MAT3420 2024, Exercises week 11 (for Friday 15 March)

Exercise 1. Exercise 6.1.1(a) and (b) in [1]. Hint: look first at the case of 2×2 matrices.

Exercise 2. Exercise 6.1.2 in [1], the case $N = 2$.

Exercise 3. Exercise 6.5.1 in [1].

Exercise 4 (Simon's problem). Suppose that $f : \{0,1\}^3 \to \{0,1\}^3$ is a function such that

$$f(\bar{x}) = f(\bar{y}) \Leftrightarrow \bar{y} = \bar{x} \oplus \bar{s} \tag{1}$$

for 3-bit strings $\bar{x}, \bar{y}, \bar{s}$, where $\bar{s} = s_1 s_2 s_3$ is the secret string.

(a) Suppose that $\bar{s} = 110$. Write down the possible values of $\bar{y}$ with $\bar{y} = \bar{x} \oplus \bar{s}$, for all (8 in total) choices of $\bar{x}$. What can you say about these values of $\bar{y}$?

(b) Suppose that $f(000) = 111, f(001) = 100, f(010) = 010, f(011) = 001, f(100) = 010, f(101) = 001, f(110) = 111, f(111) = 100$. Is this a valid function for the key $\bar{s} = 110$?

(c) Same question as in (b) for $f(000) = 111, f(001) = 100, f(010) = 010, f(011) = 001, f(100) = 010, f(101) = 001, f(110) = 110, f(111) = 100$. How many possibilities are there for a function f that satisfies (1)?

(d) Suppose that you run Simon's algorithm three times and get states $|000\rangle, |001\rangle, |111\rangle$ as possible $|z\rangle$ with $\bar{z} \cdot \bar{s} = 0 (\mathrm{mod}\, 2)$. What is $\bar{s}$ in this case?

References

[1] P. Kaye, R. Laflamme and M. Mosca, An Introduction to Quantum Computing, Oxford University Press, 2007.