Quantum Computing

Korben Rusek

7-16-2019

1 Global Phase

1.1 Global Phase

Let's begin with a definition of global phase. It is a rather simple concept. We can basically just say that global phase is multiplying a of qubit by a constant of length 1. It is important to distinguish this from multiplication in a controlled fashion. That is, multiplying qubit q_0 by α whenever q_1 is in the $|1\rangle$ state.

In the end we will show that a quantum computer cannot distinguish two qubits that differ by a global phase. That is to say, suppose you have two buckets of qubits. The qubits in the first bucket are all the same and the qubits in the second bucket are all the same. Now someone tells you that all the qubits in the second bucket are either the same as the first or differ by a global phase. There would be no way of knowing which of the two was the case. The implication being that we can safely disregard global phase.

1.2 Measurement

Let's begin by a short discussion of measurement. We begin with two qubits $|a\rangle$ and $|b\rangle$ that form a basis. This means that any qubit $|q\rangle$ can be written as a linear combination $|q\rangle = a_0 |a\rangle + b_0 |b\rangle$, with $|a_0|^2 + |b_0|^2 = 1$. Next we have a measurement M that for which $|a\rangle$ has eigenvalue α and $|b\rangle$ has eigenvalue β. This means that upon measurement of $|q\rangle$ using M, we are given either $(\alpha, |a\rangle)$ or $(\beta, |b\rangle)$ with probabilities $|a_0|^2$ and $|b_0|^2$, respectively. Note that the coefficients on $|a\rangle$ and $|b\rangle$ disappear entirely.

It is worth realizing that the concept of measurement is the *only* way to dig into the inside of a qubit. Furthermore, it is the only way to distinguish between two qubits. This is a fundamental property of quantum physics.

We can make this more precise with a definition.

Definition 1.1 (Measurably Distinct)**.** Let $|q_0\rangle$ and $|q_1\rangle$ be two qubits. Let $|a\rangle$ and $|b\rangle$ be a basis with eigenvalues α and β, respectively. Let M be a measurement that emits $|a\rangle$ and $|b\rangle$. Finally suppose

$$\begin{aligned} |q_0\rangle &= a_0 |a\rangle + b_0 |b\rangle \\ |q_1\rangle &= a_1 |a\rangle + b_1 |b\rangle . \end{aligned}$$

Then $|q_0\rangle$ and $|q_1\rangle$ are *measureably distinct* if $|a_0|^2 \neq |a_1|^2$ or $|b_0|^2 \neq |b_1|^2$.

If we have understood everything thus far, then our task to show that global phase is inconsequential is to show that a global phase change will not affect any measurement. That is, if the only way for a quantum computer to differentiate two qubits is through measurement then we must show that a global phase has no bearing on measurements.

We will start by showing that global phase has no bearing on Z measurement.

Lemma 1.2. Global phase has no bearing on Z measurement.

Proof. This is very easy. Let $q = \alpha |0\rangle + \beta |1\rangle$. Now if you measure q then you get $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$. We will write that as

$$M(q) = \begin{cases} |0\rangle & p = |\alpha|^2 \\ |1\rangle & p = |\beta|^2 \end{cases}$$

Let $\gamma \in \mathbb{C}$ such that $|\gamma|^2 = 1$. That is, γq differs from q by a global phase. This means that $\gamma g = \gamma\alpha |0\rangle + \gamma\beta |1\rangle$. In this case measurement will give

$$M(\gamma q) = \begin{cases} |0\rangle & p = |\gamma\alpha|^2 = |\alpha|^2 \\ |1\rangle & p = |\gamma\beta|^2 = |\beta|^2 \end{cases}$$

That is the two qubits are not measurably distinct when we use a Z measurement. □

Corollary 1.3. Global phase has no bearing on general measurements.

Proof. Based on the proof of the above lemma it is easy to see how this follows. □

Corollary 1.4. Global phase has no bearing on measurements even when other operations are involved.

Proof. Let q be a qubit. Let $\gamma \in \mathbb{C}$ such that $|\gamma|^2 = 1$. We will show that a chain of operators applied to q is not measurably distinct from the same chain of operators applied to γq. Let us start by simplifying the question to a single operator applied to q and γq. We can make this assumption because the product of operators is yet another operator. Let N be any operator. Let $\psi = Nq$ be the qubit that results from applying N to q. Then we have

$$\begin{aligned} N\gamma q &= \gamma N q \\ &= \gamma\psi. \end{aligned}$$

Now by corollary 1.3 we know that ψ and $\gamma\psi$ are not measurably distinct. Hence we have the desired result. □