

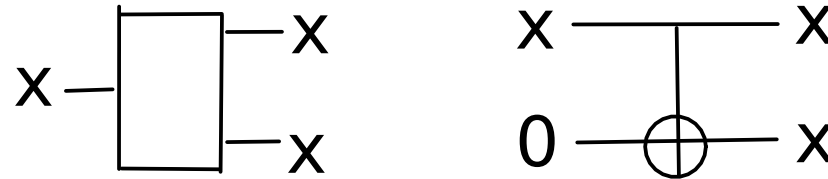
4. Immediate information processing consequences of QM

i.e., more examples of QM :)

- (a) No-cloning theorem (NC 1.3.5, box 12.1)
- (b) Non-distinguishability of non-orthogonal states
(NC p56-57)
- (c) Communication of data
 - protocols, bounds, and non-signalling principle
 - encoding and extraction of classical data in QM
- (d) Superdense coding and teleportation
(NC 2.3, 1.3.7, KLM 5.1-5.2, M 6.4-6.5)
- (e) Bell's inequality and nonlocal games (NC 2.6, M 6.6)

The no-cloning theorem

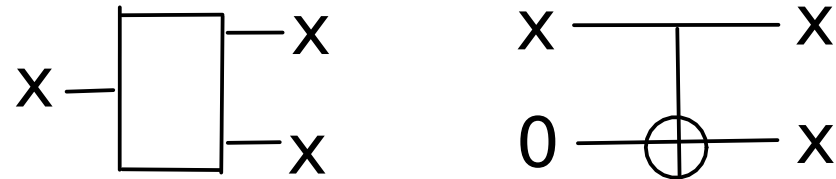
An arbitrary unknown bit x can be "cloned," say, by one use of the FANOUT or the CNOT :



Can we clone an arbitrary unknown qubit $a|0\rangle + b|1\rangle$?

/
definition pending
basically from one
copy we get two ...

An arbitrary unknown bit x can be "cloned," say, by one use of the FANOUT or the CNOT :



Can we clone an arbitrary unknown qubit $a|0\rangle + b|1\rangle$?

FANOUT does not preserve dimension, and not unitary.

An arbitrary unknown bit x can be "cloned," say, by one use of the FANOUT or the CNOT :



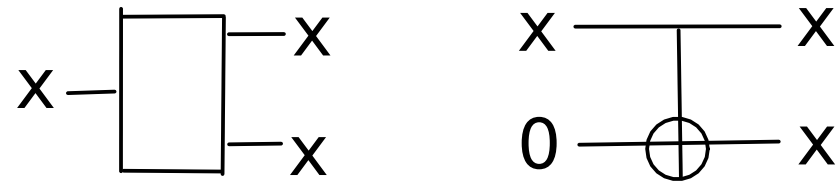
Can we clone an arbitrary unknown qubit $a|0\rangle + b|1\rangle$?

FANOUT does not preserve dimension, and not unitary.

CNOT takes $|0\rangle$ to $|0\rangle|0\rangle$, $|1\rangle$ to $|1\rangle|1\rangle$.

By linearity, CNOT takes $a|0\rangle + b|1\rangle$ to $a|00\rangle + b|11\rangle$,

An arbitrary unknown bit x can be "cloned," say, by one use of the FANOUT or the CNOT :



Can we clone an arbitrary unknown qubit $a|0\rangle + b|1\rangle$?

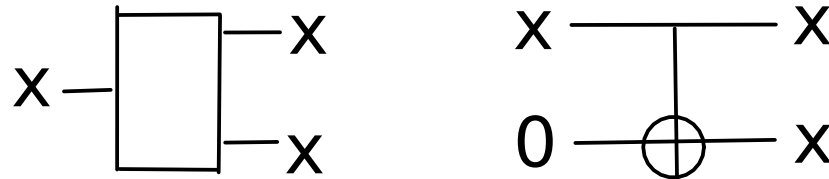
FANOUT does not preserve dimension, and not unitary.

CNOT takes $|0\rangle$ to $|0\rangle|0\rangle$, $|1\rangle$ to $|1\rangle|1\rangle$.

By linearity, CNOT takes $a|0\rangle + b|1\rangle$ to $a|00\rangle + b|11\rangle$,
 which is not $(a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle)$ if $ab \neq 0$.

Note: when $ab = 0$, we have classical bits !

An arbitrary unknown bit x can be "cloned," say, by one use of the FANOUT or the CNOT :



Can we clone an arbitrary unknown qubit $a|0\rangle + b|1\rangle$?

FANOUT does not preserve dimension, and not unitary.

CNOT takes $|0\rangle$ to $|0\rangle|0\rangle$, $|1\rangle$ to $|1\rangle|1\rangle$.

By linearity, CNOT takes $a|0\rangle + b|1\rangle$ to $a|00\rangle + b|11\rangle$,
 which is not $(a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle)$ if $ab \neq 0$.

Did we miss a better method / circuit ?

Is there something fundamentally wrong with cloning ?

No-cloning theorem:

There is no valid unitary taking
an arbitrary $|\psi\rangle$ and some ancilla
to $|\psi\rangle|\psi\rangle$ and some other state.

No-cloning theorem:

There is no valid unitary taking
an arbitrary $|\psi\rangle$ and some ancilla
to $|\psi\rangle|\psi\rangle$ and some other state.

indep of $|\psi\rangle$ else
cheated by starting
with more than 1
copy of $|\psi\rangle$

can depend on $|\psi\rangle$

No-cloning theorem:

There is no valid unitary taking
an arbitrary $|\psi\rangle$ and some ancilla
to $|\psi\rangle|\psi\rangle$ and some other state.

indep of $|\psi\rangle$ else
cheated by starting
with more than 1
copy of $|\psi\rangle$

can depend on $|\psi\rangle$

Proof: suppose such a unitary U exists.

The plan is to prove by contradiction:
assume the opposite of what we want to prove
and obtain a contradiction.

No-cloning theorem:

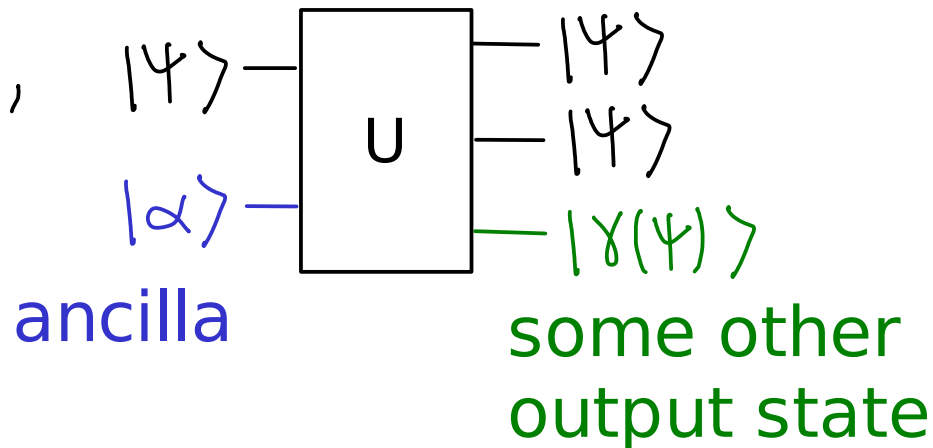
There is no valid unitary taking an arbitrary $|\psi\rangle$ and some ancilla to $|\psi\rangle|\psi\rangle$ and some other state.

indep of $|\psi\rangle$ else
cheated by starting
with more than 1
copy of $|\psi\rangle$

can depend on $|\psi\rangle$

Proof: suppose such a unitary U exists.

So, $\forall |\psi\rangle,$



$$\begin{aligned} & \dim \text{ of } |\alpha\rangle \\ &= \dim \text{ of } |\psi\rangle \\ & \times \dim \text{ of } |\gamma(\psi)\rangle \end{aligned}$$

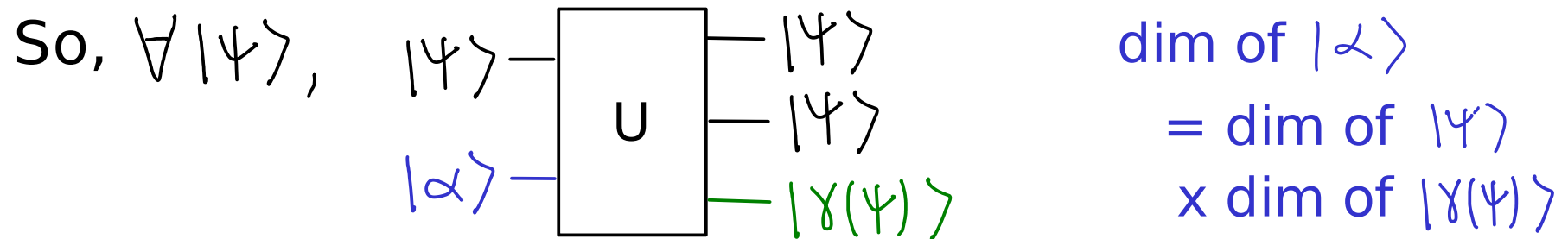
No-cloning theorem:

There is no valid unitary taking an **arbitrary** $|\psi\rangle$ and some ancilla to $|\psi\rangle|\psi\rangle$ and some other state.

indep of $|\psi\rangle$ else cheated by starting with more than 1 copy of $|\psi\rangle$

can depend on $|\psi\rangle$

Proof: suppose such a unitary U exists.



Apply to $|\psi_1\rangle, |\psi_2\rangle$, non-orthogonal with $|\langle\psi_1|\psi_2\rangle| < 1$

$$U(|\psi_1\rangle|\alpha\rangle) = |\psi_1\rangle|\psi_1\rangle|\gamma_1(\psi_1)\rangle$$

$$U(|\psi_2\rangle|\alpha\rangle) = |\psi_2\rangle|\psi_2\rangle|\gamma_2(\psi_2)\rangle$$

same $|\alpha\rangle$

states are "distinct"

Equating the inner products:

$$\left(\langle \psi_1 | \langle \alpha | U^\dagger \right) \left(U | \psi_2 \rangle | \alpha \rangle \right) = \left(\langle \psi_1 | \langle \psi_1 | \langle \gamma_1(\psi_1) | \right) \left(| \psi_2 \rangle | \psi_2 \rangle | \gamma_2(\psi_2) \rangle \right)$$

cancels out

$$U \left(| \psi_1 \rangle | \alpha \rangle \right) = | \psi_1 \rangle | \psi_1 \rangle | \gamma_1(\psi_1) \rangle$$

$$U \left(| \psi_2 \rangle | \alpha \rangle \right) = | \psi_2 \rangle | \psi_2 \rangle | \gamma_2(\psi_2) \rangle$$

|
same $|\alpha\rangle$

Equating the inner products:

$$\left(\langle \psi_1 | \langle \alpha | \underbrace{U^\dagger}_{\text{cancels out}} (U | \psi_2 \rangle | \alpha \rangle) \right) = \left(\langle \psi_1 | \langle \psi_1 | \langle \gamma_1(\psi_1) | \right) (| \psi_2 \rangle | \psi_2 \rangle | \gamma_2(\psi_2) \rangle)$$

Note: $(\langle a | \otimes \langle b |) (| c \rangle \otimes | d \rangle) = \langle a | c \rangle \langle b | d \rangle$

So: $\langle \psi_1 | \psi_2 \rangle \langle \alpha | \alpha \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle \langle \gamma_1(\psi_1) | \gamma_2(\psi_2) \rangle$

Equating the inner products:

$$\left(\langle \psi_1 | \langle \alpha | U^\dagger \right) \left(U | \psi_2 \rangle | \alpha \rangle \right) = \left(\langle \psi_1 | \langle \psi_1 | \langle \gamma_1(\psi_1) | \right) \left(| \psi_2 \rangle | \psi_2 \rangle | \gamma_2(\psi_2) \rangle \right)$$

cancels out

Note: $(\langle a | \otimes \langle b |) (| c \rangle \otimes | d \rangle) = \langle a | c \rangle \langle b | d \rangle$

So: $\langle \psi_1 | \psi_2 \rangle \langle \alpha | \alpha \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle \langle \gamma_1(\psi_1) | \gamma_2(\psi_2) \rangle$

$$\langle \psi_1 | \psi_2 \rangle \left(1 - \langle \psi_1 | \psi_2 \rangle \langle \gamma_1(\psi_1) | \gamma_2(\psi_2) \rangle \right) = 0$$

Equating the inner products:

$$\left(\langle \psi_1 | \langle \alpha | \underbrace{U^\dagger}_{\text{cancels out}} (U | \psi_2 \rangle | \alpha \rangle \right) = \left(\langle \psi_1 | \langle \psi_1 | \langle \gamma_1(\psi_1) | \right) (| \psi_2 \rangle | \psi_2 \rangle | \gamma_2(\psi_2) \rangle)$$

Note: $(\langle a | \otimes \langle b |) (| c \rangle \otimes | d \rangle) = \langle a | c \rangle \langle b | d \rangle$

So: $\langle \psi_1 | \psi_2 \rangle \langle \alpha | \alpha \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle \langle \gamma_1(\psi_1) | \gamma_2(\psi_2) \rangle$

$$\underline{\langle \psi_1 | \psi_2 \rangle} \left(1 - \underline{\langle \psi_1 | \psi_2 \rangle} \langle \gamma_1(\psi_1) | \gamma_2(\psi_2) \rangle \right) = 0$$

(i) $\langle \psi_1 | \psi_2 \rangle \neq 0$

(ii) $|\langle \psi_1 | \psi_2 \rangle| < 1$

$$\therefore |\langle \gamma_1(\psi_1) | \gamma_2(\psi_2) \rangle| \leq 1$$

$$\langle \psi_1 | \psi_2 \rangle \langle \gamma_1(\psi_1) | \gamma_2(\psi_2) \rangle \neq 1$$

Contradiction!



Note: we can infer from the proof that we cannot clone one out of two possible "distinct", non-ortho quantum states.

The no-cloning theorem presents both challenges & opportunities in quantum information processing.

For example, techniques in classical information processing such as repetition coding, transcribing, rewinding/backtracking fail. (Researchers found methods to circumvent the difficulties).

The no-cloning theorem presents both challenges & opportunities in quantum information processing.

For example, techniques in classical information processing such as repetition coding, transcribing, rewinding/backtracking fail. (Researchers found methods to circumvent the difficulties).

It is also one component of earlier versions of the blackhole information paradox.

The no-cloning theorem presents both challenges & opportunities in quantum information processing.

For example, techniques in classical information processing such as repetition coding, transcribing, rewinding/backtracking fail. (Researchers found methods to circumvent the difficulties).

It is also one component of earlier versions of the blackhole information paradox.

Meanwhile, we are given new opportunities to perform secure QKD, key recycling etc. THESE ARE REALLY REALLY COOL !

4. Immediate information processing consequences of QM

i.e., more examples of QM :)

✓ (a) No-cloning theorem (NC 1.3.5, box 12.1)

→ (b) Non-distinguishability of non-orthogonal states
(NC p56-57)

(c) Communication of data

- protocols, bounds, and non-signalling principle
- encoding and extraction of classical data in QM

(d) Superdense coding and teleportation

(NC 2.3, 1.3.7, KLM 5.1-5.2, N 6.4-6.5)

(e) Bell's inequality and nonlocal games (NC 2.6, M 6.6)

Non-distinguishability of non-orthogonal states

The state discrimination problem:

Consider two parties, Alice and the referee Richard.
Alice and Richard agree on a set of quantum states

$$T = \{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_k\rangle\} \subseteq \mathbb{C}^d$$

The state discrimination problem:

Consider two parties, Alice and the referee Richard. Alice and Richard agree on a set of quantum states

$$T = \{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_k\rangle\} \subseteq \mathbb{C}^d$$

Richard picks a state $|\psi_i\rangle$ from T , and prepares "a copy" -- a d -dim quantum system S in the state $|\psi_i\rangle$. Richard gives the quantum system S to Alice, who does not know $|\psi_i\rangle$.

The state discrimination problem:

Consider two parties, Alice and the referee Richard. Alice and Richard agree on a set of quantum states

$$T = \{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_k\rangle\} \subseteq \mathbb{C}^d$$

Richard picks a state $|\psi_i\rangle$ from T , and prepares "a copy" -- a d -dim quantum system S in the state $|\psi_i\rangle$.

Richard gives the quantum system S to Alice, who does not know $|\psi_i\rangle$.

Alice applies a measurement to S , gets an outcome j , and tells Richard " j ". She wins if $j = i$ (she has distinguished or discriminated the state correctly).

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

Theorem:

Let $|\psi_1\rangle, |\psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \psi_1 | \psi_2 \rangle = 0$.

Proof:

If $\langle \psi_1 | \psi_2 \rangle = 0$, measure in a basis that includes both $|\psi_1\rangle, |\psi_2\rangle$.

If there is a meas that distinguishes $|\psi_1\rangle, |\psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\psi_2\rangle$.

Theorem:

Let $|\psi_1\rangle, |\psi_2\rangle$ be two arbitrary quantum states in d -dim.
Then, they can be perfectly distinguished iff $\langle \psi_1 | \psi_2 \rangle = 0$.

Proof:

If $\langle \psi_1 | \psi_2 \rangle = 0$, measure in a basis that includes both $|\psi_1\rangle, |\psi_2\rangle$.

If there is a meas that distinguishes $|\psi_1\rangle, |\psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\psi_2\rangle$.

$1 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\psi_2\rangle)$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d -dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\Psi_2\rangle$.

$1 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\Psi_2\rangle)$

$$= \|\mathcal{P}_2 |\Psi_2\rangle\|^2 = \langle \Psi_2 | \mathcal{P}_2^\dagger \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_2 | \mathcal{P}_2 | \Psi_2 \rangle$$

$$\mathcal{P}_i^\dagger = \mathcal{P}_i, \mathcal{P}_i^2 = \mathcal{P}_i$$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\Psi_2\rangle$.

1 = Prob (answer = 2 | state is $|\Psi_2\rangle$)

$$= \|\mathcal{P}_2 |\Psi_2\rangle\|^2 = \langle \Psi_2 | \mathcal{P}_2^\dagger \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_2 | \mathcal{P}_2 | \Psi_2 \rangle \Rightarrow \mathcal{P}_2 |\Psi_2\rangle = |\Psi_2\rangle.$$

$\mathcal{P}_i^\dagger = \mathcal{P}_i, \mathcal{P}_i^2 = \mathcal{P}_i$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\Psi_2\rangle$.

1 = Prob (answer = 2 | state is $|\Psi_2\rangle$)

$$= \|\mathcal{P}_2 |\Psi_2\rangle\|^2 = \langle \Psi_2 | \mathcal{P}_2^\dagger \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_2 | \mathcal{P}_2 | \Psi_2 \rangle \Rightarrow \mathcal{P}_2 |\Psi_2\rangle = |\Psi_2\rangle.$$

$\mathcal{P}_i^\dagger = \mathcal{P}_i, \mathcal{P}_i^2 = \mathcal{P}_i$

0 = Prob (answer = 2 | state is $|\Psi_1\rangle$) = $\|\mathcal{P}_2 |\Psi_1\rangle\|^2$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\Psi_2\rangle$.

$$1 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\Psi_2\rangle)$$

$$= \|\mathcal{P}_2 |\Psi_2\rangle\|^2 = \langle \Psi_2 | \mathcal{P}_2^\dagger \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_2 | \mathcal{P}_2 | \Psi_2 \rangle \Rightarrow \mathcal{P}_2 |\Psi_2\rangle = |\Psi_2\rangle.$$

$\mathcal{P}_i^\dagger = \mathcal{P}_i, \mathcal{P}_i^2 = \mathcal{P}_i$

$$0 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\Psi_1\rangle) = \|\mathcal{P}_2 |\Psi_1\rangle\|^2$$

$$\Rightarrow \mathcal{P}_2 |\Psi_1\rangle = 0$$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let P_2 be the projector that identifies $|\Psi_2\rangle$.

$$1 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\Psi_2\rangle)$$

$$= \|P_2|\Psi_2\rangle\|^2 = \langle \Psi_2 | P_2^\dagger P_2 |\Psi_2\rangle = \langle \Psi_2 | P_2 |\Psi_2\rangle \Rightarrow P_2|\Psi_2\rangle = |\Psi_2\rangle.$$

$P_i^\dagger = P_i, P_i^2 = P_i$

$$0 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\Psi_1\rangle) = \|P_2|\Psi_1\rangle\|^2$$

$$\Rightarrow P_2|\Psi_1\rangle = 0 \Rightarrow \langle \Psi_1 | P_2^\dagger = 0 \Rightarrow \langle \Psi_1 | P_2 = 0$$

$$\therefore \langle \Psi_1 | \Psi_2 \rangle = 0$$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\Psi_2\rangle$.

$$1 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\Psi_2\rangle)$$

$$= \|\mathcal{P}_2 |\Psi_2\rangle\|^2 = \langle \Psi_2 | \mathcal{P}_2^\dagger \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_2 | \mathcal{P}_2 | \Psi_2 \rangle \Rightarrow \mathcal{P}_2 |\Psi_2\rangle = |\Psi_2\rangle.$$

$\mathcal{P}_i^\dagger = \mathcal{P}_i, \mathcal{P}_i^2 = \mathcal{P}_i$

$$0 = \text{Prob}(\text{answer} = 2 \mid \text{state is } |\Psi_1\rangle) = \|\mathcal{P}_2 |\Psi_1\rangle\|^2$$

$$\Rightarrow \mathcal{P}_2 |\Psi_1\rangle = 0 \Rightarrow \langle \Psi_1 | \mathcal{P}_2^\dagger = 0 \Rightarrow \langle \Psi_1 | \mathcal{P}_2 = 0$$

$$\therefore \langle \Psi_1 | \Psi_2 \rangle = \langle \Psi_1 | \mathcal{P}_2 | \Psi_2 \rangle$$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\Psi_2\rangle$.

1 = Prob (answer = 2 | state is $|\Psi_2\rangle$)

$$= \|\mathcal{P}_2 |\Psi_2\rangle\|^2 = \langle \Psi_2 | \mathcal{P}_2^\dagger \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_2 | \mathcal{P}_2 | \Psi_2 \rangle \Rightarrow \mathcal{P}_2 |\Psi_2\rangle = |\Psi_2\rangle.$$

$\mathcal{P}_i^\dagger = \mathcal{P}_i, \mathcal{P}_i^2 = \mathcal{P}_i$

0 = Prob (answer = 2 | state is $|\Psi_1\rangle$) = $\|\mathcal{P}_2 |\Psi_1\rangle\|^2$

$$\Rightarrow \mathcal{P}_2 |\Psi_1\rangle = 0 \Rightarrow \langle \Psi_1 | \mathcal{P}_2^\dagger = 0 \Rightarrow \langle \Psi_1 | \mathcal{P}_2 = 0$$

$$\therefore \langle \Psi_1 | \Psi_2 \rangle = \langle \Psi_1 | \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_1 | \mathcal{P}_2 | \Psi_2 \rangle$$

Theorem:

Let $|\Psi_1\rangle, |\Psi_2\rangle$ be two arbitrary quantum states in d-dim.
Then, they can be perfectly distinguished iff $\langle \Psi_1 | \Psi_2 \rangle = 0$.

Proof:

If $\langle \Psi_1 | \Psi_2 \rangle = 0$, measure in a basis that includes both $|\Psi_1\rangle, |\Psi_2\rangle$.

If there is a meas that distinguishes $|\Psi_1\rangle, |\Psi_2\rangle$ perfectly.

Let \mathcal{P}_2 be the projector that identifies $|\Psi_2\rangle$.

1 = Prob (answer = 2 | state is $|\Psi_2\rangle$)

$$= \|\mathcal{P}_2 |\Psi_2\rangle\|^2 = \langle \Psi_2 | \mathcal{P}_2^\dagger \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_2 | \mathcal{P}_2 | \Psi_2 \rangle \Rightarrow \mathcal{P}_2 |\Psi_2\rangle = |\Psi_2\rangle.$$

$\mathcal{P}_i^\dagger = \mathcal{P}_i, \mathcal{P}_i^2 = \mathcal{P}_i$

0 = Prob (answer = 2 | state is $|\Psi_1\rangle$) = $\|\mathcal{P}_2 |\Psi_1\rangle\|^2$

$$\Rightarrow \mathcal{P}_2 |\Psi_1\rangle = 0 \Rightarrow \langle \Psi_1 | \mathcal{P}_2^\dagger = 0 \Rightarrow \langle \Psi_1 | \mathcal{P}_2 = 0$$

$$\therefore \langle \Psi_1 | \Psi_2 \rangle = \langle \Psi_1 | \mathcal{P}_2 | \Psi_2 \rangle = \langle \Psi_1 | \mathcal{P}_2 | \Psi_2 \rangle = 0.$$

□

Exercise:

For the quantum state discrimination problem, Alice can perfectly distinguish the set of k states iff those k states are mutually orthogonal

If two states are not orthogonal, can they be distinguished with very small errors?

Intuitively, two similar states are harder to distinguish than two very different states (in terms of Alice's probability of "winning").

We will define a measure of "similarity" between two quantum states, and see how Alice's losing probability depends on the similarity.

Definition:

For $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^d$, the fidelity of $|\psi_1\rangle, |\psi_2\rangle$ is given by

$$F(|\psi_1\rangle, |\psi_2\rangle) = |\langle \psi_1 | \psi_2 \rangle|$$

e.g., $F = 0$ for orthogonal states,

$F = 1$ for states differing by a phase factor.

Holevo-Helstrom Theorem

If each of $|\Psi_1\rangle, |\Psi_2\rangle$ is chosen with probability $1/2$, then the max prob to distinguish the state is

$$\frac{1}{2} + \frac{1}{2} \sqrt{1 - F(|\Psi_1\rangle, |\Psi_2\rangle)^2} = \frac{1}{2} + \frac{1}{2} \sqrt{1 - |\langle \Psi_1 | \Psi_2 \rangle|^2}$$

Holevo-Helstrom Theorem

If each of $|\Psi_1\rangle, |\Psi_2\rangle$ is chosen with probability $1/2$, then the max prob to distinguish the state is

$$\frac{1}{2} + \frac{1}{2} \sqrt{1 - F(|\Psi_1\rangle, |\Psi_2\rangle)^2} = \frac{1}{2} + \frac{1}{2} \sqrt{1 - |\langle \Psi_1 | \Psi_2 \rangle|^2}$$

Alice can achieve winning prob of $1/2$ by guessing

this term is called the "bias" -- the advantage above guess because Alice can make a meas on one copy of the state

$|\langle \Psi_1 | \Psi_2 \rangle|$ closer to 1 means a smaller bias

Holevo-Helstrom Theorem

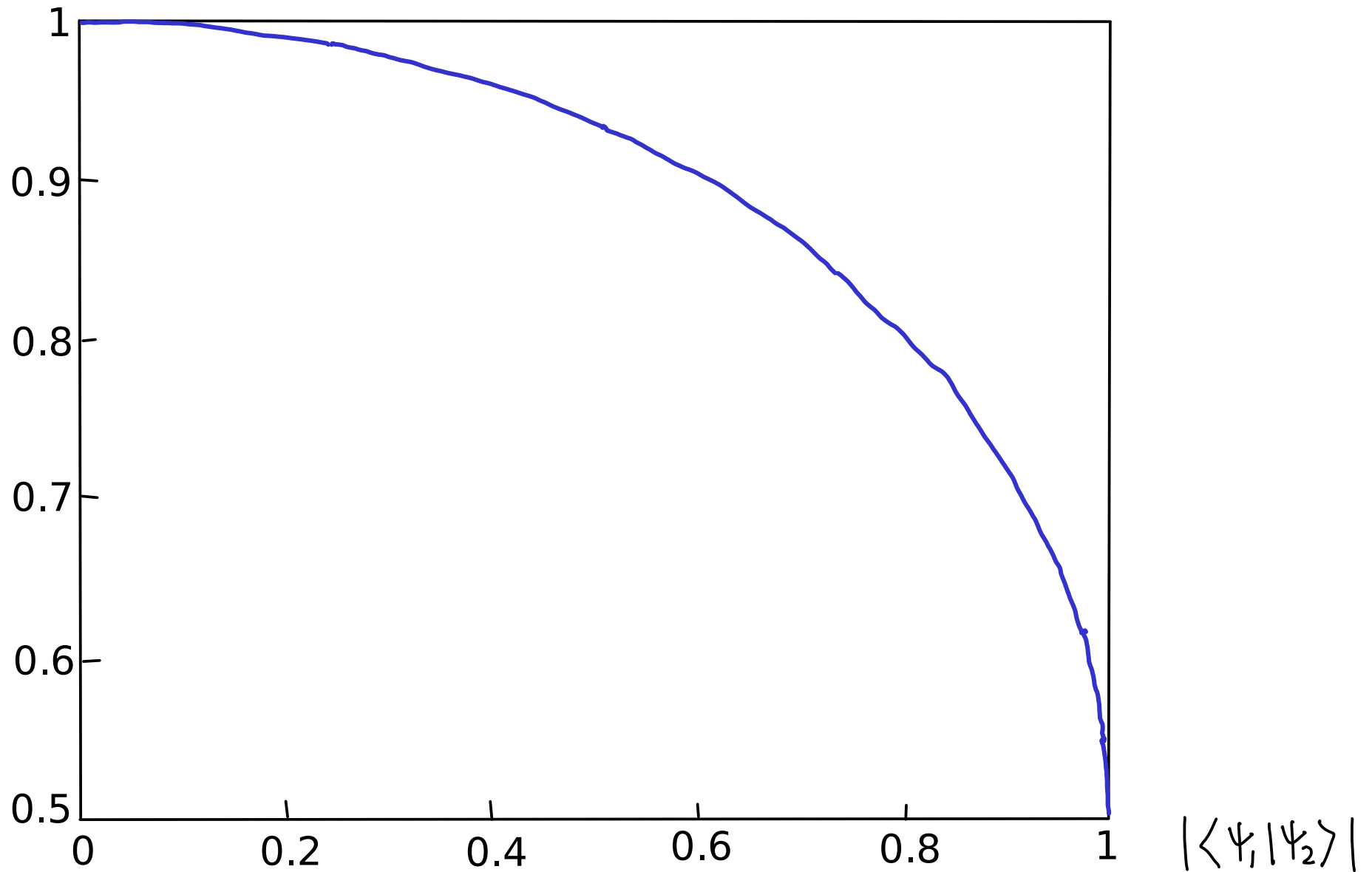
If each of $|\Psi_1\rangle, |\Psi_2\rangle$ is chosen with probability $1/2$, then the max prob to distinguish the state is

$$\frac{1}{2} + \frac{1}{2} \sqrt{1 - F(|\Psi_1\rangle, |\Psi_2\rangle)^2} = \frac{1}{2} + \frac{1}{2} \sqrt{1 - |\langle \Psi_1 | \Psi_2 \rangle|^2}$$

Proof: see NC 9.2.3 relating the fidelity to the trace distance, and Prof Watrous textbook Theorem 3.4.

e.g., Prob = 1 for orthogonal states,
Prob = 1/2 for states differing by a phase factor,
Prob = 85.36% for $|0\rangle, |+\rangle$.

Prob of correctly discriminating the two states



Quick question:

Which of the following three pairs of states are least distinguishable (Alice wins with smallest prob)?

For $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^d$ non-orthogonal,

(a) $|\psi_1\rangle, |\psi_2\rangle$

(b) $|\psi_1\rangle^{\otimes 2}, |\psi_2\rangle^{\otimes 2}$

(c) $|\psi_1\rangle \otimes |\psi_2\rangle, |\psi_2\rangle \otimes |\psi_1\rangle$

Relating

the no-cloning theorem

and

the non-distinguishability of non-orthogonal states

The no-cloning theorem and the non-distinguishability of non-orthogonal states are qualitatively equivalent !

The no-cloning theorem and the non-distinguishability of non-orthogonal states are qualitatively equivalent !

Suppose we can clone. When given one of $|\psi_1\rangle, |\psi_2\rangle$ make many copies, say n . Then, we have

$$|\psi_1\rangle^{\otimes n}, |\psi_2\rangle^{\otimes n}$$

The no-cloning theorem and the non-distinguishability of non-orthogonal states are qualitatively equivalent !

Suppose we can clone. When given one of $|\psi_1\rangle, |\psi_2\rangle$ make many copies, say n . Then, we have

$$|\psi_1\rangle^{\otimes n}, |\psi_2\rangle^{\otimes n}$$

which are nearly distinguishable (HH Thm) because

$$F(|\psi_1\rangle^{\otimes n}, |\psi_2\rangle^{\otimes n}) = |\langle \psi_1 | \psi_2 \rangle|^n \rightarrow 0$$

as long as $|\langle \psi_1 | \psi_2 \rangle| \neq 1$.

The no-cloning theorem and the non-distinguishability of non-orthogonal states are qualitatively equivalent !

Suppose we can clone. When given one of $|\psi_1\rangle, |\psi_2\rangle$ make many copies, say n . Then, we have

$$|\psi_1\rangle^{\otimes n}, |\psi_2\rangle^{\otimes n}$$

which are nearly distinguishable (HH Thm) because

$$F(|\psi_1\rangle^{\otimes n}, |\psi_2\rangle^{\otimes n}) = |\langle \psi_1 | \psi_2 \rangle|^n \rightarrow 0$$

as long as $|\langle \psi_1 | \psi_2 \rangle| \neq 1$.

Conversely, suppose we can distinguish $|\psi_1\rangle, |\psi_2\rangle$ with very high probability. Then, if the outcome is i , prepare copies of $|\psi_i\rangle$.

The non-distinguishability of non-orthogonal states implies that there is a big difference between knowing the description of a quantum state and having a copy of the quantum state.

We have to be specific when talking about "a quantum state" throughout this course.

4. Immediate information processing consequences of QM

i.e., more examples of QM :)

✓ (a) No-cloning theorem (NC 1.3.5, box 12.1)

✓ (b) Non-distinguishability of non-orthogonal states
(NC p56-57)

→ (c) Communication of data

- protocols, bounds, and non-signalling principle
- encoding and extraction of classical data in QM

(d) Superdense coding and teleportation
(NC 2.3, 1.3.7, KLM 5.1-5.2, N 6.4-6.5)

(e) Bell's inequality and nonlocal games (NC 2.6, M 6.6)

How many states are there in a quantum system of n qubits?

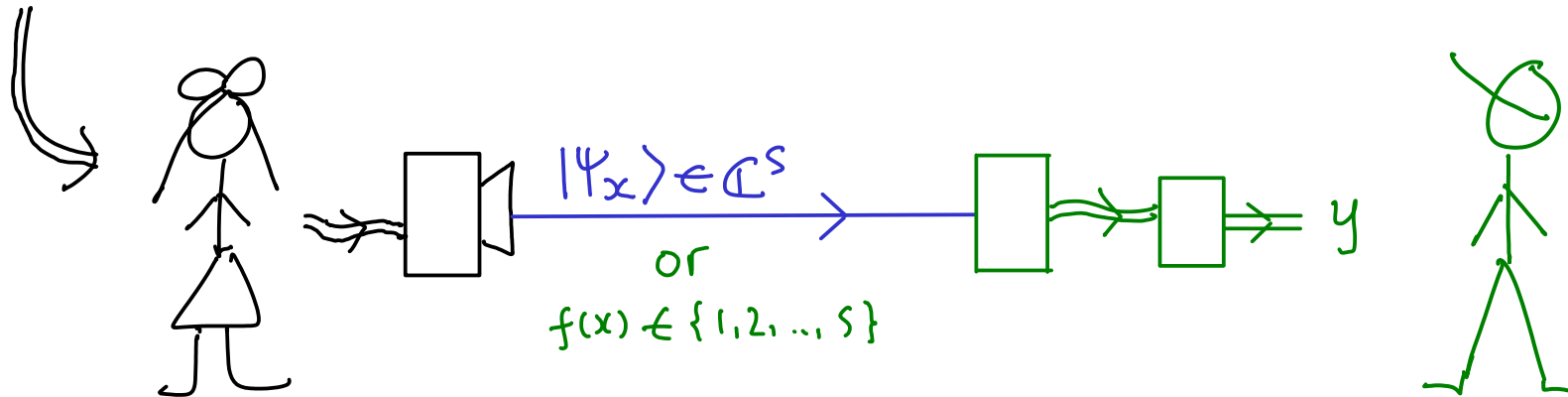
As many as described by $2^n - 1$ complex numbers.

How many bits of classical information can it carry?

/
What does this mean?

Communication scenario:

$$x \in \{1, 2, \dots, t\}$$



Alice (sender)

Bob (receiver)

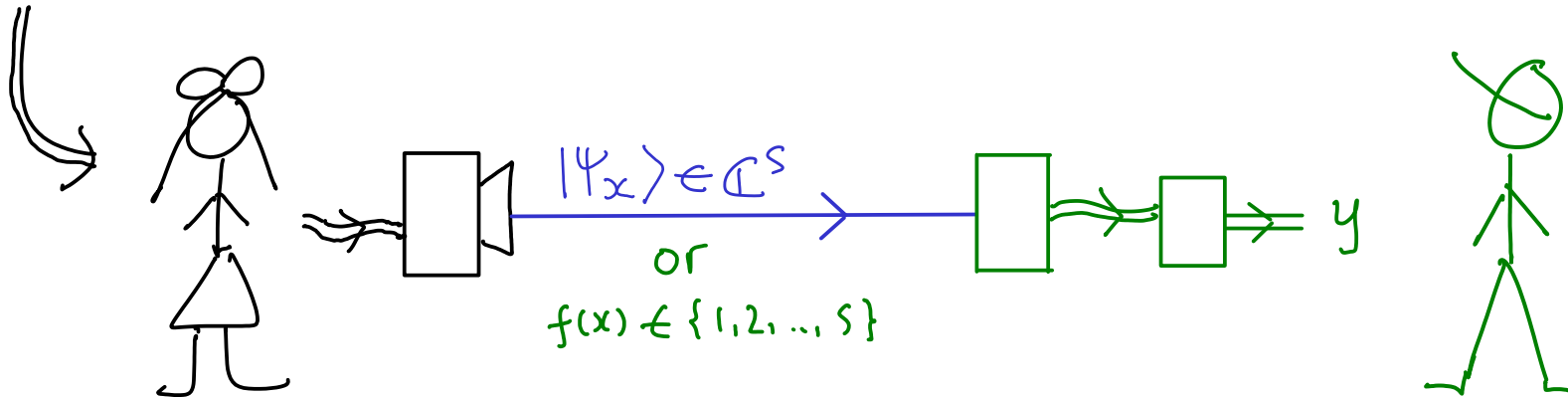
Goal: transmitting classical data by physically sending classical or quantum data

We say that s dimensions (or one out of s messages if classical) are (physically) sent from Alice to Bob.

Communication scenario:

Goal: transmitting classical data by physically sending classical or quantum data

$$x \in \{1, 2, \dots, t\}$$



Alice (sender)

Bob (receiver)

We say that s dimensions (or one out of s messages if classical) are (physically) sent from Alice to Bob.

If $y=x$ with high probability, we say that t messages are communicated from Alice to Bob.

Remarks on how to think about quantum protocols:

1. Note which party has which quantum system
(thus what operations he/she is allowed to do)
2. Note which party has what classical information
(e.g., Alice knows the message, Bob doesn't)

These will determine how we set up the mathematics to describe the physics, and how we proceed with the proofs.

The non-signalling principle says there is no free lunch:

Alice cannot affect Bob's output if nothing (classical or quantum) is being sent physically;

i.e., if $s = 0$ or 1 , x and y are independent.

The non-signalling principle says there is no free lunch:

Alice cannot affect Bob's output if nothing (classical or quantum) is being sent physically;

i.e., if $s = 0$ or 1 , x and y are independent.

The following theorem says there is no discounted lunch for the classical setting.

i.e., $x = y$ with high prob, then $s \geq t$.

Theorem: (no discounted lunch thm)

Alice cannot communicate $t > s$ messages to Bob by sending s messages.

Theorem:

Alice cannot communicate $t > s$ messages to Bob by sending s messages.

Proof (by contradiction):

Suppose there is a method for Alice to communicate t messages to Bob by sending only s messages.

Theorem:

Alice cannot communicate $t > s$ messages to Bob by sending s messages.

Proof (by contradiction):

Suppose there is a method for Alice to communicate t messages to Bob by sending only s messages.

WLOG, when Alice's message is x , she produces an $f(x)$ in $\{1, \dots, s\}$ and sends $f(x)$ to Bob, who decodes $f(x)$ to obtain an output y . For each x , $\Pr(x=y) \approx 1$.

Theorem:

Alice cannot communicate $t > s$ messages to Bob by sending s messages.

Proof (by contradiction):

Suppose there is a method for Alice to communicate t messages to Bob by sending only s messages.

WLOG, when Alice's message is x , she produces an $f(x)$ in $\{1, \dots, s\}$ and sends $f(x)$ to Bob, who decodes $f(x)$ to obtain an output y . For each x , $\Pr(x=y) \approx 1$.

Now modify the above method:

Alice generates $f(x)$ but does not send it to Bob. Bob, without an incoming message, just guesses it randomly, $\text{prob}(\text{correct}) = 1/s$.

In the modified method, $x=y$ with prob $1/s$.
With $1/t$ values of x , so, x and y are NOT independent.

In the modified method, $x=y$ with prob $1/s$.
With $1/t$ values of x , so, x and y are NOT independent.

But Alice doesn't send anything in the modified method, this contradict the no-signalling principle.

So, it's impossible to communicate t messages from Alice to Bob by sending s messages.



In the modified method, $x=y$ with prob at least $1/s$.
With $1/t$ values of x , so, x and y are NOT independent.

But Alice doesn't send anything in the modified method, this contradict the no-signalling principle.

So, it's impossible to communicate t messages from Alice to Bob by sending s messages.



What happens if Alice sends a quantum message to Bob instead?

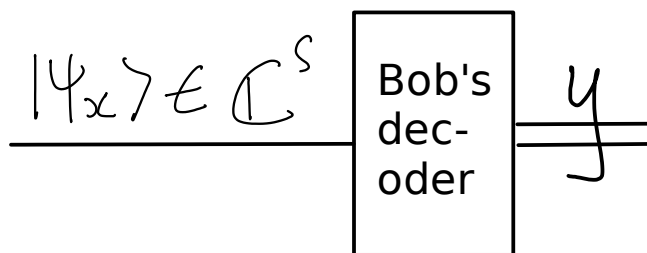
Theorem (Holevo73): Alice cannot communicate $t > s$ messages to Bob by sending an s -dim quantum sys.

Theorem (Holevo73): Alice cannot communicate $t > s$ messages to Bob by sending an s -dim quantum sys.

Transmitting quantum is not better than classical ...

Intuition for the theorem:

Easy case:



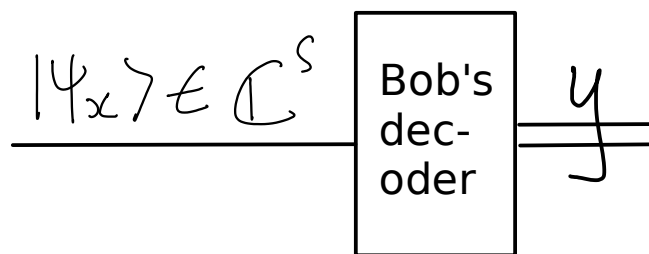
At most s outcomes
for y .

Theorem (Holevo73): Alice cannot communicate $t > s$ messages to Bob by sending an s -dim quantum sys.

Transmitting quantum is not better than classical ...

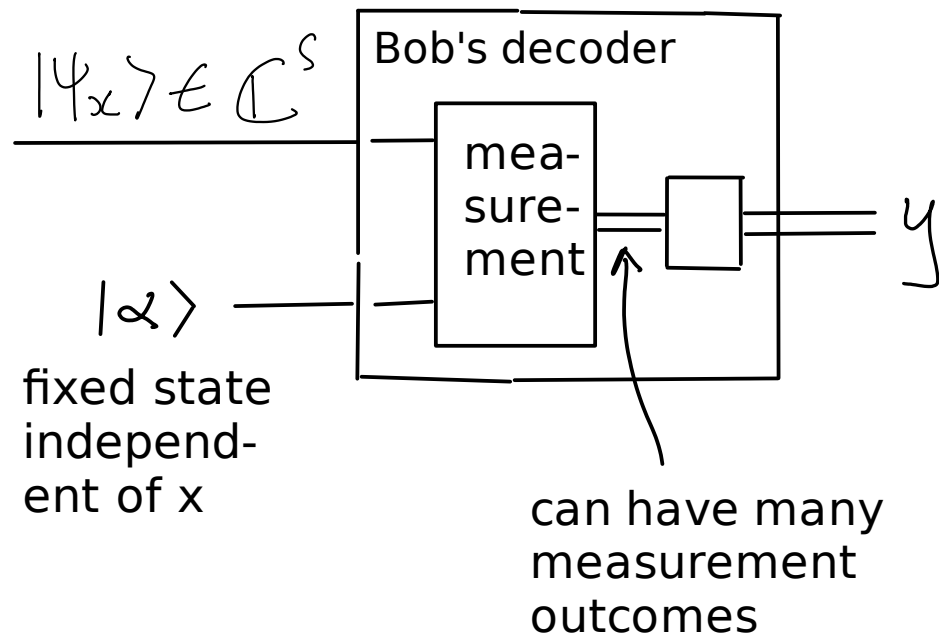
Intuition for the theorem:

Easy case:



At most s outcomes for y .

General case (out of scope):



send s classical
messages
comm no more
than s messages

send s -dimensional
quantum system
comm no more
than s messages

What if Alice and Bob share an entangled state
that they can use ?

send s classical
messages
comm no more
than s messages

send s -dimensional
quantum system
comm no more
than s messages

send s classical
messages & use
entanglement
comm no more
than s messages

How to see this?

Theorem: (no discounted lunch thm +)

Alice cannot communicate $t > s$ messages to Bob by sending s messages, even if Alice and Bob share an entangled state.

Proof sketch:

Theorem: (no discounted lunch thm +)

Alice cannot communicate $t > s$ messages to Bob by sending s messages, even if Alice and Bob share an entangled state.

Proof sketch:

Similar to the proof without entanglement!

Theorem: (no discounted lunch thm +)

Alice cannot communicate $t > s$ messages to Bob by sending s messages, even if Alice and Bob share an entangled state.

Proof sketch:

Similar to the proof without entanglement!

(1) start with some discounted-lunch protocol with entanglement, (2) replace Alice's message with Bob's random guess, (3) Bob's output is correlated with Alice's input and contradicts the no-signalling principle which holds even in the presence of entanglement.

send s classical
messages
comm no more
than s messages

send s -dimensional
quantum system
comm no more
than s messages

send s classical
messages & use
entanglement
comm no more
than s messages

send s -dimensional
quantum system &
use entanglement
comm how many
messages ?

The no discounted lunch proof breaks down since Bob cannot guess a quantum state. Holevo's theorem applies but to larger dim ...

Theorem: superdense coding (Bennett-Wiesner 93)

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}} \sum_{i=1}^s |i\rangle \otimes |i\rangle$ and Alice can send an s -dimensional quantum system to Bob. Then, Alice can communicate $t=s^2$ messages to Bob!

Theorem: superdense coding (Bennett-Wiesner 93)

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}} \sum_{i=1}^s |i\rangle \otimes |i\rangle$ and Alice can send an s-dimensional quantum system to Bob. Then, Alice can communicate $t=s^2$ messages to Bob!

How to think about quantum protocols:

Which party has what classical information ?

Which party has what quantum system ?

What operations he/she is allowed to do ?

Theorem: superdense coding (Bennett-Wiesner 93)

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}} \sum_{i=1}^s |i\rangle \otimes |i\rangle$
and Alice can send an s-dimensional quantum system to Bob. Then, Alice can communicate $t=s^2$ messages to Bob!

A B

How to think about quantum protocols:

Which party has what classical information ?

Alice has a message v . Bob has nothing.

Which party has what quantum system ?

Initially, Alice has register A, Bob has register B of the shared state. Alice also has an s-dim system C. She then sends C to Bob. Then, Bob has both B, C.

Theorem: superdense coding (Bennett-Wiesner 93)

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}} \sum_{i=1}^s |i\rangle \otimes |i\rangle$ and Alice can send an s-dimensional quantum system to Bob. Then, Alice can communicate $t=s^2$ messages to Bob!

How to think about quantum protocols:

What operations he/she is allowed to do ?

Before Alice sends C to Bob, she can apply any operation on AC that depends on v. C depends on A and v, and C can be A itself.

After Bob receives C from Alice, he can apply any operation on AC that does not depend on v.

Proof: for simplicity, first consider $s=2$.

Suppose Alice & Bob share the state $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

so that Alice (Bob) holds the first (second) qubit A (B).

Proof: for simplicity, first consider $s=2$.

Suppose Alice & Bob share the state $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

so that Alice (Bob) holds the first (second) qubit A (B).

Recall the Pauli matrices:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Proof: for simplicity, first consider $s=2$.

Suppose Alice & Bob share the state $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
so that Alice (Bob) holds the first (second) qubit.

Recall the Pauli matrices:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Suppose Alice wants to communicate a message v
from the set $\{0, x, y, z\}$.

If her message is v , she applies σ_v to A.

The shared state $|\Phi_0\rangle$ on AB is transformed by $\sigma_v \otimes \mathbb{I}$.

For $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\Phi_0\rangle = \sigma_0 \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi_x\rangle = \sigma_x \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

$$|\Phi_y\rangle = \sigma_y \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(i|10\rangle - i|01\rangle)$$

$$|\Phi_z\rangle = \sigma_z \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

These 4 states are mutually orthogonal, forming the "Bell basis". Note that Alice operates on a 2-dim system A, but the shared state on AB traverses to 1 out of 4 possible distinguishable (ortho) states.

For $|\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\Phi_0\rangle = \sigma_0 \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi_x\rangle = \sigma_x \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

$$|\Phi_y\rangle = \sigma_y \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(-i|10\rangle + i|01\rangle)$$

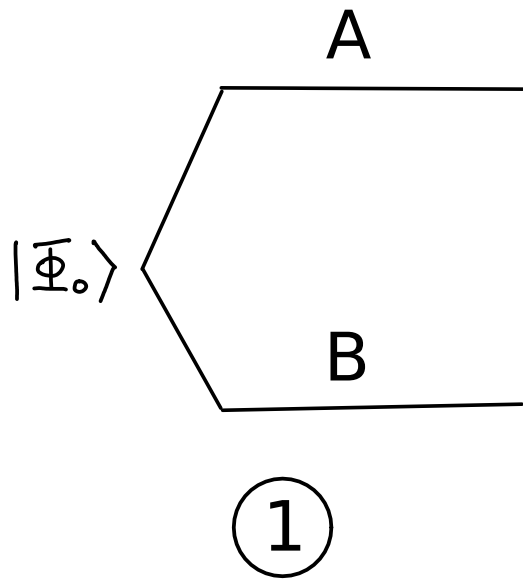
$$|\Phi_z\rangle = \sigma_z \otimes I |\Phi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

These 4 states are mutually orthogonal, forming the "Bell basis". Note that Alice operates on a 2-dim system A, but the shared state on AB traverses to 1 out of 4 possible distinguishable (ortho) states.

If Alice sends C=A to Bob, he has AB in the state $|\Phi_v\rangle$.

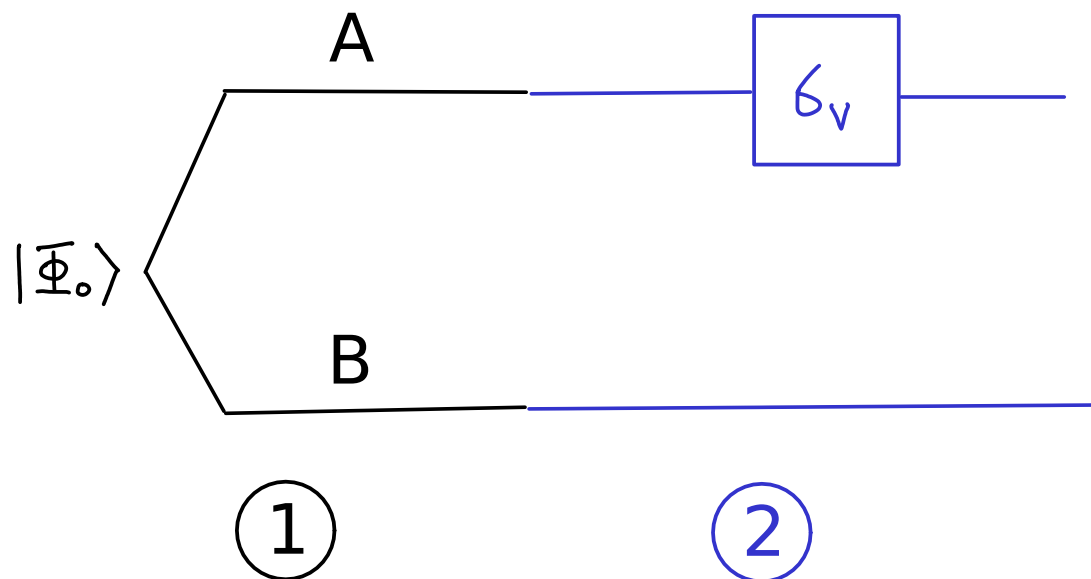
He can measure AB along the Bell basis to find v !

Communication protocol:



Initial state shared between Alice and Bob. Alice is holding system A; Bob is holding system B.

Communication protocol:

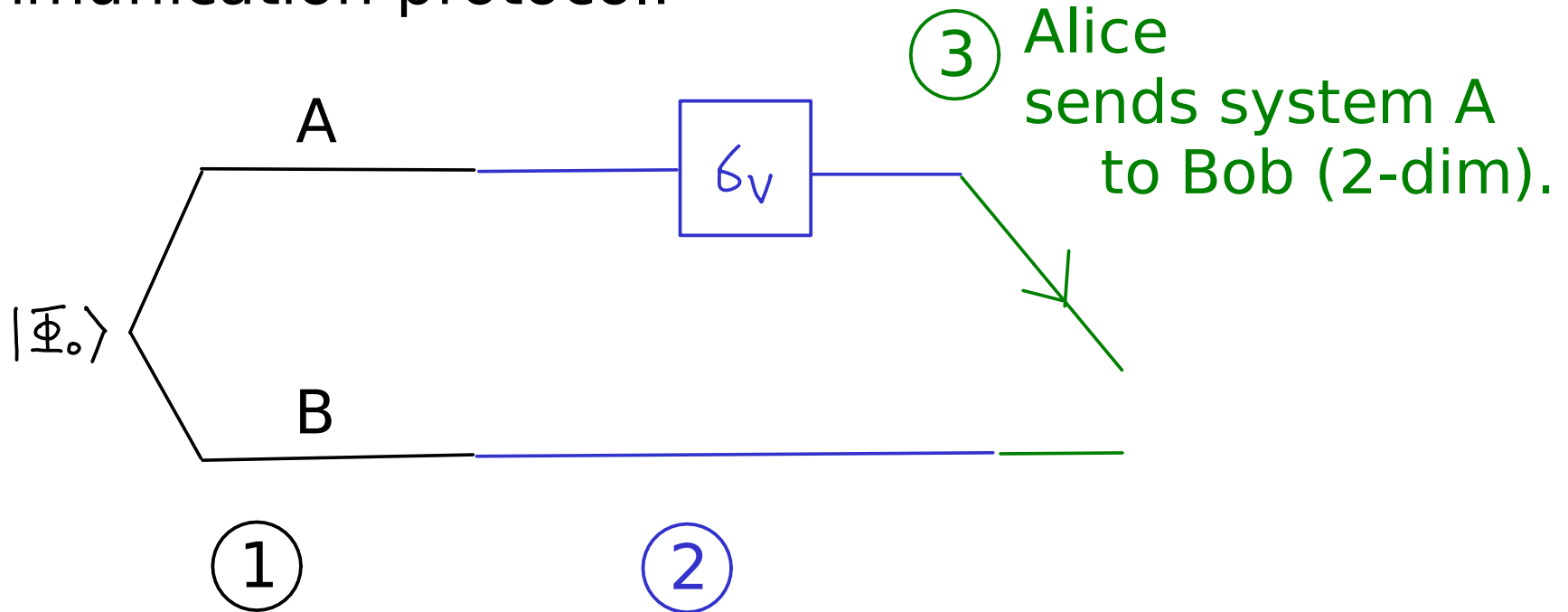


① Initial state shared between Alice and Bob. Alice is holding system A; Bob is holding system B.

② If Alice wants to communicate "v" $\in \{0,x,y,z\}$ to Bob she applies G_v to qubit A.

(4 possibilities)

Communication protocol:

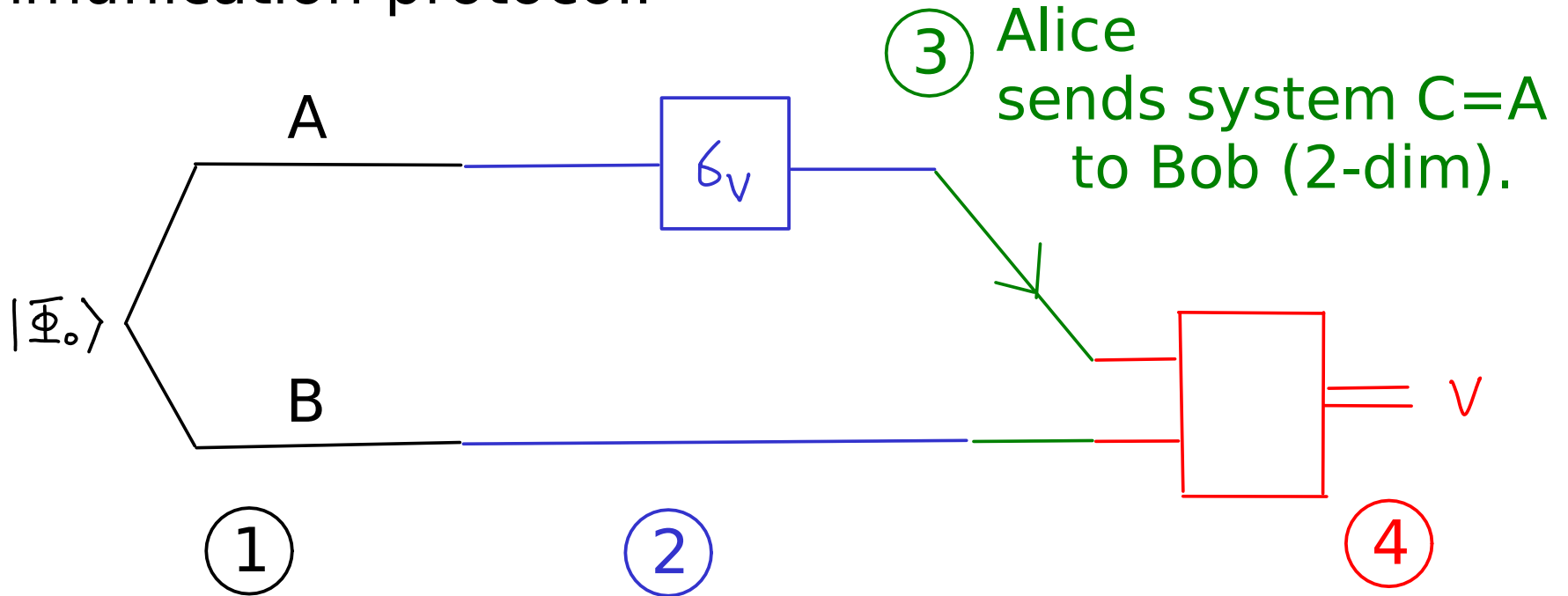


① Initial state shared between Alice and Bob. Alice is holding system A; Bob is holding system B.

② If Alice wants to communicate "v" $\in \{0,x,y,z\}$ to Bob she applies σ_v to qubit A.

(4 possibilities)

Communication protocol:

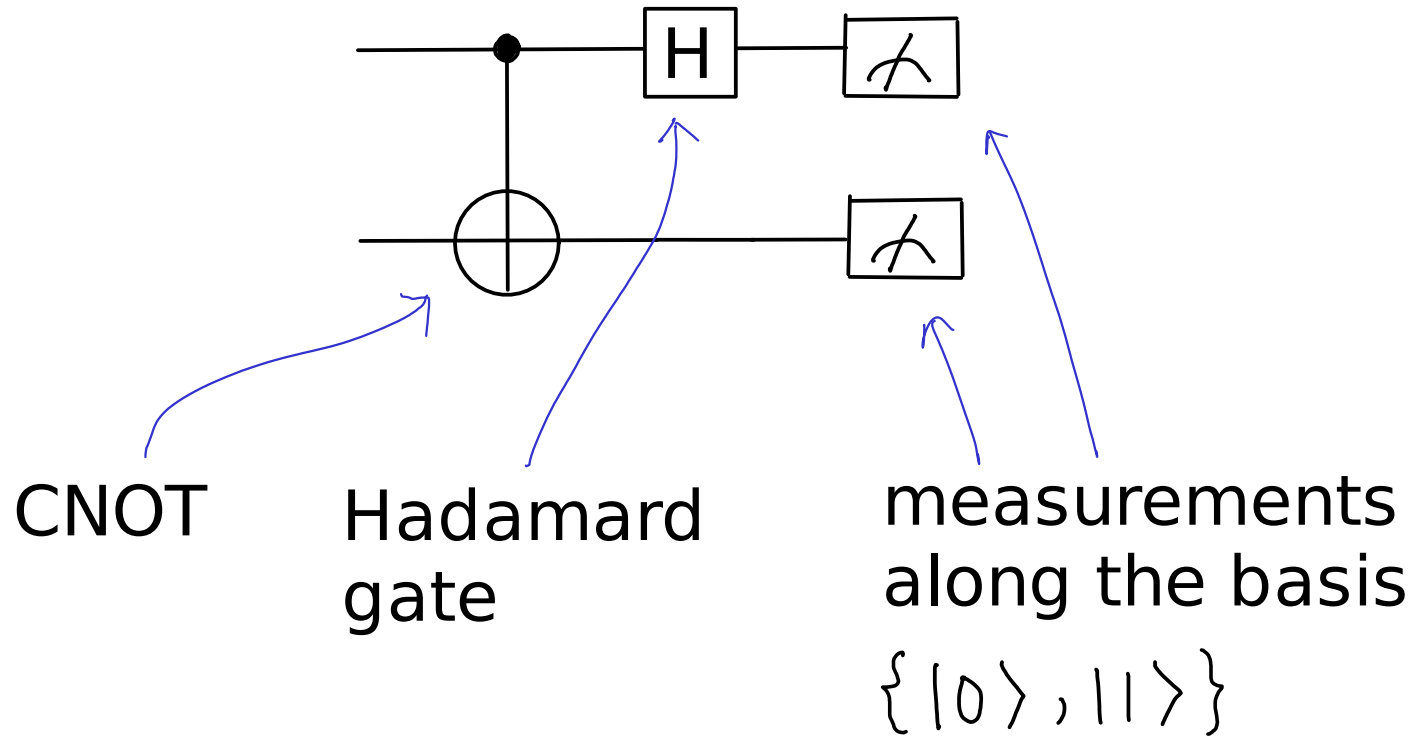


① Initial state shared between Alice and Bob. Alice is holding system A; Bob is holding system B.

② If Alice wants to communicate " v " $\in \{0,x,y,z\}$ to Bob she applies σ_v to qubit A.
(4 possibilities)

③ Alice sends system $C=A$ to Bob (2-dim).
④ Having both systems A & B, Bob measures along the Bell basis. Outcome is v with certainty.

Exercise: verify that the following circuit measures along the Bell basis.



Thoughts:

1. Entanglement enables the operation on a 2-dim system to map the shared state over 4 dimensions.
2. Bob has a 4-dim system (AB) after the channel transmission, so superdense coding is consistent with Holevo's bound.

Thoughts:

1. Entanglement enables the operation on a 2-dim system to map the shared state over 4 dimensions.
2. Bob has a 4-dim system (AB) after the channel transmission, so superdense coding is consistent with Holevo's bound.
3. Is there a catch? Does Alice also need to prepare the entangled state in AB and send B to Bob before superdense coding so altogether she sends 4 dims?

Please do not scroll down. Which is true?

- (a) yes Alice must send 4 dims
- (b) no

Thoughts:

1. Entanglement enables the operation on a 2-dim system to map the shared state over 4 dimensions.
2. Bob has a 4-dim system (AB) after the channel transmission, so superdense coding is consistent with Holevo's bound.
3. Is there a catch? Does Alice also need to prepare the entangled state in AB and send B to Bob before superdense coding so altogether she sends 4 dims?

Not really. Bob can prepare the entangled state in AB and send A to Alice instead, or a common friend Charlie can prepare the entangled state and send A to Alice and B to Bob.

SD turns entanglement or back quantum comm into increased forward classical communication !!

Exercise:

How does SD coding work for general s?

Exercise:

How does SD coding work for general s ?

Note that for $s = 2^{2^n}$,

we can simply repeat "SD coding for $s=2$ " n times.

Exercise:

How does SD coding work for general s ?

Note that for $s = 2^{2^n}$,

we can simply repeat "SD coding for $s=2$ " n times.

For general s : let ω be a primitive s -th root of unity.

Let Alice's message be $(k,j) \in \{1,2,\dots,s\} \times \{1,2,\dots,s\}$.

Exercise:

How does SD coding work for general s ?

Note that for $s = 2^{2n}$,

we can simply repeat "SD coding for $s=2$ " n times.

For general s : let ω be a primitive s -th root of unity.

Let Alice's message be $(k,j) \in \{1,2,\dots,s\} \times \{1,2,\dots,s\}$.

Consider the S^2 unitaries:

$$U_{kj} = \sum_{\bar{i}} |\bar{i} + k \bmod s\rangle \langle \bar{i}| \cdot \sum_{\bar{l}} \omega^{j\bar{l}} |\bar{l}\rangle \langle \bar{l}|$$

|
like σ_x^k |
like σ_z^j

NB for $s=2$, $\sigma_y = \sigma_x \sigma_z$. U_{kj} 's are "generalized Pauli's."

Exercise:

How does SD coding work for general s ?

Note that for $s = 2^{2n}$,

we can simply repeat "SD coding for $s=2$ " n times.

For general s : let ω be a primitive s -th root of unity.

Let Alice's message be $(k,j) \in \{1,2,\dots,s\} \times \{1,2,\dots,s\}$.

Consider the S^2 unitaries:

$$U_{kj} = \sum_{\bar{i}} |\bar{i} + k \bmod s\rangle \langle \bar{i}| \cdot \sum_{\bar{l}} \omega^{j\bar{l}} |\bar{l}\rangle \langle \bar{l}|$$
$$= \sum_{\bar{i}} \omega^{j\bar{i}} |\bar{i} + k \bmod s\rangle \langle \bar{i}|$$

Verify that the S^2 states

$$|\bar{\Phi}_{kj}\rangle = U_{kj} \frac{1}{\sqrt{s}} \sum_{u=1}^s |u\rangle \otimes |u\rangle \text{ are mutually orthogonal.}$$

Theorem: superdense coding (Bennett-Wiesner 93)

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}} \sum_{i=1}^s |i\rangle \otimes |i\rangle$ and Alice can send an s -dimensional quantum system to Bob. Then, Alice can communicate $t=s^2$ messages to Bob!

Converting the units of various resources:

s -dim quantum state = $\log s$ qubits
 s^2 classical messages = $2 \log s$ bits

Theorem: superdense coding (Bennett-Wiesner 93)

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}} \sum_{i=1}^s |i\rangle \otimes |i\rangle$ and Alice can send an s -dimensional quantum system to Bob. Then, Alice can communicate $t=s^2$ messages to Bob!

Converting the units of various resources:

s -dim quantum state = $\log s$ qubits

s^2 classical messages = $2 \log s$ bits

max entangled state of local dim s = $\log s$ "ebits"

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{A_1 B_1} \otimes \dots \otimes \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{A_n B_n} = \frac{1}{\sqrt{2^n}} \sum_{u \in \{0,1\}^n} |u\rangle_{A_1 \dots A_n} \otimes |u\rangle_{B_1 \dots B_n}$$

Theorem: superdense coding (Bennett-Wiesner 93)

Suppose Alice and Bob share the state $\frac{1}{\sqrt{s}} \sum_{i=1}^s |i\rangle \otimes |i\rangle$ and Alice can send an s-dimensional quantum system to Bob. Then, Alice can communicate $t=s^2$ messages to Bob!

Converting the units of various resources:

s-dim quantum state = $\log s$ qubits

s^2 classical messages = $2 \log s$ bits


max entangled state of local dim s = $\log s$ "ebits"

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{A_1 B_1} \otimes \dots \otimes \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)_{A_n B_n} = \frac{1}{\sqrt{2^n}} \sum_{u \in \{0,1\}^n} |u\rangle_{A_1 \dots A_n} \otimes |u\rangle_{B_1 \dots B_n}$$

Dividing everything by $\log s$, on average, SD coding uses 1 ebit and sends 1 qubit to communicate 2 bits (doubling the rate).

4. Immediate information processing consequences of QM

i.e., more examples of QM :)

- ✓ (a) No-cloning theorem (NC 1.3.5, box 12.1)
- ✓ (b) Non-distinguishability of non-orthogonal states
(NC p56-57)
- ✓ (c) Communication of data
 - protocols, bounds, and non-signalling principle
 - encoding and extraction of classical data in QM
- (d) Superdense coding and teleportation 
 - ✓ (NC 2.3, 1.3.7, KLM 5.1-5.2, N 6.4-6.5)
- (e) Bell's inequality and nonlocal games (NC 2.6, M 6.6)