A Note on Ligero and Logarithmic Randomness

Guillermo Angeris* gangeris@baincapital.com
Alex Evans aevans@baincapital.com
Gyumin Roh min@succinct.xyz

September 2024

Abstract

We revisit the Ligero proximity test and its logarithmic randomness variant in the framework of [EA23]. We also show a simple proof that improves the soundness error of the original logarithmic randomness construction of [DP23] by a factor of two. This note was originally given as a presentation in ZK Summit 11.

Introduction

In this short note, we will make use of the framework of [EA23] to explain the Ligero [AHIV17] protocol and its variants, such as the ones presented in [DP23]. In particular, we will show, using this framework, that Ligero can be viewed as a simple protocol that proves that a matrix-vector product was correctly performed for an ahead-of-time fixed, but otherwise unknown, matrix. (We note this is already shown in [AHIV17], but we focus on this as its main use case.) We then give a self-contained and short proof of the logarithmic randomness extension constructed first by [DP23], which allows for slightly more structured randomness. Our proof in this note slightly improves the error probability and uses the tools of [EA23].

1 Notation and conventions

We use the same notation and conventions as [EA23], which we quickly review here. For (much) more, including proofs of these statements, see [EA23, §1].

Probabilistic implications. Given some statements P_r and $Q_{r'}$ each depending on some random variables r and r', we say that

$$P_r \underset{p}{\implies} Q_{r'},$$

*Authors are listed in alphabetical order.

if $\Pr(P_r \wedge \neg Q_{r'}) \leq p$, where we call p the *error probability* (sometimes known as the *soundness error*). This is a relaxation of traditional logic, which is the case where the error probability $p = 0$. Note that the distribution from which r and r' are drawn is otherwise arbitrary and is specified in the text. (In almost all cases, we will either have $r' = r$, or r and r' independently drawn.) A simple exercise shows that, if

$$P_r \underset{p}{\implies} Q_{r'} \quad \text{and} \quad Q_{r'} \underset{p'}{\implies} T_{r''},$$

then

$$P_r \underset{p+p'}{\implies} T_{r''},$$

where we make no assumptions about the distribution from which r, r', and r'' are drawn. In general, we sometimes call probabilistic implications *tests* since they greatly strengthen our belief about the conclusion, but do not guarantee it; *i.e.*, they are a type of *statistical test* about an object which we might not have direct access to.

1.1 Linear algebra

All linear algebra in this note will be over some finite field $\mathbf{F}$.

Basic results. We will only rely on two important results from linear algebra over finite fields. The first is that any vector (sub)space $V \subseteq \mathbf{F}^m$ has a basis which forms the columns of a matrix $T \in \mathbf{F}^{m \times n}$ such that, for every vector $y \in V$, there is a unique $x \in \mathbf{F}^n$ such that

$$y = Tx.$$

(In this case n is often called the *dimension* of the subspace V.) We write the *range* of T as $\mathcal{R}(T)$ which is the set of all linear combination of the columns of T. The fact above can then be restated as: for any subspace $V \subseteq \mathbf{F}^m$, there exists a matrix $T \in \mathbf{F}^{m \times n}$ with linearly-independent columns such that $\mathcal{R}(T) = V$. The second fact is that, if some matrix T has linearly-independent columns then it is *injective*. As a reminder, T has linearly independent columns if

$$Tx = 0 \qquad \text{implies} \qquad x = 0.$$

Such a matrix T must be injective since, if $Tx = Ty$, then

$$T(x - y) = 0 \qquad \text{implies} \qquad x = y.$$

Weight. We will also define the (Hamming) *weight* of a vector $x \in \mathbf{F}^n$ as

$$\|x\| = |\{i = 1, \ldots, n \mid x_i \neq 0\}|.$$

In English: the weight of a vector x, written $\|x\|$, is the number of nonzero entries of x. Note that the weight $\|\cdot\|$ is almost, but not quite, a norm as it satisfies the triangle inequality: for $x, y \in \mathbf{F}^m$ we have

$$\|x + y\| \leq \|x\| + \|y\|,$$

definiteness,

$$\|x\| = 0 \quad \text{if, and only if,} \quad x = 0,$$

and 0-homogeneity,

$$\|\alpha x\| = \|x\|,$$

for any nonzero $\alpha \in \mathbf{F}$. (The weight is not quite a norm since norms must satisfy 1-homogeneity.)

Weight of a matrix. It will be very useful in what follows to overload notation slightly and define the weight for a matrix $X \in \mathbf{F}^{m \times n}$, which we write

$$\|X\| = \text{number of nonzero rows of } X.$$

This definition also satisfies the triangle inequality since, for $X, Y \in \mathbf{F}^{m \times n}$,

$$\|X + Y\| \leq \|X\| + \|Y\|,$$

along with definiteness and 0-homogeneity. It also satisfies the following two useful facts. First, for any vector $z \in \mathbf{F}^n$, we have that

$$\|Xz\| \leq \|X\|. \tag{1}$$

(The symbols here must be parsed very carefully: on the left hand side we are taking the weight of a vector Xz, resulting from a matrix-vector product, while on the right hand side we are taking the weight of a matrix X as defined above.) Second, if we interpret some n vector $x \in \mathbf{F}^n$ as an n-by-1 matrix, then the definition of weight for the vector x and its corresponding n-by-1 matrix coincide exactly. This justifies overloading the notation $\|\cdot\|$ to stand for both the matrix and the vector cases.

Weight of a set. For convenience, we define the weight of a set S (composed of either vectors or matrices) to be

$$\|S\| = \min_{x \in S} \|x\|.$$

In other words, the weight of a set S is the weight of its 'smallest' element. If we write $z - S = \{z - x \mid x \in S\}$ for the (Minkowski) difference of z and S, then we can interpret

$$\|z - S\|,$$

as the distance between the vector z and its 'nearest' vector in the subset S.

Subspace matrices. Finally, given a vector subspace $V \subseteq \mathbf{F}^m$, we write V^n for the set of $m \times n$ matrices whose columns lie in V. Since this is a subspace, note that any linear combination of matrices in V^n is also a matrix with columns in V.

1.2 Error correcting codes

We will not use any deep results from error correcting codes in this note except for two basic definitions.

Distance. We define the *distance* $d \geq 0$ of a code (which we write as a matrix $G \in \mathbf{F}^{m \times n}$) to be

$$d = \min_{x \neq 0} \|Gx\|.$$

(Note that the matrix G is injective if, and only if, its distance $d > 0$.) We similarly define the distance d of a vector subspace $V \subseteq \mathbf{F}^m$ as the smallest nonzero element in the subspace

$$d = \min_{v \in V \setminus \{0\}} \|v\|.$$

Note that when G has linearly independent columns, the distance of G (as a matrix/code) and the distance of its range $\mathcal{R}(G)$ (as a subspace) are the same. One useful consequence of this definition is the fact that, given two vectors $x, y \in \mathbf{F}^n$ if we can show, for some matrix G with distance $d > 0$ that

$$\|G(x - y)\| < d, \tag{2}$$

then, necessarily, we know that $x - y = 0$, or that $x = y$, since $G(x - y) = 0$ and G must be injective since its distance d is strictly positive.

Distance to a subspace. We will constantly make use of the following (nearly-obvious) fact in the proof of this paper. Let V be a subspace with distance at least d, then, any matrix $X \in V^n$ with columns in V, which has weight smaller than d,

$$\|X\| < d,$$

must be the zero matrix, $X = 0$. The proof follows from applying the fact that, if some vector $x \in V$ has weight smaller than d then $x = 0$, to each column of X. One consequence of this fact is that, if any matrix $Y \in \mathbf{F}^{m \times n}$ satisfies

$$\|Y - V^n\| < d/2,$$

then there exists a unique matrix $X \in V^n$ with

$$\|Y - X\| < d/2. \tag{3}$$

This is an easy consequence since, letting $X' \in V^n$ satisfy $\|Y - X'\| < d/2$ implies that

$$\|X - X'\| \leq \|Y - X\| + \|Y - X'\| < d$$

so, since $X - X' \in V^n$, we know that $X - X' = 0$, or that $X = X'$. This fact is often called 'unique decoding' since there exists a unique matrix in V^n closest to Y if the distance between Y and V^n is less than $d/2$.

1.3 Sparsity checks

An important 'primitive' we will use repeatedly in what follows is the ability to probabilistically check that two vectors are 'close' under the norm $\|\cdot\|$. In particular, to check that two vectors $x, y \in \mathbf{F}^m$ are no further apart than, say, some distance q, it suffices to randomly sample a few entries of x and y, and verify that these entries are equal. We can write this in the language of probabilistic implications as

$$(x-y)_S = 0 \quad \underset{p}{\Longrightarrow} \quad \|x-y\| < q, \tag{4}$$

where

$$p \leq \left(1 - \frac{q}{m}\right)^{|S|}, \tag{5}$$

and $S \subseteq \{1, \ldots, m\}$ is a set of uniformly randomly sampled indices of x and y. Here, $|S|$ denotes the cardinality of S; *i.e.*, the number of entries that were randomly sampled and checked. In particular, for any given probability p, this implies that the number of checks $|S|$ required to achieve this error probability p is no more than

$$|S| \leq \left\lceil \frac{m}{q} \log\left(\frac{1}{p}\right) \right\rceil. \tag{6}$$

Here, we have used the bound that $\log(1-t) \leq -t$ for $t < 1$.

Discussion. Note that the above implication is only in one direction: in particular, this implication does *not* say that, if $\|x-y\| < q$, then $(x-y)_S = 0$ with high probability. (Indeed, if $\|x-y\| = q-1$, then the probability of failure is roughly the same as if $\|x-y\| = q$, even though the conclusion is satisfied in the former.) This plays particularly nicely in the case that x and y are known to belong to a subspace V with some distance d. In this case, x and y are equal only when they differ in less than d entries. If so, then it suffices only to randomly sample entries of x and y and check equality of these randomly sampled entries. If these checks all pass, then we know that, with high probability, not only are these vectors close, but, in fact, they must be equal everywhere. This 'amplification of differences' is the reason why error correcting codes are extremely natural in the construction of succinct proofs.

1.4 Interaction model

Throughout this note we will use one simple interaction model. In this model, we send and receive vectors, and we are allowed to access only a small number of rows of some fixed, but otherwise opaque, matrix $X \in \mathbf{F}^{m \times n}$. These models can be practically realized in a number of ways: for example, one could use a Merkle commitment to commit to the rows of X, publish this commitment, and only 'open' up a small number of rows, or one could provide X to a trusted third party who only allows a bounded number of queries.

Matrix-vector products. An important consequence of this interaction model is that we can efficiently query a small number of indices of the matrix-vector product Xv: if we wish to query, say entry i of Xv, it suffices to query the ith row of X, which we will write as $\tilde{x}_i^T$ and take the inner product with v since

$$(Xv)_i = \tilde{x}_i^T v. \tag{7}$$

By assumption on the interaction model, it is easy to query a specific row of the matrix X, so this computation is easy to perform. At a high level, one of our goals will be to make sure that the number of rows we query of the matrix X is small—much smaller than the total number of rows m of X.

Distance of a matrix-vector product. Using the above observation, it is not hard to see that, in this interaction model, we can easily certify that the matrix-vector product Xv is not 'too far' from a given vector, say y, using the sparsity check presented in (4). To do this, pick a random subset $S \subseteq \{1, \dots, m\}$ and then simply verify that

$$(Xv)_S = y_S,$$

which will imply that $\|Xv - y\| \leq q$ with error probability no more than that given in (5). From the observation provided in (7), we know that to compute $(Xv)_S$, it suffices only to request rows S of X, meaning that we only need $|S|$ queries to verify this statement. As an illustrative example, in what follows, q will be roughly $m/3$ and m will be reasonably large, roughly $m \sim 2^{10}$. Making the probability of failure very small, say $p \sim 2^{-80}$, means that the number of rows we need to query is no more than around

$$\lceil 3 \log(2^{80}) \rceil \approx 167,$$

queries, which is much smaller than the naïve deterministic test requiring $2m/3$ queries, which would be on the order of $\sim 2^{10}$ (!).

2 Proximity testing

The second tool we will use in this note is that of a *proximity test*. In a proximity test, we are provided with some vector space $V \subseteq \mathbf{F}^m$ with distance $d > 0$, and we would like to make sure that the columns of some matrix $X \in \mathbf{F}^{m \times n}$ are 'close' to the vector space; *i.e.*, we would like to verify that

$$\|X - V^n\| \leq q, \tag{8}$$

for some *proximity parameter* $q > 0$. Note that, if $q < d/2$ and G is injective and generates the subspace V (*i.e.*, that $\mathcal{R}(G) = V$) then we immediately know that there exists a unique(!) matrix $\tilde{X}$ such that

$$\|X - G\tilde{X}\| \leq q.$$

We will show that there is a very simple probabilistic implication that ensures (8) holds with high probability.

Succinct proximity test. The succinct test is as follows. Let $G' \in \mathbf{F}^{m' \times n}$ be a code with distance $d' > 0$, and let ${g'_r}^T$ be its rth row. Then, the following probabilistic implication is true:

$$\|X g'_r - V\| \leq q \quad \underset{p}{\Longrightarrow} \quad \|X - V^n\| \leq q, \tag{9}$$

where the row index r is uniformly randomly chosen from $1, \ldots, m'$, while the error probability p depends on the distance of G' and the proximity parameter q. We give a concrete bound on p in what follows. Note that, at no point, does the whole matrix G' (which may be extremely large) ever have to be formed: it suffices only to be able to form a specific (randomly sampled) row of G'.

Discussion. We can write the test of (9) in English: to verify that all of the columns of some matrix X are q-close to a vector space V, it suffices to verify that a structured random linear combination of the columns of X (with the randomly chosen coefficients given by g'_r) is q-close to the vector space V, so long as we are willing to accept a probability of error no larger than p. We may view this as a succinct proximity test as we have reduced checking that all of the columns of some matrix X are q-close to a vector subspace to checking that a single vector is q-close to a vector subspace, while potentially taking on some (small) probability of error, p, which we bound next.

This note. In this note, we will show that when the code matrix G' can be written as

$$G' = \underbrace{\tilde{G} \otimes \tilde{G} \otimes \cdots \otimes \tilde{G}}_{k \text{ times}}, \tag{10}$$

where $\tilde{G} \in \mathbf{F}^{|\mathbf{F}| \times 2}$ is the matrix whose rows are of the form $(1 - t, t)$ for each $t \in \mathbf{F}$, the proximity test (9) satisfies

$$p \leq \frac{k(q+1)}{|\mathbf{F}|},$$

for any $q < d/3$. This fact was first discovered by [DP23] and used to construct a protocol to succinctly evaluate a multilinear polynomial at a given point. The bound found in that work, $p \leq 2k(q+1)/|\mathbf{F}|$, is weaker by a factor of 2 compared to the bound above. (While writing this note, the bound was improved to the case of $q < d/2$ when the vector space V has certain properties, with slightly worse probability bound, $p \leq kn/|\mathbf{F}|$, by [DG24, DP24] using techniques from the proof presented below, originally from our presentation [EA24] and private communication.) Our proof of the tighter bound is short, fitting in about a page, and relatively straightforward. For now, we will take the above test (9) as given, describe the protocol, and prove this bound for p later in §4. We will use generic parameters to describe the protocol in what follows.

Extension. We note that the proof provided also has an immediate extension to the slightly more general case where the matrices $\tilde{G}$ are not all the same and are otherwise

arbitrary codes. In this case, if we have matrices $\tilde{G}_i \in \mathbf{F}^{m_i \times 2}$ for $i = 1, \ldots, k$, each with distance $d_i > 0$, and $G' = \tilde{G}_1 \otimes \cdots \otimes \tilde{G}_k$, then

$$p \leq (q+1) \sum_{i=1}^{k} \left(1 - \frac{d_i}{m_i}\right).$$

3 The protocol

In this section we give a simple explanation of Ligero [AHIV17], using the framework of [EA23], as a protocol that can be used to prove that the matrix-vector product for a given matrix X and vector v was correctly computed, up to some (very small) error probability. For the remainder of this section, we will set $V \subseteq \mathbf{F}^m$ to be some vector subspace with generator matrix $G \in \mathbf{F}^{m \times k}$ with distance $d > 0$; *i.e.*, the vector space is the range of the matrix, $V = \mathcal{R}(G)$.

3.1 High level description

We will give a short description of two conditions, which, once verified, show that a certain matrix-vector product has been correctly performed. We will then use these conditions to construct a protocol which allows a player, who we call the *prover*, to convince another, who we call the *verifier*, that any desired matrix-vector product has been correctly computed. More interestingly, it will allow the verifier to be certain of this with very high probability while requiring only a very small amount of communication and a relatively small amount of computation. (Indeed, the amount of communication and computation will be far smaller than having the prover send the complete matrix so the verifier can compute and then check the resulting matrix-vector product.)

Conditions. Given a matrix $X \in \mathbf{F}^{m \times n}$, if we know its columns are no further than $q < d/2$ to the vector space V, *i.e.*,

$$\|X - V^n\| \leq q, \tag{11}$$

then we know that there exists a unique matrix $\tilde{X} \in \mathbf{F}^{k \times n}$ such that

$$\|X - G\tilde{X}\| \leq q.$$

(This follows from the discussion in §2.) Intuitively, this condition guarantees that there is some unique matrix $\tilde{X}$ from which X must have been derived by encoding the columns of $\tilde{X}$ using G. From (1) we also know that, for any $v \in \mathbf{F}^n$,

$$\|(X - G\tilde{X})v\| \leq q, \tag{12}$$

by the definition of the weight of a matrix. Keep this fact in mind as we will use it soon. Now, if we verify that Xv is closer than $(d-q)$ to some vector $y \in V$, or, equivalently, there is some vector $\tilde{y} \in \mathbf{F}^k$ such that $G\tilde{y}$ is close to Xv, we can write

$$\|Xv - G\tilde{y}\| < d - q. \tag{13}$$

Finally, putting it all together, we get

$$\|G\tilde{X}v - G\tilde{y}\| \leq \|(X - G\tilde{X})v\| + \|Xv - G\tilde{y}\| < q + (d - q) = d,$$

where there first inequality follows from the triangle inequality and we have used observation (12) and inequality (13) in the strict inequality. Now, since G has distance at least d, we know that the left hand side, which satisfies

$$\|G(\tilde{X}v - \tilde{y})\| < d,$$

will immediately imply that

$$\tilde{X}v = \tilde{y}. \tag{14}$$

(This is simply an application of (2) and the surrounding discussion.)

Discussion of conditions. One way of looking at this set of claims is that if we can verify condition (11) and condition (13), then we immediately know that $\tilde{X}v = \tilde{y}$, where $\tilde{X}$ is the unique matrix whose encoding is closest to X. Of course, we know that condition (11) can be succinctly tested using the proximity test of §2, while condition (13), given $\tilde{y}$ and the ability to query rows of X, is also easily verified using the sparsity check of §1.3. We will use these two checks to verify both conditions succinctly and give bounds on the probability of error, leading to a succinct proof of the matrix-vector product (14). We will then show how to use this to construct a succinct protocol which convinces a verifier that a matrix-vector product was correctly performed for any given $\tilde{X}$.

3.2 Checks and the final protocol

In this subsection, we outline a simple probability bound on the checks and show how this results in a protocol, played by two parties, which allows one to show the other that a certain matrix-vector product was correctly computed, using only a very small number of queries and a very small amount of computation.

Protocol. The protocol involves two parties: a *prover* who wishes to show that the matrix-vector product of some matrix $\tilde{X}$ (known only to the prover) and vector v has been correctly computed, and a *verifier* who wishes to check this claim. The steps are as follows:

1. The prover constructs a matrix $X = G\tilde{X}$, which simply encodes the columns of $\tilde{X}$ by G and commits to the rows of the matrix. (The rows of X are fixed and accessible to the verifier, who will only query a small number of these rows. This can be practically achieved via a Merkle commitment to the rows of X.)

2. The verifier selects a random row r of G', denoted g'_r, and sends it to the prover. (As a reminder, the matrix G' is defined in the proximity test §2.)

3. The prover computes and returns $\tilde{z}_r = \tilde{X} g'_r$.

4. The verifier checks, using the sparsity check in §1.3, whether $\|Xg'_r - G\tilde{z}_r\| \leq q$. If this condition holds, the verifier can conclude that $\|X - G\tilde{X}\| \leq q$, or that X is close to a correctly encoded matrix, failing with probability no more than p, based on the result in (9).

5. The verifier sends the desired vector v to the prover to compute the matrix-vector product.

6. The prover computes and sends back the 'correct' matrix vector product $\tilde{y} = \tilde{X}v$.

7. The verifier checks whether $\|Xv - G\tilde{y}\| < d - q$. If this inequality holds, the verifier concludes that the matrix-vector product $\tilde{X}v = \tilde{y}$ has been correctly computed by the reasoning in §3.1.

In fact, in some practical cases, steps 5-7 are not required, such as when Ligero is used as a multilinear polynomial commitment scheme, since then we have $v = g'_r$ and the result is given by $\tilde{z}_r$, as was originally proposed in [DP23,DP24]. From this description and the proofs below, it is not hard to see that the same proofs apply and result in less communication and total work.

Correctness. The fact that the verifier always accepts if the prover is honest is immediate from the protocol description. If the prover correctly encodes $X = G\tilde{X}$ and commits to this matrix, then every check passes by definition: the first because $Xg'_r = Gz_r = G\tilde{X}g'_r$ so the sparsity check does not fail, while the second is true for a similar reason.

Soundness. The soundness of this protocol—*i.e.*, the verifier falsely concludes the product was computed correctly with low probability—follows directly from combining probabilistic implications and the discussions of §1.3 and §2.

To see this, note the verifier samples r uniformly from $1, \ldots, m'$ and a subset $S \subseteq \{1, \ldots, m\}$ of fixed size $|S|$, to get

$$(Xg'_r - G\tilde{z}_r)_S = 0 \quad \underset{p'}{\Longrightarrow} \quad \|Xg'_r - G\tilde{z}_r\| \leq q, \tag{15}$$

where $p' \leq (1 - (q+1)/m)^{|S|}$ and the randomness here is over S, with r independent. Since, by definition of G and V at the beginning of this section, we have $G\tilde{z}_r \in V$, then this is the same as saying

$$\|Xg'_r - V\| \leq \|Xg'_r - G\tilde{z}_r\| \leq q,$$

for uniformly randomly sampled r. From §2 we know that

$$\|Xg'_r - V\| \leq q \quad \underset{p}{\Longrightarrow} \quad \|X - G\tilde{X}\| \leq q, \tag{16}$$

with the randomness again over r uniform from $1, \ldots, m$ and where $\tilde{X} \in \mathbf{F}^{k \times n}$ is some (unique) matrix. From before, $p \leq kq/|\mathbf{F}|$. Finally, the verifier checks that

$$(Xv - G\tilde{y})_{S'} = 0 \quad \underset{p''}{\Longrightarrow} \quad \|Xv - G\tilde{y}\| < d - q, \tag{17}$$

with $p'' \leq (1 - (d-q)/m)^{|S'|}$, where $S' \subseteq \{1, \ldots, m\}$ uniformly randomly chosen of fixed size $|S'|$.

From the high level description in §3.1, the conclusions of (15), (16), and (17), and the basic probabilistic implications, we must have

$$\tilde{X}v = y,$$

except with probability no more than

$$p + p' + p'' \leq \left(1 - \frac{q+1}{m}\right)^{|S|} + \frac{k(q+1)}{|\mathbf{F}|} + \left(1 - \frac{d-q}{m}\right)^{|S'|}. \tag{18}$$

3.3 Proof size and total work

In this subsection, we compare the total proof size and computational work necessary for both the prover and the verifier in the 'naïve' case where the prover simply sends the complete matrix $\tilde{X}$ and the verifier computes the matrix-vector product, compared to the succinct case, where the prover and verifier perform the protocol presented in §3.2.

Naïve proof. A 'naïve' proof of this statement would involve sending the complete matrix $\tilde{X} \in \mathbf{F}^{k \times n}$ which has a total of kn elements, each of size $\log(|\mathbf{F}|)$. The verifier simply computes the complete matrix-vector product $\tilde{X}v$, which takes $\sim kn$ operations.

Succinct proof. In comparison, set a threshold probability $0 < \varepsilon < 1$ of failure and set $q = d/3 - 1$. Using (6) gives

$$|S| \geq \frac{3m}{d} \log\left(\frac{1}{\varepsilon}\right), \qquad |S'| \geq \frac{3m}{2d} \log\left(\frac{1}{\varepsilon}\right) \tag{19}$$

samples are sufficient. For now, we assume that the field size $|\mathbf{F}|$ is large enough such that $k(q+1)/|\mathbf{F}| \leq \varepsilon$. In this case, the total error probability (18) is no more than 3ε, by construction.

Communication for succinct proof. Following the protocol above, the verifier sends randomness r of size $\log_2(m')$ (as a reminder, G' has dimensions $m' \times n$) and v which is n field elements. The verifier sends the indices corresponding to the chosen rows S and S', which totals $(|S| + |S'|)\log_2(m)$ bits. (We do not include this in the total as $|S|\log_2(m) \ll n$ for reasonable parameters.) The prover sends back $|S|$ rows of X, each of size m field elements, committed to by some commitment opening of size, say, C for each row (a similar thing is true for S') along with $\tilde{z}_r$ and $\tilde{y}$, which are of size k field elements, each. The total number of field elements is, from the prover, $2k + Cm(|S| + |S'|)$, while the verifier sends n field elements (for v) and $\log_2(m')$ bits for the random row of G'.

	Communication		Work	
	Prover	Verifier	Prover	Verifier
Naïve	knF	0	0	kn
Succinct	$(2k + (C + m)(\|S\| + \|S'\|))F$	$nF + \log_2(m')$	nkm	$(\|S\| + \|S'\|)(k + n)$

Table 1: Comparison of naïve and succinct protocols in the general setting, where $F = \log_2(|\mathbf{F}|)$.

	Communication		Work	
	Prover	Verifier	Prover	Verifier
Naïve	n^2F	0	0	n^2
Succinct	$180nF$	$nF + \log_2(m')$	$2n^3$	$360n$

Table 2: Comparison of naïve and succinct protocols in the concrete setting.

Computational work for succinct proof. Finally, the total computational work for the prover comes from computing $G\tilde{X}$ which is around nkm operations for general G (but can be much lower for more structured matrices G), committing to the result's rows, which we assume is much smaller than the nkm operations, and computing the matrix-vector products of $\tilde{X}$ with g'_r and v, which are $km \ll nkm$ operations each, which means that the total prover work is around $\sim nkm$. The verifier's work comes from computing $|S| + |S'|$ inner products of rows of X with g'_r and v, each of which are a total of k operations, along with computing $|S| + |S'|$ inner products of rows of G with $\tilde{z}_r$ and $\tilde{y}$, respectively, each of which are a total of n operations, totaling up to around $\sim (|S| + |S'|)(k + n)$ operations. (We assume that checking the commitment is negligible relative to this number.)

Putting it all together. We can see the results in table 1 for 'essentially' general parameters m, k, n, and fields $\mathbf{F}$ so long as the field size is large enough. For slightly more concrete parameters, set the matrix dimensions of $\tilde{X}$ to be square, *i.e.*, $k = n$, and the block size as $m = 2n$, such that $G \in \mathbf{F}^{2n\times n}$. If we use a maximum-distance-separable code, such as a Reed–Solomon code, we have that $d = m - n = n$. Setting the parameter $\varepsilon = e^{-20} \approx 2^{-29}$ such that the probability of failure is no more than 3ε, we then have that $|S| = 120$ and $|S'| = 60$. (Here, we have used (19).) Finally, let the commitment be a Merkle commitment such that $C \sim \log_2(n) \ll n$. We place these 'more concrete' results in table 2. Note that, in this setting, the succinct protocol has both lower communication and total work for the verifier, whenever $n \gg 360$; indeed, the verifier work only grows linearly(!) in n, the side length of the square matrix $\tilde{X} \in \mathbf{F}^{n\times n}$. In many practical applications, we have $n \sim 2^{10}$ making the total communication and verification time considerably smaller than those of the naïve protocol. In the particular case of a Reed–Solomon code, we also have that the work necessary for the prover is also much smaller: the matrix G is structured so $G\tilde{X}$ can

be computed in $\sim n^2 \log_2(n)$ operations, versus $2n^3$, as is the case here.

Discussion. In general, both tables and the corresponding results show a particularly interesting pattern in succinct proofs: often, the prover has to do some additional work over the naïve protocol, yet the result is that the succinct proof is considerably smaller than the naïve proof in both computation for the verifier and total communication. We note that it is also possible to squeeze out slightly more performance in a number of places, but we have not done so here. (For example, in the protocol description, S and S' are sampled independently, yet the bound applies even in the case where they are not. Choosing $S' \subseteq S$ reduces the communication overhead, so long as the order of operations ensures that the prover does not learn S before sending the proposed result $\tilde{y}$.)

4 Proof of test

In this section, we prove the proximity testing claim given at the end of §2 along with the provided bounds. In particular, we will show that, letting $G' \in \mathbf{F}^{|\mathbf{F}|^k \times 2^k}$ be the Kronecker product code of (10), and letting g'_r be its rth row, the following probabilistic implication is true, for any matrix $X \in \mathbf{F}^{m \times 2^k}$ and any vector space $V \subseteq \mathbf{F}^m$ with distance $d > 0$:

$$\|X g'_r - V\| \leq q \quad \underset{p}{\Longrightarrow} \quad \|X - V^n\| \leq q,$$

whenever $q < d/3$ while $p \leq k(q+1)/|\mathbf{F}|$. The proof provided in this section was originally presented by the authors at [EA24], and has been subsequently used in a number of improved results [DG24] during the preparation of this note.

Proof outline. We will prove the result in two steps. We will show that, given two matrices $X_1, X_2 \in \mathbf{F}^{m \times n}$ then the following probabilistic implication is true:

$$\|r' X_1 + (1 - r') X_2 - V^n\| \leq q \quad \underset{p'}{\Longrightarrow} \quad \|[X_1 \; X_2] - V^{2n}\| \leq q, \tag{20}$$

where $r' \in \mathbf{F}$ is uniformly randomly chosen, $q < d/3$, and $p' \leq (q+1)/|\mathbf{F}|$. In other words, if we take a random linear combination of X_1 and X_2, and this random linear combination is q-close to a vector space V, then the matrix formed by concatenating both X_1 and X_2 must also be q-close to the vector space. Then, the easy part of the proof follows essentially by induction and the definition of the Kronecker product. We prove this 'easy' part, assuming the probabilistic implication (20) is true, next.

Proof of second statement. The bound essentially directly follows from the probabilistic implications given in the introduction and a basic application of induction. First, note that

$$g'_r = (1 - r_1, r_1) \otimes (1 - r_2, r_2) \otimes \cdots \otimes (1 - r_k, r_k), \tag{21}$$

for $r_1, \ldots, r_k \in \mathbf{F}$ sampled uniformly and independently. We would like to show that

$$\|Xg'_r - V\| \leq q \quad \underset{kp'}{\Longrightarrow} \quad \|X - V^{2^k}\| \leq q, \tag{22}$$

for any k, where $p' \leq (q+1)/|\mathbf{F}|$ as before. Assume the claim is true for $k-1$. Note that, if $X = [X_1\, X_2]$ and $X_1, X_2 \in \mathbf{F}^{m \times 2^{k-1}}$, then

$$Xg'_r = ((1-r_k)X_1 + r_k X_2)\tilde{g}'_{\tilde{r}},$$

where $\tilde{g}'_{\tilde{r}}$ is the tensor product (21) with the last term, $(1-r_k, r_k)$, removed and $r = (\tilde{r}, r_k)$; *i.e.*,

$$\tilde{g}'_{\tilde{r}} = (1-r_1, r_1) \otimes (1-r_2, r_2) \otimes \cdots \otimes (1-r_{k-1}, r_{k-1}).$$

If claim (22) is true for $k-1$, then we have that, for any $r_k \in \mathbf{F}$:

$$\|((1-r_k)X_1 + r_k X_2)y'_{\tilde{r}} - V\| \leq q \quad \underset{(k-1)p}{\Longrightarrow} \quad \|(1-r_k)X_1 + r_k X_2 - V^{2^{k-1}}\| \leq q,$$

with $\tilde{r} \in \mathbf{F}^{k-1}$ uniformly and independently sampled. But, from the original claim (20), we know

$$\|(1-r_k)X_1 + r_k X_2 - V^{2^{k-1}}\| \leq q \quad \underset{p}{\Longrightarrow} \quad \|[X_1\ X_2] - V^{2^k}\| \leq q,$$

for $r_k \in \mathbf{F}$ uniformly sampled, so we recover the final result that $p \leq kp' \leq k(q+1)/|\mathbf{F}|$, by chaining the probabilistic implications.

4.1 Proof of the first statement

Here, we prove the first statement given in the general proof outline (20).

Outline. The proof's main goal will be to reduce this check to the matrix sparsity check of [EA23, §3.2.2], and we provide a simple, self-contained proof of the special case used here in appendix A. Now, let R be the set of $r' \in \mathbf{F}$ such that $\|(1-r')X_1 + r'X_2 - V^n\| \leq q$, and, for notational convenience, define

$$Z_{r'} = (1-r')X_1 + r'X_2, \tag{23}$$

for every $r' \in \mathbf{F}$. We can then rewrite the set R to be $R = \{r' \in \mathbf{F} \mid \|Z_{r'} - V^n\| \leq q\}$. The first part of the proof will be to show that, given two elements $r', r'' \in R$ with $r' \neq r''$, then we can always write the error matrix of $Z_{\bar{r}}$ for some other index $\bar{r} \in R$ as a (fixed) linear combination of the errors in $Z_{r'}$ and $Z_{r''}$. The second part will then show that if $|R| > q+1$, then it must be the case that there are at most q errors in the combined matrix $[Z_{r'}\ Z_{r''}]$. This will mean that any linear combination of the errors of $Z_{r'}$ and $Z_{r''}$ also has at most q errors. Finally, we then note that we can write the error matrices for X_1 and X_2 as linear combinations of the error matrices of $Z_{r'}$ and $Z_{r''}$, which means that the combined matrix must also have no more than q errors when $|R| > q+1$, which completes the claim since this

is the same as saying that, if there are more than q errors, the number of entries in which this implication fails is $|R| \leq q+1$, which leads to the error bound $p' = |R|/|\mathbf{F}| \leq (q+1)/|\mathbf{F}|$.

Purely in the probabilistic implication language, we will show that

$$\|(1-\bar{r})X_1+\bar{r}X_2-V^n\| \leq q \implies \|a_{\bar{r}}\xi+b_{\bar{r}}\xi'\| \leq q \underset{p'}{\implies} \|[\xi\ \xi']\| \leq q \implies \|[X_1\ X_2]-V^{2n}\| \leq q,$$

where ξ and ξ' are some (in fact, as we will show, *the*) error matrices corresponding to $Z_{r'}$ and $Z_{r''}$, respectively with $\bar{r}$ uniformly drawn from $\mathbf{F}$ and $a_{\bar{r}}, b_{\bar{r}} \in \mathbf{F}$ some coefficients to be determined later.

Notation. For notational convenience, for any $r' \in \mathbf{F}$, let $Y_{r'} \in V^n$ be a closest matrix, with columns in V, to $Z_{r'}$. Define $\xi_{r'} = Z_r - Y_r$ to be an 'error' matrix for index r. There may be many error matrices $\xi_{r'}$ (as there may be many 'closest' matrices Y) but we will only really make use of these within the unique decoding radius such that $\xi_{r'}$ is unique.

Part one. In the first part of the proof, we will show that the error matrices for an index $\bar{r} \in R$, written, from before,

$$\xi_{\bar{r}} = Z_{\bar{r}} - Y_{\bar{r}},$$

has at most q nonzero rows and can be written as a linear combination of the error matrices ξ and ξ' of any two indices $r', r'' \in R$ with $r \neq r'$. (We fix indices r' and r'' in what follows and assume that $|R| > 1$ since, otherwise, the claim is trivial.) Because these indices will be fixed for the remainder of the proof, and we will reference their corresponding matrices often, write

$$Z = Z_{r'} \quad \text{and} \quad Z' = Z_{r''},$$

and similarly for Y, Y', and ξ, ξ', where r' and r'' are the (fixed) indices above.

Note that, for each $\bar{r} \in \mathbf{F}$, there are coefficients $a_{\bar{r}}, b_{\bar{r}} \in \mathbf{F}$ such that

$$\begin{aligned}(1-r')a_{\bar{r}} + (1-r'')b_{\bar{r}} &= 1-\bar{r}\\ r'a_{\bar{r}} + r''b_{\bar{r}} &= \bar{r}.\end{aligned}$$

(This linear system has a solution since $r' \neq r''$.) Because this is true for each $\bar{r} \in \mathbf{F}$ we have, using the definitions of Z and Z' along with (23):

$$Z_{\bar{r}} = a_{\bar{r}}Z + b_{\bar{r}}Z'.$$

Now, since $\bar{r} \in R$, then, by definition of the set R, we know $\xi_{\bar{r}} = Z_{\bar{r}} - Y_{\bar{r}}$ has at most q nonzero rows. Finally, note that

$$\xi_{\bar{r}} - (a_{\bar{r}}\xi + b_{\bar{r}}\xi') = a_{\bar{r}}Y + b_{\bar{r}}Y' - Y_{\bar{r}},$$

from the definition of $a_{\bar{r}}$, $b_{\bar{r}}$, and the ξ_r. Note that this matrix has no more than $3q < d$ nonzero rows, as $\xi_{\bar{r}}$, ξ, and ξ' each have at most q nonzero rows, by definition of the set R. On the other hand, the right hand side has columns lying in V—as each of Y, Y', and

$Y_{\bar{r}}$ has columns in V—and this subspace V has distance at least d, so the matrix must be identically zero. The errors therefore satisfy

$$\xi_{\bar{r}} = a_{\bar{r}}\xi + b_{\bar{r}}\xi',$$

for every $\bar{r} \in R$, which means that

$$\|a_{\bar{r}}\xi + b_{\bar{r}}\xi'\| \leq q$$

for each $\bar{r} \in R$.

Part two. We will now show that, if $|R| > q + 1$, then the matrix $[\xi\ \xi']$ has at most q nonzero entries.

We can view the vector $(a_{\bar{r}}, b_{\bar{r}})$ as the $\bar{r}$th row of an $|\mathbf{F}|$ by 2 generator matrix. We will show that the distance of this code is at least $|\mathbf{F}| - 1$, which will imply that, by the matrix sparsity check of appendix A, if $|R| > q + 1$ then

$$\|[\xi\ \xi']\| \leq q.$$

To see that the generator matrix with rows $(a_{\bar{r}}, b_{\bar{r}})$ has distance $|\mathbf{F}| - 1$, we will show that, for any $\bar{r} \neq \bar{r}'$, we have

$$\begin{bmatrix} a_{\bar{r}} & b_{\bar{r}} \\ a_{\bar{r}'} & b_{\bar{r}'} \end{bmatrix} x = 0, \tag{24}$$

then $x = 0$. (In other words, if any two distinct symbols of the encoding of x are zero, then x must be zero.) This will immediately imply that either at most one entry of the codeword is zero, or the whole codeword is equal to zero; *i.e.*, that the code has distance at least $|\mathbf{F}| - 1$.

The proof of this fact is nearly immediate: note that, using the definition of the coefficients $a_{\bar{r}}, b_{\bar{r}}$, we can write

$$\begin{bmatrix} a_{\bar{r}} & b_{\bar{r}} \\ a_{\bar{r}'} & b_{\bar{r}'} \end{bmatrix} \begin{bmatrix} 1 - r' & r' \\ 1 - r'' & r'' \end{bmatrix} = \begin{bmatrix} 1 - \bar{r} & \bar{r} \\ 1 - \bar{r}' & \bar{r}' \end{bmatrix}.$$

Since $r' \neq r''$ (which are the fixed coefficients of part one) and $\bar{r} \neq \bar{r}'$, then the matrix on the right hand side has linearly independent columns, while the second matrix on the left hand side is invertible. This immediately implies that the columns of the first matrix are also linearly independent, implying (24).

Part three. Finally, when we know that $[\xi\ \xi']$ has at most q nonzero rows, then certainly any linear combination of ξ and ξ' also has at most q nonzero rows. Since we know that

$$X_1 = aZ_r + bZ_{r'},$$

for some $a, b \in \mathbf{F}$, then the errors of X_1, which we write as ξ_1, can be written as $\xi_1 = a\xi + b\xi'$. (This follows from the fact that $q < d/2$ so we're in unique decoding and the nonzero entries

of ξ and ξ' are aligned.) Similarly, we can write the error matrix of X_2, ξ_2, as a linear combination of ξ and ξ', which means that $[\xi_1\ \xi_2]$ also has at most the number of nonzero rows as $[\xi\ \xi']$, which is at most q. This implies, finally, that

$$\|[X_1\ X_2] - V^{2n}\| \leq \|[\xi_1\ \xi_2]\| \leq q,$$

if $|R| > q+1$. The claim then is immediate from the definition of probabilistic implications.

Extensions. The proof technique here was used for a code G' whose rows are given by Kronecker products of pairs $(1-t, t)$ for each $t \in \mathbf{F}$. (Equivalently, when G' is a matrix which is the Kronecker product of k matrices, each with rows of the form $(1-t, t)$ for each $t \in \mathbf{F}$.) On the other hand, note that the argument applies very generally to any code G' of the form

$$G' = \tilde{G}_1 \otimes \cdots \otimes \tilde{G}_k,$$

where $\tilde{G}_i \in \mathbf{F}^{m_i \times 2}$ and has distance $d_i > 0$. In this case, the probabilistic implication is

$$\|X g'_r - V\| \quad \underset{p}{\Longrightarrow} \quad \|X - V^{2^k}\|,$$

with r uniformly chosen from $1, \ldots, \prod_i m_i$ and

$$p \leq (q+1) \sum_i \left(1 - \frac{d_i}{m_i}\right).$$

References

[AHIV17] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight sublinear arguments without a trusted setup. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 2087–2104, Dallas Texas USA, October 2017. ACM.

[DG24] Benjamin E. Diamond and Angus Gruen. Proximity gaps in interleaved codes. Cryptology ePrint Archive, Paper 2024/1351, 2024.

[DP23] Benjamin E. Diamond and Jim Posen. Proximity testing with logarithmic randomness. Cryptology ePrint Archive, Paper 2023/630, 2023.

[DP24] Benjamin E. Diamond and Jim Posen. Polylogarithmic proofs for multilinears over binary towers. Cryptology ePrint Archive, Paper 2024/504, 2024.

[EA23] Alex Evans and Guillermo Angeris. Succinct proofs and linear algebra. Cryptology ePrint Archive, Paper 2023/1478, 2023.

[EA24] Alex Evans and Guillermo Angeris. Folding, codes, and linear algebra. Talk at ZK Summit 11, Athens, Greece, April 2024.

A Matrix sparsity check

We show that, given two matrices $\xi_1, \xi_2 \in \mathbf{F}^{m' \times n}$ and a code $G \in \mathbf{F}^{m \times 2}$ with distance d, that

$$\|G_{r1}\xi_1 + G_{r2}\xi_2\| \leq q \quad \underset{p}{\Longrightarrow} \quad \|[\xi_1 \ \xi_2]\| \leq q,$$

with r uniformly chosen from $1, \ldots, m$, and $p \leq (q+1)(1-d/m)$. The proof is essentially that of [EA23, §3.2.2], but we reproduce it here for completeness. Additionally, note that this is equivalent to saying: if there are at least $(q+1)(m-d)$ indices r satisfying $\|G_{r1}\xi_1+G_{r2}\xi_2\| \leq q$, then it must be the case that $\|[\xi_1 \ \xi_2]\| \leq q$. This is the form we use in the proof above.

Proof. This is easy to see. Let $[\xi_1 \ \xi_2]$ have more than q nonzero rows and pick any $q+1$ of them to form some reduced matrix $[\hat{\xi}_1 \ \hat{\xi}_2]$ with $q+1$ rows, all nonzero. It is clear that

$$\|G_{r1}\xi_1 + G_{r2}\xi_2\| \geq \|G_{r1}\hat{\xi}_1 + G_{r2}\hat{\xi}_2\|,$$

so we will show that

$$\|G_{r1}\hat{\xi}_1 + G_{r2}\hat{\xi}_2\| \leq q$$

with probability no more than p. A simple observation is that, if x_1^T and x_2^T are two row vectors, then

$$G_{r1}x_1^T + G_{r2}x_2^T = 0 \quad \underset{p'}{\Longrightarrow} \quad [x_1^T \ x_2^T] = 0,$$

where $p' \leq 1 - d/m$, which follows from the definition of the distance of G. But it can only be the case that $\|G_{r1}\hat{\xi}_1 + G_{r2}\hat{\xi}_2\| \leq q$ if at least one of the linear combinations of the rows of $\hat{\xi}_1$ and $\hat{\xi}_2$ is equal to zero, so, by the union bound, $p \leq (q+1)p' \leq (q+1)(1-d/m)$, as required.

Special case. A special, but very useful, case is when the matrix $G \in \mathbf{F}^{m \times 2}$ has rows of the form $(1-t, t)$ for each $t \in \mathbf{F}$. In this case it is easy to prove that the distance is $|\mathbf{F}| - 1$ and $m = |\mathbf{F}|$. The linear combination

$$G_{r1}\xi_1 + G_{r2}\xi_2,$$

where r is uniformly randomly sampled from $1, \ldots, m$ is the same as the random linear combination

$$(1-t)\xi_1 + t\xi_2,$$

with $t \in \mathbf{F}$ uniformly drawn, and gives the direct implication

$$\|(1-t)\xi_1 + t\xi_2\| \leq q \quad \underset{p}{\Longrightarrow} \quad \|[\xi_1 \ \xi_2]\| \leq q,$$

with $p \leq (q+1)(1-d/m) = (q+1)/|\mathbf{F}|$.