Literature: Nielsen & Chuang, 10.4 Constructing Quantum Codes, p. 445 and 10.5 Stabilizer Codes, p. 453.

Exercise 1. *Classical Linear Codes.*

A *linear code* C encoding k bits of information into an n bit code space is specified by an n by k *generator matrix* G whose entries are all elements of $\mathbb{Z}_2$, that is, zeros and ones. The matrix G maps a message x to its encoded equivalent, Gx, where all operations are done modulo 2.

(a) Write an expression for a generator matrix encoding k bits using r repetitions for each bit, i.e. that encodes each bit into r repetitions of that bit.

(b) Show that adding one column of G to another results in a generator matrix generating the same code (i.e., the two codes have the same code space).

A linear code may also be defined by its *parity check matrix* H, where one defines the code space to be the kernel of H.

(c) Show that adding one row of the parity check matrix to another does not change the code. Using Gaussian elimination and swapping of bits it is therefore possible to assume that the parity check matrix has the *standard form* $(A|\mathbb{1}_{n-k})$, where A is an $(n-k)\times k$ matrix.

(d) Suppose a linear code C encoding k logical bits into n physical bits has parity matrix H of the form $(A|\mathbb{1}_{n-k})$. Show that the corresponding generator matrix is

$$G = \begin{bmatrix} \mathbb{1}_k \\ A \end{bmatrix} . \tag{1}$$

Because $Hx = 0$ for any codeword x, H is cabable of detecting errors (by noticing that $Hx \neq 0$ for a corrupt x). In such a case, one should correct this error by choosing e.g. the codeword which is closest to the corrupt message.

Exercise 2. *Stabilizer Codes.*

This exercise introduces the important formalism of stabilizers, which often allows for a more efficient representation of quantum codes and errors in cryptographic applications.

The Pauli-Group G_n is the smallest closed group which contains all possible n-fold tensor products of the Pauli-matrices $\mathbb{1}, X, Y, Z$. Let S be a subgroup of G_n and let $\mathscr{H}$ be an n-qubit Hilbert space. We say that an element $|\phi\rangle \in \mathscr{H}$ is stabilized by an operator $O \in S$ if $O|\phi\rangle = |\phi\rangle$. We define $V_S \subseteq \mathcal{H}$ to be the set of states which are stabilized by all elements of S.

(a) Which necessary conditions does S have to fulfill such that V_S is non-trivial?

(b) Show that V_S is the intersection of the subspaces fixed by each operator in S, and that V_S is a subspace itself.

(c) Show that $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where $\{|0\rangle, |1\rangle\}$ is the computational basis, is stabilized by $X_1 \otimes X_2$ and $Z_1 \otimes Z_2$. Find a state that is stabilized by $S = \{X \otimes Z, Z \otimes X\}$.