Recycling Quantum Computation.

David Ponarovsky

May 10, 2023

Consider the CSS code composed by C_x, $C_z^{\perp}$ at length n. Define the 1-**SWAP** test on $|\psi\rangle \otimes |\phi\rangle$ to be:

1. Applay the hadamard gate on ancile.
2. Pick a random coordinate $i \sim [n]$.
3. condinatal on the ancile a swap between the ith qubit of $|\psi\rangle$ to the ith qubit of $|\phi\rangle$.
4. Applay the hadammard again on the ancile and massure. If $|0\rangle$ massured then accept, otherwise reject.

suppose for the moment that $|\psi\rangle$ and $|\phi\rangle$ are in the code. Thus:

$$\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{|C_z^{\perp}|}} \sum_{z \in C_z^{\perp}} |\psi + z\rangle \\
(1 - \mathbf{SWAP}) |0\rangle |\psi\rangle |\phi\rangle &= \frac{1}{|C_z^{\perp}|} \sum_{z,\xi \in \in C_z^{\perp}} (1 - \mathbf{SWAP}) |0\rangle |\psi + z\rangle |\phi + \xi\rangle \\
&= \frac{1}{\sqrt{2}|C_z^{\perp}|} \sum_{z,\xi \in \in C_z^{\perp}} H |\pm\rangle \Big(|\psi + z\rangle |\phi + \xi\rangle \pm |(\phi+\xi)_i (\psi+z)_{/i}\rangle |(\psi+z)_i (\phi+\xi)_{/i}\rangle \Big) \\
\Rightarrow \mathbf{Pr}[|0\rangle] &= \frac{1}{4|C_z^{\perp}|^2} (\\
& 2|C_z^{\perp}|^2 + 2 \sum_{z',\xi',z,\xi \in \in C_z^{\perp}} \\
& \overbrace{\Big(\langle \psi + z'| \langle \phi + \xi'| |(\phi+\xi)_i (\psi+z)_{/i}\rangle |(\psi+z)_i (\phi+\xi)_{/i}\rangle \Big)}^{A} + \\
& \overbrace{\Big(\langle (\phi+\xi')_i (\psi+z')_{/i}| \langle (\psi+z')_i (\phi+\xi')_{/i}| |(\phi+\xi)_i (\psi+z)_{/i}\rangle |(\psi+z)_i (\phi+\xi)_{/i}\rangle \Big)}^{B} \\
&)
\end{aligned}$$

$$\begin{aligned}
A &= \langle \psi + z'| |(\phi+\xi)_i (\psi+z)_{/i}\rangle \langle \phi + \xi'| |(\psi+z)_i (\phi+\xi)_{/i}\rangle \\
&= \begin{cases} 0 & z' \neq z \text{ Assume that } d(C_z^{\perp}) > 1 \\ 1 & z' = z, \text{ and } (\psi+z)_i = (\phi+\xi)_i \end{cases}
\end{aligned}$$

And the equalitiy $(\psi+z)_i = (\phi+\xi)_i$ holds if ethir both ψ, ϕ agree and z, ξ agree on i or both pair disagree.

Lemma 1. *Denote by X_z the r.v indecates that $(\psi+\phi+z)_i = 0$ where the probability is over i. Then:*

$$\mathbf{Pr}\left[\sum_{z\in C_z^{\perp}} X_z > \left(1-\frac{d}{2n}\right)|C_z^{\perp}|\right] \le 1-\frac{d}{2n}$$

Proof. Noicte that by the conditial probability formula we have that:

$$\begin{aligned}
\mathbf{Pr}_i\left[X_z=1\right] &= \mathbf{Pr}\left[X_z=1 \mid z_i=1\right]\cdot \mathbf{Pr}\left[z_i=1\right] \\
&\quad + \mathbf{Pr}\left[X_z=1 \mid z_i=0\right]\cdot \mathbf{Pr}\left[z_i=0\right] \\
&\le \mathbf{Pr}_i\left[z_i=1\right] + \mathbf{Pr}_i\left[\phi_i=\psi_i\right]\cdot \mathbf{Pr}\left[z_i=0\right] \\
&\le \mathbf{Pr}_i\left[z_i=1\right] + \left(1-\frac{d\left(C_x/C_z^{\perp}\right)}{n}\right)\cdot \mathbf{Pr}\left[z_i=0\right] \\
&\le \mathbf{Pr}_i\left[z_i=1\right] + \mathbf{Pr}_i\left[z_i=0\right] - \frac{d\left(C_x/C_z^{\perp}\right)}{n}\cdot\left(1-\frac{d\left(C_z^{\perp}\right)}{n}\right) \\
&\le 1-\frac{d\left(C_x/C_z^{\perp}\right)}{n}+\frac{d\left(C_z^{\perp}\right)\cdot d\left(C_x/C_z^{\perp}\right)}{n^2} \\
\Rightarrow \mathbf{E}\left[\sum_{z\in C_z^{\perp}} X_z\right] &\le \left(1-\frac{d\left(C_x/C_z^{\perp}\right)}{n}+\frac{d\left(C_z^{\perp}\right)\cdot d\left(C_x/C_z^{\perp}\right)}{n^2}\right)|C_z^{\perp}|
\end{aligned}$$

$$\begin{aligned}
\sum_{z\in C_z^{\perp}} \mathbf{Pr}_i\left[z_i=1\right] &= |C_z^{\perp}| \sum_{z\in C_z^{\perp}} \mathbf{Pr}_i\left[z_i=1 \mid z\right]\cdot \mathbf{Pr}\left[z\right] \\
&= |C_z^{\perp}| \sum_{i\in[n]} \mathbf{Pr}_z\left[z_i=1 \mid i\right]\cdot \mathbf{Pr}\left[i\right] \\
&\le |C_z^{\perp}|\frac{1}{n}\sum_{i\in[n]} \mathbf{Pr}\left[\text{sample generator in the support of } i\right] \\
&\le |C_z^{\perp}|\frac{1}{n}\cdot n\frac{2^{\Delta}}{2^{\dim C_z^{\perp}}} = 2^{\Delta} \\
\Rightarrow \mathbf{E}\left[\sum_{z\in C_z^{\perp}} X_z\right] &\le \left(1-\frac{d\left(C_x/C_z^{\perp}\right)}{n}+\frac{2^{\Delta}}{|C_z^{\perp}|}\right)|C_z^{\perp}|
\end{aligned}$$

□