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 \(\alpha\) 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:

\[
x_{126} + x_{120} + x_{119} + x_{117} + x_{115} + x_{114} + x_{111} + x_{110} + x_{109} + x_{107} + x_{106} + x_{105} + x_{103} + \\
x_{100} + x_98 + x_96 + x_95 + x_94 + x_92 + x_90 + x_82 + x_74
\]

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 \((C_{i,j}, j = 1, 2, \ldots)\) 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 \(\sum_{i=0}^{d-1} \binom{n_i}{1} < \frac{n^d}{2^{n_i-1}},\) 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 \((\mathcal{F}_i, i = 1, 2, \ldots)\) 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 \(C\) self-orthogonal if \(1^n \in C\) and \(C \subset C^\perp\). Show that the number of codes \(C^\perp\) 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 \(C^\perp\) that asymptotically attain the GV bound, i.e., satisfy \((n-k)/n \geq 1 - h(d/n)\).

(d) An \([[n, k]]\) quantum CSS code \(Q\) can be defined by a pair of binary linear codes \(C_0, C_1\) such that \(C_0 \subset C_1^\perp\). The dimension of the code \(Q\) is \(\dim(C_1^\perp/C_0) = n - \dim(C_1) - \dim(C_0)\). Assume that \(C_0 = C_1\) and show using part (c) that there exists a sequence of CSS codes \(Q_i\) 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 \{\ket{n}\}_{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 \(a\ket{n} = \sqrt{n}\ket{n-1}\) for \(n > 0\) and \(a\ket{0} = \ket{0}\)) and its Hermitian conjugate the raising operator \(a^\dagger\).

a). Consider the following single-mode encoding:

\[
\ket{\vec{j}} = \frac{1}{2} \left( \ket{0} + \sqrt{3} \ket{1} \right)
\]

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

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

\[
\ket{\vec{j}} = \frac{1}{2} \left( \ket{00} + \ket{4} \right)
\]

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

c). The two-mode code can in fact do much more with respect to dephasing errors \(\hat{n}_1^a \hat{n}_2^b\). 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

\[
H^{\otimes n} = \frac{1}{\sqrt{2^n}} \left( \begin{array}{cl} 1 & 1 \\
-1 & 1 \end{array} \right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y \in \mathbb{F}_2^n} (-1)^{x \cdot y} \ket{x} \bra{y}.
\]

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
\[
\begin{align*}
&ZZZZIII, XXXIII, \\
&ZZIIZZI, XXIIXXI, \\
&ZIZIZIZ, XIIXIXX.
\end{align*}
\]
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 $\text{CNOT}$, a two-qubit gate acting as
\[
\begin{align*}
\text{CNOT} (X \otimes I) \text{CNOT} &= X \otimes X \\
\text{CNOT} (I \otimes X) \text{CNOT} &= I \otimes X \\
\text{CNOT} (Z \otimes I) \text{CNOT} &= Z \otimes I \\
\text{CNOT} (I \otimes Z) \text{CNOT} &= Z \otimes Z.
\end{align*}
\]
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?