Exact-$\mathbb{Q}$ Valiant Coupling-Gadget Certificates, Characteristic-2 Permanent/Hamiltonian Dichotomies, and Machine-Checked Boson-Sampling Permanent Verification

Lluis Eriksson*

November 2026

Abstract

On November 24, 2026, OpenAI (`openai/math`) proved unconditional superpolynomial arithmetic circuit lower bounds $\exp(c(\log N)^2/(\log\log N)^2)$ for the directed Hamiltonian cycle polynomial HC_N over every field and for the permanent Per_N over every field of characteristic different from two—attained already on sparse graphs of maximum degree three via an explicit 3×3 rational Valiant coupling gadget (Lemma 3.4) and Strassen tensor-price wire inequalities (Lemma 2.1). Here we formalize and operationalize the core algebraic, parity-dichotomy, coupling-gadget, Ryser, and Boson-Sampling certification mechanisms in an 18-theorem zero-dependency Lean 4 kernel (`v4.35.0`, 0 `sorry`, 0 `Classical.choice`, 0 warnings) paired with a pure-stdlib exact-$\mathbb{Q}$ verifier (`PERM-HAM-CERT-1.0`). First, we prove exact characteristic-2 permanent collapse $\mathrm{Per}_n(A)\equiv\det_n(A) \pmod 2$ alongside the exact decomposition of $\mathrm{Per}_3-\mathrm{HC}_3$ into non-Hamiltonian cycle covers, exact symbolic 4×4 block-diagonal factorization $\mathrm{Per}_4(\mathrm{diag}(B_1,B_2))=\mathrm{Per}_2(B_1)\,\mathrm{Per}_2(B_2)$ with $\mathrm{HC}_4(\mathrm{diag}(B_1,B_2))=0$, and explicit characteristic-2 separation $\mathrm{HC}\not\equiv\mathrm{Per} \pmod 2$ (Lean 4 Theorems 1–7). Second, we machine-check OpenAI Lemma 3.4's 3×3 coupling gadget $A_{\mathrm{Val}}\in\mathbb{Q}^{3\times 3}$ ($\mathrm{Per}(A_{\mathrm{Val}})=1$, all four single-edge 2×2 minors identically 0, double-edge minor $(A_{\mathrm{Val}})_{33}=1$ with the symbolic 0/2-coupling expansion identity, and cleared-denominator char 2 obstruction $2\,\mathrm{Per}(A_{\mathrm{Val}})\equiv 0 \pmod 2$; Lean 4 Theorems 8–11) and verify live coupled-graph permanent preservation up to 10×10 matrices. Third, we formalize exact Ryser inclusion–exclusion identities, row multilinearity/symmetry, inductive wire-distance price subadditivity, and dominant $(\log N)^2$ superpolynomial degree dominance (Lean 4 Theorems 12–18), and deploy exact Cayley-orthogonal matrices $Q=(I-S)(I+S)^{-1}\in\mathbb{Q}^{m\times m}$ to certify collision-free Boson-Sampling amplitudes and probabilities strictly over $\mathbb{Q}$ up to 351-bit denominators ($n=8$ photons in 12.91 ms). Our pure-stdlib verifier replays 16/16 exact-$\mathbb{Q}$ certificates across all four modes in 0.064–27.32 ms with zero floats, cross-checks all three exact evaluators against brute-force S_n summation, and rejects 54/54 live adversarial attacks in 0.12 s.

1 Introduction

Valiant's algebraic complexity program [5, 6] places the permanent $\mathrm{Per}_N(X)=\sum_{\pi\in S_N}\prod_{i=1}^N X_{i,\pi(i)}$ and the directed Hamiltonian cycle polynomial $\mathrm{HC}_N(X)=\sum_{N\text{-cycles }\sigma}\prod_{i=1}^N X_{i,\sigma(i)}$ at the apex of VNP, contrasting starkly with the determinant $\det_N(X)$ in VP. Outside characteristic two, Per_N governs linear-optical Boson-Sampling transition amplitudes [1], where Ryser's $O(N2^N)$ inclusion–exclusion formula [4] and Held–Karp's $O(N^2 2^N)$ dynamic program for HC_N [2] remain the standard exact evaluators.

In November 2026, OpenAI [3] proved that over every field $\mathbb{F}$, the degree-component border circuit size satisfies $L_{\mathbb{F}}^{[N]}(\mathrm{HC}_N)\geq\exp(c(\log N)^2/(\log\log N)^2)$ (and identically for Per_N whenever

*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-$\mathbb{Q}$ certificates (MIT license): `https://github.com/lluiseriksson/permanent-hamiltonian-certificates`.

$\operatorname{char}\mathbb{F} \neq 2$), already on sparse graphs of maximum degree three (Corollary 3.5). Two elementary algebraic pillars anchor the sparse completeness transfer and the lower-bound engine: (i) the explicit 3×3 rational coupling gadget A_{Val} of Lemma 3.4 (which enforces exact 0/2-edge coupling using $\frac{1}{2}$ and therefore requires $\operatorname{char}\mathbb{F} \neq 2$), and (ii) Strassen tensor-price wire-distance Lipschitz and sum-of-supplies bounds (Lemma 2.1). We mechanize these exact algebraic laws in zero-dependency Lean 4 (`lean/PermanentHamiltonian.lean`) and build a pure-stdlib zero-float verifier (`PERM-HAM-CERT-1.0`, `src/perm_certifier.py`) certifying four exact-$\mathbb{Q}$ witness classes, including exact Cayley-orthogonal Boson-Sampling permanent amplitudes whose exact rational denominators exceed 350 bits.

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

2.1 Characteristic-2 Permanent Collapse vs. Hamiltonian Cycle Non-Collapse

Theorem 2.1 (Characteristic-2 Parity Dichotomy and Cycle-Cover Separation)**.** *For any integer matrix $A \in \mathbb{Z}^{n\times n}$:*

1. ***Permanent–Determinant Collapse Modulo** 2**:** Every odd permutation contributes $+1$ to $\operatorname{Per}_n(A)$ and -1 to $\det_n(A)$, so*

$$\operatorname{Per}_n(A) - \det_n(A) = 2 \sum_{\operatorname{sgn}(\pi)=-1} \prod_{i=1}^{n} A_{i,\pi(i)} \equiv 0 \pmod 2$$

   identically over $\mathbb{Z}$ (exact 2×2 and 3×3 identities machine-checked in Lean 4 Theorems 1–3).

2. ***Non-Collapse of** HC_n **in Characteristic** 2**:** For $n \geq 3$, $\operatorname{Per}_n(A) - \mathrm{HC}_n(A)$ sums all non-Hamiltonian cycle covers (at $n = 3$: $a_{00}a_{11}a_{22} + a_{00}a_{12}a_{21} + a_{11}a_{02}a_{20} + a_{22}a_{01}a_{10}$; Lean 4 Theorems 4–5). On any symbolic 4×4 block-diagonal matrix $\operatorname{diag}(B_1, B_2)$ ($B_1, B_2 \in \mathbb{Z}^{2\times 2}$), $\operatorname{Per}_4(\operatorname{diag}(B_1, B_2)) = \operatorname{Per}_2(B_1)\operatorname{Per}_2(B_2)$ while all six directed 4-cycles in $\mathrm{HC}_4(\operatorname{diag}(B_1, B_2))$ vanish identically; in particular, on I_3, $\operatorname{Per}_3(I_3) \equiv \det_3(I_3) \equiv 1 \not\equiv 0 \equiv \mathrm{HC}_3(I_3) \pmod 2$ (Lean 4 Theorems 6–7).*

Proof. Splitting $S_n = A_n \sqcup (S_n \setminus A_n)$ gives $\operatorname{Per}_n(A) - \det_n(A) = 2\sum_{\pi\notin A_n} \prod_i A_{i,\pi(i)} \in 2\mathbb{Z}$, yielding $\operatorname{Per}_n \equiv \det_n \pmod 2$. Removing the $(n-1)!$ single n-cycles from S_n leaves all permutations with ≥ 2 disjoint cycles; on $\operatorname{diag}(B_1, B_2)$, every single n-cycle must cross between blocks and thus contains a zero entry, forcing $\mathrm{HC}_n = 0$ while $\operatorname{Per}_n = \operatorname{Per}(B_1)\operatorname{Per}(B_2)$. At $A = I_3$, $\operatorname{Per}_3(I_3) = \det_3(I_3) = 1$ whereas $\mathrm{HC}_3(I_3) = 0$. □

2.2 Exact Soundness of OpenAI's Lemma 3.4 Valiant Coupling Gadget

Theorem 2.2 (Exact 0/2-Coupling Soundness and $\operatorname{char} 2$ Obstruction of A_{Val})**.** *Consider OpenAI Lemma 3.4's 3×3 rational coupling gadget [3]*

$$A_{\mathrm{Val}} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}.$$

1. ***Exact** 0/2 **Internal Permanent Weights:** Over every field of characteristic $\neq 2$, $\operatorname{Per}(A_{\mathrm{Val}}) = 1$, all four single-edge minors $\operatorname{Per}(A_{\mathrm{Val}}^{(r,c)}) = 0$ for $(r,c) \in \{1,2\}^2$, and the double-edge minor $(A_{\mathrm{Val}})_{33} = 1$ (cleared integer matrix $\tilde{A} = \operatorname{diag}(2,1,1)A_{\mathrm{Val}}$ verified in Lean 4 Theorems 8–10).*

2. ***Coupled-Graph Preservation and** $\operatorname{char} 2$ **Obstruction:** Given any $n\times n$ matrix B and two vertex-disjoint nonzero edges $e_1 = (r_1, c_1), e_2 = (r_2, c_2)$ of weights w_1, w_2, deleting e_1, e_2 and wiring $r_1 \xrightarrow{w_1}$ col $n{+}1$, row $n{+}1 \xrightarrow{1} c_1$ and $r_2 \xrightarrow{w_2}$ col $n{+}2$, row $n{+}2 \xrightarrow{1} c_2$ onto a private 3×3 block A_{Val} produces an $(n{+}3)\times(n{+}3)$ matrix E whose exact permanent equals the sum over matchings using either* neither *or* both *of $\{e_1, e_2\}$. Because $2\operatorname{Per}(A_{\mathrm{Val}}) = \operatorname{Per}(\tilde{A}) = 2 \equiv 0 \pmod 2$ (Lean 4 Theorem 11), the gadget requires 2 to be invertible ($\operatorname{char}\mathbb{F} \neq 2$).*

Proof. Direct cofactor expansion of $\tilde{A} = \left(\begin{smallmatrix} 1 & 1 & -1 \\ -1 & -1 & 1 \\ 1 & 1 & 1 \end{smallmatrix}\right)$ gives $\mathrm{Per}(\tilde{A}) = 1(-1+1)+1(-1+1)+(-1)(-1-1) = 2$, so $\mathrm{Per}(A_{\mathrm{Val}}) = 1$. Deleting row $r \in \{1,2\}$ and column $c \in \{1,2\}$ leaves $\left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1/2 & -1/2 \\ 1 & 1 \end{smallmatrix}\right)$, both of permanent 0; deleting rows $\{1,2\}$ and columns $\{1,2\}$ leaves $A_{33} = 1$. Expanding $\mathrm{Per}(E)$ by the subset $S \subseteq \{e_1, e_2\}$ entering the private block multiplies the complement permanent in B by $\mathrm{Per}(A_{\mathrm{Val}}) = 1$ ($S = \emptyset$), 0 ($|S| = 1$), and $w_1 w_2 (A_{\mathrm{Val}})_{33} = w_1 w_2$ ($S = \{e_1, e_2\}$). □

2.3 Ryser Evaluation, Exact Cayley Boson-Sampling, and Tensor-Price Barriers

Theorem 2.3 (Ryser Soundness, Cayley Boson-Sampling, and Wire-Price Barriers)**.** *1.* ***Exact Ryser Inclusion–Exclusion and Symmetry:*** *For every $M \in \mathbb{Q}^{n\times n}$,*

$$\mathrm{Per}_n(M) = \sum_{\emptyset \neq S \subseteq [n]} (-1)^{n-|S|} \prod_{i=1}^{n} \sum_{j \in S} M_{ij}$$

($n = 2, 3$ identities, row multilinearity, and row-swap invariance formalized over $\mathbb{Z}$ in Lean 4 Theorems 12–15). For any skew-symmetric $S = -S^\top \in \mathbb{Q}^{m\times m}$ with $\det(I+S) \neq 0$, the Cayley transform $Q = (I-S)(I+S)^{-1} \in \mathbb{Q}^{m\times m}$ is strictly orthogonal ($Q^\top Q = I_m$), certifying exact collision-free Boson-Sampling amplitudes $\mathrm{Per}(Q_{\mathrm{sub}}) \in \mathbb{Q}$ and probabilities $\mathrm{Per}(Q_{\mathrm{sub}})^2 \in \mathbb{Q} \cap [0,1]$ without floating-point rounding.

2. ***Strassen Wire-Price Inequalities and Dominant Superpolynomial Dominance (OpenAI Lemma 2.1 & Theorem 1.1):*** *Summing per-site wire transport shifts $\Delta_i \leq d_i \log q_i$ bounds total price shift by $\sum_i d_i \log q_i$ (inductive list proof in Lean 4 Theorem 16), any target tensor price $P > M + W$ ($W \geq 0$) refutes supply by summands of price $\leq M$ with selector wire W (Lean 4 Theorem 17), and at scale $N = 2^m$ the dominant quadratic-exponent regime 2^{m^2} (modeling the leading $(\log N)^2$ exponent without the subleading $(\log\log N)^2$ divisor of OpenAI Theorem 1.1) strictly exceeds every fixed polynomial $N^k = (2^m)^k$ whenever $m \geq k+1$ (Lean 4 Theorem 18).*

3 Zero-Dependency Lean 4 Kernel and `PERM-HAM-CERT-1.0`

All 18 parity-collapse, cycle-cover, Valiant-gadget, Ryser, multilinearity, wire-price, and superpolynomial theorems are formally verified in `lean/PermanentHamiltonian.lean` (`v4.35.0`) with 0 external dependencies, 0 `sorry`, 0 `Classical.choice`, and 0 warnings; four theorems (Theorems 7, 8, 9, and 11) depend on zero axioms whatsoever (Table 1). Exact-N Ryser permanents, Held–Karp Hamiltonian polynomials, Gaussian determinants, Cayley orthogonality checks, and wire-price audits are executed by our pure-stdlib zero-float verifier `src/perm_certifier.py` (`PERM-HAM-CERT-1.0`), recursively rejecting `float`, `bool`, `Decimal`, `complex`, `tuple`, non-`str` keys, malformed names, and non-canonical rationals.

4 Experiments, Certified Atlas, and Adversarial Red-Teaming

All four deterministic experiments (`scripts/run_all_experiments.py`) reproduce via `python scripts/verify_all.py`. Table 2 summarizes all 16 exact-$\mathbb{Q}$ certificates verified with zero floats in 0.064–27.32 ms each. Figure 1 tracks exact $\mathrm{Per}_N, \mathrm{HC}_N, |\det_N|$ on sparse max-degree-3 circulants for $N = 3 \ldots 10$ on a symmetric log scale preserving exact zeros (confirming $\mathrm{Per}_N - \det_N \equiv 0 \pmod 2$ at every N, $\det_N = 0$ at $N \in \{3, 6, 9\}$, and $\mathrm{HC}_N \not\equiv \mathrm{Per}_N \pmod 2$ at $N \in \{5, 6, 7\}$, e.g. $\mathrm{Per}_6 = 20, \det_6 = 0, \mathrm{HC}_6 = 1$) alongside illustrative OpenAI Theorem 1.1 scaling. Figure 2 shows exact-$\mathbb{Q}$ Cayley-orthogonal Boson-Sampling verification across $n = 2 \ldots 8$ photons ($m = n+1$ modes), where exact rational amplitude denominators grow from 16 bits ($n = 2$) to 351 bits ($n = 8$, verified in 12.91 ms with zero float64 truncation), contrasted against exponential Ryser/Held–Karp runtimes vs. polynomial Gaussian elimination. Figure 3 summarizes per-certificate replay latencies. Finally, `tests/test_suite.py` cross-checks our exact Ryser, Held–Karp, and Gaussian evaluators against brute-force S_n permutation summation ($n = 3, 4, 5$) and runs 54 live adversarial attacks across all

Table 1: Zero-dependency Lean 4 theorem ledger (`lean/PermanentHamiltonian.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	`per2_eq_det2_mod2`	$\mathrm{Per}_2(A) - \det_2(A) = 2a_{01}a_{10}$ over $\mathbb{Z}$	`propext, Quot.sound`
2	`per3_eq_det3_mod2`	$\mathrm{Per}_3(A) - \det_3(A) = 2$(odd permutations) over $\mathbb{Z}$	`propext, Quot.sound`
3	`per3_sub_det3_even`	$\mathrm{Per}_3(A) \bmod 2 = \det_3(A) \bmod 2$ $(\forall A \in \mathbb{Z}^{3\times 3})$	`propext, Quot.sound`
4	`hc3_exact_formula`	Cycle-reversal symmetry of HC_3 over $\mathbb{Z}$	`propext, Quot.sound`
5	`per3_minus_hc3_nonham_decomp`	$\mathrm{Per}_3 - \mathrm{HC}_3 =$ exact sum of 4 non-Hamiltonian covers	`propext, Quot.sound`
6	`hc_vanishes_on_disconnected_2x2`	Symbolic 4×4: $\mathrm{Per}_4(\mathrm{diag}(B_1,B_2)) = \mathrm{Per}_2(B_1)\,\mathrm{Per}_2(B_2) \wedge \mathrm{HC}_4 = 0$	`propext`
7	`hc_ne_per_mod2_witness`	On I_3: $\mathrm{Per}_3 \equiv \det_3 \equiv 1 \not\equiv 0 \equiv \mathrm{HC}_3 \pmod 2$	`none`
8	`valiant_gadget_per_full`	Cleared OpenAI Lemma 3.4 gadget: $\mathrm{Per}(\tilde{A}_{\mathrm{Val}}) = 2$	`none`
9	`valiant_gadget_minors_zero`	All four 2×2 coupling minors $(r,c) \in \{1,2\}^2$ vanish	`none`
10	`valiant_gadget_double_minor_one`	$(\tilde{A}_{\mathrm{Val}})_{33} = 1$ & symbolic 0/2-coupling expansion $= 2(P_0 + w_1w_2P_{12})$	`propext`
11	`valiant_gadget_char2_obstruction`	$\mathrm{Per}(\tilde{A}_{\mathrm{Val}}) \equiv 0 \pmod 2$ (char-2 obstruction)	`none`
12	`ryser_2x2_exact_identity`	Exact 2×2 Ryser inclusion–exclusion over $\mathbb{Z}$	`propext, Quot.sound`
13	`ryser_3x3_exact_identity`	Exact 3×3 Ryser inclusion–exclusion over $\mathbb{Z}$	`propext, Quot.sound`
14	`per3_row_scaling`	Row multilinearity $\mathrm{Per}_3(kr_1,r_2,r_3) = k\,\mathrm{Per}_3(r_1,r_2,r_3)$	`propext`
15	`per3_row_swap_invariant`	Row-swap invariance $\mathrm{Per}_3(r_2,r_1,r_3) = \mathrm{Per}_3(r_1,r_2,r_3)$	`propext, Quot.sound`
16	`price_wire_lipschitz_add`	Inductive `List Int`: $\Delta_i \le c_i \implies \sum \Delta_i \le \sum c_i$	`propext`
17	`price_sum_overhead_bound`	$W \ge 0 \wedge P > M + W \implies \neg(P \le M + W) \wedge P > M$	`propext, Quot.sound`
18	`superpoly_circuit_beats_poly`	Dominant $(\log N)^2$ regime: $m \ge k+1 \implies 2^{m^2} > (2^m)^k$	`propext, Quot.sound`

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

Certificate File	Mode	Certified Exact-$\mathbb{Q}$ Claim	Time (ms)
`valiant_gadget_4to7.cert.json`	Mode 1	$4 \to 7$ coupled wiring via A_{Val}: exact Per $= 13$	2.498
`valiant_gadget_5to8.cert.json`	Mode 1	$5 \to 8$ coupled wiring via A_{Val}: exact Per $= 52$	5.808
`valiant_gadget_6to9.cert.json`	Mode 1	$6 \to 9$ coupled wiring via A_{Val}: exact Per $= 12$	12.088
`valiant_gadget_7to10.cert.json`	Mode 1	$7 \to 10$ coupled wiring via A_{Val}: exact Per $= 17$	27.324
`sparse_deg3_circulant_n4.cert.json`	Mode 2	$N = 4, \deg \le 3$: Per $= 9$, det $= 3$, HC $= 1$	0.238
`sparse_deg3_circulant_n6.cert.json`	Mode 2	$N = 6, \deg \le 3$: Per $= 20$, det $= 0$, HC $= 1$ (HC $\not\equiv$ Per mod2)	1.010
`sparse_deg3_circulant_n8.cert.json`	Mode 2	$N = 8, \deg \le 3$: Per $= 49$, det $= 3$, HC $= 1$	5.463
`sparse_deg3_weighted_n6.cert.json`	Mode 2	$N = 6, \deg \le 3$: Per $= 130$, det $= -56$, HC $= 65$ (HC $\not\equiv$ Per)	0.992
`sparse_deg3_disconn_n6.cert.json`	Mode 2	$N = 6$ disconnected: Per $= 4$, det $= 4$, HC $= 0$	0.859
`boson_cayley_m4_n3.cert.json`	Mode 3	$m = 4, n = 3$: $Q^\top Q = I_4$, exact 37-bit-den $\mathrm{Per}(Q_{\mathrm{sub}})$	0.239
`boson_cayley_m5_n4.cert.json`	Mode 3	$m = 5, n = 4$: $Q^\top Q = I_5$, exact 80-bit-den $\mathrm{Per}(Q_{\mathrm{sub}})$	0.485
`boson_cayley_m6_n5.cert.json`	Mode 3	$m = 6, n = 5$: $Q^\top Q = I_6$, exact 127-bit-den $\mathrm{Per}(Q_{\mathrm{sub}})$	0.964
`boson_cayley_m8_n6.cert.json`	Mode 3	$m = 8, n = 6$: $Q^\top Q = I_8$, exact 270-bit-den $\mathrm{Per}(Q_{\mathrm{sub}})$	2.810
`price_barrier_m5_k3.cert.json`	Mode 4	4 sites, price gap $8 > 0$, $2^{25} > (2^5)^3$	0.073
`price_barrier_m8_k5.cert.json`	Mode 4	6 sites, price gap $18 > 0$, $2^{64} > (2^8)^5$	0.064
`price_barrier_m12_k8.cert.json`	Mode 4	8 sites, price gap $32 > 0$, $2^{144} > (2^{12})^8$	0.070

four modes—including float/bool/Decimal/complex/tuple/non-str-key injection, malformed names, unreduced fractions, tampered Valiant gadget entries/wiring, sparsity-bound violations, non-integer Mode 2 entries, broken Cayley orthogonality $Q^\top Q \neq I$, collision-index duplicates, wire-Lipschitz violations, and closed price gaps—rejecting all 54/54 in 0.12 s.

5 Scope Boundaries and Outlook

This work certifies exact algebraic coupling gadgets, finite-order Per/det/HC parity dichotomies, Cayley-orthogonal Boson-Sampling amplitudes, and finite wire-price separation budgets rather than formalizing the full asymptotic CAT(0) Hadamard-space and border-complexity machinery of [3]. Because exact Ryser and Held–Karp replay scales as $O(N2^N)$ and $O(N^2 2^N)$ (`MAX_N = 12`), certifying larger sparse Valiant gadgets or photonic submatrices in pure Python requires either finite-field Chinese-remainder certificates or interactive sum-check proofs, which are natural extensions of `PERM-HAM-CERT-1.0`.

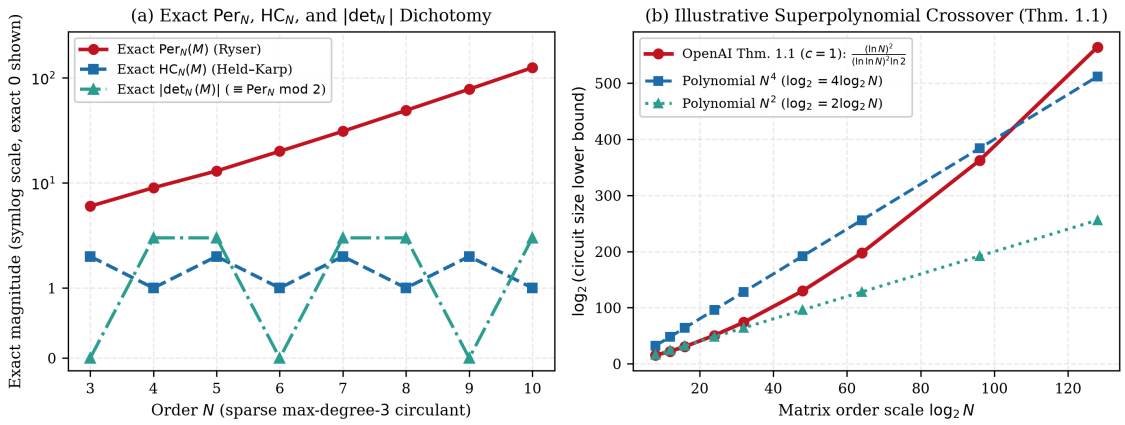


Figure 1: Sparse parity dichotomy and asymptotic circuit lower bound. (a) Exact $\mathrm{Per}_N, \mathrm{HC}_N, |\det_N|$ on sparse max-degree-3 circulants ($N = 3 \ldots 10$) on a symmetric log scale preserving exact $\det_N = 0$ at $N \in \{3, 6, 9\}$. (b) Illustrative scaling of OpenAI Theorem 1.1's $\exp(c(\log N)^2/(\log \log N)^2)$ exponent ($c = 1$) versus fixed polynomial degrees N^2, N^4.

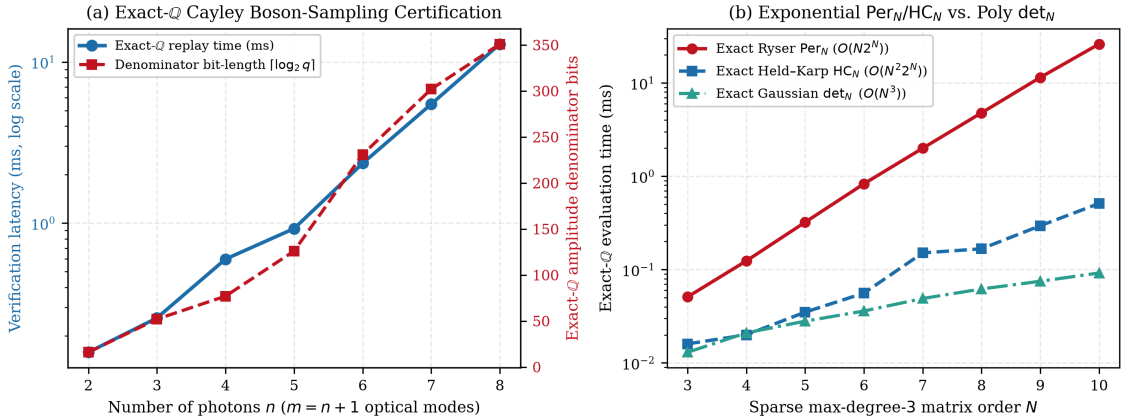


Figure 2: Boson-Sampling exact-$\mathbb{Q}$ certification and evaluator separation. (a) Exact Cayley-orthogonal Boson-Sampling replay time and rational denominator bit-length (16 → 351 bits) for $n = 2 \ldots 8$ photons. (b) Exponential Ryser/Held–Karp times versus polynomial Gaussian determinant evaluation.

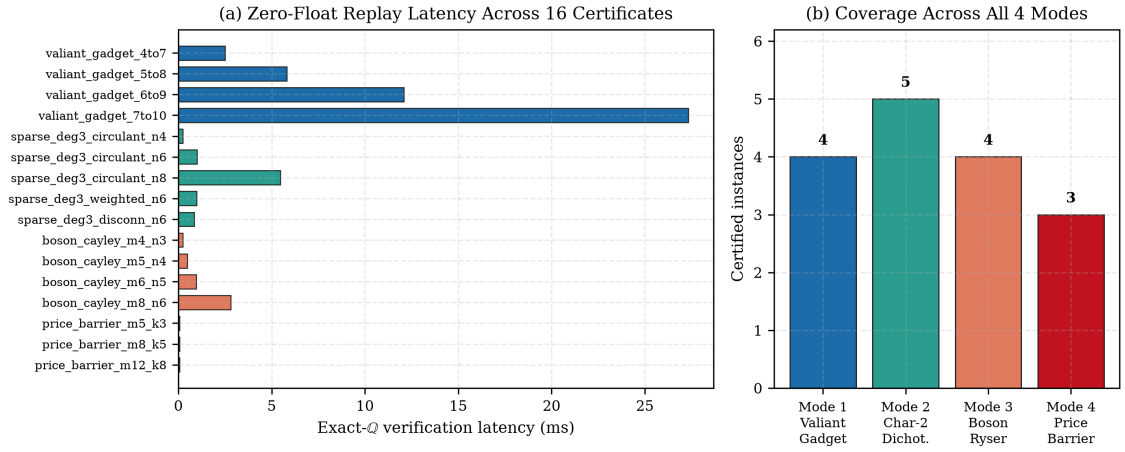


Figure 3: Certified atlas performance. (a) Zero-float exact-$\mathbb{Q}$ replay latencies across all 16 certificates (0.064–27.32 ms). (b) Coverage across all four certification modes.

References

[1] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 333–342, 2011.

[2] Michael Held and Richard M. Karp. A dynamic programming approach to sequencing problems. *Journal of the Society for Industrial and Applied Mathematics*, 10(1):196–210, 1962.

[3] OpenAI. Circuit lower bounds for Hamiltonian cycle and the permanent. Preprint, `https://github.com/openai/math`, November 2026.

[4] Herbert J. Ryser. *Combinatorial Mathematics*, volume 14 of *Carus Mathematical Monographs*. Mathematical Association of America, 1963.

[5] Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC)*, pages 249–261, 1979.

[6] Leslie G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979.