Quantum communication, computing, simulation and sensing: a review from a quantum statistics perspective

Leonardo Lavagna

***Abstract*—In this work we will review some recent trends in the fields of Quantum Communication, Quantum Simulation, Quantum Computing, Quantum Metrology and Sensing, focusing on the novel approaches to Information Theory brought by Quantum Principles and on some key Algorithms that can be implemented in Noisy Intermediate-Scale Quantum (NISQ) devices that can be directly applied to some feasible Networking-related applications.**

I. Introduction

In recent years there has been an increasing interest towards quantum mechanical applications primarily in the fields of Communications and Computing, due to the achieved technological maturity which realistically allows to have, in the near future, in a service-oriented context, new products, new protocols and efficiency gains in a wide range of ventures: from an innovative conception of the Internet to securer cryptographic schemes, from faster processors to more resilient clock timing and synchronization techniques. The interest is not purely academic, and the research in the aforementioned areas is starting to bring out commercial products, in particular in the field of Quantum Security. These first proofs-of-concept, a steady focus of the media and some concerns (see for example [3]) have contributed to the flow of investments which in turn are boosting the research in a virtuous circle. In this sense it is worth mentioning the recent EU flagship program on Quantum Technologies [4] with a budget of one billion € and a scope of 10 years which finances projects in Quantum Communication, Quantum Simulation, Quantum Computing, Quantum Metrology and Sensing.

In this work we will review some recent trends in the fields highlighted in the cited EU flagship program from a Quantum Statistics perspective. In particular we will focus on the novel approaches to Information Theory brought by Quantum Principles, on some feasible Networking-related applications that leverage quantum features (e.g. superposition and entanglement) and on some key Algorithms that can be implemented in Noisy Intermediate-Scale Quantum (NISQ) devices [5].

The paper is organized as follows: in Sec. II we will review some basic concepts in quantum information theory and the fundamental differences with the classical theory, covering the theoretical aspects of Quantum Communication, in Sec. III we will dive into Quantum Computing and Quantum Simulation, talking primarily about quantum processing (summarized in [6]) and quantum machine learning (summarized in [7]), then in Sec. IV we will briefly talk about Quantum Metrology and Sensing (summarized in [8]). In section V we will analyze some of the promising applications of the topics discussed previously, with particular attention to communication strategies (encodings, compression, error recovery, noise, security, networking) but we will also mention some of the new trends in related areas (chemistry, physics) where a "quantum approach" can result in substantial advantages.

II. Quantum Communication

In the traditional approach to quantum mechanics, a physical system is described in a Hilbert space: observables are self-adjoint operators, and statistical operators (i.e. density matrices) are associated to the states (pure states or mixed states). The main difficulty here is then to associate a notion of "information" to statistical operators and to define the "entropy" in this new setting in a way that most of the classical properties will be preserved.

A. Quantum Information

In the context of quantum communication the unit of classical information, the bit $B = \{0, 1\}$, is translated into the *qubit*, that is a system described by the Hilbert space $\mathbb{H} = \mathbb{C}^2$ where the translation $B \to \mathbb{H}$ will depend on the choice of a basis on $\mathbb{H}$ (see Sec. IV Subsec. A for further details). In this context we have messages mapped into states $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, which are subject to some strict and unintuitive rules:

- *Reversibility of computation*: since the observables are self adjoint operators on $\mathbb{H}$, every transformation of a state is invertible[1].
- *No cloning*: it is impossible to clone the states[2]. More precisely if $\mathbb{H}$ is the Hilbert space representing any quantum system, and $|\eta\rangle \in \mathbb{H}$, then there is no unitary operator U (called "quantum cloner") satisfying $U|\psi\rangle \otimes |\eta\rangle = |\psi\rangle \otimes |\psi\rangle$ for every $|\psi\rangle \in \mathbb{H}$
- *Superposition*: prior to any measurement every state of a system is unknown ad it is represented as a superposition of pure states $|\phi_i\rangle$ of the form $|\psi\rangle = \sum_i \alpha_i |\phi_i\rangle$.
- *Probabilistic outputs*: If ψ is written in terms of a orthonormal basis $\{|\phi_i\rangle\}$ of the Hilbert space $\mathbb{H}$, that is $|\psi\rangle = \sum_i \alpha_i |\phi_i\rangle$ with $\alpha_i \in \mathbb{C}$, then any measure of $|\psi\rangle$ will result in a single $|\phi_i\rangle$ with probability $|\alpha_i|^2$.

[1] Notice that this is not true in a classical setting, e.g. the AND operator is not invertible.

[2] Even if this is a strong limitation there is a workaround, see the teleporting protocol discussed later in this section.

- *Equivalence of states and density matrixes:* Pure states are seen up to a phase shift, that is if $|v\rangle$ is a ket with norm 1 then $|v\rangle$ and $|w\rangle = e^{ik}|v\rangle$ are indistinguishable. In other words pure states can be identified with the $1-$dimensional orthogonal projectors in $\mathbb{H}$ of the form $\varrho_v = |v\rangle\langle v|$ with $\langle v|v\rangle = 1$. In this sense if there is a lack of knowledge of the physical conditions of a system, its state can be represented as a statistical mixture of pure states, called mixed state $\varrho = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ where the weights satisfy $\lambda_i \geq 0$, and $\sum_i \lambda_i = 1$, that is ϱ is a positive definite matrix with $Tr(\varrho) = 1$ called density matrix or statistical operator.
- *Entanglement:* A state $|\psi\rangle \in \mathbb{H}_A \otimes \mathbb{H}_B$ is called separable if $|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$ is decomposed into a tensor product, otherwise it is called entangled and it will be written as a linear combination of tensor products, where the maximally entangled state will have density matrix of the form $\rho = n^{-\frac{1}{2}} \sum_{i,j} e_{i,j} \otimes e_{i,j}$. In this case there is a particular correlation between the states.

Consider now a message $|\psi\rangle \in \mathbb{H}$, it will be associated to a statistical operator $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ via the so called Schatten decomposition. Since this decomposition is not unique von Newman in [9] and [10] argued that the (quantum) entropy S should be independent on the state ψ and should be defined as

$$S(\rho) = -k \sum_i \lambda_i \log \lambda_i = kTr(f(\varrho))$$

where S is zero on pure states, k is a multiplicative constant usually omitted, and $f(t) = -t \log t$. Here the eigenvalues λ_is play the role of "probabilities", and it is interesting to note that after von Neumann it was Shannon who initiated the interpretation of the quantity $H(p_1, \ldots, p_n) = -\sum_i p_i \log p_i$ as an "uncertainty measure" or "information measure". At this point we can extend the definition of S to composite messages $|\psi\rangle \in \mathbb{H}_A \otimes \mathbb{H}_B$ with density matrix ρ_{AB} in anaology with classical information theory. The difference $S(\rho_{AB} \mid B) = S(\rho_{AB}) - S(\rho_B)$ is the *conditional entropy* given the subsystem B. From the definition of S it is also possible to recover the notion of *relative entropy* (or I-divergence) as $S(\rho_1 \mid\mid \rho_2) = Tr\rho_1(\log \rho_1 - \log \rho_2)$ which expresses the statistical distinguishability and therefore decreases under stochastic mappings. Likewise we can extend the notion of classical mutual information to the *quantum mutual information* $S(\rho_{AB} \mid\mid \rho_A \otimes \rho_B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$ of the subsystems A and B.

Quantum information and classical information are very different concepts and it can be difficult to compare them. However, transmission of a single qubit can carry two bits of classical data and transmitting classical information of two bits can yield the "teleportation" of the state of a quantum spin. From this point of view a qubit is equivalent to two classical bits. To explore this analogy consider two famous protocols: *dense coding* and *teleportation*. Both protocols use a basis with maximally entangled states on $\mathbb{C}^2 \otimes \mathbb{C}^2$, called the Bell basis: $|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\beta_1\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$, $|\beta_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$, $|\beta_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. Notice that for $i > 0$ it holds $|\beta_i\rangle = (\sigma_i \otimes \mathbf{1})|\beta_0\rangle$ with σ_i a Pauli operator. For *dense coding* [11]:

1) If Alice want to comunicate a number k to Bob, Alice applies the unitary σ_k to her spin, so after this operation the joint state of the two spins will be the kth vector of the Bell basis;
2) Alice sends her qubit to Bob and Bob will be in possession of both spins;
3) Bob performs the measurement corresponding to the Bell basis, the outcome will be exactly k.

For *teleportation* [12]:

1) Take a $3-$qubit system in the initial state $|\psi\rangle_A \otimes |\beta_0\rangle_{XB}$. Assume that Alice is in possession of A and X, and Bob is in possession of the spin B which we want to convert into the state of A.
2) Alice measures the Bell basis on the spins A and X which will result in an element of $\{0, 1, 2, 3\}$.
3) Alice comunicate the outcome k to Bob in a classical communication channel. This require sending two bits to distinguish among $\{01, 2, 3\}$.
4) Bob apply the unitary σ_k to the state vector of spin B and at this point the state of the spin B is the same as was the state of A at the beginning of the procedure.

B. Classical-Quantum Channels and their Capacity

Information to be transmitted needs a channel, and in a classical setting those are mappings $c : X \to Y$ from two alphabets such that c sends a probability measure on X to a probability measure on Y via conditional probabilities $\mathbb{P}(R = y \mid M = x)$ where R is a random variable on Y modeling the receiver, and M is a random variable on X describing the message source. A simple example is the *noisy typewriter* given by a channel c such that $x \in X$ is received with probability $\frac{1}{2}$. In the quantum setting it is difficult to talk about conditional probabilities so channels are formulated in terms of affine transformations acting on density matrixes. In this sense a *quantum channel* is a completely positive and trace-preserving linear mapping from the source Hilbert space to the receiver Hilbert space, usually represented as $\mathcal{C}(\rho) = \sum_i V_i \rho V_i^*$, where V_i, V_i^* are state-transforming operators satisfying $\sum_i V_i V_i^* = \mathbf{1}$ (the identity matrix), and where, for $i \neq j$, the quantity $S_{\mathcal{C}}(\rho) = Tr(V_i \rho V_j^*)$ describes the *entropy exchange*. In this setting the famous channel coding theorem [13] can be reformulated in terms of Holevo quantity

$$I(p_x, \rho_x, \mathcal{C}) = S(\mathcal{C}(\rho)) - \sum_x p_x S(\mathcal{C}(\rho_x))$$

where $\rho = \sum_x p_x \rho_x$, p_x is a probability distribution and ρ_x a probability density: if (p_x, ρ_x) describes a quantum code (i.e. a probability distribution of finite support on the input densities) and $\mathcal{C}$ is a quantum channel with Holevo quantity $I(p_x, \rho_x, \mathcal{C})$, if $C_{Ho}(\mathcal{C}) = \sup I(p_x, \rho_x, \mathcal{C})$ on all quantum codes, then

- Shannon's mutual information is bounded by the Holevo quantity;

- If D is a relative entropy center with radius $\leq R$ (i.e. $S(\rho_s \mid\mid \rho) \leq R$ for every state ρ_s) then $I(p_x, \rho_x, \mathcal{C}) \leq R$;
- If $\mathcal{F}$ is a convex family of states and we restrict C_{Ho} on states $\rho_x \in \mathcal{F}$, then C_{Ho} equals the relative entropy radius of $\mathcal{C}(\mathcal{F})$.

These results where proven by Holevo in 1973 (see [14]) and are discussed in [15] Section 3.4. Some important examples of quantum channels are (see again [15] Section 2.2):

- the *depolarizing channel* $\mathcal{C}_{p,n}(A) = pA + (1-p)\frac{\mathbf{1}TrA}{n}$ where $-(n^2-1)^{-1} \leq p \leq 1$, which has relative entropy $S = \log n - H(p + \frac{1-p}{n}, \frac{1-p}{n}, \ldots, \frac{1-p}{n})$ equal to its Holevo capacity.
- the *entanglement braking channel* $\sum_i X_i Tr(Y_i B)$ with additive Holevo capacity (see the general additivity question for quantum capacity [16], [17]).
- the *amplitude damping* channel with matrix representation
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3^{-\frac{1}{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{3} & 0 & 0 & \frac{1}{3} \end{pmatrix}$$
which shrinks the Bloch sphere to the north pole.
- the *phase-damping* channel that describe decoherence of qubits in terms of matrixes
$$\begin{pmatrix} 1 & 0 \\ 0 & diag(p, p, 2p-1) \end{pmatrix} .$$

Clearly any real channel will introduce some noise, so if we start with a pure state $|\psi\rangle$ we could end up with a state $|\psi'\rangle$ different from the starting one. Usually noise is not explicitly modeled, indeed all results in a quantum setting are of probabilistic nature, instead a way to quantify errors is given. We will address this problem in the next subsection.

C. Quantum state's estimation

Let's start with an interesting example based on hypothesis testing. Suppose we have to decide between two states ρ_0 and ρ_1 and we can decide using a two-valued measurement $\{P, \mathbf{1} - P\}$ where P is a projector operator which correspond to the acceptance of ρ_0 (so $\mathbf{1} - P$ correspond to the acceptance of ρ_1). Errors of the first kind are then $Tr\rho_0(\mathbf{1} - P)$ and errors of the second kind are $Tr\rho_1 P$. The problem is to decide which hypothesis is true in an asymptotic situation where $n-$fold product states ρ_0^n and ρ_1^n are available together with a test P_n. The quantum Stein lemma (conjectured in [18] and proven in [19]) guarantees that

$$\lim_{n\to\infty} n^{-1} \log \beta(n, \epsilon) = -S(\rho_0 \mid\mid \rho_1)$$

where

$$\beta(n, \epsilon) = \inf\{Tr\rho_1^n P_n, Tr\rho_0^n(\mathbf{1} - P_n) \leq \epsilon\} .$$

In general, how close are two quantum states $|\psi\rangle$ and $|\psi'\rangle$? The main answer to this question is given by transition probabilities $|\langle\psi \mid \psi'\rangle|^2$ whose square root is called *fidelity*. Since a quantum operation can convert pure states into mixed states one considers the following extension $F_{\psi,\rho,\psi'} = \sqrt{|\langle\psi \mid \rho \mid \psi'\rangle|}$ of fidelity. More in general $F_{\rho_1,\rho_2} = Tr\sqrt{\rho_1^{\frac{1}{2}}\rho_2\rho_1^{\frac{1}{2}}}$ as studied by Uhlmann in [20].

The goal of *state estimation* is to determine the density operator ρ of a quantum system by measurements on n replicas (pay attention here that we are not violating the no-cloning theorem since we can prepare symultaneously n systems with state ρ) of the quantum system. Since the result of each measurement is random standard statistical techniques can be applyied here. If we have a set Θ of density matrixes acting on an Hilbert space $\mathbb{H}$ and we have a measurements operator F_n with values on $\mathbb{H}^{\otimes n}$ (it measures simultaneously the n states), an estimator Φ_n with values on Θ, the couple (F_n, Φ_n) is an *estimation scheme* that is *consistent* if for every $\rho \in \Theta$ the distribution of the random variable Φ_n weakly converges to the point measure concentrated on ρ.

III. Quantum Computing and Quantum Simulation

A quantum computer is a device that is able to implement quantum algorithms based on a universal set of gates acting on qubits with "almost no error". In this section we will review quantum computation in general, focusing on oracles, and quantum computation applied to machine learning problems, focusing on the "translation" of classical machine learning algorithms into quantum machine learning algorithms that has been carried out in recent years. Notice that quantum computing is a prerequisite for any quantum communication strategy (see Sec. V Subsec. E).

A. Quantum Data Processing

Quantum Data Processing is a vast subject that can stretch to topics in computer graphics and imaging. Here we will analyze only *Quantum Oracles* which are a key ingredient of many processing methods. In computability theory an oracle is a "black box" that allows to compute a function $f : \mathbb{B}^n \to \mathbb{B}^m$ in one operation (here $\mathbb{B}^k$ represent the space of $k-$bit strings). In a quantum setting we can implement oracles that have a strong advantage with respect to their classical counterparts: quantum gates are always reversible, so we can leverage the basis encoding of the binary variables $b \oplus f(a), a, b$ where $\oplus$ is the sum modulo 2. For example suppose you want to know if the function $f : \{0,1\} \to \{0,1\}$ is constant, here, unlike the classical setting, we have an input register for to store a and an output register to store b. With this encoding $|a\rangle$ is the input and $|b\rangle, |b \oplus f(a)\rangle$ are the output, so the input register performs $|a\rangle \to |a\rangle$ and the output register performs $|b\rangle \to |b \oplus f(a)\rangle$. The quantum oracle we wanted is then given by the unitary operator U_f defined on the tensor product of the hilbert spaces of the inputs and the outputs which acts as $U_f(|a\rangle \otimes |b\rangle) := |a\rangle \otimes |b \oplus f(a)\rangle$. A simple generalization of this example yields the Deutsch-Joza algorithm [21] which represents one of the first quantum algorithms that show a "quantum advantage" (i.e. it is exponentially faster then its classical counterpart).

B. Quantum Machine Learning

Important aspects of machine learning have been successfully tackled by quantum methods, for example clustering [22], classification [23] and pattern recognition [24], and we can say that most of the standard techniques in classical machine learning have found a quantum counterpart, even neural networks [25], [26]. Many of these techniques rely on two key algorithms: the *SWAP test* and the *Qdist* routine. For the *SWAP test* (see for example [27] or the simpler [7] Section 5.3):

- Consider two unknown pure states $|\psi\rangle$ and $|\varphi\rangle$ from which you would like to recover the real number $|\langle\psi \mid \varphi\rangle|^2$.
- Take two qubit registers initialized in $|\psi\rangle$ and $|\varphi\rangle$, with n Fredkin gates controlled by the same ancillary qubit initialized at $|0\rangle$ (this allow to perform the SWAP of the two registers).
- The unitary $(H \otimes \mathbf{1} \otimes \mathbf{1})U(H \otimes \mathbf{1} \otimes \mathbf{1})$, where U is the action of the controlled SWAP, returns the state $\frac{1}{2}|0\rangle(|\psi\varphi\rangle + |\varphi\psi\rangle) + \frac{1}{2}|1\rangle(|\psi\varphi\rangle - |\varphi\psi\rangle)$. We have that $\mathbb{P}(0) = \frac{1}{2} + \frac{1}{2}|\langle\psi \mid \varphi\rangle|^2$ and repeated measurements on the ancillary qubit allow to estimate the square modulus of the inner product of the two unknown states.

For the *Qdist* (see [7] Section 5.4) routine we can apply the SWAP test to calculate dot products and distances using amplitude encoding and two ancillary qubits:

- Consider two ancillary qubits, one, called $|a_1\rangle$ entangled with the $n-$qubit register where the balanced superposition of the input vectors $|x\rangle$ and $|y\rangle$ is stored, and the second $|a_2\rangle$ in the initial state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
- Apply the SWAP test on the ancillary qubits. This allows to estimate $||\Phi||^2 = ||\frac{1}{\sqrt{2}}(|x\rangle - |y\rangle)||^2 = 1 - \frac{x \cdot y}{||x||||y||}$.
- Recover $||x-y||^2 = ||x||^2+||y||^2-2x \cdot y$ using the identity $x \cdot y = (1 - ||\Phi||^2)||x||||y||$. The number of repeated measurements required to run the SWAP test will control the accuracy in the estimation of the distance, but it is independent on the dimension of the space where the distance is calculated.

From Qdist it is easy to implement a Quantum $K-$Means algorithm and distance-based quantum classification methods like Quantum $K-$Nearest Neighbors. Also some distance-based Principal Component Analysis (PCA) methods can be performed.

C. Quantum Simulation

The term "quantum simulation" can either mean "simulate with a classical computer quantum computations" or "use quantum methods to simulate a phenomenon". Both this approaches are at a relative mature stage: we currently have good simulators (e.g. those provided by IBM [28]) that emulate the behavior of a quantum computer, and we have also good simulation methods in many areas, e.g. materials (see Sec. V Subsec. I) and particle physics (see Sec. V Subsec. J). Currently the winning strategy seems to be to work with hybrid systems: use a real quantum computer to tackle only the most difficult parts of a problem or when the quantum principles yield important advantages and rely on classical computers for the rest[3], likewise in simulation one can prepare a quantum neural network where the inputs are classical data points (see for example [30]).

IV. Quantum Metrology and Sensing

In general with sensors one seeks optimal setups for probing a parameter of interest, e.g. the magnetic field, with minimal shot noise. In the absence of noise the analytical solution for the optimal probe state can be usually derived, but in general the problem is hard to solve by hand. Quantum metrology aims to increase the precision of a measured quantity that is estimated in the presence of statistical errors using entangled quantum states [31], [32]. For example, sensing magnetic fields with high precision is crucial in many applications, such as determining chemical structure [33] or imaging cells [34]. Various different types of high-performance magnetic field sensors have been developed, including hall-effect sensors [35], superconducting quantum interference devices (SQUID) [36] and force sensors [37]. In particular, in case of qubit-based magnetic field sensors, a qubit system interacts with the magnetic field and the information about the magnetic field is encoded as an internal relative phase of the quantum state This information can then be extracted via a Ramsey-type measurement (see for example [38]) that uses repeated projective measurements. One of the principal aims of Quantum Metrology is then to derive quantum states that are robust to environmental noise but also sensitive to the external field of interest.

A. Sensor 's state preparation

For state preparation two approaches seem to work well: Variational Quantum Circuits used for example in [39], [40] and optical tweezer arrays used for example in [41]. Concretely one can prepare a probe state depending on a variational parameter, probes the field of interest under a noisy environment, measures the quantum Fisher information used in this kind of settings as a cost function, and update the parameters to maximize it. Unfortunately there are no known efficient algorithms to compute the quantum Fisher information, but some heuristics seem to work well [39]. To understand the difficulties one can face in this setting let's discuss the intricacies of the cost functions one has to deal with, linked with the quantum Fisher information.

B. Quantum Fisher information

Assume to have a smooth curve of density matrixes of the form $\varrho_\theta = \varrho + \theta B$ where $B = \dot{\varrho}$ is the tangent at ϱ. The quantum Fisher information $F_\varrho(B)$ is an information quantity associated with the pair (ϱ, B) and appeared "naturally" in the setting of Cramer-Rao inequalities. In theory there are a wide class of quantum Fisher informations since F_ϱ can be

[3] This is particularly evident in optimization problems, where the cost function can be prepared using a quantum computer and the optimization step can be carried out with classical methods, see for example [29].

expressed in terms of a Riemannian metric γ_ϱ on the manifold of density matrixes, but usually it is given by a *quadratic cost function* $\gamma_\varrho(B,C) = TrB\mathbf{J}_\varrho^{-1}(C)$ for an operator $\mathbf{J}_\varrho$ acting on all matrices. In order to understand this formula consider a diagonal matrix $\varrho = \sum_i p_i E_{ii}$ where the matrix units E_{ik} are eigenvectors of $\mathbf{J}_\varrho$, and $\mathbf{J}_\varrho$ acts as $R_\varrho^{\frac{1}{2}} f(L_\varrho R_\varrho^{-1}) R_\varrho^{\frac{1}{2}}$ and where L_ϱ and R_ϱ are the left and right multiplication operators. Since E_{ik} are eigenvectors, the symmetrized matrix units $E_{kl} + E_{lk}$ and $iE_{kl} - iE_{lk}$ are eigenvectors as well. Since

$$B = \sum_{k<l} Re(B_{kl}(E_{kl} + E_{lk})) + \\ + \sum_{k<l} Im(B_{kl}(iE_{kl} - iE_{lk})) + \sum_{k<l} B_{ii}E_{ii}$$

we have

$$\gamma_\varrho(B,B) = 2\sum_{k<l} \frac{1}{f(\frac{p_k}{p_l})}|B_{kl}|^2 + \sum_i |B_{ii}|^2 \frac{1}{p_i}$$

for $f : \mathbb{R}^+ \to \mathbb{R}$ any monotone function.

V. Applications

Here we analyze some of the promising applications of the topics discussed above.

A. Encodings

The techniques that allow to translate classical inputs into quantum states are called encodings. There are many different such techniques, let's just review the main ones:

- *Basis encoding*: represent every classical data point as a basis vector, that is, if X is the set of classical inputs we want to translate into the physical states of a given quantum system we can just consider $x \in X \to |x\rangle \in \mathbb{H}$ where x is represented as a binary string and where $\mathbb{H}$ is an Hilbert space of dimension $|X|$ when X is finite. In particular one can map $\{0,1\}$ to $\{|0\rangle, |1\rangle\}$ where by convention $|0\rangle := \binom{1}{0}$, and $|1\rangle := \binom{0}{1}$.
- *Amplitude encoding*: represent every classical data point as the amplitudes of a quantum state, that is, if $\mathbb{H}$ is an Hilbert space of dimension n with basis $\{\psi_1, \dots, \psi_n\}$ consider the map $x \in \mathbb{C}^n \to |\phi_x\rangle := \sum_{i=1}^n x_i \psi_i \in \mathbb{H}$ where the various x_i are the components of x.
- *Angle encoding*: every classical data point is mapped to a rotation $x \to |x\rangle := \bigotimes_{i=1}^n (\cos(x_i)|0\rangle + \sin(x_i)|1\rangle)$.

B. Data compression

It is not always clear if reliable compression schemes can be efficiently implemented in a quantum setting, but in many cases it is possible to work as follows:

- Consider a source which produces n iid random variables $X_i \sim X$ which can be prepared as $\varrho^n = \bigotimes_{i=1}^n \varrho_{X_i}$ where in general the ϱ_{X_i}s are unknown.
- The source perform the transformation $\varrho^n \to \sigma^n$ which is the compression of the source data.
- A receiver gets σ^n and try to recover ϱ^n by a transformation $\sigma^n \to \overline{\varrho}^n$ where $\mathbb{E}(||\overline{\varrho}^n - \varrho^n||_1) \to 0$ as $n \to \infty$.

The main problem here is to define a suitable transformation in such a way not all the n states are needed to recover the original state from the transformed one with high probability and small error. A simple solution is given by $\sigma^n = T\varrho^n T$ where T is the projector over a particular subspace one can recover from the source message. For example, in Schumacher's source coding theorem (see [15] Section 6.2) one encodes the message $x = x_1 x_2 \dots x_n$ where $\mathbb{P}(X_i = x_i) = p_i$ with a message matrix $M = \sum_{i=1}^n p_i |x_i\rangle\langle x_i|$, apply the spectral decomposition to diagonalize $M = \sum_{i=1}^m \alpha_i V_i V_i^*$ (here $m \leq n$), define a sequence of iid random variables $Y_i \sim Y$ with $\mathbb{P}(Y_i = i) = \alpha_i$, then projects over $Span(\bigotimes_{i=1}^m V_{Y_i})$. In this case we know that if the transmission rate is $R > S(M) = Tr(M \log M)$ then the compression scheme is reliable.

C. Autoencoders

The idea behind autoencoders is to force information through a bottleneck while still maintaining recoverability of the data. In [42] are proposed some approaches to quantum autoencoders. Generally speaking the input of such algorithms is an ensamble of pure quantum states $\{p_\mu, |\psi_\mu\rangle\}$ on a bipartite system AB. The goal is then to train an *ansaz* $U(\theta)$ (i.e. a parametrized circuit, equivalently a parametrized family of unitary operators) to compress the ensamble into one of the subsystems, e.g. A. At the end of the process one should be able to recover $|\psi_\mu\rangle$ with high fidelity, only looking at subsystem A. The subsystem B can be thought as a "trash". Quantum autoencoders have also seen an experimental implementation into hardware, see [43].

D. Error correction codes

Quantum Error Correction (QEC) protects qubit states from hardware or environmental noise. Due to the large qubit requirements needed for QEC it seems that their implementation is beyond the reach of NISQ devices. Nevertheless QEC could still be of benefit by suppressing the error up to a certain extent and in combination with other error correction methods. For example QVECTOR [44] was first proposed to discover a device-tailored quantum error-correctiong code for a quantum memory, or "universal" conventional QEC compiled into a given quantum hardware with specific levels of noise where studied in [45] (also numerically). Just to fix the ideas consider a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the computational basis. One can construct a frustration-free Hamiltonian $H = -a_0 P - \sum_{k\geq 1} a_k G_k$ with positive coefficients, projector operator $P = |\psi\rangle\langle\psi| - |\psi^\perp\rangle\langle\psi^\perp|$ and stabilizers G_k. One at this point can discover the circuit that implements $|\psi\rangle$ with a given hardware structure, leverage the fact that the eigenstate energies are known to have fidelity $F \geq \frac{1-(E-E_G)}{a}$ where $E_G = -(a_0 + \sum_{k\geq 1} a_k)$ is the ground energy state, and $a = \min\{a_0, a_k\}$.

E. Quantum Internet

Quantum Internet will provide the infrastructure to transmit the qubits and share their state among the quantum end-nodes (quantum computers, etc.) [51]. To talk about a quantum network, it is not sufficient that it consists of quantum nodes communicating in classical mode, but it is necessary that the nodes exchange qubits and distribute entanglement states among themselves. Quantum Internet will operate in synergy with the existing network, going on to form a hybrid, classical and quantum Internet. In particular, the architecture of the quantum networks will mirror that of the classical networks, in that it will consist of elements that will have similar roles to their classical correspondents, but the technology is not yet mature. The most realistic solution at present for the transmission of qubits (so-called "flying" qubits to distinguish them from "matter qubits" residing in quantum end-nodes and used to process or store information), consists in using photons, also to take advantage of the existing fiber optic infrastructure, however, the distances at which quantum information can be transported without significant losses are still very low. Some preliminary work on quantum switches and routers have been made, see [49], [53], [54] and also some on-the-ground tests were carried out, see for example [1]. Unfortunately it seems difficult to implement Quantum Internet on a large scale, due technological limitations [46], but also due to protocol limitations [55]. It is worth noting, however, that since June 2019, all EU Member States have signed the EuroQCI Declaration [56], agreeing to work together, with the Commission and with the support of the European Space Agency, towards the development of a quantum communication infrastructure covering the whole EU (EuroQCI).

F. Secure Communications and Key Distribution

An encrypted signal sent over a public channel is potentially vulnerable to being intercepted and subsequently decrypted. To date, there is no mathematical proof that guarantees the absolute security of the cryptographic systems currently in use: the security of a cryptographic key is therefore placed in the time required for its encryption. For this reason it is necessary that the cryptographic keys are periodically renewed. In any cryptographic system between remote users, in fact, one of the most critical aspects is the secure exchange of cryptographic keys. In a quantum setting Heisenberg's uncertainty principle and the non-cloning theorem allow to build keys exchange protocols intrinsically secure since the end users who exchange the keys are able to understand if the keys have been intercepted. For concreteness consider the following standard *Quantum Key Distribution BB84* protocol [58]:

- Alice encodes two n bits long strings $a = (a_i)_{i\in\{1,\dots,n\}}$ and $b = (b_i)_{i\in\{1,\dots,n\}}$ in the tensor product $\bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle$ and chooses an index qubit among $|\psi_{00}\rangle = |0\rangle$, $|\psi_{10}\rangle = |1\rangle$, $|\psi_{01}\rangle = |+\rangle$, $|\psi_{1}\rangle = |-\rangle$ (either the computational basis or the Hadamard basis).
- Alice sends $|\psi\rangle$ over a public authenticated quantum channel $\mathcal{E}$ whose action encompass also the noise and the presence of the eavesdropper Eve.
- Bob receives $\mathcal{E}(\varrho) = \mathcal{E}(|\psi\rangle\langle\psi|)$ and Eve cannot share a copy of the same message Bob has received by the no-cloning theorem, unless Eve made a measurement. If Eve made a measurement with probability $\frac{1}{2}$ a bit in $\mathcal{E}(\varrho)$ is changed. After Bob receives the string of qubits, both Bob and Eve have their own states. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits.
- Bob produces a string b' of length n and measures the qubit received by Alice obtaining a string a'.
- Bob anounces publicly that he has recieved a communication by Alice, at this point Alice can safely announce b, i.e. the bases in which the qubits were prepared
- Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the bits in a and a', where b and b' do not match.
- From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $\frac{k}{2}$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques (see for example [59]) to create some number of shared secret keys. Otherwise, they cancel and start over.

G. Quantum Random Number Generators

Quantum physics, that is inherently of probabilistic nature, can be exploited to generate true random numbers (where the randomness is usually measured in terms of information-theoretic entropy) which have important roles in many applications, especially in cryptography and are generally impossible to obtain with only classical means. There are many possible approaches to Quantum Random Number Generators (QRNGs), see [60], among them devices that rely on radioactivity, on qubit's measurement in superposition, arrival times of photons, etc... Just to fix the ideas consider measuring the photon number of a coherent state (this is usually achieved by utilizing a multi-pixel detector arrangement):

$$|\alpha\rangle = e^{\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

with mean number of photons $|\alpha|^2$. In this case it is possible to create truly random numbers that follow a Poisson distribution which we can post-process to get a uniform distribution.

H. Factoring

Shor's algorithm [61] provides an efficient (polylogarithmic) quantum technique that can be used to break RSA encryption or Diffie-Hellman key exchange. Even if large-scale implementations of the Shor's algorithm seem not to be possible in the NISQ era, one cannot avoid the problems that will arise from efficient factoring. Indeed many alternatives have been proposed, one of the most promising is given by considering large factoring as an optimization problem, in particular as a ground state problem for a classical Ising model which can be solved with current methods. See for example [62] which uses the QAOA method with $p \in O(n)$.

I. Chemistry

Characterizing entanglement is crucial in many applications such as material science. Classical methods for materials simulations usually rely on density-functional theory (e.g. the local density approximation). However many effects arising from strongly correlated systems cannot be efficiently studied under such classical framework. Unfortunately a quantum approach is yet not feasible since many quantum methods rely on phase estimation (see for example [63]) that lie beyond the scope of NISQ devices. Some investigations have also been made on the design of novel organic photovoltaics [64].

J. Nuclear and Particle physics

NISQ computers will likely play a central role in understanding the foundations of quantum mechanics since these devices provide an experimental platform to test the fundamental theories (from quantum gravity to quantum Darwinism). Along these lines Quantum Machine Learning methods have been successfully used in Nuclear Physics applications to obtain a quantum advantage in finding nuclear ground states (see the first result about the binding energy of the deuteron in [65]) and in simulating neutrino-nucleon scattering [66]. In particle physics even though there are many analytical tools that allow to describe and study theories, many areas are still intractable. In particular the study of some gauge theories (e.g. quantum chromodynamics) still heavily rely on simulations which cannot usually be classically ran [67] and there seems to be potential also in this field, too [68].

References

[1] Aa.Vv, Field Trial of a finite-key quantum key distribution system in the Florence metropolitan area, Quantum Proceeding, March 2019

[2] M. Sasaki et al., ”Field test of quantum key distribution in the Tokyo QKD Network”. Optics Express. 19 (11): 10387–10409, 2011.

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[4] https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

[5] J. Preskill, ”Quantum Computing in the NISQ era and beyond”. Quantum. 2: 79, 2018.

[6] E. R. Johnston, N. Harrigan, M. Gimeno-Segovia, Programming Quantum Computers, Essential Algorithms and Code Samples, O'Reilly, 2019.

[7] D. Pastorello, Concise Guide to Quantum Machine Learning, Springer 2023.

[8] W. Nawrocki, Introduction to Quantum Metrology, The Revised SI System and Quantum Standards, Second Edition, Springer, 2019.

[9] J. Von Neumann, Thermodynamik quantummechanisher Gesamheiten, Gött. Nach.

[10] J. Von Neumann, Mathematical foundations of quantum mechanics, english translation, Dover, 1954.

[11] D. Bruß, G. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen, Distributed quantum dense coding, Phys. Rev. Lett, vol. 93, p. 210501, 2005.

[12] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels, Phys. Rev. Lett, vol. 70, p. 1895,1983.

[13] C. E. Shannon, A Mathematical Theory of Communication. The Bell System Technical Journal 27,3: 379–423, 1948

[14] A. S. Holevo (Kholevo), “Bounds for the quantity of information transmitted by a quantum communication channel,” Probl. Peredachi Inf., vol. 9, p. 3, 1973, translated in Problems Inf. Transmiss. 9, 177183 (1973).

[15] D. Petz, Quantum Information Theory and Quantum Statistics. Springer-Verlag Berlin Heidelberg, 2010.

[16] G. G. Amosov, A. S. Holevo, R. F. Werner, “On the Additivity Conjecture in Quantum Information Theory”, Probl. Inform. Transm., vol. 36, no. 4, pp. 305–313, 2000.

[17] A. Winter, Scalable programmable quantum gates and a new aspect of the additivity problem for the classical capacity of quantum channels, J. Math. Phys., vol. 43, p. 4341, 2002.

[18] F. Hiai, D. Petz, The proper formula for relative entropy for exponential operators, in Linear operators, Warsaw, 1994, 119-181, Banach Center Publ., 38, Polish Acad. Sci. Warsaw, 1997.

[19] T. Ogawa, H. Nagaoka, Strong converse and Stein's lemma in quantum hypothesis testing, IEEE Tans. Inform. Theory 46(2000), 2428-2433.

[20] A. Uhlmann, The transition probability in the state space of a *-algebra, Rep. Math. Phys. 9(1976), 273-279.

[21] D. Deutsch, R. Jozsa, Rapid solutions of problems by quantum computation, Proceedings of the Royal Society of London A. 439 (1907): 553–558, 1992.

[22] W. Aïmeur, G. Brassard, S. Gambs, Quantum clustering algorithms, ICML '07: Proceedings of the 24th international conference on Machine Learning (2007).

[23] M. Schuld, F. Petruccione, Supervised Learning with Quantum Computers, Springer, 2018.

[24] S. Loyd, M. Mohseni, P. Rebentrost, Quantum algorithms for supervised and unsupervised machine learning (2013) arXiv:1307.0411v2.

[25] M. Andrecut, M. Ali, A quantum perceptron, International Journal of Modern Physics B 16, 639 (2002)

[26] A. Abbas et a., The power of quantum neural networks, in Nature Computational Science 1, 403-409 (2021)

[27] K. Min-Sung, H. Jino, C. Seong-Gon, M. Sung, H. Sang-Wook, Implementation of SWAP test for two unknown states in photons via cross-Kerr nonlinearities under decoherence effect, Scientific Reports. 9 (1): 6167 (2019).

[28] https://quantum-computing.ibm.com/

[29] E. Farhi, J. Goldstone, S. Gutmann, A Quantum Approximate Optimization Algorithm, arXiv:1411.4028 [quant-ph].

[30] M. Negoro, K. Mitarai, M. Kitagawa, K. Fuji, Quantum circuit learning, Phys. Rev. A 98, 032309, September 2018.

[31] V. Giovannetti, S. Lloyd, L. Maccone, Quantum-enhanced measurements: beating the standard quantum limit. Science, 306(5700):1330–1336, 2004

[32] V. Giovannetti, S. Lloyd, L. Maccone, Advances in quantum metrology. Nat. Phot., 5(4):222, 2011.

[33] M. H. Levitt. Spin dynamics: basics of nuclear magnetic resonance. John Wiley and Sons, Chichester, 2001.

[34] D. Le Sage, et al., Optical magnetic imaging of living cells. Nature, 496(7446):486, 2013.

[35] E. Ramsden. Hall-effect sensors: theory and application. Elsevier, 2011.

[36] M. E. Huber, et a., Gradiometric micro-SQUID susceptometer for scanning measurements of mesoscopic samples. Rev. Sci. Instr., 79(5):053704, 2008

[37] M. Poggio, C. L. Degen, Force-detected nuclear magnetic resonance: recent advances and future challenges. Nanotech., 21(34):342001, 2010.

[38] M. Bal, C. Deng, et al., Ultrasensitive magnetic field detection using a single artificial atom. Nat. Comm., 3:1324, 2012.

[39] J. L. Beckey, M. Cerezo, A. Sone, P. J. Coles, Variational quantum algorithm for estimating the quantum Fisher information, arXiv preprint, arXiv:2010.10488 (2020)

[40] Z. Ma, et. al, Adaptive circuit learning for quantum metrology, arXiv preprint arXiv:2010.08702 (2020)

[41] B. Koczor, et al., Variational spin-squeezing algorithms on programmable quantum sensors, Physical Review Letters 123, 260505 (2019)

[42] J. Romero, J.P. Olson, A. Aspuru-Guzik, Quantum autoencoders for efficient compression of quantum data, Quantum Science and Technology 2, 045001 (2017)

[43] A. Pepper, N. Tischler, G. J. Pryde, Experimental realization of a quantum autoencoder: The compression of qutrits via machine learning, Physical Review Letters 122, 060501 (2019)

[44] P. D. Johnson, J. Romero, J.P. Olson, Y. Cao, A. Aspuru-Guzik: Qvector: an algorithm for device-tailored qunatum error correction, arXiv preprint, arXiv:1711.02249

[45] X. Xu, S. X. Benjamin, X. Yuan, Variational circuit compiler for quantum error correction, arXiv preprint, arXiv:1911.05759

[46] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp and L. Gyongyosi, ”Wireless myths realities and futures: From 3G/4G to optical and quantum wireless”, Proc. IEEE, vol. 100, no. Special Centennial Issue, pp. 1853-1888, May 2012.

[47] ITU Workshop on Quantum Information Technology for Networks (Shanghai, China, 5-7 June 2019)

[48] H. V. Nguyen et al., ”Towards the quantum Internet: Generalised quantum network coding for large-scale quantum communication networks”, IEEE Access, vol. 5, pp. 17288-17308, 2017.

[49] Pant, M., Krovi, H., Towsley, D. et al. ”Routing entanglement in the quantum internet” in npj Quantum Inf 5, 25, 2019.

[50] H. Barnum, E. Knill and M.A. Nielsen, ”On quantum fidelities and channel capacities” in IEEE Transactions on Information Theory, 46(4), 1317–1329.

[51] S. Pirandola and S. L. Braunstein, ”Physics: Unite to build a quantum Internet”, Nature, vol. 532, no. 7598, pp. 169-171, Apr. 2016.

[52] B. Rosgen and J. Watrous, ”On the hardness of distinguishing mixed-state quantum computation” in 20th Annual IEEE Conference on Computational Complexity (CCC'05), 2005, pp. 344–354.

[53] M. Caleffi, A. S. Cacciapuoti, ”Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels” in IEEE journal on selected areas in communications, vol. 38, no. 3, march 2020

[54] M. Caleffi, A. S. Cacciapuoti, G. Bianchi, ”Quantum Internet: from Communication to Distributed Computing” in Association for Computing Machinery. 2018.

[55] Angela S. Cacciapuoti et al, ”The Quantum Internet: Networking Challenges in Distributed Quantum Computing” in Quantum Internet: Networking Challenges in Distributed Quantum Computing, 2019.

[56] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[57] Xiao-Ling Pang, Ai-Lin Yang et al. ”Hacking Quantum Key Distribution via Injection Locking” in Physical Review Applied 13 (3), 2020.

[58] Quantum Key Distribution: Use Cases – ETSI GS QKD 002 v1.1.1, 2010-06

[59] H.F. Chau,Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate, Physical Review A. 66 (6): 60302 (2002).

[60] Vaisakh Mannalath, Sandeep Mishra, Anirban Pathak ”A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness” https://arxiv.org/pdf/2203.00261.pdf

[61] P.W. Shor, ”Algorithms for quantum computation: discrete logarithms and factoring”. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134 (1994).

[62] E. Anschuetz, J. Olson, A. Aspuru-Guzik, Y. Cao, Variational quantum factoring, International Workshop on Quantum Technology and Optimization Problems, Springer 2019, pp. 74-85.

[63] B. Bauer, et al., Hybrid quantum classical approach to correlated materials, Physical Review X 6,031045 (2016)

[64] M. Gross, et al., Improving the performance of doped $\pi-$conjugated polymers for use in organic light-emitting, Nature 405,661-665 (2000)

[65] E. Dumitrescu, et al., Cloud quantum computing of an atomic nucleus, Physical Review Letters 120, 210501 (2018)

[66] A. Roggero, et al., Quantum computing for neutrino-nucleus scattering, Physical Review D 101,074038 (2020)

[67] M. C. Banuls, et al., Simulating lattice gauge theories within quantum technologies, The European physical journal D 74, 1-42 (2020)

[68] J. Preskill, Simulating quantum field theory with quantum computer, arXiv preprint, arXiv:1811.10085