CS-150 Quantum Computer Science: Problem Set 2

Instructor: Saeed Mehraban
TA: Samuel Katzman

Spring, 2026

Guidelines: ***The deadline to return this problem set is 11.59pm on April 17***. *Please show all work for full credit. You are welcome to collaborate with each other, but you must write your solutions independently. Use of AI is forbidden unless indicated otherwise. Submission of the problem set should be via Gradescope only. Best wishes!*

Problem 1 (The five-qubit code, logical operators, and error classification) *The five-qubit code is a stabilizer code on 5 qubits with generators*

$$g_1 = XZZXI, \quad g_2 = IXZZX, \quad g_3 = XIXZZ, \quad g_4 = ZXIXZ.$$

Let $S = \langle g_1, g_2, g_3, g_4 \rangle$ *be the stabilizer group.*

(a) *Show that* S *is abelian and does not contain* $-I$*. Deduce that the code space has dimension* 2.

(b) *Give an expression for a projector* Π *such that the logical* $|0_L\rangle$ *and* $|1_L\rangle$ *states (up to normalization) as*

$$|0_L\rangle \propto \Pi|00000\rangle, \quad |1_L\rangle \propto \Pi|11111\rangle.$$

Verify that $|0_L\rangle$ *and* $|1_L\rangle$ *are stabilized by* S*. Specify operator* $\overline{X} \in \mathcal{P}_5$ *such that* $|1_L\rangle = \overline{X}|0_L\rangle$.

(c) *Show that any single-qubit Pauli error* E *anticommutes with at least one generator* g_i*, and hence is detectable.*

(d) *Let* $N(S)$ *denote the normalizer of* S *in the* n*-qubit Pauli group. Show that logical operators correspond to elements of* $N(S)/S$.

Find Pauli operators $\overline{X}, \overline{Z} \in N(S)$ *such that:*

$$\overline{X} \notin S, \quad \overline{Z} \notin S, \quad \overline{XZ} = -\overline{ZX}.$$

You can choose $\overline{X}$ *to be the same operator you found in part (b).*

(e) *Give four Pauli operators in* $N(S) \setminus S$ *representing four distinct cosets in* $N(S)/S$*. How do you interpret the action of these operations on the code space?*

(f) *Let* $\mathcal{E}$ *be a set of Pauli errors containing one representative from each syndrome class (for example, all single-qubit Pauli errors).*

Show that any Pauli operator E *can be written as*

$$E = LFS,$$

where $L \in N(S)$ *represents a logical operator (modulo* S*),* $F \in \mathcal{E}$*, and* $S \in S$*.*

Describe a procedure to determine L *and* F *from* E *using commutation relations with the generators of* S*.*

Problem 2 (CSS codes and the Steane code) *Recall a CSS code is defined from two classical linear codes $C_1^\perp \subseteq C_2 \subseteq \mathbb{F}_2^n$.*

(a) *Let H_X and H_Z be parity check matrices corresponding to C_1 and C_2 respectively. Recall that the stabilizer generators of the corresponding CSS code corresponds to the following symplectic representation*

$$S = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}$$

what condition should H_X and H_Z satisfy in order for S to correspond to a valid Abelian subgroup of Pauli? Explain why this condition is equivalent to $C_1^\perp \subseteq C_2 \subseteq \mathbb{F}_2^n$.

(b) *Consider the $[7, 4, 3]$ Hamming code with parity check matrix*

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

Construct a CSS code by taking $H_X = H_Z = H$.

Write down the stabilizer generators explicitly.

(c) *Show that this defines a $[[7, 1, 3]]$ quantum code.*

(d) *Give expressions for logical $|0_L\rangle$ and $|1_L\rangle$.*

(e) *Find logical operators $\overline{X}$ and $\overline{Z}$.*

(f) *Explain why this code corrects any single-qubit error.*

Problem 3 (From prism symmetries to the Abelian hidden subgroup problem) *We study a natural Abelian group arising from geometric symmetries and use it to formulate and solve an instance of the Abelian Hidden Subgroup Problem (HSP).*

Part I: Geometry and group structure

(a) *Consider a regular pentagonal prism (a 5-gon prism) with labeled vertices. See Figure 1 below.*

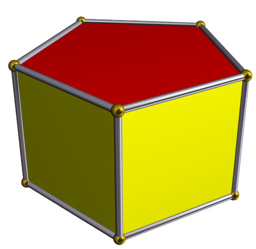

Figure 1: Pentagonal prism. Image source: Wikipedia.

Define the following two symmetries:

- *r: rotation by $2\pi/5$ around the vertical axis,*
- *f: reflection across the horizontal midplane swapping the top and bottom faces.*

(a) *Show that $r^5 = e$ and $f^2 = e$.*

(b) *Show that $rf = fr$.*

(c) *Describe all elements generated by r and f. Call the resulting group G_5.*

(b) Generalize to an M-gonal prism. Let r be rotation by $2\pi/M$ and f be the top-bottom flip. Show that the group generated by r and f (call the resulting group G_M) is isomorphic to

$$G_M \cong \mathbb{Z}_M \times \mathbb{Z}_2.$$

(c) Show that G_M is Abelian.

Part II: Fourier transform on G

(d) Show that any element of G can be written uniquely as (x, y) with $x \in \mathbb{Z}_M$, $y \in \mathbb{Z}_2$.

(e) Show that all irreducible characters of G are given by

$$\chi_{a,b}(x, y) = e^{2\pi i a x/M} \cdot (-1)^{by},$$

where $a \in \mathbb{Z}_M$, $b \in \mathbb{Z}_2$.

(f) Define the quantum Fourier transform (QFT) over G by

$$|x, y\rangle \mapsto \frac{1}{\sqrt{2M}} \sum_{a \in \mathbb{Z}_M, b \in \mathbb{Z}_2} e^{2\pi i a x/M} (-1)^{by} |a, b\rangle .$$

Verify that this transformation is unitary.

Part III: Hidden Subgroup Problem

(g) Let $H \leq G_M$ be a subgroup. Write a general form for any such subgroup. Formulate the hidden subgroup problem for the group of symmetries for G_M.

Part IV: Quantum algorithm

(h) (Coset state preparation)

Show that the following procedure produces a uniform superposition over a random coset of H:

- *(a) Prepare the uniform superposition*

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle .$$

- *(b) Apply the oracle $U_f : |g\rangle |0\rangle \mapsto |g\rangle |f(g)\rangle$.*
- *(c) Measure the second register.*

Show that the resulting state in the first register is

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g_0 + h\rangle$$

for some random $g_0 \in G$.

(i) (Fourier sampling)

Apply the QFT over G to a coset state. Show that measurement yields (a, b) such that

$$\chi_{a,b}(h) = 1 \quad \text{for all } h \in H.$$

(j) *(Recovering the hidden subgroup)*

Suppose $H = \langle (d, e) \rangle$ *is a cyclic subgroup of* G*.*

Show that any observed outcome (a, b) *satisfies*

$$e^{2\pi i a d / M} \cdot (-1)^{be} = 1.$$

Rewrite this as a linear constraint modulo M *and* 2*.*

Explain how collecting sufficiently many samples (a, b) *allows one to recover* (d, e) *and hence determine* H*.*