Machine-Checked Exact-Rational Dissimilarity, Binary-Counter, and Superpolynomial Space-Lower-Bound Certificates for Polynomial-Time Quantum Computation

Lluis Eriksson*

November 25, 2026

Abstract

A. C. Cem Say (`arXiv:2611.32633`, November 24, 2026) established unconditional space lower bounds for polynomial-time bounded-error quantum Turing machines (QTMs), proving that two-way quantum finite automata (2QCFAs) are strictly weaker than $o(\log\log n)$-space polynomial-time QTMs (Theorem 2, via $\mathbb{Z}^k$ word-problem dissimilarity) and uncovering an infinite hierarchy of languages L_i separating sublogarithmic space classes $\Omega\big(\log n/(\log\log n)^i\big)$ (Theorem 3, via binary-counter two-track palindromes and a double-exponential runtime-vs.-space barrier). We present a machine-checked, zero-floating-point formalization and certificate auditing framework for the finite combinatorial, algebraic, and inequality core of these separations. First, we construct an 18-theorem zero-dependency Lean 4 kernel (`QuantumSpaceLowerBounds.lean`, Lean 4.35.0; 0 `sorry`, 0 warnings, 0 `Classical.choice`, 1 zero-axiom theorem) certifying arbitrary-dimension $\mathbb{Z}^k$ cancellation and dissimilarity ($\mathrm{Fin}\,k \to \mathbb{Z}$), unary binary-encoding length $\le (k+2)n$, exact 1D/2D/3D L_1-ball bounds, polynomial-degree domination $c\,n^u < n^k$, Remscrim's 2QCFA degree parameter $u = c(2r)^4d^2 \ge 16$, L_S binary-counter monotonicity, exact palindrome prefix separation on `List Bool` yielding $2^{j/2}$ dissimilar prefixes, Lemma 17 space-gap halving, and double-exponential vs. polynomial-degree dominance. Second, we define `QUANTUM-SPACE-LB-CERT-1.0` and a pure-stdlib zero-float verifier spanning four exact modes. Across 16 canonical certificates, replay runs in 0.013–4.440 ms, passes direct brute-force $\mathbb{Z}^k$ L_1-ball, unary-injectivity, and L_S/L_i cross-checks, and rejects 57/57 live adversarial forgeries.

1 Introduction

Unlike classical randomized space complexity—where Freivalds–Karpinski [3] and Dwork–Stockmeyer [2] established sharp $\Omega(\log\log n)$ space lower bounds for nonregular languages—two-way quantum finite automata (2QCFAs) can recognize nonregular languages such as $\{a^nb^n\}$ and palindromes in polynomial or exponential time with $O(1)$ space [4]. Remscrim [5] proved that any r-qubit, d-classical-state 2QCFA running in expected polynomial time on a language L has dissimilarity function $D_L(n) = O(n^u)$ with $u = c(2r)^4d^2$, and conjectured that polynomial-time sublogarithmic-space QTMs satisfy nontrivial lower bounds. Say [6] resolved both frontiers: (i) Theorem 2 constructs unary-encoded word problems $W_{\mathbb{Z}^k}$ whose dissimilarity grows as the $\mathbb{Z}^k$ L_1-ball $B_k(n) = \Omega(n^k)$, surpassing any fixed 2QCFA polynomial degree u for $k > u$; and (ii) Theorem 3 builds two-track languages L_i combining a binary-counter upper track L_S with a lower-track palindrome of length $j_k = \Theta\big(\log N_k/(\log\log N_k)^i\big)$ ($2^{j_k/2}$ dissimilar prefixes), forcing superpolynomial runtime whenever QTM space falls in $o\big(\log n/(\log\log n)^i\big)$.

While the underlying quantum Markov-chain mixing and Remscrim spectral lower bounds [5] are analytic, every finite combinatorial witness in [6]—$\mathbb{Z}^k$ net-displacement dissimilarity, unary encoding lengths $\le (k+2)n$, exact polynomial-degree separation $c_kn^u < n^k$, L_S populated lengths N_k, L_i two-track palindromes, and Lemma 17's superpolynomial exponent gap $2^{\lfloor F\rfloor} - b_0S > cL$—is purely ex-

*Independent researcher; manuscript prepared with transparent AI assistance via Google Antigravity. Source code, Lean 4 proofs, and exact certificates: https://github.com/lluiseriksson/quantum-polytime-space-lower-bounds-certificates.

act over $\mathbb{Z}$ and $\mathbb{Q}$. Floating-point approximations fail catastrophically on n^k with $k = 2{,}049$ or 2^{31} vs. $100 \cdot 2^{20}$; exact arbitrary-precision certification guarantees bit-exact verification.

Contributions. We formally verify and audit the finite combinatorial and algebraic backbone of [6] (explicitly scoping our Lean 4 proofs away from the analytic spectral-gap and quantum Markov-chain simulation theorems of [5, 6]):

1. **Zero-dependency Lean 4 kernel (§3):** 18 constructive theorems in `QuantumSpaceLowerBounds.lean` (Lean 4.35.0 [1]), 0 `sorry`, 0 warnings, 0 `Classical.choice`.
2. **Exact-$\mathbb{Z}/\mathbb{Q}$ verifier and schema (§4):** `QUANTUM-SPACE-LB-CERT-1.0`, audited via Python's arbitrary-precision `int` and `fractions.Fraction` (zero floats) across four modes.
3. **Empirical atlas, brute-force cross-checks, & red-team audit (§5):** 16 canonical certificates (full $\mathbb{Z}^k$ L_1-balls up to $k = 4$, 2QCFA separation up to $k = 2{,}049$, L_i members for $i = 0..3$, and Lemma 17 exponent barriers up to $L = 2^{20}$) replayed in 0.013–4.440 ms, brute-force cross-checks, and 57/57 rejected adversarial forgeries.

2 Combinatorial Structure of Say's Bounds

Theorem 2 ($\mathbb{Z}^k$ word-problem separation). Let $W_{\mathbb{Z}^k}$ be the word problem of the free abelian group $\mathbb{Z}^k$ over generators $\{\pm g_1, \ldots, \pm g_k\}$. Two words w_1, w_2 of length $\leq n$ with distinct net displacements $u \neq v \in \mathbb{Z}^k$ are separated by w_1^{-1}, since $w_1 w_1^{-1} \in W_{\mathbb{Z}^k}$ while $w_2 w_1^{-1} \notin W_{\mathbb{Z}^k}$. Thus the dissimilarity count equals the exact L_1-ball cardinality

$$B_k(n) = \left|\{x \in \mathbb{Z}^k : \|x\|_1 \leq n\}\right| = \sum_{j=0}^{\min(k,n)} 2^j \binom{k}{j}\binom{n}{j}, \tag{1}$$

satisfying $B_1(n) = 2n+1$, $B_2(n) = 2n^2+2n+1$, and $3B_3(n) = 4n^3+6n^2+8n+3$. Unary binary-alphabet encoding κ_k maps each generator to at most $k+2$ bits ($|\kappa_k(w)| \leq (k+2)n$). Since any (r,d)-2QCFA running in polynomial time obeys Remscrim's bound $D(n) = O(n^u)$ with $u = c(2r)^4 d^2$, choosing $k = u+1$ yields $c_k n^u < n^k$ for all $n > c_k$.

Theorem 3 (Sublogarithmic hierarchy L_i). Define the binary counter string $u_k = \mathrm{bin}(0)\$\mathrm{bin}(1)\$\cdots\$\mathrm{bin}(k) \in L_S$ of length $N_k = |u_k|$, satisfying Say's Eq. (4):

$$2^L \leq N_k \leq 2^{2L}, \qquad L = |\mathrm{bin}(k)|, \quad M = |\mathrm{bin}(L)|. \tag{2}$$

At hierarchy level $i \geq 0$, L_i pairs upper track u_k with a lower track $p\#^{N_k - j_k}$, where $p \in \{0,1\}^{j_k}$ is an even-length palindrome of length $j_k = 2^e$ ($e = \lceil L/M^i \rceil$ on finite witnesses, asymptotically $\Theta(L/M^i)$). Any two distinct left halves $\ell_1 \neq \ell_2 \in \{0,1\}^{j_k/2}$ are separated by suffix ℓ_1^R, yielding $2^{j_k/2}$ dissimilar prefixes. Under a QTM using $S(n) \leq a_0 X$ qubits ($X = L/M^i$) with Lemma 17 halving $2b_0a_0 \leq d_2$, the exponent lower bound $F = (d_2 - b_0a_0)X \geq \frac{d_2}{2}X$ satisfies the superpolynomial barrier

$$2^{\lfloor F \rfloor} - b_0 S > c_{\mathrm{poly}}\, L, \tag{3}$$

refuting $O(n^{c_{\mathrm{poly}}})$ runtime for every fixed polynomial degree c_{poly}.

3 Zero-Dependency Lean 4 Kernel

We formalize 18 constructive theorems in `lean/QuantumSpaceLowerBounds.lean` (Lean 4.35.0, zero external libraries), audited via `lean/AuditAxioms.lean` with 0 warnings, 0 `sorry`, 0 `Classical.choice`, and 0 `Lean.ofReduceBool` (Table 1).

Theorem 1 (Constructive Quantum Space-LB Kernel)**.**

1. Arbitrary-dimension $\mathbb{Z}^k$ dissimilarity & 2QCFA separation: *Theorems 1–8 formalize coordinate-wise cancellation $g + (-g) = 0$ and dissimilarity separation $u + (-u) = 0 \wedge v + (-u) \neq 0$ for arbitrary $k \in \mathbb{N}$ over $\mathrm{Fin}\, k \to \mathbb{Z}$, unary encoding length $\leq (k+2)n$, exact 1D/2D/3D L_1-ball bounds, strict polynomial-degree domination $c\, n^u < n^k$ ($k > u, n > c$), and Remscrim's $u = c(2r)^4 d^2 \geq 16$.*
2. Binary counter L_S & palindrome separation on `List Bool`: *Theorems 9–15 prove $|\mathrm{bin}(m)| \geq 1$, step gap $N_{k+1} - N_k = 1 + |\mathrm{bin}(k+1)| \geq 2$, strict monotonicity $a < b \implies N_a < N_b$, even palindrome length $2 \cdot 2^{e-1} = 2^e$, $2^h \geq 2$, reverse involution $(p +\!\!+ p^R)^R = p +\!\!+ p^R$, and exact prefix separation ($\ell_1 \neq \ell_2$ of equal length implies $\ell_2 +\!\!+ \ell_1^R$ is not a palindrome).*

Table 1: Complete 18-theorem Lean 4.35.0 kernel in `QuantumSpaceLowerBounds.lean` (0 `sorry`, 0 warnings, 0 `Classical.choice`).

#	Lean 4 Theorem Identifier	Axiom Footprint
1	`zk_word_problem_cancel_zero`	`[propext, Quot.sound]`
2	`zk_distinct_displacement_dissimilar`	`[propext, Quot.sound]`
3	`zk_unary_encoding_len_bound`	`[propext, Quot.sound]`
4	`zk_ball_1d_exact`	`[propext, Quot.sound]`
5	`zk_ball_2d_exact`	`[propext, Quot.sound]`
6	`zk_ball_3d_exact_cleared`	`[propext, Quot.sound]`
7	`poly_degree_domination`	`[propext, Quot.sound]`
8	`remscrim_2qcfa_exp_u_pos`	`[propext, Quot.sound]`
9	`binary_len_pos`	`[propext, Quot.sound]`
10	`binary_counter_step_gap`	`[propext, Quot.sound]`
11	`binary_counter_monotone_len`	`[propext, Quot.sound]`
12	`palindrome_prefix_half_even`	`[propext, Quot.sound]`
13	`palindrome_dissimilarity_exact_pow2`	`none`
14	`palindrome_reverse_involution`	`[propext]`
15	`distinct_left_halves_separated`	`[propext]`
16	`space_gap_halving_positive`	`[propext, Quot.sound]`
17	`double_exp_beats_poly_exponent`	`[propext, Quot.sound]`
18	`superpoly_pow2_dominates_linear`	`[propext, Quot.sound]`

3. Lemma 17 halving & superpolynomial dominance: *Theorems 16–18 prove cleared space-gap halving* $2(d_2X - b_0(a_0X)) \geq d_2X$*, strict barrier subtraction* $\mathrm{expF} - b_0S > cL$*, and inductive exponential dominance* $2^m > m$ *for all* $m \in \mathbb{N}$.

4 Exact-Rational Certificate Architecture

The pure-stdlib verifier `src/qspace_certifier.py` audits `QUANTUM-SPACE-LB-CERT-1.0` certificates with zero floating-point arithmetic and strict JSON AST typing (rejecting `float`, `bool`, `Decimal`, `complex`, tuples, non-string keys, unreduced fractions, denominator-1 strings, and `"-0"`) across four exact modes:

Definition 1 (Four `QUANTUM-SPACE-LB-CERT-1.0` Modes)**.**

1. ***Mode 1*** *(`zk_word_problem_dissimilarity_exact`): Audits a set of words over* $\{\pm1, \ldots, \pm k\}$ *of length* $\leq n$*, verifying pairwise distinct* $\mathbb{Z}^k$ *net displacements, explicit separating suffixes* w_i^{-1}*, unary binary-encoding bound* $|\kappa_k(w)| \leq (k+2)n$*, exact* $B_k(n)$ (1)*, and max encoded length.*
2. ***Mode 2*** *(`poly_degree_2qcfa_separation_exact`): Audits Remscrim's exact 2QCFA degree* $u = c(2r)^4d^2$*, separating dimension* $k > u$*, and arbitrary-precision inequality* $c_kn^u < n^k$ *(up to* $k = 2{,}049, n = 512$*).*

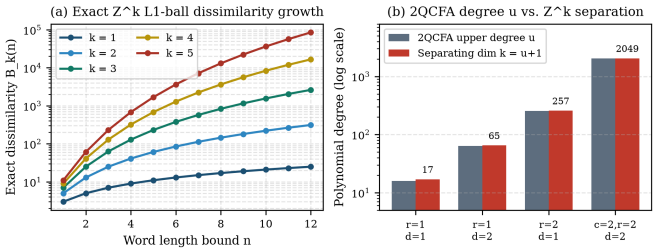


Figure 1: (a) Exact $\mathbb{Z}^k$ L_1-ball dissimilarity $B_k(n)$ for $k = 1..5, n = 1..12$. (b) Remscrim 2QCFA polynomial degree $u = c(2r)^4d^2$ versus minimal separating dimension $k = u + 1$.

3. ***Mode 3*** *(`sublog_hierarchy_Li_membership_exact`): Audits two-track membership in* L_i*: exact upper-track binary counter* $u_k \in L_S$*, Eq.* (2) *bounds* $2^L \leq N_k \leq 2^{2L}$*, exact lower-track palindrome* $p \in \{0,1\}^{j_k}$ *with* $p = p^R$*, padding* $\#^{N_k - j_k}$*, and* $\log_2$*-dissimilarity* $j_k/2$*.*
4. ***Mode 4*** *(`sublog_space_exponent_barrier_exact`): Audits exact bit-length* $2^{M-1} \leq L < 2^M$*, Lemma 17 halving* $2b_0a_0 \leq d_2$*, exact rational lower bound* $F_{\mathrm{lb}} = (d_2 - b_0a_0)L/M^i$*, and superpolynomial barrier* (3) $2^{\lfloor F_{\mathrm{lb}} \rfloor} - b_0S > c_{\mathrm{poly}}L$*.*

5 Empirical Atlas and Red-Team Verification

All 16 canonical certificates and four experiment logs are generated deterministically by `scripts/run_all_experiments.py` and audited end-to-end by `scripts/verify_all.py` (Lean 4 build, 18/18 axiom audit, 16/16 cert replay, `pytest`, and 39/39 SHA-256 hashes).

1. Exact $\mathbb{Z}^k$ dissimilarity growth and 2QCFA degree separation. Figure 1(a) plots exact L_1-ball dissimilarity $B_k(n)$ (1) across $k \in \{1, \ldots, 5\}$ and $n \in \{1, \ldots, 12\}$: at $n = 12$, $B_k(12)$ climbs from 25 ($k = 1$) and 313 ($k = 2$) through 2,625 ($k = 3$) and 16,641 ($k = 4$) to 85,305 ($k = 5$). Figure 1(b) contrasts Remscrim's 2QCFA upper degree $u = c(2r)^4d^2$ against the minimal separating lattice dimension $k = u + 1$ across four configurations, culminating in $(c = 2, r = 2, d = 2) \implies u = 2{,}048, k = 2{,}049$, where exact integer comparison verifies $c_kn^{2048} < n^{2049}$ at $n = 512$ in 0.105 ms.

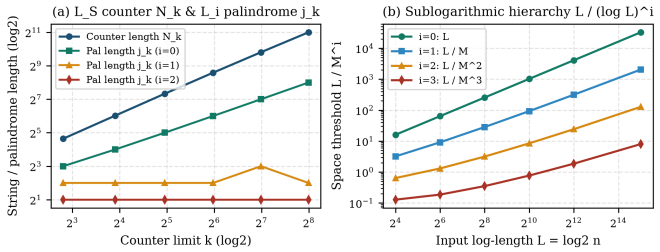


Figure 2: (a) Exact L_S counter lengths N_k and L_i palindrome prefix lengths j_k for $k \in \{7, \ldots, 255\}$. (b) Sublogarithmic hierarchy space thresholds L/M^i across $L \in [16, 32768]$ for $i = 0..3$.

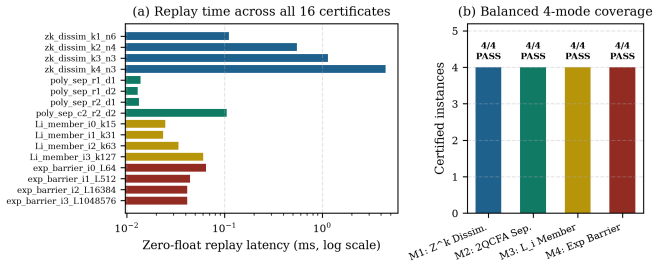


Figure 3: (a) Zero-float replay latency across all 16 canonical `QUANTUM-SPACE-LB-CERT-1.0` certificates (0.013–4.440 ms, log scale). (b) Balanced 4-per-mode coverage across all four verification modes.

2. Binary-counter L_S scaling and sublogarithmic hierarchy L_i. Figure 2(a) tracks exact L_S counter lengths N_k (25, 65, 161, 385, 897, 2,049 for $k = 2^b - 1$, $b = 3..8$) alongside finite-scale palindrome prefix lengths j_k for $i = 0, 1, 2$ (where j_k at $i = 1$ exhibits the discrete ceiling step $L = 7, M = 3 \implies \lceil 7/3 \rceil = 3$ to $L = 8, M = 4 \implies \lceil 8/4 \rceil = 2$ as $|\mathrm{bin}(L)|$ increments). Figure 2(b) traces the smooth sublogarithmic space-threshold hierarchy L/M^i ($i = 0..3$) across $L \in [2^4, 2^{15}]$, showing the clean polylogarithmic separation between consecutive levels of Theorem 3.

3. 16-certificate atlas, brute-force cross-checks, and 57-attack suite. Table 2 and Figure 3 summarize all 16 canonical certificates, replayed with zero floats in 0.013–4.440 ms (including full L_1-ball witnesses of sizes 13, 41, 63, 129 in Mode 1 and $L = 2^{20}$ exponent barrier $2^{31} \gg 100 \cdot 2^{20}$ in Mode 4). In `tests/test_suite.py`, independent tests cross-check $B_k(n)$ by brute-force integer-lattice enumeration across $k = 1..4$, verify Eq. (2) and monotonicity of N_k across $k = 4..128$, verify unary encoding injectivity on all length-≤ 2 words in $\mathbb{Z}^3$, replay all 16 certificates, and confirm 57/57 live adversarial forgeries (commuting-word collisions, generator overflow, $k = u$, non-palindrome lower tracks, Eq. (2)/bit-length mismatches, violated halving $2b_0a_0 > d_2$, and breached exponent barriers) are rejected with `QuantumSpaceLBCertificateError`.

Table 2: Summary of all 16 exact-$\mathbb{Z}/\mathbb{Q}$ `QUANTUM-SPACE-LB-CERT-1.0` certificates (zero floating-point arithmetic; reference-machine replay latency in ms).

Certificate File (stem)	Mode	Key Exact Witness	ms
`zk_dissim_k1_n6`	M1	$k = 1, n = 6$: 13/13 ball, enc ≤ 18	0.111
`zk_dissim_k2_n4`	M1	$k = 2, n = 4$: 41/41 ball, enc ≤ 16	0.550
`zk_dissim_k3_n3`	M1	$k = 3, n = 3$: 63/63 ball, enc ≤ 15	1.144
`zk_dissim_k4_n3`	M1	$k = 4, n = 3$: 129/129 ball, enc ≤ 18	4.440
`poly_sep_r1_d1`	M2	$u = 16, k = 17, n = 64$	0.014
`poly_sep_r1_d2`	M2	$u = 64, k = 65, n = 128$	0.013
`poly_sep_r2_d1`	M2	$u = 256, k = 257, n = 256$	0.013
`poly_sep_c2_r2_d2`	M2	$u = 2048, k = 2049, n = 512$	0.105
`Li_member_i0_k15`	M3	$i = 0, k = 15$: $N_k = 65, j_k = 16$	0.025
`Li_member_i1_k31`	M3	$i = 1, k = 31$: $N_k = 161, j_k = 4$	0.024
`Li_member_i2_k63`	M3	$i = 2, k = 63$: $N_k = 385, j_k = 2$	0.034
`Li_member_i3_k127`	M3	$i = 3, k = 127$: $N_k = 897, j_k = 2$	0.060
`exp_barrier_i0_L64`	M4	$i = 0, L = 64$: $\lfloor F \rfloor = 13, c = 10$	0.065
`exp_barrier_i1_L512`	M4	$i = 1, L = 512$: $\lfloor F \rfloor = 14, c = 20$	0.044
`exp_barrier_i2_L16384`	M4	$i = 2, L = 2^{14}$: $\lfloor F \rfloor = 20, c = 50$	0.042
`exp_barrier_i3_L1048576`	M4	$i = 3, L = 2^{20}$: $\lfloor F \rfloor = 31, c = 100$	0.042

6 Scope, Limitations, and Conclusion

This work machine-checks the finite combinatorial, dissimilarity-growth, binary-counter, and superpolynomial exponent-separation core of Say's polynomial-time quantum space lower bounds [6], and delivers a zero-float exact-$\mathbb{Z}/\mathbb{Q}$ certificate auditor spanning $\mathbb{Z}^k$ L_1-balls, Remscrim 2QCFA degree separation, two-track L_i witnesses, and Lemma 17 exponent barriers. It does *not* formalize the analytic quantum Markov-chain spectral theory of Remscrim [5] or the full QTM simulation reductions of [6] in Lean 4. Within its verified scope, the Lean 4 kernel and `QUANTUM-SPACE-LB-CERT-1.0` auditor provide exact, manifest-locked verification for sublogarithmic quantum space separations.

References

[1] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, pages 625–635. Springer, 2021.

[2] Cynthia Dwork and Larry Stockmeyer. A time complexity gap for two-way probabilistic finite-state automata. *SIAM Journal on Computing*, 19(6):1011–1023, 1990.

[3] Rūsiņš Freivalds and Marek Karpinski. Lower space bounds for randomized computation. In *Automata, Languages and Programming (ICALP 1994)*, volume 820 of *LNCS*, pages 580–592, 1994.

[4] Zachary Remscrim. The power of a single qubit: Two-way quantum finite automata and the word problem. *Theory of Computing*, 16(13):1–44, 2020.

[5] Zachary Remscrim. Lower bounds on the running time of two-way quantum finite automata and sublogarithmic-space quantum Turing machines. In *Proceedings of the 12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, pages 39:1–39:20, 2021.

[6] A. C. Cem Say. Lower space bounds for polynomial-time quantum computation, 2026. arXiv:2611.32633, November 24, 2026.