An approximate $\log n$ depth circuit for decoding waterfall states, with aplication to position based cryptography

Alvaro Piedrafita, Subhasree Patro, Arjan Corneliessen, Farrokh Labib, Florian Speelman

September 17, 2019

1 Correctness of the circuit

Our goal here is to prove that the circuit from figure **??** extracts the value x_k while leaving the state mostly unperturbed. That is, we will prove the following lemma.

Lemma 1. *Let $\vec{x} = (x_1, \ldots, x_k) \in \{0,1\}^k$ be a k bit string, and $|Enc(\vec{x})\rangle$ its encoding.*

$$|\langle Enc(\vec{x})|\langle x_k|U_k|Enc(\vec{x})\rangle|0\rangle| = \sqrt{1 - \frac{\sin^2 \frac{\pi}{8}}{2^{k-1}}} \tag{1}$$

Proof. We begin by noticing that we can split U_k into $V_k^\dagger CNOT_{(k,A)}V_k$, where V_k are unitaries that only act on the block of k qubits and the controlled not operation acts on the last qubit of the block and the ancilla. The crucial part of the proof will be to understand the structure of $V_k|Enc(\vec{x})\rangle$. Indeed, allow us to write $V_k|Enc(\vec{x})\rangle$ as

$$V_k|Enc(\vec{x})\rangle = |\psi\rangle|x_k\rangle + |\phi\rangle|\bar{x_k}\rangle,$$

For some vectors $|\psi\rangle$ and $|\phi\rangle$. Observe that the $CNOT$ with a target initialized at $|0\rangle$ simply copies into the ancillary register the value of the k-th bit of $V_k|Enc(\vec{x})\rangle$, hence we have

$$CNOT_{(k,A)}V_k|Enc(\vec{x})\rangle|0\rangle = |\psi\rangle|x_k\rangle|x_k\rangle + |\phi\rangle|\bar{x_k}\rangle|\bar{x_k}\rangle. \tag{2}$$

Hence, the inner product that we are interested in reads

$$\begin{aligned} |\langle Enc(\vec{x})|\langle x_k|V_k^\dagger CNOT_{(k,A)}V_k|Enc(\vec{x})\rangle|0\rangle| &= |\left[\left(\langle\psi|\langle x_k| + \langle\phi|\langle\bar{x_k}|\right)\langle x_k|\right]\left[|\psi\rangle|x_k\rangle|x_k\rangle + |\phi\rangle|\bar{x_k}\rangle|\bar{x_k}\rangle\right]| \quad (3) \\ &= |\langle\psi|\psi\rangle| = \sqrt{1 - |\langle\phi|\phi\rangle|^2}. \quad (4) \end{aligned}$$

Now, we shall characterize $V_k|Enc(\vec{x})\rangle$ and prove that $||\phi\rangle|$ is really small. □