Exercises for Introduction to Quantum Computing (physics7514) Wise 2025

L. Funcke, A. Bulgarelli and N. Dichter

---

1 Shor's algorithm

Consider a four-qubit system and the operator U_x used in Kitaev's phase estimation formulation of Shor's algorithm. We set $x = 13$, such that

$$U_{13}\,|y\rangle = |13y \mod 15\rangle \qquad \text{for} \quad y < 15\,,$$
$$U_{13}\,|15\rangle = |15\rangle\ .$$

- Compute all the eigenvalues and eigenvectors of U_{13} *(1 point).*
- Find a subset S of N eigenvectors $|i\rangle$, such that

$$\frac{1}{\sqrt{N}} \sum_{i \in S} |i\rangle = |12\rangle$$

(1 point).

2 Breaking RSA

You are given the following key pair:

$$\{e, N\} \ = \ \{20579, 121130231\},$$

where it is guaranteed that N is the product of two prime numbers p, q.

a) Use Shor's algorithm to factor N. You may use a classical order-finding procedure. For computing the greatest common divisor, you can use Euclid's algorithm *(4 points).*

b) Once you have factored N, decrypt the string "blhhay". The alphabet contains only lower-case letters, which are mapped to integers as "a"$\to c_a = 0$, "b"$\to c_b = 1$, and so on until "z"$\to c_z = 25$. For example, the word "hallo" would be mapped to

$$\text{"hallo"} \quad \to \quad c_h 26^4 + c_a 26^3 + c_l 26^2 + c_l 26^1 + c_o = 3206568$$

with $c_h = 7, c_a = 0, c_l = 11$ and $c_o = 14$ *(4 points).*