CSE610(C): Topics in Quantum Computing Fall 2021, Kenneth W. Regan

Purpose of Course: To promote understanding of current research in quantum computing *widgets*.

1. Mathematical fundamentals with attention to physics (4-6 weeks, blending into...).
2. Quantum Circuits --- as examples of quantum systems.
3. Quantum Walks.
4. Quantum Communication. What and how much to do depends on interests. Certainly quantum teleportation, basic security protocols, and quantum "paradoxes" from the viewpoint of communication.
5. Quantum physical systems: formulation via Hamiltonians, "Boson Sampling", lots of etc...
6. How much computational complexity theory to involve is an open question. (The Lipton-Regan text on-purpose avoids naming complexity classes until the last main chapter.)

As-such, computer science theory background not presupposed, nor physics background, beyond some (negotiable) basics---e.g., deterministic and nondeterministic finite automata (DFAs and NFAs), the notion of universal computation (whether via Turing machines or random-access machines or high-level programming languages), and "P vs. NP" with factoring and much of classical cryptography in the middle.

Organization: As a 6xx course with graded assignments, take-home final, and project option.

Philosophy I: "Simple Realism"

- Show polarizing filters.
- Show part of talk https://cse.buffalo.edu/~regan/Talks/UnionCollege52115.pdf

Philosophy II: Is Nature *Lexical*?

- The idea of *Logos* from 500 BCE. Identified, perhaps incorrectly, with "word".
- The possible meaning of the final sentence of Umberto Eco's novel *The Name of the Rose,* quoting Bernard of Cluny, 1100s*:*

Stat rosa pristina nomine; nomina nuda tenemus

This means: The rose stands by its original name; we hold the bare name. It is possibly a misquote of "Stat *Roma*..." meaning that we (in the 1100s or 2000s) only know the glory of ancient Rome through recorded memory of it. I, however, believe that a deeper reading treats "pristina" as meaning "unsullied" rather than "original" and taking some liberties of grammar:

The rose abides unsullied by a name; we hold only the bare name.

Regarding the rose as representing Nature, the issue is whether Nature's workings must be read as paying heed to the symbolic way we describe them. The (theoretically-)efficient quantum factoring algorithm is a real challenge to the idea that nature is symbolically mathematical.

Philosophy III: Evolution of the Lipton-Regan text.

- The original intent of a 60-page "Springer Brief".
- The "physics-free" first edition.
- The overlay nature of the current edition.

Discussion...

One particular request was for quantum devices that create highly accurate time and distance measurements.

Quantum States

[Note: I have edited the following to number from zero in "underlying co-ordinates" as in the text. This is different from how most linear algebra texts do it. It will however be conventional to number "quantum coordinates" from 1.] Natural systems can be modeled (inefficiently!?) by vectors

$$\mathbf{a} = \begin{bmatrix} a_0 \\ a_2 \\ a_3 \\ \vdots \\ a_i \\ \vdots \\ a_{N-1} \end{bmatrix}.$$

We say that **a** has N "underlying coordinates." Often N will be a power of 2, $N = 2^n$, where n will be the number of "quantum coordinates" or **qubits**. We can also have powers of larger numbers d, $N = d^n$. When $d = 3$ we will get **qutrits**, $d = 4$ will give **quarts**, and the general case gives **qudits**. Maybe over 99% of the "QC" literature is about qubits. But actually, let's first think of N as not being subdivided at all.

One insight of linear algebra is that the entries a_i are not just "things unto themselves" but stand for multiples of corresponding **basis vectors**:

$$\mathbf{a} = a_0\,\mathbf{e_0} + a_1\,\mathbf{e_1} + a_2\,\mathbf{e_2} + \cdots + a_i\,\mathbf{e_i} + \cdots a_N\,\mathbf{e_N}\ ,$$

where for each i,

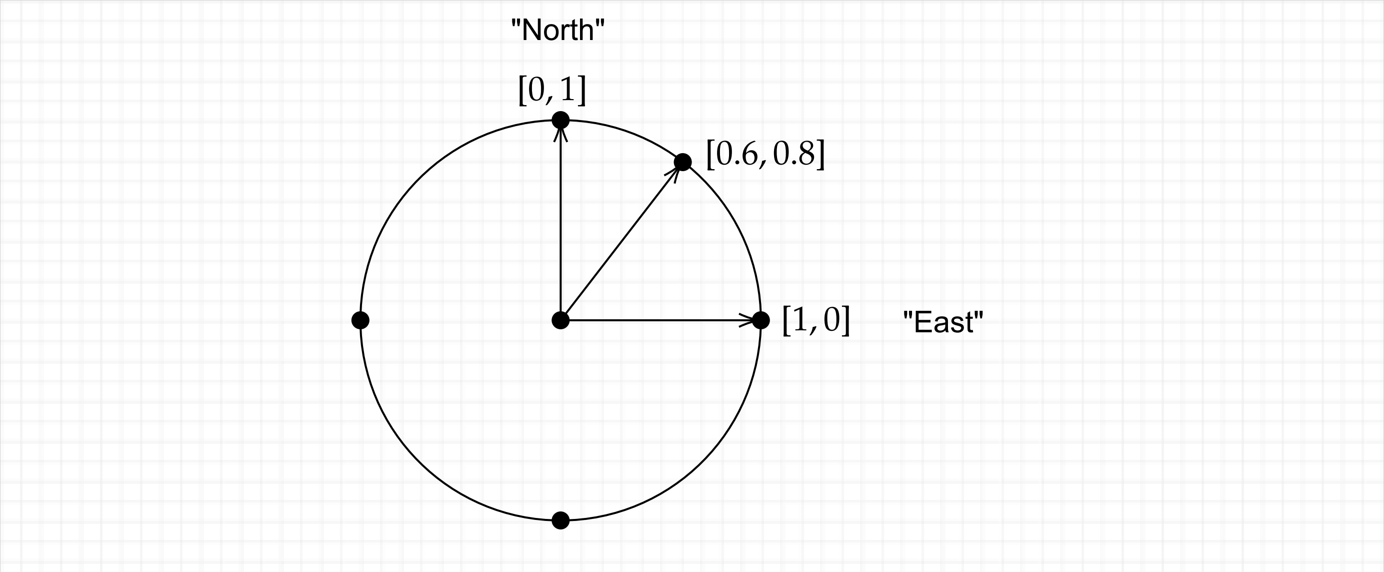
$$\mathbf{e_i} = [0, 0, 0, \ldots, 0, 1, 0, \ldots, 0]^T$$

with the lone 1 in position i. Notice we're being picky about considering vectors to be column vectors and writing transpose ^{T} to make $\mathbf{e_i}$ be a column vector. (Whether Nature really makes this distinction is a real question. We took the "no" side in the first edition, but using the angle-bracket notation from physics makes an initial commitment to the "yes" side.) With this notation, the vectors $\mathbf{e_i}$ are collectively called the **standard basis**.

A second insight of linear algebra is that one need not be "wedded to the standard basis"---one can do a **change-of-basis**. In general N-dimensional linear algebra, any set of N *linearly independent* vectors can be a basis. For instance, in $N = 2$ dimensions, the vectors

$[1,0]$ and $[0.6,0.8]$

are linearly independent (since there are only two vectors, the point is that neither is a multiple of the other). However, the second one is kind-of redundant in the first coordinate with the first. Whereas $\mathbf{e_0} = [1,0]$ is "only East" and $\mathbf{e_1} = [0,1]$ is "only North"---they are **orthogonal**, meaning that their *inner product* is zero.



We can diagram these vectors on the *unit circle*---note that $0.6^2 + 0.8^2 = 0.36 + 0.64 = 1$. The inner product of $[0.6,0.8]$ and our "East" vector is $0.6 \cdot 1 + 0.8 \cdot 0 = 0.6$.

There are several ways to write the inner product of two vectors $\mathbf{a}$ and $\mathbf{b}$:

$$\mathbf{a} \cdot \mathbf{b}, \quad \langle \mathbf{a}, \mathbf{b} \rangle, \quad \langle \mathbf{a} \mid \mathbf{b} \rangle.$$

The last is what feeds into **Dirac Notation**, as the **bra**(c)**ket** of the row vector $\langle \mathbf{a}|$ and the column vector $|\mathbf{b}\rangle$. I will introduce this notation in a conceptual manner, building from how orthogonal vectors are exclusive of each other.

Consider any finite set of attributes that are mutually exclusive. For example, whether a playing card is a heart $\heartsuit$, diamond $\diamondsuit$, spade $\spadesuit$, or club $\clubsuit$ are exclusive---a "basic card" cannot be two or more of these at once. We will also suppose that the attributes are *collectively exhaustive;* this will be reflected in probabilities over the basic attributes summing to 1. That is, our deck has no unseen Jokers (but we will revisit this when we discuss **decoherence** later). The first idea of Dirac Notation is that these mutually exclusive attributes can be treated abstractly as orthogonal basis vectors by putting each inside a **ket**:

$$|\heartsuit\rangle, |\diamondsuit\rangle, |\spadesuit\rangle, |\clubsuit\rangle.$$

We can form vectors just as if these were the standard basis vectors $\mathbf{e}_0$, $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$ in $N = 4$ dimesnions, for instance

$$0.3|\heartsuit\rangle + 0.4|\diamondsuit\rangle - 0.5|\spadesuit\rangle + \sqrt{0.5}|\clubsuit\rangle.$$

(This is a little different from the example I drew in lecture.) This is weird: what does it mean to subtract half a spade from four-tenths of a diamond, anyway? Why the extra square root on the clubs? Actually, if you erased the coefficient of $|\clubsuit\rangle$, you'd know its absolute value squared would have to be 0.5 anyway. That's because the other entries' squares give $0.09 + 0.16 + 0.25 = 0.5$ and all the squares must sum to 1 (unless there is an unknown chance of turning up a Joker). Let's not worry about the interpretation yet: for now all we care is that it's a legal unit vector.

The two simplest exclusive attributes are "being 0" and "being 1". We thus write $|0\rangle$ and $|1\rangle$ as our basis. Because we have two basic attributes, we use vectors in 2-dimensional space. Our standard basis vectors in that space are $\mathbf{e}_0 = [1, 0]$ and $\mathbf{e}_1 = [0, 1]$. It is convenient to use $\mathbf{e}_0$ for $|0\rangle$ and $\mathbf{e}_1$ for $|1\rangle$. This could be confusing insofar as $\mathbf{e}_0$ "starts with" 1 while $\mathbf{e}_1$ starts with 0, and more concretely, $(1, 0)$ usually comes after $(0, 1)$ in sorting rather than before. We can form many other vectors from these basis vectors, but only the ones of unit magnitude can be valid states. For example, the difference

$|0\rangle - |1\rangle$ is normalized by multiplying by $\sqrt{0.5}$ to make $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} = \sqrt{0.5}[1, -1]^T$.

This looks "more numerical" than subtracting half a spade from four-tenths of a diamond, but is it really? If you are sending binary code, what does it mean for the ones to be negative? Whatever it means, the mode of calculation that arises---and which we will go into more deeply next week---has been successful for real computations and promises even more.

The purpose of using the playing-card tokens is to clarify relationships that might be confused when 0 and 1 appear as both tokens and numbers. Here is one more example. We can make tokens out of the ranks rather than suits of the cards:

$$|2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle, |8\rangle, |9\rangle, |10\rangle, |J\rangle, |Q\rangle, |K\rangle, |A\rangle$$

Note that the ten is one token, even though two bits are used to write it. We coud even make fifty-two separate tokens, one for each individual card:

$$|2\clubsuit\rangle, |3\clubsuit\rangle, \dots, |A\clubsuit\rangle, |2\diamondsuit\rangle, |3\diamondsuit\rangle, \dots, |A\diamondsuit\rangle, |2\heartsuit\rangle, |3\heartsuit\rangle, \dots, |A\heartsuit\rangle, |2\spadesuit\rangle, |3\spadesuit\rangle, \dots, |A\spadesuit\rangle$$

using now the order of suits in the game of bridge, where also the first two are "minor suits" and hreats and spades are "major." This would use $N = 52$. When we forget the suit, however, we have $N = 13$; call that a "**q13-it**". Now suppose we have four q13-its, one for clubs, one for diamonds, one for hearts,a dn one for spades. Does that give us $N = 52$ back again?

Ah, no. Now we are talking about hands of four cards, one of each suit. That's more than just having one card. The number of such possible hands is $13^4 = 28,561$. (The number of possible four-card hands when you allow any number of a suit is even bigger.) Going back to the stat of the lecture, this is when we want to use n to stand for 4 "q13-its" and $d = 13$ for the width of any one of them. So we get $N = d^n = 28,561$ for the total possible basic outcomes. It is much more economical to think of "four cards" than 28,561 possible hands! The 4 here is the dimension in "quantum coordinates"---so you can think about the problem in dimensions of "4×13" even though the underlying number is not 52 but really 28,561. Whether Nature really operates on the more economical level is the philosophical big question.