CHAPTER 0: A (VERY) BRIEF TOUR OF QUANTUM MECHANICS, COMPUTATION, AND CATEGORY THEORY.

This chapter is intended to be a brief treatment of the basic mechanics, framework, and concepts relevant to the study of quantum computing and information for review and reference. Part 1 (sections 1–4) surveys quantum mechanics and computation, with sections organized according to the commonly known postulates of quantum theory. The second part (sections 5–7) provides a survey of category theory. Additional references to works in this volume are included throughout, and general references appear at the end.

Part 1: Quantum mechanics & computation

1. Qubits & Quantum states

Postulate of quantum mechanics: Representing states of systems. The state of a quantum system is represented by a unit-length vector in a complex Hilbert space[1], $\mathcal{H}$, that corresponds to that system. The state space of a composite system is the tensor product of the state spaces of the subsystems.

The Dirac bra-ket notation for states of quantum systems is ubiquitous in the literature, and we adopt it here. A vector in a complex Hilbert space representing a quantum state is written as a *ket*, $|\psi\rangle$, and its conjugate-transpose (adjoint, or sometimes Hermetian conjugate) is written as a *bra*, $\langle\psi|$. In this notation, a bra-ket denotes an inner product, $\langle\varphi|\psi\rangle$, and a ket-bra denotes an outer product, $|\varphi\rangle\langle\psi|$.

Each one-dimensional subspace of $\mathcal{H}$ corresponds to a possible state of the system, and a state is usually described as a linear combination in a relevant orthonormal basis. The basis elements are often thought of as *basic states*. Quantum systems can exist in a *superposition* of more than one basic state: If a quantum system has access to two basic states, say $|\alpha\rangle$ and $|\beta\rangle$, then, in general, the system's "current state" can be represented by a linear combination of these states in complex Hilbert space:

$$|\psi\rangle = c_1|\alpha\rangle + c_2|\beta\rangle, \text{ where } ||\psi\rangle| = 1.$$

The complex coefficients, c_1 and c_2, of $|\alpha\rangle$ and $|\beta\rangle$ give classical probabilistic information about the state. For example, the value $|c_1|^2$ is the probability that the system would be found to be in state $|\alpha\rangle$ upon measurement. The coefficient itself, c_1, is called the *probability amplitude*. Two vectors in $\mathcal{H}$ represent the same state if they differ only by a global phase factor: If $|\psi\rangle = e^{i\theta}|\varphi\rangle$, then $|\psi\rangle$ and $|\varphi\rangle$ represent the same state, and the (real) probabilities described by the coefficients are the same.

The squared norm of the state vector $|\psi\rangle$ is the inner product of $|\psi\rangle$ with itself, i.e., the bra-ket $\langle\psi|\psi\rangle$. The quantity $|\langle\varphi|\psi\rangle|^2$ is the probability that upon

[1]A Hilbert space is a complete, normed metric space, where the norm and distance function are induced by an inner product defined on the space.

measurement, $|\psi\rangle$ will be found to be in state $|\varphi\rangle$, and $\langle\varphi|\psi\rangle$ is the corresponding probability amplitude. (More about measurement of quantum systems in Section 3 below.)

1.1. **Qubits.** A classical bit can be in only one of two states at a given time, $|0\rangle$ or $|1\rangle$. A quantum bit or *qubit* may exist in a *superposition* of these basic (orthogonal) states, $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$, where c_1 and c_2 are complex probability amplitudes. More precisely, a qubit is a 2-dimensional quantum system, the state of which is a unit-length vector in $\mathcal{H} = \mathbb{C}^2$. The basic states for this space are usually thought of as $|0\rangle$ and $|1\rangle$, but at times other bases are used (for example, $\{|+\rangle, |-\rangle\}$ or $\{|\uparrow\rangle, |\downarrow\rangle\}$. Basic states are typically the eigenstates (eigenvectors) of an observable of interest (see discussion of measurement below).

Any unit vector that is a (complex) linear combination of the basic states is a *pure* state and non-trivial linear combinations are *superpositions*. So-called *mixed* states are not proper state vectors, they are classical probabilistic combinations of pure states and are best represented by *density matrices*.

The state space of a qubit is often visualized as a point on the *Bloch sphere*. The norm of a state vector is always one, and states that differ only by a global phase factor are identified, so two real numbers, θ and ϕ, suffice to specify a distinct state via the decomposition

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

Respectively, the range of values taken on by θ and ϕ may be restricted to the intervals $[0, \pi]$ and $[0, 2\pi)$ without any loss of generality, and so the corresponding distinct states may be mapped uniquely onto the unit sphere in $\mathbb{R}^3$. In this visualization, the basic vector $|0\rangle$ points up and $|1\rangle$ points down, θ describes the latitudinal angle, and φ the longitudinal angle. Orthogonal states are antipodal on the Bloch sphere. Note that states that differ by a global phase factor will (by design) coincide in this visualization.

1.2. **Composite quantum systems.** As described above, a single quantum system (for example, a single qubit) exists in a pure state that may be a superposition of basic states. A composition of systems may exist either in a *separable* or an *entangled* state. Separable states are states that can be written as tensor products of pure states of the constituent subsystems; entangled states cannot be so written: they are non-trivial (complex) linear combinations of separable states. In the case of an entangled state, the subsystems cannot be thought of as existing in states independent of the composed system.

Example 1.1. Suppose we have a system of two qubits, the first in state $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and the second in state $|\varphi\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. The state of the combined system is

$$|\psi\rangle \otimes |\varphi\rangle = |\psi\rangle|\varphi\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$$

Such a state of the composite system that can be written as a tensor product of pure states is called *separable*.

Example 1.2. The *Bell states* of a 2-qubit system are not separable; they are important and canonical examples of *entangled* states:

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}} \quad \frac{|00\rangle-|11\rangle}{\sqrt{2}}$$

$$\frac{|01\rangle+|10\rangle}{\sqrt{2}} \quad \frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

Example 1.3. The *GHZ states* (for Greenberger-Horne-Zeilinger) are examples of entangled states in composite systems that have three or more subsystems. The GHZ state for a system with n subsystems is

$$\frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}.$$

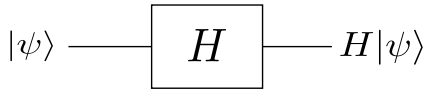
For more on entangled states, see Parke's article in this volume, or Section 6 of Kauffman's article.

2. Transformations and quantum gates

Postulate of quantum mechanics: Evolution of systems. The time evolution of a closed quantum system is described by a unitary transformation.

A transformation is *unitary* if its inverse is equal to its adjoint. Such transformations preserve inner products and are reversible, deterministic, and continuous. In quantum computing, algorithms are often described as circuits in which information (and time) flows from left to right. Quantum gates represent unitary transformations applied to qubits in such a circuit.

Example 2.1. *The Hadamard gate.* The 1-qubit Hadamard gate has as input and output one qubit, as shown in the simple circuit diagram below:

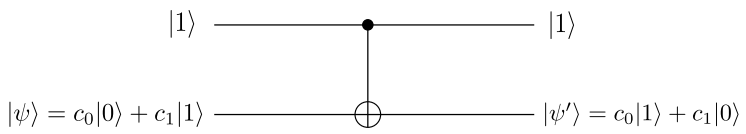


Its matrix representation is (with respect to the basis $\{|0\rangle = [1\ 0]^T, |1\rangle = [0\ 1]^T\}$):

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

This transformation applied to the basic state $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ results in the superposition $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$.

Example 2.2. *The controlled-not gate.* Another important quantum gate is the *controlled-not* or CNOT gate. The gate requires two inputs, one designated as the *control* input (passing through the solid dot) and the other as the *target* input:



When the control input is in state $|0\rangle$, the gate does nothing. If the control is in state $|1\rangle$ (as it is in the diagram above), the gate acts by "flipping" the non-control (target) input as follows: If the target input is in state $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, then flipping transforms the state to $|\psi'\rangle = c_0|1\rangle + c_1|0\rangle$. The gate does not alter the control bit. The matrix representation of CNOT is the following (given with respect to the basis $\{|00\rangle = [1\ 0\ 0\ 0]^T, |01\rangle = [0\ 1\ 0\ 0]^T, |10\rangle = [0\ 0\ 1\ 0]^T, |11\rangle = [0\ 0\ 0\ 1]^T\}$):

$$\text{CNOT} = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

For more on quantum gates and unitary transformations of quantum systems, see Parke's and Kauffman's articles in this volume.

3. Measurement

Postulate of quantum mechanics: Measurement. The notion of measurement is described in terms of *observables* represented by Hermitian (self-adjoint) matrices. (It should be noted that not all such matrices describe physically meaningful measurements.)

A Hermitian matrix has all real eigenvalues, and these represent the possible values obtained upon measurement of the observable. Moreover, distinct eigenvalues yield orthogonal eigenvectors. These matrices are often described in terms of their spectral decompositions. Upon measurement, a system's state (or wave function) experiences a "collapse" and is not preserved. After measurement, the state of the system is the eigenvector corresponding to the eigenvalue that was the result of the measurement.

Example 3.1. If the matrix A corresponding to an observable $\mathcal{A}$ has (real) eigenvalue a and corresponding unit-length eigenvector $|v_a\rangle$, then the probability that measuring $\mathcal{A}$ on state $|\varphi\rangle$ will yield the value a is given by $|\langle v_a|\varphi\rangle|^2$. If a is the result of the measurement of $\mathcal{A}$ on $|\varphi\rangle$, the system is left in state $|v_a\rangle$. If we consider the result of such a measurement as a random variable, the expected value (expectation value) of that quantity is given by $\langle\varphi|A|\varphi\rangle$.

Very briefly, if the matrices representing two different observables are non-commuting, then the observables are often referred to as *complementary* and measurements of these observables are subject to uncertainty limits. Complementary observables suffer from necessarily limited precision when measured simultaneously as a result of the Heisenberg Uncertainty Principle.

4. No-go theorems and teleportation

4.1. **No cloning.** In classical computation, it is possible to implement error correction by simply duplicating the classical data as needed. This is not the case in quantum computations.

Let $|\psi\rangle$ be an arbitrary state in state space $\mathcal{H}$, and $|e\rangle$ be an ancillary state (independent of $|\psi\rangle$) in an identical state space. To "clone" the state $|\psi\rangle$, we would need to have a unitary transformation that when applied to $|\psi\rangle|e\rangle$ replaces the ancillary state with a copy of $|\psi\rangle$, yielding $|\psi\rangle|\psi\rangle$.

Theorem 4.1 (No cloning theorem)**.** *There is no unitary operator U so that for all states $|\psi\rangle$ and ancillary states $|e\rangle$,*

$$U|\psi\rangle|e\rangle = |\psi\rangle|\psi\rangle.$$

Proof. To see why, consider the possibility that there does exist such an operator U. As U must be unitary, it must preserve inner products, hence for any ψ and φ, we must have the following:

$$\langle\varphi|\psi\rangle = \langle e|\langle\varphi|\psi\rangle|e\rangle = \langle e|\langle\varphi|U^\dagger U|\psi\rangle|e\rangle = \langle\varphi|\langle\varphi|\psi\rangle|\psi\rangle = (\langle\varphi|\psi\rangle)^2.$$

We see that $\langle\varphi|\psi\rangle$ must be either 0 or 1 in order for this equality to hold, and so such a U preserves inner product only selectively — the states $|\varphi\rangle$ and $|\psi\rangle$ must be identical or orthogonal. □

4.2. **The EPR paradox, hidden variables, and Bell's Theorem.** In 1935, Einstein, Podolsky, and Rosen (EPR) questioned the completeness of quantum mechanics in the form of a thought experiment involving the measurement of one part of a 2-particle entangled system. According to EPR, two mutually exclusive conclusions may be reached regarding quantum mechanics: either quantum mechanics is incomplete, or the physical quantities associated with two non-commuting operators cannot have simultaneous reality. Subsequently, building on the behavior of a two component system under the laws of quantum theory, EPR argue for the incompleteness of quantum theory.

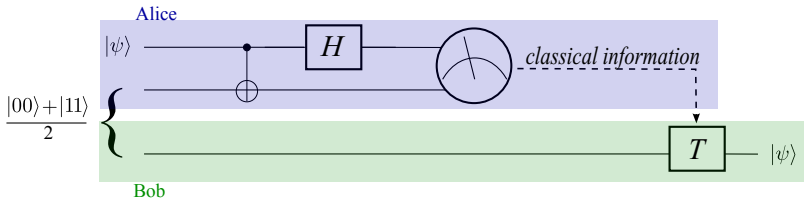
The following scenario captures the idea of the quandary they posed. Imagine that two particles, A and B, interact and then part ways. If one measures the momentum of particle A, he may *compute* the momentum of particle B exactly due to entanglement. If he subsequently *measures* the momentum of particle B, the result will be exactly that computed value. Similarly, the particles' positions may be observed, computed, and checked. However, the measurement operators corresponding to these observables (position and momentum) do not commute, and hence an exact knowledge of position entails some uncertainty in the value of momentum. The EPR argument makes a case for being able to assign two different wave functions (or states) to the same reality (particle B), by judicious choice of measurements on particle A, which leads to the conclusion that quantum mechanics must be incomplete.

A related question is this: How does particle B "know" to have a precisely defined momentum and an uncertain position when particle A's momentum is measured? According to the principle of locality, a physical process occurring in one place should not be able to affect a physical process in another location (outside the light-cone of the first process). This scenario seems to entail either superluminal transmission of information between the particles (violating locality), or some "hidden variable" or "element of reality" encoding the information as yet unaccounted for by quantum mechanics (assuming determinism or realism). This is the idea underlying the famous EPR paradox.

In 1964, John Stewart Bell formalized (mathematically) the notions of locality and realism, and gave a set of inequalities that would provide a test of quantum mechanics against a local hidden variable theory. In the 1970s and 1980s, physical experiments (carried out most famously by Alain Aspect) demonstrated in favor of the former. What is known as *Bell's Theorem* is the summary of all this, asserting that no locally realistic theory can make the predictions of quantum mechanics.

Another related theorem is the *Kochen-Specker Theorem*, which says that a non-contextual hidden variable theory (one in which the value of an observable in a system is independent of the apparatus used to measure it) is unable to make the predictions of quantum mechanics.

4.3. **Quantum teleportation.** It would be difficult to overstate the importance of entanglement in quantum computing and the difficulty in representing and interpreting this phenomenon in possible quantum logics . A basic illustration of the power of entanglement is in the *quantum teleportation* protocol: An *EPR pair*, that is, a pair of qubits in a (entangled) Bell state, are prepared. One qubit is in the possession of entity A (Alice) and the other is in the possession of entity B (Bob). Alice also has a qubit, $|\psi\rangle$, which she would like to send to Bob. To do this, Alice applies a CNOT transformation to her two qubits, using $|\psi\rangle$ as the control, followed by an application of the Hadamard transformation to $|\psi\rangle$. She then measures both of her qubits[2] (they are destroyed in the process), and (classically) communicates to Bob the (classical) information that results of her measurements. Upon receiving this information, Bob preforms one of four corresponding transformations, T, resulting in the transformation of his qubit into the state $|\psi\rangle$, which Alice wished to transmit to him.



Note that this protocol does not violate the no-cloning theorem (Alice's copy is destroyed), nor Bell's Theorem (classical information must be transmitted subluminally).

For alternative formulations of the quantum teleportation protocol in a graphical language and another (similar) formulation in quantum topology, see Coecke's and Kauffman's (respectively) articles in this volume.

For more detailed exposition on all these ideas and topics, the following texts may be useful:

Textbooks at the undergraduate level

- Quantum Computing for Computer Scientists, by Noson Yanofsky and Mirco Manucci, Cambridge University Press, 2008.
- Quantum Computing Explained, by Phillip Kaye, Raymond Laflamme, and Michele Mosca, Oxford University Press, 2007.
- Quantum Computing: A Gentle Introduction, by Eleanor Rieffel and Wolfgang Polak, MIT Press, 2011.
- Quantum Computer Science, by N. David Mermin, Cambridge University Press, 2007.

At the graduate or research level

[2]This entire process is sometimes called a *Bell measurement*.

– Quantum Computing and Information, by Michael Nielsen and Isaac Chuang, Cambridge University Press, 2011.

Part 2: Category theory for quantum computing

In physics, in the 1970s, Penrose used graphical language to represent linear operators, their products, and tensor products: boxes for operators, incoming wires for superscripts, and outgoing wires for subscripts. These diagrams represented various categories, which are of importance in physics and quantum computing. Of particular importance are *tensor categories*, also called *monoidal categories,* which have been used by S. Abramsky and B. Coecke as a framework for quantum theory. Their categorical quantum mechanics can be also viewed as a suitable quantum logic. We will give a brief survey of monoidal categories. For more details see [3] and [1].

5. Basic Category Theory

A *category* $\mathcal{C}$ consists of a class of *objects*, $Ob(\mathcal{C})$, and a class of *morphisms*, $hom(\mathcal{C})$, also called maps or arrows with specific abstract properties. For every pair of objects, A and B, there is a class of *morphisms* denoted by $\hom_{\mathcal{C}}(A, B)$, or simply $\hom(A, B)$ when the category is clear from the context. A morphism f has a domain $dom(f)$ (also called source) and a codomain $cod(f)$ (also called target), which we write $f : dom(f) \to cod(f)$. The morphisms are equipped with composition $\circ$, which is an associative operation that respects domain and codomain information. That is,

$$\text{(i) } (f \circ g) \circ h = f \circ (g \circ h),$$

where $f : A \to B$, $g : D \to A$, and $h : C \to D$. For every object A, the set $\hom(A, A)$ contains the identity morphism id_A such that for every $f : A \to B$, we have

$$\text{(ii) } \quad f \circ id_A = f$$

and

$$\text{(iii) } id_B \circ f = f.$$

The equations (i)–(iii) can be viewed as the axioms for the categories. The *opposite category* (also called *dual category*) of $\mathcal{C}$ is formed by reversing the morphisms, that is, by interchanging the domain and the codomain of each morphism. It is denoted by $\mathcal{C}^{op}$. A category $\mathcal{C}$ is called *small* if both $ob(\mathcal{C})$ and $hom(\mathcal{C})$ are sets, and it is called *locally small* is for every pair of objects A, B, the class $hom(A, B)$ is a set.

A morphism $f : A \to B$ is called a *monomorphism* or *split monic* if $f \circ g_1 = f \circ g_2$ implies $g_1 = g_2$ for all morphisms $g_1, g_2 : C \to A$. A morphism $f : A \to B$ has a *left inverse*, also called a *retraction* of f, if there is a morphism $g : B \to A$ such that $g \circ f = id_A$. Clearly, a morphism with a left inverse is a monomorphism. The converse may not be true. A morphism $f : A \to B$ is called an *epimorphism* or *split epic* if $g_1 \circ f = g_2 \circ f$ implies $g_1 = g_2$ for all morphisms $g_1, g_2 : B \to C$. A morphism $f : A \to B$ has a *right inverse*, also called a *section* of f, if there is a morphism $g : B \to A$ such that $f \circ g = id_B$. A morphism with a right inverse is an epimorphism, but the converse may not be true. If a morphism has both a left inverse and a right inverse, then the two inverses are equal. Hence we have the following definition. A morphism $f : A \to B$ is called an *isomorphism* if there

exists a morphism $g : B \to A$ such that $f \circ g = id_B$ and $g \circ f = id_A$. If it exists, g is unique and is called the *inverse* of f, and hence f is the inverse of g.

Examples of well-known categories include the category of sets as objects with functions as morphisms, the category of vector spaces as objects with linear maps as morphisms, and the category of Hilbert spaces as objects with unitary transformations as morphisms. In the graphical representation, object variables label edges ("wires") and morphism variables label nodes ("boxes"). The composition is represented by connecting the outgoing edge of one diagram to the incoming edge of another, while the identity morphism is represented as a continuing edge.

Functors capture the notion of a homomorphism between two categories. They preserve identity morphisms and composition of morphisms. More precisely, a *functor* Φ from a category $\mathcal{C}$ to a category $\mathcal{D}$ is a function that maps every object A of $\mathcal{C}$ to an object $\Phi(A)$ of $\mathcal{D}$, as well as every morphism of $\mathcal{C}$ to a corresponding morphism of $\mathcal{D}$ such that the following is satisfied. For every pair A, B of objects from $\mathcal{C}$, each morphism $f \in \hom(A, B)$ in $\mathcal{C}$ is mapped to a morphism $\Phi(f) \in \hom(\Phi(A), \Phi(B))$ in $\mathcal{D}$ such that

$$\Phi(g \circ h) = \Phi(g) \circ \Phi(h) \wedge \Phi(id_A) = id_{\Phi(A)}.$$

A functor from $\mathcal{C}$ to $\mathcal{D}$ is also called a *covariant functor*, in order to distinguish it from a contravariant functor, which reverses the order of composition. A *contravariant functor* Ψ from $\mathcal{C}$ to $\mathcal{D}$ is a map that associates to each object A in $\mathcal{C}$ an object $\Psi(A)$ in $\mathcal{D}$, and associates to each morphism $f \in \hom(A, B)$ in $\mathcal{C}$ a morphism $\Psi(f) \in \hom(\Psi(B), \Psi(A))$ in $\mathcal{D}$ such that

$$\Psi(g \circ h) = \Psi(h) \circ \Psi(g) \wedge \Psi(id_A) = id_{\Psi(A)}.$$

A functor Φ between locally small categories $\mathcal{C}$ and $\mathcal{D}$ is called *faithful* if it is is injective when restricted to each set of morphisms that have a given domain and codomain. That is, for every pair A, B of objects in $\mathcal{C}$, the induced function

$$\Phi_{A,B} : \hom_{\mathcal{C}}(A, B) \to \hom_{\mathcal{D}}(\Phi(A), \Phi(B))$$

is injective. On the other hand, a faithful functor may not be injective on objects or morphisms. A functor Φ is called *full* if the induced functions $\Phi_{A,B}$ are surjective.

Natural transformations capture the notion of a homomorphism between two functors. That is, given two categories, $\mathcal{C}$ and $\mathcal{D}$, and two functors from $\mathcal{C}$ to $\mathcal{D}$, Φ and Ψ, a *natural transformation* $\mathcal{N} : \Phi \to \Psi$ consists of the family of morphisms for every object A of $\mathcal{C}$, $\mu_A : \Phi(A) \to \Psi(A)$, such that for every $f \in \hom_{\mathcal{C}}(A, B)$, we have

$$\Psi(f) \circ \mu_A = \mu_B \circ \Phi(f).$$

The content of the equation is captured by the following diagram.

$$\begin{array}{ccc} \Phi(A) & \xrightarrow{\mu_A} & \Psi(A) \\ {\scriptstyle \Phi(f)}\downarrow & & \downarrow{\scriptstyle \Psi(f)} \\ \Phi(B) & \xrightarrow{\mu_B} & \Phi(B) \end{array}$$

6. Monoidal Categories

A *monoidal category* captures the notion of a tensor product as a binary operation of objects, $A \otimes B$, and of morphisms, $f \otimes g$. The domain of $f \otimes g$ is the tensor product of the domains of f and g, and the codomain of $f \otimes g$ is the tensor product of the codomains of f and g. The tensor product of objects is associative in the sense that for every triple (A, B, C) of objects, there is an isomorphism

$$\alpha_{A,B,C} : (A \otimes B) \otimes C \to A \otimes (B \otimes C).$$

The tensor product is a *bifunctor*, which means that it satisfies the following equations for morphisms:

$$(f_1 \otimes f_2) \circ (f_3 \otimes f_4) = (f_1 \circ f_2) \otimes (f_3 \circ f_4)$$

and

$$id_{A \otimes B} = id_A \otimes id_B.$$

(See Coecke's article in this volume for a wire diagram representation of this equation.)

A monoidal category also has a constant unit object denoted by I. For every object A, there is an isomorphsm (left)

$$\lambda_A : I \otimes A \to A$$

and an isomorphism (right)

$$\rho_A : A \otimes I \to A.$$

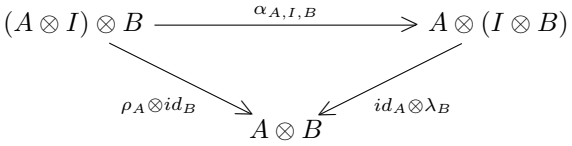
For morphisms $f : A \to A'$, $g : B \to B'$, $h : C \to C'$, we have

$$\begin{aligned} (f \otimes (g \otimes h)) \circ \alpha_{A,B.C} &= \alpha_{A',B'.C'} \circ (f \otimes g) \otimes h), \\ f \circ \lambda_A &= \lambda_{A'} \circ (id_I \otimes f), \\ f \circ \rho_A &= \rho_{A'} \circ (f \otimes id_I). \end{aligned}$$

In addition, the following *triangle axiom* is satisfied for every pair of objects A, B:

$$\rho_A \otimes id_B = (id_A \otimes \lambda_B) \circ \alpha_{A,I,B}.$$

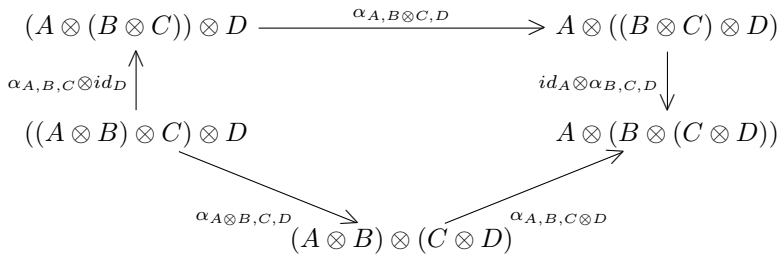
Both sides map $(A \otimes I) \otimes B)$ to $A \otimes B$. This equation is captured in the following diagram.



Also, the following *pentagon axiom* is satisfied for every quadruple of objects A, B, C, D:

$$(id_A \otimes \alpha_{B,C,D}) \circ (\alpha_{A,B \otimes C,D} \circ (\alpha_{A,B,C} \otimes id_D)) = \alpha_{A,B.C \otimes D} \circ \alpha_{A \otimes B,C,D}.$$

Both sides map $((A \otimes B) \otimes C) \otimes D$ to $A \otimes (B \otimes (C \otimes D)$. This relationship is visualized in the following diagram.



In the graphical language, the tensor product of objects is represented by parallel wires (input or output) from the bottom to the top, and the unit object is represented by no wire. Tensor product of morphisms is represented by stacking their diagrams. Examples of monoidal categories are vector spaces, or Hilbert spaces, with either direct sum or tensor product, as well as sets with direct products or disjoint unions. When no additional properties are assumed for a monoidal category, we often call it *planar monoidal category*.

Joyal and Street [2] established a coherence theorem for planar monoidal categories, which captures the correspondence between the formal language and the graphical language we described. The formal language of categories uses object variables and morphism variables, and object constants (such as I) and morphism constants (such as id_A), and operation symbols (such as $\circ$ and $\otimes$). These are used to form terms and equations (formulas). The *coherence theorem* of Joyal and Street states that an equation in the language of monoidal categories follows from the axioms of monoidal categories if and only if it holds in the graphical language, up to planar equivalence. Roughly speaking, here, a diagram D_1 is planar equivalent to a diagram D_2 if it is possible to transform D_1 to D_2 by continuously moving the boxes and wires of D_1 (without crossing or cutting). Other coherence theorem for special categories are of the similar nature. The part of a coherence theorem that states that an equation following from the axioms holds in the graphical language of is called a *soundness theorem*, and its converse a *completness theorem*. Soundness is assured by assuring that the axioms hold in the graphical language.

A *braided monoidal category* is a monoidal category with a family of isomorphisms for every pair of objects A, B,

$$\sigma_{A,B} : A \otimes B \to B \otimes A.$$

Hence $\sigma^{-1}_{A,B}$ exists, where

$$\sigma^{-1}_{A,B} : B \otimes A \to A \otimes B.$$

Two *hexagon axioms* are satisfied for every triple of objects A, B, C:

$$(id_B \otimes \sigma_{A,C}) \circ \alpha_{B,A,C} \circ (\sigma_{A,B} \otimes id_C) = \alpha_{A,B,C} \circ \sigma_{A,B\otimes C} \circ \alpha_{B,C,A}$$

and

$$(id_B \otimes \sigma^{-1}_{C,A}) \circ \alpha_{B,A,C} \circ (\sigma^{-1}_{B,A} \otimes id_C) = \alpha_{A,B,C} \circ \sigma^{-1}_{B\otimes C,A} \circ \alpha_{B,C,A}.$$

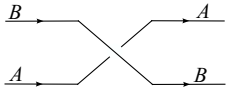
The first of these is captured in the diagram below.

$$\begin{array}{ccc}
(B\otimes A)\otimes C & \xrightarrow{\alpha_{B,A,C}} & B\otimes(A\otimes C) \\
{\scriptstyle \sigma_{A,B}\otimes id_C}\uparrow & & \downarrow{\scriptstyle id_B\otimes\sigma_{A,C}} \\
(A\otimes B)\otimes C & & B\otimes(C\otimes A) \\
{\scriptstyle \alpha_{A,B,C}}\downarrow & & \uparrow{\scriptstyle \alpha_{B,C,A}} \\
A\otimes(B\otimes C) & \xrightarrow{\sigma_{A,B\otimes C}} & (B\otimes C)\otimes A
\end{array}$$

If follows that

$$\sigma_{A,B}\circ\sigma_{A,B}^{-1} = id_{A\otimes B}.$$

Graphical language is extended to picture braiding and is represented by an under- (over-) crossing.



A *symmetric monoidal category* is a braided monoidal category where the braiding σ is its own inverse σ^{-1}. It is called symmetry and is graphically represented by a crossing.

For monoidal categories $\mathcal{C}$ and $\mathcal{D}$, a functor $\Phi : \mathcal{C} \to \mathcal{D}$ is called a *monoidal functor*, if there are also morphisms $\phi_{A,B} : \Phi(A)\otimes\Phi(B) \to \Phi(A\otimes B)$ and $\phi : I_{\mathcal{D}} \to \Phi(I_{\mathcal{C}})$, which preserve the tensor structure as follows: For every triple of objects A, B, C of $\mathcal{C}$,

$$\begin{aligned}
\Phi(\alpha_{A,B,C})\circ\phi_{A\otimes B,C}\circ(\phi_{A,B}\otimes id_{\Phi(C)}) &= \phi_{A,B\otimes C}\circ(id_{\Phi(A)}\otimes\phi)\circ\alpha_{\Phi(A),\Phi(B),\Phi(C)}, \\
\rho_{\Phi(A)} &= \Phi(\rho_A)\circ\phi_{A,I}\circ(id_{\Phi(A)}\otimes\phi), \\
\lambda_{\Phi(A)} &= \Phi(\lambda_A)\circ\phi_{I,A}\circ(\phi\otimes id_{\Phi(A)}).
\end{aligned}$$

$$\begin{array}{ccc}
I\otimes\Phi(A) & \xrightarrow{\lambda_{\Phi(A)}} & \phi(A) \\
{\scriptstyle \phi\otimes id_{\Phi(A)}}\downarrow & & \uparrow{\scriptstyle \Phi(\lambda_A)} \\
\Phi(I)\otimes\Phi(A) & \xrightarrow{\phi_{I,A}} & \Phi(I\times A)
\end{array}$$

If the maps $\phi_{A,B}$ and ϕ are also invertible (isomorphisms), the functor is called a *strong monoidal functor*; if they are the identity maps, the functor is called a *strict monoidal functor*.

Given two monoidal categories, $\mathcal{C}$ and $\mathcal{D}$, and two strict monoidal functors from $\mathcal{C}$ to $\mathcal{D}$, Φ with ϕ^{Φ} and Ψ with ϕ^{Ψ} , a natural transformation $\mathcal{N} : \Phi \to \Psi$ with morphisms $\mu_A : \Phi(A) \to \Psi(A)$ is a *monoidal natural transformation* if for every pair of objects A, B of $\mathcal{C}$, we have

$$\mu_{A\otimes B}\circ\phi^{\Phi}_{A,B} = \phi^{\Psi}_{A,B}\circ(\mu_A\otimes\mu_B).$$

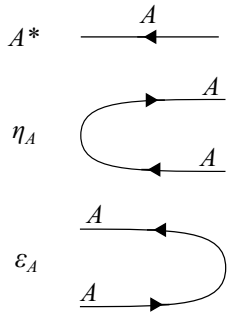
For braided monoidal categories $\mathcal{C}$ and $\mathcal{D}$, a monoidal functor $\Phi : \mathcal{C} \to \mathcal{D}$ is called a *braided monoidal functor* if it is compatible with braiding as follows, for every pair of objects A, B of $\mathcal{C}$,

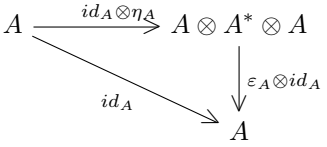
$$\Phi(\sigma_{A,B})\circ\phi_{A,B} = \phi_{B,A}\circ\sigma_{\Phi(A),\Phi(B)}.$$

An example of a symmetric monoidal category is the category of sets with functions as morphisms, with Cartesian product and symmetry given by $\sigma_{A,B}(x,y) = (y,x)$. Another example of a symmetric monoidal category is the category of vector spaces with linear maps as morphisms, with tensor product and symmetry given by $\sigma_{A,B}(x \otimes y) = y \otimes x$.

A monoidal category $\mathcal{C}$ is called *right autonomous* if every object A of $\mathcal{C}$ has a right dual, denoted by A^*, and there are two morphisms, the unit $\eta_A : I \to A^* \otimes A$ and the counit $\epsilon_A : A \otimes A^* \to I$, which satisfy the following adjunction triangle equalities:

$$\begin{aligned} id_A \otimes \eta_A &= id_A \circ (\epsilon_A \otimes id_A), \\ (id_{A^*} \otimes \epsilon_A) \circ (\eta_A \otimes id_{A^*}) &= id_{A^*}. \end{aligned}$$





A *left autonomous* monoidal category is defined dually and a left dual of A is denoted by ${}^*A$. A monoidal category is *autonomous* if it is both right and left autonomous. In a braided right autonomous category, a right dual of A is also a left dual of A, so the category is autonomous. A *compact closed category* is a right autonomous symmetric monoidal category. A category of sets with binary relations as morphisms and direct product as tensor product and where $A^* = A$ is a compact closed category. The category of finite dimensional vector spaces (or finite dimensional Hilbert spaces) with tensor product and with A^* being the dual space of A is a compact closed category. On the other hand, if we allow infinite dimensional vector spaces, the categories of vector spaces and of Hilbert spaces are not autonomous.

7. Dagger Categories

A *dagger category* is a category $\mathcal{C}$ equipped with a contravariant functor $\dagger : \mathcal{C} \to \mathcal{C}$, which is identity on the objects and involutive on the morphisms. More specifically, to each morphism $f : A \to B$ a morphism $f^\dagger : B \to A$ is assigned such that

$$(f^\dagger)^{f^\dagger} = f \wedge id_A^\dagger = id_A,$$

and for every morphism $g : B \to C$,

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger.$$

Morphism $f^\dagger$ is called the *adjoint* of f. The adjoint is diagrammatically represented by reversing the location but not the direction of the wires and by marking the upper right corner (in contrast to the upper left corner) in the box. In general, the adjoint of a diagram is its mirror image.

The category of sets with binary relations as morphisms is a dagger category with relational inverse $R^\dagger$ as adjoint of R. The category of Hilbert spaces with bounded linear maps is a dagger category with the usual adjoints. A morphism f is called *hermitian* if it self-adjoint: $f^\dagger = f$. A morphism f is called *unitary* if it is and isomorphism and $f^{-1} = f^\dagger$. A *dagger functor* Φ between two dagger categories $\mathcal{C}$ and $\mathcal{D}$ is a functor that satisfies the following additional equality for every morphism f in $\mathcal{C}$:

$$\Phi(f^\dagger) = (\Phi(f))^\dagger.$$

A *dagger monoidal category* C is a category that is both monoidal and dagger and the two structures are compatible in the sense that the morphism from the monoidal structure $\alpha_{A,B,C}$, λ_A, ρ_A are unitary and following equality is satisfied for every pair of morphisms f, g:

$$(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger.$$

A *dagger symmetric monoidal category* is a dagger braided monoidal category such that its symmetry (braiding) is unitary. A *dagger compact closed category* $\mathcal{C}$, also simply called *dagger compact category* is a dagger symmetric monoidal category that is also compact closed, together with a relation to connect the dagger structure to the compact structure. Specifically, the dagger is used to connect the unit to the counit so that for all objects A in $\mathcal{C}$, we have:

$$\eta_A = \epsilon_A^\dagger \circ \sigma_{A \otimes A^*}.$$

Dagger compact categories are of great importance for foundations of quantum information and computing. Selinger [4] proved a completeness and hence coherence result for dagger compact closed categories. That is, he established that an equation follows from the axioms of dagger compact closed categories if and only if it holds in finite dimensional Hilbert spaces. Thus, this coherence theorem allows us to use the diagrammatic calculus of dagger compact categories to precisely express and verify some fundamental quantum information notions and protocols.

References

[1] S. Abramsky and B. Coecke, A categorical semantics of quantum protocols, *Proceedings of the 19th IEEE conference on Logic in Computer Science* (LiCS'04), IEEE Computer Science Press, 2004.

[2] A. Joyal and R. Street, The geometry of tensor calculus I, *Advances in Mathematics* 88 (1991), pp. 55–112.

[3] P. Selinger, A survey of graphical languages for monoidal categories, in: *New Structures for Physics*, B. Coecke, editor, Lecture Notes in Physics 813, Springer, 2011, pp. 289–355.

[4] P. Selinger, Finite dimensional Hilbert spaces are complete for dagger compact closed categories, *Logical Methods in Computer Science* 8 (2012), pp.1–12.