Computação Quântica

Problem 3 - 27 May 2020 - 27 June 2020

Problem 3

This exercise aims at improving your understanding of some techniques and procedures relevant to the Shor's algorithm.

- The *order-finding* algorithm as discussed in the lectures resorts to the following oracle:

$$U_a(|q\rangle) \;=\; |\mathsf{rem}\,(qa, n)\rangle \quad \text{for } 0 \leq q < n$$

  Show this is unitary.

- A fundamental remark in the explanation of the *order-finding* algorithm is captured by the following equality (cf slide 22, `CQ-5.pdf`).

$$|1\rangle \;=\; \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle$$

  Explain its relevance on your own words, and prove the equality.

- The following exercise relates the algorithms for *period-finding* and *eigenvalue estimation* (discussed in `CQ-6.pdf`). Consider an operator

$$U_r|f(x)\rangle \;=\; |f(x+r)\rangle$$

  for a periodic function f with period $0 < r < 2^n$, i.e. such that

$$f(x+r) \;=\; f(x) \quad \text{with } x, r \in \{0, 1, 2, \cdots\}$$

  Show that the eigenvectors of U_r are exactly the states

$$|\bar{f}(l)\rangle \;=\; \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-\frac{2\pi i l x}{r}} |f(x)\rangle$$

  (cf slide 4, `CQ-6.pdf`). Compute the corresponding eigenvalues.

- Can you resort to the result just proved to justify why the *period-finding* algorithm actually works? Explain.