M526/P623 Quantum Computation *Lecturer: Ninnat Dangniam*

Homework Assignment 4

DUE: 24 Jan 2025 35+10 points

1. Solving Deutsch-Josza and Bernstein-Vazirani classically (10 points).

(a) Moore and Mertens (MM) Exercise 15.16 (p.846)

(b) MM 15.19 (p.892)

2. Spanning Simon (10 points): MM 15.20

(**Alternative hint:** For the first question, think of a collection $\{\mathbf{k}_1, \ldots, \mathbf{k}_t\}$ of d-dimensional vectors in V as a d-by-t rectangular matrix whose columns are the $\mathbf{k}$ vectors.)

For Problem 3 and 4, you may choose to solve just one. If you solve both, you'll earn extra credit.

3. Primes and public keys (10 points)

(a) The largest known prime number discovered in October 2024 is a 41,024,320-digit Mersenne prime (a prime number of the form $2^p - 1$ for some prime p),

$$2^{136,279,841} - 1.$$

Show that the number is not divisible by 41. (You may use the fact that 41 is a prime number.)

(b) Let $p = 97$ and $q = 109$. Let $N = pq$ and $e = 5003$. Alice's public key is (N, e). What is her decryption exponent d? In other words, what d has the property that $m^{ed} \equiv m \mod N$ as long as m and N are mutually prime?

4. Shor's algorithm works at least half the time (10 points): MM 15.29

5. The swap test (5 points): MM 15.33

(The second term in the last equation should be $|-\rangle \otimes |\psi_{\text{asym}}\rangle$.)