Main points from intro [ZCZW19]:

- Classical phases of matter described by Landau's theory of symmetry breaking
- Fractional quantum hall (FQH) states discovered in 1989 led to discovery of new topological phases/order with emergent particle physics with fractional charge
- Entanglement has no classical counterpart, and topological order comes from many-body entanglement
- Quantum theory unifies information and matter

Main points from intro `http://web.math.ucsb.edu/~zhenghwa/data/course/cbms.pdf`:

- Beyond Shor's factoring algorithm, quantum computers could be used to simulate quantum many-body systems and quantum field theories
- Emergent quasiparticles from quantum systems like FQH are called *anyons* as they need not have integer (*boson*), half-integer (*fermion*), or quarter-integer (*semion*) statistics.
- Anyons can be used to perform topological quantum computation, which is manifestly fault-tolerant. Moreover, some anyonic systems are universal for quantum computation.
- Mathematically, anyons are simple objects in a *unitary modular tensor category*

Basic outline of the course:

- Basics of quantum information theory [ZCZW19, Ch. 1-3]
- Local Hamiltonian lattice models (Ising, Potts, transverse field Ising), quantum error correction codes (Toric code), Gapped quantum systems, entanglement area law, [ZCZW19, Ch. 4-5]
- Basics of tensor categories [EGNO15]
- UMTC of localized excitations [SKK20, **?**], topological order and ground state degeneracy, string-net condensation [ZCZW19, Ch. 6]
- Higher linear algebra [HV19], condensations in higher categories [GJF19, JF20]
- Phase transitions: anyon condensation, gauging, condensing domain walls

## 1. Basics of quantum information

To understand entanglement of quantum many-body systems, we must have a basic understanding of quantum information.

1.1. **Basics of probability.** We rapidly recall some basic notions from probability theory.

- A *probability space* is a measure space $(\Omega, \mathcal{F}, \mathbb{P})$ where $\mathbb{P}(\Omega) = 1$.
- A *random variable* is a (Borel measurable) function $X : \Omega \to \mathbb{C}$.
- The *push-forward measure* of $\mathbb{P}$ to $\mathbb{C}$ via $X$ is given by $p_X(E) := \mathbb{P}(X^{-1}(E))$.
- The *expected value* of $X$ is $\mathbb{E}(X) := \int X(\omega)\, \mathrm{d}\mathbb{P}(\omega)$.
- The *correlation* of $X, Y$ is $C(X, Y) := \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y)$.

We will concern ourselves with finite spaces $\Omega$, which drastically simplifies the above.

**Definition 1.1.1.** A *bit* is a random variable which only takes the values $0, 1$.

**Notation 1.1.2.** Sometimes we will identify a random variable $X : \Omega \to \mathbb{C}$ with its image $X \subset \mathbb{C}$. We then write $p_X(x) := \mathbb{P}(X^{-1}(\{x\}))$ for the push-forward measure, and by convention, we can remove from $X$ any points for which $p_X(x) = 0$. If there is only one random variable $X$ around, we just write $p$. In this case, $\mathbb{E}(X) = \sum_{x \in X} xp(x)$.

**Example 1.1.3.** Suppose we roll a fair die, so $\Omega = \{1, \ldots, 6\}$, and $\mathbb{P}(1) = \cdots = \mathbb{P}(6) = 1/6$. Let $X$ denote the number of 6's in 3 rolls. Then $p_X(j) = \binom{3}{j}(5/6)^{3-j}(1/6)^j$ for $j = 0, 1, 2, 3$, which is the binomial distribution.

Often in quantum information, there are two 'players' Alice and Bob who are performing joint experiments. Classically, Alice ($A$) has probability space $(\Omega_A, \mathbb{P}_A)$ , and Bob ($B$) has probability space $(\Omega_B, \mathbb{P}_B)$. The *joint probability space* is $\Omega_A \times \Omega_B$, on which we may consider any *joint probability distribution* $\mathbb{P}_{AB}$. The *conditional probability* of $\omega_A$ given $\omega_B$ is

$$\mathbb{P}_{A|B}(\omega_A|\omega_B) := \frac{\mathbb{P}_{AB}(\omega_A, \omega_B)}{\mathbb{P}_B(\omega_B)},$$

and similarly for $\mathbb{P}_{B|A}$.

**Exercise 1.1.4.** The following are equivalent for $(\Omega_A, \mathbb{P}_A)$, $(\Omega_B, \mathbb{P}_B)$, and $(\Omega_A \times \Omega_B, \mathbb{P}_{AB})$:

(1) $\mathbb{P}_{AB}(\omega_A, \omega_B) = \mathbb{P}_A(\omega_A)\mathbb{P}_B(\omega_B)$ for all $\omega_A \in \Omega_A$ and $\omega_B \in \Omega_B$.
(2) $\mathbb{P}_{A|B}(\omega_A|\omega_B) = \mathbb{P}_{A|B}(\omega_A|\omega'_B)$ for all $\omega_A \in \Omega_A$ and $\omega_B, , \omega'_B \in \Omega_B$
(3) Similar to (2) with roles of $A$ and $B$ swapped.
(4) For all random variables $X_A$ on $\Omega_A$ and $X_B$ on $\Omega_B$, $\mathbb{E}_{AB}(X_A X_B) = \mathbb{E}_A(X_A)\mathbb{E}_B(X_B)$, i.e., $C(X_A, X_B) = 0$.

In this case, we say that $\mathbb{P}_{AB}$ does not have correlation.

1.2. **Shannon entropy and mutual information.** Suppose you roll 2 dice and you measure the sum of the values. Observe that you learn more information from an outcome of 2 than you do from an outcome of 7. If we wanted to define an 'information function' $h : (0, 1] \to \mathbb{R}_{\geq 0}$ that can applied to a probability distribution $\{p_i\}$, it is natural to ask for the following properties:

(I1) $h$ is *strictly decreasing* with $\lim_{p \to 0+} h(p) = \infty$ and $h(1) = 0$, as observing an unlikely event gives more information than observing a likely event. Observing an event that is certain to happen yields no information, and one cannot measure an event that has no change of happening.
(I2) $h(pq) = h(p) + h(q)$, since the information obtained from observing independent events should be the sum of the information of observing each event individually.

**Exercise 1.2.1.**

(1) Show that any continuous homomorphism $g : (\mathbb{R}, +) \to (\mathbb{R}, +)$ is of the form $g(x) = tx$ for some $t \in \mathbb{R}$. Deduce this result still holds for the semigroup $(\mathbb{R}_{>0}, +)$.
(2) Show that the only function $h : (0, 1] \to \mathbb{R}_{\geq 0}$ satisfying (I1) and (I2) which is continuous on $(0, 1]$ is $h(p) = -c \cdot \ln(p)$ where $c \in (0, \infty)$.
*Hint: Consider* $h|_{(0,1)} \to \mathbb{R}_{>0}$.

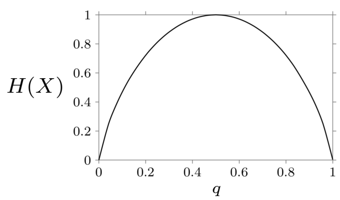
Since the constant $c > 0$ above is equivalent to a choice of base for the logarithm, we define $h(p) := -\log(p)$. The entropy of the distribution $\{p_i\}$ will be defined as $-\sum_i p_i \log(p_i)$, which is the average/expected information gained from observing a measurement. More entropy then means you gain more information from taking a measurement, which means the system is more disordered, i.e., in a more uncertain state.

**Definition 1.2.2.** Given a random variable $X$ on a finite probability space $(\Omega, \mathbb{P})$, the *(Shannon) entropy* of $X$ is

$$H(X) := -\sum_{x \in X} p(x) \log p(x),$$

where log means base 2. It is a measure of *uncertainty* of the random variable $X$ which only depends on $p$, and not the values of $X$.

**Example 1.2.3.** Suppose $X$ is a bit with probability distribution $p(0) = q$ and $p(1) = 1 - q$, like counting the number of heads in one flip of a weighted coin, or successes in one Bernoulli trial. Then $H(X) = -q \log q - (1-q)\log(1-q)$, called the *binary entropy function*.




[arXiv:1508.02595, p. 11]

**Exercise 1.2.4.** Suppose $\{p_i\}_{i=1}^N$ is some probability distribution on a finite set with $N$ elements. Prove that $H(\{p_i\}_{i=1}^N)$ is maximized by the uniform distribution.

**Definition 1.2.5.** Given random variables $X_A$ on $(\Omega_A, \mathbb{P}_A)$ and $X_B$ on $(\Omega_B, \mathbb{P}_B)$ and a joint probability distribution $\mathbb{P}_{AB}$ on $\Omega_A \times \Omega_B$, we have the following quantities:

- (joint entropy) $H(X, Y) := -\sum_{x,y} p(x, y) \log p(x, y)$
- (conditional entropy) $H(X|Y = y) := -\sum_x p(x|y) \log p(x|y)$, similarly $H(Y|X = x)$

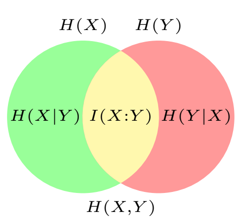
**Definition 1.2.6.** The *mutual information* for $(\Omega_A, \mathbb{P}_A, X_A)$ and $(\Omega_B, \mathbb{P}_B, X_B)$ is given by

$$I(X : Y) := \sum_{y \in Y} \sum_{x \in X} p(x, y) \log \left( \frac{p(x, y)}{p(x)p(y)} \right).$$

(Observe that by convention, $x \in X$ means that $p(x) \neq 0$!)

**Exercise 1.2.7.** Prove the following identities:

(1) $H(X) = H(X|Y) + I(X : Y)$
(2) $H(Y) = H(Y|X) + I(X : Y)$
(3) $H(X, Y) = H(X|Y) + H(Y|X) + I(X : Y)$.




(1.2.8)

adapted from [arXiv:1508.02595, p. 12]

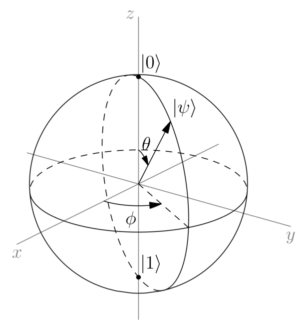
**Exercise 1.2.9.** Prove that $I(X : Y) = 0$ implies $C(X, Y) = 0$. Does the converse hold? *Hint: Observe* $I(X : Y) = 0$ *if and only if* $p(x, y) = p(x)p(y)$.

1.3. **Basics of quantum mechanics.** A *state vector* is a unit (norm 1) vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$; we denote the inner product by $\langle \cdot | \cdot \rangle$, which is linear on the right. Vectors are denoted by *kets* $|\eta\rangle$ and covectors (linear functionals) are denoted by *bras* $\langle\xi|$. Given a bounded operator $x \in B(H)$, the *adjoint* $x^\dagger \in B(H)$ is defined by $\langle\psi|x\phi\rangle = \langle x^\dagger\psi|\phi\rangle$ for all $\psi, \phi \in \mathcal{H}$ by the Riesz Representation Theorem.

**Principle of superposition:** Given orthogonal state vectors $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}$ and $c_1, c_2 \in \mathbb{C}$ with $|c_1|^2 + |c_2|^2 = 1$, $c_1|\psi_1\rangle + c_2|\psi_2\rangle \in \mathcal{H}$ is another state vector.

**Example 1.3.1.** The state vector of a free electron is a unit vector in $\mathbb{C}|0\rangle \oplus \mathbb{C}|1\rangle$, which is also called a *quantum bit* or *qubit*. Here, $|0\rangle$ is *spin up* and $|1\rangle$ is *spin down*. We can represent a qubit *up to a phase* in $U(1) := \{z \in \mathbb{C} | \, |z| = 1\}$ by a point on the surface of the *Bloch sphere*:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$




[arXiv:1508.02595, p. 14]

**Definition 1.3.2.** An *observable* is a self-adjoint (Hermitian) operator $M$ on $\mathcal{H}$. A *measurement* is an eigenvalue $\mu$ of $M$; the set of eigenvalues of $M$ is called the *spectrum* $\operatorname{spec}(M)$ of $M$. Since $\mathcal{H}$ is finite dimensional, by the spectral theorem, we can decompose $M$ canonically as a weighted sum of orthogonal projections:

$$M = \sum_{\mu \in \operatorname{spec}(M)} \mu p_\mu \qquad \sum_{\mu \in \operatorname{spec}(M)} p_\mu = \mathrm{id}_{\mathcal{H}} \qquad E_\mu := p_\mu\mathcal{H} = \{\eta \in H | M\eta = \mu\eta\}.$$

Given an observable $M$, its *avergage/expected value* in state vector $|\psi\rangle$ is

$$\langle M\rangle_\psi := \langle\psi|M|\psi\rangle := \langle\psi|M\psi\rangle.$$

When the system is in state vector $|\psi\rangle$, the probability of observing the measurement $\mu$ for $M$ is $\langle p_\mu\rangle = \langle\psi|p_\mu\psi\rangle$. Observe $\langle M\rangle$ and $\langle p_\mu\rangle$ are independent of the phase of $|\psi\rangle$.

**Definition 1.3.3.** The *Pauli spin matrices* in $M_2(\mathbb{C})$ are given by

$$X := \sigma_X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y := \sigma_Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z := \sigma_Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Observe that $\{I, X, Y, Z\}$ is a basis for $M_2(\mathbb{C})$.

**Example 1.3.4.** If we measure the Pauli $Z$ operator in the qubit state vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the probability of measuring 1 is $|\alpha|^2$, while the probability of measuring $-1$ is $|\beta|^2$. If we measure the Pauli $X$ operator in the same state vector, the probability of measuring $\pm 1$ is

$$\left\langle \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \middle| \frac{1}{2}\begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right\rangle = \frac{1}{2}\left\langle \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \middle| \begin{pmatrix} \alpha \pm \beta \\ \pm\alpha + \beta \end{pmatrix} \right\rangle = \frac{1}{2} \pm \operatorname{Re}(\alpha\overline{\beta}).$$

Whereas all random variables on a probability space share the same distribution, measurements do not. Thus we must choose an observable in order to assign a value of uncertainty.

**Definition 1.3.5.** A *Hamiltonian* of a quantum system is an (unbounded) self-adjoint/Hermetian operator $H$ acting on a (dense subset of) a Hilbert space $\mathcal{H}$. (Here, unbounded only applies to systems where $\mathcal{H}$ is infinite dimensional.) Eigenvalues of the Hamiltonian are meant to represent energy levels of the system. The time evolution of states is governed by Schrödinger's equation:

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle \qquad \rightsquigarrow \qquad |\psi(t)\rangle = e^{-itH/\hbar}|\psi(0)\rangle. \tag{1.3.6}$$

Note that even if $H$ is unbounded, $e^{-itH/\hbar}$ is always unitary. This means that time evolution of the system is reversible. In Heisenberg's formulation, time dependence lies on the observables $M$:

$$\langle\phi(t)|M|\psi(t)\rangle = \langle\phi(0)|\underbrace{e^{itH/\hbar}Me^{-itH/\hbar}}_{:=M(t)}|\psi(0)\rangle$$

Heisenberg's equation of motion for an observable $M$ is

$$i\hbar\frac{\partial}{\partial t}M = [M,H] := MH - HM$$

**Exercise 1.3.7.** Use Equation (1.3.6) to show that time evolution of a mixed state is given by

$$i\hbar\frac{\partial}{\partial t}\rho(t) = -[\rho(t),H]$$

Then show that $\rho(t) = e^{-itH/\hbar}\rho(0)e^{itH/\hbar}$ is a solution of the above differential equation. *Hint: $e^{\pm itH/\hbar}$ commutes with $H$.*

## 1.4. **States.**

**Definition 1.4.1.** A *state* on $B(\mathcal{H})$ is a linear functional $\omega : B(\mathcal{H}) \to \mathbb{C}$ such that $\omega(I) = 1$ and $x \geq 0$ ($\langle\psi|x\psi\rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$) implies $\omega(x) \geq 0$.

**Example 1.4.2.** A state vector $|\psi\rangle$ gives a *vector state* $\omega_\psi(x) := \langle\psi|x\psi\rangle$. Observe that the vector state corresponding to a state vector is independent of the phase.

**Exercise 1.4.3.**

(1) Show that $\omega_{\psi_1} = \omega_{\psi_2}$ if and only if $|\psi_1\rangle = c|\psi_2\rangle$ for some $c \in U(1)$.

(2) Recall that the *trace* on $B(\mathcal{H})$ is given by $\mathrm{Tr}(x) := \sum\langle\eta_i|x\eta_i\rangle$ where $\{|\eta_i\rangle\}$ is any orthonormal basis of $\mathcal{H}$. When $x$ is *normal* ($xx^\dagger = x^\dagger x$), $\mathrm{Tr}(x) = \sum_{\mu\in\mathrm{spec}(x)}\mu\dim(E_\mu)$.

Show that for every state $\omega$ on $B(\mathcal{H})$, there is a unique positive operator $\rho \in B(\mathcal{H})$ called the *density operator*[1] of $\omega$ such that $\omega(x) = \mathrm{Tr}(x\rho)$ for all $x \in B(\mathcal{H})$.

(3) Prove that the density operator $\rho$ of a state $\omega$ satisfies $\mathrm{Tr}(\rho^2) \leq 1$ with equality if and only if $\rho = |\psi\rangle\langle\psi|$ for some state vector $|\psi\rangle \in \mathcal{H}$.

**Vector states and density operators.** A vector state $|\psi\rangle \in H$ is really only physically relevant up to a phase in $U(1)$. The $U(1)$-orbit of $|\psi\rangle$ corresponds to the rank one density operator $|\psi\rangle\langle\psi| \in B(\mathcal{H})$, which is called a *pure state.* A non-trivial convex combination of pure states is called a *mixed state.*

[1]Sometimes, $\rho$ is called the (non-commutative) *Radon-Nikodym derivative* of $\omega$ with respect to Tr.

**Remark 1.4.4.** A mixed state is not in a superposition; rather, a mixed state is what we get by imposing classical probability theory on top of quantum mechanics.

First, a superposition really only makes sense with respect to a certain basis, which are the classical outcomes of a certain observable we would like to measure. For example, suppose Alice wants to measure the spin of an electron in state $|\psi\rangle \in \mathbb{C}^2$ which is in a superposition of $|0\rangle$ and $|1\rangle$. She measures Pauli $Z$; if she observes 1, then the electron is now in state $|0\rangle$, and if she measures -1, the electron is in state $|1\rangle$.

Suppose now $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ so that it is equally likely to measure either outcome, and that Bob measures the electron, but does not tell Alice the result. The electron is either in state $|0\rangle$ or $|1\rangle$, but Alice cannot tell which one; the state of the electron may then be described by the mixed state $\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}I$.

Indeed, a mixed state $\rho$ can be viewed as a classical probability distribution of a finite collection of pure states:

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i| \qquad\qquad 0 \le p_i \le 1,\ \sum_i p_i = 1.$$

Its von Neumann entropy is then equal to the Shannon entropy of the corresponding classical probability distribution $\{p_i\}$:

$$S(\rho) = -\operatorname{Tr}(\rho\log(\rho)) = -\operatorname{Tr}(\sum p_i \log(p_i)|\psi_i\rangle\langle\psi_i|) = -\sum p_i \log(p_i) = H(\{p_i\}).$$

However, observe that the same mixed state can be viewed in multiple ways as a distribution:

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i| = \sum q_j |\phi_j\rangle\langle\phi_j|.$$

But quantum mechanics cannot distinguish which probability distribution we have!

Some physicists/mathematicians think that in pure quantum mechanics, there are really only pure states; $|\psi\rangle$ describes the state of the universe, and it evolves in time with respect to some Hermitian/self-adjoint Hamiltonian $H$. However, our local information is not enough information to determine this global pure state $|\psi\rangle$. We can thus try and approximate the state based on certain reduced density matrices that we can measure using the principle of maximum entropy below in §1.8.

**Exercise 1.4.5.** An *extreme point* of a convex subset $S$ of a vector space $\mathcal{V}$ is a point $x \in S$ such that

$$x = ty + (1-t)z \text{ for some } 0 \le t \le 1 \qquad \Longrightarrow \qquad y = z = x.$$

Show that the pure states are the extreme points of the convex set of states on $B(\mathcal{H})$.
*Note: the state space is the convex hull of the pure states.*

**Exercise 1.4.6.**

(1) Prove that every mixed state in $B(\mathbb{C}^2)$ can be written as

$$\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}) = \frac{1}{2}(I + r_x X + r_y Y + r_z Z) = \frac{1}{2}\begin{pmatrix} 1 + r_z & r_x - ir_y \\ r_x + ir_y & 1 - r_z \end{pmatrix}$$

where $X, Y, Z$ are the Pauli matrices and $\vec{r} \in \mathbb{R}^3$ is called the *Bloch vector*.

(2) Deduce that the Bloch sphere is the state space of $M_2(\mathbb{C})$, and the interior corresponds to the mixed states. Which states lie at the intersection of the axes and the surface of the Bloch sphere?

(3) Calculate the eigenvalues of $\rho$ in terms of $\vec{r}$.

**Various notions of states.**

| | |
|---|---|
| state vector | norm 1 $\|\psi\rangle \in \mathcal{H}$ |
| state | positive linear functional $\omega$ on $B(H)$ with $\omega(I) = 1$ <br> or density operator $\rho \geq 0$ with $\mathrm{Tr}(\rho) = 1$ |
| vector state | $B(H) \ni x \mapsto \langle\psi\|x\psi\rangle \in \mathbb{C}$ where $\|\psi\rangle \in \mathcal{H}$ norm 1 |
| pure state | rank 1 projection $\rho = \|\psi\rangle\langle\psi\| \in B(H)$ |
| mixed state | non-trivial convex combination of orthogonal pure states |

One gets a vector state from a pure state by $x \mapsto \mathrm{Tr}(\rho x)$. Thus pure states correspond to state vectors modulo a phase in $U(1)$.

**Expected values of observables for various notions of states.**

| | |
|---|---|
| state vector $\|\psi\rangle$ <br> vector state $\omega_\psi$ <br> pure state $\|\psi\rangle\langle\psi\|$ | $\langle\psi\|M\psi\rangle$ |
| mixed state $\rho$ | $\mathrm{Tr}(M\rho)$ |

**Definition 1.4.7.** The *von Neumann entropy* of a state $\rho$ is given by

$$S(\rho) := -\operatorname{Tr}(\rho\log(\rho)).$$

Here, $\rho\log(\rho)$ is defined via the spectral theorem:

$$\rho = \sum_{\mu\in\operatorname{spec}(\rho)} \mu p_\mu \qquad \Longrightarrow \qquad \rho\log(\rho) = \sum_{\mu\in\operatorname{spec}(\rho)} \mu\log(\mu) p_\mu$$

where by convention, $0\log(0) = 0$.

**Exercise 1.4.8.** Show that von Neumann entropy $S$ is a continuous function from states on $B(\mathcal{H})$ to $[0,\infty)$.
*Hint: One could proceed as follows.*

(1) *For any convergent sequence of normal operators $a_n \to a$ in $B(\mathcal{H})$ and any open neighborhood $U$ of* $\operatorname{spec}(a)$*, eventually* $\operatorname{spec}(a_n) \subset U$.
(2) *For any convergent sequence of normal operators $a_n \to a$ in $B(\mathcal{H})$ and any open neighborhood $U$ of* $\operatorname{spec}(a)$ *and continuous $f : U \to \mathbb{C}$, $f(a_n) \to f(a)$.*

**Exercise 1.4.9.** Prove that the entropy is maximized at a unique point in the state space of $B(\mathcal{H})$. What is this point? For $\mathcal{H} = \mathbb{C}^2$, where does this point lie in the Bloch sphere?
*Hint: Use Exercise 1.2.4*

1.5. **Tensor products.** Given independent observers Alice ($A$) and Bob ($B$) with Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, the total Hilbert space is

$$\mathcal{H}_A \otimes \mathcal{H}_B := \operatorname{span}\{|\varphi\otimes\phi\rangle = |\varphi\rangle\otimes|\phi\rangle \,|\, |\varphi\rangle \in \mathcal{H}_A \text{ and } |\phi\rangle \in \mathcal{H}_B\}$$

subject to the relations

$$|c\psi_1 + \psi_2\rangle \otimes |\phi\rangle = c|\psi_1\rangle\otimes|\phi\rangle + |\psi_2\rangle\otimes|\phi\rangle \qquad |\psi\rangle\otimes|c\phi_1+\phi_2\rangle = c|\psi\rangle\otimes|\phi_1\rangle + |\psi\rangle\otimes|\phi_2\rangle,$$

with inner product

$$\langle \varphi_1 \otimes \phi_1 | \varphi_2 \otimes \phi_2 \rangle := \langle \varphi_1 | \varphi_2 \rangle_{\mathcal{H}_A} \cdot \langle \phi_1 | \phi_2 \rangle_{\mathcal{H}_B}.$$

**Notation 1.5.1.** When we have distinguished bases $\mathcal{B}_A$ for $\mathcal{H}_A$ and $\mathcal{B}_B$ for $\mathcal{H}_B$, we write $|\alpha\beta\rangle := |\alpha\rangle \otimes |\beta\rangle$ for $|\alpha\rangle \in \mathcal{B}_A$ and $|\beta\rangle \in \mathcal{B}_B$.

**Exercise 1.5.2.** If $\dim(\mathcal{H}_A) = d_A$ and $\dim(\mathcal{H}_B) = d_B$, then $\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = d_A d_B$.
*Hint: Show that given bases $\mathcal{B}_A$ for $\mathcal{H}_A$ and $\mathcal{B}_B$ for $\mathcal{H}_B$, $\{|\alpha\beta\rangle \,|\, |\alpha\rangle \in \mathcal{B}_A$ and $|\beta\rangle \in \mathcal{B}_B\}$ is a basis for $\mathcal{H}_A \otimes \mathcal{H}_B$.*

> **Tensor product composite:** The Hilbert space of a composite quantum system is the tensor product of all Hilbert spaces of its subsystems.

**Example 1.5.3.** The *computational basis* for an $N$-qubit state is $\{|i_1 \cdots i_N\rangle | i_1, \ldots, i_N \in \{0, 1\}\}$.

**Definition 1.5.4.** Recall that $B(\mathcal{H}_{AB}) \cong B(\mathcal{H}_A) \otimes B(\mathcal{H}_B)$. We have a canonical (non-normalized) *conditional expectation*

$$\mathbb{E}_A : B(\mathcal{H}_{AB}) \cong B(\mathcal{H}_A) \otimes B(\mathcal{H}_B) \to B(\mathcal{H}_A) \qquad\qquad x \otimes y \mapsto \mathrm{Tr}_B(y)x,$$

The conditional expectation of $x \in B(\mathcal{H}_{AB})$ is also determined by the following formula:

$$\langle \phi_1 | \mathbb{E}_A(x) | \phi_2 \rangle = \sum_{\beta \in \mathcal{B}_B} \langle \phi_1 \beta | x | \phi_2 \beta \rangle \qquad\qquad \forall |\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}_A.$$

**Remark 1.5.5.** Sometimes $\mathbb{E}_A$ is called the *partial trace* and denoted by $\mathrm{Tr}_B$ (rather than $\mathrm{id} \otimes \mathrm{Tr}_B$) by a slight abuse of notation. To avoid overloading the notation, we will stick to conditional expectations.

**Definition 1.5.6.** Given a *bipartite* (in tensor product) state vector $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, we get the *reduced density operator* $\rho_A^{\mathrm{red}} := \mathbb{E}_A(\rho_{AB})$ determined by the formula

$$\langle \phi_1 | \rho_A^{\mathrm{red}} \phi_2 \rangle = \sum_{\beta \in \mathcal{B}_B} \langle \phi_1 \beta | \psi_{AB} \rangle \langle \psi_{AB} | = | \phi_2 \beta \rangle \qquad\qquad \forall |\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}_A.$$

Conversely, given a state $\rho_B$, we can construct a state vector $|\psi_{AB}\rangle$ such that $\rho_B = \mathrm{Tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|)$ via *quantum state purification*. Just pick any ONB $\mathcal{B}_A$ for $\mathcal{H}_A$ and use a spectral decomposition of $\rho_B$:

$$\rho_B = \sum_{j=1}^{d_B} p_j |\beta_j\rangle\langle\beta_j| \qquad \rightsquigarrow \qquad |\psi_{AB}\rangle := \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} \sqrt{p_i} |\alpha_i \beta_j\rangle.$$

This depends on the choice of basis for the auxiliary system $A$.

**Exercise 1.5.7.** Show that any pure state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ has a *Schmidt decomposition*, i.e., there is a $d \leq \min\{d_A, d_B\}$, $p_1, \ldots, p_d > 0$ with $\sum_{i=1}^d p_i = 1$, and orthonormal sets $\{\alpha_1, \ldots, \alpha_d\} \subset \mathcal{H}_A$ and $\{\beta_1, \ldots, \beta_d\} \subset \mathcal{H}_B$ such that

$$|\psi_{AB}\rangle = \sum_{i=1}^{d} \sqrt{p_i} |\alpha_i \beta_i\rangle.$$

*Hint: Use quantum state purification for* $\rho_A^{\text{red}} = \mathbb{E}_A(|\psi_{AB}\rangle\langle\psi_{AB}|)$.
*Note: A high level proof uses the canonical isomorphism* $\mathcal{H}_A \otimes \mathcal{H}_B \cong \operatorname{Hom}(\mathcal{H}_A \to \overline{\mathcal{H}_B})$ *and polar decomposition.*

**Exercise 1.5.8.** Suppose we have a pure bipartite state in a Schmidt decomposition $|\psi_{AB}\rangle = \sum \sqrt{p_i}|\alpha_i\beta_i\rangle$. Compute the reduced density operators $\rho_A^{\text{red}}, \rho_B^{\text{red}}$.

1.6. **Quantum is not classical.**

**Example 1.6.1** (Einstein-Podolsky-Rosen (EPR) Paradox, *spooky action at a distance*)**.** Consider the *singlet state* (all electrons paired) $|EPR\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ in $\mathbb{C}^2 \otimes \mathbb{C}^2$. If $B$ measures $|0\rangle$ ($+1$ for Pauli $Z$), then $A$ has state $|1\rangle$. One might think that this means information has travelled faster than the speed of light, contradicting the theory of special relativity. However, before and after $B$'s measurement, $A$ still has the same reduced density matrix

$$\rho_A^{\text{red}} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}I.$$

If $B$ does not tell $A$ they have performed a measurement, then $A$ will not know the state has collapsed. So the information has not really travelled!

It is worth mentioning that if $A$ measures along a different axis than $B$, e.g., $X$ instead of $Z$, there is still a $\frac{1}{2}$ probability for either outcome.

**Example 1.6.2** (Bell's Inequality)**. TODO:**

**Exercise 1.6.3** (Greenberger-Horne-Zeilinger (GHZ) Paradox, *no hidden variables*)**.** Consider the *GHZ state vector* on $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2 \otimes \mathbb{C}_C^2$ given by

$$|GHZ\rangle := \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

(1) Prove that the operators $Z_A \otimes Z_B \otimes I_C$, $I_A \otimes Z_B \otimes Z_C$, and $X_A \otimes X_B \otimes X_C$ pairwise commute. Describe the finite group generated by these operators in terms of tensor products of Pauli operators.
(2) Show that $(X_A^a \otimes Z_B^b \otimes X_Z^c)|GHZ\rangle$ for $a, b, c \in \{0, 1\}$ are an orthonormal basis of eigenvectors for the commuting operators in (1) above. Deduce that $|GHZ\rangle$ spans the intersection of the eigenspaces $E_1$ for the commuting operators in (1) above.
(3) Compute $\langle X_A \otimes X_B \otimes X_C\rangle$, $\langle -Y_A \otimes Y_B \otimes X_C\rangle$, $\langle -Y_A \otimes X_B \otimes Y_C\rangle$, and $\langle -X_A \otimes Y_B \otimes Y_C\rangle$.
(4) Suppose that each of $X_i, Y_j, Z_k$ for $i, j, k \in \{A, B, C\}$ has a universal 'hidden value' in $\{\pm 1\}$ denoted by $v(-)$. Deduce this is impossible by considering the following four equalities:

$$\begin{aligned} v(X_A)v(X_B)v(X_C) &= \langle X_A \otimes X_B \otimes X_C\rangle \\ -v(Y_A)v(Y_B)v(X_C) &= \langle -Y_A \otimes Y_B \otimes X_C\rangle \\ -v(Y_A)v(X_B)v(Y_C) &= \langle -Y_A \otimes X_B \otimes Y_C\rangle \\ -v(X_A)v(Y_B)v(Y_C) &= \langle -X_A \otimes Y_B \otimes Y_C\rangle. \end{aligned}$$

*Hint: Each* $v(-)$ *appears exactly twice on the left, and* $(\pm 1)^2 = 1$.

**Example 1.6.4** (Diecks-Wootters-Zurek, *no cloning*)**.** Suppose $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}$, and fix a state $|\beta\rangle \in \mathcal{H}_B$. There is no unitary $u \in B(\mathcal{H} \otimes \mathcal{H})$ such that

$$u|\alpha\beta\rangle \in U(1)|\alpha\alpha\rangle \qquad \forall\, |\alpha\rangle \in \mathcal{H}_A.$$

Indeed, if $|\alpha\rangle, |\gamma\rangle \in \mathcal{H}_A$, then

$$\langle\gamma|\alpha\rangle_A = \langle\gamma\beta|\alpha\beta\rangle_{AB} = \langle\gamma\gamma|u^\dagger u|\alpha\alpha\rangle_{AB} \in U(1)\langle\gamma\gamma|\alpha\alpha\rangle_{AB} = U(1)\langle\gamma|\alpha\rangle_A^2$$

Taking moduli, we get $|\langle\gamma|\alpha\rangle| = |\langle\gamma|\alpha\rangle|^2$, so $|\langle\gamma|\alpha\rangle| \in \{0,1\}$. But $\alpha, \gamma$ were arbitrary, a contradiction.

1.7. **Quantum entanglement.** A *product* state vector is a state vector $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ for some state vectors in $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. A non-product state vector is called an *entangled* state vector. Similarly, a *product* mixed state is a mixed state $\rho_{AB}$ of the form $\rho_A \otimes \rho_B$ where $\rho_A$ is a mixed state on $\mathcal{H}_A$ and $\rho_B$ is a mixed state on $\mathcal{H}_B$. A *separable* mixed state is a convex combination of product mixed states. A non-separable mixed state is called an *entangled* state.

**Separable vs. entangled states.**

| | |
|---|---|
| product state vector | $\|\psi_{AB}\rangle = \|\psi_A\rangle \otimes \|\psi_B\rangle$ |
| product pure state | $\|\psi_{AB}\rangle\langle\psi_{AB}\| = \|\psi_A\rangle\langle\psi_A\| \otimes \|\psi_B\rangle\langle\psi_B\|$ |
| product mixed state | $\rho_{AB} = \rho_A \otimes \rho_B$ |
| separable mixed state | convex combination of product mixed states |
| entangled state | non-separable mixed state |

Product state vectors, pure states, and mixed states are all separable.

**Exercise 1.7.1.** Show that if $\rho_{AB} = \rho_A \otimes \rho_B$ is a product state, then $S(\rho_{AB}) = S(\rho_A) + S(\rho_B)$.

**Remark 1.7.2.** Determining whether a state is separable is called the *separability problem* and is known to be NP-hard.

**Exercise 1.7.3.** The *partial adjoint with respect to $B$* of a state $\rho = \sum p^{ij}_{k\ell}|i\rangle\langle j| \otimes |k\rangle\langle\ell|$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ is

$$\rho^{T_B} := (I \otimes T)(\rho) = \sum p^{ij}_{k\ell}|i\rangle\langle j| \otimes |\ell\rangle\langle k| = \sum p^{ij}_{\ell k}|i\rangle\langle j| \otimes |k\rangle\langle\ell|$$

The *positive partial transpose condition* (PPT) is that $\mathrm{spec}(\rho^{T_B}) \subset \mathbb{R}_{>0}$.

(1) Show that PPT for $B$ is equivalent to PPT for $A$.
*Hint:*$\rho^{T_A} = (\rho^{T_B})^T$.
(2) Prove that PPT is necessary for separability.

*Note: In fact, PPT is sufficient for separability in the $2 \times 2$ case, but this is beyond the scope of this course.*

**Definition 1.7.4.** Suppose $\mathcal{H}_A \otimes \mathcal{H}_B$ is a product system in state $\rho_{AB}$ and $M_A, M_B$ are two observables acting locally on the subsystems $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. The *correlation function* is given by

$$\begin{aligned} C(M_A, M_B) :&= \langle M_A \otimes M_B\rangle - \langle M_A \otimes 1_B\rangle\langle 1_A \otimes M_B\rangle \\ &= \mathrm{Tr}_{AB}((M_A \otimes M_B)(\rho_{AB} - \rho_A^{\mathrm{red}} \otimes \rho_B^{\mathrm{red}})). \end{aligned}$$

**Exercise 1.7.5.** Prove that the following are equivalent.

(1) $\rho_{AB}$ has no correlations, i.e., $C(M_A, M_B) = 0$ for all subsystem observables $M_A, M_B$.

(2) The joint probability distribution on $\mathcal{B}_A \times \mathcal{B}_B$ given by the *projective measurements* (measurement of an observable which is a projection)

$$p_{AB}(\alpha, \beta) := \mathrm{Tr}_{AB}(p_{\alpha\beta}\rho_{AB})$$

has no correlation, where $p_{\alpha\beta} = |\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|$.

(3) $\rho_{AB} = \rho_A^{\text{red}} \otimes \rho_B^{\text{red}}$.

(4) $\rho_{AB}$ is a product state.

**Definition 1.7.6.** The *quantum mutual information* of the bipartite state $\rho_{AB}$ is given by

$$I(A : B) := S(\rho_A^{\text{red}}) + S(\rho_B^{\text{red}}) - S(\rho_{AB}).$$

is a measure of total correlation between $A$ and $B$ which does not depend on an observable.

**Exercise 1.7.7.** Suppose $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$ is pure so that $S(\rho_{AB}) = 0$. Use the Schmidt decomposition $|\psi_{AB}\rangle = \sum \sqrt{p_i}|\alpha_i\beta_i\rangle$ where $\sum p_i = 1$ and Exercise 1.5.8 to show that $S(\rho_A^{\text{red}}) = S(\rho_B^{\text{red}}) = H(\{p_i\})$ where $\{p_i\}$ denotes a discrete probability distribution.

**Definition 1.7.8.** The *entanglement* of a bipartite state vector $|\psi_{AB}\rangle$ is given by

$$S(|\psi_{AB}\rangle) = S(\rho_A^{\text{red}}) = S(\rho_B^{\text{red}}).$$

Define the *quantum conditional entropy* by

$$S(A|B) := S(\rho_{AB}) - S(\rho_B^{\text{red}}) \qquad\qquad S(B|A) := S(\rho_{AB}) - S(\rho_A^{\text{red}}).$$

This means there is a similar Venn diagram for quantum mutual information similar to the Venn diagram (1.2.8) for classical mutual information.

**Warning 1.7.9.** While classical conditional entropy can never be negative, quantum conditional entropy can be! Indeed, if $|\psi_{AB}\rangle$ is an entangled state vector, then $S(\rho_{AB}) = 0$, but $S(\rho_A^{\text{red}}) = S(\rho_B^{\text{red}}) > 0$, so $S(A|B) = S(B|A) < 0$.

**Exercise 1.7.10.** Prove that $I(A : B)$ is always non-negative, and equals zero if and only if $\rho_{AB}$ is a product state.

**Exercise 1.7.11.** Use quantum state purification $\rho_{AB} = \mathbb{E}_C(|\psi_{ABC}\rangle\langle\psi_{ABC}|)$ to show that

$$|S(\rho_A^{\text{red}}) - S(\rho_B^{\text{red}})| \leq S(\rho_{AB}).$$

1.8. **Many body correlation.** We are now interested in quantum systems with more than 2 subsystems; for simplicity, we will study those of the form $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$. States on this system will be called *tripartite/3-particle* states.

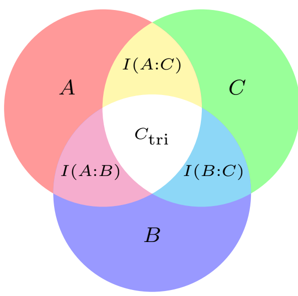
**Definition 1.8.1.** The *total correlation* in the tripartite state $\rho_{ABC}$ is

$$C_T(\rho_{ABC}) := S(\rho_A^{\text{red}}) + S(\rho_B^{\text{red}}) + S(\rho_C^{\text{red}}) - S(\rho_{ABC}).$$

**Example 1.8.2.** For the tripartite state $\rho_{ABC} = \frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$, observe that

$$\begin{aligned} C_T(\rho_{ABC}) &= 3 \cdot S\left(\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)\right) - S\left(\frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)\right) \\ &= -6\frac{1}{2}\log\left(\frac{1}{2}\right) + 2\frac{1}{2}\log\left(\frac{1}{2}\right) = 3 - 1 = 2. \\ I(A:B) &= 2 \cdot S\left(\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)\right) - S\left(\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)\right) = 1 \\ &= I(B:C) = I(A:C) \end{aligned}$$

This means that whereas the mutual information $I(A:B)$ can be viewed as the intersection in a Venn diagram, the corresponding triple intersection $C_{\text{tri}}$ in the following Venn diagram can be negative, and is thus not the correct notion of total correlation between 3 subsystems.




adapted from [arXiv:1508.02595, p.28]

$$\begin{aligned} C_{\text{tri}} :&= S(\rho^{\text{red}}_{AB}) + S(\rho^{\text{red}}_{BC}) + S(\rho^{\text{red}}_{AC}) \\ &\quad - S(\rho^{\text{red}}_{A}) - S(\rho^{\text{red}}_{B}) - S(\rho^{\text{red}}_{C}) - S(\rho_{ABC}) \\ &= C_T(\rho_{ABC}) - I(A:B) - I(B:C) - I(A:C). \end{aligned}$$

Indeed, in the example above, $C_{\text{tri}} < 0$!

**Definition 1.8.3.** For a tripartite state $\rho_{ABC}$, we define its sets of *$k$-reduced density matrics* ($k$-RDMs) for $k = 1, 2, 3$ by

$$\begin{aligned} \text{1-RDMs} &= \{\rho^{\text{red}}_{A}, \rho^{\text{red}}_{B}, \rho^{\text{red}}_{C}\} \\ \text{1-RDMs} &= \{\rho^{\text{red}}_{AB}, \rho^{\text{red}}_{BC}, \rho^{\text{red}}_{AC}\} \\ \text{3-RDMs} &= \{\rho_{ABC}\} \end{aligned}$$

For $k = 1, 2, 3$, we define the sets

$$\begin{aligned} \mathbf{L}_1 &:= \left\{\text{states } \sigma_{ABC} \middle| \sigma^{\text{red}}_{A} = \rho^{\text{red}}_{A},\ \sigma^{\text{red}}_{B} = \rho^{\text{red}}_{B},\ \text{and } \sigma^{\text{red}}_{C} = \rho^{\text{red}}_{C}\right\} \\ \mathbf{L}_2 &:= \left\{\text{states } \sigma_{ABC} \middle| \sigma^{\text{red}}_{AB} = \rho^{\text{red}}_{AB},\ \sigma^{\text{red}}_{BC} = \rho^{\text{red}}_{BC},\ \text{and } \sigma^{\text{red}}_{AC} = \rho^{\text{red}}_{AC}\right\} \\ \mathbf{L}_3 &:= \{\text{states } \sigma_{ABC} | \sigma_{ABC} = \rho_{ABC}\} = \{\rho_{ABC}\} \end{aligned}$$

We can do this in general for an $n$-partite state as well.

Now given a set of density matrices, we can ask if it is a collection of $k$-RDMs for some $N$-partite state.

**Principle of maximum entropy.** For a given set $R$ of $k$-RDMs, the best inference of the $N$-partite state $\rho_{A_1 \cdots A_N}$ is the unique state $\rho^*_k \in \mathbf{L}_k$ with maximal von Neumann entropy.

$$\rho^*_k = \operatorname{argmax}\{S(\sigma) | \sigma \in \mathbf{L}_k(R)\}$$

**Exercise 1.8.4** ($\star$, [MR1979011]). Let $J \subset \mathbb{R}$ be an interval. A function $f : J \to \mathbb{R}$ is called *operator convex* if for all Hermetian/self-adjoint operators $a, b \in M_n(\mathbb{C})$ with $\mathrm{spec}(a), \mathrm{spec}(b) \subset J$, we have $f(ta+(1-t)b) \leq tf(a)+(1-t)f(b)$. Show that $f(x) := x\log(x)$ is operator convex.

**Exercise 1.8.5.** Show that $\rho_k^*$ is well-defined, i.e., given a set of $k$-RDMs, there is a unique state in $\mathbf{L}_k$ with maximum entropy.

**Exercise 1.8.6.** Suppose $\rho_{ABC}$ is a tripartite state.

(1) Calculate $\rho_1^*$ and $\rho_3^*$.
(2) Show that the total correlation satisfies $C_T(\rho_{ABC}) = S(\rho_1^*) - S(\rho_3^*)$.

**Exercise 1.8.7.** If $j \leq k$, is $\rho_j^* \in \mathbf{L}_k$?

**Definition 1.8.8.** The *irreducible $k$-partite correlation* of $\rho_{A_1\cdots A_N}$ is

$$C_k := S(\rho_{k-1}^*) - S(\rho_k^*),$$

which measures the $k$-partite correlations that cannot be learned from the $(k-1)$-RDMs. Observe that $C_k \geq 0$, and by Exercise 1.8.6,

$$C_T(\rho_{ABC}) = S(\rho_1^*) - S(\rho_3)^* = S(\rho_1^*) - S(\rho_2)^* + S(\rho_2^*) - S(\rho_3)^* \geq 0.$$

**Exercise 1.8.9.** Compute $C_1, C_2, C_3$ for $|GHZ\rangle$ as in Exercise 1.6.3.

**Remark 1.8.10.** A tripartite state $\rho_{ABC}$ is determined by its 2-RDMs if $C_3 = 0$, or equivalently, $\rho_{ABC} = \rho_2^*$. The only pure tripartite states $|\psi_{ABC}\rangle\langle\psi_{ABC}|$ on $(\mathbb{C}^2)^{\otimes 3}$ with $C_3 \neq 0$ are

$$\alpha|000\rangle + \beta|111\rangle \qquad \alpha, \beta \neq 0,\ |\alpha|^2 + |\beta|^2 = 1.$$

**Definition 1.8.11.** A pure tripartite state vector $|\psi_{ABC}\rangle$ is

- a *product* state vector if it can be written as $|\psi_{ABC}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle$,
- *entangled* if it is not a product state (eg: $|\psi_A\rangle \otimes |\psi_{BC}\rangle$ for some entangled state $|\psi_{BC}\rangle$), and
- *genuinely entangled* if it cannot be written as a product state with respect to any tensor product decomposition.

**Definition 1.8.12.** Suppose $|\psi_{ABC}\rangle$ is a pure tripartite stat vector, and denote by $|\alpha\rangle = |\alpha_A\rangle \otimes |\alpha_B\rangle \otimes |\alpha_C\rangle$ a product pure tripartite state vector. The *geometric measure of entanglement* is given by

$$E_G(|\psi_{ABC}\rangle) := -\log(\Lambda^2_{\max}(|\psi_{ABC}\rangle) \qquad \text{where} \qquad \Lambda^2_{\max}(|\psi_{ABC}\rangle) := \max_{|\alpha\rangle} |\langle\alpha||\psi_{ABC}\rangle\rangle|.$$

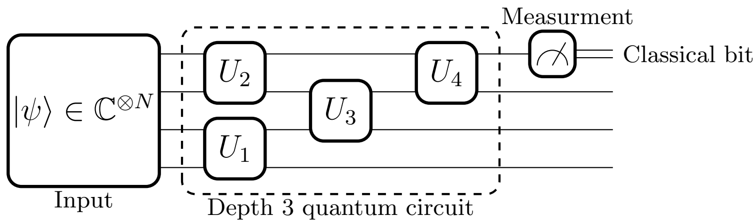
We view $E_G(|\psi_{ABC}\rangle)$ as a measurement of how far $|\psi_{ABC}\rangle$ is from the set of product pure tripartite state vectors.

**Exercise 1.8.13.** Compute $E_G(|GHZ\rangle)$ where $|GHZ\rangle$ is as in Exercise 1.6.3.

1.9. **Quantum computation.** Classical computers manipulate bits to perform calculations. Quantum computers manipulate qubits (state vectors in $\mathbb{C}^2$) or qudits (state vectors in $\mathbb{C}^d$) to perform calculations using *quantum gates*, which are unitary matrices on a tensor product Hilbert space $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$. We have already seen some examples of quantum gates: the Pauli $X, Y, Z$ operators, which are self-adjoint unitaries.

To perform a quantum calculation, we take our state vector $|\psi\rangle \in \mathcal{H}$ and apply a finite sequence of unitary quantum gates to transform the state. Finally, we perform a measurement on part or all of the total space. It is important to note from the beginning that in contrast with classical computation, this process is *probabilistic*, not deterministic, due to the process of measurement in quantum mechanics.

Here is a cartoon of a quantum computation:




These diagrams exploit the *graphical calculus* for tensor categories; here we work with the tensor C* category of finite dimensional Hilbert spaces. We will use two conventions for these diagrams in these notes. Sometimes these diagrams are written sideways to use less space on a page, where time increases from left to right; sometimes we write these diagrams vertically, where time increases from bottom to top; this is known as the *optimistic convention* (always look up!).

**Some physical realizations of qubits.**

| Name | Physical support | Realized system size |
|---|---|---|
| superconducting qubits | Josephson junction (charge, flux, phase) | 53[a] $\geq$ 2000 DWave[b] |
| photonic | boson sampling | 76[c] |
| cold atom | neutral atoms/ | $72 - 1000$ qubits |
| trapped ion | electrodynamic ion trap | 32 qubits[d] |
| silicon qubits | quantum dots | 2 qubits at 1.5K[e] |
| topological qubits/ anyons | anyon braiding in gapped TPM | $< 1$ qubit |

[a]Google's quantum supremacy [AAB+19]
[b]DWave microchip implements quantum annealing, which is not universal for quantum computation.
[c]Jiuzhang quantum supremacy [ZWD+20]
[d]IonQ [Gib20]. Previously, IBM had 27 trapped ion qubits.
[e]Silicon qubits at higher temperatures could interface better with existing conventional computes [YLH+20]

There are (at least) two sources of error in quantum computation:

- *decoherence*, when information is lost due to interaction with the environment, and
- *accuracy*, our inability to perfectly construct a specific unitary quantum gate.

Both are a manifestation of non-unitary time evolution of the system. We have already seen from the *no cloning theorem* that we cannot just send the same message multiple times, so more robust techniques are necessary. One way to deal with error is via *software*, e.g., error correcting codes, and another method is *hardware*, e.g., *topological quantum computation*.

It is not the case that having $N$ *physical* qubits for a quantum computer gives $N$ *logical* qubits for quantum computation, as many physical qubits are needed for error correction. As topology is robust to deformation, it is believed that topological qubits are manifestly fault tolerant [Kit03] so that one topological qubit would equal one logical qubit.

## 1.10. **Non-unitary time evolution by completely positive maps.**

### 1.10.1. *Completely positive maps.*

**Exercise 1.10.1.** Suppose $\mathcal{H}$ and $\mathcal{K}$ are finite dimensional vector spaces with $\dim(\mathcal{K}) = k$. Construct a unitary isomorphism $\mathcal{H} \otimes \mathcal{K} \cong \mathcal{H}^{\oplus k}$. Deduce that $B(\mathcal{H}) \otimes \mathcal{B}(\mathcal{K}) \cong M_k(\mathcal{B}(\mathcal{H}))$.

**Definition 1.10.2.** Suppose $\mathcal{H}_A$ and $\mathcal{H}_B$ are two quantum systems. A linear map $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is called

- *unital* if $\Phi(I_A) = I_B$,
- *trace preserving* if $\operatorname{Tr}_B(\Phi(x)) = \operatorname{Tr}_A(x)$ for all $x \in \mathcal{B}(\mathcal{H}_A)$,
- *positive* if $x \geq 0$ in $\mathcal{B}(\mathcal{H}_A)$ implies $\Phi(x) \geq 0$, and
- *completely positive* if $(x_{ij}) \geq 0$ in $M_k(\mathcal{B}(\mathcal{H}_A))$ implies $(\Phi(x_{ij})) \geq 0$ in $M_k(\mathcal{B}(\mathcal{H}_B))$ for all $k \in \mathbb{N}$.

A *quantum operation* is a completely positive map such that for all states $\rho$, $\operatorname{Tr}(\Phi(\rho)) \leq 1$. Observe that a quantum operation maps states to states if and only if it is trace preserving. In this case, we call the quantum operation a *quantum channel*. That is, quantum channels are trace preserving completely positive (TPCP) maps.

**Exercise 1.10.3.** Suppose that $E_i : \mathcal{H}_A \to \mathcal{H}_B$ is a family of transformations such that $\sum E_i^\dagger E_i = I_A$. Show that $\Phi(x) := \sum_i E_i x E_i^\dagger$ is completely positive.
*Hint: When $(x_{ij})$ is positive in $M_k(\mathcal{B}(\mathcal{H}_A))$, find a $y$ such that $(\Phi(x_{ij})) = y^\dagger y$.*

**Exercise 1.10.4** (Stinespring Dilation)**.** Suppose $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is completely positive.

(1) Show that $\langle x \otimes \eta | y \otimes \xi \rangle := \langle \eta | \Phi(x^\dagger y) \xi \rangle_H$ on $\mathcal{B}(\mathcal{H}_A) \otimes \mathcal{H}_B$ linearly extends to a well-defined positive sesquilinear form.
(2) Show that for $V$ a vector space with positive sesquilinear form $B(\,\cdot\,|\,\cdot\,)$, $N_B = \{v \in V | B(v|v) = 0\}$ is a subspace of $V$, and $B$ descends to an inner product on $V/N_B$.
(3) Define $\mathcal{K}$ to be completion of $(\mathcal{B}(\mathcal{H}_A) \otimes \mathcal{H}_B)/N_{\langle\cdot|\cdot\rangle}$ in $\|\cdot\|_2$. Find a unital $*$-homormophism $\Psi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{K})$, and an isometry $v \in \mathcal{B}(\mathcal{H}_B \to \mathcal{K})$ such that $\Phi(x) = v^\dagger \Psi(x) v$ for all $x \in \mathcal{B}(\mathcal{H}_A)$.

*Note: For this problem, we may replace $\mathcal{B}(\mathcal{H}_A)$ with any* C*-*algebra, and $\mathcal{H}_B$ need not be finite dimensional.*

**Exercise 1.10.5** (Kraus operators)**.** Suppose $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is completely positive.
[[maybe quantum operation or TPCP?]]

(1) Prove there are a family of transformations $T_i : \mathcal{H}_A \to \mathcal{H}_B$ with $\sum E_i^\dagger E_i = I_A$ such that $\Phi(x) = \sum_i E_i x E_i^\dagger$ for all $x \in \mathcal{B}(\mathcal{H}_A)$.
*Note: Such a family* $(E_i)$ *is called a system of* Kraus operators *for* $\Phi$.

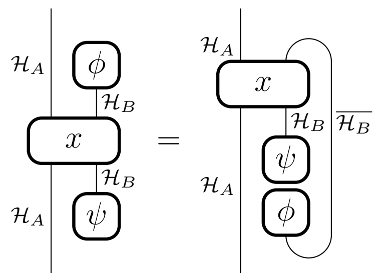
(2) Suppose $(E_i)_{i=1}^N$ and $(F_i)_{i=1}^N$ are systems of Kraus operators for $\Phi$. Prove that there is a unitary $(u_{ij}) \in M_N(\mathcal{B}(\mathcal{H}_B))$ such that $F_i = \sum_{j=1}^N u_{ij} E_j$.

1.10.2. *Non-unitary time evolution.* Suppose we have a quantum system $\mathcal{H}_S$, which is unavoidably coupled with the environment $\mathcal{H}_E$, so that the total space is $\mathcal{H}_S \otimes \mathcal{H}_E$. Suppose the system is in state vector $|\psi_{SE}\rangle$ at time $t_0$, and set $\rho_{SE}(t_0) := |\psi_{SE}\rangle\langle\psi_{SE}|$. Recall that in the Hamiltonian formulation of quantum mechanics, the state of the system at time $t > t_0$ is given by

$$\rho_{SE}(t) = U_{SE}(t)\rho_{SE}U_{SE}(t)^\dagger.$$

The time evolution of the quantum system $S$ is given by the RDM $\rho_S^{\mathrm{red}}(t) = \mathbb{E}_S(\rho_{SE}(t))$.

**Notation 1.10.6.** For two state vectors $\phi, \psi \in \mathcal{H}_B$ and $x \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$, we write

$\langle\phi|x|\psi\rangle_A := (I_A \otimes \phi)x(I_A \otimes \psi) =$  $= \mathbb{E}_A(x(I_A \otimes |\psi\rangle\langle\phi|))$.



In the diagram, we identify $|\psi\rangle$ with a linear map $\mathbb{C} \to \mathcal{H}_B$ and $\langle\phi|$ with a linear map $\mathcal{H}_B \to \mathbb{C}$. In the middle equality, we use the graphical calculus to rotate $\phi$ around the right hand side. We will justify this step later.

**Exercise 1.10.7.** Prove that the canonical trace preserving conditional expectation $\mathbb{E}_A = \mathrm{id}_A \otimes \mathrm{Tr}_B : \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ is given by $\mathbb{E}_A(x) = \sum_\beta \langle\beta|x|\beta\rangle_A$ for any orthonormal basis $\{\beta\}$ of $\mathcal{H}_B$.

Suppose now that $\rho_{SE}(t_0) = \rho_S(t_0) \otimes |0_E\rangle\langle 0_E|$ is a product state and $\{|i\rangle\}$ is some orthonormal basis of $\mathcal{H}_E$. In this case,

$$\begin{aligned}
\rho_S^{\mathrm{red}}(t) = \mathbb{E}_S(\rho_{SE}(t)) &= \mathbb{E}_S(U_{SE}(t)(\rho_S(t_0) \otimes |0_E\rangle\langle 0_E|)U_{SE}(t)^\dagger) \\
&= \sum_i \langle i|U_{SE}(t)(\rho_S(t_0) \otimes |0_E\rangle\langle 0_E|)U_{SE}(t)^\dagger|i\rangle_S \\
&= \sum_i \underbrace{\langle i|U_{SE}(t)|0_E\rangle_S}_{=:E_i} \rho_S(t_0)\langle 0_E|U_{SE}(t)^\dagger|i\rangle_S \\
&= \sum_i E_i(t)\rho_S(t_0)E_i(t)^\dagger
\end{aligned}$$

where $E_i(t) := \langle i|U_{SE}(t)|0_E\rangle_S$. the reader is encouraged to perform the above calculation diagrammatically.

**Exercise 1.10.8.** Verify that $\sum_i E_i(t)^\dagger E_i(t) = I_S$ so that $\Phi_t(x) := \sum_i E_i(t)xE_i(t)^\dagger$ is completely positive by Exercise 1.10.3.

These Kraus operators $\{E_i\}$ are the *noise* or *error* operators when $\Phi$ represents the error-producing quantum operation of the environment. Hence we see that the time evolution of $\rho_S(t)$ under interaction with the environment is no longer given by conjugation by a unitary operator, but instead by the family $\{\Phi_t\}$ of completely positive maps $\rho_S^{\mathrm{red}}(t) = \Phi_t(\rho_S(t_0))$.

1.11. **Error correction.** We have seen in the previous section that errors are introduced in quantum computation due to non-unitary evolution of the system $\mathcal{H}$. Our presentation of error correction codes follows [KL97, §3], but we use different notation.

**Definition 1.11.1.** For $k \le n$, an $(n,k)$-*quantum code* is a triple $(\mathcal{Q}, \mathcal{H}, u)$ where

- $\mathcal{Q}$ is a $k$ dimensional Hilbert space,
- $\mathcal{H}$ is an $n$-dimensional Hilbert space called the *coding space*, and
- $u : \mathcal{Q} \to \mathcal{H}$ is an injective partial isometry called the *encoding operator*. Its adjoint $u^\dagger$ is called the *decoding operator*.

For such a triple, we define the associated *code* $\mathcal{C} := u\mathcal{Q} \subset \mathcal{H}$, whose state vectors are called *code words*.

**Definition 1.11.2.** Suppose we have a quantum code $(\mathcal{Q}, \mathcal{H}, u, \mathcal{C} = u\mathcal{Q})$, and suppose $\Phi : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ is an 'error-producing' quantum operation. A *recovery operator* is a quantum operation $\Theta : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, and we call $(\mathcal{C}, \Theta)$ a *quantum error correcting code*. The *error* of $(\mathcal{C}, \Phi, \Theta)$ is given by

$$\mathrm{Err}(\mathcal{C}, \Phi, \Theta) := 1 - F(\mathcal{C}, \Phi, \Theta) \qquad \text{where} \qquad F(\mathcal{C}, \Phi, \Theta) := \min_{\substack{\text{state vectors} \\ |\psi\rangle \in \mathcal{C}}} \langle \psi | \Theta(\Phi(|\psi\rangle\langle\psi|)) | \psi \rangle$$

is called the *fidelity*.

**Exercise 1.11.3.** Why may we define the fidelity in terms of a min and not an inf?

**Exercise 1.11.4.** Suppose $\{E_i\}, \{R_j\}$ are systems of Kraus operators for $\Phi, \Theta$ respectively. Show that the fidelity is given by

$$F(\mathcal{C}, \Phi, \Theta) := \min_{\substack{\text{state vectors} \\ |\psi\rangle \in \mathcal{C}}} \sum_{i,j} |\langle \psi | R_j E_i | \psi \rangle|^2$$

and the error is given by

$$\mathrm{Err}(\mathcal{C}, \Phi, \Theta) = \max_{\substack{\text{state vectors} \\ |\psi\rangle \in \mathcal{C}}} \sum_{i,j} \|(R_j E_i - \langle \psi | R_j E_i | \psi \rangle) |\psi\rangle\|^2.$$

**Example 1.11.5** (Bit flip code, [ZCZW19, §3.2.1])**.** Suppose we have a qubit $|\psi\rangle \in \mathbb{C}^2$ together with a noisy quantum operation $\Phi : M_2(\mathbb{C}) \to M_2(\mathbb{C})$ which flips $|0\rangle \leftrightarrow |1\rangle$ with probability $p$, e.g.,

$$\Phi(\rho) := (1-p)\rho + p(X\rho X).$$

Observe that $\Phi$ is completely positive by Exercise 1.10.3, since the Kraus operators here are $\{\sqrt{1-p}I, \sqrt{p}X\}$. If the qubit is in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, then applying $\Phi$ gives us the mixed state

$$\rho = (1-p)|\psi\rangle\langle\psi| + p(|X\psi\rangle\langle X\psi|).$$

The only reasonable choice for the error correction code is to set $\mathcal{C} = \mathbb{C}^2$ and $\Theta = \mathrm{id}$. The error is then given by

$$\begin{aligned}\mathrm{Err}_1(\alpha,\beta) &= 1 - \langle\psi|\rho|\psi\rangle = 1 - ((1-p)\langle\psi|\psi\rangle^2 + p\langle\psi|X|\psi\rangle^2) = p(1-\langle\psi|X|\psi\rangle^2)\\ &= p(1 - 4\,\mathrm{Re}(\alpha\overline{\beta})^2).\end{aligned}$$

We thus see that the maximum the error can be is $p$.

However, if we amplify the space $\mathbb{C}^2$ and use an error correcting code, we can decrease our error by an order of magnitude. Setting $\mathcal{A} = (\mathbb{C}^2)^{\otimes 2}$, we amplify the total space to $\mathcal{H}\otimes\mathcal{A}$, and we encode our basis elements by $|0\rangle \mapsto |000\rangle$ and $|1\rangle \mapsto |111\rangle$. We assume that each of the 3 qubits we have prepared are independently subject to bit flip noise with probability $p$. After applying $\Phi^{\otimes 3}$ to $|\psi\rangle\langle\psi|$, we get the mixed state

$$\begin{aligned}\Phi^{\otimes 3}(|\psi\rangle\langle\psi|) &= (1-p)^3|\psi\rangle\langle\psi| + p(1-p)^2\sum_{i=1}^{3} X_i|\psi\rangle\langle\psi|X_i\\ &\qquad + p^2(1-p)\sum_{i=1}^{3}\widehat{X_i}|\psi\rangle\langle\psi|\widehat{X_i} + p^3 X_1X_2X_3|\psi\rangle\langle\psi|X_1X_2X_3,\end{aligned}\tag{1.11.6}$$

where we use the shorthand $\widehat{X_i} = X_jX_k$ for distinct $i,j,k\in\{1,2,3\}$. Observe $\Phi^{\otimes 3}$ is again visibly completely positive by Exercise 1.10.3. (What are the Kraus operators $E_i$ for $\Phi^{\otimes 3}$?)

Our quantum code is now $\mathcal{C} = \mathrm{span}_{\mathbb{C}}\{|000\rangle, |111\rangle\}$, and our recover operator is given by

$$\Theta(\rho) := \sum_{j=0}^{3} R_j\rho R_j^\dagger := P_0\rho P_0 + \sum_{j=1}^{3} X_jP_j\rho P_jX_j \qquad\qquad R_0 := P_0,\ R_j := X_jP_j$$

where the $P_j$ are the orthogonal projections

$$\begin{aligned}P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111|\\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011|\\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101|\\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|.\end{aligned}$$

**Exercise 1.11.7.** Verify that $\sum_j R_j^\dagger R_j = I$. Check that the map $\rho\mapsto P_0\rho P_0$ acts as the identity on $|\phi\rangle\langle\psi|$ for $|\phi\rangle,|\psi\rangle\in\{|111\rangle\langle 111|\}$. Then check that the map $\rho\mapsto X_jP_j\rho P_jX_j$:

- $\underline{j=1}$: corrects $|100\rangle$ to $|000\rangle$ and $|011\rangle$ to $|111\rangle$ on operators of the form $|\phi\rangle\langle\psi|$ for $|\phi\rangle,|\psi\rangle\in\{|100\rangle\langle 011|\}$.
- $\underline{j=2}$: corrects $|010\rangle$ to $|000\rangle$ and $|101\rangle$ to $|111\rangle$ on operators of the form $|\phi\rangle\langle\psi|$ for $|\phi\rangle,|\psi\rangle\in\{|010\rangle\langle 101|\}$.
- $\underline{j=3}$: corrects $|001\rangle$ to $|000\rangle$ and $|110\rangle$ to $|111\rangle$ on operators of the form $|\phi\rangle\langle\psi|$ for $|\phi\rangle,|\psi\rangle\in\{|001\rangle\langle 110|\}$.

For $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$, we write $\Phi^{\otimes 3}(|\psi\rangle\langle\psi|)$ from (1.11.6) as $\rho_0+\rho_1+\rho_2+\rho_3$ where

$$\begin{aligned}
\rho_0 &= (1-p)^3|\psi\rangle\langle\psi| + p^3X_1X_2X_3|\psi\rangle\langle\psi|X_1X_2X_3\\
\rho_1 &= p(1-p)^2X_1|\psi\rangle\langle\psi|X_1 + p^2(1-p)X_2X_3|\psi\rangle\langle\psi|X_2X_3\\
\rho_2 &= p(1-p)^2X_2|\psi\rangle\langle\psi|X_1 + p^2(1-p)X_1X_3|\psi\rangle\langle\psi|X_1X_3\\
\rho_3 &= p(1-p)^2X_3|\psi\rangle\langle\psi|X_1 + p^2(1-p)X_1X_2|\psi\rangle\langle\psi|X_1X_2.
\end{aligned}$$

Observe that $R_j\rho_kR_j^\dagger$ vanishes if $j\neq k$. We calculate $\Theta(\Phi^{\otimes 3}(|\psi\rangle\langle\psi|)) = \sum_{j=0}^3 R_j\rho_jR_j^\dagger$ where

$$\begin{aligned}
R_0\rho_0R_0^\dagger &= (1-p)^3|\psi\rangle\langle\psi| + p^3X_1X_2X_3|\psi\rangle\langle\psi|X_1X_2X_3\\
R_1\rho_1R_1^\dagger &= R_2\rho_2R_2^\dagger = R_3\rho_3R_3^\dagger = p(1-p)^2|\psi\rangle\langle\psi| + p^2(1-p)X_1X_2X_3|\psi\rangle\langle\psi|X_1X_2X_3.
\end{aligned}$$

Finally, we compute the error as

$$\begin{aligned}
\mathrm{Err}_3(\alpha,\beta) &= 1-\langle\psi|\Theta(\Phi^{\otimes 3}(|\psi\rangle\langle\psi|))|\psi\rangle = 1-\sum_{j=0}^{3}\langle\psi|R_j\rho_jR_j|\psi\rangle\\
&= 1-(1-p)^3+3p(1-p)^2-(p^3+3p^2(1-p))\langle\psi|X_1X_2X_3|\psi\rangle^2\\
&= p^2(3-2p)(1-\langle\psi|X_1X_2X_3|\psi\rangle^2) = p^2(3-2p)(1-4\,\mathrm{Re}(\alpha\overline{\beta})^2)\le p^2(3-2p).
\end{aligned}$$

Observe that when $p<1/2$, $\mathrm{Err}_3<\mathrm{Err}_1$. To achieve arbitrarily good precision, we can encode $|0\rangle$ as $|0\cdots 0\rangle\in(\mathbb{C}^2)^{\otimes 2r-1}$.

**Remark 1.11.8.** Although we will not discuss it here, one should read about the phase flip code and Shor's code.

**Definition 1.11.9.** Ideally, we would like to choose our code $(\mathcal{Q},\mathcal{H},u,\mathcal{C}=u\mathcal{Q})$ and our recovery operator $\Theta$ to minimize the error. When $\Theta$ satisfies $\mathrm{Err}(\mathcal{C},\Phi,\Theta)=0$, we say that $(\mathcal{C},\Theta)$ is a $\Phi$-*correcting code*.

**Exercise 1.11.10** ($\star$ [KL97, Thm. 3.2],[Got10, Thm. 2 and 3],[Pre, §7.2])**.** Prove that the following are equivalent for a quantum code subspace $\mathcal{C}\subset\mathcal{H}$ and error producing quantum operation $\Phi(x)=\sum_i E_i^\dagger xE_i$ with $\sum_i E_i^\dagger E_i = I_{\mathcal{H}}$.

(QEC1) $\mathcal{C}$ corrects the error set $\{E_i\}$,

(QEC2) There is an orthonormal basis $\{\kappa_k\}$ of $\mathcal{C}$ such that

$$\langle\kappa_k|E_i^\dagger E_j|\kappa_\ell\rangle_{\mathcal{H}} = c_{ij}\delta_{k=\ell}$$

where $c_{ij}$ is a constant independent of $k,\ell$,

(QEC3) Denoting the orthogonal projection onto $\mathcal{C}$ by $p_{\mathcal{C}}$,

$$p_{\mathcal{C}}E_i^\dagger E_jp_{\mathcal{C}} = c_{ij}p_{\mathcal{C}}$$

where $c_{ij}$ is a constant, and

(QEC4) For all state vectors $|\kappa\rangle,|\kappa'\rangle\in\mathcal{C}$ and all $E\in\mathrm{span}\{E_i\}\subset\mathcal{B}(\mathcal{H})$,

$$\langle\kappa|E^\dagger E|\kappa\rangle_{\mathcal{H}} = \langle\kappa'|E^\dagger E|\kappa'\rangle_{\mathcal{H}}.$$

## References


[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis, *Quantum supremacy using a programmable superconducting processor*, Nature **574** (2019), no. 7779, 505–510, `DOI:10.1038/s41586-019-1666-5`.

[EGNO15] Pavel Etingof, Shlomo Gelaki, Dmitri Nikshych, and Victor Ostrik, *Tensor categories*, Mathematical Surveys and Monographs, vol. 205, American Mathematical Society, Providence, RI, 2015, `MR3242743` `DOI:10.1090/surv/205`. MR 3242743

[Gib20] Elizabeth Gibney, *Quantum computer race intensifies as alternative technology gains steam*, 2020, `DOI:10.1038/d41586-020-03237-w`, pp. 342–343.

[GJF19] Davide Gaiotto and Theo Johnson-Freyd, *Condensations in higher categories*, 2019, `arXiv:1905.09566`.

[Got10] Daniel Gottesman, *An introduction to quantum error correction and fault-tolerant quantum computation*, Quantum information science and its contributions to mathematics, Proc. Sympos. Appl. Math., vol. 68, Amer. Math. Soc., Providence, RI, 2010, `MR2762145` `DOI:10.1090/psapm/068/2762145` `arXiv:0904.2557`, pp. 13–58. MR 2762145

[HV19] Chris Heunen and Jamie Vicary, *Categories for quantum theory*, Oxford Graduate Texts in Mathematics, vol. 28, Oxford University Press, Oxford, 2019, An introduction, `MR3971584` `DOI:10.1093/oso/9780198739623.001.0001`. MR 3971584

[JF20] Theo Johnson-Freyd, *On the classification of topological orders*, 2020, `arXiv:2003.06663`.

[Kit03] A. Yu. Kitaev, *Fault-tolerant quantum computation by anyons*, Ann. Physics **303** (2003), no. 1, 2–30, `MR1951039` `DOI:10.1016/S0003-4916(02)00018-0` `arXiv:quant-ph/9707021`. MR 1951039

[KL97] Emanuel Knill and Raymond Laflamme, *Theory of quantum error-correcting codes*, Phys. Rev. A **55** (1997), 900–911, `DOI:10.1103/PhysRevA.55.900` `arXiv:quant-ph/9604034`.

[Pre] John Preskill, *Lecture notes on Quantum Computation*, Available at `http://theory.caltech.edu/~preskill/ph219/index.html`.

[SKK20] Bowen Shi, Kohtaro Kato, and Isaac H. Kim, *Fusion rules from entanglement*, Ann. Physics **418** (2020), 168164, 49, `MR4109024` `DOI:10.1016/j.aop.2020.168164` `arXiv:1906.09376`. MR 4109024

[YLH+20] C. H. Yang, R. C. C. Leon, J. C. C. Hwang, A. Saraiva, T. Tanttu, W. Huang, J. Camirand Lemyre, K. W. Chan, K. Y. Tan, F. E. Hudson, K. M. Itoh, A. Morello, M. Pioro-Ladrière, A. Laucht, and A. S. Dzurak, *Operation of a silicon quantum processor unit cell above one kelvin*, Nature **580** (2020), no. 7803, 350–354, `DOI:10.1038/s41586-020-2171-6`.

[ZCZW19] Bei Zeng, Xie Chen, Duan-Lu Zhou, and Xiao-Gang Wen, *Quantum information meets quantum matter*, Quantum Science and Technology, Springer, New York, 2019, From quantum entanglement to topological phases of many-body systems, With a foreword by John Preskill, `MR3929747` `DOI:10.1007/978-1-4939-9084-9` `arXiv:1508.02595`. MR 3929747

[ZWD+20] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, Peng Hu, Xiao-Yan Yang, Wei-Jun Zhang, Hao Li, Yuxuan Li, Xiao Jiang, Lin Gan, Guangwen Yang, Lixing You, Zhen Wang, Li Li, Nai-Le Liu, Chao-Yang

Lu, and Jian-Wei Pan, *Quantum computational advantage using photons*, Science **370** (2020), no. 6523, 1460–1463, DOI:10.1126/science.abe8770.