Week 2 work: Sept. 13 — Sept. 20
12-hour week
Obligatory problems are marked with [**]

---

1. **[Migdał–Hes–Krupiński.]**

   (a) [∗∗] Play some of the wonderful Quantum Game.

   A few words of explanation. The photon in this game has one qubit devoted to *polarization*, which can be either horizontal $|\leftrightarrow\rangle$ or vertical $|\updownarrow\rangle$. You can sort of see this visually from the direction in which the photon is shown oscillating. I kind of prefer the "oscilloscope" view, which you can get to by toggling from "orthogonal" in the bottom-right corner of the screen. As an example "gate", sugar-water has the effect of applying a 45° rotation on the polarization.

   The photon also has a 4-dimensional "qudit" devoted to direction of travel (North / South / East / West). This is visually depicted in the obvious way. Put together, this means the photon has an 8-dimensional state. The Encyclopedia gives the 8×8 unitary matrix for each physical component. (Actually, some of these matrices are not unitary because they have a sort of "measurement" component. For example, you can think of the North-South Absorptive Polarizer as follows: first, it measures the photon; then, if the measurement showed vertical polarization and North or South travel, the Polarizer regenerates a photon in that state, passing through; otherwise, the Polarizer does nothing.)

   Finally, the photon actually also has a 10-dimensional qudit devoted to its North/South position and a 13-dimensional qudit devoted to its East/West position. Hence overall, the photon is a 1040-dimensional quantum system. Describing its state requires 1040 complex amplitudes, although in most circumstances (e.g., when there are few Beam Splitters involved), most of these amplitudes are 0. You can see the state at the bottom of the screen during a simulation; it's shown as $|x, y, s|$, where x is the East/West position, y is the North/South position, and s is one of 8 ASCII drawings showing the combined direction (>, <, `v`, `^`) and polarization (a tick mark if the polarization is opposed to the direction of travel).

   (b) Beat at least 16 levels and look through all the Encyclopedia entries.

2. **[Complex number exercises.]** Let $z = x + iy$ be a complex number, where x and y are real numbers and $i = \sqrt{-1}$. Here is some standard notation:

- $\mathrm{Re}(z) = x$, the *real part* of z
- $\mathrm{Im}(z) = y$, the *imaginary part* of z
- $z^* = x - iy$, the *complex conjugate* of z ; this is also often written as $\overline{z}$
- $|z| = \sqrt{x^2 + y^2}$, the *magnitude* (or *modulus* or *length*) of z
- $\arg(z)$ is the (counterclockwise) angle of vector (x, y) from the x-axis in the *complex plane* (i.e., $\mathbb{R}^2$ with the x-axis being the real axis and the y-axis being the imaginary axis); $\arg(z)$ is called the *argument* (or *angle*) of z
- if $r = |z|$ and $\theta = \arg(z)$, then the pair (r, θ) is called the *polar coordinates* of z
- $e^{i\theta} = \cos\theta + i\sin\theta$ (you can either treat this as just notation, or else it's a theorem, depending on your definition of the exponential function $w \mapsto e^w$)

Verify the following facts:

(a) $\mathrm{Re}(z) = \frac{1}{2}(z + z^*)$

(b) $\mathrm{Im}(z) = \frac{1}{2i}(z - z^*)$

(c) $(z + w)^* = z^* + w^*$. Also, if A and B are complex matrices, $(A + B)^\dagger = A^\dagger + B^\dagger$

(d) $(zw)^* = z^* w^*$

(e) $|z| = \sqrt{zz^*}$

(f) $1/z = \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}$

(g) If (r, θ) are the polar coordinates of z, then $r = \sqrt{zz^*}$ and $\theta = \tan^{-1}\frac{\mathrm{Im}(z)}{\mathrm{Re}(z)}$

(h) Conversely, $z = re^{i\theta} = r(\cos\theta + i\sin\theta)$

(i) $1/z$ has polar coordinates $(1/r, -\theta)$

(j) z^* has polar coordinates $(r, -\theta)$

(k) if $|z| = 1$, then $1/z = z^*$

(l) if w is another complex number with polar coordinates (R, ϕ), then zw has polar coordinates $(rR, \theta + \phi)$ (where you may take $\theta + \pi$ modulo $2\pi = 360°$)

The last fact here is perhaps the most conceptually important; if z has polar coordinates (r, θ), then the meaning of multiplying some complex number w by z is to "rotate" w in the complex plane by θ and "scale" its length by r.

A few more problems:

(m) If z has polar coordinates (r, θ) then z^n has polar coordinates $(r^n, n\theta)$ for any integer $n \in \mathbb{Z}$

(n) If $n \in \mathbb{Z}^+$ is a positive integer, there are exactly n distinct complex numbers w satisfying $w^n = 1$. (These are called the *nth roots of unity.*)

(o) The nth root of unity with smallest nonzero argument is usually called the *primitive nth root of unity*, and is sometimes denoted ω_n. Show that ω_n^j is an nth root of unity for all integers $j \in \mathbb{Z}$, and that $\{\omega_n^0, \omega_n^1, \ldots, \omega_n^{n-1}\}$ is the set of all n distinct nth roots of unity

3. **[Dirac notation and measurement exercises.]**

   (a) Let $|\phi\rangle = 3\,|0\rangle - 5i\,|1\rangle$. What is $\langle\phi|\phi\rangle$?

   (b) What number, C, should $|\phi\rangle$ be divided by to make it a "normalized" state; i.e., a unit vector? For future reference, define $|\psi\rangle = \frac{1}{C}\,|\phi\rangle$ to be this state vector.

   (c) What are the possible outcomes and associated probabilities if $|\psi\rangle$ is measured in the standard $\{|0\rangle, |1\rangle\}$ basis?

   (d) Same question as above for measuring in the $\{|+\rangle, |-\rangle\}$ basis.

   (e) Verify that $\frac{1}{\sqrt{2}}\,|0\rangle + \frac{i}{\sqrt{2}}\,|1\rangle$ and $\frac{1}{\sqrt{2}}\,|0\rangle - \frac{i}{\sqrt{2}}\,|1\rangle$ form an orthonormal basis for $\mathbb{C}^2$. (These two vectors are sometimes called $|i\rangle$ and $|-i\rangle$. Then do the prior question for measuring in the $\{|i\rangle, |-i\rangle\}$ basis.

4. **[Projectors and reflections.]** Let $|\psi\rangle$ and $|\phi\rangle$ be two unit vectors in $\mathbb{R}^d$. (Actually, it's fine if they're complex unit vectors, but let's keep it real.) We will be interested in $Q = |\phi\rangle\langle\psi|$, which is a $d \times d$ matrix, and can therefore be thought of as a transformation on d-dimensional vectors.

   (a) Explicitly work out the matrix Q in the case $|\psi\rangle = |0\rangle$ and $|\phi\rangle = |+\rangle$, and also in the opposite case $|\psi\rangle = |+\rangle$ and $|\phi\rangle = |0\rangle$.

   (b) [$**$] Practice hand-drawing the expression $|\phi\rangle\langle\psi|$. The trick is this:
   - Start by drawing the first bar and ϕ, like so: $|\phi$
   - Next — and this is the key — *draw an X*, like so: $|\phi\rangle\!\langle$
   - Finally, draw the ψ and the final bar, forming $|\phi\rangle\!\langle\psi|$

   If you try to draw the $\rangle$ and the $\langle$ separately, you'll never get the points to match up.

   Congratulations, you now know the first secret of the quantum club :)

   (c) Fill in the blanks: The transformation Q maps the vector $|\psi\rangle$ to _____, and maps every vector orthogonal to $|\psi\rangle$ to _____.

   (d) [$**$] Suppose now that $|\psi\rangle = |\phi\rangle$. Let $P = |\psi\rangle\langle\psi|$. Describe in (geometric) words the transformation P.

   (e) [$**$] Let $\mathbb{1}$ denote the identity matrix in $\mathbb{R}^d$.[1] Describe in (geometric) words the transformation $\mathbb{1} - 2P$. Your description should include the words "hyperplane perpendicular to". Prove that this transformation is unitary.

   (f) Suppose we are interested in the change-of-(orthonormal-)basis operation U that takes the orthonormal basis $|\psi_1\rangle, \ldots, |\psi_d\rangle$ to the orthonormal basis $|\phi_1\rangle, \ldots, |\phi_d\rangle$. Show that U can be written as

$$U = |\phi_1\rangle\langle\psi_1| + \cdots + |\phi_d\rangle\langle\psi_d|,$$

   and that U is unitary.

[1] In math, it's more traditional to write I for this matrix — the diagonal matrix with 1's on the diagonal, that does nothing to a vector. But $\mathbb{1}$ is a better name :) and is used somewhat commonly in quantum.

5. **[Vazirani Lectures.]** Watch Lectures 6–10 of Vazirani's nice video lectures on YouTube.

6. **[Unitary Matrices.]** [$**$] Let $A \in \mathbb{C}^{d\times d}$ be a matrix that preserves lengths; that is, $\|A|\psi\rangle\| = \||\psi\rangle\|$ for all kets (vectors) $|\psi\rangle \in \mathbb{C}^d$. Prove that A is unitary, i.e., that $A^\dagger A = \mathbb{1}$.

7. **[Quantum Anti-Zeno Effect.]** [$**$] Assume you have a single qubit that you know is in the state $|0\rangle$. You really wish to change its state to $|1\rangle$. You have the ability to build any measurement device, and use it as many times as you want. How can you (almost surely) get the qubit's state changed to $|1\rangle$? (Hint: very similar to the Elitzur–Vaidman Bomb.)

   Remark: This trick is called the "Quantum Anti-Zeno Effect", by analogy to a earlier-discovered trick called the "Quantum Zeno Effect". In the Quantum Zeno Effect (aka Watchdog Effect), you have a qubit in state $|0\rangle$ and you wish to keep it that way; however, there is some physical process which is slowly "rotating" your qubit towards $|1\rangle$. By rapid repeated measurement in the $|0\rangle$-$|1\rangle$ basis, you can counteract this rotation and keep your qubit in the state $|0\rangle$ with high probability. This Quantum Zeno Effect was first described by Alan Turing!

8. **[GCD.]** This problem is about the task of computing the GCD (greatest common divisor) of two input numbers, A and B. As usual, you should imagine these to be numbers to be, like, 2000 binary digits long. The grade school algorithm for GCD is: (i) find the prime factorizations of A and B; (ii) pick out all the common prime factors, and multiply them together. Of course, this algorithm is not actually possible to implement in physical reality for 2000-bit numbers (given known classical factoring algorithms). However, there *is* a physically possible algorithm (i.e., computing GCD is in "P"): it is called *Euclid's Algorithm*[2], and is arguably the first known nontrivial algorithm in history.

   (a) (Warmup to Euclid's Algorithm — how he actually described it.) Show that if Q is a divisor of both A and B, then it's also a divisor of $A - B$. Conversely, show that if Q is a divisor of $A - B$ and B, then it's also a divisor of A. Conclude the rule $\text{GCD}(A, B) = \text{GCD}(A - B, B)$.

   (b) (Warmup continuation.) Of course, we also have the rule $\text{GCD}(A, B) = \text{GCD}(B, A)$. By iterating these two rules, compute $\text{GCD}(42, 30)$. The "base case" is that $\text{GCD}(A, 0) = A$ for all A (since everything is a divisor of 0). You should have to do 5 subtractions in total.

   (c) Suppose you were computing $\text{GCD}(A, 6)$, where $A = 6 \times 10^{500} + 4$. You would not want to do the subtraction rule 10^{500} times before getting to the swapping rule. But... it should be obvious what subproblem you'll get down to after performing all those subtractions... Prove that the following is a correct algorithm for computing the GCD:

```
Euclid(A, B) :
    if B = 0, return A
    else return Euclid(B, A mod B)
```

   (d) [$**$] Compute

$$\text{GCD}(106113609170668254652391269192197757215334846951209743863306173107325600,$$
$$894128743023837450195367301428030915619905056250057436341104142570200).$$

   (e) [$**$] When we execute $\texttt{Euclid}(A, B)$, it produces a descending chain of numbers; e.g., $\texttt{Euclid}(100, 18)$ produces

$$100 \quad 18 \quad 10 \quad 8 \quad 2.$$

   Any three consecutive numbers in this chain are of the form C, D, (C mod D). Prove that for any three consecutive numbers F_{t-1}, F_t, F_{t+1} in the chain, we have $F_{t+1} \leq (1/2)F_{t-1}$. (Hint: case analysis based on how large F_t is, compared with F_{t-1}.) Conclude that $F_t F_{t+1} \leq (1/2)F_{t-1}F_t$; further conclude that the total length of the chain is at most $\log_2 A + \log_2 B$.

   Thus if A is m bits long, and B is n bits long, the length of the chain produced by $\texttt{Euclid}(A, B)$ is at most $m + n$. Also, on the last homework you saw that computing A mod B via the grade school method takes a number of steps proportional to mn. Combining these facts, we see that the GCD of two n-bit numbers can be computed in $O(n^3)$ steps; i.e., computing the GCD is in "P". (Remark: with a more sophisticated algorithm than Euclid's, one can compute the GCD of two n-bit numbers in $\widetilde{O}(n^2)$ steps.)

[2] As is consistent with Stigler's Law, it was probably not originally discovered by Euclid.

9. **[Perfect Powers.]**

(a) Give pseudocode for an algorithm that takes as input a positive integer A and determines whether or not A is a perfect square. If it is, your algorithm should also determine the number B such that $B^2 = A$. If A is n binary digits long, your algorithm should take $O(nM(n))$ steps, where $M(n)$ is the number of steps required to multiply two numbers of at most n binary digits. Thus, your algorithm should take $O(n^3)$ with the usual grade school multiplication algorithm; or, it would be $\widetilde{O}(n^2)$ steps with the sophisticated FFT-based multiplication algorithm. (Hint: binary search.)

(b) [$**$] Give pseudocode for an algorithm that takes as input a positive integer A and determines whether or not A is a perfect power (i.e., a perfect square, cube, fourth power, etc.). If it is, your algorithm should also determine numbers B and $C > 1$ such that $B^C = A$. When A is an n-bit number, justify that your algorithm takes at most $O(n^d)$ steps for some constant d (such as $d = 5$).

(Remark: In 1998, Daniel Bernstein showed how to solve this problem in $\widetilde{O}(n)$ steps; the algorithm is sophisticated, though.)