

# Magic States Distillation Using Quantum Expander Codes.

David Ponarovsky

March 4, 2024

## 1 Good Codes With Large $\Lambda$ .

**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.

*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.  $\square$

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

**Claim 1.2.** Let  $\Lambda$  be a set of  $k'$  independent codewords in a  $[n, k, d]$  code. Then there exists a code  $C' = [\leq 2n, \geq k - k'/2, d]$  and a set of independent codewords  $\Lambda'$  in it, such that  $|\Lambda'| > \frac{1}{2}|\Lambda|$  and for every pair  $x, y \in \Lambda'$ , we have  $x \cdot y = 0$ .

*Proof.* First, consider the upper triangular matrix obtained by applying Gaussian elimination on  $\Lambda$  that has the 1-stair property. Now, consider the following process: go uphill, from right to left, iterating over the matrix. Let  $j = k$  be the first non-zero coordinate in the bottom row of the matrix. In the  $i$ th iteration, we ask how many rows  $u_m$ , such that  $m < j$ , satisfy  $u_m u_j = 0$ .

- If more than half of such  $u_m$  satisfy the equality, 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  $u_m u_j$  for any pair, so we get that the majority of pairs satisfy the equality.

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

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

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  $\Lambda_{23}$  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  $xx = 1$ .*

*Proof.* We return to the process in Claim 1.2, but taking the standard upper triangular form of  $\Lambda$  instead the 1-stairs form. Notice that the rows are linear combinations of the original vectors in  $\Lambda$  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.  $\square$

**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:*

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

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