Interleaving Stability for Mutual Correlated Agreement and Curve Decodability

Sunghyeon Jo
sjo65@gatech.edu
Georgia Institute of Technology

August 19, 2026

Abstract

We prove that row-wise interleaving does not impose a linear loss on two coding-theoretic soundness properties used in recent IOP/SNARK analyses: generator mutual correlated agreement and curve decodability.

For generator-MCA, let $G : \Omega \to \mathbb{F}_q^\ell$ be a coefficient generator over a finite seed set and let C be an $\mathbb{F}_q$-additive code. For every interleaving width s and distance parameter δ, we show

$$\varepsilon_G(C, \delta) \le \varepsilon_G(C^{\equiv s}, \delta) \le \left(1 + \frac{1}{q} + \cdots + \frac{1}{q^{s-1}}\right) \varepsilon_G(C, \delta).$$

Moreover, if $|\Omega| \le q$, then the transfer is exact:

$$\varepsilon_G(C^{\equiv s}, \delta) = \varepsilon_G(C, \delta).$$

In particular, affine-line MCA is invariant under row-wise interleaving. This answers the interleaving-loss question of [ABF26] and removes the linear interleaving factor from the affine-line MCA bound. It also implies that the polynomial-generator MCA bounds of [BCGM25] transfer to interleaved codes without an additional interleaving-width factor.

We further establish interleaving stability for curve decodability in the sense of [GG25]. We introduce a marked formulation, prove its equivalence to Definition 3.1 of [GG25] for $\mathbb{F}_q$-additive codes and $1 \le b \le a \le q$, and use it to transfer curve decodability to row-wise interleavings. If C is (ℓ, δ, a, b)-curve-decodable and $\binom{a}{b} \le q$, then $C^{\equiv s}$ is also (ℓ, δ, a, b)-curve-decodable for every s. We also give a field-size-weighted variant that transfers larger base-code witness parameters to smaller interleaved-code witness parameters.

1 Introduction

Coding theory enters IOP and SNARK soundness because a verifier sees only a small number of random local views of the prover's oracle. This perspective goes back to interactive proofs of proximity and interactive oracle proofs [RVW13, BCS16], and it underlies several code-based succinct-argument and proximity-testing constructions [AHIV17, BGKS20, GLSTW23, ACFY25, NA25, CFW26]. The prover's oracle may encode a computation trace, a collection of constraint evaluations, or several committed messages. The verifier cannot read this oracle in full, and instead checks random coordinates, random linear combinations, or random low-dimensional restrictions. The soundness proof must then convert these local checks into a global coding statement: the oracle is close to a valid codeword, or to a small list of candidate codewords with enough consistency to extract a witness.

Mutual correlated agreement (MCA), introduced in the recent proximity-gap and SNARK literature [ACFY25, ABF26], is one such coding statement. It justifies random linear-combination checks. If a verifier checks a random combination of several received words and that combination is locally in the code, MCA says that the underlying words are locally consistent with the code on the same coordinate set, except with a controlled error probability. This same-coordinate-set requirement is exactly what is needed in the toy protocol of [ABF26]: the round-by-round knowledge soundness error contains a term of the form

$$\varepsilon_{\mathrm{mca}}(C,\delta) + \frac{|\Lambda(C^{\equiv 2},\delta)|}{|\mathbb{F}|}.$$

Here the MCA term controls the random linear-combination step, while the interleaved list-size term controls the remaining candidate list.

Curve decodability plays a parallel role for local curve restrictions. It is part of a line of work on proximity gaps and correlated agreement for Reed–Solomon and related codes [BKS18, BCIKS20, BGKS20, BCHKS25, GG25]. In the framework of [GG25], if many points on a degree-ℓ curve are close to codewords, then many of those close codewords must themselves lie on a codeword-valued degree-ℓ curve with the same parametrization. This converts curve-local proximity information into algebraic structure and is used in [GG25] as a route to proximity gaps, correlated agreement, and MCA for several code families.

In modern proof systems, the relevant oracles are often vector-valued. Trace columns, batched constraints, folded views, and packed messages naturally lead to row-wise interleavings. For a base code C, the s-fold row-wise interleaving is

$$C^{\equiv s} := \{(c_1,\dots,c_s) : c_i \in C\}.$$

The soundness analysis then needs MCA or curve decodability for $C^{\equiv s}$, even when the available theorem is for C. A common first analysis is a row-wise union bound. For mutual correlated agreement, [ABF26, Lemma 4.7] proves

$$\varepsilon_{\mathrm{mca}}(C^{\equiv s},\delta) \le s \cdot \varepsilon_{\mathrm{mca}}(C,\delta),$$

and asks whether this loss in the interleaving parameter is tight. The same linear loss is present for general generator-MCA in the interleaving operation lemma of [BCGM25, Lemma 10.1]. These bounds suggest that interleaving may contribute a width-dependent term to the MCA part of the analysis.

In the unique-decoding regime, [ABF26] notes that the affine-line result of [DG24] gives

$$\varepsilon_{\mathrm{mca}}(C^{\equiv s},\delta) = \varepsilon_{\mathrm{mca}}(C,\delta)$$

for $\delta < \delta_{\min}(C)/2$. The affine-line theorem here proves this identity for every $\delta \in (0,1)$ in the MCA formulation of [ABF26].

1.1 Our results

This paper replaces row-wise union bounds by row-combination projections. Instead of analyzing the s rows of $C^{\equiv s}$ separately, choose $\lambda = (\lambda_1, \ldots, \lambda_s) \in \mathbb{F}_q^s$ and project an interleaved word $U = (u_1, \ldots, u_s)$ to the base-code word

$$\lambda \cdot U := \sum_{i=1}^{s} \lambda_i u_i.$$

For each fixed witness that an interleaved instance fails to preserve the desired property, the choices of λ for which this witness disappears form a proper linear subspace of $\mathbb{F}_q^s$. Therefore the transfer from C to $C^{\equiv s}$ is controlled by avoiding proper subspaces of $\mathbb{F}_q^s$, not by taking a union bound over the rows.

Our first contribution is a general interleaving theorem for generator-MCA. For every generator $G : \Omega \to \mathbb{F}_q^\ell$, every $\mathbb{F}_q$-additive code C, every interleaving width $s \geq 1$, and every $\delta \in (0,1)$, we prove

$$\varepsilon_G(C,\delta) \leq \varepsilon_G(C^{\equiv s},\delta) \leq A(q,s)\varepsilon_G(C,\delta), \qquad A(q,s) := 1 + \frac{1}{q} + \cdots + \frac{1}{q^{s-1}}.$$

Since $A(q,s) < q/(q-1)$, this removes any linear dependence on the interleaving width. When $|\Omega| \leq q$, the transfer is exact:

$$\varepsilon_G(C^{\equiv s},\delta) = \varepsilon_G(C,\delta).$$

Affine-line MCA is the case $G(\gamma) = (1,\gamma)$, so this answers the interleaving-loss question of [ABF26]. The univariate powers generator $\alpha \mapsto (1,\alpha,\ldots,\alpha^d)$ is another exact case. Combined with the closure lemmas of [BCGM25], this transfers the polynomial-generator MCA bounds of [BCGM25] to row-wise interleavings without an additional interleaving-width factor.

Our second contribution is the corresponding transfer for curve decodability in the sense of [GG25, Definition 3.1]. We first introduce a marked formulation, where the close set is fixed in advance, and prove that it is equivalent to the original definition for $\mathbb{F}_q$-additive codes and $1 \leq b \leq a \leq q$. This lets the final theorem be stated directly in the language of [GG25]: if C is (ℓ,δ,a,b)-curve-decodable and

$$\binom{a}{b} \leq q,$$

then $C^{\equiv s}$ is also (ℓ,δ,a,b)-curve-decodable for every $s \geq 1$. More generally, (ℓ,δ,a,b_0)-curve decodability of C transfers to (ℓ,δ,a,b)-curve decodability of $C^{\equiv s}$ whenever

$$\frac{\binom{b_0}{b}}{\binom{a}{b}} > \frac{q^{s-1}-1}{q^s-1}.$$

The proof mechanism is the same row-combination principle in both settings. For generator-MCA, the witness family is indexed by bad seeds; for curve decodability, it is indexed by b-subsets of a fixed close set. The relevant row-combinations form linear subspaces indexed by these witnesses. Exact transfer follows from a subspace-cover lemma, and the field-size-weighted bounds follow by counting incidences between nonzero row-combinations and the corresponding witness subspaces.

2 Preliminaries

2.1 Codes and Distances

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field, and write $[n] := \{1, \dots, n\}$. We sample uniformly whenever a finite set is used as a probability space.

Definition 2.1 ($\mathbb{F}_q$-additive code)**.** Let Σ be an $\mathbb{F}_q$-vector space. An error-correcting code $C \subseteq \Sigma^n$ is $\mathbb{F}_q$-additive if it is an $\mathbb{F}_q$-linear subspace of Σ^n.

Throughout the paper, Σ denotes an $\mathbb{F}_q$-vector space and $C \subseteq \Sigma^n$ denotes an $\mathbb{F}_q$-additive code.

Definition 2.2 (Restricted Hamming distance)**.** Let $T \subseteq [n]$ and let $x, y \in \Sigma^T$. The relative Hamming distance between x and y over T is

$$\Delta_T(x, y) := \frac{|\{i \in T : x_i \neq y_i\}|}{|T|}.$$

For full words $x, y \in \Sigma^n$, write $\Delta(x, y) := \Delta_{[n]}(x, y)$. For $A \subseteq \Sigma^T$, write

$$\Delta_T(x, A) := \min_{a \in A} \Delta_T(x, a).$$

For $x \in \Sigma^n$, write

$$\Delta(x, C) := \min_{c \in C} \Delta(x, c).$$

For a coordinate set $T \subseteq [n]$, the puncturing of C to T is

$$C_T := \{c|_T : c \in C\} \subseteq \Sigma^T.$$

Since C is additive, C_T is again an $\mathbb{F}_q$-linear subspace.

Definition 2.3 (List size)**.** For $x \in \Sigma^n$ and $\delta \in (0, 1)$, the list around x at distance δ is

$$\Lambda(C, x, \delta) := \{c \in C : \Delta(x, c) \leq \delta\},$$

and the worst-case list size is

$$|\Lambda(C, \delta)| := \max_{x \in \Sigma^n} |\Lambda(C, x, \delta)|.$$

2.2 Interleaved Codes

Definition 2.4 (Row-wise interleaving)**.** For $s \geq 1$, the s-fold row-wise interleaving of C is the code

$$C^{\equiv s} := \{(c_1, \dots, c_s) : c_i \in C \text{ for all } i \in [s]\} \subseteq (\Sigma^s)^n.$$

We view a word $U \in (\Sigma^s)^n$ row-wise as

$$U = (u_1, \dots, u_s), \qquad u_i \in \Sigma^n.$$

Puncturing commutes with row-wise interleaving:

$$(C^{\equiv s})_T = (C_T)^{\equiv s}.$$

Definition 2.5 (Row-combination)**.** For $\lambda = (\lambda_1, \ldots, \lambda_s) \in \mathbb{F}_q^s$, define the row-combination of $U = (u_1, \ldots, u_s)$ by

$$\lambda \cdot U := \sum_{i=1}^{s} \lambda_i u_i \in \Sigma^n.$$

If $f : \mathbb{F}_q \to C^{\equiv s}$ and

$$f(\alpha) = (f_1(\alpha), \ldots, f_s(\alpha)), \qquad f_i(\alpha) \in C,$$

then

$$\lambda \cdot f(\alpha) := \sum_{i=1}^{s} \lambda_i f_i(\alpha) \in C.$$

2.3 Generator-MCA

Definition 2.6 (Generator MCA error)**.** Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code, and let $G : \Omega \to \mathbb{F}_q^\ell$ be a coefficient generator over a finite seed set Ω, sampled uniformly. Fix $\delta \in (0, 1)$ and $f = (f_1, \ldots, f_\ell) \in (\Sigma^n)^\ell$.

For $\omega \in \Omega$, a coordinate set $T \subseteq [n]$ is a G-MCA witness for (f, ω) with respect to C and δ if $|T| \geq (1 - \delta)n$ and

$$\left(\sum_{j=1}^{\ell} G_j(\omega) f_j \right) |_T \in C_T \qquad \text{and} \qquad (f_1|_T, \ldots, f_\ell|_T) \notin C_T^\ell.$$

We say that ω is G-MCA-bad for f if such a witness exists. The generator-MCA error is

$$\varepsilon_G(C, \delta) := \max_{f \in (\Sigma^n)^\ell} \Pr_{\omega \leftarrow \Omega} [\omega \text{ is } G\text{-MCA-bad for } f].$$

The affine-line MCA error of [ABF26] is the special case $\ell = 2$, $\Omega = \mathbb{F}_q$, and $G(\gamma) = (1, \gamma)$. Definition 2.6 is the punctured-code formulation of the generator-MCA condition in [BCGM25, Definition 3.14], where the linear combination and the tuple are tested on the same coordinate set. We specialize to a finite seed set with the uniform distribution and to vector alphabets.

2.4 Curve Decodability

We use relative Hamming distance $\Delta(\cdot, \cdot)$. The following is Definition 3.1 of [GG25] in the notation of this paper.

Definition 2.7 (Curve decodability)**.** An $\mathbb{F}_q$-additive code $C \subseteq \Sigma^n$ is (ℓ, δ, a, b)-curve-decodable if for every $u = (u_0, \ldots, u_\ell) \in (\Sigma^n)^{\ell+1}$ and every function $f : \mathbb{F}_q \to C$, the following holds. Define the close set

$$A_\delta(u, f) := \left\{ \alpha \in \mathbb{F}_q : \Delta \left(\sum_{j=0}^{\ell} u_j \alpha^j, f(\alpha) \right) \leq \delta \right\}.$$

If $|A_\delta(u, f)| \geq a$, then there exist $c_0, \ldots, c_\ell \in C$ such that

$$\left| \left\{ \alpha \in A_\delta(u, f) : f(\alpha) = \sum_{j=0}^{\ell} c_j \alpha^j \right\} \right| \geq b.$$

3 The Row-Combination Principle

This section isolates the linear-algebraic principle used in both transfer arguments. A failed transfer produces proper subspaces of row-combinations; small witness families are handled by a covering argument, while larger witness families are handled by averaging.

Lemma 3.1 (Avoiding one proper subspace)**.** *Let $K \subsetneq \mathbb{F}_q^s$ be a proper linear subspace. If λ is sampled uniformly from $\mathbb{F}_q^s \setminus \{0\}$, then*

$$\Pr[\lambda \notin K] \geq \frac{q^{s-1}(q-1)}{q^s - 1}.$$

Proof. The largest proper subspaces of $\mathbb{F}_q^s$ have dimension $s-1$, and hence have q^{s-1} points, including 0. Thus K contains at most $q^{s-1} - 1$ nonzero points. The claimed lower bound follows by dividing by $q^s - 1$. □

Lemma 3.2 (Proper subspaces do not cover)**.** *A union of at most q proper linear subspaces of $\mathbb{F}_q^s$ is not all of $\mathbb{F}_q^s$.*

Proof. Every proper linear subspace of $\mathbb{F}_q^s$ has at most q^{s-1} points, and all linear subspaces contain 0. Hence the union of any $m \leq q$ proper subspaces has size at most

$$1 + m(q^{s-1} - 1) \leq 1 + q(q^{s-1} - 1) = q^s - q + 1 < q^s.$$

Thus the union cannot be all of $\mathbb{F}_q^s$. □

The following consequence is the mechanism behind both transfer theorems. If a failed interleaving transfer assigns one proper subspace $K_w \subsetneq \mathbb{F}_q^s$ to each index w in a finite set $\mathcal{W}$, then:

- if $|\mathcal{W}| \leq q$, the subspaces cannot cover $\mathbb{F}_q^s$, so there is a row-combination avoiding all of them;
- if $\mathcal{W}$ is larger, a random nonzero row-combination avoids any fixed K_w with probability at least $q^{s-1}(q-1)/(q^s - 1)$.

The two applications below instantiate this template with different index sets.

4 Generator-MCA Under Interleaving

We first apply the row-combination mechanism to generator-MCA. The witness family is the set of G-MCA-bad seeds.

4.1 Field-Size-Weighted Transfer

Lemma 4.1 (Bad-seed preservation)**.** *Let $G : \Omega \to \mathbb{F}_q^\ell$ be a coefficient generator. Let*

$$U_1, \ldots, U_\ell \in (\Sigma^s)^n$$

be interleaved words, written row-wise as

$$U_j = (u_{j,1}, \ldots, u_{j,s}), \qquad u_{j,i} \in \Sigma^n.$$

Let $B \subseteq \Omega$ be the set of seeds that are G-MCA-bad for $(U_1, \dots, U_\ell)$ with respect to $C^{\equiv s}$ and distance δ. For each $\omega \in B$, there is a proper linear subspace

$$K_\omega \subsetneq \mathbb{F}_q^s$$

such that every $\lambda \notin K_\omega$ makes ω G-MCA-bad for the base-code tuple

$$u_{j,\lambda} := \sum_{i=1}^{s} \lambda_i u_{j,i}, \qquad j \in [\ell],$$

with respect to C and distance δ.

Proof. For every $\omega \in B$, choose one witness set $T_\omega \subseteq [n]$. Thus $|T_\omega| \geq (1-\delta)n$,

$$\left(\sum_{j=1}^{\ell} G_j(\omega) U_j \right) \Big|_{T_\omega} \in (C^{\equiv s})_{T_\omega},$$

but

$$(U_1|_{T_\omega}, \dots, U_\ell|_{T_\omega}) \notin ((C^{\equiv s})_{T_\omega})^\ell.$$

Since $(C^{\equiv s})_{T_\omega} = (C_{T_\omega})^{\equiv s}$, the first condition means that for every row $i \in [s]$,

$$\left(\sum_{j=1}^{\ell} G_j(\omega) u_{j,i} \right) \Big|_{T_\omega} \in C_{T_\omega}.$$

The second condition means that there exist $j \in [\ell]$ and $i \in [s]$ such that

$$u_{j,i}|_{T_\omega} \notin C_{T_\omega}.$$

Indeed, membership in $((C_{T_\omega})^{\equiv s})^\ell$ is equivalent to $u_{j,i}|_{T_\omega} \in C_{T_\omega}$ for every pair $(j,i) \in [\ell] \times [s]$.

Define

$$K_\omega := \left\{ \lambda \in \mathbb{F}_q^s : \left(u_{1,\lambda}|_{T_\omega}, \dots, u_{\ell,\lambda}|_{T_\omega}\right) \in C_{T_\omega}^\ell \right\}.$$

This is a linear subspace of $\mathbb{F}_q^s$, because $C_{T_\omega}^\ell$ is a linear subspace. It is proper: if $K_\omega = \mathbb{F}_q^s$, then every standard basis vector e_i lies in K_ω, which implies

$$u_{j,i}|_{T_\omega} \in C_{T_\omega} \qquad \text{for every } j \in [\ell] \text{ and } i \in [s],$$

contradicting the chosen witness.

Now fix $\lambda \notin K_\omega$. By linearity of C_{T_ω},

$$\left(\sum_{j=1}^{\ell} G_j(\omega) u_{j,\lambda} \right) \Big|_{T_\omega} = \sum_{i=1}^{s} \lambda_i \left(\sum_{j=1}^{\ell} G_j(\omega) u_{j,i} \right) \Big|_{T_\omega} \in C_{T_\omega}.$$

On the other hand, $\lambda \notin K_\omega$, so

$$\left(u_{1,\lambda}|_{T_\omega}, \dots, u_{\ell,\lambda}|_{T_\omega}\right) \notin C_{T_\omega}^\ell.$$

Thus T_ω witnesses that ω is G-MCA-bad for the base-code tuple $(u_{1,\lambda}, \dots, u_{\ell,\lambda})$. □

Theorem 4.2 (Field-size-weighted generator-MCA interleaving bound)**.** *Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code, let $G : \Omega \to \mathbb{F}_q^\ell$ be any coefficient generator over a finite seed set, let $s \geq 1$, and let $\delta \in (0, 1)$. Then*

$$\varepsilon_G(C, \delta) \leq \varepsilon_G(C^{\equiv s}, \delta) \leq A(q, s)\varepsilon_G(C, \delta),$$

where

$$A(q, s) := \frac{q^s - 1}{q^{s-1}(q - 1)} = 1 + \frac{1}{q} + \cdots + \frac{1}{q^{s-1}}.$$

Proof. The lower bound is by embedding a base-code instance into one row. Given any tuple $f_1, \ldots, f_\ell \in \Sigma^n$, define interleaved words

$$U_j = (f_j, 0, \ldots, 0).$$

Since C is additive, $0 \in C$. Every G-MCA-bad seed for the base tuple remains G-MCA-bad for the embedded interleaved tuple. Maximizing over base tuples gives

$$\varepsilon_G(C^{\equiv s}, \delta) \geq \varepsilon_G(C, \delta).$$

For the upper bound, fix arbitrary interleaved words $U_1, \ldots, U_\ell \in (\Sigma^s)^n$, and let $B \subseteq \Omega$ be their set of G-MCA-bad seeds. Put

$$\beta := \frac{|B|}{|\Omega|}.$$

For each $\omega \in B$, let $K_\omega \subsetneq \mathbb{F}_q^s$ be the proper subspace from Lemma 4.1.

Choose λ uniformly from $\mathbb{F}_q^s \setminus \{0\}$. By Lemma 3.1, for every $\omega \in B$,

$$\Pr_\lambda[\lambda \notin K_\omega] \geq \frac{q^{s-1}(q - 1)}{q^s - 1}.$$

Therefore the expected fraction of all seeds in Ω that both lie in B and are preserved as G-MCA-bad seeds by λ is at least

$$\frac{q^{s-1}(q - 1)}{q^s - 1} \cdot \beta.$$

Hence there exists a nonzero λ for which the base-code tuple $(u_{1,\lambda}, \ldots, u_{\ell,\lambda})$ has G-MCA-bad seed probability at least

$$\frac{q^{s-1}(q - 1)}{q^s - 1} \cdot \beta.$$

By the definition of $\varepsilon_G(C, \delta)$,

$$\frac{q^{s-1}(q - 1)}{q^s - 1} \cdot \beta \leq \varepsilon_G(C, \delta).$$

Thus

$$\beta \leq \frac{q^s - 1}{q^{s-1}(q - 1)}\varepsilon_G(C, \delta) = A(q, s)\varepsilon_G(C, \delta).$$

Since the interleaved inputs were arbitrary, this proves the upper bound. □

Remark 4.3 (The field-size factor). The factor $A(q, s)$ is sharp for the subspace-avoidance step. A codimension-one obstruction $K \subseteq \mathbb{F}_q^s$ is avoided by exactly

$$\frac{q^s - q^{s-1}}{q^s - 1} = \frac{1}{A(q, s)}$$

of the nonzero row-combinations. The small-seed theorem below identifies a large class of generators where all G-MCA-bad seeds can be preserved simultaneously and the factor is removed.

4.2 Small-Seed Invariance

Theorem 4.4 (Small-seed generator-MCA interleaving invariance)**.** *Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code, let $G : \Omega \to \mathbb{F}_q^\ell$ be a coefficient generator with $|\Omega| \leq q$, let $s \geq 1$, and let $\delta \in (0, 1)$. Then*

$$\varepsilon_G(C^{\equiv s}, \delta) = \varepsilon_G(C, \delta).$$

Proof. The lower bound is the lower bound of Theorem 4.2.

For the reverse inequality, fix arbitrary interleaved inputs $U_1, \ldots, U_\ell$, and let $B \subseteq \Omega$ be their set of G-MCA-bad seeds. For every $\omega \in B$, let $K_\omega \subsetneq \mathbb{F}_q^s$ be the proper subspace from Lemma 4.1. Since $|B| \leq |\Omega| \leq q$, Lemma 3.2 gives a $\lambda \in \mathbb{F}_q^s$ outside every K_ω. By Lemma 4.1, every seed in B is G-MCA-bad for the base-code tuple $(u_{1,\lambda}, \ldots, u_{\ell,\lambda})$. Hence

$$\frac{|B|}{|\Omega|} \leq \varepsilon_G(C, \delta).$$

Maximizing over the interleaved inputs proves $\varepsilon_G(C^{\equiv s}, \delta) \leq \varepsilon_G(C, \delta)$. □

Corollary 4.5 (Affine lines and univariate powers)**.** *For the affine-line generator*

$$G_{\mathrm{aff}} : \mathbb{F}_q \to \mathbb{F}_q^2, \qquad G_{\mathrm{aff}}(\gamma) = (1, \gamma),$$

one has

$$\varepsilon_{G_{\mathrm{aff}}}(C^{\equiv s}, \delta) = \varepsilon_{G_{\mathrm{aff}}}(C, \delta).$$

More generally, for any $S \subseteq \mathbb{F}_q$ and any $d \geq 0$, the univariate powers generator

$$G_d : S \to \mathbb{F}_q^{d+1}, \qquad G_d(\alpha) = (1, \alpha, \ldots, \alpha^d),$$

satisfies

$$\varepsilon_{G_d}(C^{\equiv s}, \delta) = \varepsilon_{G_d}(C, \delta).$$

Proof. Both generators have seed set size at most q, so the result follows from Theorem 4.4. □

4.3 Affine-Line MCA and the Toy Protocol

The affine-line case removes the interleaving factor in the MCA bound of [ABF26, Lemma 4.7].

Corollary 4.6 (Affine-line MCA and interleaved Reed–Solomon codes)**.** *The affine-line MCA error of [ABF26] is invariant under row-wise interleaving:*

$$\varepsilon_{\mathrm{mca}}(C^{\equiv s}, \delta) = \varepsilon_{\mathrm{mca}}(C, \delta).$$

Consequently, for the interleaved Reed–Solomon code considered in [ABF26], namely

$$\mathrm{IRS}[\mathbb{F}, L, k, s] := \big(\mathrm{RS}[\mathbb{F}, L, k/s]\big)^{\equiv s},$$

one has

$$\varepsilon_{\mathrm{mca}}(\mathrm{IRS}[\mathbb{F}, L, k, s], \delta) = \varepsilon_{\mathrm{mca}}(\mathrm{RS}[\mathbb{F}, L, k/s], \delta).$$

For proof-system analyses, Corollary 4.6 replaces uses of the row-union estimate

$$\varepsilon_{\mathrm{mca}}(C^{\equiv s}, \delta) \leq s \cdot \varepsilon_{\mathrm{mca}}(C, \delta)$$

by an exact identity in the affine-line setting. In the toy protocol of [ABF26], the relevant combination-round error contains an MCA term and an interleaved list-size term. In the interleaved Reed–Solomon instantiation, write

$$C_{\mathrm{IRS}} := \mathrm{IRS}[\mathbb{F}, L, k, s] = \big(\mathrm{RS}[\mathbb{F}, L, k/s]\big)^{\equiv s}.$$

The MCA component of the soundness bound of [ABF26] was previously controlled by

$$\varepsilon_{\mathrm{mca}}(C_{\mathrm{IRS}}, \delta) \leq s \cdot \varepsilon_{\mathrm{mca}}(\mathrm{RS}[\mathbb{F}, L, k/s], \delta).$$

Corollary 4.6 replaces this by the identity

$$\varepsilon_{\mathrm{mca}}(C_{\mathrm{IRS}}, \delta) = \varepsilon_{\mathrm{mca}}(\mathrm{RS}[\mathbb{F}, L, k/s], \delta).$$

Thus the MCA contribution to the combination-round term of [ABF26] changes from

$$s \cdot \varepsilon_{\mathrm{mca}}(\mathrm{RS}[\mathbb{F}, L, k/s], \delta) + \frac{|\Lambda(C_{\mathrm{IRS}}^{\equiv 2}, \delta)|}{|\mathbb{F}|}$$

to

$$\varepsilon_{\mathrm{mca}}(\mathrm{RS}[\mathbb{F}, L, k/s], \delta) + \frac{|\Lambda(C_{\mathrm{IRS}}^{\equiv 2}, \delta)|}{|\mathbb{F}|}.$$

The list-size term remains the interleaved list-size term. This separates the agreement contribution, where interleaving has no cost in the affine-line case, from the list-decoding contribution, which is the subject of separate interleaved list-size bounds such as [GGR11].

In the concrete parametrizations of [ABF26, Section 6.3], the argument size expression is governed by the number of spot checks and Merkle openings; the replacement above changes the MCA component of the soundness calculation. On that component alone, removing the multiplicative factor s corresponds to a $\log_2 s$-bit improvement. For example, interleaving widths $s = 2^5$ and $s = 2^{12}$, both considered in the parameter tables of [ABF26], correspond to 5 and 12 bits in the MCA contribution, respectively.

4.4 Polynomial Generators

Theorem 4.2 applies to every generator, in particular to the polynomial generators studied in [BCGM25]. For the polynomial generators of [BCGM25], the interleaving penalty can be removed entirely from their stated upper bounds. Equivalently, row-wise interleaving does not degrade the polynomial-generator MCA bounds of [BCGM25].

We use two closure properties from [BCGM25]. First, applying a left-invertible linear transformation to a generator does not increase its MCA error [BCGM25, Lemma 4.1]. Second, the MCA error of a tensor-product generator is bounded by the sum of the MCA errors of its factors [BCGM25, Lemma 4.4]. These statements apply to arbitrary $\mathbb{F}_q$-additive codes, hence also to row-wise interleavings $C^{\equiv s}$.

Theorem 4.7 (Interleaving-stable polynomial-generator bound)**.** *Let*

$$G : S_1 \times \cdots \times S_h \to \mathbb{F}_q^{\ell}$$

be a polynomial generator in the sense of [BCGM25], with

$$G(x) = (P_j(x))_{j\in[\ell]}, \qquad d_i := \max_{j\in[\ell]} \deg_{X_i}(P_j),$$

and assume $|S_i| \geq d_i + 1$ *for every* $i \in [h]$*. For each* i*, let*

$$H_i : S_i \to \mathbb{F}_q^{d_i+1}, \qquad H_i(\alpha) = (1, \alpha, \ldots, \alpha^{d_i})$$

be the corresponding univariate powers generator. Then, for every $\mathbb{F}_q$*-additive code* C*, every interleaving width* $s \geq 1$*, and every* $\delta \in (0, 1)$*,*

$$\varepsilon_G(C^{\equiv s}, \delta) \leq \sum_{i=1}^{h} \varepsilon_{H_i}(C, \delta).$$

Proof. Run the proof of [BCGM25, Theorem 8.2] with the code $C^{\equiv s}$ in place of C. For every $i \in [h]$, the powers generator H_i has seed set $S_i \subseteq \mathbb{F}_q$, so Corollary 4.5 gives

$$\varepsilon_{H_i}(C^{\equiv s}, \delta) = \varepsilon_{H_i}(C, \delta).$$

Let

$$\widetilde{G} := H_1 \otimes \cdots \otimes H_h.$$

By the tensor-product closure lemma of [BCGM25, Lemma 4.4], $\widetilde{G}$ has MCA error at most

$$\sum_{i=1}^{h} \varepsilon_{H_i}(C^{\equiv s}, \delta) = \sum_{i=1}^{h} \varepsilon_{H_i}(C, \delta)$$

for the code $C^{\equiv s}$.

As in the proof of [BCGM25, Theorem 8.2], the polynomial generator G is obtained from $\widetilde{G}$ by a left-invertible linear transformation. The linear-transformation closure lemma of [BCGM25, Lemma 4.1] therefore gives the same MCA upper bound for G over $C^{\equiv s}$. □

Corollary 4.8 (Polynomial-generator bounds transfer without interleaving loss)**.** *Let* $G : S_1 \times \cdots \times S_h \to \mathbb{F}_q^{\ell}$ *be as in Theorem 4.7. If*

$$\varepsilon_{H_i}(C, \delta) \leq \xi_{C,d_i,|S_i|}(\delta)$$

is the univariate powers-generator bound used in [BCGM25, Theorem 8.2], then

$$\varepsilon_G(C^{\equiv s}, \delta) \leq \sum_{i=1}^{h} \xi_{C,d_i,|S_i|}(\delta).$$

Thus the same polynomial-generator bound obtained in [BCGM25, Theorem 8.2] for the base code C *applies to* $C^{\equiv s}$*, with no additional factor depending on the interleaving width.*

Corollary 4.9 (Reed–Solomon polynomial-generator bounds)**.** *Let* $C = \mathrm{RS}[\mathbb{F}, L, k]$*. The polynomial-generator MCA bounds for Reed–Solomon codes in [BCGM25, Theorem 9.2] transfer to the interleaved code* $C^{\equiv s}$ *without an additional interleaving-width factor.*

Proof. The proof of [BCGM25, Theorem 9.2] first proves the required univariate powers-generator bounds for C and then extends them to polynomial generators using the same tensor-product and linear-transformation closure lemmas used above. Corollary 4.5 transfers each powers generator bound from C to $C^{\equiv s}$ exactly, and the closure lemmas then give the same polynomial-generator bound for $C^{\equiv s}$. □

The corollaries in this subsection are sufficient for the polynomial-generator upper bounds used in [BCGM25]. Exact equality for larger multivariate seed spaces remains a separate structural question: characterize generators for which

$$\varepsilon_G(C^{\equiv s}, \delta) = \varepsilon_G(C, \delta)$$

holds when the seed space has size larger than q.

5 Curve Decodability Under Interleaving

We now apply the same row-combination mechanism to curve decodability. The main difference from generator-MCA is that the relevant index set consists of b-subsets of a close set.

5.1 Marked Formulation and Equivalence

Definition 2.7 uses the full close set A. For interleaving, the row-combination proof naturally fixes a close set in advance. This is because row-combination projections can create additional close points by cancellation, and a witness using those projected-only close points would not be a witness for the original interleaved instance.

Definition 5.1 (Marked curve decodability)**.** An $\mathbb{F}_q$-additive code $C \subseteq \Sigma^n$ is marked (ℓ, δ, a, b)-curve-decodable if for every $u_0, \ldots, u_\ell \in \Sigma^n$, every $f : \mathbb{F}_q \to C$, and every specified set $A_0 \subseteq \mathbb{F}_q$ of size a satisfying

$$\Delta\left(\sum_{j=0}^{\ell} u_j \alpha^j, f(\alpha)\right) \leq \delta \qquad \text{for all } \alpha \in A_0,$$

there exist $c_0, \ldots, c_\ell \in C$ such that

$$\left|\left\{\alpha \in A_0 : f(\alpha) = \sum_{j=0}^{\ell} c_j \alpha^j\right\}\right| \geq b.$$

Lemma 5.2 (The small-witness regime)**.** *Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code. If $1 \leq b \leq \ell + 1$, then C is marked (ℓ, δ, a, b)-curve-decodable for every $a \geq b$ and every δ.*

Proof. Given a marked instance and any b distinct points $\alpha_1, \ldots, \alpha_b \in A_0$, Lagrange interpolation gives a degree-$(b-1)$ codeword-valued curve passing through the values

$$f(\alpha_1), \ldots, f(\alpha_b).$$

Since $b - 1 \leq \ell$ and C is $\mathbb{F}_q$-linear, all interpolation coefficients lie in C. □

Remark 5.3. The nontrivial regime for curve-decodability applications is $b > \ell + 1$. When $b \leq \ell + 1$, the marked witness follows from interpolation alone, independently of the distance parameter.

Lemma 5.4 (Curve decodability gives a non-covering condition)**.** *Let $C \subseteq \Sigma^n$ be a nonzero $\mathbb{F}_q$-additive code. Suppose C is (ℓ, δ, a, b)-curve-decodable in the sense of [GG25] with $a \leq q$ and $b > \ell + 1$. Then for every $y \in \Sigma^n$, there is a codeword $c \in C$ with*

$$\Delta(y, c) > \delta.$$

Proof. Suppose, toward a contradiction, that there is $y \in \Sigma^n$ such that every $c \in C$ satisfies $\Delta(y, c) \leq \delta$. Choose $0 \neq v \in C$, and set

$$u_0 = y, \qquad u_1 = \cdots = u_\ell = 0, \qquad f(\alpha) = \alpha^{\ell+1} v.$$

Then every $\alpha \in \mathbb{F}_q$ belongs to the full close set, because $f(\alpha) \in C$ is δ-close to y. By curve decodability in the sense of [GG25], there are $c_0, \ldots, c_\ell \in C$ such that

$$\alpha^{\ell+1} v = \sum_{j=0}^{\ell} c_j \alpha^j$$

for at least b values of α. Choose an $\mathbb{F}_q$-linear functional $\varphi : C \to \mathbb{F}_q$ with $\varphi(v) = 1$. Applying φ gives a nonzero scalar polynomial

$$X^{\ell+1} - \sum_{j=0}^{\ell} \varphi(c_j) X^j$$

of degree $\ell + 1$ with at least $b > \ell + 1$ roots, a contradiction. Thus the claimed codeword exists for every y. □

Theorem 5.5 (Marked/original equivalence)**.** *Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code, and let $1 \leq b \leq a \leq q$. Then C is (ℓ, δ, a, b)-curve-decodable in the sense of [GG25] if and only if C is marked (ℓ, δ, a, b)-curve-decodable.*

Proof. The marked property immediately implies the original property: if the full close set A has size at least a, choose any $A_0 \subseteq A$ with $|A_0| = a$. A marked witness inside A_0 is also a witness inside A.

We prove the converse. If $b \leq \ell + 1$, it follows from Lemma 5.2. If $C = \{0\}$, the marked conclusion is immediate. We may therefore assume $b > \ell + 1$ and $C \neq \{0\}$.

Now fix an arbitrary marked instance

$$u_0, \ldots, u_\ell \in \Sigma^n, \qquad f : \mathbb{F}_q \to C, \qquad A_0 \subseteq \mathbb{F}_q, \quad |A_0| = a,$$

and write

$$u_\alpha := \sum_{j=0}^{\ell} u_j \alpha^j.$$

Define $f' : \mathbb{F}_q \to C$ by setting $f'(\alpha) = f(\alpha)$ for $\alpha \in A_0$, and for each $\alpha \notin A_0$ choosing, using the non-covering condition from Lemma 5.4, a codeword $f'(\alpha) \in C$ with

$$\Delta(u_\alpha, f'(\alpha)) > \delta.$$

The full close set of the instance $(u_0, \ldots, u_\ell, f')$ is exactly A_0. Applying curve decodability in the sense of [GG25] gives $c_0, \ldots, c_\ell \in C$ such that

$$\left| \left\{ \alpha \in A_0 : f'(\alpha) = \sum_{j=0}^{\ell} c_j \alpha^j \right\} \right| \geq b.$$

Since $f' = f$ on A_0, this is the required marked witness. □

5.2 Exact Preservation

Lemma 5.6 (Projection does not increase distance)**.** *Let $U_0, \ldots, U_\ell \in (\Sigma^s)^n$, let $f : \mathbb{F}_q \to C^{\equiv s}$, and let $\lambda \in \mathbb{F}_q^s$. If*

$$\Delta\left(\sum_{j=0}^{\ell} U_j \alpha^j, f(\alpha)\right) \leq \delta,$$

then

$$\Delta\left(\sum_{j=0}^{\ell} (\lambda \cdot U_j)\alpha^j, \lambda \cdot f(\alpha)\right) \leq \delta.$$

Proof. At every coordinate $i \in [n]$ where

$$\left(\sum_{j=0}^{\ell} U_j \alpha^j\right)_i = f(\alpha)_i \quad \text{in } \Sigma^s,$$

all row-combinations of the two symbols also agree in Σ. Therefore the projected disagreement set is contained in the interleaved disagreement set. □

Theorem 5.7 (Exact preservation of curve decodability)**.** *Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code, let $1 \leq b \leq a \leq q$, and suppose C is (ℓ, δ, a, b)-curve-decodable in the sense of [GG25]. If*

$$\binom{a}{b} \leq q,$$

then $C^{\equiv s}$ is (ℓ, δ, a, b)-curve-decodable in the sense of [GG25] for every interleaving width $s \geq 1$. In fact, $C^{\equiv s}$ is marked (ℓ, δ, a, b)-curve-decodable.

Proof. By Theorem 5.5, C is marked (ℓ, δ, a, b)-curve-decodable.

Fix a marked instance over the interleaved code

$$U_0, \ldots, U_\ell \in (\Sigma^s)^n, \qquad f : \mathbb{F}_q \to C^{\equiv s},$$

and a specified close set $A_0 \subseteq \mathbb{F}_q$ with $|A_0| = a$. Thus, for every $\alpha \in A_0$,

$$\Delta\left(\sum_{j=0}^{\ell} U_j \alpha^j, f(\alpha)\right) \leq \delta.$$

For each b-subset $B \subseteq A_0$, define $V_B \subseteq \mathbb{F}_q^s$ as the set of row-combinations λ for which there exist $h_0, \ldots, h_\ell \in C$ satisfying

$$\lambda \cdot f(\alpha) = \sum_{j=0}^{\ell} h_j \alpha^j \qquad \text{for every } \alpha \in B.$$

First, V_B is a linear subspace. If $\lambda, \mu \in V_B$, witnessed by h_j's and g_j's respectively, then $\lambda + \mu$ is witnessed by $h_j + g_j$. Scalar closure is identical, and $0 \in V_B$ is witnessed by the zero codewords.

Second, the subspaces V_B cover $\mathbb{F}_q^s$. Fix any $\lambda \in \mathbb{F}_q^s$. By Lemma 5.6, the projected data

$$\lambda \cdot U_0, \ldots, \lambda \cdot U_\ell \in \Sigma^n, \qquad \lambda \cdot f : \mathbb{F}_q \to C$$

form a marked instance over C on the same set A_0. Since C is marked (ℓ, δ, a, b)-curve-decodable, there is a set $S_\lambda \subseteq A_0$ with $|S_\lambda| \geq b$ and codewords $h_0, \ldots, h_\ell \in C$ such that

$$\lambda \cdot f(\alpha) = \sum_{j=0}^{\ell} h_j \alpha^j \qquad \text{for all } \alpha \in S_\lambda.$$

Choose any b-subset $B \subseteq S_\lambda$. Then $\lambda \in V_B$. Hence

$$\mathbb{F}_q^s = \bigcup_{\substack{B \subseteq A_0 \\ |B|=b}} V_B.$$

If the desired interleaved conclusion failed, then every V_B would be a proper subspace. Indeed, if $V_B = \mathbb{F}_q^s$, then every standard basis vector e_i lies in V_B. For each row i, choose codewords

$$h_{0,i}, \ldots, h_{\ell,i} \in C$$

witnessing $e_i \in V_B$. Thus

$$f_i(\alpha) = \sum_{j=0}^{\ell} h_{j,i} \alpha^j \qquad \text{for every } \alpha \in B.$$

Define interleaved codewords

$$c_j = (h_{j,1}, \ldots, h_{j,s}) \in C^{\equiv s}.$$

Then for every $\alpha \in B$,

$$f(\alpha) = \sum_{j=0}^{\ell} c_j \alpha^j,$$

which is an interleaved marked witness of size b, contradiction.

Therefore failure would cover $\mathbb{F}_q^s$ by at most $\binom{a}{b} \leq q$ proper subspaces, contradicting Lemma 3.2. The marked conclusion follows, and marked curve decodability implies curve decodability in the sense of [GG25]. □

5.3 Field-Size-Weighted Transfer

Theorem 5.8 (Field-size-weighted curve-decodability transfer)**.** *Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code, let $s \geq 1$, let $1 \leq b \leq b_0 \leq a \leq q$, and suppose C is (ℓ, δ, a, b_0)-curve-decodable in the sense of [GG25]. If*

$$\frac{\binom{b_0}{b}}{\binom{a}{b}} > \frac{q^{s-1} - 1}{q^s - 1},$$

then $C^{\equiv s}$ is (ℓ, δ, a, b)-curve-decodable in the sense of [GG25]. In fact, $C^{\equiv s}$ is marked (ℓ, δ, a, b)-curve-decodable.

Proof. By Theorem 5.5, C is marked (ℓ, δ, a, b_0)-curve-decodable. Use the same notation as in the proof of Theorem 5.7. For each b-subset $T \subseteq A_0$, define the same subspace V_T.

Fix a nonzero $\lambda \in \mathbb{F}_q^s$. Projection gives a marked instance over C on A_0. Since C is marked (ℓ, δ, a, b_0)-curve-decodable, there is a set $S_\lambda \subseteq A_0$ with $|S_\lambda| \geq b_0$ such that λ belongs to V_T for every b-subset

$$T \subseteq S_\lambda.$$

Thus λ is incident to at least $\binom{b_0}{b}$ of the subspaces V_T.

If the interleaved (ℓ, δ, a, b) conclusion failed, then every V_T would be proper by the same standard-basis argument as before. A proper subspace contains at most $q^{s-1} - 1$ nonzero vectors. Counting incidences between nonzero $\lambda \in \mathbb{F}_q^s$ and b-subsets $T \subseteq A_0$ gives

$$(q^s - 1)\binom{b_0}{b} \leq \binom{a}{b}(q^{s-1} - 1),$$

contradicting the hypothesis. Thus $C^{\equiv s}$ is marked (ℓ, δ, a, b)-curve-decodable, and therefore curve-decodable in the sense of [GG25]. □

Corollary 5.9 (Black-box transfer for curve-decodability theorems)**.** *Let $C \subseteq \Sigma^n$ be an $\mathbb{F}_q$-additive code, and suppose a result of [GG25] proves that C is (ℓ, δ, a, b_0)-curve-decodable, where $1 \leq b_0 \leq a \leq q$. Then for every interleaving width $s \geq 1$ and every $1 \leq b \leq b_0$ satisfying*

$$\frac{\binom{b_0}{b}}{\binom{a}{b}} > \frac{q^{s-1} - 1}{q^s - 1},$$

the interleaved code $C^{\equiv s}$ is (ℓ, δ, a, b)-curve-decodable in the sense of [GG25].

In particular, if $\binom{a}{b_0} \leq q$, then $C^{\equiv s}$ is (ℓ, δ, a, b_0)-curve-decodable in the sense of [GG25] for every $s \geq 1$.

Proof. The field-size-weighted statement is Theorem 5.8. The exact statement follows from Theorem 5.7. □

Thus every curve-decodability theorem in [GG25] whose hypotheses give an $\mathbb{F}_q$-additive code and parameters $1 \leq b_0 \leq a \leq q$ can be combined with Corollary 5.9. Under those hypotheses, this includes the subspace-design route [GK16, GG25] and its folded Reed–Solomon and multiplicity-code consequences [CZ25, GG25], as well as the random linear and random Reed–Solomon route.

Corollary 5.10 (Subspace-design curve-decodability transfer)**.** *Let $C \subseteq \Sigma^n$ be a τ-subspace-design additive code in the sense of [GG25]. Fix positive integers r, ℓ, a, and let $\epsilon \geq (\ell + 1)/r$. Set*

$$\delta := 1 - \tau(r) - \epsilon, \qquad b_0 := \left\lfloor \frac{\epsilon a}{r + \epsilon} \right\rfloor.$$

Assume $1 \leq b_0 \leq a \leq q$. Then, for every interleaving width $s \geq 1$ and every $1 \leq b \leq b_0$ satisfying

$$\frac{\binom{b_0}{b}}{\binom{a}{b}} > \frac{q^{s-1} - 1}{q^s - 1},$$

the interleaved code $C^{\equiv s}$ is (ℓ, δ, a, b)-curve-decodable in the sense of [GG25]. In particular, if $\binom{a}{b_0} \leq q$, then $C^{\equiv s}$ is (ℓ, δ, a, b_0)-curve-decodable for every $s \geq 1$.

Proof. By [GG25, Theorem 4.7], C is (ℓ, δ, a, b_0)-curve-decodable. Apply Corollary 5.9. □

This supplies the curve-decodability input for the subsequent reductions of [GG25]. Those reductions combine curve decodability with additional ingredients, such as list-decoding bounds, to obtain proximity-gap or MCA statements. After interleaving, the same reductions use the transferred witness parameter b supplied by Corollary 5.9 or Corollary 5.10.

5.4 Parameter Regimes

The exact transfer condition

$$\binom{a}{b} \le q$$

is a witness-count condition. It is most useful when b is small. Using the standard estimate

$$\binom{a}{b} \le \left(\frac{ea}{b}\right)^b,$$

exact transfer follows whenever $q \ge (ea/b)^b$. Thus for fixed b, including the first nontrivial regime $b = \ell + 2$, the required field size is polynomial in a with degree b.

This regime is compatible with small-witness curve-decoding scales that appear in [GG25]. For example, in the V-decodability route of [GG25, Section 5.4], one may take

$$a = \left\lceil \frac{(\ell+2)^2}{\epsilon^2} \right\rceil$$

for V-decodability. By [GG25, Proposition 5.4], this yields $(\ell, \delta, a, \ell{+}2)$-curve-decodability whenever $q > a^{2\ell+2}$, so the resulting curve witness parameter is $b = \ell + 2$. If $\epsilon = 2^{-8}$ and $\ell = 2$, then $a = 2^{20}$, $b = 4$, and

$$a^{2\ell+2} = 2^{120}, \qquad \log_2 \binom{a}{b} \approx 75.4.$$

Thus a 2^{128}-size field satisfies both the GG25 conversion condition and the exact-transfer condition for this small-witness curve-decoding statement.

The field-size-weighted transfer gives a complementary interpretation. For fixed b, its condition is approximately

$$\left(\frac{b_0}{a}\right)^b \gtrsim \frac{1}{q}.$$

Thus the weighted theorem trades a stronger base-code witness parameter b_0 for a smaller interleaved-code witness parameter b, with the required field size controlled by the witness density b_0/a. Subsequent MCA or proximity-gap reductions can then be applied with the transferred witness parameter supplied by Theorem 5.8 and Corollary 5.9.

6 Discussion and Further Directions

The results above show that the transfer from C to $C^{\equiv s}$ is controlled by row-combinations rather than row-wise union bounds. For generator-MCA, the relevant indices are G-MCA-bad seeds, giving exact invariance for small-seed generators and near-invariance for arbitrary generators. For curve decodability, the relevant indices are b-subsets of a close set, giving exact preservation under $\binom{a}{b} \le q$ and a field-size-weighted transfer from b_0 to b otherwise.

The corresponding interleaved list-decoding question remains a natural next direction. The general bound of [GGR11], recalled in [ABF26], is independent of the interleaving width but worsens as the radius approaches the minimum distance. The unique-decoding proximity-gap result of [DG24] shows that interleaving can preserve strong agreement structure in that regime. A row-combination viewpoint suggests a complementary approach beyond agreement: large interleaved lists over large fields should force low-row-rank structure, since high-rank differences are unlikely to collide under a random row-combination. Developing this rank-sensitive viewpoint for Reed–Solomon and related codes would connect the present transfer results with the interleaved list-size term in proof-system soundness bounds.

Acknowledgements

The author thanks Dan Boneh and Giacomo Fenzi for helpful discussions and comments.

AI usage disclosure. OpenAI Codex was used to assist with writing and revising the manuscript, including drafting text, editing, reorganization, consistency checks, and LaTeX maintenance. The author developed the main idea independently of AI tools, verified all mathematical claims and proofs, and takes full responsibility for the paper's contents and correctness.

References

[ABF26] Gal Arnon, Dan Boneh, and Giacomo Fenzi. Open Problems in List Decoding and Correlated Agreement. IACR Cryptology ePrint Archive, Paper 2026/680, 2026. `https://eprint.iacr.org/2026/680`.

[ACFY25] Gal Arnon, Alessandro Chiesa, Giacomo Fenzi, and Eylon Yogev. WHIR: Reed–Solomon Proximity Testing with Super-Fast Verification. In *Advances in Cryptology – EUROCRYPT 2025*, 2025.

[AHIV17] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight Sublinear Arguments Without a Trusted Setup. In *Proceedings of the 24th ACM Conference on Computer and Communications Security*, pages 2087–2104, 2017.

[BCHKS25] Eli Ben-Sasson, Dan Carmon, Ulrich Haböck, Swastik Kopparty, and Shubhangi Saraf. On Proximity Gaps for Reed–Solomon Codes. IACR Cryptology ePrint Archive, Paper 2025/2055, 2025. `https://eprint.iacr.org/2025/2055`.

[BCIKS20] Eli Ben-Sasson, Dan Carmon, Yuval Ishai, Swastik Kopparty, and Shubhangi Saraf. Proximity Gaps for Reed–Solomon Codes. In *Proceedings of the 61st Annual IEEE Symposium on Foundations of Computer Science*, pages 900–909, 2020.

[BCS16] Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. Interactive Oracle Proofs. In *Proceedings of the 14th Theory of Cryptography Conference*, pages 31–60, 2016.

[BCGM25] Sarah Bordage, Alessandro Chiesa, Ziyi Guan, and Ignacio Manzur. All Polynomial Generators Preserve Distance with Mutual Correlated Agreement. IACR Cryptology ePrint Archive, Paper 2025/2051, 2025. `https://eprint.iacr.org/2025/2051`.

[BGKS20] Eli Ben-Sasson, Lior Goldberg, Swastik Kopparty, and Shubhangi Saraf. DEEP-FRI: Sampling Outside the Box Improves Soundness. In *Proceedings of the 11th Innovations in Theoretical Computer Science Conference*, 5:1–5:32, 2020.

[BKS18] Eli Ben-Sasson, Swastik Kopparty, and Shubhangi Saraf. Worst-Case to Average Case Reductions for the Distance to a Code. In *Proceedings of the 33rd Computational Complexity Conference*, 24:1–24:23, 2018.

[CFW26] Alessandro Chiesa, Giacomo Fenzi, and Guy Weissenberg. Zero-Knowledge IOPPs for Constrained Interleaved Codes. IACR Cryptology ePrint Archive, Report 2026/391, 2026. `https://eprint.iacr.org/2026/391`.

[CZ25] Yeyuan Chen and Zihan Zhang. Explicit Folded Reed–Solomon and Multiplicity Codes Achieve Relaxed Generalized Singleton Bounds. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, 2025.

[DG24] Benjamin Diamond and Angus Gruen. Proximity Gaps in Interleaved Codes. IACR Cryptology ePrint Archive, Report 2024/1351, 2024.

[GG25] Rohan Goyal and Venkatesan Guruswami. Optimal Proximity Gaps for Subspace-Design Codes and (Random) Reed–Solomon Codes. IACR Cryptology ePrint Archive, Paper 2025/2054, 2025. `https://eprint.iacr.org/2025/2054`.

[GGR11] Parikshit Gopalan, Venkatesan Guruswami, and Prasad Raghavendra. List Decoding Tensor Products and Interleaved Codes. *SIAM Journal on Computing*, 40(5):1432–1462, 2011.

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit Subspace Designs. *Combinatorica*, 36(2):161–185, 2016.

[GLSTW23] Alexander Golovnev, Jonathan Lee, Srinath T. V. Setty, Justin Thaler, and Riad S. Wahby. Brakedown: Linear-time and Field-agnostic SNARKs for R1CS. In *Advances in Cryptology – CRYPTO 2023*, 2023.

[NA25] Andrija Novakovic and Guillermo Angeris. Ligerito: A Small and Concretely Fast Polynomial Commitment Scheme. IACR Cryptology ePrint Archive, Report 2025/1187, 2025. `https://eprint.iacr.org/2025/1187`.

[RVW13] Guy N. Rothblum, Salil P. Vadhan, and Avi Wigderson. Interactive Proofs of Proximity: Delegating Computation in Sublinear Time. In *Proceedings of the 45th ACM Symposium on Theory of Computing*, pages 793–802, 2013.