

Query Bounds and Explicit Quantum Circuits for Periodic Weighted Decisions

Annan Chen

`annan.chen24@imperial.ac.uk`

Imperial College London <https://orcid.org/0009-0000-1308-0466>

Research Article

Keywords: Quantum algorithms, Query complexity, Quantum phase estimation, Reversible circuits, Numerical certification, Kernel methods

Posted Date: October 28th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11513670/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Query Bounds and Explicit Quantum Circuits for Periodic Weighted Decisions

Annan Chen

Department of Physics, Imperial College London
London, United Kingdom

ORCID: [0009-0000-1308-0466](https://orcid.org/0009-0000-1308-0466)

Preprint • October 2026

Abstract

We study the query complexity and public circuit cost of deciding the sign of a weighted sum of unknown binary labels. The weights are derived from a periodic heat kernel with a specified off-grid interpolation rule. Classical and quantum algorithms share all public information and query the same unknown labels, with N denoting the size of an implicit oracle address space. At fixed model parameters, a fixed positive raw-score margin and a fixed failure probability in $(0, 1/2)$, we prove tight query bounds. For sufficiently large even N , these scale as $(\log N)^2$ and $\log N$ for randomized classical and quantum algorithms, respectively. A regularity criterion gives sufficient conditions for this separation and for dimension-independent truncation. We construct a reversible implementation using bounded polynomial responses and compressed coordinate computation, avoiding a full table of remote weights. A finite randomized phase-grid measurement provides a sign guarantee for every admissible input. At $N = 2^{68}$, one construction uses 20,479 label queries against a classical lower bound of 472,711. It uses approximately 2.42×10^8 T gates and 586 logical qubits. Its maximum of 16,383 consecutive oracle calls matches the three-run sign-QPE readout. The failure bound is below 0.05 at score margin 0.002, conditional on whole-program logical failure being at most 0.01. Gate totals exclude the internal label-oracle implementation and physical error correction. These results connect a family-specific query separation with explicit circuits and finite resource guarantees.

Keywords: Quantum algorithms; Query complexity; Quantum phase estimation; Reversible circuits; Numerical certification; Kernel methods.

1 Introduction

A quantum algorithm may need fewer accesses to its input than a classical algorithm while still requiring substantial computation between those accesses [2, 3]. Weighted sign decisions provide a concrete setting in which to examine this distinction. The output is only one bit, but preparing the observation and extracting that bit can dominate the circuit cost. This paper studies both the information required for the decision and the reversible computation needed to make it.

We consider a structured family of weights derived from a periodic heat kernel with a specified off-grid interpolation rule. The weights are known to both algorithms; only the binary labels are unknown. The analysis connects the number of label queries to an implementation that avoids a full table of remote weights. It also addresses how the final sign can be read with a finite error guarantee.

The input consists of known real weights $w_0, \dots, w_{N-1}$ and unknown binary labels $y_i \in \{-1, +1\}$. We seek the sign of

$$s = \sum_{i=0}^{N-1} w_i y_i, \quad |s| \geq \gamma > 0. \quad (1)$$

We call s the raw, or unnormalized, score. The known margin γ is a lower bound on $|s|$; the algorithm is not given the actual score. On every promised input the algorithm must output the correct sign with probability at least $1 - \delta$. Refusing to decide counts as failure.

A classical label query chooses an index and receives y_i . It can choose later indices using earlier answers and private random bits. A quantum query accesses the same labels through one application of the exclusive-or (XOR) unitary

$$O_y|i, b\rangle = |i, b \oplus (1 - y_i)/2\rangle, \quad (2)$$

possibly on a superposition of indices. Here *public* means known to both algorithms and independent of the unknown labels. The weights, their descriptions and all label-independent preprocessing are available to both parties. Query complexity counts calls to this oracle; we separately count public computation and storage. The classical lower bound allows arbitrary randomized and adaptive query strategies, including importance sampling.

1.1 Periodic heat-kernel weights

Place N sites on a cycle, let S shift by one site, and let $C = (S + S^\dagger)/2$ be its normalized adjacency. The heat time $\tau > 0$ controls diffusion and $\lambda > 0$ controls ridge regularization. Let q be the interpolation vector for the prediction location, specified below, and define

$$\begin{aligned} K_\tau &= \exp[-2\tau(I - C)], & \alpha &= (K_\tau + \lambda I)^{-1}y, & k_* &= K_\tau q, \\ s &= k_*^T \alpha = q^T K_\tau (K_\tau + \lambda I)^{-1}y = w^T y, & w &= F(C)q, \\ & & F(x) &= \frac{1}{1 + \lambda e^{2\tau(1-x)}}. \end{aligned} \quad (3)$$

Thus the weighted decision is a particular regularized kernel prediction. This functional provides a concrete setting in which to compare an oracle query bound with the cost of the public quantum computation. The analysis concerns this specified periodic functional and does not include the cost of acquiring classical data.

The coordinate $\eta \in (0, 1)$ specifies a query between sites 0 and 1. We use the real Nyquist interpolation convention on an even cycle: paired Fourier modes have phase $e^{-i\eta\theta}$, while the Nyquist mode uses the real coefficient $\cos(\pi\eta)$. The resulting cardinal vector is

$$q(r) = (-1)^{r+1} \frac{\sin(\pi\eta)}{N} \cot \frac{\pi(r - \eta)}{N}, \quad r = -N/2 + 1, \dots, N/2. \quad (4)$$

It interpolates a fractional position and has positive and negative entries. For grid values f , $q^T f$ evaluates their chosen real-Nyquist trigonometric interpolant at η . At an integer interpolation position, the cardinal vector is the corresponding coordinate vector. The multiplier of $F(C)$ is $h(\theta) = F(\cos \theta)$. The off-grid interpolation rule determines the spatial tail: the fractional Fourier phase has an endpoint mismatch at the finite bandwidth, while $h(\pi) \neq 0$, so their product retains a harmonic tail. The separation below therefore depends on this interpolation rule.

1.2 A signed observation and its classical counterpart

Suppose a public decomposition satisfies $w_i = \sum_j u_{ji}$ and $Z = \sum_{j,i} |u_{ji}| > 0$. Select (j, i) with probability $|u_{ji}|/Z$ and return $X = \text{sign}(u_{ji})y_i$. Then

$$\mathbb{E}X = s/Z, \quad \Pr(X = +1) = (1 + s/Z)/2. \quad (5)$$

Taking the expectation combines the signed components. A reversible sampler retains its random seeds and work registers while preserving this marginal expectation. A classical sampler using the same public

decomposition has exactly the same ordinary output law. Coherent repeated use permits the improved query dependence.

For a generic four-component example, take $w = (1/2, -1/4, 1/8, -1/8)$ and $y = (1, 1, -1, -1)$. Here $Z = 1$, the selection probabilities are $(1/2, 1/4, 1/8, 1/8)$, and the four possible signs are $(+, -, -, +)$. Their mean is $1/4 = s$.

The implementation problem is to realize this observation coherently, with controlled inverses and reflections, without an N -entry weight table or a costly function-value register on every call.

1.3 Contributions and related work

We establish matching classical and quantum query bounds for a family of periodic heat-weighted sign decisions and identify the regularity conditions governing the separation. We then construct a reversible algorithm whose approximation error is bounded uniformly over all label assignments. Finally, we give a finite randomized-grid phase measurement and account for its full public logical cost. The comparison uses the same label oracle, margin promise and failure requirement throughout.

Quantum summation and amplitude estimation already supply the generic upper-bound mechanism [2, 3]. Gil-Fuster et al. [1] explicitly study all-at-once quantum-kernel inference as a single observable and the tradeoff between query and gate costs. Their trained coefficients are supplied, and their unknown black boxes implement feature-map states; our public heat weights act on unknown Boolean labels in (2). Their optimality result concerns a restricted feature-map-query access problem. Our query bounds concern the Boolean-label oracle defined here.

Bernstein coin simulation, structured preparation, phase randomization and sine windows are established tools [6, 7, 12, 14, 15, 16]. Structured sampling constructions are discussed by Lemieux et al. [8, Eq. (59) and Appendix A.1]. The results below establish the required coefficient ranges and approximation errors, give a reversible coordinate construction, and combine them with a finite sign-error bound. Table 1 distinguishes the query theorem from the explicit circuit and lists the costs excluded by each result.

Result	Guarantee	Cost model
Query theorem	Tight classical and quantum query orders for fixed $\tau, \lambda, \eta, \gamma, \delta$	Identical unknown-label oracle; label-independent computation is free
Reversible circuit	Uniform score bias with a compressed weight description	Explicit public gates and allocated logical qubits
Finite sign decision	Per-input failure below 0.05 at $N = 2^{68}$, $\gamma = 0.002$	Complete public readout, assuming whole-program logical failure at most 0.01

Table 1 Scopes of the main results. Circuit costs exclude oracle internals and physical implementation; classical preprocessing and decoding are accounted for separately. Table 2 gives the finite resource counts.

2 Query complexity

The harmonic tail in (4) causes the separation. We first give a finite lower bound. Write R_δ and Q_δ for the minimum worst-case numbers of classical randomized and quantum label queries, respectively, over algorithms meeting the same per-input failure bound δ .

Lemma 1 (Finite diffuse tail). *Fix the labels on a publicly specified set of indices, called the head, and let c be their known contribution to the score. Call the remaining indices the tail and absorb their known weight signs into the unknown labels, so that the tail weights a_i are positive. Set $M = \sum_i a_i$ and $V = \sum_i a_i^2$, and let $\gamma > 0$ and $0 \leq \delta < 1/2$. If*

$$0 < \rho < 1/2 - \delta, \quad V \leq \frac{\gamma^2}{2 \log(1/\rho)}, \quad \mu_{\pm} = \frac{-c \pm 2\gamma}{M} \in [-1/2, 1/2], \quad (6)$$

put $D_* = 1 - 2\delta - 2\rho + 2\delta\rho$. For worst-case query budgets,

$$R_{\delta} \geq \frac{3D_*^2}{32}(M/\gamma)^2, \quad (7)$$

$$Q_{\delta} \geq \frac{D_*}{\arcsin \mu_+ - \arcsin \mu_-} \geq \frac{\sqrt{3}D_*}{8}M/\gamma. \quad (8)$$

More sharply, set $p_{\pm} = (1 + \mu_{\pm})/2$ and $d_{\max} = \max\{D_{\text{KL}}(p_+ \| p_-), D_{\text{KL}}(p_- \| p_+)\}$ for Bernoulli relative entropy. Then $R_{\delta} \geq 2D_*^2/d_{\max}$.

For the lower bound, consider two distributions of independent tail labels with means μ_+ and μ_- , respectively. Their expected total scores are $\pm 2\gamma$, and Hoeffding's inequality bounds the probability of violating the margin promise. Distinguishing the resulting classical query transcripts requires many previously unqueried labels because the two distributions for each label have small relative entropy. For quantum algorithms a bounded acceptance polynomial limits how rapidly the output law can change. Appendix C proves the lemma including adaptivity, repeats and off-promise behavior.

Theorem 1 (Heat weights and a regularity boundary). *Fix $\tau, \lambda > 0$, $\eta \in (0, 1)$, $\gamma > 0$ and $0 < \delta < 1/2$. For all sufficiently large even N , the exact heat weights in (3) satisfy*

$$R_{\delta} = \Theta((\log N)^2/\gamma^2), \quad Q_{\delta} = \Theta(\log N/\gamma). \quad (9)$$

More generally replace h by a real even continuous periodic multiplier m . Let $b = m(\pi)$ and suppose the periodic function $g(\theta) = (m(\theta) - b)e^{-i\eta\theta}$ has absolutely summable Fourier coefficients. If $b \neq 0$, (9) holds. If $b = 0$, a fixed number of deterministic label queries suffices at fixed raw margin. Interpolation at an integer site also allows dimension-independent truncation when the Fourier coefficients of m are absolutely summable.

Constants and sufficient dimension depend on the fixed parameters, including the margin. This is not a uniform theorem for shrinking $\gamma(N)$; querying all N labels is always a separate upper bound. At fixed normalized margin $|s|/\|w\|_1 \geq \Gamma$, $0 < \Gamma \leq 1$, both query complexities are bounded independently of N .

Finite-cycle aliasing gives $w_N = bq_N + v_N$ with $\|v_N\|_1 = O(1)$, whereas

$$\|w_N\|_1 = \frac{2|b \sin(\pi\eta)|}{\pi} \log N + O(1).$$

A fixed sufficiently large head leaves small squared tail mass but diverging absolute tail mass. The lemma gives the lower bounds. Signed importance sampling and amplitude estimation give the matching upper bounds [2, 3]. Amplitude estimation coherently estimates a binary-event probability, improving the inverse-error query dependence of ordinary sampling. This is a weighted specialization of established summation and polynomial techniques [4, 5]. Appendix D gives the regularity proof and an effective sufficient threshold.

3 Constructing the signed observable

Define the continuous Fourier coefficients, before discretizing, by

$$\alpha_m = \frac{1}{2\pi} \int_{-\pi}^{\pi} h(\theta) e^{-im\theta} d\theta, \quad \alpha_{-m} = \alpha_m \in \mathbb{R}, \quad b = h(\pi). \quad (10)$$

Absolute convergence gives

$$w = bq + \sum_{m \geq 1} \alpha_m \Delta_m q, \quad \Delta_m q(r) = q(r - m) + q(r + m) - 2(-1)^m q(r). \quad (11)$$

The alternating subtraction in $\Delta_m q$ cancels the leading $1/r$ term of the shifted cardinal weights.

For the circuits take $N = 2^n$, where n is the address-register length; the query theorem also applies to other even dimensions. The near-field weights are combined on a common index set, called the *head*, before their absolute values are taken. Choose one certified coefficient approximation $\tilde{\alpha}_1, \dots, \tilde{\alpha}_d$ and set $g_d = \sum_{m=1}^d \tilde{\alpha}_m \Delta_m q$. Evaluate the signed sum $bq + g_d$ on paired coordinates $r = -j, j+1$, $j < R_{\text{desc}}$, before taking absolute values. For $j \geq R_{\text{desc}}$ retain only bq . A dyadic shell is an interval $j \in [L, 2L)$ with $L = 2^k$. On each side use the ideal proposal mass $m_{\text{sh}}^{(0)} = b \sin(\pi\eta)/\pi$. For its uniformly proposed address let $t = j + \eta$ or $j + 1 - \eta$ and accept with probability

$$p(t, L) = \frac{L}{t} \frac{\pi t}{N} \cot \frac{\pi t}{N}. \quad (12)$$

The ideal proposal mass $m_{\text{sh}}^{(0)}/L$ times this probability equals $|bq(r)|$. Let R_{desc} be the radius used for the smooth-residual truncation just described. The circuit may measure a larger dyadic radius $R_{\text{head}} = 2^{r_0} < N/2$, with $R_{\text{head}} \geq R_{\text{desc}}$. The measured head is $r = -j, j+1$ for $0 \leq j < R_{\text{head}}$; remaining addresses are exactly the paired shells $k = r_0, \dots, n-2$, with $L = 2^k$. Thus $J = n-1-r_0$ shells cover the rest without overlap. The residual certificate remains valid when the measured head is enlarged. For $R_{\text{desc}} \geq 2d$ the omitted smooth residual has all-label raw error at most

$$B_{R_{\text{desc}}} = \frac{8 \sin(\pi\eta)}{3\pi} \left(\sum_{m=1}^d |\tilde{\alpha}_m| m^2 \right) [T(R_{\text{desc}} + \eta) + T(R_{\text{desc}} + 1 - \eta)], \quad T(x) = x^{-3} + \frac{1}{2}x^{-2}. \quad (13)$$

Coefficient generation uses $O(d)$ frequency samples rather than an N -point fast Fourier transform (FFT). For a target descriptor error $\varepsilon > 0$ in the raw score and fixed heat parameters, $d = O(\log(1/\varepsilon))$ and $R_{\text{desc}} = O(\max\{d, \varepsilon^{-1/2}\})$ suffice. The description contains $O(R_{\text{desc}} + n)$ entries and requires $O(R_{\text{desc}}d + d^2 + n)$ public scalar operations at the certified working precision. These operations are included in the preprocessing cost. Appendix F supplies the bounds.

For implementation, round the retained weights and the common proposal mass to dyadic numbers, that is, rationals with power-of-two denominators. Write m_{sh} for the stored approximation to $m_{\text{sh}}^{(0)}$ and $\bar{w}$ for the resulting weight description before response and source approximations. Let H be the measured head. From this point on, $Z = 2Jm_{\text{sh}}$ is the total proposal mass of the remaining tail; it need not equal the sum of the tail weight magnitudes. Rejected proposals contribute zero in expectation. Rounding errors are included in the raw-score bias β as specified in Appendix A. The algorithm is as follows:

1. Generate the Fourier coefficients, dyadic head weights, shell masses and bounded response controls. All of these are independent of unknown labels.
2. Query each selected head label once and compute $c_H = \sum_{i \in H} \bar{w}_i y_i$ exactly for the dyadic descriptor $\bar{w}$. Classical competitors receive the same head information.

3. Prepare a side, a uniform shell and an offset; reversibly compute the label address and probability coordinate. Independent comparison seeds select the bounded response. Rejected proposals return a fair sign, with no postselection.
4. Use the accepted public sign and label phase in compute–phase–uncompute. Retain every seed and use the exact inverse of the actual compiled source in the reflection. Approximation is certified for the final raw score.
5. Use the quantum phase-estimation (QPE) readout of Section 5 to estimate the implemented tail mean $\mathbb{E}X$ by $\hat{\mu}$, and return $\text{sign}(c_H + Z\hat{\mu})$. The phase-register dimension and number of repetitions depend only on public parameters and the promised margin.

For every label vector, the approximation satisfies $|s - (c_H + Z\mathbb{E}X)| \leq \beta$. Figure 1 summarizes the algorithm. The head contribution shifts the decision threshold. When $R_{\text{head}} > R_{\text{desc}}$, the additional head entries use the stored dyadic approximations to bq ; the omitted residual is still bounded at R_{desc} .

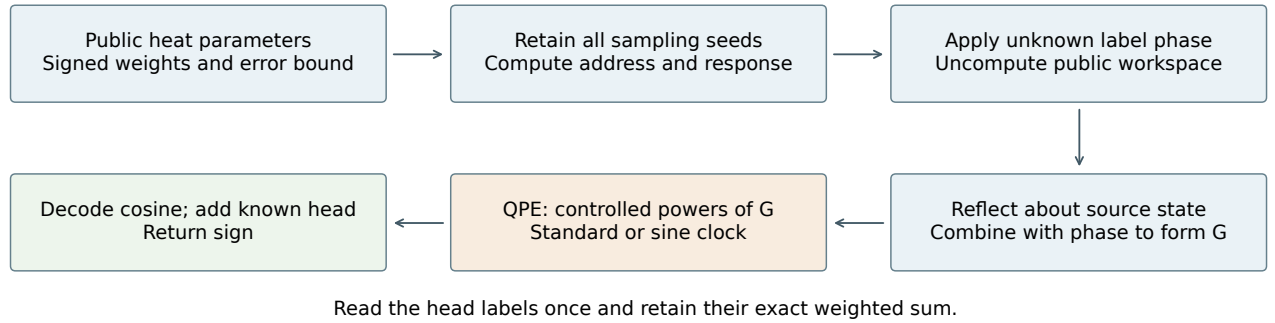


Fig. 1 Schematic of the algorithm. The head labels are read once; the remaining labels are accessed through the coherent oracle phase. This phase and the source-state reflection define the iterate G , whose controlled powers are used within QPE (Section 5). The output is a sign with the stated per-input error guarantee.

4 Reversible circuit construction

4.1 Bounded polynomial observations

Writing $x = t/L$ and $a = \pi L/N$, the shell acceptance probability in (12) becomes

$$f_a(x) = a \cot(ax), \quad x = t/L \in [1, 2], \quad a = \pi L/N \leq \pi/4, \quad f_0(x) = 1/x.$$

Accepting with probability $f_a(x)$ and returning a fair sign on rejection gives the required signed contribution. The construction therefore needs a probability or expectation equal to $f_a(x)$: a state amplitude p would instead give probability $|p|^2$. We implement comparisons using independent uniform random seeds, retain those seeds, and use the computation coherently.

Proposition 1 (A bounded polynomial observation). *Let $b_0, \dots, b_d \in [-1, 1]$. Given d independent Bernoulli(θ) bits, let K be their sum. Conditional on $K = k$, accept with probability $|b_k|$ and output $\text{sign}(b_k)$; on rejection output an independent fair sign. Then*

$$\mathbb{E}X = \sum_{k=0}^d b_k \binom{d}{k} \theta^k (1 - \theta)^{d-k}.$$

An error at most e_b in every control changes the mean by at most e_b .

Conditioning on K proves the identity; the Bernstein weights are nonnegative and sum to one. This classical probability representation is established background in Bernoulli simulation [12, Section 2 and Proposition 3]. The coherent implementation keeps every random seed and all information needed to reverse the computation. This probability basis is distinct from *Bernstein’s derivative inequality*, which bounds acceptance polynomials in the query lower-bound proof.

On a cell $[l, l + h]$, write $x = l + h\theta$. Let $v_j = f_a(l + jh/3)$ for $j = 0, 1, 2, 3$, and let Q be the cubic interpolating these values. Its coefficients in the Bernstein basis, called controls, are

$$\begin{aligned} b_0 &= v_0, & b_1 &= (-5v_0 + 18v_1 - 9v_2 + 2v_3)/6, \\ b_2 &= (2v_0 - 9v_1 + 18v_2 - 5v_3)/6, & b_3 &= v_3. \end{aligned} \quad (14)$$

Theorem 2 (Bounded heat-response construction). *For $0 \leq a \leq \pi/4$ and every cell $[l, l + h] \subset [1, 2]$, the four controls in (14) lie in $[0, 1]$, and their cubic polynomial Q obeys*

$$|Q(x) - f_a(x)| \leq h^4/(81l^5). \quad (15)$$

For one side of a shell with 2^k uniformly proposed addresses and $M = 2^{9\text{cell}}$ equal cells, where $k \geq g_{\text{cell}}$, the average absolute interpolation error is at most $A_5(M)/(81M^4)$, where

$$A_5(M) = \frac{1}{M} \sum_{j=0}^{M-1} (1 + j/M)^{-5}. \quad (16)$$

Multiplying by that side’s proposal mass gives a raw-score error bound valid for every label assignment.

The fourth derivative is nonnegative and at most $24/x^5$. In the normalized coordinate $\theta \in [0, 1]$, the interpolation nodal product has absolute maximum $1/81$. The control-range proof compares endpoint derivatives with a Hermite interpolant; Appendix G includes the argument. Each cell receives exactly the same number of proposed addresses, even after the specified coordinate flooring. This proves (16) for every assignment of unknown label signs. Figure 2 illustrates the cubic observation on one cell.

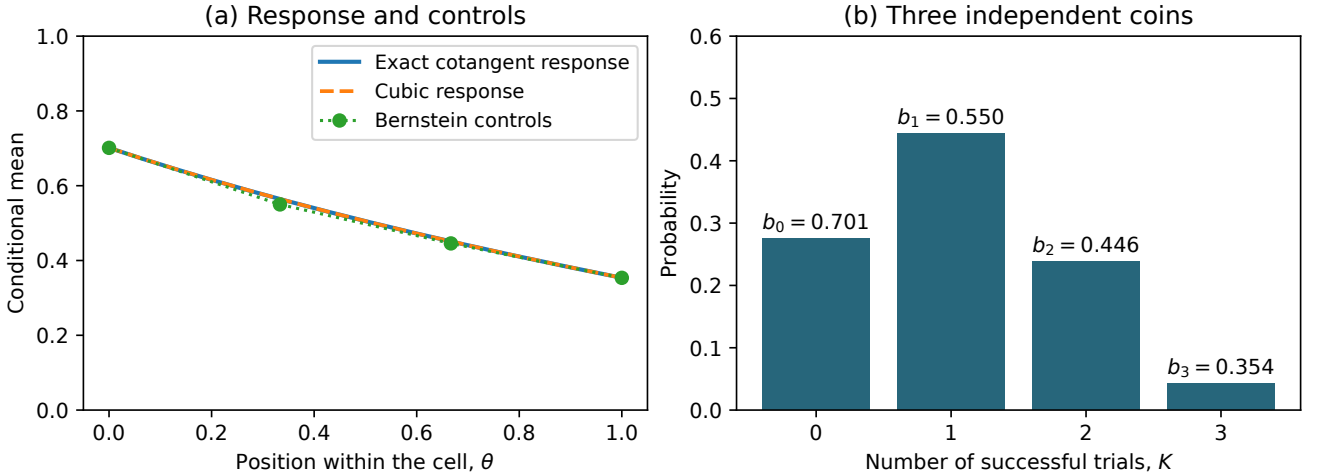


Fig. 2 Cubic observation on a cell with $(a, l, h) = (0.65, 1.15, 0.5)$. (a) The response and its Bernstein controls. (b) Three independent coins with $\theta = 0.35$ select K ; bar heights are probabilities, and b_K is the conditional mean.

4.2 Source preparation and joint coordinates

A source state coherently represents the sampler’s seed distribution, with amplitudes equal to square roots of probabilities. The shell register is prepared in an equal superposition of its allowed indices,

with independent registers for the side and offset. A one-hot decoder marks the chosen shell by setting exactly one output bit. The label address and a finite-precision representation of $x - 1$ are computed together. This probability coordinate determines the interpolation cell and its local parameter θ , so the cost includes selecting its bits as well as forming the address. The circuit assumes consecutive dyadic shells, $N = 2^n$, a dyadic η with e bits, and a probability coordinate with f bits. Here J is the number of shells. Appendix A describes the circuit layout and error budget; Appendix I proves the coordinate mapping.

Proposition 2 (Retained dyadic coordinates). *For J consecutive shells within an n -bit address space, the joint label-address and f -bit probability-coordinate mapping has an exact reversible implementation using $O(n + f \log J)$ nonlinear reversible Boolean gates (Toffoli or controlled-SWAP gates) and $O(n + f + e)$ coordinate workspace. It includes the one-hot decoder, signed-address carries and retained permutation history. Shell-source synthesis and response lookup are separate costs. The inverse gate sequence restores every source bit before reflection about the prepared state.*

A compiled circuit is an explicit sequence of Clifford and T gates, where $T = \text{diag}(1, e^{i\pi/4})$. Approximating arbitrary rotations by this gate set is called rotation synthesis; its cost is included using the Ross–Selinger method [9]. The inverse reverses the sequence and takes each gate’s adjoint.

Proposition 3 (A fixed compiled source). *Suppose a compiled unitary $\tilde{U}$ prepares a source at Euclidean distance at most ϵ_U , up to global phase, from the ideal source. For any diagonal signed observation with operator norm at most one, the induced raw-score error is at most $2Z\epsilon_U$. If the iterate uses the exact reflection $\tilde{U}(2|0\rangle\langle 0| - I)\tilde{U}^\dagger$, this source approximation contributes to the score bias, rather than a separate error term at each iteration.*

For normalized states, subtract their quadratic forms and apply Cauchy–Schwarz twice. The readout theorem then applies exactly to the implemented source and its implemented score. The argument uses the exact inverse of the compiled preparation circuit. Every repetition includes initialization, and every reflection includes preparation and its inverse.

If ϵ_{raw} is the raw-score error budget for response interpolation, the cubic construction requires $M = O((n/\epsilon_{\text{raw}})^{1/4})$ cells per table. Linear interpolation has square-root dependence on n/ϵ_{raw} . This improvement concerns the response tables: public head computation, seed registers, controlled source preparation, lookup and readout still contribute to the complete cost.

5 Finite sign readout

QPE estimates an eigenphase of a unitary by applying its controlled powers and an inverse quantum Fourier transform (QFT). Here the unitary is the iterate G defined below, and the desired tail mean is the cosine of its eigenphase. Throughout this section $P = 2^m$ is the phase-register dimension and m its number of qubits. Recall that c_H is the exactly accumulated dyadic head sum, Z is the tail proposal normalization, and β bounds the raw-score bias for every label assignment. The implemented tail score is $\tilde{s}_{\text{tail}} = Z\mathbb{E}[X_y]$, with $|s - (c_H + \tilde{s}_{\text{tail}})| \leq \beta$. Let $|\psi\rangle = \tilde{U}|0\rangle$ include the implemented shell source and all other independent uniform seeds. For a seed string u , a reversible computation B determines the label address $r(u)$, public sign $\sigma(u)$ and acceptance flag. The independent bit $\text{fair}(u)$ supplies the fair sign on rejected proposals. Compute–phase–uncompute implements the diagonal seed observation

$$D_y|u\rangle = X_y(u)|u\rangle, \quad X_y(u) = \begin{cases} \sigma(u)y_{r(u)}, & \text{accepted,} \\ (-1)^{\text{fair}(u)}, & \text{rejected.} \end{cases}$$

All work qubits return to zero for every seed string and hence for every superposition of seeds. The subspace with zeroed work registers is therefore invariant, and the source reflection acts within this

subspace. The iterate is $G = R_\psi D_y$, where $R_\psi = 2|\psi\rangle\langle\psi| - I$. Writing $a = \Pr[X_y = -1] = \sin^2 \theta$, its two relevant eigenphases are $\pm 2\theta$, and $\cos(2\theta) = \tilde{s}_{\text{tail}}/Z$.

A single query to the XOR oracle implements the phase conditioned on the phase-estimation control qubit. Its target is $|-\rangle$ when acceptance and this control are both enabled, and $|+\rangle$ otherwise. The public-sign and fair-rejection phases use the same control, so the operation is exactly the identity when the control is zero. A Z gate on the control supplies the required overall sign of the reflection. The controlled reflection about the all-zero state is conjugated by the compiled source-preparation circuit and its exact inverse. These two circuits cancel when the control is disabled. The classical cosine decoder has error less than $\varepsilon_{\text{dec}} = 2^{-48}$ (Appendix H). A zero decoded score is assigned the positive sign and is conservatively counted as a failure in the analysis. For an odd number K of independent runs, the median of the decoded score estimates is computed classically. The corresponding binomial error bound is

$$B_K(p) = \sum_{j=(K+1)/2}^K \binom{K}{j} p^j (1-p)^{K-j}. \quad (17)$$

5.1 A uniform bound on sign errors

Throughout the finite bounds, $\pi_- < \pi < \pi_+$ are certified rational endpoints; Appendix J.2 specifies them. Let ϕ be either relevant eigenphase, with implemented tail mean $Z \cos \phi$. The observed head labels, called the head transcript, determine c_H and shift the cosine threshold to $t = -c_H/Z$. Define the public gap

$$g = (\gamma - \beta)/Z - \varepsilon_{\text{dec}} > 0. \quad (18)$$

Proposition 4 (Uniform decision reduction). *For every promised input and every reachable head transcript, an error on a positive-score input is contained in $\{\cos(2\pi j/P) \leq \cos \phi - g\}$; an error on a negative-score input is contained in $\{\cos(2\pi j/P) \geq \cos \phi + g\}$. Thus a uniform bound p_* on either one-sided cosine event yields statistical failure at most $B_K(p_*)$.*

Proof. For $s \geq \gamma$, the implemented score is at least $\gamma - \beta$. A nonpositive decoded score therefore lowers the exact cosine by at least $(\gamma - \beta)/Z - \varepsilon_{\text{dec}}$. The negative case reverses the signs. Independence across complete runs gives the binomial bound. The argument allows any real threshold t , including values outside $[-1, 1]$, and requires no lower bound on the unknown tail score alone. $\square$

5.2 Preparing the sine-window state

A sine-window measurement prepares the phase register in the state

$$|a\rangle = \sum_{t=0}^{P-1} \sqrt{2/P} \sin\left(\frac{\pi(t+1/2)}{P}\right) |t\rangle. \quad (19)$$

Let a_t denote the amplitude of $|t\rangle$ in (19). Write $t = x + bP/2$, where $0 \leq x < P/2$ and $b \in \{0, 1\}$. Prepare the low $m-1$ bits in a uniform superposition and the top bit in $|0\rangle$, then apply $R_y(\pi - \pi/P - 2\pi x/P)$ to the top bit. This is one fixed rotation and $m-1$ singly controlled rotations. Its two top-bit amplitudes are the required sine and cosine. Each controlled rotation uses paired half-angle gate sequences and their exact adjoints, so the global phases introduced by synthesis cancel. Controlled powers of G and the inverse QFT then follow.

For a signed circular displacement d from the true phase, measured in Fourier bins, the outcome probability is

$$p(d) = \frac{2 \cos^2(\pi d) \cos^2(\pi d/P) \sin^2(\pi/(2P))}{P^2 [\sin^2(\pi d/P) - \sin^2(\pi/(2P))]^2}. \quad (20)$$

At $d = \pm 1/2$ the removable value is $1/2$. Appendix J.2 proves the kernel identity and the circular tails.

5.3 Randomized phase grids and zero-padded measurement

The signed observable retains its seeds coherently. The readout also samples a classical grid shift independently of the labels and each run's source preparation. For every fixed input satisfying the margin promise, the error guarantee averages over the algorithm's randomness. Let S_g be the number of grid shifts. Draw z uniformly from $\{0, \dots, S_g - 1\}$, $S_g = 2^r$, and put $\xi = z/S_g$. After preparing (19), apply

$$D_z|t\rangle = e^{-2\pi i z t / (S_g P)}|t\rangle. \quad (21)$$

Follow with the same controlled powers and inverse P -point QFT. For outcome j , decode the score as $c_H + Z \cos(2\pi(S_g j + z)/(S_g P))$, using the finite cosine decoder. The negative phase ramp is paired with a positive decoder offset. Each run executes one of the S_g possible shifted circuits. For fixed z , the ramp is a product of known single-qubit phases; the implementation applies at most $r \log_2 P$ rotation gate sequences to the existing phase register.

Theorem 3 (Finite randomized sign certificate). *Suppose the implemented raw score has bias at most β for every label assignment, with tail normalization Z , an exactly accumulated head sum c_H , and positive gap g from (18). Let $P \geq 32$ and S_g be powers of two. Set $q_f = Pg/(2\pi_+)$ and $q_b = P\sqrt{2g}/(2\pi_+)$, where $\sqrt{2g}$ is a certified rational lower bound on $\sqrt{2g}$. These are lower bounds on the forward and backward bad-outcome distances in Fourier bins. Suppose $q_f > 3/4$ and $q_b \geq q_f$. Let $R(v)$ be the explicit decreasing bound on the one-sided kernel tail in (37), with $a_* = 127/128$. Define on a closed cell $I = [L, U]$ of width at most $1/128$,*

$$H(I) = \frac{C_I}{2\pi_-^2} [R(\lceil q_f - U \rceil + L) + R(\lceil q_b + L \rceil - U)], \quad C_I \geq \max_{f \in I} \cos^2(\pi f).$$

Writing $I_i = [i/(128S_g), (i+1)/(128S_g)]$, a uniform single-run statistical bound is

$$p_{P, S_g} = \min \left\{ 1, \frac{8}{P^3(9/256 - 4/P^2)^2} + \max_{0 \leq i < 128} \frac{1}{S_g} \sum_{z=0}^{S_g-1} H(I_i + z/S_g) \right\}. \quad (22)$$

It bounds $\sup_{y: |w^T y| \geq \gamma} \mathbb{E}_z \Pr(\text{wrong} \mid y, z)$, including both eigenphases, ties and every reachable head transcript. Numerical evaluation uses enclosing intervals and upward rounding of the final probability bound. If a stated sufficient condition is not met, the bound is taken to be one.

The proof in Appendix J.2 uses forward and backward bad-outcome angular distances of at least g and $\sqrt{2g}$, respectively. It averages the bounds for the finite set of shifted grids before taking the supremum over phases.

The same measurement can be implemented by zero padding. Prepare the m -qubit sine clock and append r zero qubits as its high bits. Apply controlled powers only on the low m bits and perform the $(m+r)$ -qubit inverse QFT. If $k = S_g j + z$, its Kraus operator obeys

$$K_{S_g j + z}^{\text{pad}} = S_g^{-1/2} K_{z, j}^{\text{shift}}, \quad K_{z, j}^{\text{shift}} = P^{-1/2} \sum_{t=0}^{P-1} a_t e^{-2\pi i (j+z/S_g)t/P} G^t. \quad (23)$$

Thus the padded measurement has the same positive-operator-valued measure (POVM) as the joint randomized outcome (z, j) , for every input density operator, including arbitrary weights of the two eigenphases. Zero padding replaces the classical grid choice with an enlarged inverse QFT of dimension $S_g P$. The controlled powers use $P-1$ calls to the label oracle. The larger QFT and allocated width are included in the cost.

Lu and Lin [15, Section II, Eqs. (4)–(8)] and Patel et al. [14, Section VI] analyze a continuous one-bin shift with a corrected decoder; averaging over the algorithm's randomness yields a guarantee for each

fixed phase. Sine and cosine windows, their improved tails and compact preparation are also established [13, 14, 16]. Here we certify a finite set of dyadic shifts for the head-shifted cosine sign decision and compile the resulting measurement explicitly. Zero padding is standard Fourier interpolation [17]; (23) identifies its POVM with that of the randomized measurement for arbitrary input states.

5.4 Synthesis and the complete failure budget

Let $\varepsilon_{\text{clk}}, \varepsilon_{\text{ramp}}, \varepsilon_{\text{QFT}}$ bound the operator-norm errors of the sine-window preparation, phase ramp and inverse QFT, respectively. For the ramp, take the largest error over all random choices. With fresh independent z on every one of K runs, exact binomial amplification gives

$$\delta_{\text{total}} \leq B_K(p_{P,S_g}) + 2K(\varepsilon_{\text{clk}} + \varepsilon_{\text{ramp}} + \varepsilon_{\text{QFT}}) + 0.01. \quad (24)$$

For zero padding, $\varepsilon_{\text{ramp}} = 0$, and ε_{QFT} bounds the error of the enlarged inverse QFT. For ordinary QPE, $\varepsilon_{\text{clk}} = \varepsilon_{\text{ramp}} = 0$, and its statistical bound p_* replaces p_{P,S_g} . The binomial bound uses fresh independent grid shifts across runs (Appendix J). Source approximation defines the actual reflection and contributes to β . Clock and ramp are prepared once per run. Within each fixed classical branch, the phase introduced by ramp synthesis is global and preserves outcome probabilities. Each inverse is the exact reversed gate sequence with adjoint gates. Resource estimates assume that the eventual fault-tolerant implementation has whole-program logical failure probability at most 0.01. Head-sum arithmetic and the 48-bit cosine decoder are classical computations.

6 Logical resource counts

All rows below use the same margin, approximation-bias and failure requirements: $\gamma = 0.002$, $\beta \leq 0.0002$, $\delta < 0.05$, including the conditional whole-program logical-failure allowance 0.01. The gate totals use explicit Clifford+T sequences and include initialization, source preparation, reversible computation and its inverse, controlled gates, reflections, sine-window preparation, phase ramps, inverse QFT and all repetitions. The opaque label-oracle internals are excluded. Non-oracle depth counts layers of public gates along the compiled dependency schedule; T depth counts T-gate layers in that schedule. The reported bounds are conservative, with QFT gates serialized and no parallel oracle copies. Width is the number of allocated logical qubits. Maximum consecutive oracle calls means the most oracle calls in one coherent QPE run, between initialization and measurement; public gates may intervene. It equals $P - 1$ for these schedules, whereas total label queries include the measured head and all K runs: $|H| + K(P - 1)$. Table 2 compares complete readout schedules for the same cubic observable; Figure 3 compares total T count, maximum consecutive oracle calls and allocated logical qubits.

Readout	Total label queries	Maximum consecutive oracle calls	T count (10^6)	T depth (10^6)	Logical qubits
Numerical QPE (7 runs)	118,777	16,383	1693.156	959.656	586
Sign QPE (3 runs)	53,245	16,383	725.638	411.281	586
Sine QPE (1 run)	36,863	32,767	483.762	274.184	587
Randomized grid (1 run)	20,479	16,383	241.884	137.096	586
Zero padding (1 run)	20,479	16,383	241.888	137.102	588

Table 2 Complete logical counts for the same $N = 2^{68}$ cubic observable and measured 4096-label head. Numerical QPE uses the standard numerical-error bound; sign QPE bounds sign errors directly. The remaining methods use a sine window. The randomized row selects one of four shifts for one run. All repetitions are sequential, and T counts are worst-case over the random choice. Counts are calculated from compiled gate sequences and finite loop lengths.

The randomized-grid program has non-oracle depth 414,917,110. Zero padding has non-oracle depth 414,931,532 and uses 241,887,769 T gates. The randomized scheme uses 241,883,741 T gates in the worst case and 241,882,843.5 on average over the four grid shifts. The phase ramp selected by the two random bits adds at most 1,795 T gates and 4,544 non-oracle gates, with T depth 147 and non-oracle depth 374. Each iterate costs 14,763 T gates and has T-depth 8,367. The lower total cost comes chiefly from reducing the number of uses of this same iterate.

The $N = 4096$ and $N = 2^{68}$ instances both use $(\tau, \lambda, \eta) = (1, 0.1, 0.375)$, coefficient-truncation degree 25, 51 Fourier samples and residual-truncation radius $R_{\text{desc}} = 128$. At $N = 4096$, the head has 256 labels; the cubic response uses $M = 2$, exact fraction coordinates, $b_{\text{coin}} = 18$ and 28 stored controls. At $N = 2^{68}$ the cubic construction uses $M = 8$, $b_{\theta} = 19$, $b_{\text{coin}} = 23$, nine response tables shared across shells, and 225 stored controls occupying 5,400 bits. The stored head weights and addresses occupy 479,232 bits. These storage figures describe the label-independent data used by the circuit. The readout schemes in Table 2 use the same response circuit and source state. For $N = 2^{68}$,

$$Z = 89698095963077/17592186044416, \quad \beta < 0.00003850407.$$

The randomized-grid failure bound is

$$0.029589694438 + 0.000031917874 + 0.01 < 0.05,$$

where the terms are the statistical bound, synthesis-error allowance and whole-program logical-failure reserve, respectively. The gap g incorporates the raw bias and finite decoder error. The finite classical certificate (Appendix E) gives $20,479 < 472,711 \leq R_{0.05}$ for this same exact functional and oracle.

6.1 Parameter dependence and limits of the comparison

At $N = 2^{68}$ and fixed $P = 16,384$, the certified probabilities for $S_g = 1, 2, 4, 8, 16$ are 0.098735832769, 0.049369062488, 0.029589694438, 0.021706251487 and 0.018326817905 (bounds rounded upward). For $S_g = 1$ and 2, these sufficient bounds do not certify a single run within the stated failure budget. The comparison considers powers $P = 2^m$, $1 \leq m \leq 18$, odd $K \leq 127$ and the actual synthesis cost, separately for each measurement implementation and response. The reported minima apply to this finite set. At $N = 4096$, unshifted cubic sine readout uses 2,303 label queries and 8,725,747 T gates; four shifts add 1,367 T gates without reducing $P = 2048$. At $n = 18$ and $(\tau, \lambda, \eta) = (1.0625, 0.13, 0.34375)$, the least-cost compiled schedule in the comparison uses $S_g = 1$ for the cubic response and $S_g = 2$ for the linear response. At $n = 30$ and $(\tau, \lambda, \eta) = (0.8125, 0.11, 0.21875)$, the selected schedules for both responses use $S_g = 4$, reducing P from 16,384 to 8,192. The companion reproducibility archive contains all 80 comparisons, with their exact parameters and certificate identifiers. Its public-deposit status is stated under Data and code availability below.

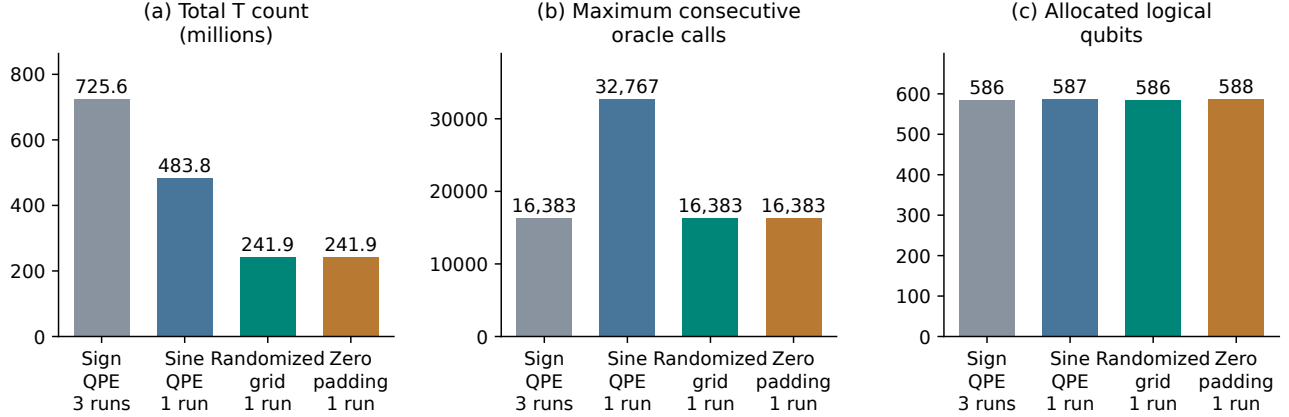


Fig. 3 Logical costs for the same cubic observable and measured 4096-label head as Table 2, at $N = 2^{68}$, margin 0.002 and failure below 0.05, under the whole-program logical-failure assumption of 0.01. Panels show (a) total T count, (b) maximum consecutive oracle calls and (c) allocated logical qubits. The randomized-grid readout samples one of four shifts per run. Public logical costs exclude oracle internals and physical error correction. Values come from the compiled resource records.

7 Discussion and conclusions

The results connect a family-specific query separation to an explicit quantum circuit. The chosen real-Nyquist interpolation rule produces the harmonic tail. Bounded polynomial observations and reversible coordinate generation give an explicit implementation of the resulting signed observable. For the principal finite instance, randomized phase-grid readout reduces total T count and total query count while retaining the maximum number of consecutive oracle calls of the three-run sign-QPE schedule in Table 2.

The query theorem treats label-independent preparation as free, whereas the circuit comparison includes its public quantum cost. Classical algorithms may sample the same signed observation, use the measured head, or query adaptively. An explicitly supplied array permits $w^T y$ to be accumulated during an $O(N)$ pass, and a public label generator supplies information beyond oracle access. The lower bound here assumes access through the specified label oracle.

The query-complexity theorem uses a fixed raw margin, and the finite cost comparisons concern the stated parameter set and compiled schedules. Here N is the size of an implicit oracle address space. A physical implementation would additionally require oracle realization, routing and error correction, together with an assessment of end-to-end runtime and the assumed whole-program logical failure of 0.01.

Declarations

Use of artificial intelligence. ChatGPT and OpenAI Codex assisted with proof development, code development and numerical verification. That said, the author takes responsibility for the original idea and human verification.

Appendix

A Reversible implementation and error analysis

The sampler selects a side and a shell, and a uniform offset determines an n -bit address. Retain g_{cell} bits to select one of $M = 2^{g_{\text{cell}}}$ cells and another b_θ bits for the local position $\tilde{\theta}$ within the cell. Three separate b_θ -bit seeds produce three comparison results. A reversible count of successful comparisons selects b_K . The lookup loads a threshold with b_{coin} fractional bits and a separate flag for probability one. Another independent seed tests acceptance. Rejected branches receive a fair sign; they are never postselected or restarted.

Neighboring cubics share their endpoints. We therefore compute the index $3j + K$ reversibly and store $3M + 1$ controls per angle table. The additions, their carries, lookup decoder and their inverses are included in the compiled gate sequences and resource counts. This layout saves T gates but can increase allocated width.

Let x' be x rounded down to the retained coordinate precision. This rounding changes f_a by at most $(\pi^2/8)2^{-(g_{\text{cell}}+b_\theta)}$, since $|f'_a| \leq \pi^2/8$. We bound the interpolation term $Q(x') - f_a(x')$ and the coordinate-rounding term $f_a(x') - f_a(x)$ separately. Rounding each control to b_{coin} probability bits costs at most $2^{-b_{\text{coin}}}$ once, by convexity of the Bernstein basis.

For small-angle shells $L \leq N/2^c$, one common reciprocal table suffices:

$$0 \leq 1/x - a \cot(ax) \leq 8(L/N)^2, \quad B_{\text{small}} \leq (64/3)m_{\text{sh}}4^{-c}.$$

This follows from the positive cotangent expansion $0 \leq 1 - z \cot z \leq (2z/\pi)^2$ on $[0, \pi/2]$. For J shells, $Z = 2Jm_{\text{sh}}$. The measured-head bias satisfies, for every label vector,

$$\begin{aligned} \beta \leq & B_{\text{Fourier}} + B_{R_{\text{desc}}} + B_{\text{dyadic}} + B_{\text{source}} + B_{\text{small}} \\ & + 2m_{\text{sh}} \sum_k \left[e_{\text{int},k} + 2^{-b_{\text{coin}}} + \frac{\pi^2}{8} 2^{-(g_{\text{cell}}+b_\theta)} \right]. \end{aligned} \quad (25)$$

The last term is zero for exact coordinates. Use $e_{\text{int},k} = A_5(M)/(81M^4)$ when $k \geq g_{\text{cell}}$ and the uniform bound otherwise. Here m_{sh} is the stored dyadic mass defined in Section 3; its rounding error is included in B_{dyadic} . The sum runs over $k = r_0, \dots, n-2$ with $r_0 = \log_2 R_{\text{head}}$. Here B_{Fourier} is the coefficient truncation and finite-transform error, $B_{R_{\text{desc}}}$ is the residual tail in (13), and B_{dyadic} covers head and shell-mass rounding. The source term is $B_{\text{source}} = 2ZE_U$, as in Proposition 3. A categorical selector with E outcomes and b_{sel} -bit probability thresholds instead has the bound $2ZE2^{-b_{\text{sel}}}$.

At fixed heat parameters $J = O(n)$, so $M = O((n/\varepsilon_{\text{raw}})^{1/4})$ suffices for the response interpolation allocation, compared with the square-root dependence of centered linear interpolation. Sharing small angles leaves $O(M \log(1/\varepsilon_{\text{raw}}))$ controls. The weight description still contains $O(\varepsilon^{-1/2})$ head entries at descriptor accuracy ε . The joint coordinate mapping uses $O(n + f \log J)$ nonlinear Boolean gates, and the cubic response uses three independent comparison seeds rather than the single seed of linear interpolation.

A.1 Equal-shell source

After measuring the head, every side-shell has the same proposal mass. A generic categorical implementation compares a uniform seed with every cumulative boundary. Equal shell masses allow the simpler preparation

$$|\psi_J\rangle = J^{-1/2} \sum_{s=0}^{J-1} |s\rangle$$

and an independent side bit. A reversible binary decoder supplies the bits identifying the selected shell. For $J = 4$ the source is two Hadamards. For $J = 56$, factor it as a uniform seven-state source and three Hadamards. The compiled preparation uses 325 T gates; reversing the gate sequence gives its inverse at the same cost.

For arbitrary J , the binary probability tree has at most one incomplete prefix at each depth. Full subtrees use Hadamards. Synthesized rotations are needed only along that prefix, giving at most $\lceil \log_2 J \rceil$ angles and $O(\log^2 J)$ exact prefix-control work in our construction. The one-hot decoder costs $O(J)$; the following construction reduces the joint address and fraction work.

A.2 Joint address and probability layout

Let the consecutive shells be $k = r_0 + s$, $0 \leq s < J$, with binary shell index s and one-hot bits e_k . An independent uniform offset seed U gives $j = 2^k + (U \bmod 2^k)$. The label address is $j + 1$ or $-j$ modulo N , according to the side. Probability generation also needs

$$F_{\text{coord}} = \left\lfloor 2^f \frac{(U \bmod 2^k) + \alpha}{2^k} \right\rfloor, \quad \alpha \in \{\eta, 1 - \eta\}.$$

Here $f = g_{\text{cell}} + b_\theta$ and η has an exact e -bit dyadic representation. The same shell index also determines the bit window needed for the probability coordinate.

For the address, a suffix chain of controlled-NOT (CNOT) gates temporarily turns e_k into cumulative masks. One AND per bit then gives $j_i = e_i \oplus (U_i \wedge \bigoplus_{k>i} e_k)$; reversing the CNOTs restores the decoder. Conditional complementation followed by a reversible increment and copy produces either sign of the address.

For the fraction, write $\alpha = a/2^e$, $A = 2^e U + a$ and $t = f - e - r_0$. Then $F_{\text{coord}} = \lfloor A2^{t-s} \rfloor \bmod 2^f$. With $m = \lceil \log_2 J \rceil$, select register wires without copying their contents to obtain the $W = f + 2^m - 1$ consecutive bits of the binary expansion of $A2^t$ starting at the units bit, adding zero-initialized wires where padding is needed. For $b = m - 1, \dots, 0$, conditionally rotate the prefix of length $L_b = f + 2^{b+1} - 1$ by 2^b , controlled by s_b . Its shorter output prefix never contains wrapped bits. Retaining the unused suffix preserves the information required to reverse the permutation. Appendix I proves the claim.

The permutation is applied after the label address has been computed. Subsequent coin comparisons read the resulting fraction wires, while all offset wires remain part of the source reflection. For the large instance, this construction uses 267 Toffoli (CCX) gates for the address and 246 for the fraction. Computing a separate address and coordinate for every shell would use 2557 and 1196, respectively. Including the inverse, their T costs are 4104 and 30,024. The two implementations produce the same probability coordinates. For even f , two reversal passes and coherent control copies in clean borrowed carry wires give the same swap count with a better joint dependency schedule. Odd f may require extra swaps, so the finite implementation retains the cycle schedule there.

A.3 Measured head and exact descriptor threshold

Use $\bar{w}$ for the public descriptor before response and source approximation. Query a public head H once and accumulate the exact dyadic quantity $c_H = \sum_{i \in H} \bar{w}_i y_i$. In this section and the readout, $\tilde{s}_{\text{tail}}$ denotes the implemented tail mean $Z\mathbb{E}X$, after every response, probability and source approximation. Set $\tilde{s} = c_H + \tilde{s}_{\text{tail}}$. Equation (25) guarantees $|s - \tilde{s}| \leq \beta$ on every label vector. The decision is $\text{sign}(c_H + \hat{s}_{\text{tail}})$. If $|s - \tilde{s}| \leq \beta$ for all labels and $|\hat{s}_{\text{tail}} - \tilde{s}_{\text{tail}}| \leq e$ except with probability δ , then $\beta + e < \gamma$ guarantees the promised sign with probability at least $1 - \delta$ on every input. Indeed, on that event, $|c_H + \hat{s}_{\text{tail}} - s| \leq \beta + e < \gamma \leq |s|$. The observed head sum shifts the decision threshold. The phase size, repetition count and tail precision depend only on public parameters and the promised margin.

The cost includes all $|H|$ label calls, public weights, coefficient generation, products, additions and storage. The radius is selected from the stated finite parameter set, with the same head supplied to

every measurement method in the comparison. The signed weights are summed before magnitudes are taken, so cancellation in the head is preserved. Classical algorithms receive the same head and may also exploit it.

In the finite constructions the coefficient degree is 25 and the residual truncation radius is 128. Enlarging the measured radius beyond 128 uses the same public descriptor: outside the truncation radius its weights moved into the measured head are dyadic roundings of bq . Their rounding is charged to B_{dyadic} , and the omitted residual is still charged at $R_{\text{desc}} = 128$. The tail shells begin at R_{head} (2048 in the large case). At measured radius 2048, the head contains 4096 labels; the additional 3840 cardinal evaluations are public preprocessing.

A.4 Restricted relative-phase replacement

A monomial relative-phase implementation $\tilde{B}$ has the same basis permutation as B and differs by a diagonal input phase. If the middle operation D is diagonal on the registers computed by B and restores its ancillary targets, then

$$\tilde{B}^\dagger D \tilde{B} = B^\dagger D B. \quad (26)$$

The exact adjoint cancels the relative phases because $B^\dagger D B$ is diagonal on that subspace. This is a specialization of the established relative-phase framework of Maslov [10]. The implementation applies this identity with the exact adjoint and an exact middle operation diagonal on the relevant subspace.

The source reflection uses a fully coherent one-clean-ancilla conditionally clean ancilla construction following Khatarr–Gidney [11]. Its computation is paired with its exact adjoint around a central exact operation. This replacement is used only where all ancillary work registers are restored to zero. All comparison methods use the same compilation rules, retention of random seeds and synthesis precision.

B Numerical-estimation baseline

For comparison, the amplitude-estimation bound of Brassard et al. [3, Theorem 12] gives raw numerical error

$$e(P, Z) = 2Z(\pi/P + \pi^2/P^2) \quad (27)$$

with success at least $8/\pi^2 > 0.81$. With the binomial function in (17), seven independent runs suffice, since $B_7(0.19) < 0.027927555723$. The median tail estimate, added to the exact head, has the correct promised sign when

$$\beta + e(P, Z) + 2Z^{-48} < \gamma. \quad (28)$$

The last term bounds classical cosine decoding (Appendix H); ties are counted as failures. This numerical guarantee is stronger than a sign guarantee. The direct ordinary-QPE and sine-window bounds are derived together in Appendix J.

C Proof of the finite diffuse-tail lemma

Let the tail signs t_i be independent with mean $\mu_\pm$, and define the total score $S = c + \sum_i a_i t_i$. Then $\mathbb{E}_\pm S = \pm 2\gamma$. Since $a_i t_i$ has range $2a_i$, one-sided Hoeffding gives

$$\Pr_{\mu_+}\{S < \gamma\}, \Pr_{\mu_-}\{S > -\gamma\} \leq e^{-\gamma^2/(2V)} \leq \rho.$$

Let $P(t)$ be the probability of output $+1$, so $0 \leq P \leq 1$ also off promise. Then $\mathbb{E}_+ P \geq (1 - \rho)(1 - \delta)$ and $\mathbb{E}_- P \leq (1 - \rho)\delta + \rho$; their difference is at least D_* . Using the unconditioned priors preserves independence of the unqueried labels.

Expose a classical algorithm's private randomness, which is input independent. Given its transcript, each unqueried tail bit retains its Bernoulli prior. A repeated query or a public-head query adds no relative entropy. The adaptive chain rule bounds transcript KL by $Td_{\max}$ after at most T queries, including stopping padded to T . Total variation is at least D_* , while Pinsker bounds it by $\sqrt{Td_{\max}/2}$. Hence $T \geq 2D_*^2/d_{\max}$. For $(p, q) = (p_+, p_-)$ or (p_-, p_+) , we have $p, q \in [1/4, 3/4]$ and $|p - q| = 2\gamma/M$, so

$$D_{\text{KL}}(p||q) \leq \frac{(p - q)^2}{q(1 - q)} \leq \frac{64\gamma^2}{3M^2},$$

which gives (7).

A T -query quantum algorithm has a multilinear acceptance polynomial of degree at most $2T$ in the unknown signs [4]. Oracle entries, including controlled entries, are affine in the addressed sign. Public gates do not depend on labels. Deferring intermediate measurements and averaging classical randomness preserve this bound. If the original budget holds only on promised inputs, truncate every branch before query $T + 1$ and output an arbitrary sign on truncated branches. Promised behavior is unchanged; off-promise acceptance now also lies in $[0, 1]$ on the entire Boolean cube. Refusal may be mapped to an arbitrary sign since it already counts as failure on promised inputs.

Independence gives the polynomial $F(\mu) = \mathbb{E}_\mu P(t) = \sum_A p_A \mu^{|A|}$, of degree at most $2T$, with $0 \leq F \leq 1$ throughout $[-1, 1]$. Bernstein's inequality for $2F - 1$ implies $|F'(\mu)| \leq T/\sqrt{1 - \mu^2}$. Integrating between the two means yields

$$D_* \leq F(\mu_+) - F(\mu_-) \leq T[\arcsin(\mu_+) - \arcsin(\mu_-)].$$

On $[-1/2, 1/2]$, the derivative of arcsine is at most $2/\sqrt{3}$; the mean gap is $4\gamma/M$. This proves (8).

D Regularity, localization and a sufficient threshold

We first consider the case $b \neq 0$ in Theorem 1. Write $w_N = bq_N + v_N$. The Fourier-series coefficients of the periodic function g , with the inverse-transform sign convention, are $\hat{g}_j = (2\pi)^{-1} \int_{-\pi}^{\pi} g(\theta) e^{ij\theta} d\theta$. Absolute summability of the Fourier coefficients permits finite-cycle aliasing: $v_N(r) = \sum_{\ell \in \mathbb{Z}} \hat{g}_{r+\ell N}$. Since $g(\pi) = g(-\pi) = 0$, the real Nyquist convention adds no residual. Set $B(R) = \sum_{|j| > R} |\hat{g}_j|$ and $G = \sum_j |\hat{g}_j|$. Then $\|v_N\|_1 \leq G$ and $\sum_{|r| > R} |v_N(r)| \leq B(R)$ for $N \geq 2R + 4$.

For a fixed integer $R \geq 1$ and $N \geq 2R + 4$, define

$$M_N = \sum_{|r| > R} |w_N(r)|, \quad V_N = \sum_{|r| > R} |w_N(r)|^2, \quad c_N = \sum_{|r| \leq R} w_N(r).$$

Thus c_N is the known head contribution when all its labels are fixed to $+1$. Put $\kappa = |b \sin(\pi\eta)|/\pi$. Harmonic comparison of the cotangent sum gives $\|bq_N\|_1 = 2\kappa \log N + O(1)$, hence the same leading term for $\|w_N\|_1$. Outside this head,

$$\sqrt{V_N} \leq \kappa \sqrt{(R - \eta)^{-1} + (R + \eta)^{-1}} + B(R).$$

This tends to zero uniformly in large N . Fix all head labels to $+1$. The full signed weight sum is $m(0)$; the alternating cardinal tail is bounded by its first terms, giving

$$|c_N| \leq \bar{c} = |m(0)| + \kappa[(R + 1 - \eta)^{-1} + (R + 1 + \eta)^{-1}] + B(R).$$

A convenient mass lower bound is

$$M_N \geq 2\kappa \left[\log \frac{N}{2(R + 1 + \eta)} - 1 \right] - B(R).$$

Choose a fixed R for the variance condition in (6). For this R , every even N exceeding both $2R + 4$ and

$$2(R + 1 + \eta) \exp \left[1 + \frac{2\bar{c} + 4\gamma + B(R)}{2\kappa} \right]$$

satisfies $M_N \geq 2\bar{c} + 4\gamma$, placing both prior means in $[-1/2, 1/2]$. Increasing the threshold until $M_N \geq \kappa \log N$ gives explicit lower constants. An algorithm for the original task also solves this restricted family, since its head queries can be answered from the publicly fixed labels. Hence a lower bound for the restricted family also applies to the original task.

Signed importance sampling with $\lceil 2\|w\|_1^2 \log(2/\delta)/\gamma^2 \rceil$ samples proves the classical upper bound. Exact public preparation and the amplitude-estimation algorithm of Brassard et al. [3], repeated with median postprocessing, give the quantum upper bound in the query model, where label-independent preparation is free.

If $b = 0$, choose R with $B(R) < \gamma$. The weighted sum over the queried head differs from s by at most $B(R) < \gamma \leq |s|$, so it has the correct sign. At an integer interpolation site, truncation uses the Fourier tail of m . For real even C^2 periodic m , g, g' match at the endpoints and $|\hat{g}_j| \leq \|g''\|_1/(2\pi j^2)$. The analytic heat multiplier has exponentially decaying Fourier coefficients, so its weights at an integer interpolation site have exponential tails. The even brick-wall multiplier $\mathbf{1}_{\{|\theta| < \pi/2\}}$ has zero endpoint but harmonic coefficients caused by its interior jumps. It rules out an endpoint-only classification without regularity. For fixed feasible normalized margin $0 < \Gamma \leq 1$, importance sampling and amplitude estimation use $O(\Gamma^{-2})$ and $O(\Gamma^{-1})$ queries. At least one query is necessary for nonzero weights and $\delta < 1/2$, using the two opposite inputs $\pm \text{sign}(w)$.

E A finite classical lower bound

The calculation uses exact parameters and rigorous enclosing intervals; the displayed decimals summarize these certified quantities. Let $h_0 = (1 + \lambda)^{-1}$, $b = (1 + \lambda e^{4\tau})^{-1}$, $\kappa = b \sin(\pi\eta)/\pi$, and

$$D_1 = \tau/2, \quad D_2 = \tau/2 + \tau^2, \quad D_3 = \tau/2 + 3\tau^2 + 2\tau^3.$$

These constants satisfy $\|h^{(j)}\|_\infty \leq D_j$ for $j = 1, 2, 3$. Three integrations by parts for $g = (h - b)e^{-i\eta\theta}$, including the endpoint jump of g'' , give $|\hat{g}_j| \leq E_3/|j|^3$, where

$$E_3 = D_3 + 3\eta D_2 + 3\eta^2 D_1 + \eta^3(h_0 - b) + 2\tau b(1 - b) \sin(\pi\eta)/\pi.$$

The last term is the boundary jump divided by 2π ; g and g' themselves match. Thus $B(R) \leq E_3/R^2$. For $N = 2^n$, the quantities defined in Appendix D satisfy $|c_N| \leq \bar{c}$, $V_N \leq \bar{V}$ and $M_N \geq \underline{M}$, where

$$\begin{aligned} \bar{c} &= h_0 + \kappa[(R + 1 - \eta)^{-1} + (R + 1 + \eta)^{-1}] + E_3/R^2, \\ \bar{V} &= \left[\kappa \sqrt{(R - \eta)^{-1} + (R + \eta)^{-1} + E_3/R^2} \right]^2, \\ \underline{M} &= 2\kappa[(n - 1) \log 2 - \log(R + 1 + \eta) - 1] - E_3/R^2. \end{aligned} \tag{29}$$

Use the finite parameters

$$(n, \tau, \lambda, \eta, \gamma, \delta, \rho, R) = (68, 1, 0.1, 0.375, 0.002, 0.05, 0.02, 8111).$$

Here $R = 8111$ is the publicly fixed head radius used in the hard-input proof; the circuit uses $R_{\text{head}} = 2048$. The proof supplies its fixed head labels freely and bounds queries to the remaining labels. Restricting to this family gives a lower bound for the original oracle problem.

With these parameters, outward intervals verify $\bar{V} \leq \gamma^2/[2 \log(1/\rho)]$ and $\underline{M} \geq 2\bar{c} + 4\gamma$. Here $\underline{M} \approx 3.3178010976$ and $D_* = 0.862$.

Define the extremal prior parameters $p_{\pm}^* = (1 + (-\bar{c} \pm 2\gamma)/\underline{M})/2$ and

$$d_{\text{ext}} = \max\{D_{\text{KL}}(p_+^* \| p_-^*), D_{\text{KL}}(p_-^* \| p_+^*)\}.$$

For $M = \underline{M}$, joint convexity makes the worst directed relative entropy over $c \in [-\bar{c}, \bar{c}]$ occur at an endpoint. The two endpoints give the same maximum over the two directions by Bernoulli complement symmetry. For fixed c , increasing M contracts both sign means by the same factor $\underline{M}/M$. This contraction is a binary symmetric channel, so data processing cannot increase either directed relative entropy. Thus $d_{\text{max}} \leq d_{\text{ext}}$ for every admissible actual head sum and tail mass. Inserting this uniform upper bound into Lemma 1 gives

$$R_{\delta} \geq \left\lceil 2(0.862)^2/d_{\text{ext}} \right\rceil = 472,711.$$

F Coefficient generation and raw descriptor bounds

Choose the strip width $a_{\text{strip}} = 0.9 \operatorname{asinh}(\pi/(4\tau))$ and put $z = e^{-a_{\text{strip}}}$. On $|\Im\theta| \leq a_{\text{strip}}$, the exponential term in the denominator of $F(\cos\theta)$ has positive real part, so $|h(\theta)| \leq 1$ and $|\alpha_m| \leq z^{|m|}$. Let $c_{\eta} = \sin(\pi\eta)/\pi$, $A_{\eta} = \eta^{-1} + (1 - \eta)^{-1}$, and

$$B_m = 4c_{\eta}[A_{\eta} + 2(1 + \log(4m + 1))] + \pi^2 \sin(\pi\eta).$$

To prove $\|\Delta_m q\|_1 \leq B_m$, first suppose $m < N/8$. On $|r - \eta| < 2m$, the triangle inequality bounds the four cardinal terms by harmonic partial sums of radius $3m$, giving

$$\sum_{|r-\eta| < 2m} |\Delta_m q(r)| \leq 4c_{\eta}[A_{\eta} + 2(1 + \log(3m + 1))].$$

On the complement, the second-difference estimate $|\Delta_m q(r)| \leq 2\pi^2 \sin(\pi\eta)m^2/|r - \eta|^3$ also follows from the sharper cotangent estimate below. The two tails obey

$$\sum_{|r-\eta| \geq 2m} |r - \eta|^{-3} \leq 2 \left[(2m)^{-3} + \int_{2m}^{\infty} x^{-3} dx \right] \leq \frac{1}{2m^2},$$

so their contribution is at most $\pi^2 \sin(\pi\eta)$. If $m \geq N/8$, use $\|\Delta_m q\|_1 \leq 4\|q\|_1$ and

$$\|q\|_1 \leq c_{\eta}[A_{\eta} + 2(1 + \log(N/2))].$$

Since $N/2 \leq 4m$ in this case, both cases give the stated B_m , uniformly for every integer $m \geq 1$ and every even $N \geq 2$. Because $1 + \log(4m + 1) \leq \log 5 + m$, put $U = 4c_{\eta}(A_{\eta} + 2\log 5) + \pi^2 \sin(\pi\eta)$ and $V_0 = 8c_{\eta}$. The omitted Fourier terms contribute at most

$$\sum_{m > d} |\alpha_m| B_m \leq z^{d+1} \left[\frac{U + V_0(d+1)}{1-z} + \frac{V_0 z}{(1-z)^2} \right]$$

to the raw-score error, uniformly over all label assignments. Approximating the retained coefficients by an M_F -point trapezoidal transform, with $M_F > d$, gives raw-score aliasing error at most

$$\sum_{m=1}^d \frac{z^{M_F-m} + z^{M_F+m}}{1 - z^{M_F}} B_m.$$

The numerical examples use $M_F = 51$, $d = 25$.

For the inverse-cubic spatial tail bound, take $t = |r - \eta| \geq 2m$ in the canonical half-cycle, so $t \leq N/2$, and define

$$C_{m,N}(t) = \cot \frac{\pi(t-m)}{N} + \cot \frac{\pi(t+m)}{N} - 2 \cot \frac{\pi t}{N}.$$

This difference is nonnegative on $2m \leq t \leq N/2$. Its partial-fraction power series equals the harmonic symmetric difference minus nonnegative even differences of positive powers, giving

$$0 \leq \frac{C_{m,N}(t)}{N} \leq \frac{2m^2}{\pi t(t^2 - m^2)}.$$

Since $|\Delta_m q(r)| = \sin(\pi\eta)C_{m,N}(t)/N$ and $m/t \leq 1/2$, $|\Delta_m q(r)| \leq 8 \sin(\pi\eta)m^2/(3\pi t^3)$. Summing both rays by the integral test gives (13).

Rounding the signed head entries adds the sum of their absolute errors. Rounding the common shell mass contributes at most $2J|m_{\text{sh}} - m_{\text{sh}}^{(0)}|$, since each of the $2J$ side-shells has an acceptance probability at most one.

A selector distribution error in ℓ_1 changes the score by at most Z times that error. For the response construction, the bias formula (25) combines the response and source errors. Public cardinal and Fourier evaluations use outward intervals, followed by exact dyadic thresholds.

G Control range, cell occupancy and retained sources

Derivative bounds. For $0 < z \leq \pi/2$, put $t = \cot z \geq 0$ and write $(d/dz)^r \cot z = P_r(t)$, $P_0 = t$ and $P_{r+1} = -(1+t^2)P'_r$. Then $(-1)^r P_r$ has nonnegative coefficients by induction. Even derivatives of f_a are nonnegative. For $a > 0$, the convergent cotangent expansion gives $f_a(x) = 1/x - \sum_{m \geq 1} d_m x^{2m-1}$, $d_m > 0$. Termwise even differentiation on $ax \leq \pi/2$ therefore gives $0 \leq f_a^{(2r)}(x) \leq (2r)!/x^{2r+1}$, including the $a = 0$ limit. In particular $f_a^{(4)} = 8a^5 \cot(ax) \csc^2(ax)(2 + 3 \cot^2(ax))$.

Control range and interpolation error. Write $f = f_a$ and let H be its cubic Hermite interpolant on $[l, l+h]$. Its Bernstein controls are $H_0 = f(l)$, $H_1 = f(l) + hf'(l)/3$, $H_2 = f(r) - hf'(r)/3$, $H_3 = f(r)$, $r = l+h$. Convexity gives $0 \leq H_2 \leq f(l) \leq 1$ and $H_1 \leq f(l)$. Moreover

$$\frac{f(l)}{-f'(l)} = \frac{\sin(2al)}{2a} \geq \frac{2(2-l)}{\pi} \geq \frac{2h}{\pi} > \frac{h}{3}.$$

To justify the first inequality, for fixed l the function $\sin(2al)/(2a)$ decreases with a on this interval, and at $a = \pi/4$ use the chord of sine from $\pi/2$ to π . The zero-angle limit is immediate. Hence $H_1 \geq 0$. The Hermite remainder lies in $[0, h^4/(16l^5)]$ for $f - H$.

For the equispaced cubic, divided-difference endpoint derivative remainders give $Q'(l) = f'(l) + d_l$ and $Q'(r) = f'(r) - d_r$, where $0 \leq d_l, d_r \leq 2h^3/9$. Thus $b_1 \geq H_1 \geq 0$, $b_2 \geq H_2 \geq 0$. Since $-f'(x) \geq 1/x^2 \geq 1/4$ and $h \leq 1$, $Q'(l) < 0$ and $b_1 \leq f(l)$. Also

$$f(l) - H_2 \geq 2h|f'(r)|/3 \geq h/6, \quad b_2 - H_2 \leq 2h^4/27 < h/6.$$

This proves $b_2 \leq f(l) \leq 1$. The endpoint controls are already bounded. The nodal product $\theta(\theta - 1/3)(\theta - 2/3)(\theta - 1)$ has maximum absolute value $1/81$, attained at $1/2 \pm \sqrt{5}/6$. The standard interpolation remainder proves (15).

Cell occupancy. Suppose first that $k \geq g_{\text{cell}}$. Write the integer offset as $u = jD + r$, where $D = 2^{k-g_{\text{cell}}}$ and $0 \leq r < D$. Both side fractions $\alpha = \eta, 1 - \eta$ lie in $(0, 1)$, so $\lfloor j + (r + \alpha)/D \rfloor = j$. Each cell therefore contains D offsets. Flooring after $g_{\text{cell}} + b_\theta$ bits preserves the first g_{cell} cell bits. Summing local absolute remainder bounds proves the mean-cell certificate for arbitrary label signs. For $k < g_{\text{cell}}$, the uniform interpolation bound applies.

Independent seeds and exact endpoints. Three independent comparison seeds are essential. If controls are $(1, 0, 0, 0)$ and $\theta = 1/2$, independent coins give expectation $1/8$; reusing one seed gives $1/2$. The coherent circuit retains the seeds and all correlated work until uncomputation. A magnitude register must also represent threshold $2^{b_{\text{coin}}}$ for probability one; a separate reversible predicate handles that case. This flag distinguishes probability one from zero, since the threshold $2^{b_{\text{coin}}}$ has zero in each of its lower b_{coin} bits.

The shared table uses index $3j + K$; $K = 3$ at cell j and $K = 0$ at cell $j + 1$ have identical endpoint values. Clean-output reversible adders retain their carries until the inverse. The shared endpoint controls use the same quantized value in both adjacent cells. The circuit also defines its reversible computation on unused register codes and assigns them a bounded observation in $[-1, 1]$.

To prepare a uniform superposition of the first J computational-basis states, consider a binary prefix containing both valid and unused codes. Let L and R be its left and right valid-leaf counts. Rotate its next bit with amplitudes $\sqrt{L/(L+R)}$, $\sqrt{R/(L+R)}$; a full child subtree uses Hadamards. There is at most one incomplete child per level. Compute its prefix predicate, perform its controlled rotation, and uncompute that predicate. Rotation gate sequences are certified up to projective operator error. A single uncontrolled phase is global; phases in paired controlled-rotation decompositions cancel because the paired sequences are exact adjoints. We sum the remaining errors to bound the prepared-state distance. The same compiled gate sequence defines the repeated reflection, proving the fixed-source bias bound in Proposition 3.

H Finite rational phase decoding

Use the certified rational upper bound π_+ from Appendix J.2:

$$3.14159265358979323846264338327950288419716939937511.$$

For a phase outcome $j \in \{0, \dots, P-1\}$, set $x = 2\pi_+ j/P$ and compute

$$t_0 = 1, \quad t_k = -\frac{x^2 t_{k-1}}{(2k-1)(2k)}, \quad C_{64}(x) = \sum_{k=0}^{32} t_k \quad (30)$$

using exact rational arithmetic. The Taylor polynomial through degree 65 coincides with C_{64} because all odd coefficients vanish. Its remainder has absolute value at most $(2\pi_+)^{66}/66!$ over the entire outcome range. Replacing π by π_+ changes the argument by at most $2(\pi_+ - \pi)$. Since cosine is one-Lipschitz, the resulting cosine error has the same bound. The sum of this error and the Taylor remainder satisfies

$$(2\pi_+)^{66}/66! + 2(\pi_+ - \pi) < 2^{-49}.$$

Nearest rounding to a 48-fractional-bit dyadic contributes at most 2^{-49} , giving a uniform error strictly less than 2^{-48} . This remains true at quadrant boundaries and the endpoints.

Approximating each cosine estimate changes their median by at most the largest individual approximation error. Multiplication by Z gives the raw-score decoder allowance in (28); the normalized error enters the gap in (18). Exact dyadic head accumulation introduces no additional error. The deterministic implementation evaluates 32 nonconstant terms per outcome; its rational arithmetic and final rounding are classical work, separate from QFT synthesis.

I Reversible dyadic coordinate mapping

Use the shell index, registers and coordinate precision from Appendix A, with $k = r_0 + s$ and $0 \leq s < J$. For a valid one-hot encoding e_k , the suffix XOR above position i equals one exactly when $i < k$. The

leading one and masked offset occupy disjoint positions. Conditional bitwise complementation followed by a single increment-and-copy operation produces either $j + 1$ or $(\neg j) + 1 \equiv -j \pmod{2^n}$, according to the side. All ripple carries are cleared before probability routing.

Writing $U = q2^k + u$ shows $\lfloor 2^f(U + \alpha)/2^k \rfloor = q2^f + \lfloor 2^f(u + \alpha)/2^k \rfloor$. Reduction modulo 2^f proves the coordinate-window formula in Appendix A. If the fixed shift $t = f - e - r_0$ is negative, the selected output begins above the lowest bits; those lower bits remain in the source register.

Before stage b , the possible remaining shift is at most $2^{b+1} - 1$, so $L_b = f + 2^{b+1} - 1$ bits suffice. For every position $i < L_b - 2^b$ in the shorter output prefix, an enabled rotation reads position $i + 2^b < L_b$. Thus no wrapped bit enters the retained prefix. If the control is zero, the prefix is unchanged. Induction establishes the desired f output bits after the last stage. Every stage is a permutation. The unused suffix remains in its register and is restored by the inverse circuit.

A rotation by d on L wires has $\gcd(L, d)$ cycles and uses $L - \gcd(L, d)$ controlled swaps. Summing over stages gives at most $mf + 2^{m+1} - m - 2 = O(f \log J + J)$ swaps; $2^m < 2J$ for $J > 1$. For $J = 1$, no shell-index register is needed and the output uses a fixed selection of wires. The mask, signed increment and decoder add $O(n + J)$ nonlinear Boolean gates. The routing register uses $O(f + J)$ wires, with $O(n)$ retained address/carry work and e side-fraction bits. Representing a general dyadic η requires $O(e)$ additional workspace and Clifford gates; this cost is constant when η is fixed.

For even f , each prefix length is odd, so power-of-two distances have gcd one. Reversing each of the two blocks separated by the rotation offset, then reversing the full prefix, implements the same rotation with $L - 1$ swaps. A CNOT tree copies the shell-index control bit into clean ancillas to control disjoint swaps coherently; these copies are then uncomputed. All borrowed wires must be clean and disjoint from every data/source bit. Depth is computed from dependencies in the complete compiled gate sequence.

The response circuit reads its probability-coordinate input solely from the routed fraction wires. The intervening query phase is diagonal in the computational basis of the registers computed by B . Under the restricted replacements described in Appendix A, the basis-dependent phases introduced by relative-phase gates cancel against the exact adjoint circuit. Seeds return to their original positions before source reflection. Equality on every basis state in the ideal source support preserves the score bound; a different bounded observation on invalid source codes is covered by the same fixed-source norm bound.

J Uniform finite sign guarantees

The implemented observable and the decoder gap. Let $G = (2|\psi\rangle\langle\psi| - I)D_y$ be the implemented iterate, with relevant eigenphases $\pm\phi$ and normalized mean $\cos\phi$. Write the implemented raw score as $\tilde{s} = c_H + Z \cos\phi$, where the measured head sum c_H is accumulated exactly, and assume $|s - \tilde{s}| \leq \beta$ for every label assignment. The promise is $|s| \geq \gamma$; the reported finite instances use $\gamma = 0.002$. The finite cosine decoder $\hat{c}_j$ satisfies $|\hat{c}_j - \cos(2\pi j/P)| < \varepsilon_{\text{dec}} = 2^{-48}$. Define the strictly positive public gap

$$g = \frac{\gamma - \beta}{Z} - \varepsilon_{\text{dec}} > 0. \quad (31)$$

Proposition 4 reduces both score signs to one-sided cosine events with this gap, for every reachable head transcript and with ties counted as failures. The bounds below therefore apply to both eigenphase branches.

J.1 Ordinary QPE: one-sided cosine tails

For $P = 2^m \geq 2$ and $x = P\phi/(2\pi)$, ordinary QPE gives

$$q_\phi(j) = \frac{\sin^2(\pi x)}{P^2 \sin^2(\pi(x - j)/P)}. \quad (32)$$

When x is an integer, the distribution is a point mass at $j = x \bmod P$; the formula is understood by continuity. The map $(\phi, j) \mapsto (-\phi, -j \bmod P)$ preserves measured cosines and their law. The map $(\phi, j) \mapsto (\pi - \phi, P/2 - j \bmod P)$ negates both cosines and preserves the probabilities. Consequently it suffices to bound the lower cosine tail with $0 \leq \phi \leq \pi$; the result covers both error directions and any mixture of the two eigenphase branches.

If $\cos \phi - g < -1$, the lower event is empty. Otherwise let $a = \arccos(\cos \phi - g)$. Its outcome angles lie in the closed arc $[a, 2\pi - a]$. Since cosine is one-Lipschitz, $a - \phi \geq g$. Also $\cos a \leq 1 - g$ and $1 - \cos a \leq a^2/2$, so $a + \phi \geq \sqrt{2g}$. Represent a bad outcome angle relative to ϕ on the real line by adding integer multiples of 2π . Every positive representative is at least g , and every negative representative has magnitude at least $\sqrt{2g}$. We call these representatives periodic lifts. The absolutely convergent identity

$$\csc^2(\pi z) = \frac{1}{\pi^2} \sum_{n \in \mathbb{Z}} (z - n)^{-2}$$

expresses (32) as a sum over these periodic lifts. Dropping the periodic restriction on the bad lifts enlarges their mass. For any positive rational lower bounds $d \leq Pg/(2\pi)$, $b \leq P\sqrt{2g}/(2\pi)$, and $f = x - \lfloor x \rfloor$, this proves

$$p_{\text{wrong}} \leq B(f) := \frac{\sin^2(\pi f)}{\pi^2} \{T(\lceil f + d \rceil - f) + T(\lceil b - f \rceil + f)\}, \quad T(v) = \sum_{k=0}^{\infty} (v + k)^{-2}. \quad (33)$$

At a grid-aligned phase, $x \in \mathbb{Z}$, the point-mass outcome cannot be wrong because $g > 0$, so the bad-outcome probability is zero. Hence no singular term is used in (33). The lift argument includes the periodic endpoints and all threshold equalities.

Here is a finite rational certificate for the supremum in (33). Cover $[0, 1]$ by closed dyadic intervals $J = [L, U]$. On each interval, valid lower tail arguments are

$$v_+ = \max\{d, \lceil L + d \rceil - U\}, \quad v_- = \max\{b, \lceil b - U \rceil + L\}.$$

These inequalities hold at switches of either ceiling as well as between switches. Since T is decreasing, evaluating it at v_+ and v_- gives upper bounds for the two tails. Convexity and the midpoint integral bound give, for $M \geq 1$,

$$T(v) \leq H_M(v) := \sum_{k=0}^{M-1} (v + k)^{-2} + \frac{1}{v + M - 1/2}. \quad (34)$$

Indeed the integral over each unit interval centered at an integer is at least its central value. If S_J is a rational upper bound on $\max_{f \in J} \sin^2(\pi f)$ and $\pi_- < \pi$, then

$$p_{\text{uni}} = \min \left\{ 1, \max_J \frac{S_J}{\pi_-^2} (H_{24}(v_+) + H_{24}(v_-)) \right\} \quad (35)$$

is a uniform single-run certificate. The interval algorithm subdivides until each cell satisfies the chosen rational upper bound. Certification requires both valid cell bounds and exact coverage of $[0, 1]$.

J.2 Sine clock and finite grids: a uniform circular tail

The identity $\sum_{t=0}^{P-1} \sin^2(\pi(t + 1/2)/P) = P/2$, obtained by a roots-of-unity sum, normalizes the state in (19). Writing $t = x + bP/2$, the high-bit rotation specified in the main text gives this state's exact amplitudes. Expanding the sine into two exponentials and summing each finite geometric series gives (20). At $d = \pm 1/2 \pmod{P}$, direct summation gives the removable value $1/2$. The kernel $p(d)$ is even

and P -periodic. After the negative ramp, $d = x - j - z/S_g$ modulo P , where $x = P\phi/(2\pi)$. Each (z, j) corresponds uniquely to the fine-grid point $j + z/S_g$ modulo P , with joint probability $p(d)/S_g$.

Write $v = j + z/S_g$ for the measured grid point. The reflection $(x, v) \mapsto (-x, -v)$, interpreted modulo P , preserves the kernel and both cosines, and permutes the shift indices together with their integer bins. The transformation $(x, v) \mapsto (P/2 - x, P/2 - v)$ preserves the kernel and negates both cosines. Thus the averaged lower-error bound for $0 \leq \phi \leq \pi$ also covers upper errors and both eigenphases, for arbitrary spectral weights. An individual nonzero-offset branch need not possess these symmetries.

For a nonempty lower-error event let $\alpha = \arccos(\cos \phi - g)$. The bad arc is $[\alpha, 2\pi - \alpha]$ and its lifts relative to ϕ are $[\alpha - \phi + 2\pi l, 2\pi - \alpha - \phi + 2\pi l]$. Every positive lift is at least $\alpha - \phi \geq g$ by cosine's unit Lipschitz constant. Every negative lift has magnitude at least $\alpha + \phi \geq \sqrt{2g}$, because $\cos \alpha \leq 1 - g$ and $1 - \cos \alpha \leq \alpha^2/2$. The shortest signed representative, of magnitude at most π , is one of these lifts and has the same directional lower bound. Antipodal ties may be assigned either orientation, or overcounted conservatively. If the bad arc is empty its probability is zero. These directional thresholds therefore apply to the circular probability kernel.

In the following tail estimates, d denotes the nonnegative circular bin distance. Put $a_* = 127/128$ and split this distance at $P/16$. For $d \leq P/16$, $\sin(\pi d/P) \geq a_* \pi d/P$, since $1 - \pi_+^2/(6 \cdot 16^2) > a_*$. If $C \geq \cos^2(\pi d)$ and $d > 1/(2a_*)$, the exact kernel gives

$$p(d) \leq \frac{C}{2\pi_-^2} F_*(d), \quad F_*(d) = (a_*^2 d^2 - 1/4)^{-2}. \quad (36)$$

Cancel the common factors involving the exact π before applying $1/\pi^2 \leq 1/\pi_-^2$. The function F_* is positive and decreasing on this domain. The corresponding one-sided tail sum satisfies

$$\sum_{j \geq 0} F_*(v + j) \leq R(v) := \sum_{j=0}^7 F_*(v + j) + \frac{1}{3(v+7)^3 [a_*^2 - 1/(4(v+7)^2)]^2}. \quad (37)$$

For omitted $j \geq 8$, monotonicity bounds the sum by the integral from $v + 7$; there $F_*(t) \leq t^{-4} [a_*^2 - 1/(4(v+7)^2)]^{-2}$. On $P/16 < d \leq P/2$, $\sin(\pi d/P) \geq \sin(\pi/16) > 3/16$ and $\sin(\pi/(2P)) < 2/P$. At most P outcomes per branch give the entire far bound $8/[P^3(9/256 - 4/P^2)^2]$. The same bound holds after averaging over the S_g shift branches.

Set $f_z = \text{frac}(z/S_g - x)$. Forward distances are $f_z + n$ and backward distances $n - f_z$, with common numerator $\cos^2(\pi f_z)$. On a closed cell $[L, U]$, the forward integer index is at least $\lceil q_f - U \rceil$ and the backward one at least $\lceil q_b + L \rceil$. Their distances are therefore bounded below by

$$v_f = \lceil q_f - U \rceil + L, \quad v_b = \lceil q_b + L \rceil - U.$$

These inclusions hold throughout each closed cell, including every ceiling switch. Both starts exceed $3/4 - 1/128 > 1/(2a_*)$ under the theorem's hypotheses. Thus all kernel singularities are outside these bad near tails. The endpoints $f = 0$ and 1 enumerate the same lattice after an integer-index shift.

The multiset $\{\text{frac}(f + z/S_g) : 0 \leq z < S_g\}$ is periodic in f with period $1/S_g$. The 128 closed base cells cover this whole interval; their translates cover the needed fractions without gaps. On any one base cell average its S_g valid ray bounds first. Taking the largest such average and adding the far bound proves (22), including endpoints. The interval cover therefore bounds the error for all phases. The head-dependent threshold disappeared in Proposition 4, so the proof remains valid for every head transcript, including thresholds outside $[-1, 1]$. Each mixture component is bounded for a fixed input; averaging head transcripts or eigenphase weights preserves the result.

Rational implementation. Machin's identity $\pi = 16 \arctan(1/5) - 4 \arctan(1/239)$ and 48 alternating terms with their next-term remainders enclose π between

$$3.14159265358979323846264338327950288419716939937510 \quad \text{and the same endpoint plus } 10^{-50}.$$

A dyadic square-root enclosure with 80 fractional bits is verified by squaring both endpoints. For $h = \max(|L - 1/2|, |U - 1/2|)$, the exact maximum numerator is $\sin^2(\pi h)$. At $h = 1/2$ use one; otherwise the alternating sine polynomial through degree 17 is an upper bound. Evaluate its positive terms at $\pi_+ h$ and negative terms at $\pi_- h$, then square and round upward to 64 fractional bits. Ray sums and final probabilities are rounded upward to 96 and 80 fractional bits, respectively. Every monotonicity and remainder inequality holds on the whole interval.

Unshifted measurements and synthesis. For the unshifted sine clock, use the probability kernel (20); here d is a signed circular displacement measured in Fourier bins. At $d = \pm 1/2$ its continuous value is $1/2$. A wrong sign implies circular angular distance at least g radians, since cosine is one-Lipschitz. For $q = Pg/(2\pi_+) > 16/31$ and $P \geq 32$, one explicit uniform bound is

$$p_* \leq \frac{q^{-4} + (3q^3)^{-1}}{\pi^2 [(31/32)^2 - 1/(4q^2)]^2} + \frac{800}{P^3}. \quad (38)$$

For the unshifted symmetric certificate take $S_g = 1$ and replace q_b by q_f in the preceding proof. This gives the refined unshifted sine bound. The simpler bound (38) follows by splitting at $P/8$, using $\sin z/z \geq 31/32$ and the ray sum $\sum d^{-4} \leq q^{-4} + 1/(3q^3)$; the far part contributes at most $800/P^3$. Both bounds certify the same unshifted sine-clock measurement. When the refined construction applies, the unshifted resource certificate takes the smaller of these bounds, capped at one. The comparison over S_g in Section 6 instead uses (22), including at $S_g = 1$. For a finite grid, a fixed classical z expands (21) into single-qubit negative R_z gate sequences, using exact Clifford phase and T gates when applicable. The phases introduced by projective synthesis are global within that branch. Very small angles not represented in the synthesis library may use the identity with explicit error $\|I - R_z(\pi/2^j)\| \leq \pi/2^{j+1}$. The inverse is the exact reversed compiled gate sequence with adjoint gates. The hybrid argument bounds the change in outcome probability as in (24), with clock and ramp preparation charged once per run. The fixed source remains part of β and defines the actual reflection. The decoder uses the integer pair $(S_g j + z, S_g P)$ in the rational cosine bound of Appendix H.

Independent repetition. The binomial bound based on the average single-run error uses independent shifts in successive runs. For example, suppose the conditional error probability is 0 or $2/5$, each with probability $1/2$. Its mean is $1/5$, but a three-run majority fails with probability $22/125$ for a shared shift and $13/125$ for independent shifts.

Padded POVM. For a clock supported on $0 \leq t < P$, with all high bits zero, the inverse $S_g P$ -point Fourier transform gives the operator amplitude $(S_g P)^{-1/2} \sum_t a_t e^{-2\pi i k t / (S_g P)} G^t$. Substituting $k = S_g j + z$ proves the Kraus-operator identity (23), so the equivalence holds for arbitrary input states. The controlled powers are G^{2^l} , $0 \leq l < m$, totaling $P - 1$ calls. The additional Fourier gates and wires have their own compiled synthesis cost.

References

- [1] E. Gil-Fuster, S. Shin, S. Jerbi, J. Eisert and M. J. Kramer, *Optimal algorithmic complexity of inference in quantum kernel methods*, arXiv:2604.15214v2 (2026), <https://doi.org/10.48550/arXiv.2604.15214>.
- [2] S. Heinrich, *Quantum Summation with an Application to Integration*, arXiv:quant-ph/0105116v1 (2001).

- [3] G. Brassard, P. Høyer, M. Mosca and A. Tapp, *Quantum Amplitude Amplification and Estimation*, Contemporary Mathematics 305, 53–74 (2002), arXiv:quant-ph/0005055v1, <https://doi.org/10.1090/conm/305/05215>.
- [4] R. Beals, H. Buhrman, R. Cleve, M. Mosca and R. de Wolf, *Quantum Lower Bounds by Polynomials*, arXiv:quant-ph/9802049; J. ACM 48, 778–797 (2001), <https://doi.org/10.1145/502090.502097>.
- [5] A. Nayak and F. Wu, *The quantum query complexity of approximating the median and related statistics*, arXiv:quant-ph/9804066v2 (1998).
- [6] S. McArdle, A. Gilyén and M. Berta, *Quantum state preparation without coherent arithmetic*, arXiv:2210.14892v2 (2025).
- [7] O. O’Brien and C. Sünderhauf, *Quantum state preparation via piecewise QSVT*, arXiv:2409.07332v2; Quantum 9, 1786 (2025), <https://doi.org/10.22331/q-2025-07-03-1786>.
- [8] J. Lemieux et al., *Quantum sampling algorithms for quantum state preparation and matrix block-encoding*, arXiv:2405.11436v1 (2024).
- [9] N. J. Ross and P. Selinger, *Optimal ancilla-free Clifford+T approximation of z-rotations*, arXiv:1403.2975v3; Quantum Information and Computation 16, 901–953 (2016), <https://doi.org/10.26421/QIC16.11-12-1>.
- [10] D. Maslov, *Advantages of using relative-phase Toffoli gates with an application to multiple control Toffoli optimization*, arXiv:1508.03273v2; Phys. Rev. A 93, 022311 (2016), <https://doi.org/10.1103/PhysRevA.93.022311>.
- [11] T. Khattar and C. Gidney, *Rise of conditionally clean ancillae for efficient quantum circuit constructions*, arXiv:2407.17966v2; Quantum 9, 1752 (2025), <https://doi.org/10.22331/q-2025-05-21-1752>.
- [12] S. Nacu and Y. Peres, *Fast simulation of new coins from old*, Annals of Applied Probability 15, 93–115 (2005), arXiv:math/0309222v5, <https://doi.org/10.1214/105051604000000549>.
- [13] G. Rendon, T. Izubuchi and Y. Kikuchi, *Effects of cosine tapering window on quantum phase estimation*, Phys. Rev. D 106, 034503 (2022), <https://doi.org/10.1103/PhysRevD.106.034503>.
- [14] D. Patel, S. J. S. Tan, Y. Subaşı and A. T. Sornborger, *Optimal Coherent Quantum Phase Estimation via Tapering*, arXiv:2403.18927v3; PRX Quantum 7, 020302 (2026), <https://doi.org/10.1103/15y6-6zxv>.
- [15] X. Lu and H. Lin, *Unbiased Quantum Phase Estimation*, arXiv:2210.00231v1; Quantum Information and Computation 23, 16–26 (2023), <https://doi.org/10.26421/QIC23.1-2-2>.
- [16] H. Apel, C. L. Cortes, J. Lemieux and M. Steudtner, *Reducing quantum resources for observable estimation with window-assisted coherent QPE*, arXiv:2508.06677v1 (2025).
- [17] J. O. Smith III, *Mathematics of the Discrete Fourier Transform (DFT), with Audio Applications*, 2nd ed., W3K Publishing (2007), ISBN 978-0-9745607-4-8, “Zero Padding Theorem (Spectral Interpolation),” https://ccrma.stanford.edu/~jos/mdft/Zero_Padding_Theorem_Spectral.html.