Homework #12. Due Tue 11/13.

#1 – We say \([a_0, a_1, \ldots, a_M]\) – where the \(a_i\) are positive integers except \(a_0\) is permitted to be zero – is the continued fraction expansion of the rational number \(a/b\) provided

\[
\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_M}}}}
\]

Example:

\[
\frac{8}{3} = 2 + \cfrac{2}{3} = 2 + \cfrac{1}{\frac{3}{2}} = 2 + \cfrac{1}{1 + \frac{1}{2}},
\]

so the continued fraction expansion of \(8/3\) is \([2, 1, 2]\). Find the continued fraction expansion for \(10/7\).

#2 – Exercise 9.1.1.

#3 – Exercise 9.1.4.

#4 – Exercise 10.1.2.

#5 – Exercise 10.2.5; note the errata: “10.2.1, 10.2.2, and 10.2.3” should read “10.2.2, 10.2.3, and 10.2.4.”

Twelfth week summary

Tue 10/30. We had one “final word,” actually two, about Shor’s algorithm: continued fractions. There is a mathematical theory of continued fractions, and that is what is needed for the one missing link in our understanding. Namely, after executing Shor’s circuit and making a measurement, we have a \(q\)-bit quantity we have been calling \(y\). The thing we are after is the order of \(a\), where \(a\) is the randomly selected base used in the function \(F(x) = a^x \mod N\). (\(N\) is the number to be
factored.) We indicated that the measured quantity $y$ would be related to the desired order $o(a)$ by the relationship

$$o(a) \approx \frac{\text{a multiple of } Q}{y},$$

but we never gave any specifics for how to deduce $o(a)$ from $y$.

Jay gave a presentation based on Chapter 9. In a nutshell, two parties communicate by an encipher-decipher protocol which requires that they share a common, secret bit-string (called a “key”). Key-exchange using public-key cryptography permits a secure sharing. However, certain quantum protocols for exchanging a key provide, in addition to a secure exchange, protection against unknown eavesdropping or tampering. The most basic quantum protocol is BB84. Here a series of qubits, $|0\rangle$’s and $|1\rangle$’s, are sent by Alice to Bob, but using one of two bases (denoted $+$ and $\times$). The sequence of bases are chosen at random. Bob then chooses another random sequence of bases with which to decrypt. He reports to Alice his decrypt sequence. She tells him which members of his sequence are the same as hers; these are now bits which they share. By using up some small number of them – say Bob reveals them to Alice – allows them to check for tampering. If the qubits have been handled during transit, then there is only a 50% chance that Bob’s and Alice’s versions will agree – despite the fact that they have been generated and measured with respect to the same basis. Section 9.3, a slightly different protocol although similar in nature, was also presented.

Wed 10/31. An informal handout was given to the class. This was some material about the Advanced Encryption Standard (AES) taken from Wiki. This shows an example of how a shared key would be used. The key, call it $k_0$, is expanded according to a key-schedule to produce $k_0, k_1, \ldots, k_{10}$. The number 10 is peculiar to the 128-bit version of AES; longer expansions are used for 192 or 256 bit keys. These $k_i$ are exclusive-ored into the 128 bit target throughout the ten rounds. At round zero, we start with plain text; by the end of round 10 we have cipher text. At each round, one finds substitution ($S$-box), row rotation, column mixing (a linear transformation) and exclusive-or’ing with
To decipher, the same process is applied in reverse, using the same sequence $k_0, k_1, \ldots, k_{10}$. The informal handout also contained some information about the homework problems which were due in yesterday (HW 10).

Thu 11/1. James presented sections 10.1 and 10.2 on classical (Shannon) and quantum (von Neumann) entropy. Given a probability distribution $p_1, \ldots, p_n$ its entropy is defined as

$$H = - \sum_i p_i \log p_i.$$ 

It is a measure of how much information is gained each time a message is received chosen from $n$ messages having the given frequencies. It also indicates a theoretical limit on how well the messages can be compressed. There is some way to indicate which message of the $n$ is being transmitted using, on average, $\sum_i p_i \log p_i$ bits per message.

Now we turn to the quantum analog. Assume that Alice has $n$ possible states $|w_1\rangle, \ldots, |w_n\rangle$ which she sends with the frequencies $p_1, \ldots, p_n$. This gives rise to the density operator $D$ defined by

$$D = p_1 |w_1\rangle\langle w_1| + \cdots + p_n |w_n\rangle\langle w_n|.$$ 

The action of $D$ on a vector $|v\rangle$ is given by

$$D|v\rangle = p_1 \langle w_1|v\rangle |w_1\rangle + \cdots + p_n \langle w_n|v\rangle |w_n\rangle.$$ 

Suppose that Bob measures the incoming vectors with respect to some basis $|v_1\rangle, \ldots, |v_n\rangle$. Then $\langle v_i|D|v_i\rangle$ is the probability that Bob will see $|v_i\rangle$ after his measurement. These frequencies may be fed into the Shannon entropy formula. The resulting Shannon entropy is dependent on the choice of the basis $|v_1\rangle, \ldots, |v_n\rangle$.

There is a basis that will minimize the Shannon entropy. Because the density operator $D$ is Hermetian, it has an orthogonal basis of eigenvectors, and associated eigenvalues $\lambda_1, \ldots, \lambda_n$. The von Neumann entropy is defined by

$$H_V = - \sum_i \lambda_i \log \lambda_i.$$
It has the minimization property stated above.

**Thirteenth week topics**

Tue 11/6. Joey will start Section 10.3 on classical and quantum data compression.

Wed 11/7 and Thu 11/8. Next two scheduled talks are Kevin on Section 10.4, Error-Correcting Codes; then Clay and Mark on Chapter 11, Hardware. Not sure how the timing will work out, and we might very well continue into next week.