CQC class, Final Exam. Date due May 15, 2022, 11:59pm EDT.

Instructors: Victor Albert and Alexander Barg

Please submit your work as a **single PDF file** to ELMS (under the "Assignments" tab)

- Papers submitted as multiple separate files (pictures of individual pages) are difficult for grading and **will not be accepted**.
- Justification of solutions is required.
- Please note the clickable links in the assignment.

Problem 1 (The Sugiyama decoding algorithm) (20pt)

In this problem you will learn one more decoding algorithm for BCH codes. Please click on the link and read the description.

Consider a $[n = 127, k = 99]$ binary BCH code C of length $n = 127$ with zeros $\alpha^i, i = 1, 3, 5, 7$, where α satisfies $\alpha^7 = \alpha + 1$.

(a) What is the maximum number of errors that the code C can correct (justify your answer)?

(b) What is the generator polynomial of C (in the simplest possible form)? It's fine to do the actual calculation by computer (GAP, Sagemath), but please explain how you obtained it.

(c) You are given a vector received from the channel, represented in polynomial form as follows:

$x^{126} + x^{120} + x^{119} + x^{117} + x^{115} + x^{114} + x^{112} + x^{111} + x^{110} + x^{109} + x^{107} + x^{106} + x^{105} + x^{103} + x^{100} + x^{98} + x^{96} + x^{95} + x^{94} + x^{92} + x^{90} + x^{82} + x^{74}$

Please program the Sugiyama algorithm and find the corrected codeword. Please submit your work as in HW1 (giving just the codeword will not earn you credit).

Problem 2 (**GV bound for CSS codes**, another proof) (25pt)

(a) Let $R \in (0, 1)$ and for each $i \in \mathbb{N}$, let $\mathcal{F}_i$ be a set of $[n_i, k_i]$ linear binary codes $(C_{i,j}, j = 1, 2, \dots)$ such that

- $k_i/n_i > R$;
- the quantity $N_i := |\{j : x \in C_{i,j}\}|$ does not depend on the choice of the nonzero vector $x \in \{0, 1\}^{n_i}$.

Prove that as long as $\sum_{l=0}^{d-1} \binom{n_i}{l} < \frac{2^{n_i}-1}{2^{k_i}-1}$, the set $\mathcal{F}_i$ contains a code with distance $\geq d$.

(b) Suppose that $n_i \to \infty$ as $i \to \infty$ and conclude that asymptotically the sequence $(\mathcal{F}_i, i = 1, 2, \dots)$ contains codes such that $R \geq 1 - h_2(d/n)$, i.e., it asymptotically meets the GV bound.

(c) Call an $[n, k]$ linear code $\mathcal{C}$ *self-orthogonal* if $1^n \in \mathcal{C}$ and $\mathcal{C} \subset \mathcal{C}^\perp$. Show that the number of codes $\mathcal{C}^\perp$ that contain a given nonzero, *even-weight* vector $x \in \{0, 1\}^n$ does not depend on x. Using the approach of parts (a)-(b), conclude that there exists a sequence of codes $\mathcal{C}^\perp$ that asymptotically attain the GV bound, i.e., satisfy $(n - k)/n \geq 1 - h(d/n)$.

(d) An $[[n, k]]$ quantum CSS code $\mathcal{Q}$ can be defined by a pair of binary linear codes $\mathcal{C}_0, \mathcal{C}_1$ such that $\mathcal{C}_0 \subset \mathcal{C}_1^\perp$. The dimension of the code $\mathcal{Q}$ is $\dim(\mathcal{C}_1^\perp/\mathcal{C}_0) = n - \dim(\mathcal{C}_1) - \dim(\mathcal{C}_0)$. Assume that $\mathcal{C}_0 = \mathcal{C}_1$ and show using part (c) that there exists a sequence of CSS codes $\mathcal{Q}_i$ that attains the bound $R \geq 1 - 2h_2(\delta)$ on the rate vs. relative distance.

Problem 3: Fock-state codes (15pt)

For this problem, we study the error-correcting capabilities of various Fock-state codes, bosonic codes encoding a qubit in one or more oscillators. Each mode's Hilbert space is spanned by the Fock states $\{|n\rangle\}_{n=0}^{\infty}$. The noise model we consider is amplitude damping, whose errors are expressed as powers of products of the lowering operator a (acting as $a|n\rangle = \sqrt{n}|n-1\rangle$ for $n > 0$ and $a|0\rangle = \vec{0}$) and its Hermitian conjugate the raising operator $a^\dagger$.

a). Consider the following single-mode encoding:

$$|\overline{0}\rangle = \frac{|0\rangle + \sqrt{3}\rangle|4\rangle}{2}$$
$$|\overline{1}\rangle = \frac{\sqrt{3}|2\rangle + |6\rangle}{2}.$$

Show that this is a QECC correcting the error set $\mathcal{E} = \{I, a, \hat{n} = a^\dagger a\}$.

b). Now consider the following two-mode encoding:

$$|\overline{0}\rangle = \frac{|40\rangle + |04\rangle}{\sqrt{2}}$$
$$|\overline{1}\rangle = |22\rangle$$

Show that this is a QECC correcting the error set $\mathcal{E} = \{I, a_1, a_2\}$ for two modes.

c). The two-mode code can in fact do much more with respect to *dephasing errors* $\hat{n}_1^p \hat{n}_2^q$. How is the two-mode code able to correct *all* powers of $\hat{n}_1 + \hat{n}_2$ while the single-mode code can only correct a single power of $\hat{n}$?

Problem 4: Transversal gates. (20pt) Transversal gates for multi-qubit codes are gates that can be expressed as a tensor product of operators acting on single qubits. They are particularly beneficial because faults during a transversal gate cannot spread too far among the physical qubits.

a). Consider acting with a Hadamard gate on each qubit, i.e., with the 7-qubit gate

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y \in \mathbb{F}_2^n} (-1)^{x \cdot y} |x\rangle\langle y| .$$

The Hadamard gate *switches* bit-flip errors to phase-flip errors, meaning that the two errors can in principle be treated on the same footing. Let

$$E_{a,b} = \bigotimes_{i=1}^{n} X^{b_i} Z^{a_i} = X^{b_1} Z^{a_1} \otimes X^{b_2} Z^{a_2} \otimes \cdots$$

be a Pauli error string defined by strings $a, b \in \mathbb{F}_2^n$. Let $|\psi\rangle$ be an equal superposition of codewords $c \in \mathbb{F}_2^n$ of a binary linear code C,

$$|\psi\rangle = \frac{1}{\sqrt{|C|}} \sum_{c \in C} |c\rangle .$$

Defining an error state

$$E_{a,b}|\psi\rangle = \frac{1}{\sqrt{|C|}} \sum_{c \in C} (-1)^{a \cdot c} |c + b\rangle ,$$

show that the Hadamarded error state is

$$H^{\otimes n} E_{a,b}|\psi\rangle = \frac{(-1)^{a \cdot b}}{\sqrt{|C^\perp|}} \sum_{c \in C^\perp} (-1)^{b \cdot c} |c + a\rangle ,$$

where $C^\perp$ is the dual code of C.

b). Consider the $[[7, 1, 3]]$ Steane code, with the six stabilizer generators

$$ZZZZIII, XXXXIII,$$
$$ZZIIZZI, XXIIXXI,$$
$$ZIZIZIZ, XIXIXIX.$$

Is $H^{\otimes n}$ a logical gate of the Steane code? Is it a logical gate for any CSS code; why or why not?

c). Consider the CNOT gate CNOT, a two-qubit gate acting as

$$\text{CNOT}\,(X \otimes I)\,\text{CNOT} = X \otimes X$$
$$\text{CNOT}\,(I \otimes X)\,\text{CNOT} = I \otimes X$$
$$\text{CNOT}\,(Z \otimes I)\,\text{CNOT} = Z \otimes I$$
$$\text{CNOT}\,(I \otimes Z)\,\text{CNOT} = Z \otimes Z\,.$$

Is this transversal gate a logical gate between two logical blocks of the Steane code? Is it a logical gate for any CSS code; why or why not?