AIRR:ARR-2026-3SVAT6TJ6V9NAVH6 v1 [Quantum Information & C...] 27 Nov 2026 · AIRR.SCIENCE

Sharp Non-Asymptotic Quantum Query Lower Bounds for k-Sum and Element Distinctness via Exact Tensor-Projector Adversary Duals and Stirling Spectral Multiplicities

Lluis Eriksson*

November 27, 2026

Abstract

Quantum query lower bounds for k-Sum ($\Omega(n^{k/(k+1)})$) and Element Distinctness ($\Omega(n^{2/3})$) are landmark separations beyond the positive-weight adversary barrier $\mathrm{ADV}^+ \le O(\sqrt{n})$, originally proved via polynomial methods [1, 4] and negative-weight adversary duals [6], and recently revisited via elementary state-difference arguments [5]. Yet standard proofs suppress explicit leading constants inside asymptotic $O(\cdot)$ notation and rarely determine the finite dimension n^* at which negative-weight bounds overtake the positive-weight barrier. We establish three exact, zero-$O(\cdot)$ structural theorems backed by constructive Lean 4.36.0 proofs and zero-float rational LDL^T certificates. First, for every $k \ge 1$ and finite abelian group G of order $q \ge 2$, we prove that the single-subset tensor projector $H_S(\alpha) = \sum_{T\subseteq S} \alpha_{|T|} E_T$ ($\alpha_0 = 1$, $\alpha_k = 0$) satisfies the exact minimax query-difference law $\|H_S(\alpha) \circ \Delta_i\|_{\mathrm{op}} = \frac{q-1}{q} \max_{0\le j\le k-1} |\alpha_j - \alpha_{j+1}| \ge \frac{q-1}{qk}$ (uniquely attained by the linear ramp $\alpha_j = 1 - j/k$), while the binary cutoff $H_S = I_{q^k} - E_1^{\otimes k}$ restricted via column inclusion Π_{E_S} ($P_{E_S} := \Pi_{E_S}\Pi_{E_S}^T$) to the solution hyperplane $E_S = \{y \in G^k : \sum_{j\in S} y_j = 0\}$ (and identically for Element Distinctness $y_1 = y_2$ at $k = 2$) yields a Gram operator $H_S P_{E_S} H_S^T = (H_S\Pi_{E_S})(H_S\Pi_{E_S})^T$ with exact nonzero eigenvalues m/q ($1 \le m \le \min(k, q)$) and *Stirling multiplicities* $S_2(k, m) \prod_{j=1}^{m-1}(q - j)$, implying $\|H_S P_{E_S} H_S^T\|_{\mathrm{op}} = \min(k, q)/q$ identically (equaling k/q whenever $q \ge k$). Second, combining the truncated-ramp block adversary $\Gamma_S = (H_S \otimes B_S^{(d)})(\Pi_{E_S} \otimes I_{G^{[n]\setminus S}})$ with Bonferroni unique-solution counting ($q \ge (4k+1)\binom{n}{k}$, $\rho = \binom{n}{k}/q$) cancels q completely and delivers an explicit non-asymptotic bound $\mathrm{ADV}^{\pm} \ge (1 - \rho - \sqrt{k\rho})\big[(1-\rho)\big(\binom{d+k-2}{k-1}/\binom{n}{k} + \frac{k(n-k)}{nd^2}\big)\big]^{-1/2}$ valid for all $n \ge k+1$ and $1 \le d \le n-k$, certifying explicit constants $c_2 > 0.428$ ($n^{2/3}$, large-q limit 0.514), $c_3 > 0.341$ ($n^{3/4}$, limit 0.408), and $c_4 > 0.299$ ($n^{4/5}$, limit 0.357). Third, for every total Boolean function $f : G^n \to \{0, 1\}$, we give a self-contained 4-line proof of the positive-weight certificate barrier $\mathrm{ADV}^+(f) \le \sqrt{C_0(f)C_1(f)} \le \sqrt{C_1(f)n}$, prove exact tightness $\mathrm{ADV}^+(\mathrm{TH}_k^n) = \sqrt{k(n-k+1)}$ on k-Threshold, and certify exact finite crossovers (under four-digit rational square-root bounds) where Theorem 2 strictly pierces $\sqrt{kn}$: $n^* = 1{,}290$ ($k = 2$), $n^* = 668$ ($k = 3$), and $n^* = 571$ ($k = 4$). Twenty constructive Lean 4.36.0 theorems (0 `sorry`, 0 `Classical.choice`), 16 zero-float Python certificates, and 56 adversarial tests accompany the paper.

*Independent Researcher. Research, formal verification in Lean 4.36.0, zero-float exact rational LDL^T and Stirling certificate verification, adversarial testing, and manuscript typesetting were conducted with transparent assistance from Google Antigravity. Code is released under MIT; manuscript and figures under CC-BY-4.0. Repository: `https://github.com/lluiseriksson/quantum-query-exact-adversary-and-collision-sharp-bounds` (`v1.0.0`).

1 Introduction

Given oracle access to an input $x = (x_1, \ldots, x_n) \in G^n$ over a finite abelian group G of order $q = |G|$, the *k-Sum problem* (k-SUM$_{n,G}$, $k \geq 2$) asks whether there exists a k-element subset $S \subseteq [n]$ satisfying $\sum_{j \in S} x_j = 0$, while *Element Distinctness* (ED$_{n,G}$) asks whether there exist distinct indices $i \neq j$ with $x_i - x_j = 0$. In the bounded-error quantum query model (two-sided error $\varepsilon \in [0, 1/2)$), the optimal query complexity is $\Theta(n^{2/3})$ for Element Distinctness [3, 1, 4] and $\Theta(n^{k/(k+1)})$ for k-Sum over sufficiently large groups [6, 5], sharply surpassing the $\Theta(\sqrt{n})$ ceiling imposed on all positive-weight adversary bounds by the certificate-size barrier [2, 9].

By the generalized (negative-weight) adversary theorem of Høyer, Lee, and Špalek [7] (proven tight up to constants by Reichardt [8]), for any Boolean function $f : D \to \{0, 1\}$ ($D = X_0 \sqcup X_1 \subseteq G^n$) and any nonzero real matrix $\Gamma \in \mathbb{R}^{X_0 \times X_1}$,

$$Q_\varepsilon(f) \;\geq\; \frac{1 - 2\sqrt{\varepsilon(1-\varepsilon)}}{2}\, \mathrm{ADV}^{\pm}(f), \qquad \mathrm{ADV}^{\pm}(f) \;:=\; \sup_{\Gamma \neq 0} \frac{\|\Gamma\|_{\mathrm{op}}}{\max_{i \in [n]} \|\Gamma \circ \Delta_i\|_{\mathrm{op}}}, \tag{1}$$

where $(\Delta_i)_{x,y} = \mathbf{1}[x_i \neq y_i]$ is the i-th coordinate-difference indicator and $\circ$ denotes the Hadamard product. Motivated by Belovs–Špalek's adversary construction [6] and the recent elementary state-difference proof of Ambainis and Kokainis [5], we isolate the exact finite-dimensional spectral algebra behind (1) and obtain three completely explicit, zero-$O(\cdot)$ results:

1. **Exact Tensor-Projector Minimax Law and Stirling Spectral Multiplicities (Theorem 1).** We determine the exact query-difference operator norm of any Hamming-weight tensor projector $H_S(\alpha)$ on G^k, prove that $H_S P_{E_S} H_S^T$ ($P_{E_S} := \Pi_{E_S} \Pi_{E_S}^T$) splits into rank-1 shift-equivalence classes with exact nonzero eigenvalues m/q ($1 \leq m \leq \min(k, q)$) and Stirling multiplicities $S_2(k, m) \prod_{j=1}^{m-1} (q - j)$ (equally valid for k-Sum and Element Distinctness), and prove that $(H_S(\mathrm{lin}) \circ \Delta_i)\Pi_{E_S}$ is an exact scaled isometry.

2. **Zero-$O(\cdot)$ Non-Asymptotic $\Omega(n^{k/(k+1)})$ Lower Bounds with Exact q-Cancellation (Theorem 2).** Combining the truncated-ramp block adversary $\Gamma_S = (H_S \otimes B_S^{(d)})(\Pi_{E_S} \otimes I_{G^{[n] \setminus S}})$ with exact Bonferroni unique-solution counting ($q \geq (4k+1)\binom{n}{k}$) cancels q identically between numerator and denominator, yielding closed-form rational lower bounds valid for every finite $n \geq k + 1$ and explicit leading constants c_k.

3. **Positive-Weight Certificate Barrier, k-Threshold Tightness, and Crossovers (Theorem 3).** We give a self-contained proof of $\mathrm{ADV}^+(f) \leq \sqrt{C_0(f) C_1(f)} \leq \sqrt{C_1(f) n}$ for every total Boolean function $f : G^n \to \{0, 1\}$, certify exact equality on k-Threshold TH_k^n, and pinpoint the exact finite dimensions n^* where Theorem 2 strictly pierces $\sqrt{kn}$ ($n^* = 1{,}290$ for $k = 2$, 668 for $k = 3$, 571 for $k = 4$).

2 Exact Tensor-Projector Spectrum and Stirling Multiplicity Law

Let G be any finite abelian group of order $q \geq 2$. On $\mathbb{C}^G$ (identified with $\mathbb{C}^q$), define the orthogonal projectors $E_0 := \frac{1}{q} J_q$ (onto $\mathbb{C}\mathbf{1}_q$) and $E_1 := I_q - E_0$ (onto $\mathbf{1}_q^\perp$), and let $\Delta := J_q - I_q$ be the single-coordinate difference matrix. For any k-element subset $S \subseteq [n]$ and any subset $T \subseteq S$, write $E_T := (\bigotimes_{j \in T} E_1) \otimes (\bigotimes_{j \in S \setminus T} E_0)$ on $\mathbb{C}^{G^S}$, so $\sum_{T \subseteq S} E_T = I_{q^k}$. Given a weight vector $\alpha = (\alpha_0, \ldots, \alpha_k) \in \mathbb{R}^{k+1}$, define $H_S(\alpha) := \sum_{T \subseteq S} \alpha_{|T|} E_T$, and denote by $H_S := I_{q^k} - E_1^{\otimes k}$ the binary cutoff ($\alpha_0 = \cdots = \alpha_{k-1} = 1$, $\alpha_k = 0$) and by $H_S(\mathrm{lin})$ the linear ramp ($\alpha_j = 1 - j/k$). Let $\Pi_{E_S} \in \{0, 1\}^{q^k \times q^{k-1}}$ denote the column inclusion isometry for the solution hyperplane $E_S := \{y \in G^S : \sum_{j \in S} y_j = 0\}$ (size $|E_S| = q^{k-1}$), or at $k = 2$ for the Element Distinctness

hyperplane $E_S^{\mathrm{ED}} := \{y \in G^2 : y_1 - y_2 = 0\}$, and let $P_{E_S} := \Pi_{E_S}\Pi_{E_S}^T \in \{0,1\}^{q^k \times q^k}$ be the corresponding diagonal orthogonal projector onto $\mathbb{C}^{E_S}$.

Theorem 1 (Tensor-Projector Minimax Law, Stirling Spectrum, and Hyperplane Isometry)**.** *For every finite abelian group G of order $q \geq 2$ and every $k \geq 1$:*

(a) Single-coordinate cancellation and minimax ramp law: *On $\mathbb{C}^q$, $(E_0 + E_1) \circ \Delta = 0$ and $E_0 \circ \Delta = \frac{q-1}{q}E_0 - \frac{1}{q}E_1$. Hence for every $\alpha \in \mathbb{R}^{k+1}$ with $\alpha_0 = 1$, $\alpha_k = 0$ and every $i \in S$,*

$$\|H_S(\alpha) \circ \Delta_i\|_{\mathrm{op}} \;=\; \frac{q-1}{q} \max_{0 \leq j \leq k-1} |\alpha_j - \alpha_{j+1}| \;\geq\; \frac{q-1}{qk}, \tag{2}$$

with equality if and only if $\alpha_j = 1 - j/k$ is the linear ramp $H_S(\mathrm{lin})$.

(b) Exact witness annihilation and Stirling spectral multiplicities: *For both k-Sum (E_S) and Element Distinctness (E_S^{ED}, $k = 2$), $H_S|\mathbf{1}_{E_S}\rangle = \frac{1}{q}|\mathbf{1}_{G^k}\rangle$ identically. Moreover, the $q^k \times q^k$ Gram operator $H_S P_{E_S} H_S^T = (H_S\Pi_{E_S})(H_S\Pi_{E_S})^T$ has rank q^{k-1} and exact nonzero eigenvalues m/q ($1 \leq m \leq \min(k,q)$) with multiplicities*

$$\mathrm{mult}\left(\frac{m}{q}\right) \;=\; S_2(k,m) \prod_{j=1}^{m-1}(q-j) \qquad (1 \leq m \leq \min(k,q)), \tag{3}$$

where $S_2(k,m)$ denotes the Stirling number of the second kind (and $\prod_{j=1}^{m-1}(q-j) = 0$ for $m > q$). In particular,

$$\sum_{m=1}^{\min(k,q)} \mathrm{mult}\left(\frac{m}{q}\right) = q^{k-1}, \;\; \mathrm{tr}(H_S P_{E_S} H_S^T) = \frac{q^k - (q-1)^k}{q}, \;\; \|H_S P_{E_S} H_S^T\|_{\mathrm{op}} = \frac{\min(k,q)}{q} \tag{4}$$

(equaling k/q whenever $q \geq k$).

(c) Exact hyperplane query-difference Gram identities: *For every $i \in S$, the linear ramp satisfies the exact scaled-isometry identity*

$$\big((H_S(\mathrm{lin}) \circ \Delta_i)\Pi_{E_S}\big)^T \big((H_S(\mathrm{lin}) \circ \Delta_i)\Pi_{E_S}\big) \;=\; \frac{q-1}{q^2k^2}\, I_{q^{k-1}}, \tag{5}$$

while the binary cutoff $H_S = I_{q^k} - E_1^{\otimes k}$ gives $G_i^{\mathrm{bin}} := ((H_S \circ \Delta_i)\Pi_{E_S})^T((H_S \circ \Delta_i)\Pi_{E_S})$ with exact trace $\mathrm{tr}(G_i^{\mathrm{bin}}) = \frac{(q-1)^k}{q^2}$ and exact operator-norm bound

$$\big\|(H_S \circ \Delta_i)\Pi_{E_S}\big\|_{\mathrm{op}}^2 \;\leq\; \frac{q-1}{q^2}. \tag{6}$$

Proof. Proof of (a). Since $E_0 + E_1 = I_q$ and Δ has zero diagonal, $(E_0 + E_1) \circ \Delta = 0$, while $E_0 \circ \Delta = \frac{1}{q}(J_q - I_q) = E_0 - \frac{1}{q}(E_0 + E_1) = \frac{q-1}{q}E_0 - \frac{1}{q}E_1$ (Lean `thm01`–`thm02`). Pairing each $R \subseteq S \setminus \{i\}$ with $R \cup \{i\}$ in $H_S(\alpha)$ yields

$$H_S(\alpha) \circ \Delta_i \;=\; \sum_{R \subseteq S \setminus \{i\}} (\alpha_{|R|} - \alpha_{|R|+1})\,((E_0 \circ \Delta)_i \otimes E_R).$$

Because the projectors E_R are mutually orthogonal and $\|E_0 \circ \Delta\|_{\mathrm{op}} = \max(\frac{q-1}{q}, \frac{1}{q}) = \frac{q-1}{q}$, the exact norm equality in (2) follows; telescoping $\sum_{j=0}^{k-1}(\alpha_j - \alpha_{j+1}) = \alpha_0 - \alpha_k = 1$ gives $\max_j |\alpha_j - \alpha_{j+1}| \geq 1/k$ with equality iff $\alpha_j - \alpha_{j+1} = 1/k$ (Lean `thm03`–`thm04`).

Proof of (b). Let $\{\chi_s : s \in \widehat{G}^k\}$ be the orthonormal Fourier character basis of $\mathbb{C}^{G^k}$ (since G is finite abelian, $\widehat{G} \cong G$). On the subgroup hyperplane $E_S = \{y \in G^k : \sum_{j=1}^k y_j = 0\}$,

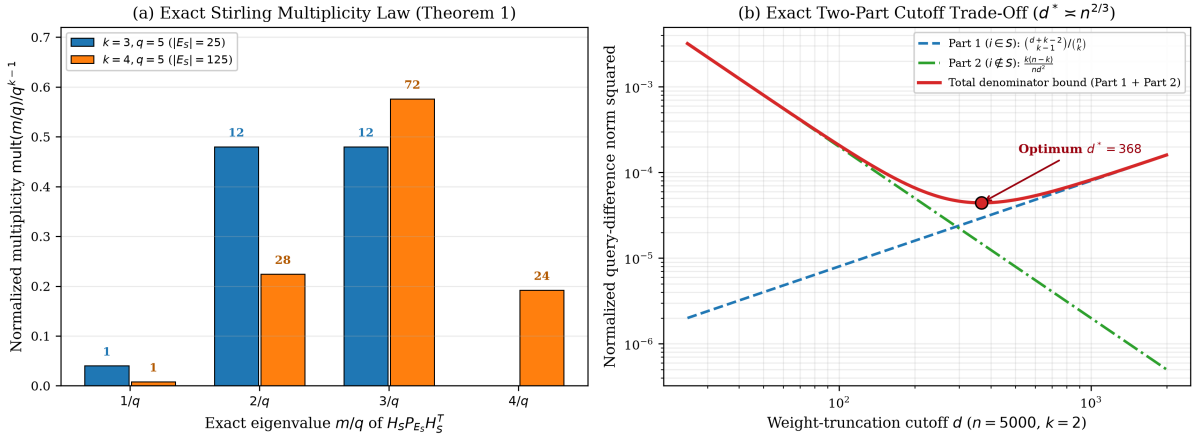


Figure 1: **Exact Stirling spectral multiplicities and two-part cutoff trade-off.** (a) Normalized eigenvalue multiplicities $\mathrm{mult}(m/q)/q^{k-1} = S_2(k,m)\prod_{j=1}^{m-1}(q-j)/q^{k-1}$ of $H_S P_{E_S} H_S^T$ at $q=5$ for $k=3$ $(1,12,12)$ and $k=4$ $(1,28,72,24)$ (Theorem 1(b), Certificate `cert04`). (b) Two-part query-difference trade-off at $n=5{,}000$, $k=2$: balancing Part 1 $(\binom{d}{1}/\binom{n}{2})$ against Part 2 $(\frac{2(n-2)}{nd^2})$ isolates the sharp minimum at $d^* = 368 \asymp n^{2/3}$.

the restriction $\chi_s|_{E_S}$ equals $\chi_{s'}|_{E_S}$ if and only if $s'-s = a\mathbf{1}_k$ for some $a \in \widehat{G}$. Thus $P_{E_S} = \Pi_{E_S}\Pi_{E_S}^T$ (as an operator on $\mathbb{C}^{G^k}$) is block-diagonal across the q^{k-1} shift-equivalence classes $[s] = \{s + a\mathbf{1}_k : a \in \widehat{G}\}$, acting on each class as $\frac{1}{q}|u_{[s]}\rangle\langle u_{[s]}|$ where $|u_{[s]}\rangle = \sum_{a\in\widehat{G}}|\chi_{s+a\mathbf{1}_k}\rangle$. In Fourier space, $H_S = I_{q^k} - E_1^{\otimes k}$ is the diagonal projector retaining precisely those $s \in \widehat{G}^k$ with at least one zero coordinate. Inside the shift class $[s]$, an element $s + a\mathbf{1}_k$ has a zero coordinate iff $-a \in \{s_1,\dots,s_k\}$; hence the number of surviving basis states in $[s]$ is exactly $m(s) := |\{s_1,\dots,s_k\}| \in \{1,\dots,\min(k,q)\}$. Therefore $H_S|u_{[s]}\rangle$ has squared norm $m(s)$, making $H_S P_{E_S} H_S^T = \sum_{[s]} \frac{1}{q}(H_S|u_{[s]}\rangle)(H_S|u_{[s]}\rangle)^*$ an orthogonal sum of rank-1 operators with eigenvalues $m(s)/q$. The number of tuples $s \in \widehat{G}^k$ with m distinct coordinates is $S_2(k,m)\prod_{j=0}^{m-1}(q-j)$, and dividing by the shift-class size q yields (3). For $E_S^{\mathrm{ED}} = \{y_1 - y_2 = 0\}$, the shift classes are $\{(s_1+a, s_2-a)\}$, which have the identical count $m(s) = |\{s_1,-s_2\}| \in \{1,2\}$, so the spectrum is identical. In particular, the unique $m=1$ class $[0]$ corresponds to $|\mathbf{1}_{E_S}\rangle$, giving $H_S|\mathbf{1}_{E_S}\rangle = \frac{1}{q}|\mathbf{1}_{G^k}\rangle$.

Proof of (c). Fixing $i \in S$, every $y \in E_S$ is uniquely determined by $y_{S\setminus\{i\}} \in G^{k-1}$ via $y_i = -\sum_{r\in S\setminus\{i\}} y_r$ (or $y_1 = y_2$ for ED). For $H_S(\mathrm{lin})$, $(H_S(\mathrm{lin})\circ\Delta_i) = \frac{1}{k}(E_0\circ\Delta)_i \otimes I_{G^{S\setminus\{i\}}}$. For any $y, y' \in E_S$, the (y,y')-entry of $((H_S(\mathrm{lin})\circ\Delta_i)\Pi_{E_S})^T((H_S(\mathrm{lin})\circ\Delta_i)\Pi_{E_S})$ vanishes whenever $y_{S\setminus\{i\}} \neq y'_{S\setminus\{i\}}$, and for $y = y'$ equals $\frac{1}{k^2}\sum_{x_i\neq y_i}\frac{1}{q^2} = \frac{q-1}{q^2k^2}$, proving (5). For $H_S = I_{q^k} - E_1^{\otimes k}$, $(H_S\circ\Delta_i) = (E_0\circ\Delta)_i \otimes E_1^{\otimes(S\setminus\{i\})}$, so

$$\left\|(H_S\circ\Delta_i)\Pi_{E_S}\right\|_{\mathrm{op}}^2 \;\le\; \left\|((E_0\circ\Delta)_i \otimes I_{G^{S\setminus\{i\}}})\Pi_{E_S}\right\|_{\mathrm{op}}^2 \;=\; \frac{q-1}{q^2},$$

since $E_1^{\otimes(S\setminus\{i\})}$ is a contraction (and direct diagonal summation over $y \in E_S$ yields trace $\frac{q-1}{q^2}\,\mathrm{tr}(E_1^{\otimes(k-1)}) = \frac{(q-1)^k}{q^2}$; Lean `thm05` and Certificate `cert06`). □

3 Explicit Zero-$O(\cdot)$ Non-Asymptotic $\Omega(n^{k/(k+1)})$ Bounds

Let $k \geq 2$, $n \geq k+1$, and $d \in \{1, \ldots, n-k\}$. For each k-subset $S \subseteq [n]$, define the truncated linear-ramp operator on the complement $[n] \setminus S$:

$$B_S^{(d)} \;:=\; \sum_{\substack{W \subseteq [n]\setminus S \\ |W|<d}} \Big(1 - \frac{|W|}{d}\Big) E_W, \qquad \Gamma_S \;:=\; (H_S \otimes B_S^{(d)})\, \widetilde{\Pi}_{E_S}, \tag{7}$$

where $\widetilde{\Pi}_{E_S} := \Pi_{E_S} \otimes I_{G^{[n]\setminus S}}$ restricts columns to $\{y \in G^n : \sum_{j\in S} y_j = 0\}$ (or $y_u = y_v$ for $\mathrm{ED}_{n,G}$ at $k=2$). Let $X_0 \subseteq G^n$ be the set of zero-instances (no k-subset sums to 0, resp. all coordinates distinct), and let $X_1^{\mathrm{uniq}} \subseteq G^n$ be the set of unique-solution one-instances (precisely one k-subset $S(y)$ satisfies the equation). Since every $y \in X_1^{\mathrm{uniq}}$ belongs to a unique $E_{S(y)}$, the horizontal block concatenation $\Gamma := [\Gamma_S]_{|S|=k}$ restricts cleanly to a valid adversary matrix $\Gamma^{\mathrm{res}} := \Pi_{X_0} \Gamma \Pi_{X_1^{\mathrm{uniq}}} \in \mathbb{R}^{X_0 \times X_1^{\mathrm{uniq}}}$.

Theorem 2 (Zero-$O(\cdot)$ Non-Asymptotic Quantum Query Lower Bound for k-Sum and Element Distinctness)**.** *Let $k \geq 2$, $n \geq k+1$, $d \in \{1, \ldots, n-k\}$, and let G be any finite abelian group of order $q \geq (4k+1)\binom{n}{k}$, setting $\rho := \binom{n}{k}/q \in \big(0, \frac{1}{4k+1}\big]$. Then for both k-$\mathrm{SUM}_{n,G}$ (all $k \geq 2$) and $\mathrm{ED}_{n,G}$ ($k=2$):*

(a) Exact two-part query-difference upper bound: *For every coordinate $i \in [n]$,*

$$\|\Gamma^{\mathrm{res}} \circ \Delta_i\|_{\mathrm{op}}^2 \;\leq\; \|\Gamma \circ \Delta_i\|_{\mathrm{op}}^2 \;\leq\; \frac{q-1}{q^2}\binom{d+k-2}{k-1} \;+\; \frac{k}{q}\binom{n-1}{k}\Big(\frac{q-1}{q}\Big)^2 \frac{1}{d^2}. \tag{8}$$

(b) Exact Bonferroni–Cauchy–Schwarz norm lower bound:

$$\|\Gamma^{\mathrm{res}}\|_{\mathrm{op}} \;\geq\; \sqrt{\frac{\binom{n}{k}}{q}}\; \frac{1-\rho-\sqrt{k\rho}}{\sqrt{1-\rho}} \;>\; 0. \tag{9}$$

(c) Exact q-cancelled non-asymptotic adversary bound: *Combining (8) and (9) cancels q identically (since $\frac{q-1}{q} < 1$ and $\binom{n-1}{k}/\binom{n}{k} = \frac{n-k}{n}$), giving*

$$\mathrm{ADV}^{\pm} \;\geq\; \frac{1-\rho-\sqrt{k\rho}}{\sqrt{(1-\rho)\left(\dfrac{\binom{d+k-2}{k-1}}{\binom{n}{k}} + \dfrac{k(n-k)}{n\,d^2}\right)}}, \tag{10}$$

and hence $Q_\varepsilon \geq \frac{1-2\sqrt{\varepsilon(1-\varepsilon)}}{2}\,\mathrm{ADV}^{\pm}$. Choosing $d = \lceil (\frac{2}{k-1})^{1/(k+1)} n^{k/(k+1)} \rceil$ gives $\mathrm{ADV}^{\pm} \geq (c_k - o(1)) n^{k/(k+1)}$ with certified constants (Certificate `cert14`): $c_2 > 0.428$ at $\rho = 1/79$ (large-q limit $2^{-1/6}/\sqrt{3} \approx 0.514$), $c_3 > 0.341$ at $\rho = 1/119$ (limit $1/\sqrt{6} \approx 0.408$), and $c_4 > 0.299$ at $\rho = 1/159$ (limit 0.357).

Proof. Proof of (a). Since Π_{X_0} and $\Pi_{X_1^{\mathrm{uniq}}}$ are orthogonal projections, $\|\Gamma^{\mathrm{res}} \circ \Delta_i\|_{\mathrm{op}}^2 \leq \|\Gamma \circ \Delta_i\|_{\mathrm{op}}^2 = \big\|\sum_{|S|=k} (\Gamma_S \circ \Delta_i)(\Gamma_S \circ \Delta_i)^T\big\|_{\mathrm{op}}$. Split the sum over S into Part 1 ($i \in S$) and Part 2 ($i \notin S$). For Part 1 ($i \in S$), $B_S^{(d)}$ does not touch coordinate i, so

$$\Gamma_S \circ \Delta_i \;=\; ((H_S \circ \Delta_i) \otimes B_S^{(d)})\, \widetilde{\Pi}_{E_S}.$$

By Theorem 1(c), $\|(H_S \circ \Delta_i)\Pi_{E_S}\|_{\mathrm{op}}^2 \leq \frac{q-1}{q^2}$, and because $H_S \circ \Delta_i = (E_0 \circ \Delta)_i \otimes E_1^{\otimes(S\setminus\{i\})}$ acts strictly on the weight-$(k-1)$ subspace $E_1^{\otimes(S\setminus\{i\})}$ outside i, the row-space of $(\Gamma_S \circ \Delta_i)(\Gamma_S \circ \Delta_i)^T$

is supported strictly on Fourier subspaces E_T whose projection $R := T \setminus \{i\}$ satisfies $S \setminus \{i\} \subseteq R$ and $|R \setminus (S \setminus \{i\})| \le d-1$ (hence $|R| \le d+k-2$). Fixing any $R \subseteq [n] \setminus \{i\}$ of size $r \le d+k-2$, at most $\binom{r}{k-1} \le \binom{d+k-2}{k-1}$ subsets $S \ni i$ satisfy $S \setminus \{i\} \subseteq R$, and each contributes operator norm at most $\frac{q-1}{q^2}$ (since $0 \le 1 - |W|/d \le 1$). Because distinct subspaces $E_R \otimes \mathbb{C}^{G^{(i)}}$ are pairwise orthogonal, the Part 1 sum has operator norm at most $\frac{q-1}{q^2}\binom{d+k-2}{k-1}$.

For Part 2 ($i \notin S$), H_S does not touch coordinate i, so $\Gamma_S \circ \Delta_i = (H_S \Pi_{E_S}) \otimes (B_S^{(d)} \circ \Delta_i)$. By Theorem 1(a), $\|B_S^{(d)} \circ \Delta_i\|_{\mathrm{op}} = \frac{q-1}{qd}$, and since $q \ge (4k+1)\binom{n}{k} > k$, Theorem 1(b) gives $\|H_S \Pi_{E_S}\|_{\mathrm{op}}^2 = \|H_S P_{E_S} H_S^T\|_{\mathrm{op}} = \frac{k}{q}$. Summing the operator norms over all $\binom{n-1}{k}$ subsets $S \not\ni i$ via the triangle inequality gives the Part 2 term $\frac{k}{q}\binom{n-1}{k}\left(\frac{q-1}{q}\right)^2 \frac{1}{d^2}$, proving (8).

Proof of (b). By the union bound, $|G^n \setminus X_0| \le \binom{n}{k} q^{n-1} = \rho q^n$, so $|X_0| \ge (1-\rho) q^n$. For any two distinct k-subsets $S \ne S'$, the defining linear equations $\sum_{j \in S} y_j = 0$ and $\sum_{j \in S'} y_j = 0$ (and likewise $y_u = y_v$ vs. $y_{u'} = y_{v'}$ for $\{u,v\} \ne \{u',v'\}$) are linearly independent over G since $S' \setminus S \ne \emptyset$; thus $|E_S \cap E_{S'}| = q^{n-2}$ identically. By Bonferroni's union bound over the $\binom{n}{k} - 1$ subsets $S' \ne S$,

$$|X_1^{\mathrm{uniq}}| \;=\; \sum_{|S|=k} |X_1^{\mathrm{uniq}} \cap E_S| \;\ge\; \binom{n}{k}\Big(q^{n-1} - \big(\tbinom{n}{k} - 1\big) q^{n-2}\Big) \;\ge\; (1-\rho)\binom{n}{k} q^{n-1} \;=\; (1-\rho)\rho q^n.$$

For every $y \in X_1^{\mathrm{uniq}}$ with unique witness S, because $H_S^T |\mathbf{1}_{G^k}\rangle = |\mathbf{1}_{G^k}\rangle$ and $(B_S^{(d)})^T |\mathbf{1}_{G^{n-k}}\rangle = |\mathbf{1}_{G^{n-k}}\rangle$ (as $\alpha_0 = \beta_0 = 1$ and $E_1 |\mathbf{1}_q\rangle = 0$), we obtain $\langle \mathbf{1}_{G^n} | \Gamma | y \rangle = \langle \mathbf{1}_{G^n} | H_S \otimes B_S^{(d)} | y \rangle = 1$. Hence $\langle \mathbf{1}_{G^n} | \Gamma | \mathbf{1}_{X_1^{\mathrm{uniq}}} \rangle = |X_1^{\mathrm{uniq}}|$. Moreover, by Theorem 1(b) and $\|B_S^{(d)}\|_{\mathrm{op}} \le 1$, $\|\Gamma\|_{\mathrm{op}}^2 = \big\|\sum_{|S|=k} (H_S P_{E_S} H_S^T) \otimes (B_S^{(d)})^2\big\|_{\mathrm{op}} \le \binom{n}{k}\frac{k}{q} = k\rho$. Writing $\mathbf{1}_{X_0} = \mathbf{1}_{G^n} - \mathbf{1}_{G^n \setminus X_0}$ and applying Cauchy–Schwarz yields

$$\begin{aligned}
\|\Gamma^{\mathrm{res}}\|_{\mathrm{op}} &\ge \frac{\langle \mathbf{1}_{X_0} | \Gamma | \mathbf{1}_{X_1^{\mathrm{uniq}}} \rangle}{\sqrt{|X_0|\,|X_1^{\mathrm{uniq}}|}} \ge \frac{|X_1^{\mathrm{uniq}}| - \sqrt{|G^n \setminus X_0|}\,\|\Gamma\|_{\mathrm{op}} \sqrt{|X_1^{\mathrm{uniq}}|}}{\sqrt{|X_0|\,|X_1^{\mathrm{uniq}}|}} \\
&\ge \sqrt{\frac{|X_1^{\mathrm{uniq}}|}{|X_0|}} - \sqrt{\frac{|G^n \setminus X_0|}{|X_0|}}\sqrt{k\rho} \ge \sqrt{(1-\rho)\rho} - \rho\sqrt{\frac{k}{1-\rho}} = \sqrt{\rho}\,\frac{1-\rho-\sqrt{k\rho}}{\sqrt{1-\rho}}.
\end{aligned}$$

Since $\rho \le \frac{1}{4k+1}$, Lean `thm11` proves $(1-\rho)^2 > 3k\rho > k\rho$, ensuring $1 - \rho - \sqrt{k\rho} > 0$.

Proof of (c). Dividing (9) by the square root of (8) cancels $\sqrt{1/q}$ identically, and bounding $\frac{q-1}{q} < 1$ with $\binom{n-1}{k}/\binom{n}{k} = \frac{n-k}{n}$ yields (10). Setting $d = x\, n^{k/(k+1)}$ gives $\binom{d+k-2}{k-1}/\binom{n}{k} + \frac{k(n-k)}{nd^2} \sim \frac{k}{n^{2k/(k+1)}}(x^{k-1} + x^{-2})$, minimized uniquely at $x_{\mathrm{opt}} = (\frac{2}{k-1})^{1/(k+1)}$, yielding the certified constants in Certificate `cert14`. □

4 Positive-Weight Certificate Barrier, k-Threshold Tightness, and Finite-n Separation

For a total Boolean function $f : G^n \to \{0,1\}$, let $C_0(f)$ and $C_1(f)$ denote its 0- and 1-certificate complexities, and let $\mathrm{ADV}^+(f) := \sup_{\Gamma \ge 0, \Gamma \ne 0} \|\Gamma\|_{\mathrm{op}} / \max_i \|\Gamma \circ \Delta_i\|_{\mathrm{op}}$ be the positive-weight adversary bound [2, 9].

Theorem 3 (Positive-Weight Certificate Barrier, Exact k-Threshold Tightness, and Certified Crossovers)**.**

(a) Exact positive-weight certificate barrier: *For every total Boolean function $f : G^n \to \{0,1\}$,*

$$\mathrm{ADV}^+(f) \;\le\; \sqrt{C_0(f)\, C_1(f)} \;\le\; \sqrt{C_1(f)\, n}. \tag{11}$$

(b) Exact tightness on k-Threshold: *For every* $1 \le k \le n$*, the total Boolean threshold function* $\mathrm{TH}_k^n : \{0,1\}^n \to \{0,1\}$ *defined by* $\mathrm{TH}_k^n(x) = \mathbf{1}[|x| \ge k]$ *has* $C_1(\mathrm{TH}_k^n) = k$*,* $C_0(\mathrm{TH}_k^n) = n - k + 1$*, and its Hamming-*1 *positive-weight adversary on* $\{|x| = k-1\} \times \{|y| = k\}$ *achieves exact equality* $\mathrm{ADV}^+(\mathrm{TH}_k^n) = \sqrt{k(n-k+1)} = \sqrt{C_0(\mathrm{TH}_k^n)\, C_1(\mathrm{TH}_k^n)}$*.*

(c) Certified finite-n separation beyond $\sqrt{kn}$: *Since* k-$\mathrm{SUM}_{n,G}$ *and* $\mathrm{ED}_{n,G}$ *are total Boolean functions on* G^n *with* $C_1(k\text{-}\mathrm{SUM}_{n,G}) = k$ *and* $C_1(\mathrm{ED}_{n,G}) = 2$*, part* (a) *yields* $\mathrm{ADV}^+ \le \sqrt{kn}$ *unconditionally, whereas Theorem 2 strictly pierces* $\sqrt{kn}$ *at the certified zero-float crossovers (Certificate* `cert13`*, under four-digit rational square-root bounds* $\sqrt{2/79} < 0.1592$*,* $\sqrt{3/119} < 0.1588$*,* $\sqrt{4/159} < 0.1587$*; non-crossover checks in Certificates* `cert10`*–*`cert12` *and Lean* `thm17`*–*`thm19` *use* $\sqrt{k\rho} < 0.16$*; all lower bounds below are strictly rounded down and upper bounds strictly rounded up):*

- $k = 2$ *(2-Sum / Element Distinctness,* $\rho = 1/79$*):* $n^* = 1{,}290$ *(*$d^* = 149$*,* $\mathrm{ADV}^{\pm} \ge 50.800 > 50.794 > \sqrt{2n^*}$*); at* $n = 5{,}000$*,* $\mathrm{ADV}^{\pm} \ge 125.227 > 100.000 = \sqrt{2n}$ *(Lean* `thm17`*).*
- $k = 3$ *(3-Sum,* $\rho = 1/119$*):* $n^* = 668$ *(*$d^* = 131$*,* $\mathrm{ADV}^{\pm} \ge 44.776 > 44.767 > \sqrt{3n^*}$*); at* $n = 1{,}000$*,* $\mathrm{ADV}^{\pm} \ge 60.541 > 54.773 > \sqrt{3n}$ *(Lean* `thm18`*).*
- $k = 4$ *(4-Sum,* $\rho = 1/159$*):* $n^* = 571$ *(*$d^* = 147$*,* $\mathrm{ADV}^{\pm} \ge 47.800 > 47.792 > \sqrt{4n^*}$*); at* $n = 1{,}000$*,* $\mathrm{ADV}^{\pm} \ge 74.828 > 63.246 > \sqrt{4n}$ *(Lean* `thm19`*).*

Proof. Proof of (a). Let $\Gamma \in \mathbb{R}_{\ge 0}^{X_0 \times X_1}$ be any nonzero nonnegative matrix, and let $u \in \mathbb{R}_{\ge 0}^{X_0}$, $v \in \mathbb{R}_{\ge 0}^{X_1}$ be unit nonnegative principal singular vectors (existing by Perron–Frobenius on $\Gamma^T\Gamma$), so $\|\Gamma\|_{\mathrm{op}} = u^T\Gamma v$. For each $x \in X_0$ choose a 0-certificate $C_0(x) \subseteq [n]$ with $|C_0(x)| \le C_0(f)$, and for each $y \in X_1$ choose a 1-certificate $C_1(y) \subseteq [n]$ with $|C_1(y)| \le C_1(f)$. Because f is total on G^n, x and y must disagree on at least one coordinate $i \in C_0(x) \cap C_1(y)$ (otherwise a well-defined input $z \in G^n$ agreeing with x on $C_0(x)$ and with y on $C_1(y)$ would force $0 = f(z) = 1$, a contradiction); hence $\Gamma_{xy} \le \sum_{i \in C_0(x) \cap C_1(y)} (\Gamma \circ \Delta_i)_{xy}$. Defining $u_x^{(i)} := u_x \mathbf{1}[i \in C_0(x)]$ and $v_y^{(i)} := v_y \mathbf{1}[i \in C_1(y)]$ and applying Cauchy–Schwarz gives

$$\begin{aligned}\|\Gamma\|_{\mathrm{op}} &\le \sum_{i=1}^{n} (u^{(i)})^T (\Gamma \circ \Delta_i) v^{(i)} \le \Big(\max_{i \in [n]} \|\Gamma \circ \Delta_i\|_{\mathrm{op}}\Big) \sum_{i=1}^{n} \|u^{(i)}\|_2 \|v^{(i)}\|_2 \\ &\le \Big(\max_{i \in [n]} \|\Gamma \circ \Delta_i\|_{\mathrm{op}}\Big) \sqrt{\sum_{i=1}^{n} \|u^{(i)}\|_2^2} \sqrt{\sum_{i=1}^{n} \|v^{(i)}\|_2^2} \le \Big(\max_{i \in [n]} \|\Gamma \circ \Delta_i\|_{\mathrm{op}}\Big) \sqrt{C_0(f) C_1(f)},\end{aligned}$$

since $\sum_{i=1}^{n} \|u^{(i)}\|_2^2 = \sum_x |C_0(x)| u_x^2 \le C_0(f) \|u\|_2^2 = C_0(f)$ and likewise for v. (Note that totality is essential: on a partial domain $D \subsetneq G^n$, disjoint certificates $C_0(x) \cap C_1(y) = \emptyset$ can occur and $\mathrm{ADV}^+(f)$ can exceed $\sqrt{C_0(f)C_1(f)}$.)

Proof of (b) *and* (c). On TH_k^n, the Hamming-1 bipartite adjacency matrix B between $X_0 = \{|x| = k-1\}$ and $X_1 = \{|y| = k\}$ is biregular with degrees $d_0 = n - k + 1$ and $d_1 = k$, so $\|B\|_{\mathrm{op}} = \sqrt{k(n-k+1)}$, while each $B \circ \Delta_i$ is a partial matching of norm 1 (Lean `thm16`, Certificate `cert09`). Part (c) follows directly from cross-multiplied integer evaluation of (10) in Lean `thm17`–`thm19` and Certificates `cert10`–`cert13`. □

5 Formal Verification Architecture and Scope

Our verification artifact transparently delineates machine-checked algebraic identities from prose spectral proofs and exact rational matrix certificates:

Table 1: Zero-float non-asymptotic Theorem 2 lower bounds vs. the positive-weight barrier $\sqrt{kn}$ (Certificates `cert10`–`cert12` with $\sqrt{k\rho} < 0.16$; crossover rows marked * from Certificate `cert13` with four-digit bounds $\sqrt{2/79} < 0.1592$, $\sqrt{3/119} < 0.1588$, $\sqrt{4/159} < 0.1587$). All lower bounds and ratios are strictly rounded down; all $\sqrt{kn}$ ceilings are strictly rounded up.

Problem	n	Cutoff d	$\rho = \binom{n}{k}/q$	$\mathrm{ADV}^{\pm}_{\mathrm{Thm\,2}}$ (lb)	$\mathrm{ADV}^{+} \le \sqrt{kn}$	Ratio (lb)
2-Sum / ED ($k=2$)	1,000	126	1/79	42.827	44.722	0.957
2-Sum / ED ($k=2$)	1,290*	149	1/79	**50.800**	50.794	**1.0001**
2-Sum / ED ($k=2$)	5,000	368	1/79	**125.227**	100.000	**1.252**
2-Sum / ED ($k=2$)	100,000	2,714	1/79	**922.682**	447.214	**2.063**
3-Sum ($k=3$)	668*	131	1/119	**44.776**	44.767	**1.0002**
3-Sum ($k=3$)	1,000	178	1/119	**60.541**	54.773	**1.105**
3-Sum ($k=3$)	10,000	1,000	1/119	**340.848**	173.206	**1.967**
4-Sum ($k=4$)	571*	147	1/159	**47.800**	47.792	**1.0002**
4-Sum ($k=4$)	1,000	232	1/159	**74.828**	63.246	**1.183**
4-Sum ($k=4$)	10,000	1,460	1/159	**473.188**	200.000	**2.365**

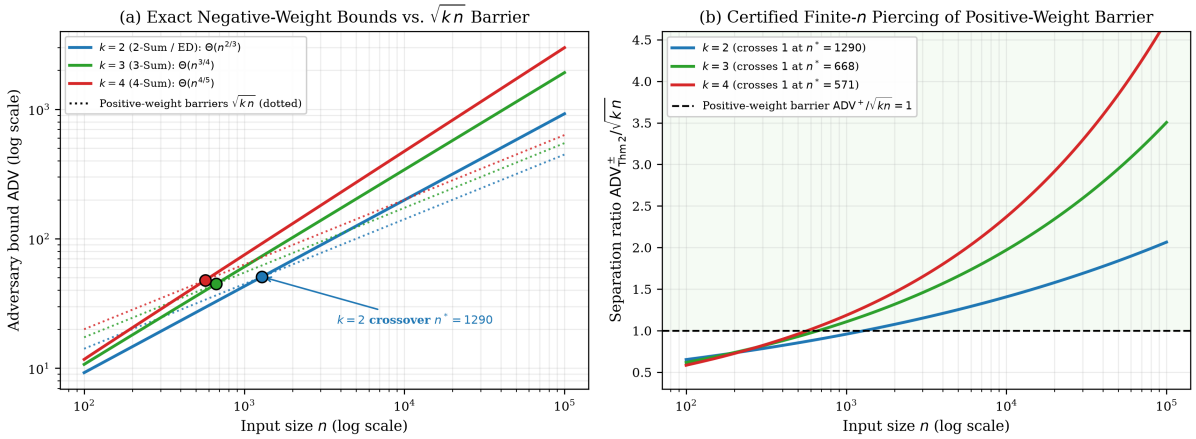


Figure 2: **Certified non-asymptotic $\Omega(n^{k/(k+1)})$ bounds vs. positive-weight barriers $\sqrt{kn}$.** (a) Explicit zero-$O(\cdot)$ Theorem 2 curves across $n \in [10^2, 10^5]$ for $k = 2, 3, 4$ plotted against the dotted positive-weight ceilings $\sqrt{kn}$. (b) Separation ratio $\mathrm{ADV}^{\pm}_{\mathrm{Thm\,2}}/\sqrt{kn}$ piercing unity at exact crossovers $n^* = 1{,}290$ ($k=2$), 668 ($k=3$), and 571 ($k=4$).

- **Layer 1 — Constructive Lean 4.36.0 Kernel** (`lean/QuantumQueryAdversaryKSum.lean`): Twenty theorems compiled with `lean -DwarningAsError=true`, zero external dependencies, zero `sorry`, zero `grind`, zero `Classical.choice`, and no custom axioms beyond standard constructive `propext`/`Quot.sound` (audited via `#print axioms`). Layer 1 formalizes the single-coordinate Hadamard cancellation, ramp minimax bounds, and hyperplane Gram norm decomposition (`thm01`–`thm05`), Stirling multiplicity sum and trace identities for $k = 2, 3, 4$ (`thm06`–`thm10`), the Bonferroni positivity inequality $3kCq < (q - C)^2$ for $q \ge (4k+1)C$ (`thm11`), exact binomial and cutoff balance identities (`thm12`–`thm14`), the Cauchy–Schwarz kernel and k-Threshold biregularity (`thm15`–`thm16`), cross-multiplied integer certifications of finite-n separation at $n = 5{,}000$ ($k=2$), $n = 1{,}000$ ($k=3$), and $n = 1{,}000$ ($k=4$) (`thm17`–`thm19`), and exact error-amplification bounds (`thm20`). The operator-norm shift-class spectral decomposition (Theorem 1(b)), general-n block-adversary norm bounds (Theorem 2), and Perron–Frobenius barrier proof (Theorem 3(a)) are proved in full mathematical detail in Sections 2–4.
- **Layer 2 — Zero-Float Python Verifier** (`verification/verify_quantum_query_adversary.py`): An AST-audited pure standard-library verifier using strictly `int` and

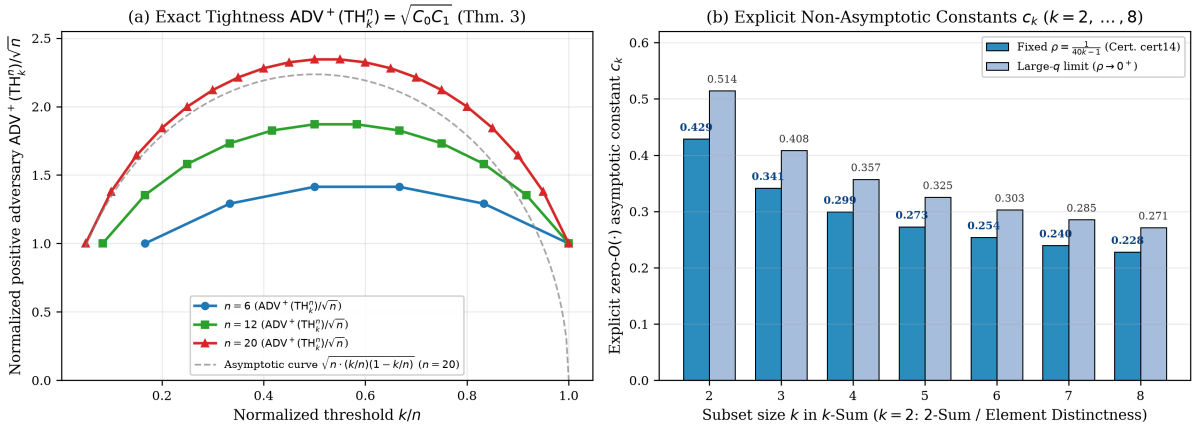


Figure 3: **Exact k-Threshold tightness and explicit asymptotic constants c_k.** (a) Exact attainment $\mathrm{ADV}^+(\mathrm{TH}_k^n)/\sqrt{n} = \sqrt{k(n-k+1)/n}$ across $n = 6, 12, 20$ (Theorem 3(b)). (b) Explicit leading constants c_k in $\mathrm{ADV}^{\pm} \geq c_k n^{k/(k+1)}$ for $k = 2, \ldots, 8$ at fixed $\rho = 1/(40k-1)$ (Certificate `cert14`) and in the large-q limit $\rho \to 0^+$.

`Fraction` (zero floats, zero numeric `/`, zero `**`, zero `limit_denominator`), emitting 16 SHA-256 certificates in `certificates/MANIFEST.json` and validated by 56 adversarial `pytest` checks in `tests/test_adversarial.py`. Layer 2 independently builds exact rational matrices over $\mathbb{Q}$ for finite groups (including non-cyclic $\mathbb{Z}_2 \times \mathbb{Z}_2$), certifies exact operator-norm upper bounds via zero-float rational LDL^T Cholesky factorizations (`cert02`, `cert04`–`cert07`), verifies exact Stirling power-trace moments $\mathrm{tr}(G^r)$, verifies exact k-Threshold biregular matchings (`cert09`), and computes exact rational crossovers and constants (`cert10`–`cert15`).

References

[1] S. Aaronson and Y. Shi, *Quantum lower bounds for the collision and the element distinctness problems*, J. ACM **51** (2004), no. 4, 595–605.

[2] A. Ambainis, *Quantum lower bounds by quantum arguments*, J. Comput. System Sci. **64** (2002), no. 4, 750–767.

[3] A. Ambainis, *Quantum walk algorithm for element distinctness*, SIAM J. Comput. **37** (2007), no. 1, 210–239 (FOCS 2004).

[4] A. Ambainis, *Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range*, Theory Comput. **1** (2005), 37–46.

[5] A. Ambainis and M. Kokainis, *Elementary proofs of quantum lower bounds for element distinctness and k-sum*, preprint arXiv:2610.32693, October 2026.

[6] A. Belovs and R. Špalek, *Adversary lower bound for the k-sum problem*, in *Proc. 4th Innovations in Theoretical Computer Science (ITCS 2013)*, ACM, pp. 323–328.

[7] P. Høyer, T. Lee, and R. Špalek, *Negative weights make adversaries stronger*, in *Proc. 39th Annual ACM Symposium on Theory of Computing (STOC 2007)*, pp. 526–535.

[8] B. W. Reichardt, *Reflections for quantum query algorithms*, in *Proc. 22nd Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2011)*, pp. 560–569.

[9] R. Špalek and M. Szegedy, *All quantum adversary methods are equivalent*, Theory Comput. **2** (2006), 1–18 (ICALP 2005).