

**Exercice 1** *Estimation de phase basée sur la transformée de Fourier quantique*

Soit  $U$  une matrice unitaire  $2^n \times 2^n$  (ici  $n \geq 1$ ) possédant un vecteur propre  $|u\rangle$  avec valeur propre  $e^{2\pi i \varphi}$ . C'est à dire :

$$U|u\rangle = e^{2\pi i \varphi}|u\rangle.$$

On suppose

$$\varphi = \frac{\varphi_1}{2} + \frac{\varphi_0}{4}$$

avec  $\varphi_1, \varphi_0 \in \{0, 1\}$  binaires. Dans ce problème on étudie un "algorithme d'estimation de phase" qui permet de découvrir  $\varphi$  en supposant le vecteur propre  $|u\rangle$  connu.

On rappelle que la transformée de Fourier quantique agissant sur deux qubits est définie par

$$QFT|x_1, x_0\rangle = \frac{1}{2} \sum_{y_0, y_1 \in \{0, 1\}} e^{\frac{2\pi i}{4}(2x_1+x_0)(2y_1+y_0)} |y_1, y_0\rangle$$

où ici  $x_1, x_0 \in \{0, 1\}$ . Nous définissons aussi les opérations (contrôlées) suivantes qui agissent sur  $2 + n$  qubits (ici  $x, y \in \{0, 1\}$  et  $|\psi\rangle \in \mathbb{C}^{\otimes n}$ )

$$R_1 |x\rangle \otimes |y\rangle \otimes |\psi\rangle = |x\rangle \otimes |y\rangle \otimes U^{2x}|\psi\rangle$$

$$R_2 |x\rangle \otimes |y\rangle \otimes |\psi\rangle = |x\rangle \otimes |y\rangle \otimes U^y|\psi\rangle.$$

Soit maintenant la matrice unitaire

$$S = ((QFT)^\dagger \otimes I_n) R_2 R_1 (H \otimes H \otimes I_n)$$

où  $H$  est la matrice de Hadamard usuelle et  $I_n$  est la matrice unité agissant sur  $n$  qubits. Ici  $(QFT)^\dagger$  est l'adjoint de  $QFT$  (c.à.d transposé et complexe conjugué).

- (a) Quelle est la dimension de la matrice unitaire  $S$ ? Faites un dessin du circuit correspondant à  $S$ .
- (b) On initialise le circuit dans l'état  $|0\rangle \otimes |0\rangle \otimes |u\rangle$ . Calculez l'état des  $2 + n$  qubits juste avant la porte  $(QFT)^\dagger$ .
- (c) Vérifiez que l'expression trouvée sous (b) n'est rien d'autre que  $QFT|\varphi_1, \varphi_0\rangle$ . Quel est donc l'état à la sortie du circuit ?
- (d) En déduire que l'on peut découvrir  $\varphi$  en faisant *une et une seule mesure* des deux premiers qubits à la sortie du circuit.