MATH 4440/5440 Assessment, Module 5 (Quantum Computing, Coding Theory)

Katherine Stange, CU Boulder, Fall 2020

Honor Code Rules

Assessments are open book, but are to be completed on your own without collaboration. To be specific, you may use your course notes, textbook, course website resources, course videos. You may not use the internet beyond the course websites. You may not ask anyone else for help (except your professor), including other humans, or posting/entering your question or any part of it into the internet. You may not share the questions or answers with anyone else. You may not use calculators (even from the course websites) unless explicitly permitted in the question.

Have you read, understood, and followed the honor code rules above?

YES / *NO*

Some instructions on formatting.

You may use the accompanying LaTeX source document to produce LaTeX'ed answers. You may typeset answers separately. You may print the pages and solve the questions on them by hand. You may handwrite answers on separate sheets. You may upload PDF or image files (JPG or PNG). No matter what you do, just make sure it is clearly and easily legible before you upload it to canvas.

1 Question 1

Consider a binary code given by

$$C = \{(0,0,0,0,0,0,0,0), (1,1,0,0,0,0,0,0), (0,0,1,1,0,0,0,0), (0,0,0,0,1,1,0,0), (0,0,0,0,0,0,1,1)\}.$$

1. Find n, M and d so that this is an (n, M, d)-code.
2. How many errors can this code detect?
3. How many errors can this code correct?
4. Prove that it is not linear.
5. Determine the code rate of C.
6. Find one codeword that can be *removed* from the code in order to increase the number of errors that can be detected and corrected. How many errors can now be detected and corrected? Explain.

Solutions.

1. The length of this code is $n = 8$. The number of codewords is $M = 5$. The minimum distance (by checking all possible pairs, with some attention to symmetry), is $d = d(C) = 2$.
2. Since the minimum distance is 2, this code can detect 1 error.
3. Since the minimum distance is 2, this code can correct no errors.
4. The code is not linear since the sum of the second and third codewords is not a codeword.
5. The code rate is $C = log_q(M)/n = log_2(5)/8 \sim 0.29$.
6. If we remove the codeword $(0,0,0,0,0,0,0,0)$ then the minimum distance jumps to 4. Therefore, the code can now detect 3 errors and correct 1 error.

2 Question 2

(10 points) You are using a binary code given by generating matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

1. Find the parity check matrix H. Please double and triple-check this, since the following questions all depend on it.

2. Determine the syndromes of *all* the standard basis vectors $(1,0,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0,0)$ etc. (eight total vectors).

3. You receive the message 01100001. Decode this message using syndrome decoding, i.e. what codeword was mostly likely sent? (Hint: your work above ought to be enough.)

4. Next, you receive the message 01110000. Decode this message. More precisely, find a codeword at minimum distance from this one (i.e. find a codeword such that there is no other codeword which is strictly closer to the message in Hamming distance). For this, you may need to think a little further than in the previous example.

5. Find three rows of H^T which add to zero. What is the minimum distance of this code? Explain why.

Solution.

1. If $G = [IP]$, the parity check matrix is formed as $H = [P^T, I]$. That is,

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

2. The syndromes of the standard basis vectors are the rows of H^T, i.e., in order:

$$1011, 0111, 1110, 1111, 1000, 0100, 0010, 0001$$

3. We determine the syndrome by multiplying $v = (0,1,1,0,0,0,0,1)$ with H^T, obtaining

$$vH^T = (1,0,0,0).$$

Since this is the syndrome of the fifth standard basis vector, we guess there is an error in the fifth position. So the codeword sent was

$$01101001.$$

A good check (but not required) is to check that this is in the left kernel of H^T, i.e.

$$(0,1,1,0,1,0,0,1)H^T = (0,0,0,0).$$

4. We can try syndrome decoding with this message: we obtain

$$vH^T = (0, 1, 1, 0).$$

This is not $(0, 0, 0, 0)$, so this is not a codeword. This is not a syndrome of a standard basis vector, which means that more than one error must have occurred. Could two errors have occurred? If so, then this syndrome should be a sum of two rows of H^T. It is in fact the sum of the 6th and 7th rows. It is also the sum of the 3rd and 5th rows. Or the 2nd and last rows. So any of these error patterns will correspond to viable decodings. They are:

$$01110110, 01011000, 00110001.$$

5. There are no rows that are all 0, so no single-error patterns result in syndrome 0000. There are no repeated rows, so no two-error patterns result in syndrome 0000. In other words, there are no codewords of Hamming weight 1 or 2. But there are three rows that add to 0, namely 0111, 1111, and 1000 (2nd, 4th and 5th). This means that the vector 01011000 has syndrome 0000 and is therefore a codeword. The minimum distance of the code is equal to its minimum non-zero Hamming weight, which, by the argument just given, is 3.

3 Question 3

Suppose you are doing Quantum Key Exchange BB84 and you are playing the role of Bob. You choose bases L, V, V, L, L, V, V, L for your measurements of 8 photons. Alice sends you eight photons and you measure $0, 1, 1, 0, 1, 1, 0, 0$. She then reveals that her bases were L, V, L, L, V, V, L, V.

1. What is the shared secret you compute?
2. It turns out that Eve was on the line, listening in. She measured all eight of the photons, with basis L, L, L, L, L, L, L, L. Now that you know this, which of the bits you computed in the last part are still reliable, i.e. will definitely agree between your computed secret and the secret Alice computed?
3. For the remaining bits, what will you and Alice observe? (Will they agree between your computed secret and Alice's computed secret, or not, or something else?)

Solution.

1. The shared positions (where bases matched) is $1, 2, 4, 6$ (bases L, V, L, V). So your shared secret is the bits at those positions: $0, 1, 0, 1$.
2. Eve will go undetected when Alice and Bob agreed on an L basis, i.e. in the first and fourth bits of the secret.
3. When Eve measures with an L basis, while Alice and Bob used a V basis, Eve will turn the polarization to horizontal or vertical, so Bob's measurement will be randomly 0 or 1 in the V basis, and has a 50% chance of agreement with Alice's bits.

4 Question 4

1. Write the qubit
$$|\phi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
as a superposition of $|i\rangle$ and $|-i\rangle$. (In other words, change to the i basis.)

2. For the state $|\phi_0\rangle$ just discussed, imagine measuring in the $|i\rangle$, $|-i\rangle$ basis. Give the probability of measuring $|i\rangle$ and the probability of measuring $|-i\rangle$.

3. Suppose one has two unentangled qubits in the following states:
$$|\phi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |\phi_2\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle.$$
Determine the quantum superposition of $|00\rangle$, $|10\rangle$, $|01\rangle$ and $|11\rangle$ which represents the two-qubit state they are jointly in.

4. Is the following state entangled? Prove that it is or is not.
$$|\phi_3\rangle = \frac{1}{\sqrt{10}}|00\rangle + \frac{2}{\sqrt{10}}|01\rangle + \frac{2}{\sqrt{10}}|10\rangle + \frac{1}{\sqrt{10}}|11\rangle.$$

5. Apply the CNOT gate to the state $|\phi_3\rangle$ given in the last part. Determine the resulting state.

Solutions.

1. Recall that
$$|i\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle, \quad |-i\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle.$$
Solving for $|0\rangle$ and $|1\rangle$ gives
$$|0\rangle = \frac{1}{\sqrt{2}}|i\rangle + \frac{1}{\sqrt{2}}|-i\rangle, \quad |1\rangle = \frac{-i}{\sqrt{2}}|i\rangle + \frac{i}{\sqrt{2}}|-i\rangle.$$
Therefore, substituting into the given qubit expression, we find that
$$|\phi_0\rangle = \frac{1-i}{2}|i\rangle + \frac{1+i}{2}|-i\rangle.$$

2. The square of the magnitude of the amplitude gives the probability. In particular, the probability of measuring $|i\rangle$ is
$$\left|\frac{1-i}{2}\right|^2 = \frac{|1-i|^2}{|2|^2} = (1^2+1^2)/4 = 1/2.$$
Similarly (or by the fact that the probabilities must sum to 1), the probability of measuring $|-i\rangle$ is also $1/2$.

3. This requires multiplying the corresponding amplitudes together. So the amplitude of $|00\rangle$ is the amplitude of $|0\rangle$ in the first expression, times that of $|0\rangle$ in the second expression, etc. We obtain
$$\frac{1}{\sqrt{10}}|00\rangle + \frac{2}{\sqrt{10}}|01\rangle + \frac{1}{\sqrt{10}}|10\rangle + \frac{2}{\sqrt{10}}|11\rangle.$$

4. The state $|\phi_3\rangle$ is entangled, yes. To see this, note that the probability of measuring a 1 in the second qubit is higher if a 0 is measured in the first qubit, i.e. they are not independent. If you prefer an algebraic solution, one sets

$$a_1b_1 = \frac{1}{\sqrt{10}}, \quad a_1b_2 = \frac{2}{\sqrt{10}}, \quad a_2b_1 = \frac{2}{\sqrt{10}}, \quad a_2b_2 = \frac{1}{\sqrt{10}}.$$

Then, one tries to find a solution. But, from the first two equations, $b_2 = 2b_1$. From the last two, $b_1 = 2b_2$. The only solution, then, would appear to require $b_1 = 0 = b_2$ which clearly isn't a solution.

5. On the basis $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, the CNOT gate has the matrix form

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Therefore, applied to the state given above,

$$|\phi_3\rangle = \frac{1}{\sqrt{10}}|00\rangle + \frac{2}{\sqrt{10}}|01\rangle + \frac{1}{\sqrt{10}}|10\rangle + \frac{2}{\sqrt{10}}|11\rangle.$$

Remark: Note that this state is not entangled (it's one we saw above).

5 Question 5

Suppose you are trying to factor $N = 899$ using Shor's algorithm. You use a quantum computer with 20 qubits. You try $\alpha = 5$. When you make the final measurement in the first register, you get an answer of $y = 424423$.

Explain how the rest of Shor's algorithm works, i.e. demonstrate the steps to determine the non-trivial factor of N from this information. For credit, you must do this according to Shor's algorithm[1].

Because this involves some computation, I provide you with a list of what you may use a calculator and/or computer for:

1. multiplication, addition, and subtraction of integers,
2. division of integers with remainder,
3. at most ONE gcd computation,
4. at most ONE modular exponentiation.

You may not use a computer or calculation aid for anything other than what is listed above. Also, when I say "at most one," I mean that your solution should depend on at most one modular exponentiation, and at most one gcd computation. If you get it wrong and need to do another in scratchwork, that's fine. But the final writeup must depend upon only one of each.[2]

All that being said, the amount of computation required on this problem is within the scope of doing by hand. It would just be mildly tedious and prone to error. The computation required is *not* insane here. I just don't trust you to divide 7-digit numbers.

Solutions.

From the information given, you must take the continued fraction expansion of $y/2^{20} = 424423/1048576$. You can do this as follows:

$$\frac{424423}{1048576} = \frac{1}{\frac{1048576}{424423}} = \frac{1}{2 + \frac{199730}{424423}} = \frac{1}{2 + \frac{1}{\frac{424423}{199730}}} = \frac{1}{2 + \frac{1}{2 + \frac{24963}{199730}}} = \frac{1}{2 + \frac{1}{2 + \frac{1}{\frac{199730}{24963}}}} = \frac{1}{2 + \frac{1}{2 + \frac{1}{8 + \frac{26}{24963}}}}$$

Stopping at this point, we can compute the partial convergents:

$$\frac{1}{2}, \quad \frac{1}{2 + \frac{1}{2}}, \quad \frac{1}{2 + \frac{1}{2 + \frac{1}{8}}}$$

Or, simplified,

$$\frac{1}{2}, \quad \frac{2}{5}, \quad \frac{17}{42}.$$

The denominator 42 is even, so it is a good candidate for r. We compute

$$\alpha^{r/2} \equiv 5^{21} \equiv 869 \pmod{899}.$$

Finally, we take a gcd,

$$\gcd(869 - 1, 899) = 31.$$

(Some students will take $\gcd(869 + 1, 899) = 29$, which is the other non-trivial factor.)

[1] No credit for just trial-dividing N to factor it... I already know this is a non-realistic example!

[2] The point of this is to prevent you from just doing an exhaustive computer search of some sort that factors N in some way unrelated to Shor's algorithm. You won't receive credit for other methods, anyway. But this way the problem emphasizes the fact that the final classical phase of Shor's algorithm is polynomial-time. Exhaustive search methods would not be polynomial-time.