Qubits vs. bits: a naive account

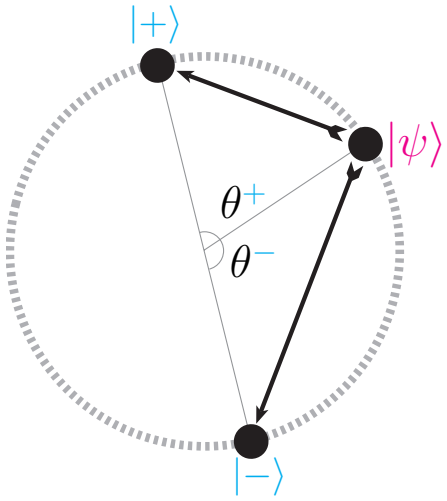
A **bit**:

- admits two values 0 and 1,
- admits arbitrary transformations.
- is freely readable,

A **qubit**:

- a *sphere* of values, which is 'spanned' in projective sense by two quantum states $|0\rangle$ and $|1\rangle$.
- only admits special transformations which preserve the angles, and hence opposites on the sphere; hence these transformations are *reversible*.
- only admits 'reading' through so-called *quantum measurements* $M(|+\rangle, |-\rangle)$ which
  - only have two possible outcomes $|+\rangle$ and $|-\rangle$,
  - change the initial state $|\psi\rangle$ to either $|+\rangle$ or $|-\rangle$,

  so in a sense a measurement $M(|+\rangle, |-\rangle)$ does not tell us $|\psi\rangle$ but destroys $|\psi\rangle$!



The two transitions

$$\mathrm{P}_+ :: |\psi\rangle \mapsto |+\rangle \qquad\qquad \mathrm{P}_- :: |\psi\rangle \mapsto |-\rangle$$

have respective chance $\mathsf{prob}(\theta_+)$ and $\mathsf{prob}(\theta_-)$ with

$$\mathsf{prob}(\theta_+) + \mathsf{prob}(\theta_-) = 1$$

with

$$\mathsf{prob}(\theta) = cos^2\frac{\theta}{2}\,.$$

Due to impossible transitions ($\mathsf{prob}(180^o) = 0$), we obtain two 'partial constant maps' on the sphere Q

$$\mathrm{P}_+ : Q \setminus \{|-\rangle\} \to Q :: |\psi\rangle \mapsto |+\rangle.$$

$$\mathrm{P}_- : Q \setminus \{|+\rangle\} \to Q :: |\psi\rangle \mapsto |-\rangle$$

capturing the *dynamics of measurement*.

This can be used as a *dynamic resource* when designing algorithms and protocols.

The **state of a qubit** is described by a pair of complex numbers $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ *up to a non-zero complex multiple*.

Hence for any $z \in \mathbb{C}_0$

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \qquad \text{and} \qquad z \cdot \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} := \begin{pmatrix} z \cdot z_1 \\ z \cdot z_2 \end{pmatrix}$$

both define the same state. Typically one writes

$$|\psi\rangle := z \cdot |0\rangle + z' \cdot |1\rangle$$

to emphasise a connection with bits.

Measurements are special families of *projectors* e.g.

$$\mathrm{P}_0 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathrm{P}_1 := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

They induce a change of state

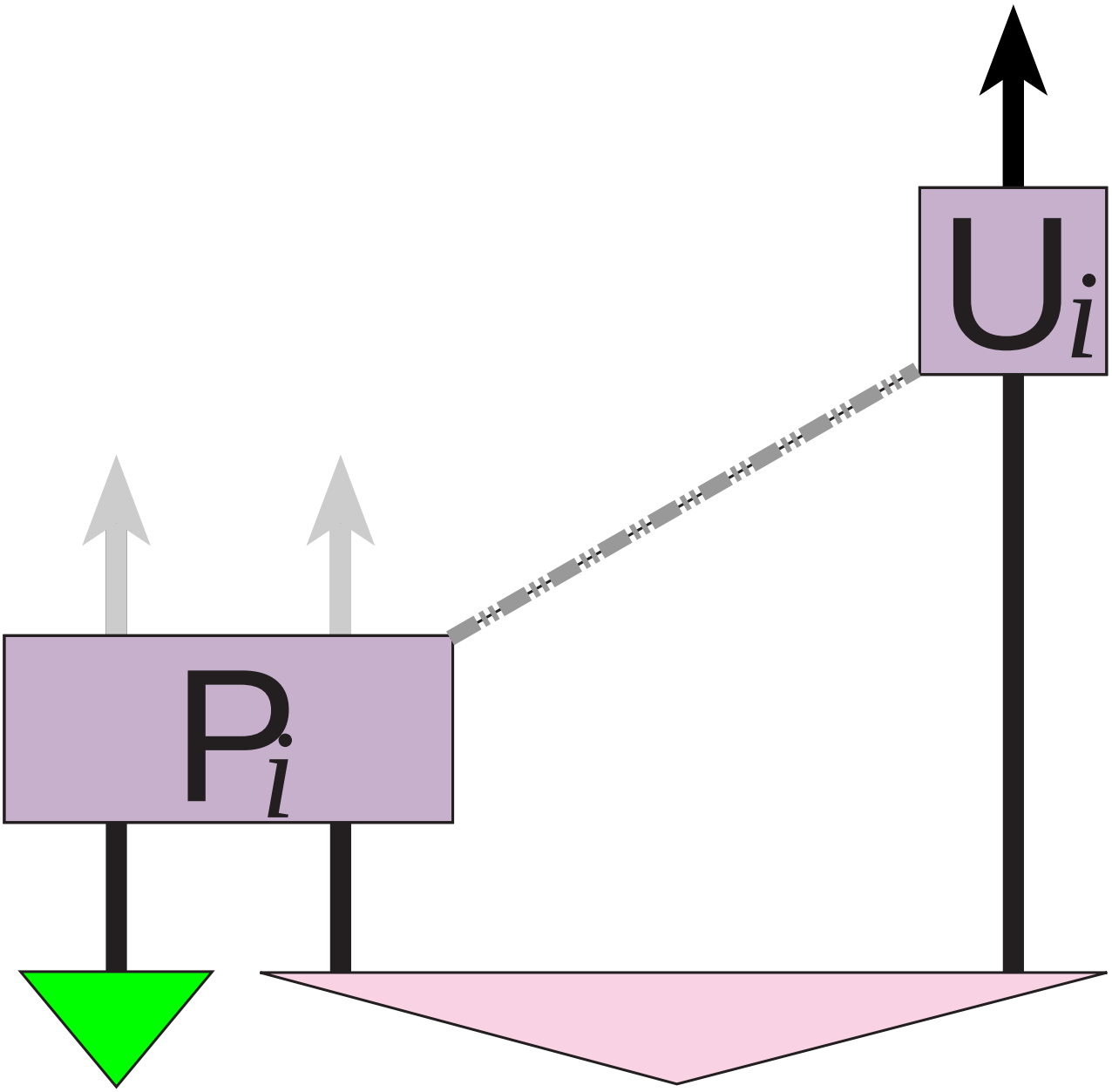
$$|\psi\rangle \;\mapsto\; \mathrm{P}_0(|\psi\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} z_1 \\ 0 \end{pmatrix} \sim \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|\psi\rangle \;\mapsto\; \mathrm{P}_1(|\psi\rangle) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ z_2 \end{pmatrix} \sim \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

What can we do with multiple qubits?

1. Quantum teleportation

theory: 1993; 1st experimental realisation: 1997

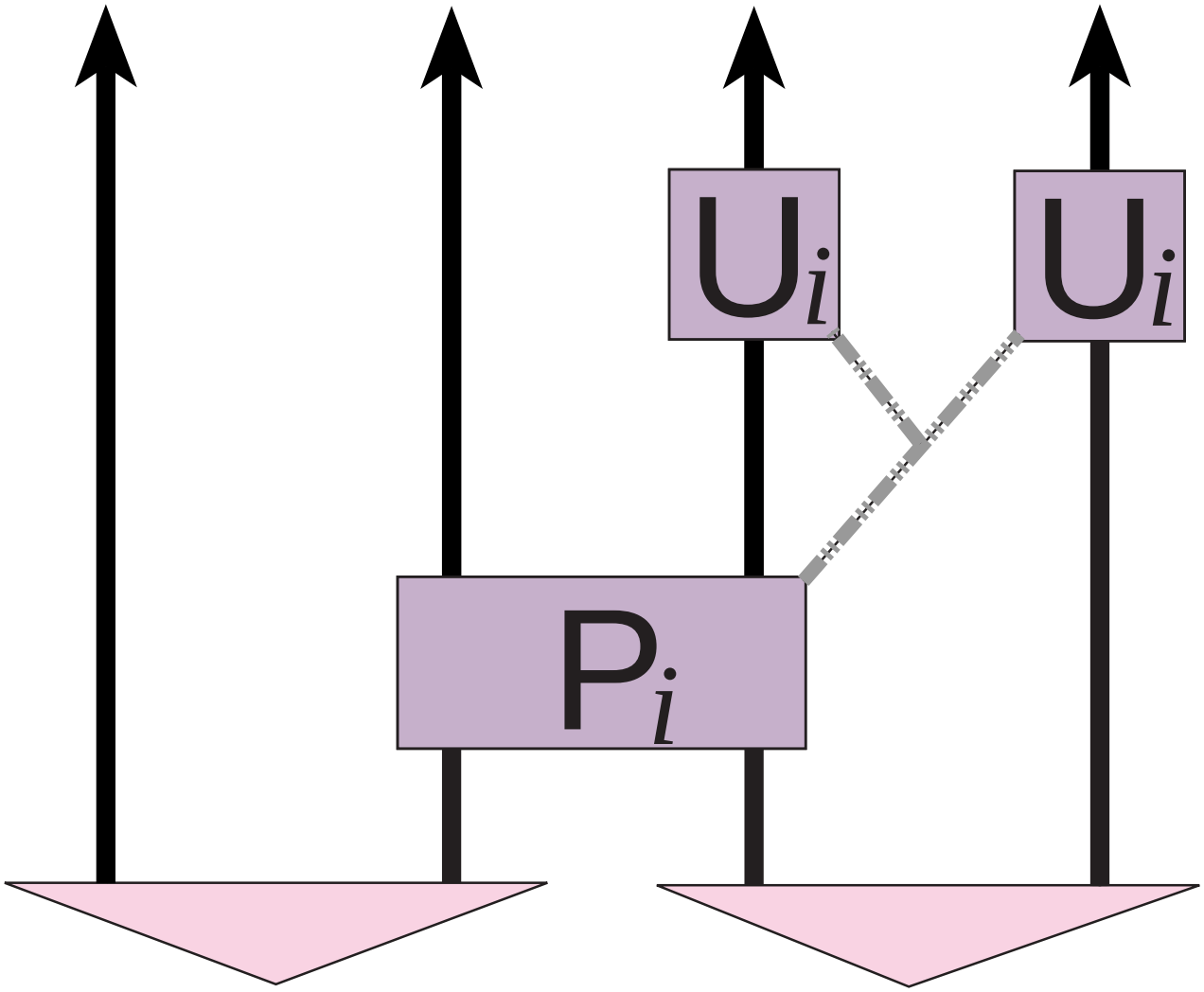


$\Rightarrow$ Transmit continuous data by finite means

What can we do with multiple qubits?

2. Entanglement swapping

theory: 1993; 1st experimental realisation: 2007



$\Rightarrow$ Entangle without touching

What can we do with multiple qubits?

3. Public key exchange

theory: 1984, ’91; you can buy one online

$\Rightarrow$ Can’t be cracked

4. Fast algorithms

theory: 1992, ’94, ’96; science fiction

$\Rightarrow$ Brings in research money and jobs!

Why this sudden new activity?

A bug became a feature, ...

after experimental confirmation of violation of the Bell inequalities by aspect and Gragnier in 1982.

Note in particular the time it took to discover quantum teleportation! (people weren't looking for it)

Exposing quantum phenomena is a 'balancing act':

- Exploit enlarged state space
- Avoid destruction of data by measurement

Most interesting are things which can't be done:

- No faster than light communication
- No hyper-entanglement (e.g. non-local boxes)

von Neumann's pure state formalism

What we won't talk about:

- Continuous time Schrödinger evolution.
- Continuous observable quantities.
- Spaces of observable values

---

pure state $\equiv$ 'closed system'

Definition. A finite-dimensional *Hilbert space* is a fd vector space $\mathcal{H}$ over the complex number field $\mathbb{C}$ with a *sesquilinear inner-product* i.e. a map

$$\langle - \mid - \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

which satisfies

$$\langle \psi | c_1 \cdot \psi_1 + c_2 \cdot \psi_2 \rangle = c_1 \langle \psi | \psi_1 \rangle + c_2 \langle \psi | \psi_2 \rangle$$

$$\langle c_1 \cdot \psi_1 + c_2 \cdot \psi_2 | \psi \rangle = \bar{c}_1 \langle \psi_1 | \psi \rangle + \bar{c}_2 \langle \psi_2 | \psi \rangle$$

$$\langle \psi | \phi \rangle = \overline{\langle \phi | \psi \rangle} \qquad \langle \psi | \psi \rangle \in \mathbb{R}^+ \quad \langle \psi | \psi \rangle = 0 \Leftrightarrow \psi = \mathbf{0}$$

for all $c_1, c_2 \in \mathbb{C}$ and all $\psi, \psi_1, \psi_2 \in \mathcal{H}$.

The condition

$$\forall \psi \in \mathcal{H}_1, \phi \in \mathcal{H}_2 : \quad \langle f^\dagger(\phi)|\psi\rangle = \langle \phi | f(\psi)\rangle$$

defines the (always existing and unique) **adjoint**

$$f^\dagger : \mathcal{H}_2 \to \mathcal{H}_1 \qquad \text{of} \qquad f : \mathcal{H}_1 \to \mathcal{H}_2.$$

We have $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$ i.e. $(-)^\dagger$ is contravariant.

A linear operator is **unitary** if, equivalently,

- its inverse exist and is equal to its adjoint,
- it preserves the inner-product.

Rays are subspaces spanned by a single vector i.e.

$$\mathsf{span}(\psi) = \{c \cdot \psi \mid c \in \mathbb{C}\}.$$

Postulate 1. [states and transformations] The state of a quantum system $\mathcal{S}$ is described by a ray in a Hilbert space $\mathcal{H}$. Deterministic transformations of $\mathcal{S}$ are described by unitary operators acting on $\mathcal{H}$.

Self-adjoint operators satisfy $H^\dagger = H$ i.e.

$$\langle H(\phi)|\psi\rangle = \langle\phi|H(\psi)\rangle.$$

Self-adjoint idempotent operators $\mathrm{P} : \mathcal{H} \to \mathcal{H}$, i.e.

$$\mathrm{P} \circ \mathrm{P} = \mathrm{P} = \mathrm{P}^\dagger\,,$$

are called **projectors**.

Special examples of projectors on $\mathcal{H}$ are the identity

$$1_{\mathcal{H}} : \mathcal{H} \to \mathcal{H} :: \psi \mapsto \psi$$

and the *zero-operator*

$$O_{\mathcal{H}} : \mathcal{H} \to \mathcal{H} :: \psi \mapsto \mathbf{0}\,.$$

Proposition. Each self-adjoint operator $H : \mathcal{H} \to \mathcal{H}$ admits a so-called **spectral decomposition**

$$H = \sum_i a_i \cdot \mathrm{P}_i$$

where all $a_i \in \mathbb{R}$ and all $\mathrm{P}_i : \mathcal{H} \to \mathcal{H}$ are projectors which are *mutually orthogonal* i.e.

$$\mathrm{P}_i \circ \mathrm{P}_j = O_{\mathcal{H}} \qquad \text{for} \qquad i \neq j.$$

Postulate 2. [measurements] A measurement on a quantum system is described by a self-adjoint operator. The set $\{a_i\}$ in the operator's spectral decomposition are the *measurement outcomes* while the set of projectors $\{\mathrm{P}_i\}$ describes the *change of the state* that takes place during a measurement.

In particular, when a measurement takes place:

1. The initial state ψ undergoes one of the transitions
$$\mathrm{P}_i :: \psi \mapsto \mathrm{P}_i(\psi)$$
and the probability of the possible transitions is
$$\mathsf{prob}(\mathrm{P}_i, \psi) = \langle \psi | \mathrm{P}_i(\psi) \rangle$$
where ψ needs to be normalized.
2. The *observer* which performs the measurement receives the value a_i as a token-witness of that fact.

Remark. The measurements represented by
$$\sum_i a_i \cdot \mathrm{P}_i \qquad \text{and} \qquad \sum_i i \cdot \mathrm{P}_i$$
are 'equivalent', in particular, the latter is completely determined by the set $\{\mathrm{P}_i\}_i$.

The **direct sum**

$$\mathcal{H}_1 \oplus \mathcal{H}_2 := \{(\psi, \phi) \mid \psi \in \mathcal{H}_1, \phi \in \mathcal{H}_2\}$$

enables embedding of *states of subsystems* via

$$\iota_1 : \mathcal{H}_1 \to \mathcal{H}_1 \oplus \mathcal{H}_2 :: \psi \mapsto (\psi, \mathbf{0})$$
$$\iota_2 : \mathcal{H}_2 \to \mathcal{H}_1 \oplus \mathcal{H}_2 :: \psi \mapsto (\mathbf{0}, \psi)\,.$$

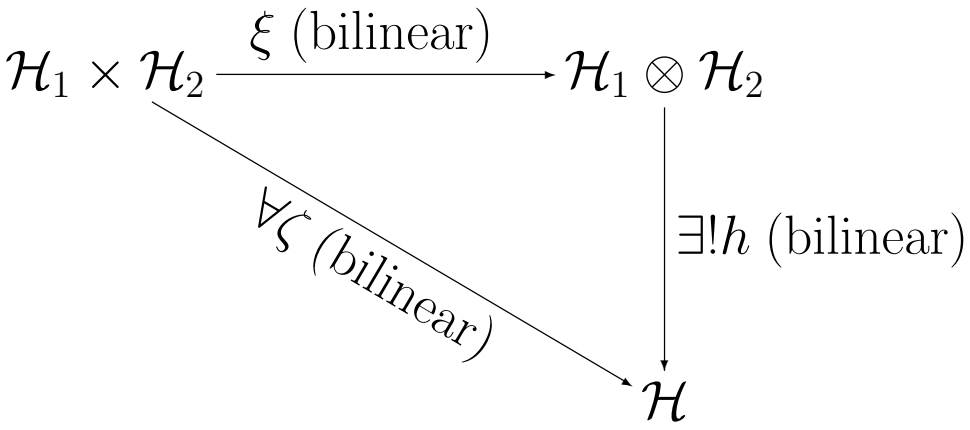
A base for $\mathcal{H}_1 \oplus \mathcal{H}_2$ arises canonically as

$$\{(e_1, \mathbf{0}), \ldots, (e_n, \mathbf{0}), (\mathbf{0}, e'_1), \ldots, (\mathbf{0}, e'_n)\}\,.$$

The **tensor product**

$$\mathcal{H}_1 \otimes \mathcal{H}_2 := \frac{\{\sum_i \alpha_i(\psi_i, \phi_i) \mid \psi_i \in \mathcal{H}_1, \phi_i \in \mathcal{H}_2\}}{\sum_i \alpha_i((\sum_j \beta_j \psi_{ij}), \phi_i) \sim \sum_{ij} \alpha_i \beta_j (\psi_{ij}, \phi_i)}$$

enables embedding of *subsystems* (but not states!) via



A base for $\mathcal{H}_1 \otimes \mathcal{H}_2$ arises canonically as

$$\{e_1, \ldots, e_n\} \times \{e'_1, \ldots, e'_n\}\,.$$

$$dim(\mathcal{H}_1 \oplus \mathcal{H}_2) = dim(\mathcal{H}_1) + dim(\mathcal{H}_2),$$
$$dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = dim(\mathcal{H}_1) \times dim(\mathcal{H}_2).$$

Inner product for $\oplus$ is:

$$\langle(\psi, \psi')|(\phi, \phi')\rangle = \langle\psi|\phi\rangle + \langle\psi'|\phi'\rangle\,.$$

On *pure tensors* $\psi \otimes \psi' = (\psi, \psi')$ for $\otimes$ it is:

$$\langle\psi \otimes \psi' \mid \phi \otimes \phi'\rangle = \langle\psi|\phi\rangle \times \langle\psi'|\phi'\rangle\,.$$

Map-state duality

$$\mathcal{H}_1^* \otimes \mathcal{H}_2 \simeq \mathcal{H}_1 \multimap \mathcal{H}_2$$

shows that $\otimes$ describes functions, not pairs!

Postulate 3. [compound systems] The joint state of a compound quantum system consisting of two subsystems is described by the tensor product of the Hilbert spaces which describe the two subsystems.

Non-local correlations

The **Bell-state** and **EPR-state**

$\mathsf{Bell} := e_1 \otimes e_1 + e_2 \otimes e_2 \qquad \mathsf{EPR} := e_1 \otimes e_2 - e_2 \otimes e_1$

respectively correspond to the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} .$$

i.e. the Bell-state corresponds to the identity.

Since there are no $a_1, a_2, a_3, a_4 \in \mathbb{C}$ such that either

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

the Bell-state and the EPR-state are truly **entangled**.

But if we measure the left system i.e. we apply

$$\{\mathrm{P}_1 \otimes \mathsf{id}, \mathrm{P}_2 \otimes \mathsf{id}\}$$

to the whole system we obtain

$(\mathrm{P}_1 \otimes \mathsf{id})(\mathsf{Bell}) = e_1 \otimes e_1 \qquad (\mathrm{P}_1 \otimes \mathsf{id})(\mathsf{EPR}) = e_1 \otimes e_2$

$(\mathrm{P}_2 \otimes \mathsf{id})(\mathsf{Bell}) = e_2 \otimes e_2 \qquad (\mathrm{P}_2 \otimes \mathsf{id})(\mathsf{EPR}) = e_2 \otimes e_1$

that is, we get a certain answer if next we apply

$$\{\mathsf{id} \otimes \mathrm{P}_1, \mathsf{id} \otimes \mathrm{P}_2\} .$$

Hence we witness here a **'non-local'** spatial effect.

The no-cloning 'theorem'

For an initial state $\psi \otimes \phi_0 \in \mathcal{H}$, by means of some

$$U : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$$

we wish to obtain $\psi \otimes \psi$, *clone* the state of the first quantum system to the second quantum system.

Assume we can do this for $\psi := \psi_1$ and $\psi := \psi_2$ i.e.

$$U(\psi_1 \otimes \phi_0) = \psi_1 \otimes \psi_1 \quad \text{and} \quad U(\psi_2 \otimes \phi_0) = \psi_2 \otimes \psi_2.$$

Taking the inner-product of the above equalities yields

$$\langle U(\psi_1 \otimes \phi_0) | U(\psi_2 \otimes \phi_0) \rangle = \langle \psi_1 \otimes \psi_1 | \psi_2 \otimes \psi_2 \rangle \,,$$

that is, by $U^\dagger = U^{-1}$,

$$\langle \psi_1 | \psi_2 \rangle \langle \psi_0 | \psi_0 \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1 | \psi_2 \rangle$$

and hence, assuming that all vectors are normalized,

$$\langle \psi_1 | \psi_2 \rangle = \langle \psi_1 | \psi_2 \rangle^2$$

which forces

$$\langle \psi_1 | \psi_2 \rangle = 0 \quad \text{or} \quad \langle \psi_1 | \psi_2 \rangle = 1$$

i.e. ψ_1 and ψ_2 need to be either equal or orthogonal,

so we cannot clone arbitrary states!

Dirac notation

In literature:

- 'merely' a quite convenient notation,
- too informal and mathematically unsound.

For us

- step-stone to high-level formalism,
- initiates purely graphical notation,

When representing $\psi \in \mathcal{H}$ to be

$$\psi : \mathbb{C} \to \mathcal{H} :: 1 \mapsto \psi$$

Dirac notation is formally justified by letting

- $|\psi\rangle := \psi$ and called *KET* ,
- $\langle\psi| := \psi^\dagger$ and called *BRA*,
- concatenation be composition,

so the inner-product is a *BRA-KET*:

linear map	matrix	Dirac notation
$\psi^\dagger \circ \phi$	$\begin{pmatrix} \bar{c}_1 & \dots & \bar{c}_m \end{pmatrix} \begin{pmatrix} c'_1 \\ \vdots \\ c'_m \end{pmatrix}$	$\langle \psi \mid \phi \rangle$

A projector on the ray spanned by $|\psi\rangle$ is a *KET-BRA*:

linear map	matrix	Dirac
$\psi \circ \psi^\dagger$	$\begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \begin{pmatrix} \bar{c}_1 & \dots & \bar{c}_m \end{pmatrix}$	$\mathrm{P}_\psi := \|\psi\rangle\langle\psi\|$

linear map	matrix	Dirac
$f \circ \psi$	$\begin{pmatrix} m_{11}\dots m_{1m} \\ \vdots \quad\quad \vdots \\ m_{n1}\dots m_{nm} \end{pmatrix} \begin{pmatrix} c'_1 \\ \vdots \\ c'_m \end{pmatrix}$	$f\|\psi\rangle$
$\phi^\dagger \circ f$	$\begin{pmatrix} \bar{c}_1 & \dots & \bar{c}_m \end{pmatrix} \begin{pmatrix} m_{11}\dots m_{1m} \\ \vdots \quad\quad \vdots \\ m_{n1}\dots m_{nm} \end{pmatrix}$	$\langle\phi\|f$
$\phi^\dagger \circ f \circ \psi$	$\dots = \sum_i \bar{c}'_i m_{ij} c_j \in \mathbb{C}$	$\langle\phi\|f\|\psi\rangle$

For projectors on a ray $\mathrm{P}_\phi = |\phi\rangle\langle\phi|$ probabilities are

$$\langle\psi|\mathrm{P}_\phi|\psi\rangle = \langle\psi|\phi\rangle\langle\phi|\psi\rangle = |\langle\phi|\psi\rangle|^2 .$$

Also,

$$\mathrm{P}_\psi \circ \mathrm{P}_\phi = |\psi\rangle\underline{\langle\psi|\phi\rangle}\langle\phi| = O_{\mathcal{H}}$$

if and only if $\langle\psi|\phi\rangle = \mathbf{0}$ i.e. ψ and ϕ are orthogonal.

Base for $\mathcal{H} \otimes \mathcal{H}'$ iss $|\, i\,\rangle \otimes |\, j\,\rangle$, $|\, i\,\rangle|\, j\,\rangle$ or $|\, ij\,\rangle$. Is

$$(|\psi\rangle\langle\psi|)(|\phi\rangle\langle\phi|)$$

either as a composition or a tensor i.e.

$$|\psi\rangle\langle\psi|\phi\rangle\langle\phi| \qquad \text{or} \qquad |\psi \otimes \phi\rangle\langle\psi \otimes \phi| \,?$$

Examples are:

$$Bell := |\, 00\rangle + |\, 11\rangle$$
$$EPR := |\, 01\rangle - |\, 10\rangle$$
$$GHZ := |\, 000\rangle + |\, 111\rangle$$
$$W := |\, 100\rangle + |\, 010\rangle + |\, 001\rangle$$

Usually one introduces a normalization e.g.

$$\frac{1}{\sqrt{2}}\,(|\, 00\rangle + |\, 11\rangle) \qquad \text{and} \qquad \frac{1}{\sqrt{2}}\,(|\, 000\rangle + |\, 111\rangle)$$

Bell-base and Bell/'Pauli'-matrices

While a *standard 2-qubit measurement*

$$\{|00\rangle\langle 00|, |01\rangle\langle 01|, |10\rangle\langle 10|, |11\rangle\langle 11|\}$$

is against the *computational base*

$$|00\rangle \qquad |01\rangle \qquad |10\rangle \qquad |11\rangle$$

a *Bell-base measurement* is against the *Bell-base*

$$|00\rangle + |11\rangle \quad |00\rangle - |11\rangle \quad |01\rangle + |10\rangle \quad |01\rangle - |10\rangle.$$

It can be obtained by respectively applying *Bell-matrices*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

to the second qubit of the Bell-state.

Quantum teleportation

The 1st qubit is in state

$$|\psi\rangle = c_0 \cdot |0\rangle + c_1 \cdot |1\rangle,$$

and the 2nd and 3rd one are in the Bell-state.

Perform Bell-base measurement on 1st and 2nd qubit.

When obtaining the i-th outcome perform the transposed to the i-th Bell-matrix on the 3rd qubit.

Lemma 1 $(\langle Bell| \otimes 1) \circ (1 \otimes |Bell\rangle) = 1$

$= \langle 0|\otimes|0\rangle + \langle 1|\otimes|1\rangle = |0\rangle\langle 0| + |1\rangle\langle 1| = 1$

Lemma 2: $(f \otimes 1)|Bell\rangle = (1 \otimes f^T)|Bell\rangle$

$\sum_i f(|i\rangle)|i\rangle = \sum_{ij} f_{ji}|ji\rangle = \sum_{ij} f^T_{ij}|ji\rangle = \sum_j |j\rangle f(|ij\rangle)$

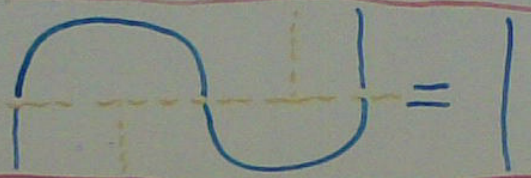
Teleportation: $(1 \otimes 1 \otimes M_i^\dagger) \circ (\langle Bell| \otimes 1) \circ (1 \otimes |Bell\rangle)$

$(\langle Bell| \otimes 1) \circ (1 \otimes M_i^\dagger \otimes 1)$ ⋮

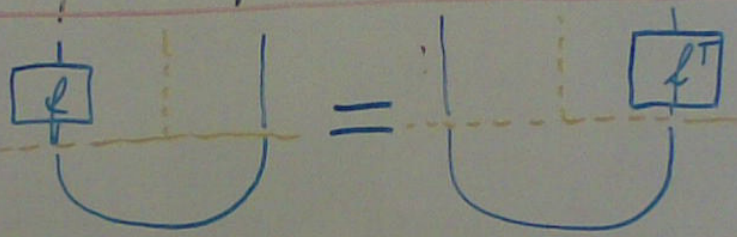
$(1 \otimes 1 \otimes \overline{M_i}) \circ (1 \otimes |Bell\rangle)$

Lemma 1 $\Rightarrow = 1$

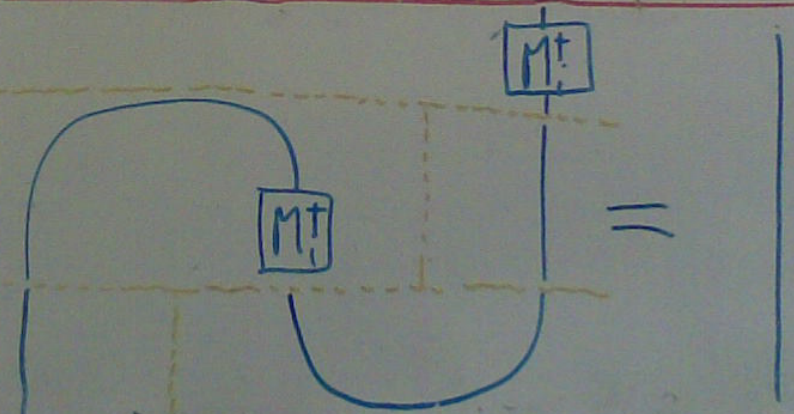
Lemma 1: $(\langle Bell| \otimes 1) \circ (1 \otimes |Bell\rangle) = 1$



Lemma 2: $(f \otimes 1)|Bell\rangle = (1 \otimes f^T)|Bell\rangle$



Teleportation: $(1 \otimes 1 \otimes M_i^\dagger) \circ (\langle Bell_i| \otimes 1) \circ (1 \otimes |Bell\rangle)$



Trace

For $f : \mathcal{H} \to \mathcal{H}$ there exists a unique scalar

$$\mathrm{Tr}(f) = \sum_i \langle i \,|f|\, i\rangle = \sum_i f_{ii}$$

which is independent of the choice of the base.

$$\mathrm{tr}(f) = \langle Bell|(1_{\mathcal{H}} \otimes f)|Bell\rangle.$$

$$\begin{aligned}\langle Bell|(1_{\mathcal{H}} \otimes (f \circ g))|Bell\rangle \\ = \langle Bell|(1_{\mathcal{H}} \otimes (g \circ f))|Bell\rangle\,.\end{aligned}$$

For

$$f : \mathcal{H} \otimes \mathcal{H}_1 \to \mathcal{H} \otimes \mathcal{H}_2$$

we can now also define

$$\mathrm{tr}^{\mathcal{H}}_{\mathcal{H}_1,\mathcal{H}_2}(f) := (\langle Bell| \otimes 1_{\mathcal{H}_2})(1_{\mathcal{H}} \otimes f)(|Bell\rangle \otimes 1_{\mathcal{H}_1}).$$

$$\mathrm{tr}^{\mathcal{H}}_{\mathcal{H}_1,\mathcal{H}_2}(|\Psi_g\rangle\langle\Psi_f|) = g \circ f^\dagger.$$

von Neumann's mixed state formalism

A more general notion is needed to describe:

1. Lack of complete knowledge on actual state.
2. Large statistical ensembles of systems.
3. Subsystems of a bigger entangled systems.
4. Non-isolated (=open) quantum systems.

A **density operator** is a linear map which is:

- positive i.e. of form $\rho = g^\dagger \circ g$ – so self-adjoint;
- has trace equal to one.

Postulate [extension to mixed states]. The state of a system is a density operator $\rho : \mathcal{H} \to \mathcal{H}$. Deterministic transformations correspond to $\rho \mapsto U \circ \rho \circ U^\dagger$ where $U : \mathcal{H} \to \mathcal{H}$ is unitary. Pure measurements are described by a set of projectors $\{\mathrm{P}_i : \mathcal{H} \to \mathcal{H}\}_i$ with $\sum_i \mathrm{P}_i = 1_{\mathcal{H}}$ and they cause a state transition

$$\rho \mapsto \frac{\mathrm{P}_i \circ \rho \circ \mathrm{P}_i}{\mathrm{Tr}(\mathrm{P}_i \circ \rho)}$$

and this transition happens with probability $\mathrm{Tr}(\mathrm{P}_i \circ \rho)$.

Probabilistic lack of knowledge. Consider a family of pure states $\{\psi_i\}_i$ with probabilistic weights $\{\omega_i\}_i$.

The probability for a certain outcome in a measurement is the weighted sum of individual probabilities:

$$\begin{aligned}\sum_j \omega_j \langle\psi_j|\mathrm{P}_i|\psi_j\rangle &= \sum_j \omega_j \mathrm{Tr}\left(\mathrm{P}_i \circ |\psi_j\rangle\langle\psi_j|\right) \\ &= \mathrm{Tr}(\mathrm{P}_i \circ (\sum_j \omega_j |\psi_j\rangle\langle\psi_j|)) \\ &= \mathrm{Tr}(\mathrm{P}_i \circ \rho)\,.\end{aligned}$$

$\sum_j \omega_j |\psi_j\rangle\langle\psi_j|$ is indeed a density matrix:

- Since $\langle\phi|\psi_j\rangle\langle\psi_j|\phi\rangle = |\langle\phi|\psi_j\rangle|^2 \geq 0$ hence
$$\sum_j \omega_j \langle\phi|\psi_j\rangle\langle\psi_j|\phi\rangle = \langle\phi|(\sum_j \omega_j |\psi_j\rangle\langle\psi_j|)|\phi\rangle \geq 0$$
- $\mathrm{Tr}(\sum_j \omega_j |\psi_j\rangle\langle\psi_j|) = \sum_j \omega_j \mathrm{Tr}(|\psi_j\rangle\langle\psi_j|) \ = 1$

Conversely, all mixed states clearly arise in this way.

Part of a larger system. We now have $|\Phi\rangle \in \mathcal{K} \otimes \mathcal{H}$.

A measurement of $\mathcal{H}$ 'alone' is realised by $\{1_{\mathcal{K}} \otimes \mathrm{P}_i\}_i$ where $\{\mathrm{P}_i : \mathcal{H} \to \mathcal{H}\}_i$ a measurement of $\mathcal{H}$. Hence the respective probabilities are

$$\begin{aligned}\langle\Phi|(1_{\mathcal{K}} \otimes \mathrm{P}_i)|\Phi\rangle &= \langle Bell|(1_{\mathcal{K}} \otimes (f^\dagger \circ \mathrm{P}_i \circ f))|Bell\rangle \\ &= \mathrm{Tr}(f^\dagger \circ \mathrm{P}_i \circ f) \\ &= \mathrm{Tr}(\mathrm{P}_i \circ f \circ f^\dagger) \\ &= \mathrm{Tr}(\mathrm{P}_i \circ \rho)\end{aligned}$$

$f \circ f^\dagger$ is indeed a density matrix:

- It is positive.
- $\mathrm{Tr}(f \circ f^\dagger) = \langle\Phi|\Phi\rangle = 1$ for $|\Phi\rangle$ is normalised.

All mixed states arise in this way by setting $f := \sqrt{\rho}$.