Magic States Distillation Using Quantum Expander 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 $j < i$.*

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

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.*

Proof. Consider the following algorithm: Let M be our initial matrix. We iterate over the rows from left to right. In the ith 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 ith row to the jth row. Since M is an upper triangular matrix, adding the ith 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. □

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 $m < j$, satisfy $G_m G_j = 0$ and how many pairs of rows $G_m, G_{m'}$ such that $m, m' < j$ 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 jth 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 $m, m' < j$, so we get that the majority of the equations are satisfied. Set G to be the new matrix after the concatenation by C_0.

Notice that because we iterate on the upper triangular matrix, we don't change the value of $u_m u_{j'}$ for any $j' > j$ (since its jth coordinate was 0 before the encoding, the encoded bit will also be 0, thus not affecting the multiplication).

Denote the set of the obtained vectors by Γ. Let $S \subset \Gamma$ be the group of vectors for which there exists at least one vector in Γ whose multiplication with them is not zero. Note that the total number of pairs with zero multiplication is greater than:

$$\frac{k'-1}{2} + \frac{k'-2}{2} + .. + \frac{2}{2} = \frac{1}{2}\frac{(k'-1)(k'-2)}{2}$$

So

$$|S| \cdot (k'-1) \leq \binom{k'}{2} - \frac{1}{2}\frac{(k'-1)(k'-2)}{2} < \frac{k'(k'-1)}{2} \Rightarrow |S| < \frac{k'}{2}$$

Set $\Lambda' \leftarrow \Gamma / S$. And we got what we wanted.

$\square$

Claim 1.3. *We can repeat Claim 1.2 by considering triple multiplications instead of pair multiplications. Let C_2 and C_3 be the codes obtained from this process. We can then guarantee the existence of $\Lambda_2 \in C_2$ and $\Lambda_3 \in C_3$ such that for any $x, y \in \Lambda_2$, $xy = 0$, and for any triple $x, y, z \in \Lambda_3$, $xyz = 0$. The code $C_2 \otimes C_3$ has a group of codewords Λ_{23} such that for any $x, y, z \in \Lambda_{23}$, $xy = 0$ and $xyz = 0$.*

Claim 1.4. *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 jth coordinate such that the multiplication of a row by itself is 1 residue 4. $\square$

Claim 1.5. *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:*

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

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