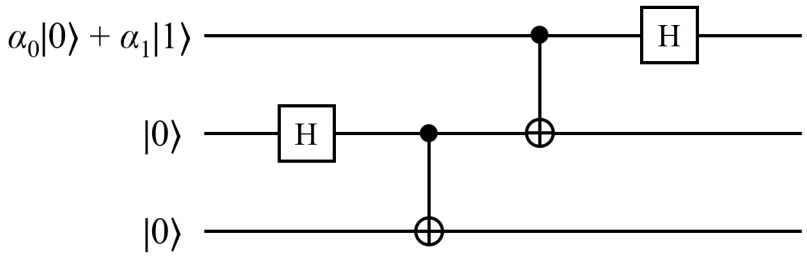
Week 4 work: Sept. 27 — Oct. 4
9-hour week
Obligatory problems are marked with [**]

---

1. **[Quantum circuit practice.]** Consider the following quantum circuit operating on 3 qubits:



(a) [**] Determine with proof the state of the three qubits at the end of the circuit's operation.

(b) [**] Suppose the top two qubits are measured. Determine the probabilities of the possible outcomes, and what state the third qubit collapses to in each of the four cases.

2. [**Fun with gates.**] The following questions concern 2-qubit circuits. We desginate the 2 qubits "A" and "B".

   (a) Suppose that (for some physical reason) you *are* able to build a device that effects the CNOT operation with the A qubit as the 'control' and the B qubit as the 'target'; yet, you *aren't* able to build a device that does the CNOT the other way around. Show how to nevertheless implement a CNOT with the A qubit as the 'target' and the B qubit as the 'control', assuming you can also build and use Hadamard gates.

   (b) Suppose you now can build CNOT gates that work in both of the two ways. Using only CNOT gates, show how to build a SWAP gate.

3. **[Implausible consequences of superstrong nonlocality.]** The usual terminology for the CHSH game is as follows:

   - Alice's referee's challenge is called x and is either 1 (Red) or 0 (Yellow);
   - Bob's referee's challenge is called y and is either 1 (Green) or 0 (Orange);
   - Alice's response is called $a \in \{0,1\}$ (rather than Solid/Dotted);
   - Bob's response is called $b \in \{0,1\}$ (rather than Solid/Dotted);
   - the "success condition" is $a + b = x \cdot y \pmod 2$.

   Now suppose that Alice and Bob could build magic "non-local boxes" that would allow them to succeed at the CHSH game with 100% probability.[1] That is, even though Alice and Bob are spatially distant: Alice can put a bit $x \in \{0,1\}$ into the box and get back a bit $a \in \{0,1\}$; Bob can put a bit $y \in \{0,1\}$ into the box and get back a bit $b \in \{0,1\}$; and, these bits will always satisfy $a + b = x \cdot y \pmod 2$.

   (a) Assume that Alice and Bob are spatially distant, but they have access to n of these magic "non-local boxes". Assume also that Alice knows N bits $x_1, \ldots, x_N \in \{0,1\}$, Bob knows N bits $y_1, \ldots, y_N \in \{0,1\}$, and they have a desire to compute the "inner product mod 2" function of their bits,

   $$\mathrm{IP}_2(x_1, \ldots, x_N, y_1, \ldots, y_N) = x_1 \cdot y_1 + \cdots + x_N \cdot y_N \pmod 2.$$

   Show that by using the non-local boxes, and then allowing *one* classical bit of communication from Alice to Bob, they can jointly learn the value $\mathrm{IP}_2(x_1, \ldots, x_N, y_1, \ldots, y_N)$.

   (b) Recall that every Boolean function $f : \{0,1\}^m \to \{0,1\}$ can be computed by a Boolean circuit using fan-in-2 AND gates and fan-in-1 NOT gates. (Normally fan-in-2 OR gates are also allowed, but these are technically superfluous, since $g \vee h = \neg(\neg g \wedge \neg h)$.) Show that every Boolean function $f : \{0,1\}^m \to \{0,1\}$ can also be computed by a polynomial modulo 2.

   (c) Suppose that we have a Boolean function on $2n$ inputs, $f : \{0,1\}^{2n} \to \{0,1\}$, where use the notation x_i for the first n input variables and the notation y_i for the second n. Prove that it is possible to express f as

   $$f(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{j=1}^{N} A_j(x) \cdot B_j(y) \pmod 2,$$

   where $A_1(x), \ldots, A_N(x)$ are each products of zero or more x_i's, and similarly $B_1(y), \ldots, B_N(y)$ are each products of zero or more y_i's. (The product of zero terms is considered to be 1.) For example, if $n = 2$ and f is the function EQ indicating equality of the two 2-bit strings formed by x and y, it holds that

   $$\mathrm{EQ}(x_1, x_2, y_1, y_2) = 1 \cdot 1 + x_1 \cdot 1 + x_2 \cdot 1 + 1 \cdot y_1 + 1 \cdot y_2 + x_1 x_2 \cdot 1 + x_1 \cdot y_2 + x_2 \cdot y_1 + 1 \cdot y_1 y_2$$

   modulo 2.

[1] Recall that these generate "no-signaling" joint distributions, and therefore do not yield any ability to do faster-than-light communication.

(d) Return to the scenario from part (a), but instead that Alice knows n bits $x_1, \ldots, x_n \in \{0,1\}$, Bob knows n bits $y_1, \ldots, y_n \in \{0,1\}$, and they have a desire to compute a certain Boolean function $f : \{0,1\}^{2n} \to \{0,1\}$ applied to their two inputs,

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n).$$

(They both know the function f.) Show that by using as many non-local boxes as they want, and then allowing *one* classical bit of communication from Alice to Bob, they can jointly learn the value $f(x_1, \ldots, x_N, y_1, \ldots, y_N)$.

Remark: It seems very implausible that Alice and Bob should be able to remotely compute any joint function of arbitrarily long private input strings while only communicating one classical bit. This can be taken as evidence of the physical impossibility of succeeding at the CHSH game with 100% probability. In fact, Brassard–Buhrman–Linden–Méthot–Tapp–Unger showed that Alice and Bob could do this implausible task even if their magic nonlocal boxes only succeeded at the CHSH game with probability exceeding $\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 91\%$.

4. **[A perfect magic trick.]** Alice is on Mars, Bob is on Jupiter, Charlie is on Saturn. With each of them is a referee. At the stroke of midnight, Pittsburgh time, each referee flips a fair coin to choose a challenge that is either "top" ($\top$) or "bottom" ($\bot$). Assume that among the referees, there are an odd number of $\top$'s.[2] Alice, Bob, and Charlie are required to promptly respond to their challenges with a "0" or "1". They "succeed with the magic trick" under the following conditions:

all three referee challenges were $\top$:	three responses have an even number of 1's
referee challenges were one $\top$ and two $\bot$'s:	three responses have an odd number of 1's

As usual, assume that the spatial distance between Alice, Bob, and Charlie prevents them from communicating at all.

(a) [$**$] Prove that if Alice, Bob, and Charlie respond deterministically to their challenges, the probability with which they can succeed in the magic trick is at most 3/4.

(Remark: as with the CHSH game, from this one can also easily conclude that if Alice, Bob, and Charlie can share classical random bits, they still cannot succeed with probability more than 3/4.)

(b) [$**$] Suppose that Alice, Bob, and Charlie prepare the following 3-qubit state on Earth before the magic trick begins:

$$\frac{1}{2}|000\rangle - \frac{1}{2}|011\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle .$$

Alice takes the first qubit to Mars, Bob takes the second qubit to Jupiter, Charlie takes the third qubit to Saturn. Now, when they receive their challenges, they each use the following strategy: If they are challenged with $\top$, they measure their qubit and respond with the outcome. If they are challenged with $\bot$, they first apply a Hadamard gate to their qubit, and then they measure and respond with the outcome.

Prove that Alice, Bob, and Charlie succeed with the magic trick with 100% probability.

[2] In other words, the three challenges are either $\top\top\top$, $\top\bot\bot$, $\bot\top\bot$, or $\bot\bot\top$, with each of these possibilities being equally likely. You might protest that there's no way for the referees to immediately enforce this, since they are so far apart. That's true. So in practice what you do is have the referees and Alice/Bob/Charlie do the whole process a bunch of times in quick succession. Then, when they're all back on Earth comparing notes, they just throw out the "rounds" in which the referees happened to pick an even number of $\top$'s. Alternatively, if you assume that Alice, Bob, and Charlie can't spy on the referees, the referees can jointly and secretly choose their challenges from the four possibilities while they're still on Earth, before the magic trick begins.

5. **[Hardy's Paradox.]** Alice and Bob prepare the following 2-qubit state:

$$|\psi\rangle = (H \otimes H)\left(\frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle + \frac{1}{\sqrt{3}}|10\rangle\right).$$

Alice now takes control of the first qubit and Bob takes control of the second qubit.

Each of Alice and Bob now flips a coin and does the following: If they flip Tails, they directly measure their qubit; if they flip Heads, they first apply a Hadamard to their qubit and then they measure.

(a) [$**$] Prove the following statements:

If Alice flips T and Bob flips T,	it's	*possible* A & B will measure 1, 1 respectively
If Alice flips T and Bob flips H,	it's	*im*possible A & B will measure 1, 0 respectively
If Alice flips H and Bob flips T,	it's	*im*possible A & B will measure 0, 1 respectively
If Alice flips H and Bob flips H,	it's	*im*possible A & B will measure 1, 1 respectively

(b) [$**$] Lucien says the following: "Let's consider the situation before any coin flips or measurement happens, and try to decide what outcomes the qubits are capable of producing when measured.

- One one hand, consider the first statement in (a). Since it's possible that Alice will flip Tails and Bob will flip Tails, we conclude that prior to any coin flips/measuring, it's *possible* for Alice's qubit to register 1 after being directly measured.
- Now consider the second statement in (a). Since Alice's qubit is capable of generating a 1 when she flips Tails, it must be *im*possible for Bob's qubit to produce a 0 when he flips Heads, and consequently Hadamards-then-measures.
- Let's repeat the previous two bullet points, interchanging 'Alice' and 'Bob'. By the first statement in (a), we conclude that prior to any coin flips/measuring, it's *possible* for Bob's qubit to register a 1 when directly measured. Hence by the third statement in (a), since Bob's qubit is capable of generating a 1 when directly measured, we conclude that it must be *im*possible for Alice's qubit to produce a 0 when she Hadamards-then-measures.
- We've concluded that in case of flipping Heads, for both Alice and Bob it's impossible for them to register a 0 when they Hadamard-and-measure; i.e., they must both register a 1 in this case. But this contradicts the fourth statement in (a)."

Critique the four bullet points above. Do you agree or disagree with Lucien?

(c) [$**$] Read Scott Aaronson's blog post from Sept. 25th, 2018, *It's hard to think when someone Hadamards your brain*. Critique his argument. Do you agree or disagree with Scott?

6. **[Multiplicative generators modulo a prime.]** For this problem, first please recall Problem 5 from the previous homework. (You may cite its results.)

   (a) Show that for any $M \geq 1$,
   $$\sum_{D|M} \varphi(D) = M,$$
   where the sum is over all divisors D of M. (Hint: consider the M fractions $\frac{1}{M}, \frac{2}{M}, \ldots, \frac{M}{M}$. Suppose we put each of them into lowest terms, and then group together the ones with denominator D. How many fractions go into D's group?)

   (b) [$**$] Let $A \in \mathbb{Z}_M^*$. Define the *order* of A, denoted $\mathrm{ord}_M(A)$, to be the smallest positive integer R such that $A^R = 1 \pmod{M}$. Prove that $\mathrm{ord}_M(A)$ divides evenly into $\varphi(M)$. Conclude that if P is prime then $\mathrm{ord}_P(A)$ divides evenly into $P-1$.

   (c) Let P be a prime, let D be a divisor of $D-1$, and let $N_P(D)$ be the number of elements of $\mathbb{Z}_P^*$ with order D. Show that
   $$\sum_{D|P-1} N_P(D) = P - 1.$$

   (d) Continuing part (c), show that if $\mathrm{ord}_P(A) = D$, then $1, A, A^2, \ldots, A^{D-1}$ are distinct (mod P) and that they all solve the equation $x^D - 1 = 0 \pmod{P}$. Since every degree-D polynomial equation mod P has at most D solutions,[3] this proves that $1, A, A^2, \ldots, A^{D-1}$ constitute *all* the numbers x satisfying $x^D = 1 \pmod{P}$.

   (e) Continuing part (d), show that if $\mathrm{ord}_P(A) = D$, then *every* element $B \in \mathbb{Z}_P^*$ with $\mathrm{ord}_P(B) = D$ is of the form A^K, where $\mathrm{ord}_P(A^K) = D$. Show that these are precisely the K with $\mathrm{GCD}(K, D) = 1$. Therefore deduce that if there exists *any* A with $\mathrm{ord}_P(A) = D$, then it must be that $N_P(D) = \varphi(D)$.

   (f) Having shown that $N_P(D)$ is either 0 or $\varphi(D)$ for each divisor D of $P-1$, deduce from parts (a) and (c) that we must in fact have $N_P(D) = \varphi(D)$ for each divisor D of $P-1$.

   (g) Conclude that $N_P(P-1) = \varphi(P-1) \geq 1$ and hence (for any prime P) there exists an A such that $\mathrm{ord}_P(A) = P-1$; i.e., $\mathbb{Z}_P^* = \{A, A^2, \cdots, A^{P-1}\}$. Such an A is called a *generator* of the multiplicative group Z_P^*.

[3] You can take this for granted; it's because the integers modulo P form a *field*. In other words, besides the standard addition, subtraction, and multiplication, they also allow for division (except for division by 0). Given this, it's not hard to show that whenever you have a solution α of a degree-D polynomial equation $Q(x) = 0$, you can divide $Q(x)$ by $x - \alpha$. Since you can repeat this at most D times, the equation can have at most D solutions.