MPRI 2.34.2: Quantum Information and Cryptograph **2023 - 2024**

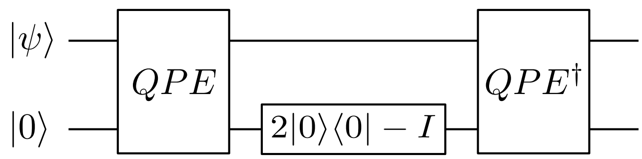
Exercises 1: Random walks and quantum walks

Lecturer: Simon Apers (apers@irif.fr)

Exercise 1 (Reflecting around $|\pi\rangle$)**.** We can use a quantum walk W to reflect around the quantum state $|\pi\rangle$, i.e., implement the map

$$|\psi\rangle = \alpha |\pi\rangle + \beta |\pi^\perp\rangle \longrightarrow (2 |\pi\rangle \langle\pi| - I) |\psi\rangle = \alpha |\pi\rangle - \beta |\pi^\perp\rangle .$$

Assume that $|\psi\rangle = \alpha |\pi\rangle + \sum_j \beta_j |v_j\rangle$ such that $W |\pi\rangle = |\pi\rangle$ and $W |v_j\rangle = e^{i2\pi\theta_j} |v_j\rangle$ with $1/2 > |\theta_j| > \Delta > 0$. We call Δ the *spectral gap of the quantum walk.* Analyze the following circuit (where QPE represents quantum phase estimation on W to precision $\Delta/2$). How many calls does it make to the quantum walk operator?



Exercise 2 (Quantum walk search)**.** We can implement Grover search using quantum walks by considering the initial state $|\pi\rangle$, a marked element $|\psi_m\rangle$ (for $m \in V$), and the Grover operator

$$(2 |\pi\rangle \langle\pi| - I)(2 |\psi_m\rangle \langle\psi_m| - I).$$

How many times do we have to apply the Grover operator on $|\pi\rangle$ to have a good overlap with $|\psi_m\rangle$? Argue that this yields a quantum walk algorithm for finding a marked element that makes $O\left(\frac{1}{\Delta\sqrt{\pi(m)}}\right)$ calls to a quantum walk.[1]

[1] Szegedy (FOCS'04) showed that $\Delta \in \Omega(\sqrt{\delta})$ so this becomes $O(1/\sqrt{\delta\pi(m)})$, quadratically improving over the upper bound $O(1/(\delta\pi(m)))$ on the classical hitting time of a random walk.