The Dual-Tensor Polynomial Code Is Not w-Robust.

David Ponarovsky

April 2, 2023

Abstract

w-Robust codes are among the main ingredients in the novel constructions of good Quantum LDPC and LTC codes made by [Din+22], [LZ22], and [PK21]. The Robustness property grantees that any small weight local view of the codeword will spreads a fraction of it in both direction of the Left Right Cayley Complex. On our way to construct a Locally Testable Quantum Codes we have test a particular case on which the small code set on each local view is the polynomial code and focus on the question is it can be w-robust code. Unfortunately our answer to the that question negative. In this work we share our experience, ideas and insights. We hope that all those would serve others in the task of bringing closer a Quantum PCP Theorem.

1 Preambles

Locally Testable Codes and good Quantum LDPC codes has more in common besides the fact that their existence been, for a long time, an open question that solved at once. For example, It has shown that sampling uniformly a code would be, with probability 1, nether LTC [BHR03] nor qLDPC code. That in totally contrast for many other valuable entities in computer science which can be achieved by random process, such as good classic LDPC codes. Thus it is not a surprise that the recent constructions hings on complex that relatively rich with algebraic structure. And even though those result indeed used for proving the NLTS conjecture [ABN22], Yet one could expect that a construction of a qLTC will follow soon after them.

LTC, are error correction codes such that verifying a uniformly randomly chosen check would be enough to detect any error with probability proportional to its size. Simply put, one can imagine puzzle parts such that any trial to connect pieces in order far from a correct assignment would fail (w.p) at an early step of the process. The analogy for not testability is the case in which the contradiction is observed only in the attempt to putting the last piece.

[AB99]. Besides their clear computational advantage, they are known for their significant roles in the early PCP theorems proofs. And still, the existence of good LTC was considered an open question for decades. Moreover, Sasson proved that codes obtained by the standard randomized constructions could not be LTC [BHR03], which raises the suspicion that maybe codes can not be both good and locally testable. However, recent works by [Din+22], [PK21], and [LZ22] yield a positive answer.

In a nutshell, their sophisticated constructions ensure that no sublinear dependency of restriction exists and yet guarantee that the restrictions are linear far from independent. Namely, no restriction is more important than another, and removing a linear number of constraints would yield the same code.

Their constructions require that the local restrictions, or the local codes, have two properties: the w-robustness and p-resistance for puncturing. Even though they showed probabilistic proof for the existence of an infinite family of such codes, they are more oversized for any practical use. Therefore, we would not formally restate them here; instead, we refer the reader to [LZ22]. Nevertheless, any assumption over the local structure of the code is also an obstacle to encoding a universal computation in the code.

In this work, we propose a new construction for good LTC that demands small codes only to have a large distance. In short, by associating each check with a small code over 2/3-fraction of the vertex's edges, instead of all of them as in the standard Tanner code, we successfully obtain an LTC with a constant rate. Then by considering graphs, such that both the graph and his subgraph obtained by taking an $\frac{1}{2}$-fraction of the edges of each vertex are good expanders, we also succeed in proving that the codes have linear distance.

Finally, we show how to construct such a graph given a Ramanujan *Cayley* graph. Nevertheless, although we succeeded in simplifying the LTC, we still needed to understand how they can be used to encode a universal computation.

2 Background.

2.1 Polynomial Code

. Consider the field $\mathbb{F}_m$ for an arbitrary prime power $m = q^l$ greater than n. The polynomial codes relay on the fact that any two different polynomials in the ring $\mathbb{F}_m[x]$ at degree at most d different by at least $n - d + 1$ points. By define the code to be the subspace contains all the polynomials at degree at most d encoded by n numbers associated with their values. Formally we define:

Definition 1. *Fix $m > n$ to be a prime power and let $a_0, a_1, a_2, \dots a_n$ distinct points of the field $\mathbb{F}_m = R$ and define the code $C \subset R$ as follows:*

$$C = \{p(a_0), p(a_1), p(a_2), \cdots p(a_n) : p \textit{ is polynomial at degree at most } k\}$$

Lemma 1. *Fix the degree of the polynomial code to be at most d. Then the parameters of the code are $[n, d+1, n-d]$.*

Proof. The dimension of the code equals to the dimension of the polynomials space at degree at most d which is spanned by the vectors $e_1, e_2..e_d = 1, x..x^d$ and therefore is $d + 1$. In addition suppose that f, g are different polynomials i.e $f \neq g$.

Hence $h = f - g$ is a non-0 polynomial at degree at most d and therefore has at most d roots. Namely at most d points in which f equals g and at least $n - d$ in which they disagree. Put in another way the distance between any two different codewords of the code is at least $n - d$. □

Notice that encoding naively the aleph-bet of $\mathbb{F}_p$ in binary strings require to pay a factor $\log n$ bits, So the asymptotic rate of the code attends to zero. **[COMMENT]** Add a statement about the vanishing rate of the binary encoded version. And add a paragraph about Tanner code in which each edge correspond to a non binary alpha-bet.

2.1.1 Note On Quantum Polynomial Code.

Let's define the code C such that any state in C is a coset of the polynomials at degree at most d shifted by $x \in \mathbb{F}_p$. In other words the codeword associated with x is the state $|\underline{c}\rangle = \sum_{\substack{f \in \mathbb{F}_d[x] \\ f(0)=0}} |c + f\rangle$. The inner product between any d-degree polynomial with zero free coefficient is:

$$\langle f | x^j \rangle = \sum_{i \leq d} \langle a_i x^i | x^j \rangle = \sum_{i \leq d} a_i \mathbf{E}\left[x^i x^j\right] = \sum_{i \leq d} a_i \mathbf{1}_{i+j=_n 0}$$

[COMMENT] Say some words about the classily testability of the polynomial code, and why for quantum it doesn't work. (The dual space of polynomials of low degree is the subspace of all the polynomials with heigh degree.)

Next, we will review Tanner's construction, that in addition to being a critical element to our proof, also serves as an example of how one can construct a code with arbitrary length and positive rate.

3 The Polynomial-Code Is Not w-Robust.

One idea for constructing is to use the polynomial code instead C_0, The follow form the fact that if one pick degree strictly greater than $\Delta/2$ then $C_0^\perp \subset C_0$ and therefore one could choose C_z to be the same code defined on the negative vertices of the graph.

Here we prove that the dual-tensor code, in that case, is not w-robust, meaning that any such construction should be consider other way for proving the reduction Lemma.

Claim 1. *Let C_0 be the $[\Delta, d, \Delta - d]$ polynomial code. Then any code word in $\left(C_0^\perp \otimes C_0^\perp\right)^\perp$ is a polynomial in $F[x, y]$ at degree at most $\Delta + d$*

Proof. Consider base element $C_0 \otimes \mathbb{F}$, denote it by $c = g_i \otimes e_j$. And notice that c has representation in $F[x, y]$ of $\prod_{y' \neq j} (y - y') g_i(x)$. By the fact that $g_i(x) \in C_0$ we have that degree of c is at most $\Delta + \delta$. Hence any element in the subspace of $C_0 \otimes \mathbb{F}$ is a polynomial at degree at most $\Delta + d$. □

Claim 2. *The dual-tensor polynomial code is not w-robust.*

Proof.

$$\begin{aligned} P(x,y) &= \prod_{i\neq\Delta-1}(x+iy) = \prod_{i\neq 1}(x-iy) \\ P(x,x) &= \prod_{i\neq\Delta-1}(x+ix) = x^{\Delta-1}\prod_{i\neq\Delta-1}(1+i) = (\Delta-1)! =_\Delta -1 \neq_\Delta 0 \end{aligned}$$

□

References

[AB99] Dorit Aharonov and Michael Ben-Or. *Fault-Tolerant Quantum Computation With Constant Error Rate*. 1999. arXiv: quant-ph/9906129 [quant-ph].

[BHR03] Eli Ben-Sasson, Prahladh Harsha, and Sofya Raskhodnikova. "Some 3CNF Properties Are Hard to Test". In: *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*. STOC '03. San Diego, CA, USA: Association for Computing Machinery, 2003, pp. 345–354. ISBN: 1581136749. DOI: 10.1145/780542.780594. URL: https://doi.org/10.1145/780542.780594.

[PK21] Pavel Panteleev and Gleb Kalachev. *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes*. 2021. DOI: 10.48550/ARXIV.2111.03654. URL: https://arxiv.org/abs/2111.03654.

[ABN22] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. *NLTS Hamiltonians from good quantum codes*. 2022. arXiv: 2206.13228 [quant-ph].

[Din+22] Irit Dinur et al. *Good Locally Testable Codes*. 2022. DOI: 10.48550/ARXIV.2207.11929. URL: https://arxiv.org/abs/2207.11929.

[LZ22] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes*. 2022. arXiv: 2202.13641 [quant-ph].