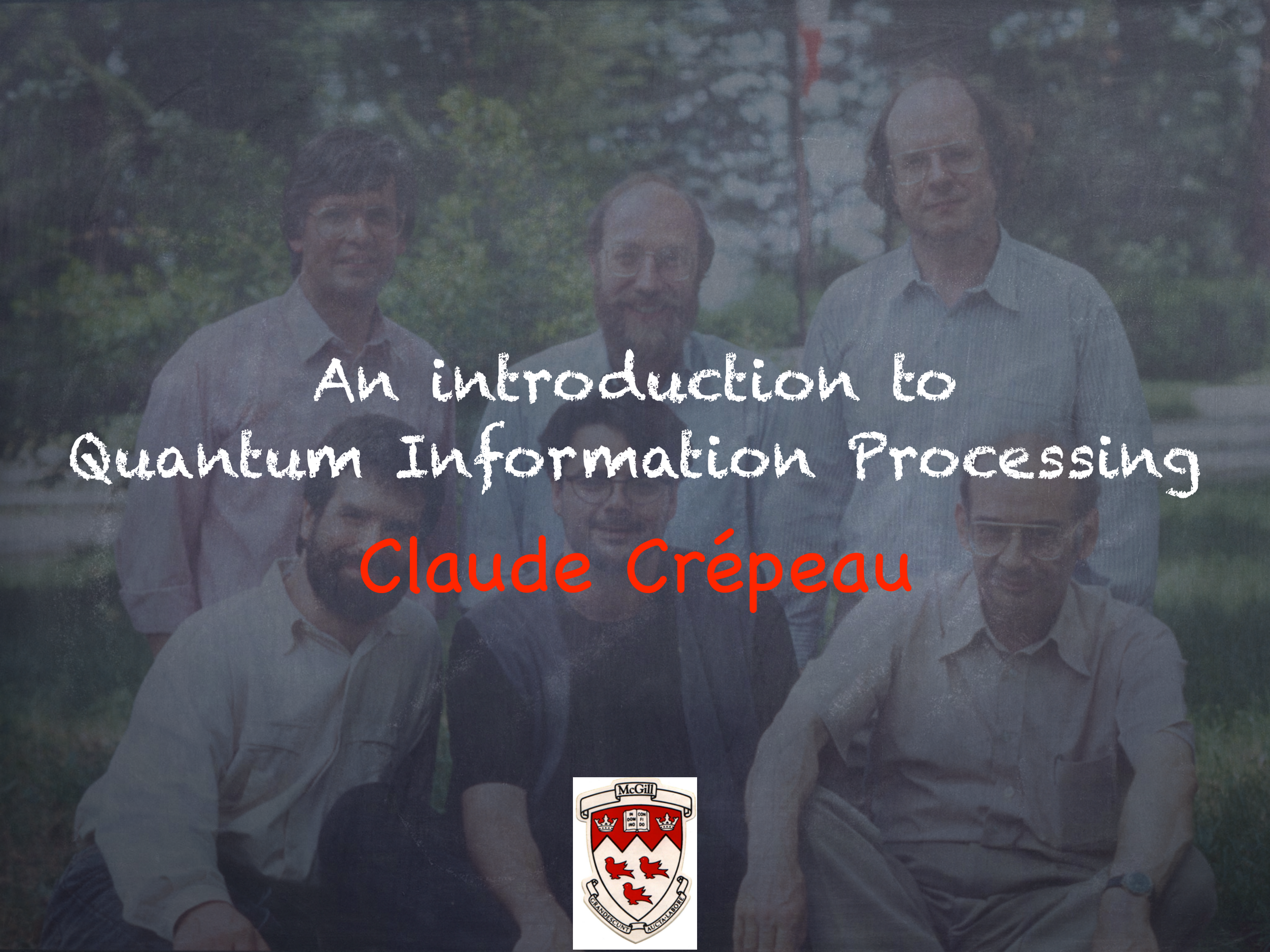


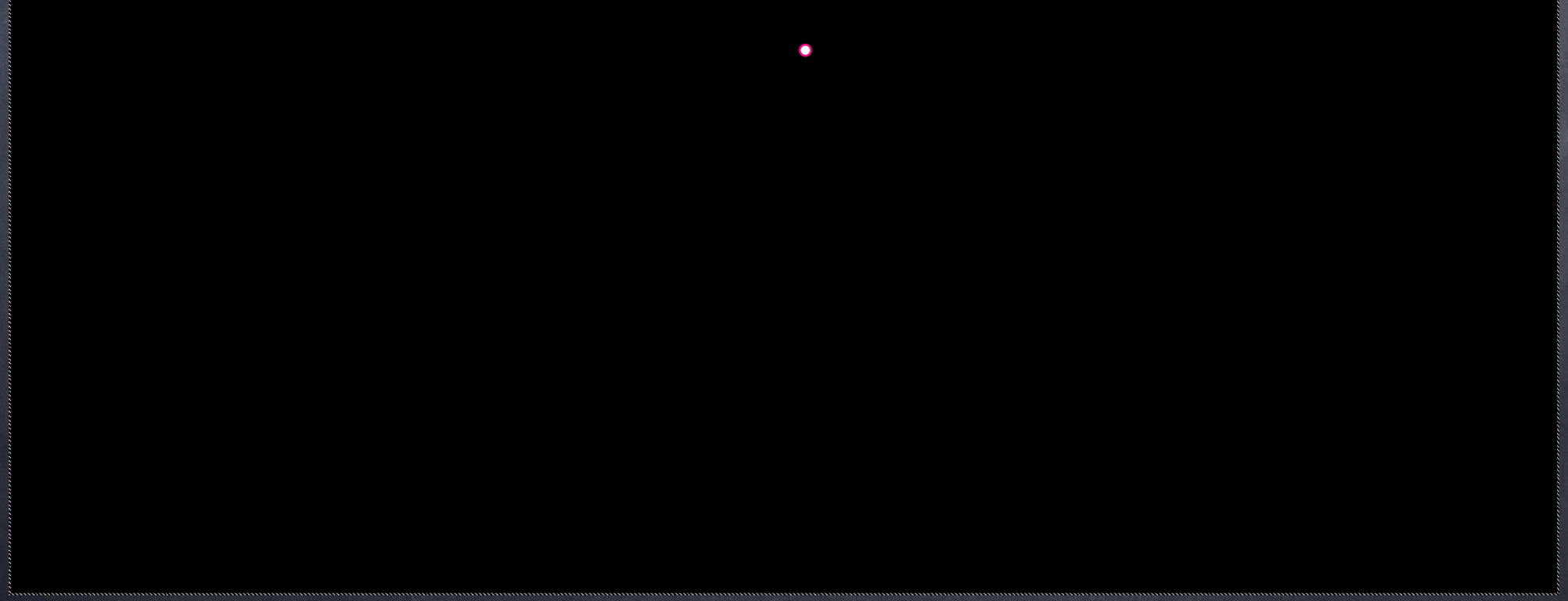
An introduction to Quantum Information Processing

Claude Crépeau

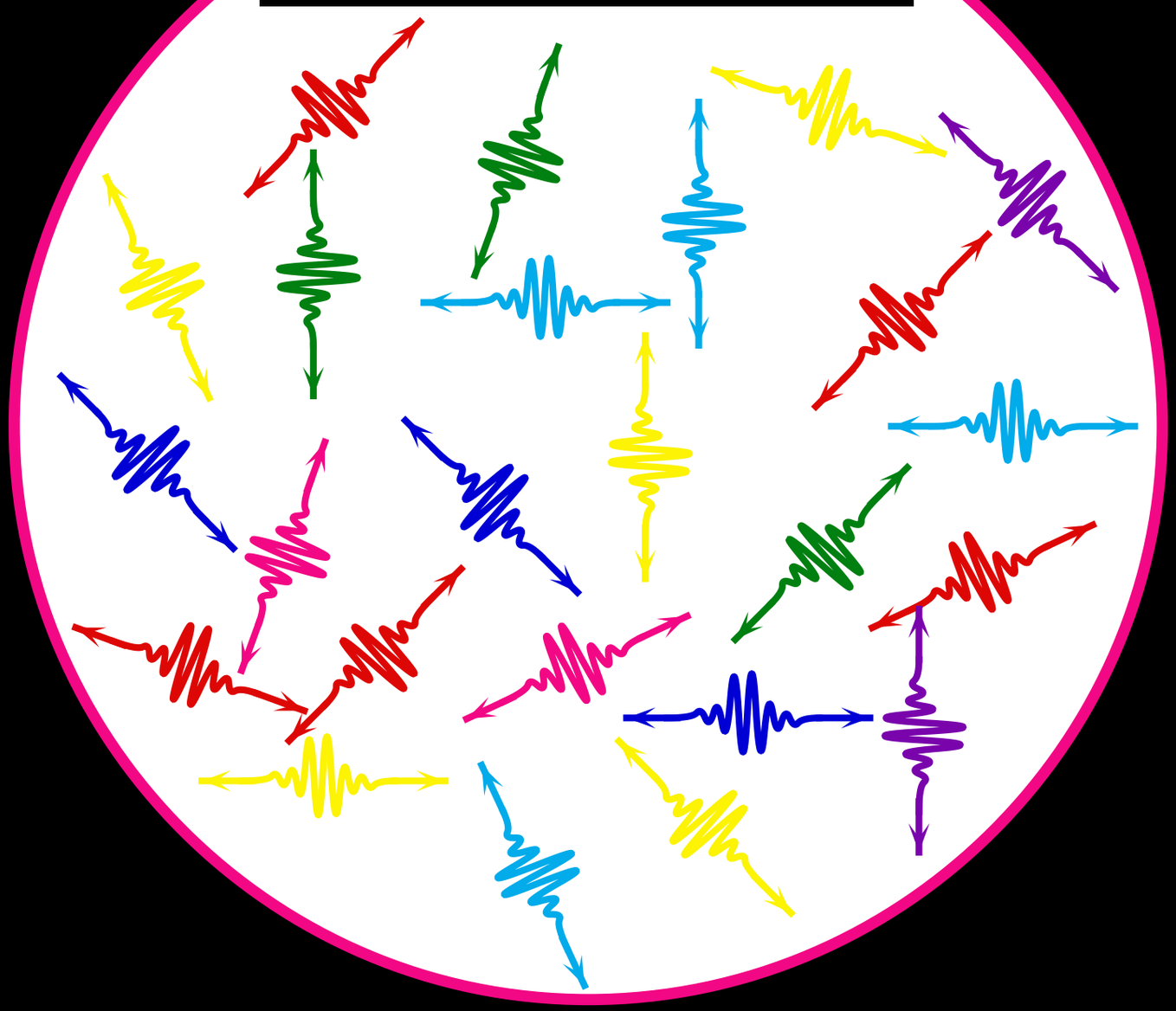
(1)

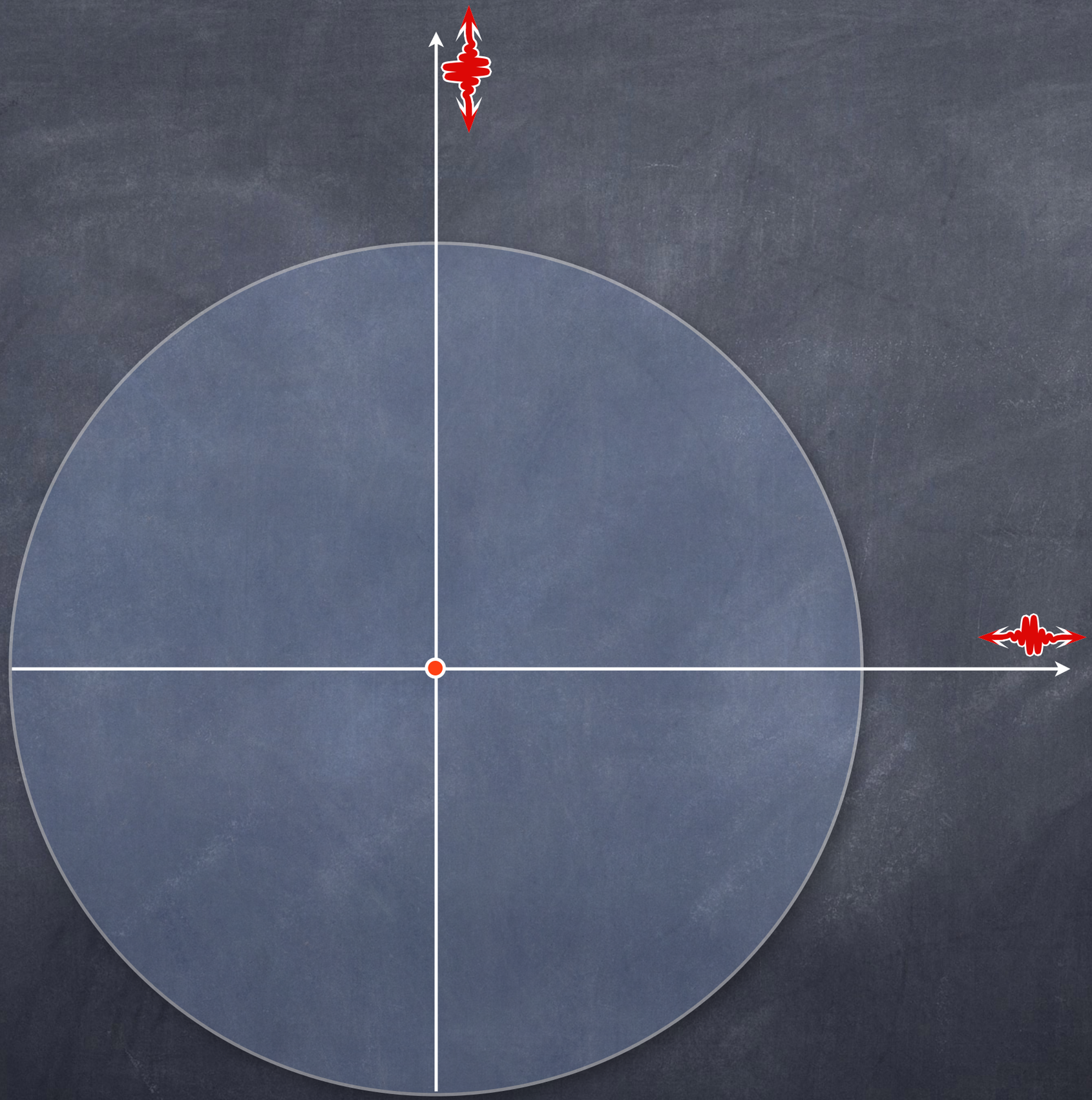
Quantum Information

Photons



Photons

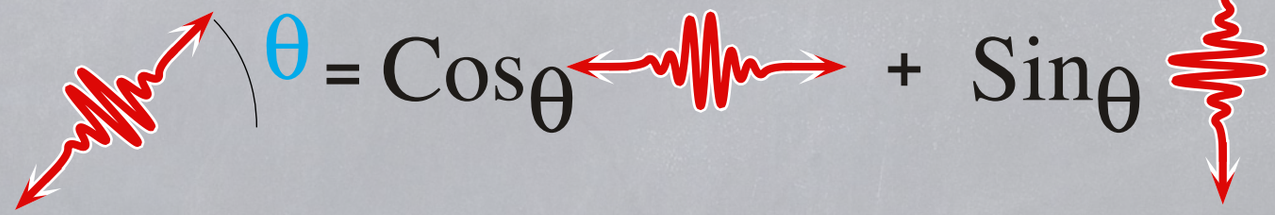




Bits & Qubits

0: 

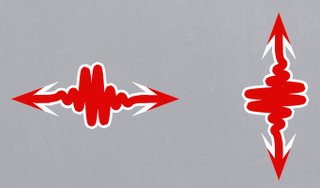
1: 

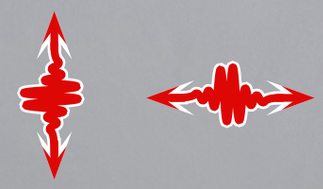


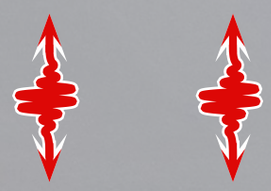
$$|\Psi\rangle = C_0 + C_1$$

$$C_i, C_{ij} \in \mathbb{C}$$

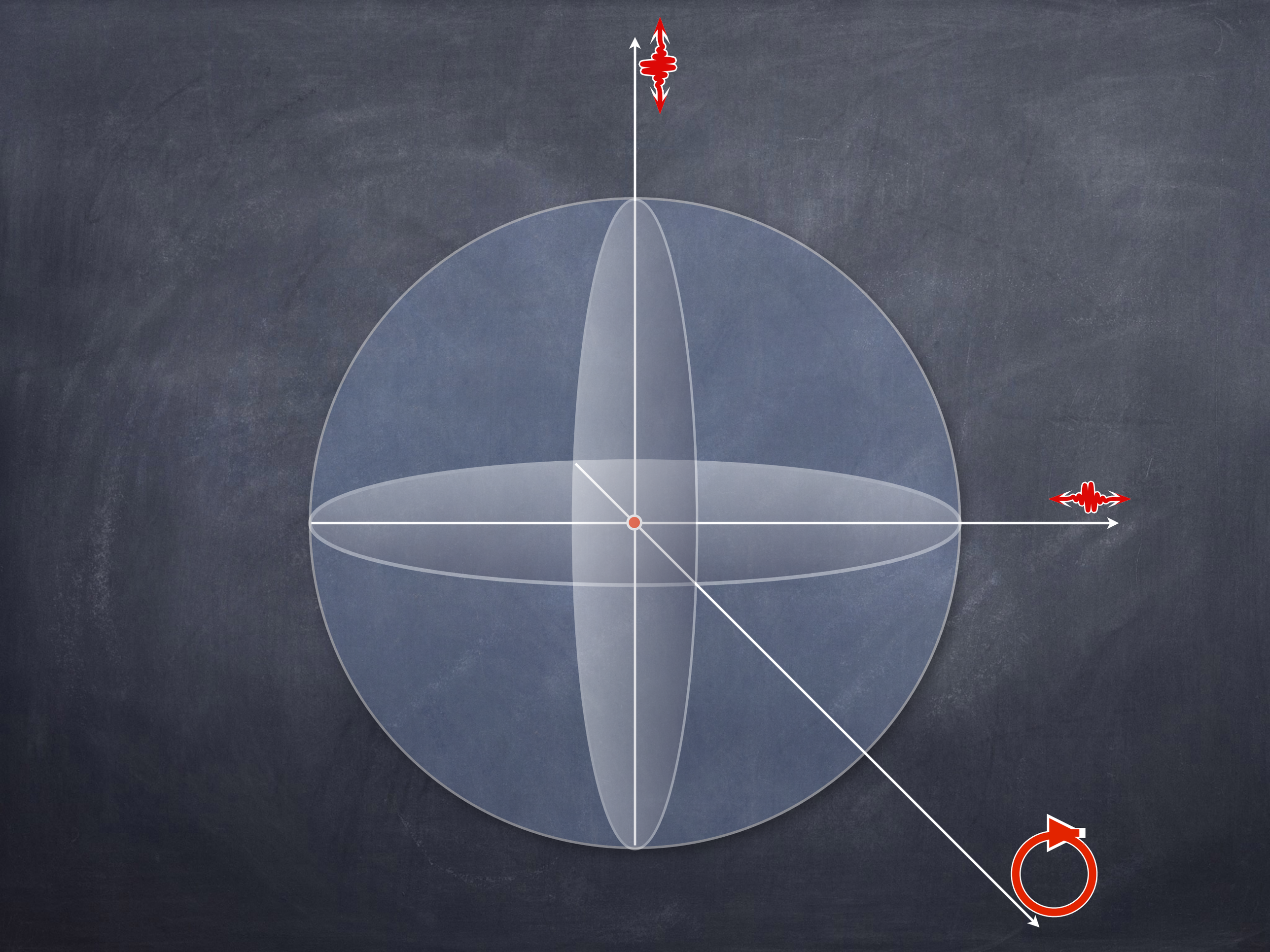
00: 

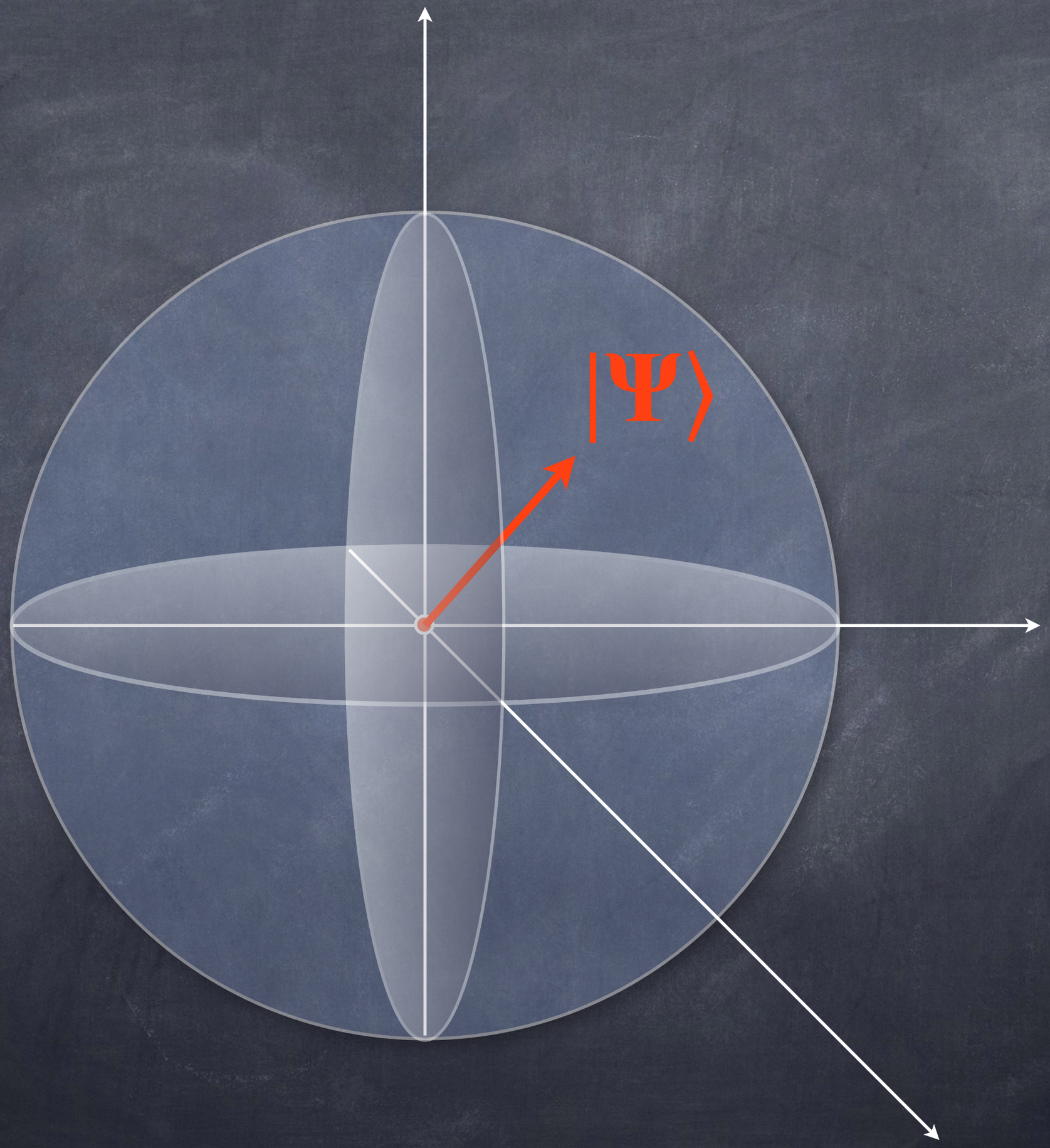
01: 

10: 

11: 

$$|\Psi\rangle = C_{00} + C_{01} + C_{10} + C_{11}$$




|Ψ⟩

Notations

Basis vectors: $|0\rangle$ and $|1\rangle$

Notations

Basis vectors: $|0\rangle$ and $|1\rangle$

Arbitrary states: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
such that $|\alpha|^2+|\beta|^2=1$

$\alpha,\beta \in \mathbb{C}$

Notations

Basis vectors: $|0\rangle$ and $|1\rangle$

Arbitrary states: $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$
such that $|\alpha|^2+|\beta|^2=1$

Arbitrary multi-states: $\alpha,\beta,\delta,\gamma\in\mathbb{C}$

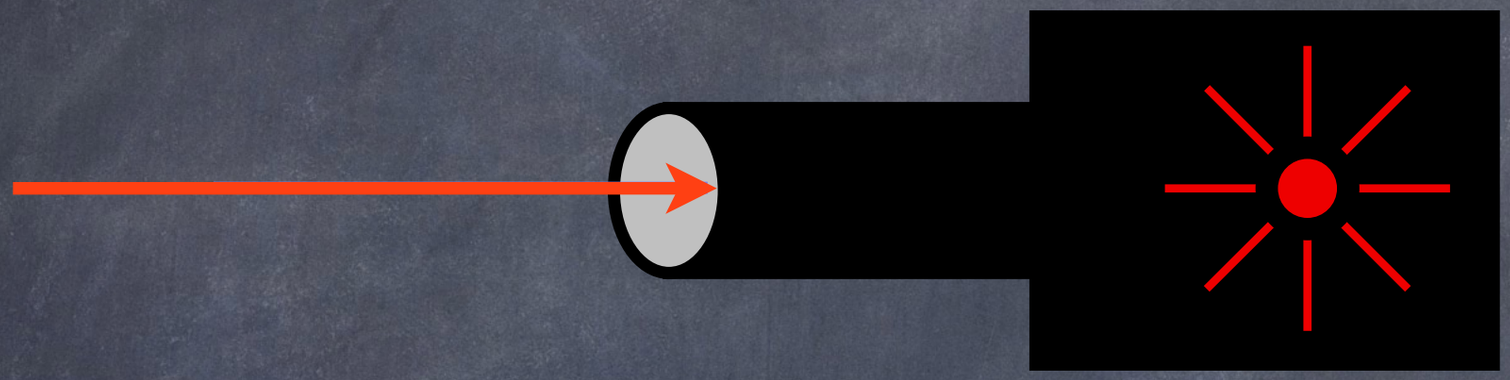
$$|\psi\rangle=\alpha|00\rangle+\beta|01\rangle+\delta|10\rangle+\gamma|11\rangle$$

such that $|\alpha|^2+|\beta|^2+|\delta|^2+|\gamma|^2=1$

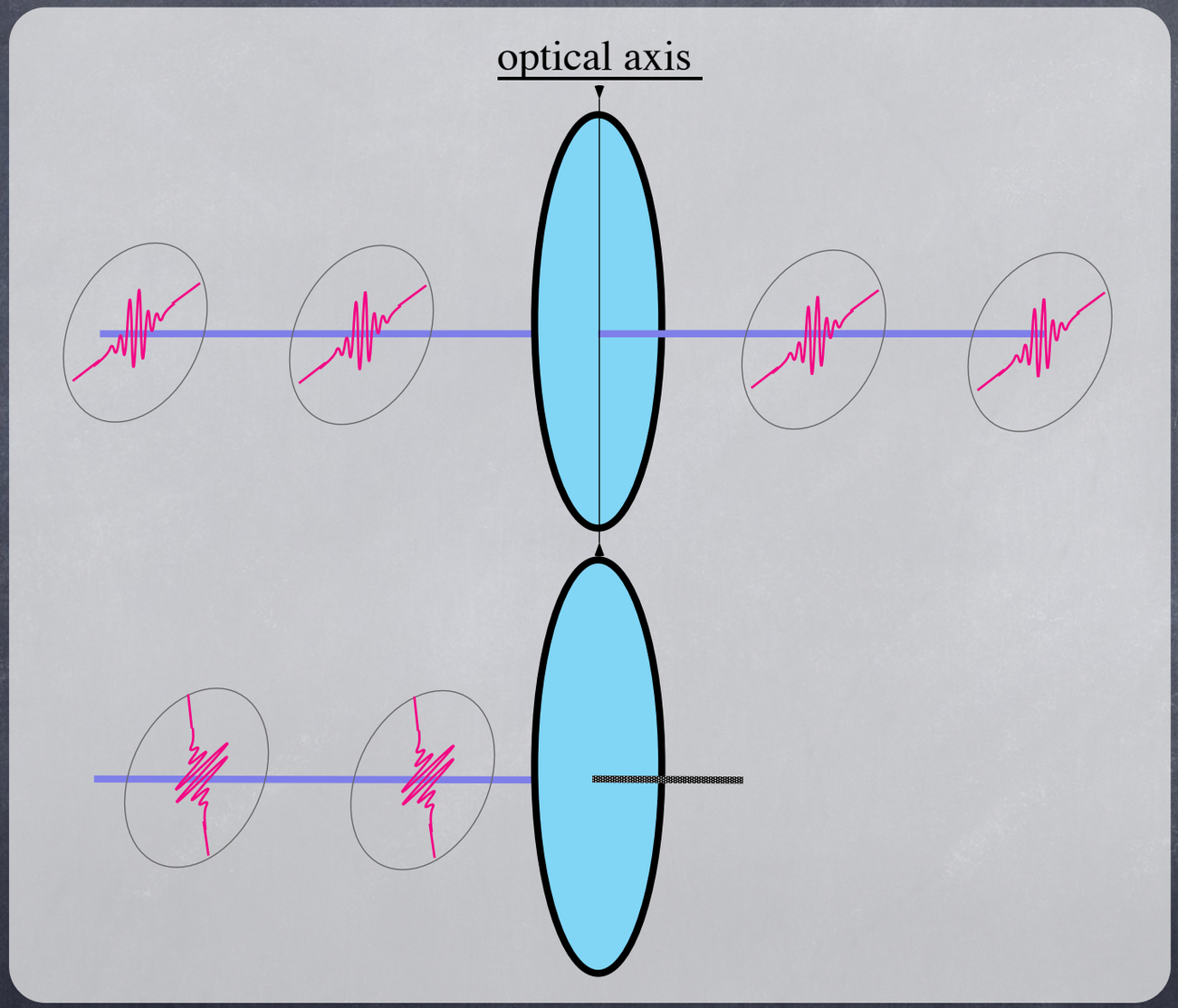
(2)

Quantum Measurements

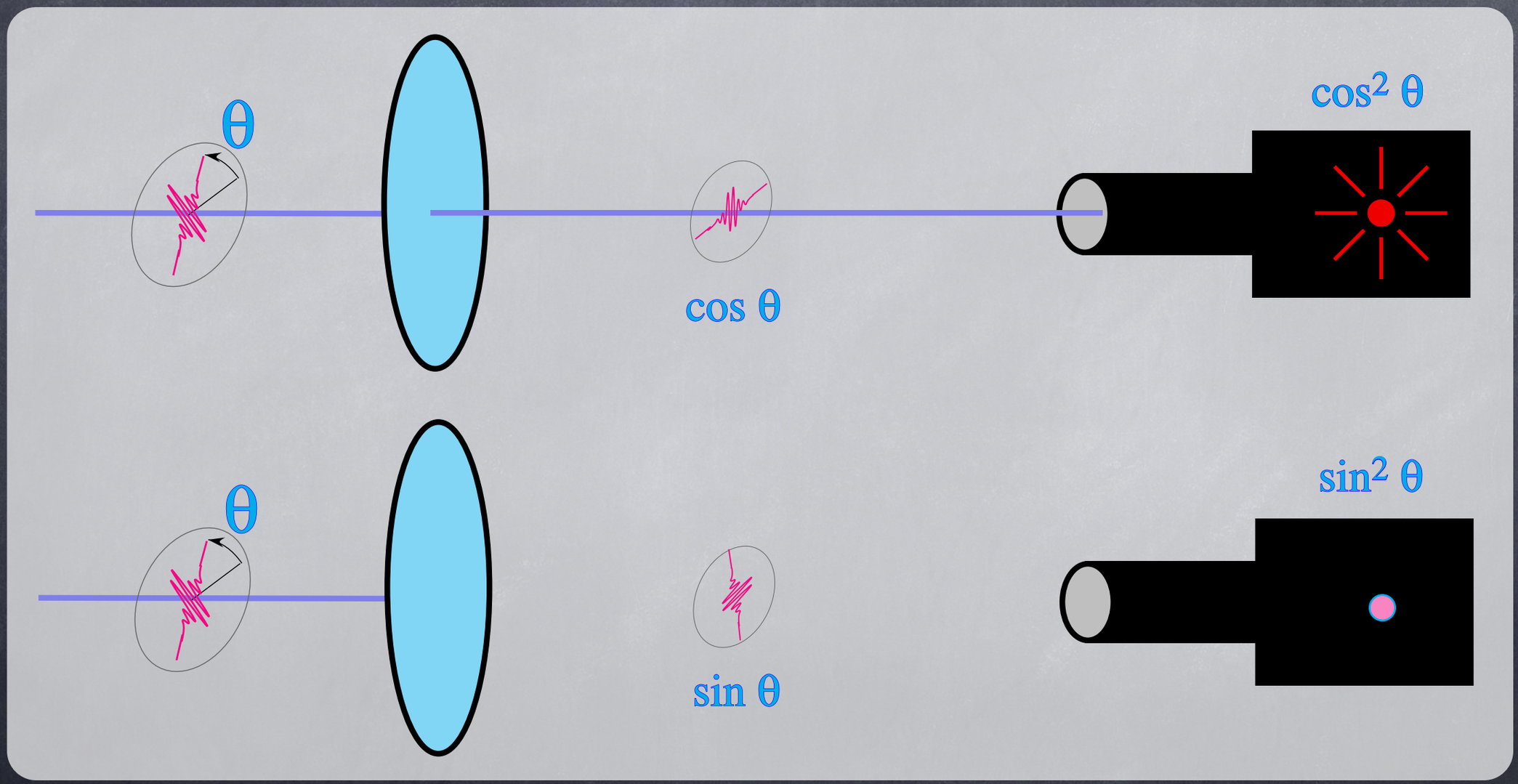
Photo Multipliers



Polarizing Filter

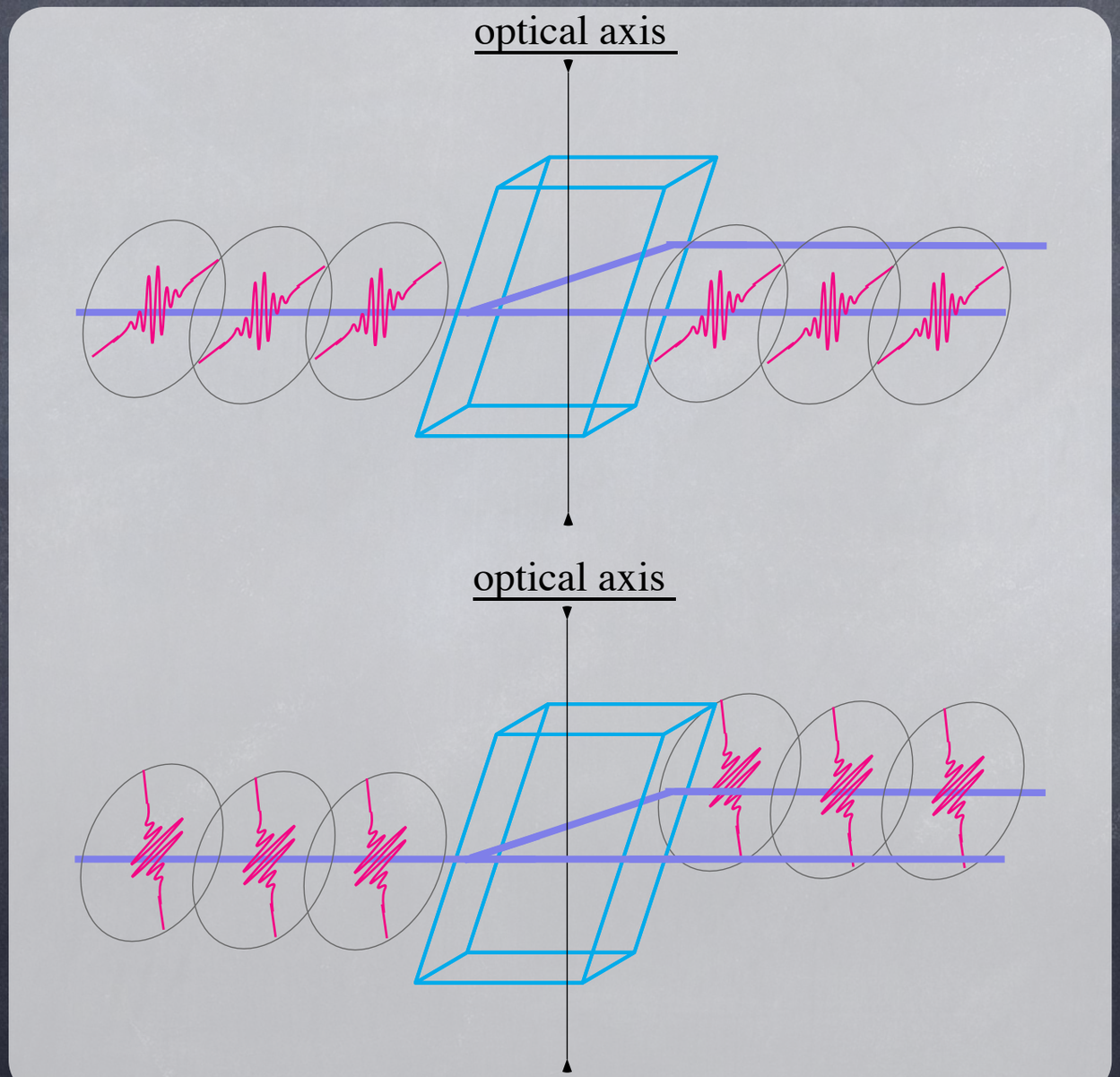


Polarizing Filter

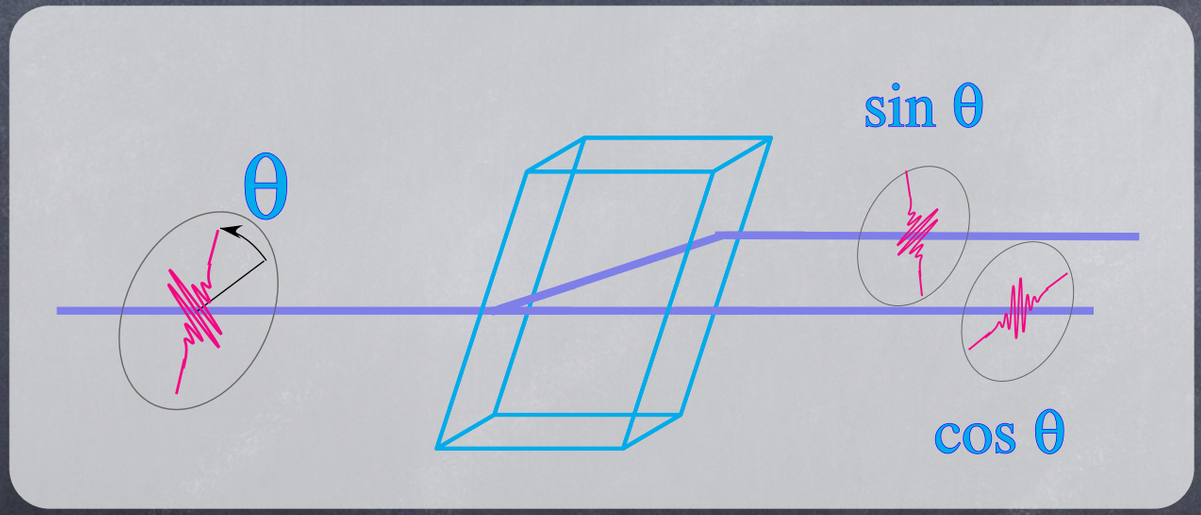


Photons

Calcite Crystal

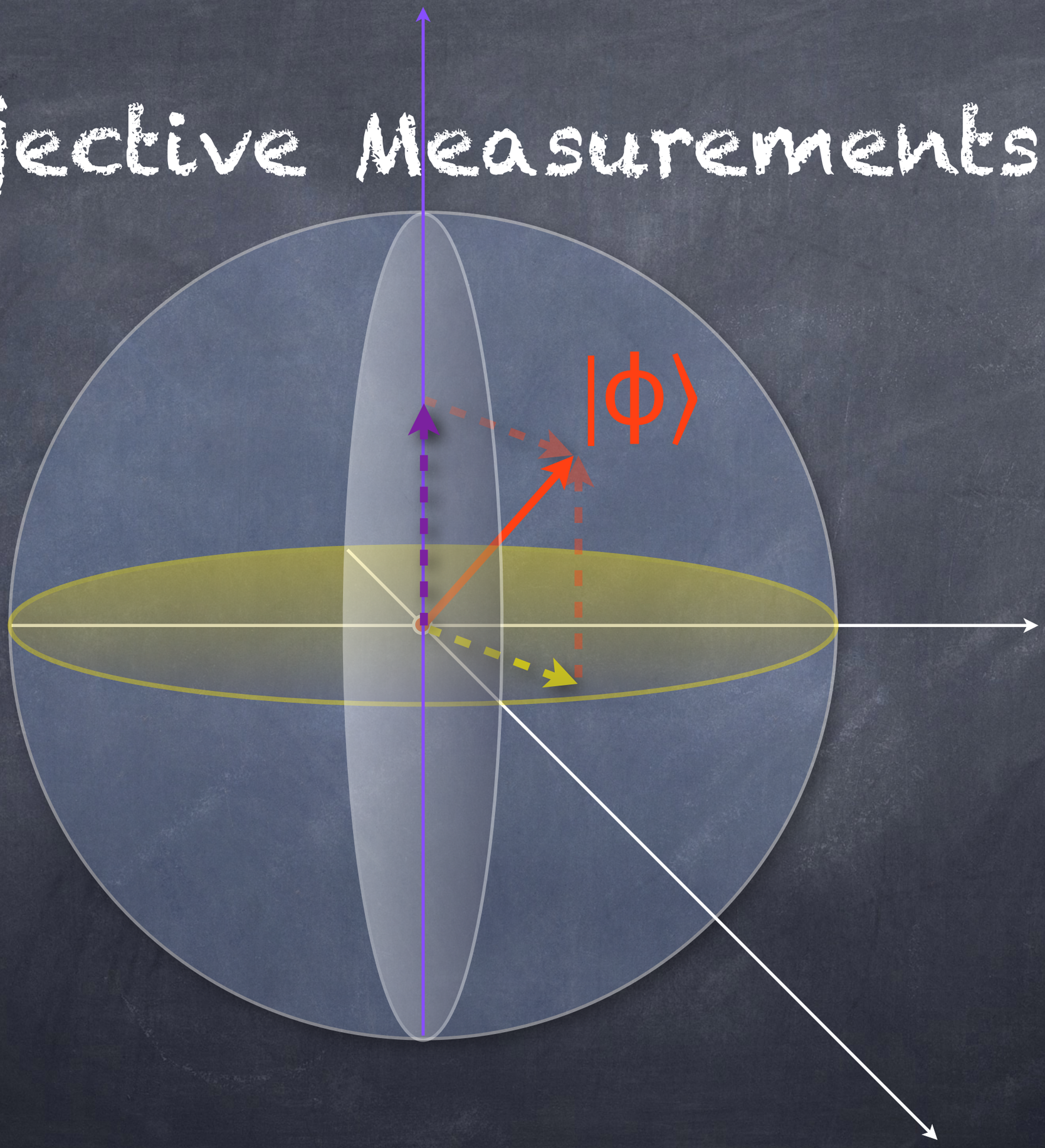


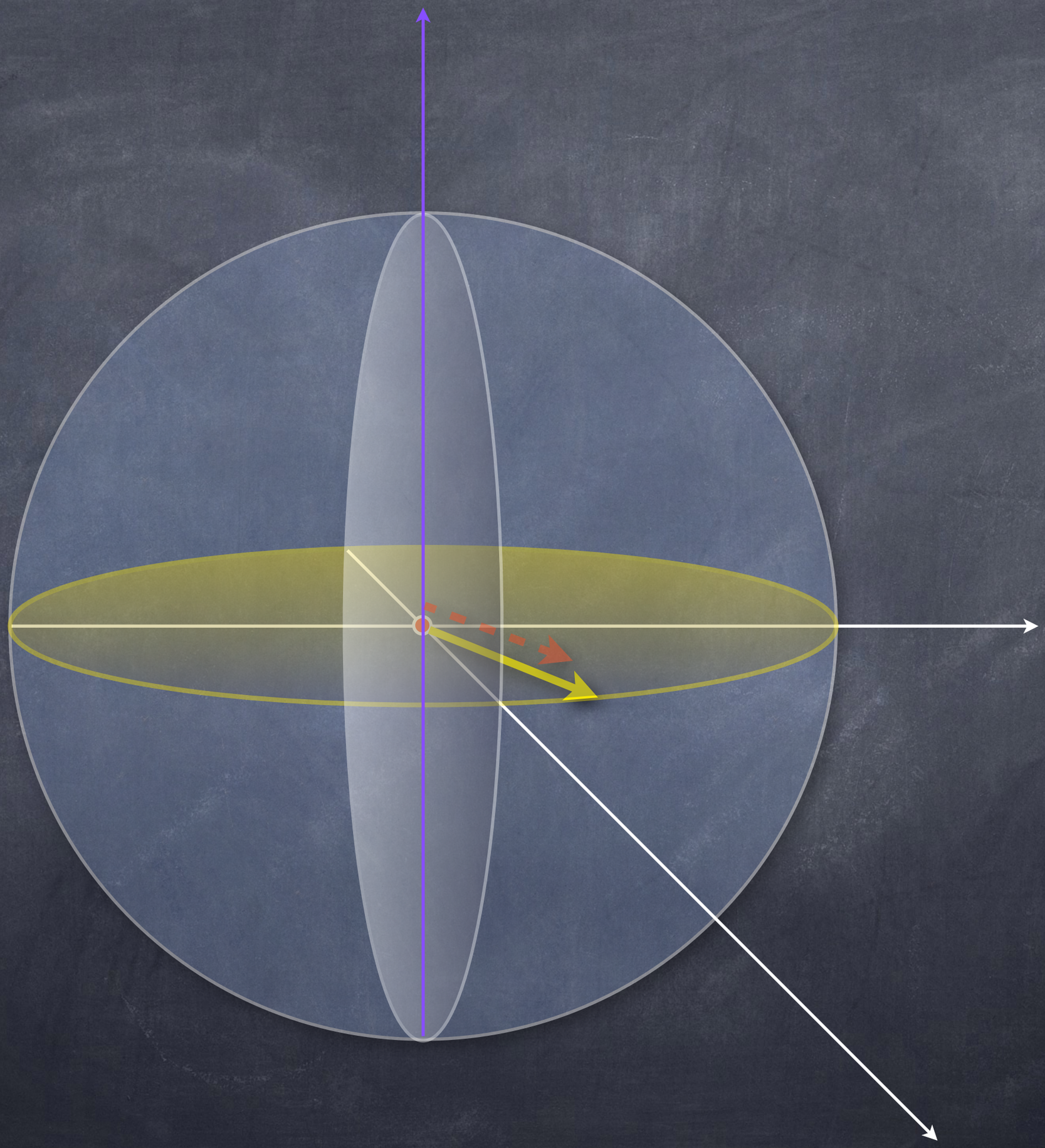
Calcite Crystal

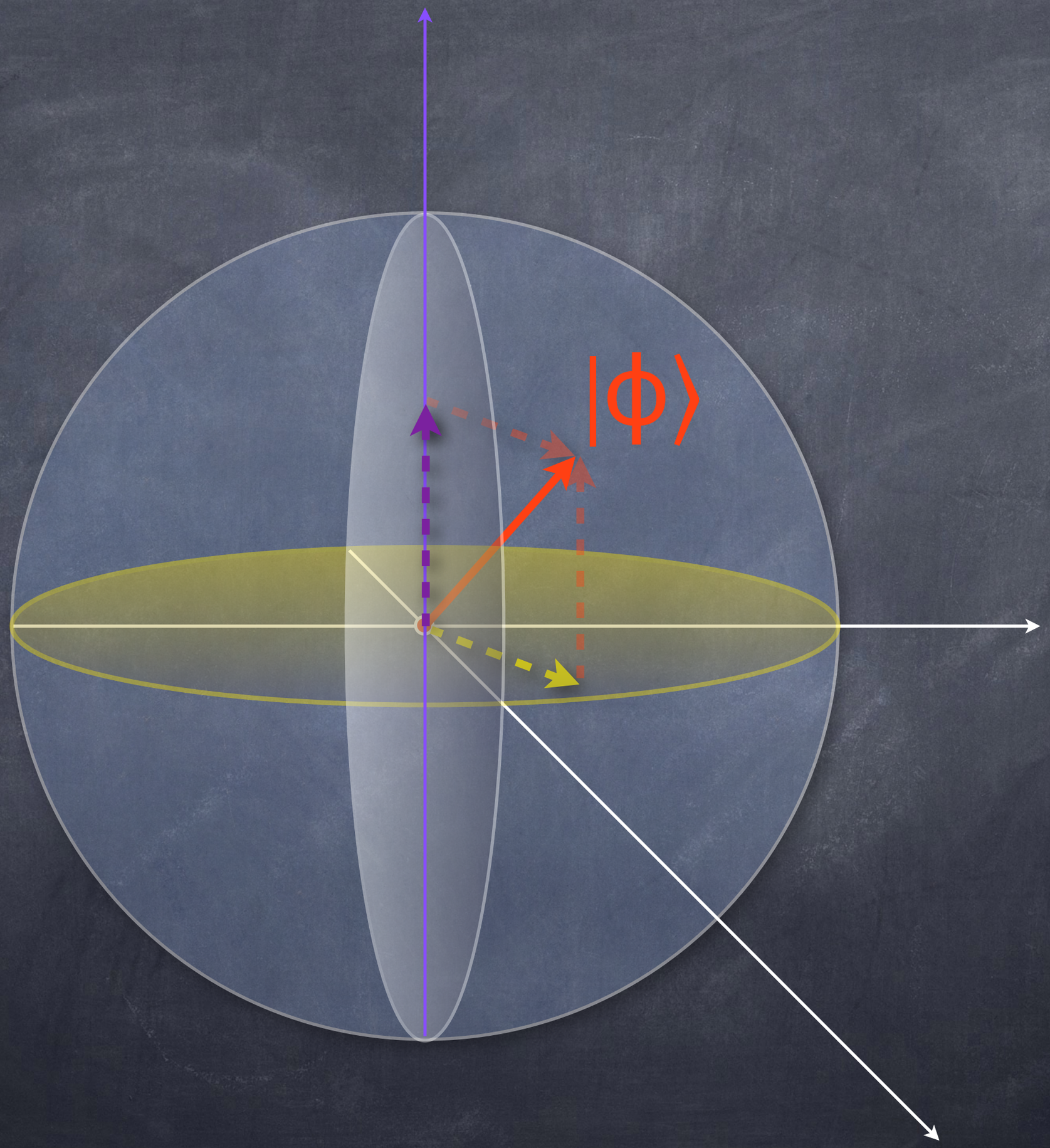


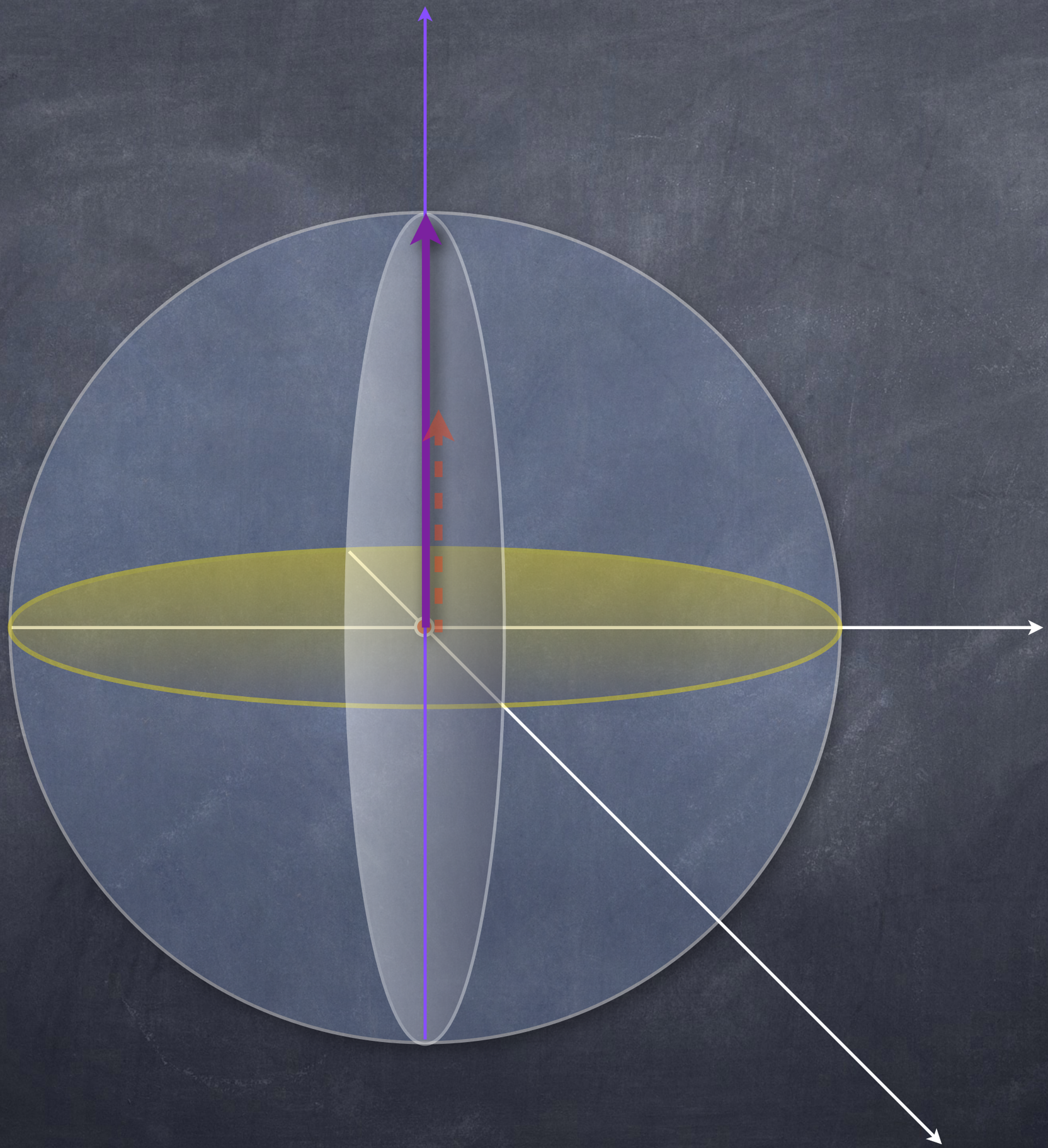
Photons

Projective Measurements





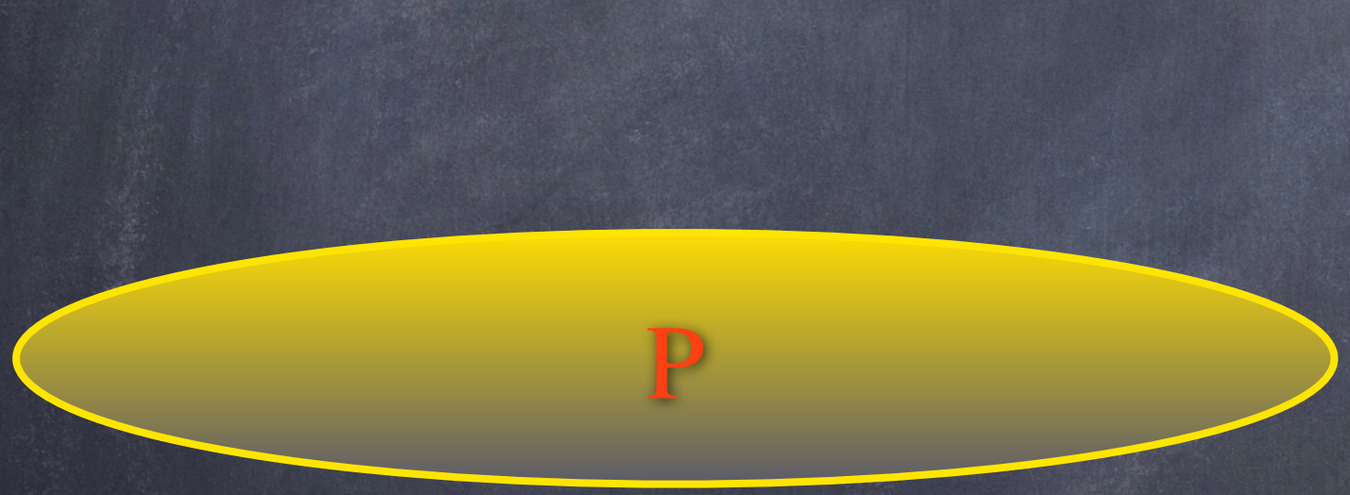

$|\phi\rangle$

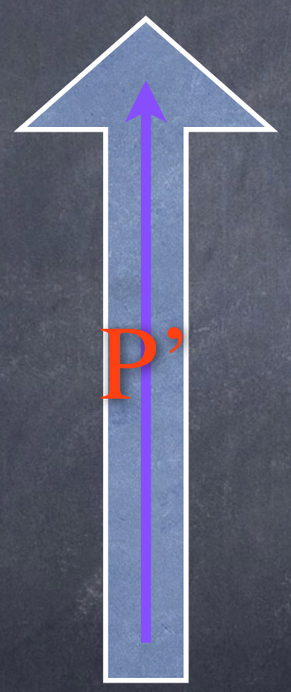


Notations

Projector: (state) $P_\psi = |\psi\rangle\langle\psi|$

(space) $P = \sum P_i$ where $P_i P_{i'} = \delta_{i,i'} P_i$





Notations

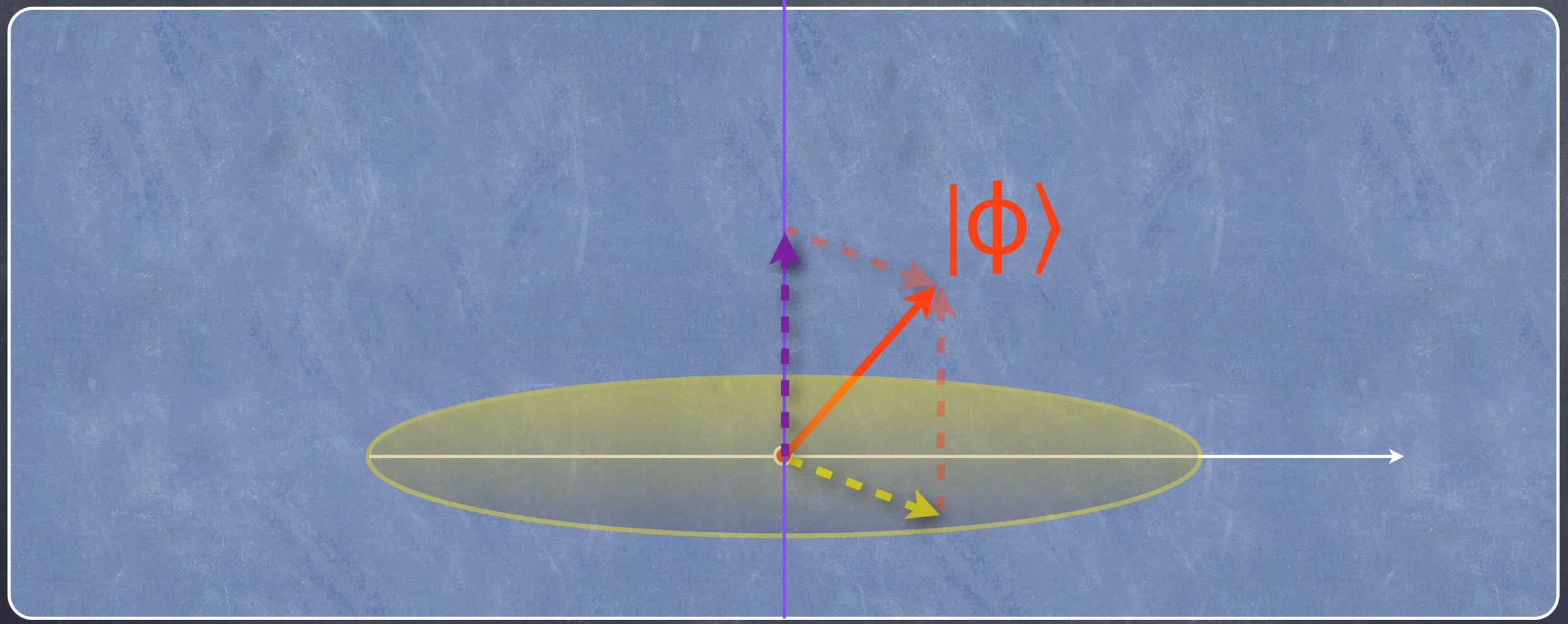
Projector: (state) $P_\psi = |\psi\rangle\langle\psi|$

(space) $P = \Sigma P_i$ where $P_i P_{i'} = \delta_{i,i'} P_i$

Measurement: $\{ P_m \}$

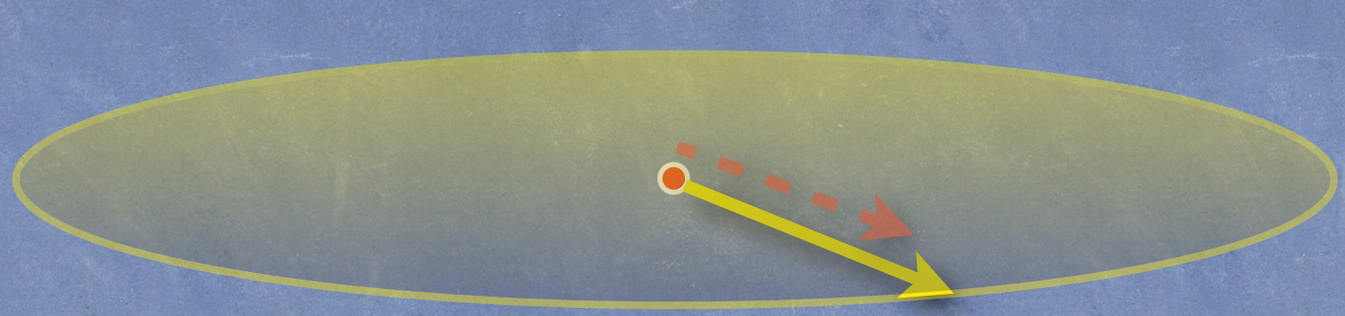
$$\Sigma P_m = I, \quad P_m P_{m'} = \delta_{m,m'} P_m$$

Notations



Measuring: $\Pr[m]=\langle\phi|P_m|\phi\rangle$

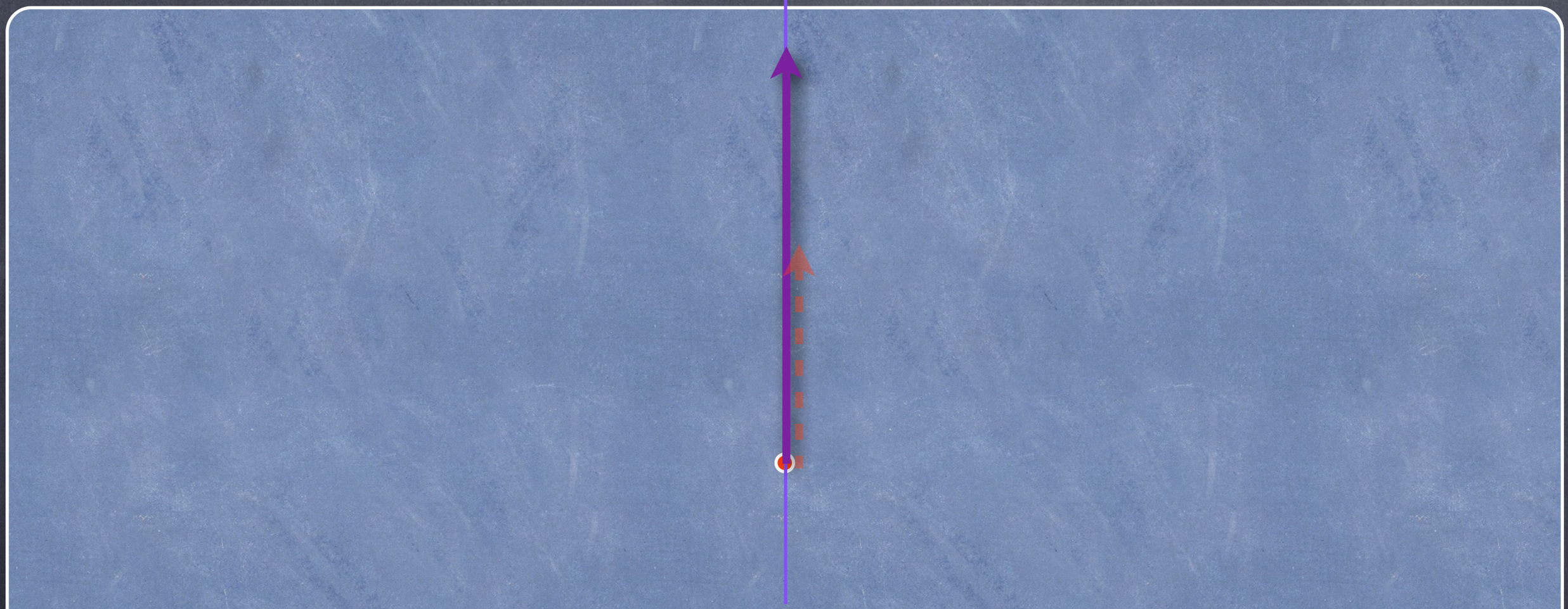
Notations



Measuring: $\Pr[m]=\langle\phi|P_m|\phi\rangle$

Resulting: $P_m|\phi\rangle/\sqrt{\Pr[m]}$

Notations



Measuring: $\Pr[m]=\langle\phi|P_m|\phi\rangle$

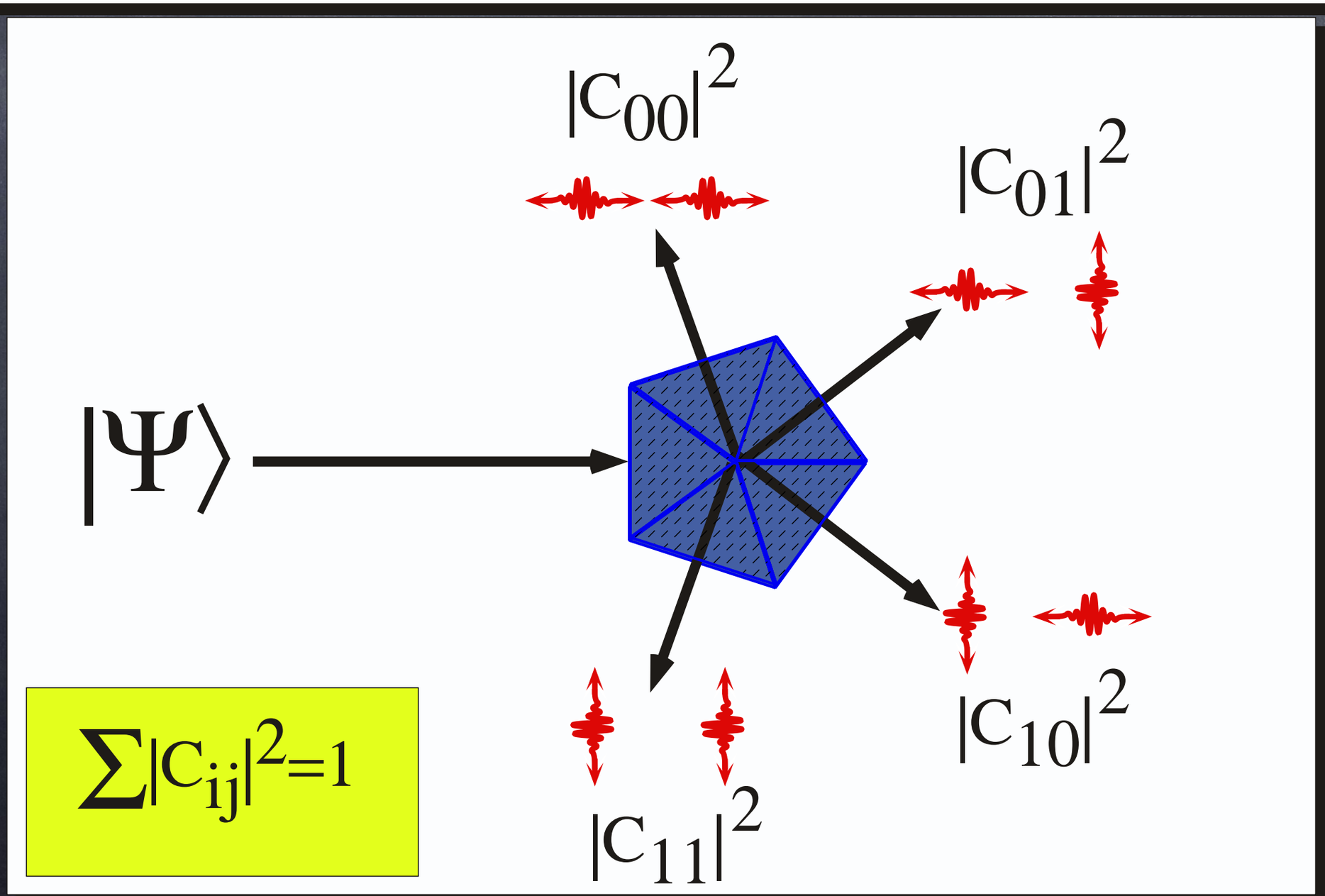
Resulting: $P_m|\phi\rangle/\sqrt{\Pr[m]}$

Projective Measurements

$$|\Psi\rangle = C_{00} \; + \; C_{01} \; + \; C_{10} \; + \; C_{11}$$

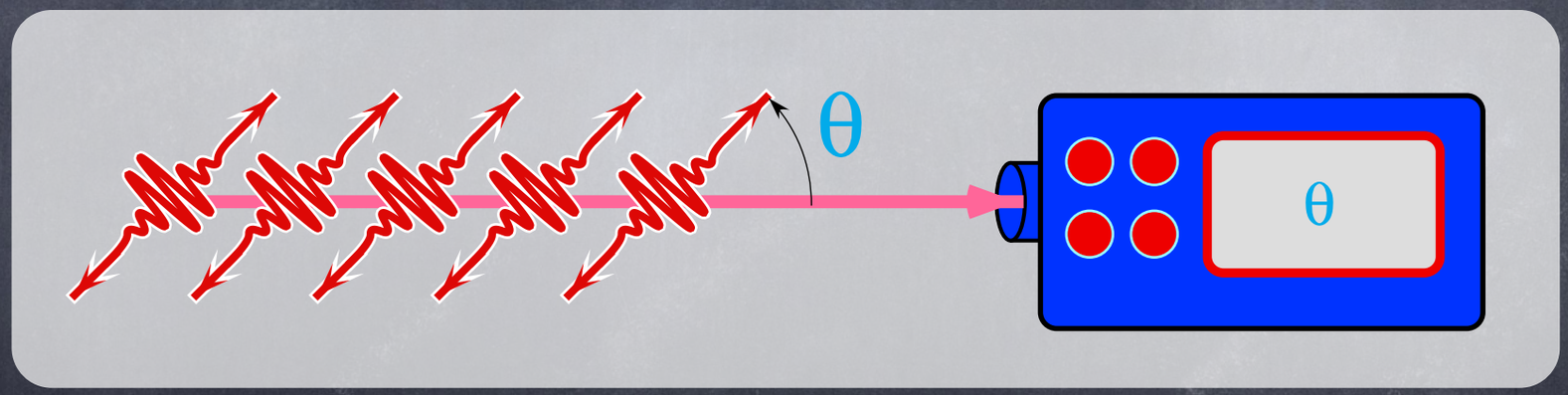
Projective Measurements

$$|\Psi\rangle = C_{00} + C_{01} + C_{10} + C_{11}$$

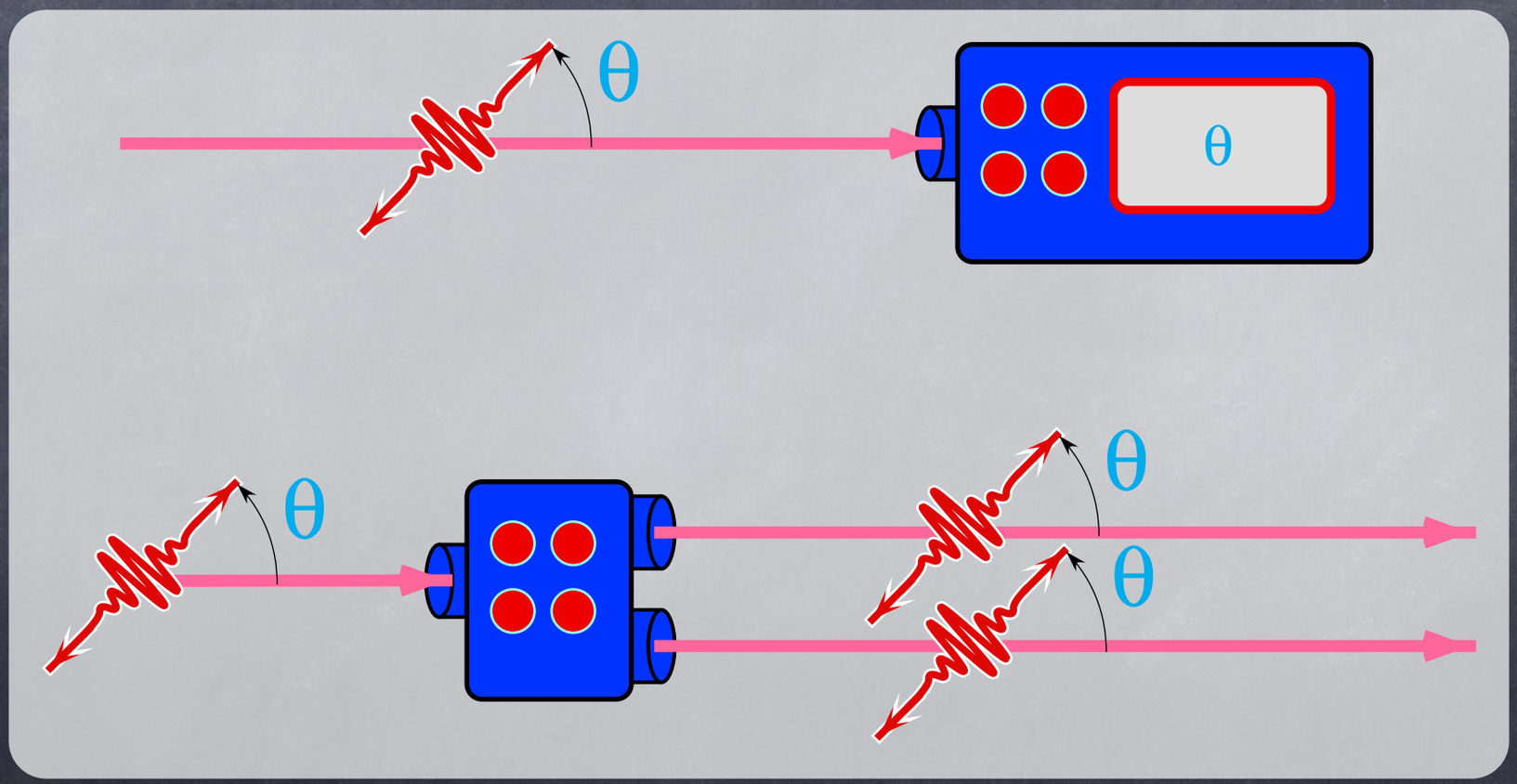


$$\sum |C_{ij}|^2 = 1$$

Possible



Impossible

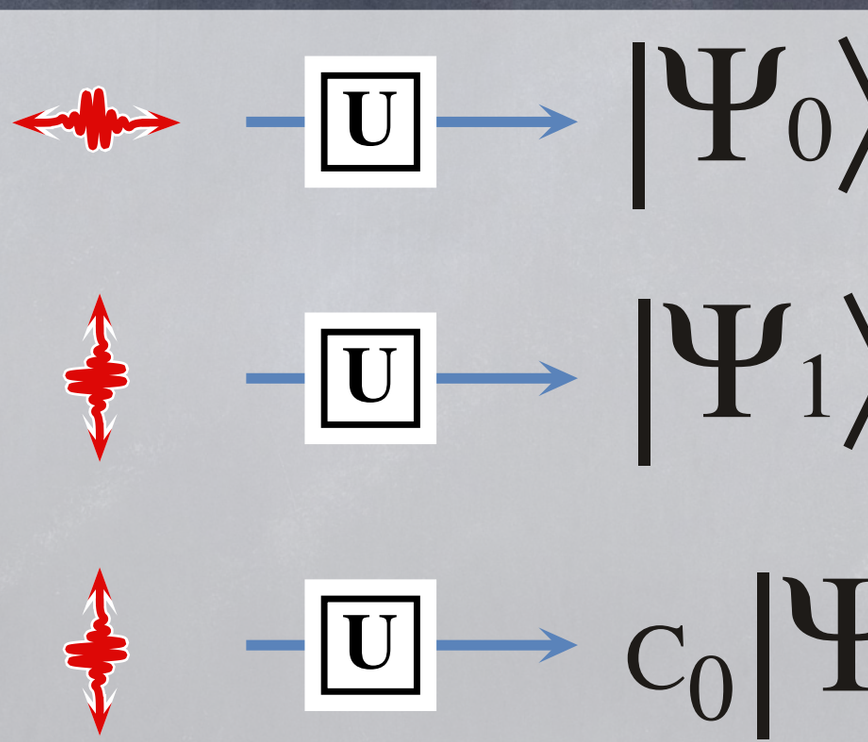


(3)

Quantum Computations

Unitary Operators

$$|\Psi\rangle \xrightarrow{U} |\Psi'\rangle$$



Notations

Unitary Operators: $U^{\dagger}U=UU^{\dagger}=I$

Notations

Unitary Operators: $U^\dagger U = U U^\dagger = I$

linear: $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$

Notations

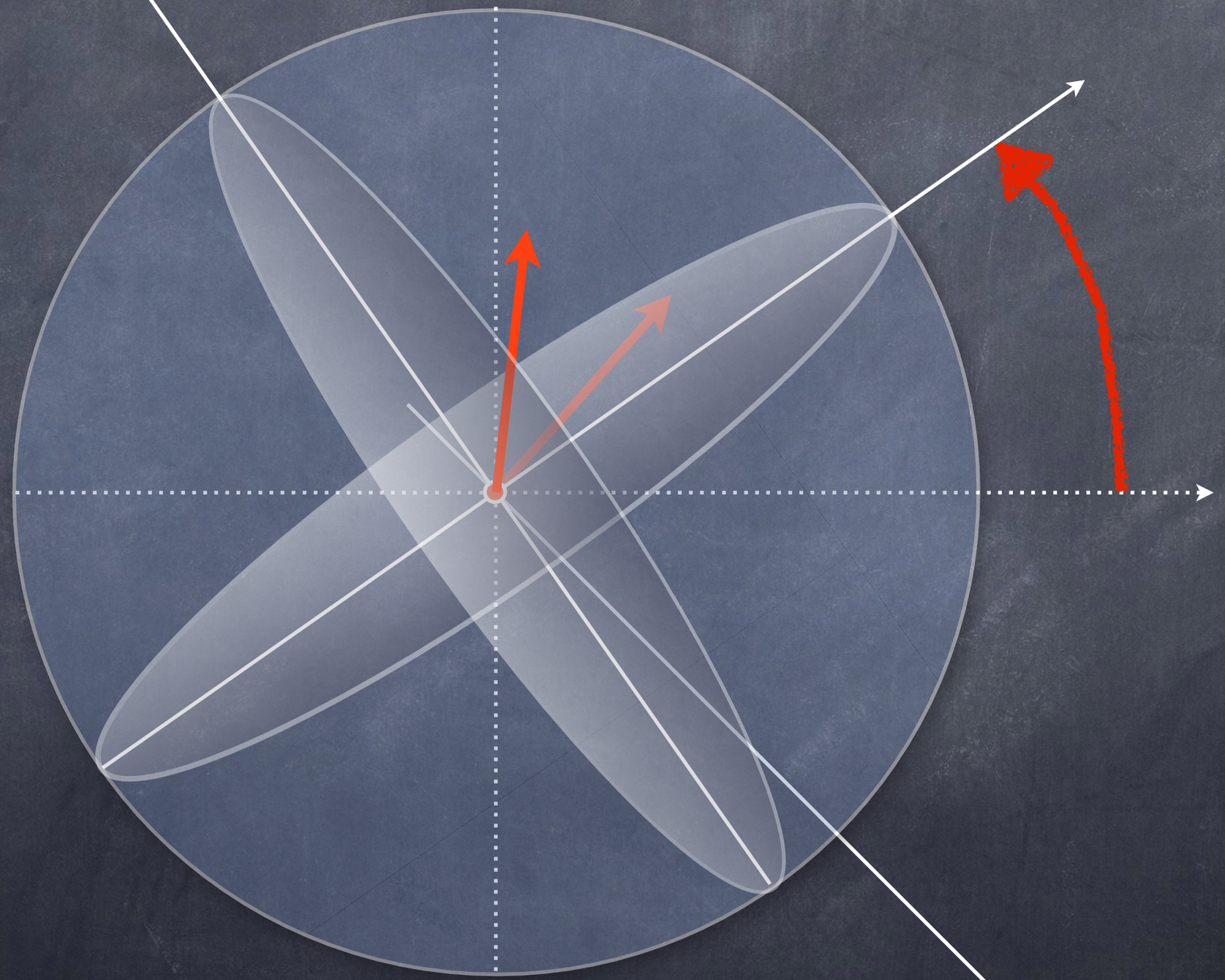
Unitary Operators: $U^\dagger U = U U^\dagger = I$

linear: $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$

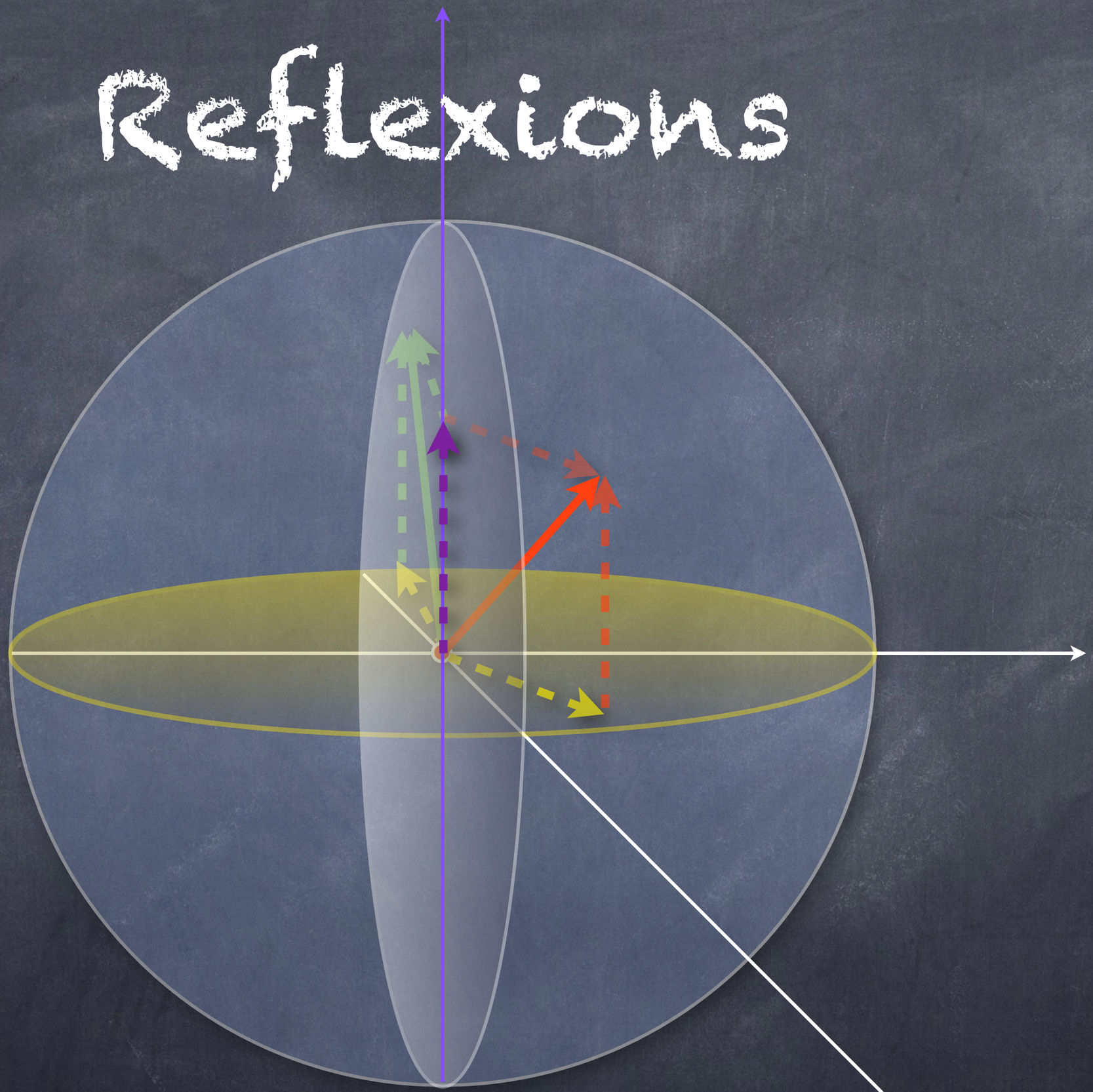
preserves scalar products:

$$(\langle\psi|U^\dagger)(U|\phi\rangle)$$
$$= \langle\psi|U^\dagger U|\phi\rangle = \langle\psi|I|\phi\rangle = \langle\psi|\phi\rangle$$

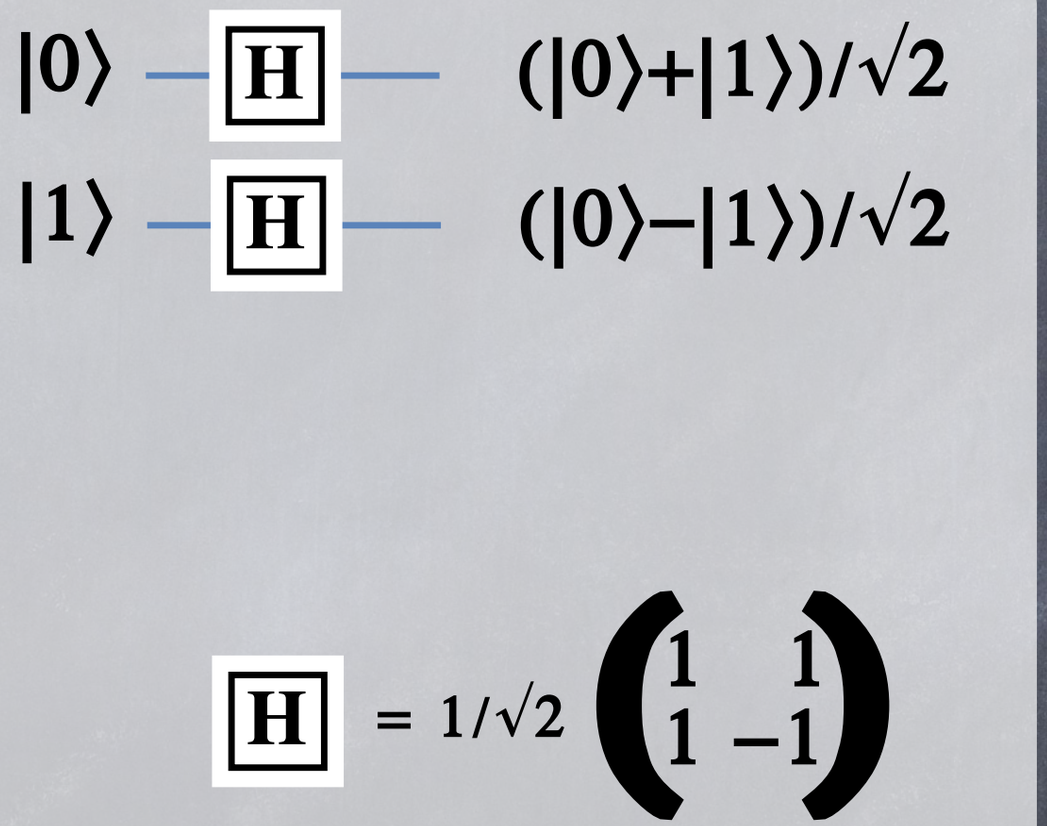
Rotations



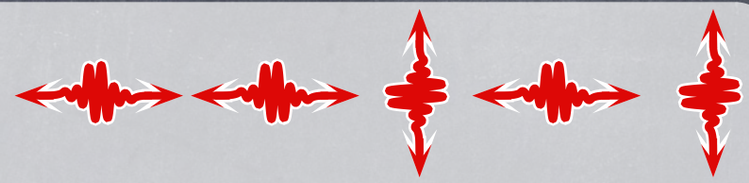
Reflexions



Example: Hadamard

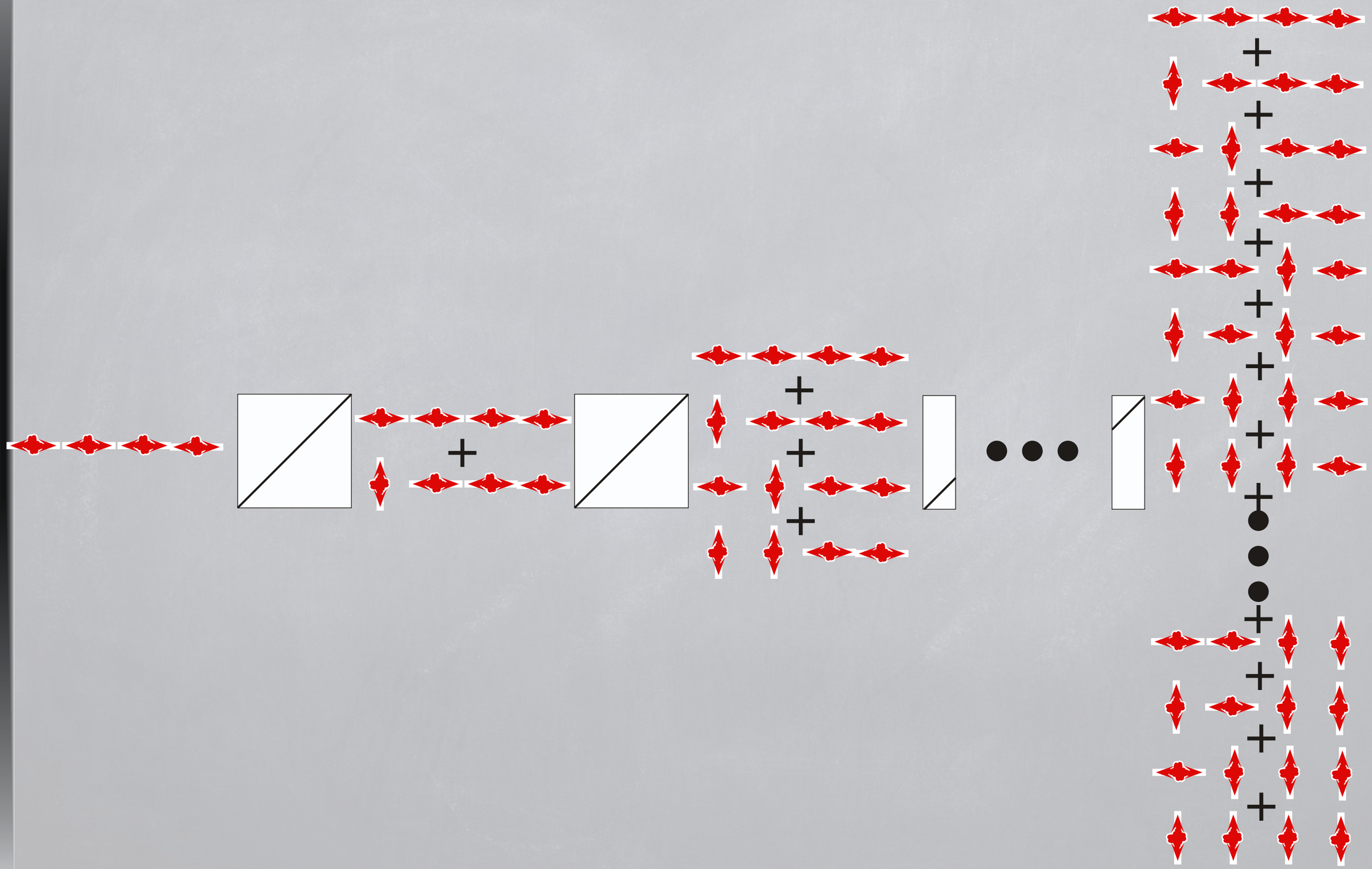


Classical vs Quantum

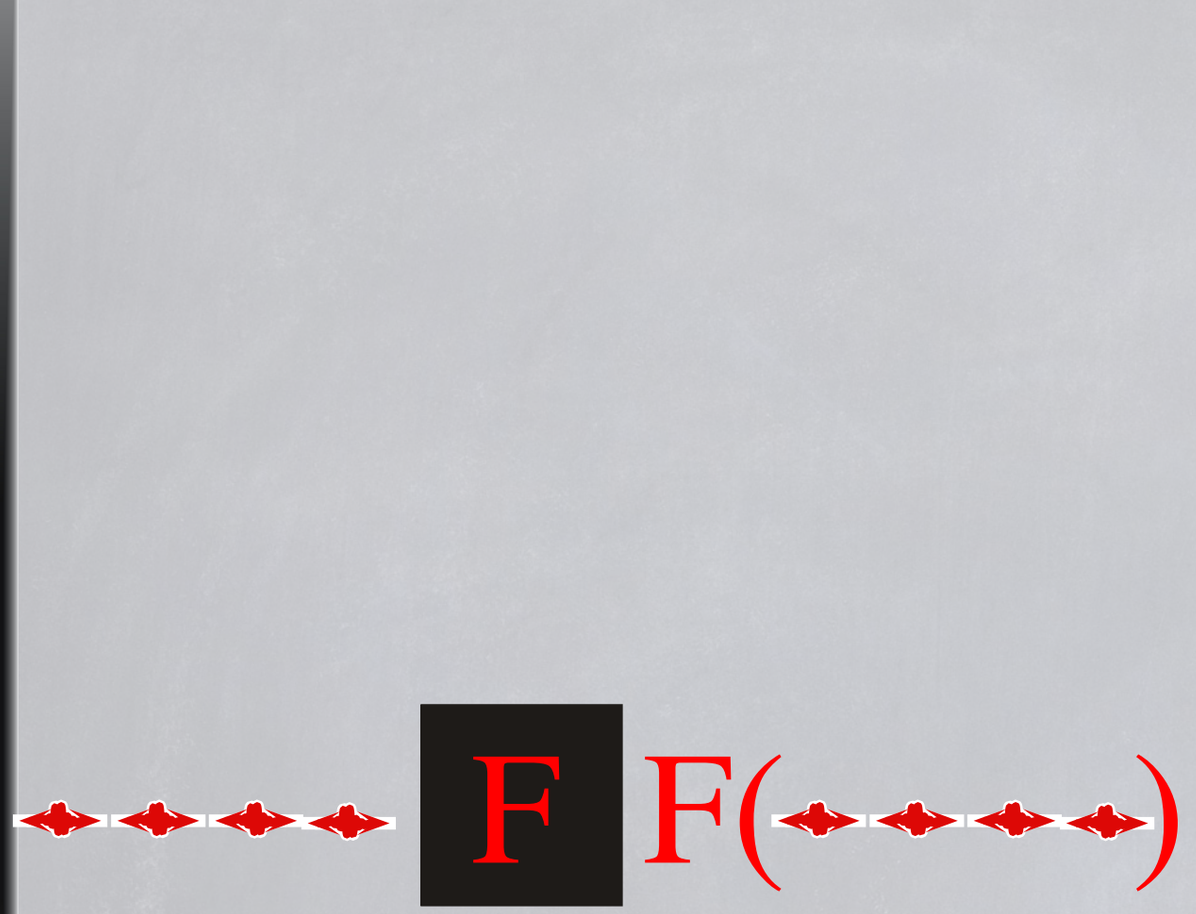
0011011110001l0 Classical	Quantum 
Copying: Yes	NO
Measuring: Yes	partial
Broadcasting: Yes	NO
Superposing: NO	Yes
Interfering: NO	Yes

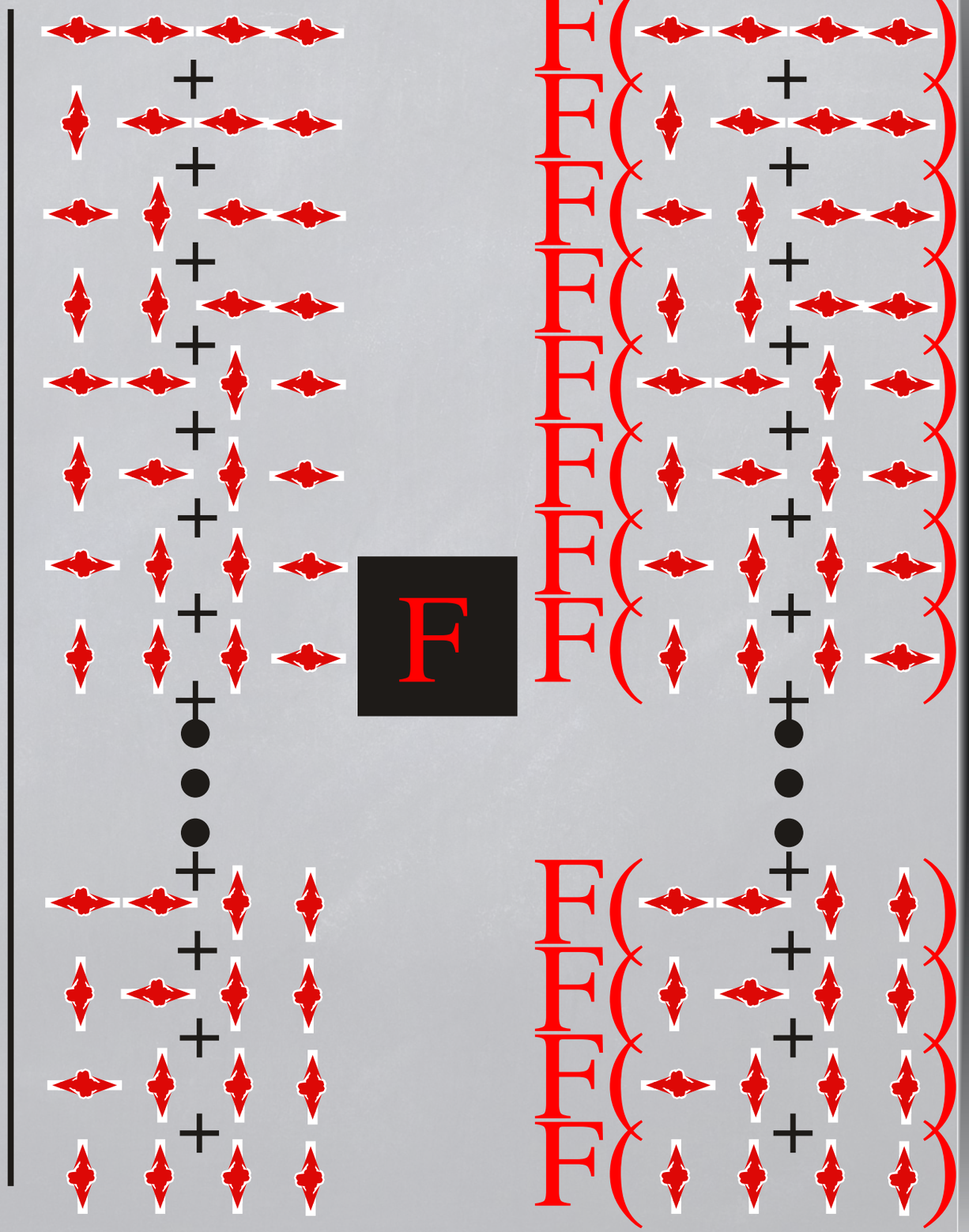
(6)
Quantum Factoring

Quantum Superposition



Quantum Superposition





Quantum Factoring

Given $n=pq$ and $\phi(n)=(p-1)(q-1)$

it is easy to find p and q because

$\phi(n)=(p-1)(q-1)=pq-p-q+1=n-p-(n/p)+1$

$p+(n/p)+n-\phi(n)+1=0$

$p^2+(n-\phi(n)+1)p+n=0$ has solutions:

$p=(-b\pm\sqrt{4ac})/2a \quad (a=1,\ b=n-\phi(n)+1,\ c=n)$

Quantum Factoring

Euler's theorem

$$a^{\phi(n)} \bmod n = 1$$

$$F(a,r,n) := (a^r \bmod n, r, n)$$

$$F(a,r,n) := (\circlearrowright, r, n)$$

$$F(a,k\phi(n),n) := (\circlearrowright, k\phi(n), n)$$

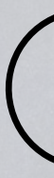
Quantum Factoring

$F(a,r,n):=(a^r \bmod n,r,n)$

$F(a_1,r,n):=($  $,r,n)$

$F(a_2,r,n):=($  $,r,n)$

...

$F(a_i,r,n):=($  $,r,n)$

but .

$F(a_1,k\phi(n),n):=($  $,k\phi(n),n)$

$F(a_2,k\phi(n),n):=($  $,k\phi(n),n)$

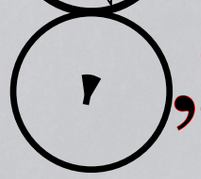
...

$F(a_i,k\phi(n),n):=($  $,k\phi(n),n)$

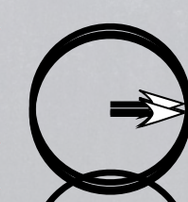
Quantum Factoring

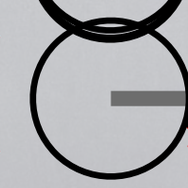
$F(a,r,n):=(a^r \bmod n,r,n)$

$F(*,r,n):=($  $,r,n)$

. $=($  $,r,n)$

but .

$F(*,k\phi(n),n):=($  $,k\phi(n),n)$

$F(*,k\phi(n),n):=($  $,k\phi(n),n)$

Quantum Factoring

(,1,n)

(,2,n)

(,3,n)

...

(,ϕ(n)-1,n)

(,ϕ(n),n)

(,ϕ(n)+1,n)

...

(,kϕ(n),n)

(,ϕ(n)+1,n)

...

Quantum Factoring

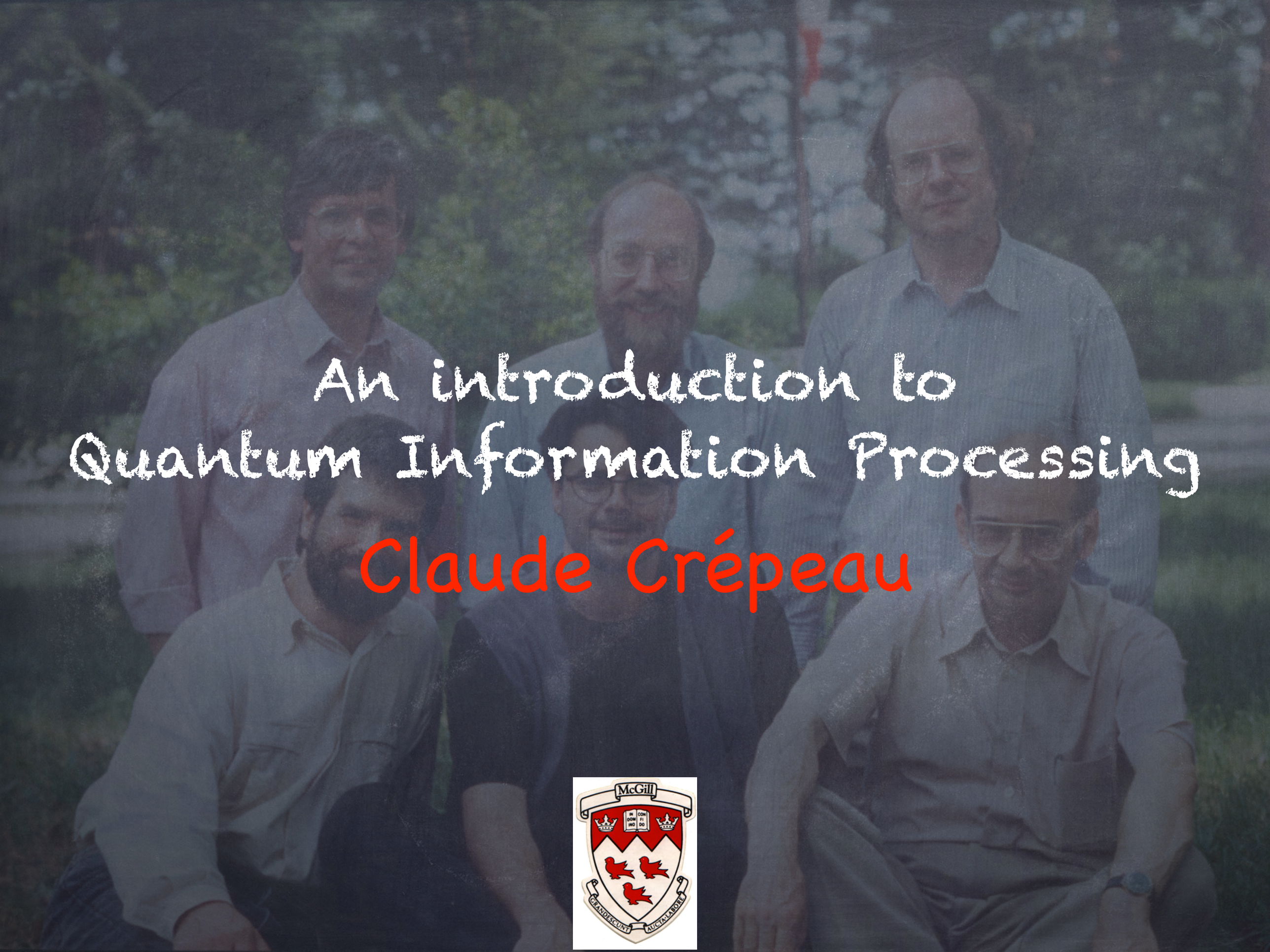
Quantum Factoring

Construct the superposition
for all r and all a of

$(a^r \bmod n, r, n)$

measure r, and with high
probability $r = k\phi(n)$
for some integer k

repeat to obtain $r' = k'\phi(n)$
$\gcd(r,r') = \phi(n)$.



An introduction to Quantum Information Processing

Claude Crépeau