# Quantum Computation and Quantum Information

Jack Ceroni
*Xanadu, Toronto, ON, M5G 2C8, Canada*
(Dated: February 8, 2022)

The purpose of these notes is two-fold: to provide a primer on some foundational and cutting-edge techniques in quantum computation and quantum information, and to help me develop my own understanding of these concepts.

## CONTENTS

# I. BASIC QUANTUM INFORMATION

## A. Measurements

In this section, we will introduce quantum mechanical measurements.

In quantum theory, measurements are characterized by a list of operators of the form $\{M_m\}$, where the operator $M_m$ corresponds to the outcome of an experiment labelled $m$. Given the state $|\psi\rangle$, the probability of measuring outcome $m$ is given by $\langle\psi|M_m^\dagger M_m|\psi\rangle$, and the state after measurement becomes:

$$|\psi\rangle \to |\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

More specifically, many of the measurements we will deal with in quantum information are **projection measurements**, where a measurement is specified.

A little bit of thought shows us that this is a specific case of our original definition of a measurement, where the projectors onto eigenstates play the role of

---

In many instances, we cannot "choose" an aribtrary operator to measure when executing a quantum circuit. Usually, the operator we measure with repsect to is given by the matrix $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, which corresponds to performing a measurement in the computational basis. Measuring this operator is effectively the same as measuring the $Z$ operator, up to multiplying by a constant and adding the identity. Thus, going forward, we will assume that for some quantum circuit, we can measure the $Z$ operator.

Suppose we have a quantum circuit which implements the unitary $U$, and we wish to measure the state $U|\psi\rangle$ with respect to $Z$. We will show that this is the same as measuring $|\psi\rangle$ with respect to the operator $U^\dagger ZU$.

Indeed, note that when we measure $U|\psi\rangle$ with respect to $Z$, we get the result 1 with probability $|\langle 0|U|\psi\rangle|^2$, or $-1$ with probability $|\langle 1|U|\psi\rangle|^2$. Similarly, if we measure $|\psi\rangle$ with respect to $U^\dagger ZU$, which has the same eigenvalues the same, and eigenvectors $U^\dagger|0\rangle$, $U^\dagger|1\rangle$, we get the exact same probabilities of measuring 1 or $-1$.

This is why, in order to measure with respect to $X = H^\dagger ZH$ on a quantum computer, we apply a Hadamard $H$ and then measure with respect to $Z$. Note that the state after performing these different procedures is different: in the former case, we collapse the state to an eigenvector of $X$, while in the latter, we collapse to an eigenstate of $Z$. However, this can be remedied by applying $U$ to the state after measurement.

In general, we can find a nice correspondence between measuring with respect to an arbitrary, Hermitian operator $H$, and applying a corresponding unitary $U$, then measuring in the $Z$ basis. Suppose we have an arbitrary, normalized Hermitian of the form:

$$n \cdot \hat{P} = \sin\phi$$

## B. Bells Inequality

In this section, we will be discussing Bell's inequality, which refutes the claim that there exists a hidden-variables interpretation of quantum theory.

Suppose we prepare a quantum system, and we wish to take a measurement of the spin-operator projection $\hat{a} \cdot \hat{\sigma}$. Let us assume that the outcome of this measurement, which we call $a$ is pre-determined by some "hidden variable". That is to say that $a$ is a function of some "true characteristic" $\lambda$ of the quantum system. In fact, we write $a$ as a function of $\lambda$, $a(\lambda)$, depending on what this parameter is set to.

Averaging across all values of $\lambda$, we find that the expected value of $a$ is precisely $\int a(\lambda)p(\lambda)\ d\lambda$, where $p(\lambda)$ is the probability density function of $\lambda$. In order for the hidden variables theory to be valid, this quantity must coincide with the "quantum mechanical" expectation value, which is $\langle \hat{a} \cdot \hat{\sigma} \rangle$.

Now, suppose that we prepare a quantum system in the state $|\beta_2\rangle = -\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

### C. The Schmidt Decomposition

---

One of the things that we wish to do in the field of quantum information is characterize the amount of entanglement contained in some quantum system. We will come back to this topic later, when we discuss entanglement measures. However, for the time-being, we will highlight a more simple/intuitive technique. The **Bell state** is defined as the following state of a two-qubit system:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1}$$

Unsurprisingly, this state is said to be **maximally entangled**: possesing the largest possible "amount" of entanglement. We can define "higher-order" analogues of the Bell state for systems of qudits, by simply considering states of the form $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle + |22\rangle + \cdots + |nn\rangle)$. The Schmidt decomposition essentially says that for a bipartite system of this form, for any $|\psi\rangle$, we can always choose local unitaries $U_A$ and $U_B$ such that we have:

$$|\psi\rangle = (U_A \otimes U_B) \sum_j \lambda_j |jj\rangle \tag{2}$$

The implications of this statement are far-reaching. We effectively know "how much" entanglement is contained in a state of the form $\sum_j \lambda_j |jj\rangle$. We also know, intuitively, that application of local unitaries will not affect the amount of entanglement in a system. Thus, writing a state in this form immediately tells us "how entangled" it is.

The proof of this statement is simple: we simply write $|\psi\rangle = \sum_{i,j} \chi_{ij}|ij\rangle$, and treating $\chi_{ij}$ as the elements of a matrix $\boldsymbol{\chi}$, which we can identify with linear transformation $T_{\boldsymbol{\chi}}$ (with respect to the computational/standard basis). We can take the singular-value decomposition of the matrix, which allows us to write $\boldsymbol{\chi} = U\Lambda V^\dagger$, where both $U$ and $V^\dagger$ are unitary matrices, and $\Lambda$ is diagonal, containing the singular values of $T_{\boldsymbol{\chi}}$. This yields:

$$\chi_{ij} = \sum_k U_{ik}\Lambda_{kk}V^*_{jk} = \sum_k U_{ik}s_k V^*_{jk}$$

where $s_k$ is the $k$-th singular value. From this formula, it follows that:

$$|\psi\rangle = \sum_{i,j} \chi_{ij}|ij\rangle = \sum_{i,j}\left(\sum_k U_{ik}s_k V^*_{jk}\right)|ij\rangle = \sum_k s_k \left(\sum_i U_{ik}|i\rangle\right) \otimes \left(\sum_j V^*_{jk}|j\rangle\right) = (U \otimes V^*)\sum_k s_k|kk\rangle$$

where we know that $V^*$ is unitary, as $V^*(V^*)^\dagger = V^*V^T = (VV^\dagger)^T = I^T = I$. Computation of the Schmidt decomposition is fairly simple: we simply need to find the singular values $s_k$, as well as the matrices $U$ and $V^*$. Indeed, note that:

$$\boldsymbol{\chi}\boldsymbol{\chi}^\dagger = U\Lambda^2 U^\dagger \quad \text{and} \quad \boldsymbol{\chi}^\dagger\boldsymbol{\chi} = V\Lambda^2 V^\dagger$$

where $\Lambda^2$ is clearly the matrix with diagonal the squared singular values, which are precisely the eigenvalues of $\boldsymbol{\chi}\boldsymbol{\chi}^\dagger$ and $\boldsymbol{\chi}^\dagger\boldsymbol{\chi}$. Thus, we simply need to diagonalize these two matrices, and we are left with $U, V$, and the singular values.

---

For the sake of completeness, we can do a short example. Consider the state:

$$|\psi\rangle = \frac{1}{10}\left(i\sqrt{27}|00\rangle + 3|01\rangle - 4|10\rangle - i\sqrt{48}|11\rangle\right)$$

The matrix $\boldsymbol{\chi}$ is clearly given by:

$$\boldsymbol{\chi} = \frac{1}{10}\begin{pmatrix} i\sqrt{27} & 3 \\ -4 & -i\sqrt{48} \end{pmatrix}$$

so to perform the Schmidt decomposition, we diagonalize the following matrices:

$$\boldsymbol{\chi}^\dagger\boldsymbol{\chi} = \frac{1}{100}\begin{pmatrix} 43 & 7\sqrt{3}i \\ -7\sqrt{3}i & 57 \end{pmatrix} \quad \text{and} \quad \boldsymbol{\chi}\boldsymbol{\chi}^\dagger = \frac{1}{100}\begin{pmatrix} 36 & 0 \\ 0 & 64 \end{pmatrix}$$

Luckily, the second matrix is already diagonal, so it follows immediately that $V = \mathbb{I}$, and the singular values are precisely $\frac{4}{5}$ and $\frac{3}{5}$. Our task is to diagonalize $\boldsymbol{\chi}^\dagger\boldsymbol{\chi}$. It has the same eigenvalues of $\boldsymbol{\chi}\boldsymbol{\chi}^\dagger$, so we note:

$$\begin{pmatrix} 43 & 7\sqrt{3}i \\ -7\sqrt{3}i & 57 \end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = 36\begin{pmatrix}\alpha\\\beta\end{pmatrix} \Rightarrow \begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\sqrt{3}\\ i\end{pmatrix}$$

$$\begin{pmatrix} 43 & 7\sqrt{3}i \\ -7\sqrt{3}i & 57 \end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = 64\begin{pmatrix}\alpha\\\beta\end{pmatrix} \Rightarrow \begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}i\\ \sqrt{3}\end{pmatrix}$$

are representatives of the eigenspaces corresponding to both eigenvalues. We want to choose our change-of-basis matrix such that it is unitary. We can do this by multiplying both eigenvector by $\frac{1}{2}$, so the change-of-basis matrix from the computational basis to the eigenvector basis is:

$$R = \frac{1}{2}\begin{pmatrix} \sqrt{3} & i \\ i & \sqrt{3} \end{pmatrix}$$

so it follows that $U = R^\dagger = \frac{1}{2}\begin{pmatrix} \sqrt{3} & -i \\ -i & \sqrt{3} \end{pmatrix}$. This concludes our calculations: the Schmidt decomposition tells us that:

$$|\psi\rangle = \left(\frac{1}{2}\begin{pmatrix} \sqrt{3} & -i \\ -i & \sqrt{3} \end{pmatrix} \otimes \mathbb{I}\right)\left(\frac{3}{5}|00\rangle + \frac{4}{5}|11\rangle\right)$$

Let's verify this very quickly, as a sanity check. We have:

$$\left(\frac{1}{2}\begin{pmatrix} \sqrt{3} & -i \\ -i & \sqrt{3} \end{pmatrix} \otimes \mathbb{I}\right)\left(\frac{3}{5}|00\rangle + \frac{4}{5}|11\rangle\right) = \frac{3}{10}\left(\sqrt{3}|0\rangle - i|1\rangle)\otimes|0\rangle\right) + \frac{2}{5}\left((-i|0\rangle + \sqrt{3}|1\rangle)\otimes|1\rangle\right)$$

$$= \frac{3\sqrt{3}}{10}|00\rangle - \frac{3i}{10}|10\rangle - \frac{4i}{10}|01\rangle + \frac{4\sqrt{3}}{10}|11\rangle$$

In this section, we review some basic techniques in linear algebra, which allow us to prove certain facts.

### A. Singular Values

Suppose we are given a linear operator $T$. Clearly, the operator $T^*T$ will be positive, so it has a unique positive square-root, $\sqrt{T^*T}$. Such an operator, by spectral theorem, will have a basis of orthonormal eigenvectors with positive eigenvalues. We call these eigenvalues the **singular values** of $T$.

**Theorem 1.** *The singular values of $T$ are precisely the square roots of the eigenvalues of $T^*T$, repeated with multiplicity.*

### B. Singular Value Decomposition

We know from the polar decomposition that we can write $T$ in the form $S\sqrt{T^*T}$. Since $\sqrt{T^*T}$ is self-adjoint, it is diagonalizable. If we let $v_j$ be an orthonormal basis of eigenvectors for $\sqrt{T^*T}$, and let $e_j$ be the standard basis, we let $T'e_j = s_j e_j$, and let $U$ be the map which sends $v_j$ to $e_j$. Clearly, $U$ is an isometry. Thus:

$$T = S\sqrt{T^*T} = SU^{-1}T'U$$

If we let $\mathcal{M}(\cdot)$ denote the matrix of a linear operator, with respect to the standard basis, then we have:

$$\mathcal{M}(T) = \mathcal{M}(SU^{-1})\mathcal{M}(T')\mathcal{M}(U)$$

where both $\mathcal{M}(SU^{-1})$ and $\mathcal{M}(U)$ are unitary matrices, and $\mathcal{M}(T')$ is diagonal, with the singular values along the diagonal.