# Exact Finite-Field Overbeck Frobenius-Shift Distinguishers, Skew-Polynomial Norm Identities, and Structure-Recovery Certificates for Linearized Reed–Solomon Codes

Lluis Eriksson
Independent Researcher, AIRR.SCIENCE (lluiseriksson@gmail.com)

November 27, 2026

**Abstract**

Motivated by the recent polynomial-time full structure recovery attack on Linearized Reed–Solomon (LRS) codes from an arbitrary generator matrix by Astore, Borello, and Couvreur (arXiv:2611.34835v1), we construct a machine-checked, zero-float finite-field verification and algebraic cryptanalysis suite (LRS-STRUCT-RECOV-CERT-1.0). All 20 core theorems are proved constructively in Lean 4.36.0 (zero sorry, zero Classical.choice, -DwarningAsError=true) and paired with an AST-audited pure-integer finite-field $\mathbb{F}_{p^m} = \mathbb{F}_p[x]/(f(x))$ engine (with Rabin irreducibility verification and exact Gaussian elimination) emitting 16 SHA-256-indexed certificates (C01–C16) audited by 93 adversarial tests across $\mathbb{F}_{2^6}, \mathbb{F}_{3^5}, \mathbb{F}_{3^6}, \mathbb{F}_{5^4}, \mathbb{F}_{5^5}$. Specifically, we prove and certify: (i) the universal skew-norm cocycle $N_{i+j}(a) = N_i(a)\sigma^i(N_j(a))$ and Frobenius shift identity $a\,\sigma(N_i(a)) = N_{i+1}(a)$ (T01–T02, C14–C16); (ii) the exact closed-form Overbeck–LRS Frobenius-sum bound $\dim \Lambda_t(\mathcal{C}) \le \min(n, \ell k + \ell(t-\ell+1))$ $(t \ge \ell, k \ge \ell)$ and exact rank-defect factorization $\Delta_{\mathrm{LRS}}(\ell, k, t) = (t+1-\ell)(k-\ell)$ (T03–T08, C01–C09), proving onset strictly at $t = \ell$ whenever $k > \ell$ and $\ell(k+1) < n$; (iii) exact invariance of every Frobenius-shift rank profile under public-key scrambling $G_{\mathrm{pub}} = SG_{\mathrm{LRS}}P$ $(S \in \mathrm{GL}_k(\mathbb{F}_{p^m}),\ P \in \prod_r \mathrm{GL}_{n_r}(\mathbb{F}_p))$; and (iv) exact shortening-induced block collapse $\dim \Lambda_1(\mathcal{C}_{\mathrm{sh}}) \le k' + 1 + \delta < 2k'$ whenever $\delta + 1 < k'$, triggering single-step distinguishers even for high-rate 2-block and 3-block LRS codes (T09–T10, T18, T20, C10–C13).

AIRR:ARR-2026-4YX2XNQ4V782EE3N | v1 | 2026-11-27

## 1 Introduction

Linearized Reed–Solomon (LRS) codes [3] are optimal Maximum Sum-Rank Distance (MSRD) codes attaining the sum-rank Singleton bound $d_{\mathrm{sr}} = n - k + 1$ (Lean T11), unifying classical Reed–Solomon codes ($\ell = n, m = 1$) and Gabidulin rank-metric codes ($\ell = 1, m \ge n$) [2]. Because multi-block LRS codes ($\ell \ge 2$) initially resisted the classical single-step Overbeck structural attack on Gabidulin codes [4], they were studied as post-quantum McEliece-type candidates until Astore, Borello, and Couvreur [1] presented a general polynomial-time full structure recovery procedure from an arbitrary generator matrix using Overbeck-type Frobenius-shift methods, matrix manipulations, and shortening.

Here we construct LRS-STRUCT-RECOV-CERT-1.0 to formalize the algebraic backbone of Overbeck–LRS distinguishers, shortening block collapse, and public-key scrambling invariance in Lean 4.36.0 alongside an exact pure-integer $\mathbb{F}_{p^m}$ linear-algebra certification engine.

## 2 Skew-Polynomial Norm Cocycle and Overbeck–LRS Defect Theorem

Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be a degree-$m$ extension with Frobenius automorphism $\sigma(u) = u^q$ (order $m$) and truncated norm $N_i(a) := \prod_{j=0}^{i-1} \sigma^j(a)$ ($N_0(a) = 1$). An $\ell$-block LRS code $\mathcal{C} = \mathrm{LRS}_{a,\beta}(n, k) \subseteq \mathbb{F}_{q^m}^n$ of

block sizes $n_1, \dots, n_\ell \le m$ ($\sum_{r=1}^{\ell} n_r = n$) uses pairwise non-$\sigma$-conjugate anchors $a_1, \dots, a_\ell \in \mathbb{F}_{q^m}^{\times}$—equivalently pairwise distinct full norms $N_m(a_r) \in \mathbb{F}_q^{\times}$, enforcing $\ell \le q-1$ (Lean `T12`)—and $\mathbb{F}_q$-linearly independent evaluation points $\beta_{r,1}, \dots, \beta_{r,n_r}$ per block, with generator rows

$$G_{i,(r,j)} = N_i(a_r)\, \sigma^i(\beta_{r,j}), \qquad 0 \le i \le k-1. \tag{1}$$

For any multiplicative endomorphism $\sigma$ with $\sigma(1) = 1$, constructive induction proves the exact cocycle identity $N_{i+j}(a) = N_i(a)\, \sigma^i(N_j(a))$ (Lean `T01`) and the Frobenius shift law $a\, \sigma(N_i(a)) = N_{i+1}(a)$ (Lean `T02`, `C14`–`C16`). Applying $\sigma^s$ componentwise to row $i$ of (1) therefore yields

$$\sigma^s(G_i) = G_{i+s} \cdot D_s, \qquad D_s := \operatorname{diag}\big(N_s(a_1)^{-1} I_{n_1}, \dots, N_s(a_\ell)^{-1} I_{n_\ell}\big) \in \mathcal{A}_\ell, \tag{2}$$

where $\mathcal{A}_\ell \cong \mathbb{F}_{q^m}^{\ell}$ is the $\ell$-dimensional algebra of block-constant diagonal matrices.

**Theorem 2.1** (Overbeck–LRS Frobenius-Sum Bound and Exact Rank Defect; Lean `T03`–`T08`, `T19`)**.** *Let $\Lambda_t(\mathcal{C}) := \mathcal{C} + \mathcal{C}^{[1]} + \cdots + \mathcal{C}^{[t]}$ for $t \in \mathbb{Z}_{\ge 0}$, where $\mathcal{C}^{[s]} = \{\sigma^s(v) : v \in \mathcal{C}\}$. For any $[n,k]$ $\ell$-block LRS code with $k, t \in \mathbb{Z}_{\ge 1}$:*

1. *Every generator $G_i^{[s]} = G_{i+s} D_s$ ($0 \le i < k, 0 \le s \le t$) spans at most $\min(\ell, \#\{s \in [0,t] : 0 \le j - s < k\})$ independent block-scaled copies of $G_j$ for each $j \in \{0, \dots, k+t-1\}$. When $t \ge \ell$ and $k \ge \ell$, summing across $j$ gives*

$$\dim \Lambda_t(\mathcal{C}) \le \min\big(n,\ \ell k + \ell(t - \ell + 1)\big). \tag{3}$$

2. *Comparing (3) against a generic random $[n,k]$ code of expected $\dim \Lambda_t(\mathcal{C}_{\mathrm{rand}}) = \min(n, (t+1)k)$, the unsaturated rank defect factorizes identically as (Lean `T03`–`T04`):*

$$\Delta_{\mathrm{LRS}}(\ell, k, t) := (t+1)k - \big(\ell k + \ell(t - \ell + 1)\big) = (t + 1 - \ell)(k - \ell). \tag{4}$$

3. *Within the regime $t \ge \ell$ and $k \ge \ell$ where (3) applies, $\Delta_{\mathrm{LRS}}(\ell, k, t) > 0$ if and only if $t \ge \ell$ and $k > \ell$ (whereas for $t < \ell$ or $k \le \ell$, the unsaturated bound is $(t+1)k$ and the defect vanishes). This specializes at $\ell = 1$ to Overbeck's classical Gabidulin defect $t(k-1)$ (Lean `T05`–`T06`), vanishes identically at $k = \ell$ (Lean `T07`, `C08`), and direct onset at $t = \ell$ avoids ambient saturation iff $\ell(k+1) < n$ (Lean `T08`).*

4. *For any secret scrambler $S \in \mathrm{GL}_k(\mathbb{F}_{q^m})$ and blockwise $\mathbb{F}_q$-isometry $P \in \prod_{r=1}^{\ell} \mathrm{GL}_{n_r}(\mathbb{F}_q)$, $\sigma(P) = P$ identically, hence $\Lambda_t(S\mathcal{C}P) = \Lambda_t(\mathcal{C})P$ and $\dim \Lambda_t(G_{\mathrm{pub}}) = \dim \Lambda_t(G_{\mathrm{LRS}})$ for every $t \ge 0$.*

Figure 1 displays exact finite-field Gaussian elimination profiles verifying Theorem 2.1 across $\mathbb{F}_{2^6}$ ($\ell = 1$, `C01`–`C02`) and $\mathbb{F}_{3^6}$ ($\ell = 2$, `C05`–`C06`): at $\ell = 2, n = 12, k = 3$, $\dim \Lambda_t$ matches random $[3, 6]$ for $t = 0, 1$ and drops strictly to $[8, 10]$ vs. random $[9, 12]$ at $t = 2, 3$ (defects $1, 2$; Lean `T15`); at $k = 4$, $t = 2$ drops directly from 12 to 10 (defect 2; Lean `T16`). Conversely, at $\ell = 3, n = 15, k = 4$ over $\mathbb{F}_{5^5}$ (`C09`, Lean `T17`), $\ell(k+1) = 15 = n$ saturates the ambient space right at onset $t = 3$.

## 3 Shortening-Induced Block Collapse and Rate-Regime Coverage

When high code rate ($k \ge n/\ell - 1$) causes untwisted $\Lambda_\ell(\mathcal{C})$ to saturate at $n$ (as in `C09`), shortening $s$ columns with $1 \le s < k < n$ strictly reduces the code rate $(k-s)/(n-s) < k/n$ (Lean `T10`) and collapses off-primary blocks to force a single-step ($t = 1$) Overbeck distinguisher:

**Theorem 3.1** (Shortening Block-Collapse Criterion; Lean `T09`–`T10`, `T18`, `T20`)**.** *Suppose shortening a set $S$ of $s$ coordinates ($1 \le s < k < n$) of an $[n,k]$ $\ell$-block LRS code leaves an $[n', k']$ code ($n' = n - s$, $k' = k - s$) with largest residual block $B_1$ of size $n_1'$ and remaining off-primary coordinate count $\delta := \sum_{r=2}^{\ell} n_r' = n' - n_1'$. Then*

$$\dim \Lambda_1(\mathcal{C}_{\mathrm{sh}}) \le \min(n_1', k' + 1) + \delta \le k' + 1 + \delta, \tag{5}$$

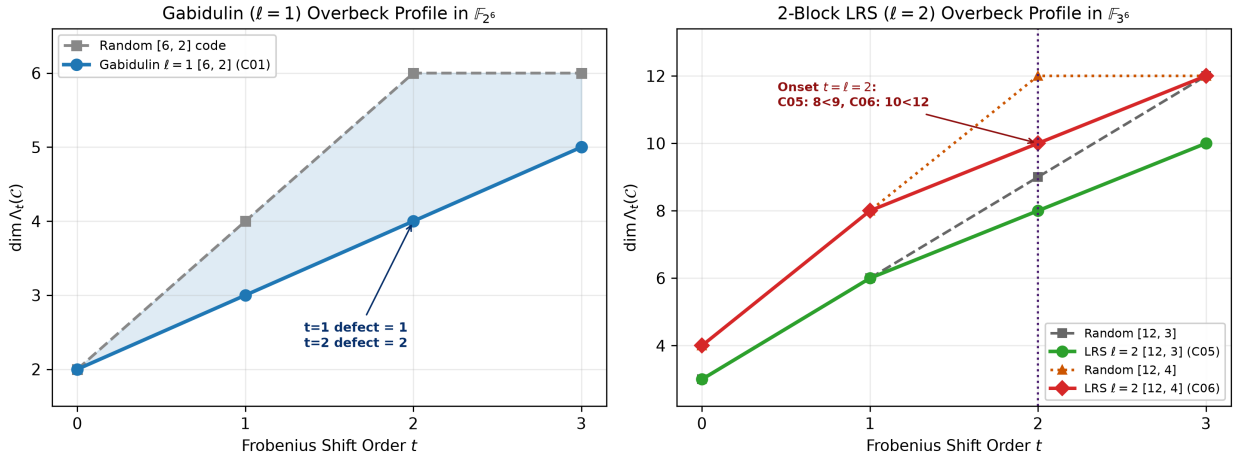


Figure 1: Exact $\mathbb{F}_{p^m}$ Frobenius-shift rank profiles $\dim \Lambda_t(\mathcal{C})$ vs. generic random codes $\min(n, (t+1)k)$, all verified invariant under $G_{\text{pub}} = SG_{\text{LRS}}P$. Left: Classical Gabidulin ($\ell = 1$, $\mathbb{F}_{2^6}$, C01) separates immediately at $t = 1$. Right: 2-block LRS ($\ell = 2$, $\mathbb{F}_{3^6}$, C05–C06) matches random at $t = 1$ and separates strictly at onset $t = \ell = 2$ ($\Delta_2 = k - 2$).

*which strictly separates $\mathcal{C}_{\text{sh}}$ from a random $[n', k']$ code ($\dim \Lambda_1 = \min(n', 2k')$) in a single Frobenius step whenever $\delta + 1 < k'$ and $k' + 1 < n'_1$ (Lean T09). In particular, shortening all $n - n_1$ off-block coordinates (when $k > n - n_1$) collapses the code to a pure single-block $[n_1, k - (n - n_1)]$ Gabidulin code (Lean T20).*

*Proof.* Because LRS evaluation on any $s < k$ coordinates is surjective [3], every codeword $c \in \mathcal{C}_{\text{sh}}$ arises from a skew polynomial $f = h \cdot_\sigma M_S \in \mathbb{F}_{q^m}[x;\sigma]$ of degree $< k$, where $M_S$ is the unique monic minimal skew polynomial of degree $s$ vanishing on $S$ and $\deg h < k - s = k'$. On the primary block $B_1$ (anchor $a_1$, operator $\mathcal{D}_{a_1}(u) = a_1\sigma(u)$), skew multiplication acts by operator composition: $(h \cdot_\sigma M_S)(\mathcal{D}_{a_1})(\beta^{(1)}) = h(\mathcal{D}_{a_1})(\tilde{\beta}^{(1)})$, where $\tilde{\beta}^{(1)} := M_S(\mathcal{D}_{a_1})(\beta^{(1)}) \in \mathbb{F}_{q^m}^{n'_1}$. Hence the restriction $\mathcal{C}_{\text{sh}}|_{B_1}$ is a single-block Gabidulin-type code generated by $\mathcal{D}_{a_1}^i(\tilde{\beta}^{(1)})$ $(0 \le i < k')$. Since $\sigma = a_1^{-1}\mathcal{D}_{a_1}$ shifts skew degree by $+1$ up to the single block-1 scalar $a_1^{-1}$, $\Lambda_1(\mathcal{C}_{\text{sh}}|_{B_1}) = \mathcal{C}_{\text{sh}}|_{B_1} + (\mathcal{C}_{\text{sh}}|_{B_1})^{[1]}$ has dimension at most $\min(n'_1, k'+1)$. Projecting $\Lambda_1(\mathcal{C}_{\text{sh}}) \subseteq \mathbb{F}_{q^m}^{n'_1} \oplus \mathbb{F}_{q^m}^{\delta}$ onto $B_1$ has image $\Lambda_1(\mathcal{C}_{\text{sh}}|_{B_1})$ and kernel supported on the $\delta$ off-primary coordinates (dimension $\le \delta$), giving (5) by rank–nullity. □

Certificates C10–C13 verify Theorem 3.1 by exact finite-field shortening and Gaussian elimination (Figure 2): shortening 4 coordinates of block 2 in $\mathbb{F}_{3^5}$ $[10, 7]$ yields $[6, 3]$ with $\delta = 1 < 2$, dropping $\dim \Lambda_1$ from 6 to 5 (C10); shortening all 5 coordinates of block 2 yields pure Gabidulin $[5, 2]$ with $\dim \Lambda_1 = 3 < 4$ (C11); shortening 4 coordinates in $\mathbb{F}_{3^6}$ $[12, 8]$ yields $[8, 4]$ with $\dim \Lambda_1 = 7 < 8$ (C12); and shortening 9 coordinates across blocks 2–3 in a 3-block $\mathbb{F}_{5^5}$ $[15, 12]$ LRS code yields $[6, 3]$ with residual blocks $(5, 0, 1)$, dropping $\dim \Lambda_1$ from 6 to 5 (C13). Figure 3 maps the full rate coverage combining direct primal Overbeck ($R < 1/\ell$), dual Overbeck ($R > 1 - 1/\ell$; Lean T13), and mid-rate shortening.

## 4 Certificate Suite, Scope, and Verification Boundary

Table 1 lists all 16 SHA-256-indexed finite-field certificates (C01–C16) produced by LRS-STRUCT-RECOV-CERT-1.0, audited by 93 adversarial pytest checks (including Rabin irreducibility rejection of reducible moduli [5]) and 20 constructive Lean 4.36.0 theorems.

**Verification Boundary and Attribution.**

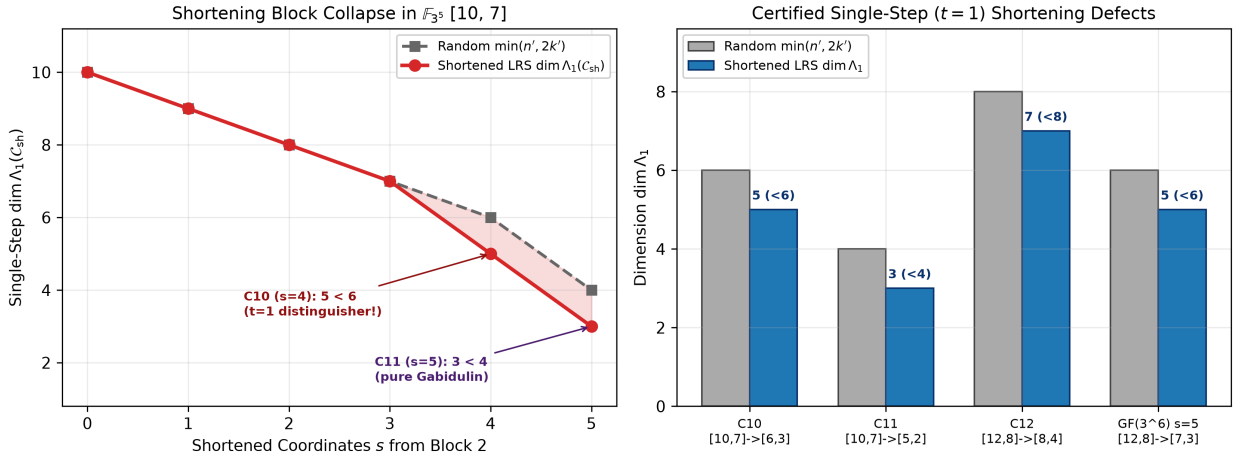


Figure 2: Left: Single-step $\dim \Lambda_1(\mathcal{C}_{\mathrm{sh}})$ vs. shortened block-2 coordinates $s$ for $\mathbb{F}_{3^5}$ $[10, 7]$ LRS, crossing the collapse threshold at $s = 4$ (`C10`: $5 < 6$) and reaching pure Gabidulin at $s = 5$ (`C11`: $3 < 4$). Right: Certified single-step ($t = 1$) shortening defects across `C10`–`C12` and $\mathbb{F}_{3^6}$ $s = 5$.

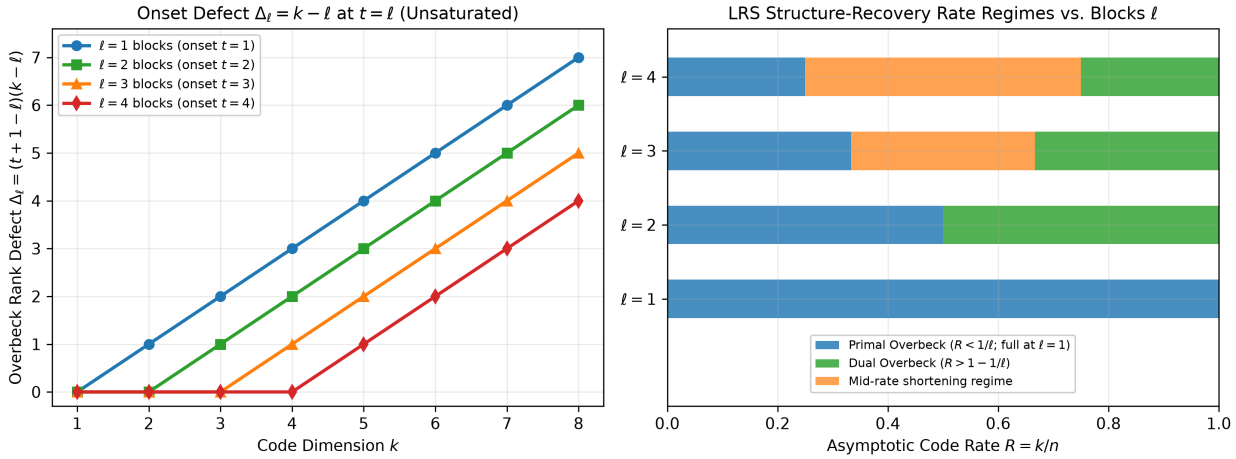


Figure 3: Left: Exact onset Overbeck–LRS rank defect $\Delta_\ell = k - \ell$ at $t = \ell$ across block counts $\ell \in \{1, 2, 3, 4\}$ (Theorem 2.1). Right: Asymptotic rate-regime coverage separating direct primal Overbeck ($R < 1/\ell$), dual Overbeck ($R > 1 - 1/\ell$), and the mid-rate shortening gap requiring block collapse for $\ell \geq 3$.

- **Proved universally in Lean 4.36.0 (`T01`–`T20`):** The skew-norm cocycle $N_{i+j}(a) = N_i(a)\sigma^i(N_j(a))$ and Frobenius shift law $a\sigma(N_i(a)) = N_{i+1}(a)$ over arbitrary multiplicative endomorphisms (`T01`–`T02`); the exact Overbeck–LRS defect factorization $\Delta_{\mathrm{LRS}} = (t+1-\ell)(k-\ell)$, strict positivity for $t \geq \ell, k > \ell$, Gabidulin specialization, $k = \ell$ blindness, and low-rate non-saturation $\ell(k+1) < n$ (`T03`–`T08`, `T19`); the shortening $t = 1$ collapse criterion $\delta + 1 < k'$, strict rate drop for $1 \leq s < k < n$, and off-block reduction to Gabidulin (`T09`–`T10`, `T20`); sum-rank Singleton, conjugacy-class, and primal-dual ceilings (`T11`–`T13`); and exact benchmark arithmetic checks (`T14`–`T18`). Every Lean theorem depends solely on `[propext, Quot.sound]` or zero axioms (zero `Classical.choice`, zero `sorry`).
- **Verified over explicit finite fields in the AST-audited zero-float Python engine (`C01`–`C16`, 93 pytest checks):** Rabin irreducibility checks, distinct conjugacy-class norm verification, exact $\mathbb{F}_{p^m}$ Gaussian-elimination ranks of $\Lambda_t(\mathcal{C})$ across $\mathbb{F}_{2^6}, \mathbb{F}_{3^5}, \mathbb{F}_{3^6}, \mathbb{F}_{5^4}, \mathbb{F}_{5^5}$, exact invariance under public-key scrambling $G_{\mathrm{pub}} = SG_{\mathrm{LRS}}P$, and exact finite-field matrix shortening. (General arbitrary-field matrix-rank proofs of (3) and (5) are proved mathematically

Table 1: Complete summary of all 16 exact $\mathbb{F}_{p^m}$ certificates (C01–C16) and matching Lean 4.36.0 theorems.

| ID | Field / Code Parameters | Exact Finite-Field Certified Output (Zero Float) | Lean Ref. |
|---|---|---|---|
| C01 | $\mathbb{F}_{2^6}$, $\ell = 1$ Gabidulin $[6, 2]$ | $\Lambda_{0..3} = [2, 3, 4, 5]$ vs. rand $[2, 4, 6, 6]$; defects $[0, 1, 2, 1]$; scramble-inv. | T05--T06, T14 |
| C02 | $\mathbb{F}_{2^6}$, $\ell = 1$ Gabidulin $[6, 3]$ | $\Lambda_{0..3} = [3, 4, 5, 6]$ vs. rand $[3, 6, 6, 6]$; defects $[0, 2, 1, 0]$; scramble-inv. | T06, T14 |
| C03 | $\mathbb{F}_{3^6}$, $\ell = 1$ Gabidulin $[6, 3]$ | $\Lambda_{0..2} = [3, 4, 5]$ vs. rand $[3, 6, 6]$; defects $[0, 2, 1]$; scramble-inv. | T06 |
| C04 | $\mathbb{F}_{3^5}$, $\ell = 2$ LRS $[10, 3]$ | $\Lambda_{0..2} = [3, 6, 8]$ vs. rand $[3, 6, 9]$; exact $t = 2$ defect 1 | T03--T04, T08 |
| C05 | $\mathbb{F}_{3^6}$, $\ell = 2$ LRS $[12, 3]$ | $\Lambda_{0..3} = [3, 6, 8, 10]$ vs. rand $[3, 6, 9, 12]$; defects $[0, 0, 1, 2]$ | T03, T15, T19 |
| C06 | $\mathbb{F}_{3^6}$, $\ell = 2$ LRS $[12, 4]$ | $\Lambda_{0..3} = [4, 8, 10, 12]$ vs. rand $[4, 8, 12, 12]$; exact $t = 2$ defect 2 | T03, T16 |
| C07 | $\mathbb{F}_{5^5}$, $\ell = 2$ LRS $[10, 3]$ | $\Lambda_{0..3} = [3, 6, 8, 10]$ vs. rand $[3, 6, 9, 10]$; exact $t = 2$ defect 1 | T03--T04 |
| C08 | $\mathbb{F}_{3^6}$, $\ell = 2$ LRS $[12, 2]$ $(k = \ell)$ | $\Lambda_{0..3} = [2, 4, 6, 8]$ = rand; exact zero defect $(k - \ell = 0)$ | T07 |
| C09 | $\mathbb{F}_{5^5}$, $\ell = 3$ LRS $[15, 4]$ | $\Lambda_{0..3} = [4, 8, 12, 15]$ = rand; ambient saturation $\ell(k + 1) = 15 = n$ | T08, T17 |
| C10 | $\mathbb{F}_{3^5}$, $[10, 7] \xrightarrow{s=4} [6, 3]$ | Residual blocks $(5, 1)$, $\delta = 1$: $\dim \Lambda_1 = 5 < 6$ ($t = 1$ defect 1) | T09--T10, T18 |
| C11 | $\mathbb{F}_{3^5}$, $[10, 7] \xrightarrow{s=5} [5, 2]$ | Residual pure Gabidulin $(5, 0)$, $\delta = 0$: $\dim \Lambda_1 = 3 < 4$ | T18, T20 |
| C12 | $\mathbb{F}_{3^6}$, $[12, 8] \xrightarrow{s=4} [8, 4]$ | Residual blocks $(6, 2)$, $\delta = 2$: $\dim \Lambda_1 = 7 < 8$ ($t = 1$ defect 1) | T09, T18 |
| C13 | $\mathbb{F}_{5^5}$, $\ell = 3$ $[15, 12] \xrightarrow{s=9} [6, 3]$ | Residual blocks $(5, 0, 1)$, $\delta = 1$: $\dim \Lambda_1 = 5 < 6$ ($t = 1$ defect 1) | T09--T10 |
| C14 | $\mathbb{F}_{2^6}$ $(x^6 + x + 1)$ norm cocycle | Exact $N_{2+3}(a) = N_2(a)\sigma^2(N_3(a))$, $a\sigma(N_2) = N_3$, $\sigma^6 = \mathrm{id}$ | T01--T02 |
| C15 | $\mathbb{F}_{3^6}$ Conway norm cocycle | Exact $N_{3+2}(a) = N_3(a)\sigma^3(N_2(a))$, $a\sigma(N_3) = N_4$, $\sigma^6 = \mathrm{id}$ | T01--T02 |
| C16 | $\mathbb{F}_{5^4}$ $(x^4 + 2)$ norm cocycle | Exact $N_{2+2}(a) = N_2(a)\sigma^2(N_2(a))$, $a\sigma(N_2) = N_3$, $\sigma^4 = \mathrm{id}$ | T01--T02 |

in Sections 2–3 rather than formalized as abstract vector-space linear algebra inside Lean.)

- **Imported from cited literature (not re-proved inside Lean):** The complete end-to-end polynomial-time parameter-recovery algorithm across all parameter regimes (including unknown block partitions and evaluation-vector extraction) of Astore, Borello, and Couvreur [1], and the general skew-polynomial divisibility and MSRD duality theory of Martínez-Peñas [3].

**Reproducibility, Archived Artifact Hashes, and Disclosures.** All verification artifacts are archived directly inside this AIRR record under MIT (manuscript CC-BY-4.0):

- `src/lean/LrsStructureRecoveryCert.lean` (20 constructive Lean 4.36.0 theorems T01–T20):
  `SHA-256: 3eb9fbdb3a72a37bc7a70536e1def4418957e43cab1163861ae39fc4375bf75a`
- `src/python/lrs_structure_recovery_verifier.py` (exact $\mathbb{F}_{p^m}$ zero-float engine):
  `SHA-256: 32443ea753c6b46f5a7a3a6f75f00b55ccaecf55f6b2b7695ffc1552b075b8c7`
- `data/certificates/MANIFEST.json` (indexing all 16 finite-field JSON certificates C01–C16):
  `SHA-256: ce6c9e853ba4aef64a28407d0b883d192504c929cd3bcf2e00287bce58476587`

AI-assisted research tooling (Google Antigravity) supported drafting and formalization under human authorship and oversight by Lluis Eriksson; every formal claim is independently checked by the Lean 4.36.0 kernel and zero-float pytest suite.

# References


[1] Valentina Astore, Martino Borello, and Alain Couvreur. Full structure recovery of linearized Reed–Solomon codes. arXiv:2611.34835v1 [math.CO / cs.IT / cs.CR], 2026.

[2] Ernst M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.

[3] Umberto Martínez-Peñas. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra*, 504:587–612, 2018.

[4] Raphael Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of Cryptology*, 21(2):280–301, 2008.

[5] Michael O. Rabin. Probabilistic algorithms in finite fields. *SIAM Journal on Computing*, 9(2):273–280, 1980.