la phase** des états *good*

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

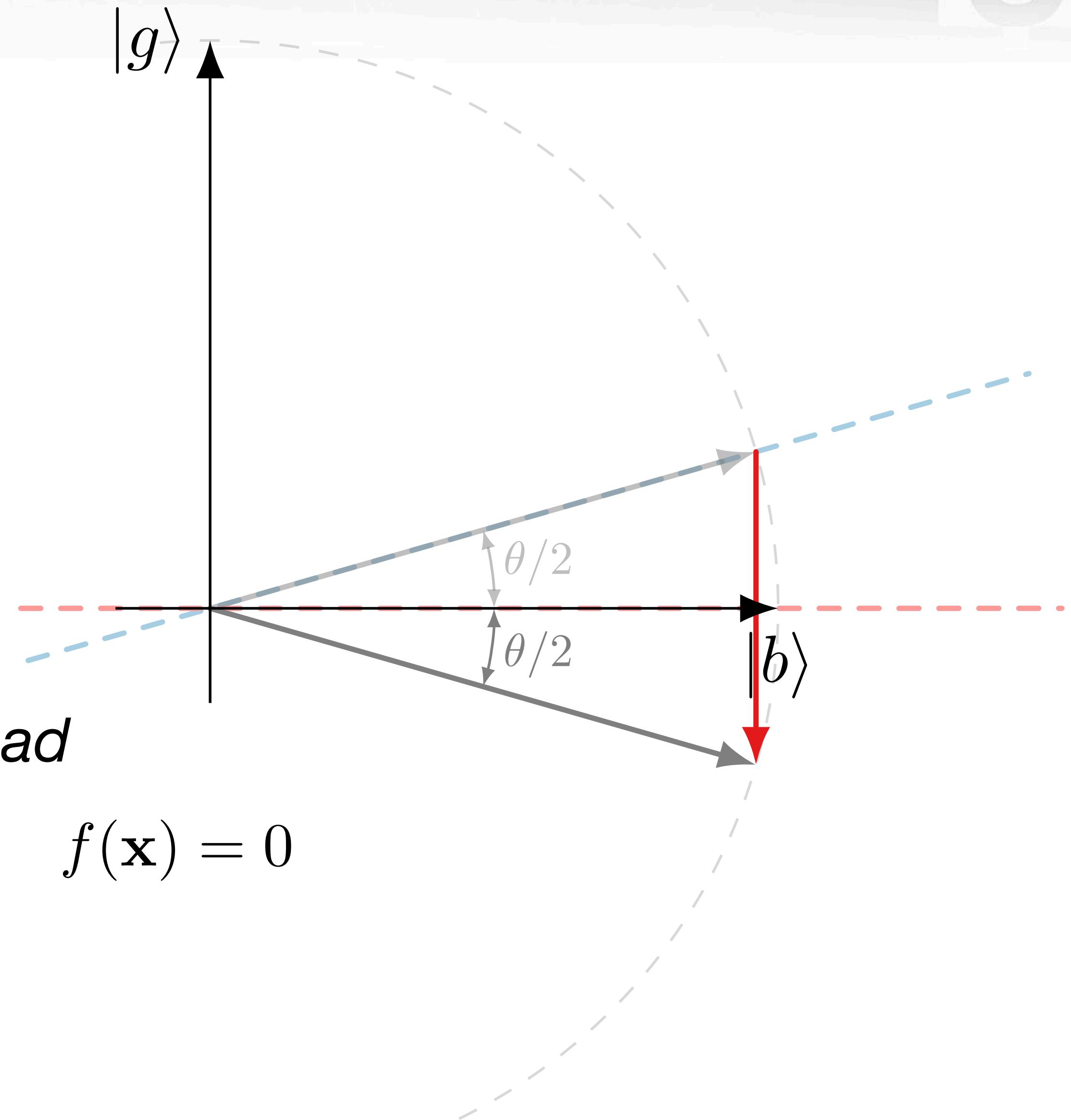
On se rappelle que les états sont *good* ou *bad*

$$\mathbf{x} \in G \quad \text{si} \quad f(\mathbf{x}) = 1$$

$$\mathbf{x} \in B \quad \text{si} \quad f(\mathbf{x}) = 0$$

On peut résumer l'effet de l'**oracle** à

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

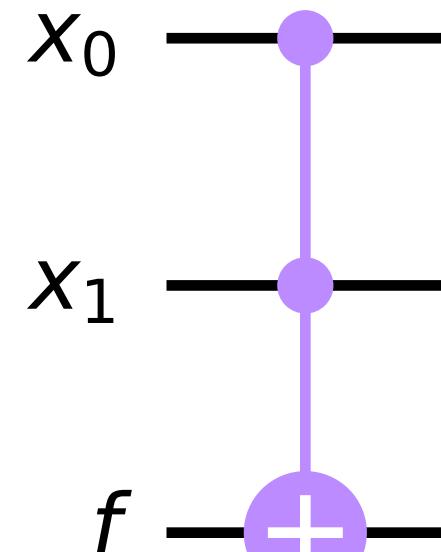


Logique et portes quantiques

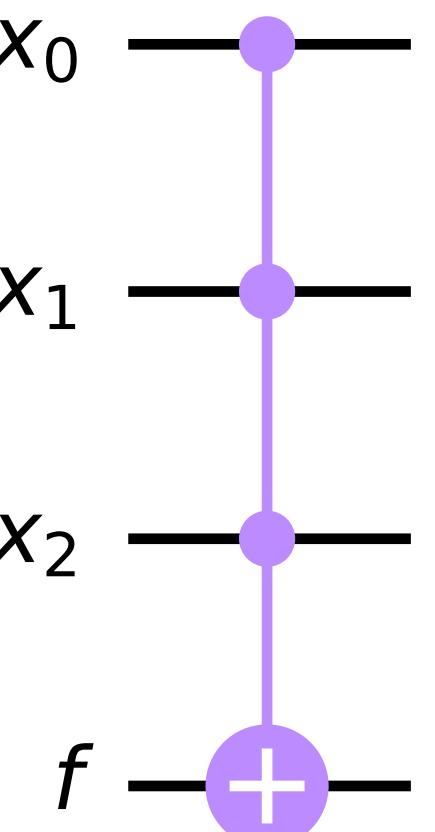
Porte de conjonction (et) vers qubit

On peut écrire, dans un **qubit ancillaire**, l'évaluation d'une **conjonction**.

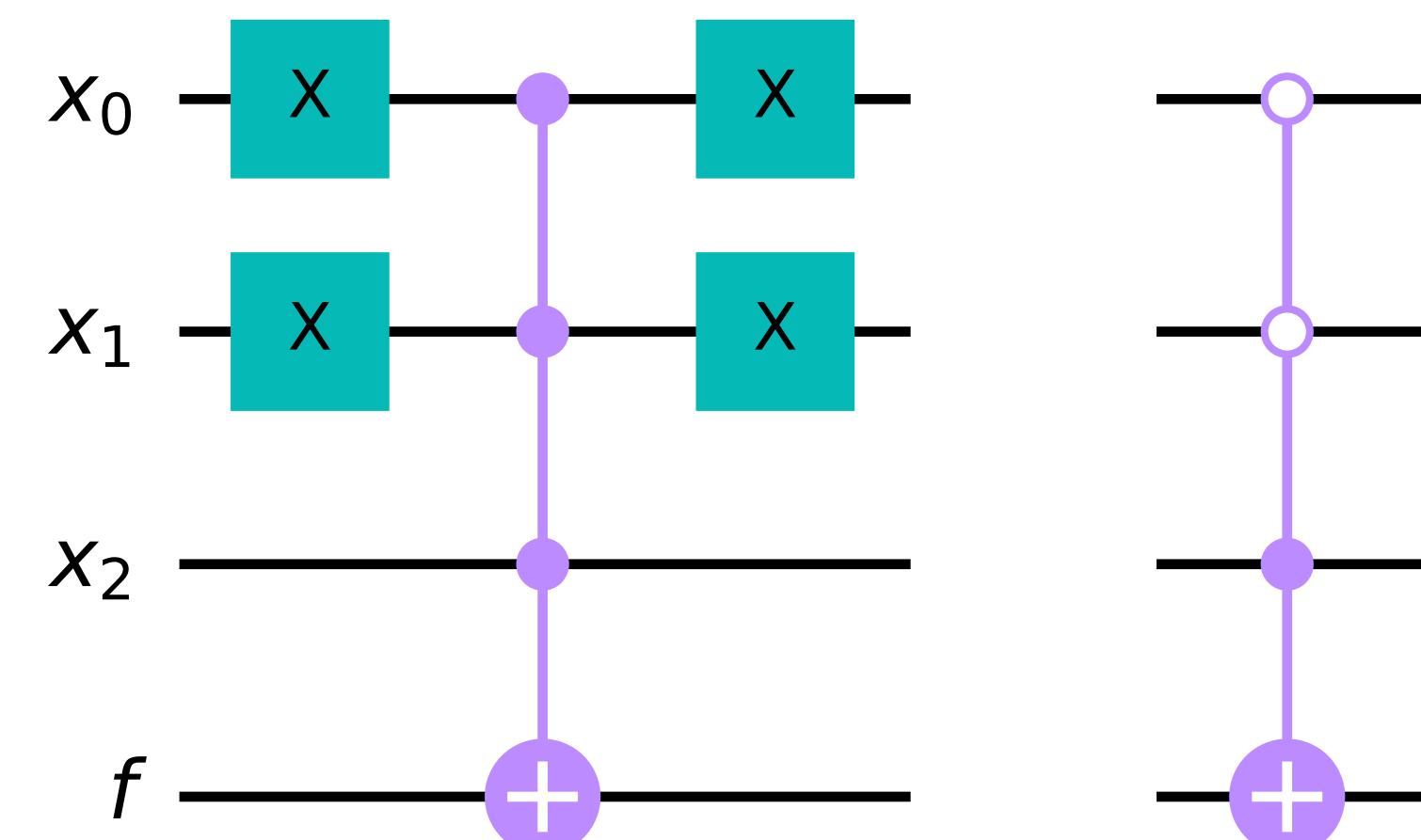
$$f = x_0 \wedge x_1$$



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



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



Logique et portes quantiques

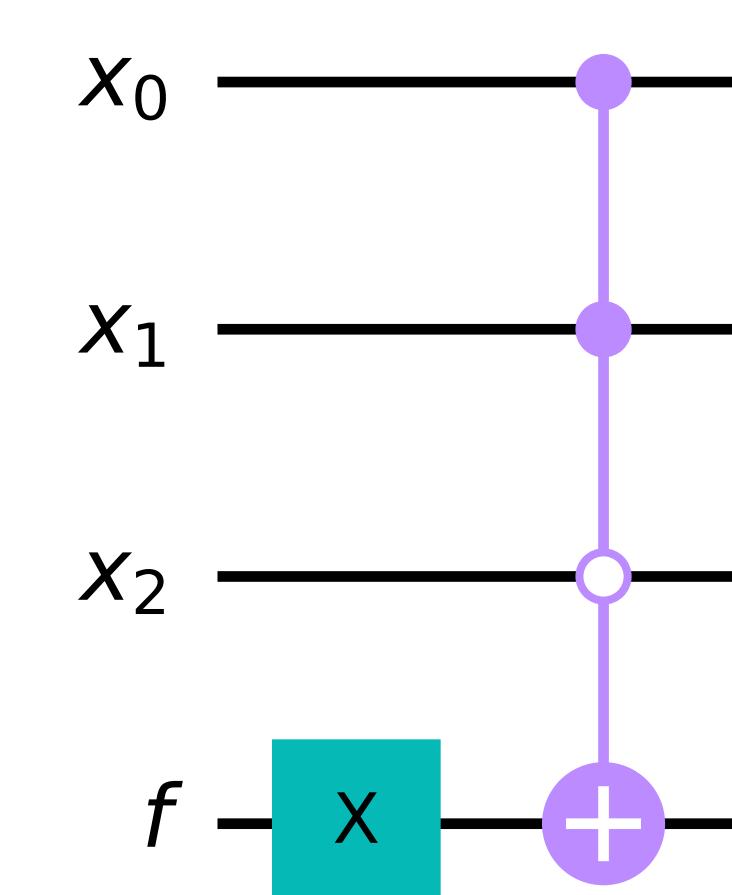
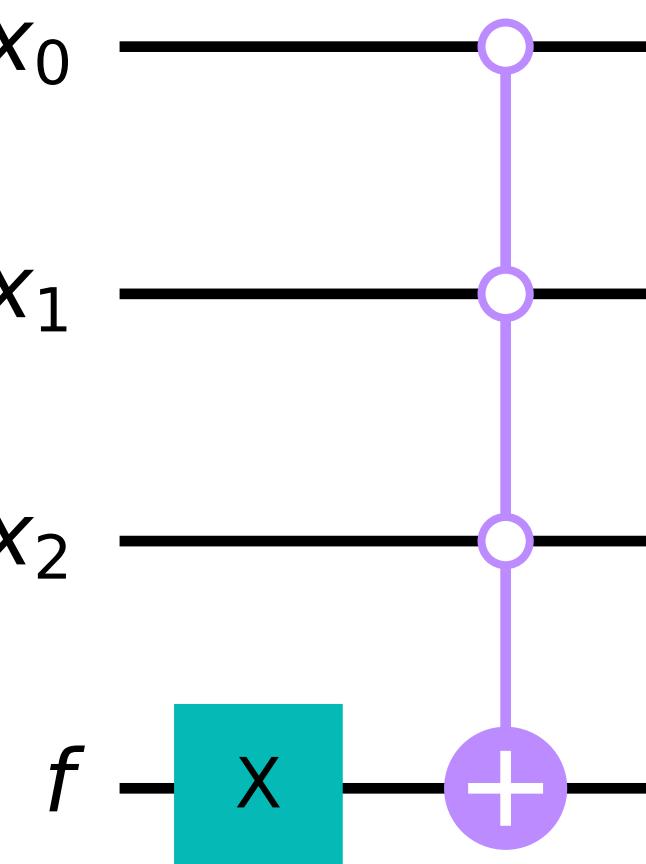
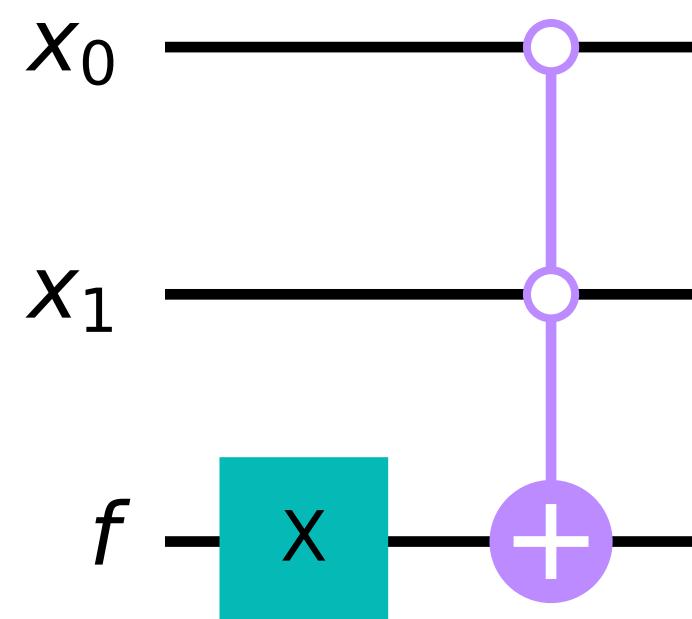
Porte de disjonction (ou) vers qubit

On peut écrire, dans un **qubit ancillaire**, l'évaluation d'une **disjonction**.

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

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

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



L'oracle

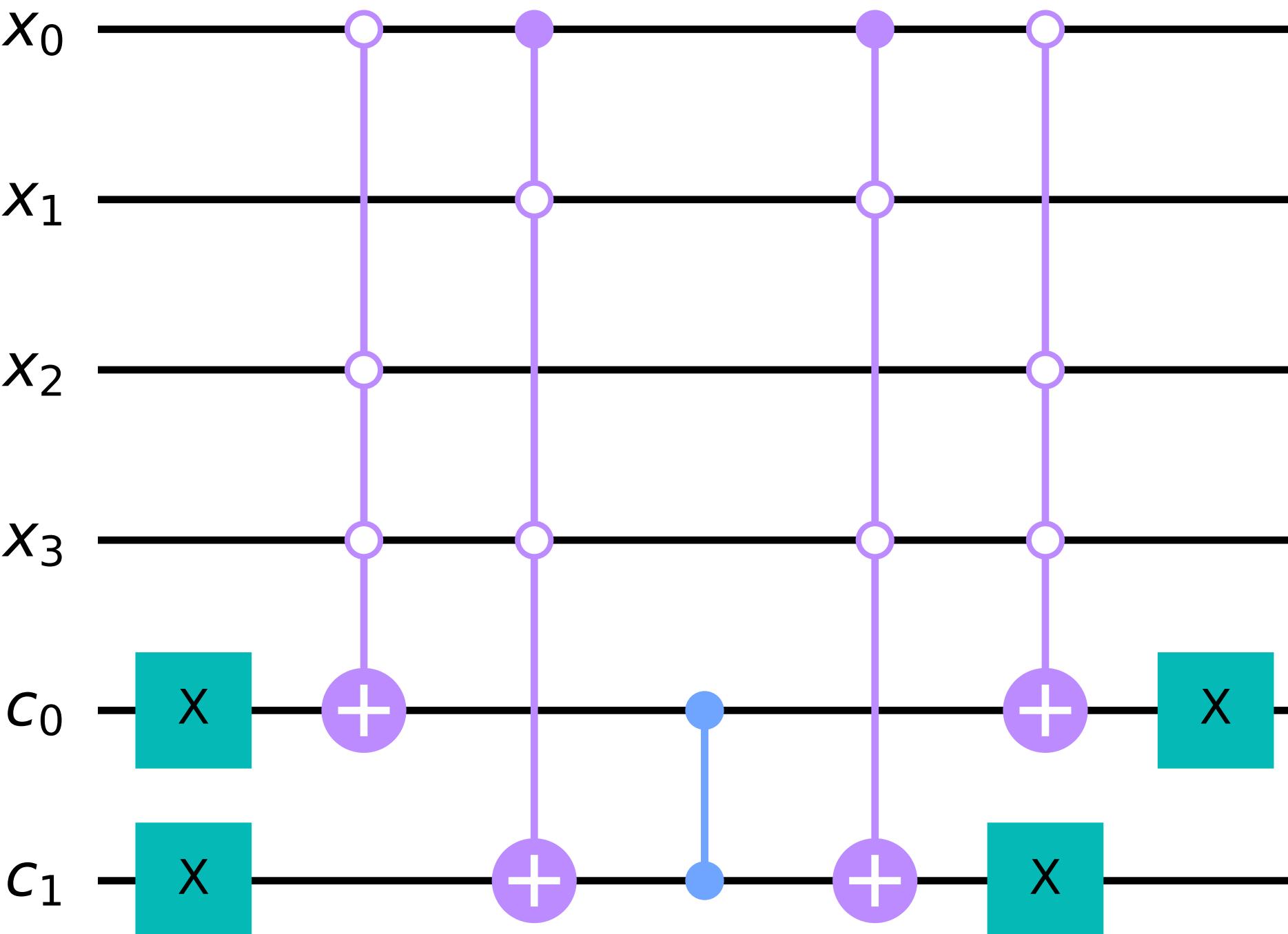
Exemple de circuit

Construisons l'oracle pour les **deux premières propositions** du problème.

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

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

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



L'oracle

Exemple de circuit

Construction de l'oracle pour le problème de la planète Pincus.

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

À vous de jouer!

