No cloning theorem -met brakets

Het is niet mogelijk om een qubit te kopiëeren, dit is fysisch verboden. In de natuurkunde wordt dit ook wel het 'no cloning theorem' genoemd. Het is best onhandig dat we niet zomaar qubits kunnen kopiëeren, want dat betekent dat we niet zo makkelijk qubit toestanden kunnen namaken, iets wat we wel graag zouden willen om bijvoorbeeld fouten in een quantum berekening op te sporen (als je drie keer precies dezelfde berekening doet, heb je meer kans dat je op het goede antwoord uitkomt). Er bestaat een heel kort bewijs voor de no cloning theorem dat we hier zullen bespreken.

Stel, je hebt een qubit operatie die een qubit kan kopiëeren, bijvoorbeeld de operatie U kan de toestand $|0\rangle$ in een arbitraire toestand $|\psi\rangle$ veranderen, dus:

$$U\,|0\rangle\,|\psi\rangle = |\psi\rangle\,|\psi\rangle$$

Maar dan zou U ook iedere andere qubit toestand moeten kunnen kopiëeren, zoals de toestand $|\phi\rangle$:

$$U\,|0\rangle\,|\phi\rangle = |\phi\rangle\,|\phi\rangle$$

Omdat U een quantumoperatie moet zijn, is U unitair. Als we beide kopieerpogingen met elkaar vermenigvuldigen, krijgen we het volgende:

$$\langle\psi|\,\langle 0|\,U^*U\,|0\rangle\,|\phi\rangle = \langle\psi|\,\langle\psi|\phi\rangle\,|\phi\rangle$$

We weten dat een in product van een object met zichzelf 1 is, dus $\langle 0|0\rangle = 1$ en $U^*U = 1$, dus we krijgen:

$$|\,\langle\psi|\phi\rangle\,| = |\,\langle\psi|\phi\rangle\,\langle\psi|\phi\rangle\,| = |\,\langle\psi|\phi\rangle\,|^2$$

Deze formule klopt alleen als $|\,\langle\psi|\phi\rangle\,| = 1$ of als $|\,\langle\psi|\phi\rangle\,| = 0$, dus als ofwel $\phi = \psi$, ofwel ϕ staat loodrecht op ψ. Maar we hadden ϕ en ψ als twee random toestanden gekozen. Een operatie U kan dus geen *algemene* quantumtoestand kopiëren.

No cloning staat in de bolletjes bij H2, lineariteit wordt pas in H3 behandeld. opl: noem in H2, verwijs naar H3, daar ook het bewijs (ruim een pagina

No cloning theorem too

Het is niet mogelijk een qubit te kopiëren. Dit staat bekend als het 'no-cloning theorema'. We geven een bewijs uit het ongerijmde. In zo'n bewijs probeer je eerst aan te tonen dat de stelling geldt, daarna laat je zien dat dat een foute aanname is, waarna je moet concluderen dat de stelling ongeldig is.

Om te kopiëren hebben we een mal nodig. We nemen daarvoor de basistoestanen $|0\rangle$ en $|1\rangle$. Met de regels van lineariteit kunnen we dan ook een willekeurige toestand $|\Psi\rangle$ uitrekenen. Je moet ook iets in de mal 'gieten'. Dat kan een basistoestand zijn. We nemen daarvoor $|0\rangle$.

We zetten de twee qubits in één ket. De **U**-poort kopieert het linker qubit.

$$\mathbf{U}\,|00\rangle = |00\rangle \quad \text{en} \quad \mathbf{U}\,|10\rangle = |11\rangle$$

Vraag A: Stel de operatie op die toestand $|\Psi\rangle$ kopieert.

$U\,|0\psi\rangle = |\psi\psi\rangle$

De twee operaties mogen we samenvoegen (in superpositie brengen). We passen daarbij de regels van lineariteit toe (ref):

$$\mathbf{U}(\tfrac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = \tfrac{1}{\sqrt{2}}(\mathbf{U}\,|00\rangle + \mathbf{U}\,|10\rangle) = \tfrac{1}{\sqrt{2}}((|00\rangle + |11\rangle)$$

Je moet tot hetzelfde resultaat komen als je $|0\rangle$ in de begintoestand buiten haakjes haalt:

$$\mathbf{U}\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right) = \mathbf{U}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\,|0\rangle\right) =$$
$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$
$$\neq \frac{1}{\sqrt{2}}((|00\rangle + |11\rangle)$$

Vraag B: Geef het no-cloning bewijs met $|1\rangle$ als mal.

Vraag C: Waarom geldt het no-cloning theorema voor een willekeurige toetstand $|\Psi\rangle$?

No cloning theorem ronald

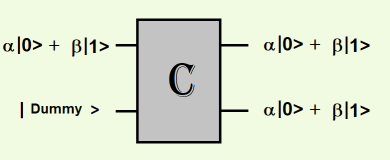
Stel dat je een unitaire 2-qubit operatie U hebt die een qubit kan clonen (dwz een kopie van het eerste qubit kan maken in het tweede qubit, dat begint in toestand |0>). Omdat U in ieder geval de 2 basistoestanden |0> en |1> moet kunnen clonen, heb je: U|0> |0> =|0> |0> U|1> |0> =|1> |1>

Stel nu dat je probeert een qubit in toestand |+> =1/sqrt2(|0> +|1>) te clonen. We hebben:

U|+> |0> =1/sqrt2(U|0> |0> +U|1> |0>)=1/sqrt2(|0> |0> +|1> |1>), wegens lineariteit. Die laatste toestand is een EPR-paar, dus entangled, dus kan niet gelijk zijn aan de toestand |+> |+> die de cloner had moeten maken. De aanname dat zo'n U bestaat leidt dus tot een tegenspraak, QED.

No cloning theorem Guido

Waarom is cloning bij qubits niet mogelijk? Het antwoord heeft te maken met het feit dat een quantum-operator reversibel moet zijn. Bekijk onderstaande afbeelding.



Figuur 1.1: schema waarmee je een biqubit zou kunnen clonen

.

Deze oplossing past overal, simpelheid zelve

Cloning houdt in dat de toestand van een qubit wordt gedupliceerd. Een tweede qubit moet dus de toestand van de te clonen qubit overnemen. De werking van een poort is bekend als de werking bekend is op de basistoestanden. Er zijn vier verschillende combinaties van de input mogelijk. In de tabel hieronder is weergegeven wat de output is bij deze vier combinaties.

in	*out*
00	00
01	00
10	11
11	11

Figuur 1.2: Aan de tabel is te zien dat de werking van de poort niet ongedaan kan worden gemaakt. Er gaat door de werking van de poort informatie verloren. De poort is niet reversibel. Een qunatumpoort die een qubit cloont bestaat dus niet.