Ligerito: A Fast and Concretely Small Multilinear Polynomial Commitment Scheme

XXX

Soon 2025

Abstract

XXX

1 Introduction

In this short note, we

2 Notes

High level idea: we would like to reduce checking that some vector x is close to a tensor encoding, in the sense that there exists some $\tilde{x}$ such that $(G_\ell \otimes \cdots \otimes G_1)\tilde{x}$ and x are close. In particular, we will view x as a tensor which is (hopefully) encoded via the tensor code $G_\ell \otimes \cdots \otimes G_1$. We will show a protocol that both verifies that there is a unique correctly-encoded tensor 'closest' to x and that the reductions of each tensor to a smaller correspond to (partial) evaluations of a multilinear polynomial whose coefficients are $\tilde{x}$.

Basic check. From the tensor distance check of [**?**], we know that, given uniformly sampled $r \in \mathbf{F}^k$ and $S \subseteq \{1, \dots, m\}$, if a matrix $X \in \mathbf{F}^{m \times 2^k}$ satisfies

$$X_S \bar{g}_r = \bar{X}_S G'^T \qquad \text{and} \qquad \bar{X}_S \bar{g}_r = G_S y_r,$$

for some y_r depending on r but not on S and some $\bar{X}_S$, then we know that, with high probability, there exists a unique matrix $\tilde{X}$ such that $\|X - G\tilde{X}G'^T\| < d/3$ and

$$X_S = G_S \tilde{X} G'^T \qquad \text{and} \qquad y_r = \tilde{X}\bar{g}_r. \tag{1}$$

The probability of error here is bounded from above by, setting $\delta = d/m$,

$$\left(1 - \frac{\delta}{3}\right)^{|S|} + \frac{k(d+9)}{|\mathbf{F}|}. \tag{2}$$

(Note that the distance of G' does not matter in this particular test; intuitively this is because we are verifying that the each of the S rows are completely correctly encoded.)

Basic operations. Given a vector $x \in \mathbf{F}^{mn}$, we will write the 'natural' operation

$$\mathbf{Mat} : \mathbf{F}^{mn} \to \mathbf{F}^{m \times n}$$

which interprets the mn-sized vector x as an $m \times n$ matrix, row-wise. More specifically, the first row of $\mathbf{Mat}(x)$ corresponds exactly to the first n entries of x, and so on, with the dimensions clear from context. Unfortunately, this 'row-major' construction, which clashes with the standard 'column-major' construction, is unavoidable here without introducing additional complexity down the line.

Although not used later, it is also possible define the inverse operation, $\mathbf{vec} : \mathbf{F}^{m \times n} \to \mathbf{F}^{mn}$, which simply stacks the rows of the input matrix into an mn-sized vector, such that $\mathbf{vec}(\mathbf{Mat}(x)) = x$.

Kronecker product. The *Kronecker product* of two matrices $G \in \mathbf{F}^{m \times n}$ and $G' \in \mathbf{F}^{m' \times n'}$ is written $G \otimes G' \in \mathbf{F}^{mm' \times nn'}$ and is defined as

$$G' \otimes G = \begin{bmatrix} G'_{11}G & G'_{12}G & \dots & G'_{1n'}G \\ \vdots & \vdots & \ddots & \vdots \\ G'_{m'1}G & G'_{m'2}G & \dots & G'_{m'n'}G \end{bmatrix}.$$

First, this operation is easily shown to be associative; *i.e.*, for another matrix $G'' \in \mathbf{F}^{m'' \times n''}$ we have

$$(G'' \otimes G') \otimes G = G'' \otimes (G' \otimes G),$$

so we may write $G'' \otimes G' \otimes G$ without ambiguity. We will constantly use the fact that this operation is associative in what follows. Note also that, for any $x \in \mathbf{F}^{nn'}$, using the above definition, we know

$$\mathbf{Mat}((G' \otimes G)x) = G'\mathbf{Mat}(x)G^T,$$

which also serves as another definition of the Kronecker product that we use throughout the text. (It is very important to note here that, due to the row-major ordering of the $\mathbf{Mat}$ operation, the product is reversed from many standard linear algebra texts.) Another useful consequence of this definition is that, for some provided $x \in \mathbf{F}^{2^k}$ and $r_1, \dots, r_k \in \mathbf{F}$, we may interpret

$$x^T((1 - r_1, r_1) \otimes \dots \otimes (1 - r_k, r_k)), \tag{3}$$

as the evaluation of a multilinear polynomial of k variables, with coefficients in x, at the point $(r_1, \dots, r_k)$. (Care has to be taken in interpreting the individual entries of x as coefficients over the different possible monomials, but this is a good exercise for the reader not deeply familiar with linear algebra.)

Structured randomness. For convenience, we will define, for a vector $r \in \mathbf{F}^k$, the 'structured random' vector

$$\bar{g}_r = (1 - r_1, r_1) \otimes \dots (1 - r_k, r_k),$$

which results in a vector with dimensions $\bar{g}_r \in \mathbf{F}^{2^k}$. When the values $r \in \mathbf{F}^k$ are uniformly randomly drawn, this type of structured vector is sometimes called 'logarithmically random' [**?**]. From before (3), we can interpret the product $\bar{g}_r^T x$ as the evaluation of a multilinear polynomial over k variables, with coefficients in x, at the point $(r_1, \dots, r_k)$.

3 Protocol

3.1 General reduction

High level idea. The reduction is simple at a high level. We begin with any $x \in \mathbf{F}^{mm'}$ and a tensor code $G \otimes G'$. We would like to reduce checking that x uniquely decodes to some message $\tilde{x}$ to checking some smaller claim of the same form. Doing this, we will also see that, as a byproduct, we get a partial evaluation of $\tilde{x}$ on some uniformly randomly chosen coefficients, when $\tilde{x}$ is interpreted as the coefficients of a multilinear polynomial, at a random point. To do this, we will use the basic check presented previously. First, we may verify that x is indeed close to some tensor codeword by using the basic check presented previously on $\mathbf{Mat}(x)$:

$$\mathbf{Mat}(x)_S = \bar{X}_S G'^T \qquad \text{and} \qquad \bar{X}_S \bar{g}_r = G_S y_r. \tag{4}$$

If this is true, the claim is satisfied by the conclusions of (1). Unfortunately, it is difficult to verify the latter claim in (4): in the standard protocol (used in the tensor distance check of [**?**]), verifying this latter claim involves sending the complete vector y_r which may be very large, as we will see next. Instead, we will have the prover commit to a new vector, which we will call z_r, which it claims satisfies $(z_r)_S = G_S y_r$, for some (unknown to the verifier) y_r. The claim (4) will then be

$$\mathbf{Mat}(x)_S = \bar{X}_S G'^T \qquad \text{and} \qquad \bar{X}_S \bar{g}_r = (z_r)_S \qquad \text{and} \qquad (z_r)_S = G_S y_r. \tag{5}$$

Now, it suffices only to prove that the committed vector z_r, when opened at the S positions, is indeed equal to the correct encoding (via G only, instead of $G \otimes G'$) of some message.

Observation. In standard Ligero and its tensor variation used in ZODA, as mentioned before, the standard way of verifying this is to send z_r (or its corresponding message y_r) and have the verifier check the encoding (or encode the message) and verify equality at the corresponding S entries. On the other hand, if G is itself a tensor code, say $G = G_2 \otimes G_1$, then the proposition $(z_r)_S = G_S y_r$ is implied by the conclusion of (1) except over G_1 and G_2. (See figure XXX.) This means that we can use the same check, again, to reduce verifying that z_r is close to a good tensor encoding down to a simpler claim, which is, in turn, even smaller.

Construction. Writing this out, let $G_1 \otimes \cdots \otimes G_\ell$ be a tensor code. Let $d_1, \dots, d_\ell > 0$ be the distances and $\delta_1, \dots, \delta_\ell$ be the relative distances of each matrix and define $d = d_1 \dots d_{\ell-1}$. We will show that there exists a unique $\tilde{x}$ such that $\|\mathbf{Mat}(x) - (G_1 \otimes \cdots \otimes G_{\ell-1})\mathbf{Mat}(\tilde{x})G_\ell^T\| < d/3$ and that $\tilde{x}^T(\bar{g}_{r_1} \otimes \cdots \otimes \bar{g}_{r_k}) = t$ if the following tests pass

$$\mathbf{Mat}(z^{(i)})_{S_i} = \bar{X}_{S_i}^{(i)} G'^T \qquad \text{and} \qquad \bar{X}_{S_i}^{(i)} \bar{g}_{r_i} = z_{S_i}^{(i+1)},$$

for $i = 1, \ldots, \ell - 1$, where $z^{(1)} = x$, and S_{i-1} is defined as the subset of rows which contain the indices of S_i after these indices are passed through the $\mathbf{Mat}$ operation. (See figure **??**.) The error probability of this test is

$$\sum_{i=1}^{\ell-1} \left(\left(1 - \frac{\delta_1 \ldots \delta_i}{3}\right)^{|S_i|} + \frac{k_i(d_1 \ldots d_i + 9)}{3|\mathbf{F}|} \right). \tag{6}$$

Note that we may choose $|S_i| \geq -\lambda / \log(1 - \delta_1 \ldots \delta_i)$, where λ is the natural log of the desired error probability; or, if the matrices G_i are all the same code, this is simply $|S_i| \geq -\lambda / \log(1 - \delta^i)$. While this exponential decay in relative distance may seem problematic, we will show that, by appropriately choosing the rank ℓ of the tensor code, we receive a total proof size of roughly $\lambda C \exp(C' \sqrt{\log(N)})$ that is smaller than N^ε for any $\varepsilon > 0$, where N is the number of elements of $\tilde{x}$, but asymptotically larger than $\log^c(N)$ for any $c > 0$.

3.2 Protocol

Prover algorithm. The prover algorithm is relatively simple. It begins with some vector $\tilde{x} \in \mathbf{F}^{2^{k_1 + \cdots + k_\ell}}$ and code matrices $G_i \in \mathbf{F}^{m_i \times 2^{k_i}}$ for $i = 1, \ldots, \ell$, then proceeds as follows.

1. Set $x = z^{(1)} = (G_1 \otimes \cdots \otimes G_\ell)\tilde{x}$
2. For $i = 1, \ldots, \ell - 1$, receive uniform randomness $r_i \in \mathbf{F}^{k_i}$, compute and commit to

   $$z^{(i+1)} = (G_i \otimes \cdots \otimes G_\ell)\mathbf{Mat}(\tilde{x})(\bar{g}_{r_i} \otimes \cdots \otimes g_{r_1});$$

   note that the dimensions for the $\mathbf{Mat}$ operation are clear from context XXX: Check indices
3. Send the entirety of $z^{(\ell)}$

Note that, if G_i are systematic codes, it is not necessary to recompute the complete Kronecker product in step 2 at every iteration: it suffices only to take the systematic part over the ith axis and take the random linear combination of this result. Also the commitment to $z^{(\ell)}$ is unnecessary since the entire vector is being sent. XXX: Clarify

Verifier algorithm. The verifier algorithm is also relatively simple. We assume that the verifier only has access to a small number of entries of the vectors $z^{(i)}$.

1. Uniformly randomly sample some set $S_1 \subseteq \{1, \ldots, (m_1 \ldots m_\ell)\}$
2. For $i = 1, \ldots, \ell - 1$ perform the following:

(a) Receive S_i rows of $\mathbf{Mat}(z^{(i)}) \in \mathbf{F}^{(m_{i+1} \dots m_\ell) \times m_i}$

(b) Verify that the S_i rows of $\mathbf{Mat}(z^{(i)})$ are encodings via G_i of some message $\bar{X}^{(i)}_{S_i}$

(c) Check that $\bar{X}^{(i)}_{S_i} \bar{g}_{r_i} = z^{(i+1)}_{S_i}$

(d) Set S_{i+1} to be the indices of rows that contain at least one index of S_i XXX: clarify

3. Verify that $z^{(\ell)}$ is a codeword of G_ℓ

Proof. The proof of the error bound is essentially by induction. The base case is exactly the basic check: when the code is $G_1 \otimes G_2$, the conclusions of the check (1) is satisfied directly.

References