Unstructured Search

via Grover’s Algorithm

Fernando Granha Jeronimo

Unstructured Search

Unstructured Search

- Given a function $f\colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)

Unstructured Search

- Given a function $f\colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)
- The function f is given as black-box oracle: $O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ for any $x \in \{0,1\}^n$

Unstructured Search

- Given a function f: $\{0,1\}^n \rightarrow \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)
- The function f is given as black-box oracle: $O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ for any $x \in \{0,1\}^n$
- How many queries are needed?

Unstructured Search

- Given a function $f\colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)
- The function f is given as black-box oracle: $O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ for any $x \in \{0,1\}^n$
- How many queries are needed?

Any classical computer requires $\Omega(2^n)$ queries!

Unstructured Search

Unstructured Search

Can a quantum computer beat brute-force search?

Unstructured Search

- Given a function $f\colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)
- The function f is given as black-box oracle: $O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ for any $x \in \{0,1\}^n$
- First, why should we care about this problem at all?

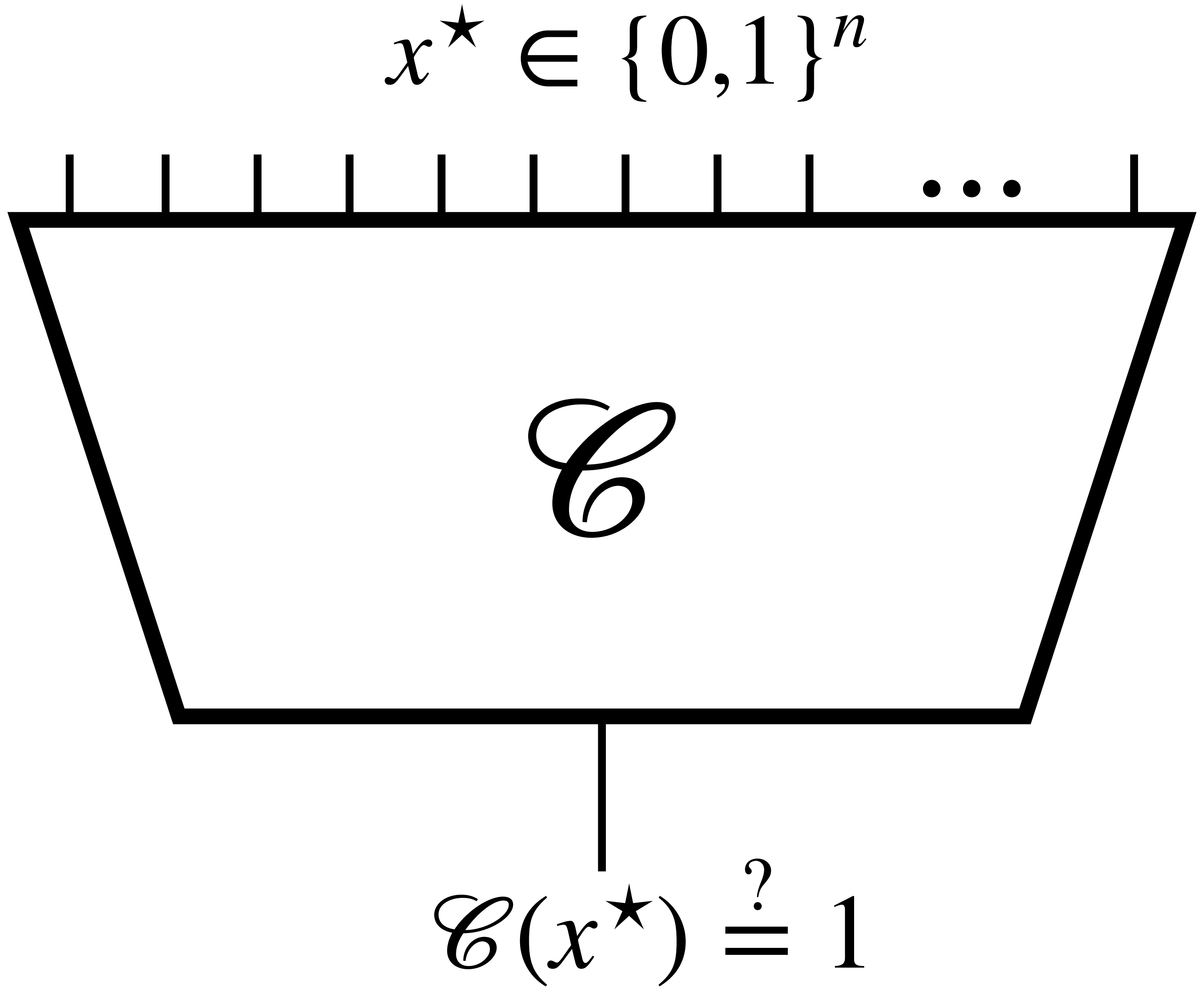
Unstructured Search

- Given a function $f\colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)
- The function f is given as black-box oracle: $O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ for any $x \in \{0,1\}^n$
- First, why should we care about this problem at all?

In particular, f can encode the evaluation of a classical circuit $\mathscr{C}$

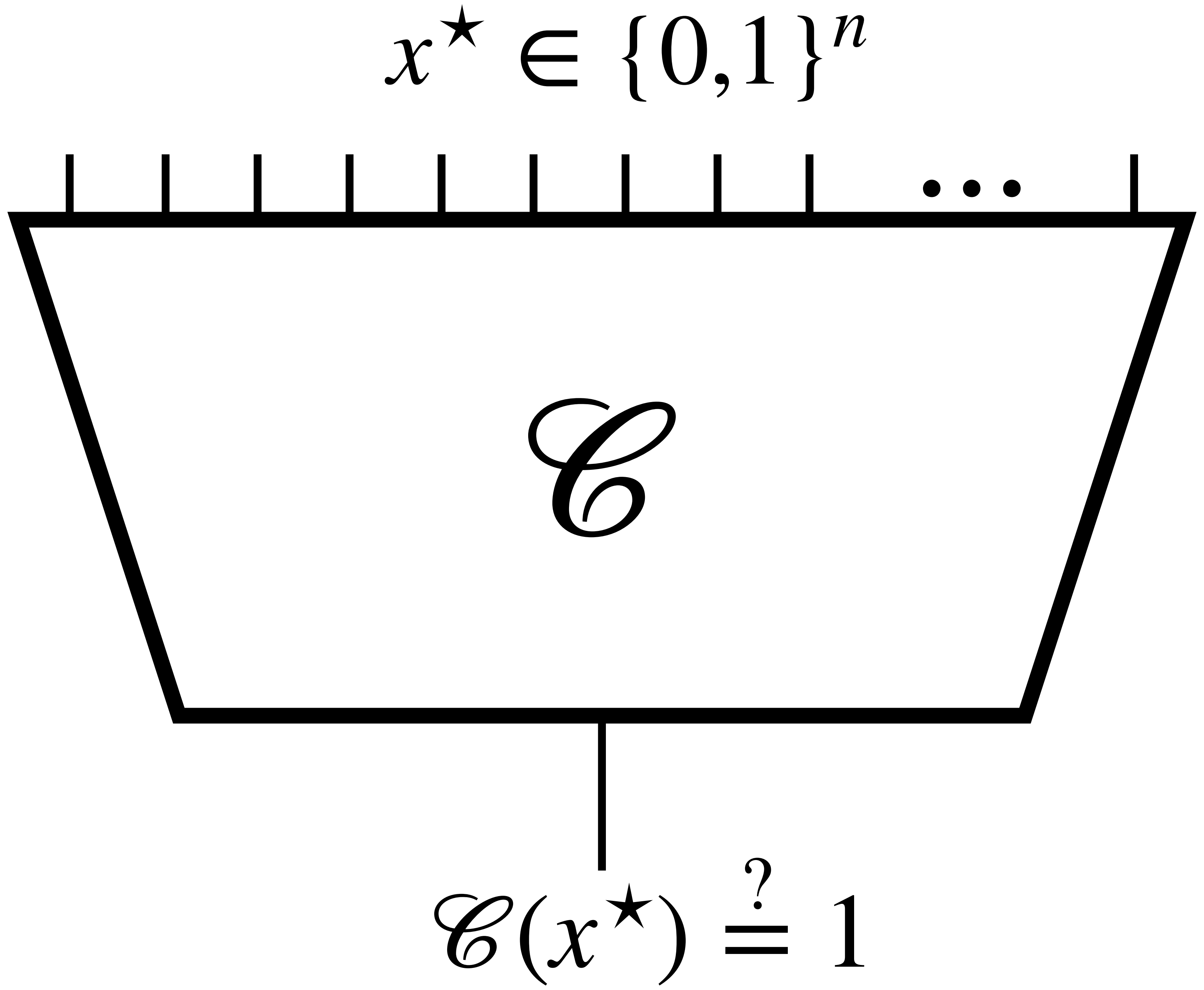
Unstructured Search

In particular, f can encode the evaluation of a classical circuit $\mathscr{C}$



Unstructured Search

In particular, f can encode the evaluation of a classical circuit $\mathscr{C}$



Determining if $\mathscr{C}$ has a satisfying input is NP-complete

Unstructured Search

- Given a function $f \colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)
- The function f is given as black-box oracle: $O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ for any $x \in \{0,1\}^n$

Unstructured Search

- Given a function $f\colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)

- The function f is given as black-box oracle: $O_f|x\rangle = (-1)^{f(x)}|x\rangle$ for any $x \in \{0,1\}^n$

  (Phase Oracle)

Unstructured Search

- Given a function $f\colon \{0,1\}^n \to \{0,1\}$, find any $x \in \{0,1\}^n$ such that $f(x) = 1$ (if one exists)
- The function f is given as black-box oracle: $O_f|x\rangle = (-1)^{f(x)}|x\rangle$ for any $x \in \{0,1\}^n$

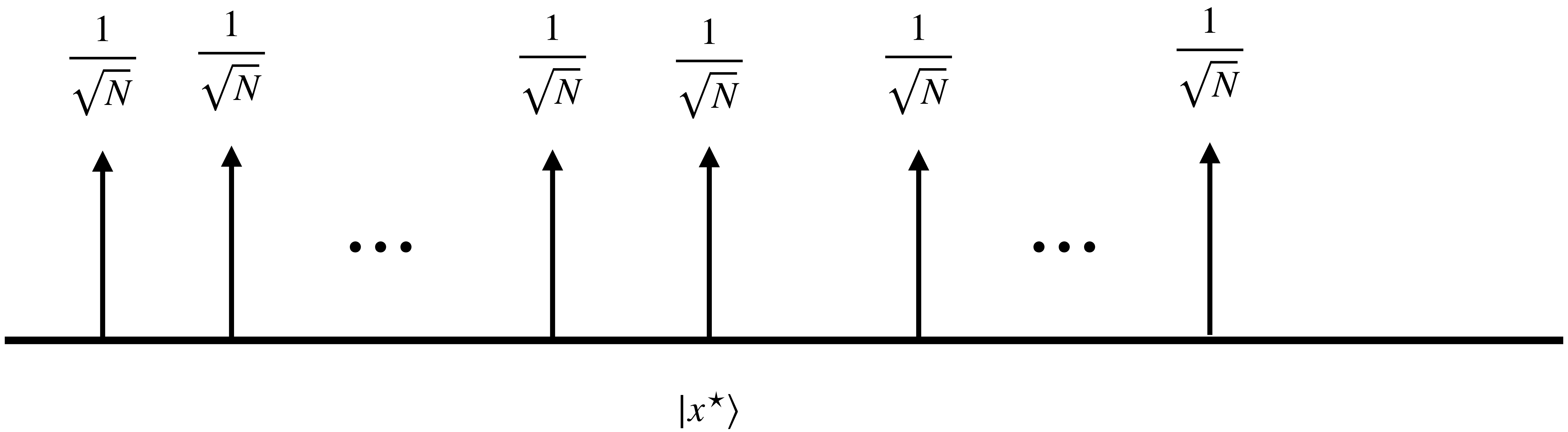
(Phase Oracle)

$$\Uparrow$$

$$O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$$

Some Intuition

$N = 2^n$

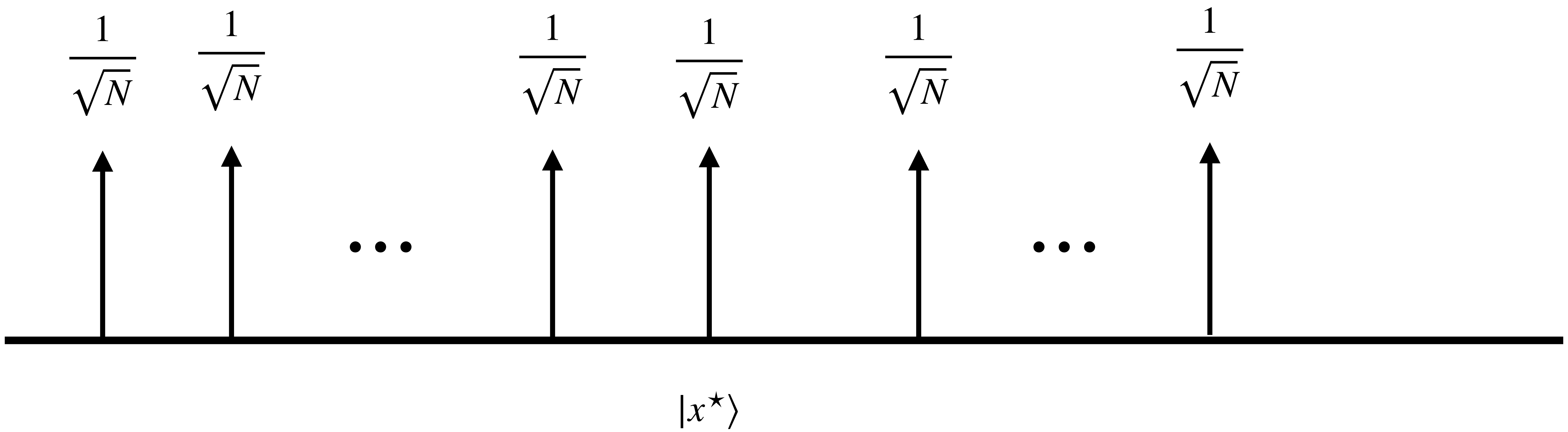


$$|u\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Some Intuition

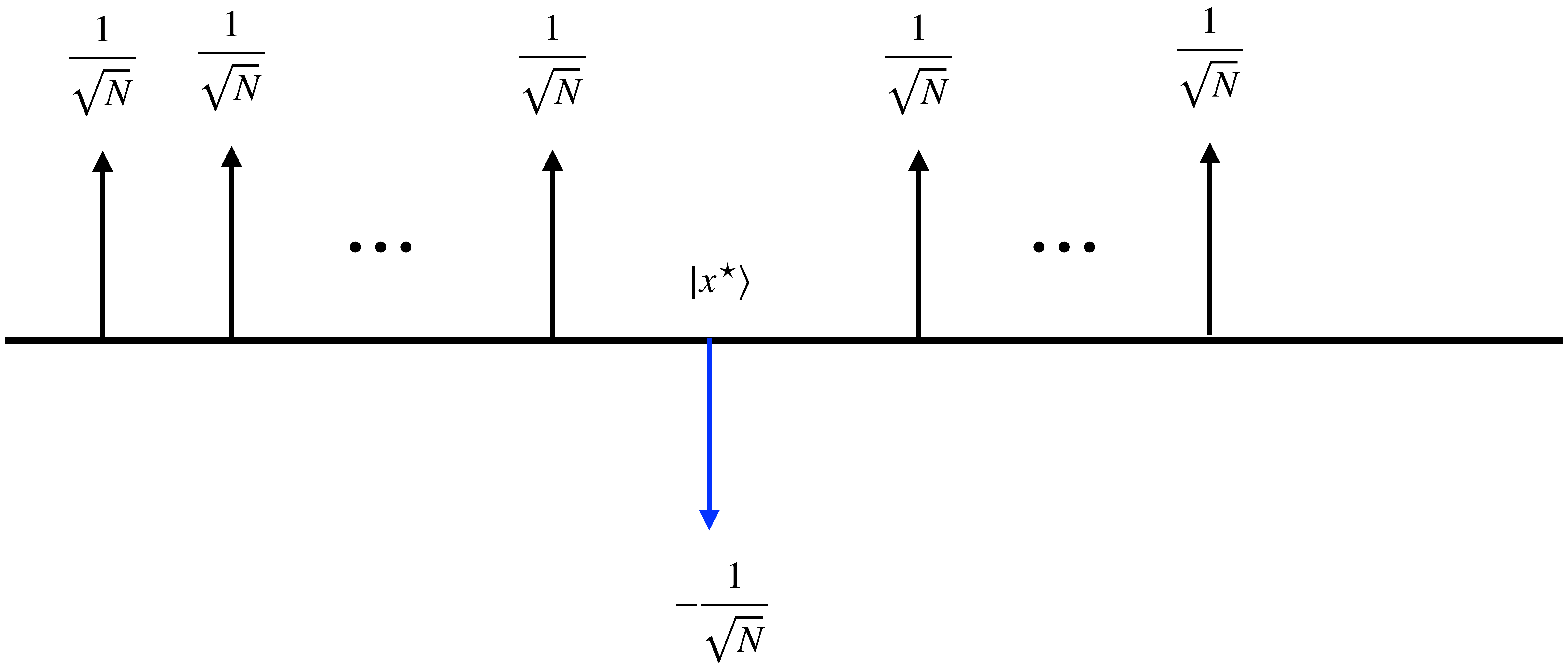
$N = 2^n$

For now, assume there is exactly one $x^\star$ with $f(x^\star) = 1$



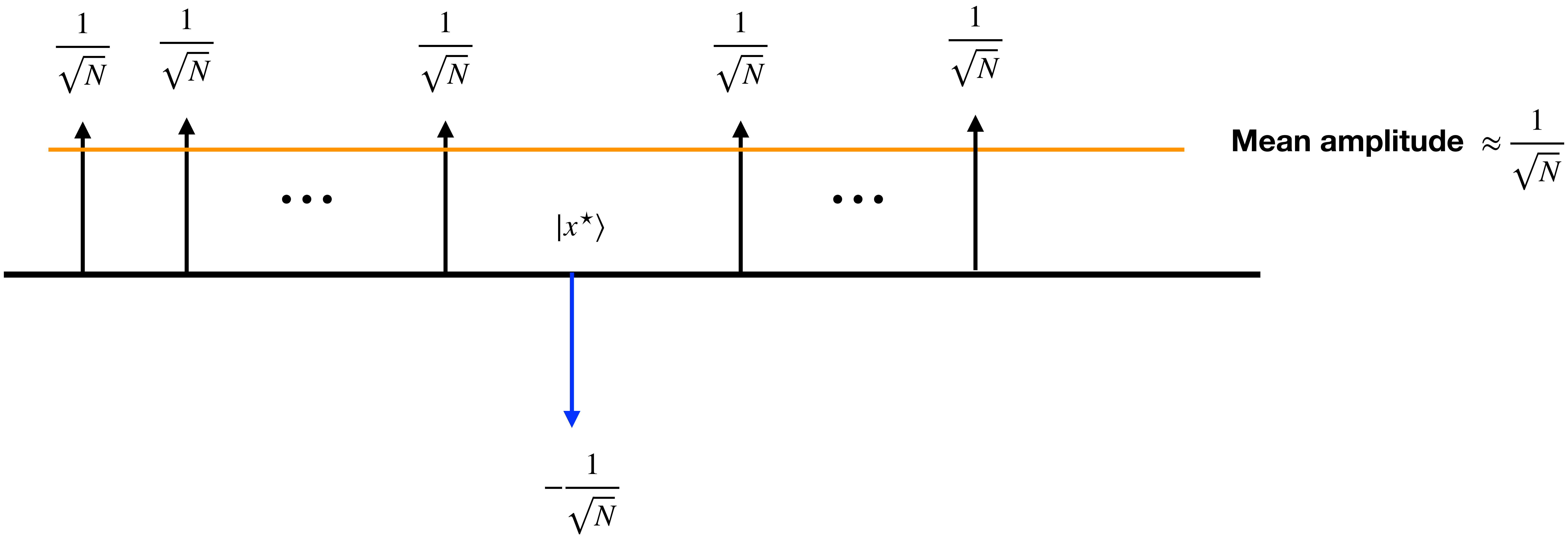
$$|u\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Some Intuition



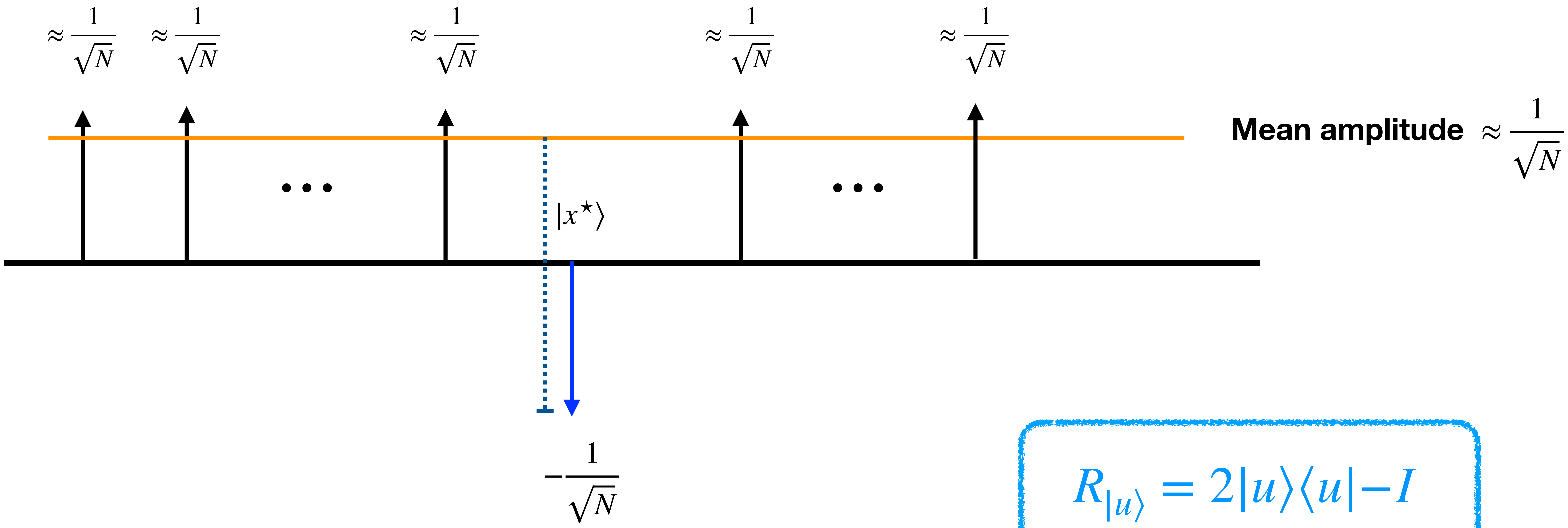
$O_f|u\rangle$

Some Intuition



$$O_f|u\rangle$$

Some Intuition

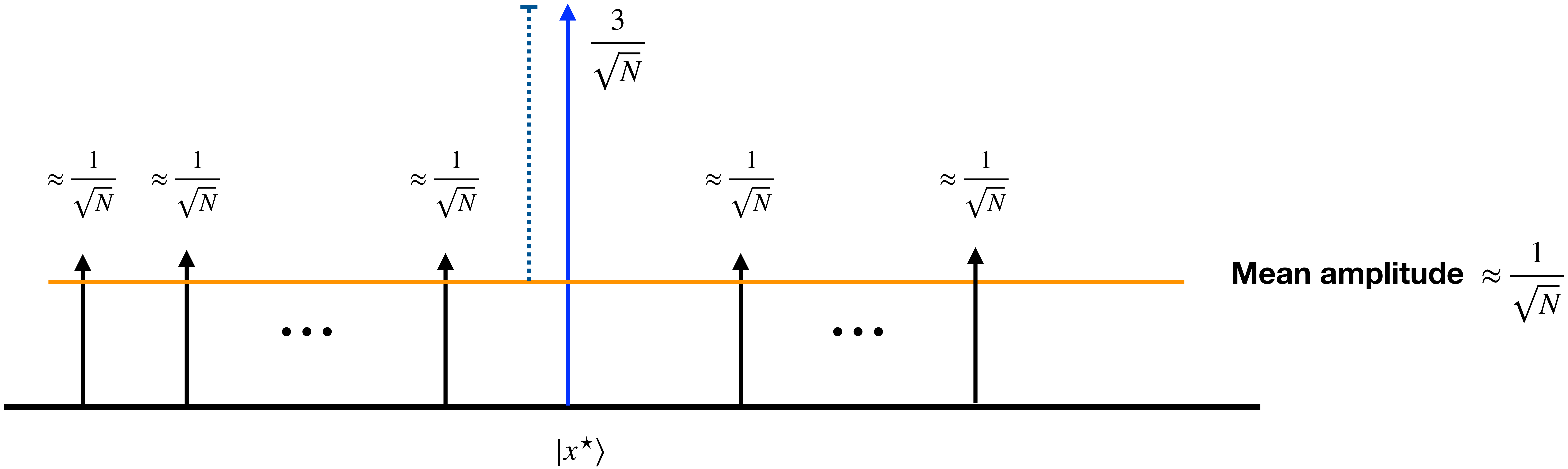


$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

Reflect around the "mean"

$$R_{|u\rangle} O_f |u\rangle$$

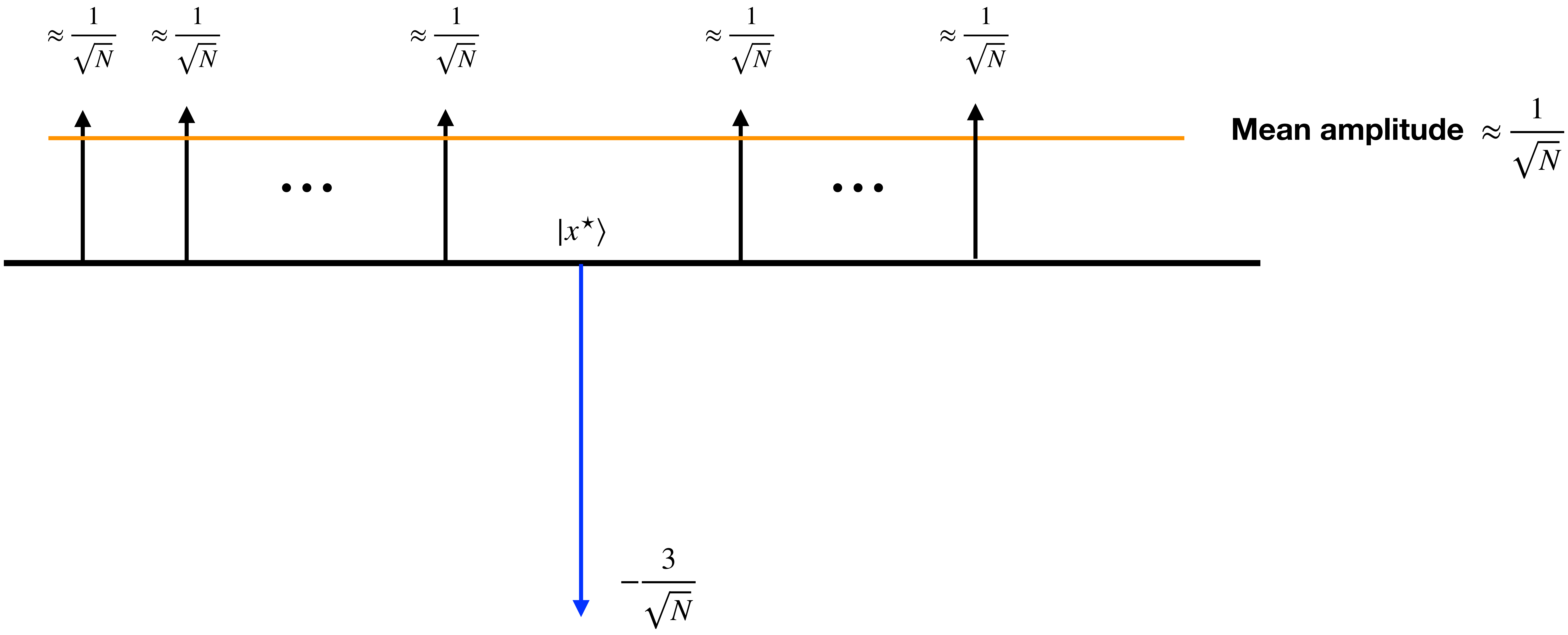
Some Intuition



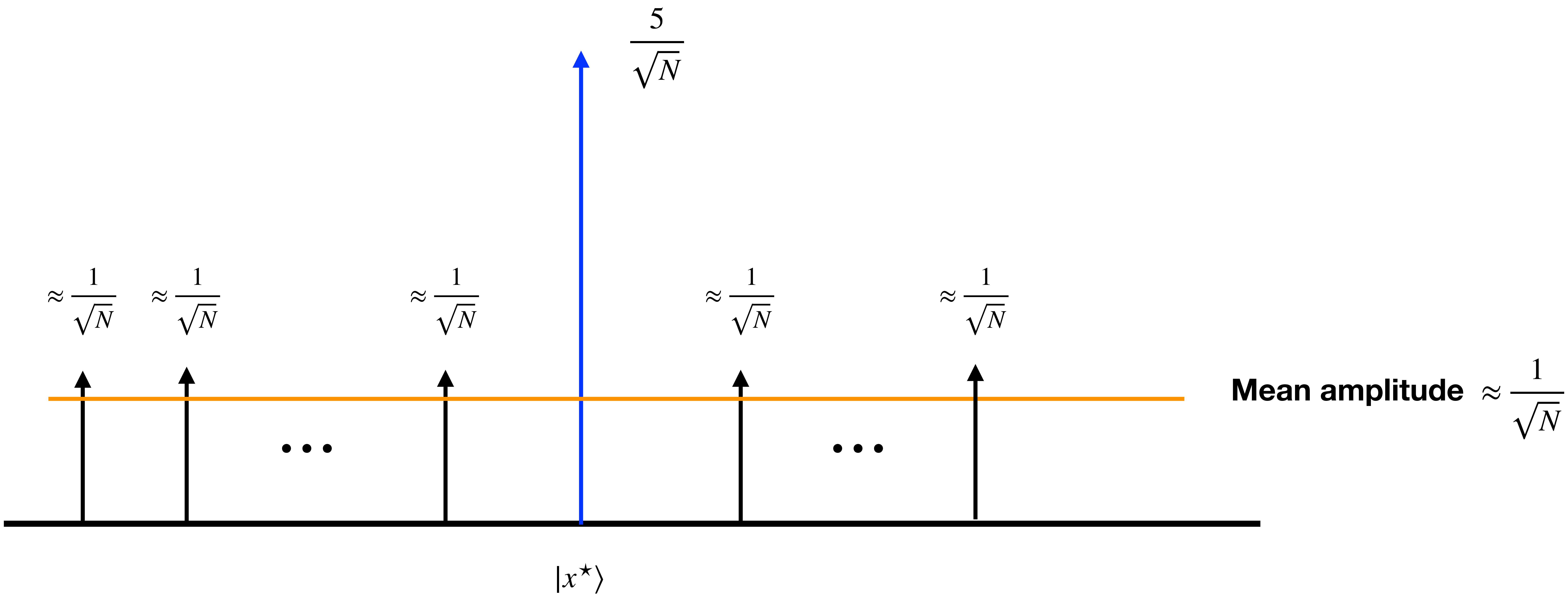
$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

Reflect around the "mean" $R_{|u\rangle} O_f |u\rangle$

Some Intuition



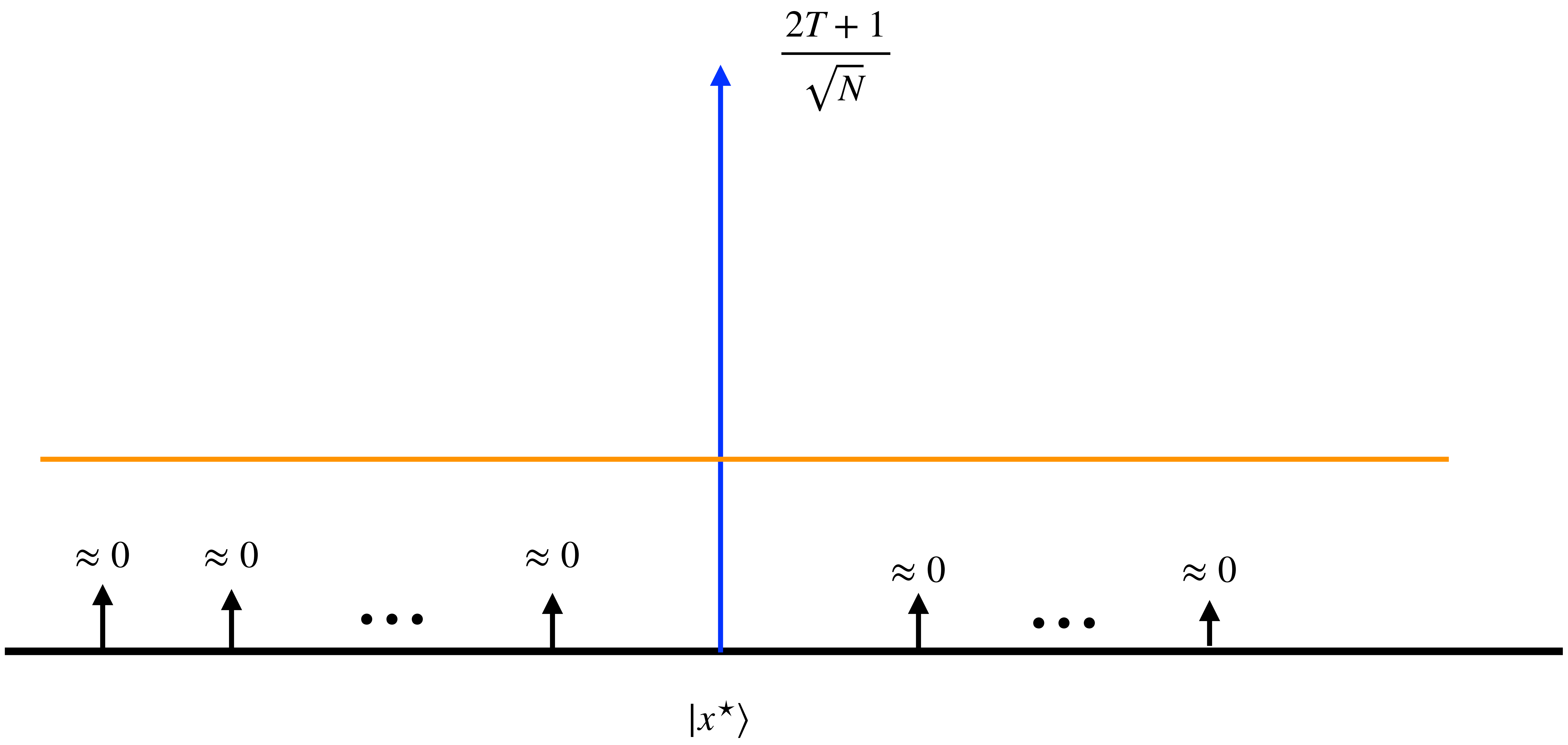
$$O_f R_{|u\rangle} O_f |u\rangle$$



Reflect around the "mean"

$$R_{|u\rangle} O_f R_{|u\rangle} O_f |u\rangle$$

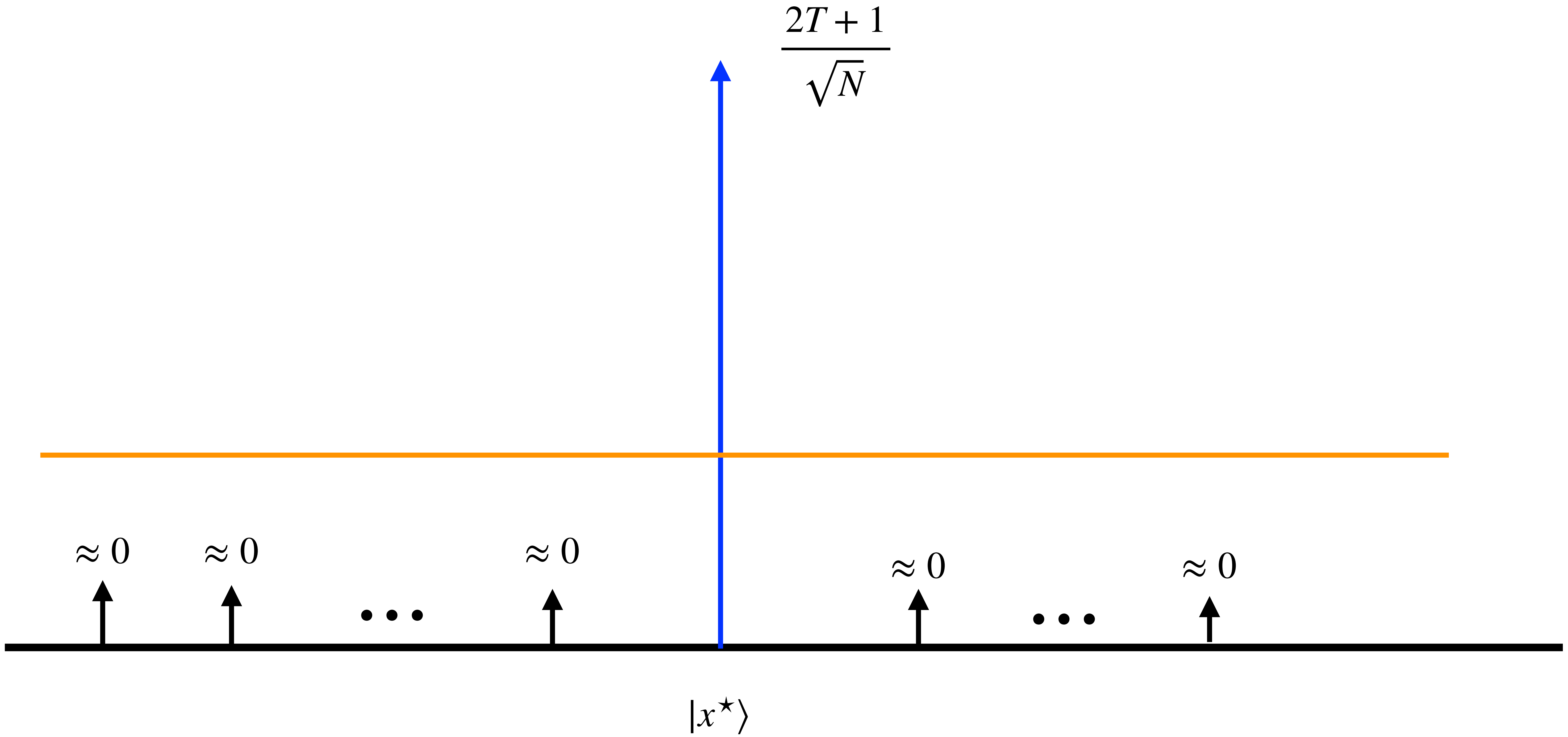
Extrapolating, we would guess…



After T queries $(R_{|u\rangle} O_f)^T |u\rangle$

Extrapolating, we would guess…

Suggests $T = O(\sqrt{N})$ suffice, beating brute-force search!

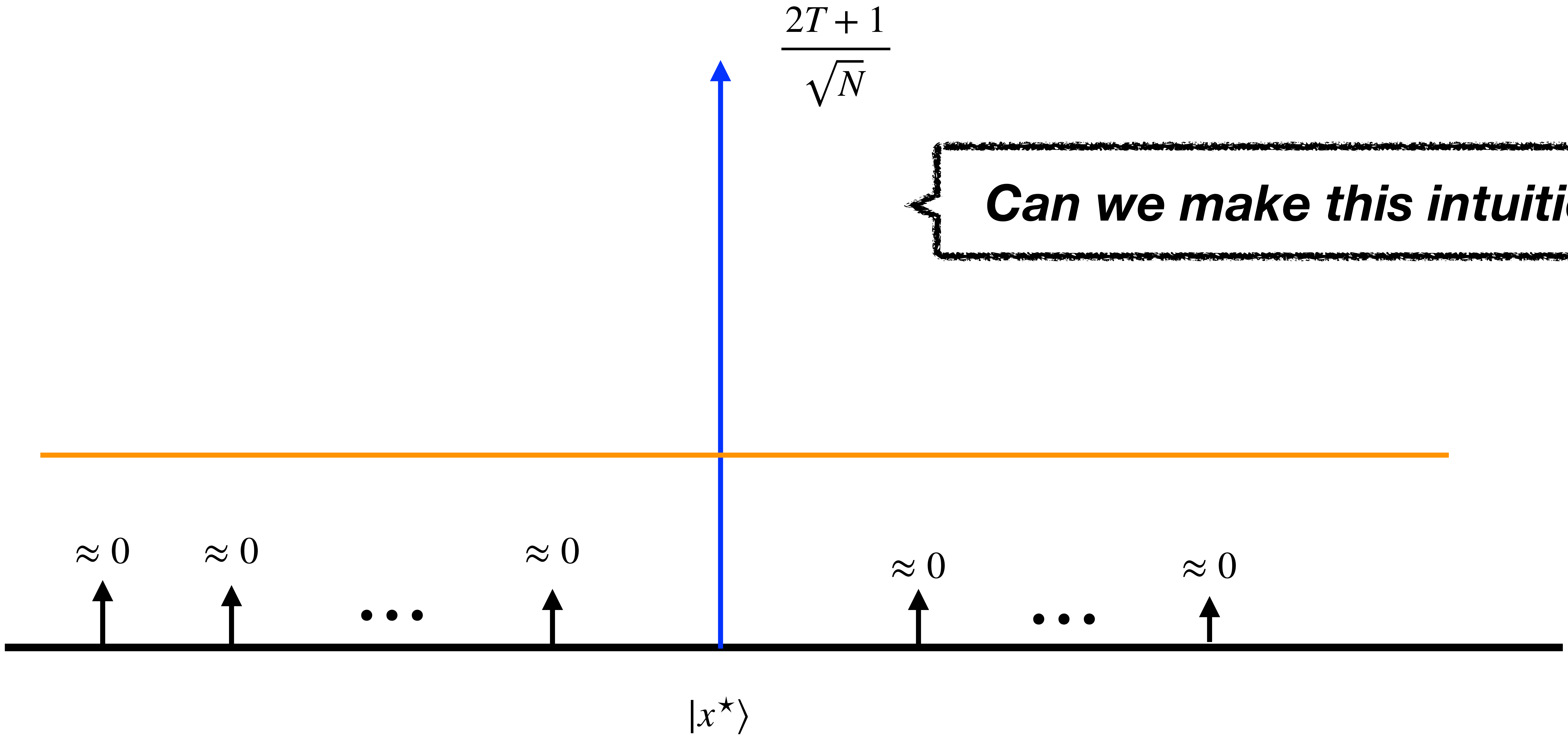


After T queries

$$(R_{|u\rangle} O_f)^T |u\rangle$$

Extrapolating, we would guess…

Suggests $T = O(\sqrt{N})$ suffice, beating brute-force search!



Can we make this intuition rigorous?

After T queries

$$(R_{|u\rangle} O_f)^T |u\rangle$$

Some Definitions

$A = \{x \in \{0,1\}^n \mid f(x) = 1\}$ **Accepting Inputs**

$B = \{x \in \{0,1\}^n \mid f(x) = 0\}$ **Bad Inputs**

Some Definitions

$$A = \{x \in \{0,1\}^n \mid f(x) = 1\}$$ **Accepting Inputs**

$$B = \{x \in \{0,1\}^n \mid f(x) = 0\}$$ **Bad Inputs**

$$|A\rangle = \frac{1}{\sqrt{A}} \sum_{x \in A} |x\rangle \qquad |B\rangle = \frac{1}{\sqrt{B}} \sum_{x \in B} |x\rangle$$

Understanding O_f

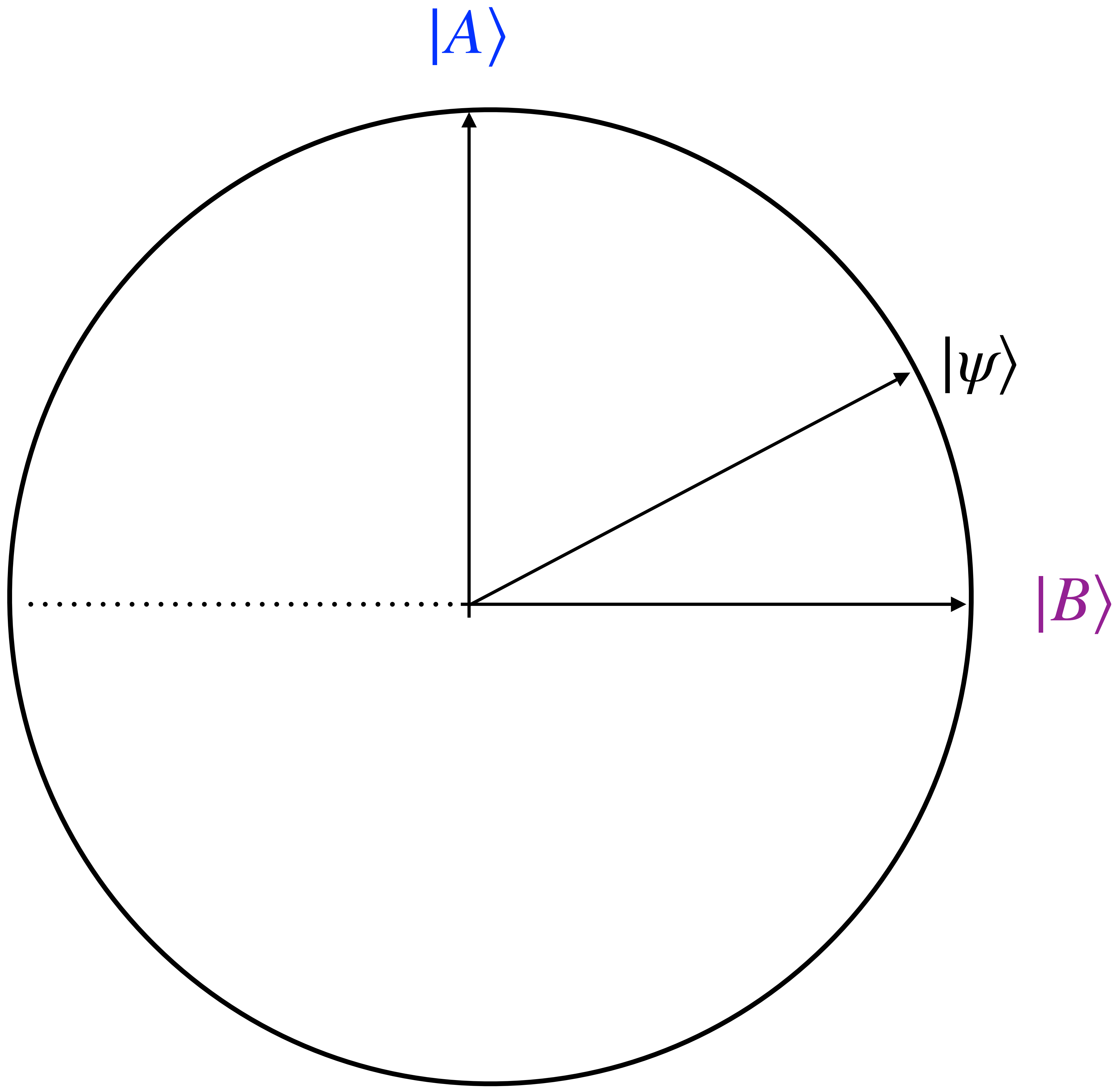
$$A = \{x \in \{0,1\}^n \mid f(x) = 1\}$$ **Accepting Inputs**

$$B = \{x \in \{0,1\}^n \mid f(x) = 0\}$$ **Bad Inputs**

$$|A\rangle = \frac{1}{\sqrt{A}} \sum_{x \in A} |x\rangle \qquad |B\rangle = \frac{1}{\sqrt{B}} \sum_{x \in B} |x\rangle$$

$$O_f|A\rangle = -|A\rangle \qquad O_f|B\rangle = |B\rangle$$

Understanding O_f

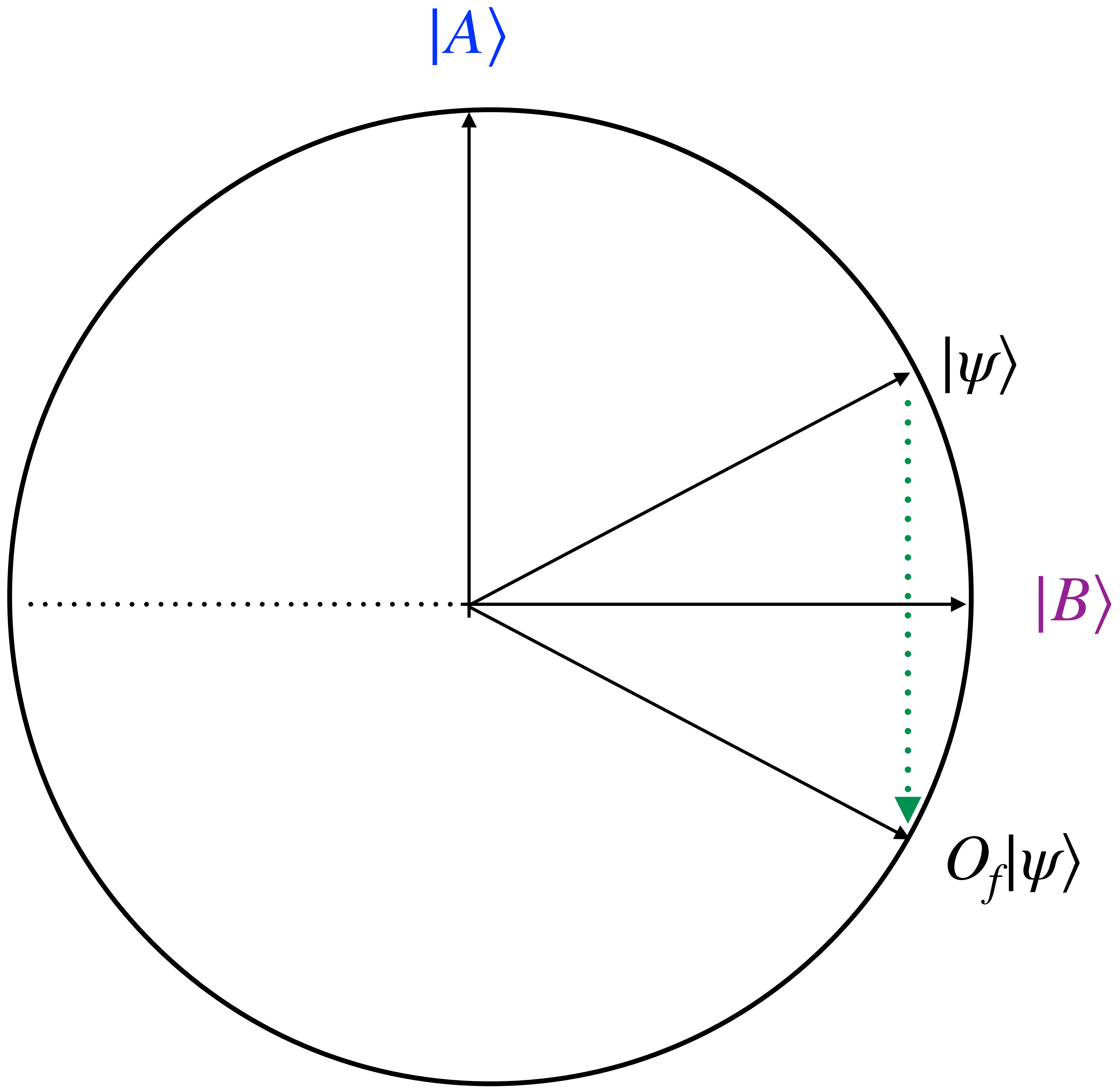


$$\langle A \mid B \rangle = 0$$

$$O_f|A\rangle = -|A\rangle$$

$$O_f|B\rangle = |B\rangle$$

Understanding O_f



$\langle A \mid B \rangle = 0$

$O_f|A\rangle = -|A\rangle$

$O_f|B\rangle = |B\rangle$

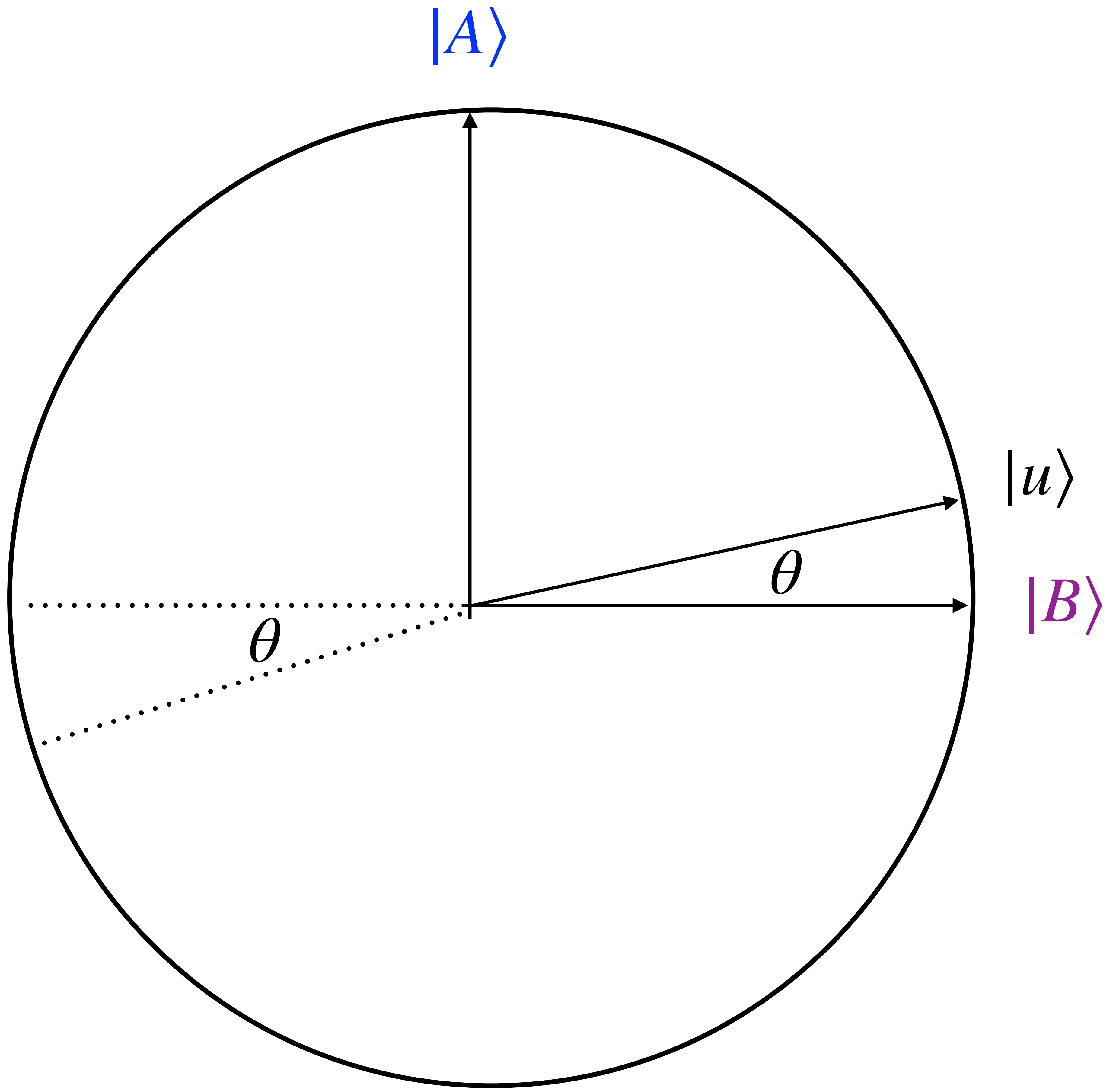
O_f **is a reflection around** $|B\rangle$

Composing two Reflections

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

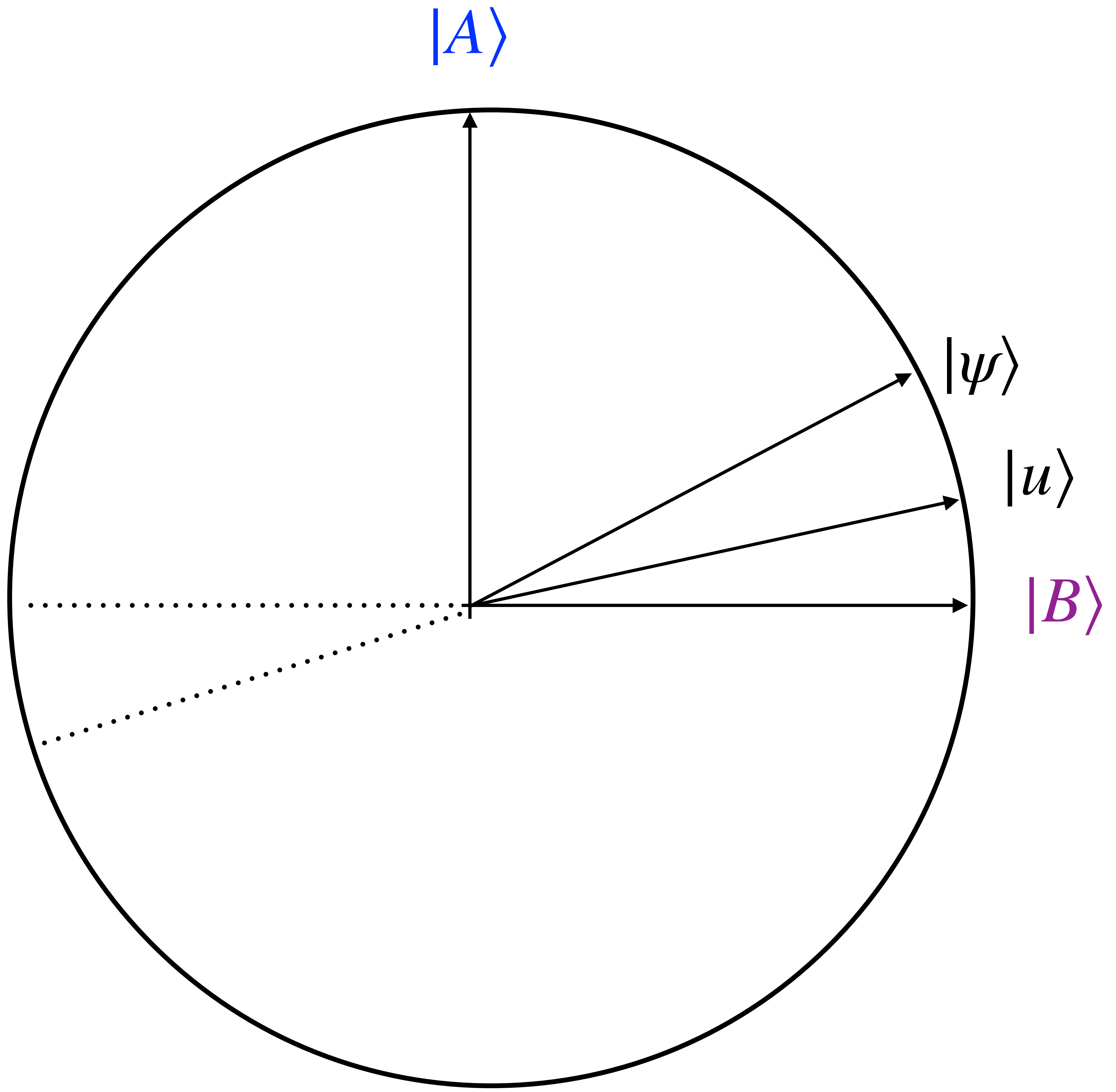


Composing two Reflections

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

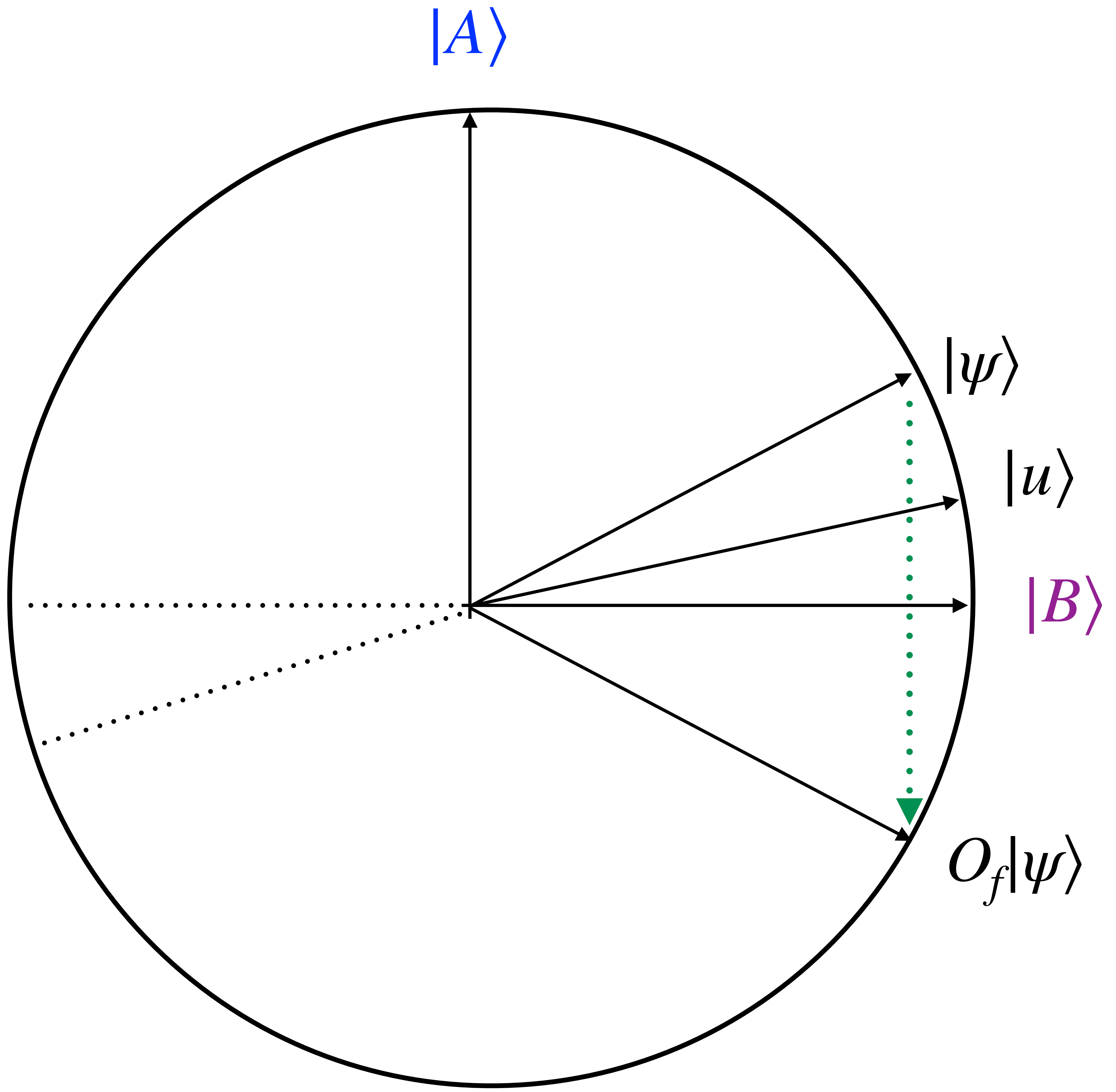


Composing two Reflections

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

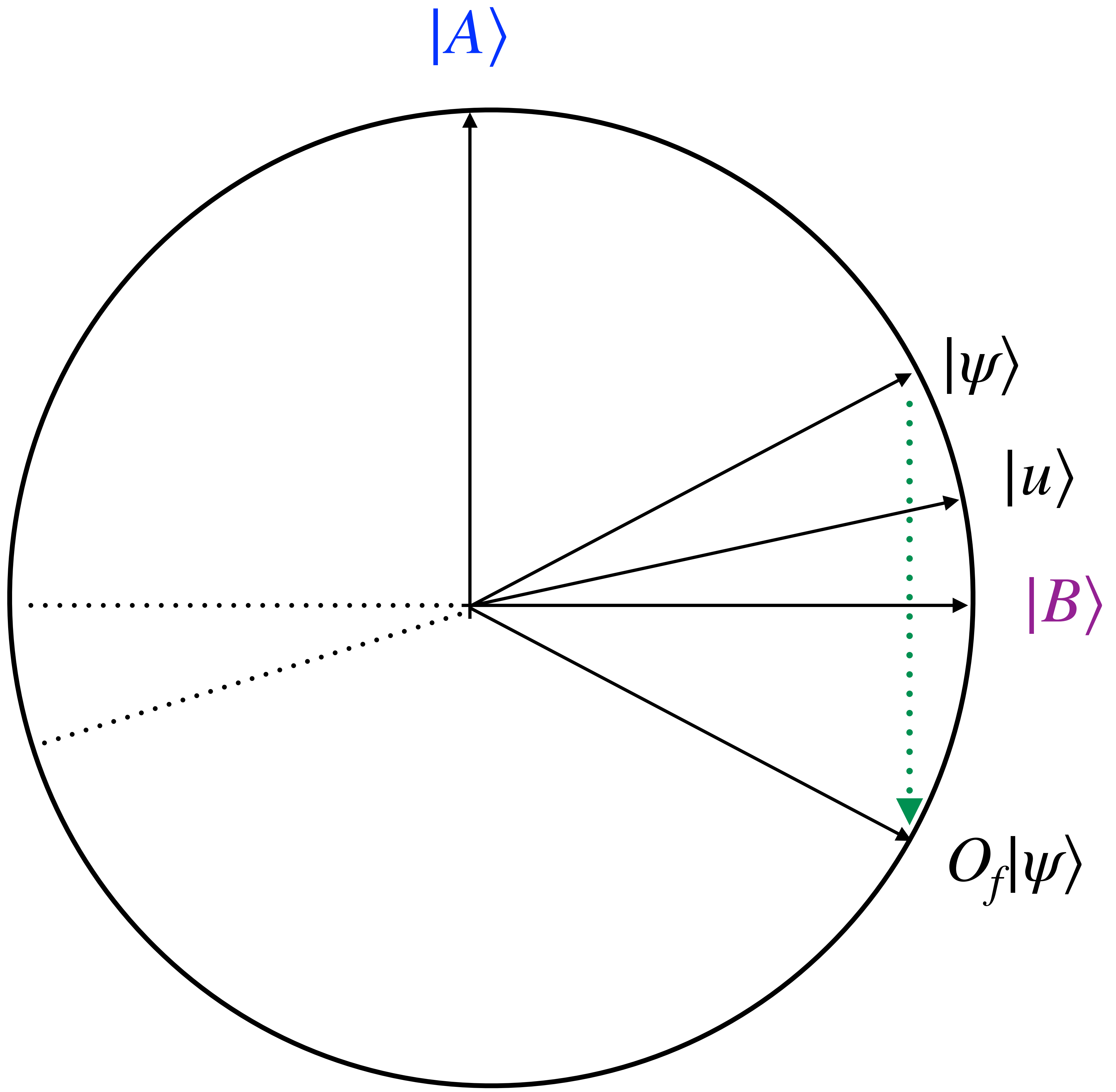


Composing two Reflections

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$



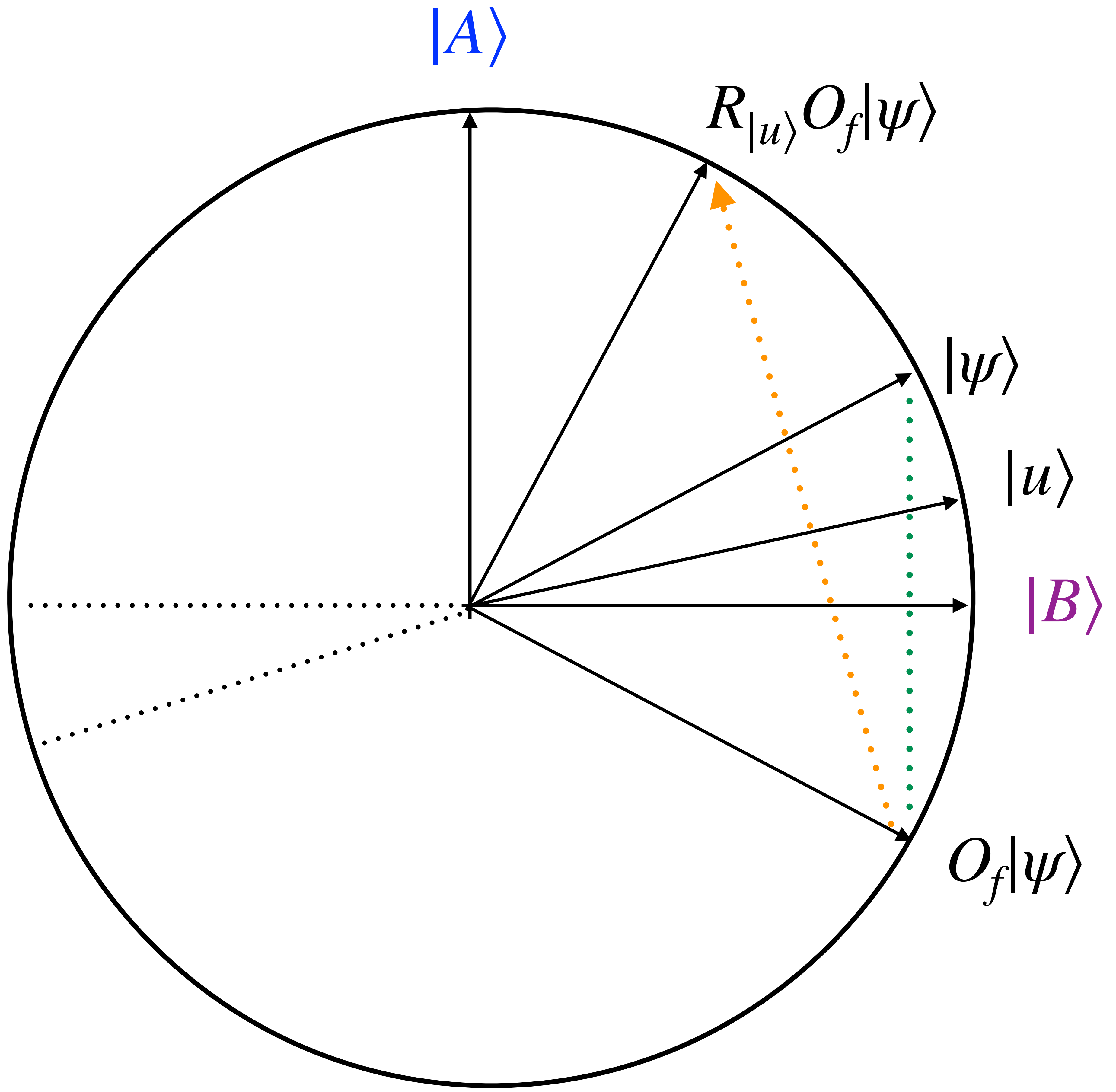
$R_{|u\rangle}$ **is a reflection around** $|u\rangle$

Composing two Reflections

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$



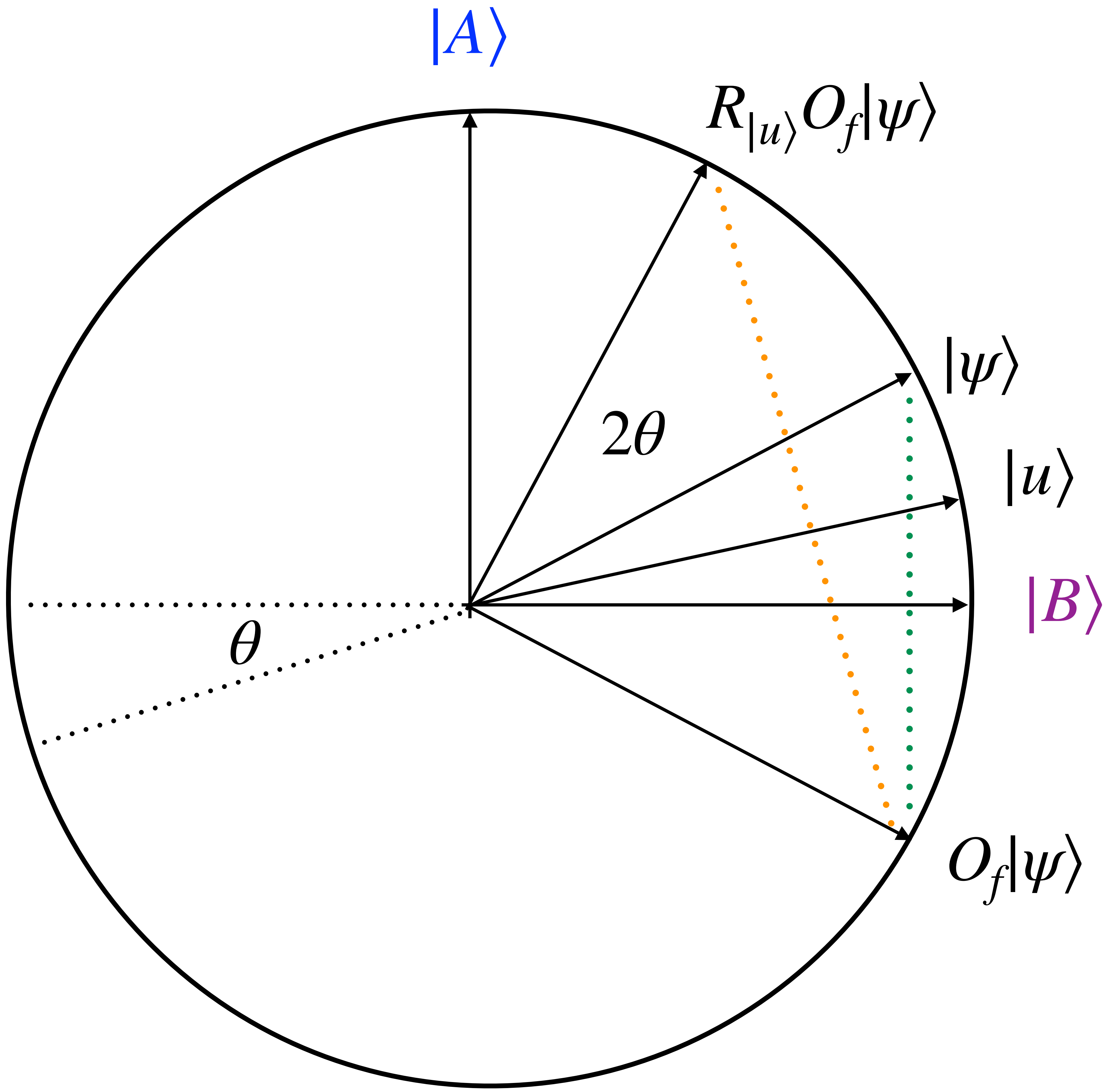
$R_{|u\rangle}$ **is a reflection around** $|u\rangle$

Composing two Reflections gives a Rotation

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

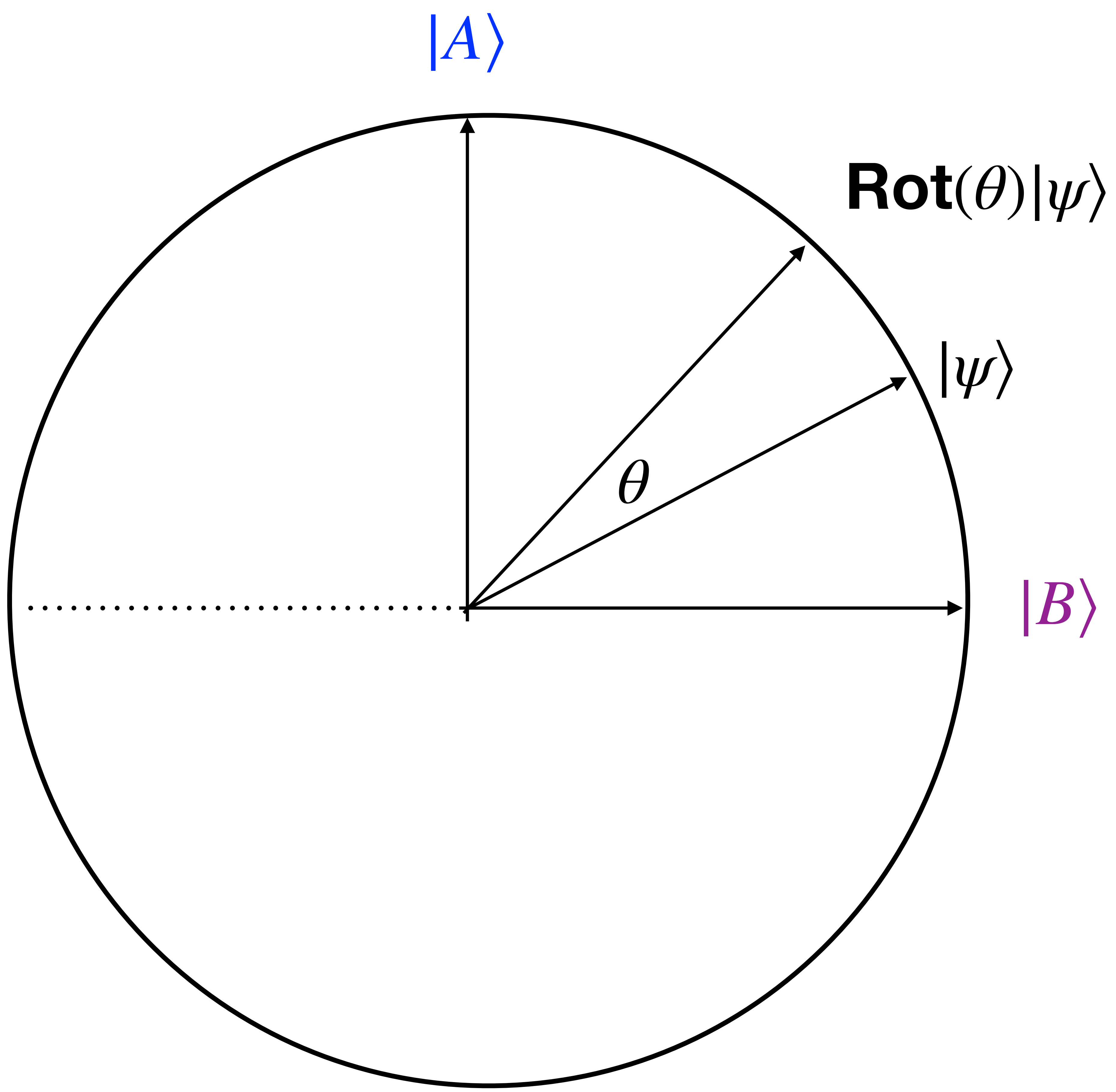
$$R_{|B\rangle} = O_f$$



Fact: $R_{|u\rangle}R_{|B\rangle} =$ **Rot**(2θ)

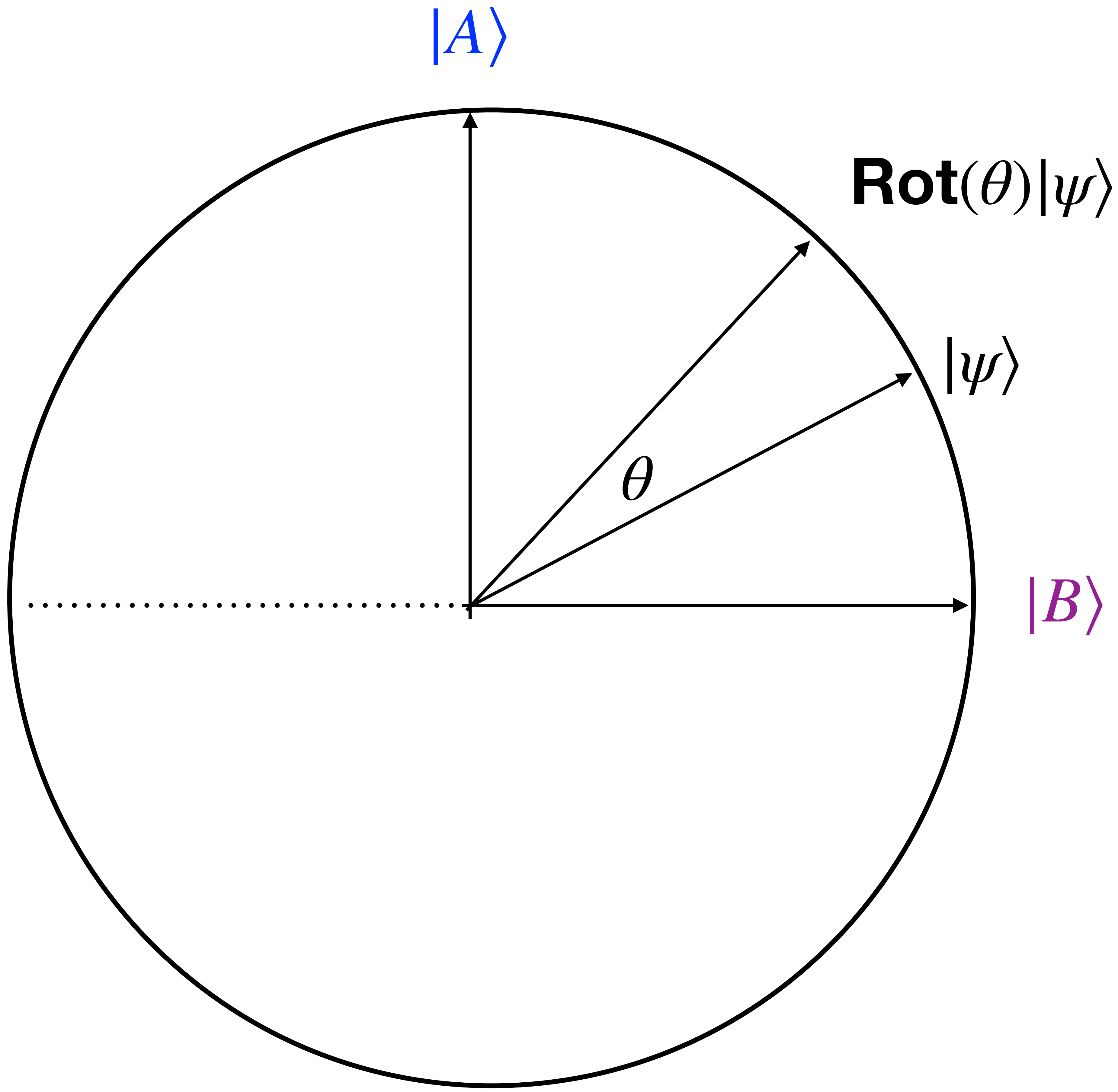
θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

Refresher on Rotation Matrices



$$\mathbf{Rot}(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Refresher on Rotation Matrices



$$\textbf{Rot}(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

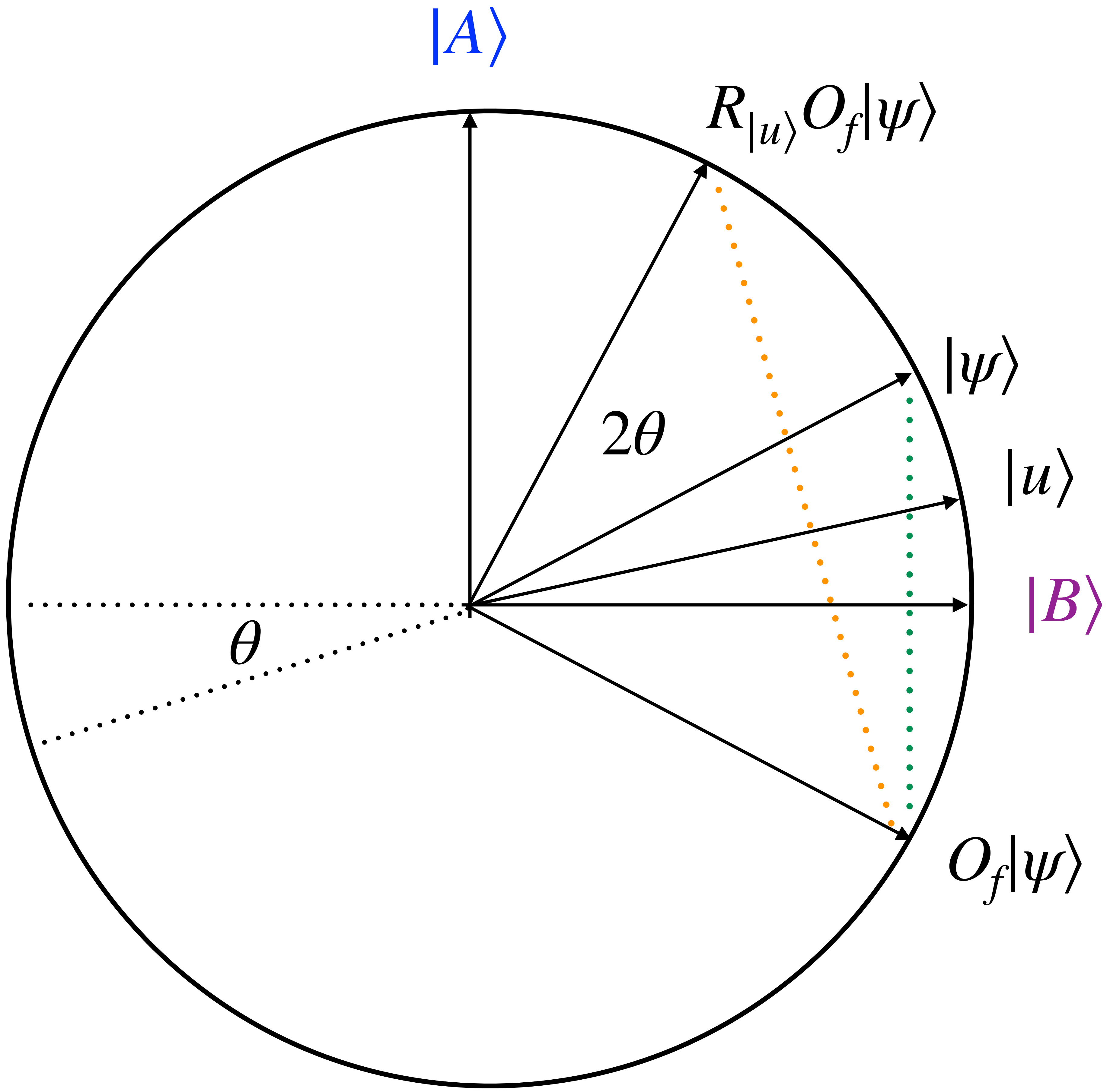
$$\textbf{Rot}(\theta)^k = \begin{pmatrix} \cos(k\theta) & -\sin(k\theta) \\ \sin(k\theta) & \cos(k\theta) \end{pmatrix} = \textbf{Rot}(k\theta)$$

Composing two Reflections gives a Rotation

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$



Fact: $R_{|u\rangle}R_{|B\rangle} =$ **Rot**(2θ)

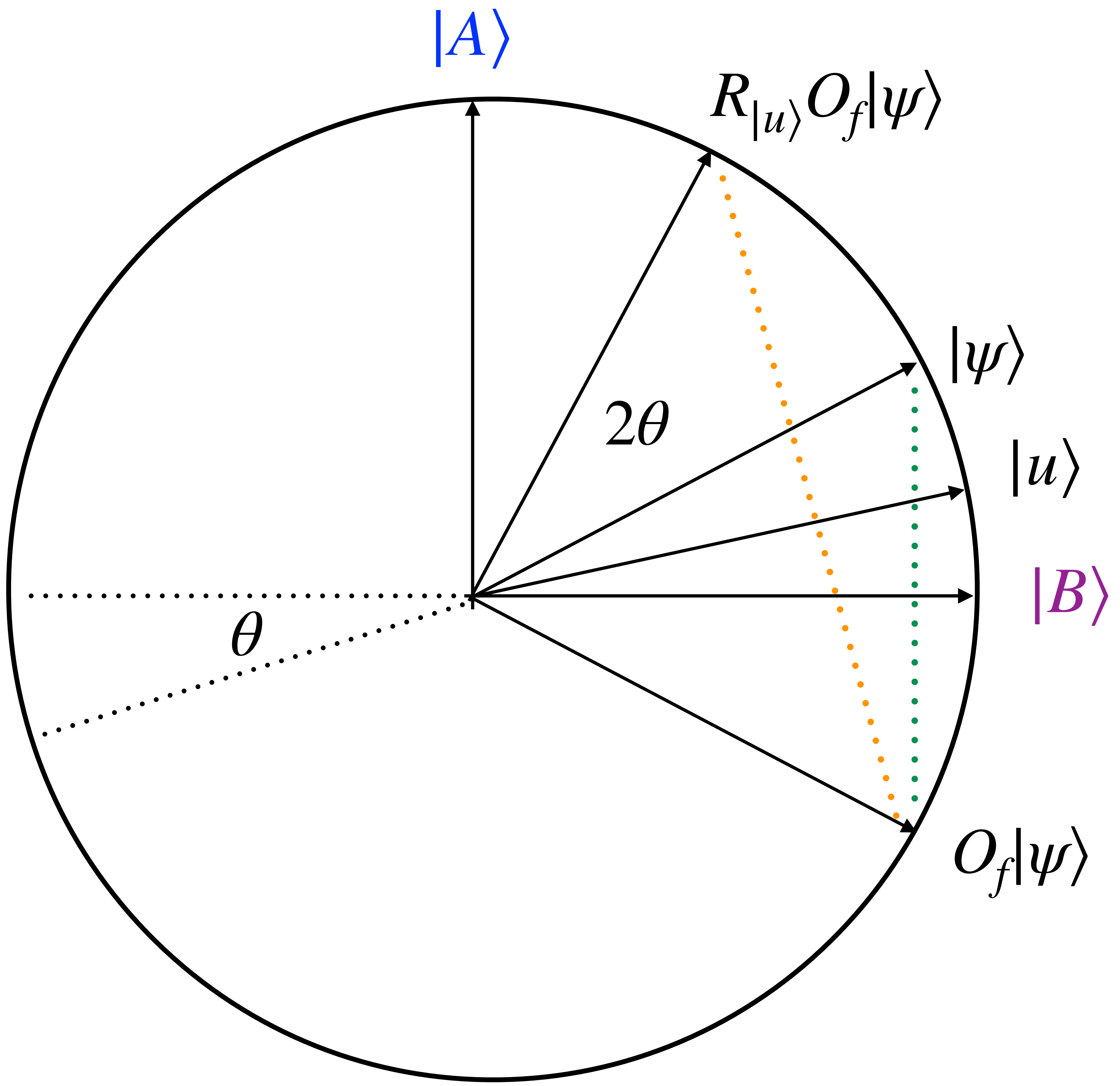
θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

Analyzing the Number of Queries

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

$$\theta = \sin^{-1}\left(\sqrt{\frac{A}{N}}\right)$$



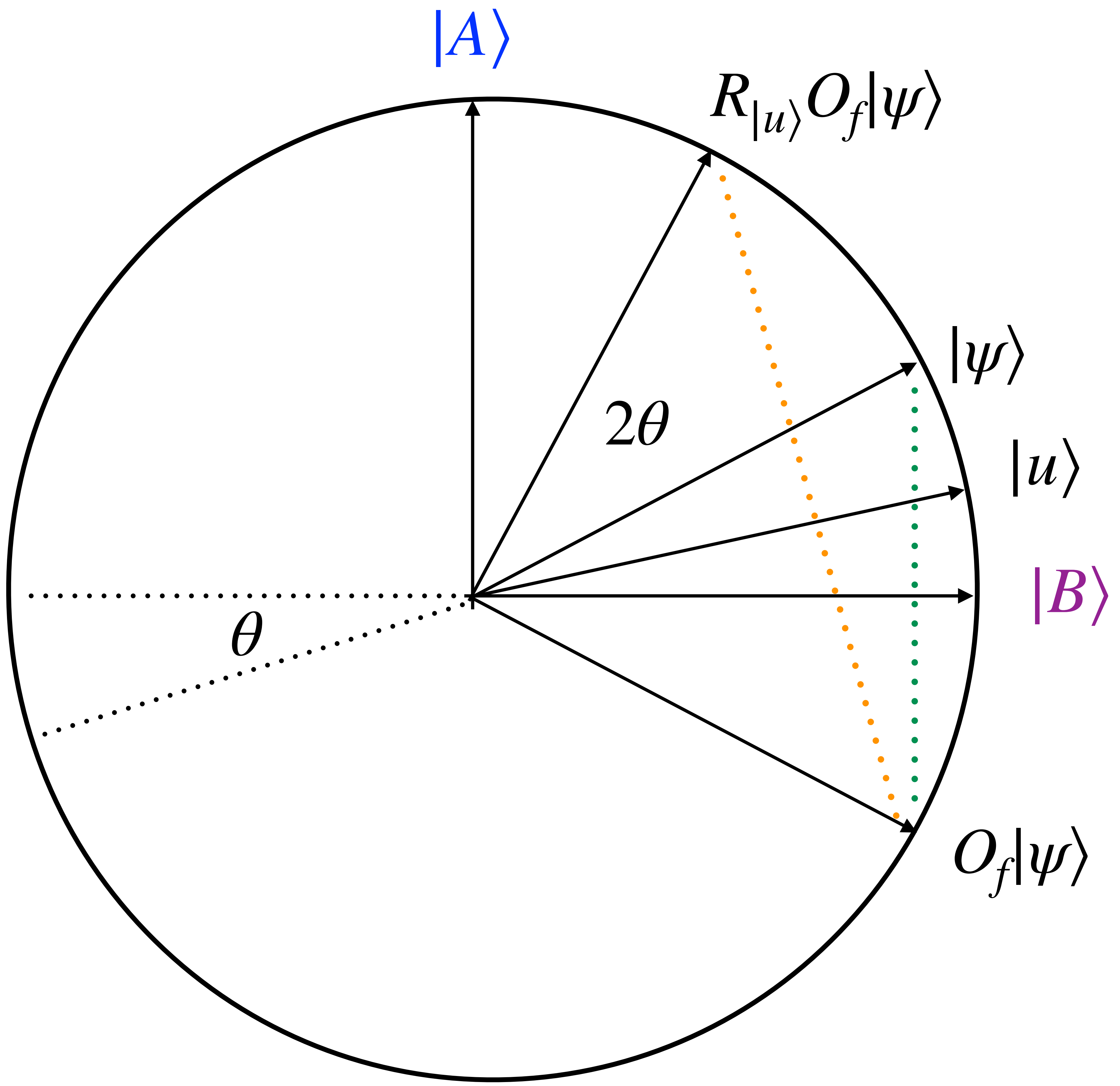
$$(R_{|u\rangle}R_{|B\rangle})^T|u\rangle = \textbf{Rot}(2T\theta)|u\rangle = \sin((2T+1)\theta)|A\rangle + \cos((2T+1)\theta)|B\rangle$$

Analyzing the Number of Queries

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

$$\theta = \sin^{-1}\left(\sqrt{\frac{A}{N}}\right)$$



$$(R_{|u\rangle}R_{|B\rangle})^T|u\rangle = \textbf{Rot}(2T\theta)|u\rangle = \sin((2T+1)\theta)|A\rangle + \cos((2T+1)\theta)|B\rangle$$

Want: $(R_{|u\rangle}R_{|B\rangle})^T|u\rangle \approx |A\rangle \implies (2T+1)\theta \approx \frac{\pi}{2}$

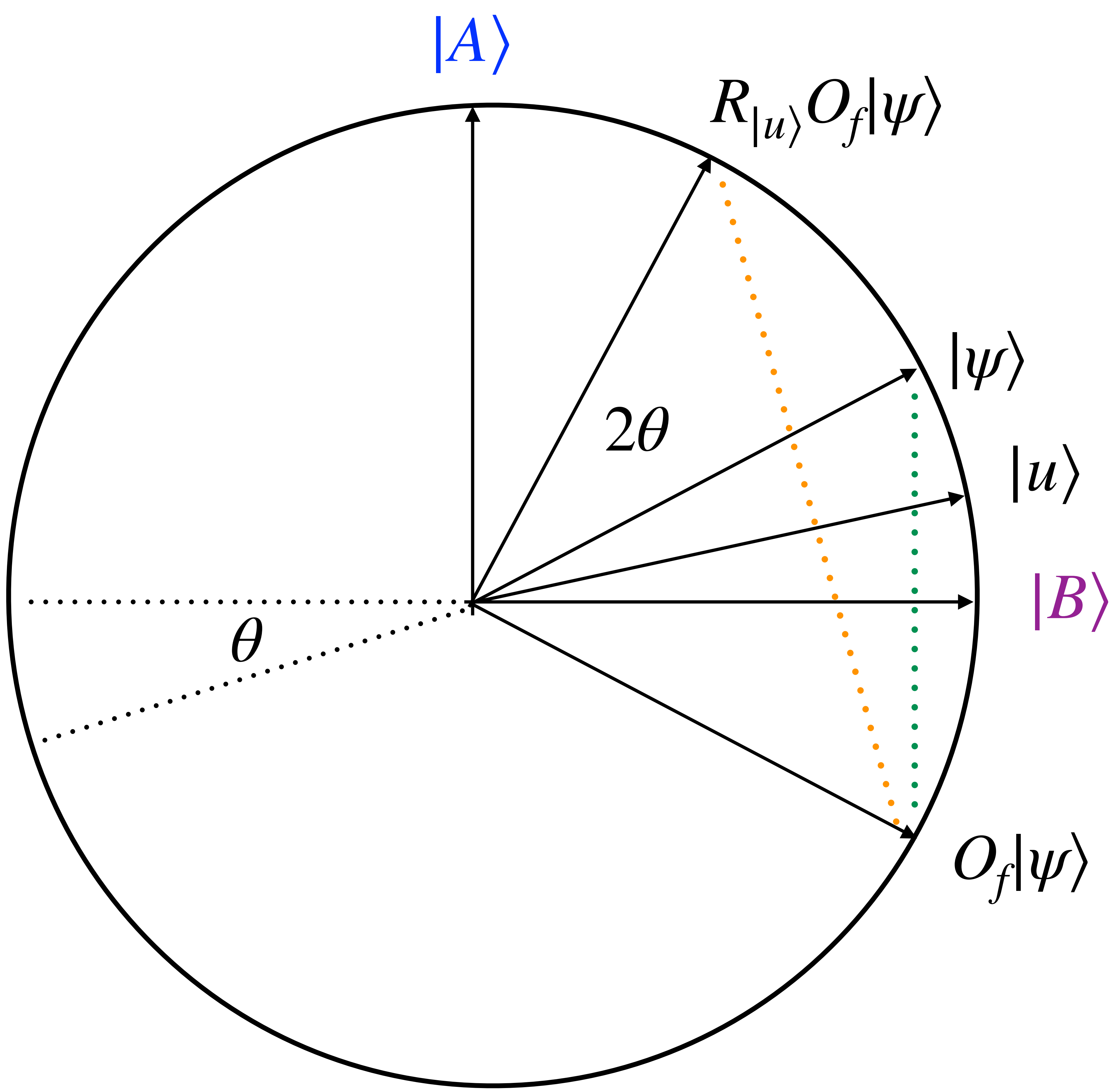
Analyzing the Number of Queries

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \mathbf{Rot}(2\theta)$

$$\theta = \sin^{-1}\left(\sqrt{\frac{A}{N}}\right)$$

$$\theta \geq \sqrt{\frac{A}{N}}$$ **(Taylor series)**



$$(R_{|u\rangle}R_{|B\rangle})^T|u\rangle = \mathbf{Rot}(2T\theta)|u\rangle = \sin((2T+1)\theta)|A\rangle + \cos((2T+1)\theta)|B\rangle$$

Want: $(R_{|u\rangle}R_{|B\rangle})^T|u\rangle \approx |A\rangle \implies (2T+1)\theta \approx \dfrac{\pi}{2}$

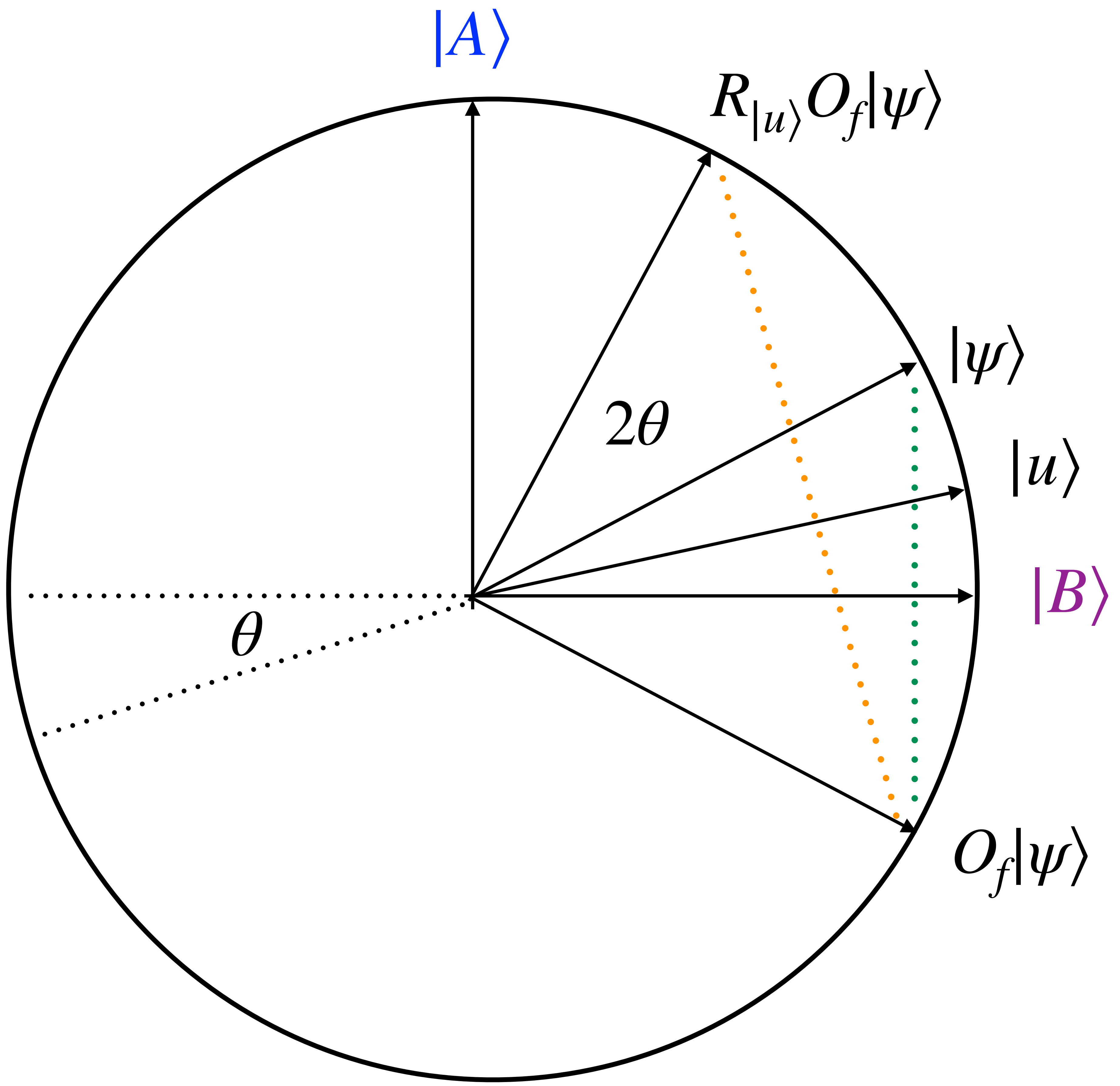
Analyzing the Number of Queries

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

$$\theta = \sin^{-1}\left(\sqrt{\frac{A}{N}}\right)$$

$\theta \geq \sqrt{\frac{A}{N}}$ **(Taylor series)**



$$(R_{|u\rangle}R_{|B\rangle})^T|u\rangle = \textbf{Rot}(2T\theta)|u\rangle = \sin((2T+1)\theta)|A\rangle + \cos((2T+1)\theta)|B\rangle$$

Want: $(R_{|u\rangle}R_{|B\rangle})^T|u\rangle \approx |A\rangle \implies (2T+1)\theta \approx \frac{\pi}{2}$

Number of Queries: $T \approx \frac{\pi}{4}\sqrt{\frac{N}{A}}$

In Summary: Grover's Algorithm gives a quadratic speedup

<u>**Grover'96**</u>

Unstructured Search can be solved with $O(\sqrt{N})$ quantum queries

In Summary: Grover's Algorithm gives a quadratic speedup

Grover'96

Unstructured Search can be solved with $O(\sqrt{N})$ ***quantum queries***

One of the most important quantum algorithms discovered so far

In Summary: Grover's Algorithm gives a quadratic speedup

<u>Grover'96</u>

Unstructured Search can be solved with $O(\sqrt{N})$ quantum queries

One of the most important quantum algorithms discovered so far

Widely used to obtain many other polynomial quantum speedups

In Summary: Grover's Algorithm gives a quadratic speedup

Grover'96

Unstructured Search can be solved with $O(\sqrt{N})$ quantum queries

One of the most important quantum algorithms discovered so far

Widely used to obtain many other polynomial quantum speedups

Provably optimum in the black-box query model

Simple Technicalities to Handle

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$$

Number of Queries: $T \approx \frac{\pi}{4}\sqrt{\frac{N}{A}}$

We (implicitly) assumed that $|A| \neq 0$ (the case $|A| = 0$ is easy to analyze, do you see this?)

Simple Technicalities to Handle

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$$

Number of Queries: $T \approx \frac{\pi}{4}\sqrt{\frac{N}{A}}$

We (implicitly) assumed that $|A| \neq 0$ (the case $|A| = 0$ is easy to analyze, do you see this?)

Can we implement the reflection $R_{|u\rangle}$ efficiently?

Simple Technicalities to Handle

$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle = \sin(\theta)|A\rangle + \cos(\theta)|B\rangle$

Number of Queries: $T \approx \frac{\pi}{4}\sqrt{\frac{N}{A}}$

We (implicitly) assumed that $|A| \neq 0$ (the case $|A| = 0$ is easy to analyze, do you see this?)

Can we implement the reflection $R_{|u\rangle}$ efficiently?

We do not know $|A|$ in advance, can think of strategies to deal with this?

Number of Queries in Grover's Algorithm

Can we do better (fewer queries) when $|A|$ is large?

Number of Queries in Grover's Algorithm

Can we do better (fewer queries) when $|A|$ is large?

<u>Grover's Search</u>

Unstructured Search can be solved with $O\left(\sqrt{\frac{N}{A}}\right)$ ***quantum queries if*** $|A| \neq 0$

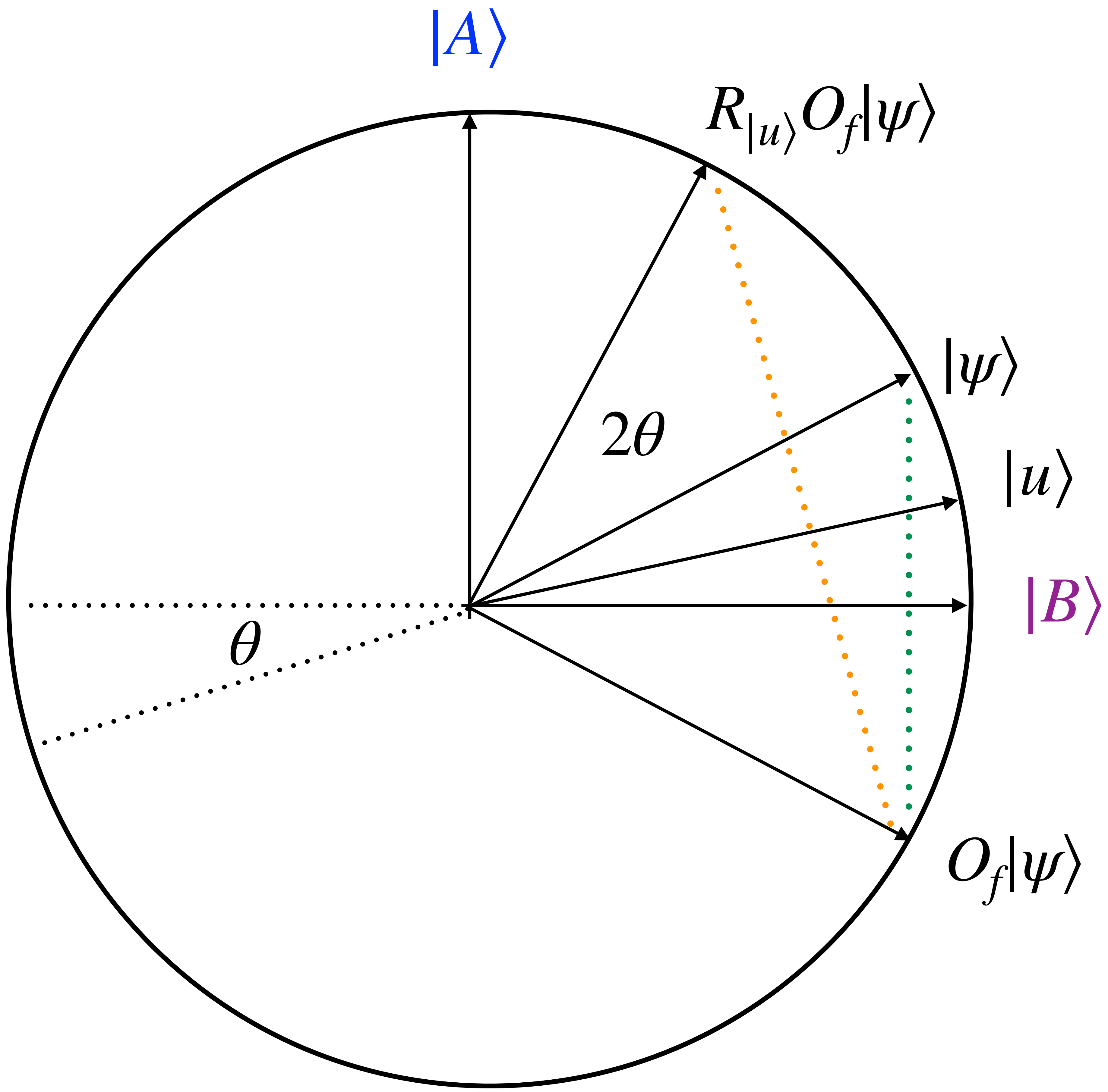
Completing the Proofs…

Proving the Composition Fact

$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$

$R_{|u\rangle} = 2|u\rangle\langle u| - I$

$R_{|B\rangle} = O_f$



Fact: $R_{|u\rangle}R_{|B\rangle} = \mathbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

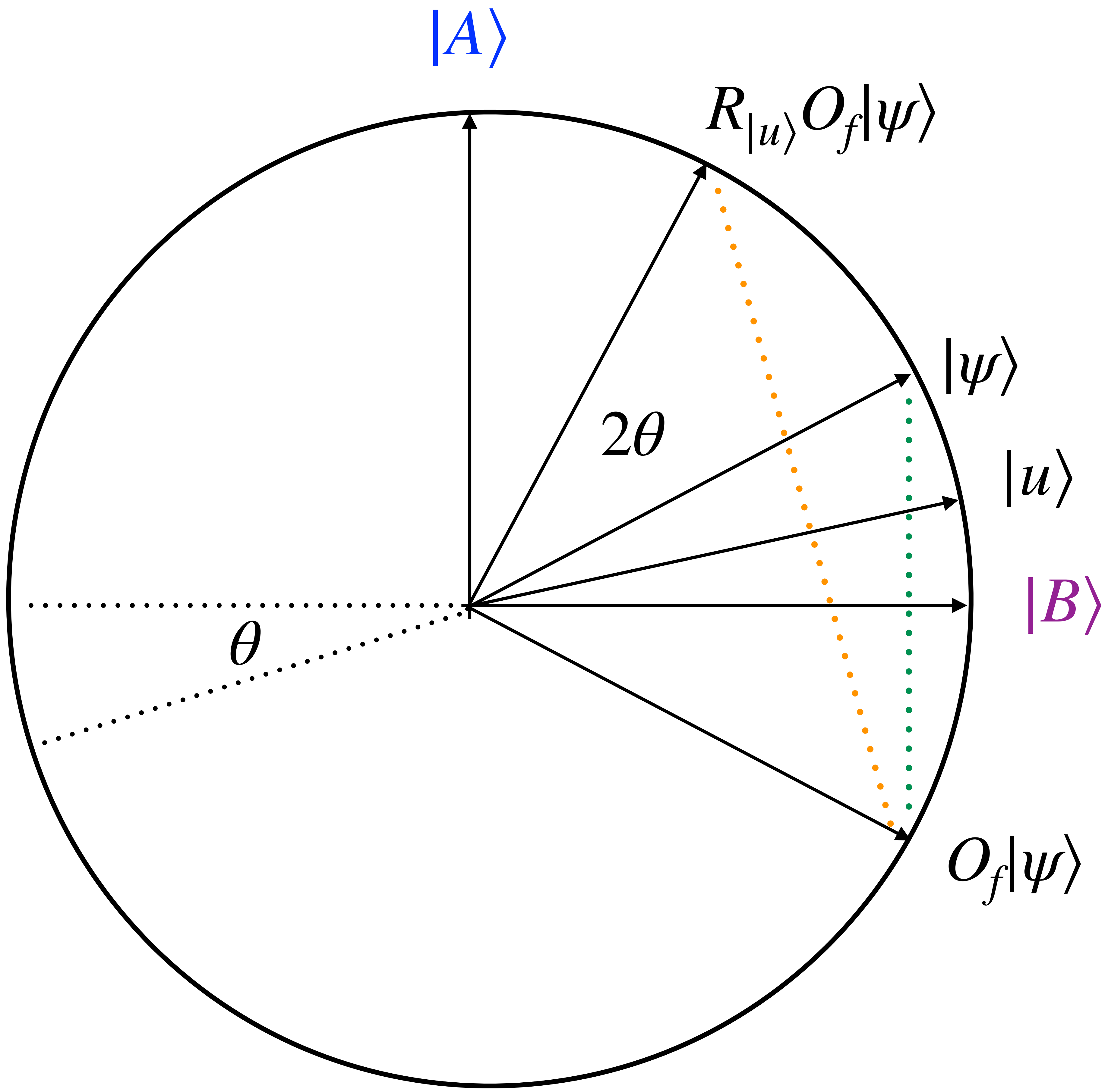
$$R_{|u\rangle}R_{|B\rangle}|A\rangle = -R_{|u\rangle}|A\rangle = -(2|u\rangle\langle u| - I)|A\rangle$$

Proving the Composition Fact

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$



Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = -R_{|u\rangle}|A\rangle = -(2|u\rangle\langle u| - I)|A\rangle$$

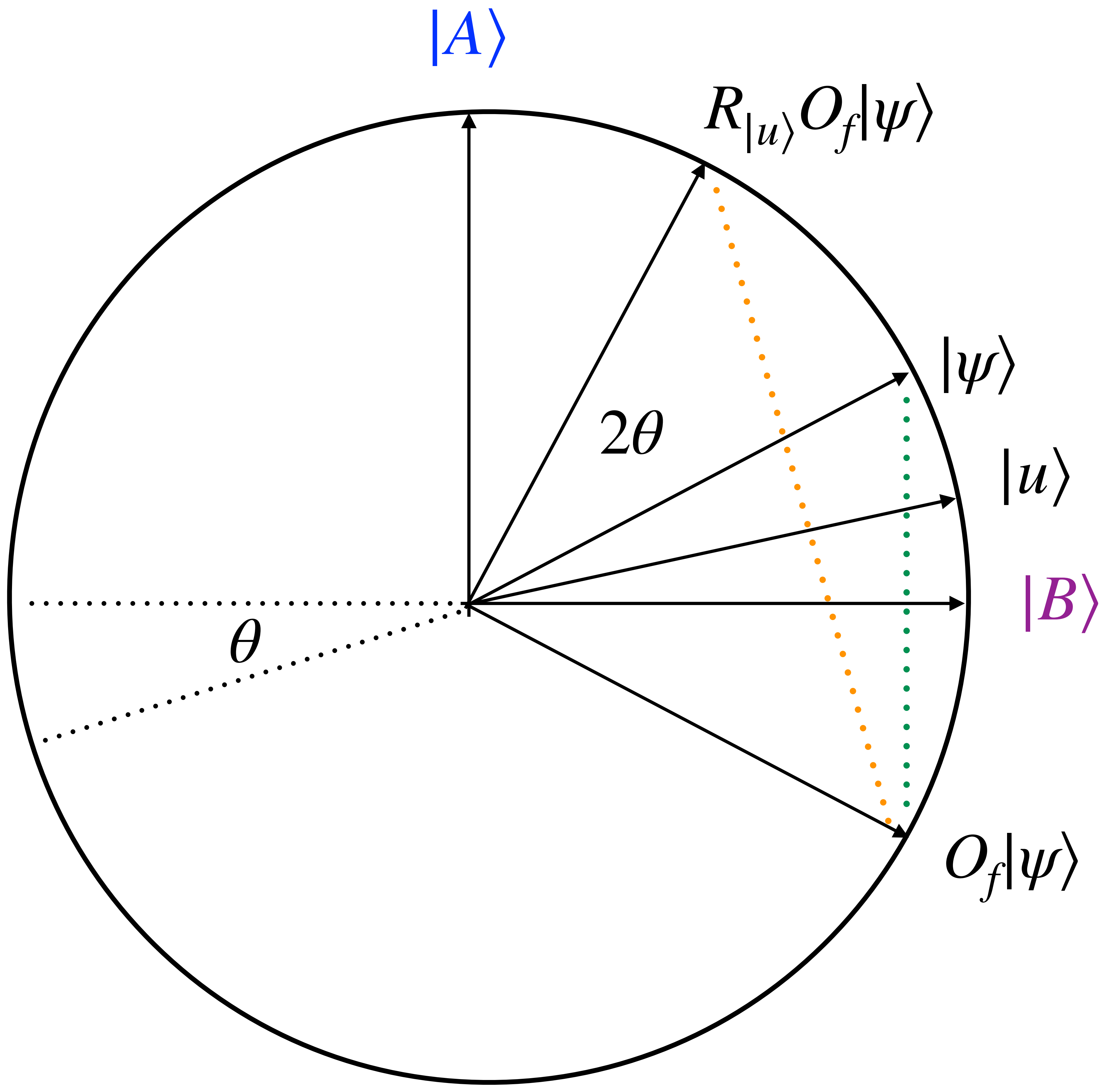
$$= -2\sqrt{\frac{A}{N}}|u\rangle + |A\rangle$$

Proving the Composition Fact

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$



Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = -R_{|u\rangle}|A\rangle = -(2|u\rangle\langle u| - I)|A\rangle$$

$$= -2\sqrt{\frac{A}{N}}|u\rangle + |A\rangle$$

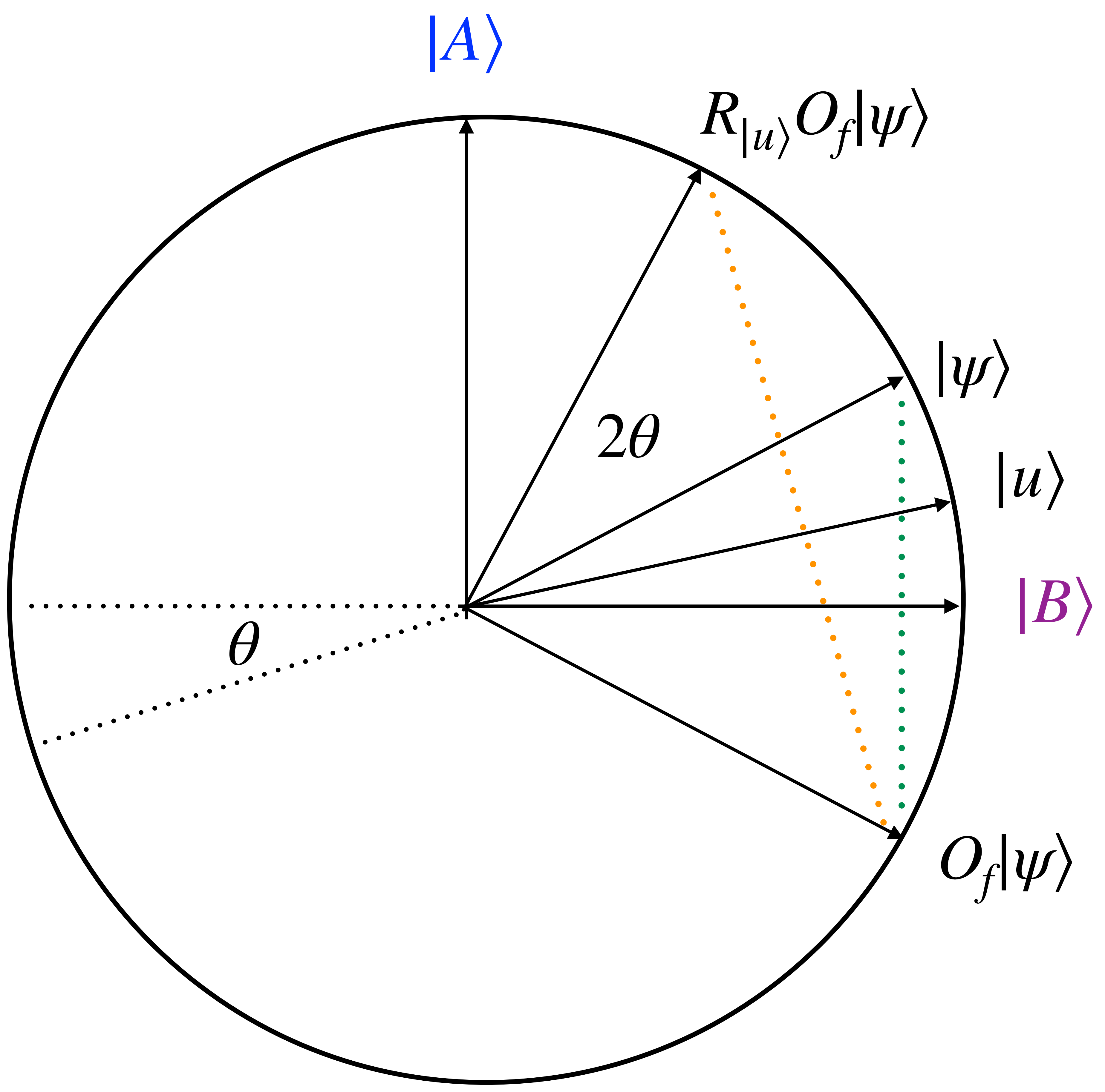
$$= \frac{N-2A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle$$

Proving the Composition Fact

$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$

$R_{|u\rangle} = 2|u\rangle\langle u| - I$

$R_{|B\rangle} = O_f$



Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

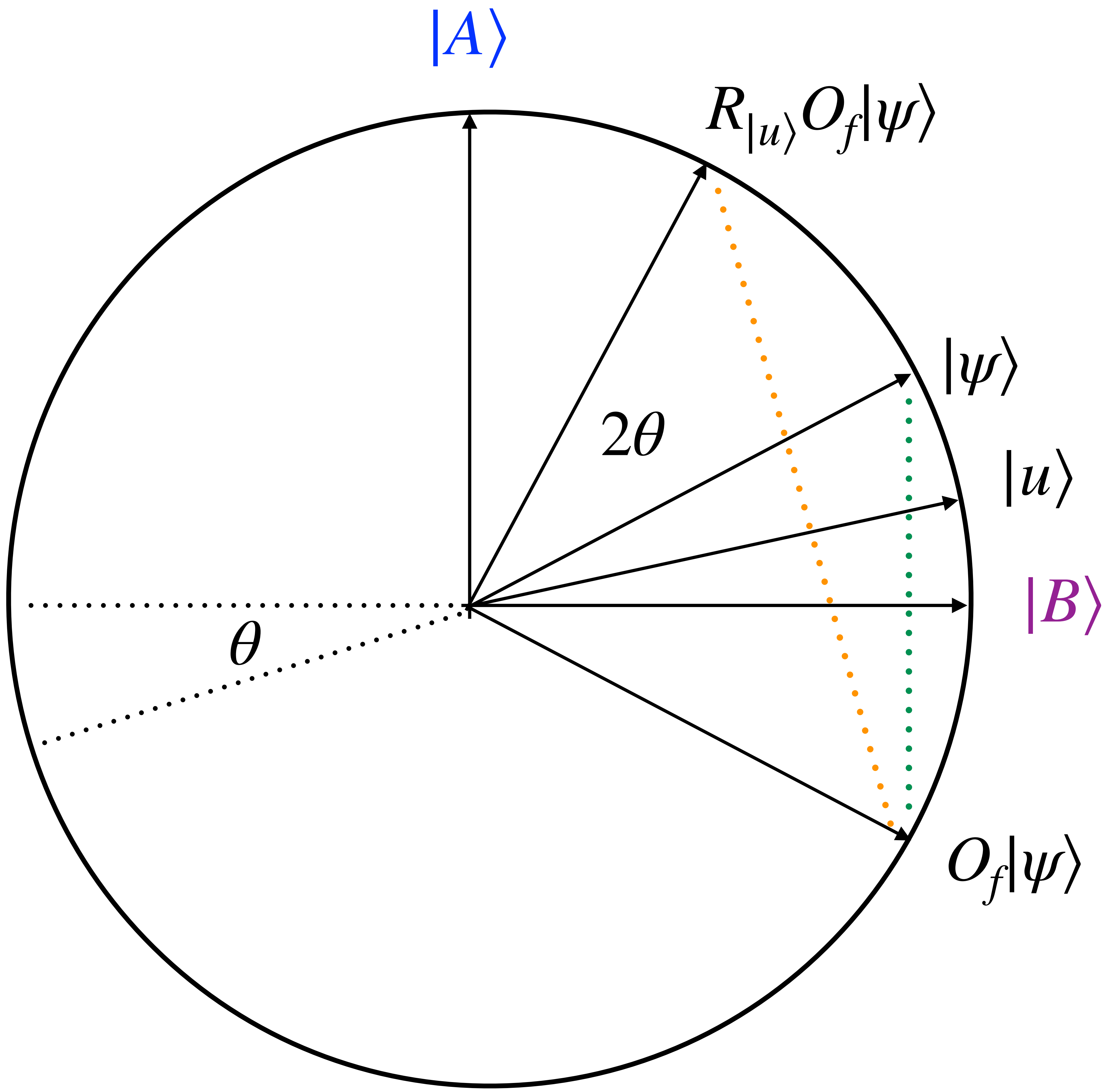
$$
\begin{aligned}
R_{|u\rangle}R_{|B\rangle}|A\rangle = -R_{|u\rangle}|A\rangle &= -(2|u\rangle\langle u| - I)|A\rangle \\
&= -2\sqrt{\frac{A}{N}}|u\rangle + |A\rangle \\
&= \frac{N-2A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle \\
&= \frac{B-A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle
\end{aligned}
$$

Proving the Composition Fact

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$



Fact: $R_{|u\rangle}R_{|B\rangle} = \mathbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

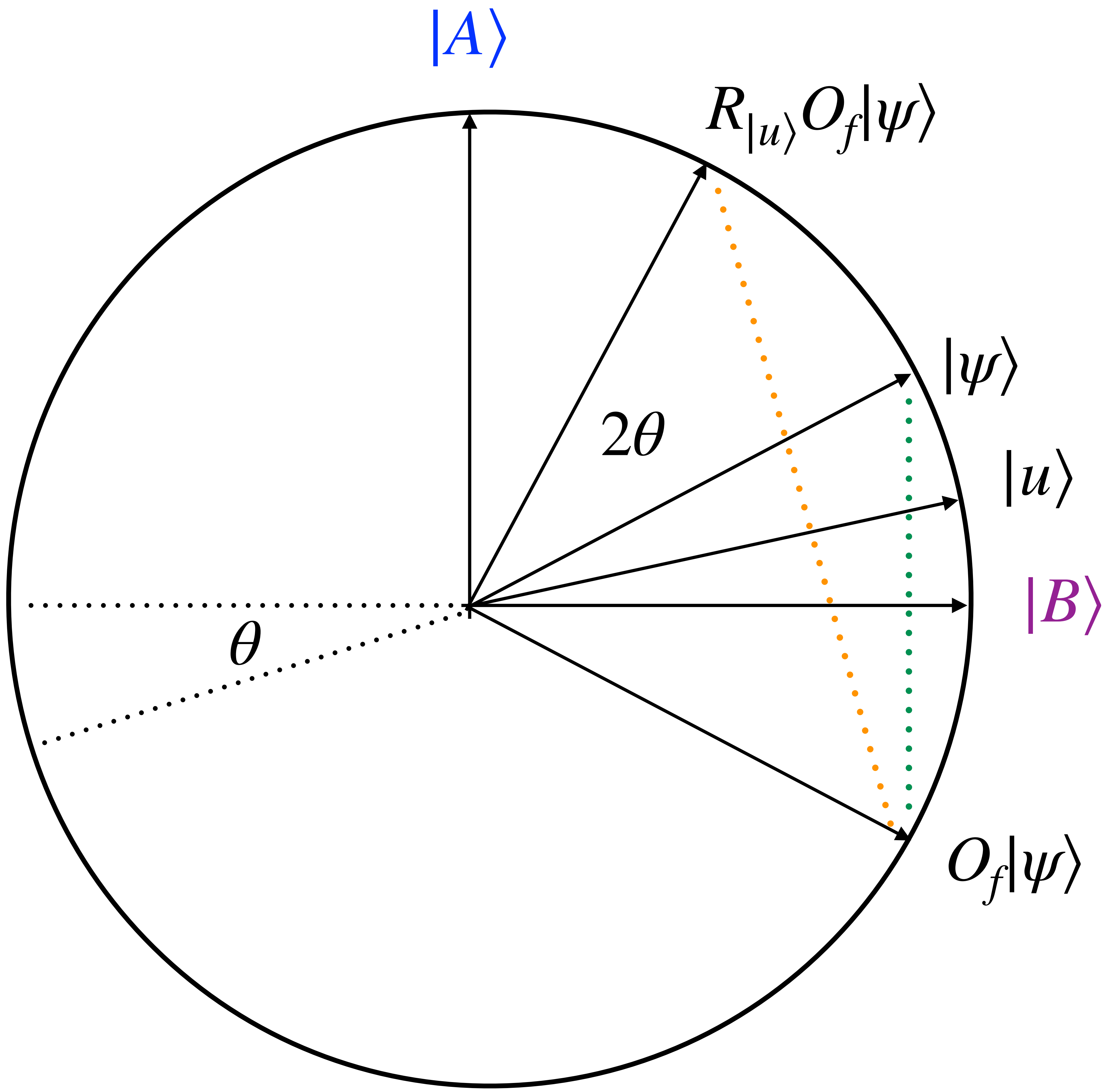
$$R_{|u\rangle}R_{|B\rangle}|B\rangle = R_{|u\rangle}|B\rangle = (2|u\rangle\langle u| - I)|B\rangle$$

Proving the Composition Fact

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$



Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

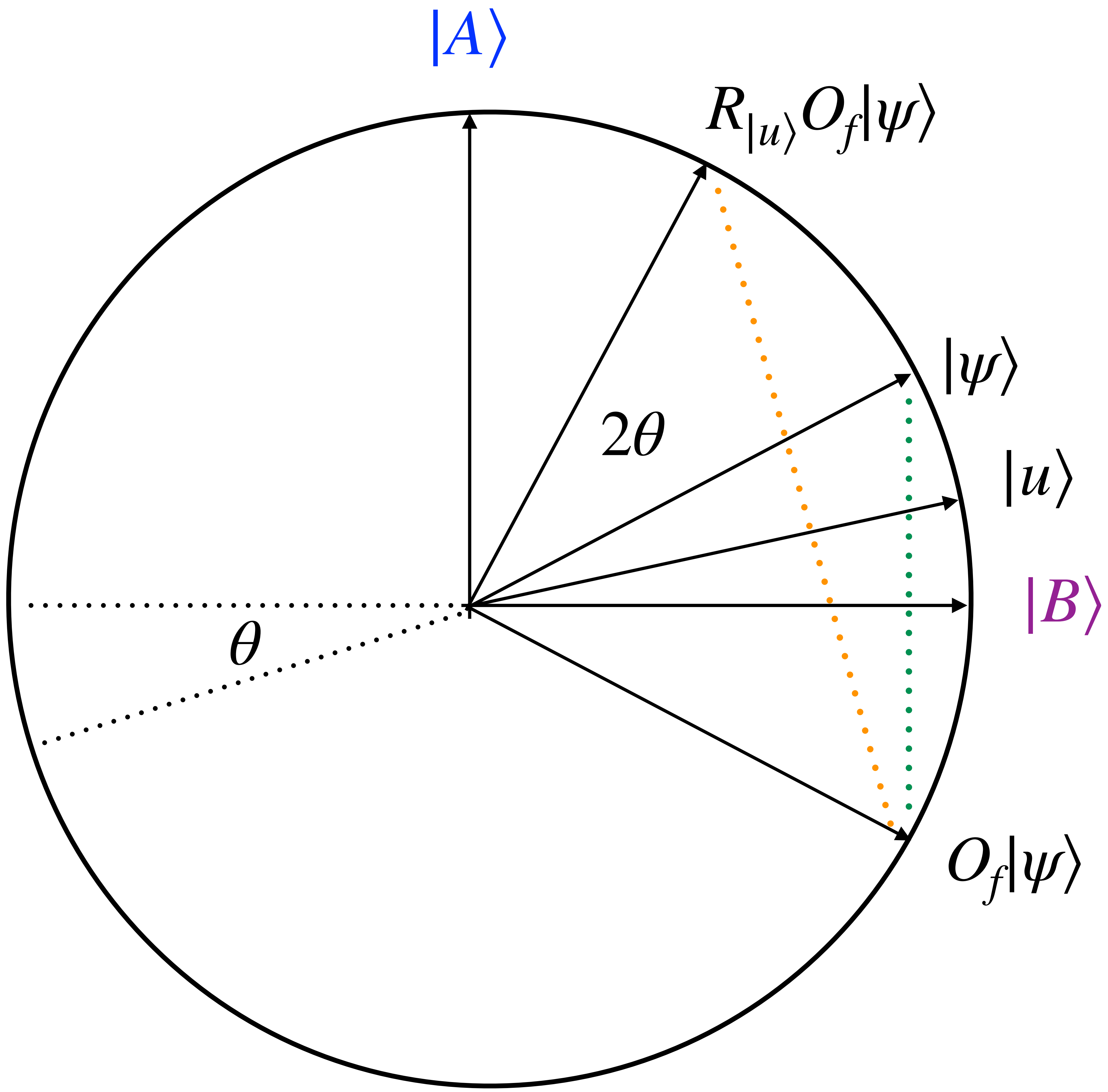
$$R_{|u\rangle}R_{|B\rangle}|B\rangle = R_{|u\rangle}|B\rangle = (2|u\rangle\langle u| - I)|B\rangle$$
$$= 2\sqrt{\frac{B}{N}}|u\rangle - |B\rangle$$

Proving the Composition Fact

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$



Fact: $R_{|u\rangle}R_{|B\rangle} = \mathbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

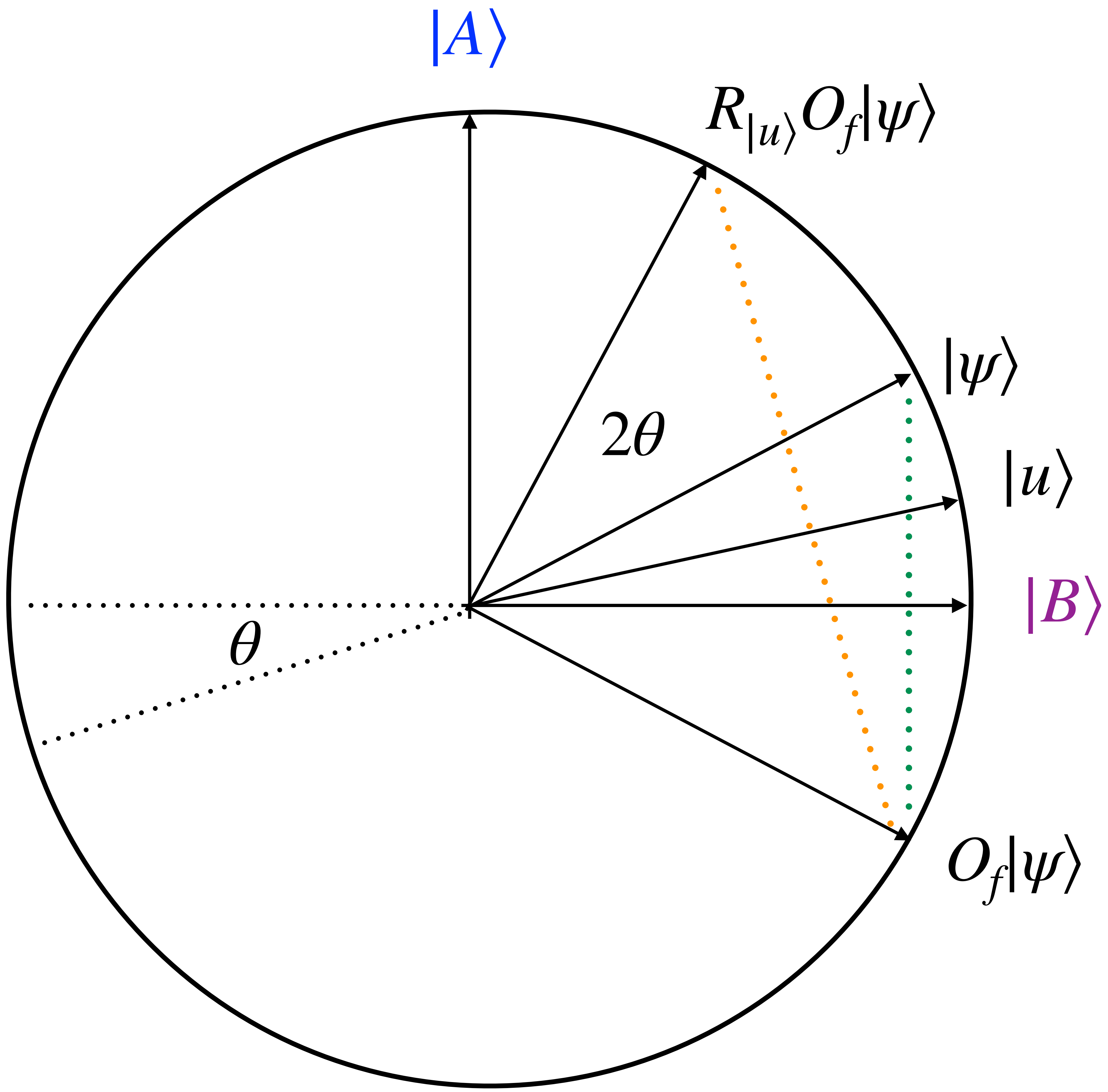
$$\begin{aligned} R_{|u\rangle}R_{|B\rangle}|B\rangle = R_{|u\rangle}|B\rangle &= (2|u\rangle\langle u| - I)|B\rangle \\ &= 2\sqrt{\frac{B}{N}}|u\rangle - |B\rangle \\ &= \frac{2\sqrt{AB}}{N}|A\rangle + \frac{2B-N}{N}|B\rangle \end{aligned}$$

Proving the Composition Fact

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$



Fact: $R_{|u\rangle}R_{|B\rangle} =$ **Rot**(2θ)

θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

$$\begin{aligned} R_{|u\rangle}R_{|B\rangle}|B\rangle = R_{|u\rangle}|B\rangle &= (2|u\rangle\langle u| - I)|B\rangle \\ &= 2\sqrt{\frac{B}{N}}|u\rangle - |B\rangle \\ &= \frac{2\sqrt{AB}}{N}|A\rangle + \frac{2B-N}{N}|B\rangle \\ &= \frac{2\sqrt{AB}}{N}|A\rangle + \frac{B-A}{N}|B\rangle \end{aligned}$$

Proving the Composition Fact

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|B\rangle = \frac{2\sqrt{AB}}{N}|A\rangle + \frac{B-A}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = \frac{B-A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle$$

Proving the Composition Fact

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

Fact: $R_{|u\rangle}R_{|B\rangle} =$ **Rot**(2θ)

θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|B\rangle = \frac{2\sqrt{AB}}{N}|A\rangle + \frac{B-A}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = \frac{B-A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle} =$$

Proving the Composition Fact

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|B\rangle = \frac{2\sqrt{AB}}{N}|A\rangle + \frac{B-A}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = \frac{B-A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle} = \begin{array}{cc} & \begin{array}{cc} |B\rangle & \quad |A\rangle \end{array} \\ \begin{array}{c} |B\rangle \\ |A\rangle \end{array} & \begin{pmatrix} \frac{B-A}{N} & -2\frac{\sqrt{AB}}{N} \\ 2\frac{\sqrt{AB}}{N} & \frac{B-A}{N} \end{pmatrix} \end{array}$$

Proving the Composition Fact

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|B\rangle = \frac{2\sqrt{AB}}{N}|A\rangle + \frac{B-A}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = \frac{B-A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle} = \begin{array}{cc} & \begin{array}{cc} |B\rangle & |A\rangle \end{array} \\ \begin{array}{c} |B\rangle \\ |A\rangle \end{array} & \begin{pmatrix} \frac{B-A}{N} & -2\frac{\sqrt{AB}}{N} \\ 2\frac{\sqrt{AB}}{N} & \frac{B-A}{N} \end{pmatrix} \end{array} = \begin{pmatrix} \sqrt{\frac{B}{N}} & -\sqrt{\frac{A}{N}} \\ \sqrt{\frac{A}{N}} & \sqrt{\frac{B}{N}} \end{pmatrix}^2$$

Proving the Composition Fact

$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$

$R_{|u\rangle} = 2|u\rangle\langle u| - I$

$R_{|B\rangle} = O_f$

Fact: $R_{|u\rangle}R_{|B\rangle} =$ **Rot**(2θ)

θ **is the angle between** $|u\rangle$ **and** $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|B\rangle = \frac{2\sqrt{AB}}{N}|A\rangle + \frac{B-A}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = \frac{B-A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle} = \begin{array}{cc} & \begin{array}{cc} |B\rangle & |A\rangle \end{array} \\ \begin{array}{c} |B\rangle \\ |A\rangle \end{array} & \begin{pmatrix} \frac{B-A}{N} & -2\frac{\sqrt{AB}}{N} \\ 2\frac{\sqrt{AB}}{N} & \frac{B-A}{N} \end{pmatrix} \end{array} = \begin{pmatrix} \sqrt{\frac{B}{N}} & -\sqrt{\frac{A}{N}} \\ \sqrt{\frac{A}{N}} & \sqrt{\frac{B}{N}} \end{pmatrix}^2 = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}^2 = \textbf{Rot}(2\theta)$$

where $\theta = \sin^{-1}\left(\sqrt{\frac{A}{N}}\right)$

Proving the Composition Fact

$$|u\rangle = \sqrt{\frac{A}{N}}|A\rangle + \sqrt{\frac{B}{N}}|B\rangle$$

$$R_{|u\rangle} = 2|u\rangle\langle u| - I$$

$$R_{|B\rangle} = O_f$$

Fact: $R_{|u\rangle}R_{|B\rangle} = \textbf{Rot}(2\theta)$

θ is the angle between $|u\rangle$ and $|B\rangle$

$$R_{|u\rangle}R_{|B\rangle}|B\rangle = \frac{2\sqrt{AB}}{N}|A\rangle + \frac{B-A}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle}|A\rangle = \frac{B-A}{N}|A\rangle - \frac{2\sqrt{AB}}{N}|B\rangle$$

$$R_{|u\rangle}R_{|B\rangle} = \begin{array}{cc} & \begin{array}{cc} |B\rangle & |A\rangle \end{array} \\ \begin{array}{c} |B\rangle \\ |A\rangle \end{array} & \begin{pmatrix} \frac{B-A}{N} & -2\frac{\sqrt{AB}}{N} \\ 2\frac{\sqrt{AB}}{N} & \frac{B-A}{N} \end{pmatrix} \end{array} = \begin{pmatrix} \sqrt{\frac{B}{N}} & -\sqrt{\frac{A}{N}} \\ \sqrt{\frac{A}{N}} & \sqrt{\frac{B}{N}} \end{pmatrix}^2 = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}^2 = \textbf{Rot}(2\theta)$$

where $\theta = \sin^{-1}\left(\sqrt{\frac{A}{N}}\right)$ $\blacksquare$

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ **Hadamard Gate**

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ **Hadamard Gate**

$$O_{\mathbf{OR}}|x\rangle = (-1)^{\mathbf{OR}(x)}|x\rangle, \forall x \in \{0,1\}^n$$

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ **Hadamard Gate**

$$O_{\textbf{OR}}|x\rangle = (-1)^{\textbf{OR}(x)}|x\rangle, \forall x \in \{0,1\}^n$$

Claim: $R_{|u\rangle} = H^{\otimes n} O_{\textbf{OR}} H^{\otimes n}$

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ **Hadamard Gate**

$$O_{\mathbf{OR}}|x\rangle = (-1)^{\mathbf{OR}(x)}|x\rangle, \forall x \in \{0,1\}^n$$

Claim: $R_{|u\rangle} = H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}$

$$H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}|u\rangle = H^{\otimes n} O_{\mathbf{OR}}|0\rangle = H^{\otimes n}|0\rangle = |u\rangle$$

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ **Hadamard Gate**

$$O_{\mathbf{OR}}|x\rangle = (-1)^{\mathbf{OR}(x)}|x\rangle, \forall x \in \{0,1\}^n$$

Claim: $R_{|u\rangle} = H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}$

$$H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}|u\rangle = H^{\otimes n} O_{\mathbf{OR}}|0\rangle = H^{\otimes n}|0\rangle = |u\rangle$$

$$H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}|u^{\perp}\rangle = H^{\otimes n} O_{\mathbf{OR}}|0^{\perp}\rangle = -H^{\otimes n}|0^{\perp}\rangle = -|u^{\perp}\rangle$$

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ **Hadamard Gate**

$$O_{\textbf{OR}}|x\rangle = (-1)^{\textbf{OR}(x)}|x\rangle, \forall x \in \{0,1\}^n$$

Claim: $R_{|u\rangle} = H^{\otimes n} O_{\textbf{OR}} H^{\otimes n}$

$$H^{\otimes n} O_{\textbf{OR}} H^{\otimes n}|u\rangle = H^{\otimes n} O_{\textbf{OR}}|0\rangle = H^{\otimes n}|0\rangle = |u\rangle$$

$$H^{\otimes n} O_{\textbf{OR}} H^{\otimes n}|u^{\perp}\rangle = H^{\otimes n} O_{\textbf{OR}}|0^{\perp}\rangle = -H^{\otimes n}|0^{\perp}\rangle = -|u^{\perp}\rangle$$

$\blacksquare$

Efficient Implementation of the Reflection $R_{|u\rangle}$

$$\boxed{R_{|u\rangle} = 2|u\rangle\langle u| - I}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$ **Hadamard Gate**

$$O_{\mathbf{OR}}|x\rangle = (-1)^{\mathbf{OR}(x)}|x\rangle, \forall x \in \{0,1\}^n$$

Claim: $R_{|u\rangle} = H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}$

$$H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}|u\rangle = H^{\otimes n} O_{\mathbf{OR}}|0\rangle = H^{\otimes n}|0\rangle = |u\rangle$$

$$H^{\otimes n} O_{\mathbf{OR}} H^{\otimes n}|u^{\perp}\rangle = H^{\otimes n} O_{\mathbf{OR}}|0^{\perp}\rangle = -H^{\otimes n}|0^{\perp}\rangle = -|u^{\perp}\rangle$$

$\blacksquare$

Can you implement other reflections?

Thank you!

Thank you!

More Questions?