Quantum Computation 2017

Sheet 5 Abgabe 18/12/2017

1. Delayed measurement with Clifford only circuits

For universal quantum circuits, it is possible to defer all measurements to the end without loss of generality. Show that this is not true for circuits that involve only Clifford gates.

2. Unitarity of the order-finding operator

For integers x, N and L with $x < N \leq 2^L - 1$ and $\mathrm{gcd(x, N)} = 1$, consider the following operation,

$$U = \sum_{y=0}^{2^L-1} |\, f(y)\rangle \langle y\,| \,, \tag{1}$$

Where $f(y) = x \times y \mod N$ for $0 \leq y < N$ and $f(y) = y$ otherwise. Show that U is unitary.

3. Eigenstates of the order-finding operator

(a) Show that the following states are eigenstates of U,

$$|\, u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] \left| x^k \mod N \right\rangle . \tag{2}$$

Here $0 \leq s \leq r-1$, where r is the smallest integer such that $x^r = 1 \mod N$. Show also that the corresponding eigenvalues are $u_s = \exp(2\pi i s/r)$.

(b) There are also many states with eigenvalue 1. What are these?