Advanced Quantum Information and Computing

Exercise Sheet 2

Exercise 1 (On Pauli matrices)**.**

1. *Let* $\mathbf{M} = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$*. Show that it exists* $\alpha, \beta \in \mathbb{C}$ *such that* $\mathbf{M} = \alpha\mathbf{X} + \beta\mathbf{Y}$*.*
2. *Let* $\mathbf{M}$ *be any* 2×2 *complex matrix. Show that it exists* $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ *such that* $\mathbf{M} = \alpha\mathbf{I}_2 + \beta\mathbf{X} + \gamma\mathbf{Y} + \delta\mathbf{Z}$.
3. *Compute* $\mathbf{XZ}, \mathbf{XY}$ *and* $\mathbf{YZ}$*. Let* $\mathbf{P}_1, \mathbf{P}_2 \in \{\mathbf{I}_2, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$*. Show that* $\mathrm{tr}(\mathbf{P}_1\mathbf{P}_2) = 0$ *if* $\mathbf{P}_1 \neq \mathbf{P}_2$ *and* $\mathrm{tr}(\mathbf{P}_1\mathbf{P}_2) = 2$ *if* $\mathbf{P}_1 = \mathbf{P}_2$*.*
4. *Let* $\mathbf{U}$ *be any unitary matrix on* 1 *qubit. We can hence write* $\mathbf{U} = \alpha\mathbf{I} + \beta\mathbf{X} + \gamma\mathbf{Y} + \delta\mathbf{Z}$*. Show that*
$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

Exercise 2 (Shor's code is a CSS code)**.** *Show that the following codes are* CSS *codes and give* $(\mathcal{C}_{\mathbf{Z}}, \mathcal{C}_{\mathbf{X}})$ *for them*

1. $\mathrm{Vect}\left(|000\rangle, |111\rangle\right)$
2. $\mathrm{Vect}\left((|0\rangle + |1\rangle)^{\otimes 3}, (|0\rangle - |1\rangle)^{\otimes 3}\right)$
3. $\mathrm{Vect}\left((|000\rangle + |111\rangle)^{\otimes 3}, (|000\rangle - |111\rangle)^{\otimes 3}\right)$

Exercise 3 (Steane's code)**.** *Let* $\mathcal{C}$ *be the* $[7,4,3]$ *Hamming code (that we have seen during the lecture). Recall that it has parity-check matrix*

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

Let $\mathcal{C}_{\mathbf{X}} \stackrel{def}{=} \mathcal{C}$ *and* $\mathcal{C}_{\mathbf{Z}} \stackrel{def}{=} \mathcal{C}^{\perp}$*.*

1. *Show that* $\mathbf{H}\mathbf{H}^{\top} = \mathbf{0}$*.*
2. *Deduce that* $\mathcal{C}_{\mathbf{Z}} \subseteq \mathcal{C}_{\mathbf{X}}$*.*

3. *From the above question,* $(\mathcal{C}_{\mathbf{Z}}, \mathcal{C}_{\mathbf{X}})$ *defines a* CSS*-code. How many qubits does it enable to encode? How many errors can it correct?*

Exercise 4 (CSS codes are stabilizer codes)**.** *Let* $\mathcal{C}_{\mathbf{X}}$ *and* $\mathcal{C}_{\mathbf{Z}}$ *be two linear code such that* $\mathcal{C}_{\mathbf{Z}} \subseteq \mathcal{C}_{\mathbf{X}}$*.*

1. *Show that for all* $\mathbf{e}_1, \mathbf{e}_2 \in \mathcal{C}_{\mathbf{Z}}$*,* $\mathbf{f}_1, \mathbf{f}_2 \in \mathcal{C}_{\mathbf{X}}^{\perp}$ *we have*
$$\left(\mathbf{X}^{\mathbf{e}_1}\mathbf{Z}^{\mathbf{f}_1}\right)\left(\mathbf{X}^{\mathbf{e}_2}\mathbf{Z}^{\mathbf{f}_2}\right) = \left(\mathbf{X}^{\mathbf{e}_2}\mathbf{Z}^{\mathbf{f}_2}\right)\left(\mathbf{X}^{\mathbf{e}_1}\mathbf{Z}^{\mathbf{f}_1}\right)$$

2. *Show that for any* $\mathbf{e} \in \mathcal{C}_{\mathbf{Z}}$*,* $\mathbf{f} \in \mathcal{C}_{\mathbf{X}}^{\perp}$*, and* $|\psi\rangle$ *belonging to the* CSS *code given by* $(\mathcal{C}_{\mathbf{X}}, \mathcal{C}_{\mathbf{Z}})$*, we have*
$$\mathbf{Z}^{\mathbf{f}}\mathbf{X}^{\mathbf{e}}|\psi\rangle = |\psi\rangle$$

3. *Deduce that any* CSS *code is a stabilizer code and precise the subgroup of* $\mathbb{G}_n$ *which stabilizes it, in particular, give its description in terms of* $(\mathcal{C}_{\mathbf{X}}, \mathcal{C}_{\mathbf{Z}})$ *(up to an isomorphism).*

Exercise 5 (A 5 qubits code)**.** *Let*

$$\begin{aligned}
\mathbf{M}_1 &= \mathbf{X} \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{X} \otimes \mathbf{I} \\
\mathbf{M}_2 &= \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{Z} \otimes \mathbf{Z} \otimes \mathbf{X} \\
\mathbf{M}_3 &= \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{Z} \otimes \mathbf{Z} \\
\mathbf{M}_4 &= \mathbf{Z} \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{Z}
\end{aligned}$$

Consider the stabilizer code associated to

$$\mathbb{S} \stackrel{def}{=} \langle \mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3, \mathbf{M}_4 \rangle$$

1. *Show that every error in* $\mathbb{G}_5$ *of weight* 1 *or* 2 *has a syndrome* $\neq \mathbf{0}$*.*

2. *Find a harmful error (type B) of weight* 3*.*

3. *How many errors can be corrected by such a code?*

4. *In which "sense" is this code better than Steane's code?*

Exercise 6 (A proof useful for CSS codes)**.** *Our aim in this exercise is to prove*

$$\mathbf{H}^{\otimes n} |\mathcal{C}\rangle = |\mathcal{C}^{\perp}\rangle$$

where $\mathcal{C}$ *is a subspace of* $\mathbb{F}_2^n$*,*

$$\mathcal{C}^{\perp} = \left\{ \mathbf{c}^{\perp} \in \mathbb{F}_2^n \;:\; \forall \mathbf{c} \in \mathcal{C},\; \langle \mathbf{c}, \mathbf{c}^{\perp} \rangle = \sum_{i=1}^{n} c_i c_i^{\perp} = 0 \mod 2 \right\}$$

and

$$|\mathcal{C}\rangle \stackrel{def}{=} \frac{1}{\sqrt{\sharp \mathcal{C}}} \sum_{\mathbf{c} \in \mathcal{C}} |\mathbf{c}\rangle \quad ; \quad |\mathcal{C}^{\perp}\rangle \stackrel{def}{=} \frac{1}{\sqrt{\sharp \mathcal{C}^{\perp}}} \sum_{\mathbf{c}^{\perp} \in \mathcal{C}^{\perp}} |\mathbf{c}^{\perp}\rangle$$

Exercise 7 (Building CSS encoding)**.** *We are given two linear codes* $\mathcal{C}_{\mathbf{X}}$ *and* $\mathcal{C}_{\mathbf{Z}}$ *of length* n *such that* $\mathcal{C}_{\mathbf{Z}} \subseteq \mathcal{C}_{\mathbf{X}} \subseteq \mathbb{F}_2^n$*. Recall that* $\mathcal{C}_{\mathbf{X}}/\mathcal{C}_{\mathbf{Z}}$ *is a subspace defined as*

$$\mathcal{C}_{\mathbf{X}}/\mathcal{C}_{\mathbf{Z}} = \{ \overline{\mathbf{x}} \;:\; \mathbf{x} \in \mathcal{C}_{\mathbf{X}} \} \quad \text{where } \overline{\mathbf{x}} \stackrel{def}{=} \mathbf{x} + \mathcal{C}_{\mathbf{Z}} = \{ \mathbf{x} + \mathbf{c}_{\mathbf{Z}} \;:\; \mathbf{c}_{\mathbf{Z}} \in \mathcal{C}_{\mathbf{Z}} \} \subseteq \mathcal{C}_{\mathbf{X}}$$

Let,

$$k \stackrel{def}{=} \dim \mathcal{C}_{\mathbf{X}}/\mathcal{C}_{\mathbf{Z}} = \dim \mathcal{C}_{\mathbf{X}} - \dim \mathcal{C}_{\mathbf{Z}}$$

Recall that

$$\mathcal{C}_{\mathbf{X}}/\mathcal{C}_{\mathbf{Z}} = \left\{ \mathbf{x}_i + \mathcal{C}_{\mathbf{Z}} \;:\; 1 \leq i \leq 2^k \right\} \quad \text{and} \quad \mathcal{C}_{\mathbf{X}} = \bigsqcup_{1 \leq i \leq 2^k} \mathbf{x}_i + \mathcal{C}_{\mathbf{Z}}$$

for 2^k *vectors* $\mathbf{x}_i \in \mathcal{C}_{\mathbf{X}}$ *which are called the representatives of* $\mathcal{C}_{\mathbf{X}}/\mathcal{C}_{\mathbf{Z}}$*.*

1. *Show how to efficiently compute the following mappings (we naturally identify* $\mathbf{i} \in \mathbb{F}_2^k$ *to an integer* $1 \leq i \leq 2^k$*)*

$$\mathbf{i} \in \mathbb{F}_2^k \longmapsto \mathbf{x}_i \in \mathbb{F}_2^n, \quad \mathbf{x}_i \in \mathbb{F}_2^n \longmapsto \mathbf{i} \in \mathbb{F}_2^k$$

$$\mathbf{y} \in \mathcal{C}_{\mathbf{X}} \mapsto \mathbf{x}_i \quad \text{when } \mathbf{y} \in \mathbf{x}_i + \mathcal{C}_{\mathbf{Z}}$$

Notice that the first two mappings "fix" a choice of representatives $\mathbf{x}_i$*'s; recall that if* $\{\mathbf{x}_i \;:\; 1 \leq i \leq 2^k\}$ *is a set of representatives of* $\mathcal{C}_{\mathbf{X}}$*, then* $\{\mathbf{x}_i + \mathbf{c}_i \;:\; \mathbf{c}_i \in \mathcal{C}_{\mathbf{Z}} \text{ and } 1 \leq i \leq 2^k\}$ *is also a set of representatives. The last mapping is well defined by the decomposition of* $\mathcal{C}_{\mathbf{X}}$ *as disjoint union of cosets.*

2. *Show how to compute* $|\mathbf{x}\rangle\,|\mathbf{x}+\mathcal{C}_{\mathbf{Z}}\rangle$ *where*

$$|\mathbf{x}+\mathcal{C}_{\mathbf{Z}}\rangle \stackrel{def}{=} \frac{1}{\sqrt{\sharp\mathcal{C}_{\mathbf{Z}}}}\sum_{\mathbf{y}\in\mathcal{C}_{\mathbf{Z}}}|\mathbf{x}+\mathbf{y}\rangle\,.$$

and supposing that we have access to $|\mathbf{x}\rangle$.

Hint: *use the matrix* $\mathbf{G}\in\mathbb{F}_2^{k_{\mathbf{Z}}\times n}$ *(*$k_{\mathbf{Z}}\stackrel{def}{=}\dim\mathcal{C}_{\mathbf{Z}}$*) whose rows form a basis of* $\mathcal{C}_{\mathbf{Z}}$ *(which is supposed to be given to have a description of* $\mathcal{C}_{\mathbf{Z}}$*); recall that*

$$\mathcal{C}_{\mathbf{Z}} = \left\{\mathbf{m}\mathbf{G}\ :\ \mathbf{m}\in\mathbb{F}_2^{k_{\mathbf{Z}}}\right\}$$

3. *Deduce how to implement the following* CSS *encoding:*

$$\sum_{\mathbf{i}\in\{0,1\}^k}\alpha_{\mathbf{i}}\underbrace{|\mathbf{i}\rangle}_{k\ \ qubits}\longmapsto\sum_{\mathbf{x}_i}\alpha_{\mathbf{i}}\underbrace{|\mathbf{x}_i+\mathcal{C}_{\mathbf{Z}}\rangle}_{n\ \ qubits}$$