

Magic States Distillation Using Quantum LDPC Codes.

David Ponarovsky

March 4, 2024

1 Good Codes With Large Λ .

Definition 1.1. Let $M \in \mathbb{F}_2^{k \times n}$ upper triangular matrix such that $k < n$. We say that M has the 1-stairs property if $M_{ij} = 1$ any $j < i$.

Claim 1.1. Any $M \in \mathbb{F}_2^{k \times n}$ upper triangular matrix can be turn into upper triangular matrix that has the 1-stairs property by elementary operation.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

Proof. Consider the following algorithm: Let M be our initial matrix. We iterate over the rows from left to right. In the i th iteration, we check for any row $j < i$ if $M_{ji} = 1$. If not, we set M to be the matrix obtained by adding the i th row to the j th row. Since M is an upper triangular matrix, adding the i th row does not change any entry M_{js} for $s < i$. Therefore, the obtained matrix is still an upper triangular matrix and the entries at M_{js} for $j, s < i$ remain the same, namely 1 if and only if $j \leq s$.

Continuing with the process eventually yields, after k iterations, a matrix with the 1-stair property. \square

Claim 1.2. Let C be a $[n, k, d]$ binary linear code, and let Λ be subcode $\Lambda \subset C$ at dimension k' and distance d' . Then there exists a code $C' = [\leq 2n, \geq k - k'/2, d]$ and a subcode of it Λ' in it at dimension $\geq k'/2$ and distance d' , such:

1. For every $x \in \Lambda'$ and $y \in C'$ $x \cdot y = 0$
2. For every $x \in \Lambda'$ and $y, z \in C'$ $x \cdot y \cdot z = 0$

Proof. First, we can assume that the generator matrix of C is an upper triangular matrix, such that the first k' rows span Λ . Notice that after applying the algorithm from claim 1.1 starting from the first row and stopping at the k' th row, the first k' rows are kept in Λ . So let's assume that is the form of the generator matrix.

Now, let's consider the following process: going uphill, from right to left, starting at the k' row. Initially, set $j \leftarrow k'$ and in each iteration, advance it to be the index of the next row, namely $j \leftarrow j - 1$. In each iteration, ask how many rows G_m , such that $m \leq j$, satisfy $G_m G_j = 0$ and how many pairs of rows $G_m, G_{m'}$ such that $m, m' \leq j$ satisfy $G_m \cdot G_{m'} \cdot G_j = 0$. Denote by p the probability to fall on unsatisfied equation from the above.

- If $p \geq \frac{1}{2}$ then we move on to the next iteration.
- Otherwise, we encode the j th coordinate by C_0 , which maps $1 \rightarrow w$ such that $w \cdot w = 0$. This flips the value of $G_m G_j$ for any pair and $G_m G_{m'} G_j$ for any triple such that $m, m' \leq j$, so we get that the majority of the equations are satisfied. Also notice that the concatenation doesn't change the value of any multiplication at the form $G_m G_{j'}$ for $j' > j$. Therefore, for any $j < j' \leq k'$ the number of the satisfied equations relative to j' is not changed, meaning it is still the majority.

Set G to be the new matrix after the concatenation by C_0 .

In the end of the process G is going to be the generator matrix of C' . It's left to construct Λ' , we are going to do so by taking from the k' rows a subset that satisfies the desired property in Claim 1.2.

Let S be the set of rows among the first k' rows for which there is at least one unsatisfied equation. We will now prove that if k' is large enough, specifically linear in k , then $|S|$ is small enough to obtain Λ' by removing the rows in S .

Observe that the number of satisfied equations is at least:

$$\begin{aligned} & \frac{1}{2} (k' - 1 + (k' - 1)^2) + \frac{1}{2} (k' - 1 + (k' - 1)^2) + \frac{1}{2} (k' - 2 + (k' - 2)^2) + \dots + \frac{1}{2} (1 + (1)^2) \\ &= \frac{1}{2} \left(\binom{k' + 1}{2} + \frac{k'(k' + 1)(2k' + 1)}{6} \right) \end{aligned}$$

So

$$\begin{aligned} |S| \cdot k + |S| \cdot k^2 &\leq k' (k + k^2) - \frac{1}{2} \left(\binom{k' + 1}{2} + \frac{k'(k' + 1)(2k' + 1)}{6} \right) \\ \Rightarrow |S| &< k' - \frac{1}{2} \left(\frac{1}{k^2 + k} \binom{k' + 1}{2} + \frac{1}{k^2 + k} \frac{k'(k' + 1)(2k' + 1)}{6} \right) \\ \Rightarrow |S| &< k' - \frac{k'^3}{24k^2} \end{aligned}$$

Therefore, if $k' \geq \alpha k$ we have that $|S| < (\alpha - \frac{\alpha^3}{24})k$ implies that $\dim \Lambda' \geq \frac{\alpha^3}{24}k$. □

Claim 1.3 (Not Formal). *It is easy to see that by using concatenation again, one can obtain the code $\dim \Lambda' \leftarrow \frac{1}{2} \dim \Lambda'$. For any $x \in \Lambda'$, $|x|_4 = 1$, and for any $x \in C'/\Lambda'$, we have $|x|_4 = 0$.*

[COMMENT] The argument above that the distance d' remain the same is not correct. Yet, if we are defining the distance of any codeword in $C/(C/\Lambda)$ to be greater than d' then we win. (The problem was that gauss elimination might change the weight of rows associate with Λ generators.

2 Distillate $|\Lambda + C_Z^\perp\rangle$ Into Magic.

Claim 2.1. *Suppose that a set of vectors $\Lambda \subset C$ satisfies the relation $xy = 0$ and $xyz = 0$ for any $x, y, z \in \Lambda$. Then, there exists a code C' with a code length roughly equal to C and a subset $\Lambda' \subset C'$ such that for any distinct $x, y, z \in \Lambda'$, $xy = 0$, $xyz = 0$, and $xx =_4 1$.*

Proof. We return to the process in Claim 1.2, but taking the standard upper triangular form of Λ instead the 1-stairs form. Notice that the rows are linear combinations of the original vectors in Λ and therefore also preserve the original relations. So now, for any $j < k$, we have that encoding the M_{jj} bit only affects the multiplication of $u_j u_j$. Thus, we will encode the j th coordinate such that the multiplication of a row by itself is 1 residue 4. □

Claim 2.2. *We can repeat Claim 1.2 by flipping the bit, ensuring that the majority of pairs and triple multiplications are zero. In the end, we will have the following inequality:*

$$|S| \cdot (k + k^2) \leq \frac{1}{2} (k^2 + k^3)$$

And still we will get that $|S| \leq k/2$