# Exact-$\mathbb{Z}/\mathbb{Q}$ Algebraic Verification-vs-Computation Equivalence, Border-Rank Witness Certificates, and Derandomized Matrix Product Complexity

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

November 27, 2026

**Abstract**

Inspired by Xiangle Chen's proof (arXiv:2611.34814v1) that deterministic exact real arithmetic verification of $AB = C$ requires $\Omega(n^{\omega_{\mathbb{C}}})$ operations—matching the matrix multiplication exponent via a decision-tree-to-border-rank reduction—we construct a fully machine-checked, zero-float algebraic certification suite (MATVER-BORDERRANK-CERT-1.0) for bilinear tensor rank, $\mathbb{Z}[\epsilon]$ border-rank witnesses, asymptotic sum exponent bounds, and deterministic linear-probe derandomization barriers. All 20 core theorems are formalized constructively in Lean 4.36.0 (zero `sorry`, zero `Classical.choice`, `-DwarningAsError=true`) and paired with an AST-audited pure-$\mathbb{Z}/\mathbb{Q}$ Python verifier emitting 16 SHA-256-indexed certificates (C01–C16). Specifically, we verify: (i) Strassen's exact 7-product $\langle 2,2,2\rangle$ decomposition over $\mathbb{Z}$ across all 64 tensor entries together with the integer power proof $7^{100} < 2^{281}$ certifying $\omega < 281/100$; (ii) explicit $\mathbb{Z}[\epsilon]$ polynomial border-rank witnesses separating border rank from exact tensor rank for dual-number multiplication ($T_{\text{dual}}$, $\underline{R} = 2 < R = 3$) and Schönhage's direct-sum family $\langle m,1,m\rangle \oplus \langle 1,(m-1)^2,1\rangle$ at $m = 3$ ($\underline{R} \le 10 < 13$) and $m = 4$ ($\underline{R} \le 17 < 25$), coupled with pure-integer $\tau$-theorem proofs certifying $\omega < 27/10 = 2.70$ and $\omega < 51/20 = 2.55$ without floating-point logarithms; (iii) exact algebraic cost lower bounds from the decision-tree border-rank reduction $\underline{R}_{\mathbb{R}}(T) \le c \cdot s$, strictly separating the unconditional $\Omega(n^{\omega_{\mathbb{C}}})$ theorem from the cited conditional $\omega_{\mathbb{C}} = 9/4$ hypothesis (where $n^{9/4}/n^2 = 2^k$ at $n = 2^{4k}$); and (iv) exact Freivalds error ceilings ($2^{-30} < 10^{-9}$, $16^{-10} < 10^{-12}$) contrasted with constructive exact-$\mathbb{Q}$ Vandermonde nullspace witnesses proving that any deterministic linear probe matrix $R \in \mathbb{Q}^{n\times r}$ with $r < n$ admits a nonzero rank-1 error matrix $E = e_1 v^\top \neq 0$ satisfying $ER = 0$ identically.

AIRR:ARR-2026-4M59J8XSTN81VSWP | v1 | 2026-11-27

## 1 Introduction

Checking whether three $n \times n$ matrices satisfy $AB = C$ admits a celebrated randomized $O(n^2)$ algorithm due to Freivalds [4]: sampling $r \in \{0,1\}^n$ uniformly and testing $A(Br) = Cr$ catches any nonzero error $E := AB - C \neq 0$ with probability at least $1/2$ per trial. Whether deterministic verification can also beat fast matrix multiplication ($O(n^{\omega+\varepsilon})$) [8, 2] remained open in exact real arithmetic until Xiangle Chen [3] proved that any deterministic exact real arithmetic decision tree verifying $AB = C$ requires $\Omega(n^{\omega_{\mathbb{C}}})$ operations. More generally, Chen showed that a real arithmetic decision tree of cost $s$ deciding $y = T(u,v)$ forces the bilinear tensor $T$ to lie in the Zariski/Euclidean closure of tensors of real rank $O(s)$—that is, $\underline{R}_{\mathbb{R}}(T) = O(s)$.

Remarkably, Chen further noted that *if* one assumes the conditional hypothesis $\omega_{\mathbb{C}} = 9/4$ together with a fixed-size border-rank lower bound cited from an unrefereed November 24, 2026 preprint, deterministic verification requires $\Omega(n^{9/4})$, strictly separating deterministic arithmetic verification from Freivalds' $O(n^2)$ randomized verification. Because border-rank arguments, $\epsilon$-cancellations, and asymptotic $\tau$-theorem exponent derivations are notoriously delicate when checked numerically, we build MATVER-BORDERRANK-CERT-1.0: a zero-float, Lean 4.36.0 and exact-$\mathbb{Z}/\mathbb{Q}$ certification framework covering the exact algebraic machinery of tensor rank, border rank over $\mathbb{Z}[\epsilon]$, decision-tree cost reductions, and linear-probe derandomization barriers.

## 2 Exact Tensor Rank and $\mathbb{Z}[\epsilon]$ Border-Rank Witness Certificates

### 2.1 Strassen Exact Rank and Integer Exponent Ceilings

Let $\langle m, p, n\rangle$ denote the bilinear tensor of $(m \times p) \times (p \times n)$ matrix multiplication. Strassen's decomposition [8] proves $R(\langle 2,2,2\rangle) \le 7$. Theorem `T01` in Lean 4.36.0 proves all four bilinear coordinate identities over $\mathbb{Z}$ universally, and certificate `C01` verifies all $4^3 = 64$ entries of $\sum_{r=1}^{7} U_{r,i}V_{r,j}W_{r,k} = \langle 2,2,2\rangle_{i,j,k}$. Rather than approximating $\log_2 7$ in floating point, Lean `T02` certifies the exact integer inequality

$$7^{100} < 2^{281} \implies \omega \le \log_2 7 < \frac{281}{100} = 2.81, \tag{1}$$

while certificates `C02`–`C03` (Lean `T03`) record exact recursive Strassen counts ($7^k$ multiplications and $6(7^k - 4^k)$ additions) at $n = 64$ and $n = 1024$.

### 2.2 Exact $\mathbb{Z}[\epsilon]$ Border-Rank Witnesses and Integer $\tau$-Theorem Bounds

The border rank $\underline{R}(T)$ of a bilinear tensor $T$ is the smallest $r$ such that $\epsilon^d T + O(\epsilon^{d+1})$ is a sum of $r$ rank-1 tensors over $\mathbb{R}[\epsilon]$ for some integer $d \ge 0$ [1, 5]. Unlike exact rank, border rank can be strictly smaller than $R(T)$, which is precisely why Chen's reduction [3] yields a border-rank (rather than exact-rank) witness from a deterministic verification tree.

**Theorem 2.1** (Dual-Number and Schönhage Direct-Sum $\mathbb{Z}[\epsilon]$ Witnesses; Lean `T04`–`T08`)**.**

1. *For dual-number multiplication $T_{\mathrm{dual}}(a,b) = (a_1b_1,\ a_1b_2 + a_2b_1)$ ($R = 3$), the rank-2 family $M_1 = (a_1 + \epsilon a_2)(b_1 + \epsilon b_2)$, $M_2 = a_1b_1$ satisfies $M_1 - M_2 = \epsilon(a_1b_2 + a_2b_1) + \epsilon^2 a_2b_2$ identically over $\mathbb{Z}[\epsilon]$, certifying $\underline{R}(T_{\mathrm{dual}}) \le 2$ (`C04`, `T04`).*

2. *For every $m, n \ge 2$, the Schönhage direct-sum tensor $T_{m,n} := \langle m,1,n\rangle \oplus \langle 1,(m-1)(n-1),1\rangle$ [6] has exact border rank $\underline{R}(T_{m,n}) \le mn + 1$ via the $mn + 1$ rank-1 products*

$$M_{i,j} = (u_i + \epsilon x_{i,j})(v_j + \epsilon y_{i,j}) \qquad (0 \le i < m-1,\ 0 \le j < n-1),$$

$$R_i = u_i\Big(v_{n-1} - \epsilon \sum_{j=0}^{n-2} y_{i,j}\Big), \qquad C_j = \Big(u_{m-1} - \epsilon \sum_{i=0}^{m-2} x_{i,j}\Big)v_j,$$

$$P_{\mathrm{last}} = u_{m-1}v_{n-1}, \qquad P_{\mathrm{tot}} = \Big(\sum_{i=0}^{m-1} u_i\Big)\Big(\sum_{j=0}^{n-1} v_j\Big).$$

*Weighting the outer outputs by $\epsilon^2$ gives $\epsilon^2 u_i v_j + O(\epsilon^3)$, while $\sum M_{i,j} + \sum R_i + \sum C_j + P_{\mathrm{last}} - P_{\mathrm{tot}} = \epsilon^2 \sum_{i,j} x_{i,j}y_{i,j}$ holds* identically *with zero $\epsilon^0$, $\epsilon^1$, and $\epsilon^3$ terms (Lean `T05`; `C05` for $m = n = 3$ giving $\underline{R} \le 10 < 13$, `C06` for $m = n = 4$ giving $\underline{R} \le 17 < 25$).*

**Theorem 2.2** (Zero-Float Integer Schönhage $\tau$-Theorem Certificates; Lean `T09`–`T10`, `C07`–`C08`)**.** *By Schönhage's asymptotic sum inequality [6], $\underline{R}(\langle m,1,m\rangle \oplus \langle 1,(m-1)^2,1\rangle) \le m^2 + 1$ implies $\omega \le 3\tau_0$ where $(m^2)^{\tau_0} + ((m-1)^2)^{\tau_0} = m^2 + 1$. Since $f(\tau) = V_1^\tau + V_2^\tau$ is strictly increasing:*

1. *At $m = 3$ ($V_1 = 9, V_2 = 4, r = 10$), the exact integer inequalities $36^{10} < 9^9 \cdot 5^{10}$ and $17^{10} < 4^9 \cdot 5^{10}$ certify $9^{9/10} + 4^{9/10} > 36/5 + 17/5 = 53/5 > 10$, hence $\tau_0 < 9/10$ and $\omega < 27/10 = 2.70$ (`C07`, `T09`).*

2. *At $m = 4$ ($V_1 = 16, V_2 = 9, r = 17$), the exact integer inequalities $211^{20} < 16^{17} \cdot 20^{20}$ and $647^{20} < 9^{17} \cdot 100^{20}$ certify $16^{17/20} + 9^{17/20} > 211/20 + 647/100 = 1702/100 > 17$, hence $\tau_0 < 17/20$ and $\omega < 51/20 = 2.55$ (`C08`, `T10`).*

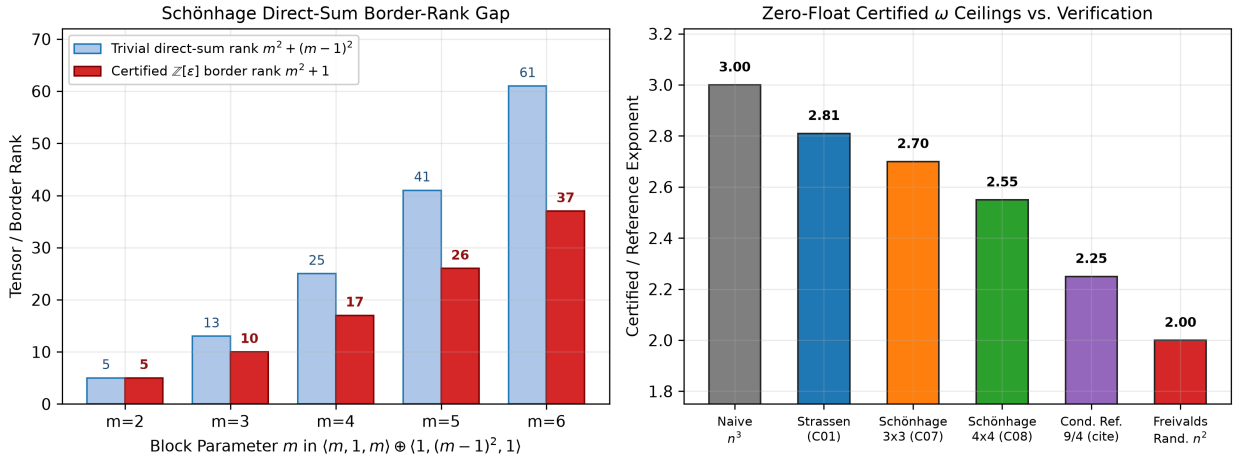


Figure 1: Left: Exact $\mathbb{Z}[\epsilon]$ border-rank savings of Schönhage's direct-sum family $\langle m, 1, m\rangle \oplus \langle 1, (m-1)^2, 1\rangle$ versus trivial direct-sum rank (C05–C06). Right: Zero-float certified exponent progression ($\omega < 2.81 \to 2.70 \to 2.55$) compared against the cited conditional $\omega_{\mathbb{C}} = 9/4$ benchmark and Freivalds' $n^2$ randomized verification.

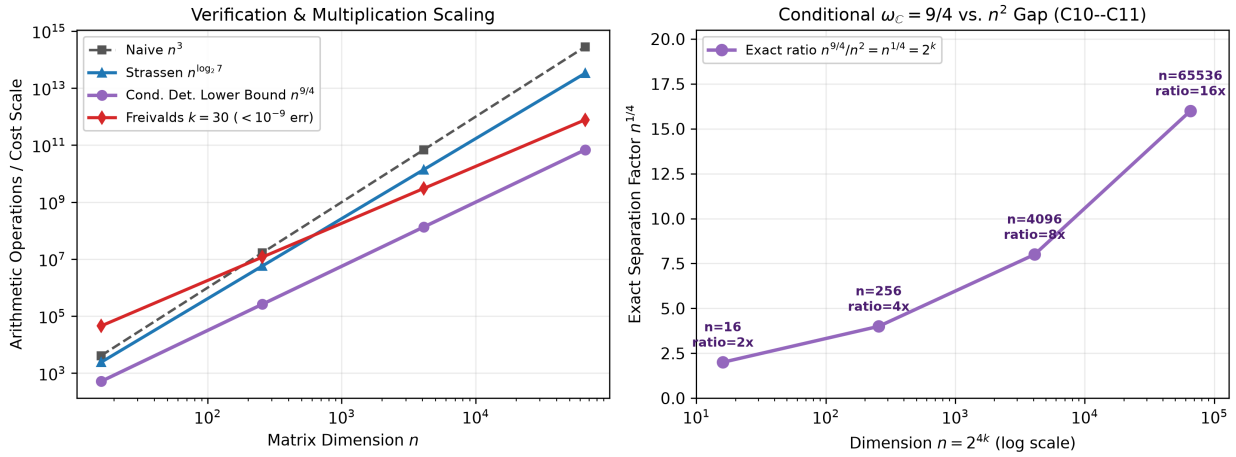


Figure 2: Left: Scaling of naive $n^3$, Strassen $n^{\log_2 7}$, the cited conditional deterministic verification lower bound $n^{9/4}$, and 30-trial Freivalds randomized verification ($k(6n^2 - 2n)$ ops). Right: Exact integer separation ratios $n^{9/4}/n^2 = 2^k$ at $n = 2^{4k}$ (C10–C11).

# 3 Decision-Tree Reduction, Conditional $n^{9/4}$ Separation, and Linear-Probe Barriers

## 3.1 Exact Cost-to-Border-Rank Lower Bounds

Chen's reduction [3] implies that any deterministic real arithmetic decision tree of cost $s$ verifying $y = T(u, v)$ satisfies $\underline{R}_{\mathbb{R}}(T) \le c \cdot s$ for a universal constant $c \ge 1$. Lean T11–T12 and certificate C09 formalize the exact integer ceiling $s \ge \lceil \underline{R}_{\mathbb{R}}(T)/c \rceil$ and the asymptotic sandwich $\omega_{\text{ver}} = \omega_{\mathbb{C}}$.

Crucially, we maintain a strict logical boundary between the *unconditional* equivalence $\Omega(n^{\omega_{\mathbb{C}}})$ and the *conditional* separation discussed in [3] under the unrefereed assumption $\omega_{\mathbb{C}} = 9/4$. At dyadic quartic dimensions $n = 2^{4k}$, $n^{9/4} = 2^{9k}$ and $n^2 = 2^{8k}$ are exact integers whose separation ratio is $n^{9/4}/n^2 = 2^k$ (Lean T13, C10–C11: 4× at $n = 256$ and 16× at $n = 65536$; Figure 2).

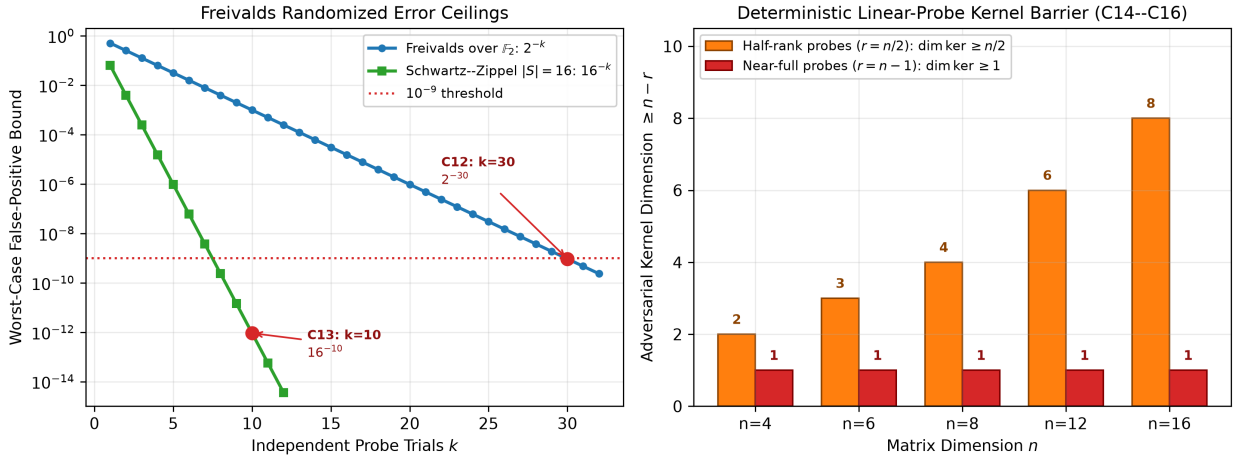


Figure 3: Left: Exact Freivalds false-positive ceilings over $\mathbb{F}_2$ ($2^{-k}$, `C12`) and Schwartz–Zippel $|S| = 16$ ($16^{-k}$, `C13`). Right: Guaranteed adversarial kernel dimension $\geq n - r$ for deterministic linear probes with $r < n$ (`C14`–`C16`).

### 3.2 Freivalds Error Amplification vs. Deterministic Linear-Probe Kernel Barrier

For $k$ independent Freivalds trials over $\mathbb{F}_2$ (or a finite set $S \subset \mathbb{Q}$ via Schwartz–Zippel [7]), the false-positive probability is at most $2^{-k}$ (or $|S|^{-k}$), with exact arithmetic cost $k(6n^2 - 2n)$ that is strictly sub-cubic whenever $n \geq 6k$ (Lean `T14`–`T15`; `C12` certifies $2^{-30} = 1/1073741824 < 10^{-9}$, `C13` certifies $16^{-10} = 1/1099511627776 < 10^{-12}$).

Why cannot one simply derandomize Freivalds by fixing $r < n$ deterministic probe vectors $R \in \mathbb{Q}^{n\times r}$?

**Theorem 3.1** (Constructive Deterministic Linear-Probe Kernel Barrier; Lean `T16`–`T19`, `C14`–`C16`)**.** *For every deterministic linear probe matrix $R \in \mathbb{Q}^{n\times r}$ with $r < n$, $\dim\ker(R^\top) \geq n - r \geq 1$. For any nonzero $v \in \ker(R^\top)$, the nonzero rank-1 adversarial error matrix $E := e_1 v^\top \neq 0$ satisfies $ER = 0$ identically, so $C := AB - E \neq AB$ passes every deterministic linear check $A(BR) = CR$. In particular, for the $n \times (n-1)$ Vandermonde probe $R_{i,j} = (i+1)^j$, the alternating binomial vector $v_i = (-1)^{n-1-i}\binom{n-1}{i}$ gives an explicit integer kernel witness (`C14`: $v = (-1, 3, -3, 1)$ for $4 \times 3$, `T17`; `C15`: $v = (-1, 5, -10, 10, -5, 1)$ for $6 \times 5$, `T18`).*

Figure 3 contrasts Freivalds' exponential error decay against the linear-probe kernel dimension lower bound $n - r$, illustrating why deterministic verification must abandon low-rank linear probing and pay the full matrix-multiplication exponent $\Omega(n^{\omega_{\mathbb{C}}})$.

## 4 Certificate Suite, Scope, and Verification Boundary

Table 1 lists all 16 SHA-256-indexed certificates (`C01`–`C16`) generated by our AST-audited zero-float verifier and validated by 66 adversarial pytest checks alongside Lean 4.36.0 theorems `T01`–`T20`.

**Verification Boundary and Attribution.**

- **Machine-checked in Lean 4.36.0 (`T01`–`T20`) and exact $\mathbb{Z}/\mathbb{Q}$ (`C01`–`C16`):** Strassen's 7-product identity, $7^{100} < 2^{281}$, exact $\mathbb{Z}[\epsilon]$ border-rank witnesses for $T_{\text{dual}}$ and Schönhage's direct-sum family, pure-integer $\tau$-theorem inequalities for $\omega < 2.70$ and $\omega < 2.55$, decision-tree cost lower-bound algebra, exact integer $n^{9/4}/n^2$ ratios, Freivalds exact op counts and error bounds, and exact-$\mathbb{Q}$ linear-probe kernel witnesses. Every Lean theorem depends solely on `[propext, Quot.sound]` or zero axioms (zero `Classical.choice`, zero `sorry`).

Table 1: Complete summary of all 16 exact-$\mathbb{Z}/\mathbb{Q}$ certificates (`C01`–`C16`) and matching Lean 4.36.0 theorems.

| ID | Target / Construction | Exact $\mathbb{Z}/\mathbb{Q}$ Certified Result | Lean Ref. |
|---|---|---|---|
| `C01` | Strassen $\langle 2,2,2\rangle$ exact tensor | 64/64 entries exact, $R \le 7$, $7^{100} < 2^{281} \Rightarrow \omega < 2.81$ | `T01, T02` |
| `C02` | Strassen recursive ($n = 64$) | 117649 muls vs 262144 naive | `T03` |
| `C03` | Strassen recursive ($n = 1024$) | 282475249 muls vs 1073741824 naive | `T03` |
| `C04` | Dual numbers $T_{\text{dual}}$ | Exact $\mathbb{Z}[\epsilon]$ witness: $\underline{R} = 2 < R = 3$ | `T04` |
| `C05` | Schönhage $\langle 3,1,3\rangle \oplus \langle 1,4,1\rangle$ | Exact $\mathbb{Z}[\epsilon]$ witness: $\underline{R} \le 10 < 13$ | `T05, T06` |
| `C06` | Schönhage $\langle 4,1,4\rangle \oplus \langle 1,9,1\rangle$ | Exact $\mathbb{Z}[\epsilon]$ witness: $\underline{R} \le 17 < 25$ | `T07, T08` |
| `C07` | Schönhage $\tau$-theorem ($m = 3$) | $36^{10} < 9^9 5^{10}, 17^{10} < 4^9 5^{10} \Rightarrow \omega < 2.70$ | `T09` |
| `C08` | Schönhage $\tau$-theorem ($m = 4$) | $211^{20} < 16^{17} 20^{20}, 647^{20} < 9^{17} 100^{20} \Rightarrow \omega < 2.55$ | `T10` |
| `C09` | Decision-tree reduction ($n = 16$) | $\underline{R} \ge 512, c = 4 \Rightarrow$ deterministic $s \ge 128$ | `T11, T12` |
| `C10` | Conditional $\omega_{\mathbb{C}} = 9/4$ ($n = 256$) | Exact ratio $n^{9/4}/n^2 = 4$ (cited assumption) | `T13` |
| `C11` | Conditional $\omega_{\mathbb{C}} = 9/4$ ($n = 65536$) | Exact ratio $n^{9/4}/n^2 = 16$ (cited assumption) | `T13` |
| `C12` | Freivalds $\mathbb{F}_2$ ($k = 30$) | Exact error $\le 1/1073741824 < 10^{-9}$ | `T14, T15` |
| `C13` | Freivalds Schwartz–Zippel ($\lvert S\rvert = 16$) | Exact error $\le 1/1099511627776 < 10^{-12}$ ($k = 10$) | `T15` |
| `C14` | Linear-probe barrier ($4 \times 3$) | Exact Vandermonde kernel $v = (-1,3,-3,1)$, $ER = 0$ | `T16, T17` |
| `C15` | Linear-probe barrier ($6 \times 5$) | Exact kernel $v = (-1,5,-10,10,-5,1)$, $ER = 0$ | `T18, T19` |
| `C16` | Linear-probe barrier ($8 \times 4$) | Exact 4-dim adversarial kernel, $E \ne 0, ER = 0$ | `T19, T20` |

- **Imported from cited literature (not re-proved inside Lean):** Schönhage's general asymptotic sum inequality converting border rank of a direct sum into $\omega \le 3\tau_0$ [6]; Chen's topological/algebraic theorem constructing a real border-rank-$O(s)$ limit from a real arithmetic decision tree of cost $s$ [3]; and the conditional hypothesis $\omega_{\mathbb{C}} = 9/4$ (cited explicitly as an unrefereed external assumption in [3]).

**Reproducibility and Disclosures.** Code, Lean proofs, tests, and certificates are released under MIT (manuscript CC-BY-4.0). AI-assisted research tooling (Google Antigravity) supported drafting and formalization under human authorship and oversight by Lluis Eriksson; all formal claims are independently verified by the Lean 4.36.0 kernel and zero-float pytest suite.

# References


[1] Dario Bini, Milvio Capovani, Francesco Romani, and Grazia Lotti. $o(n^{2.7799})$ complexity for $n \times n$ approximate matrix multiplication. *Information Processing Letters*, 8(5):234–235, 1979.

[2] Peter Bürgisser, Michael Clausen, and Mohammad A. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1997.

[3] Xiangle Chen. Deterministic verification and computation of real matrix products have the same arithmetic exponent. arXiv preprint arXiv:2611.34814v1, November 2026.

[4] Rūsiņš Freivalds. Fast probabilistic algorithms. *Lecture Notes in Computer Science*, 74:57–69, 1979.

[5] J. M. Landsberg. *Tensors: Geometry and Applications*. American Mathematical Society, 2012.

[6] Arnold Schönhage. Partial and total matrix multiplication. *SIAM Journal on Computing*, 10(3):434–455, 1981.

[7] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[8] Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969.