Ph/CS 219b

Exercises
Due: Thursday 25 January 2018

1.1 More CSS codes

We've seen how to construct the [7,4,3] Hamming code, and its [7,3,4] dual code. From this pair of classical linear codes we constructed a [[7,1,3]] Calderbank-Shor-Steane (CSS) quantum code.

a) Using a similar method as in the construction of the [7,4,3] code, construct a [15,11,3] classical linear code, and find its dual code. From this pair of classical codes, show that a [[15,7,3]] CSS quantum code can be constructed.

b) Generalizing further, construct a $[[n, k, 3]]$ CSS code, where $n = 2^m - 1$, $k = n - 2m$, and $m \geq 3$ is an integer.

1.2 Hamming's hat game

Consider the following game with n players. For each player, a flip of a fair coin determines whether that player wears a red hat or a blue hat, but the player cannot see the color of her own hat. Then all the players enter a room, so that each player can see the hat color of the other $n-1$ players, but still not her own.

Now, all players make simultaneous moves, without knowing the moves made by the other players. In a move, each player either guesses the color of her own hat, or says "pass." It at least one player correctly guesses her own hat color, and no players guess wrong, then all the players win. But if at least one player guesses wrong, or all players pass, then they all lose.

The players are allowed to confer before the game begins, and decide on a strategy, before the hat colors are determined. Here is one possible strategy. One of the n players is designated team captain. In each round of the game, the captain guesses his hat is red, and all other players pass. With this strategy, the players will win with probability 1/2, averaging uniformly over the outcomes of the coin flips. Is there a better strategy that allows them to win with higher probability?

One might argue as follows. The hat colors of the players are completely uncorrelated, because the n coin flips are independent. Therefore looking at the other $n-1$ hats provides no useful information about one's own hat color. Thus no player can guess his hat color with probability of success better than 1/2 and the above strategy is optimal.

We can see that this reasoning is wrong by exhibiting a better strategy. Consider the version of the game with $n = 3$ players. Suppose that each player looks at the hats of the other two players. If she sees two hats of different colors, she passes. If she sees two hats of the same color, then she guesses that her hat is the opposite color.

This strategy succeeds if two of the three hats are the same color, and the third hat is a different color. In that case, two players will pass, and the one who guesses will guess correctly. The strategy fails if all three hats have the same color. In that case all three players guess incorrectly.

Now, of the 8 possible choices for the three hat colors, there are 2 such that all three hats are the same color, and 6 such that one hat is a different color than the other two. Since all 8 choices are equiprobable, this means that the players win the game with probability 3/4, which is greater than 1/2.

Note, though, that the expected number of right guesses is the same as the expected number of wrong guesses. In the winning rounds, which occur with probability 3/4, only one player guesses and that guess is correct. In the losing rounds, which occur with probability 1/4, all three players guess incorrectly. Therefore, these expected number of right guesses per round is 3/4, and the expected number of wrong guesses is also 3/4. In this sense, we were correct to suspect that right and wrong guesses are equally likely. Nevertheless, winning with probability greater than 1/2 is possible with this strategy, because there are multiple wrong guesses in the losing rounds, and just one right guess in the winning rounds.

Thinking more deeply about this strategy, we recognize the structure of an underlying error-correcting code, namely the three-bit repetition code for which RRR and BBB are valid codewords, where R denotes a red hat and B denotes a blue hat. Each player, after observing the other two hats, asks herself whether it is possible to choose her own hat color so that the three hat colors define a valid codeword. If not she passes; if so she guesses that her own hat color is such that the three hat colors are not a valid codeword. This strategy fails only if the players are dealt a valid codeword, which occurs with probability 1/4.

a) Now consider the version of the game with $n = 7$ players. Find a strategy that wins the game with probability 7/8 and prove that it works. **Hint**: The title of this problem is a clue.

b) Generalize this strategy to the case $n = 2^m - 1$, where $m \geq 2$ is an integer. What probability of winning can be achieved?

1.3 Polynomial CSS codes

Consider a *pit* that takes the p possible values $\{0, 1, 2, \ldots, p-1\}$, where p is prime. The set $\{0, 1, 2, \ldots, p-1\}$ can be regarded as a finite field $\mathbb{F}_p$ with addition and multiplication defined modulo p; $\mathbb{F}_p$ is a field because each nonzero element has a multiplicative inverse.

In this exercise, you will study the properties of a family of quantum codes for *qupits* (p-level quantum systems). These quantum codes are related to linear classical codes that are vector spaces over the field $\mathbb{F}_p$. We will refer to the quantum codes as *polynomial CSS codes*.

Let $x_0, x_1, \ldots x_{n-1}$ (where $n \leq p$) be specified distinct elements of $\mathbb{F}_p$, and consider a classical code C_1 that contains all strings of n elements of $\mathbb{F}_p$ of the form

$$\Big(f(x_{n-1}), f(x_{n-2}) \ldots, f(x_2), f(x_1), f(x_0)\Big) \ , \tag{1}$$

where $f(x)$ is a polynomial of degree at most m with coefficients in $\mathbb{F}_p$. (The code depends on how the elements $x_0, x_1, \ldots x_{n-1}$ of $\mathbb{F}_p$ are chosen. Different codewords within the code are obtained by varying the polynomial f.)

a) Show that C_1 is a vector space over $\mathbb{F}_p$.

b) The *weight* of a vector in $\mathbb{F}_p^n$ is the number of nonzero components of the vector, and the *distance* of a linear code is the minimum weight of a nonzero vector in the code. Show that the distance d_1 of C_1 satisfies

$$d_1 \geq n - m \ . \tag{2}$$

[**Hint:** A nonzero polynomial $f(x)$ of degree m has at most m zeros over the field $\mathbb{F}_p$.]

Now let C_2 be the subcode of C_1 such that $f(x)$ has degree at most $m-1$.

c) Show that C_2 is a vector space over $\mathbb{F}_p$, and a subspace of C_1.

d) Suppose that $\{z_1, z_2, \ldots, z_m\}$ are distinct elements of $\mathbb{F}_p$, and that $\{y_1, y_2, \ldots, y_m\}$ are arbitrary elements of $\mathbb{F}_p$ (not necessarily distinct). Show that there is a polynomial $f(x)$ of degree less than m such that

$$\begin{aligned} f(z_1) &= y_1 \ , \\ f(z_2) &= y_2 \ , \\ &\cdot \\ &\cdot \\ f(z_m) &= y_m \ . \end{aligned} \tag{3}$$

[**Hint:** It is easy to construct such a polynomial $f(x)$ explicitly.]

e) The code $C_2^\perp$ *dual* to C_2 contains all vectors in $\mathbb{F}_p^n$ that are orthogonal to all vectors in C_2. Show that the distance d_2 of $C_2^\perp$ satisfies

$$d_2 \geq m+1 \ . \tag{4}$$

[**Hint:** Choose any m components of the n-component C_2 codewords, and consider the corresponding projection of C_2 into $\mathbb{F}_p^m$. Using the result of (d), show that the image of C_2 under this projection is all of $\mathbb{F}_p^m$. Conclude that any vector orthogonal to all vectors in C_2 must have weight at least $m+1$.]

f) Now consider a quantum error-correcting code of the CSS type, based on the codes C_1 and $C_2 \subset C_1$. We can choose a basis for the code space such that each element of the basis is a uniform superposition of all C_1 codewords that belong to the same C_2 coset. What is the number of encoded qupits? (How many distinct C_2 cosets are contained in C_1?)

g) A CSS code can correct t errors if $d_1 \geq 2t+1$ and $d_2 \geq 2t+1$. Explain how to construct polynomial CSS codes that encode one qupit, correct t errors, and have block size $4t+1$. For what values of p can such codes be constructed?

1.4 Generating the Clifford Group

Recall that the n-qubit *Pauli group* is defined as

$$\mathcal{P}_n = \{\boldsymbol{I}, \boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}\}^{\otimes n} \times \{\pm 1, \pm i\} \tag{5}$$

where $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}$ are the 2×2 Pauli matrices. That is, each element of $\mathcal{P}_n$ is (up to an overall phase $\pm 1, \pm i$) a tensor product of Pauli matrices and identity matrices acting on the n qubits. The n-qubit *Clifford group* $\mathcal{C}_n$ is the *normalizer* of the Pauli group – a unitary operator $\boldsymbol{U}$ acting on n qubits is contained in $\mathcal{C}_n$ iff

$$\boldsymbol{U}\boldsymbol{M}\boldsymbol{U}^{-1} \in \mathcal{P}_n \text{ for each } \boldsymbol{M} \in \mathcal{P}_n \ . \tag{6}$$

That is, $\boldsymbol{U}$ acting by conjugation takes a tensor product of Pauli matrices to a tensor product of Pauli matrices. Actually, an element of the Clifford group is defined as this action by conjugation, so that the overall phase of $\boldsymbol{U}$ is not relevant.

In this exercise, you will show that the Clifford group can be generated by three quantum gates: the single-qubit gates $\boldsymbol{H}$ and $\boldsymbol{S}$, and the two-qubit gate CNOT$= \Lambda(\boldsymbol{X})$. Here $\boldsymbol{H}$ denotes the Hadamard gate

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{7}$$

(a rotation by π about the axis $\hat{x} + \hat{z}$), and $\boldsymbol{S}$ denotes the phase gate

$$\boldsymbol{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{8}$$

(a rotation by $\pi/2$ about the $\hat{z}$ axis). It follows that quantum circuits constructed from these gates can be efficiently simulated by a classical computer, because the action of $\mathcal{C}_n$ on $\mathcal{P}_n$ can be succinctly described and easily updated after each gate.

a) Compute how $\boldsymbol{H}$, $\boldsymbol{S}$, and $\Lambda(\boldsymbol{X})$ act on Pauli operators by conjugation, and verify that $\boldsymbol{H}$ and $\boldsymbol{S}$ are in $\mathcal{C}_1$ and that $\Lambda(\boldsymbol{X})$ is in $\mathcal{C}_2$.

b) Show that $\boldsymbol{H}$ and $\boldsymbol{S}$ generate $\mathcal{C}_1$. [**Hint**: Note that the elements of the one-qubit Clifford group are the permutations of $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}$, with minus signs appropriately chosen so that the product $\boldsymbol{X}\boldsymbol{Y}\boldsymbol{Z} = i\boldsymbol{I}$ remains invariant.]

c) Let $\Lambda(\boldsymbol{\sigma})$ denote the two-qubit gate that applies $\boldsymbol{\sigma}$ to the target qubit if the control qubit is $|1\rangle$, and acts trivially if the control qubit is $|0\rangle$. Let $\boldsymbol{\sigma}_j$ denote $\boldsymbol{\sigma}$ acting on qubit j. Show that $\Lambda(\boldsymbol{Z})$ and $\Lambda(\boldsymbol{Y})$ can be constructed from $\Lambda(\boldsymbol{X})$, $\boldsymbol{H}$, and $\boldsymbol{S}$. Show that

$$\Lambda(\boldsymbol{\sigma})\boldsymbol{Z}_1\Lambda(\boldsymbol{\sigma}) = \boldsymbol{Z}_1, \quad \Lambda(\boldsymbol{\sigma})\boldsymbol{X}_1\Lambda(\boldsymbol{\sigma}) = \boldsymbol{X}_1\boldsymbol{\sigma}_2 \ , \tag{9}$$

where qubit 1 is the control of the $\Lambda(\boldsymbol{\sigma})$ and qubit 2 is its target. Here $\boldsymbol{\sigma}$ is one of $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}$, so that in particular $\boldsymbol{\sigma}^2 = \boldsymbol{I}$.

We will prove that $\boldsymbol{H}$, $\boldsymbol{S}$, and $\Lambda(\boldsymbol{X})$ generate $\mathcal{C}_n$ by induction. We have already shown (*b*). Now assume, as an inductive hypothesis, that $\boldsymbol{H}$, $\boldsymbol{S}$, and $\Lambda(\boldsymbol{X})$ generate $\mathcal{C}_n$. We need to show that they generate $\mathcal{C}_{n+1}$.

d) Suppose that $\boldsymbol{U}$ is an element of $\mathcal{C}_{n+1}$. Show that there is a $\boldsymbol{W}$ generated by $\boldsymbol{H}$, $\boldsymbol{S}$, and $\Lambda(\boldsymbol{X})$ such that the action of $\boldsymbol{WU}$ by conjugation is

$$\begin{aligned} \boldsymbol{WU}: \quad \boldsymbol{X}_1 &\to \boldsymbol{X}_1\boldsymbol{M} \\ \boldsymbol{Z}_1 &\to \boldsymbol{Z}_1\boldsymbol{N} \ . \end{aligned} \tag{10}$$

where each of $\boldsymbol{M}, \boldsymbol{N}$ is a tensor product of Pauli matrices acting on qubits 2 through $n+1$.

e) Now consider

$$\boldsymbol{V} \equiv \Lambda(\boldsymbol{M})\boldsymbol{H}_1\Lambda(\boldsymbol{N})\boldsymbol{H}_1\boldsymbol{WU} \ , \tag{11}$$

where $\Lambda(\boldsymbol{M})$ denotes the transformation controlled by the first qubit that applies $\boldsymbol{M}$ to the other n qubits, and similarly for $\Lambda(\boldsymbol{N})$. Note that $\Lambda(\boldsymbol{M})$ and $\Lambda(\boldsymbol{N})$ can be constructed from $\boldsymbol{H}$, $\boldsymbol{S}$, and $\Lambda(\boldsymbol{X})$. It follows from (*c*) that the action of $\Lambda(\boldsymbol{M})$ by conjugation is

$$\begin{aligned} \Lambda(\boldsymbol{M}): \quad \boldsymbol{X}_1 &\to \boldsymbol{X}_1\boldsymbol{M} \\ \boldsymbol{Z}_1 &\to \boldsymbol{Z}_1 \ . \end{aligned} \tag{12}$$

Show that the action of $\boldsymbol{V}$ by conjugation is

$$\begin{aligned} \boldsymbol{V}: \quad \boldsymbol{X}_1 &\to \boldsymbol{X}_1 \\ \boldsymbol{Z}_1 &\to \boldsymbol{Z}_1 \ . \end{aligned} \tag{13}$$

f) Show that $\boldsymbol{V}$ is in $\mathcal{C}_n$, and therefore can be constructed from $\boldsymbol{H}$, $\boldsymbol{S}$, and $\Lambda(\boldsymbol{X})$. Show that $\boldsymbol{U}$ can also be constructed from $\boldsymbol{H}$, $\boldsymbol{S}$, and $\Lambda(\boldsymbol{X})$. This completes the inductive step, and the proof.