ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

QSIT: Quantum Information Theory. Solutions 7.

Autumn 2012
Prof. M. Christandl

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).

Solution.

(a) We can obviously choose the $k\,r \times k$ matrix

$$G = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \vdots & \vdots & & \\ 1 & 0 & \dots & \\ 0 & 1 & & \\ & \vdots & & \vdots \\ & 1 & & \\ \vdots & & \ddots & \\ & & & 1 \\ & & & \vdots \\ 0 & \dots & & 1 \end{pmatrix} . \tag{S.1}$$

Then any message will be encoded into a codeword that has r copies of each bit.

(b) This follows from the fact that adding a column of a matrix to another results in the same spanned space (see linear algebra lecture). The codewords might change, however, but this can be seen as a simple relabelling of the input bits.

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.

Solution.

(c) The argument is similar as in point (b). The kernel of a matrix is invariant under the addition of rows (see linear algebra lecture).

(d) Let H have the form $H = (A|\mathbb{1}_{n-k})$. Let G be the corresponding generator matrix. Then we must have $HG = 0$, because G maps messages to codewords, which by definition are in the kernel of H. Letting G be of the form (1), we have

$$HG = \left(A|\mathbb{1}_{n-k}\right)\begin{pmatrix}\mathbb{1}_k \\ A\end{pmatrix} = A + A = 0\ , \tag{S.2}$$

since all arithmetic is done modulo 2, and thus $A = -A$. In addition, all the kernel of H is spanned because the dimension of the image of G is k.

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 $S = \{X \otimes Z, Z \otimes X\}$.

Solution.

(a) There are two immediate necessary conditions. First, all operators in S have to commute. Second, $-\mathbb{1} \notin S$, since $-\mathbb{1}|\psi\rangle = |\psi\rangle$ has the only solution $|\psi\rangle = 0$.

(b) Let V_{S_i} denote the set stabilized by the i-th element S_i of S. By definition, each $|\psi\rangle \in V_S$ is stabilized by all operators S_i in S, thus they are contained in all V_{S_i}, thus $V = \bigcap V_{S_i}$.
V_s inherits the vector space structure from $\mathscr{H}$. It is clear that $\mathbb{1} \in V_s$, since $\mathbb{1}|\psi\rangle = |\psi\rangle$. That V_s is closed follows from the linearity of the operators S_i. Thus V_s is a vector space.

(c) We can check the conjecture easily if we recall the action of X and Z on the basis states $|0\rangle, |1\rangle$. X flips the state and Z shifts the phase,

$$X|0\rangle = |1\rangle, \qquad X|1\rangle = |0\rangle, \qquad Z|0\rangle = |0\rangle, \qquad Z|1\rangle = -|1\rangle.$$

Which state is stabilized by $S = \{X \otimes Z, Z \otimes X\}$? There are several approaches to answer that question. The most direct one is certainly to calculate all eigenstates of $X \otimes Z$ and $Z \otimes X$ and take the intersection. However, we might also suspect that Bell states behave naturally under elements of the Pauli-group. Indeed, the images of Bell states are given by

$$\begin{aligned}
XZ(\phi^+) = XZ\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) &= \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) = -\psi^- \\
XZ(\phi^-) = XZ\left(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\right) &= \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = \psi^+ \\
XZ(\psi^+) = XZ\left(\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\right) &= \frac{1}{\sqrt{2}}(-|11\rangle + |00\rangle) = \phi^- \\
XZ(\psi^-) = XZ\left(\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right) &= \frac{1}{\sqrt{2}}(|00\rangle - |00\rangle) = -\phi^+
\end{aligned}$$

We see immediately that, e.g., $\phi^- + \psi^+$ is stabilized by S.