EXERCISES FOR INTRODUCTION TO MATHEMATICAL QUANTUM ERROR CORRECTION

DHEERAN E. WIGGINS

1. Monday

Exercise 1.1 (Complex Arithmetic)**.** Simplify the following expressions in $\mathbb{C}$:

(i) $i^3 + i^2 + i + 1$
(ii) $(-3 + 2i)(6 - 8i)$
(iii) $(9i)(-i)$

Exercise 1.2 (Pauli Matrix Multiplication)**.** Let $I, X, Y, Z \in \mathbb{M}_2(\mathbb{C})$ be defined by

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(i) Compute the matrix products I^2, IX, IY, and IZ. What can you guess is true about multiplying matrices in $\mathbb{M}_2(\mathbb{C})$ by I, in general?
(ii) Compute the matrix products XY and YX. Simplify both products into the form cZ, where $c \in \mathbb{C}$. Is c different in each case?

The matrix I is called the identity. The other three matrices X, Y, Z are called the *Pauli matrices*. Together, these generate the *Pauli group*, a multiplicative group of order 16.

Exercise 1.3 (Recalling Definitions)**.**

(i) Let A, B be sets. What is an *injective* function $f : A \rightarrowtail B$? What is a *surjective* function $f : A \twoheadrightarrow B$? What do we call a function $f : A \xrightarrow{\sim} B$ which is *both* injective and surjective?
(ii) Write the definition of a *group* $(G, \cdot)$. What is the general difference between just a set and a group?[1]
(iii) What is the difference between a group and an *abelian* group?
(iv) Let $S \subseteq G$ be a subset of a group. Write the definition of the *normalizer* $\mathcal{N}_G(S)$ and *centralizer* $C_G(S)$ of S in G.

Date: January 14, 2025.

[1] You can be informal about this.

2. Tuesday

Exercise 2.1 (Conjugates and Adjoints)**.** Compute the following, where $*$ denotes the complex *conjugate* $(a+bi)^* = a - bi$ in $\mathbb{C}$ and $\dagger$ denotes the *adjoint* in $\mathbb{C}^n$:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}^\dagger = \begin{pmatrix} a_1^* & \cdots & a_n^* \end{pmatrix}.$$

(i) $i(i^*)$
(ii) $(7+i)^* + (1+3i) + (1-4i)^*$
(iii)

$$\begin{pmatrix} i \\ 1+i \\ 0 \\ 2+2i \end{pmatrix}^\dagger$$

Exercise 2.2 (Basics of $\mathbb{C}^2$)**.** As mentioned in lecture, $\mathbb{C}^2$ is an example of a vector space over $\mathbb{C}$. Notably, the elements of $\mathbb{C}^2$ are ordered pairs (z, w) where z, w are complex numbers. The functions (linear transformations) in this case are realizable as 2×2 complex matrices $\mathbb{M}_2(\mathbb{C})$.

(i) What is the *dimension* of $\mathbb{C}^2$? In turn, what is the size of a basis for $\mathbb{C}^2$?[2]
(ii) Write down a *basis* β for $\mathbb{C}^2$. That is, find a subset of $\mathbb{C}^2$ such that $\operatorname{span}\beta$ gives you every possible ordered pair/vector $(z, w) \in \mathbb{C}^2$.
(iii) Generalize your answers from (i) and (ii) to $\mathbb{C}^n$: determine its dimension and find a basis. These solutions should be analogous (look very similar) to your answers for $\mathbb{C}^2$.

Exercise 2.3 (Recalling Definitions)**.**

(i) Write down the definition of a *vector space* from lecture. How does a vector space differ from an *inner product* space?
(ii) What is a *Hilbert space* in finite dimensions?
(iii) How do we define the *direct sum/coproduct* $\bigoplus \mathcal{W}_i$ of an indexed family of vector spaces $\{\mathcal{W}_i\}_{i\in I}$? How is this different from a vector space *product*? Do the definitions differ when $I = \{1, \ldots, n\}$?

Exercise 2.4 (Challenge Problems)**.** These problems are more abstract and require quite a bit more thinking (and probably, more background) than I expect from just two days of watching lecture. Still, if you are interested, here are two relevant challenge problems. [These questions were adapted from Chris Dodd at Illinois.]

(i) Let $\mathcal{V}$ be a vector space of dimension n. A flag $\mathfrak{F}$ of length r in $\mathcal{V}$ is a collection of subspaces $\{0\} = \mathcal{V}_0 \subset \mathcal{V}_1 \subset \cdots \subset \mathcal{V}_r = \mathcal{V}$, where $\mathcal{V}_i \neq \mathcal{V}_{i+1}$ for all i. Show that $r \leq n$. If $r = n$, we call the flag $\mathfrak{F}$ *complete*. Show that $\mathfrak{F}$ is complete *if and only if* $\dim(\mathcal{V}_i/\mathcal{V}_{i+1}) = 1$ for all i.[3]
(ii) Let $T : \mathcal{V} \to \mathcal{W}$ and $S : \mathcal{W} \to \mathcal{U}$ be linear maps of vector spaces. Let T^* and S^* denote the dual maps $T^* : \mathcal{W}^* \to \mathcal{V}^*$ and $S^* : \mathcal{U}^* \to \mathcal{W}^*$, defined in the natural way $\varphi \mapsto \varphi \circ T$ or S. Show that $(S \circ T)^* = T^* \circ S^*$. Use this to show that if A, B are matrices so that AB exists, then $(AB)^t = B^t A^t$.

[2]Remember, this is the same as asking for the number of "copies" of $\mathbb{C}$ in $\mathbb{C}^2$.

[3]Here, $\mathcal{V}_i/\mathcal{V}_{i+1}$ is the *quotient space*. That is, the elements of the underlying group are additive cosets $v + \mathcal{V}_{i+1}$, where $v \in \mathcal{V}_i$, and the operations work via $(v + \mathcal{V}_{i+1}) + (k + \mathcal{V}_{i+1}) = (v + k) + \mathcal{V}_{i+1}$ and $c(v + \mathcal{V}_{i+1}) = cv + \mathcal{V}_{i+1}$, for a scalar $c \in \mathbb{C}$.

University of Illinois Urbana-Champaign, Illinois, 61801
Email address: dheeran2@illinois.edu