$\sqrt{n} \mapsto \Theta(n)$ Magic States 'Distillation' Using Quantum LDPC Codes.

David Ponarovsky

August 15, 2024

1 The Construction.

Let x_0 be a codeword of $C_X/C_Z^{\perp}$, Denote by $w \in \mathbb{F}_2^n$ the binary string presents the Z-generator that anti commute with the X-generator corresponds to x_0. Let $\mathcal{X} = \{x_0, x_1, ..x_{k'}\} \in \mathbb{F}_2^n$ be a subset of a base for the code $C_X/C_Z^{\perp}$. Such $(\text{ span } \mathcal{X}/x_0\ )|_w$ is Triorthogonal code. Let us denote by $\mathcal{X}'$ the base $\{y_1, y_2, .., y_{k'}\} \in \mathbb{F}_2^n$ defined such: $y_i = x_j + x_0$.

Denote by E the circuit that encodes the logical ith bit to y_i, by $T^{(w)}$ the application of T gates on the qubits for which w act non trivial, means $T^{(w)}$ is a tensor product of T's and identity where on the ith qubit $T^{(w)}$ apply T if w_i is 1 and identity otherwise. And finally by D denote the gate that decode binary strings in $\mathbb{F}_2^n$ back into the logical space.

Let $|\mathcal{X}'\rangle \propto \sum_{x \in \text{span } \mathcal{X}'} |x\rangle$.

2 Proof of Theorem 1.

Definition 2.1. *Let Δ be a constant integer, $C_0, \tilde{C}_0$ codes over Δ bits such $\tilde{C}_0$ is Triorthogonal and $C_0^{\perp}$ contains $\tilde{C}_0$, C_0 has parameters $\Delta[1, \delta_0, \rho_0]$, and $C_0^{\top}$ has relative distance greater than δ_0. Let C_{Tanner} be a Tanner code, defined by taking an expander graph with good expansion and C_0 as the small code. Let $C_{initial}$ be the dual-tensor code obtained by taking $(C_{Tanner}^{\perp} \otimes C_{Tanner}^{\perp})^{\perp}$. Notes that first this code has positive rate and $\Theta(\sqrt{n})$ distance, second this code is an LDPC code as well. Notice also that $C_{initial}^{\top}$ obtained by transporting the parity check matrix, and therefore equals to $(C_{Tanner}^{\top,\perp} \otimes C_{Tanner}^{\top,\perp})^{\perp}$. Hence $C_{initial}^{\top}$ has a square root distance as well.*

Let Q the CSS code, obtained by taking the Hyperproduct of $C_{initial}$ with itself. So Q is an quantum qLDPC code with parameters $[n, \Theta(n^{\frac{1}{4}}), \Theta(n)]$.

Claim 2.1. *There exists family of non-trivial distance quantum LDPC codes Q such the codes span $\mathcal{X}'$ chosen respect to them has a positive rate. Furthermore, the rate of span $\mathcal{X}'$ is a asymptotically converges to Q rate:*

$$|\rho(Q) - \rho(\textit{span } \mathcal{X}')| = o(1)$$

Proof. Pick x_0 and $w \in \mathbb{F}_2^n$, which correspond to the supports of anti commute X and Z generators, such that w can be obtains by setting a codeword of C_{Tanner} on the first $n^{\frac{1}{4}}$ bits and padding by zeros the rest. Clearly, $|w| = \Theta(n^{\frac{1}{4}})$.

Now for defying span $\mathcal{X}$, we are going to consider the parity checks matrix obtained by adding restrictions to C_X's restrictions as follows: Divide the first w bits into Δ-size buckets, define by $w(i)$ the ith coordinate on which w isn't trivial. For example if $w(1) = j$ then j is the first nonzero coordinate of w, Denote by $B_1, B_2, .., B_{|w|/\Delta}$ the partion of w's bits:

$$\begin{aligned} B_1 &= \{w(1), w(2), .., w(\Delta)\} \\ B_2 &= \{w(\Delta+1), w(\Delta+2), .., w(2\Delta)\} \\ B_i &= \{w((i-1)\Delta+1), w((i-1)\Delta+2), .., w(i\Delta)\} \end{aligned}$$

Then let span $\mathcal{X}$ be all the codewords of $C_X/C_Z^\perp$ satisfying $\tilde{C}_0$ restrictions for each bucket, Let us name the union of $\tilde{C}_0$ restrictions over the buckets by B. The dimension of the space satisfies both C_X restrictions and B is at least:

$$\rho(C_X)\cdot n - |B|\cdot(1-\rho(\tilde{C}_0))\Delta \geq \rho(C_X)\cdot n - n^{\frac{1}{4}}$$

And by the fact that the dimension of $C_Z^\perp$'s codewords satisfying B is strictly lower then $\dim C_Z^\perp$, we get the following lower bound:

$$\begin{aligned}\dim \text{span}\ \mathcal{X} &\geq \rho(C_X)\cdot n - n^{\frac{1}{4}} + \rho(C_Z)\cdot n - n \\ &\geq \rho(Q) - n^{\frac{1}{4}}\end{aligned}$$

□

Remark 2.1. *We emphasise that the above proof can be easily adapted to result the following for general CSS codes:*

$$|\rho(Q) - \rho(\textit{span}\ \mathcal{X}')| = d(Q)(1-\rho(\tilde{C}_0))$$

For example lets consider the quantum Tanner code. Since the distance of the quantum Tanner codes is $\sim n/\Delta$, where Δ^2 is the degree of the square complex graph, (obtained by taking a codeword for which each local view of it is supported only on rows correspond to a specific single left generator), we get that for any $\rho \in (0, \frac{1}{2})$ one there is a good qLDPC such that the dimension of span $\mathcal{X}'$ obtained respecting to it $\geq (1-2\rho)^2 n - n/\Delta\cdot(1-\rho(\tilde{C}_0))$.

Claim 2.2. *There is a family of quantum circuits $\mathcal{C}$ consists of Clifford gates and at most $o(\sqrt{n})$ number of T gates such that:*

$$T^{(w)}\,|\mathcal{X}' + C_Z^\perp\rangle \propto E\,\mathcal{C}\ (TH)^{\rho\left(\textit{span}\ \mathcal{X}'\right)n}\,|0\rangle$$

Proof. Let $\tau \in$ span $\mathcal{X}' + C_Z^\perp$, applying $T^(w)$ on $|\tau\rangle$ add phase of $i\frac{\pi}{4}\,|\tau|_w$ □