Homework 3 Solutions

E2-210, Jan–Apr 2025

1. Show that the set of Pauli matrices $\{X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \{0,1\}^n\}$ is an orthonormal basis for the vector space, $\mathbb{C}^{N\times N}$, of $N \times N$ complex matrices, under the Hilbert-Schmidt inner product: $(A, B) \stackrel{\text{def}}{=} \frac{1}{N}\operatorname{tr}(A^\dagger B)$. (Here, as usual $N = 2^n$.)

   Solution: Recall that $X(\mathbf{a})Z(\mathbf{b})$ denotes the Pauli operator $M_1 \otimes M_2 \otimes \cdots \otimes M_n$, with

   $$M_j = \begin{cases} I & \text{if } (a_j, b_j) = (0,0) \\ X & \text{if } (a_j, b_j) = (1,0) \\ Y & \text{if } (a_j, b_j) = (1,1) \\ Z & \text{if } (a_j, b_j) = (0,1) \end{cases}$$

   In particular, if $M = X(\mathbf{a})Z(\mathbf{b})$, then $M^\dagger = M$.

   Now, consider any pair of Pauli matrices $M = X(\mathbf{a})Z(\mathbf{b})$ and $M' = X(\mathbf{a}')Z(\mathbf{b}')$ with $(\mathbf{a}, \mathbf{b}) \neq (\mathbf{a}', \mathbf{b}')$. Recall that MM' is, up to a phase factor, equal to $X(\mathbf{a} \oplus \mathbf{a}')Z(\mathbf{b} \oplus \mathbf{b}')$. Since $(\mathbf{a}, \mathbf{b}) \neq (\mathbf{a}', \mathbf{b}')$, we have $(\mathbf{a} \oplus \mathbf{a}', \mathbf{b} \oplus \mathbf{b}') \neq (\mathbf{0}, \mathbf{0})$. Hence, $X(\mathbf{a} \oplus \mathbf{a}')Z(\mathbf{b} \oplus \mathbf{b}') \neq I_N$, so that $\operatorname{tr}\big(X(\mathbf{a} \oplus \mathbf{a}')Z(\mathbf{b} \oplus \mathbf{b}')\big) = 0$. Therefore,

   $$(M, M') = \frac{1}{N}\operatorname{tr}(M^\dagger M') = \frac{1}{N}\operatorname{tr}(MM') = \frac{\text{(phase factor)}}{N}\operatorname{tr}\big(X(\mathbf{a} \oplus \mathbf{a}')Z(\mathbf{b} \oplus \mathbf{b}')\big) = 0.$$

   On the other hand, $(M, M) = \frac{1}{N}\operatorname{tr}(M^2) = \frac{1}{N}\operatorname{tr}(I_N) = 1$.

   Thus, with respect to the Hilbert-Schmidt inner product, $\{X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \{0,1\}^n\}$ is a collection of orthonormal matrices. Since the matrices are mutually orthogonal, they are linearly independent. There are $2^{2n} = N^2$ such matrices and $\dim(\mathbb{C}^{N\times N}) = N^2$, so they must form a basis of $\mathbb{C}^{N\times N}$.

2. Let G be a graph on the vertex set $[n] := \{1, 2, \ldots, n\}$ having edge set $E \subseteq \binom{[n]}{2}$. (Here, $\binom{[n]}{2}$ denotes the set of all 2-subsets of $[n]$, so that edges are certain 2-subsets of $[n]$. In particular, the graph has no self-loops, i.e., edges that connect a vertex to itself.)

   Let A be the adjacency matrix of G; this is the $n \times n$ matrix with $0/1$ entries, whose (i, j)-th entry is 1 iff $\{i, j\}$ is an edge of G. Set $H = [I \mid A]$, where I is the $n \times n$ identity matrix. Thus, H is an $n \times 2n$ matrix having rank n.

   (a) Show that the symplectic product between any pair of rows of H is 0.

Solution: Let $a_{i,j}$ denote the (i,j)-th entry of the adjacency matrix A, and let $\mathbf{a}_i = [a_{i,1}\ a_{i,2}\ \dots\ a_{i,n}]$ be the i-th row of A. Note that A is symmetric: $a_{i,j} = a_{j,i} = 1$ if the vertices i and j are connected by an edge in the graph G, and $a_{i,j} = a_{j,i} = 0$ otherwise.

The i-th row of H is of the form $[\mathbf{e}_i \mid \mathbf{a}_i]$, where $\mathbf{e}_i = [0\ \cdots\ 0\ 1\ 0\ \cdots\ 0]$ with the 1 appearing in the i-th coordinate. Thus, the symplectic product between the i-th and j-th rows of H is $\mathbf{e}_i \cdot \mathbf{a}_j - \mathbf{e}_j \cdot \mathbf{a}_i \mod 2$. This equals 0, since $\mathbf{e}_i \cdot \mathbf{a}_j - \mathbf{e}_j \cdot \mathbf{a}_i = a_{j,i} - a_{i,j} = 0$.

(b) If $\mathcal{S}$ is the stabilizer group defined by the check matrix H, what is $\dim \mathcal{Q}_{\mathcal{S}}$?

Solution: The check matrix H has rank n, so its rows correspond to n independent generators. Hence, $|\mathcal{S}| = 2^n$ and $\dim(\mathcal{Q}_{\mathcal{S}}) = 2^n/2^n = 1$. Thus, $\mathcal{Q}_{\mathcal{S}}$ is an $[[n, 0]]$ stabilizer code.

3. In this exercise, we will prove the following proposition:

Proposition: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be, respectively, $[n, k_1]$ and $[n, k_2]$ binary linear codes such that $\mathcal{C}_1^\perp \subseteq \mathcal{C}_2$. Let $A_0 := \mathcal{C}_1^\perp, A_1, \dots, A_{K-1}$ be a listing of the $K = 2^{k_1+k_2-n}$ cosets of $\mathcal{C}_1^\perp$ within $\mathcal{C}_2$. Then, the quantum states

$$|\phi_j\rangle := \frac{1}{\sqrt{2^{n-k_1}}} \sum_{\mathbf{x} \in A_j} |\mathbf{x}\rangle, \quad j = 0, 1, \dots, K-1,$$

form an orthonormal basis of the quantum code $\mathcal{Q}$ obtained via the CSS construction from $\mathcal{C}_1$ and $\mathcal{C}_2$.

(a) Show that $\langle \phi_i | \phi_j \rangle = \delta_{i,j}$.

Solution: First, note that $\langle \mathbf{x} | \mathbf{x}' \rangle = 0$ for any pair of distinct binary n-tuples $\mathbf{x}$ and $\mathbf{x}'$. To see this, write $|\mathbf{x}\rangle = |x_1 x_2 \dots x_n\rangle$ and $|\mathbf{x}'\rangle = |x_1' x_2' \dots x_n'\rangle$, with $x_1, x_i' \in \{0, 1\}$ for all i. We then have $\langle \mathbf{x} | \mathbf{x}' \rangle = \prod_{i=1}^n \langle x_i | x_i' \rangle = 0$, since for at least one index i, we have $x_i \neq x_i'$.

Now, use the fact that cosets A_i and A_j are disjoint for $i \neq j$. This means that for all $\mathbf{x} \in A_i$ and $\mathbf{x}' \in A_j$, we have $\mathbf{x} \neq \mathbf{x}'$, and hence, $\langle \mathbf{x} | \mathbf{x}' \rangle = 0$. It follows (by linearity of the inner product) that $\langle \phi_i | \phi_j \rangle = 0$ for $i \neq j$.

By similar reasoning, we have $\langle \phi_i | \phi_i \rangle = \frac{1}{2^{n-k_1}} \sum_{\mathbf{x} \in A_i} \underbrace{\langle \mathbf{x} | \mathbf{x} \rangle}_{=1} = \frac{1}{2^{n-k_1}} |A_i| = 1$, since all cosets A_i have size equal to $|\mathcal{C}_1^\perp| = 2^{n-k_1}$. □

Let H_1 and H_2 be any pair of parity-check matrices for $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, of full row-rank. Thus, H_1 and H_2 are, respectively, $(n-k_1) \times n$ and $(n-k_2) \times n$ binary matrices such that $H_1 H_2^T = \mathbf{0}$ over $\mathbb{F}_2$. By the CSS construction, the stabilizer generators are $X(\mathbf{h})$ and $Z(\mathbf{h}')$, where $\mathbf{h}$ and $\mathbf{h}'$ range over the rows of H_1 and H_2, respectively.

(b) Argue that, for any binary n-tuples $\mathbf{x}$, $\mathbf{h}$ and $\mathbf{h}'$, we have $X(\mathbf{h}) |\mathbf{x}\rangle = |\mathbf{x} \oplus \mathbf{h}\rangle$ and $Z(\mathbf{h}') |\mathbf{x}\rangle = (-1)^{\mathbf{h}' \cdot \mathbf{x}} |\mathbf{x}\rangle$. In other words, the Pauli operator $X(\mathbf{h})$ applied to $|\mathbf{x}\rangle$ yields $|\mathbf{x} \oplus \mathbf{h}\rangle$, and the Pauli operator $Z(\mathbf{h}')$ applied to $|\mathbf{x}\rangle$ yields $(-1)^{\mathbf{h}' \cdot \mathbf{x}} |\mathbf{x}\rangle$.

Solution: This is more or less by definition of the X and Z operators. Note that $X(\mathbf{h}) = \bigoplus_i X_i^{h_i}$, where X_i is the X operator acting on the ith qubit. Thus, $X(\mathbf{h}) |\mathbf{x}\rangle = \bigotimes_i X_i^{h_i} |x_i\rangle = \bigotimes_i |x_i \oplus h_i\rangle = |\mathbf{x} \oplus \mathbf{h}\rangle$.

Similarly, $Z(\mathbf{h}')\,|\mathbf{x}\rangle = \bigotimes_i Z_i^{h'_i}\,|x_i\rangle = \bigotimes_i (-1)^{h'_i x_i}\,|x_i\rangle = \left[\prod_i (-1)^{h'_i x_i}\right]|\mathbf{x}\rangle = (-1)^{\mathbf{h}'\cdot\mathbf{x}}\,|\mathbf{x}\rangle$. $\square$

(c) Show, using (b), that for any row $\mathbf{h}$ of H_1, we have $X(\mathbf{h})\,|\phi_j\rangle = |\phi_j\rangle$, and for any row $\mathbf{h}'$ of H_2, we have $Z(\mathbf{h}')\,|\phi_j\rangle = |\phi_j\rangle$.

Solution: Write the sum $\sum_{\mathbf{x}\in A_j} |\mathbf{x}\rangle$ as $\sum_{\mathbf{c}\in\mathcal{C}_1^\perp} |\mathbf{a}\oplus\mathbf{c}\rangle$, where $\mathbf{a}$ is a fixed binary vector (a "coset leader") in A_j. Then, for any row $\mathbf{h}$ of H_1, we have

$$\begin{aligned} X(\mathbf{h})\,|\phi_j\rangle &= \frac{1}{\sqrt{2^{n-k_1}}}\sum_{\mathbf{c}\in\mathcal{C}_1^\perp} X(\mathbf{h})\,|\mathbf{a}\oplus\mathbf{c}\rangle \\ &\overset{\text{by (b)}}{=} \frac{1}{\sqrt{2^{n-k_1}}}\sum_{\mathbf{c}\in\mathcal{C}_1^\perp} |\mathbf{a}\oplus\mathbf{c}\oplus\mathbf{h}\rangle \\ &= \frac{1}{\sqrt{2^{n-k_1}}}\sum_{\mathbf{c}'\in\mathcal{C}_1^\perp} |\mathbf{a}\oplus\mathbf{c}'\rangle \;=\; |\phi_j\rangle\,. \end{aligned}$$

In the last line above, we have used the fact that as $\mathbf{c}$ runs over the codewords in $\mathcal{C}^\perp$, so does $\mathbf{c}' := \mathbf{c}+\mathbf{h}$, since $\mathbf{h}$, being a row of the parity-check matrix of $\mathcal{C}_1$, is some (fixed) codeword of $\mathcal{C}_1^\perp$.

Next, for any row $\mathbf{h}'$ of H_2, we have

$$\begin{aligned} Z(\mathbf{h}')\,|\phi_j\rangle &= \frac{1}{\sqrt{2^{n-k_1}}}\sum_{\mathbf{x}\in A_j} Z(\mathbf{h}')\,|\mathbf{x}\rangle \\ &\overset{\text{by (b)}}{=} \frac{1}{\sqrt{2^{n-k_1}}}\sum_{\mathbf{x}\in A_j} (-1)^{\mathbf{h}'\cdot\mathbf{x}}\,|\mathbf{x}\rangle \\ &= \frac{1}{\sqrt{2^{n-k_1}}}\sum_{\mathbf{x}\in A_j} |\mathbf{x}\rangle \;=\; |\phi_j\rangle\,. \end{aligned}$$

In the last line above, we have used the fact that $\mathbf{h}'\in\mathcal{C}_2^\perp$ (since it is a row of a parity-check matrix of $\mathcal{C}_2$) and $\mathbf{x}\in\mathcal{C}_2$ (since it is an element of a coset of $\mathcal{C}_1^\perp$ within $\mathcal{C}_2$), so that $\mathbf{h}'\cdot\mathbf{x} = 0 \pmod 2$. $\square$