

MAT3420 (2022 SPRING) MANDATORY ASSIGNMENT

MAKOTO YAMASHITA

Choose (at least) one of the problems from the list below, and submit your solutions via Canvas. The deadline is April 30.

Problem 1. Consider the BB84 quantum key distribution protocol, as explained in Section 8.2 of Aaronson's lecture note. Suppose that Alice chose the strings $x = 0101$ and $y = 0110$, and Bob chose the string $y' = 1010$.

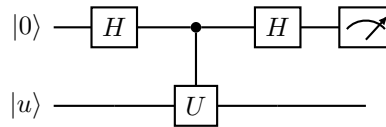
- (1) What would be x' ?
- (2) What will be the shared secret for Alice and Bob?

Problem 2. Work out the factorization of matrices that we used in March 23 lecture: any $W \in \text{U}(2)$ can be factorized as

$$W = e^{i\alpha} AXBXC, \quad ABC = I_2, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Ref. Nielsen–Chuang Section 4.2

Problem 3. Explain why the following version of Kitaev's algorithm works: Let U be a unitary gate acting on the single qubit space, and $|u\rangle$ be an eigenvector of U , with eigenvalue $e^{2\pi i\theta}$. Under the measurement in the following circuit:



we observe $|0\rangle$ with probability $\cos^2(\pi\theta)$.

Ref. Nielsen–Chuang Problem 5.3

Problem 4. Let E be the 3-dimensional real vector space

$$\{xX + yY + zZ \mid x, y, z \in \mathbb{R}\},$$

where X, Y, Z are the Pauli matrices.

- (1) Show that E can be characterized as the set of matrices $A \in M_2(\mathbb{C})$ such that $A^\dagger = A$ and $\text{Tr}(A) = 0$.
- (2) Show that $\text{Ad}_U(A) = UAU^\dagger \in E$ for $U \in \text{U}(2)$ and $A \in E$.
- (3) Show that the transformations $\text{Ad}_{\exp(itZ)}$ correspond to rotations around the z -axis.
- (4) Explain that the transformations $\text{Ad}_{\exp(itY)}$ and $\text{Ad}_{\exp(itZ)}$ generate all rotations centered at the origin of E .