The No-Cloning Theorem Made Easy

P. Reany

September 14, 2023

Abstract

This paper contains my attempt to present an easy-to-understand version of the proof that an arbitrary qubit cannot be duplicated — the 'No-Cloning Theorem' The proof will be in two forms. The first form uses only the linearity property of a unitary operator. The second form uses the inner product which is defined on state vectors in Hibert space.

1 Preparation before the theorem

Is it possible to clone (make a duplicate of) an arbitrary qubit? A qubit, when measured can be in only one of two possible states, which we'll refer to as $|\,0\,\rangle$ and $|\,1\,\rangle$. In quantum mechanics, an arbitrary qubit $|\,\psi\,\rangle$ is in a superposition of these two states, and we represent that superposition as

$$|\,\psi\,\rangle = \alpha\,|\,0\,\rangle + \beta\,|\,1\,\rangle \ , \tag{1}$$

where α and β are complex numbers, and we can stipulate the normalization equation, too:

$$|\,\alpha\,|^2 + |\,\beta\,|^2 = 1\,. \tag{2}$$

What we are interested in doing is to take an arbitrary qubit and to clone it, without knowing what its 'real' state is. In fact, if we perform a measurement operation on the qubit, all we'll get out is either $|\,0\,\rangle$ and $|\,1\,\rangle$, but we can't determine the coefficients α and β in (1) from that.

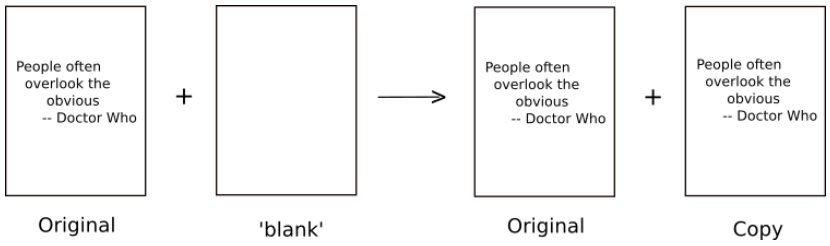

Figure 1. Duplicating (or cloning) a qubit is similar to making a photocopy of a non-blank page (the original). Two pages go in; two pages come out.

In contrast, to duplicate the qubit, we know on general principles that we need to apply a unitary operator to it. Specifically, we want this unitary operator U to do the following on the tensor product of the two particles $|\,\psi\,\rangle_1\,|\,0\,\rangle_2$:[1]

$$U(|\,\psi\,\rangle_1\,|\,0\,\rangle_2) = |\,\psi\,\rangle_1\,|\,\psi\,\rangle_2 = |\,\psi\,\rangle_1 \otimes |\,\psi\,\rangle_2 \ , \tag{3}$$

[1]The tensor product of the two particles is the juxtipostion of their respective wave functions, or we can place the tensor product sign $\otimes$ between them.

where particle 1 is the source qubit and particle 2 is the duplication.[2] Two qubits go in; two qubits come out. (See Fig. 1.) That the second particle is initially in the $|\,0\,\rangle$ state is not relevant, as it could also be in the $|\,1\,\rangle$ state.

Corollaries to (3) are

$$U(|\,0\,\rangle_1\,|\,0\,\rangle_2) = |\,0\,\rangle_1\,|\,0\,\rangle_2\ , \tag{4a}$$
$$U(|\,0\,\rangle_1\,|\,1\,\rangle_2) = |\,0\,\rangle_1\,|\,0\,\rangle_2\ , \tag{4b}$$
$$U(|\,1\,\rangle_1\,|\,0\,\rangle_2) = |\,1\,\rangle_1\,|\,1\,\rangle_2\ , \tag{4c}$$
$$U(|\,1\,\rangle_1\,|\,1\,\rangle_2) = |\,1\,\rangle_1\,|\,1\,\rangle_2\ , \tag{4d}$$

Or, more succinctly, using position from lef to right as particle indicator:

$$U\,|\,00\,\rangle = |\,00\,\rangle\ , \tag{5a}$$
$$U\,|\,01\,\rangle = |\,00\,\rangle\ , \tag{5b}$$
$$U\,|\,10\,\rangle = |\,11\,\rangle\ , \tag{5c}$$
$$U\,|\,11\,\rangle = |\,11\,\rangle\ . \tag{5d}$$

Now, it's necessary to treat the second particle as the donor particle, whether it's in state $|\,0\,\rangle$ or $|\,1\,\rangle$. By the way, either of those states is presumably easy to prepare experimentally.

2 The E operator

There is one more operator we can apply to a tensor product: I call it the "expansion operator" E. (It is similar to the *Expand* operator defined in Mathematica.) This operator takes a tensor product, like $|\,\psi\,\rangle_1\,|\,\psi\,\rangle_2$ and expands it in terms of the standard basis

$$|\,00\,\rangle\ ,\quad |\,01\,\rangle\ ,\quad |\,10\,\rangle\ ,\quad |\,11\,\rangle\ . \tag{6}$$

For example, we can demonstrate this on the two arbitrary, independent qubits $|\,\psi_1\,\rangle$ and $|\,\psi_2\,\rangle$ with definitions

$$|\,\psi_1\,\rangle = a\,|\,0\,\rangle + b\,|\,1\,\rangle\ , \tag{7a}$$
$$|\,\psi_2\,\rangle = c\,|\,0\,\rangle + d\,|\,1\,\rangle\ , \tag{7b}$$

where a, b, c, d are complex numbers. The tensor product $|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle$ has meaning even without a basis, but with a basis, we can employ this (standard) basis to get

$$|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle = \big(a\,|\,0\,\rangle + b\,|\,1\,\rangle\,\big) \otimes \big(c\,|\,0\,\rangle + d\,|\,1\,\rangle\,\big)\,. \tag{8}$$

Now here's where we can apply the E operator:

$$\begin{aligned} E(\,|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle) &= E[\,\big(a\,|\,0\,\rangle + b\,|\,1\,\rangle\,\big) \otimes \big(c\,|\,0\,\rangle + d\,|\,1\,\rangle\,\big)\,] \\ &= ac\,|\,0\,\rangle \otimes |\,0\,\rangle + ad\,|\,0\,\rangle \otimes |\,1\,\rangle + bc\,|\,1\,\rangle \otimes |\,0\,\rangle + bd\,|\,1\,\rangle \otimes |\,1\,\rangle \\ &= ac\,|\,0\,\rangle\,|\,0\,\rangle + ad\,|\,0\,\rangle\,|\,1\,\rangle + bc\,|\,1\,\rangle\,|\,0\,\rangle + bd\,|\,1\,\rangle\,|\,1\,\rangle \\ &= ac\,|\,00\,\rangle + ad\,|\,01\,\rangle + bc\,|\,10\,\rangle + bd\,|\,11\,\rangle\ , \end{aligned} \tag{9}$$

where, instead of using subscripts, we're using the order of the digits from left to right to correspond to particle number. In other words, the only effect of the application of E is to perform an algebraic identity operation. It is neither a measurement (hermitian) operator nor a unitary operator.

[2] Technically, we should write for (3) the more accurate

$$1 \otimes U_2(|\,\psi\,\rangle_1 \otimes |\,0\,\rangle_2) = |\,\psi\,\rangle_1 \otimes U_2\,|\,0\,\rangle_2 = |\,\psi\,\rangle_1 \otimes |\,\psi\,\rangle_2\ .$$

3 The $EU = UE$ Lemma

Let U be an arbitrary unitary (hence linear) operator, it seems intuitive to suppose that U should commute with this E operator. Hence, we conjecture that

$$EU = UE\,. \tag{10}$$

To prove this conjecture, We have to show that

$$EU(|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle) = UE(|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle)\,. \tag{11}$$

On applying U to (9), we get

$$UE(|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle) = acU\,|\,00\,\rangle + adU\,|\,01\,\rangle + bcU\,|\,10\,\rangle + bdU\,|\,11\,\rangle\ , \tag{12}$$

where we have used the linearity of $U = U_1 \otimes U_2$. As for the LHS of (11),

$$\begin{aligned} U(|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle) &= U_1 \otimes U_2(|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle) \\ &= U_1\,|\,\psi_1\,\rangle \otimes U_2\,|\,\psi_2\,\rangle \\ &= U_1(a\,|\,0\,\rangle + b\,|\,1\,\rangle) \otimes U_2(c\,|\,0\,\rangle + d\,|\,1\,\rangle) \\ &= \big(aU_1\,|\,0\,\rangle + bU_1\,|\,1\,\rangle\,\big) \otimes \big(cU_2\,|\,0\,\rangle + dU_2\,|\,1\,\rangle\,\big)\,. \end{aligned} \tag{13}$$

On applying E to both sides of this, we have that

$$\begin{aligned} EU(|\,\psi_1\,\rangle\,|\,\psi_2\,\rangle) &= E[\,\big(aU_1\,|\,0\,\rangle + bU_1\,|\,1\,\rangle\,\big) \otimes \big(cU_2\,|\,0\,\rangle + dU_2\,|\,1\,\rangle\,\big)\,] \\ &= acU_1\,|\,0\,\rangle \otimes U_2\,|\,0\,\rangle + adU_1\,|\,0\,\rangle \otimes U_2\,|\,1\,\rangle) \\ &\quad + bcU_1\,|\,1\,\rangle \otimes U_2\,|\,0\,\rangle + bdU_1\,|\,1\,\rangle \otimes U_2\,|\,1\,\rangle \\ &= acU\,|\,00\,\rangle + adU\,|\,01\,\rangle + bcU\,|\,10\,\rangle + bdU\,|\,11\,\rangle\ . \end{aligned} \tag{14}$$

From the equality of results in (12) and (14), we have shown that (10) is true.

4 The No-Cloning Theorem Proof #1

The No-Cloning Theorem (a proof by contradiction): The central idea of the proof to the No-Cloning Theorem is that we assume that some unitary operator U exists that performs the role of qubit duplication. That is,

$$U(\,|\,\psi\,\rangle\,|\,0\,\rangle) = |\,\psi\,\rangle\,|\,\psi\,\rangle\ . \tag{15}$$

But, when we try to conform this U to both (15) and (10), we get a contradiction, proving that no such U can exist. More specifically, we get that

$$EU(|\,\psi\,\rangle\,(|\,0\,\rangle) \neq UE(|\,\psi\,\rangle\,(|\,0\,\rangle)\,. \tag{16}$$

On hitting both sides of (15) by E, we get

$$\begin{aligned} EU(\,|\,\psi\,\rangle\,|\,0\,\rangle) &= E[\,|\,\psi\,\rangle\,|\,\psi\,\rangle\,] \\ &= E[\,\big(\alpha\,|\,0\,\rangle + \beta\,|\,1\,\rangle\,\big) \otimes \big(\alpha\,|\,0\,\rangle + \beta\,|\,1\,\rangle\,\big)\,] \\ &= \alpha^2\,|\,00\,\rangle + \alpha\beta\,|\,01\,\rangle + \beta\alpha\,|\,10\,\rangle + \beta^2\,|\,11\,\rangle\ . \end{aligned} \tag{17}$$

Now, since E is merely an algebraic identity operation, then

$$\begin{aligned} U(\,|\,\psi\,\rangle\,|\,0\,\rangle) &= UE(|\,\psi\,\rangle\,|\,0\,\rangle) \\ &= UE[\,\big(\alpha\,|\,0\,\rangle + \beta\,|\,1\,\rangle\,\big) \otimes |\,0\,\rangle\,] \\ &= U[\,\alpha\,|\,00\,\rangle + \beta\,|\,10\,\rangle\,] \\ &= \alpha\,|\,00\,\rangle + \beta\,|\,11\,\rangle\ . \end{aligned} \tag{18}$$

So, to make (17) jive with (18), we need the following contraints:

$$\alpha^2 = \alpha\,, \quad \alpha\beta = \beta\alpha = 0\,, \quad \beta^2 = \beta\,. \tag{19}$$

But to satisfy these severely restrictive constraints, we need either

$$\alpha = 1 \text{ and } \beta = 0 \quad \text{or} \quad \alpha = 0 \text{ and } \beta = 1\,, \tag{20}$$

in which case ψ cannot exist as a nontrivial superposition of $|\,0\,\rangle$ and $|\,1\,\rangle$, much less as an arbitrary one. Thus, we have proven that there is no unitary operator that can clone an arbitrary qubit.

5 Afterthought for Proof #1

The essense of our use of the $EU = UE$ Lemma was to show that any 'real' unitary operator that claims to be able to clone an arbitrary qubit is intending on cheating, for it certainly can't do it by following the rules that define it.

If we follows the arrows from the top left to the bottom right of Fig. 2, we will find that the end result is not the same for the two paths. Thus the diagram does not 'commute', as one says in formal mathematics. Although we made sure that our U conformed to linearity, we could not keep it from running afoul of the $EU = UE$ Lemma.

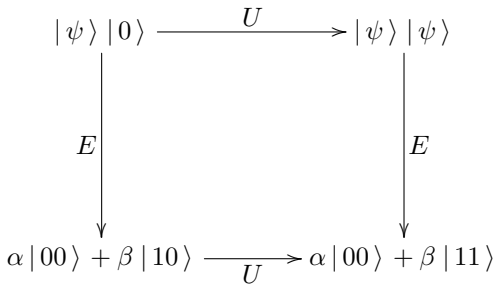

Figure 2. Here we attempt to fit the duplication rule $U(\,|\,\psi\,\rangle\,|\,0\,\rangle\,) = |\,\psi\,\rangle\,|\,\psi\,\rangle$ into a commutative diagram to see if it conforms to the $EU = UE$ Lemma. Turns out, it doesn't, because the order that we apply E and U makes a difference, but it's not supposed to.

6 The No-Cloning Theorem Proof #2

Let $|\,\psi_1\,\rangle$ and $|\,\psi_2\,\rangle$ be any two arbitrary qubits. Again, we'll approach the proof by contradiction: We will assume that it is possible to clone an arbitrary qubit along with a 'blank' qubic as we indicated before:

$$U(\,|\,\psi\,\rangle\,|\,0\,\rangle\,) = |\,\psi\,\rangle\,|\,\psi\,\rangle\ . \tag{21}$$

So, assuming the above equation is true, it must be true for special cases $|\,\psi_1\,\rangle$ and $|\,\psi_1\,\rangle$:

$$U(\,|\,\psi_1\,\rangle\,|\,0\,\rangle\,) = |\,\psi_1\,\rangle\,|\,\psi_1\,\rangle\ , \tag{22}$$

$$U(\,|\,\psi_2\,\rangle\,|\,0\,\rangle\,) = |\,\psi_2\,\rangle\,|\,\psi_2\,\rangle\ . \tag{23}$$

We now need three rules: First, that $U^\dagger U = 1$;[3] second, that $\langle\,0\,|\,0\,\rangle = 1$ (for normalization); and third, that for arbitrary states A, B, C, D (the tensor-product rule):

$$\langle\,A \otimes B\,|\,C \otimes D\,\rangle = \langle\,A\,|\,C\,\rangle\,\langle\,B\,|\,D\,\rangle\ . \tag{24}$$

[3]This is standard for the definition of a unitary operator.

Thus, (note: VE stands for 'virtual emplacement')[4]

$$\begin{aligned}
\langle\, \psi_1 \mid \psi_2 \,\rangle &\overset{\text{VE}}{=} \langle\, \psi_1 \mid \psi_2 \,\rangle \langle\, 0 \mid 0 \,\rangle \\
&= \langle\, \psi_1 \otimes 0 \mid \psi_2 \otimes 0 \,\rangle \qquad \text{(see Eq. (24))} \\
&= \big\langle\, \psi_1 \otimes 0 \mid U^\dagger U \,\big|\, \psi_2 \otimes 0 \,\big\rangle \\
&= \langle\, U(\psi_1 \otimes 0) \mid U(\psi_2 \otimes 0) \,\rangle \\
&= \langle\, \psi_1 \otimes \psi_1 \mid \psi_2 \otimes \psi_2 \,\rangle \\
&= \langle\, \psi_1 \mid \psi_2 \,\rangle \langle\, \psi_1 \mid \psi_2 \,\rangle \\
&= \langle\, \psi_1 \mid \psi_2 \,\rangle^2 \,. \qquad (25)
\end{aligned}$$

This last equation has very simple solutions for the inner product $\langle\, \psi_1 \mid \psi_2 \,\rangle$; it's either 0 or 1. In the former case, we demand that ψ_1 and ψ_2 be orthogonal to each other in the quantum mechanical sense, but that means that they're not arbitrary. In the latter case, they must be 1) equal to each other, or 2) if

$$\begin{aligned}
\langle\, \psi_1 \mid \psi_2 \,\rangle &= \big\langle\, a \,|\, 0 \,\rangle + b \,|\, 1 \,\rangle \,\big|\, c \,|\, 0 \,\rangle + d \,|\, 1 \,\rangle \,\big\rangle \\
&= \big(a^* \langle\, 0 \,| + b^* \langle\, 1 \,|\,\big)\big(c \,|\, 0 \,\rangle + d \,|\, 1 \,\rangle\,\big) \\
&= a^* c + b^* d \\
&= 1 \,, \qquad (26)
\end{aligned}$$

which means that the four coefficients used to define these two states are constrained (even more than by normalization), and hence they're not arbitrary state vectors, which is a contradiction.

7 Afterthought for Proof #2

I showed ChatGPT 3.5 my version of the 'inner-product proof' of the No-Cloning Theorem and it responded that it looked good for an inner-product proof, but that the usual proof (I assume it meant the first proof of this article) is more 'rigorous'. Really? That's interesting.

8 Conclusion

These two proofs are all I could find in the literature. They **both** seem rigorous to me, anyway. So, what do we even mean by 'rigorous'. Nontechnically, a rigorous proof must be without error and must be just enough to get the job done. Well, both proofs (if accurate) get the job done. Each proof exploits some aspect of unitary operators that the other proof does not. I find that interesting.

My last observation about these proofs is that, taken together, they provide a playground to learn how to use qubits, tensor products, inner products, and unitary operators. As I see it, the first proof relies heavily on the linearity of U, whereas the second proof does not. Instead, it relies crucially on the rule $U^\dagger U = 1$ and on the properties of inner products on states of a Hilbert space.

[4] A virtual emplacement is nothing more than multiplication of an expression by unity or adding zero to an expression. In both cases, the new expression is equal in value to the old.