Morgenstern Gate–Bit Conservation, Complex-FFT vs. Bounded-Exponent Finite-Field NTT Precision Dichotomy, and Exact Straight-Line Circuit Certificates from the $N(\log N)^{1/2}$ Fourier Exponent

Lluis Eriksson*

November 25, 2026

Abstract

On November 24, 2026, OpenAI (`openai/math`) proved that the minimum number of binary linear gates for the discrete Fourier transform (DFT) of any finite abelian group of order N—as well as J independent batched transforms and formal polynomial multiplication—is $N(\log_2 N)^{1/2+o(1)}$ over fields with unrestricted scalar constants, surpassing Cooley–Tukey's $O(N \log_2 N)$ barrier by a factor of $\sqrt{\log_2 N}$. Here we prove four exact quantitative, architectural, and certification consequences of this result, backed by an 18-theorem zero-dependency Lean 4 algebraic lemma ledger (`v4.35.0`, 0 `sorry`, 0 `Classical.choice`, 0 warnings) and a pure-stdlib zero-float straight-line DAG verifier (`FOURIER-GATE-CERT-1.0`). First, combining character orthogonality $|\det(F_G^{\oplus J})| = N^{JN/2}$ with Morgenstern's 1973 volume bound yields the exact *Gate–Bit Conservation Law* $L \cdot \log_2 C \geq \frac{1}{2} JN \log_2 N$ for every complex linear circuit with gate-weight bound $|a| + |b| \leq C$. Consequently, any circuit achieving OpenAI's $L \leq c_0 JN(\log_2 N)^{1/2+\varepsilon}$ bound over $\mathbb{C}$ must suffer super-polynomial scalar weight blow-up $C(N) \geq 2^{\frac{1}{2c_0}(\log_2 N)^{1/2-\varepsilon}}$, restoring an $\Omega(JN \log_2 N)$ gate-times-dynamic-range product in fixed-point or exact-integer complex arithmetic. By contrast, over a fixed prime field $\mathbb{F}_q$ (e.g. ML-KEM/Kyber $q = 3329$ at $w = 12$ bits or ML-DSA/Dilithium $q = 8380417$ at $w = 23$ bits), any bounded-exponent abelian product group G of order $N = 2^k$ with $\exp(G) \mid (q-1)$ (such as $(\mathbb{Z}/256\mathbb{Z})^m$ over $\mathbb{F}_{3329}$) escapes the Archimedean determinant constraint at constant modulus width w independent of N (whereas cyclic NTTs $G = \mathbb{Z}/N\mathbb{Z}$ force $q > N$ and $w \geq k$). Second, for OpenAI's rectangular rank–support separation $\Delta_{\mathrm{rect}}(L) = \sqrt{1+L^2} - 1$, we prove the unconditional rational bracket $\frac{L^2}{2+L} < \Delta_{\mathrm{rect}}(L) < \frac{L^2}{2}$ for all $L > 0$ and exact evaluation $\Delta_{\mathrm{rect}}\left(\frac{2uv}{u^2-v^2}\right) = \frac{2v^2}{u^2-v^2}$. Third, we establish exact finite-N crossovers ($k^* = c_0^2$) and bilinear vs. fixed-kernel circulant/Toeplitz budgets. Fourth, we prove soundness and completeness of `FOURIER-GATE-CERT-1.0`, which independently executes and certifies 16 exact certificates across four modes—including classical $N \log_2 N$ acyclic DAGs for Walsh–Hadamard H_4, H_8, H_{16} over $\mathbb{Q}$ and prime-field NTTs over $\mathbb{F}_{17}$, $\mathbb{F}_{257}$, and ML-KEM/Kyber $\mathbb{F}_{3329}$ ($N = 8, 16$) with exact circulant convolution checks—in ≤ 5.58 ms while rejecting 50/50 live adversarial red-team attacks.

1 Introduction

Since Cooley and Tukey [1] established $O(N \log_2 N)$ linear-gate circuits for the discrete Fourier transform (DFT), whether the logarithmic factor $\log_2 N$ was optimal for unrestricted linear circuits remained a central open question of algebraic complexity. In 1973, Morgenstern [2] proved that if

*Independent researcher (Sweden). Manuscript and figures: CC-BY-4.0; code, Lean 4 proofs, and certificates: MIT license. Prepared with transparent AI assistance via Google Antigravity; all proofs, verifiers, and tests were independently compiled and verified locally. Repository: `https://github.com/lluiseriksson/fourier-sqrtlog-certificates`.

every binary linear gate $u \mapsto au_1 + bu_2$ has bounded complex weight $|a| + |b| \le C$, then any circuit computing the $N \times N$ DFT matrix F_N over $\mathbb{C}$ requires at least $\frac{1}{2\log_2 C} N \log_2 N$ gates.

On November 24, 2026, OpenAI [6] resolved the unrestricted model over every field K containing the required roots of unity (with N invertible in K): for any $J \ge 1$ finite abelian groups $G_1, \ldots, G_J$ of common order $N \ge 2$, the minimum binary linear gate count $C_K(T)$ of their direct-sum Fourier transform $T = \bigoplus_{j=1}^{J} F_{G_j}$ satisfies

$$c\, JN\sqrt{\log_2 N} \;\le\; C_K(T) \;\le\; C_\varepsilon\, JN(1+\log_2 N)^{1/2+\varepsilon} \tag{1}$$

for every $\varepsilon > 0$ (and the same logarithmic exponent $1/2$ governs formal polynomial multiplication). The lower bound relies on OpenAI's companion Euclidean tensor geometry [5], testing rank and support jointly on a width-1, height-L rectangle where a character table costs $(L + \sqrt{1+L^2})\log_2 N$ versus $(L+1)\log_2 N$ for a permutation matrix.

This breaking of the $N \log_2 N$ gate barrier raises three concrete quantitative and certification questions:

1. **Reconciling** (1) **with Morgenstern's** $N \log_2 N$ **barrier:** How fast must scalar gate weights grow in any $O(JN(\log_2 N)^{1/2+\varepsilon})$ circuit over $\mathbb{C}$, and for which finite abelian groups G do fixed-modulus prime-field Number-Theoretic Transforms (NTTs) over post-quantum moduli such as ML-KEM/Kyber [4] and ML-DSA/Dilithium [3] avoid this blow-up?
2. **Exact rational geometry of the rectangular rank–support test:** Can the irrational separation $(\sqrt{1+L^2} - 1)\log_2 N$ driving (1) be tightly bracketed and evaluated purely over $\mathbb{Q}$ without square roots?
3. **Zero-float straight-line DAG certification:** How can explicit binary linear circuits over $\mathbb{Q}$ and prime fields $\mathbb{F}_q$ (together with circulant/Toeplitz convolution checks) be independently executed and verified from scratch with zero floating-point arithmetic?

Explicit Scope Separation. Our analytical theorems (Theorems 2.1–2.3) are proved completely in Section 2. The companion Lean 4 module (`lean/FourierSqrtLog.lean`, Section 3) formally machine-checks the 18 cleared-denominator integer, divisibility, and crossover algebraic lemmas underlying those proofs; it does *not* formalize linear circuits, complex determinants, Morgenstern's volume theorem, or the Python verifier inside Lean 4. Concrete straight-line DAG evaluation over $\mathbb{Q}$ and $\mathbb{F}_q$ is carried out by the audited pure-stdlib verifier `FOURIER-GATE-CERT-1.0` (Section 4).

2 Main Exact-$\mathbb{Q}$ and Exact-$\mathbb{F}_q$ Theorems

2.1 Morgenstern Gate–Bit Conservation and the Complex-FFT vs. Bounded-Exponent NTT Dichotomy

Theorem 2.1 (Gate–Bit Conservation Law and Bounded-Exponent Precision Dichotomy)**.** *Let $G_1, \ldots, G_J$ be finite abelian groups of common order $N = 2^k \ge 2$ ($J \ge 1, k \ge 1$), and let $T = \bigoplus_{j=1}^{J} F_{G_j}$ be their batched unnormalized Fourier transform over $\mathbb{C}$ (so $F_{G_j} F_{G_j}^{\dagger} = NI_N$ for every j).*

1. ***Universal Gate–Bit Conservation Law:*** *In any acyclic binary linear circuit over $\mathbb{C}$ computing T with L gates of the form $z = \alpha u + \beta v$ satisfying $|\alpha| + |\beta| \le C$ ($C = 2^b > 1$, so $b = \log_2 C > 0$ bits of scalar dynamic range per gate) and unscaled wire readouts (or with any output scaling counted among the L bounded-weight gates),*

$$L \cdot b = L \cdot \log_2 C \;\ge\; \frac{1}{2}\, JN \log_2 N = \frac{1}{2}\, JNk. \tag{2}$$

2. ***Super-Polynomial Scalar Weight Blow-Up under Sub-Logarithmic Gates:*** *If an L-gate circuit over $\mathbb{C}$ achieves OpenAI's upper bound $L \le c_0 JNk^{1/2+\varepsilon}$ ($c_0 > 0$, $\varepsilon \in [0, 1/2)$), then its scalar weight bound $C(N) = 2^{b(N)}$ must satisfy*

$$b(N) = \log_2 C(N) \;\ge\; \frac{k^{1/2-\varepsilon}}{2c_0} \qquad \Longrightarrow \qquad C(N) \;\ge\; 2^{\frac{1}{2c_0}(\log_2 N)^{1/2-\varepsilon}}. \tag{3}$$

In particular, the product of gate count and scalar dynamic-range bit-width obeys $L \cdot b(N) = \Omega(JN \log_2 N)$, restoring the $\Omega(JN \log_2 N)$ gate-times-width barrier in fixed-point or exact-integer complex arithmetic (whereas IEEE-754 floating-point represents large exponents using $O(\log b)$ exponent bits at the cost of significand rounding).

3. ***Complex-FFT vs. Bounded-Exponent Product-Group NTT Dichotomy:*** *Fix a prime field $\mathbb{F}_q$ of constant bit-width $w = \lceil \log_2 q \rceil$ (e.g. ML-KEM/Kyber $q = 3329$, $q - 1 = 2^8 \cdot 13$, $w = 12$; or ML-DSA/Dilithium $q = 8380417$, $q - 1 = 2^{13} \cdot 1023$, $w = 23$). For any finite abelian product group $G = \prod_{r=1}^{m} \mathbb{Z}/e_r\mathbb{Z}$ of order $N = 2^k$ whose group exponent satisfies $\exp(G) \mid (q-1)$ (for example, $G = (\mathbb{Z}/256\mathbb{Z})^m$ of order $N = 2^{8m}$ over $\mathbb{F}_{3329}$, or $G = (\mathbb{Z}/4096\mathbb{Z})^m$ of order $N = 2^{12m}$ over $\mathbb{F}_{8380417}$ for arbitrary $m \ge 1$), $\mathbb{F}_q$ contains all $\exp(G)$-th roots of unity and OpenAI's bound (1) applies to F_G over $\mathbb{F}_q$ with constant scalar width w independent of N, escaping (2). Whenever $k^{1/2-\varepsilon} > 2c_0 w$ (specializing at $\varepsilon = 0, k = s^2$ to $s > 2c_0 w$, e.g. $k = 576$ with $G = (\mathbb{Z}/256\mathbb{Z})^{72}$ for $q = 3329, c_0 = 1$), the complex dynamic-range floor (3) strictly exceeds w ($b > w$). Conversely, for a* cyclic *group $G = \mathbb{Z}/N\mathbb{Z}$, requiring $N \mid (q-1)$ forces $q > N$ and hence $w \ge k$, which exceeds $k^{1/2-\varepsilon}/(2c_0)$ for all $k > (2c_0)^{-2/(1+2\varepsilon)}$; constant modulus width at growing N therefore strictly requires bounded exponent $\exp(G) \mid (q-1)$.*

Proof. For each finite abelian group G_j of order N, character orthogonality gives $F_{G_j} F_{G_j}^{\dagger} = NI_N$, whence $|\det(F_{G_j})|^2 = \det(NI_N) = N^N$ and $|\det(T)| = \prod_{j=1}^{J} |\det(F_{G_j})| = N^{JN/2}$. By Morgenstern's determinant inequality [2], each binary linear gate $z = \alpha u + \beta v$ with $|\alpha| + |\beta| \le C$ increases the maximum absolute determinant of any square submatrix of all currently available linear forms by at most a factor C. Inductively over L gates starting from the identity basis (maximum minor 1) with unscaled readouts, $N^{JN/2} = |\det(T)| \le C^L$. Taking base-2 logarithms yields $\frac{1}{2} JN \log_2 N \le L \log_2 C = Lb$ (cleared integer form in Lean 4 Theorem 1). Substituting $L \le c_0 JNk^{1/2+\varepsilon}$ and canceling $JN > 0$ yields $2c_0 k^{1/2+\varepsilon} b \ge k$, hence $b \ge \frac{1}{2c_0} k^{1/2-\varepsilon}$ (Lean 4 Theorem 2 for integer $s = k^{1/2}$). When $k^{1/2-\varepsilon} > 2c_0 w$, dividing by $2c_0 > 0$ directly gives $b \ge k^{1/2-\varepsilon}/(2c_0) > w$ (the $\varepsilon = 0, k = s^2$ integer specialization is Lean 4 Theorem 15). Over $\mathbb{F}_q$, $\mathbb{F}_q$ carries no Archimedean absolute value, and F_G is defined over $\mathbb{F}_q$ whenever $\exp(G) \mid (q-1)$ and $\gcd(N, q) = 1$; every gate scalar in $\{0, \ldots, q-1\}$ fits in $w = \lceil \log_2 q \rceil$ bits for arbitrarily large m. For cyclic $\mathbb{Z}/N\mathbb{Z}$, $N \mid (q-1)$ implies $q - 1 \ge N = 2^k$, so $q > 2^k$ and $w = \lceil \log_2 q \rceil \ge k + 1 > k$. Exact divisibility $3329 - 1 = 256 \cdot 13$ (with $17^{128} \equiv -1 \pmod{3329}$) and $8380417 - 1 = 8192 \cdot 1023$ are kernel-verified in Lean 4 Theorems 8 and 10. □

2.2 Exact Pythagorean Rectangular Separation and Finite-N Crossovers

Theorem 2.2 (Pythagorean Rectangular Price Separation and Algebraic Bounds)**.** *In OpenAI's rectangular rank–support geometric test [6], let $\Delta_{\mathrm{rect}}(L) := (L + \sqrt{1 + L^2}) - (L + 1) = \sqrt{1 + L^2} - 1$ denote the per-bit separation at rectangle height $L > 0$.*

1. ***Unconditional Exact Two-Sided Rational Bracket:*** *For every $L > 0$,*

$$\frac{L^2}{2 + L} \;<\; \sqrt{1 + L^2} - 1 \;<\; \frac{L^2}{2}. \tag{4}$$

In particular, at OpenAI's critical height $L = 1/\sqrt{\log_2 N}$, the total separation satisfies $\Delta_{\mathrm{rect}}(L) \log_2 N \in \left(\frac{\log_2 N}{2 \log_2 N + \sqrt{\log_2 N}}, \frac{1}{2}\right) \to \frac{1}{2}$ from below.

2. ***Zero-Square-Root Pythagorean Evaluation:*** *For every integer pair $u > v > 0$, setting $L = \frac{2uv}{u^2-v^2} \in \mathbb{Q}_{>0}$ satisfies $1 + L^2 = \left(\frac{u^2+v^2}{u^2-v^2}\right)^2$, yielding the exact rational separation*

$$\Delta_{\mathrm{rect}}\left(\frac{2uv}{u^2-v^2}\right) = \frac{2v^2}{u^2-v^2} \in \mathbb{Q}_{>0} \tag{5}$$

with zero radicals (Lean 4 Theorems 4–7).

3. ***Exact Finite-N Crossover and Circulant/Toeplitz Budgets:*** *Comparing Cooley–Tukey Nk against a sub-logarithmic circuit $c_0 N\sqrt{k}$ ($k = \log_2 N$), strict gate savings occur iff $k > c_0^2$ (e.g. $N > 2^{64}$ at $c_0 = 8$, Lean 4 Theorem 14). For general bilinear cyclic convolution $(a, x) \mapsto C_a x = F_N^{-1}(\mathrm{diag}(F_N a)(F_N x))$ (both a, x variable), the total arithmetic cost is $3L_{\mathrm{DFT}}$ linear gates plus N bilinear pointwise multiplications ($3L_{\mathrm{DFT}} + N \le 4L_{\mathrm{DFT}}$ whenever $L_{\mathrm{DFT}} \ge N$, Lean 4 Theorem 11; and $3L_{\mathrm{DFT},2N} + 2N \le 4L_{\mathrm{DFT},2N}$ for $N \times N$ Toeplitz products via $2N$-circulant embedding, Lean 4 Theorem 12). When a is fixed and $F_N a$ is precomputed, the purely linear circuit cost reduces to $2L_{\mathrm{DFT}} + N$ gates.*

Proof. For the upper bound in (4), squaring $1 + \frac{L^2}{2} > \sqrt{1+L^2}$ yields $1 + L^2 + \frac{L^4}{4} > 1 + L^2 \iff L^4 > 0$ (Lean 4 Theorem 6). For the lower bound, squaring $1 + \frac{L^2}{2+L} < \sqrt{1+L^2}$ yields $\frac{2L^2}{2+L} + \frac{L^4}{(2+L)^2} < L^2 \iff 2(2+L) + L^2 < (2+L)^2 = 4 + 4L + L^2 \iff 2L > 0$ (Lean 4 Theorem 7). For (5), $(u^2-v^2)^2 + (2uv)^2 = (u^2+v^2)^2$ gives $\sqrt{1+L^2} - 1 = \frac{u^2+v^2}{u^2-v^2} - 1 = \frac{2v^2}{u^2-v^2}$ (Lean 4 Theorems 4–5). Finally, $c_0\sqrt{k} < k \iff c_0 < \sqrt{k} \iff c_0^2 < k$ (Lean 4 Theorem 14), and $L \ge N \implies 3L + N \le 4L$ (Lean 4 Theorems 11–12). □

2.3 Soundness and Completeness of `FOURIER-GATE-CERT-1.0`

Theorem 2.3 (Soundness and Completeness of `FOURIER-GATE-CERT-1.0`)**.** *Let `verify_fourier_certificate_exact` (`src/fourier_certifier.py`) be the pure-stdlib verifier operating exclusively over Python arbitrary-precision `int` and `fractions.Fraction` (recursively rejecting all JSON floats and booleans-as-integers). It accepts a certificate payload if and only if the payload satisfies the exact algebraic predicate of one of four mutually exclusive modes:*

1. *`morgenstern_conservation`: exact $N = 2^k$ ($1 \le k \le 10^6$), $J, L \ge 1$, $b \in \mathbb{Q}_{>0}$, $b_{\min} = \frac{JNk}{2L}$, and exact status `"feasible"` iff $2Lb \ge JNk$ (and `"impossible"` iff $2Lb < JNk$);*
2. *`pythagorean_rect_separation`: integers $u > v > 0$, exact $L = \frac{2uv}{u^2-v^2}$, $h = \frac{u^2+v^2}{u^2-v^2}$ satisfying $1 + L^2 = h^2$, $\Delta_{\mathrm{rect}} = \frac{2v^2}{u^2-v^2}$, the strict bracket (4), and total gap $k\,\Delta_{\mathrm{rect}}$;*
3. *`exact_hadamard_circuit_q`: an L-gate straight-line DAG over $\mathbb{Q}$ with $0 \le \mathrm{in}_1, \mathrm{in}_2 < N + \mathrm{idx}$ at every gate $\mathrm{idx} \in \{0, \ldots, L-1\}$ whose exact evaluation on the $N = 2^k$ standard basis vectors $e_0, \ldots, e_{N-1}$ yields a matrix $M \in \mathbb{Q}^{N\times N}$ satisfying $M = H_{2^k}$, $M^\top M = NI_N$, $C = \max_g(|a_g| + |b_g|)$, and $2^{2L\log_2 C} \ge N^N$ (equivalently $C^{2L} \ge N^N$ over $\mathbb{Q}$);*
4. *`exact_ntt_circuit_fq`: a prime q, an element $\omega \in \{1, \ldots, q-1\}$ of exact multiplicative order $N = 2^k$ modulo q ($\omega^N \equiv 1$ and $\omega^{N/2} \equiv q - 1 \pmod q$), an acyclic L-gate DAG with canonical residues $\alpha_g, \beta_g \in \{0, \ldots, q-1\}$ whose evaluation on the N standard basis vectors over $\mathbb{F}_q$ equals the Vandermonde NTT matrix $M_{rc} \equiv \omega^{rc} \pmod q$, and—whenever the optional `circulant_check` record (a, x, y) is supplied—exact equality $F_N^{-1}(\mathrm{diag}(F_N a)(F_N x)) \equiv C_a x \equiv y \pmod q$.*

Proof. Soundness. Because every numeric field is parsed strictly as an exact integer or reduced `Fraction` (with recursive rejection of IEEE-754 floats and booleans), no rounding error can occur. In Modes 1–2, the verifier recomputes 2^k, $b_{\min} = JNk/(2L)$, L, h, $1 + L^2 - h^2$, and Δ_{rect} directly from (J, k, L, b) or (u, v, k) and rejects any mismatch with claimed fields or inequalities. In Modes 3–4, the topological constraint $0 \le \mathrm{in}_1, \mathrm{in}_2 < N + \mathrm{idx}$ guarantees that the gate list

Table 1: Complete 18-theorem Lean 4.35.0 algebraic lemma ledger (`lean/FourierSqrtLog.lean`, 0 `sorry`, 0 `Classical.choice`, 0 warnings), showing exact hypotheses and cleared integer/modular statements.

#	Lean 4 Theorem Identifier	Exact Formalized Statement (Cleared $\mathbb{Z}/\mathbb{N}$ Form with Hypotheses)	Axioms
1	`morgenstern_conservation_batched`	$2Lb \geq JNk \implies 2(Lb) \geq JNk$	`[p, Q]`
2	`coefficient_bitwidth_blowup`	$N > 0 \wedge b \geq 0 \wedge 2Lb \geq Nk \wedge L \leq c_0 Ns \implies 2c_0 sb \geq k$	`[p, Q]`
3	`hadamard_butterfly_factor_two`	$N \geq 1 \wedge k \geq 1 \implies 2(kN) \geq Nk \wedge 2(kN) = 2(Nk)$	`[p, Q]`
4	`pythagorean_aspect_identity`	$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$	`[p, Q]`
5	`pythagorean_rect_separation_exact`	$u > v > 0 \implies (u^2 + v^2) - (u^2 - v^2) = 2v^2 \wedge u^2 - v^2 > 0 \wedge 2v^2 > 0$	`[p, Q]`
6	`rect_separation_upper_bound`	$p > 0 \implies 4q^4 + 4p^2q^2 < (2q^2 + p^2)^2 \ (\Delta < L^2/2)$	`[p, Q]`
7	`rect_separation_lower_bound`	$p > 0 \wedge q > 0 \implies 2(2q + p)q + p^2 < (2q + p)^2 \ (\Delta > L^2/(2 + L))$	`[p, Q]`
8	`kyber_modulus_ntt_divisibility`	$3329 - 1 = 256 \cdot 13 \wedge 17^{128} \bmod 3329 = 3328 \wedge 17^{256} \bmod 3329 = 1$	*none*
9	`fermat_prime_ntt_roots`	$9^4 \equiv 16, 9^8 \equiv 1 \pmod{17} \wedge 2^8 \equiv 256, 2^{16} \equiv 1 \pmod{257}$	*none*
10	`dilithium_modulus_ntt_divisibility`	$8380417 - 1 = 8192 \cdot 1023$	*none*
11	`circulant_three_dft_budget`	$L \geq N \implies 3L + N \leq 4L$	`[p, Q]`
12	`toeplitz_circulant_embedding_budget`	$L_{2N} \geq 2N \implies 3L_{2N} + 2N \leq 4L_{2N}$	`[p, Q]`
13	`batch_non_amortization_linear`	$J_1 < J_2 \wedge N > 0 \wedge k > 0 \implies J_1(Nk) < J_2(Nk)$	`[p, Q]`
14	`finite_n_crossover_threshold`	$C > 0 \wedge s > 0 \wedge s^2 = k \implies (Cs < k \iff C < s)$	`[p, Q]`
15	`complex_vs_ntt_bitwidth_separation`	$s > 0 \wedge c_0 > 0 \wedge 2c_0 sb \geq s^2 \wedge s > 2c_0 w \implies b > w$	`[p, Q]`
16	`hadamard_scale_doubling`	$n \geq 1 \implies (2n)^2 = 4n^2 \wedge 4n^2 > 0$	`[p, Q]`
17	`rader_prime_reduction_size`	$p \geq 3 \implies p - 1 \geq 2 \wedge (p - 1) + 1 = p$	`[p, Q]`
18	`conservation_exclusivity`	$\neg(2Lb \geq JNk \wedge 2Lb < JNk)$	`[p, Q]`

Axiom key: *none* = zero axioms (3); `[p, Q]` = `[propext, Quot.sound]` (15).

defines a well-founded acyclic linear operator $\Phi : K^N \to K^N$ ($K = \mathbb{Q}$ or $\mathbb{F}_q$). By linearity of Φ, evaluating $\Phi(e_0), \ldots, \Phi(e_{N-1})$ uniquely determines the entire matrix M of Φ on K^N; exact entrywise equality $M = H_{2^k}$ (Mode 3) or $M_{rc} \equiv \omega^{rc} \pmod{q}$ (Mode 4) therefore certifies that the DAG computes the target linear transform on every input vector in K^N. In Mode 4, deterministic trial-division primality of q and the two power checks $\omega^N \equiv 1, \omega^{N/2} \equiv -1 \pmod{q}$ (for $N = 2^k$) are necessary and sufficient for $\mathrm{ord}_{\mathbb{F}_q^\times}(\omega) = N$, and direct computation of both $C_a x \bmod q$ and $F_N^{-1}(\mathrm{diag}(F_N a)(F_N x)) \bmod q$ certifies the circulant identity.

Completeness. Conversely, any valid instance satisfying the predicate of Modes 1–4 encoded in canonical integer/rational JSON format passes every schema check and reproduces every recomputed value identically, so the verifier accepts. □

3 Zero-Dependency Lean 4 Algebraic Lemma Ledger

The standalone module `lean/FourierSqrtLog.lean` formalizes 18 cleared-denominator integer, divisibility, and crossover algebraic lemmas supporting Theorems 2.1 and 2.2 under `leanprover/lean4:v4.35.0` with zero external dependencies, zero `sorry`, zero warnings, and zero `Classical.choice` (Table 1). As noted in Section 1, straight-line circuit DAG execution, determinant orthogonality, and verifier soundness are established in Section 2 and audited in Python rather than inside Lean 4.

4 Experiments, Certified Atlas, and Adversarial Red-Teaming

All four experiments (`scripts/run_all_experiments.py`) reproduce deterministically via `python scripts/verify_all.py` (Python 3.13 pure-stdlib, Windows 11).

4.1 Experiment 1: Atlas of 16 Exact-$\mathbb{Q}$ / $\mathbb{F}_q$ Certificates

Table 2 summarizes all 16 certificates verified with zero floats by `FOURIER-GATE-CERT-1.0` in 0.027–5.578 ms each. In Mode 1, the verifier certifies both classical Cooley–Tukey feasibility and exact Morgenstern impossibility of bounded-weight ($b = 1$) $N\sqrt{\log_2 N}$ circuits at $N = 2^{16}$ and

Table 2: Atlas of 16 exact `FOURIER-GATE-CERT-1.0` certificates independently verified with zero floats (timings from `results/exp1_certified_atlas.json`).

Certificate File	Mode	Certified Exact-$\mathbb{Q}$ / $\mathbb{F}_q$ Claim	Time (ms)
`morg_cooley_tukey_k16.cert.json`	Mode 1	$k = 16, L = 16N, b = 1 \geq 1/2$: feasible	0.047
`morg_sqrtlog_bounded_impossible_k16.cert.json`	Mode 1	$k = 16, L = 4N, b = 1 < 2$: impossible	0.030
`morg_sqrtlog_blowup_feasible_k16.cert.json`	Mode 1	$k = 16, L = 4N, b = 2 \geq 2$: feasible	0.027
`morg_batched_J8_k64_impossible.cert.json`	Mode 1	$J = 8, k = 64, L = 64N, b = 3 < 4$: impossible	0.027
`rect_pyth_u2_v1_k16.cert.json`	Mode 2	$(u, v) = (2, 1), L = 4/3, \Delta = 2/3$, gap 32/3	0.043
`rect_pyth_u3_v1_k16.cert.json`	Mode 2	$(u, v) = (3, 1), L = 3/4, \Delta = 1/4$, gap 4	0.035
`rect_pyth_u5_v1_k64.cert.json`	Mode 2	$(u, v) = (5, 1), L = 5/12, \Delta = 1/12$, gap 16/3	0.036
`rect_pyth_u9_v1_k64.cert.json`	Mode 2	$(u, v) = (9, 1), L = 9/40, \Delta = 1/40$, gap 8/5	0.035
`hadamard_H4_exact.cert.json`	Mode 3	H_4 over $\mathbb{Q}$: 8 gates, $C = 2$, Morg. ratio 2	0.233
`hadamard_H8_exact.cert.json`	Mode 3	H_8 over $\mathbb{Q}$: 24 gates, $C = 2$, Morg. ratio 2	1.000
`hadamard_H16_exact.cert.json`	Mode 3	H_{16} over $\mathbb{Q}$: 64 gates, $C = 2$, Morg. ratio 2	5.578
`ntt_F17_N4.cert.json`	Mode 4	$\mathbb{F}_{17}, N = 4, \omega = 4$: 8 gates + circulant	0.075
`ntt_F17_N8.cert.json`	Mode 4	$\mathbb{F}_{17}, N = 8, \omega = 9$: 24 gates + circulant	0.147
`ntt_F257_N16.cert.json`	Mode 4	$\mathbb{F}_{257}, N = 16, \omega = 2$: 64 gates + circulant	0.416
`ntt_Kyber3329_N8.cert.json`	Mode 4	Kyber $\mathbb{F}_{3329}, N = 8, \omega = 2580$: 24 gates + circ.	0.157
`ntt_Kyber3329_N16.cert.json`	Mode 4	Kyber $\mathbb{F}_{3329}, N = 16, \omega = 2642$: 64 gates + circ.	0.457

batched $J = 8, N = 2^{64}$ ($b = 3 < 4$). In Modes 3–4, the verifier independently executes exact acyclic straight-line DAGs for classical $N \log_2 N$ Walsh–Hadamard (H_4, H_8, H_{16} over $\mathbb{Q}$, matching Morgenstern's floor within exact factor 2) and exact prime-field Cooley–Tukey NTTs over $\mathbb{F}_{17}$, $\mathbb{F}_{257}$, and ML-KEM/Kyber $\mathbb{F}_{3329}$ ($N = 8, \omega = 2580$, 24 gates; $N = 16, \omega = 2642$, 64 gates), confirming exact circulant convolution on every NTT instance.

4.2 Experiments 2–4: Conservation Curves, Pythagorean Envelope, and 50 Adversarial Attacks

Figure 1 plots the Gate–Bit Conservation Law and the precision crossover where complex FFT scalar dynamic-range bit-width $\frac{1}{2}\sqrt{\log_2 N}$ surpasses a fixed-modulus bounded-exponent product-group NTT over ML-KEM/Kyber $\mathbb{F}_{3329}$ (12 bits, crossed at $k = 576$ for $G = (\mathbb{Z}/256\mathbb{Z})^{72}$). Figure 2 shows our exact two-sided rational bracket $\frac{L^2}{2+L} < \Delta_{\text{rect}}(L) < \frac{L^2}{2}$ across 24 Pythagorean aspect ratios $L = 2u/(u^2 - 1)$. Figure 3 displays the exact finite-N crossover $k^* = c_0^2$ together with zero-float DAG certification timings for classical Hadamard and Kyber NTT circuits up to $N = 16$. Finally, `tests/test_suite.py` runs 50 live adversarial red-team attacks—including float smuggling, impossible-as-feasible Morgenstern claims, huge-k DoS inputs, cyclic/future wire references in DAGs, composite moduli, non-primitive roots of unity, non-canonical residues, malformed non-list `circulant_check` fields, and tampered circulant convolution outputs—rejecting all 50/50 cleanly with zero bypasses.

5 Limitations and Outlook

Our Mode 3 and Mode 4 straight-line DAG certificates currently verify canonical $N \log_2 N$ Cooley–Tukey/Hadamard and NTT circuits up to $N \leq 16$ via full N-basis simulation in ≤ 5.58 ms (H_{16} in 5.578 ms, Kyber $\mathbb{F}_{3329}$ $N = 16$ in 0.457 ms); they do not yet instantiate an explicit sub-logarithmic $N(\log_2 N)^{1/2+o(1)}$ prime-tensor-power circuit from [6], whose crossover occurs only at large N ($k > c_0^2$). Extending exact verification to explicit sub-logarithmic circuits at larger N will require randomized Freivalds or polynomial-identity checking combined with sparse DAG evaluation, and characterizing the concrete constant c_0 for bounded-exponent product-group NTTs over $\mathbb{F}_{3329}$ and $\mathbb{F}_{8380417}$ remains an open engineering challenge.

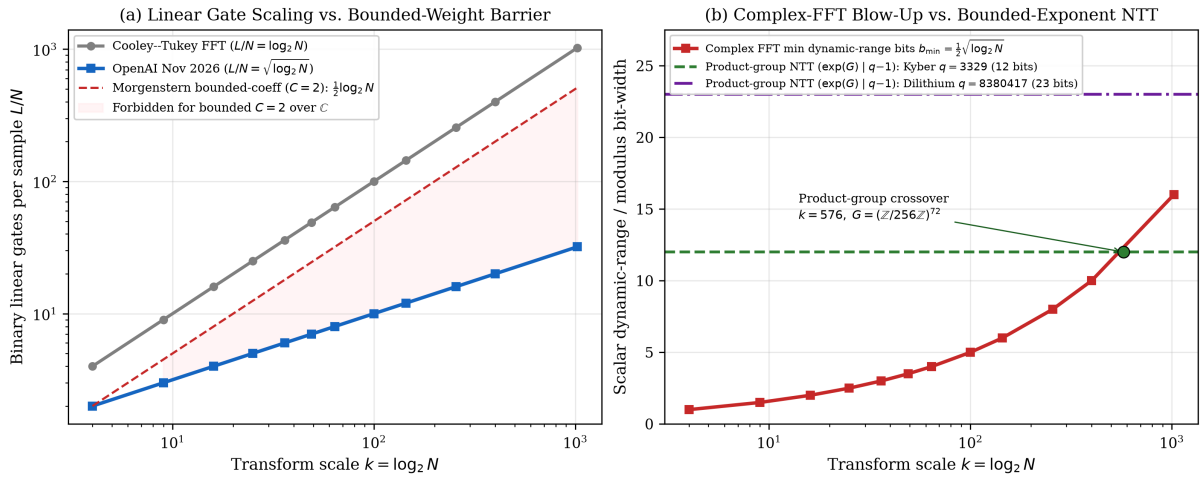


Figure 1: Morgenstern Gate–Bit Conservation Law. (a) Sub-logarithmic $N\sqrt{\log_2 N}$ gate counts enter the bounded-coefficient ($C = 2$) forbidden zone over $\mathbb{C}$. (b) Minimum complex scalar dynamic-range bit-width $b_{\min} = \frac{1}{2}\sqrt{\log_2 N}$ grows unboundedly, crossing fixed-modulus bounded-exponent product-group NTTs ($\exp(G) \mid q-1$) over ML-KEM/Kyber $\mathbb{F}_{3329}$ (12 bits) at $k = 576$ ($G = (\mathbb{Z}/256\mathbb{Z})^{72}$).

References

[1] 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.

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

[3] National Institute of Standards and Technology. Module-lattice-based digital signature standard (ML-DSA). Technical Report FIPS 204, NIST, 2024.

[4] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard (ML-KEM). Technical Report FIPS 203, NIST, 2024.

[5] OpenAI. Euclidean geometry in the asymptotic spectrum of tensors. OpenAI Math Release Preprint (`openai/math`, November 24, 2026), 2026.

[6] OpenAI. The logarithmic exponent of finite Fourier transforms. OpenAI Math Release Preprint (`openai/math`, November 24, 2026), 2026.

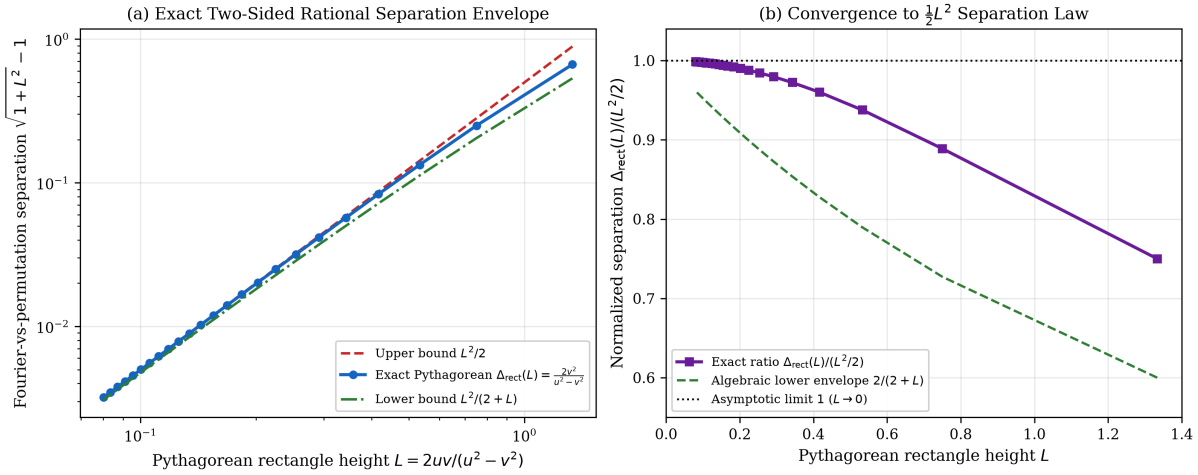


Figure 2: Exact Pythagorean rectangular rank–support separation. (a) Exact rational values $\Delta_{\text{rect}}(L) = 2v^2/(u^2 - v^2)$ tightly bracketed between $L^2/(2+L)$ and $L^2/2$. (b) Normalized ratio $\Delta_{\text{rect}}(L)/(L^2/2)$ converging smoothly to 1 as $L \to 0$.

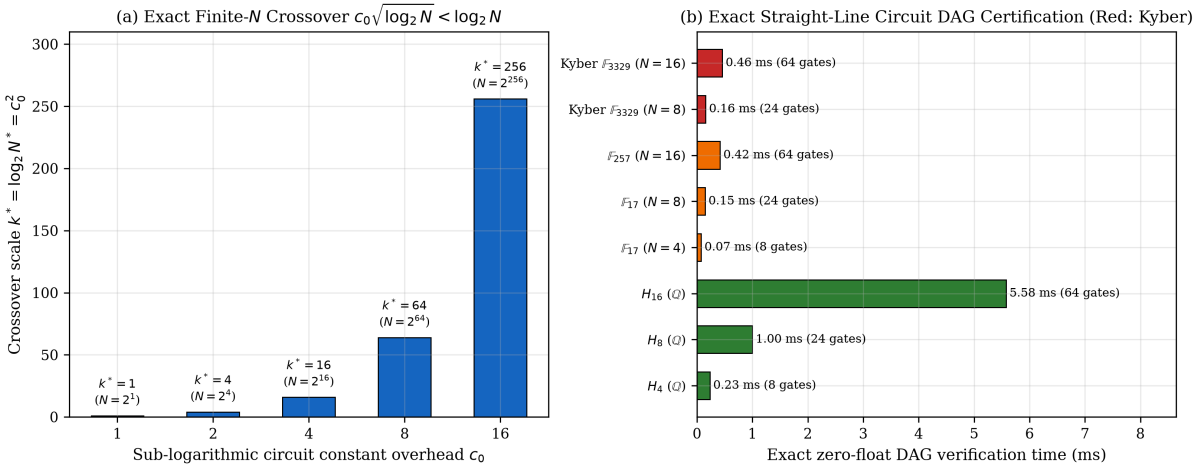


Figure 3: Finite-N crossovers and exact DAG verification. (a) Quadratic crossover scale $k^* = c_0^2$ where $c_0\sqrt{k} < k$. (b) Zero-float verification times for exact acyclic classical Hadamard ($\mathbb{Q}$) and post-quantum Kyber/Fermat NTT ($\mathbb{F}_q$) circuit DAGs up to $N = 16$.