Quantum Computing and Shor's Algorithm

Applying Quantum Mechanics to Computation

A Brief Introduction

- What is a **Quantum Computer**?

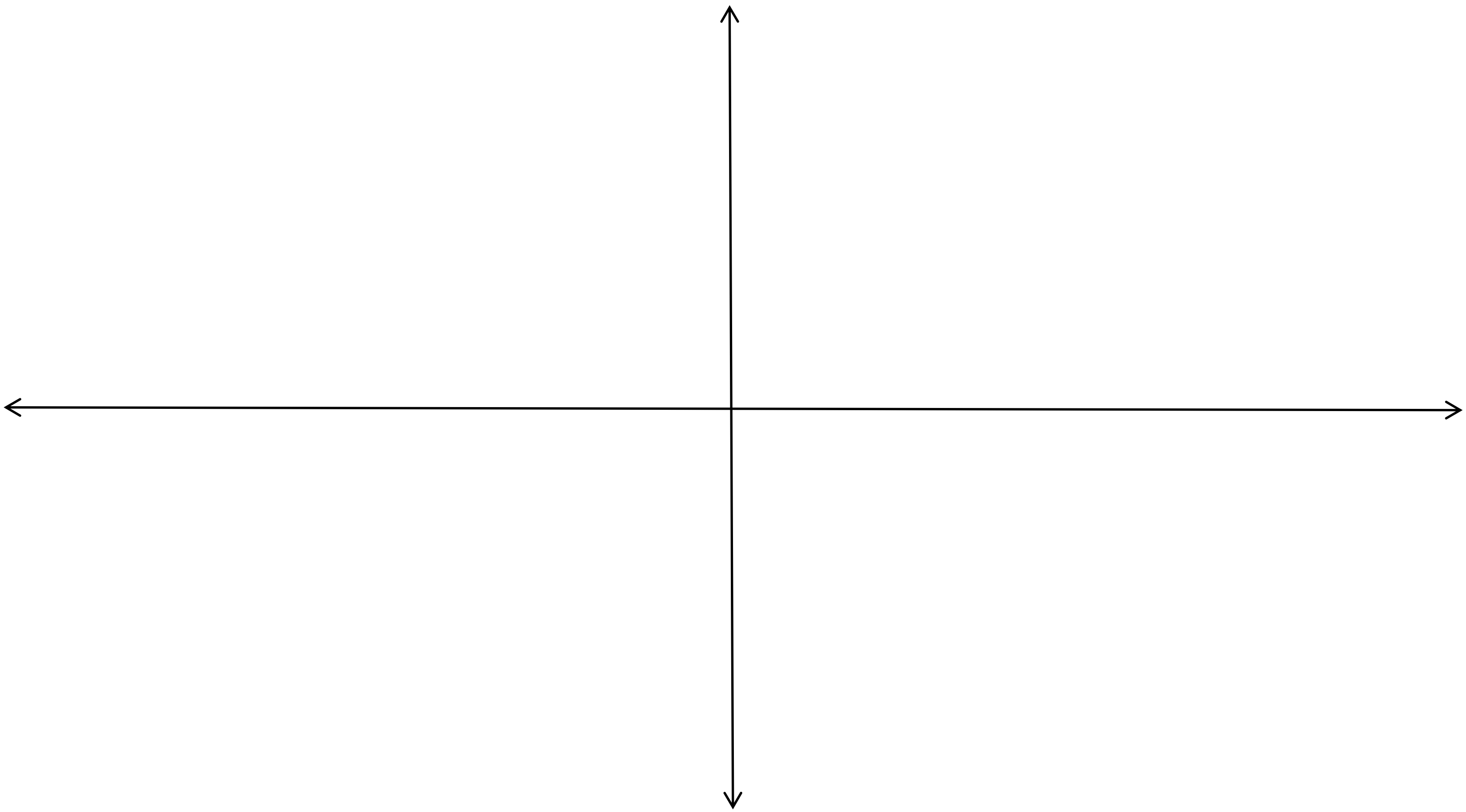
A Brief Introduction

- What is a **Quantum Computer**?
- We don’t know where an electron is (until we observe it)

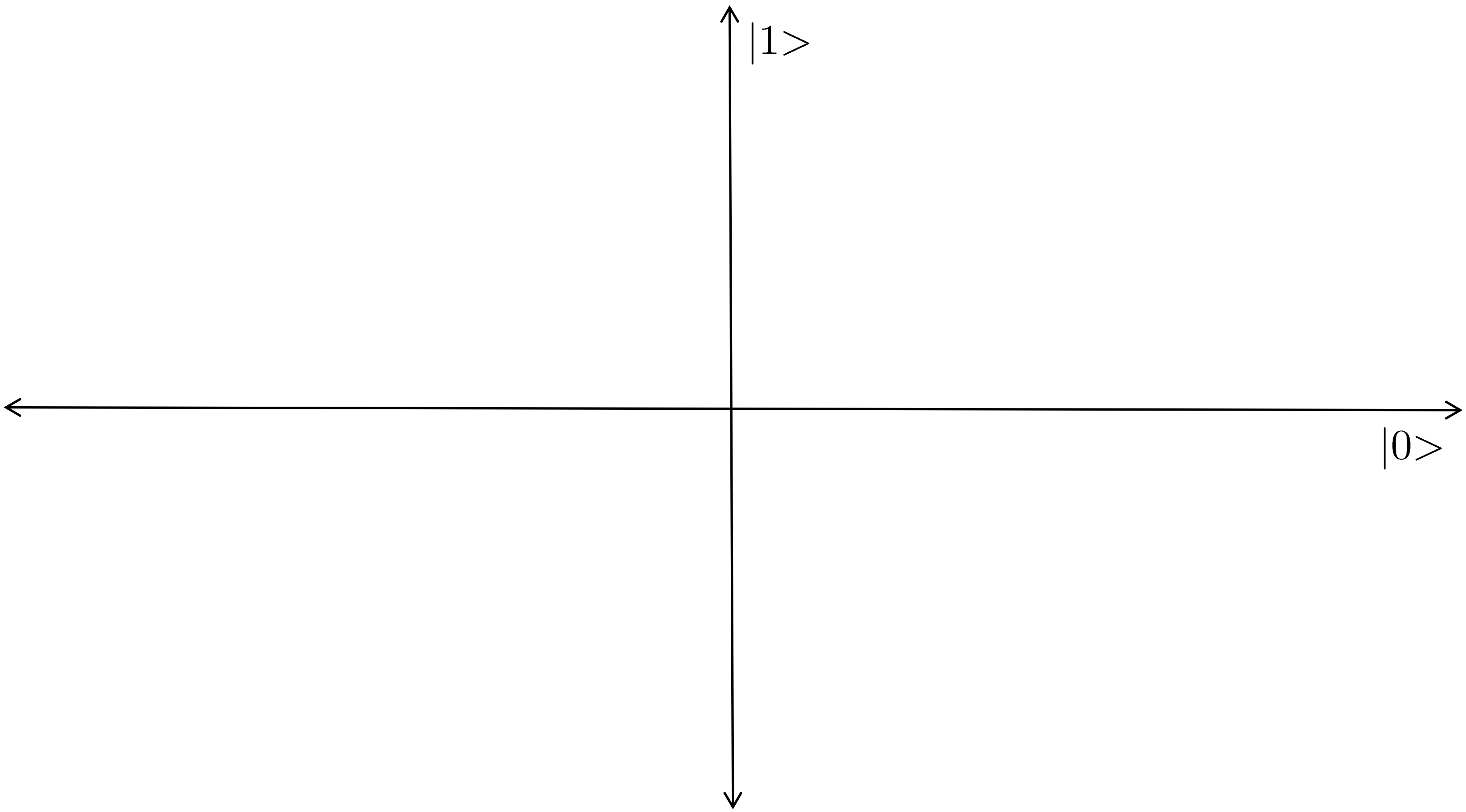
A Brief Introduction

- What is a **Quantum Computer**?
- We don't know where an electron is (until we observe it)
- **Amplitudes** – square to find probabilities

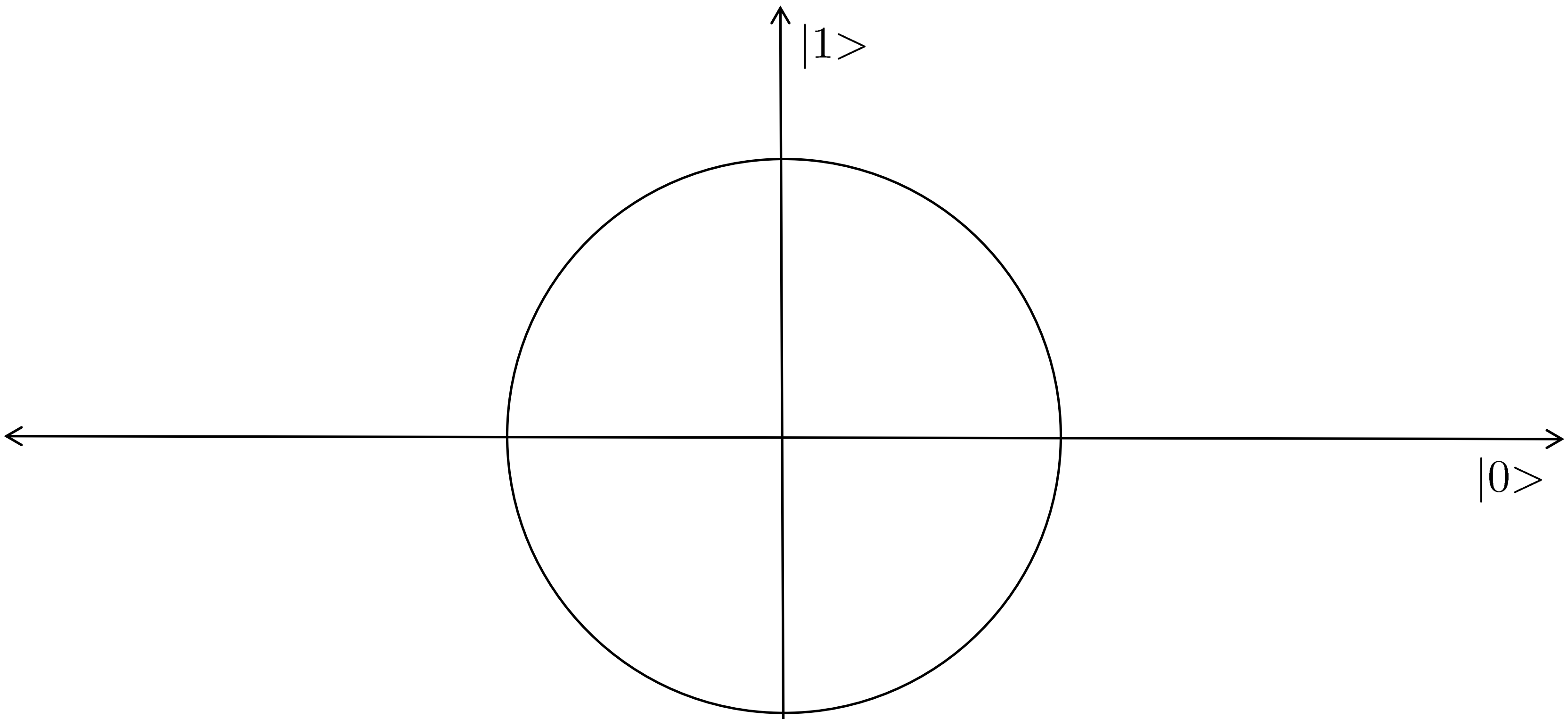
Quantum States and Dirac Notation



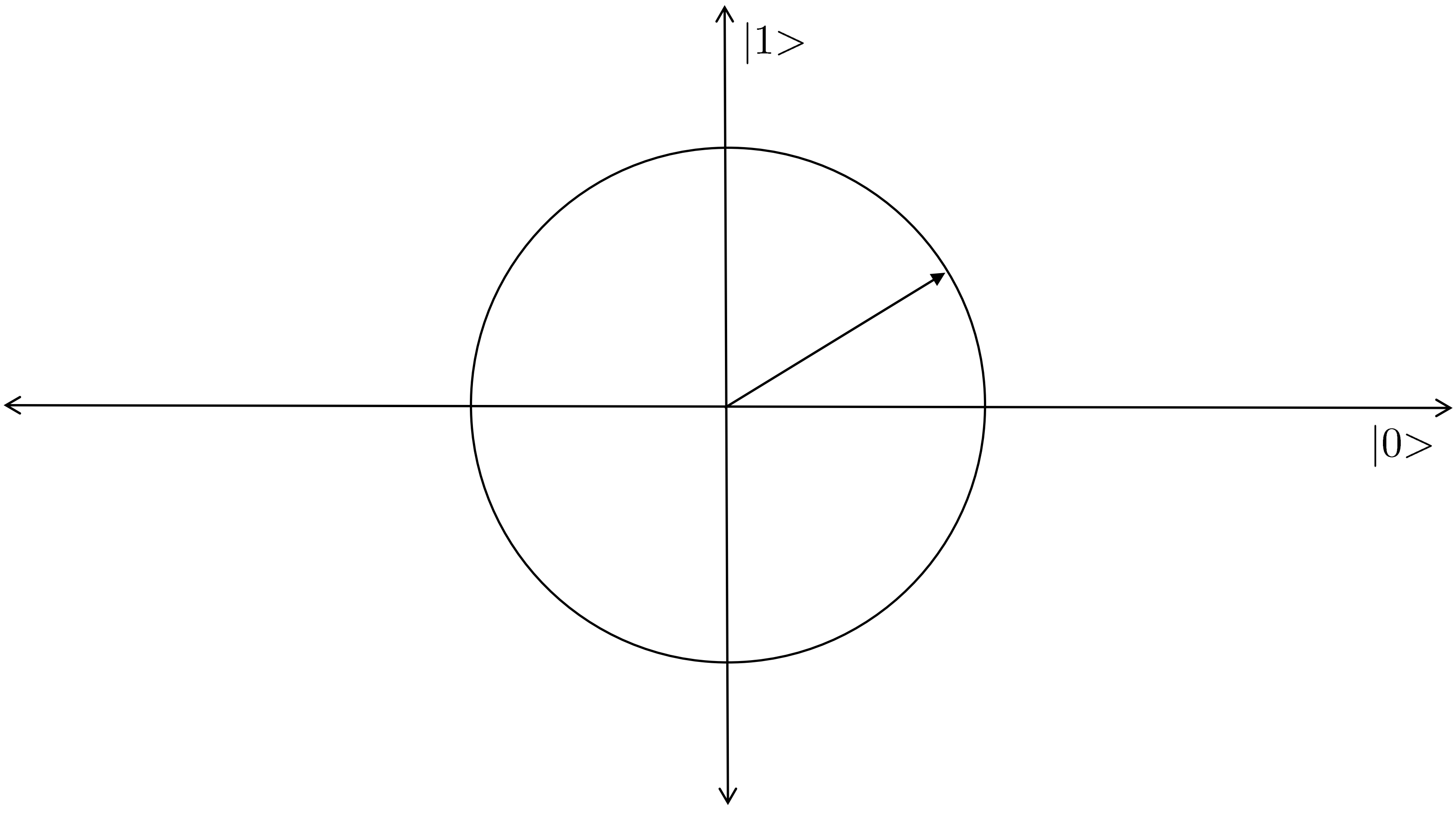
Quantum States and Dirac Notation



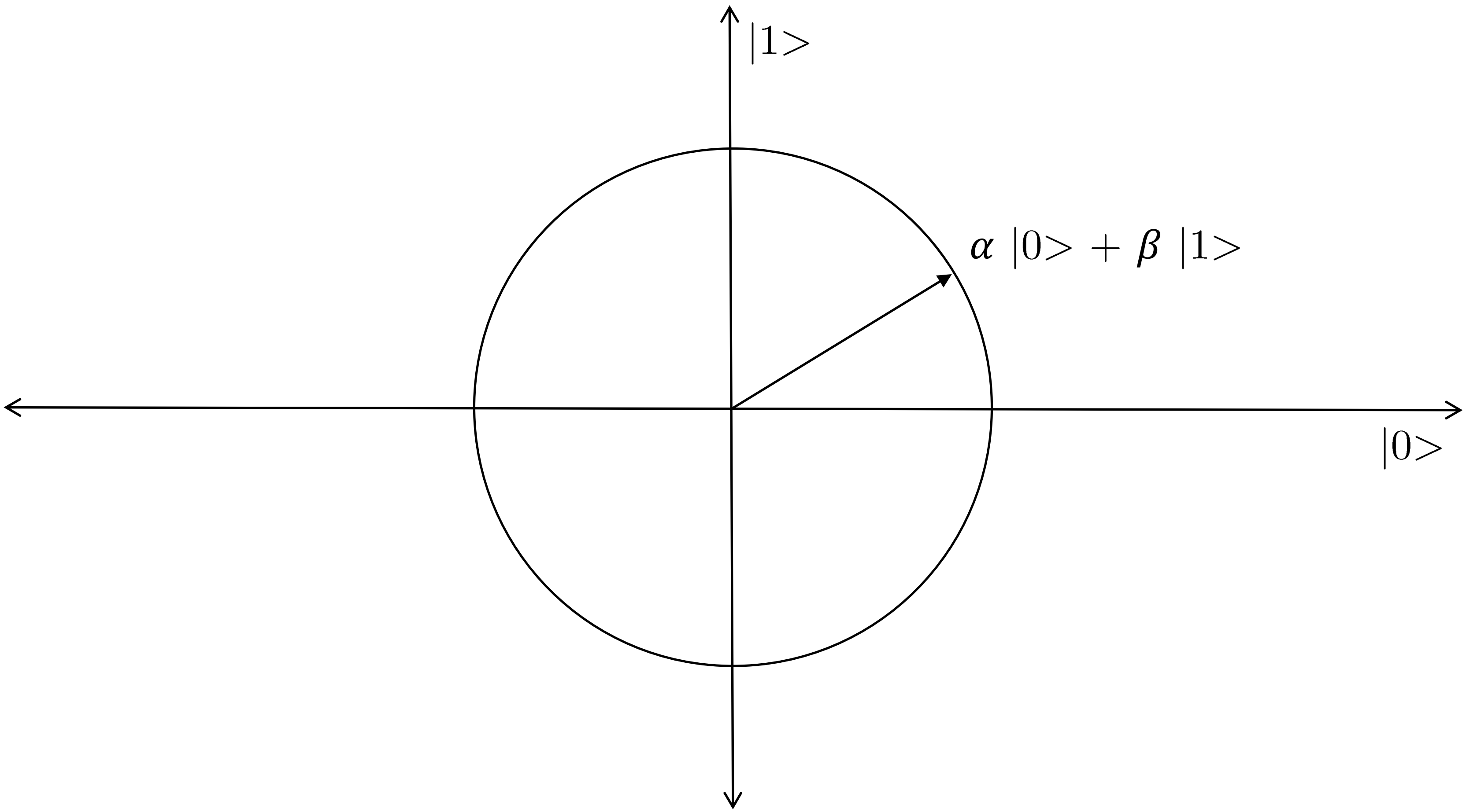
Quantum States and Dirac Notation



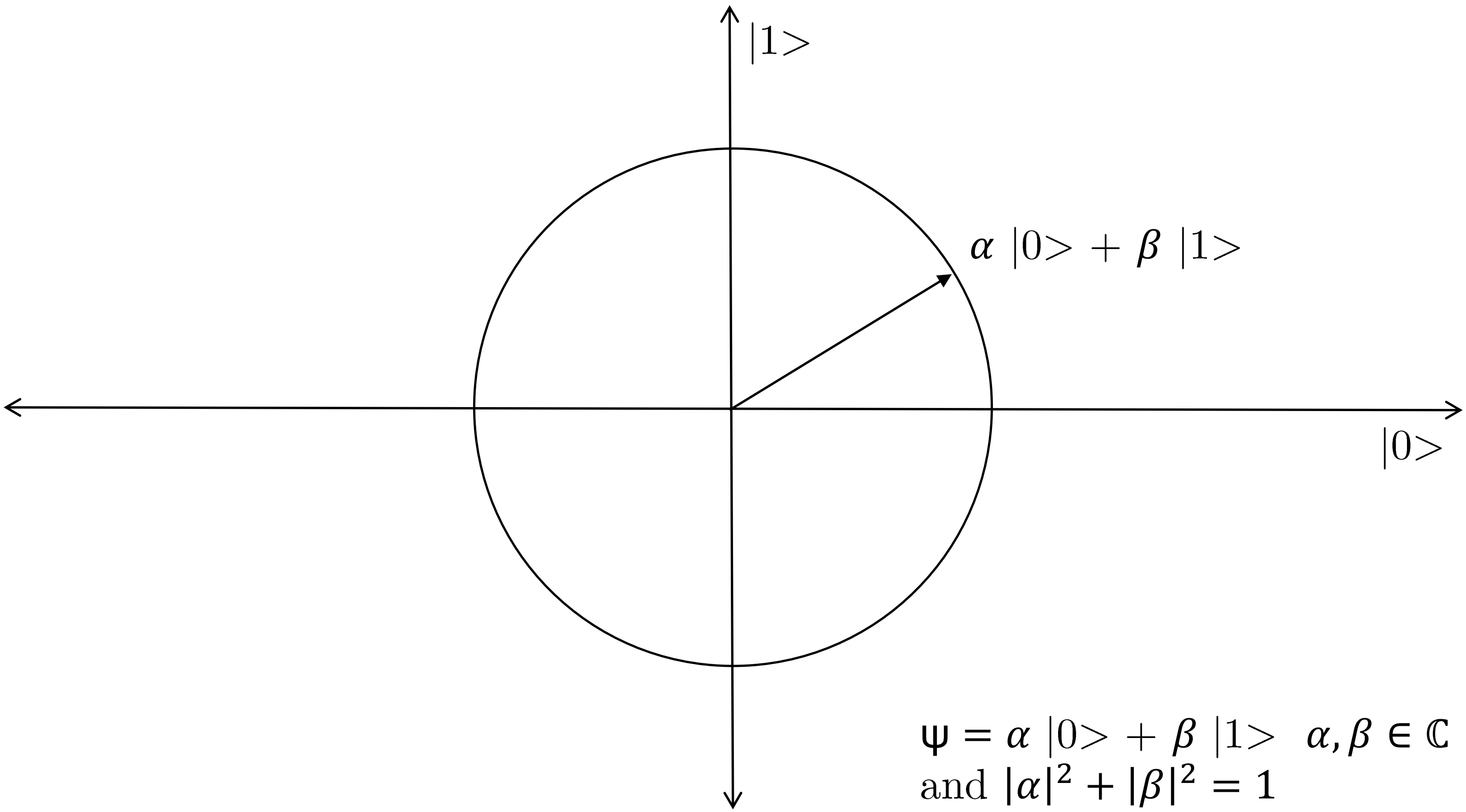
Quantum States and Dirac Notation



Quantum States and Dirac Notation



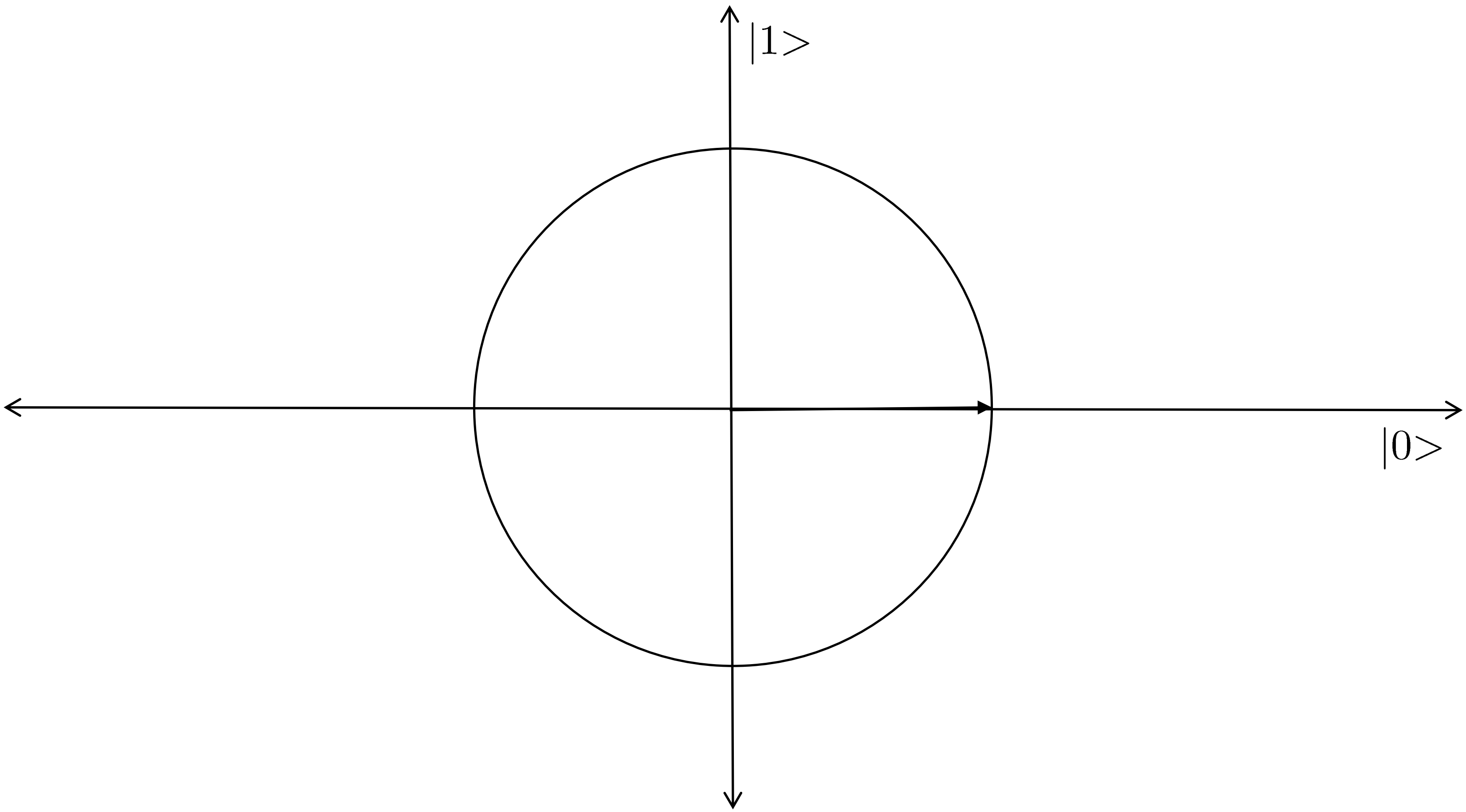
Quantum States and Dirac Notation



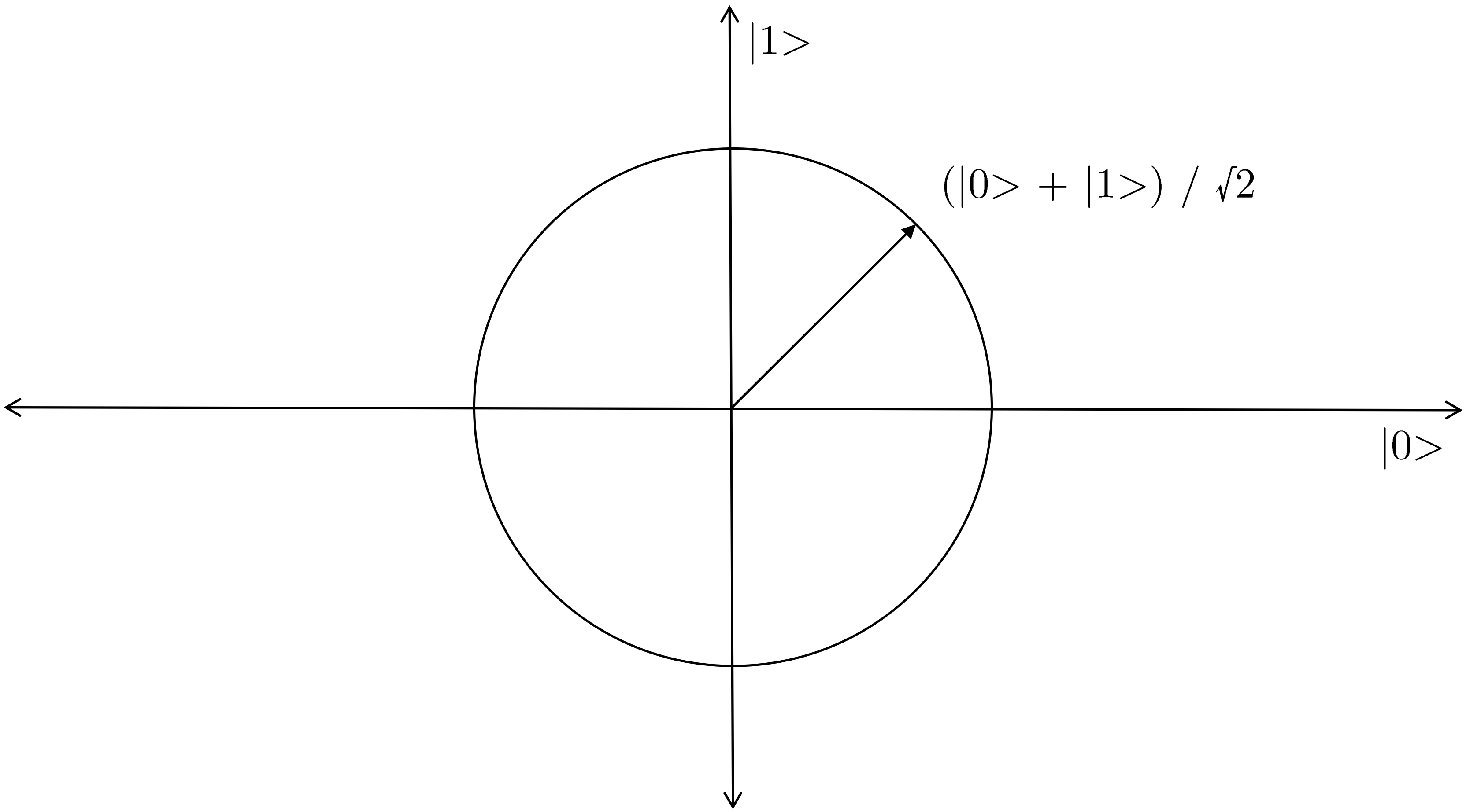
$\psi = \alpha\ |0> + \beta\ |1>\quad \alpha, \beta \in \mathbb{C}$
and $|\alpha|^2 + |\beta|^2 = 1$

Intrinsic Randomness

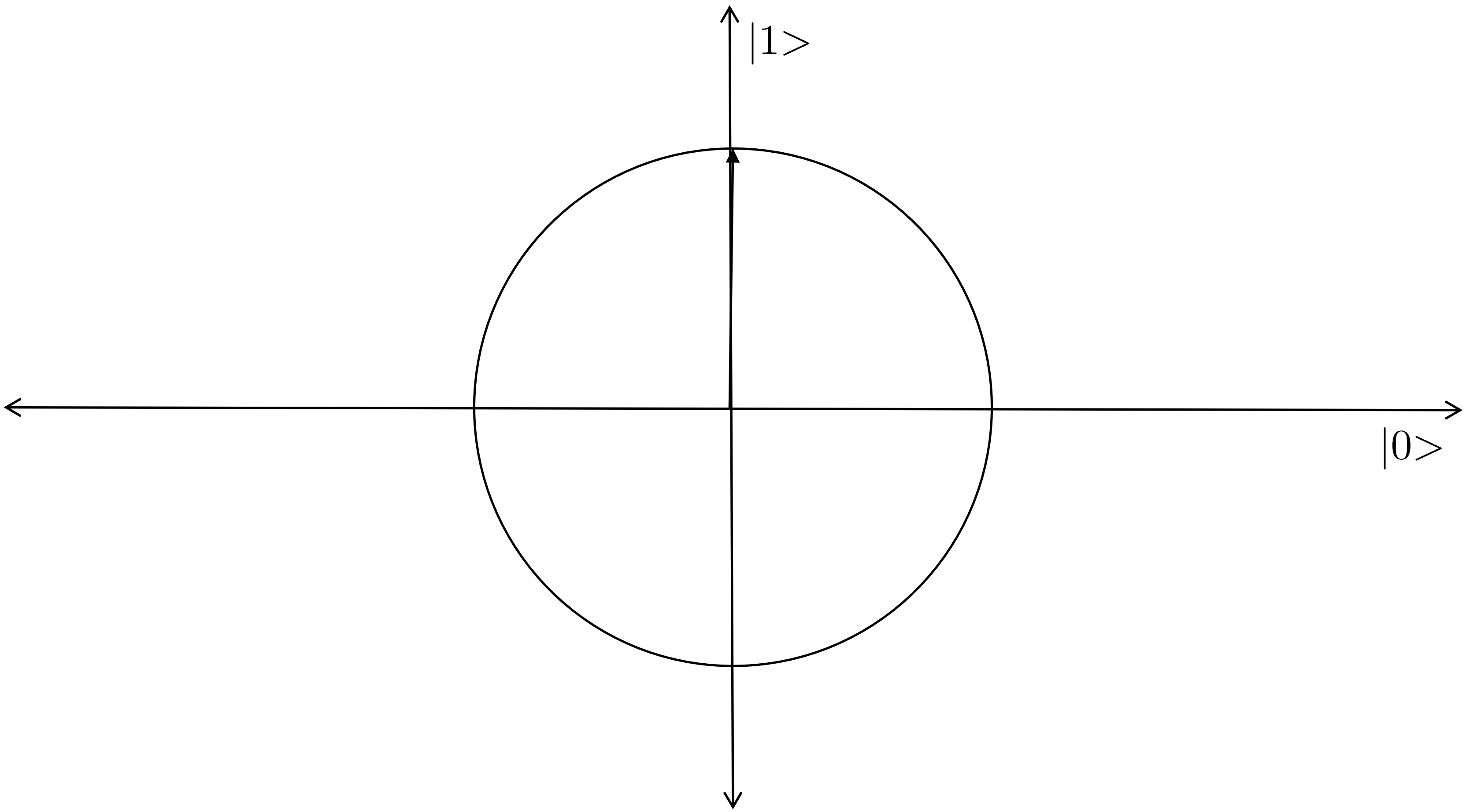
Intrinsic Randomness



Intrinsic Randomness



Intrinsic Randomness



Interference

Interference

- $|0> \rightarrow (|0> + |1>) \,/\, \sqrt{2}$
- $|1> \rightarrow (-\,|0> + |1>) \,/\, \sqrt{2}$

Interference

- $|0> \rightarrow (|0> + |1>) / \sqrt{2}$
- $|1> \rightarrow (- |0> + |1>) / \sqrt{2}$

E.g. Test on $(|0> + |1>) / \sqrt{2}$

Interference

- $|0> \rightarrow (|0> + |1>) / \surd 2$
- $|1> \rightarrow (-|0> + |1>) / \surd 2$

E.g. Test on $(|0> + |1>) / \surd 2$

$((|0> + |1> - |0> + |1>) / \surd 2) / \surd 2$

Interference

- $|0> \rightarrow (|0> + |1>) / \surd 2$
- $|1> \rightarrow (- |0> + |1>) / \surd 2$

E.g. Test on $(|0> + |1>) / \surd 2$

$((|0> + |1> - |0> + |1>) / \surd 2) / \surd 2$

$= ((2|1>) / \surd 2) / \surd 2 = |1>$ as required

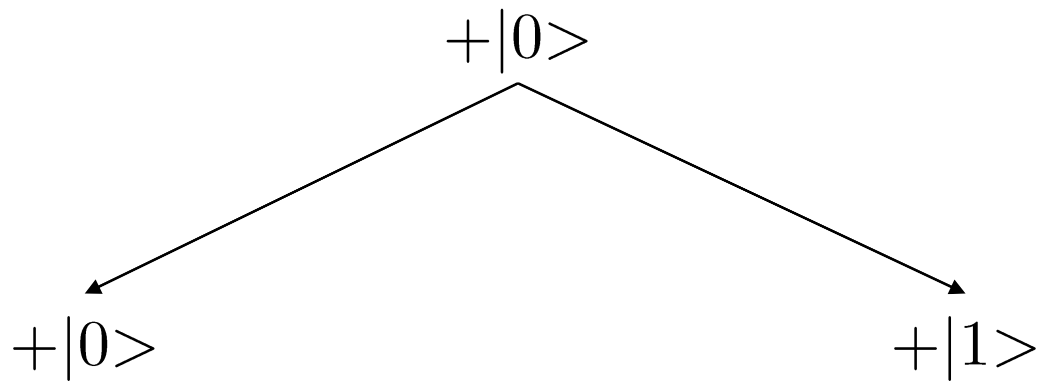
Interference

$|0> \rightarrow (|0> + |1>) / \sqrt{2}$
$|1> \rightarrow (- 0> + |1>) / \sqrt{2}$

$$+|0>$$

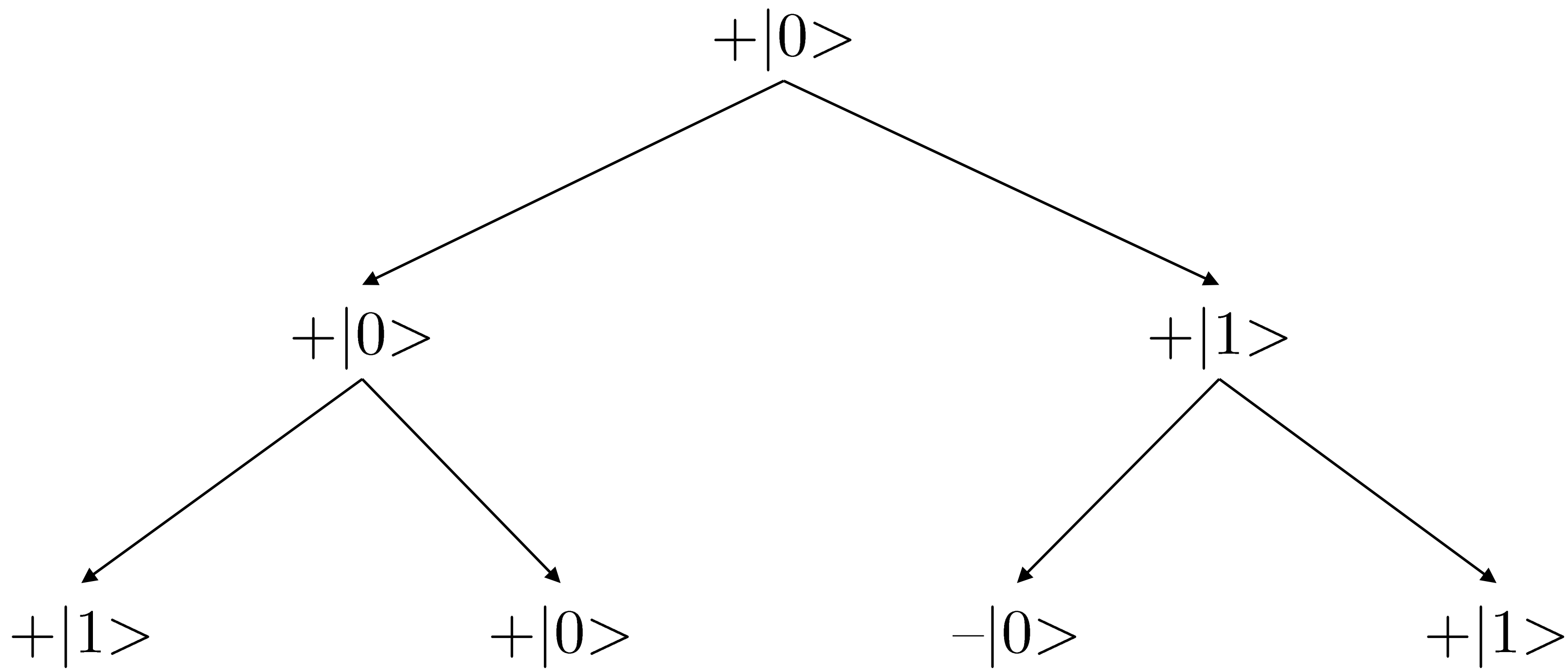
Interference

$|0> \rightarrow (|0> + |1>) \,/\, \sqrt{2}$
$|1> \rightarrow (- \, 0> + |1>) \,/\, \sqrt{2}$



Interference

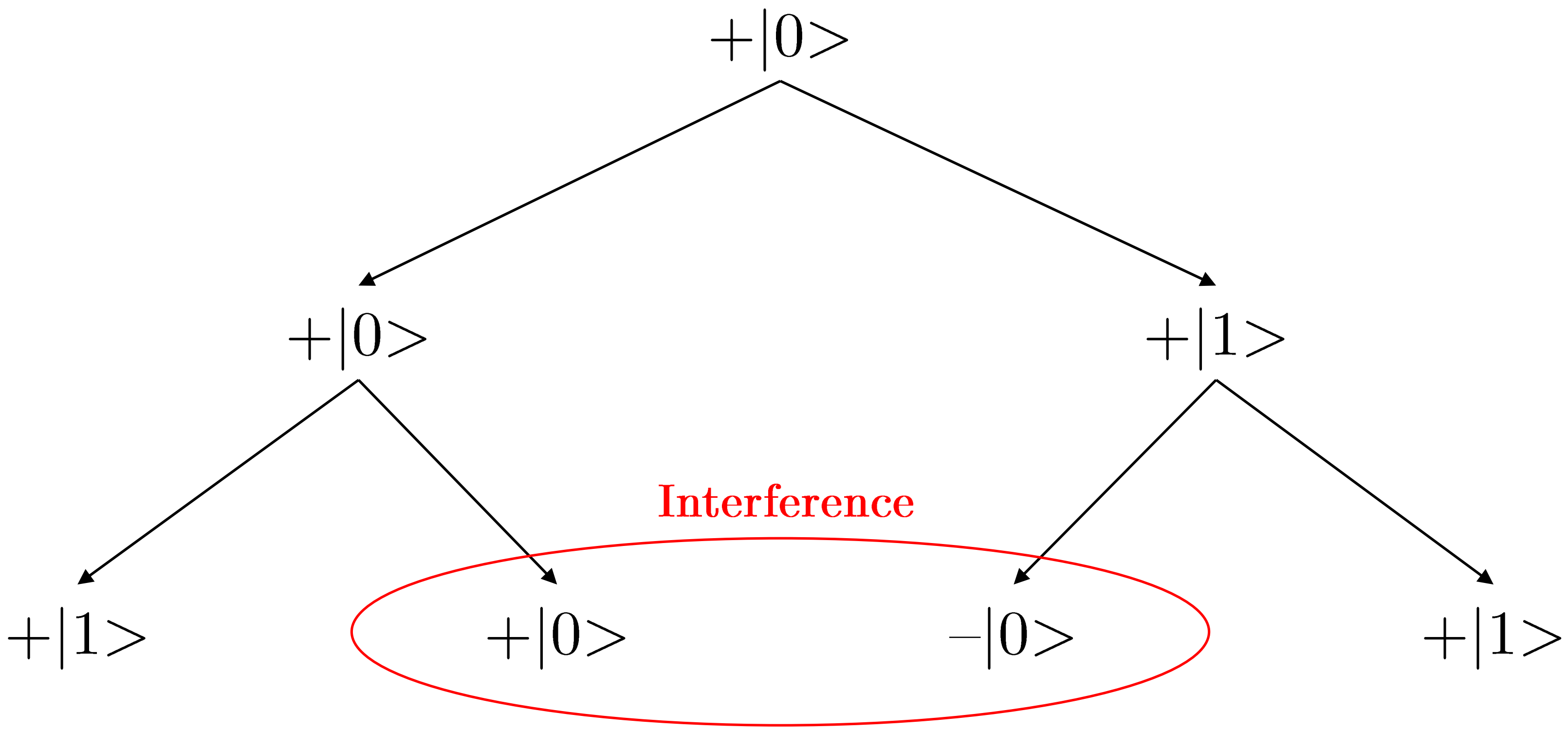
$|0> \rightarrow (|0> + |1>) \; / \; \sqrt{2}$
$|1> \rightarrow (- \, 0> + |1>) \; / \; \sqrt{2}$



Interference

$|0> \rightarrow (|0> + |1>) \,/\, \sqrt{2}$

$|1> \rightarrow (- 0> + |1>) \,/\, \sqrt{2}$



Applying to Computation

Taking 2 bits / qubits:

<table>
<tr><th>CLASSICAL COMPUTER
(Bits)</th><th>QUANTUM COMPUTER
(Qubits)</th></tr>
<tr><td>00</td><td>|0, 0></td></tr>
<tr><td>01</td><td>|s> = |0, 1 – 1, 0> / √2</td></tr>
<tr><td>10</td><td>|T_0> = |0, 1 + 1, 0> / √2</td></tr>
<tr><td>11</td><td>|1, 1></td></tr>
</table>

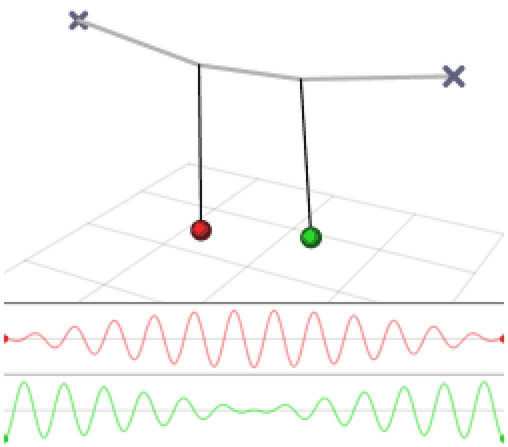
Applying to Computation

Taking 2 bits / qubits:

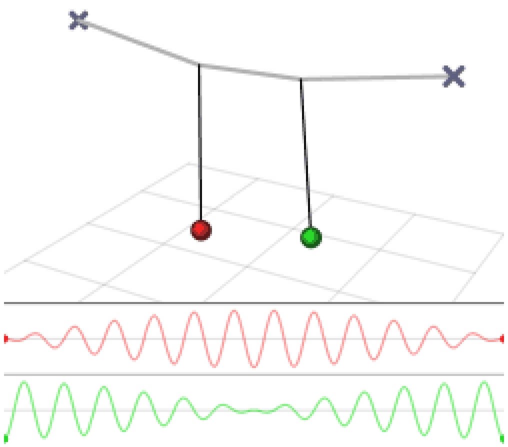
CLASSICAL COMPUTER (Bits)	**QUANTUM COMPUTER (Qubits)**
00	$\vert 0, 0>$
01	$\vert s> = \vert 0, 1 - 1, 0> / \sqrt{2}$
10	$\vert T\_0> = \vert 0, 1 + 1, 0> / \sqrt{2}$
11	$\vert 1, 1>$

Entangled States

Explaining the Entangled States



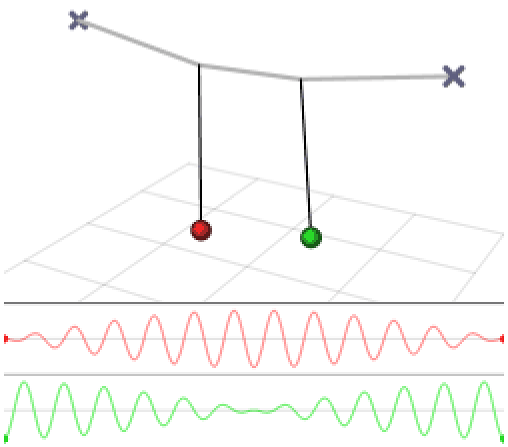
Explaining the Entangled States



$|0,1>$

$|1,0>$

Explaining the Entangled States



$|0,1>$
$|1,0>$

$$\frac{1}{\sqrt{2}}|0,1> - \frac{1}{\sqrt{2}}|1,0>$$ (Singlet State)

(Qubits are not independent of each other!)

$$\frac{1}{\sqrt{2}}|0,1> + \frac{1}{\sqrt{2}}|1,0>$$ (T_0 State)

Superposition of States

α $|0,\ 0>$

β $|\text{T\_0}> = |0,\ 1 - 1,\ 0> /\ \sqrt{2}$

γ $|\text{s}> = |0,\ 1 + 1,\ 0> /\ \sqrt{2}$

δ $|1,\ 1>$

Superposition of States

$\alpha\ |0,\ 0>$

$\beta\ |T\_0> = |0,\ 1 - 1,\ 0>\ /\ \sqrt{2}$

$\gamma\ |s> = |0,\ 1 + 1,\ 0>\ /\ \sqrt{2}$

$\delta\ |1,\ 1>$

No. of bits	No. of values held by classical bits	No. of values held by qubits
1	1	2
2	2	4
3	3	8
n	n	2^n

Problems

Problems

- Classical Algorithms

Problems

- Classical Algorithms
- Superpositions

The Prime Factorisation Problem

The Prime Factorisation Problem

$O(e^{(\log n \log\log n)^{\frac{1}{2}}})$ problem using classical algorithms

The Period Finding Problem

2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...

The Period Finding Problem

2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...

2, 4, 8, 1, 2, 4, 8, 1, 2, 4, ...

The Period Finding Problem

2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...

2, 4, 8, 1, 2, 4, 8, 1, 2, 4, ...

2, 4, 8, 1, 16, 11, 2, 4, 8, 16, ...

Euler’s Totient Function

x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...

Period evenly divides (p-1)(q-1)

Euler's Totient Function

x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...

Period evenly divides (p-1)(q-1)

Let x=2, N=15

Euler's Totient Function

x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...

Period evenly divides (p-1)(q-1)

Let x=2, N=15

Hence p=3, q=5

Euler's Totient Function

x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...

Period evenly divides (p-1)(q-1)

Let x=2, N=15

Hence p=3, q=5

(p-1)(q-1) = 8, and 8|4 as required

Euler's Totient Function

x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...

Period evenly divides (p-1)(q-1)

Let x=2, N=15

Hence p=3, q=5

(p-1)(q-1) = 8, and 8|4 as required

x=2, N=21; p=3, q=7

Euler's Totient Function

x mod N, x^2 mod N, x^3 mod N, x^4 mod N, ...

Period evenly divides (p-1)(q-1)

Let x=2, N=15

Hence p=3, q=5

(p-1)(q-1) = 8, and 8|4 as required

x=2, N=21; p=3, q=7

(p-1)(q-1) = 12 and 12|6 as required

Shor's Algorithm: The Classical Part

x^r mod N (r may be very large)

Shor's Algorithm: The Classical Part

x^r mod N (r may be very large)

Let N=17, x=3, r=14

Shor's Algorithm: The Classical Part

x^r mod N (r may be very large)

Let N=17, x=3, r=14

r = 2^3 + 2^2 + 2^1

Shor's Algorithm: The Classical Part

x^r mod N (r may be very large)

Let N=17, x=3, r=14

r = 2^3 + 2^2 + 2^1

$$x^r = 3^{14} = 3^{2^3+2^2+2^1} = 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^1} = ((3^2)^2)^2 \cdot (3^2)^2 \cdot 3^2$$

Shor's Algorithm: The Classical Part

x^r mod N (r may be very large)

Let N=17, x=3, r=14

r = 2^3 + 2^2 + 2^1

$$x^r = 3^{14} = 3^{2^3+2^2+2^1} = 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^1} = ((3^2)^2)^2 \cdot (3^2)^2 \cdot 3^2$$

6561 mod 17 * 81 mod 17 * 9 mod 17 = 16 * 13 * 9

Shor's Algorithm: The Classical Part

x^r mod N (r may be very large)

Let N=17, x=3, r=14

r = 2^3 + 2^2 + 2^1

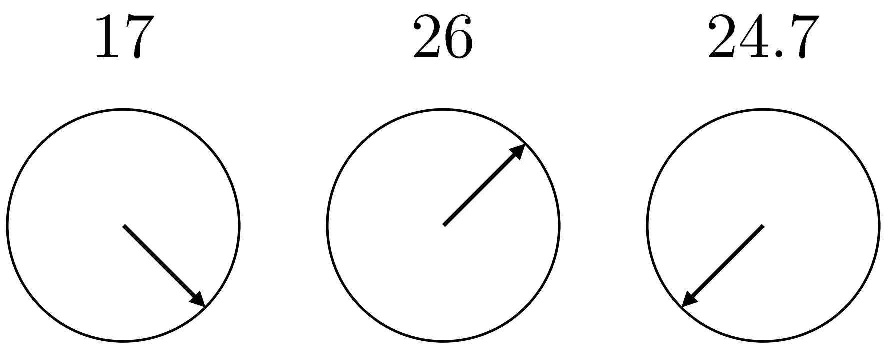
$$x^r = 3^{14} = 3^{2^3+2^2+2^1} = 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^1} = ((3^2)^2)^2 \cdot (3^2)^2 \cdot 3^2$$

6561 mod 17 * 81 mod 17 * 9 mod 17 = 16 * 13 * 9

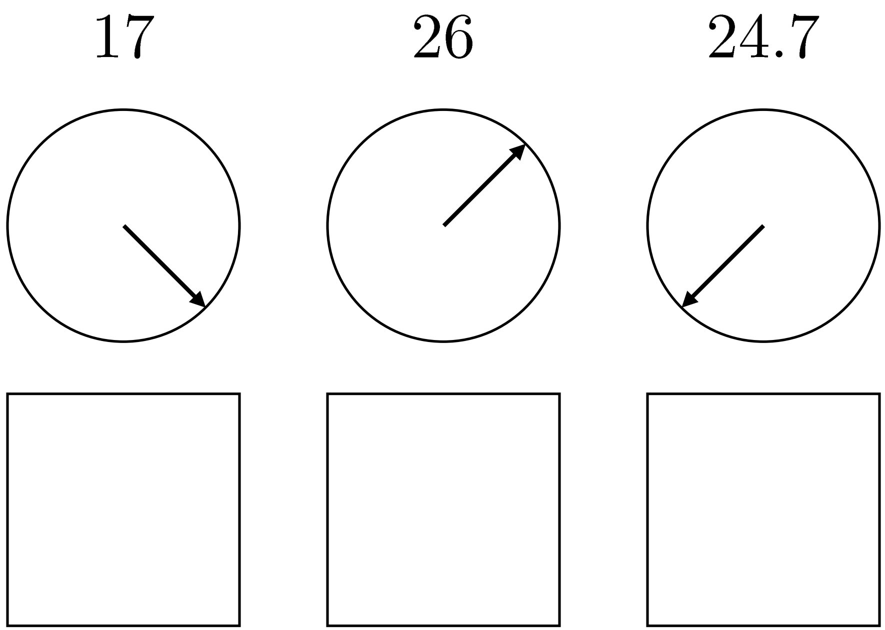
and (16 * 13 * 9) mod 17 = 2

Shor's Algorithm: The Quantum Part

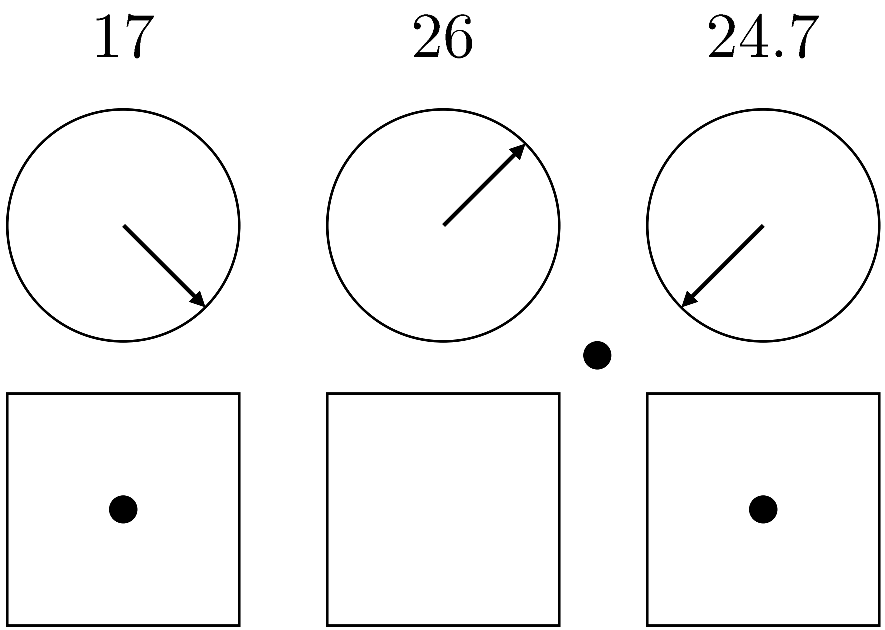
Shor's Algorithm: The Quantum Part



Shor's Algorithm: The Quantum Part



Shor's Algorithm: The Quantum Part



The Quantum Fourier Transform

The Quantum Fourier Transform

$$X_k = \frac{1}{N}\sum_{n=0}^{N-1} x_n e^{i2\pi k \frac{n}{N}}$$

To find the energy at a particular frequency, spin your signal around a circle at that frequency, and average a bunch of points along that path.

The Quantum Fourier Transform

$$X_k = \frac{1}{N}\sum_{n=0}^{N-1} x_n e^{i2\pi k \frac{n}{N}}$$

To find the energy at a particular frequency, spin your signal around a circle at that frequency, and average a bunch of points along that path.

http://betterexplained.com/articles/an-interactive-guide-to-the-fourier-transform/

Back to Interference