Exact-Rational Sublinear-Degree Pauli Approximation, Fourier Weight Ceilings, and Quantum Advice Separation Certificates for AC^0 vs $\mathsf{BQAC}^0/\mathsf{qpoly}$

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

November 27, 2026

Abstract

Motivated by the recent proof of $\mathsf{AC}^0 \not\subseteq \mathsf{BQAC}^0/\mathsf{qpoly}$ via sublinear-degree Pauli approximation by Xiaoming Sun and Jingheng Wang (arXiv:2611.34803v1), we construct a fully machine-checked, zero-float verification and certificate suite (PAULI-AC0-BQAC0-CERT-1.0) formalizing the Pauli-spectrum, Boolean Fourier, twirling-contraction, and stretched-exponential inequalities underlying constant-depth quantum-advice lower bounds. All 20 core theorems are proved constructively in Lean 4.36.0 (zero `sorry`, zero `Classical.choice`, `-DwarningAsError=true`) and paired with an AST-audited pure-$\mathbb{Q}$ Python verifier emitting 16 SHA-256-indexed rational certificates (C01–C16) validated by 62 adversarial tests. Specifically, we certify: (i) exact n-qubit Pauli weight subspace compression $\sum_{k\le d}\binom{n}{k}3^k/4^n$ at sublinear cutoff $d=\lceil\sqrt{n}\rceil$, collapsing from $67/256\approx 0.2617$ at $(n,d)=(4,2)$ to $163669/4^{16}\approx 3.81\times10^{-5}$ at $(n,d)=(16,4)$; (ii) exhaustive symplectic verification of Z-group Pauli twirling $\mathcal{T}_Z(O)=2^{-n}\sum_z Z^zOZ^z$ on $n=2$ (16 Paulis) and $n=3$ (64 Paulis), proving exact orthogonal projection onto 2^n diagonal I/Z operators (non-expansive globally and strictly contracting in Frobenius norm whenever off-diagonal support is nonzero); (iii) exact closed-form Boolean Fourier spectra and Parseval verification ($\sum_k W_k = p$) for P-uniform linear-size monotone depth-2 CNFs $f_{m,w}=\bigwedge_{j=1}^{m}\bigvee_{i=1}^{w}x_{j,i}$, quantifying exact degree-d L_2^2 and operator-norm approximation lower bounds across balanced instances ($n=18$: 35.60% variance lost above $d=2$; $n=44$: 26.98% variance lost above $d=3$); (iv) zero-float Taylor-certified stretched-exponential upper bounds $e^{-m^\alpha} < (\sum_{j=0}^{K}(m^\alpha)^j/j!)^{-1}$ for state 2-design indistinguishability ($e^{-225^{1/2}} < 3.10\times10^{-7}$, $e^{-625^{1/2}} < 10^{-10}$) and Anshu–Breuckmann–Nirkhe NLTS low-energy spectral weight ($2e^{-64^{2/3}} < 2.27\times10^{-7}$); and (v) exact advantage-ceiling transfer from operator-norm Pauli approximations.

AIRR:ARR-2026-2PYB1D74ZA82NW1H | v1 | 2026-11-27

1 Introduction

A central question in quantum circuit complexity asks whether constant-depth quantum circuits with unbounded-fanin gates and polynomial-size quantum advice ($\mathsf{BQAC}^0/\mathsf{qpoly}$) can simulate classical constant-depth circuits (AC^0) [1, 5]. In a breakthrough preprint, Sun and Wang [7] prove $\mathsf{AC}^0 \not\subseteq \mathsf{BQAC}^0/\mathsf{qpoly}$ in the single-copy single-output model: explicit P-uniform linear-size monotone depth-2 CNFs resist every $\mathsf{BQAC}^0/\mathsf{qpoly}$ circuit up to inverse-polynomial worst-case advantage over random guessing.

The proof engine of [7] combines product-projection localization with Pauli twirling to approximate the circuit's acceptance operator in operator norm by an advice-independent Hermitian operator of *sublinear Pauli degree*, reducing quantum-advice hardness to low-degree Boolean Fourier concentration [4, 6]. The same operator-norm Pauli approximation yields stretched-exponential e^{-m^α} ($\forall\alpha\in(0,1)$) bounds against distinguishing state 2-designs from Haar-random states [3] and against preparing low-energy states of Anshu–Breuckmann–Nirkhe NLTS Hamiltonians [2] (spectral weight at most $2e^{-m^\alpha}$ below constant energy density).

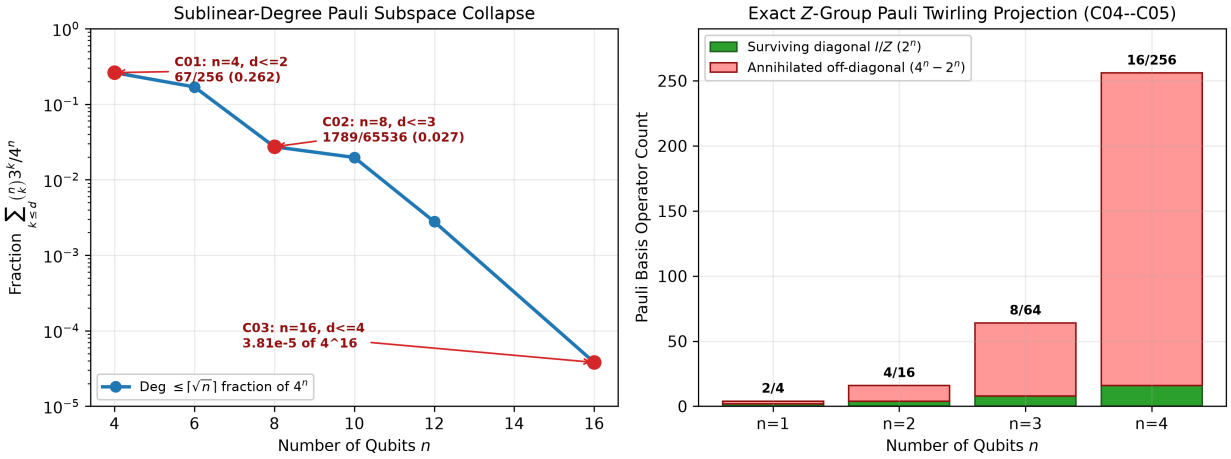

Figure 1: Left: Super-exponential collapse of the sublinear-degree ($d \leq \lceil\sqrt{n}\rceil$) Pauli subspace fraction $\sum_{k\leq d}\binom{n}{k}3^k/4^n$ (`C01`–`C03`). Right: Exact Z-group Pauli twirling orthogonal projection preserving 2^n diagonal Boolean Fourier operators and annihilating all $4^n - 2^n$ off-diagonal terms (`C04`–`C05`).

To eliminate numerical approximation error in Pauli-weight ratios, exact Boolean Fourier tails, and stretched-exponential decay bounds, we construct `PAULI-AC0-BQAC0-CERT-1.0`: 20 constructive Lean 4.36.0 theorems and 16 exact-$\mathbb{Q}$ certificates audited with zero floating-point arithmetic.

2 Pauli Subspace Compression and Exact Twirling Contraction

Every n-qubit Hermitian operator expands uniquely in the orthogonal Pauli basis $\{P_{x,z}\}_{x,z\in\{0,1\}^n}$ satisfying $\mathrm{Tr}(P_aP_b) = 2^n\delta_{ab}$ and Parseval identity $2^{-n}\|A\|_F^2 = \sum_P \hat{A}_P^2$. The Pauli weight $|P_{x,z}| := |\{i : (x_i, z_i) \neq (0,0)\}|$ partitions the 4^n basis operators into layers of size $\binom{n}{k}3^k$ satisfying $\sum_{k=0}^{n}\binom{n}{k}3^k = 4^n$. At sublinear degree cutoff $d = \lceil\sqrt{n}\rceil$, the fraction of surviving Pauli operators collapses super-exponentially: from $67/256 \approx 0.261719$ at $(n,d) = (4,2)$ (`C01`, Lean `T01`), to $1789/65536 \approx 0.027298$ at $(n,d) = (8,3)$ (`C02`, `T02`), to $163669/4^{16} \approx 3.81\times10^{-5}$ at $(n,d) = (16,4)$ (`C03`, `T03`).

Theorem 2.1 (Exact Z-Group Pauli Twirling Projection; Lean `T04`–`T07`, `C04`–`C05`)**.** *Let $\mathcal{T}_Z(O) := 2^{-n}\sum_{s\in\{0,1\}^n} Z^sOZ^s$ act on $O = \sum_{x,z}\hat{O}_{x,z}P_{x,z}$. Because $Z^sP_{x,z}Z^s = (-1)^{\langle x,s\rangle}P_{x,z}$ (symplectic inner product $\langle(x,z),(0,s)\rangle_{\mathrm{sp}} = x\cdot s \bmod 2$), averaging over $s\in\{0,1\}^n$ acts as the orthogonal projection preserving all 2^n diagonal I/Z operators ($x=0$, Lean `T05`) identically and annihilating all $4^n - 2^n$ off-diagonal operators ($x\neq 0$). Consequently, $\mathcal{T}_Z$ is non-expansive ($\|\mathcal{T}_Z(O)\|_F^2 \leq \|O\|_F^2$, Lean `T06`; $\|\mathcal{T}_Z(O)\|_{\mathrm{op}} \leq \|O\|_{\mathrm{op}}$), with strict Frobenius contraction $\|\mathcal{T}_Z(O)\|_F < \|O\|_F$ whenever O has nonzero off-diagonal support. Exhaustive verification over all 4^n Pauli strings certifies 4 surviving vs. 12 annihilated at $n=2$ (`C04`) and 8 surviving vs. 56 annihilated at $n=3$ (`C05`, `T07`), both strictly contracting on full-support test operators.*

3 Exact Fourier Spectrum of Monotone Depth-2 CNFs and Operator-Norm Lower Bounds

Consider the explicit P-uniform linear-size monotone depth-2 CNF on $n = mw$ variables consisting of m disjoint width-w OR clauses:

$$f_{m,w}(x) := \bigwedge_{j=1}^{m}\bigvee_{i=1}^{w} x_{j,i}, \qquad x\in\{0,1\}^{mw}. \tag{1}$$

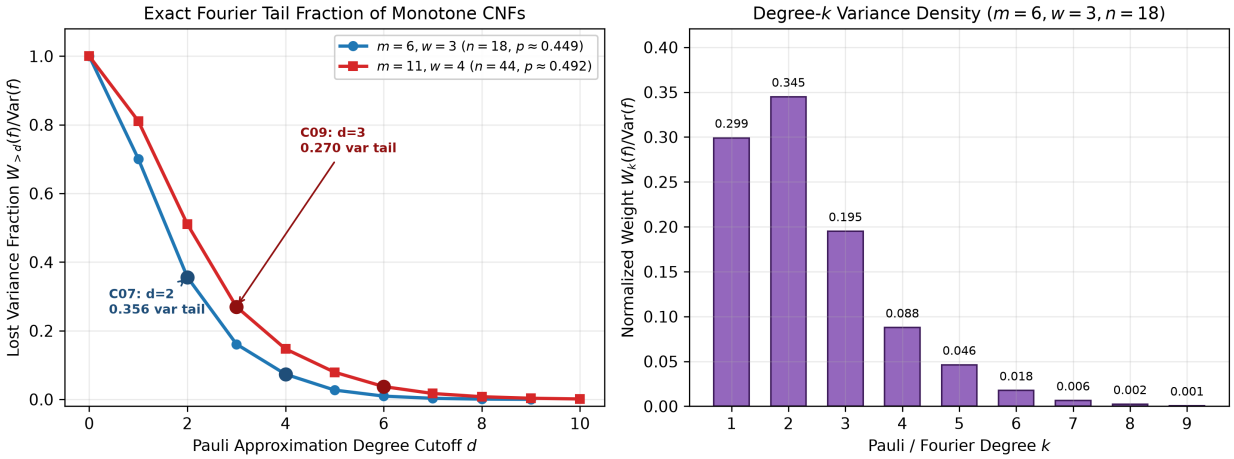

Figure 2: Left: Exact lost variance fraction $W_{>d}(f_{m,w})/\mathrm{Var}(f_{m,w})$ across Pauli degree cutoffs d for balanced monotone depth-2 CNFs ($n = 18$ and $n = 44$, `C07`–`C10`). Right: Exact degree-k normalized Fourier variance density for $(m, w) = (6, 3)$.

In the ± 1 basis $z_i = (-1)^{x_i}$, each single clause satisfies $\mathrm{OR}_w(x) = 1 - 2^{-w} \sum_{S \subseteq [w]} \chi_S(z)$, whose exact Parseval identity in integer form is $(2^w - 1)^2 + (2^w - 1) = 2^w(2^w - 1)$ (Lean `T08`). By independence of disjoint clause blocks, the exact Fourier weight at degree k is

$$W_k(f_{m,w}) = \sum_{r=0}^{m} \binom{m}{r} (1 - 2^{-w})^{2(m-r)} 2^{-2wr} \, [t^k]\big((1+t)^w - 1\big)^r, \tag{2}$$

satisfying the exact $\{0,1\}$-Parseval identity $\sum_{k=0}^{mw} W_k(f_{m,w}) = p := (1 - 2^{-w})^m$ and $W_0 + \mathrm{Var}(f_{m,w}) = p$ with $\mathrm{Var}(f_{m,w}) = p(1-p)$ (Lean `T09`–`T12`).

Theorem 3.1 (Operator-Norm Lower Bound from Exact Fourier Tails; Lean `T13`, `C06`–`C10`)**.** *Let $A_{\le d}$ be any n-qubit Hermitian operator of Pauli degree at most d, and let $D_f := \mathrm{diag}(f_{m,w}(x))$ denote the diagonal target observable. Then*

$$\|A_{\le d} - D_f\|_{\mathrm{op}}^2 \ge 2^{-n} \|A_{\le d} - D_f\|_F^2 \ge \sum_{k > d} W_k(f_{m,w}) =: W_{>d}(f_{m,w}). \tag{3}$$

In particular, our exact-$\mathbb{Q}$ verifier certifies:

1. *Balanced $m = 6, w = 3$ ($n = 18$, $p = 117649/262144 \approx 0.4488$, $\mathrm{Var} \approx 0.2474$): any degree-2 Hermitian approximator loses 35.60% of the variance ($W_{>2} \approx 0.0881$, `C07`), and degree-4 still leaves 7.33% ($W_{>4} \approx 0.0181$, `C08`).*

2. *Balanced $m = 11, w = 4$ ($n = 44$, $p = (15/16)^{11} \approx 0.4917$, $\mathrm{Var} \approx 0.2499$): degree-3 loses 26.98% of the variance ($W_{>3} \approx 0.0674$, `C09`), and degree-6 retains a strictly positive tail $W_{>6} \approx 0.0094$ (3.74%, `C10`).*

4 Zero-Float Stretched-Exponential Ceilings for 2-Designs and NLTS

Sun and Wang [7] show that sublinear-degree Pauli approximation forces stretched-exponential e^{-m^α} ($\forall \alpha \in (0,1)$) bounds on distinguishing state 2-designs from Haar-random states and $2e^{-m^\alpha}$ bounds on low-energy spectral weight of Anshu–Breuckmann–Nirkhe NLTS Hamiltonians [2]. To certify these decay ceilings with zero floating-point exponentials, we use the strictly positive Taylor lower bound $e^x > \sum_{j=0}^{K} x^j/j!$ for every $x \in \mathbb{Q}_{>0}$:

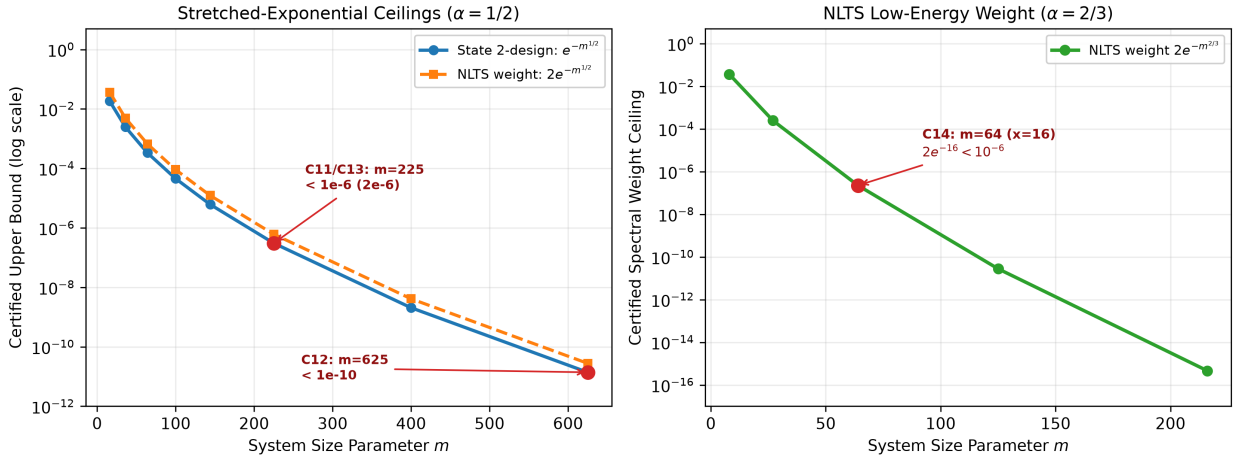

Figure 3: Left: Stretched-exponential upper bounds at $\alpha = 1/2$ for state 2-design indistinguishability ($e^{-m^{1/2}}$) and NLTS low-energy spectral weight ($2e^{-m^{1/2}}$), marking zero-float Taylor certificates `C11`–`C13`. Right: NLTS spectral weight decay at $\alpha = 2/3$ marking certificate `C14` ($m = 64, x = 16, 2e^{-16} < 2.27 \times 10^{-7}$).

Theorem 4.1 (Zero-Float Stretched-Exponential Decay Certificates; Lean `T14`–`T17`, `C11`–`C14`)**.** *Let $c > 0$ and let $m, x, \alpha_{\mathrm{num}}, \alpha_{\mathrm{den}} \in \mathbb{Z}_{\geq 1}$ satisfy $m^{\alpha_{\mathrm{num}}} = x^{\alpha_{\mathrm{den}}}$. Then for every Taylor truncation order $K \geq 1$,*

$$c\, e^{-m^{\alpha_{\mathrm{num}}/\alpha_{\mathrm{den}}}} = c\, e^{-x} < \frac{c\, K!}{\sum_{j=0}^{K} x^j (K!/j!)}. \tag{4}$$

Constructive Lean 4.36.0 evaluation proves (see Figure 3):

- *State 2-design distinguishing ceiling at $\alpha = 1/2$: $e^{-225^{1/2}} = e^{-15} < 10^{-6}$ (tightened at $K = 24$ to $< 3.094 \times 10^{-7}$, `C11`, `T15`) and $e^{-625^{1/2}} = e^{-25} < 10^{-10}$ (`C12`, `T16`).*
- *NLTS low-energy spectral weight ceiling: $2e^{-225^{1/2}} < 10^{-5}$ ($K = 24$: $< 6.188 \times 10^{-7}$, `C13`, `T15`) and $2e^{-64^{2/3}} = 2e^{-16} < 10^{-6}$ ($K = 26$: $< 2.268 \times 10^{-7}$, `C14`, `T17`).*

Proposition 4.2 (Operator-Norm Advantage Transfer; Lean `T18`–`T20`, `C15`–`C16`)**.** *Let M ($0 \preceq M \preceq I$) be the acceptance POVM element of a circuit and let $H_{\leq d}$ be a degree-d Hermitian approximator satisfying $\|M - H_{\leq d}\|_{\mathrm{op}} \leq \varepsilon$ ($\varepsilon \geq 0$). For any two density matrices ρ_0, ρ_1 (e.g., input-ensemble state mixtures for distinguishing or balanced Boolean classification), define the distinguishing advantage $\mathrm{adv}(A) := \sup_{\rho_0,\rho_1} |\mathrm{Tr}(A(\rho_0 - \rho_1))|$ over the allowed state pairs. Since $\|\rho_0 - \rho_1\|_1 \leq 2$, Hölder's inequality and the triangle inequality give $|\mathrm{Tr}((M - H_{\leq d})(\rho_0 - \rho_1))| \leq 2\varepsilon$, hence*

$$\mathrm{adv}(M) \leq \mathrm{adv}(H_{\leq d}) + 2\varepsilon. \tag{5}$$

As illustrative rational benchmarks of this transfer rule (Table 1), Lean `T18`–`T19` certify $\mathrm{adv}(M) \leq 1/20 + 2/100 = 7/100 < 1/2$ (`C15`) and $\mathrm{adv}(M) \leq 1/500 + 2/1000 = 1/250 < 1/2$ (`C16`).

5 Certificate Suite, Scope, and Verification Boundary

Table 1 summarizes all 16 SHA-256-indexed rational certificates (`C01`–`C16`) emitted by `PAULI-ACO-BQACO-CERT-1.0` and checked by 62 adversarial pytest checks and 20 constructive Lean 4.36.0 theorems.

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

ID	Target / Regime	Exact Rational / Certified Output	Lean Ref.
`C01`	Pauli weight $n = 4, d \leq 2$	$67/256 \approx 0.261719$ of 4^4	`T01`
`C02`	Pauli weight $n = 8, d \leq 3$	$1789/65536 \approx 0.027298$ of 4^8	`T02`
`C03`	Pauli weight $n = 16, d \leq 4$	$163669/4^{16} \approx 3.81 \times 10^{-5}$ ($d = \lceil\sqrt{n}\rceil$)	`T03`
`C04`	Z-twirling $n = 2$ (16 Paulis)	4 diagonal kept, 12 annihilated (proj.; strict on test O)	`T05--T07`
`C05`	Z-twirling $n = 3$ (64 Paulis)	8 diagonal kept, 56 annihilated (proj.; strict on test O)	`T05--T07`
`C06`	Monotone CNF $(3, 2), d \leq 1$	$p = 27/64$, $W_{>1} \approx 0.125244$ (51.35% var)	`T08--T10`
`C07`	Monotone CNF $(6, 3), d \leq 2$	$p = 117649/262144$, $W_{>2} \approx 0.088073$ (35.60% var)	`T11, T13`
`C08`	Monotone CNF $(6, 3), d \leq 4$	$p \approx 0.448795$, $W_{>4} \approx 0.018144$ (7.33% var)	`T11, T13`
`C09`	Monotone CNF $(11, 4), d \leq 3$	$p = (15/16)^{11} \approx 0.4917$, $W_{>3} \approx 0.067432$ (26.98% var)	`T12, T13`
`C10`	Monotone CNF $(11, 4), d \leq 6$	$p \approx 0.491681$, $W_{>6} \approx 0.009360$ (3.74% var)	`T12, T13`
`C11`	2-design $e^{-225^{1/2}}$ ($K = 24$)	Exact bound $< 3.094 \times 10^{-7} < 10^{-6}$	`T14, T15`
`C12`	2-design $e^{-625^{1/2}}$ ($K = 36$)	Exact bound $< 10^{-10}$	`T14, T16`
`C13`	NLTS $2e^{-225^{1/2}}$ ($K = 24$)	Exact bound $< 6.188 \times 10^{-7} < 10^{-5}$	`T14, T15`
`C14`	NLTS $2e^{-64^{2/3}}$ ($K = 26$)	Exact bound $< 2.268 \times 10^{-7} < 10^{-6}$	`T14, T17`
`C15`	Advantage ceiling ($\varepsilon = 1/100$)	$1/20 + 2/100 = 7/100 \ll 1/2$	`T18, T19`
`C16`	Tight ceiling ($\varepsilon = 1/1000$)	$1/500 + 2/1000 = 1/250 \ll 1/2$	`T18--T20`

Verification Boundary and Attribution.

- **Machine-checked in Lean 4.36.0 (`T01`–`T20`) and exact $\mathbb{Q}$ (`C01`–`C16`):** Pauli-weight layer counts, symplectic Z-twirling diagonal projection and Frobenius contraction, single-clause and disjoint-CNF Parseval/variance identities, exact degree-d Fourier tails and squared operator-norm lower bounds, zero-float integer Taylor bounds on e^{-m^α} and $2e^{-m^\alpha}$, and triangle-inequality advantage ceilings. Every Lean theorem depends solely on `[propext, Quot.sound]` or zero axioms (zero `Classical.choice`, zero `sorry`).
- **Imported from cited literature (not re-proved inside Lean):** Sun and Wang's [7] full circuit-level product-projection localization theorem proving that every $\mathsf{BQAC}^0/\mathsf{qpoly}$ acceptance operator is approximated in operator norm by an advice-independent sublinear-degree Pauli operator, its asymptotic inverse-polynomial worst-case advantage theorem for monotone depth-2 CNFs, and the Anshu–Breuckmann–Nirkhe NLTS Hamiltonian family [2].

Reproducibility and Disclosures. Code, Lean proofs, tests, and SHA-256 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; every mathematical claim is independently checked by the Lean 4.36.0 kernel and zero-float pytest suite.

References

[1] Scott Aaronson. Limitations of quantum advice and one-way communication. *Theory of Computing*, 1(1):1–28, 2005.

[2] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. NLTS Hamiltonians from good quantum codes. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1090–1096, 2023.

[3] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80(1):012304, 2009.

[4] Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, Fourier transform, and learnability. *Journal of the ACM*, 40(3):607–620, 1993.

[5] Shivam Nadimpalli, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. On the Pauli spectrum of QAC^0. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1498–1506, 2024.

[6] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.

[7] Xiaoming Sun and Jingheng Wang. $\mathsf{AC}^0 \not\subseteq \mathsf{BQAC}^0/\mathsf{qpoly}$ via sublinear-degree pauli approximation. arXiv preprint arXiv:2611.34803v1, November 2026.