Quantum Information and Quantum Computation: Term paper

S. Gauthameshwar

1. Quantum Fourier transform

The idea behind Quantum Fourier Transform (QFT)

A Fourier transform is a transform of writing a periodic function in terms of orthonormal functions of the form $\phi_k(x) \sim e^{i k x}$. If we have a set of complete orthonormal functions in a vector space, a transform of basis can be done from our current basis of defining a function to that orthonormal basis without any loss of information. In simple terms, it is rewriting the same function in a different language. Now, if we have a discrete domain of N values for a periodic function $X_n = \{x_i\}$, the resultant fourier transform gives us the components of frequencies corresponding to each fourier function present in it defined by: $X_k = \{k_i\}$. Mathematically, a Discrete Fourier Transform as mentioned above is given by:

$$X_k = \sum_{i=0}^{N-1} x_n \, e^{\frac{2 \pi n i}{N} k}$$

We immediately see the periodicity of our X_k in N as on replacing n with $N + n$, we get: $e^{\frac{2 \pi (N+n) i}{N} k} = e^{2 \pi i k} e^{\frac{2 \pi n i}{N} k} = e^{\frac{2 \pi n i}{N} k}$ as $k \in Z$. Our input x_i can be defined over the domain of **C** but in our quantum algorithms implemented below, we stick to their values being integers for the sake of simplicity.

Mathematical Formulation

To establish any integer y written in terms of n qubits ($y < 2^n$), we explain the two notations of qubits: $| y \rangle \equiv | y_1, y_2 ..., y_n \rangle$:

Let $| y_1, y_2 ..., y_n \rangle$ be a quantum state in the Hilbert space of n qubits representing an integer. Each y_i corresponds to a spin state of either 0 or 1. We translate this binary qubit $| y_1, y_2 ..., y_n \rangle$ to an integer state $| y \rangle$ by the relation:

$$y = \sum_{i=0}^{n-1} 2^{n-i} y_i \tag{1}$$

So for example, if we have $| 0 \times 1 \times 1 \rangle$, it translates to $y = 2^2 y_1 + 2^1 y_2 + 2^0 y_3 = 2 + 1 = 3$. The maximum integer we can achieve to write in this n qubits is $N = 2^n$

Now, we shall define the fourier basis written in terms of computational basis as:

$$| k \rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{\frac{2 \pi i x}{N} k} \left| x \right\rangle \tag{2}$$

To get a good idea of what the above definition means, we look at some examples! Consider a single qubit case. We can represent the integers 0 and 1 with this. Fourier function corresponding to 0, from Eq.2, is:

$$| 0 \rangle = \frac{1}{\sqrt{2^1}} \left(e^{\frac{2 \pi i 0}{2} 0} \left| 0 \right\rangle + e^{\frac{2 \pi i 1}{2} 0} \left| 1 \right\rangle \right) = \frac{1}{\sqrt{2}} \left| 0 \right\rangle + \left| 1 \right\rangle$$

Similarly, for the fourier basis corresponding to integer 1, we have:

$$| 1 \rangle = \frac{1}{\sqrt{2^1}} \left(e^{\frac{2 \pi i 0}{2} 1} \left| 0 \right\rangle + e^{\frac{2 \pi i 1}{2} 1} \left| 1 \right\rangle \right) = \frac{1}{\sqrt{2}} \left| 0 \right\rangle - \left| 1 \right\rangle$$

Thus, we have defined the fourier function corresponding to every integer writable in n-qubit form. An interesting property of these fourier functions is that they all lie in the x-y plane of the Bloch's Sphere. Now, if we extend our integers to n-qubits, the computational basis $| x \rangle$ can be expanded and rewritten in the form of direct product as:

$$|\,k\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{\frac{2\pi i x}{N} k} \left|x\right\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{x_0=0}^{1} \sum_{x_1=0}^{1} \ldots \sum_{x_n=0}^{1} e^{\frac{2\pi i \left(\sum_{i=0}^{n-1} 2^{n-i} x_i\right)}{N} k} \left|x_0,\; x_1,\; \ldots x_{n-1}\right\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{x_0, x_1, \ldots x_n} \bigotimes_{i=0}^{n-1} e^{\frac{2\pi i x_i}{N} 2^{n-i} k} \left|x_i\right\rangle$$

$$= \frac{1}{\sqrt{N}} \bigotimes_{i=0}^{n-1} \sum_{x_0, x_1, \ldots x_n} e^{\frac{2\pi i x_i}{N} 2^{n-i} k} \left|x_i\right\rangle$$

$$= \bigotimes_{i=0}^{n-1} \frac{1}{\sqrt{2}} \left(\left|\,0\right\rangle + e^{2\pi i \frac{k}{2^i}} \left|\,1\right\rangle \right)$$

Hence, we see that after some algebra manipulation, our fourier basis can be equivalently expressed as unitary operators acting on individual fourier qubits.

$$|\,k\rangle = |\,k_0,\; k_1 \ldots k_{n-1}\rangle = \frac{1}{\sqrt{2}} \left(\vdots|0\rangle + e^{2\pi\,\mathrm{i}\,\frac{\mathrm{k}}{2^0}} \left|1\right\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(\vdots|0\rangle + e^{2\pi\,\mathrm{i}\,\frac{\mathrm{k}}{2^1}} \left|1\right\rangle \right) \otimes \ldots \otimes \frac{1}{\sqrt{2}} \left(\vdots|0\rangle + e^{2\pi\,\mathrm{i}\,\frac{\mathrm{k}}{2^{\mathrm{n}-1}}} \left|1\right\rangle \right) \tag{3}$$

After this simplification, it is more illuminating as to how our quantum circuit is to be constructed to achieve the QFT.

Quantum Circuit Implementation

From Eq.3, we see that each individual qubit lies in the x-y plane of Bloch's Sphere ($\theta = \pi/2$) and is defined by a unitary operation that rotates a qubit around this equator. We also saw the example of a single qubit fourier basis where $|\,k\rangle$ is given by the Hadamard acting on $|\,0\rangle$ and $|\,1\rangle$ to give $|\,k=0\rangle$ and $|\,k=1\rangle$ respectively. Define H and U_k as:

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

$$U_j = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^j}} \end{pmatrix}$$

$U_j\,|\,x_i\rangle = e^{\frac{2\pi i}{2^j} x_i} \left|x_i\right\rangle$ s.t it only adds a phase if $x_i = 1$. Equivalently, it can also be written as a conditional phase addition on a qubit iff our $x_i = 1$

Now, to achieve $\frac{1}{\sqrt{2}}\left(\vdots|0\rangle + (-1)^{\mathrm{k}_0} e^{2\pi\,\mathrm{i}\,\frac{\mathrm{k}}{2^{\mathrm{n}-1}}}\left|1\right\rangle\right) \otimes \left|\mathrm{x}_1\right\rangle \otimes \ldots \otimes \left|\mathrm{x}_{\mathrm{n}-1}\right\rangle = \frac{1}{\sqrt{2}}\left(\vdots|0\rangle + (-1)^{\mathrm{k}_0} e^{2\pi\,\mathrm{i}\,\frac{\mathrm{k}_{\mathrm{n}-1}}{2^{\mathrm{n}-1}}}\, e^{2\pi\,\mathrm{i}\,\frac{\mathrm{k}_{\mathrm{n}-2}}{2^{\mathrm{n}-1}}} \ldots e^{2\pi\,\mathrm{i}\,\frac{\mathrm{k}_0}{2^{\mathrm{n}-1}}}\left|1\right\rangle\right) \otimes \left|\mathrm{x}_1\right\rangle \otimes \ldots \otimes \left|\mathrm{x}_{\mathrm{n}-1}\right\rangle$ we act k_0 with H first to rotate our qubit onto the x-y plane, then repeatedly act U_j for all $j \in \{2,\, n-1\}$. After obtaining the desired first qubit, we move to second and repeat the same but now only the U_k for all $k \in \{2,\, n-2\}$ since the coefficient in the denominator goes only up to 2^{n-2} for the second qubit. Hence, by performing this operation till we obtain the desired last qubit, we have Eq(3), but reversed in order. The circuit below gives the implementation of the unitaries as explained here:

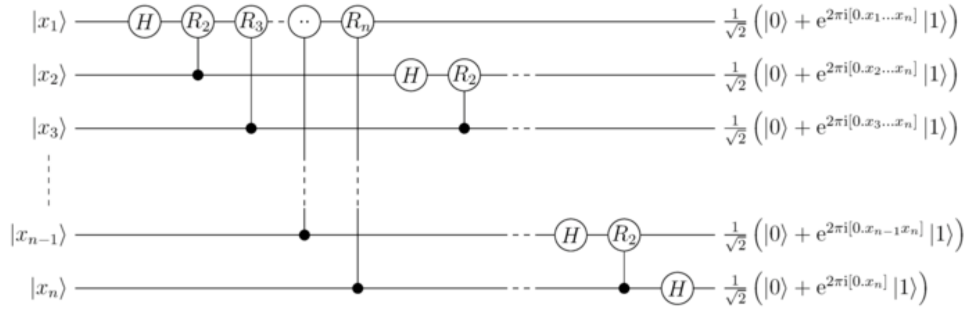

$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|x_{n-1}\rangle$
$|x_n\rangle$
H
R_2
R_3
R_n
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_1 \ldots x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_2 \ldots x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_3 \ldots x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_{n-1} x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_n]}|1\rangle\right)$

Fig.1 Quantum circuit for converting our computational basis to fourier basis. Note: $R_j \equiv U_j$

If we wish to remove the reverse ordering obtaines at the end, we simply swap x_i with x_{n-i} at the end of our operations.

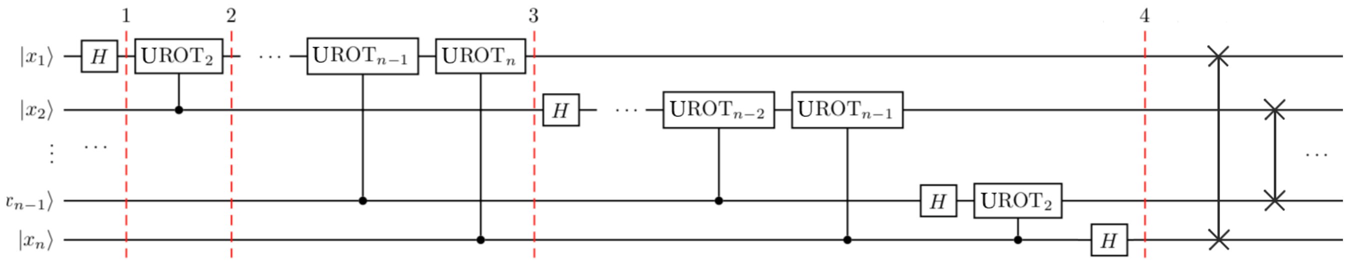


Fig.2 Quantum circuit for converting our computational basis to fourier basis without reversing the qubits. Note: $\mathrm{UROT}_j \equiv U_j$

The advantage of QFT over classical DFT or FFT is the time taken to apply our fourier transform. Classical take exponential runtime w.r.t input data size n of $O\left(e^{n^{1/3}}(\ln(n))^{2/3}\right)$. However Shor's Algorithm takes only poly runtime of $O\left(n^2 \ln(n) \ln(\ln(n))\right)$. Hence, we get an exponential improvement in the speed of out algorithm. This is extremely useful when we need to compute QFT of very large data size. So any direct application of FFT can also be optimised by implementing QFT for the sake of computational efficiency. One example of FFT is to filter out noise from useful data and signals. Noises tend to occupy the signal with significant contribution in higher frequency ranges. So on transforming to our fourier space, detecting and eliminating the sharp lines corresponding to those noises, we can retrieve the signal but now, without the noise present in it.

However, I felt another application of QFT that is more amusing than just making it a computationally upgraded version of DFT.

Efficient Quantum Phase Estimators: Application of QFT

Suppose we have a state $|\psi\rangle = |0\rangle|\phi\rangle$. Acting H on the first qubit gives us:

$$|\psi\rangle = 1/\sqrt{2}\,(|0\rangle|\phi\rangle + |1\rangle|\phi\rangle) \tag{4}$$

If a unitary is defined by $U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$, it adds a relative phase between the $|0\rangle$ and $|1\rangle$ state of $|\psi\rangle$ on acting on the first qubit. Estimating this phase by any physical measurement is not possible since probability only cares of its norm squared coefficient. And if we try to be a bit smart and apply H on the first qubit again, we have a physical way of measuring this phase:

$$|\psi\rangle = 1/\sqrt{2}\,(|0\rangle|\phi\rangle + e^{i\theta}|1\rangle|\phi\rangle) \tag{5}$$

$$H|\psi\rangle = 1/2\,((|0\rangle + |1\rangle)|\phi\rangle + e^{i\theta}(|0\rangle - |1\rangle)|\phi\rangle) = 1/2\left(\left(1 + e^{i\theta}\right)|0\rangle + \left(1 - e^{i\theta}\right)|1\rangle\right)$$

It now seems that we have a physical way of measuring this phase as the probability of getting spin value ± 1 is $\left|\frac{1 \pm e^{i\theta}}{2}\right|^2$. However we still need lots of statistical copies of our state and make several measurements to achieve a good resolution of the probabilities to get the phase introduced by our U. However, this method is really inefficient for small values of θ. For instance if $\theta = 1\,°$, $P(+1) = 0.9999$ and if $\theta = 10\,°$, $P(+1) = 0.9924$. This precision of resolving our probabilities and extracting θ can be made efficient by applying a QFT in disguise using our unitary U and taking its inverse QFT. Instead of tensor product of $|\phi\rangle$ with one qubit, we now do it with n qubits to obtain a n-qubit output that holds the information of the phase at the end.

Step-1: Apply H, to get similar to Eq.4 as:

$$|\psi\rangle = \left(\bigotimes^{n} \frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle)\right)|\phi\rangle$$

Step-2: Act U n times on the first qubit, n-1 times on the second qubit and so on till the last qubit has $U^0 = I$ acted. Fig. 3 for illustrated implementation of the above unitary. This gives us the state after the step:

$$|\psi\rangle = \frac{1}{\sqrt{N}}\left(\left(\vdots|0\rangle + e^{\mathrm{i}\,\theta\,2^{\mathrm{n}-1}}|1\rangle\right)\left(\vdots|0\rangle + e^{\mathrm{i}\,\theta\,2^{\mathrm{n}-2}}|1\rangle\right)\ldots\left(\vdots|0\rangle + e^{\mathrm{i}\,\theta\,2^{0}}|1\rangle\right)|\phi\rangle\right) \tag{6}$$

We immediately see striking similarity with Eq.3 and on comparing the coefficients, we get :

$$x = \frac{2^n}{2\pi}\theta \tag{7}$$

Step-3 and 4: Perform inverse fourier transform on the output state to extract x. Finally measure $|x\rangle$ to find θ

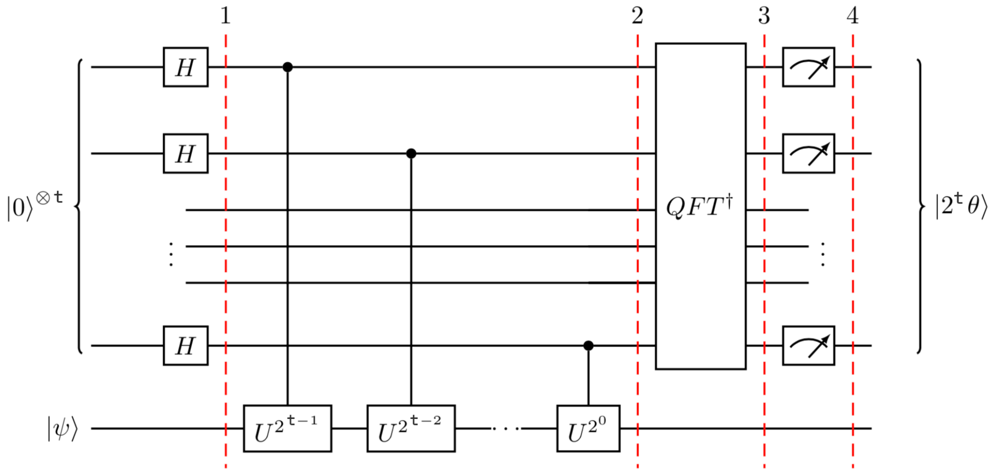


Fig.3 Quantum circuit for a Quantum Phase estimator.Note: t≡n

We see that the resultant output has amplified the phase whose resolution gets better as we increase n as 2^n multiplies the phase θ. Hence, QFT can be used to find the relative phases introduced by unitary U to a desirable resolution.

Quantum Entanglement

Basics

LOCC based definition of Entanglement

LOcal quantum operation with Classical Communication (LOCC) is a way of creating a state of two spins by performing unitary operations locally after concurrently deciding on classical probability $p^{(k)}$ of the state $\rho^{(k)}$. If Alice and Bob has two spins with each and has decided to create a quantum state based on the above definition, it takes the form:

$$\rho = \sum p^{(k)} \rho_{\mathrm{ab}}{}^{(k)} \tag{8}$$

$p^{(k)}$ is the classical probabilities introduced to decide the classical coherence between the final ρ_{ab}. Now, if the above state is separable to two independent direct products, it is most generally written as:

$$\rho = \sum p^{(k_1,k_2)} \rho_a{}^{(k_1)} \otimes \rho_b{}^{(k_2)} \tag{9}$$

Eq.9 is the most general form of an unentangled state generated by LOCC. If we CANNOT write a given state in the form of Eq.9, then our state is defined as an entangled state.

Examples of entangles and unentangled states based on LOCC defined states:

$\rho_{\mathrm{ent}} = 1/2\,(|00\rangle\langle 00| + |11\rangle\langle 11|)$. $\rho^{(1)} = |00\rangle\langle 00|$, $p^{(1)} = \frac{1}{2}$; $\rho^{(2)} = |11\rangle\langle 11|$, $p^{(2)} = \frac{1}{2}$

$\rho_{\mathrm{unent}} = 1/2\,(|01\rangle\langle 01| + |11\rangle\langle 11|) = 1/2\,(|0\rangle\langle 0| + |1\rangle\langle 1|)\otimes |1\rangle\langle 1|$. $\rho^{(1)} = |0\rangle\langle 0| \otimes |1\rangle\langle 1|$, $p^{(1)} = \frac{1}{2}$; $\rho^{(2)} = |1\rangle\langle 1| \otimes |1\rangle\langle 1|$ $p^{(2)} = \frac{1}{2}$

LOCC does NOT increase entanglement

Suppose we have an unentangled state of the form:

$$\rho = \sum p^{(k)} \rho_a{}^{(k)} \otimes \rho_b{}^{(k)} \tag{10}$$

This equation tells us the fact that Alice and Bob can introduce classical correlations by fixing on $p^{(k)}$ for each density state in their respective hands. Now this corresponds to local operation performed by Alice and Bob on their respective states at their disposal. To understand why

LOCC must NOT lead to entanglement, let us consider a case where Alice and Bob uses their states to perform teleportation. Clearly teleportation demands entanglement since entanglement is a non-local phenomenon and teleportation uses this as it main principle. Suppose Alice wishes to send $|\psi\rangle$ to Bob via teleportation with their prepared states. Alice only has ρ_a at her disposal. So any operation that she does on the tensor product of $|\psi\rangle$ and ρ_a remains within her Hilbert space and never influences the Hilbert space of Bob from the definition of direct product. Thus, it will not be possible to achieve teleportation of qubit from Alice to Bob with an unentangled state of the form as Eq.8. If, however, classical coherence can lead to entanglement, we see that an unentangled state is resulting in teleportation which is contradicting our above claim. Hence, classical coherence, acting locally CANNOT create entanglement that leads to non-local influence of the qubits in the hands of Alice and Bob.

Preservation of entanglement under local unitary operations

An intuitive argument is presented here without any rigorous proof. A unitary transformation is a change of basis of our Hilbert space as it is a norm preserving rotation operation. So it must not be the case that if we see the same state written in a different rotated basis, we have a different measure of entanglement since entanglement is a property of a system and not on which language (in terms of basis vectors) it is expressed in. Hence, we impose the condition that local unitary matrices must preserve the entanglement of our state after being acted.

Positive and Completely positive maps

A positive map is defined as an operator acting on a positive operator and maps it to another positive operator. Mathematically,

$$\Theta : \mathcal{A}_1 \to \mathcal{A}_2 \; s.t$$

$$\Theta(A) \geq 0 \quad \forall A \in \mathcal{A}_1 \tag{11}$$

Where $\mathcal{A}_1$, $\mathcal{A}_2$ are spaces of positive operators. Here, we will use the positive maps to act on density matrices.

A complete positive map on the other hand is defined on an extended tensor product space of the positive operators as an operator acting on it and maps it to another positive operator. Mathematically,

$$\Theta \otimes \mathbb{1}_d : \mathcal{A}_1 \otimes \mathcal{M}_d \to \mathcal{A}_2 \otimes \mathcal{M}_d \; s.t$$

$$\Theta(A) \geq 0 \quad \forall A \in \mathcal{A}_1 \otimes \mathcal{M}_d \tag{12}$$

Where $\mathcal{A}_1$, $\mathcal{A}_2$ are spaces of positive operators and $\mathcal{M}_\mathrm{d}$ is any matrix in the Hilbert space of $\mathcal{H}_{d\times d}$. This definition of positive maps will be useful in checking if our maps are positive in higher dimension Hilbert spaces where phenomenon such as entanglement can exist and can result in violation of complete positivity while still preserving positivity.

An example of positive maps: Consider a set of all density matrices $\mathcal{A}_1 = \{\rho_i\}$ mapped to another density matrix by the following map: $\rho \to \rho^T$. Here ρ^T is the transpose matrix of our density matrix. This map is a positive map since by definition, $\rho^T = \rho^*$ and as the eigenvalues of ρ are real, conjugating it still preserves the positivity of our original density matrix.

An example of completely positive maps: Given in Peres separability measure section.

Requirement for Bipartite Entanglement measures

There are four conditions that a bipartite entanglement measure must satisfy certain axioms to cover our basic intuition while measuring entanglement.

1. For any separable state or direct product density matrix ρ_{ab} the measure of entanglement should be zero (i.e), $E(\rho_{\mathrm{ab}}) = 0$
2. For any state ρ_{ab} and any local unitary transformation, i.e. a unitary transformation of the form $U_a \otimes U_b$, the entanglement remains unchanged (i.e), $E(\rho) = E\left(U_a \otimes U_b . \rho_{\mathrm{ab}} . U^\dagger{}_a \otimes U^\dagger{}_b\right)$
3. Local operations, classical communication and subparts cannot increase the expected entanglement, i.e. if we start with an ensemble in state ρ and end up with probability p_k in sub-ensembles in state $\rho^{(k)}$ then we will have: $E(\rho) \geq \sum p_k \, E\left(\rho^{(k)}\right)$
4. Given two partition a and b of entangled particles in the total state $\rho = \rho_a \otimes \rho_b$, we have: $E(\rho) \leq E(\rho_a) + E(\rho_b)$

Detection

Peres Separability Criteria

Peres Separability criteria states that entanglement can be detected if the partial transpose operation of our joint density matrices destroys complete positivity. The same statement can be rewritten as a condition on separable state:

A state is separable iff its partial transpose is a completely positive operator.

We already saw an instance where a transpose map on a separate ρ leads to positivity. A Peres test on a separable state can be expressed from Eq.10 as:

$$(T\otimes\mathbb{1})\,\rho = \sum p^{(k)}\,\rho^{T}{}_{a}{}^{(k)}\otimes\rho_{b}{}^{(k)} \tag{13}$$

Since, we have already seen individual positivity is preserved for all density matrices, the complete positivity also holds true for a separable state, thus proving our assertion. This shows that our partial transpose map is a complete positive operator in the domain of all separable density matrices.

We shall now see an example to test this criteria:

Consider a Werner state ρ_α with a fidelity α defined by:

$$\rho_\alpha = \alpha\,|\,\psi^-\rangle\left\langle\psi^-\,\right| + \frac{1-\alpha}{4}\mathbb{1}\otimes\mathbb{1} = \begin{pmatrix} \frac{1-\alpha}{4} & 0 & 0 & 0 \\ 0 & \frac{1+\alpha}{4} & \frac{-\alpha}{2} & 0 \\ 0 & \frac{-\alpha}{2} & \frac{1+\alpha}{4} & 0 \\ 0 & 0 & 0 & \frac{1-\alpha}{4} \end{pmatrix} \tag{14}$$

Taking the partial Transpose, we get:

$$\left(\rho^{T_a}\right)_\alpha = \begin{pmatrix} \frac{1-\alpha}{4} & 0 & 0 & \frac{-\alpha}{2} \\ 0 & \frac{1+\alpha}{4} & 0 & 0 \\ 0 & 0 & \frac{1+\alpha}{4} & 0 \\ \frac{-\alpha}{2} & 0 & 0 & \frac{1-\alpha}{4} \end{pmatrix}$$

In[∘]:=

$$\mathtt{m} = \begin{pmatrix} \frac{1-\alpha}{4} & 0 & 0 & -\frac{\alpha}{2} \\ 0 & \frac{1+\alpha}{4} & 0 & 0 \\ 0 & 0 & \frac{1+\alpha}{4} & 0 \\ -\frac{\alpha}{2} & 0 & 0 & \frac{1-\alpha}{4} \end{pmatrix};$$

```
Eigenvalues[m] // MatrixForm
```

Out[∘]//MatrixForm=

$$\begin{pmatrix} \frac{1}{4}\,(1-3\,\alpha) \\ \frac{1+\alpha}{4} \\ \frac{1+\alpha}{4} \\ \frac{1+\alpha}{4} \end{pmatrix}$$

We see that the eigenvalues of the above Werner states gives us one value $\lambda = \frac{1}{4}(1-3\,\alpha)$ which can become negative if $\alpha > \frac{1}{3}$. Hence, this state cannot be separable and we can "detect" entanglement us the complete positivity of the ρ_α fails.

Entanglement Witness Criteria

Entanglement Witness Criteria states that if we have entanglement existing in our state, there is a way to detect (or witness) it. This witness is expressed by a witness operator 'A' whose expectation value in our density matrix gives the entanglement witness. Mathematically the same statement can be written as:

A state ρ_{ent} is entangled if and only if there exists a Hermitian operator $A \in \mathcal{A}$, called entanglement witness, such that:

$$\langle A\rangle = \mathrm{Tr}(\rho_{\mathrm{ent}}\,A) < 0\;\forall\;\rho_{\mathrm{ent}} \in\; \mathrm{NS}$$

$$\langle A\rangle = \mathrm{Tr}(\rho_{\mathrm{ent}}\,A) \geq 0\;\forall\;\rho_{\mathrm{ent}} \in\; S$$

Here, $\mathcal{A}$ is the set of all witness operators, NS and S are the set of all non-separable (entangled) and separable states respectively.

Examples of Witness theorem on Separable and Non-Separable states:

We have already briefed a necessary and sufficient method (PPT) for finding separability. Other measures of witness (such as Von-Neumann entropy) can guarantee entanglement but not assure separability (not a necessary and sufficient condition for separability). So we consider a SWAP witness for our states defined as:

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Consider the state: $\rho = \; |x\rangle \otimes |y\rangle \langle x| \otimes \langle y|$ which is clearly separable. Applying SWAP and calculating its expectation gives:

$$\langle x| \otimes \langle y| \, \text{SWAP} \, |x\rangle \otimes |y\rangle = \langle x| \otimes \langle y||y\rangle \otimes |x\rangle = \; |\langle x|y\rangle|^2 \; \geq 0$$

Hence, this witness ensures separability criteria foe a separable state.

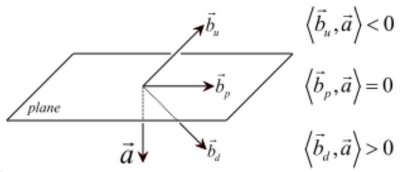
To check if the same witness can now detect entanglement, we define a maximally entangled state $|\psi^-\rangle = \frac{1}{\sqrt{2}} \left| 10 \right\rangle - \left| 01 \right\rangle$. Operating the witness as above, we get:

$$\langle \psi^- | \, \text{SWAP} \, | \psi^- \rangle = \frac{1}{2} (\langle 10| - \langle 01 |) (\vdots - |10\rangle + |01\rangle) = -\langle \psi^- | \psi^- \rangle < 0$$

Hence, we have defined a witness for our entangled state ψ^-. Note that this witness does not work for another entangled state say, ψ^+. EWT simply states the existence of a witness for every entanglement. This witness therefore, need not be unique for a given state.

Geometric Interpretation of Entanglement witness criteria

Since the witness operator introduced the notion of an expectation being less than or greater than equal to zero, we can visualise this operation as an inner product of the two vectors (which they are actually not!) A and ρ. An euclidean visualisation of this abstract inner product is given below. Now, we assume that the set of all separable states are forming a convex set in this space. Now given the convexity and inner product of A and ρ being less than or greater than equal to zero, we can say there exist a hyperplane defined by our witness vector $\bar{A}$ such that it partitions our separable and non-separable sets of states. Thus, if the inner product: $\langle A|\rho\rangle < 0$, it is classified as entangled state. If $\langle A|\rho\rangle \geq 0$, it is classified as a separable state. The existence of this hyperplane comes from the Entanglement witness theorem.


$\vec{b}_u$
$\langle \vec{b}_u, \vec{a} \rangle < 0$
$\vec{b}_p$
$\langle \vec{b}_p, \vec{a} \rangle = 0$
plane
$\vec{a}$
$\vec{b}_d$
$\langle \vec{b}_d, \vec{a} \rangle > 0$

Geometric illustration of a plane in Euclidean space and the different values of the scalar product for states above ($\vec{b}_u$), within ($\vec{b}_p$) and under ($\vec{b}_d$) the plane.

Our witness A_{opt} is termed as "optimal witness" if from our witness operator, there exists a state $\tilde{\rho}$ s.t $\langle A|\tilde{\rho}\rangle = 0$. Figure below illustrates this notion of optimal witness. These witnesses define a tangent to the set of separable states.

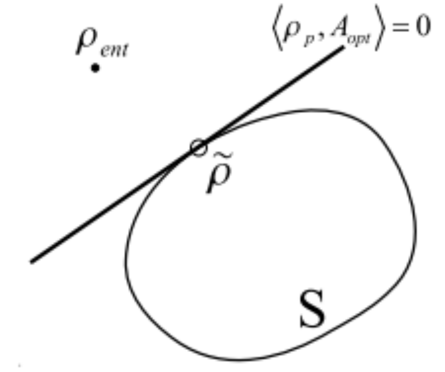


Illustration of an optimal entanglement witness

Negativity

Negativity is a measure of entanglement that is defined as:

$$\mathcal{N}(\rho) = \frac{\| \rho^{T_a} \|_1 - 1}{2}$$

where ρ^{T_a} is the partial transpose of ρ w.r.t Alice (a), $\| X \| = \mathrm{Tr}(X) = \mathrm{Tr}\left(\sqrt{X^\dagger X}\right)$. This tells us that negativity corresponds to the absolute value of the sum of the negative eigenvalues of ρ^{T_a}. Therefore, if λ_i are the eigenvalues of ρ then,

$$\mathcal{N}(\rho) = \sum \frac{| \lambda_i | - \lambda_i}{2} \tag{15}$$

An example of $| \psi^- \rangle$:

$$\rho = | \psi^- \rangle \langle \psi^- | = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Taking ρ^{T_a}, we get:

$$\rho = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

```
In[1]:=
        m = ( 0  0  0 -1
              0  1  0  0
              0  0  1  0
             -1  0  0  0 );

        Eigenvalues[m] // MatrixForm

Out[2]//MatrixForm=
        -1
         1
         1
         1
```

Hence, we use Eq.15 to obtain negativity $\mathcal{N}\left(\rho^{T_a}\right) = 1$. So our state is maximally entangled.

Classification of Entanglement

Distillation of entanglement

Distillation of entanglement states that if we have a density matrix that has an inherent entanglement, then it is possible to filter out a maximally entangled state using only local unitary operations with a certain probability. To show that an entangled 2 qubit state can be distilled, let us consider the state $| \phi \rangle = \alpha \, | 00 \rangle + \beta \, | 11 \rangle$ with $\alpha \neq \beta$. We perform the following local unitary operations on the Alice's qubit to separate our maximally entangled state from our partially entangled state.

1. Alice prepares an ancillary qubit $| \psi \rangle = \alpha \, | 0 \rangle + \beta \, | 1 \rangle$ and adds ot to our entangled state $| \phi \rangle$ between Alice and Bob.
2. Alice hen performs CNOT operation on her two qubits to obtain: $| \phi \rangle_{3\,q} = \alpha^2 \left| 000 \right\rangle + \alpha\beta \left| 011 \right\rangle + \alpha\beta \left| 110 \right\rangle + \beta^2 \left| 101 \right\rangle$
3. Alice then applies SWAP gate on the two qubits at her disposal and obtains: $| \phi \rangle_{3\,q} = | 0 \rangle \otimes \left(\alpha^2 \, | 00 \rangle + \beta^2 \, | 11 \rangle\right) + \sqrt{2\,\alpha^2\,\beta^2} \, \left| 1 \right\rangle \otimes \frac{1}{\sqrt{2}} \left(| 01 \rangle + \left| 10 \right\rangle\right)$
4. Now, on projection operation on the ancilla qubit, she can collapse the state of Bob into a maximally entangled state with a probability $p_{\max} = 2\,\alpha^2\,\beta^2$.

This gives us a distillation of our weakly entangled state into a maximally entangled one. Note that if any of our coefficients are zero, we donot obtain any entanglement thus, agreeing to the principles of LOCC.

To show for ANY entangled state, we extend the same idea and follow what is called the BBPSSW protocol:

1. We apply a local unitary transformation on both Alice and Bob that increases the fidelity fraction F of our original density matrix ρ s.t $F_{\phi^+} > \frac{1}{2}$. $F_{\phi^+}$is defined as: $F_{\phi^+} = \langle \phi^+ \,|\, \rho \,|\, \phi^+ \rangle$. The state after this local unitary operation becomes: $\rho_1 = (U_a \otimes U_b)\, \rho \, (U_a \otimes U_b)^\dagger$
2. Then Alice and Bob pass the information and allow any noise to act on their shared states. This simulates the real life errors being introduced in our qubit states due to transportation from one place to the other. This process preserves F and converts the state $\rho_1 \to \rho_F$.
3. We then apply CNOT gate after introducing identical ancillary qubits to each of them. So after introduction of ancillary, our state becomes: $\rho_F \to \rho_F \otimes \rho_F$. Then our state before collapsing becomes: $\text{CNOT}.\rho_F \otimes \rho_F.\text{CNOT}^\dagger$
4. The final state can be collapsed to a maximally entangled state if our Alice and Bob both simultaneously measure the same target qubit (the original qubit they had before adding the ancilla) they introduced in step.3. We obtain the maximally entangled state in our ancillary qubit with some probability.

Free and Bound entanglement

An entanglement is defined as free if it can be distilled. It is defined as bound if it CANNOT be distilled. An example of a bound entangled state is when an entanglement is not detectable by PPT. We take it as a fact that a PPT state cannot be distilled. Thus, if an entanglement is falling under a PPT criteria, that entangled state is not distillable and it becomes a bound entanglement by definition. The existence of such an entanglement that lies under PPT is possible since PPT is not a necessary and sufficient condition to ensure entanglement. It is only a necessary and sufficient condition for separable states. Some hypothesis also asserts the existence of NPT entangled states being bound. However, no concrete conclusion has been arrived at. Examples of bound qutrits are known, but lies out of the scope of me. So I shan't venture into them.

Acknowledgement

Big thanks to qiskit.org for their online documentation of “Introduction to Quantum Computing and Quantum Hardware” , a Qiskit Global Summer School in July 2020 as a two-week intensive summer school. Their resources made available to the public have helped me understand QFT to a great extent.

References

1. Philipp Krammer. Quantum Entanglement: Detection, Classification, and Quantification. Universitat Wien (2005)
2. Micha l Horodecki, Pawel Horodecki, Ryszard Horodecki*. Separability of mixed states: necessary and sufficient conditions (1996)
3. Martin B. Plenio and Vlatko Vedral*. Teleportation, Entanglement and Thermodynamics in the Quantum World (2008)
4. Peres Separability criterion. http://www.pas.rochester.edu/~howell/mysite2/Tutorials/Peres%20Separability.pdf
5. Peres, A. (1996). Separability criterion for density matrices. Physical Review Letters, 77(8):1413–1415.
6. Plenio, M. B. and Virmani, S. S. (2014). An introduction to entanglement theory. Quantum information and coherence, pages 173–209.