Exact-$\mathbb{Z}/\mathbb{Q}$ Pairwise-Coprime CRT Multiplication, Walsh–Hadamard Transposition, and Unpaid-Entropy Tape-Barrier Certificates

Lluis Eriksson*

November 2026

Abstract

On November 24, 2026, OpenAI (`openai/math`) resolved the exact logarithmic exponent of n-bit integer multiplication on multitape Turing machines, proving matching $\Theta(n\sqrt{\log n})$ upper and lower bounds by combining pairwise-coprime Chinese Remainder Theorem (CRT) cyclic-factor convolution and Walsh–Hadamard spectral steps with a tape-epoch unpaid-entropy transposition barrier governed by the critical paid-wire density $\rho < 1 - 1/\sqrt{2}$ (Theorem 8.1). Here we formalize and operationalize the core algebraic, reduction, spectral-transposition, and cleared-integer entropy-barrier laws in an 18-theorem zero-dependency Lean 4 kernel (`v4.35.0`, 0 `sorry`, 0 `Classical.choice`, 0 warnings) paired with a pure-stdlib zero-float verifier (`TAPE-MUL-CERT-1.0`). First, we machine-check exact unsigned product bit-length bounds, Euclidean division and integer square-root uniqueness, 3-square and 4-product polarization identities, cleared-integer Newton–Raphson reciprocal quadratic error squaring, and Newton integer-$\sqrt{N}$ monotonicity (Lean 4 Theorems 1–7). Second, we prove exact 2- and 4-point Walsh–Hadamard involution and Parseval energy conservation, pairwise-coprime Bézout CRT uniqueness and modular reconstruction, and exact $N \times N$ row-major matrix transposition involution (Lean 4 Theorems 8–14). Third, we formalize the exact cleared-integer unpaid-entropy density condition $2(q-p)^2 > q^2 \implies 10p < 3q$ (strictly certifying $\rho = p/q < 3/10$ from the quadratic threshold alone), inductive list-epoch unpaid-demand accumulation, logarithmic-exponent-1/2 separation $n < ns < ns^2$, and the epoch-vertex-to-step bound $T \geq (2k-1)N^2$ (Lean 4 Theorems 15–18). Our pure-stdlib verifier replays 16/16 exact-$\mathbb{Z}/\mathbb{Q}$ certificates across all four modes in 0.024–0.875 ms (scaling to 2048-bit CRT products with 4188-bit modulus capacity in 0.604 ms), cross-checks all engines against independent reference definitions, and rejects 54/54 live adversarial attacks in 0.04 s.

1 Introduction

For over half a century, the multitape Turing-machine complexity of n-bit integer multiplication was bracketed between Schönhage–Strassen's $O(n \log n \log\log n)$ [5] and Harvey–van der Hoeven's $O(n \log n)$ [2] upper bounds, alongside conditional network-coding lower bounds [1] and classical arithmetic reductions to squaring, division, and integer square roots [3]. On November 24, 2026, OpenAI [4] settled the exact logarithmic exponent on tapes at 1/2: both integer multiplication and $N \times N$ bit-matrix transposition ($n = N^2$) take $\Theta(n\sqrt{\log n})$ steps on multitape Turing machines.

Four elementary exact-$\mathbb{Z}/\mathbb{Q}$ algebraic mechanisms underpin both sides of [4]: (i) pairwise-coprime CRT decomposition of big-integer convolution products, (ii) exact arithmetic reductions (polarization $2ab = (a+b)^2 - a^2 - b^2$, Euclidean division, Newton–Raphson reciprocal squaring, and exact integer square roots), (iii) dyadic Walsh–Hadamard Parseval transforms paired with $N \times N$ row-major bit-matrix transposition involutions, and (iv) OpenAI Theorem 8.1's unpaid-entropy demand/supply barrier at critical density $\rho^* = 1 - 1/\sqrt{2} \approx 0.292893$, converting epoch-level vertex counts $V \geq 2Nk$

*Independent researcher (Sweden). Manuscript licensed under CC-BY-4.0. Prepared with AI-assisted formal verification, code generation, and mathematical drafting (Google Antigravity). Code, zero-dependency Lean 4 proofs, and exact-$\mathbb{Z}/\mathbb{Q}$ certificates (MIT license): `https://github.com/lluiseriksson/tape-multiplication-certificates`.

into superlinear step lower bounds $T \geq (2k-1)N^2$. We mechanize all four algebraic pillars in zero-dependency Lean 4 (`lean/TapeMultiplication.lean`) and build a pure-stdlib zero-float verifier (`TAPE-MUL-CERT-1.0`, `src/tape_mul_certifier.py`) auditing explicit finite witnesses across all four modes.

2 Main Exact-$\mathbb{Z}/\mathbb{Q}$ Theorems

2.1 Arithmetic Reductions: Polarization, Euclidean Division, and Newton Iteration

Theorem 2.1 (Exact Arithmetic Reductions and Cleared-Integer Newton Convergence)**.** *For arbitrary integers $a, b, S, d, x, s, r, N \in \mathbb{Z}$ and natural numbers $q_1, r_1, q_2, r_2, s_1, s_2 \in \mathbb{N}$:*

1. ***Bit-Length, Division, and Square-Root Uniqueness:*** *If $a, b < 2^n$ then $ab < 2^{2n}$; if $q_1 d + r_1 = q_2 d + r_2$ with $r_1, r_2 < d$ then $(q_1, r_1) = (q_2, r_2)$; and if $s_i^2 \leq N < (s_i+1)^2$ for $i \in \{1, 2\}$ then $s_1 = s_2$ (Lean 4 Theorems 1–3).*
2. ***Exact Squaring Polarization:*** *Both $2ab = (a+b)^2 - a^2 - b^2$ and $4ab = (a+b)^2 - (a-b)^2$ hold identically over $\mathbb{Z}$ (Lean 4 Theorems 4–5).*
3. ***Cleared-Integer Newton Reciprocal & Square-Root Monotonicity:*** *Setting $e = S - dx$ and $x' = x(2S - dx)$ satisfies the exact quadratic residual identity $S^2 - dx' = e^2$ over $\mathbb{Z}$; furthermore, whenever $r^2 \leq N$, $s^2 + N - 2sr = (s-r)^2 + (N - r^2) \geq 0$ (Lean 4 Theorems 6–7).*

Proof. Uniqueness of (q, r) follows because $q_1 < q_2$ forces $q_2 d + r_2 \geq (q_1+1)d > q_1 d + r_1$, and $s_1 < s_2$ forces $(s_1+1)^2 \leq s_2^2 \leq N < (s_1+1)^2$. Polarization and $S^2 - dx(2S - dx) = (S - dx)^2$ expand directly in $\mathbb{Z}$. Finally, $(s-r)^2 \geq 0$ and $N - r^2 \geq 0$ imply $s^2 + N \geq 2sr$, guaranteeing that integer Newton updates $\lfloor (s + \lfloor N/s \rfloor)/2 \rfloor$ never undershoot $\lfloor \sqrt{N} \rfloor$. □

2.2 Walsh–Hadamard Parseval Conservation, Pairwise-Coprime CRT, and Transposition

Theorem 2.2 (Spectral Conservation, Bézout CRT Reconstruction, and Transposition Involution)**.**

1. ***Walsh–Hadamard Involution and Parseval Energy:*** *Over $\mathbb{Z}$, the 2-point butterfly $W_2(x, y) = (x+y,\ x-y)$ satisfies $W_2(W_2(x, y)) = (2x,\ 2y)$ and energy conservation $\|W_2(x, y)\|_2^2 = 2(x^2 + y^2)$. Iterating two stages yields exact 4-point Parseval energy $\|W_4 x\|_2^2 = 4\|x\|_2^2$ (Lean 4 Theorems 8–10).*
2. ***Pairwise-Coprime Bézout CRT Soundness:*** *If $um_1 + vm_2 = 1$, then any d divisible by both m_1 and m_2 satisfies $d = (uk_2 + vk_1)(m_1 m_2)$, and the explicit reconstructor $X = r_1 vm_2 + r_2 um_1$ satisfies $X - r_1 = (r_2 - r_1)um_1$ and $X - r_2 = (r_1 - r_2)vm_2$ identically over $\mathbb{Z}$ (Lean 4 Theorems 11–13).*
3. ***Row-Major Matrix Transposition Involution:*** *For any $N \geq 1$ and $0 \leq i, j < N$, mapping $\text{idx} = iN + j \mapsto \text{tr} = (\text{idx} \bmod N)N + \lfloor \text{idx}/N \rfloor$ satisfies $\text{tr} \bmod N = i$ and $\lfloor \text{tr}/N \rfloor = j$ (Lean 4 Theorem 14).*

2.3 Unpaid-Entropy Threshold and Tape-Epoch Lower Bound

Theorem 2.3 (Cleared-Integer Unpaid-Entropy Barrier and Logarithmic Exponent 1/2)**.**

1. ***Sharp Density Threshold (OpenAI Theorem 8.1):*** *For any $p, q \in \mathbb{Z}$ with $p < q$, the exact cleared-integer unpaid-demand condition $2(q-p)^2 > q^2$ (for $q > 0$, equivalently $\rho = p/q < 1 - 1/\sqrt{2} \approx 0.292893$) algebraically implies $10p < 3q$, strictly certifying $\rho < 3/10$ without square roots or floats (Lean 4 Theorem 15).*

Table 1: Zero-dependency Lean 4 theorem ledger (`lean/TapeMultiplication.lean`, `v4.35.0`: 18/18 theorems, 0 `sorry`, 0 `Classical.choice`, 0 warnings).

#	Lean 4 Theorem Identifier	Exact Integer/List Statement Verified	Axioms
1	`mul_bit_length_bound`	$a < 2^n \wedge b < 2^n \implies ab < 2^{2n}$	`propext, Quot.sound`
2	`div_mod_unique_quotient`	$q_1 d + r_1 = q_2 d + r_2 \wedge r_1, r_2 < d \implies q_1 = q_2 \wedge r_1 = r_2$	`propext, Quot.sound`
3	`isqrt_unique`	$s_1^2 \le N < (s_1+1)^2 \wedge s_2^2 \le N < (s_2+1)^2 \implies s_1 = s_2$	`propext, Quot.sound`
4	`product_from_three_squares`	$(a+b)^2 - a^2 - b^2 = 2ab$ over $\mathbb{Z}$	`propext, Quot.sound`
5	`product_from_diff_squares`	$(a+b)^2 - (a-b)^2 = 4ab$ over $\mathbb{Z}$	`propext, Quot.sound`
6	`newton_div_quadratic_error`	$S^2 - d \cdot x(2S - dx) = (S - dx)^2$ over $\mathbb{Z}$	`propext, Quot.sound`
7	`newton_isqrt_monotone_step`	$r^2 \le N \implies s^2 + N - 2sr \ge 0$ over $\mathbb{Z}$	`propext, Quot.sound`
8	`walsh2_involution`	$W_2(W_2(x,y)) = (2x, 2y)$ over $\mathbb{Z}$	`propext, Quot.sound`
9	`walsh2_parseval_energy`	$(x+y)^2 + (x-y)^2 = 2(x^2+y^2)$ over $\mathbb{Z}$	`propext, Quot.sound`
10	`walsh4_parseval_energy`	2-stage 4-point Parseval: $\|W_4 x\|_2^2 = 4\|x\|_2^2$	`propext, Quot.sound`
11	`crt_uniqueness_coprime`	$um_1 + vm_2 = 1 \wedge m_1 \mid d \wedge m_2 \mid d \implies m_1 m_2 \mid d$	`propext`
12	`crt_reconstruct_mod_m1`	$(r_1 vm_2 + r_2 um_1) - r_1 = (r_2 - r_1) um_1$	`propext, Quot.sound`
13	`crt_reconstruct_mod_m2`	$(r_1 vm_2 + r_2 um_1) - r_2 = (r_1 - r_2) vm_2$	`propext, Quot.sound`
14	`transpose_index_involution`	Row-major $N \times N$ transpose: $\mathrm{tr} \bmod N = i \wedge \lfloor \mathrm{tr}/N \rfloor = j$	`propext, Quot.sound`
15	`unpaid_entropy_threshold`	$p < q \wedge 2(q-p)^2 > q^2 \implies 10p < 3q$ ($\rho < 3/10$)	`propext, Quot.sound`
16	`entropy_demand_exceeds_supply`	Inductive `List Int`: $d_i \ge s_i + g \implies \sum d_i \ge \sum s_i + Kg$	`propext, Quot.sound`
17	`sqrt_log_beats_linear_and_log`	$n \ge 1 \wedge s \ge 2 \implies n < ns \wedge ns < ns^2$	`propext, Quot.sound`
18	`tape_epoch_vertex_lower_bound`	$V \ge 2Nk \wedge k \ge 1 \wedge T + N^2 \ge VN \implies T \ge (2k-1)N^2$	`propext, Quot.sound`

2. ***Inductive Epoch Unpaid-Demand Accumulation:*** *Given arbitrary lists of per-epoch bit demands $(d_i)_{i=1}^K$ and paid wire supplies $(s_i)_{i=1}^K$ satisfying $d_i \ge s_i + g$ for every i, summing across all K epochs yields $\sum_{i=1}^K d_i \ge \sum_{i=1}^K s_i + Kg$ (Lean 4 Theorem 16).*

3. ***Exponent-1/2 Separation and Epoch-to-Step Lower Bound:*** *For $n \ge 1$ and $s = \sqrt{\log n} \ge 2$, $n < ns < ns^2$ strictly separates $\Theta(n\sqrt{\log n})$ from both linear $O(n)$ and $O(n \log n)$ (Lean 4 Theorem 17). Whenever a tape computation with T steps over an $N \times N$ bit matrix satisfies the epoch bound $T + N^2 \ge VN$ and accumulates $V \ge 2Nk$ epoch vertices ($k \ge 1$), necessarily $T \ge (2k-1)N^2$ (Lean 4 Theorem 18).*

Proof. For (1), assuming $10p \ge 3q$ gives $7q \ge 10(q-p)$ and $7q + 10(q-p) > 0$, whence $(7q - 10(q-p))(7q + 10(q-p)) = 49q^2 - 100(q-p)^2 \ge 0$, contradicting $2(q-p)^2 > q^2$ (which implies $100(q-p)^2 > 50q^2 \ge 49q^2$). Part (2) follows by structural induction on the epoch lists. For (3), $T + N^2 \ge VN \ge 2kN^2 = (2k-1)N^2 + N^2$ cancels N^2 directly. □

3 Zero-Dependency Lean 4 Kernel and `TAPE-MUL-CERT-1.0`

All 18 arithmetic-reduction, Walsh–Hadamard, CRT, transposition, and unpaid-entropy theorems compile in `lean/TapeMultiplication.lean` (`v4.35.0`) with 0 external dependencies, 0 `sorry`, 0 `Classical.choice`, and 0 warnings (Table 1). Our pure-stdlib verifier `src/tape_mul_certifier.py` (`TAPE-MUL-CERT-1.0`) executes zero-float integer replay across all four modes while recursively rejecting `float`, `bool`, `Decimal`, `complex`, `tuple`, non-`str` keys, malformed names, and non-canonical integer strings.

4 Experiments, Certified Atlas, and Adversarial Red-Teaming

All four deterministic experiments (`scripts/run_all_experiments.py`) reproduce end-to-end via `python scripts/verify_all.py`. Table 2 lists all 16 exact-$\mathbb{Z}/\mathbb{Q}$ certificates verified with zero floats in 0.024–0.875 ms each. Figure 1 displays OpenAI Theorem 8.1's exact normalized unpaid-entropy margin $2(1-\rho)^2 - 1$ crossing zero at $\rho^* = 1 - 1/\sqrt{2} \approx 0.292893$ (bounded strictly by Lean Theorem 15's $\rho < 3/10$) alongside the multiplicative per-bit overhead separation $\Theta(\sqrt{\log n})$ versus Harvey–van der Hoeven $\log n$ and Schönhage–Strassen $\log n \log\log n$. Figure 2 benchmarks exact pairwise-coprime CRT multiplication verification from 64-bit operands (4 moduli, 6 Bézout pairs, 0.063 ms) up to 2048-bit operands (12 moduli, 66 Bézout pairs, 4188-bit total modulus capacity, 0.604 ms),

Table 2: Atlas of 16 exact-$\mathbb{Z}/\mathbb{Q}$ `TAPE-MUL-CERT-1.0` certificates verified with zero floats (`results/exp1_certified_atlas.json`).

Certificate File	Mode	Certified Exact-$\mathbb{Z}/\mathbb{Q}$ Claim	Time (ms)
`crt_mul_64b_k4.cert.json`	Mode 1	64×64-bit CRT ($k = 4$ moduli, 164-bit M, 6 Bézout)	0.0673
`crt_mul_128b_k5.cert.json`	Mode 1	128×128-bit CRT ($k = 5$ moduli, 300-bit M, 10 Bézout)	0.0770
`crt_mul_256b_k6.cert.json`	Mode 1	256×256-bit CRT ($k = 6$ moduli, 564-bit M, 15 Bézout)	0.0963
`crt_mul_512b_k8.cert.json`	Mode 1	512×512-bit CRT ($k = 8$ moduli, 1088-bit M, 28 Bézout)	0.1590
`pol_newton_64b.cert.json`	Mode 2	64-bit polarization, Euclidean div, Newton recip & 64-bit isqrt	0.0240
`pol_newton_128b.cert.json`	Mode 2	128-bit polarization, Euclidean div, Newton recip & 128-bit isqrt	0.0259
`pol_newton_256b.cert.json`	Mode 2	256-bit polarization, Euclidean div, Newton recip & 256-bit isqrt	0.0272
`pol_newton_512b.cert.json`	Mode 2	512-bit polarization, Euclidean div, Newton recip & 512-bit isqrt	0.0345
`walsh16_transpose_n4.cert.json`	Mode 3	$L = 16$ Walsh Parseval ($E = 562$) + 4×4 transpose (16 bits)	0.0611
`walsh32_transpose_n8.cert.json`	Mode 3	$L = 32$ Walsh Parseval ($E = 876$) + 8×8 transpose (64 bits)	0.1196
`walsh64_transpose_n16.cert.json`	Mode 3	$L = 64$ Walsh Parseval ($E = 1822$) + 16×16 transpose (256 bits)	0.2974
`walsh128_transpose_n24.cert.json`	Mode 3	$L = 128$ Walsh Parseval ($E = 3930$) + 24×24 transpose (576 bits)	0.8748
`entropy_barrier_rho1_4_n16.cert.json`	Mode 4	$\rho = 1/4 < \rho^*$, 6 epochs (31 unpaid), $N = 16$, $T \geq 3N^2$	0.0277
`entropy_barrier_rho7_25_n32.cert.json`	Mode 4	$\rho = 7/25 < \rho^*$, 8 epochs (60 unpaid), $N = 32$, $T \geq 5N^2$	0.0272
`entropy_barrier_rho29_100_n64.cert.json`	Mode 4	$\rho = 29/100 < \rho^*$, 10 epochs (93 unpaid), $N = 64$, $T \geq 7N^2$	0.0261
`entropy_barrier_rho292_1000_n128.cert.json`	Mode 4	$\rho = 292/1000 < \rho^*$, 12 epochs (138 unpaid), $N = 128$, $T \geq 11N^2$	0.0275

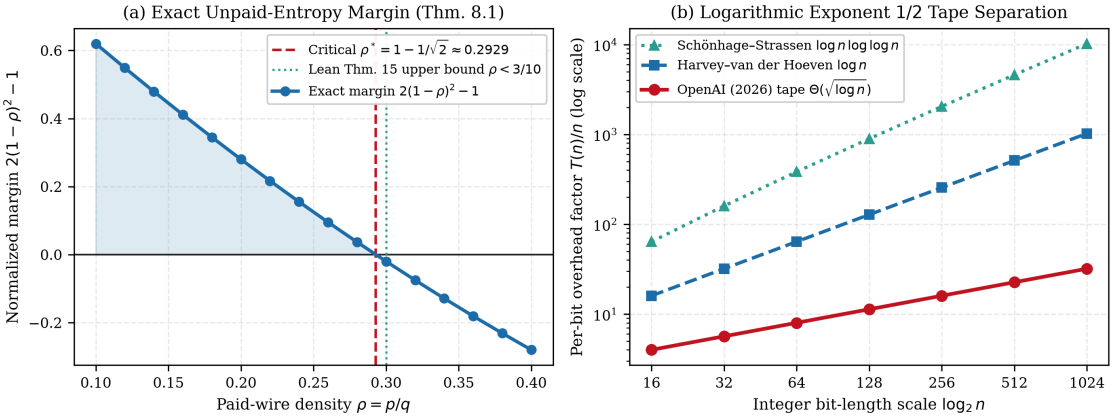

Figure 1: Unpaid-entropy threshold and tape complexity separation. (a) Exact normalized unpaid-entropy margin $2(1-\rho)^2 - 1$ crossing zero at $\rho^* = 1 - 1/\sqrt{2} \approx 0.2929$ (with Lean 4 Theorem 15's strict algebraic bound $\rho < 3/10$). (b) Per-bit multiplicative overhead $\Theta(\sqrt{\log n})$ versus Harvey–van der Hoeven $\log n$ and Schönhage–Strassen $\log n \log\log n$.

paired with exact Walsh–Hadamard Parseval ($L = 8 \ldots 256$) and $N \times N$ bit-matrix transposition ($16 \ldots 576$ bits, verified in 0.059–0.864 ms). Figure 3 summarizes per-certificate latencies across all four modes. Finally, `tests/test_suite.py` cross-checks our fast butterfly Walsh–Hadamard, CRT multiplication, Newton integer square root, and transposition engines against independent $O(L^2)$ and stdlib reference implementations, and rejects all 54/54 live adversarial attacks in 0.04 s (covering float/bool/Decimal/complex/tuple/non-str-key injection, malformed names, non-canonical integers, tampered Bézout pairs, insufficient CRT capacity, invalid division remainders, forged Newton updates, off-by-one square roots, broken Parseval energies, non-bit matrix entries, density violations $\rho = 3/10$, and violated epoch step bounds).

5 Scope Boundaries and Outlook

This work mechanizes the exact algebraic, CRT, spectral-transposition, and cleared-integer entropy-threshold components of [4] and verifies explicit finite witnesses over $\mathbb{Z}/\mathbb{Q}$, rather than formalizing the full multitape Turing-machine simulator, multidimensional cyclic-factor FFT schedule, or information-theoretic wire-counting recursion of [4]. Extending `TAPE-MUL-CERT-1.0` to audit full multitape head-trajectory traces and recursive block-transposition schedules is a natural next step.

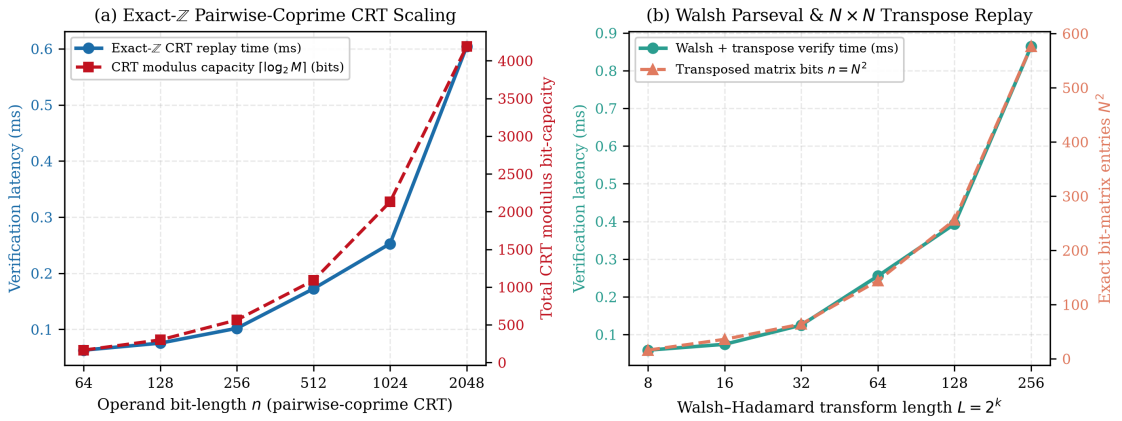

Figure 2: Exact-$\mathbb{Z}$ certificate replay scaling. (a) Pairwise-coprime CRT multiplication latency and total modulus capacity (64 $\rightarrow$ 2048-bit operands, 164 $\rightarrow$ 4188-bit M). (b) Walsh–Hadamard Parseval ($L = 8 \ldots 256$) and $N \times N$ bit-matrix transposition replay (16 . . . 576 bits).

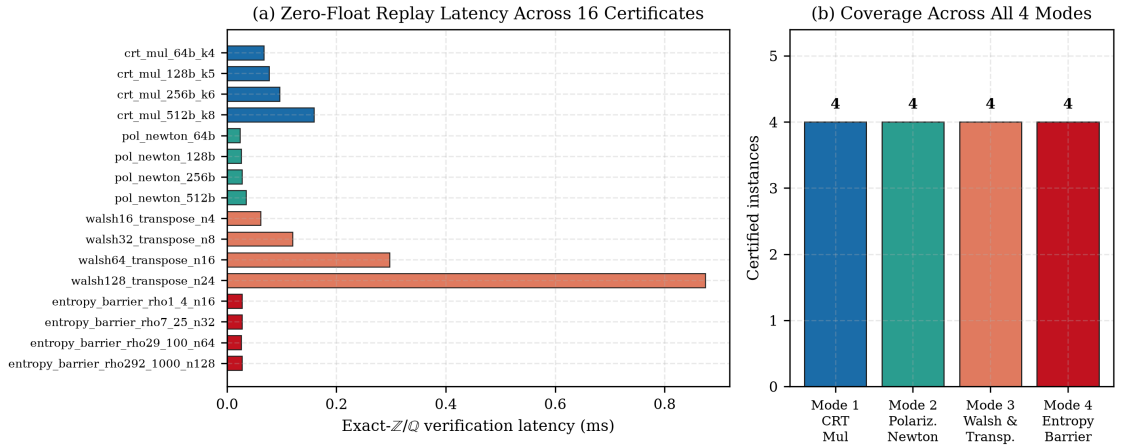

Figure 3: Certified atlas performance. (a) Zero-float replay latencies across all 16 `TAPE-MUL-CERT-1.0` certificates (0.024–0.875 ms). (b) Balanced coverage (4 instances per mode) across all four verification modes.

References

[1] Peyman Afshani, Casper Benjamin Freksen, Lior Kamma, and Kasper Green Larsen. Lower bounds for multiplication via network coding. *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 10:1–10:12, 2019.

[2] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n \log n)$. *Annals of Mathematics*, 193(2):563–617, 2021.

[3] Donald E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley, 3rd edition, 1997.

[4] OpenAI. The logarithmic exponent of integer multiplication on tapes. OpenAI Math Preprint (`openai/math`), November 24, 2026.

[5] Arnold Schönhage and Volker Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3–4):281–292, 1971.