

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 guarantees that any small weight local view of the codeword will spread a fraction of it in both directions of the Left Right Cayley Complex. On our way to construct Locally Testable Quantum Codes we have tested 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 that question is 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 (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.

Likewise Quantum LDPC codes (qLDPC), are also an error correction codes, Though that qLDPC encode qubit instead bits, and for been considered good they have to protect against to type of error, and obviously their decoders have to be designed such that any attempt to detect or fix an one type error would not cause second type error.

Good LTC and qLDPC have 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, neither LTC [BHR03] nor qLDPC code. That stands 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 hinge on complex that has 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.

Here we shatter light on that wondering by point on one reason that cause the naive-straight approach to fail.

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 rely on the fact that any two different polynomials in the ring $\mathbb{F}_m[x]$ at degree at most d differ 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:

$$C = \{p(a_0), p(a_1), p(a_2), \dots, p(a_n) : p \text{ is polynomial at degree at most } d\}$$

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 $e_1, e_2, \dots, e_d = 1, x, \dots, x^d$ 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 $n - d$. \square

Notice that encoding naively the alphabet 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 alphabet.

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 $|\underline{c}\rangle = \sum_{f(0)=0}^{f \in \mathbb{F}_d[x]} |c + f\rangle$. The inner product between any d -degree polynomial with zero free coefficient is:

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

[COMMENT] Say some words about the classical 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 high 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 from 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 $(C_0^\perp \otimes C_0^\perp)^\perp$ 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 $\Delta + d$. \square

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

Proof.

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

\square

References

- [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](https://doi.org/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](https://arxiv.org/abs/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](https://arxiv.org/abs/2206.13228) [quant-ph].
- [Din+22] Irit Dinur et al. *Good Locally Testable Codes*. 2022. DOI: [10.48550/ARXIV.2207.11929](https://arxiv.org/abs/2207.11929). URL: <https://arxiv.org/abs/2207.11929>.
- [LZ22] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes*. 2022. arXiv: [2202.13641](https://arxiv.org/abs/2202.13641) [quant-ph].