CS 593/MA 592 - Intro to Quantum Computation
Homework 8

Due Friday, April 26 at 8pm (upload to Brightspace)

This is the last homework of the semester. It is "quasi-optional." This means that you don't have to do it, but there are some reasons you might want to:

- You can use this assignment to replace a previous assignment. For example, if you didn't submit an old assignment, or you did poorly on one, you can use your score on this one to replace that old score.
- Acing this assignment is a requirement if you want an A+ in the course. Some of you have been doing very well on all of the requirements in the class, but if you want an A+, then I am requiring you to do this assignment (and ace it). If you don't do this assignment, then the highest grade you can expect to earn is an A, although not doing it won't otherwise affect your grade.

And to reiterate: you are still allowed to submit your solutions in teams of two.

The assignment consists of just one long problem, which will have you work through the structure of *CSS (Calderbank-Shor-Steane) codes*, a special subclass of Pauli stabilizer codes. CSS codes are the most popular codes that people like to (try to!) implement on current quantum computers. The toric code is a special case, and the results of this problem can be easily used to rederive the calculations I did in class for toric code.

1. A *CSS code* is a Pauli stabilizer code generated by a set of stabilizers with the property that each is either "pure X" or "pure Z." To this end, let $A = \{(\vec{x}_1, \vec{0}), \ldots, (\vec{x}_l, \vec{0})\} \subset \mathbb{F}_2^n \oplus \mathbb{F}_2^n$ and $B = \{(\vec{0}, \vec{z}_1), \ldots, (\vec{0}, \vec{z}_k)\} \subset \mathbb{F}_2^n \oplus \mathbb{F}_2^n$, and define

$$S = S(A, B) := \{X(\vec{x}_i), Z(\vec{z}_j) \mid (\vec{x}_i, \vec{0}) \in A, (\vec{0}, \vec{z}_j) \in B\}.$$

In this exercise, we will establish fairly explicit formulas for the distance and number of logical qubits for the stabilizer code

$$\mathcal{C}_S = \left\{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \mid s|\psi\rangle = |\psi\rangle,\ s \in S\right\}.$$

   (a) By a minor abuse of notation, let A denote the $n \times l$ matrix (with entries in $\mathbb{F}_2 = \{0, 1\}$) whose i^{th} column is $\vec{x}_i$, where $(\vec{x}_i, \vec{0}) \in A$. Similarly, let B denote the $n \times k$ matrix whose j column is $\vec{z}_j$, where $(\vec{0}, \vec{z}_j) \in B$.[1]

   Show that $\mathcal{C}_S \neq \{\vec{0}\}$ is a non-trivial subspace of $(\mathbb{C}^2)^{\otimes n}$ if and only if $B^T A = 0$ if and only if $A^T B = 0$.

   [Hint: remember, I explained in class that $\mathcal{C}_S \neq \{\vec{0}\}$ if and only if $-1 \notin \langle S \rangle \leq G_n$, where G_n is the Pauli group on n qubits. You need to think through what our choice of stabilizer generators has to do with the symplectic inner product.]

   For the rest of the problem, let us assume that $B^T A = 0$.

[1] These are essentially quantum parity check matrices, if that terminology is familiar to you.

(b) Let $X = \operatorname{span} A \leq \mathbb{F}_2^n \oplus \mathbb{F}_2^n$, $Z = \operatorname{span} B \leq \mathbb{F}_2^n \oplus \mathbb{F}_2^n$, and $W = \operatorname{span} A \cup B = X \oplus Z \leq \mathbb{F}_2^n \oplus \mathbb{F}_2^n$. Show that $W^\perp = X^\perp \cap Z^\perp$.

Note: as should be expected, for a subspace $V \leq \mathbb{F}_2^n \oplus \mathbb{F}_2^n$, the notation $V^\perp$ means the symplectic complement. That is

$$V^\perp = \{(\vec{a}, \vec{b}) \in \mathbb{F}_2^n \oplus \mathbb{F}_2^n \mid \omega((\vec{a}, \vec{b}), (\vec{v}_1, \vec{v}_2)) = 0, \quad (\vec{v}_1, \vec{v}_2) \in V\}$$

where

$$\omega((\vec{a}, \vec{b}), (\vec{v}_1, \vec{v}_2)) = \vec{a} \cdot \vec{v}_2 + \vec{b} \cdot \vec{v}_1 \mod 2.$$

(c) Recall that the *symplectic weight* $wt((\vec{x}, \vec{z}))$ of a vector $(\vec{x}, \vec{z}) = ((x_1, \ldots, x_n), (z_1, \ldots, z_n)) \in \mathbb{F}_2^n \oplus \mathbb{F}_2^n$ is the number of nonzero columns of the matrix

$$\begin{pmatrix} x_1 & \cdots & x_n \\ z_1 & \cdots & z_n \end{pmatrix}.$$

Show

$$\begin{aligned} \min_{(\vec{x},\vec{z}) \in W^\perp - W} wt((\vec{x}, \vec{z})) &= \min \left\{ \min_{(\vec{x},\vec{0}) \in W^\perp - W} |\vec{x}|, \min_{(\vec{0},\vec{z}) \in W^\perp - W} |\vec{z}| \right\} \\ &= \min \left\{ \min_{\vec{x} \in \ker B^T - \operatorname{im} A} |\vec{x}|, \min_{\vec{z} \in \ker A^T - \operatorname{im} B} |\vec{z}| \right\} \end{aligned}$$

where $|\vec{x}|$ is the usual Hamming weight of a vector in $\mathbb{F}_2^n$.

(d) Show

$$W^\perp = \left(\ker B^T \oplus \{\vec{0}\}\right) + \left(\{\vec{0}\} \oplus \ker A^T\right)$$

and use this to show

$$W^\perp / W = \frac{X^\perp \cap Z^\perp}{X + Z} = \frac{\left(\ker B^T \oplus \{\vec{0}\}\right) + \left(\{\vec{0}\} \oplus \ker A^T\right)}{\left(\operatorname{im} A \oplus \{\vec{0}\}\right) + \left(\{\vec{0}\} \oplus \operatorname{im} B\right)} \cong \frac{\ker B^T}{\operatorname{im} A} \oplus \frac{\ker A^T}{\operatorname{im} B}$$

(e) Show

$$\dim \left(\frac{\ker B^T}{\operatorname{im} A} \right) = \dim \left(\frac{\ker A^T}{\operatorname{im} B} \right).$$

(f) Conclude that the number of logical qubits in $\mathcal{C}_S$ is

$$\frac{1}{2} \dim W^\perp / W = \dim \left(\frac{\ker B^T}{\operatorname{im} A} \right).$$

That concludes the problem. What follows is for your enjoyment.

We can summarize/interpret the results of this problem as follows: part (a) shows that a CSS code on n qubits (together with a choice of generators for it) is essentially the same thing as matrices A and B such that the composition

$$\mathbb{F}_2^l \xrightarrow{A} \mathbb{F}_2^n \xrightarrow{B^T} \mathbb{F}_2^k$$

is $B^T A = 0$. In algebraic topology, this would be called a "chain complex of based vector spaces over $\mathbb{F}_2$." Such things can be found in many places, thanks to the following: any choice of a positive integer k and "CW complex" Δ gives rise to one, by looking at the cellular chain complex (with $\mathbb{F}_2$ coefficients) in dimension k:

$$C_{k+1}^{cellular}(\Delta; \mathbb{F}_2) \xrightarrow{\partial} C_k^{cellular}(\Delta; \mathbb{F}_2) \xrightarrow{\partial} C_{k-1}^{cellular}(\Delta; \mathbb{F}_2)$$

Part (f) shows that the number of logical qubits is exactly the rank of the homology of the chain complex. Part (c), roughly, shows that the distance of the code is determined by identifying the smallest Hamming weight representative of any non-trivial homology class. More precisely, we have to find the minimum weight we see among the non-trivial homology classes in the above chain complex, as well as in the dual cochain complex

$$C^{k+1}_{cellular}(\Delta;\mathbb{F}_2) \xleftarrow{\delta} C^{k}_{cellular}(\Delta;\mathbb{F}_2) \xrightarrow{\delta} C^{k-1}_{cellular}(\Delta;\mathbb{F}_2)$$

If this sounds interesting to you, then you should take MA 572 - Algebraic Topology!

As far as current state of the art: as of roughly 2020, "good quantum LDPC codes" are now known to exist. LD means "low-density" and PC means "parity check" (a synonym for CSS). More precisely, this means there exists an infinite family of CSS codes with generators $(A_n, B_n)_{n\in\mathbb{N}}$ with the following properties:

- the n^{th} code uses $O(n)$ many physical qubits
- the columns of the matrices A_n and B_n have $O(1)$ many non-zero entries ("low-density")
- there are $\theta(n)$ many logical qubits.
- the distance is $\theta(n)$.

The last two properties are why the codes are called "good."