Quantum Computing 101, Part 3 – The art of quantum entanglement

Aaron Turner, April 2021

Introduction

This is the third part of a blog series on **quantum computing**, broadly derived from CERN's Practical introduction to quantum computing video series, Michael Nielson's Quantum computing for the very curious / determined, and the following (widely regarded as definitive) references:

- [Hidary] *Quantum Computing: An Applied Approach*
- [Nielsen & Chuang] *Quantum Computing and Quantum Information* [a.k.a. "Mike & Ike"]
- [Yanofsky & Mannucci] *Quantum Computing for Computer Scientists*

My objective is to keep the mathematics to an absolute minimum (albeit not quite zero), in order to engender an **intuitive understanding**. You can think it as a quantum computing cheat sheet.

Quantum computer performance and reliability

As has already been alluded, real quantum computers are not perfect. Each actual machine is therefore associated with a number of **metrics** pertaining to its performance and reliability:

- T1 is the average time (in μs) for state $|1\rangle$ to decohere to state $|0\rangle$
- T2 is the average time (in μs) that a qubit will remain in superposition

Further metrics are usually provided on a qubit-by-qubit basis, for example:

- T1 and T2 for that specific qubit
- the frequency at which the qubit operates
    - note that this is typically ~1000 times faster than the corresponding T1 and T2
    - this means that it is “safe” to run a quantum algorithm for a few 100 operations
- the error rates for each of the basic gates
    - note that the error rate for CNOT is typically ~10 times higher than other gates
    - thus CNOT reliability is a critical test of any physical implementation method

Finally, a **coupling map** is often provided, indicating which qubits can be used with CNOT.

Because of these low-level reliability issues, quantum computers with large numbers of qubits quickly become unusable without **quantum error correction** (which we will meet in Part TBD).

The EPR paradox and Bell’s Inequality

The idea of quantum entanglement implies that one could, in principle:

1. create two physically local, entangled qubits (e.g. a Bell pair)
2. separate them by a great distance (e.g. across the galaxy)
3. measure one qubit, causing the entire entangled system (i.e. both qubits) to collapse
4. immediately measure the other qubit, yielding a result which will be correlated with the first

which implies that **quantum information** (specifically, the result obtained when the first qubit was measured) has somehow travelled between the two qubits at **faster than the speed of light**.

Einstein called this “spooky action at a distance”. In 1935 (at which point the idea of entanglement had been posited but not yet experimentally confirmed), Einstein, Podolsky, and Rosen (EPR) published *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?*, in which they argued that quantum behaviour might be better explained by **hidden variables**:

1. when the would-be entanglement (e.g. a quantum entangled pair) is created, **additional information** is encoded, in **hidden variables**, internally to the particles in question
2. when the particles are separated, this hidden information travels internally with them
3. when the quantum state of either particle is measured (in any order), the observable result yielded by the measurement is **pre-determined** by the internal hidden information
4. thus the two measured states are correlated, but without faster-than-light communication.

In 1964, John Bell, a theoretical physicist working at CERN, published *On the Einstein Podolsky Rosen Paradox*, in which he proved that classical hidden variables as proposed by EPR would produce **statistically weaker correlations** than those predicted by quantum mechanics. Subsequent experiments (e.g. Aspect et al 1981-82, Hensen et al 2015) have confirmed the existence of these stronger correlations. Thus, **the universe is truly quantum, not classical**.

The CHSH game

In 1969, Clauser, Horne, Shimony, and Holt (CHSH) formulated the following game:

1. initially, Alice and Bob are physically local to each other, and thus able to communicate
2. before the game begins, however, they are separated by a great distance
3. in each round of the game:
    a. Alice receives bit **x**, chosen uniformly randomly by the referee
    b. Bob receives bit **y**, also chosen uniformly randomly by the referee
    c. Alice responds (to the referee) with bit **a**, Bob responds with bit **b**
    d. Alice and Bob "win" if and only if $\mathbf{a} \oplus \mathbf{b} = \mathbf{x} \times \mathbf{y}$ (where $\oplus$ denotes XOR)

Thus the outcome of each round of the game is determined as follows:

x	y	a	b	x * y	a XOR b	win?
0	0	0	0	0	0	1
0	0	0	1	0	1	0
0	0	1	0	0	1	0
0	0	1	1	0	0	1
0	1	0	0	0	0	1
0	1	0	1	0	1	0
0	1	1	0	0	1	0
0	1	1	1	0	0	1
1	0	0	0	0	0	1
1	0	0	1	0	1	0
1	0	1	0	0	1	0
1	0	1	1	0	0	1
1	1	0	0	1	0	0
1	1	0	1	1	1	1
1	1	1	0	1	1	1
1	1	1	1	1	0	0

Before the game, while Alice and Bob can still communicate, they are able to agree on a strategy to use during the game. For example, always responding with 0 or 1, always responding with the exact same bit received from the referee, or with the opposite bit, or with some combination. The probability of winning (over many rounds) may then be calculated for each possible strategy, e.g.:

	Alice responds 0	Alice responds 1	Alice responds x	Alice responds ¬x
Bob responds 0	0.75	0.25	0.75	0.25
Bob responds 1	0.25	0.75	0.25	0.75
Bob responds y	0.75	0.25	0.25	0.75
Bob responds ¬y	0.25	0.75	0.75	0.25

As the above table shows, if Alice and Bob agree to both always respond with 0, they will win 75% of the time. It can be shown that **no classical strategy** can win more than 75% of the time.

We now modify the game in order to allow Alice and Bob to employ a **quantum** strategy.

Before the game (which will have have R rounds) starts, we create R entangled qubit pairs, and we give Alice and Bob one half of each pair, which they take with them when they are separated.

During the game, at each round r, Alice and Bob use the following pre-agreed strategy:

1. if Alice receives a 0 from the referee (x = 0), she applies rotation $R_y(0)$ to entangled qubit-pair[r][0], measures it, and returns the result of the measurement to the referee

2. if Alice receives a 1 from the referee (x = 1), she applies rotation $R_y\left(\frac{\pi}{2}\right)$ to entangled qubit-pair[r][0], measures it, and returns the result of the measurement to the referee

3. if Bob receives a 0 from the referee (y = 0), he applies rotation $R_y\left(\frac{\pi}{4}\right)$ to entangled qubit-pair[r][1], measures it, and returns the result of the measurement to the referee

4. if Bob receives a 1 from the referee (y = 1), he applies rotation $R_y\left(-\frac{\pi}{4}\right)$ to entangled qubit-pair[r][1], measures it, and returns the result of the measurement to the referee.

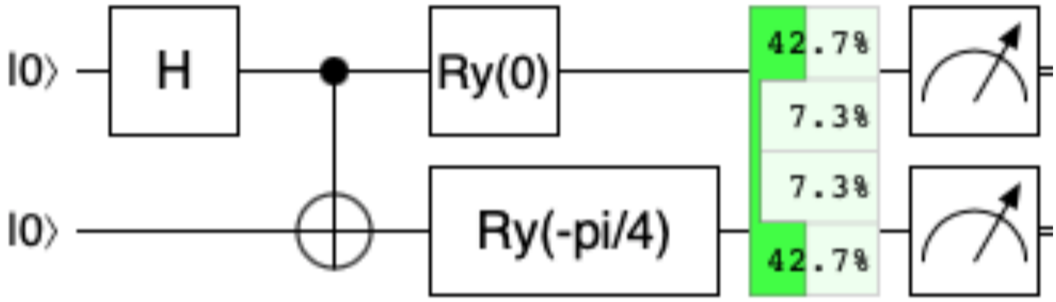
With this new **quantum** strategy, the probability of winning is now $cos^2\left(\frac{\pi}{8}\right) \approx 0.85 > 0.75$.

The easiest way to confirm this overall result is to use e.g. the Quirk simulator for each xy case:

If x = 0 and y = 0, the winning responses are ab = 00 and ab = 11:

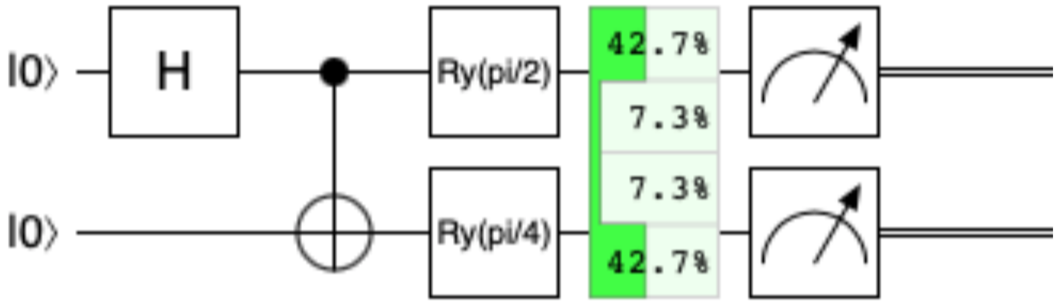
The Hadamard and CNOT gates produce entangled qubit-pair[r]. Because x=0, Alice feeds qubit-pair[r][0] (on the top line) through $R_y(0)$, and, because y=0, Bob feeds qubit-pair[r][1] (on the bottom line) through $R_y\left(\frac{\pi}{4}\right)$. Consequently, when either half of entangled qubit-pair[r] is measured it will collapse to $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ with probabilities 0.427, 0.073, 0.073, and 0.427 respectively, yielding ab = 00 with probability 0.427 and ab = 11 with probability 0.427. Thus, the probability of a win when xy = 00 will be 0.427 + 0.427 $\approx 0.85 \approx cos^2\left(\frac{\pi}{8}\right) > 0.75$.

If x = 0 and y = 1, the winning responses are ab = 00 and ab = 11:



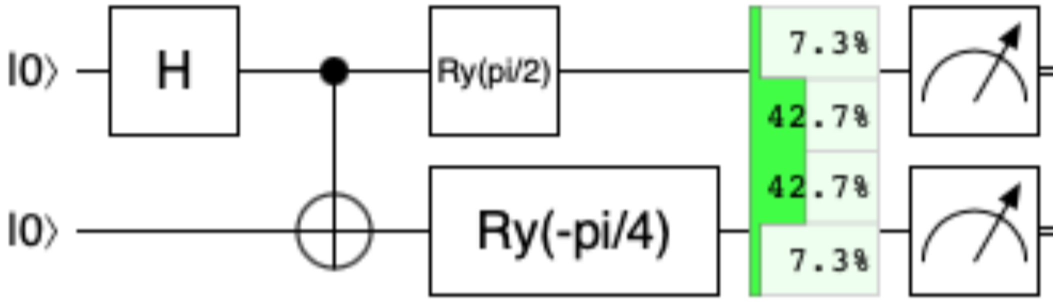
The Hadamard and CNOT gates produce entangled qubit-pair[r]. Because x=0, Alice feeds qubit-pair[r][0] (on the top line) through $R_y(0)$, and, because y=1, Bob feeds qubit-pair[r][1] (on the bottom line) through $R_y\left(-\frac{\pi}{4}\right)$. Consequently, when either half of entangled qubit-pair[r] is measured it will collapse to $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ with probabilities 0.427, 0.073, 0.073, and 0.427 respectively, yielding ab = 00 with probability 0.427 and ab = 11 with probability 0.427. Thus, the probability of a win when xy = 01 will be 0.427 + 0.427 $\approx 0.85 \approx cos^2\left(\frac{\pi}{8}\right) > 0.75$.

If x = 1 and y = 0, the winning responses are ab = 00 and ab = 11:



The Hadamard and CNOT gates produce entangled qubit-pair[r]. Because x=1, Alice feeds qubit-pair[r][0] (on the top line) through $R_y\left(\frac{\pi}{2}\right)$, and, because y=0, Bob feeds qubit-pair[r][1] (on the bottom line) through $R_y\left(\frac{\pi}{4}\right)$. Consequently, when either half of entangled qubit-pair[r] is measured it will collapse to $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ with probabilities 0.427, 0.073, 0.073, and 0.427 respectively, yielding ab = 00 with probability 0.427 and ab = 11 with probability 0.427. Thus, the probability of a win when xy = 10 will be 0.427 + 0.427 $\approx 0.85 \approx cos^2\left(\frac{\pi}{8}\right) > 0.75$.

If x = 1 and y = 1, the winning responses are ab = 01 and ab = 10:



The Hadamard and CNOT gates produce entangled qubit-pair[r]. Because x=1, Alice feeds qubit-pair[r][0] (on the top line) through $R_y\left(\frac{\pi}{2}\right)$, and, because y=1, Bob feeds qubit-pair[r][1] (on the bottom line) through $R_y\left(-\frac{\pi}{4}\right)$. Consequently, when either half of entangled qubit-pair[r] is measured it will collapse to $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$ with probabilities 0.073, 0.427, 0.427, and 0.073 respectively, yielding ab = 01 with probability 0.427 and ab = 10 with probability 0.427. Thus, the probability of a win when xy = 11 will be 0.427 + 0.427 $\approx 0.85 \approx cos^2\left(\frac{\pi}{8}\right) > 0.75$.

The overall probability of winning (over many rounds) is therefore $\approx 0.85 \approx cos^2\left(\frac{\pi}{8}\right) > 0.75$.

A similar game known as GHZ (due to Greenberger, Horne, and Zeilinger), using three players, again results in a win 75% of the time when the players are restricted to classical methods, but increases to a win 100% of the time when the players are allowed to share entangled qubits.

Protocols such as CHSH and GHZ have real-world applications, such as certifying randomness.

Quantum teleportation

If, as in the CHSH game, Alice and Bob share an entangled qubit-pair AB then Alice is able to communicate a **1-qubit** message M to Bob over a **2-bit classical** communication channel:

*** TODO

Gate teleportation

Similarly to quantum teleportation as above, if Alice and Bob share an entangled qubit-pair AB then Alice is able to communicate to Bob the result of applying unitary operation U to qubit M:

*** TODO

Superdense coding

If Alice and Bob share an entangled qubit-pair AB then Alice is able to communicate **two classical bits** c0 and c1 to Bob (effectively the inverse of quantum teleportation), as follows:

*** TODO

Entanglement swapping

If Alice and Bob share an entangled qubit-pair AB, and Alice and Charlie share an entangled qubit-pair AC, then it is possible to establish an entangled qubit-pair between Bob and Charlie:

*** TODO

