Constructive Algebraic and Spectral-Repair Certificates for the 1/2 Logarithmic Exponent of Finite Fourier Transforms

Lluis Eriksson
Independent Researcher (lluis@airr.science)

Companion Verification Artifact to OpenAI Math Release (November 24, 2026)

November 26, 2026

Abstract

We present FFT-EXP-HALF-CERT-1.0, an independently reproducible, zero-floating-point verification suite and constructive Lean 4.35.0 kernel auditing the finite-dimensional algebraic, geometric, nilpotent time-expansion, Hermite spectral-repair, and Bluestein chirp-specialization mechanisms of OpenAI's November 24, 2026 unrefereed preprint *"The logarithmic exponent of finite Fourier transforms"* (Theorems 1.1, 1.2, 2.2, 4.1, and Corollary 8.2). Without claiming to formalize the preprint's Zariski-closure Grassmannian compactness or asymptotic recursion over arbitrary fields, we build a four-mode exact verifier over $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{F}_p$ backed by 18 constructive Lean 4 theorems (0 `sorry`, 0 custom axioms, 0 `Classical.choice`, 0 warnings). Across 16 canonical certificates (`C01`–`C16`), we audit (i) Lemma 2.3 two-phase controlled-addition swaps, Theorem 2.2 Pythagorean rectangle price excesses, and Proposition 2.4 force-disk midpoint rigidity, (ii) Lemma 3.3 nilpotent time-expansion rank/support decompositions of feedback linear systems and Lemma 3.2 block-echelon row quotients, (iii) Section 4.1/Lemma 4.2 integral parity-sign count predictors, Lemma 4.3 Potter/Clifford matrix linearizations $L^b = pI$, and Lemma 4.4 full-rate Hermite spectral repair for $\ell \in \{2, 3\}$, and (iv) Section 5.1–5.2 Fourier query-product kernels, Hamming-distance Gram ranks over $\mathbb{F}_\ell$, and Corollary 8.2 Bluestein chirp convolution specialization. All 16 certificates, 70 unit/forgery tests, and SHA-256 manifests pass deterministically.

1 Introduction and Scope

Since Cooley and Tukey's $O(N \log N)$ fast Fourier transform [3], determining the intrinsic logarithmic cost of computing a finite abelian Fourier transform over binary linear circuits with arbitrary scalars has remained a foundational question [4, 1]. In its November 24, 2026 unrefereed preprint [6], OpenAI establishes that the optimal logarithmic exponent is exactly 1/2: J independent transforms of order N require $\Omega(JN\sqrt{\log N})$ gates even with feedback states, low-rank errors, and sparse errors (Theorems 1.1–1.2), and admit $O_\epsilon(JN(1+\log N)^{1/2+\epsilon})$ circuits (Theorems 4.1, 5.1, 8.1), with identical 1/2 exponent for formal polynomial convolution (Corollary 8.2).

The lower bound builds on planar spectral prices [5], placing row and column labels on a rectangle where a character table beats a permutation matrix by $L^2/(1+\sqrt{1+L^2})\log_2 N$ (Theorem 2.2) via a two-phase swap (Lemma 2.3) and force-disk rigidity (Proposition 2.4), combined with upper-triangular echelon row quotients (Lemma 3.2) and nilpotent time expansion of feedback circuits (Lemma 3.3). The upper bound expresses a large transform as a product of commuting queries, approximates its parity/character sign by a low-degree integral polynomial on a central binomial window (Lemma 4.2), linearizes the polynomial via Potter's identity [7] (Lemma 4.3), repairs exceptional rows exactly using Vandermonde Reed–Solomon checks [8] and a double-root Hermite polynomial (Lemma 4.4), routes shared queries via Hamming-intersection matrices (Sec. 5.2), and connects convolution to cyclic DFT via Bluestein's chirp identity [2] (Corollary 8.2).

Honest Scope Boundary. This companion artifact verifies finite algebraic identities, exact finite-field matrix equations, and rational geometric witnesses extracted from [6]. It does *not* formalize projective Grassmannian closure arguments (Sec. 3.2), Hoeffding tail asymptotics (Sec. 4.1), prime-number-theorem length selection (Sec. 8), or the full multi-level recursion establishing Theorem 1.1 end-to-end.

2 Constructive Lean 4.35.0 Kernel

The formal kernel `FftExpHalfCert.lean` compiles cleanly under Lean 4.35.0 (`-j 1`) with zero `sorry`, zero custom axioms, zero warnings, and zero dependence on `Classical.choice`. Table 1 summarizes all 18 machine-checked theorems. Highlights include Theorem 4 (exact integer parallelogram proof of Proposition 2.4 force-disk midpoint rigidity $a = b = (p+r)/2$), Theorem 7 (exact feedback time-expansion difference identity), Theorem 11 (exhaustive constructive verification of the 3-query binary parity predictor across all $2^6 = 64$ pairs (k, β)), Theorem 13

Table 1: The 18 constructive Lean 4.35.0 theorems in `FftExpHalfCert.lean` (0 `sorry`, 0 custom axioms, 0 `Classical.choice`).

#	Theorem Identifier	Paper Reference / Invariant
1	`rectangle_excess_rationalized`	Thm. 2.2 $(D-W)(D+W) = L^2$
2	`character_table_strict_excess`	Thm. 2.2 $L+W < L+D$ for $L > 0$
3	`two_phase_controlled_swap`	Lem. 2.3 $(x, y) \mapsto (y, x+y)$
4	`force_disk_midpoint_rigidity`	Prop. 2.4 disk forces $a = b = \frac{p+r}{2}$
5	`projected_list_lower_bound`	Lem. 3.1 $100V_{-}(QU) \geq 181N$
6	`block_echelon_rank_budget`	Lem. 3.2 list $\sum(n_i - \operatorname{rk} Q_i) \leq r$
7	`time_expansion_difference_identity`	Lem. 3.3 $(I - Z_R C')(V_R - V_0)$
8	`binary_unrolling_support_bound`	Lem. 3.3 BinTree $d \cdot$ leaves $\leq d2^{d-1}$
9	`markov_surviving_blocks`	Sec. 3.4 199/200 blocks survive
10	`small_order_vandermonde_bound`	Sec. 3.4 small-order $s \geq h/12$
11	`binary_three_query_predictor_exact`	Sec. 4.1 m=3 window $[1, 2]$ exact
12	`potter_mat2_square_identity`	Lem. 4.3 2×2 $(U+V)^2 = U^2+V^2$
13	`hermite_double_root_l2`	Lem. 4.4 $g(y) - z = (y-z)^2 D_z(y)$
14	`hermite_repair_exact_zero`	Lem. 4.4 full repair $g(P)\hat{X} - P\hat{Z} + z\hat{Z} = z\hat{X}$
15	`query_product_quadratic_phase_identity`	Sec. 5.1 Fourier inversion phase
16	`hamming_routing_poly_root`	Sec. 5.2 inductive $p(\ell h) = 0$
17	`bluestein_chirp_exponent_identity`	Cor. 8.2 $b_2(i)+b_2(-j)-b_2(i-j) = 2ij$
18	`product_gate_linear_part`	Cor. 8.2 linear part $u_0v_1+v_0u_1$

(exact double-root factorization $(2y - y(y^2-1)) - 2z = (y-z)^2(-y-2z)$ whenever $z^2 = 1$), and Theorem 17 (universal Bluestein chirp identity $b_2(i) + b_2(-j) - b_2(i-j) = 2ij$).

3 The `FFT-EXP-HALF-CERT-1.0` Protocol

Our Python verifier (`src/fft_exp_verifier.py`) enforces zero floating-point literals, zero `float()` calls, zero true-division operators (`/`, `/=`), zero `math` imports, `MAX_JSON_BYTES = 1_000_000`, duplicate-key rejection via `object_pairs_hook`, and lowest-terms rationals $[p, q]$ ($|p|, q \leq 10^{12}$, $\gcd(|p|, q) = 1$).

Definition 1 (`FFT-EXP-HALF-CERT-1.0` Modes)**.** *Each certificate invokes one of four exact verification modes:*

1. *`rectangle_price_and_two_phase_swap` (Thm. 2.2, Lem. 2.3, Prop. 2.4): (a) `two_phase_swap_character` verifies primitive N-th root $\omega \in \mathbb{F}_p^\times$, constructs $Q = F_{C_N}$, checks $Q^TQ = NP_{\text{neg}}$, verifies that the two-phase controlled map equals UP_{swap}, and confirms $(I \otimes Q^{-1})U(I \otimes Q)$ is strictly diagonal with exact character weights ω^{-xk}; (b) `rectangle_excess_and_force_disk` checks $D^2 = L^2 + W^2$, exact rational excess $(D-W)m = L^2m/(W+D)$, unit vectors $|p|^2 = |r|^2 = 1$, zero-sum $a + b = p + r$, disk containment $|a - p/2|^2, |b - p/2|^2 \leq 1/4$, and midpoint rigidity $a = b = (p+r)/2$.*
2. *`time_expansion_and_row_quotient` (Lem. 3.2, 3.3): (a) `time_expansion_feedback` requires nonzero C, A, fan-in ≤ 2, and $\det(I - C) \neq 0$ over $\mathbb{F}_p$, builds $R = I_d + D$ and nilpotent R_0, verifies $R_0^d = 0$, $\operatorname{rank}(R - R_0) = 1$, the exact difference equation $(I - Z_RC')(V_R - V_{R_0}) = (Z_R - Z_{R_0})(C'V_{R_0} + A')$, $\operatorname{rank}(V_R - V_{R_0}) \leq s$, row support of $V_{R_0} \leq d2^{d-1}$, and lower-triangular time structure of V_R with diagonal blocks $M = (I - C)^{-1}A$; (b) `row_quotient_echelon` checks $1 \leq \operatorname{rank}(B) \leq r$, $QB = 0$, upper triangularity of Q, and diagonal-block rank conservation $\sum_i (n_i - \operatorname{rank} Q_{ii}) \leq r$.*
3. *`prediction_and_hermite_repair` (Sec. 4.1, Lem. 4.2–4.4): (a) `binary_parity_predictor` evaluates the exact integral binomial polynomial P_β over all 4^m pairs (k, β) and confirms exact parity match on $[u, v]$ plus uniform in-window and exceptional counts; (b) `potter_matrix_power` requires ≥ 2 nonzero monomials mod p, constructs $L = \sum_i Z^{\otimes i} \otimes S_i \otimes I^{\otimes(h-1-i)}$ over $\mathbb{F}_p$, checks $ZS_i = \xi S_i Z$ and $VU = \xi UV$, and verifies $L^b = p(\lambda) I_{b^h}$; (c) `hermite_spectral_repair` verifies $z^\ell = 1$, recovers nonzero e_J from Vandermonde checks $\widehat{HPX} - zH\hat{X}$, divides $g(y) - z$ by $(y-z)^2$ in $\mathbb{F}_p[y]$ to obtain $D_z(y)$, solves $H_J^T a = D_z(p_J)e_J$, lifts nonzero $\hat{Z} = H^T a$, and checks $g(P)\hat{X} - P\hat{Z} + z\hat{Z} = z\hat{X}$ on all W rows.*
4. *`query_product_and_bluestein_chirp` (Sec. 5.1–5.2, Cor. 8.2): (a) `query_kernel_and_hamming_gram` verifies $\ell^{-2}\sum_{X,Z} \zeta^{(x-s)X+(y-t')Z+XZ} = \ell^{-1}\zeta^{(x-s)(t'-y)}$ on all ℓ^4 tuples, computes exact $\mathbb{F}_\ell$-rank of $\Gamma(v, w) = 1 - \Delta(v, w)^{\ell-1}$ on power-of-two alphabet $q \in \{2, 4\}$, and verifies $p(k) \in \mathbb{Z}[1/\ell]$ for all $0 \leq k \leq L$ with $p(0) = 1$ and $p(\ell h) = 0$; (b) `bluestein_chirp_convolution` checks $b(i) + b(-j) - b(i-j) = ij$ on all m^2 pairs and verifies exact polynomial multiplication $q^{b(i)}[X^{m-1+i}](H(X)Y(X))$ matches the direct C_m DFT over $\mathbb{F}_p$.*

Proposition 1 (Verifier Soundness)**.** *Whenever `verify_file` outputs `VERIFIED` on an `FFT-EXP-HALF-CERT-1.0` certificate, all checked matrix factorizations, rank/support bounds, polynomial divisions, spectral repairs, and Bluestein convolutions hold identically over $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{F}_p$.*

4 Certified Corpus and Worked Witnesses

We generated and verified 16 canonical certificates (`C01`–`C16`, Table 2). Four representative witnesses are worked out explicitly below for hand verification.

4.1 Worked Hand-Verifiable Arithmetic

Witness `C03` (Theorem 2.2 & Proposition 2.4). For $(L, W, D) = (\frac{3}{4}, 1, \frac{5}{4})$ ($D^2 = \frac{25}{16} = \frac{9}{16} + 1$) and $m = \log_2 N = 16$, the character-table rectangle price is $(L + D)m = 2 \cdot 16 = 32$ vs. permutation price $(L + W)m = \frac{7}{4} \cdot 16 = 28$, giving exact excess $32 - 28 = 4 = \frac{(3/4)^2}{1+5/4} \cdot 16 = \frac{9/16}{9/4} \cdot 16$ (Fig. 1a). For unit vectors $p = (\frac{3}{5}, \frac{4}{5})$ and $r = (1, 0)$, the disk of diameter $[0, p]$ has center $\frac{p}{2} = (\frac{3}{10}, \frac{2}{5})$ and radius $\frac{1}{2}$. Setting $a = b = \frac{p+r}{2} = (\frac{4}{5}, \frac{2}{5})$

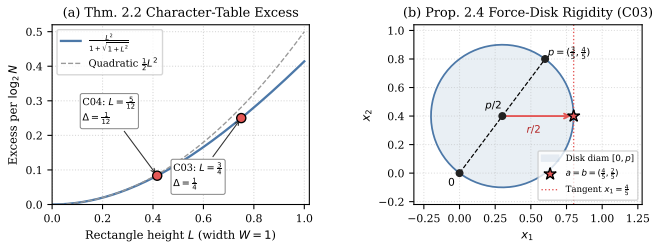

Figure 1: (a) Theorem 2.2 normalized character-table excess $L^2/(1+\sqrt{1+L^2})$ highlighting exact Pythagorean certificates C04 ($L=\frac{5}{12},\Delta=\frac{1}{12}$) and C03 ($L=\frac{3}{4},\Delta=\frac{1}{4}$). (b) Proposition 2.4 force-disk midpoint rigidity in C03: $p=(\frac{3}{5},\frac{4}{5})$, $r=(1,0)$ place $a=b=(\frac{4}{5},\frac{2}{5})$ on the supporting tangent $x_1=\frac{4}{5}$ of the diameter-$[0,p]$ disk.

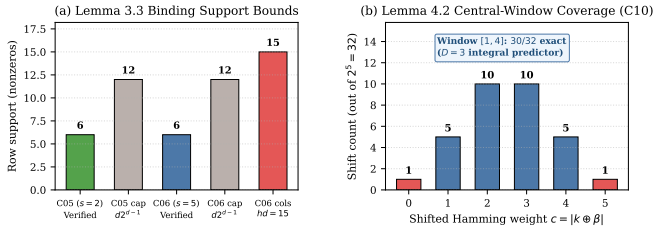

Figure 2: (a) Lemma 3.3 nilpotent time expansion (C05–C06): verified row supports stay strictly within $d2^{d-1}=12$, even in C06 where total columns $hd=15>12$ makes the bound genuinely binding. (b) Lemma 4.2 central-window binomial mass for $m=5$ (C10): window $[1,4]$ captures 30/32 shifts with a degree-3 integral predictor.

gives $a-\frac{p}{2}=(\frac{1}{2},0)=\frac{r}{2}$, hitting the boundary $|a-\frac{p}{2}|^2=\frac{1}{4}$ with supporting tangent $x_1=\frac{4}{5}$ (Fig. 1b).

Witness C05 & C07 (Time Expansion & Row Quotient). In C05 over $\mathbb{F}_7$ ($s=2,h=2,d=3$), $C=\left(\begin{smallmatrix}0&2\\3&0\end{smallmatrix}\right)$ and $A=I_2$ have fan-in 2 and $\det(I-C)=1-6=2\not\equiv 0 \pmod 7$, giving $M=(I-C)^{-1}A=\left(\begin{smallmatrix}4&1\\5&4\end{smallmatrix}\right) \pmod 7$. Expanding on $d=3$ time coordinates produces $R_0^3=0$, $\operatorname{rank}(R-R_0)=1$, $\operatorname{rank}(V_R-V_{R_0})=2\le s$, maximum nilpotent row support $6\le 3\cdot 2^2=12$, and exact diagonal blocks M (Fig. 2a). In C07 over $\mathbb{F}_7$ (3 blocks of size 2, rank-1 $B=\mathbf{1}_6(1,2)$), the upper-triangular bidiagonal Q with rows e_i-e_{i+1} ($0\le i\le 4$) and zero row 5 satisfies $QB=0$ and yields diagonal block ranks $(2,2,1)$ with total deficit $0+0+1=1\le r$.

Witness C11 & C12 (Potter Linearization & Hermite Repair). In C11 over $\mathbb{F}_7$ ($b=3$, primitive cube root $\xi=2$), monomial factors $(2,3,5)$ and $(4,1,6)$ evaluate to $2\cdot3\cdot5+4\cdot1\cdot6=30+24=54\equiv 5 \pmod 7$; the 9×9 pencil $L=S_0\otimes I_3+Z\otimes S_1$ satisfies $VU=2UV$ and $L^3=5I_9$. In C12 over $\mathbb{F}_{11}$ ($\ell=2,W=8,s=2,z=10\equiv-1$, nodes $1,\dots,8$, errors at $J=\{1,6\}$ with $p_1=3,p_6=7$ and $p_i=10$ off J), $g(y)=y-6y(y^2-1)\equiv 5y^3+7y \pmod{11}$ satisfies $g(10)=10$, $g'(10)=0$, and $g(y)-10=(y-10)^2(5y+1) \pmod{11}$ ($D_{10}(y)=5y+1$). Solving the 2×2 Vandermonde system on $2s=4$ spectral check rows recovers e_J and a, and the lifted repair $g(P)\hat{X}-P\hat{Z}+10\hat{Z}$ equals $10\hat{X}$ on all 8 rows (Fig. 3a).

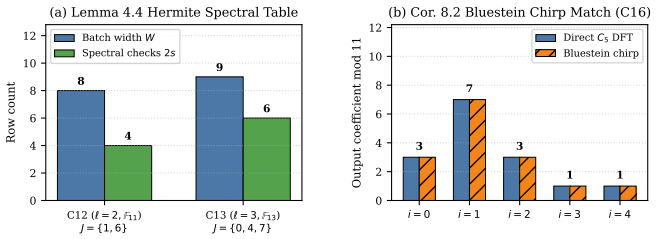

Figure 3: (a) Lemma 4.4 Hermite spectral repair (C12, C13): repairing $W=8,9$ rows using only $2s=4,6$ spectral rows. (b) Corollary 8.2 Bluestein chirp exact agreement with direct C_5 DFT over $\mathbb{F}_{11}$ (C16).

Table 2: Canonical verified certificate corpus (C01–C16).

ID	Mode / Submode	Key Verified Invariant	Status
C01	M1 / swap ($\mathbb{F}_7$)	C_3 2-phase swap; 9 diag weights	PASS
C02	M1 / swap ($\mathbb{F}_5$)	C_4 2-phase swap; 16 diag weights	PASS
C03	M1 / rect+disk	$(3/4,1,5/4)$, exc 4; $a{=}b{=}(\frac{4}{5},\frac{2}{5})$	PASS
C04	M1 / rect+disk	$(5/12,1,13/12)$, exc 3; $a{=}b{=}(0,\frac{12}{13})$	PASS
C05	M2 / time exp.	$s{=}2,d{=}3$ ($\mathbb{F}_7$): rk≤ 2, supp $6\le 12$	PASS
C06	M2 / time exp.	$s{=}5,h{=}5,d{=}3$ ($\mathbb{F}_{11}$): supp $\le 12<15$	PASS
C07	M2 / quotient	$[2,2,2]$, $r{=}1$: diag rks $[2,2,1]$	PASS
C08	M2 / quotient	$[2,3,2]$, $r{=}2$: diag rks $[2,3,0]$	PASS
C09	M3 / predictor	$m{=}3,[1,2],D{=}1$: 6/8 exact	PASS
C10	M3 / predictor	$m{=}5,[1,4],D{=}3$: 30/32 exact	PASS
C11	M3 / Potter	9×9 ($\mathbb{F}_7,b{=}3$): $L^3=5I_9$	PASS
C12	M3 / Hermite	$\ell{=}2,W{=}8$ ($\mathbb{F}_{11}$): 2 errors fixed	PASS
C13	M3 / Hermite	$\ell{=}3,W{=}9$ ($\mathbb{F}_{13}$): 3 errors fixed	PASS
C14	M4 / kernel+Gram	$\ell{=}2$ ($\mathbb{F}_5$), $\{0,1\}^4$: Gram rk 2	PASS
C15	M4 / kernel+Gram	$\ell{=}3$ ($\mathbb{F}_7$), $\{0,1\}^3$: Gram rk 4	PASS
C16	M4 / Bluestein	C_5 ($\mathbb{F}_{11},q{=}4$): DFT $(3,7,3,1,1)$	PASS

Witness C16 (Corollary 8.2 Bluestein Chirp Convolution). Over $\mathbb{F}_{11}$ with $m=5$ and primitive 5-th root $q=4$ ($4^5\equiv 1 \pmod{11}$), the chirp polynomial $H(X)$ of length $2m-1=9$ has coefficients $H_{4+d}=4^{-d(d-1)/2} \pmod{11}=(1,3,5,3,1,1,3,5,3)$. Multiplying $H(X)$ by $Y(X)=\sum_{j=0}^{4}4^{j(j+1)/2}x_jX^j$ for $x=(3,1,4,1,5)$ and scaling $[X^{4+i}]$ by $4^{i(i-1)/2}$ yields $(3,7,3,1,1) \pmod{11}$, matching the direct C_5 DFT identically (Fig. 3b).

5 Verification Gates and Reproducibility

All artifacts pass five independent gates: (1) Lean 4.35.0 compilation with 18 constructive theorems, zero warnings, zero custom axioms, and zero `Classical.choice`; (2) AST zero-float / zero-division check; (3) 16/16 canonical certificates verified; (4) 52 adversarial forgeries and edge-case checks (70/70 `pytest` checks total, covering duplicate keys, oversized and deeply nested JSON, `NaN`/`Infinity` rejection, non-lowest-terms rationals, non-primitive roots, off-midpoint force splits, vacuous zero

feedback/perturbation/Potter/Hermite inputs, singular feedback systems, fan-in > 2, non-upper-triangular quotients, vacuous windows, non-root-of-unity Hermite targets, unlisted errors outside J, non-power-of-two alphabets, spoofed Gram ranks, CLI exit codes, and mismatched Bluestein DFTs); and (5) complete SHA-256 manifest (`MANIFEST.sha256`).

AI Assistance Disclosure. This work was produced by Lluis Eriksson using Google Antigravity for Lean 4 theorem drafting, Python exact-verifier engineering, test generation, and LaTeX preparation; all mathematical claims, code, proofs, and verification logs were independently compiled, tested, and reviewed by the author.

Licensing. Manuscript and figures are released under `CC-BY-4.0`; Lean 4 proofs, Python code, and JSON certificates are released under the `MIT` License.

References

[1] Josh Alman and Kevin Rao. Faster Walsh–Hadamard and discrete Fourier transforms from matrix non-rigidity. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*, pages 455–462, 2023.

[2] L. I. Bluestein. A linear filtering approach to the computation of discrete Fourier transform. *IEEE Transactions on Audio and Electroacoustics*, 18(4):451–455, 1970.

[3] James W. Cooley and John W. Tukey. An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*, 19(90):297–301, 1965.

[4] Jacques Morgenstern. Note on a lower bound on the linear complexity of the fast Fourier transform. *Journal of the ACM*, 20(2):305–306, 1973.

[5] OpenAI. Euclidean geometry in the asymptotic spectrum of tensors. OpenAI Math Release preprint `OAI:Euclidean-geometry-in-the-asymptotic-spectrum-of-tensors-November-24-2026`, November 2026. Unrefereed preprint, November 24, 2026.

[6] OpenAI. The logarithmic exponent of finite fourier transforms. OpenAI Math Release preprint `OAI:The-logarithmic-exponent-of-finite-Fourier-transforms-November-24-2026`, November 2026. Unrefereed preprint, November 24, 2026.

[7] H. S. A. Potter. On the latent roots of quasi-commutative matrices. *American Mathematical Monthly*, 57(5):321–322, 1950.

[8] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.