PCMI topological aspects of quantum codes, problem session #1

Instructor: Jeongwan Haah, Teaching Assistant: John Bostanci

1. **(CSS code cleaning lemma.)** Prove a CSS code cleaning lemma: Let $\mathcal{S}$ be a CSS code over n qubits and $M \subset \Lambda$ be a subset of qubits such that every operator supported only on M is not a non-trivial logical X operator. Then there exists a choice of representatives of all logical Z operators such that the representatives are supported on $\Lambda \setminus M$.

   Solution: We are going to proceed by dimension counting. Since we are only dealing with X-type operators, take $\mathcal{P}_X$ as the n-dimensional vector space over $\mathbb{F}_2$, and $\mathcal{S}_Z$ to be the subspace corresponding to the Z-stabilizers of $\mathcal{S}$. Then consider the following direct sum decomposition of $\mathcal{S}$:

   $$\mathcal{S}_Z = \mathcal{S}_M \oplus \mathcal{S}_{\Lambda\setminus M} \oplus \mathcal{S}' .$$

   Here $\mathcal{S}_M$ and $\mathcal{S}_{\Lambda\setminus M}$ are the subspace of operators supported only on M and $\Lambda \setminus M$ respectively, and $\mathcal{S}'$ is whatever is left. I am dropping the subscript Z here.

   The logical Pauli X operators correspond exactly to the orthogonal subspace of $\mathcal{S}_Z$, which we will denote $\mathcal{S}^{\perp}$. We can denote by $\mathcal{S}^{\perp}_M$ the subspace of these operators that are supported only on M, and similarly for $\mathcal{S}^{\perp}_{\Lambda\setminus M}$. Note that this is *not* the same as the operators that commute with $\mathcal{S}_M$. Now consider the set of operators $\mathcal{S}^{\perp}_M$. We claim the following:

   $$\dim(\mathcal{S}^{\perp}_M) = |M| - \dim(\mathcal{S}_M) - \dim(\mathcal{S}') .$$

   Imagine building out an $n \times n$ matrix, starting with the first rows being $\mathcal{S}_Z$. When we complete the other rows of the matrix, the last few (those are aren't in the rows corresponding to $\mathcal{S}_Z$) will be logical Pauli's, the question now becomes how many of those rows will we have when we cut out the $\Lambda \setminus M$ columns. We started with n rows, and recall that $\dim(\mathcal{S}_{\Lambda\setminus M})$ of them correspond to stabilizers that are supported outside of M, so those become 0 when we remove the rows (and thus don't count towards restricting $\mathcal{S}^{\perp}_M$). Further note that $\mathcal{S}'|_M$ is distinct from $\mathcal{S}_M$, otherwise we could multiply operators from $\mathcal{S}'|_M$ by operators from $\mathcal{S}_M$ to get an operator in $S_{\Lambda\setminus M}$, which means the original operator would be in the direct sum of the two other sets (a contradiction with how we defined the decomposition). Thus, we start with $|M|$-dimensional vectors, and have to remove $\dim(\mathcal{S}_M)$ and $\dim(\mathcal{S}')$ of them to account for the fact that they must commute with those two sets.

   Now we bring in our assumption: the dimension of the set $\mathcal{S}^{\perp}_M$ is actually 0, because there are no non-trivial X-type logical Pauli's. Thus, we have

   $$\dim(\mathcal{S}_M) + \dim(\mathcal{S}') = |M|$$

   . To wrap the argument up, note that the dimension of logical X Pauli's supported on $\Lambda \setminus M$ is, more simply, given by

   $$|\Lambda \setminus M| - \dim(\mathcal{S}_{\Lambda\setminus M}) = n - |M| - \dim(\mathcal{S}_{\Lambda\setminus M}) , \tag{1}$$

because those operators have to be supported in the set, and commute with the stabilizer. Finally, let n_X be the dimension of logical X operators, then

$$n - n_X = \dim(\mathcal{S}_M) + \dim(\mathcal{S}') + \dim(\mathcal{S}_{\Lambda \setminus M}) \, .$$

Rearranging, we get

$$\dim(\mathcal{S}_{\Lambda \setminus M}) = n - n_X - |M| \, .$$

Substituting into eq. (1), we get that the number of logical X operators supported only on $\Lambda \setminus M$ is given by

$$n - |M| - n - n_X - |M| = n_X \, .$$

Thus, a full set of logical X operators is supported in $\Lambda \backslash M$.

2. **(Finishing up the quantum Singleton bound.)** In the proof of the quantum Singleton bound, show that for two parties that share a bipartite state ρ_{AB}, if for all pairs of Hermitian operators $O_{\mathsf{A}} \otimes \mathrm{id}_{\mathsf{B}}, \mathrm{id}_{\mathsf{A}} \otimes O_{\mathsf{B}}$,

$$\mathrm{Tr}((O_{\mathsf{A}} \otimes O_{\mathsf{B}})\rho_{\mathsf{AB}}) = \mathrm{Tr}((O_{\mathsf{A}} \otimes \mathrm{id}_{\mathsf{B}})\rho_{\mathsf{AB}}) \cdot \mathrm{Tr}((\mathrm{id}_{\mathsf{A}} \otimes O_{\mathsf{B}})\rho_{\mathsf{AB}}), \tag{2}$$

then their mutual information is 0.

Solution: Recall that the mutual information is given by

$$I(A;B) = H(A) - H(A|B) \, ,$$

where $H(A)$ is the Shannon entropy of the random variable. Thus, we just need to show that $H(A|B) = H(A)$, but we know that

$$\begin{aligned} \mathbf{Pr}[A = a | B = b] &= \frac{\mathbf{Pr}[A = a \ \ \& \ \ B = b]}{\mathbf{Pr}[B = b]} \\ &= \frac{\mathbf{Pr}[A = a]\mathbf{Pr}[B = b]}{\mathbf{Pr}[B = b]} \\ &= \mathbf{Pr}[A = a] \, . \end{aligned}$$

Thus when we compute the conditional entropy, we will get the same number, and the mutual information will be 0.

3. **(Subadditivity and Nonnegativity.)** Recall the definition of the von Neumann entropy, $S(\rho) = -\mathrm{Tr}(\rho \ln \rho) = -\sum_j \lambda_j \ln(\lambda_j)$, where λ_j is the j'th eigenvalue of ρ, let ρ_{AB} be a density matrix over registers A and B. Show that the Von Neumann entropy satisfies

$$S(\rho_{\mathsf{AB}}) \leq S(\rho_{\mathsf{A}}) + S(\rho_{\mathsf{B}}).$$

Solution: We first show that for two states $\rho = \sum_i p_i |v_i\rangle\langle v_i|$ and $\sigma = \sum_j q_j |w_j\rangle\langle w_j|$,

$$\begin{aligned} S(\rho \otimes \sigma) &= S(\sum_{i,j} p_i q_j |v_i w_j\rangle\langle v_i w_j|) \\ &= -\sum_{i,j} p_i q_j \ln(p_i q_j) \\ &= -\sum_{i,j} p_i q_j \ln(p_i) - \sum_{i,j} p_i q_j \ln(q_j) \\ &= S(\rho) + S(\sigma)\,. \end{aligned}$$

Here the last line uses the fact that p_i and q_j sum to 1. To prove the theorem, we consider the following

$$\begin{aligned} 0 &\leq S(\rho_{\mathsf{AB}} \| \rho_{\mathsf{A}} \otimes \rho_{\mathsf{B}}) \\ &= \mathrm{Tr}(\rho_{\mathsf{AB}}(\ln(\rho_{\mathsf{A}} \otimes \rho_{\mathsf{B}}) - \ln(\rho_{\mathsf{AB}})) \\ &= S(\rho_{\mathsf{AB}}) - \mathrm{Tr}(\rho_{\mathsf{AB}}(\ln(\rho_{\mathsf{A}} \otimes \rho_{\mathsf{B}}))) \\ &= S(\rho_{\mathsf{AB}}) - \mathrm{Tr}(\rho_{\mathsf{AB}}(\ln(\rho_{\mathsf{A}}) \otimes \mathrm{id}_{\mathsf{B}} + \mathrm{id}_{\mathsf{A}} \otimes \ln(\rho_{\mathsf{B}}))) \\ &= S(\rho_{\mathsf{AB}}) - S(\rho_{\mathsf{A}}) - S(\rho_{\mathsf{B}})\,. \end{aligned}$$

The first 3 lines are the definition of the quantum relative entropy, and rearranging terms. Then we apply the identity $\ln(\rho \otimes \sigma) = \ln(\rho) \otimes \mathrm{id} + \mathrm{id} \otimes \ln(\sigma)$. Then we use the fact that for two states ρ and σ, $\mathrm{Tr}(\rho_{\mathsf{AB}}(\sigma_{\mathsf{A}} \otimes \mathrm{id}_{\mathsf{B}})) = \mathrm{Tr}(\rho_{\mathsf{A}}\sigma_{\mathsf{A}})$.

4. **(Codes on non-orientable surfaces.)** We have bounded the number of logical qubits on any code defined on a two-dimensional torus by dividing the torus into three regions, two of which are correctable. Each correctable region is a union of two disk-like regions where the r-neighborhood of any one of the disk-like regions is also disk-like. Under the same assumption on correctable regions, bound the number of logical qubits of codes on $\mathbb{R}P^2$. Can you generalize it to higher demigenus nonorientable surfaces?

3 Hint: You may assume that the quantum relative entropy, defined below, is always non-negative:

$$S(\rho\|\sigma) = \mathrm{Tr}(\rho(\ln\sigma - \ln\rho)).$$

4 Hint: A region does not have to be the union of two subregions. There can be more.